TOKEN PROVISIONING UTILIZING A SECURE AUTHENTICATION SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This international application claims priority to U.S. Patent Application No. 15/649,923, filed on July 14, 2017, the disclosure of which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Tokens are substitutes for real credentials such as payment credentials. Tokens can be used instead of real credentials to conduct transactions such as payment transactions. Tokens provide greater data security relative to real credentials, because if token are stolen by unauthorized persons, the real credentials are not exposed. The token can be deactivated without compromising the real credential associated with the token.

[0003] The process of token issuance typically involves a token requestor requesting a token. A token service can evaluate the token request, and can issue a token to the token requestor if it is valid.

[0004] If a token is used in a transaction such as a payment transaction, the user of the token may be required to perform an authentication process before the transaction can proceed. This can involve a computer requesting a secret from the user.

[0005] It is apparent that when conducting a transaction using a token, a number of steps are required. While the number of steps required to complete a single transaction may not appear at first glance to be problematic, when millions of transactions are taking place, the burden to computing resources in a computer network can be significant.

[0006] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0007] One embodiment of the invention is directed to a method of provisioning a token. The method may comprise receiving, by a resource provider computer associated with a resource provider, transaction data corresponding to a transaction associated with a user. The method may further comprise transmitting, by the resource provider computer to a directory server computer, an authentication request message including the transaction data and a token request indicator. The directory server computer may subsequently transmit the authentication request message to an access control server computer associated with an authorizing entity. Receipt of the authentication request message may cause the access control server computer to authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer. The method may further comprise receiving, by the resource provider computer from the directory server computer, the authentication response message comprising the verification value, and a token, wherein the token is previously obtained by the directory server from a token provider computer.

[0008] Another embodiment of the invention is directed to a resource provider computer comprising a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor, for implementing a method. The method may comprise receiving transaction data corresponding to a transaction associated with a user. The method may further comprise transmitting, to a directory server computer, an authentication request message including the transaction data and a token request indicator. The directory server computer may subsequently transmit the authentication request message to an access control server computer associated with an authorizing entity. Receipt of the authentication request message may cause the access control server computer to authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer. The method may further comprise receiving, from the directory server computer, the authentication response message comprising the verification value, and a token, wherein the token is previously obtained by the directory server from a token provider computer.

[0009] Another embodiment of the invention is directed to a directory server computer comprising a processor and a computer readable medium coupled to the

processor, the computer readable medium comprising code, executable by the processor, for implementing a method. The method may comprise receiving, from a resource provider computer, an authentication request message comprising transaction data for a transaction between a user and a resource provider. The method may further comprise sending the authentication request message to an access control server computer at an issuer. Receipt of the authentication request message may cause the access control server computer to authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer. The method may further comprise receiving, from the access control server computer, the authentication response message. The method may further comprise transmitting, to a token provider computer, a token request message including at least a portion of the transaction data. Receipt of the token request message may cause the token provider computer to generate a token corresponding to the transaction. The method may further comprise receiving, from the token provider computer, the token corresponding to the transaction. The method may further comprise transmitting, to the resource provider computer, an authentication response message comprising the token.

[0010] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0012] FIG. 2 shows a block diagram of a directory server computer according to some embodiments of the invention.

[0013] FIG. 3 shows a block diagram of a token provider computer according to some embodiments of the invention.

[0014] FIG. 4 shows a flow diagram of a method of provisioning a token within a secure authentication system according to some embodiments of the invention.

[0015] FIG. 5 shows a flow diagram of a method of provisioning a token cryptogram within a secure authentication system according to some embodiments of the invention.

[0016] FIG. 6 shows a flow diagram of a method of performing a transaction according to some embodiments of the invention.

DETAILED DESCRIPTION

[0017] Embodiments of the present invention may be directed at utilizing the infrastructure of a secure authentication system to provision a token to be used for a transaction. In some embodiments of the present invention, a user may initiate a transaction (e.g., via a user computing device). A resource provider computer may receive the transaction data and request (e.g., via an authentication request message) authentication of the user to be conducted through a secure authentication system. The authentication request message may include a token request indicator that may be used to specify that a token is needed for the transaction. Thus, as part of the authentication process for the user, a token may be requested without requiring the resource provider computer to request the token via a separate message. Once the user has been authenticated, or at any suitable time, a token may be generated. The token may be returned to the resource provider computer via an authentication response message traditionally used for authentication purposes. In some embodiments, the authentication response message may further include user-specific data provided from the authentication entity (e.g., from an access control server computer associated with an authorizing entity of the transaction).

[0018] Embodiments of the present invention may use an existing secure authentication system (e.g., Verified by Visa™, MasterCard SecureCode™, American Express SafeKey™) to perform authentication techniques.

[0019] Embodiments of the present invention may be used in transaction processing systems or may use data generated during transaction processing through a transaction processing system. Such embodiments may involve transactions between consumers and merchants.

[0020] Before discussing detailed embodiments of the invention, some descriptions of certain terms may be useful.

[0021] A "user computing device" may be any suitable device that can perform computations and that can communicate with other devices. A mobile device is an example of a computing device. Other types of computing devices may not be mobile.

[0022] A "mobile device" may comprise any electronic device that may be transported and operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (*e.g.*, 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (*e.g.*, cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, wearable devices (e.g., watches), vehicles (e.g., cars), 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 relay - both devices taken together may be considered a single mobile device).

[0023] A “secure authentication system” may one or more computing devices (e.g., servers) that provide secure authentication of users with respect to transactions conducted between two entities (e.g., users and resource providers).

[0024] A “resource provider” may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of a resource provider includes merchants, access devices, secure data access points, etc. A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services. In some embodiments, the messages sent and/or received by the resource provider computer may be sent/received by a resource provider plug-in module that may function as a proxy between a resource provider computer and an authorizing entity computer or other components within the system.

[0025] 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.”

[0026] 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 computer” may be operated by, or on behalf of, an authorizing entity. An authorizing entity computer may include an “access control server computer” that may be configured to authenticate a user.

[0027] An “access control server computer” may be configured to authenticate a user. An access control server computer can receive authentication request messages. An access control server computer may be configured to transmit challenge request messages and receive challenge response messages from a user computing device (or application operating thereon) or a service provider computer. In some embodiments, the access control server computer may be further configured to verify the enrollment of an account in a secure authentication program, perform a risk analysis to determine whether the transaction should be authenticated, and return an authentication response message to a resource provider computer (e.g., via a directory server computer).

[0028] A "directory server computer” may include a server that can perform message routing. In some embodiments, the directory server computer may be capable of receiving messages (e.g., authentication request messages, authentication response messages, etc.), determining the appropriate destination computer for the received messages, and routing the received messages to the appropriate destination computer (e.g., an access control server computer). In some embodiments, the directory server computer may include or be associated with a database containing routing tables that may be used to determine an appropriate authorizing entity computer associated with an account identifier (e.g., a bank identification number). In some embodiments, the directory server computer may be further configured to perform an enrollment verification process for an account identifier and a risk analysis process.

[0029] A “transaction processing server computer” may include a server computer used for transaction processing. In some embodiments, the transaction processing server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The transaction processing server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In some embodiments, the transaction processing server computer may operate multiple server computers. In such

embodiments, each server computer may be configured to process transaction for a given region or handles transactions of a specific type based on transaction data.

[0030] The transaction processing server computer may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary transaction processing server computer may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system, which performs clearing and settlement services. The transaction processing server computer may use any suitable wired or wireless network, including the Internet.

[0031] The transaction processing server computer may process transaction-related messages (e.g., authorization request messages and authorization response messages) and determine the appropriate destination computer (e.g., issuer computer) for the transaction-related messages. In some embodiments, the transaction processing server computer may authorize transactions on behalf of an issuer. The transaction processing server computer may also handle and/or facilitate the clearing and settlement of financial transactions.

[0032] A “transaction request message” may be an electronic message that indicates that the user has initiated a transaction with a resource provider. A transaction request message may include transaction data associated with the transaction.

[0033] A “transaction response message” may be an electronic message that is used to respond to a transaction request message. In some embodiments, the transaction response message may indicate that the transaction associated with a transaction request message was successful or unsuccessful.

[0034] “Transaction data” may include data related to a transaction. Transaction data may include data for a specific transaction, including items purchased, item prices, total cost, shipping address, billing address, payment methods (e.g., a primary account number, card number, etc.), resource provider data (e.g., merchant data), user-specific data, user computing device data, etc.

[0035] “User computing device data” may include data associated with a user computing device. User computing device data may refer to data regarding a portable

computing device, such as a computer or mobile phone. Examples of user computing device data may include unique device identifiers for a computer or mobile phone, an IP address, SIM card data, application data, mobile application data, browser data, and device make and model data. User computing device data may also include the device's MSISDN, or Mobile Subscriber Integrated Services Digital Network-Number, which is a number that uniquely identifies a subscription in a mobile network.

[0036] "User-specific data" may include data specific to a user. User-specific data may include a name, mailing address, shipping address, billing address, phone number, payment account number, date of birth, marital status, income, social security number, demographic data, etc. In some embodiments, user-specific data may also include consumer preferences, notification methods, and prior transaction history.

[0037] A "challenge request message" may include a message sent as part of an authentication process for a user and/or user computing device. In some embodiments, the challenge request message may contain a request for the user to submit a pre-established authentication data in order to authenticate an account or payment device. The challenge request message may be generated and sent (e.g., by an access control server computer) prior to authenticating the account or payment device.

[0038] A "challenge response message" may include a message sent as part of an authentication process for a user and/or user computing device. In some embodiments, the challenge response message may be transmitted from a user computing device to an access control server computer or a directory server computer. The challenge response message may contain authentication data in order to authenticate an account or payment device.

[0039] **"**Authentication data" may include any data suitable for authenticating a user or mobile device. Authentication data may be initially 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), 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, biometric information of the user, phone numbers, IMEI numbers, etc.

[0040] 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.

[0041] A “token request indicator” may be value or flag that indicates a token is being requested.

[0042] 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.

[0043] “Tokenization” is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

[0044] A “token provider computer” can be any suitable device that that services tokens. In some embodiments, a token provider computer can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to values (e.g., primary account numbers (PANs)) in a repository (e.g. token vault). The token provider computer may include or be in communication with a token vault where the generated tokens are stored. The token provider computer may support token processing of transactions (e.g., payment transactions) submitted using tokens by de-tokenizing the token to obtain the original value (e.g., the PAN). In some embodiments, any suitable component of a secure

authentication system may assume the roles of the token provider computer. For example, directory server computers and/or access control server computers may become a token provider by implementing the token provider services of a token provider computer according to embodiments of the present invention.

[0045] A "token cryptogram" may include a token authentication verification value (TAVV) associated with a token. A token cryptogram may be a string of numbers, letters, or any other suitable characters, of any suitable length. In some embodiments, a token cryptogram may include encrypted token data associated with a token (e.g., a token domain, a token expiry date, etc.). A token cryptogram may be used to validate the token. For example, a token cryptogram may be used to validate that the token is being used within a token domain and/or by a token expiry date associated with the token.

[0046] A "token domain" may indicate an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and resource provider identifiers (e.g., 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 transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular resource provider (e.g., a merchant) that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0047] "Token expiry date" may refer to the expiration date/time of the token. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0048] A "token request message" may be a message for requesting a token and/or a cryptogram. If the token request message is used to request only a

cryptogram, it may be referred to as a “cryptogram request message.” A token request message may include a token requestor identifier associated with a token requestor (e.g., a directory server computer, a resource provider entity/computer, an authorizing entity/computer, or any suitable requestor). A token request message may include the payment credentials, which may be encrypted. A token request message may also include transaction data, a cryptogram, and a digital certificate (e.g., which may be signed by a key held by the token requestor), and/or any other suitable information. In some embodiments, the token request message may have an indication that it was sent by the resource provider computer on behalf of the user, and may include any suitable user information.

[0049] A “token response message” may be a message that responds to a token token request message. If the token response message is used to respond only to a cryptogram request, it may be referred to as a “cryptogram response message.” A token response message may include a token requestor identifier associated with a token requestor (e.g., a directory server computer, a resource provider entity/computer, an authorizing entity/computer, or any suitable requestor) and a token and/or a token cryptogram.

[0050] A “transaction” may include an exchange or interaction between two entities. In some embodiments, a transaction may refer to a transfer of value between two users (e.g., individuals or entities). A transaction may involve the exchange of monetary funds, or the exchange of goods or services for monetary funds between two individuals or entities. In other embodiments, the transaction may be a purchase transaction involving an individual or entity purchasing goods or services from a merchant or other entity in exchange for monetary funds. In other embodiments, the transaction may be a non-financial transaction, such as exchanging of data or information between two entities, such as the transfer of data. Examples of non-financial transactions may include transactions verifying a user’s age or identity (e.g., verifying identity with a government agency, verifying age for the purchase of alcohol).

[0051] An “authentication request message” may include a message sent as part of an authentication process. The authentication request message may request an authentication process be performed for a user, a user computing device, or a payment device.

[0052] An "authentication response message" may include a message sent as part of an authentication process in response to an authentication request message. An authentication response message may include the results of an authentication process based on data received in the authentication request message.

[0053] A "payment device" may include a device that can be used to perform a payment transaction. Payment device may be linked to a financial account associated with the holder of the payment device, and may be useable to provide payment information for a transaction. Payment devices can include debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a pre-paid or stored value cards). Payment devices can also include mobile phones, tablet computers, personal digital assistants (PDAs), portable computers, smart cards, and the like. Other payment devices may include non-physical forms of payment (e.g., virtual wallets, virtual accounts).

[0054] A "verification value" may be a value or a token that indicates successful authentication. A "verification value" may in the form of a digital signature. The digital signature may be a cryptogram that is generated after a computer such as an access control server signs transaction data with a key (e.g., a private or a symmetric key). An example of a verification value is a cardholder authentication verification value, or CAVV, that may be provided by an issuer associated with a payment device upon authentication of the payment device. The verification value may be used in processing a payment authorization for a financial transaction as proof that an issuer or other authorizing entity authenticated a user.

[0055] An "authorization request message" may be an electronic message that is sent to a transaction processing computer and/or an authorizing entity computer (e.g., 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 consumer 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.

[0056] An "authorization response message" may be an electronic message reply to an authorization request message generated by an authorizing entity computer 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 an authorizing entity (e.g., an issuer bank) returns in response to an authorization request message in an electronic message (either directly or through the transaction processing computer) to a resource provider computer that indicates approval of the transaction. The code may serve as proof of authorization. In some embodiments, a transaction processing computer may generate or forward the authorization response message to the resource provider.

[0057] 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.

[0058] A "processor" may refer to 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).

[0059] 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.

[0060] FIG. 1 shows a block diagram of a system 100 according to an embodiment of the invention. The system 100 may be used to facilitate data communications between the various computers depicted in FIG. 1 for authentication and/or authorizing financial and non-financial transactions. The system 100 includes a user computing device 102, a service provider computer 104, a resource provider computer 108, a directory server computer 110, an authorizing entity computer 112, a token provider computer, a transport computer 116, and a transaction processing computer 118. Each of these systems and computers may be in operative communication with each other. For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1. In addition, the components in FIG. 1 may communicate via any suitable communication medium (including the Internet), using any suitable communications protocol.

[0061] The user computing device 102 may be in any suitable form. For example, the user computing device 102 may be hand-held and compact so that they can fit into a user's pocket. Examples of a user computing device 102 may include any device capable of accessing the Internet. Specific examples of a user computing device 102 may include cellular or wireless phones (e.g., smartphones), tablet phones, tablet computers, laptop computers, desktop computers, personal digital assistants (PDAs), pagers, portable computers, smart cards, and the like.

[0062] The user computing device 102 may include a processor, memory, input/output devices, and a computer readable medium coupled to the processor. The computer readable medium may comprise code, executable by the processor for performing the functionality described below. The user computing device 102 may include a browser and/or applications (e.g., the browser application 102A, application 102B, etc.) stored in the memory and configured to retrieve, present, and send data across a communications network (e.g., the Internet).

[0063] The user computing device 102 may be configured to send data (e.g., utilizing browser application 102A and/or application 102B) to any suitable destination

(e.g., service provider computer 104) as part of a transaction request message. The data may include user computing device data, user-specific data, transaction data, or any suitable data. In some examples, the data may also include payment device data, geolocation data, user address, user email address, user phone number, account data, or other comparable data. In some embodiments, the browser application 102A or the application 102B used in the transaction may determine the particular data to be sent in an authentication request message. In some embodiments, the data that is sent in the authentication request message may be based on a resource provider category code for the resource provider in the transaction. For example, if the resource provider is a car rental agency, the number of days being reserved may be specifically sent as part of the transaction data in an authentication request message. In other embodiments, the data sent in the authentication request message may be dynamically determined based on the transaction data, the user-specific data, and the user computing device data.

[0064] The service provider computer 104 may be one or more computers provided by a resource provider (e.g., a merchant). In some embodiments, the service provider computer 104 may manage and provide services to a user via browser application 102A and/or an application associated with the service provider computer 104 (e.g., application 102B). The service provider computer 104 may be configured to send over-the-air (OTA) messages to the browser application 102A and/or the application 102B. In at least one example, the service provider computer 104 may be responsible for providing one or more network pages associated with the resource provider. This website may be configured to be accessible from an application (e.g., the browser application 102A, the application 102B, etc.) operating on the user computing device 102. The application 102B may be configured to receive and transmit transaction request/response messages using one or more service calls. The service provider computer 104 may be configured to handle service call requests from an application operating on the user computing device 102 (e.g., the browser application 102A and/or the application 102B). The service provider computer 104 may serve, in response to received requests, various user interfaces that may be rendered at the user computing device 102 (e.g., via the browser application 102A, the application 102B, etc.).

[0065] The service provider computer 104 may transmit and/or receive data through a communications medium to the user computing device 102, the resource provider computer 108, and/or the access control server computer 112A. The service provider computer 104 can be a large mainframe, a minicomputer cluster, or a group of

servers functioning as a unit. In one example, the service provider computer 104 may be a database server coupled to a Web server.

[0066] The resource provider computer 108 may include any suitable computational apparatus operated by a resource provider. The resource provider computer 108 may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for performing the functionality described herein. Examples of resource provider computer 108 may include an access device or a point of sale device. In some embodiments, the resource provider computer 108 may include a web server computer that may host one or more websites associated with the resource provider. Thus, the resource provider computer 108 may perform the functions described above in connection with the service provider computer 104. The resource provider computer 108 may be in any suitable form. Additional examples of a resource provider computer 108 include any device capable of accessing the Internet, such as a personal computer, cellular or wireless phones, personal digital assistants (PDAs), tablet computers, and handheld specialized readers.

[0067] In some embodiments, the resource provider computer 108 may be configured to send data to an access control server computer 112A via a directory server computer 110 as part of a authentication process for a transaction between the user (e.g., consumer) and the merchant. The resource provider computer 108 may also be configured to generate authorization request messages for transactions between the resource provider and a user, and route the authorization request messages to an authorizing entity computer 112 for additional transaction processing. In some embodiments, the messages sent by the resource provider computer 108 may be sent by a resource provider plug-in module 108A, which may function as a proxy between the resource provider computer 108 and the access control server computer 112A or other components within the system.

[0068] In some embodiments, the resource provider computer 108 may transmit data through a communications medium to a transport computer 116 as part of an authorization process for a transaction. In some embodiments of the invention, the resource provider computer 108 may receive transaction data from user computing device 102 and transmit the transaction data to the transport computer 116 for transaction-related processes (e.g., authorization) in an authorization request message. In such embodiments, the authorization request message may include a verification

value generated in the secure authentication process by the access control server computer 112A.

[0069] The directory server computer 110 may be a server computer configured to route messages between two computers. For example, the directory server computer 110 may route messages between the resource provider computer 108 and the access control server computer 112A. In some embodiments, the directory server computer 106 may route authentication request /response messages between the resource provider computer 108 (or resource provider plug-in module 108A) and the access control server computer 112A as part of a financial or non-financial transaction. In some embodiments, the directory server computer 106 may be operated by transaction processing computer 118.

[0070] In some embodiments, the directory server computer 110 may be configured to perform an enrollment verification process on behalf of the access control server computer 112A. In such embodiments, the directory server computer 110 may store data regarding accounts or account identifiers that are enrolled in the secure authentication program.

[0071] The authorizing entity computer 112 is typically associated with a business entity (e.g., a bank) which issues and maintains consumer accounts for a consumer. The authorizing entity computer 112 may issue payment devices for user accounts (e.g., consumer accounts), including credit cards and debit cards, and/or may provide user accounts stored and accessible via the user computing device 102. The authorizing entity computer 112 may be configured to conduct authorization processes. The authorizing entity computer 112 may include an access control server computer 112A. In other embodiments, the access control server computer 112A may be separate and distinct from the authorizing entity computer 112.

[0072] The access control server computer 112A may comprise a server computer that may be configured to conduct authentication processes. The access control server computer 112A may be associated with an issuer, which can be an authorization entity (e.g., bank, financial institution) that issues and maintains financial accounts for a user. The access control server computer 112A may use user-specific data, user computing device data, transaction data, PAN, payment device data, geolocation data, account data, or other comparable data, in order to perform an authentication for the transaction. In some embodiments, at the time of a transaction,

the access control server computer 112A may perform the authentication, and may provide an authentication response message to the resource provider computer 108 via the directory server computer 110. The authentication response message may provide an indication to the resource provider computer 108 that the account or user computing device has been authenticated or not authenticated. In other embodiments, the access control server computer 112A may be configured to send an authentication response message to the resource provider computer 108 directly via a direct connection. In some embodiments, the functions of the access control server computer 112A may be performed by the transaction processing computer 118 and/or the directory server computer 110 on behalf of an authorizing entity (e.g., an issue). In any example described herein, an authentication response message may be digitally signed by a component performing authentication operations (e.g., the access control server computer 112A).

[0073] The token provider computer 114 may include any suitable computational apparatus operated by a token provider. Token provider computer 114 may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for performing the functionality described herein. Token provider computer 114 can facilitate generating, maintaining, and/or issuing (provisioning, transmitting, etc.) tokens and/or token cryptograms, as well as maintaining an established mapping of tokens to information associated with a user (e.g., a PAN, a token cryptogram, etc.) in a repository (e.g. a token vault). The token provider computer 114 may include or be in communication with a token vault (e.g., one or more data stores) where the generated tokens and/or token cryptograms are stored. The token provider computer 114 may support token processing of transactions submitted using tokens by de-tokenizing the token to obtain underlying data (e.g., the PAN). In some embodiments, the token provider computer 114 may be configured to send/receive data to/from the directory server computer 110 or any suitable component of FIG. 1 configured to request tokens and/or token cryptograms.

[0074] The transport computer 116 is typically associated with a business entity (e.g., a commercial bank) that has a business relationship with a particular resource provider (e.g., a merchant) or other entity and that may be involved in the process of conducting transaction. The transport computer 116 may issue and manage accounts for resource providers and exchange funds with the authorizing entity computer 112 on

behalf of the resource provider. Some entities can perform both authorizing entity computer 112 and transport computer 116 functions. Embodiments of the present invention encompass such single entity issuer-acquirer computers.

[0075] The transaction processing computer 118 may include a network that includes or operates at least one server computer used for transaction processing (e.g., payment processing). The transaction processing computer 118 may include a processor and a computer readable medium coupled to the processor, the computer readable medium comprising code, executable by the processor for performing the functionality described herein. In some embodiments, the transaction processing computer 118 may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The transaction processing computer 118 may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In some embodiments, the transaction processing computer 118 may operate multiple server computers. In such embodiments, each server computer may be configured to process transaction for a given region or handles transactions of a specific type based on transaction data.

[0076] The transaction processing computer 118 may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary transaction processing computer 118 may include VisaNet™. Networks that include VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system, which performs clearing and settlement services. The transaction processing computer 118 may use any suitable wired or wireless network, including the Internet.

[0077] The transaction processing computer 118 may be configured to process authorization request messages and determine the appropriate destination (e.g., authorizing entity computer 112) for the authorization request messages. The transaction processing computer 118 may be configured to process authorization response messages (e.g., from an authorization entity computer 112) and determine the appropriate destination (e.g., the transport computer 116) for the authorization response

messages. The transaction processing computer 118 may also be configured to handle and/or facilitate the clearing and settlement of transactions.

[0078] FIG. 2 shows a block diagram 200 of a directory server computer (e.g., directory server computer 110 of FIG. 1) according to some embodiments of the invention.

[0079] The directory server computer 110 may comprise a processor 204, which may be coupled to a system memory 206 and an external communication interface 208. A computer readable medium 210 may also be operatively coupled to the processor 204. Computer readable medium 210 may also comprise code for implementing the methods discussed herein.

[0080] The computer readable medium 210 may comprise a number of software modules including a routing module 212, an enrollment verification module 214, a risk analysis module 216, an authentication module 218, and a token processing module 220. Although these various modules are depicted as being internal to the directory server computer 110, any number of these modules may instead be implemented as separate systems external to the directory server computer 110.

[0081] The routing module 212 may comprise code that, when executed, can cause the processor 204 to receive an authentication request message (e.g., from resource provider computer 108 of FIG. 1 or a corresponding resource provider plug-in module 108A). Upon receipt of the authentication request message, or at another suitable time, the routing module 212 may cause the processor 204 to retrieve routing data from routing data store 230, a data store configured to store routing data associated with routing message and/or information between one or more entities (e.g., between a resource provider computer and an access control server computer). Although the routing data store 230 is depicted as external to the directory server computer 110, it should be appreciated that the routing data store 230 may be stored locally with respect to the directory server computer 110 (e.g., in system memory 206) and/or any suitable storage location accessible and/or communicatively coupled to the processor 204. The routing module 212 may be configured to cause the processor to route the authentication request message to a destination (e.g., the access control server computer 112A of FIG. 1) according to the obtained routing data.

[0082] The routing module 212 may further comprise code that, when executed, can cause the processor 204 to receive an authentication response message (e.g., from

the access control server computer 112A). Upon receipt of the authentication response message, or at another suitable time, the routing module 212 may cause the processor 204 to retrieve routing data from routing data store 230 to identify a destination for the authentication response message (e.g., the resource provider computer 108 of FIG. 1). The routing module 212 may be configured to cause the processor 204 to transmit the authentication response message to the identified destination according to the obtained routing data.

[0083] The enrollment verification module 214 may comprise code that, when executed, can cause the processor 204 to access enrollment data to perform an enrollment verification process on behalf of an access control server computer (e.g., the access control server computer 112A). In such embodiments, the enrollment verification module 214 may be configured to cause the processor 204 to access previously-stored enrollment data to verify that the account associated with an authentication request message is enrolled in a secure authentication program. By way of example, the enrollment verification module 214 may cause the processor 204 to access enrollment data stored in the enrollment data store 232, a data store configured to store such information and accessible to the processor 204. If the account is not enrolled, the enrollment verification module 214 may be configured to cause the processor 204 to transmit an authentication response message indicating that the authentication request message was unsuccessful due to the lack of enrollment.

[0084] The risk analysis module 216 may comprise code that, when executed, can cause the processor 204 to perform a risk analysis using user-specific data, user computing device data, and/or transaction data received in an authentication request message. In such embodiments, the processor 204 may calculate a risk score for the transaction and transmit the risk score (e.g., to the access control server computer 112A) for additional authentication processing.

[0085] In some embodiments, the authentication module 218 may comprise code that, when executed, causes the processor 204 to conduct a challenge process with the user computing device 102. In such embodiments, the authentication module 218 may be configured to cause the processor 204 to generate a challenge request message requesting a user provide a pre-established secure data element (e.g., password, token, biometric data) in order to authenticate the transaction and/or the payment device. The processor 204 may be configured to transmit the challenge request message to a user computing device and receive a challenge response message from the user computing

device corresponding to the request. In such embodiments, the authentication module 218 may be configured to cause the processor 204 to evaluate a secure data element (e.g., a password, a PIN, authentication data, etc.) received in a challenge response message and determine whether the received secure data element matches a stored secure data element. By way of example, the authentication module 218 may cause the processor 204 to access authentication data (e.g., the secure data element) stored in the authentication information data store 234, a data store configured to store such information and accessible to the processor 204.

[0086] Although depicted as functionality performed with respect to the directory server computer 110, it should be appreciated that in some embodiments functionality related to enrollment, risk analysis, and sending/receiving challenge request/response messages may be additionally, or alternatively, performed by an access control server computer (e.g., the access control server computer 112A).

[0087] In some embodiments, the token processing module 220 may comprise code that, when executed, causes the processor 204 to transmit a token request message and/or a cryptogram request message to a token provider (e.g., the token provider computer 114 of FIG. 1). In at least one embodiment, the token processing module 220 may further comprise code that causes the processor 204 to receive a token response message and/or a cryptogram response message. In at least one embodiment, the token processing module 220 may perform one or more of the functions described in connection with the token provider computer 114 described in connection with FIG. 3.

[0088] FIG. 3 shows a block diagram 300 of a token provider computer (e.g., token provider computer 114 of FIG. 1) according to an embodiment of the invention.

[0089] The token provider computer 114 may comprise a processor 304, which may be coupled to a system memory 306 and an external communication interface 308. A computer readable medium 310 may also be operatively coupled to the processor 304. Computer readable medium 310 may also comprise code for implementing the methods discussed herein.

[0090] The computer readable medium 310 may comprise a number of software modules including a registration module 312, a token generation module 314, a cryptogram generation module 316, and a token exchange module 318. Although these various modules are depicted as being internal to the token provider computer 114, any

number of these modules may instead be implemented as separate systems external to the token provider computer 114.

[0091] The registration module 312 may comprise code which can cause the processor 304 to register a token requestor entity with a token data store 330 and to generate a token requestor identifier for the registered entity. Some non-limiting examples of the token requestor entities may include authorizing entities (e.g., issuers), resource providers (e.g., merchants, e-commerce merchants, transit authorities, etc.), directory server computers, transaction processors (e.g., transaction processing computers), transport providers (e.g., acquirers), user computing devices, or subcomponents and applications thereof.

[0092] The registration module 312 may be configured to cause the processor 304 to receive registration information such as an entity name, contact information, an entity type (e.g., user, directory server computer, resource provider, service provider, transaction processor, authorizing entity, transport entity, etc.), and any other relevant information for token generation processing. In some examples, registration module 312 may be configured to cause the processor 304 to provide one or more interfaces for collecting registration information. Such interfaces may be provided by the processor 304 and rendered via an application and/or website managed by the processor 304 as part of the functionality of registration module 312. In some embodiments, the registration module 312 may cause the processor 304 to validate the information and store the token requestor details in the token data store 330. The registration module 312 may also generate a token requestor ID after successful registration. In some embodiments, the token requestor ID may be a ten digit numerical value. However, other formats of the token requestor identifier are possible. The registration module 312 may further be configured to transmit the token requestor ID to the token requestor.

[0093] The token generation module 314 may be configured to cause the processor 304 generate a token in response to a token request message from a token requestor (e.g., directory server computer 110 on behalf of the resource provider computer 108). In one embodiment, the token generation module 314 may cause the processor 304 to receive a token request message (e.g., a message including a token requestor ID, an account number (e.g., PAN), an expiration date, a CVV2, etc.). In some embodiments, the token generation module 314 may cause the processor 304 to validate the token requestor ID and generate a token (e.g., a token for the PAN). In one embodiment, the token generation module 314 may cause the processor 304 to

generate a token response message including the generated token. The token data store 330 may be utilized by the processor 304 to maintain a correlation (e.g., a mapping) between an account number (e.g., a PAN), a token requestor ID, and a token. In one embodiment, the token generation module 314 may determine if a token already exists in the token data store 330 for the account number associated with the token requestor ID before generating a new token. In some embodiments, if a token cannot be generated, a token response message may be transmitted by the processor 304 to the requestor (e.g., a directory server computer, a resource provider computer, etc.) indicating a reason the token cannot be generated.

[0094] The cryptogram generation module 316 may be configured to cause the processor 304 to receive a cryptogram request message from a cryptogram requestor (e.g., a directory server computer, a resource provider computer, etc.). The cryptogram generation module 316 may be configured to cause the processor 304 to generate a token cryptogram (e.g., a TAVV) corresponding to the cryptogram request message. The cryptogram generation module 316 may be configured to cause to the processor 304 to generate a cryptogram response message including the generated cryptogram. The cryptogram data store 332 may be utilized by the processor 304 to maintain a correlation (e.g., a mapping) between a cryptogram requestor ID, a token, and the cryptogram, or any suitable combination of the above. In some embodiments, if a cryptogram cannot be generated, the cryptogram response message may be transmitted by the processor 304 to the cryptogram requestor indicating a reason the cryptogram could not be generated. In at least one embodiment, the functionality of the cryptogram generation module 216 may be induced by executing code of the token generation module 314.

[0095] In some embodiments, a token and token cryptogram may be generated/provisioned as a result of a single token request message. In still further embodiments, a token and a token cryptogram may be maintained in a single data store in a common record/association. For example, instead of separate mappings, a single mapping including account information, a token, a token cryptogram, an account identifier (e.g., a PAN), and a token requestor ID may be maintained by the processor 304.

[0096] The token exchange module 318 may comprise code, executable by the processor 304, to cause the processor 304 to allow registered entities to request account information (e.g., a PAN) for a given token. For example, the transaction

processing computer 118 of FIG. 1 may issue a request for a token exchange during a transaction authorization process. In one embodiment, a registered entity can provide a token requestor ID and a token, or any suitable information to request the account information associated with the token. The token exchange module 318 may validate that the requesting entity is entitled to make a request for a token exchange. In one embodiment, the token exchange module 318 may be configured to cause the processor to validate the account information/token mapping (e.g., a PAN to token mapping). Upon successful validation, the token exchange module 318 may be configured to cause the processor 304 to retrieve the account information (e.g., the PAN) and provide it to the requesting entity. In one embodiment, if the account information/token mapping is not valid, an error message may be provided.

[0097] FIG. 4 shows a flow diagram of a method 400 of provisioning a token within a secure authentication system according to some embodiments of the invention.

[0098] The method may begin at step 1, where a user initiates a transaction. In some embodiments, the user may access an application stored on the user computing device 102 (e.g., browser application 102A or application 102B of FIG. 1) in order to initiate a transaction. The application may be associated with a service provider computer 104 operating a website on behalf of a resource provider. When the user has selected goods or services via the application, the user may proceed to a checkout process for the transaction. For example, the user may select a “Buy” or “Checkout” option presented on a display of the user computing device 102.

[0099] At step 2, the application on the user computing device 102 generates and sends a transaction request message to the service provider computer 104. In some embodiments, the transaction request message may include transaction data (including user-specific data and/or user computer device data) corresponding to the transaction initiated at step 1.

[0100] At step 3, the service provider computer 104 may forward the transaction request message to the resource provider computer 108 for processing. At step 4, in response to receiving the transaction request message, the resource provider computer 108 may be configured to generate and send an authentication request message to a directory server computer 110. The authentication request message may be sent over a secure connection by the resource provider computer 108 to the directory server computer 110. In at least some embodiments, the authentication request message may

be sent by a resource provider plug-in module (e.g., resource provider plug-in module 108A) of the resource provider computer 108.

[0101] The data sent in the authentication request message may include user computing device data (e.g., operating system data, browser data, mobile application data, geo-location data), user-specific data (e.g., user name, user address data, user email address, user phone number), and/or other transaction data (e.g., shopping cart data, payment device data, payment account number), and/or other comparable data. In some embodiments, the authentication request message may include a token request indicator indicating that a token is being requested. The token request indicator may be in the form of a flag or code comprising any suitable number or type of characters.

[0102] In some embodiments, the application stored on the user computing device 102 and/or the service provider computer 104 may store all the data for the resource provider within the application, and accessing the resource provider computer 108 may not be required. In such embodiments of the present invention, software and data libraries associated with the secure authentication process may be integrated into the application stored on the user computing device 102 and/or integrated into the service provider computer 104. In such embodiments, the software, application programming interfaces, and data libraries may enable the application and/or the service provider computer 104 to generate and format the authentication request message to perform the secure authentication process with the access control server computer 112A via the directory server computer 110. An application (e.g., the browser application 102A and/or application 102B) may also store software components for the resource provider plug-in module 108A, which may act as a proxy for re-directing the user computing device 102 to a web address (or URL) associated with the directory server computer 110 and/or the access control server computer 112A. Thus, in some embodiments, the authentication request message generated at step 4 may be generated and transmitted to the directory server computer 110 by the service provider computer 104 or the user computing device 102.

[0103] At step 5, the directory server computer 110 may identify and route the authentication request message to an appropriate access control server computer 112A associated with the received transaction data (e.g., payment device data, payment account number). In some embodiments, the directory server computer 110 may evaluate the data received in the authentication request message to identify a particular

access control server computer (e.g., access control server computer 112A) to which the authentication request message will be routed.

[0104] At step 6, the access control server computer 112A may receive the authentication request message from the directory server computer 110. The access control server computer 112A may then optionally perform an enrollment verification process and/or a risk analysis using the data received in the authentication request message.

[0105] In some embodiments, as part of the enrollment verification process, the access control server computer 112A may determine whether an account identifier (e.g., an account number) has been previously enrolled in the secure authentication program provided by the access control server computer 112A. The access control server computer 112A may contain or have access to a database that stores enrolled account identifiers. In some embodiments, when the account identifier is not enrolled in the secure authentication program, the access control server computer 112A may not perform an authentication for the transaction and return an authentication response message to the resource provider computer 108 via the directory server computer 110 indicating that no authentication process was performed.

[0106] In some embodiments, when the account identifier is enrolled in the secure authentication program, the access control server computer 112A may perform a risk analysis using the user-specific data, user computing device data, and transaction data received in the authentication request message. In some embodiments, the risk analysis may include analyzing previous transactions associated with the payment device, an account identifier, and/or the user computing device data. In some embodiments, the risk analysis may return a risk score associated with the transaction. The access control server computer 112A may evaluate the risk score against a pre-established risk threshold.

[0107] When the risk score is on a first side of the threshold (e.g., below the threshold), the transaction may be deemed to be low risk. In such situations, the access control server computer 112A may not require any interaction with the user or the user computing device 102 for additional authentication data. For example, where the risk score indicates that the transaction is low risk, steps 7 and 8 may not be required.

[0108] However, when the risk score is on a second side of the threshold (e.g., above the threshold), the transaction may be deemed to be high risk. In such situation,

the access control server computer 112A may require additional data from the user associated with the user computing device 102 in order to authenticate the transaction. By way of example, when the risk score is determined to be high risk, the process may continue to step 7 for further authentication processes (e.g., a challenge process).

[0109] In some embodiments, the enrollment verification process and the risk analysis using the data received in the authentication request message may be additionally, or alternatively, performed by the directory server computer 106 on behalf of the access control server computer 112A. In some embodiments, the risk score determined by the risk analysis by the directory server computer 110 may then be sent to the access control server computer 112A for further authentication operations.

[0110] In step 7, when the access control server computer 112A requires additional data to authenticate the transaction, the access control server computer 112A may initiate a challenge process with the user. The access control server computer 112A may generate and send a challenge request message to the user computing device 102. The challenge request message may request that the user associated with the user computing device provide a pre-established secure data element (e.g., password, token or biometric data). The challenge request message may be presented to the user on the display of the user computing device as a web interface sent across a communications network (e.g., Internet), or may be sent to the consumer via other types of communications (e.g., SMS messaging, email messaging). In some embodiments, the challenge request message may be sent directly from the access control server computer 112A to the user computing device 102. In other embodiments, the challenge request message may be sent to the user computing device 102 through the directory server computer 110 and/or the service provider computer 104. The challenge request message may be sent through the secure connection established by an application operating on the user computing device 102 (e.g., the browser application 102A and/or the application 102B).

[0111] In step 8, the user computing device 102 returns a challenge response message to the access control server computer 112A. The challenge response message may include the secure data element (e.g., authentication data) requested by the access control server computer 112A in the challenge request message. In some embodiments, the challenge response message may be sent directly to the access control server computer 112A from the user computing device 102. In other embodiments, the challenge response message may be sent from the user computing

device 102 to the access control server computer 112A through the service provider computer 104 and/or the directory server computer 110. The access control server computer 112A may evaluate the received secure data element against a pre-established secure data element stored by, or accessible to, the access control server computer 112A. When the received secure data element and the stored secure data element match or are within an expected range, the transaction may be authenticated.

[0112] In some embodiments, steps 7 and 8 may be repeated until either the number of times the secure data element can be requested from the user computing device 102 is exceeded, the access control server computer 112A successfully authenticates the user and generates the verification value, or the authentication is determined to be unsuccessful and the access control server computer 112A generates the authentication response message indicating a failed authentication. By way of example, when the received secure data element and the stored secure data element do not match or are not within an expected range, the access control server computer 112A may generate and transmit an authentication response message to the resource provider computer 108 via the directory server computer 110 that indicates that authentication has failed. Receipt of an authentication response message indicating that the authentication has failed may cause the resource provider computer 108 to transmit a transaction response message to the user computer device 102 via the service provider computer 104 indicating that the transaction has failed and further processing by the resource provider computer 108 may not be performed.

[0113] In step 9, the access control server computer 112A may generate and send an authentication response message to the directory server computer 110. The generated authentication response message may include a verification value for the transaction generated in response to a successful authentication. In some embodiments, the verification value may be a card authentication verification value ("CAVV"). This value can be a cryptogram that has any suitable number of characters (e.g., 3-10). In at least one embodiment, the authentication response message may include user-specific data provided by the access control server computer 112A which was not included in the received authentication request message. By including such user-specific data, the access control server computer 112A may provide information to the directory server computer 110 and/or the resource provider computer 108 (directly, or via the directory server computer 110) that was not otherwise available to the directory server computer 110 and/or resource provider computer 108. The user-

specific data may be utilized by the directory server computer 110 and/or the resource provider computer 108 for any suitable purpose including, but not limited to fraud detection, marketing, authentication, or the like.

[0114] At step 10, the directory server computer 110 may generate and transmit a token request message to token provider computer 114 in response to receiving the authentication response message corresponding to a authentication request message for which a token requestor indicator was included indicating that a token was being requested. The token request message may include a token requestor identifier (e.g., corresponding to the directory server computer 110, the resource provider computer 108, etc.) and transaction data (e.g., a PAN) received in the authentication request message.

[0115] At step 11, a token provider computer 114 may generate, store, and transmit a token in a token response message to the directory server computer 110. In some embodiments, the token provider computer 114 may maintain a mapping between transaction data (e.g., the PAN), the generated token, and the token requestor (e.g., the directory server computer 110, the resource provider computer 108, etc.). In some embodiments, the token generated may be shared by all resource providers serviced by the directory server computer 110. In other embodiments, the token may be generated for a particular resource provider serviced by the directory server computer 110. In some embodiments, the token provider computer 114 may be configured to generate a cryptogram in response to generating a token. The generated cryptogram may be stored in the mapping.

[0116] In some embodiments, limits may be placed on the generated token. For example, a token domain and/or a token expiration date may be configured such that the token may only be usable in a certain area (e.g. based on geo-location data), at the resource provider computer 108 (e.g. based on a merchant ID), for the amount of the current transaction, and/or for a certain time period. Additionally, or alternatively, the token may be a one-time use token, and it may only be eligible for the current transaction. In some embodiments, the token may be utilized for a purchase immediately after being requested, and accordingly it may be assigned a short lifespan (e.g., it may have an expiration time in the near future). For example, the token may only be valid for 1 hour, 10 minutes, 5 minutes, 1 minute, 30 seconds, or any other suitable amount of time. In some embodiments, the generated cryptogram may include

one or more token limitations/restrictions. The limitations/restrictions may be encrypted within the cryptogram.

[0117] In some embodiments, steps 10 and 11 may be conducted prior to the directory server computer 110 forwarding the authentication request message to the access control server computer 112A in step 5.

[0118] At step 12, the directory server computer 110 may transmit the authentication response message including the generated token and any suitable user-specific data provided by the access control server computer 112A to the resource provider computer 108. The authentication response message may be transmitted directly to the resource provider computer 108, or via the resource provider plug-in module 108A of FIG. 1. The direct connection may be a wired or wireless communications connection. In some embodiments, a generated cryptogram corresponding to the token may be included in the authentication response message.

[0119] At step 13, the resource provider computer 108 may receive the authentication response message including the verification value from the directory server computer 110. In embodiments where a cryptogram has not been provided, the resource provider computer 108 may then conduct a cryptogram request process discussed further in connection with FIG. 5. In some embodiments, the resource provider computer 108 may proceed to conduct an authorization process discussed further in connection with FIG. 6.

[0120] At step 14, the resource provider computer 108 may transmit a transaction response message to the service provider computer 104. The service provider computer 104 may then forward the transaction response message to the user computing device 102 (e.g., via browser application 102A or application 102B). The transaction response message may indicate that the authentication transaction was successful or unsuccessful. In some embodiments, transmitting the transaction response message may be dependent on completion of a cryptogram request process described in connection with FIG. 5 and/or an authorization process described in connection with FIG. 6.

[0121] It is understood that the flow may be different in other embodiments. For example, the authentication request and response messages may pass between the resource provider computer 108 and the access control computer 112A via the user computing device 102 instead of the directory server computer 110.

[0122] The embodiment described in FIG. 4 may include authenticating both financial and non-financial transactions. In the case of non-financial transactions, the process may be completed when the user computing device 102 receives the transaction response message from the service provider computer 104, as an authorization process may not be required. In some embodiments, a cryptogram request process need not be conducted prior to completing the process described in connection to FIG. 4.

[0123] FIG. 5 shows a flow diagram of a method 500 of provisioning a token cryptogram within a secure authentication system according to some embodiments of the invention.

[0124] The method may begin at 502, where the resource provider computer 108 may be configured to send a cryptogram request message to the directory server computer 110. The cryptogram request message may include a token requestor ID associated with the resource provider, a previously provisioned token, or any suitable information related to requesting a token cryptogram. It should be appreciated that although the method of 500 depicts transmission of a cryptogram request message to initiate token cryptogram generation, a token cryptogram may instead be generated at a same time as a token during the authentication process described in FIG. 4. Thus, a token cryptogram may be generated and provisioned (e.g., to the directory server computer 110, the resource provider computer 108, or other suitable token requestor) by a token provider computer 114 in response to receipt of a token request message (e.g., from the directory server computer 110).

[0125] At 504, the directory server computer 110 may transmit the cryptogram request message to the token provider computer 114. The token provider computer 114 (or a module of the token provider computer 114 such as the cryptogram generation module 316 of FIG. 3) may be configured to generate a token cryptogram at 506. The token cryptogram may include information related to the token such as a token domain and/or a token expiry date. In some embodiments, the token cryptogram may be used to verify that the token is being used in conformance with restrictions associated with the token. The token provider computer 114 may store the token cryptogram as an association with the token and the token requestor ID. The token provider computer 114 may then send a cryptogram response message to the directory server computer 110 at 508.

[0126] In some embodiments, as part of the method 500, the directory server computer 110 may transmit a data request message to the access control server computer 112A requesting current user-specific data at 510. The data request message may be formatted according to any suitable protocol. For example, the data request message may be formatted as an authentication request message with an indicator specifying that authentication processes should not occur and/or that current user-specific data is requested only.

[0127] At 512, the access control server computer 112A may receive the data request message and obtain current user-specific data for the user/user computing device. At 514, the access control server computer 112A may transmit a data response message to the data requestor (e.g., the directory server computer 110). The data response message may include the user-specific data provided by the access control server computer 112A. The data response message may be formatted according to any suitable protocol. For example, the data response message may be formatted as an authentication response message with an indicator specifying that message is providing current user-specific data. It should be appreciated that in some embodiments, steps 510-514 are not performed.

[0128] Although data is requested from the access control server computer 112A as part of the method 500, it should be appreciated that the directory server computer 110 (or any component of the system 100) may transmit a data request message to the access control server computer 112A requesting current user-specific data. A data response message including current user-specific data may be provided by the access control server computer 112A in response to the data request.

[0129] At 516, the directory server computer 110 may transmit a cryptogram response message to the resource provider computer 108. The cryptogram response message may include the generated cryptogram and any suitable user-specific information obtained from the access control server computer 112A.

[0130] FIG. 6 shows a flow diagram of a method 600 of performing a transaction according to some embodiments of the invention. The steps shown in the method 600 may be performed sequentially or in any suitable order in embodiments of the invention. In some embodiments, one or more of the steps may be optional.

[0131] The user may wish to purchase a good or service from the resource provider. At 602, in order to perform the purchase, the user may provide payment

credentials (e.g. via a transaction request message) to the service provider computer 104 (e.g., via the browser application 102A and/or the application 102B operating on the user computing device 102 of FIG. 1). For example, in some embodiments, the user may provide a PAN, a security code, an expiration date, a name, an address, a phone number, and/or any other suitable payment credentials via a website hosted by the service provider computer 104 and accessible via the browser application 102A and/or the application 102B.

[0132] At 604, the service provider computer 104 may transmit a transaction request message to the resource provider computer 108. Upon receipt, the resource provider computer 108 may be configured to initiate an authentication process and/or a cryptogram provisioning processing at 606. For example, the resource provider computer 108 may determine that a token may be requested for the payment credentials. By way of example, the resource provider computer 108 may determine that the transaction request message include a PAN and not a payment token. The resource provider computer 108 may initiate the authentication process to obtain a token and/or token cryptogram. In some embodiments, the authentication process may authenticate the transaction and provide a token and a separate cryptogram provisioning process may be initiated by the resource provider computer 108. The authentication process initiated may be in conformance with the method 400 described above in connection with FIG. 4. As part of the authentication process a token may be provisioned and returned to the resource provider computer 108. A cryptogram may be returned with the token, or as part of the cryptogram provisioning process described above in connection with FIG. 5.

[0133] In some embodiments, the resource provider computer 108 may erase any record of the payment credentials upon receipt of a token, such that the payment credentials are not stored at the resource provider computer 108. Thereafter, the resource provider computer 108 may utilize the token place of the payment credentials (e.g. for transaction authorization and record-keeping purposes).

[0134] In some embodiments, the resource provider computer 108 may already have access to a previously provisioned token that may be used for the transaction. In such embodiments, the resource provider computer 108 the method 600 may refrain from initiating an authentication process and/or a cryptogram provisioning processing at 606

[0135] At 608, the resource provider computer 108 may send an authorization request message for the transaction to the transport computer 116. In some embodiments, the authorization request message may include the token instead of the real payment credentials. The authorization request message may also include transaction data (e.g. items purchased, amount, etc.), resource provider information (e.g. merchant name, merchant ID, location, etc.), user-specific data, and any other suitable information.

[0136] At 610, the transport computer 116 may forward the authorization request message to the transaction processing computer 118. At step 612, the transaction processing computer 118 may forward the authorization request message to the authorizing entity computer 112 (corresponding to the payment credentials and/or token).

[0137] At 614, the authorizing entity computer 112 may detokenize the payment token and obtain the payment credentials. For example, the authorizing entity computer 112 may obtain the payment credentials from the token provider computer 114. In some embodiments, the authorizing entity computer 112 may obtain the payment credentials from a local token record database. In some embodiments, any other suitable entity may instead detokenize the payment token. For example, the transaction processing computer 118 may detokenize the payment token (via the token provider computer 114 or via a local token record database) before forwarding the authorization request message to the authorizing entity computer 112.

[0138] At 616, the authorizing entity computer 112 may authorize or reject the transaction based on the payment credentials. For example, the authorizing entity computer 112 may identify the payment account associated with the payment credentials and/or payment token, and may determine whether there are sufficient funds.

[0139] At 618, the authorizing entity computer 112 may send an authorization response indicating whether the transaction was authorized to the transaction processing computer 118. The authorization response message may include the payment token, transaction details, merchant information, and any other suitable information. In some embodiments, in order to protect the payment credentials by limiting exposure, the authorization response message may not include the payment credentials.

[0140] At 620, the transaction processing computer 118 may forward the authorization response message to the transport computer 116. At 622, the transport computer 116 may forward the authorization response message to the resource provider computer 108.

[0141] At 624, the resource provider computer 108 may release the purchased goods and/or services to the user based on the authorization response message. Further, the resource provider computer 108 may store a transaction record including the payment token, user information, transaction details, and any other suitable information. In some embodiments, the resource provider computer 108 may erase any sensitive information, such as the encrypted or unencrypted payment credentials, but the resource provider computer 108 may store remaining information, such as the payment token.

[0142] At 626, the resource provider computer 108 may transmit a transaction response message to the service provider computer 104 indicating that the transaction was successful or unsuccessful. The transaction response message may be forwarded from by the service provider computer 104 to the user computing device 102 at 628. In some embodiments, information from the transaction response message may be provided for display on the user computing device 102.

[0143] At the end of the day or at another time, a clearing and settlement process can take place. The token may be used by the resource provider computer 108, the token provider computer 114, and the transaction processing computer 118 to determine the real account identifier. This real account identifier may then be used with to settle the transaction with the authorizing entity computer 112 via the transaction processing computer 118.

[0144] Embodiments of the present invention may also provide for faster transaction processing as it reduces the friction that occurs in transactions by combining a token request process within a secure authentication process conducted by a secure authentication system. While conventional systems require separate messages to be transmitted to request authentication and token provisioning, the methods and systems provided herein enable authentication and token provisioning to occur by initiating a single message (e.g., an authentication request message). Additionally, while conventional authentication response message provided information related to authentication success/failure, the techniques described herein enable additional

information (e.g., user-specific information) to be communicated within an authentication response message. Thus, alleviating the need for a separate interface and/or an additional message to be utilized in order to obtain such information as would be found in conventional systems.

[0145] Reducing the number of messages need to perform multiples tasks (e.g., token provisioning, authentication, data requests) also has the benefit of reducing the amount of system resources required perform such tasks between multiple computers systems and devices.

[0146] The various participants and elements described herein may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in the above-described figures, including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

[0147] A computer system may be utilized to implement any of the entities or components described above. Subsystems of the computer system may be interconnected via a system bus. Additional subsystems may include a printer, a keyboard, a fixed disk (or other memory comprising computer readable media), a monitor, which is coupled to a display adapter, and others. Peripherals and input/output (I/O) devices, which couple to an I/O controller (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as by a serial port. For example, the 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. In some embodiments, the monitor may be a touch sensitive display screen.

[0148] Specific details regarding some of the above-described aspects are provided above. The specific details of the specific aspects may be combined in any suitable manner without departing from the spirit and scope of embodiments of the technology. For example, back end processing, data analysis, data collection, and other transactions may all be combined in some embodiments of the technology. However,

other embodiments of the technology may be directed to specific embodiments relating to each individual aspect, or specific combinations of these individual aspects.

[0149] It should be understood that the present technology as described above can be implemented in the form of control logic using computer software (stored in a tangible physical medium) in a modular or integrated manner. While the present invention has been described using a particular combination of hardware and software in the form of control logic and programming code and instructions, it should be recognized that other combinations of hardware and software are also within the scope of the present invention. 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 technology using hardware and a combination of hardware and software

[0150] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0151] The above description is illustrative and is not restrictive. Many variations of the technology will become apparent to those skilled in the art upon review of the disclosure. The scope of the technology should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0152] In some embodiments, any of the entities described herein may be embodied by a computer that performs any or all of the functions and steps disclosed.

[0153] 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 technology.

[0154] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0155] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

1. A computer-implemented method for provisioning a token, comprising:

receiving, by a resource provider computer associated with a resource provider, transaction data corresponding to a transaction associated with a user;

transmitting, by the resource provider computer to a directory server computer, an authentication request message including the transaction data and a token request indicator, wherein the directory server computer subsequently transmits the authentication request message to an access control server computer associated with an authorizing entity, wherein receipt of the authentication request message causes the access control server computer to authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer; and

receiving, by the resource provider computer from the directory server computer, the authentication response message comprising the verification value, and a token, wherein the token is previously obtained by the directory server from a token provider computer.

2. The computer-implemented method of claim 1, further comprising:

generating, by the resource provider computer, an authorization request message comprising the token; and

transmitting, by the resource provider computer, the authorization request message comprising the token to an authorization entity computer for the transaction.

3. The computer-implemented method of claim 2, further comprising:

transmitting, by the resource provider computer to the directory server computer, a cryptogram request message associated with the token, wherein receipt of the cryptogram request message causes the directory server computer to:

transmit a cryptogram request message to the token provider computer; and

receive a cryptogram response message comprising a cryptogram associated with the token from the token provider computer; and

receiving, by the resource provider computer, the cryptogram response message comprising the cryptogram associated with the token, wherein the authorization request message further comprises the cryptogram associated with the token.

4. The computer-implemented method of claim 3, wherein the receipt of the cryptogram request message associated with the token further causes the directory server computer to:

transmit a data request message to the access control server computer; and

receive, from the access control server computer, a data request message comprising user-specific data associated with the user.

5. The computer-implemented method of claim 4, wherein the authentication response message received from the directory server computer further comprises the user-specific data received from the access control server computer.

6. The computer-implemented method of claim 1, wherein receipt of the authentication request message further causes the access control server computer to provide user-specific data associated with the user within the authentication response message transmitted to the directory server computer.

7. The computer-implemented method of claim 6, wherein the user-specific data comprises at least one of: a billing address, a phone number, an electronic mail address, an account identifier, or transaction device data associated with the user.

8. A resource provider computer, comprising:

a processor, and

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

receiving transaction data corresponding to a transaction associated with a user;

transmitting, to a directory server computer, an authentication request message including the transaction data and a token request indicator, wherein the directory server computer subsequently transmits the authentication request message to an access control server computer associated with an

authorizing entity, wherein receipt of the authentication request message causes the access control server computer to authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer; and

receiving, from the directory server computer, the authentication response message comprising the verification value, and a token, wherein the token is previously obtained by the directory server from a token provider computer.

9. The resource provider computer of claim 8, the method further comprising:

generating an authorization request message comprising the token; and

transmitting the authorization request message comprising the token to an authorization entity computer for the transaction.

10. The resource provider computer of claim 9, the method further comprising:

transmitting, to the directory server computer, a cryptogram request message associated with the token, wherein receipt of the cryptogram request message causes the directory server computer to:

transmit a cryptogram request message to the token provider computer; and

receive a cryptogram response message comprising a cryptogram associated with the token from the token provider computer; and

receiving the cryptogram response message comprising the cryptogram associated with the token, wherein the authorization request message further comprises the cryptogram associated with the token.

11. The resource provider computer of claim 10, wherein the receipt of the cryptogram request message associated with the token further causes the directory server computer to:

transmit a data request message to the access control server computer; and

receive, from the access control server computer, a data request message comprising user-specific data associated with the user.

12. The resource provider computer of claim 11, wherein the authentication response message received from the directory server computer further comprises the user-specific data received from the access control server computer.

13. The resource provider computer of claim 8, wherein receipt of the authentication request message further causes the access control server computer to provide user-specific data associated with the user within the authentication response message transmitted to the directory server computer.

14. The computer-implemented method of claim 13, wherein the user-specific data comprises at least one of: a billing address, a phone number, an electronic mail address, an account identifier, or transaction device data associated with the user.

15. A directory server computer, comprising:

a processor, and

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

receiving, by a directory server computer from a resource provider computer, an authentication request message comprising transaction data for a transaction between a user and a resource provider;

sending, by the directory server computer, the authentication request message to an access control server computer at an issuer, wherein receipt of the authentication request message causes the access control server computer authenticate the user, generate a verification value representing the authentication, and transmit an authentication response message comprising the verification value to the directory server computer;

receiving, by the directory server computer from the access control server computer, the authentication response message;

transmitting, by the directory server computer to a token provider computer, a token request message including at least a portion of the transaction data, wherein receipt of the token request message causes the token provider computer to generate a token corresponding to the transaction;

receiving, by the directory server from the token provider computer, the token corresponding to the transaction; and

transmitting, by the directory server computer to the resource provider computer, an authentication response message comprising the token.

16. The directory server computer of claim 15, the method further comprising:

receiving, from a resource provider computer, a cryptogram request message for a cryptogram associated with the token;

transmitting a cryptogram request message to the token provider computer, wherein receipt of the cryptogram request message causes the token provider computer to generate the cryptogram;

receiving a cryptogram response message comprising the cryptogram; and

transmitting the cryptogram response message comprising the cryptogram to the resource provider computer.

17. The directory server computer of claim 15, wherein the method further comprises:

transmitting a data request message to the access control server computer; and

receiving, from the access control server computer, a data request message comprising user-specific data associated with the user.

18. The directory server computer of claim 15, wherein the authentication response message transmitted by the directory server computer further comprises the user-specific data received from the access control server computer.

19. The directory server computer of claim 15, wherein receipt of the authentication request message further causes the access control server computer to provide user-specific data associated with the user within the authentication response message received by the directory server computer.

20. The directory server computer of claim 19, wherein the user-specific data comprises at least one of: a billing address, a phone number, an electronic mail address, an account identifier, or transaction device data associated with the user.