

METHOD AND SYSTEM FOR TOKEN PROVISIONING AND PROCESSING

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This international application claims priority to U.S. Patent Application No. 62/721,128, filed on August 22, 2018, the disclosure of which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Entities often maintain accounts for users, whereby users may access a resource utilizing an associated account with the entity (e.g., a bank, a government organization, cloud services provider, etc.). In a banking example, the bank may function as an account issuer and issue a payment card (e.g., a debit card) to the user which allows the user to utilize payment credentials (e.g., primary account number (PAN), CVV2, etc.) associated with the account to obtain a good. In some cases, the user may use the payment card for cross-border transactions. For example, the user may obtain the card from a bank in their residence country (e.g., Canada) and then travel to another country (e.g., the United States (U.S.)) to execute a payment transaction.

[0003] Also, modern systems have been created to provision a communication device (e.g., a mobile phone) with access data (e.g., a token) that is associated with a user account to be later used in conducting a transaction. For example, continuing with the banking example, the mobile phone may be provisioned with access data associated with the user's bank account (e.g., a PAN, a payment token, etc.) which may allow the mobile phone to access the account to obtain a good. Once the mobile phone is provisioned with the access data, the user may, for example, use the mobile phone to conduct e-commerce transactions utilizing the payment account. In another example, the user may go to a merchant store and tap the mobile phone on an access device (e.g., a Point-of-Sale (POS) terminal) to conduct the transaction. In a non-banking example, a cloud services provider entity may issue credentials for a particular user that allow the user to access a file associated with their account on a remote file share in the cloud. The cloud services provider may provision the user's mobile phone with access

data (e.g., a token) corresponding to the user credentials with the cloud services provider, which enables the mobile phone to access the file on the remote file share in the cloud via the mobile phone.

[0004] However, transactions may often involve multiple entities that process transaction related data at various stages of the transaction processing pipeline. In these cases, interoperability between entities in the transaction pipeline is a significant challenge. For example, a bank in a particular country may issue a payment card that corresponds to a user account information (e.g., account number) that is formatted according to banking standards in that particular country. However, merchant stores and/or websites in another country may have an existing infrastructure (e.g., POS terminals, web servers) configured to conduct transactions with account numbers in a different format, which may present obstacles to conducting the transaction. In another example, software applications (e.g., a digital wallet) on the user's mobile phone may be configured to facilitate provisioning the mobile phone with access data based on receiving a user account number in a particular format, which may differ from the format of the account credentials issued by the issuer.

[0005] Embodiments of the invention are directed to methods and systems of improving interoperability between issuers and other entities involved in a transaction. Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

[0006] Embodiments of the invention are directed to secure token processing systems and methods.

[0007] One embodiment of the invention is directed to a method comprising: receiving, by a token provider computer, a token request message from a token requestor computer, the token request message comprising an initial access identifier; transmitting, by the token provider computer, the initial access identifier to a first authorization computer; receiving, by the token provider computer, an intermediate access identifier; transmitting, by the token provider computer and based at least in part on the intermediate access identifier, a token activation request message to a second authorization computer; receiving, by the token provider computer from the second authorization computer, a token activation response message from the second

authorization computer; and providing, by the token provider computer, a token to the token requestor.

[0008] Another embodiment of the invention can be directed to a token provider computer configured to perform the above described method.

[0009] Another embodiment of the invention is directed to a method comprising: receiving, by a first authorization computer, an initial access identifier from a token provider computer. The method then includes obtaining, by the first authorization computer, an intermediate access identifier based at least in part on the initial access identifier; and transmitting, by the first authorization computer, the intermediate access identifier to the token provider computer, wherein the token provider computer transmits, based at least in part on the intermediate access identifier, a token activation request message to a second authorization computer to authorize a token to be provisioned to a token requestor computer.

[0010] Another embodiment of the invention can be directed to a first authorization computer configured to perform the above described method.

[0011] Another embodiment of the invention is directed to a method comprising: receiving, by a processing computer, an authorization request message comprising a token; providing, by the processing computer, the token to a token provider computer in a transaction; receiving, by the processing computer, an intermediate access identifier associated with the token; modifying, by the processing computer, the authorization request message to include the intermediate access identifier; and transmitting, by the processing computer, the authorization request message including the intermediate access identifier to a first authorization computer, wherein the first authorization computer modifies the authorization request message to include an initial access identifier associated with the intermediate access identifier, and transmits the authorization request message with the initial access identifier to a second authorization computer to authorize the transaction.

[0012] Other embodiments of the invention can be directed to a processing computer configured to perform the above-noted method.

[0013] These and other embodiments of the invention are described in further detail below, with reference to the Figures and Detailed Description.

BRIEF DESCRIPTION OF THE DRAWINGS

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

[0015] FIG. 2 shows a block diagram of a token requestor computer of the system according to an embodiment of the invention.

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

[0017] FIG. 4 shows a block diagram of a first authorization computer of a system according to an embodiment of the invention.

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

[0019] FIG. 6 shows a block diagram of a system and a flow sequence illustrating a first provisioning process using push provisioning according to an embodiment of the invention .

[0020] FIG. 7 shows a block diagram of a system and a flow sequence illustrating a second provisioning process using manual provisioning according to an embodiment of the invention.

[0021] FIG. 8 shows block diagram of a system and a flow sequence illustrating use of a token according to an embodiment of the invention.

[0022] FIG. 9 shows a block diagram of a system illustrating use of a token according to an embodiment of the invention.

DETAILED DESCRIPTION

[0023] Embodiments of the invention provide for mechanisms for facilitating secure token provisioning to a token requestor computer (e.g., a communication device such as a mobile phone) for later use in a transaction. In one embodiment, a high-level provisioning process flow may proceed as follows. First, the token requestor computer may initiate a provisioning process by transmitting an initial access identifier (e.g., an International Bank Account Number (IBAN) obtained from the issuer bank) and a user identifier (e.g., user name, email address, etc.) to a token provider computer. Second, the token provider computer subsequently interacts with a first authorization computer

(e.g., an intermediary that is a trusted third-party proxy for the issuer) to obtain an intermediate access identifier (e.g., a virtual PAN) based on the initial access identifier and the user identifier. The first authorization computer may store a mapping between the initial access identifier and the intermediate access identifier for future use in processing a transaction. Third, based on receiving the intermediate access identifier from the first authorization computer, the token provider computer interacts with a second authorization computer (e.g., the issuer) to obtain a token activation approval. Fourth, the token provider computer then provides the activated token to the token requestor computer, which may be stored for future use. The token provider computer may store a mapping between the intermediate access identifier and the token for future use in processing a transaction.

[0024] In some embodiments, a token may be “push” provisioned to a token requestor computer via an issuer application (e.g., bank application) that initiates a provisioning request by “pushing” a payload including user credentials to an application executing on the token requestor computer (e.g., a digital wallet). In this case, the user may simply use the issuer application to select a digital wallet to be provisioned with a token, and no manual entry of credentials by the user is required. The token requestor computer may then initiate a provisioning process with a token provider computer as described above.

[0025] In other embodiments, a token may be “manually” provisioned to a token requestor computer, whereby the token requestor application executing on the token requestor computer directly receives input from a user (e.g., via keyboard entry), for example, including a user identifier and an initial access identifier. The token requestor computer may then initiate a provisioning process with a token provider computer as described above.

[0026] In some embodiments, after the token requestor computer has been provisioned with a token, the token requestor computer may use the token to conduct a transaction. In one embodiment, and using a payment transaction as a non-limiting example, a high-level transaction process flow may proceed as follows. First, a communication device (e.g., which may be the same token requestor computer that was previously provisioned with a token) may interact with an access device (e.g., tapping the phone against a merchant POS terminal) by transmitting the provisioned token to the access device. Second, the access device may transmit an authorization request message including the token to a transport computer (e.g., an acquirer computer

affiliated with the merchant access device). Third, the transport computer may transmit the authorization request message including the token to a processing computer (e.g., a server computer within a payment processing network such as VisaNet™). Fourth, the processing computer may then use the token to retrieve the intermediate access identifier (e.g., utilizing the mapping previously stored by the token provider computer during the provisioning process). The processing computer may then modify the authorization request message to include the intermediate access identifier. Fifth, the processing computer may transmit the modified authorization request message to the first authorization computer. Sixth, the first authorization computer may use the intermediate access identifier to retrieve the initial access identifier (e.g., utilizing the mapping previously stored by the first authorization computer during provisioning). The first authorization computer may then modify the authorization request message to include the initial access identifier. Seventh, the first authorization computer may send the modified authorization request message to the second authorization computer. Eighth, the second authorization computer may approve the transaction based at least in part on receiving the initial access identifier from the first authorization computer.

[0027] Embodiments of the invention provide for a number of technical advantages. In one non-limiting example, some initial access identifiers, such as IBANs, may be incompatible with existing token provisioning systems (e.g., which may require a PAN format). Accordingly, using conventional techniques, a user may be unable to provision their communication device (e.g., mobile phone) with a payment token based on the issued IBAN. In contrast, embodiments of the present invention utilize an intermediate access identifier to provide interoperability between issuers and other entities (e.g., a token provider service) within existing token provisioning systems. In this way, a user could provision their mobile phone with a payment token using an IBAN. Thus, for example, the user may be able to tap their token-provisioned mobile phone against a merchant access device to conduct a transaction. Additionally, the user may travel to another country (e.g., with different payment processing systems) and still be able to tap their token-provisioned mobile phone against a merchant access device to conduct a transaction. In yet another example, the user could conduct remote e-commerce transactions using a digital wallet on their mobile phone based on the token associated with the otherwise incompatible IBAN. Embodiments of the invention also provide for greater data security during the authorization process. For example, even if an intermediate access identifier may be compromised in a man-in-the-middle

attack, in some embodiments, it will be of little value as it may not be used to conduct transactions.

[0028] It should be understood that the technical advantages of the present invention are not only applicable to payment-based token provisioning systems. In another non-limiting example, a cloud services provider may issue credentials used to access files whereby the credentials may have a particular format according to the particular geographical region and/or organization associated with the user. A token provisioning system may be configured to only provision tokens for accessing files upon receiving credentials in a different format. Similar to as described above, embodiments of the present invention may utilize an intermediate access identifier to provide interoperability between cloud services provider issuer and the token provisioning system, such that, for example, a user with issued credentials in an otherwise incompatible format may nevertheless be able to provision their communication device with a token so they may access files in the cloud. This also may reduce the number of infrastructure updates required by a particular issuer (e.g., bank, cloud services provider, etc.) to be interoperable with multiple token provisioning systems, and thus enable more efficient token provisioning to a wider variety of users.

[0029] Before discussing embodiments of the invention, some descriptions of some terms may be useful.

[0030] A "communication device" may comprise any suitable electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. For example, a communication device may be a personal computer (PC). A "mobile communication device" may be an example of a "communication device" that can be easily transported. 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 communication 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 communication devices include wearable devices, such as smart watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. In some embodiments, a mobile communication device

can function as a payment device (e.g., a mobile communication device can store and be able to transmit payment credentials for a transaction).

[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 (e.g., an identifier for a payment account). 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. 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 payment devices include payment 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.

[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, as well as any object or document that can serve as confirmation. Examples of credentials include value credentials, identification cards, certified documents, access cards, passcodes and other login information, etc.

[0033] “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, and verification values such as CVV, dCVV, CVV2, dCVV2, and CVC3 values.

[0034] An “application” may be a computer program that is used for a specific purpose. Examples of applications may include a banking application, digital wallet application, cloud services application, ticketing application, etc.

[0035] A “digital wallet” can include an electronic device and/or application that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, payment credentials, bank account information, access data, tokens, 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, accessing secure data, 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.

[0036] “Access data” may include any suitable data that can be used to access a resource or create data that can access a resource. In some embodiments, access data may be account information for a payment account. Account information may include a PAN, IBAN, payment token, expiration date, verification values (e.g., CVV, CVV2, dCVV, dCVV2), etc. In other embodiments, access data may be data that can be used to activate account data. For example, in some cases, account information may be stored on a mobile device, but may not be activated until specific information is received by the mobile device. In other embodiments, access data could include data that can be used to access a location. Such access data may be ticket information for an event, data to access a building, transit ticket information, etc. In yet other embodiments, access data may include data used to obtain access to sensitive data. Examples of access data may include codes or other data that are needed by a server computer to grant access to the sensitive data.

[0037] An “initial access identifier” may include an identifier originally used by a user. The initial access identifier may be an original credential that is issued by an issuer. The initial access identifier may be in any suitable format, such as alphanumeric characters, alphabetic characters, numeric, text based, etc. In some cases, the initial access identifier may be associated with an account for a single user. In other cases, the initial access identifier may be associated with multiple users, for example, who may

share an account. Examples of an initial access identifier may include an original primary account number, or IBAN identifier. An IBAN identifier (also known as an “IBAN”) may include alphanumeric characters, instead of just numbers. Other examples may include a cloud services account number, mass transit account number, a building access identifier, etc. An initial access identifier may also include a combination of fields, for example, including an IBAN identifier and an email address or other user identifier.

[0038] An “intermediate access identifier” may include an identifier that can be used as an intermediary in a process. The intermediate access identifier may be in any suitable format, such as alphanumeric characters, alphabetic characters, numeric, text based, etc. In some cases, the intermediate access identifier may be associated with a single user or with multiple users, for example, who may share an account. Also, in some cases, the intermediate access identifier may be capable of being used to conduct a transaction. In other cases, the intermediate access identifier may be incapable of being used to conduct a transaction. For example, an intermediate access identifier may include a virtual PAN that is mapped to an IBAN initial access identifier. The virtual PAN may subsequently be mapped to a token. In some cases, the intermediate access identifier is 16, 18, or 19 digits long and may resemble a real PAN (primary account number), but may not be used to conduct a transaction.

[0039] 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.

[0040] A “payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a PAN or IBAN. For example, a payment token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, a payment token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a payment token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a payment token may be generated such that the recovery of the original PAN or other account identifier from the token value

may not be computationally derived. Further, in some 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.

[0041] “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 enhances transaction efficiency and security.

[0042] A “token issuer,” “token provider,” or “token service system” can include a system that services 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 credentials (e.g., 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 tokens to obtain the actual credentials (e.g., PANs). 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.

[0043] A “token domain” may indicate an area and/or circumstance in which a token can be used. Examples of token domains 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.

[0044] A “token expiry date” may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0045] A “token request message” may be an electronic message for requesting a token. A token request message may include information usable for identifying an account (e.g., payment account) or digital wallet, and/or information for generating a 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, an account access identifier, a user 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).

[0046] 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).

[0047] A “token requestor identifier” may include any characters, numerals, or other identifiers associated with an entity associated with a network token system. For example, a token requestor identifier may be associated with an entity that is registered with the network token system. In some embodiments, a unique token requestor identifier may be assigned for each domain for a token request associated with the same token requestor. For example, a token requestor identifier can identify a pairing

of a token requestor (e.g., a mobile device, a mobile wallet provider, etc.) with a token domain (e.g., e-commerce, contactless, etc.). A token requestor identifier may include any format or type of information. For example, in one embodiment, the token requestor identifier may include a numerical value such as a ten digit or an eleven digit number (e.g., 4678012345).

[0048] A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments.

[0049] A “user identifier” may include any characters, numerals, or other identifiers associated with a user associated with a network token system. For example, a user identifier may be associated with an entity that is registered with the network token system. For example, in one embodiment, the user identifier may be a customer ID or email address associated with an authorized user of a bank account that is maintained by a bank.

[0050] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of resource providers includes merchants, data providers, transit agencies, governmental entities, venue and dwelling operators, etc.

[0051] A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0052] 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”.

[0053] 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.

[0054] An “issuer” may typically refer to a business entity (e.g., a bank, cloud services provider) that maintains an account for a user. An issuer may also issue credentials (e.g., payment credentials) stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0055] 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), server computers, 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 mobile communication or payment 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.

[0056] 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 identifier, an initial access identifier, an intermediate access identifier, an expiration date, etc. An authorization request message may also comprise “transaction

information,” such as any information associated with a current transaction, such as, in the case of a payment transaction, 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.

[0057] 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. The authorization response message may also comprise additional data elements corresponding to “identification information” similar to as described above, which may be used to route the message to back to the requestor.

[0058] A “token presentment mode” may indicate a method through which a token is submitted for a transaction. Some non-limiting examples of the token presentment mode may include machine readable codes (e.g., QR™ code, bar code, etc.), mobile contactless modes (e.g., near-field communication (NFC) communication), e-commerce remote modes, e-commerce proximity modes, and any other suitable modes in which to submit a token.

[0059] A “server computer” may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0060] An “identification and verification (ID&V) method” may be used to ensure that the payment token is replacing a PAN that was legitimately being used by the token requestor. Examples of ID&V methods may include, but are not limited to, an account verification message, a risk score based on assessment of the primary account number (PAN) and use of one time password by the issuer or its agent to verify the account holder. Exemplary ID&V methods may be performed using information such as a user signature, a password, an offline or online personal identification number (PIN), an offline or online enciphered PIN, a combination of offline PIN and signature, a combination of offline enciphered PIN and signature, user biometrics (e.g. voice recognition, fingerprint matching, etc.), a pattern, a glyph, knowledge-based challenge-responses, hardware tokens (multiple solution options), one time passwords (OTPs) with limited use, software tokens, two-channel authentication processes (e.g., via phone), etc. Using the ID&V, a confidence level may be established with respect to the token to PAN binding.

[0061] A “token assurance level” may refer to an indicator or a value that allows the token service provider to indicate the confidence level of the token to PAN binding. The token assurance level may be determined by the token service provider based on the type of identification and verification (ID&V) performed and the entity that performed the ID&V. The token assurance level may be set when issuing the token. The token assurance level may be updated if additional ID&V is performed.

[0062] A “requested token assurance level” may refer to the token assurance level requested from the token service provider by the token requestor. The requested token assurance level may be included in a field of a token request message send by the requestor to the token service provider for the generation/issuance of the token.

[0063] An “assigned token assurance level” may refer to the actual (i.e., generated) value assigned by the token service provider to the token as the result of the identification and verification (ID&V) process performed by an entity within the tokenization ecosystem. The assigned token assurance level may be provided back to the token requestor in response to the token request message. The assigned token assurance level may be different than the requested token assurance level included in the token request message.

[0064] “Token attributes” may include any feature or information about a token. For example, token attributes may include information that can determine how a token

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

[0065] The token attributes may identify a type of token indicating how the token may be used. A payment token may include a high value token that can be used in place of a real account identifier (e.g., PAN) to generate original and/or subsequent transactions for a consumer account and/or card. Another token type may be a "static" or "dynamic" token type for static and dynamic tokens, respectively.

[0066] A "token requestor" may refer to an entity that is seeking to implement tokenization according to embodiments of the present invention. In some embodiments, the token requestor may initiate a request that a primary account number (PAN) or an initial access identifier be tokenized by submitting a token request message to the token service provider. According to various embodiments discussed herein, a token requestor may no longer need to store a PAN associated with a token once the requestor has received the token in response to a token request message. The requestor may be an application, a device, a process, or a system that is configured to perform actions associated with tokens. For example, a requestor can request registration with a network token system, request token generation, token activation, token de-activation, token exchange, other token lifecycle management related processes, and/or any other token related processes. A requestor may interface with a network token system through any suitable communication networks and/or protocols (e.g., using HTTPS, SOAP and/or an XML interface among others). Some non-limiting examples of token requestors may include, for example, a communication device of an authorized account holder, card-on-file merchants, acquirers, acquirer processors, and payment gateways acting on behalf of merchants, payment enablers (e.g., original

equipment manufacturers, mobile network operators, etc.), digital wallet providers, issuers, third party wallet providers, and/or payment processing networks. In some embodiments, a token requestor can request tokens for multiple domains and/or channels. A token requestor may be registered and identified uniquely by the token service provider within the tokenization ecosystem. During token requestor registration, the token service provider may formally process token requestor's application to participate in the token service system. The token service provider may collect information pertaining to the nature of the requestor and relevant use of tokens to validate and formally approve the token requestor and establish appropriate domain restriction controls. Successfully registered token requestors may be assigned a token requestor identifier that may also be entered and maintained within the token vault. Token requestors may be revoked or assigned new token requestor identifiers. This information may be subject to reporting and audit by the token service provider.

[0067] A "token request indicator" may refer to an indicator used to indicate that the message containing the indicator is related to a token request. The token request indicator may optionally be passed to the issuer as part of the Identification and Verification (ID&V) method to inform the issuer of the reason the account status check is being performed.

[0068] A "payment network" may refer to an electronic payment system used to accept, transmit, or process transactions made by payment devices for money, goods, or services. The payment network may transfer information and funds among issuers, acquirers, merchants, and payment device users.

[0069] FIG. 1 shows a block diagram of a system 100 for provisioning a token, according to an embodiment of the invention. The system 100 comprises a token requestor computer 102 which may be associated with a user 101, a token provider computer 104, a first authorization computer 106, and a second authorization computer 108.

[0070] The token requestor computer 102, the token provider 104 computer, the first authorization computer 106, and the second authorization computer 108 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.

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.

[0071] The token requestor computer 102 may be configured to receive input from the user 101 that instructs the token requestor computer 102 to initiate a token provisioning process with the token provider computer 104 to provision a token. In some embodiments, the token requestor computer 102 may be a communication device (e.g., a mobile phone, PC, etc.) of the user 101, which receives instructions from the user 101 to provision a communication device with a token. In some embodiments, and as described in embodiments below, the token requestor computer 102 and the communication device to be provisioned may be the same device. However, it should be understood that in other embodiments, they may be different devices. For example, the token requestor computer 102 may request a token on behalf of another communication device, and then, once the token is received, transmit the token to the other communication device to be stored.

[0072] In some embodiments, the token requestor computer 102 may execute a token requestor application, for example, a digital wallet, which may be responsible for requesting, storing, and/or managing one or more tokens received by the token provider computer 104. In some embodiments, the token requestor computer 102 may also execute an issuer application such as a mobile banking application, a cloud services application, a mass transit account application, etc. The issuer application may be responsible for sending a token request message to the token requestor application to initiate a provisioning process with the token provider computer 104. However, in other embodiments, the token requestor computer 102 may not include an issuer application.

[0073] The token provider computer 104 may be a computer affiliated with a token provider. The token provider computer 104 may facilitate requesting, determining (e.g., generating) and/or issuing tokens. For example, the token provider computer 104 may receive a token request message from the token requestor computer 102, and in turn facilitate a sequence of message exchanges with the first authorization computer 106 and the second authorization computer 108, after which the token provider

computer 104 provides the activated token to the token requestor computer 102. In some embodiments, the token provider computer 104 may also maintain a mapping of tokens to identifiers in a repository (e.g., a token vault). For example, the token provider computer 104 may maintain a mapping from tokens to intermediate access identifiers, initial access identifiers, etc. The token provider computer 104 may include or be in communication with a token vault where the generated tokens are stored. The token provider computer 104 may support token processing of transactions submitted using tokens by de-tokenizing the token to obtain an associated identifier (e.g., an intermediate access identifier) and then transmitting the associated identifier to the first authorization computer 106 for further processing.

[0074] The first authorization computer 106 may be a server computer that functions as an intermediary between the token provider computer 104 and the second authorization computer 108. In some embodiments, the first authorization computer 106 may be affiliated with a third-party entity (e.g., issuer processor) that functions as a trusted proxy for the issuer entity (e.g., a bank). In other embodiments, the first authorization computer 106 may be directly affiliated with the issuer entity. In some embodiments, the first authorization computer 106 and the token provider computer 104 are both operated by the token provider, and/or the functions of each may be performed by the same server computer. During the token provisioning process, the first authorization computer 106 may be responsible for obtaining (e.g., generating) an intermediate access identifier from the initial access identifier and maintaining a mapping between the initial access identifier and the intermediate access identifier. During the transaction processing phase, the first authorization computer 106 may receive the intermediate access identifier from the token provider computer 104, use the mapping to retrieve the initial access identifier, and then transmit the initial access identifier to the second authorization computer 108 for transaction authorization.

[0075] The second authorization computer 108 may be a server computer that is affiliated with the issuer. During the token provisioning phase, the second authorization computer 108 may be responsible for approving or else denying a token activation request that is received from the token provider computer 104 on behalf of the token requestor computer 102. During the transaction processing phase, the second authorization computer 108 may be responsible for authorizing or denying an authorization request received from the token provider computer 104 on behalf of the token requestor computer 102.

[0076] FIG. 2 shows a block diagram of a token requestor computer 102 of the system according to an embodiment of the invention. In some embodiments, the token requestor computer 102 may be a communication device (e.g., a mobile phone) that can be used to make payments or a device which can allow a user to gain access to a location. The exemplary token requestor computer 102 may comprise a computer readable medium 102-B and a memory 102-C that can be present within the body 102-J of the token requestor computer 102. The body 102-J may be in the form a plastic substrate, housing, or other structure. In some cases, the memory 102-C may be a secure element, and/or may also store information such as access data such as tokens, PANs, tickets, etc. Information in the memory 102-C may be transmitted by the token requestor computer 102 to another device using an antenna 102-D or contactless element 102-I.

[0077] The computer readable medium 102-B may comprises code, executable by the processor for implementing methods according to embodiments. The computer readable medium 102-B may contain an issuer application 110 and a token requestor application 120. The issuer application 110 can be used to “push” provision the token requestor computer 102 with a token by transmitting a token request message to the token requestor application 120. The issuer application also can provide functions provided by an issuer and may allow the token requestor computer 120 to communicate with an issuer computer (e.g., the second authorization computer 108). Examples of issuer applications can include banking applications, payment applications, merchant applications, transit applications, applications to access secure data, etc. The token requestor application 120 can allow the token requestor computer 102 to communicate with a token provider computer 104. Examples of token requestor applications can include various types of digital wallet applications (e.g., used for money transfer/ personal payments, mobile commerce, accessing secure data, etc.). The token requestor application 120 may be used to facilitate the enrollment process to provision a token onto the token requestor computer 102. It may also subsequently be used to conduct a transaction with a token without requiring a user 101 to enter an account number or present a physical card.

[0078] In some embodiments, the token requestor computer 102 may further include a contactless element 102-I, which is typically implemented in the form of a semiconductor chip (or other data storage element) with an associated wireless transfer (e.g., data transmission) element, such as an antenna. Data or control instructions that

are transmitted via a cellular network may be applied to the contactless element 102-I by means of a contactless element interface (not shown). Contactless element 102-I may be capable of transferring and receiving data using a short range wireless communication capability. Thus, the token requestor computer 102 may be capable of communicating and transferring data or control instructions via both cellular network (or any other suitable wireless network - e.g. the Internet or other data network) and short range communications.

[0079] The token requestor computer 102 may also include a processor 102-A (e.g., a microprocessor) for processing the functions of the token requestor computer 102 and a display 102-G to allow a user to view information. The token requestor computer 102 may further include input elements 102-E (e.g., a touchscreen, keyboard, touchpad, sensors such as biometric sensors, etc.), a speaker 102-H, and a microphone 102-F. The token requestor computer 102 may also include an antenna 102-D for wireless data transfer.

[0080] FIG. 3 shows a block diagram of a token provider computer 104 of a system according to an embodiment of the invention. FIG. 3 shows a token provider computer 104 and a token vault 130 coupled to the token provider computer 104.

[0081] The token vault 130 may store tokens and their associated credentials in a database. The token vault 130 may store data in a token record database such as an Oracle™ database. In some embodiments, the token vault 130 may store in the database a mapping between a token and one or more associated credentials (e.g., an intermediate access identifier and/or initial access identifier).

[0082] The token provider computer 104 may comprise a processor 104-A, which may be coupled to a system memory 104-B and an external communication interface 104-C. A computer readable medium 104-D may also be operatively coupled to the processor 104-A.

[0083] The computer readable medium 104-D may comprise a number of software modules including a communication module 104-D1, an encryption module 104-D2, a token provisioning module 104-D3, a validation module 104-D4, and an enrollment facilitation module 104-D5.

[0084] The communication module 104-D1 may comprise code that causes the processor 104-A to generate messages, forward messages, reformat messages, and/or otherwise communicate with other entities.

[0085] The encryption module 104-D2 may comprise code that includes any suitable encryption algorithms to encrypt data in embodiments of the invention. Suitable data encryption algorithms may include DES, tripe DES, AES, etc. It may also store encryption keys that can be used with such encryption algorithms. The encryption module 104-D2 may utilize symmetric or asymmetric encryption techniques to encrypt and/or verify data.

[0086] The token provisioning module 104-D3 may comprise code that causes the processor 104-A to provide tokens. For example, the token provisioning module 104-D3 may contain logic that causes the processor 104-A to generate a payment token and/or associate the payment token with a set of payment credentials (e.g., an intermediate access identifier). A token record may then be stored in a token record database of the token vault 130 indicating that the payment token is associated with (i.e., mapped to) a certain user or a certain set of payment credentials.

[0087] The validation module 104-D4 may comprise code that causes the processor 104-A to validate token requests before a token is provided. For example, validation module 104-D4 may contain logic that causes the processor 104-A 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 device (e.g., a token requestor computer 102), and/or by assessing risk associated with the requesting device.

[0088] The enrollment facilitation module 104-D5 may comprise code that causes the processor 104-A to transmit messages to one or more entities to facilitate a token provisioning process. For example, the enrollment facilitation module 104-D5 may contain logic that causes the processor 104-D5 to transmit a message containing an initial access identifier, received from the token requestor computer 102, to a first authorization computer 106. The enrollment facilitation module 104-D5 may also receive back from the first authorization computer 106 an intermediate access identifier. In some embodiments, the enrollment facilitation module 104-D5 may subsequently exchange messages with the token requestor computer 102 to receive input from the user 101 to continue the enrollment process (e.g., agreeing to terms and conditions). In some embodiments, based on receiving the intermediate access identifier from the first authorization computer 106 and/or input from the user 101 indicating agreement with the terms and conditions, the enrollment facilitation module 104-D5 may subsequently send a token activation request message to the second authorization computer 108,

and receive back a token activation response message indicating approval or else denial of the activation request. The enrollment facilitation module 104-D5 may then relay that indication back to the token requestor computer 102. Assuming that the second authorization computer 108 approved the activation request, the enrollment facilitation module 104-D5 may provide the token to the token requestor computer 102 and store a mapping of the token to one or more credentials (e.g., the intermediate access identifier) in the token vault 130.

[0089] FIG. 4 shows a block diagram of a first authorization computer 106 of a system according to an embodiment of the invention. The first authorization computer 106 may be coupled to a records database (not shown), whereby the first authorization computer 106 stores a mapping between identifiers. For example, the database may store a mapping between an initial access identifier and an intermediate access identifier. In some embodiments, the mapping may also include other associations, for example, a mapping between the initial access identifier and a user identifier that corresponds to the user 101. In some embodiments, for example, if the first authorization computer 106 and the token provider computer 104 operate as one entity, the records database of the first authorization computer 106 and the token record database of the token vault 130 may correspond to the same database. In that case, the token vault 130 may store a mapping between the token, the initial access identifier, the intermediate access identifier, and/or the user identifier.

[0090] The first authorization computer 106 may comprise a processor 106-A, which may be coupled to a system memory 106-B and an external communication interface 106-C. A computer readable medium 106-D may also be operatively coupled to the processor 106-A.

[0091] The computer readable medium 106-D may comprise a number of software modules including a communication module 106-D1, an encryption module 106-D2, an identifier conversion module 106-D3, a validation module 106-D4, and an authorization request translation module 106-D5.

[0092] The communication module 106-D1 may comprise code that causes the processor 106-A to generate messages, forward messages, reformat messages, and/or otherwise communicate with other entities.

[0093] The encryption module 106-D2 may comprise code that includes any suitable encryption algorithms to encrypt data in embodiments of the invention. Suitable

data encryption algorithms may include DES, tripe DES, AES, etc. It may also store encryption keys that can be used with such encryption algorithms. The encryption module 106-D2 may utilize symmetric or asymmetric encryption techniques to encrypt and/or verify data.

[0094] The identifier conversion module 106-D3 may comprise code that causes the processor 106-A to obtain (e.g., generate or retrieve from an existing pool in the records database) an intermediate access identifier based on receiving an initial access identifier. In some embodiments, for example in the case of retrieving from an existing pool, the identifier conversion module 106-D3 may maintain a record of intermediate access identifiers that are mapped to active initial access identifiers (e.g., non-expired or not deactivated) as well as non-active initial access identifiers. For example, the first authorization computer 106 may receive updates from a token provider computer 104 about what initial access identifiers are active. If, upon receiving a request for an intermediate access identifier based on receiving an initial access identifier, the identifier conversion module 106-D3 determines that an existing intermediate access identifier is currently mapped to a non-active initial access identifier, the identifier conversion module 106-D3 may provide the existing intermediate access identifier and re-map the intermediate access identifier to the initial access identifier received as input. In other embodiments, upon receiving a request, the identifier conversion module 106-D3 may generate a new intermediate access identifier and map it to the initial access identifier received as input. In some embodiments, the generated or updated intermediate access identifier and the corresponding mapping may be stored in the records database.

[0095] The validation module 106-D4 may comprise code that causes the processor 106-A to validate requests for an identifier (e.g., intermediate access identifier) before one is provided. For example, validation module 106-D4 may contain logic that causes the processor 106-A to confirm that a request message is authentic by decrypting a cryptogram included in the message, by confirming that the credentials (e.g., initial access identifier, user identifier, etc.) are authentic and associated with the requesting device (e.g., a token requestor computer 102, token provider computer 104), and/or by assessing risk associated with the requesting device. As described above, the first authorization computer 106 may be a trusted third-party proxy or otherwise associated with an issuer of the initial access identifier. Accordingly the first authorization computer 106 may also receive predefined rules from the issuer (e.g., the

second authorization computer 108) corresponding to whether a particular initial access identifier qualifies to be issued an intermediate access identifier. For example, a rule may determine that only initial access identifiers (e.g., IBANs) within a certain range of values may qualify to be mapped to an intermediate access identifier (e.g., a virtual PAN).

[0096] The authorization request translation module 106-D5 may comprise code that causes the processor 106-A to retrieve one identifier based on receiving another identifier during a transaction process phase. For example, the authorization request translation module 106-D5 may receive an authorization request message containing an intermediate access identifier (e.g., previously generated during the token provisioning phase by the identifier conversion module 106-D3). Based on the intermediate access identifier, the authorization request translation module 106-D5 may retrieve the associated initial access identifier from the records database. The authorization request translation module 106-D5 may then modify the authorization request message to include the initial access identifier and then transmit the modified message to another entity (e.g., the second authorization computer 108) for transaction authorization.

[0097] It should be understood that, as described herein, the mappings stored may be bidirectional. For example, a mapping between a token and an initial access identifier that is stored in the token vault 130 may be operable such that an initial access identifier may be used to retrieve a token, and vice versa. In another example, a mapping between an initial access identifier and an intermediate access identifier may be operable that an intermediate access identifier may be used to retrieve an initial access identifier, and vice versa. Accordingly, for example, if the first authorization computer 106 receives an authorization response message from the second authorization computer 108 that contains the initial access identifier, the first authorization computer 106 may use the initial access identifier to retrieve the associated intermediate access identifier and transmit it to another entity (e.g., a transaction processing computer) for further processing. In this way, messages may be correctly routed in both directions.

[0098] FIG. 5 shows a block diagram of a processing computer 150 of a system according to an embodiment of the invention. FIG. 5 shows a processing computer 150 and the token vault 130 coupled to the processing computer 150. It should be understood that, in some embodiments, the processing computer 150 and the token

provider computer 104 may be housed within the unit and/or be affiliated with the same token provisioning system.

[0099] The processing computer 150 may comprise a processor 150-A, which may be coupled to a system memory 150-B and an external communication interface 150-C. A computer readable medium 150-D may also be operatively coupled to the processor 150-A.

[0100] The computer readable medium 150-D may comprise a number of software modules including a communication module 150-D1, an encryption module 150-D2, a token exchange module 150-D3, a validation module 150-D4.

[0101] The communication module 150-D1 may comprise code that causes the processor 150-A to generate messages, forward messages, reformat messages, and/or otherwise communicate with other entities.

[0102] The encryption module 150-D2 may comprise code that includes any suitable encryption algorithms to encrypt data in embodiments of the invention. Suitable data encryption algorithms may include DES, tripe DES, AES, etc. It may also store encryption keys that can be used with such encryption algorithms. The encryption module 150-D2 may utilize symmetric or asymmetric encryption techniques to encrypt and/or verify data.

[0103] The token exchange module 150-D3 may comprise code that causes the processor 150-A to retrieve an identifier based on receiving a token (or vice versa). For example, in some embodiments, upon receiving a token within an authorization request message (e.g., from a token requestor computer 102), the token exchange module 150-D3 may retrieve an intermediate access identifier from the token vault 130. The intermediate access identifier may have been previously stored in the token vault 130 by the token provider computer 104 during a token provisioning process, whereby the token was mapped to the intermediate access identifier. Upon retrieving the identifier, the token exchange module 150-D3 may transmit the identifier to another entity. For example, token exchange module 150-D3 may modify the authorization request message to include the intermediate access identifier and then transmit the modified message to another entity (e.g., the first authorization computer 106) for further processing.

[0104] The validation module 150-D4 may comprise code that causes the processor 150-A to validate authorization request messages to proceed with a

transaction based on a token received as input. For example, validation module 150-D4 may contain logic that causes the processor 104-A to validate an authorization request message by decrypting a cryptogram included in the message, confirming that the token included within the message is authentic (e.g., associated with the requesting device), and/or by assessing risk associated with the requesting device. The validation module 150-D4 may also verify that the token attributes (e.g., a user identifier, token requestor identifier, token expiration date, frequency of use, etc.) conform to a set of predetermined rules. The predetermined rules may be determined by an entity (e.g., issuer bank) that has a trusted relationship with the processing computer 150.

[0105] FIGs. 6 and 7, respectively, show a block diagram of a system and a flow sequence illustrating different options for provisioning a token to a device according to embodiments of the invention: a first “push” provisioning process and a second “manual” provisioning process. In the “push” provisioning process of FIG. 6, an issuer application 110 (e.g., an banking application) may provide a user ID (e.g., a customer ID) and an initial access identifier (e.g., an IBAN) to a token requestor application 120 (“token requestor”) (e.g., a digital wallet). The token requestor 120 may then initiate a provisioning process with a token provider computer 104. In the “manual” provisioning process of FIG. 7, a user may provide a user ID and an initial access identifier directly to a token requestor 120. The token requestor 120 may then initiate a provisioning process with a token provider computer 104.

[0106] Turning to FIG. 6 in further detail, a block diagram 600 of a system and a flow sequence illustrating a “push” provisioning process is illustrated. FIG. 6 shows a token requestor computer 102 that may request a token from a token provider computer 104. In some embodiments, the token requestor computer 102 may be a mobile communication device (e.g., a mobile phone). Also, although FIG. 6 depicts the issuer application 110 and the token requestor application 120 as being on the same device, embodiments of the invention should not be construed to be so limiting. In any case, under the “push” provisioning method, the issuer application 110 may be in communication with the token requestor 120. The token provider computer 104 may be associated with (e.g., contain or communicate with) a token vault 130. The token vault 130 may be a database that stores tokens with their associated real credentials or intermediate access identifiers. The token provider computer 104 may be in communication with a first authorization computer 106 and a second authorization computer 108.

[0107] In the illustrated flow, in step S601, a user with a mobile communication device 102 may log in to the issuer application 110. In some embodiments, the issuer application 110 may correspond to a banking account issued by a bank. The bank may provide the user with one or more payment credentials that may be associated with the banking account and may be stored on the mobile communication device 102 by the issuer application 110. In some embodiments, the payment credentials may include multiple elements such as a user identifier (e.g., user name, user email address, user phone number, etc.), account number (e.g., PAN), expiration date, CVV2 value, etc. However, in some embodiments, the payment credentials may include less elements. For example, the payment credentials provided to the user and/or issuer application may include only an account number and a user identifier. In yet other embodiments, the payment credentials may include only an account number, for example, in a case where the account may be shared by multiple users. In this case, when the user 101 logs into the issuer application (e.g., by inputting the account number and a password), the user 101 may be dynamically provided with a user identifier by the bank. In some embodiments, the account number may be an IBAN, which may have a different format than a PAN. For example, the IBAN may contain an alphanumeric string characters (e.g., "DE89 3704 0044 0532 0130 00"), whereas a PAN may be only numeric characters (e.g., "1234 5678 8765 4321"). In some embodiments, the bank may also issue a payment card (e.g., debit card) that may be associated with the account and may having printed on the card one or more payment credentials (e.g., user name, account number, etc.).

[0108] In the flow sequence discussed below in reference to FIG. 6, the payment credentials stored by the issuer application 110 on the mobile communication device may include an account number that is an IBAN, which may correspond to an initial access identifier. The payment credentials also may include a user identifier that is either generated in advance of the user 101 logging in, or at the time the user logs in. Although, as discussed below, the user identifier is a separate data element from the initial access identifier, embodiments of the invention should not be construed to be so limiting. For example, in some embodiments, the initial access identifier may include multiple fields, including a user identifier. It should be noted that, in the example of FIG. 6, the payment credentials stored on the mobile communication device 102 (and/or printed on the payment card issued to the user 101) may not include certain fields, for example, a CVV2 value.

[0109] Continuing with step S601, the issuer application 110 may prompt the user 101 to select a particular application to be provisioned with a token. The user 101 may then select the token requestor application 120, which may be a digital wallet in this example. Upon selecting the token requestor 120, the issuer application 110 may encrypt a payload containing the initial access identifier and the user identifier, and transmit the payload to the token requestor 120.

[0110] In step S602, the token requestor 120 may transmit a token request message to be received by a token provider computer 104. The token request message may contain the initial access identifier and the user identifier to enroll the initial access identifier with the token provider computer 104. In some embodiments, the token requestor 120 may first decrypt the payload from the issuer application 110 to obtain the initial access identifier and the user identifier. In some embodiments, the token requestor 120 may include other information within the token request message, including for example, a token requestor identifier (e.g. mobile device 102 identifier, digital wallet provider identifier, token domain, etc.). In some embodiments, the token request message may be encrypted.

[0111] In step S604, the token provider computer 104 may then transmit the user identifier and the initial access identifier to the first authorization computer 106, for example, by invoking the enrollment facilitation module 104-D5. Prior to transmitting the user identifier and the initial access identifier, the token provider computer 104 may first decrypt and/or validate the token request message received by the token requestor 120. For example, the token provider computer 104 may invoke the validation module 104-D4 to validate a cryptogram from the token requestor 120 to authenticate the token requestor 120 and assess a level of risk with the request. In some embodiments, if the validation module 104-D4 determines that the initial access identifier and/or device 102 is not eligible, the token provider computer 104 may return an error to the token requestor 120.

[0112] Upon receiving the user identifier and the initial access identifier, the first authorization computer 106 may then obtain (e.g., generate or retrieve from an existing pool) an intermediate account identifier, for example, by invoking the identifier conversion module 106-D3. In some embodiments, the first authorization computer 106 may first invoke the validation module 104-D4 to verify that the initial access identifier is eligible, and if not, may return an error to the token provider computer 104. In some embodiments, assuming the validation is successful, the obtained intermediate account

identifier may correspond to an account identifier that is a different format (e.g., different fields and/or field formats) than the initial access identifier (e.g., a virtual PAN). More specifically, the intermediate account identifier may be a virtual debit card number, and it may have an expiration date and CVV2 value associated with it (e.g., in contrast with the initial access identifier, which may be an IBAN that does not have an associated CVV2 value). In some embodiments, the intermediate account identifier may be associated with an expiration date that is independent of an expiration date of the initial access identifier. In other embodiments, the expiration date may be the same expiration date as the initial access identifier (or derived from an expiration date of the initial access identifier using any suitable means). Upon generating the intermediate account identifier, the first authorization computer 106 may further invoke the identifier conversion module 106-D3 to store a mapping of the initial access identifier (and associated fields, e.g., the user identifier) and the intermediate access identifier (and associated fields, e.g., the expiration date) in a records database.

[0113] In some embodiments, the intermediate account identifier may be incapable of being used to directly conduct access transactions, but may be a conduit for provisioning a token to the communication device 102 and facilitating token-based transactions. For example, in some embodiments, the intermediate account identifier may be incapable of being used by a person to conduct a payment transaction. However, in other embodiments and as discussed below, the intermediate account identifier may be capable of being used to conduct a transaction, for example, at an e-commerce website.

[0114] In step S606, the first authorization computer 106 may transmit the intermediate access identifier to the token provider computer 104. In some embodiments, the first authorization computer 106 may also transmit an expiration date associated with the intermediate access identifier to the token provider computer 104.

[0115] In some embodiments, upon receiving the intermediate access identifier and expiration date from the first authorization computer 106, the token provider computer 104 may optionally conduct a message exchange process with the token requestor 120 (not shown in FIG. 6, but depicted in FIG. 7 steps S708 and S710). As depicted in FIG. 6, the token provider computer 104 does not send an enrollment confirmation message to the token requestor application 120 and instead automatically proceeds with continuing the enrollment process, as described below.

[0116] In step S608, based at least in part on receiving the intermediate access identifier in step S606, token provider computer 104 may transmit a token activation request message to the second authorization computer 108. In some embodiments, the token activation request message may include at least the initial access identifier. In some embodiments, any suitable information may be included in the message to enable the second authorization computer 108 to validate the token activation request message, including, but not limited to, the initial access identifier and/or the user identifier. In some embodiments, the second authorization computer 108 may utilize the initial access identifier to query the user 101 of the token requestor computer 102 and authenticate the user if desired using an ID&V process (e.g., with a one-time password or OTP).

[0117] In step S610, the second authorization computer 108 may respond with a token activation response message that is received by the token provider computer 104. The token activation response message may indicate whether the token activation request was approved (e.g., authorized) or denied.

[0118] In steps S612 and S614, assuming that the second authorization computer 108 agreed to provide the token to the token requestor 120, the token provider computer 104 may retrieve a token from the token vault 130, which may have been previously stored by the token provisioning module 104-D3. As described above, the mapping between the token and the intermediate access identifier may also be stored in the token vault 130 along with the associated token.

[0119] In step S616, the token provider computer 104 may provide (e.g., transmit) a token activation notification to the second authorization computer 108.

[0120] In step S618, the token provider computer 104 may provide (provision) the token to the token requestor 120. The token requestor 120 may store the token in a memory such as a secure memory 120C of the token requestor computer 102. The token may be permanent semi-permanent, or dynamic.

[0121] FIG. 7 shows a block diagram 700 of a system and a flow sequence illustrating a second provisioning process using manual provisioning according to an embodiment of the invention. Similar to as depicted in FIG. 6, FIG. 7 shows a token requestor computer 102 that may request a token from a token provider computer 104. In some embodiments, the token requestor computer 102 may be a mobile communication device (e.g., a mobile phone). However, in contrast with FIG. 6, a token

requestor application 120 ("token requestor") (e.g., a digital wallet) on the token provider computer 104 may be configured to receive input directly from the user 101 to initiate the provisioning process, instead of having an issuer application that pushes the initiation request and payload to the token requestor. Similar to FIG. 6, the token requestor 120 may be in communication with the token provider computer 104. The token provider computer 104 may be associated with (e.g., contain or communicate with) a token vault 130. The token vault 130 may be a database that stores tokens with their associated real credentials or intermediate access identifiers. The token provider computer 104 may be in communication with a first authorization computer 106 and a second authorization computer 108.

[0122] In the illustrated flow, in step S701 the token requestor 120 may receive input from the user 101 to initiate the provisioning process. For example, the user 101 may input via an input element 102-E (e.g., keyboard) credentials such as an IBAN and a user identifier (e.g., email address, user name, etc.). The token requestor 120 may receive the credentials using any suitable method. The credentials entered may be similar to the credentials that are encrypted within the payload that is transmitted from the issuer application 110 to the token requestor 120 in FIG. 6.

[0123] Steps S702-S706, respectively, may be substantially the same as steps S602-S606 of FIG. 6. The descriptions thereof are incorporated herein and need not be repeated.

[0124] In step S708, as described earlier as an optional step in reference to FIG. 6, the token provider computer 104 may send an enrollment confirmation message to the token requestor 120. In some embodiments, upon receiving the enrollment confirmation message, the token requestor 120 may prompt the user 101 to agree to terms and conditions of token provisioning. In some embodiments, the enrollment confirmation message sent to the token requestor 120 may contain the intermediate access identifier and expiration date, which may be stored on the token requestor computer 102 and presentable to the user 101. This may be done, for example, in the case where an issuer enables a user 101 to conduct transactions directly via the intermediate access identifier. However, in other embodiments, the intermediate access identifier is completely hidden from the user 101 (e.g., managed between the token provider computer 104 and the first authorization computer). In some embodiments, the enrollment confirmation message may also contain a reference number that is associated with the token enrollment session, which the token requestor

120 may return back to the token provider computer 104 to proceed with the enrollment process, as discussed in step S710, below.

[0125] In step S710, upon the user 101 agreeing to the terms and conditions and/or selecting other provisioning options presented by the token requestor 120, the token requestor 120 may transmit an enrollment confirmation reply message to the token provider computer 104 that contains the reference number and other suitable information, indicating that the user 101 will continue with the provisioning process. The token provider computer 104, upon receiving the reference number back from the token requestor computer 102, may use the reference number to look up and retrieve information from the token vault to proceed with the enrollment process (e.g., the initial access identifier, user identifier, etc.).

[0126] Steps S712-S722, respectively, may be substantially the same as steps S608-S618 of FIG. 6. The descriptions thereof are incorporated herein and need not be repeated.

[0127] FIG. 8 shows block diagram 800 of a system and a flow sequence illustrating use of a token after it has been provisioned to a user's communication device, according to an embodiment of the invention. FIG. 8 shows a system including a communication device 102 of a user 101, an access device 820 (e.g., POS terminal), a transport computer 840 (e.g., an acquirer computer), a processing computer 150 (e.g., in a payment processing network such as VisaNet), a first authorization computer 106, and a second authorization computer 108, all in communication with each other. A token vault 130 may be in communication with the processing computer 150.

[0128] Prior to step S802, the communication device 102 may be provisioned with a token as described above in reference to FIGs. 6 and 7. In step S802, the communication device 102 can interact with the access device 820 according to any suitable token presentment mode (e.g., NFC communication). In other embodiments, for example an e-commerce transaction, the communication device 102 may submit the token over the Internet to a website associated with the access device 820. In the process, the access device 820 may receive other associated with the token information (e.g., a token expiration date, other token attributes).

[0129] In step S804, an authorization request message comprising the token may be generated by the access device 820, and then transmitted to the transport computer 840.

[0130] In step S806, the transport computer 840 may transmit the authorization request message including the token to be received by the processing computer 150. The processing server computer 150 may be in a payment processing network. The payment processing network may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network may use any suitable wired or wireless network, including the Internet.

[0131] In step S808, the processing computer 150 may validate the authorization request message by executing the validation module 150-D4. Upon a successful validation, the processing computer 150 may invoke the token exchange module 150-D3, which may provide the token to the token vault 130 (e.g., via the token provider computer 104).

[0132] In step S810, the token exchange module 150-D3 may, in turn, retrieve (e.g., receive) the intermediate access identifier associated with the token from the token vault 130.

[0133] In step S812, the processing computer 150 may provide (e.g., transmit) the intermediate access identifier to the first authorization computer 106. In some embodiments, the token exchange module 150-D3 may modify the authorization request message to include the intermediate access identifier and then transmit the modified authorization request message to the first authorization computer 106 for further processing.

[0134] In step S814, the first authorization computer 106 may retrieve the initial access identifier based on the intermediate access identifier received from the processing computer 150. In some embodiments, the first authorization computer 106 may execute the authorization request translation module 106-D5 to translate (e.g., replace, or additionally include) the intermediate access identifier with the initial access identifier in the modified authorization request message. The first authorization

computer 106 may then transmit the modified message including the initial access identifier to the second authorization computer 108 for authorizing the transaction.

[0135] If approved (e.g., authorized), the second authorization computer 108 may transmit an authorization response message back to the access device 820 via the transport computer 840, the processing computer 150, and the first authorization computer 106 (step sequence not shown in FIG. 8). In some embodiments, the authorization response message may be routed back to the access device 820 based on the initial access identifier, the intermediate access identifier, and/or the token. For example, upon the first authorization computer 106 receiving the authorization response message containing the initial access identifier, the first authorization computer 240 may switch the initial access identifier for the intermediate access identifier, and then transmit the modified authorization response message to the processing computer 150. The processing computer 150 may, in turn, switch the intermediate access identifier for the token in the authorization response message (e.g., retrieving the token from the token vault 130 based on the mapping stored within the token vault 130). The processing computer 150 may then transmit the authorization response message to the transport computer 840 based on token attributes and other suitable information that was originally received in the authorization request message in step S806. The authorization response message may be similarly routed from the transport computer 840 to the access device 820 and/or mobile device 102.

[0136] In some embodiments, the second authorization computer 108, the first authorization computer 106, the processing computer 150, and the transport computer 840 may perform a settlement process to settle the transaction.

[0137] FIG. 9 shows a block diagram 900 of a system illustrating use of a token according to an embodiment of the invention. FIG. 9 shows a system including a communication device 102 of a user 101, an access device 920 (e.g., a gateway server), and a cloud services file server 930. The access device 920 may be in further communication with other intermediary computers between the access device 920 and the file server 930 (not shown), similar to as depicted in FIG. 8 (e.g., a processing computer 150, first authorization computer 106, second authorization computer 150, token vault 130).

[0138] In FIG. 9, the mobile device 102 may be provisioned with a token as described above in reference to FIGs. 6 and 7. The mobile device 102 may interact with

the access device 920 according to any suitable token presentment mode (e.g., over the Internet). In the process, the access device 920 may receive the token and other information (e.g., an expiration date). The access device 920 may then proceed with a series of steps to request authorization, on behalf of the user 101, to access a remote file on the file server 920. In some embodiments, the steps may be substantially similar to steps S804-S814 of FIG. 8.

[0139] 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.

[0140] The above description is illustrative and is not restrictive. Many variations of the invention may become apparent to those skilled in the art upon review of the disclosure. The scope of the invention can, therefore, be determined not with reference to the above description, but instead can be determined with reference to the pending claims along with their full scope or equivalents.

[0141] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0142] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0143] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A method for facilitating provisioning of a token to a token requestor computer, the method comprising:

receiving, by a token provider computer, a token request message from a token requestor computer, the token request message comprising an initial access identifier;

transmitting, by the token provider computer, the initial access identifier to a first authorization computer;

receiving, by the token provider computer, an intermediate access identifier from the first authorization computer, the intermediate access identifier having a different format than the initial access identifier;

transmitting, by the token provider computer and based at least in part on the intermediate access identifier, a token activation request message to a second authorization computer;

receiving, by the token provider computer, a token activation response message from the second authorization computer indicating whether a token activation request was approved or denied; and

in a case that the token activation request was approved by the second authorization computer, retrieving, from a token vault of the token provider computer, a token;

storing, by the token provider computer, a mapping between the intermediate access identifier and the token, based on the token activation response message; and

providing, by the token provider computer, the token to the token requestor computer.

2. The method of claim 1, wherein the initial access identifier comprises an alphanumeric value that corresponds to an account identifier of an account.

3. The method of claim 2, wherein transmitting the initial access identifier further comprises transmitting a user identifier of an authorized user that is associated with the account.

4. The method of claim 1, wherein the intermediate access identifier comprises a virtual primary account number.
5. The method of claim 4, wherein the virtual primary account number is not operable for being used to directly conduct a transaction.
6. The method of claim 1, wherein providing the token to the token requestor computer further comprises retrieving the token from the token vault.
7. The method of claim 1, wherein the provided token is operable to be stored by the token requestor computer for future use in a transaction.
8. The method of claim 1, wherein the token provider computer provides the token to the token requestor computer based at least in part on a successful result of an identification and verification process.
9. A token provider computer comprising:
 - a processor; and
 - a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method according to any of the preceding claims.
10. A method for facilitating provisioning of a token to a token requestor computer, the method comprising:
 - receiving, by a first authorization computer, an initial access identifier from a token provider computer;
 - obtaining, by the first authorization computer, an intermediate access identifier based at least in part on the initial access identifier, the intermediate access identifier having a different format than the initial access identifier;
 - storing, by the first authorization computer, a mapping between the initial access identifier and the intermediate access identifier; and
 - transmitting, by the first authorization computer, the intermediate access identifier to the token provider computer, wherein the token provider computer transmits, based at least in part on the intermediate access identifier, a token activation request message to a second authorization computer to authorize a token to be provisioned to a token requestor computer.

11. The method of claim 10, wherein the initial access identifier comprises an alphanumeric value that corresponds to an account identifier of an account.

12. The method of claim 11, wherein receiving the initial access identifier further comprises receiving a user identifier of an authorized user that is associated with the account.

13. The method of claim 12, wherein obtaining the intermediate access identifier comprises generating a virtual primary account number that is associated with the authorized user and the account.

14. The method of claim 12, further comprising:
storing, by the first authorization computer, a mapping between the user identifier, the initial access identifier, and the intermediate access identifier.

15. The method of claim 10, wherein the intermediate access identifier comprises a virtual primary account number.

16. The method of claim 10, wherein the intermediate access identifier is associated with an expiration date and/or a CVV2 value.

17. The method of claim 16, wherein the expiration date does not match a second expiration date that is associated with the initial access identifier.

18. A system comprising:
a processor; and
a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method according to any of claims 10-17.

19. A method for facilitating provisioning of a token to a token requestor computer, the method comprising:
receiving, by a processing computer, an authorization request message comprising a token;
providing, by the processing computer, the token to a token provider computer in a transaction;

receiving, by the processing computer, an intermediate access identifier associated with the token;

modifying, by the processing computer, the authorization request message to include the intermediate access identifier; and

transmitting, by the processing computer, the authorization request message including the intermediate access identifier to a first authorization computer, wherein the first authorization computer modifies the authorization request message to include an initial access identifier associated with the intermediate access identifier, stores a mapping between the initial access identifier and the intermediate access identifier, and transmits the authorization request message with the initial access identifier to a second authorization computer to authorize the transaction, wherein the intermediate access identifier has a different format than the initial access identifier.

20. A system comprising:

a processor; and

a non-transitory computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method according to claim 19.