

TOKEN AND CRYPTOGRAM USING TRANSACTION SPECIFIC INFORMATION

BACKGROUND

[0001] This patent application is a non-provisional application of and claims the benefit of U.S. Provisional Application No. 62/117,291, filed on February 17, 2015,
5 which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Tokens can be used to protect against data breaches. For example, tokens can be used to replace personal information such as driver's license numbers, account information, and social security numbers. Tokenizing information can reduce
10 the risk of fraud, because unlike real information, a compromised token can be easily replaced so that the compromised token is rendered useless. Although tokens minimize risk, a fraudster may still potentially capture a token at the point of use and may attempt to immediately reuse the token. Further, a device (e.g., smartphone) provisioned with a token can also be stolen and used in a fraudulent manner.

15 [0003] Other problems also exist. For example, whether or not tokens are used, a party such as a merchant during a merchant transaction could inadvertently initiate the transaction for a different amount than what is displayed to the user for approval.

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

BRIEF SUMMARY

20 [0005] Embodiments of the invention relate to a cloud based single-use token processing system for performing transactions.

[0006] One embodiment of the invention is directed to a method comprising:
receiving access device data by a mobile communication device from an access device;
25 generating, by the mobile communication device, a token request including the access device data and communication device data; sending, by the mobile communication

device, the token request to a server computer, wherein the server computer thereafter determines a token and generates a cryptogram, wherein the cryptogram was generated using the access device data and the communication device data; receiving, by the mobile communication device, the token and the cryptogram; and providing, by the mobile communication device, the token and the cryptogram to the access device, wherein the access device forwards the cryptogram and the token to the server computer, which verifies the cryptogram and processes the token.

[0007] Processing the token may include any suitable activity involving the token. For example, processing the token may involve transmitting a message including the token to another computer so that the computer can verify or determine an underlying identifier associated with the token. Processing the token could alternatively include determining the underlying identifier associated with the token and/or performing additional authentication or fraud processing on the token.

[0008] Another embodiment of the invention is directed a mobile communication device configured to perform the above-noted method.

[0009] Another embodiment of the invention is directed to a method comprising providing, by an access device, access device data to a mobile communication device, wherein the mobile communication device generates a token request including the access device data and communication device data and sends the token request to a server computer, which returns a token and a token cryptogram to the mobile communication device; receiving, by the access device, the token and the cryptogram from the mobile communication device; generating, by the access device, an authorization request message; and transmitting, by the access device, the authorization request message to the server computer, wherein the server computer verifies the cryptogram and processes the transaction using the token.

[0010] Another embodiment of the invention is directed to an access device configured to perform the above-noted method.

[0011] Further details regarding embodiments of the invention are described in the Figures with reference to the Detailed Description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows a block diagram of a first transaction system according to embodiments of the invention. Steps in a process flow of a user performing a payment transaction are illustrated in FIG. 1.

5 **[0013]** FIG. 2 shows a block diagram of a mobile communication device according to an embodiment of the invention.

[0014] FIG. 3 shows a block diagram of an access device according to an embodiment of the invention.

10 **[0015]** FIG. 4 shows a block diagram of a tokenization computer according to an embodiment of the invention.

[0016] FIG. 5 shows a block diagram of a second transaction system according to embodiments of the invention. Steps in a process flow for a user obtaining access to a building are shown in FIG. 5.

DETAILED DESCRIPTION

15 **[0017]** Embodiments of the invention can incorporate a cloud based token processing system and method for performing transactions. The types of transactions in which embodiments of the invention can be used include, but are not limited to, access transactions (e.g., when a user attempts to enter a location, venue, or building), payment transactions, and data request transactions.

20 **[0018]** In one embodiment of the invention, a mobile communication device (e.g., a smartphone) belonging to a user may capture a Quick Response (QR) code displayed on a merchant POS terminal. The QR code may encode transaction specific information, location information, merchant-related information (e.g., merchant identifier), and any other relevant information. Upon capturing the QR code, the mobile
25 communication device may request a token and a cryptogram from a remote server computer (which may be a cloud based token generation and verification system) using at least the information encoded in the QR code. After the mobile communication

device obtains the token and the cryptogram, the mobile communication device may then pass the token and the cryptogram to the POS terminal. The POS terminal may then generate and send an authorization request message that includes at least some of the information encoded in the QR code, the token, and the cryptogram to an issuer
5 computer operated by the issuer of the account number that was used to create the token and/or to a transaction processing computer. One or both of these computers then receives the authorization request message and validates the cryptogram using information in the authorization request message and a shared encryption key. The issuer computer or the transaction processing computer may then determine a risk level
10 for the transaction by (i) matching the transaction data in the cryptogram and the authorization request message, (ii) ensuring that the device is in a reasonable proximity to the merchant terminal (e.g., POS terminal), and/or (iii) determining whether a recent transaction count associated with the device is reasonable.

[0019] Embodiments of the invention improve transaction security relative to
15 conventional methods and systems. For example, the cryptogram that is generated according to embodiments of the invention limits the transaction to one that has the corresponding transaction-specific information that may be passed in an authorization request message (e.g., transaction amount, merchant location, time, date, account identifier, expiration date, CVV, etc.), as well as information surrounding the interaction
20 between the mobile device and the access device at the point of sale.

[0020] Before discussing embodiments of the invention in detail, some terms are described in further detail below.

[0021] A "mobile communication device" or a "mobile device" may comprise any
suitable electronic device that may be transported and operated by a user, which may
25 also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g. 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g. cellular
30 phones), PDAs, tablet computers, net books, laptop computers, personal music players,

hand-held specialized readers, etc. Further examples of mobile devices include wearable devices, such as smart watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem – both devices taken together may be considered a single mobile device).

[0022] 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. 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. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0023] "Communication device data" may include any suitable data associated with a communication device. Such data may be stored within a communication, and in some cases, it may exist independent of any communication with an access device at a resource provider. Examples of communication device data may include account identifiers stored on the communication device, device identifiers, authentication data relating to authentication processes performed by a communication device (e.g., biometric templates, stored secrets such as passwords, etc.), timestamps created by the communication device, etc.

[0024] 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.

[0025] A "value credential" may be information associated with worth. Examples of value credentials include payment credentials, coupon identifiers, information needed to obtain a promotional offer, etc.

[0026] "Payment credentials" may include any suitable information associated with an account (e.g. a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include a PAN (primary account number or "account number"), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0027] An "application" may be computer code or other data stored on a computer readable medium (e.g. memory element or secure element) that may be executable by a processor to complete a task.

[0028] A "digital wallet" can include an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, payment credentials, bank account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like. A digital wallet may 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.

[0029] A "digital wallet provider" may include an entity, such as an issuing bank or third party service provider, that issues a digital wallet to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers, or representations of the account numbers (e.g., payment tokens), on behalf of a cardholder (or other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing multiple payment cards and other payment products on behalf of a user, storing other information including billing address, shipping addresses, and transaction history, and initiating a transaction by one or more methods.

[0030] 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.

[0031] 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.

[0032] "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
5 may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency and improve transaction security.

[0033] A "tokenization computer" or "token service system" can include a system that services payment tokens. In some embodiments, a token service system can
10 facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may include or be in
15 communication with a token vault where the generated tokens are stored. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer. Various entities
20 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.

[0034] A "token domain" may indicate an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to,
25 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.
30 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
5 cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0035] 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
10 be a numeric value (e.g. a 4-digit numeric value).

[0036] A "token request message" or "token request" may be an electronic message for requesting a token. In some embodiments, a token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a token. For example, a token request message may include
15 payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key). In some embodiments, a token request message may include a flag or
20 other indicator specifying that the message is a token request message.

[0037] A "token response message" or "token response" 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 token, mobile device identification information (e.g. a phone number or MSISDN), a
25 digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key). In some embodiments, a token response message may include a flag or other indicator specifying that the message is a token response message.

[0038] A "cryptogram" may include encrypted characters. Cryptograms can be of any suitable length and may be formed using any suitable data transformation process. Exemplary data transformation processes include encryption, and encryption processes such as DES, triple DES, AES, and ECC may be used. Keys used with such encryption process can be of any appropriate length and may have any suitable characteristics.

[0039] A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of a resource provider include merchants, access devices, secure data access points, etc. A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0040] 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".

[0041] An "authorizing entity" may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc. An "issuer" may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer. An authorizing entity may operate an authorizing computer.

[0042] An "access device" may be any suitable device that provides access to a remote system. An access device may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs),

automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments, where an access device may comprise a POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an "mPOS" terminal.

[0043] "Access device data" may include any suitable data obtained from an access device. Examples of access device data may include a merchant identifier, transaction amount, location information (e.g., a GPS location of the access device), transaction timestamp, an access device identifier, etc.

[0044] An "authorization request message" may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a user name, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank

identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0045] 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. The authorization response message may be generated by an issuing financial institution or a transaction processing computer. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a transaction processing computer may generate or forward the authorization response message to the merchant.

[0046] A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers.

[0047] A "processor" may include a a central processing unit (CPU). A processor can include a single-core processor, a plurality of single-core processors, a multi-core processor, a plurality of multi-core processors, or any other suitable combination of hardware configured to perform arithmetical, logical, and/or input/output operations of a computing device.

[0048] FIG. 1 shows a block diagram and a flow diagram of a token processing system 100 according to embodiments of the invention. The token processing system 100 may be used to perform payment transactions.

[0049] The token processing system 100 comprises a mobile device 115 that can
5 interact with an access device 125. The access device 125 may communicate with an authorization computer 160 via a resource provider computer 130, a transport computer 140, and a transaction processing computer 150. The mobile device 115 may also communicate with the tokenization computer 170. Each of the computers and devices shown in FIG. 1 may communicate using any suitable communications network.
10 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
15 (WAP), I-mode, and/or the like); and/or the like.

[0050] Messages between the computers, networks, and devices described herein 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)
20 and/or the like.

[0051] FIG. 2 shows a detailed block diagram of a mobile device 115 according to an embodiment of the invention.

[0052] Mobile device 115 may include circuitry that is used to enable certain device functions, such as telephony. The functional elements responsible for enabling
25 those functions may include a processor 115A that can execute instructions that implement the functions and operations of the device. Processor 115A may access memory 115E (or another suitable data storage region or element) to retrieve instructions or data used in executing the instructions, such as provisioning scripts and mobile applications.

[0053] Data input/output elements 115C, such as a biometric scanner (e.g., a fingerprint or retinal scanner), keyboard or touchscreen, can allow a user to operate the mobile device 115 and input data (e.g., user authentication data). Other data input elements can include a camera, which can be used to capture a two dimensional code (e.g., a QR code) that is displayed on an access device or other device. Data input/output elements may also be configured to output data (via a speaker, for example). An example of an output element may include a display 115B that may be used to output data to a user.

[0054] Communications element 115D may be used to enable data transfer between mobile device 115 and a wired or wireless network (via antenna 115H, for example) to assist in connectivity to the Internet or other network, and enabling data transfer functions. Mobile device 115 may also include contactless element interface 115F to enable data transfer between contactless element 115G and other elements of the device, where contactless element 115G may include a secure memory and a near field communications data transfer element (or another form of short range communications technology).

[0055] As noted, a cellular phone or similar device is an example of a mobile device 115 that may be used in accordance with embodiments of the present invention. However, other forms or types of devices may be used without departing from the underlying concepts of the invention. For example, the mobile device 115 may alternatively be in the form of a payment card, a key fob, a tablet computer, a wearable device, etc.

[0056] The memory 115E may comprise a digital wallet application 115E-1, a tokenization module 115E-2, and an authentication module 115E-3, and any other suitable module or data. The mobile device 115 may have any number of mobile applications installed or stored on the memory 115E and is not limited to that shown in FIG. 7. The memory 115E may also comprise code, executable by the processor 115A for implementing a method comprising: receiving access device data from an access device; generating a token request including the access device data and communication device data; sending the token request to a server computer, wherein the server

computer thereafter determines a token associated with the user and generates a cryptogram, wherein the cryptogram was generated using the access device data and the communication device data; receiving the token and the cryptogram; and providing the token and the cryptogram to the access device, wherein the access device forwards the cryptogram and the token to the server computer, which verifies the cryptogram and processes the token. In some embodiments, the memory 115E may also comprise a secure element, which may store encryption keys, account identifiers, and/or tokens and cryptograms.

[0057] The digital wallet application 115E-1 may provide a user interface for the user 110 to provide input and initiate, facilitate, and manage transactions using the mobile device 115. The digital wallet application 115E-1 may be able to store and/or access a payment token and/or payment credentials. The digital wallet application 115E-1 may also store an issuer-specific key, or any other suitable encryption means. The digital wallet application 115E-1 may be able to cause the mobile device 115 to transmit the payment token and/or payment credentials in any suitable manner (e.g., NFC, QR code, etc.).

[0058] The digital wallet application 115E-1 may be associated with and/or provided by a wallet provider computer, the authorizing computer 160, the transaction processing computer 150, the transport computer 140, the resource provider computer 130, or any other suitable entity.

[0059] The tokenization module 115E-2 may be a module of the digital wallet application 115E-1 or a separate application on the mobile device 120. The tokenization module 115E-2 may comprise code that causes the processor 115A to obtain payment tokens. For example, the tokenization module 115E-2 may contain logic that causes the processor 115A to request a token from the tokenization computer 170 or any other suitable tokenization service provider or system (e.g., the authorizing computer 160 or the transaction processing computer 150). In some embodiments, the mobile device 120 may be able to communicate over-the-air with the tokenization computer 170, and may be able to send a direct request to the tokenization computer 170.

[0060] The authentication module 115E-3 may comprise code that causes the processor 115A to conduct an authentication process to authenticate the user 110. The authentication module 115E-3 may include biometric information of the user, secrets of the user, etc., which may be used to authenticate the user 110.

5 [0061] FIG. 3 shows a detailed block diagram of an access device 125 according to an embodiment of the invention. The access device 125 may comprise a processor 125A operatively coupled to at least a network interface 125B, a device communication interface 125C, and a computer readable medium 125D. The computer readable medium 125D comprises a machine readable code generation module 125D-1 and an
10 authorization processing module 125D-2.

[0062] The code generation module 125D-1 may comprise code, which when executed by the processor 125A, may cause the access device 125 to generate a machine readable code, such as a one or two-dimensional bar code.

[0063] The authorization processing module 125D-2 may comprise code, which
15 when executed by the processor 125A, may cause the access device 125 to generate authorization request messages, transmit authorization request messages, receive authorization response messages, and process authorization response messages.

[0064] The computer readable medium 125D may also comprise code, which
20 when executed by the processor 125A may implement a method comprising providing access device data to a mobile communication device, wherein the mobile communication device generates a token request including the access device data and communication device data and sends the token request to a server computer, which returns a token and a token cryptogram to the mobile communication device; receiving, by the access device, the token and the cryptogram from the mobile communication
25 device; generating, by the access device, an authorization request message; and transmitting, by the access device, the authorization request message to the server computer, wherein the server computer verifies the cryptogram and processes the transaction using the token.

[0065] FIG. 4 shows a detailed block diagram of a tokenization computer 170 according to an embodiment of the invention. The tokenization computer 170 comprises a processor 170A, a network interface 170B, a token record database 170C, and a computer readable medium 170D.

5 **[0066]** The computer readable medium 170D may comprise a tokenization module 170D-1, a detokenization module 170D-2, a security module 170D-3, and any other suitable software module.

[0067] The tokenization module 170D-1 may comprise code that causes the processor 170A to provide payment tokens. For example, the tokenization module
10 170D-1 may contain logic that causes the processor 170A to generate a payment token and/or associate the payment token with a set of payment credentials. A token record may then be stored in the token record database 170C indicating that the payment token is associated with a certain user 110 or a certain set of payment credentials.

[0068] The detokenization module 170D-2 may comprise code that causes the
15 processor 170A to detokenize payment tokens. For example, the detokenization module 170D-2 may contain logic that causes the processor 170A to identify a token record associated with a payment token in the token record database 170C. A set of payment credentials associated with the payment token (as indicated in the token record) can then be identified.

20 **[0069]** The security module 170D-3 may comprise code that causes the processor 170A to validate token requests before a payment token is provided. For example, security module 170D-3 may contain logic that causes the processor 170A to confirm that a token request message is authentic by decrypting a cryptogram included in the message, by confirming that the payment credentials are authentic and
25 associated with the requesting user 110, by assessing risk associated with the requesting resource provider computer 130, or by using any other suitable information. If the payment credentials are encrypted, the security module 170D-3 may be able to decrypt the encrypted payment credentials (e.g. via an issuer-specific key or merchant-acquirer encryption models). Also, the security module 170D-3 may include keys and
30 algorithms (e.g., DES, TDES, AES) that can be used with the processor 170A to

generate transaction specific cryptograms and decrypt such cryptograms. The security module 170D-3 may also be programmed to cause the processor 170A to distribute keys to other entities that may perform such cryptogram encryption/decryption functions.

5 **[0070]** A method for performing a transaction can be described with reference to FIGs. 1-4. The transaction that is being performed may be a payment transaction at a resource provider such as a merchant. Initially, the user 110 may select goods or services to purchase at the resource provider.

10 **[0071]** At step S1, after the goods or services are selected, the access device 125 (e.g, a merchant terminal such as a POS terminal) may generate and display a unique QR code on a display. The QR code may encode transaction-specific information including, but not limited to, access device data such as a merchant identifier, transaction amount, location information (e.g., a GPS location of the access device), transaction timestamp, etc. Other examples of the transaction-specific
15 information may include, but are not limited to, a number of purchases in a past time period, location information of the merchant terminal, an access device ID, a token request timestamp, a mode of QR code scan (e.g., voice or manual), etc.

20 **[0072]** At step S2, the user may scan the QR code displayed on the access device 125 using his/her mobile device 115. For example, the mobile device 115 may be a smartphone with a camera. The camera may capture the QR code and storage an image of the QR code within memory of the device for further processing. In other embodiments, the access data may be transferred from the access device 125 to the mobile device 115 using a wireless connection such as WiFi, Bluetooth, or NRC, or even a contact mode of interaction.

25 **[0073]** In some embodiments, the user 110 authenticates to the mobile device 115 before obtaining transaction information (e.g., information encoded in a QR code displayed by an access device) from the access device 125. Alternatively, in some embodiments, the user 110 may use a second device (e.g., a wearable device) communicatively coupled to the mobile device 115 to capture the QR code (e.g., a head
30 mounted display connected to a smartphone device). The user may authenticate to

either device by, e.g., issuing a voice command to validate the user with the device (e.g., voice authentication). In some cases, a head mounted device may capture the QR code displayed at the access device 125 (e.g., by using a camera connected to the head mounted device such as Google glass™). The head mounted device sends the captured QR code information to the mobile device 115. This may be sent over a secure connection supported over a wireless data protocol, such as Bluetooth, Wi-Fi, etc.

[0074] In some embodiments, the system may determine whether the transaction amount in the QR code is more than the threshold transaction amount set by the authorizing entity (e.g., an issuer) operating the authorizing computer 160 and/or the user 110. For example, if the transaction amount encoded in the QR code is \$500, but the threshold transaction amount is \$250, the system (e.g., any of the computers or devices in FIG. 1, such as the combination of the mobile device 115 and the access device 125) may alert the authorizing entity operating the authorizing computer 160, the resource provider operating the resource provider computer 130, and/or the user 110. In this case, further steps may be required to continue with the transaction. For example, if the threshold transaction amount is less than the transaction amount in the QR code, then the user 110 may be prompted by the access device 125 for a challenge PIN code, by communicating with the mobile device 115. In this case, the user 110 may enter the PIN code into the access device 125 to continue with the transaction.

[0075] Returning to FIG. 1, at step S3, the mobile device 115 may send a token request message to the tokenization computer 170, which may be in or itself be a cloud based network. Prior to or concurrently with sending the token request message, the mobile device 115 may authenticate with the tokenization computer 170 using, for example, user credentials, a mobile device ID or any other suitable information.

[0076] The token request message may request a token and may include the transaction-specific information described above. For example, the token request may include a merchant ID, a transaction amount, location information of the user 110 and/or the resource provider operating the resource provider computer 130, a token request timestamp, and a resource provider (e.g., merchant) initiate timestamp. In some

embodiments, the mobile device 115 may send communication device data including transaction information, GPS information, timestamps, a transaction count, a merchant ID, and any user authentication methods to the tokenization computer 170. In some embodiments, the mobile device 115 may encrypt the above information prior to sending it to the tokenization computer 170. The information may be encrypted in a manner such that it can be only be decrypted by the tokenization computer 170.

[0077] At step S4, upon receiving the token request message and transaction-specific information from the mobile device 115, the tokenization computer 170 may generate a token for the mobile device 115, a token expiration date, and a transaction cryptogram. Appropriate encryption keys and known algorithms such as AES, TDES, and DES may be used. The transaction cryptogram may include authentication information, which may be derived from at least the transaction-specific information including the merchant ID, the transaction amount, the locations of the user and the merchant, and a time stamp. The token may be associated with a PAN of a payment account belonging to the user 110 of the mobile device 115.

[0078] At step S5, the tokenization computer 170 may transmit the generated token and cryptogram in a token response message to the mobile device 115. The generation of the token and cryptogram may be conditional upon authentication of the mobile device 115 and the user 110 by the tokenization computer 170. In some embodiments, the token and cryptogram may be sent to the mobile device 115 using ISO 8583 fields.

[0079] In some embodiments, the tokenization computer 170 may return a token provisioned for the mobile device 115 and a uniquely generated cryptogram to be used for validation and token assurance. The following information may be sent to the mobile device 115 and then to the access device 125 according and conforming to ISO 8583 fields: the token, token expiration data, and the uniquely generated cryptogram (e.g., the token cryptogram). The token cryptogram may include the following information: a user's (e.g., device's) GPS location information, a number of purchases in a past time frame (specified by the issuer), a merchant ID, a GPS location of the merchant terminal, transaction initiation timestamp, a transaction amount, token request timestamp, and a

mode of QR code scan initiation (e.g., voice initiated, manual screen unlock, manual head mounted display initiation, etc.).

[0080] At step S6, after the mobile device 115 receives the token and the cryptogram, the user 110 may interact with the access device 125 using his/her mobile device. For example, the user 110 may tap his/her mobile device 115 to the access device 125 to initiate an NFC connection. In another example, the user 110 may select the access device 125 via the mobile device 115 to establish a short range connection such as a Bluetooth™ connection. In yet another example, the mobile device 115 may generate a unique QR code that encodes the information received from the tokenization computer 170. The QR code may then be scanned by the access device 125. Regardless of the method of interacting with the access device 125, upon initiating a connection with the access device 125, the access device 125 may receive at least the token, the token expiration date, and the transaction cryptogram from the mobile device 115.

[0081] In some embodiments, the user 110 presents the token and the token cryptogram to the access device 125 at the resource provider. The token and token cryptogram may be presented to the access device 125 by, for example, tapping the mobile device 115 on an NFC reader associated with the access device 125. An application running on the mobile device 115 may transmit the token, token expiration date, and the token cryptogram to the access device 125.

[0082] In steps S7, S8, and S9, the access device 125 may generate and send an authorization request message to the transaction processing computer 150 via the transport computer 140 and the resource provider computer 130. The authorization request message may also include the token, the token expiration date, and the transaction cryptogram.

[0083] At step S10, the transaction processing computer 150 may transmit the authorization request message to the tokenization computer 170 or may provide the token and the token cryptogram to the tokenization computer 170. The transaction processing computer 150 may then decrypt the cryptogram and may also determine the real account identifier from token. Encryption keys and/or lookup tables may be used to

perform these functions. For example, a real account identifier may be obtained from a token through a lookup table. In another example, a real account identifier may be mathematically derived from a token.

5 [0084] The tokenization computer 170 may determine a token assurance level based on the transaction-specific information contained within the transaction cryptogram. For example, the token assurance level may be based in part on (i) matching the transaction data in the cryptogram and the authorization request message, (ii) ensuring reasonable proximity of the user 110 and the access device 125 (based on the location information), and/or (iii) determining that a recent transaction count is
10 reasonable. The token assurance level may be based on other transaction-specific information contained within the token cryptogram, as described above. The tokenization computer 170 may compare the transaction-specific information obtained from the decrypted cryptogram with the information in the authorization request message.

15 [0085] The token assurance level may also be based at least in part on identification and verification scoring that can be performed done based on the method used to initiate the QR code scan. For example, if both voice and PIN entry are used, a higher assurance value may be assigned. If only voice/PIN is used, then a medium assurance value may be assigned. If neither voice nor PIN are used, then the issuer
20 can decide the assurance level based solely on the mobile device that is used and any predetermined cloud authentication methods.

[0086] In some embodiments, the tokenization computer 170 may also determine if the token is subject to any domain restrictions. For example, as noted above, a single account may have many tokens associated with it. Each token may be used for a
25 different domain. For example, one token associated with an account may be used for e-commerce transactions, while another token associated with the account may be used for in person transactions with a chip card. If the received token is outside of its intended domain, then the transaction can be rejected.

[0087] In some embodiments, the tokenization computer 170, the transaction
30 processing computer 150, and/or the authorizing entity (e.g, an issuer) operating the

authorizing computer 160 may use the transaction information in the authorization request and match it against the transaction information in the cryptogram. An authorization decision may be made based at least in part on the token assurance level derived from this information. As an illustration, the issuer or the transaction processing computer 150 may verify that the transaction amount and the merchant ID in the authorization request message matches the information derived from the token cryptogram. Additionally, the issuer or the transaction processing computer 150 may ensure that the GPS locations of the user (e.g., device) and the merchant terminal indicate that they are within a reasonable proximity of each other. Further, the issuer or the transaction processing computer 150 may verify that the number of purchases associated with the PAN within a given time frame is reasonable. The issuer or the transaction processing computer 150 may then return an authorization response message to the merchant terminal indicating whether the transaction is approved/rejected.

15 [0088] At step S11, if the tokenization computer 170 verifies the cryptogram, the tokenization computer 170 can return the real account identifier associated with the token to the transaction process computer 150. If the tokenization computer 170 did not modify the authorization request message to include the token, the transaction processing computer 150 may modify the authorization request message to include the token.

[0089] At step S12, the transaction processing computer 150 may then transmit the authorization request message to the authorizing computer 160. After receiving the authorization request message, the authorizing computer 160 may then determine if the transaction is authorized. It may do this by determining if there are sufficient funds or credit in the account associated with the account identifier in the authorization request message. It may also conduct any independent fraud screening on the transaction.

[0090] At step S13, the authorizing computer 160 may transmit an authorization response message comprising the account identifier back to the transaction processing computer 150. At step S14, the transaction processing computer 150 can then transmit the authorization response message or the information therein to the tokenization

computer 170. At step S15, the tokenization computer 170 may then return the authorization response message including the token or the token itself.

[0091] If the transaction processing computer 160 only receives the token, it may then modify the authorization response message to include the token and may transmit
5 the authorization response message comprising the token to the transport computer 140 in step S16. In steps S17 and S18, the authorization response message comprising the token is transmitted to the access device 125 via the resource provider computer 130. The resource provider may then store the token instead of the real account identifier. This improves data security, since the token is stored at the resource
10 provider instead of the real account identifier. If the resource provider experiences a data breach and the token is improperly obtained, it is of limited or no use.

[0092] At the end of the day or at any other suitable time period, a clearing and settlement process, as is known in the art, may be performed between the transport
15 computer 140, the transaction processing computer 150, and the authorizing computer 160.

[0093] Although FIG. 1 shows and describes transaction processing computer 150 that detokenizes a payment token and a transaction cryptogram and that determines a token assurance level, it is understood that these functions could alternatively be performed by other computers including the transport computer 140, the
20 transaction processing computer 150, and/or the authorizing computer 160.

[0094] Although the above-described embodiment relates to payments, embodiments of the invention are not limited to payments. FIG. 5 shows a block diagram of a second transaction system according to embodiments of the invention. Steps in a process flow for a user obtaining access to a building are shown are shown
25 in FIG. 5.

[0095] In FIG. 5, the mobile device 15, the access device 125, the resource provider computer 130, and the tokenization computer 170 are described above, and the descriptions need not be repeated here. However, FIG. 5 also shows a user 110

that wishes to enter a building 180, where access to the building is restricted by the access device 125.

5 **[0096]** At step S111, the access device 125 may generate transaction information such as an access device identifier, a transaction request time, and an access device location. This information may be provided to the mobile device 115 in step S112.

[0097] At step S113, the mobile device 115 may transmit the information from the access device 125 and information from the mobile device 115 (e.g., the location of the mobile device 115, a mobile device identifier, a real account identifier, a request time, etc.) to the tokenization computer 170.

10 **[0098]** At step S114, the tokenization computer may then generate a cryptogram and obtain a token for the user 110, and may transmit them back to the mobile device 115 in step S115. Once the mobile device 115 obtains the token and the cryptogram, these may be transmitted to the access device 125 in step S116.

15 **[0099]** At step S117, the access device 125 may transmit the token and the cryptogram to the tokenization computer 170 and the tokenization computer 170 may determine that the cryptogram and the cryptogram are valid and may provide this indication to the access device 125 (step S118). After the access device 125 receives this information, the user 110 may be allowed to pass into the building 180 as shown in step S120.

20 **[0100]** A computer system may be used to implement any of the entities or components described above. The subsystems in such a system may be interconnected via a system bus. Additional subsystems include a printer, keyboard, fixed disk, and monitor, which is coupled to display adapter. Peripherals and input/output (I/O) devices, which couple to I/O controller, can be connected to the
25 computer system by any number of means known in the art, such as a serial port. For example, serial port or external interface can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor to communicate with each subsystem and to control the execution of instructions from

system memory or the fixed disk, as well as the exchange of information between subsystems. The system memory and/or the fixed disk may embody a computer-readable medium.

[0101] Embodiments of the invention have a number of advantages. For example, by providing a cryptogram with embedded information including data from an access device and a communication device, a token that is used with that cryptogram can be verified for its authenticity. Further, because the cryptogram is created using transaction data, the characteristics of the transaction can be verified to ensure that the transaction characteristics were not tampered with by a resource provider.

[0102] As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably-programmed computing device, microprocessor, data processor, or the like. The set of instructions or software code may be stored in a memory or other form of data storage element which is accessed by the computing device, microprocessor, etc. In other embodiments, the functions, processes, operations or method steps may be implemented by firmware or a dedicated processor, integrated circuit, etc.

[0103] It should be understood that the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to implement the present invention any combination of hardware and software.

[0104] Any of the software components or functions described herein 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.

[0105] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are
5 merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving access device data by a mobile communication device from an
3 access device;
4 generating, by the mobile communication device, a token request
5 including the access device data and communication device data;
6 sending, by the mobile communication device, the token request to a
7 server computer, wherein the server computer thereafter determines a token and
8 generates a cryptogram, the cryptogram generated using the access device data and
9 the communication device data;
10 receiving, by the mobile communication device, the token and the
11 cryptogram; and
12 providing, by the mobile communication device, the token and the
13 cryptogram to the access device, wherein the access device forwards the cryptogram
14 and the token to the server computer, which verifies the cryptogram and processes the
15 token,
16 wherein the access device data comprises location information of the
17 access device, and wherein the communication device data comprises location
18 information of the communication device, and
19 wherein the cryptogram is generated using token specific information, the
20 token specific information including when the token was requested.

1 2. The method of claim 1, wherein the access device data was
2 present in a two-dimensional code displayed on the access device.

1 3. The method of claim 1, wherein the access device data comprises
2 a resource provider ID and a transaction initiate timestamp.

1 4. A communication device comprising;
2 a processor, and

3 a computer readable medium, the computer readable medium comprising
4 code, executable by the processor, for implementing a method comprising:
5 receiving access device data from an access device;
6 generating a token request including the access device data and
7 communication device data;
8 sending the token request to a server computer, wherein the server
9 computer thereafter determines a token and generates a cryptogram, the cryptogram
10 generated using the access device data and the communication device data;
11 receiving the token and the cryptogram; and
12 providing the token and the cryptogram to the access device, wherein the
13 access device forwards the cryptogram and the token to the server computer, which
14 verifies the cryptogram and processes the token,
15 wherein the access device data comprises location information of the
16 access device, and wherein the communication device data comprises location
17 information of the communication device, and
18 wherein the cryptogram is generated using token specific information, the
19 token specific information including when the token was requested.

1 5. The communication device of claim 4, wherein the access device
2 data was present in a two-dimensional code displayed on the access device.

1 6. The communication device of claim 4, wherein the access device
2 data comprises a resource provider ID and a transaction initiate timestamp.

1 7. A method comprising:
2 providing, by an access device, access device data to a mobile
3 communication device, wherein the mobile communication device generates a token
4 request including the access device data and communication device data and sends the
5 token request to a server computer, which returns a token and a token cryptogram to
6 the mobile communication device;
7 receiving, by the access device, the token and the cryptogram from the
8 mobile communication device;

9 generating, by the access device, an authorization request message; and
10 transmitting, by the access device, the authorization request message to
11 the server computer, wherein the server computer verifies the cryptogram and
12 processes the transaction using the token,
13 wherein the access device data comprises location information for the
14 access device, and wherein the communication device data comprises location
15 information for the communication device, and
16 wherein the cryptogram is generated using token specific information, the
17 token specific information including when the token was requested.

1 8. The method of claim 7, wherein the access device data was
2 present in a two-dimensional code displayed on the access device.

1 9. An access device comprising:
2 a processor; and
3 a computer readable medium, the computer readable medium comprising
4 code, executable by the processor, for implementing a method comprising:
5 providing access device data to a mobile communication device, wherein
6 the mobile communication device generates a token request including the access
7 device data and communication device data and sends the token request to a server
8 computer, which returns a token and a token cryptogram to the mobile communication
9 device;
10 receiving, by the access device, the token and the cryptogram from the
11 mobile communication device;
12 generating an authorization request message; and
13 transmitting the authorization request message to the server computer,
14 wherein the server computer verifies the cryptogram and processes the transaction
15 using the token,
16 wherein the access device data comprises location information for the
17 access device, and wherein the communication device data comprises location
18 information for the communication device, and

19 wherein the cryptogram is generated using token specific information, the
20 token specific information including when the token was requested.

1 10. The access device of claim 9, wherein the access device data was
2 present in a two-dimensional code displayed on the access device.