

CLOUD TOKEN PROVISIONING OF MULTIPLE TOKENS

5 CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a PCT application claiming priority to U.S. Provisional Application No. 62/767,111, filed on November 14, 2018, which is herein incorporated by reference in its entirety.

BACKGROUND OF THE INVENTION

10 **[0002]** Users can utilize tokens as substitutes for credentials in order to gain access to a service or product. During a transaction, a token on a mobile device can be exchanged for a real credential (e.g. a primary account number (PAN) or some other payment information) that can be used in a transaction authorization process. Using tokens ensures greater security of sensitive information by eliminating any real
15 credentials from the mobile device.

[0003] In some processes, a user initially receives a token by sending a provisioning request from a mobile device. The token is bound to the mobile device and can be stored either within a secure element in the hardware of the mobile device or in the software where the security of the token can be ensured through the
20 use of encryption.

[0004] However, binding a token to a single mobile device has limitations. For example, if a user wishes to exchange a current mobile device for a new mobile device, the user must repeat the provisioning process for the new mobile device by providing a PAN or some other credential to obtain a new token. The token on the
25 user's previous mobile device is subsequently lost and cannot be transferred or used by the new mobile device.

[0005] Furthermore, a token cannot be shared by more than one device through this method. Any alternate mobile device(s) owned by a user requires a separate provisioning request, wherein a different token is generated for each individual
30 mobile device. Since the credentials (e.g., a PAN) the user provides can be assumed to remain the same, these subsequent provisioning requests are generally redundant and a waste of computing resources.

[0006] Embodiments of the invention are directed to addressing these and other problems, individually and collectively.

BRIEF SUMMARY

[0007] Embodiments of the invention include provisioning multiple access tokens in response to a single token request message. In one embodiment, a method includes receiving, by a token requestor computer, an access credential from a mobile device operated by a user and transmitting the access credential to a token service computer. In response to receiving the access credential, the method also includes transmitting, by the token service computer, an authorization request message to an authorizing entity computer in order to verify credential eligibility. Upon receiving a positive authorization response message from the authorizing entity computer, the method additionally includes obtaining, by the token service computer, at least two or more tokens, wherein at least one token can be associated with the mobile device and at least one token can be associated with a cloud server computer. The generated tokens are transmitted within a token response message to the token requestor computer.

[0008] Another embodiment of the invention is directed to a method comprising: receiving, by a token service computer, a token request message, the token request message being originated from a token requestor computer; determining, by the token service computer, two or more access tokens based upon a single credential; and transmitting, by the token service computer, the two or more access tokens to the token requestor computer in a token response message.

[0009] Another embodiment of the invention is directed to a token service computer comprising: a processor; and a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor to implement a method comprising: receiving a token request message, the token request message being originated from a token requestor computer; determining two or more access tokens based upon a single credential; and transmitting the two or more access tokens to the token requestor computer in a token response message.

[0010] Another embodiment of the invention is directed to a method comprising: receiving, by a token requestor computer from a communication device, a single credential; transmitting, by the token requestor computer, a token request message

comprising the single credential to a token service computer; receiving, by the token requestor computer from the token service computer, a token response message comprising the two or more access tokens including a first access token and a second access token; transmitting, by the token requestor computer, the first access token to the communication device; and transmitting, by the token requestor computer, the second access token to a cloud server computer

[0011] Another embodiment of the invention is directed to a token requestor computer comprising: a processor; and a non-transitory computer readable medium, the non-transitory computer readable medium comprising code, executable by the processor, for implementing a method comprising: receiving, from a communication device, a single credential; transmitting the single credential to a token service computer; receiving, from the token service computer, two or more access tokens including a first access token and a second access token; transmitting the first access token to the communication device; and transmitting the second access token to a cloud server computer

[0012] Further details regarding embodiments of the invention can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] FIG. 1 shows a system and method for provisioning multiple tokens.

[0014] FIG. 2 shows a swim lane diagram illustrating a method for the retrieval and use of a device bound token, according to one embodiment of the invention.

[0015] FIG. 3 shows a swim lane diagram illustrating the retrieval and use of a cloud token, according to some embodiments of the invention.

[0016] FIG. 4 shows a system for using a cloud token to gain access to a secure location, according to some embodiments of the invention.

[0017] FIG. 5 shows a block diagram of a mobile communication device, in accordance with some embodiments of the invention.

[0018] FIG. 6 shows a block diagram of a token service computer, in accordance with some embodiments of the invention.

[0019] FIG. 7 shows a block diagram of a token requestor computer, in accordance with some embodiments of the invention.

DETAILED DESCRIPTION OF THE INVENTION

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

[0021] A “user device” may be any suitable device that can be used by a user. User devices may be in any suitable form. Some examples of user devices include cellular phones, PDAs, personal computers (PCs), tablet computers, and the like. In some embodiments, where a user device is a mobile device, the mobile device may include a display, a memory, a processor, a computer-readable medium, and any other suitable component.

[0022] A “mobile device” may comprise any suitable electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. A mobile communication device may communicate using a mobile phone (wireless) network, wireless data network (e.g. 3G, 4G or similar networks), Wi-Fi, Bluetooth, Bluetooth Low Energy (BLE), Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g. cellular phones), PDAs, tablet computers, net books, laptop computers, wearable devices (e.g., watches), vehicles such as automobiles and motorcycles, personal music players, hand-held specialized readers, etc. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem – both devices taken together may be considered a single mobile device).

[0023] A “resource provider” can be any suitable entity that provides resources (e.g., goods, services, access to secure data, access to locations, or the like) during a transaction. For example, a resource providing entity can be a merchant, a venue operator, a building owner, a governmental entity, etc. A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0024] An "application" may be a computer program that is used for a specific purpose.

[0025] "Authentication data" may include any data suitable for verifying something. Authentication data may include data authenticating a user or a mobile device.

5 Authentication data may be obtained from a user or a device that is operated by the user. Examples of authentication data obtained from a user may include PINs (personal identification numbers), biometric data, passwords, etc. Examples of authentication data that may be obtained from a device may be include device serial numbers, hardware secure element identifiers, device fingerprints, phone numbers,
10 IMEI numbers, etc.

[0026] "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 (primary account number), payment token, expiration date,
15 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.
20 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.

25 **[0027]** An "access request" may include a request for access to a resource. The resource may be a physical resource (e.g., good), digital resources (e.g., electronic document, electronic data, etc.), or services. In some cases, an access request may be submitted by transmission of an access request message that includes access request data. Typically a device associated with a requestor may transmit the
30 access request message to a device associated with a resource provider.

[0028] "Access request data" may include any information surrounding or related to an access request. Access request data may include access data. Access request

data may include information useful for processing and/or verifying the access request. For example, access request data may include details associated with entities (e.g., resource provider computer, processor server computer, authorization computer, etc.) involved in processing the access request, such as entity identifiers (e.g., name, etc.), location information associated with the entities, and information indicating the type of entity (e.g., category code). Exemplary access request data may include information indicating an access request amount, an access request location, resources received (e.g., products, documents, etc.), information about the resources received (e.g., size, amount, type, etc.), resource providing entity data (e.g., resource provider data, document owner data, etc.), user data, date and time of an access request, a method utilized for conducting the access request (e.g., contact, contactless, etc.), and other relevant information. Access request data may also be known as access request information, transaction data, transaction information, or the like.

[0029] An “access device” may be any suitable device for providing access to an external computer system. An access device may be in any suitable form. Some examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites, 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 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 mobile device.

[0030] An “electronic wallet” or “digital wallet” can include an electronic device or service that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, credentials, bank account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as, but not limited to, eCommerce transactions, social

network transactions, money transfer/ personal payment transactions, mobile commerce transactions, proximity payment transactions, gaming transactions, etc. 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.

[0031] 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. Other examples of credentials include PANs (primary account numbers), PII (personal identifiable information) such as name, address, and phone number, and the like.

[0032] An “authorizing entity” may be an entity that authorizes a request, typically using an authorizing computer to do so. An authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An “issuer” may typically include a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the user.

[0033] A “service provider” may be an entity that can provide a resource such as goods, services, information, and/or access typically through a service provider computer. Examples of a service provider includes merchants, digital wallets, payment processors, etc.

[0034] A “user” may include an individual or a computational device. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. In some embodiments, the user may be a cardholder, account holder, or consumer.

[0035] A “token” may be a substitute value for a credential. An “access token” may be a token used to access something. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include access tokens (e.g., payment tokens), personal identification tokens, etc.

[0036] A "payment token" may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be computationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token. In some embodiments, access tokens in embodiments can be 16, 18, or 19 characters long.

[0037] A "key" may include a piece of information that is used in a cryptographic algorithm to transform data into another representation. A cryptographic algorithm can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc.

[0038] An "authorization request message" may be an electronic message that requests authorization to do something. In some embodiments, an authorization request message is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a 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), an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0039] An “authorization response message” may be an electronic message reply to an authorization request message. In some embodiments, an authorization response message is generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g., POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0040] A “server computer” is typically 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.

[0041] A “processor” may include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include CPU comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a

microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s).

[0042] A "memory" may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0043] A "token service computer" may be any suitable device that handles, supervises, or manages token generation or token processing. A token service computer may be in communication with a token requestor computer, a processing network computer, an authorizing entity computer, or the like.

[0044] A "token request message" may be an electronic message that requests a token. In some embodiments, a token request message may comprise a token requestor identifier, and an address to a token service computer.

[0045] A "token response message" may be an electronic message reply to a token request message. A token response message may include at least one or more tokens, an address of the token requestor device requesting the token, etc..

[0046] A "cloud server computer" may be a remotely located server computer that comprises information or data that a user can access from at least one or more devices. A cloud server computer may either be a separate device or included within a larger device, and may be connected to a user device(s) through a network interface(e.g., to connect to a separate device over the internet) or any suitable communication interface.

[0047] A "requestor" may be an application, a device, or a system that is configured to perform actions associated with tokens. For example, a requestor can request registration with a network token system, request token generation, token activation, token de-activation, token exchange, other token life-cycle management related processes, and/or any other token related processes. A requestor may interface with a network token system through any suitable communication networks and/or

protocols (e.g., using HTTPS, simple object access protocol (SOAP) and/or an extensible markup language (XML) interface). Some non-limiting examples of a requestor may include third party wallet providers, issuers, acquirers, merchants, and/or payment processing networks. A requestor may be referred to as a token requestor when requesting generation of a new token or requesting a new use of an existing token from a network token system. In some embodiments, a token requestor can request tokens for multiple domains and/or channels. Token requestors may include, for example, card-on-file merchants, acquirers, acquirer processors, and payment gateways acting on behalf of merchants, payment enables (e.g., original equipment manufacturers, mobile network operators, etc.), digital wallet providers, and/or card issuers.

[0048] A “token requestor identifier” (or token requestor computer 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).

[0049] In some embodiments, a token requestor identifier may uniquely identify the pairing of a token requestor with a token domain. As such, in some embodiments, if a token requestor may request tokens for multiple domains, the token requestor may have multiple token requestor identifiers, one for each domain.

[0050] For example, in some embodiments, a token requestor identifier may include an 11 digit numeric value assigned by the network token system and the token requestor identifier may be unique within the token registry for each entity (and each domain). For instance, the token requestor identifier may include a code for a token service provider (e.g., first 3 digits) such as the network token system and the

remaining digits (e.g., last 8 digits) may be assigned by the token service provider for each requesting entity (e.g., mobile wallet provider) and for each token domain (e.g., contactless, e-commerce, etc.).

[0051] Today, a mobile wallet on a communication device such as a mobile phone can provide a device bound token to a merchant application on the communication device. It can be adapted for use in both one-off and recurring use cases. The merchant application may then communicate with an application server associated with the merchant application to initiate a payment transaction using the token. If a user deletes the device bound token on their mobile wallet, any recurring transactions submitted by the merchant application will fail. Embodiments of the invention address this and other problems.

[0052] Embodiments of the invention can provide two or more access tokens to token requestor (e.g., a service provider computer such as a mobile wallet computer). The two or more access tokens may include, without limitation, a device bound token, and a cloud token. A “cloud token” may be token that is stored on a remote server computer and is used for remote access or remote transactions. In embodiments, a token requestor computer that is a mobile wallet server computer associated with a mobile wallet application on a communication device can request multiple tokens from a token service computer. The multiple tokens may comprise at least a cloud token and a device bound token. The token service computer can provide the cloud token to a cloud server computer operated by a merchant, via the token requestor computer, so that recurring transactions can be conducted on behalf of a user using the cloud token.

[0053] The cloud token can be based on the same PAN as a device token that is stored on the communication device, but is independent of the device token. A “device token” or “device bound token” may be a token that is used by the communication device which stores it in a proximity or contact transaction. Thus, while the cloud token is used to conduct remote transactions such as e-commerce transactions, a device token is used to conduct a transaction at a physical point of sale. If the device token is deleted (on purpose or accidentally), the cloud token is unaffected and recurring merchant transactions will continue to be processed. Embodiments avoid the need for the token requestor computer to make multiple calls

to a token service computer to obtain multiple tokens from the token service computer.

[0054] FIG. 1 shows a system 100 according to one embodiment of the present invention. The system includes a mobile communication device 110 including a mobile wallet application, a token requestor computer 120 which may be operated by a token requestor such as a mobile wallet application server computer, a token service computer 130, an authorizing entity computer 140 such as an issuer computer operated by an issuer, and a cloud server computer 150. The cloud server computer 150 could be operated by a resource provider such as a merchant, or a mobile wallet provider. Each of the components shown in FIG. 1 may be in operative communication with each other.

[0055] The components in the system in FIG. 1 can 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.

[0056] Some embodiments allow for the provisioning of multiple tokens after receiving a single token request message. Referring back to FIG. 1, a token provisioning method can be described.

[0057] With reference to FIG. 1, in step S102, a mobile communication device 110 containing a mobile wallet application may provide an access credential (e.g., such as a PAN) to a token requestor computer 120, which may be a digital wallet server computer (e.g., such as Apple Pay or Samsung Pay or Android Pay, etc.).

[0058] In step S104, the token requestor computer 120 may generate and transmit a token request message comprising the access credential to a token service

computer 130. The token request message may also comprise at least an address of the token service computer 130 and an identifier for the token requestor computer 120. The token service computer 130 can then perform an eligibility check on the access credential. For example, it can determine if the access credential is authentic
5 before proceeding with the token provisioning process.

[0059] The eligibility check may occur in any suitable manner. For example, the token service computer 130 may check a blacklist to see if the access credential is present and/or may run a fraud check on the access credential using a fraud engine. In other embodiments, the token service computer 130 may transmit an eligibility
10 request message to the authorizing entity computer 140. The authorizing entity computer 140 may perform the eligibility check, and may then provide an eligibility response message to the token service computer 130.

[0060] In step S106, after the token service computer 130 completes the eligibility check, and the access credential is determined to be eligible, the token service
15 computer 130 can optionally transmit a provisioning request message to the authorizing entity computer 140. The provisioning request message may comprise the access credential and an address of the authorizing entity computer 140. A routing table may be present in the token service computer 130 which maps different access credentials to specific authorizing entity computers. The authorizing entity
20 computer 140 may then determine if the access credential is authentic or is otherwise approved to have one or more tokens associated with it.

[0061] In step S108, the authorizing entity computer 140 may transmit a provisioning response message authorizing the provisioning to the token service computer 130. The provisioning response message may comprise an indication of
25 whether or not the authorizing entity computer 140 approves of the provisioning.

[0062] In response to receiving the provisioning response message, the token service computer 130 can determine (e.g., generate or retrieve) two or more access tokens, and the two or more access tokens may be associated with the access credential. In some embodiments, the access tokens may be pre-generated, while in
30 other embodiments, the access tokens can be derived from the supplied credential.

[0063] The two or more access credentials may have any suitable characteristics, and may eventually be used by a single user associated with the access credential in

different situations. For example, in some embodiments, an access token may be a resource provider (e.g., merchant) specific token, while another access token may be a device specific token tied to a specific device such as a specific mobile phone operated by the user.

5 **[0064]** In some embodiments, the two or more access token are encrypted with a first symmetric cryptographic key before being transmitted to the token requestor computer 120. The token requestor computer 120 can decrypt the two or more access tokens with a second symmetric cryptographic key.

10 **[0065]** At step S110, a token response message including the two or more access tokens, and optionally the original real credential, may be transmitted to the token requestor computer 120. The token response message may also include information on a token type, where the token type determines whether an individual token will be stored on the mobile communication device 110 or a cloud server computer 150. The information on the token type may include token type indicators, which may
15 indicate, for example, that a token is a cloud token for use with a cloud based transaction such as an e-commerce transaction, or that a token is a device bound token for use in a physical point of sale transaction. The token response message may also comprise cryptograms. A cryptogram may accompany a token in an authorization request message. The cryptogram may be validated by a processing
20 computer, and validation of the cryptogram may indicate that the token is being used in a proper transaction channel.

25 **[0066]** At step S112, after receiving the token response message, the token requestor computer 120 may extract one access token from the token response message, wherein the extracted access token is determined by the token type, and may transmit the extracted access token to the mobile communication device 110 for storage in a memory structure (e.g., in a secure element) in the mobile communication device 110. In some embodiments, the token requestor computer 120 may encrypt the first access token using a public key in an RSA encryption scheme before transmitting the first access token to the mobile communication
30 device 110. The first access token can be in encrypted form when the first access token is transmitted to the mobile communication device 110. The mobile communication device 110 stores a private key corresponding to the public key.

[0067] At S114, the token requestor computer 120 may extract another access token from the token response message, wherein the extracted access token is determined by the token type, and may provide the extracted access token to the cloud server computer 150. This access token may be stored in the cloud server computer 150 for later use by the user. For example, the access token stored in the cloud server computer 150 may be a merchant specific token that is used for recurring payment transactions such as recurring subscription payments for a newspaper.

[0068] The token requestor computer 120 may include a routing table which contains entries linking device identifiers and/or device addresses of devices (e.g., a cloud storage location on a cloud server computer) that are to be provisioned with access tokens, the real credentials, and token type indicators. The routing table may be used with the token response message is received. The token response message may include the real credential or other identifier, which may be used to identify the devices which are to be provisioned. The token type indicators may also be used to identify the specific types of devices to be provisioned (e.g., a mobile communication device or a cloud server).

[0069] In embodiments of the invention, the routing table may be populated with information during an enrollment phase with users, and/or can be populated with information as provisioning and transaction processes are conducted by the system.

[0070] Note that steps S112 and S114 can occur in any order, or sequentially in embodiments of the invention. Further, although this example describes the receipt of two access tokens by the token requestor computer 120, which distributes the two access tokens to two separate machines, in other embodiments, the token requestor computer 120 may receive three or more tokens in a single token response message and may distribute those three or more tokens to any number of machines. For example, the three or more tokens may be distributed to three or more machines, or two tokens may be distributed to one machine and one token may be distributed to another machine.

[0071] At step S116, the mobile communication device 110 may use a mobile wallet or other application (e.g., a resource provider or merchant specific application)

to access the token stored by the cloud server computer 150 to conduct a transaction, as described below.

[0072] Embodiments have a number of advantages. In embodiments, two or more access tokens may be obtained in response to a single token request message.

- 5 This reduces the time and the number of data transmissions associated with the receipt of access tokens, relative to conventional provisioning systems where only one access token per response message is received at a time.

- [0073]** Referring now to FIG. 2, a system for retrieving and using a device bound token for an in-app payment transaction is shown. In this system, a user 200 may
10 operate a mobile communication device 220 with a device bound token 226 stored within a memory element 225.

- [0074]** In step S202, the user may initiate a payment within a mobile wallet or a merchant application on the mobile communication device 220. In some embodiments, the mobile wallet or merchant application may be Apple Pay,
15 Samsung Pay, or Android Pay, and/or any application that requires an access token for completing a transaction and/or obtaining some service or product.

- [0075]** In step S203, the mobile communication device 220 may retrieve an appropriate device bound token 226 from a secure element and transmit the token 226 to an access device 240. The access device 240 may be a point of sale (POS)
20 device, an automated teller machine (ATM), and/or any suitable device for communicating with the mobile communication device 220.

- [0076]** In step S204, the access device 240 may provide an authentication request to the user 200. The authentication request might require the user 200 to provide a PIN or some other user identifying data (e.g., a password, a biometric fingerprint
25 and/or voice sample, etc.).

- [0077]** In step S206, the access device 240 may receive an authentication response with any requested authentication data. The access device 240 may validate the authentication data and generate a positive authentication indicator. If the authentication fails, then the access device 240 and/or mobile communication
30 device 220 may display an error message and/or abort the transaction, such that the ensuing steps are not executed.

[0078] In step S208, the access device 240 may generate an authorization request message, and may then transmit the authorization request to an authorizing entity 260, optionally via a transport computer operated by an entity such as an acquirer and a processing network computer operated by an entity such as a payment processing organization such as Visa™. The authorization request may include the device bound token 226 and/or one or more transaction details (e.g., such as a timestamp, a user ID, a requested amount, etc.). The authorizing entity 260 may determine if the amount requested is at least less than or equal to the user's available funds by communicating with an issuer. The authorizing entity computer 260 or a processing network computer (not shown in FIG. 2) that is in operative communication with the authorizing entity computer 260 may also exchange the device token 226 for a real credential (e.g., a PAN), before the authorizing entity computer 260 determines whether or not the transaction is authorized.

[0079] An authorization response is transmitted back to the access device 240 in step S210. The transaction may be completed upon receiving a positive authorization response. In the case of a negative authorization response, the access device 240 and/or mobile communication device 220 may display an error message and/or abort the transaction.

[0080] At the end of the day, a clearing and settlement process may take place between the authorizing entity computer 260, a processing network computer, and a transport computer associated with the resource provider (e.g., a merchant) of the access device 240.

[0081] In some embodiments, a cloud token may be retrieved from a cloud server computer and used in a transaction as depicted in FIG. 3.

[0082] FIG. 3 shows a system and method for using a cloud token for an in app payment transaction. The system comprises a user 300 operating a mobile communication device 320 which may store an application such as a mobile wallet or, as shown in this instance, a merchant application 325. An application server computer (not shown) may be affiliated with the merchant application 325. The merchant application 325 may be affiliated with a token requestor computer 340, which may be a wallet server computer. A token service computer 360 may be in

communication with both the token requestor computer 340 and an authorizing entity computer 380.

[0083] In step S302, a user 300 can initiate a payment in exchange for a product or service using the merchant application 325 on the mobile communication device 320. The merchant application 325 may be Apple Pay, Samsung Pay, or Android Pay, and/or any application that requires an access token for completing a transaction and/or obtaining some service or product.

[0084] In step S304, the merchant application 325 may send a cloud token request to the token requestor computer 340. The cloud token request could include a device bound token. The token requestor computer 340 may use a routing table that stores information associating the first access token (e.g., device bound token) with a location of a second access token (e.g., the location may be the location where a cloud token is stored on a cloud server computer 344) in order to determine the location of the corresponding cloud token 345. Using this location, the token requestor computer 340 can retrieve the correct cloud token 345 from the cloud server computer 344 as depicted in step S305. In step S306, the cloud token 345 may be transmitted, by the token requestor computer 340, to the merchant application 325 on the mobile communication device 320.

[0085] In steps S308 and S310, the token requestor computer 340 can authenticate the user 300. The authentication request might require the user 300 to provide a PIN or some other user identifying data (e.g., a password, a biometric fingerprint and/or voice sample, etc.). If the authentication fails or a negative authentication indicator is received, the token requestor computer 340 and/or mobile communication device 320 may display an error message and/or abort the transaction, such that the ensuing steps are not executed.

[0086] In steps S312 and S314, in response to a positive authentication response, the token requestor computer 340 may request an access cryptogram from the token service computer 360. The access cryptogram may be specifically associated with the particular cloud token 345 that will be used to conduct the transaction. For example, an access token that is tied to a device for use in in-store payments may require one specific cryptogram to be used. Another access token that is stored on

file in a cloud computer may require another specific cryptogram for it to be used. The cryptogram can be a TAVV (transaction authentication verification value).

[0087] In step S316, the cryptogram and an access token from the token requestor computer 340 can then be provided to the merchant application 325.

5 **[0088]** In step S318, once the merchant application 325 has the cloud token 345 and the cryptogram, the merchant application (or an application provider in communication with the merchant application) may submit an authorization request message (e.g., via an acquirer and/or a payment processing network) to the authorizing entity computer 380. The authorizing entity computer 380, token service
10 computer 360, a payment processor, or a payment processing network may verify the cryptogram, and can exchange the cloud token 345 for the real credential (e.g., a PAN) before the authorizing entity computer 380 makes a decision on the authorization request message.

[0089] The authorizing entity computer may then transmit an authorization
15 response message (e.g., via a processing network computer in a payment processing network and a transport computer operated by an acquirer) back to the merchant application on the communication device 320. In step S320, the authorizing entity computer 380 may transmit an authorization response message back to the merchant application 325 on the mobile communication device 320,
20 authorizing the transaction.

[0090] At the end of the day, a clearing and settlement process may take place between the authorizing entity computer 380, a processing network computer, and a transport computer operated by an acquirer of the merchant.

[0091] FIG. 4 shows another embodiment of the invention. FIG. 4 shows a system
25 and method for using a mobile communication device 410 to gain access to a building 430 (e.g. may refer to any secure location). In yet other embodiments, the building may be a secure server computer that houses secure data to be accessed (e.g., secure and private data records).

[0092] A user 406 can use a mobile communication device 410 to interact with an
30 access device 420. The access device 420 may either retrieve a device bound token from the mobile communication device 410 or, in the absence of a device bound

token, request a cloud token from a token requestor computer (as described in FIG. 3). The device bound token or the cloud token may be exchanged for a real credential (e.g., a PIN) which can be used to gain access to the building 430.

[0093] Embodiments of the present invention are useful in providing greater efficiency in the token provisioning process. For example, with reference to the system described in FIG. 4, a user 406 may be able to program (e.g., request a token) and use multiple mobile communication devices (e.g., a mobile phone and an access card) with a single provisioning request. Therefore, the user will only have to provide an access credential once in order to access a secure location with two or more devices (e.g., such as the aforementioned mobile phone and access card).

[0094] FIG. 5 shows a block diagram of a mobile communication device 500 that can be used in embodiments of the invention. The mobile communication device 500 may be a mobile phone or an access card.

[0095] The mobile communication device 500 may comprise a computer readable medium 502, which can be in the form of (or may be included in) a memory element that stores data (e.g., merchant applications) and can be in any suitable form (e.g., microSD chip, SIM card, or other type of memory element). The computer readable medium 502 may store a transaction initiation module 502A, one or more applications 502B, real credentials and/or tokens 502C, and an operating system 502D for the device. The transaction initiation module 502A may begin a transaction at the request of a user or an application.

[0096] The computer readable medium 502 may also comprise a storage element 502B for device bound tokens and credentials. The token/credential storage 502B may be a secure memory element that is separate from the rest of the computer readable medium, such that tokens or credentials can only be accessed or altered by certain elements of the mobile communication device 500 and/or outside devices (e.g., a token requestor computer).

[0097] In addition, the mobile communication device 500 may include some device hardware 504, comprising: a processor 506, a user interface 508, input elements 510, output elements 512. The device hardware may also include a long range antenna 516 and a short range antenna 514 for communicating with a wireless

network and/or other devices. All elements in the device hardware 504 are operatively coupled, enabling mutual communication and data transfer.

[0098] Referring to FIG. 6, a block diagram of a token service computer 600 according to embodiments of the invention is illustrated. The token service computer 600 may include a processor 602, and a network interface 608 for receiving and transmitting messages (e.g. a token provisioning request message or token response message) to outside sources (e.g., an authorizing entity and/or the token requestor computer).

[0099] The token service computer 600 may include a non-transitory computer readable medium 604, comprising a token generation module 604A and a validation module 604B. The token generation module 604A may include code, executable by the processor 602 to generate or obtain at least two or more tokens from an access credential. However, this module may also be substituted for a token retrieval module, which connects the token service computer 600 to an outside database (e.g. issuer or authorizing entity) that can provide at least two or more tokens. The validation module 604B may be used, in conjunction with the processor 602, to determine the eligibility of an access credential.

[0100] The non-transitory computer readable medium 604 may comprise code, executable by the processor 602, for implementing a method comprising: receiving a token request message, the token request message being originated from a token requestor computer; determining two or more access tokens based upon a single credential; and transmitting the two or more access tokens to the token requestor computer in a token response message.

[0101] FIG. 6 also shows a token database 612 operatively coupled with the processor 602. The token database 612 may store tokens that are pre-generated, along with other token data such as mapping to real credentials, cryptograms, etc.

[0102] FIG. 7 illustrates a block diagram of a token requestor computer 700 according to embodiments of the invention.

[0103] The token requestor computer 700 may also include a processor 702 and a network interface 708 for receiving and transmitting messages (e.g., a token response message) with the token service computer and cloud server computer.

[0104] The token requestor computer 700 may include a non-transitory computer readable medium 704, comprising a token determining module 704A and a credential transmitting module 704B. The token determining module 704A may, in conjunction with the processor 702, use a token type indicator to determine sending
5 a first access token to a mobile communication device and a second access token to a cloud server computer. The credential transmitting module 704B may, in conjunction with the processor 702, handle generating or receiving an access credential from a mobile communication device operated by a user and transmitting the access credential to a token service computer in order to request at least two or
10 more access tokens.

[0105] The non-transitory computer readable medium 704 may comprise code, executable by the processor, for implementing a method comprising: receiving, from a communication device, a single credential; transmitting the single credential to a token service computer; receiving, from the token service computer, two or more
15 access tokens including a first access token and a second access token; transmitting the first access token to the communication device; and transmitting the second access token to a cloud server computer.

[0106] The token requestor computer 700 may include a routing table 706 that stores relationships between a location of a first access token (e.g., a communication
20 device operated by a user), and a secondary location of a second access token (e.g. a cloud storage location on a cloud server computer). The routing table 706 may be accessed to retrieve an appropriate cloud token for a user.

[0107] 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
25 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-
30 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.

[0108] [0109] 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
5 reference to the pending claims along with their full scope or equivalents.

[0110] 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.

[0111] A recitation of "a", "an" or "the" is intended to mean "one or more" unless
10 specifically indicated to the contrary.

[0112] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1 1. A method comprising:

2 receiving, by a token service computer, a token request message, the
3 token request message being originated from a token requestor computer;

4 determining, by the token service computer, two or more access tokens
5 based upon a single credential including a first access token and a second access
6 token that is independent of the first access token, the first access token and the
7 second access token being associated with the single credential, and token type
8 indicators for the two or more access tokens wherein destinations of the two or more
9 access tokens are determined by the token type indicators; and

10 transmitting, by the token service computer, the two or more access
11 tokens and the token type indicators to the token requestor computer in a token
12 response message, wherein the two or more access tokens comprise a cloud token and
13 a device specific token for a mobile communication device that is associated with the
14 token requestor computer.

1 2. A method comprising:

2 receiving, by a token service computer, a token request message, the
3 token request message being originated from a token requestor computer;

4 determining, by the token service computer, two or more access tokens
5 based upon a single credential including a first access token and a second access
6 token that is independent of the first access token, the first access token and the
7 second access token being associated with the single credential, and token type
8 indicators for the two or more access tokens wherein destinations of the two or more
9 access tokens are determined by the token type indicators; and

10 transmitting, by the token service computer, the two or more access
11 tokens and the token type indicators to the token requestor computer in a token
12 response message wherein the token requestor computer comprises a routing table that
13 stores relationships between a communication device operated by a user, and a cloud
14 storage location on a cloud server computer.

1 3. The method of claim 2, wherein the routing table also stores the
2 token type indicators associated with a first token to be stored in the communication
3 device, and a second token to be stored in the cloud storage location on the cloud
4 server computer.

1 4. A token service computer comprising:
2 a processor; and
3 a non-transitory computer readable medium, the non-transitory computer
4 readable medium comprising code, executable by the processor to implement a method
5 comprising:
6 receiving a token request message, the token request message being
7 originated from a token requestor computer;
8 determining two or more access tokens based upon a single credential
9 including a first access token and a second access token that is independent of the first
10 access token, the first access token and the second access token being associated with
11 the single credential, and token type indicators for the two or more access tokens
12 wherein destinations of the two or more access tokens are determined by the token type
13 indicators; and
14 transmitting the two or more access tokens to the token requestor
15 computer in a token response message,
16 wherein the two or more access tokens are each assigned a token type
17 indicator upon generation.

1 5. A method comprising:
2 receiving, by a token requestor computer from a communication device, a
3 single credential;
4 transmitting, by the token requestor computer, a token request message
5 comprising the single credential to a token service computer;
6 receiving, by the token requestor computer from the token service
7 computer, a token response message comprising two or more access tokens including
8 a first access token and a second access token that is independent of the first access

9 token, the first access token and the second access token being associated with the
10 single credential, and token type indicators for the two or more access tokens wherein
11 destinations of the two or more access tokens are determined by the token type
12 indicators;

13 transmitting, by the token requestor computer, the first access token to the
14 communication device based on the token type indicator for the first access token; and
15 transmitting, by the token requestor computer, the second access token to
16 a cloud server computer based on the token type indicator for the second access token.

1 6. The method of claim 5, wherein the single credential is a real
2 credential.

1 7. The method of claim 5, wherein the first access token can include
2 one or more access tokens.

1 8. The method of claim 5, further comprising:
2 encrypting, by the token requestor computer, the first access token using
3 a public key in an RSA encryption scheme before transmitting the first access token to
4 the communication device, the first access token being in encrypted form when the first
5 access token is transmitted to the communication device, the communication device
6 storing a private key corresponding to the public key.

1 9. The method of claim 5, wherein the token requestor computer
2 comprises a routing table that stores relationships between a communication device
3 operated by a user, and a cloud storage location on a cloud server computer.

1 10. The method of claim 9, wherein the token requestor computer uses
2 the routing table to retrieve a cloud token.

1 11. The method of claim 5, wherein the token request message also
2 comprises a token requestor computer identifier.

1 12. The method of claim 5, wherein the token type indicators include at
2 least a type for device bound tokens and a type for cloud tokens.

1 13. The method of claim 5, wherein the two or more access tokens are
2 used to access secure data residing on remote computers.

1 14. A token requestor computer comprising:
2 a processor; and
3 a non-transitory computer readable medium, the non-transitory computer
4 readable medium comprising code, executable by the processor, for implementing a
5 method comprising:
6 receiving, from a communication device, a single credential;
7 transmitting a token request message comprising the single credential to a
8 token service computer;
9 receiving, from the token service computer, a token response message
10 comprising two or more access tokens including a first access token and a second
11 access token that is independent of the first access token, the first access token and the
12 second access token being associated with the single credential, and token type
13 indicators for the two or more access tokens wherein destinations of the two or more
14 access tokens are determined by the token type indicators;
15 transmitting the first access token to the communication device based on
16 the token type indicator for the first access token; and
17 transmitting the second access token to a cloud server computer based on
18 the token type indicator for the second access token.

1 15. The token requestor computer of claim 14, wherein the single
2 credential is sixteen digits long.

1 16. The token requestor computer of claim 14, wherein the first access
2 token is used by the communication device to access a secure location.

1 17. The token requestor computer of claim 14, wherein the non-
2 transitory computer readable medium comprises a token determining module and a
3 credential transmitting module.

1 18. The token requestor computer of claim 14, comprising a routing
2 table that stores relationships between a communication device operated by a user, and
3 a cloud storage location on a cloud server computer.

1 19. The token requestor computer of claim 18, wherein the routing
2 table can be used to retrieve a cloud token.

1 20. The token requestor computer of claim 18, wherein the routing
2 table also stores the token type indicators associated with a first token to be stored in
3 the communication device, and a second token to be stored in the cloud storage
4 location on the cloud server computer.

1 21. The token requestor computer of claim 14, wherein the token type
2 indicators may include at least a type for device bound tokens and a type for cloud
3 tokens.

1 22. The token requestor computer of claim 14, wherein the token
2 request message comprises a token requestor computer identifier.