

ACCESS IDENTIFIER PROVISIONING TO APPLICATION

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application is a non-provisional of and claims the benefit of the filing
5 date of U.S. Provisional Application No. 62/427,046, filed on November 28, 2016, which
is herein incorporated by reference in its entirety.

BACKGROUND

[0002] There are many different types of systems and methods that allow a user
to access resources. Such systems and methods can be inconvenient and the security
10 of such systems and methods can be improved.

[0003] In one example of a conventional system for accessing secure data, a
user operating a user device needs to register with a computer that is used to access
the secure data. The computer is operated by a service provider. It is relatively
straightforward for the user to access the secure data if the user has an account with
15 that service provider. However, if the user does not have such an account, then the
user will be unable to access the secure data. Furthermore, even if the user has an
account to access the secure data, the credentials associated with the account that are
used to access the secure data constitute sensitive information. Such sensitive
information is susceptible to being illegally obtained from unauthorized persons.

20 **[0004]** In another example, a user may wish to conduct a specific interaction with
a particular resource provider or an application computer associated with an application
on the user's user device (e.g., a ride-sharing application). In order to do so, the user
may be asked to provide a payment credential such as a credit card number. While this
is relatively straightforward if the user has a credit card, it is not if the user does not
25 have a credit card. If the user does not have a credit card, then the user is not able to
conduct the desired interaction. Furthermore, even if the user does have a credit card
account to conduct the desired interaction, the credit card number that is used to access
the secure data constitutes sensitive information. The credit card number is susceptible
to being illegally obtained from unauthorized persons. Still further, the issuance of a

payment device identifier such as a credit card number is slow as it can take 3-5 days to issue.

[0005] Embodiments of the invention address these and other problems.

5

BRIEF SUMMARY

[0006] Embodiments of the invention relate to systems and methods for providing user devices with access tokens. Some embodiments of the invention can allow for the performance of on demand interactions such as payment transactions using third party applications. Embodiments of the invention can allow a user (e.g., a consumer), who may possess an account at an issuer, to use those accounts to quickly and conveniently conduct on demand payment transactions using third party online applications or platforms (e.g., an online messaging platform). Certain embodiments may be particularly useful to users of third party applications that possess an account at an authorizing entity such as an issuer, but do not possess portable transaction devices (e.g., debit cards). In embodiments of the invention, the issuer may pre-allocate a virtual access identifier such as a virtual primary account number to the account. By having the issuer pre-allocate a virtual primary account number (PAN) for each of the users, embodiments of the invention enable users to perform interactions such as payment transactions nearly instantaneously using the third party applications. The users do not need to first obtain portable payment devices.

[0007] One embodiment of the invention is directed to a method comprising: receiving, by a directory service computer from an application on a user device, a request to provide an access token that is associated with a primary access identifier for an account, the request comprising identifying information that identifies the account; retrieving, by the directory service computer, a virtual access identifier based on the identifying information; and transmitting a request, by the directory service computer to a token service computer, that the access token be provisioned, wherein the request comprises the virtual access identifier, and the token service computer thereafter

provisions the user device or an application computer associated with the user device with the access token.

[0008] Another embodiment of the invention is directed to a system comprising: a directory service computer, the directory service computer comprising a data processor, and a computer readable medium, the computer readable medium comprising code, executable by the data processor, to cause the directory service computer to receive from an application on a user device, a request to provide an access token that is associated with a primary access identifier for an account, the request comprising identifying information that identifies the account, retrieve a virtual access identifier based on the identifying information, and transmit a request, by the directory service computer to a token service computer, that the access token be provisioned, wherein the request comprises the virtual access identifier, and the token service computer thereafter provisions the user device or an application computer associated with the user device with the access token.

[0009] Another embodiment of the invention is directed to a method comprising: receiving, by a token service computer and from a directory service computer, a virtual access identifier and a request to provision a user device or an application computer associated with the user device with an access token; transmitting, by the token service computer, the access token to the user device or the application computer; receiving, by the token service computer, the access token, the access token being in an authorization request message; determining, by the token service computer, the virtual access identifier using the access token; and providing, by the token service computer, the virtual access identifier to a processing computer, the processing computer transmitting an authorization request message comprising the virtual access identifier to an authorizing computer for authorization, the authorizing computer using the virtual access identifier to determine a primary access identifier to conduct an interaction.

[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 illustrating a system as well as a process flow according to an embodiment of the invention.

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

[0013] FIG. 3 shows a block diagram of a directory service computer according to an embodiment of the invention.

[0014] FIG. 4 shows a block diagram of a token service computer according to an embodiment of the invention.

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

[0016] FIG. 6 shows a flowchart illustrating a method for provisioning a user device or an application computer with an access token.

[0017] FIG. 7 shows a flowchart illustrating a method for conducting an interaction after the user device or application computer receives the access token.

DETAILED DESCRIPTION

[0018] Before discussing specific embodiments and examples, some descriptions of terms used herein are provided below.

[0019] An “access token” may include a substitute identifier for some information. For instance, an access token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. In some cases, the token may be a payment token, which may include an identifier for a payment account that is a substitute for a real account identifier, such as a primary account number (PAN), or a virtual account identifier. For example, an access token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, an access

token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, an access token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction. The
5 access token may also be used to represent an original credential in other systems where the original credential would typically be provided. In some embodiments, an access token can be used to access secure data on a computer, or access a restricted location (e.g., a transit location or building).

[0020] A “primary access identifier” may include any suitable data that may allow
10 a user to access a resource such as data, goods, money, services, etc. In some embodiments, a “primary access identifier” may be a PAN (primary account number) that can be used to conduct a payment transaction, an original badge number that allows a person to access a particular location or particular data on a computer, insurance account numbers, etc. Other examples of primary access identifiers may
15 include checking account identifiers (e.g., numbers), savings account identifiers, money market account identifiers, brokerage account identifiers, etc. A “primary access identifier” may also be characterized as a “real access identifier.”

[0021] A “virtual access identifier” may include a proxy for a primary access identifier. In embodiments of the invention, a virtual access identifier cannot be used to
20 directly conduct an interaction to obtain a resource. For example, a virtual access identifier such as a virtual PAN may not be used to directly conduct a payment transaction. A virtual access identifier such as a virtual badge number cannot be used to directly access a building or secure data. In embodiments of the invention, the format of the virtual access identifier may be the same or different than the primary access
25 identifier.

[0022] “Account information” may refer to any information associated with a user’s account. Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include an account identifier, a username, a password, user information (e.g., name,

age, email address, shipping address, etc.). In some cases, account information may also be known as payment account information, card account information, or the like, and may be associated with a payment device (e.g., payment card). For example, account information may include a PAN (Primary Account Number or “account
5 number”), user name, expiration date, CVV (Card Verification Value), dCVV (Dynamic Card Verification Value), CVV2 (Card Verification Value 2), CVC3 card verification values, etc..

[0023] A “resource providing entity” may be an entity that may make resources available to a user. Resource providing entities may also be known as resource
10 providers. Examples of resource providing entities include resource providers, vendors, suppliers, owners, traders, wallet providers, service providers, and the like. In some embodiments, such entities may be a single individual, small groups of individuals, or larger groups of individuals (e.g., companies). Resource providing entities may be associated with one or more physical locations (e.g., supermarkets, malls, stores, etc.)
15 and online platforms (e.g., e-commerce websites, online companies, etc.). In some embodiments, resource providing entities may make physical items (e.g., goods, products, etc.) available to the user. In other embodiments, resource providing entities may make digital resources (e.g., electronic documents, currency, electronic files, etc.) available to the user. In other embodiments, resource providing entities may manage
20 access to certain resources by the user. In some embodiments, the resources may be services (e.g., digital wallet services).

[0024] A “credential on file” may refer to credentials associated with an account (e.g., username, password, account identifier, account number, etc.) that is on file with a resource provider computer, application computer, digital wallet server, or other entity.
25 In such situations, the credentials may be used by a resource provider and a user to conduct purchases. In a credential on file access request, the user does not need to specifically provide his or her credentials to a resource provider when conducting an access request, since the resource provider computer associated with the resource provider already stores them. Credential on file access requests may vary in frequency

and/or amount and may represent an agreement between a user (e.g., cardholder) and a resource provider to purchase goods or services provided over a period of time or on demand. A credential on file may be alternatively referred to as a card on file or an account on file.

- 5 **[0025]** A "token service computer" can include a system that services tokens. In some embodiments, a token service computer can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of access tokens to primary or virtual access identifiers (e.g., primary or virtual account numbers (PANs)) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service computer may include or be in communication with a token vault where the generated tokens are stored. The token service computer may support the processing payment transactions submitted using tokens by de-tokenizing the tokens to obtain the actual PANs or virtual PANs. In some embodiments, a token service computer may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer.

- 20 **[0026]** A "token domain" may indicate an area and/or circumstance in which an access token can be used. Examples of token domains may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e. token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the access 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 access token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the

verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0027] A “token expiry date” may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of a tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as an time duration as measured from the time of issuance.

[0028] A “token request message” may be an electronic message for requesting a token. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token request message may include one or more primary access identifiers, payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a token service computer, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key).

[0029] A “token response message” may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include an access token such as a payment token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key).

[0030] A “token requestor identifier” may include any characters, numerals, or other identifiers associated with an entity associated with a network token system. For

example, a token requestor identifier may be associated with an entity that is registered with the network token system.

[0031] A “server computer” can be a powerful computer or a 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.

[0032] An “authorization request message” may be an electronic message that requests authorization to proceed with an interaction (e.g., a transaction). For example, in some embodiments, an authorization request message may be sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a 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. In other embodiments, an authorization request message may request authorization to access secure data or a secure location.

[0033] An “authorization response message” may be an electronic message reply to an authorization request message. In some embodiments, the authorization response message may be generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval -- transaction was

approved; Decline -- transaction was not approved; or Call Center -- response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant's access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization.

[0034] A "user device" may be any suitable electronic device operated by a user. User devices may include mobile and non-mobile devices with remote communication capabilities.

[0035] A "mobile device" (sometimes referred to as a mobile communication 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, Bluetooth, Bluetooth Low Energy (BLE), Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network. Examples of mobile devices include mobile phones (e.g. cellular phones), PDAs, tablet computers, net books, laptop computers, wearable devices (e.g., watches), vehicles such as automobiles and motorcycles, personal music players, hand-held specialized readers, etc. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem -- both devices taken together may be considered a single mobile device).

[0036] A "payment device" may include a device that may be used to conduct a financial transaction, such as to provide payment information to a merchant. A payment device may be in any suitable form. For example, suitable payment devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g.,

pocket-sized) and may be in the form of a mobile device as described above. They may include smart cards, magnetic stripe cards, keychain devices, etc. Specific examples of payment devices may include credit, debit, and stored value payment cards. Other examples of payment devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, 2-D barcodes, an electronic or digital wallet, and the like. Such devices can operate in either a contact or contactless mode.

[0037] "User identifying information" can be any information that can identify the user. User identifying information can include, but is not limited to, a primary account number (PAN), telephone, e-mail address, zip code, mailing address, photo identification, personal identification number (PIN), etc. User identifying information may also include real or primary access identifiers (e.g., savings, checking, or money market account numbers).

[0038] A "processor" or "data processor" may include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to accomplish a desired function. The processor may include a CPU comprising 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).

[0039] 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.

[0040] Embodiments of the invention can relate to providing an access token to a user device, via a directory service computer. The directory service computer may obtain a virtual access identifier associated with a primary access identifier from an authorizing computer. The primary access identifier may be a savings or checking
5 account number at an issuer operating the authorizing computer. Once the request for the access token is received by the directory service computer, it can transmit a message to a token service computer to issue the access token to the user device or an application computer associated with an application on the user device. Once the user device has access to the access token, the user device may use the access token to
10 conduct an interaction.

[0041] Some embodiments of the invention relate to performing on demand payment transactions using third party applications that may be associated with one or more application computers. Embodiments of the invention can allow a user (e.g., a consumer), who may possess an account at an issuer, to quickly and conveniently use
15 those accounts to conduct on demand payment transactions using third party online applications or platforms (e.g., an online messaging platform). In certain situations, the adoption of payment devices like credit cards and debit cards may lag the adoption of issuer accounts such as savings accounts or checking accounts. Thus, while individuals may be able to withdraw money by manually visiting their banking institution
20 or perform payment transactions using traditional methods (e.g., cash or check), these same individuals may experience difficulty in using mobile devices to conduct payment transactions online and/or through third party applications that are not banking applications (e.g., social networking applications, merchant applications, messaging applications, etc.). Additionally, the process of obtaining a credit card or debit card that
25 is associated with an issuer account may be relatively slow and cumbersome.

[0042] There are many technical advantages associated with embodiments of the invention. For example, in some embodiments of the invention, a primary access identifier can only be present at the authorizing computer or the directory service computer. The primary access identifier does not need to be exposed outside of these

entities. This decreases the chance that fraudulent transactions can be conducted with the primary access identifier, since the likelihood that it can be fraudulently obtained is very low. This consequently improves upon data security relative to conventional systems. In addition, the access token may be used to conduct an interaction, even though the primary account identifier may not actually be configured for use to conduct the user's desired interaction. For example, the real or primary account identifier may be a savings account number, and it may not be capable of being used to conduct a credit card transaction, which may be the desired interaction. Embodiments of the invention can issue an access token to an application on a user device. The access token can be used to conduct a transaction such as a credit card transaction, even though the user may not have an actual credit card account. Still further, because virtual access identifiers for primary account identifiers are provided to a directory service computer before a user requests an access token, the issuance of access tokens is fast and convenient. This increases the functionality of conventional primary access identifiers. Further, authorizing entities such as issuers can control how those virtual access identifiers are processed against their corresponding real or primary account identifiers. This helps to minimize major network infrastructure changes when accomplishing the goals of embodiments of the invention.

[0043] FIG. 1 shows a system according to embodiments of the invention.

Embodiments of the invention can include more or less components than are shown in FIG. 1. Although the specific examples described with respect to FIG. 1 include descriptions of payment tokens and payment processes, it is understood that embodiments of the invention are not limited thereto. Embodiments of the invention can also apply to the use of an access token to gain access to sensitive or secret data, as well as access to restricted locations (e.g., transit stations).

[0044] In particular, FIG. 1 shows a system comprising user device 101 and application computer 102. The application computer 102 may communicate with directory service computer 103, token service computer 104, and optional transport computer 107. In some embodiments, the application computer 102 is not needed, and

the user device 101 may communicate directly with the directory service computer 103, token service computer 104, and optional transport computer 107. The directory service computer 103 may also communicate with first and second authorizing computers 105, 106. A processing computer 108 can communicate with the transport computer 107, the token service computer 104, as well as with the first and second authorizing computers 105, 106. In some embodiments, the directory service computer 103, the token service computer 104, and/or the processing computer 108 may form parts of the same system.

[0045] The entities in FIG. 1 may communicate using any suitable communications networks. Suitable communications networks may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); mesh networks, a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like.

[0046] Messages between the entities, providers, networks, and devices illustrated in FIG. 1 may be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

[0047] The user device 101 may be a mobile device, a laptop, a desktop, or the like that may be used by the user to run a third party application that may be supported by one or more application servers, including application computer 102. The user may possess an issuer account (e.g., a savings account, a checking account) at an issuer. However, the user may have yet to receive or obtain a payment device (e.g., a credit card or a debit card) that can be used to conduct a payment transaction through the third party application.

[0048] A block diagram of an exemplary user device 101 is shown in FIG. 2. The user device 101 shown in FIG. 2 includes a data processor 101A, and a network interface 101B, input/output elements 101C, a secure memory 101D, an antenna 101E, and a computer readable medium 101F operatively coupled to the data processor 101A.

5 The computer readable medium 101F may store an application 101F-1, as well as an operating system 101F-2. The application 101F-1 may be any suitable application, including a merchant application, a social networking application, a messaging application etc. The operating system 101F-2 may be any commercially available operating system such as a Windows™ or IOS™ based operating system.

10 **[0049]** The input/output elements 101C may include devices that allow the user device 101 to input and output data. Examples of output devices include speakers, displays, etc. Examples of input devices include keyboards, peripheral devices such as mice, touchscreens, etc.

[0050] The network interface 101B (as well as the other network interfaces
15 described herein) may be any suitable combination of hardware and software that enables data to be transferred to and from the user device 101. The network interface 101B may allow the user device 101 to communicate data to and from another device (e.g., application computer 102). Some examples of the network interface 101B may include a modem, a physical network interface (such as an Ethernet card or other
20 Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 101B may include Wi-Fi™.

[0051] The antenna 101E may assist in connectivity to the Internet or other
25 communications networks and enable data transfer functions. The antenna 101E may enable SMS, USSD, as well as other types of cellular communications, such as voice call and data communications

[0052] The directory service computer 103 may implement a directory service. In some embodiments, the directory service computer 103 may form part of the processing computer 108, which may be a payment processing network. The directory service computer 103 may enable third party applications to request access tokens for user devices by providing information that identifies an authorizing entity such as an issuer account of a user. It should be noted that the directory service computer 103 is not limited to receiving requests from just a single type of third party application, and may be configured to receive such requests from application servers that support different third party applications.

[0053] A block diagram of an exemplary directory service computer 103 is shown in FIG. 3. The directory service computer 103 shown in FIG. 2 includes a data processor 103A, and a network interface 103B, a database 103C and a computer readable medium 103D operatively coupled to the data processor 103A. The computer readable medium 103D may store a data retrieval module 103D-1 and a mapping module 103D-2.

[0054] The database 103C (as well as the other databases described herein) may store any suitable data. Examples of suitable databases may include a conventional, fault tolerant, relational, scalable, secure database such as those commercially available from Oracle™ or Sybase™. The database 103C may store virtual access data 103C-1 such as virtual access identifiers, and primary access data 103C-2 such as primary access identifiers.

[0055] The data retrieval module 103D-1 may comprise code, executable by the data processor 103A, for retrieving data and storing data to the database 103C. The mapping module may comprise code, executable by the data processor 103A, for mapping virtual access data (e.g., virtual access identifiers) to primary access data (e.g., primary access identifiers).

[0056] The computer readable medium 103D also comprise code, executable by the data processor 103A for receiving, from an application on a user device, a request

to provide an access token that is associated with a primary access identifier for an account, the request comprising identifying information that identifies the account; retrieving a virtual access identifier based on the identifying information; and transmitting a request, to a token service computer 104, that the access token be

5 provisioned, wherein the request comprises the virtual access identifier, and the token service computer 104 thereafter provisions the user device 101 or an application computer 102 associated with the user device 101 with the access token.

[0057] The token service computer 104 may implement a tokenizing service. In some embodiment, the token service computer 104 may also form part of a payment processing network. Upon receiving a payment token request that includes a virtual
10 PAN, the tokenizing service may substitute the virtual PAN with a payment token. The payment token may be a substitute for the virtual PAN, and the virtual PAN may be tied to a primary or real PAN in an issuer's computer.

[0058] A block diagram of an exemplary token service computer 104 is shown in
15 FIG. 4. The token service computer 104 shown in FIG. 4 includes a data processor 104A, and a network interface 104B, a database 104C and a computer readable medium 104D operatively coupled to the data processor 104A. The computer readable medium 104D may store a detokenization module 104D-1, a token generation module 104D-2, and a token lifecycle module 104D-3. The database 104C may store a data
20 table correlating access tokens with virtual access identifiers.

[0059] The detokenization module 104D-1 may comprise code that when executed by the data processor 104A, can detokenize a received access token and resolve it into a virtual access identifier (e.g., a virtual PAN) or possibly a primary or real identifier (e.g., a primary PAN).

25 **[0060]** The token generation module 104D-2 may include code, executable by the data processor 104A, to generate access tokens. The token lifecycle module 104D-3, may comprise code, executable by the data processor 104A to manage the lifecycle of distributed access tokens. For example, access tokens may only be used under

certain domain controls or conditions (e.g., a certain time period, a certain type of transaction, etc.).

[0061] The computer readable medium 104D may also comprise code, executable by the processor, for performing a method including receiving, by a token service computer and from a directory service computer, a virtual access identifier and a request to provision a user device or an application computer associated with the user device with an access token; transmitting, by the token service computer, the access token to the user device or the application computer associated with the user device; receiving, by the token service computer, the access token, the access token being in an authorization request message; determining, by the token service computer, the virtual access identifier using the access token; and providing, by the token service computer, the virtual access identifier to a processing computer, the processing computer transmitting an authorization request message comprising the virtual access identifier to an authorizing computer for authorization, the authorizing computer using the virtual access identifier to determine a primary access identifier.

[0062] The first and second authorizing computers 105, 106 may be operated by first and second issuers, respectively. An issuer may maintain one or more issuer accounts for one or more account holders, which may include the user of user device 101. Each of the issuer accounts may be associated with an account number, where each account number may comprise a first portion that uniquely identifies the issuer (e.g., a routing number) and a second portion that uniquely identifies the issuer account within the issuer (e.g., account number). Some of the issuer accounts maintained by the issuer may each be associated with a payment device that is associated with a PAN. For example, an account holder of the issuer may have applied for and obtained a debit card, the debit card having an actual PAN. The account holder may use the debit card to make various types of payment transactions including: (1) peer to peer (P2P) payment transactions, (2) payment transactions with online merchants, and (3) payment transactions with brick-and-mortar store merchants.

[0063] Other issuer accounts that are maintained by the issuer may not be associated with a payment device. For instance, an issuer account could be a savings or brokerage account that does not have a corresponding payment device associated with it.

5 **[0064]** A block diagram of an exemplary authorizing computer is shown in FIG. 5. The authorizing computer 105 shown in FIG. 5 includes a data processor 105A, a network interface 105B, a database 105C and a computer readable medium 105D operatively coupled to the data processor 105A. The computer readable medium 105D may store an authorizing module 105D-1, a mapping module 105D-2, and a risk
10 determination module 105D-3.

[0065] The authorizing module 105D-1 may include code executable, by the data processor 105A, to determine whether or not to authorize a transaction. Criteria for authorizing a transaction may include whether the user has sufficient authority (e.g., credit) to conduct the requested interaction, whether the interaction requested is
15 potentially fraudulent, etc.

[0066] The mapping module 105D-2 may store mappings between virtual access identifiers (virtual PANs) and real or primary access identifiers (e.g., real or primary PANs). If a virtual access identifier is received by the authorizing computer 105, then the primary access identifier may be determined. An action (e.g., debiting the account)
20 may then be taken with respect to an account associated with the access identifier. The risk determination module 105D-2 may include code, executable by the data processor 105A, to determine whether the current interaction requested by the user device 101 is fraudulent or not.

[0067] Referring again to FIG. 1, the transport computer 107 may be located
25 between (in an operational sense) the application computer 102 and the processing computer 108. The transport computer 107 may be operated by an entity such as an acquirer. An acquirer can maintain an account of any number of merchants with which users may wish to interact.

[0068] The processing computer 108 may route or switch messages between a number of transport computers including the transport computer 107, and a number of authorizing computers 105, 106. The processing computer 108 may be configured to provide authorization services, and clearing and settlement services for payment transactions. The processing computer 108 may be or be part of a payment processing network, and may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular includes a Visa Integrated Payments (VIP) system which processes authorization requests and a Base II system which performs clearing and settlement services. Furthermore, the payment processing network may include a server computer and may use any suitable wired or wireless telecommunications network, including the Internet. In some embodiments, the processing computer may forward an authorization request received from a transport computer 107 to the authorizing computer via a communication channel. The processing computer may further forward an authorization response message received from the authorizing computer to the transport computer.

[0069] Methods according to embodiments of the invention can be described with reference to FIGs. 1, 6, and 7, as well as other Figures. The specific examples described below refer to the use of a virtual PAN (primary account number) as a virtual access identifier, a real PAN as a primary access identifier, and a payment token as an access token. It is understood that embodiments of the invention may be used in processing other than payment processing.

[0070] At step S101, virtual access data such as virtual access identifiers are provided to a directory service computer 103 from one or more authorizing computers. For example, one or more of the first and second authorizing computers 105, 106 can be issuer computers. An issuer computer of an issuer can allocate (i.e., pre-allocates) a

virtual PAN for each issuer account maintained by the issuer that is not already associated with a virtual PAN and communicates the associations between virtual PANs and issuer accounts to the directory service computer 103. For example, if the issuer associated with first authorizing computer 105 maintains both issuer accounts that are already associated with payment device identifiers and issuer accounts that are not associated with payment device identifiers, the authorizing computer 105 may allocate virtual access identifiers (e.g., virtual PANs) for the issuer accounts not already associated with payment device identifiers. As a result, each of the issuer accounts maintained by the issuer may be associated with either payment device identifier or a virtual access identifier such as a virtual PAN. In some embodiments, a virtual PAN that is generated at this step may initially be dormant and incapable of being used to perform a payment transaction until the virtual PAN is activated at a later time.

[0071] In some embodiments, to avoid having different issuers (e.g., the issuer associated with the first authorizing computer 105 and another issuer associated with the second authorizing computer 106) allocate or generate identical virtual PAN numbers to their issuer accounts, a payment processing network may form an arrangement with the issuers where each issuer receives a different range of numbers from which to allocate to virtual PANs.

[0072] The first authorizing computer 105 may store the associations in memory using a table (e.g., a database table stored in a database) having multiple rows and columns, where one of the columns includes payment device identifiers or virtual access identifiers, one of the columns includes routing numbers, and one of the columns includes primary or real access identifiers associated with the virtual access identifiers. The first authorizing computer 105 may export the table to a file and send the file to the directory service computer 103. Upon receiving the file, the directory service computer 103 may copy the associations stored in the file into memory (e.g., database 103C). In particular, the directory service computer 103 may store associations between issuer accounts and virtual PANs received from different issuers.

[0073] At step S102, a user having an issuer account that is not associated with a payment device such as a credit card, may make a request to perform payment transactions through a third party application using the issuer account. The payment request may also be a token request, where the token request requests an access token used in performing the payment transaction. For example, the user of user device 101 may wish to perform a payment transaction using the third party application supported by application computer 102. The user may not have any credit cards or debit cards available for performing the payment transaction. Instead, the user may attempt to perform the transaction by providing information that identifies his/her issuer account. Here, the identifying information may comprise a routing number and an account number associated with the issuer account (e.g., a savings account). The account number may be an example of a primary account identifier. Accordingly, user device 101 may generate a request to perform the payment transaction that includes the routing number and the account number. The user device 101 may transmit the request to application computer 102.

[0074] At step S103, upon receiving the request from the user device 101, the application computer 102 may forward account identifying information contained within the request to the directory service computer 103. In some embodiments, upon receiving the request from user device 101 in step S102, application computer 102 may generate a token request that includes the routing number and the account number, as well as an identifier (e.g., a phone number) for the user device 101. The payment token request including the identifying information may be forwarded to the directory service computer 103.

[0075] At step S104, upon receiving the payment token request from the application computer 102, the directory service computer 103 may retrieve the virtual access identifier such as the virtual PAN based on information provided in the request, and may forward the PAN to the token service computer 104. For instance, upon receiving the payment token request from the application computer 102, the directory service computer 103 may extract the routing number and the account number from the

payment token request and map the combination of the routing number and the account number to a virtual PAN stored in the table. In this particular case, the virtual PAN is an example of a virtual access identifier. The virtual PAN is used, because the user does not have an actual payment device or payment device identifier associated with his/her issuer account. The directory service computer 103 may provide a request to the token service computer 104 to provision an access token such as a payment token to the user device 101 or the application computer 102. In making the request, the directory service computer 103 may send the virtual PAN and a user device identifier such as a phone number, SIM card number, or e-mail address to token service computer 104.

[0076] At step S105, upon receiving the access token request, the token service computer 104 may provision an access token such as a payment token to the application computer 102. For example, upon receiving the request containing the virtual PAN from the directory service computer 103, the token service computer 104 may generate or retrieve from memory a payment token based on the virtual PAN. The token service computer 104 may then provision the payment token along with other associated information (e.g., card art, terms and conditions) to the user device 101. In some cases, this may involve sending the payment token to the application computer 102, which may then provide the access token to the user device 101 (step S106). In some cases, the application computer 102 may retain the access token as a credential on file. The user device 101 can access the access token via the application computer 102.

[0077] Once the user device 101 has been provisioned with an access token (e.g., payment token), the user device 101 may be used to initiate an action. In some embodiments, the action may be an interaction such as a transaction (e.g., a payment transaction), a request for secure data, a request to access a particular location, etc. This process can be described in greater detail with respect to the flowchart in FIG. 7.

[0078] Referring to FIG. 7, the provisioned payment token may be used to perform the requested payment transaction. In step S107, a user using the user device 101 may initiate an action such as a payment transaction on an application associated

with the application computer 102. The user may initiate the application, which may cause the user device 101 to communicate with the application computer 102. The application computer 102 may be, for example, a ride sharing application and the user may wish to pay for a ride using the ride-sharing application.

5 **[0079]** In step S108, after the user expresses an intent to pay, the application computer 102 may generate an authorization request message comprising the payment token and a transaction amount. The authorization request message may then be transmitted from the application computer 102 to the transport computer 107. In step S109, the transport computer 107 may transmit the authorization request message to
10 the processing computer 108.

[0080] In step S110, the processing computer 108 then provide the access token to the token service computer 104. The token service computer 104 may then look up the virtual PAN associated with the access token and may return the virtual PAN associated with the access token to the processing computer 108. The processing
15 computer 108 may then modify the authorization request message with the virtual account number and may forward the authorization request message to the processing computer 108. In other embodiments, the processing computer 108 may simply route the authorization request message with the payment token to the token service computer 104, and then the token service computer 104 may return the authorization
20 request message with the virtual PAN.

[0081] In step S111, the processing computer 108 may then transmit the authorization request message including the virtual PAN to the first authorizing computer 105. Upon receiving the authorization request message, the first authorizing computer 105 may map the virtual PAN to the user's issuer account by locating real or
25 primary account number. The first authorizing computer 105 may then debit the issuer account in accordance with the payment transaction. As a result, the user has been issued a digital account (i.e., the virtual PAN) via a third party application in a quick and convenient fashion, where the user may continue to use the association between the

digital account and the user's issuer account to make payment transactions through the third party application.

5 **[0082]** In some embodiments, the authorizing computer 105 may perform one or more risk decision and/or card activation steps to activate the virtual PAN. In alternative embodiments, the virtual PAN may be activated in an earlier step. In some embodiments, even after the virtual PAN is activated, the user may not receive any payment device associated with the virtual PAN or learn of the virtual PAN. The user may not use the virtual PAN to conduct payment transactions with merchants in the traditional sense (e.g., use the virtual PAN to make purchases at brick-and-mortar
10 stores).

[0083] After the first authorizing computer 105 has approved of the transaction, the first authorizing computer 105 may generate an authorization response message. The first authorizing computer 105 may then transmit the authorization response message to the processing computer 108 at step S112.

15 **[0084]** At step S113, after receiving the authorization response message, the processing computer 108 may communicate with the token service computer 104 to exchange the virtual PAN for the payment token. The processing computer 108 may then replace the virtual PAN with the payment token in the authorization response message. At step S114, the processing computer 108 may then transmit the
20 authorization response message to the transport computer 107, and then to the application computer 102 in step S115. At step S116, the application computer 102 may notify the user device 101 that the transaction has been approved.

[0085] At the end of the day or at any other suitable period of time a clearing and settlement process may be performed using the issuer account. For example, a
25 settlement or transmission of funds may be facilitated between an acquirer, the payment processing network, and the first authorizing computer 105.

[0086] In an alternative embodiment, after allocating virtual PANs for issuer accounts as described in step S101, the first authorizing computer 105 may not send

files containing associations between issuer accounts and PANs to the directory service computer 103. Instead, responsive to receiving a payment token request, the directory service computer 103 may query the first authorizing computer 105 for PANs in real-time.

5 **[0087]** Although the examples above specifically discuss payment transactions, embodiments of the invention are not limited to payment transactions. Other examples of accounts that can be quickly provided via pre-allocation of virtual PANs may include user accounts for online services, emails accounts, corporate accounts, and types of accounts that are often created via third-party applications.

10 **[0088]** As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably-programmed computing device, microprocessor, data processor, or the like. The set of instructions or software
15 code may be stored in a memory or other form of data storage element which is accessed by the computing device, microprocessor, etc. In other embodiments, the functions, processes, operations or method steps may be implemented by firmware or a dedicated processor, integrated circuit, etc.

20 **[0089]** 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
25 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.

[0090] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown
5 and described, since various other modifications may occur to those with ordinary skill in the art.

[0091] As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a directory service computer from an application on a user
3 device, a request to provide an access token that is associated with a primary access
4 identifier for an account, the request comprising identifying information that identifies the
5 account
6 retrieving, by the directory service computer, a virtual access identifier
7 based on the identifying information; and
8 transmitting a request, by the directory service computer to a token
9 service computer, that the access token be provisioned, wherein the request comprises
10 the virtual access identifier, and the token service computer thereafter provisions the
11 user device or an application computer associated with the user device with the access
12 token.

1 2. The method of claim 1, further comprising:
2 receiving, by the token service computer, the access token, the access
3 token being present in an authorization request message;
4 determining, by the token service computer, a virtual access identifier
5 associated with the access token; and
6 transmitting, by a processing computer, the authorization request
7 message comprising the virtual access identifier to an authorizing computer for
8 authorization, the authorizing computer determining the primary access identifier using
9 the virtual access identifier and performing an action with the primary access identifier.

1 3. The method of claim 2, further comprising:
2 receiving, by the directory service computer from the authorizing
3 computer, a file including a plurality of virtual access identifiers and primary access
4 identifiers, the virtual access identifiers not being capable of being used with resource
5 provider computers to conduct transactions.

1 4. The method of claim 1 wherein receiving, by the directory service
2 computer from the application on the user device, the request to provide the access
3 token occurs via the application computer associated with the application.

1 5. The method of claim 1 further comprising:
2 receiving, by the token service computer, the access token, the access
3 token being present in an authorization request message from the application computer
4 associated with the application;
5 determining, by the token service computer, a virtual access identifier
6 associated with the access token; and
7 transmitting, by a processing computer, the authorization request
8 message comprising the virtual access identifier to an authorizing computer for
9 authorization, the authorizing computer determining the primary access identifier using
10 the virtual access identifier and performing an action with the primary access identifier.

1 6. The method of claim 5, wherein the authorization request message
2 is received by the token service computer from the application computer via a transport
3 computer.

1 7. The method of claim 1, wherein the user device is a mobile phone.

1 8. The method of claim 1, wherein the access token provides access
2 to secure data.

1 9. A system comprising:
2 a directory service computer, the directory service computer comprising a
3 data processor, and a computer readable medium, the computer readable medium
4 comprising code, executable by the data processor, to cause the directory service
5 computer to

6 receive from an application on a user device, a request to provide an
7 access token that is associated with a primary access identifier for an account, the
8 request comprising identifying information that identifies the account,
9 retrieve a virtual access identifier based on the identifying information, and
10 transmit a request, by the directory service computer to a token service
11 computer, that the access token be provisioned, wherein the request comprises the
12 virtual access identifier, and the token service computer thereafter provisions the user
13 device or an application computer associated with the user device with the access
14 token.

1 10. The system of claim 9, wherein the data processor is a first data
2 processor and the computer readable medium is a first computer readable medium, and
3 wherein the system further comprises:

4 a token service computer in communication with the directory service
5 computer, the token service computer comprising a second data processor and a
6 second computer readable medium coupled to the second data processor, the second
7 computer readable medium comprising code, executable by the second data processor
8 to cause the token service computer to: receive the access token, the access token
9 being present in an authorization request message, and determine a virtual access
10 identifier associated with the access token; and

11 a processing computer comprising a third data processor and a third
12 computer readable medium coupled to the third data processor, the third computer
13 readable medium comprising code, executable by the third data processor to cause the
14 processing computer to transmit the authorization request message comprising the
15 virtual access identifier to an authorizing computer for authorization, the authorizing
16 computer determining the primary access identifier using the virtual access identifier
17 and performing an action with the primary access identifier.

1 11. The system of claim 9, wherein the computer readable medium of
2 the directory service computer further comprises code, executable by the first data
3 processor to cause the directory service computer to receive from the authorizing

4 computer, a file including a plurality of virtual access identifiers and real access
5 identifiers, the virtual access identifiers not being capable of being used with resource
6 provider computers to conduct transactions.

1 12. The system of claim 9, wherein code for causing the directory
2 service computer to receive from the application on the user device, the request to
3 provide the access token occurs via the application computer associated with the
4 application.

1 13. The system of claim 9, wherein the data processor is a first data
2 processor and the computer readable medium is a first computer readable medium, and
3 wherein the system further comprises:

4 a token service computer in communication with the directory service
5 computer, the token service computer comprising a second data processor and a
6 second computer readable medium coupled to the second data processor, the second
7 computer readable medium comprising code, executable by the second data processor
8 to cause the token service computer to receive the access token, the access token
9 being present in an authorization request message from the application computer
10 associated with the application, and determine a virtual access identifier associated with
11 the access token; and

12 a processing computer comprising a third data processor and a third
13 computer readable medium coupled to the third data processor, the third computer
14 readable medium comprising code, executable by the third data processor to cause the
15 processing computer to transmit the authorization request message comprising the
16 virtual access identifier to an authorizing computer for authorization, the authorizing
17 computer determining a primary access identifier using the virtual access identifier and
18 performing an action with the primary access identifier.

1 14. The system of claim 9, wherein the access token provides access
2 to secure data.

1 15. A method comprising:

2 receiving, by a token service computer and from a directory service
3 computer, a virtual access identifier and a request to provision a user device or an
4 application computer associated with the user device with an access token;
5 transmitting, by the token service computer, the access token to the user
6 device or the application computer associated with the user device;
7 receiving, by the token service computer, the access token, the access
8 token being in an authorization request message;
9 determining, by the token service computer, the virtual access identifier
10 using the access token; and
11 providing, by the token service computer, the virtual access identifier to a
12 processing computer, the processing computer transmitting an authorization request
13 message comprising the virtual access identifier to an authorizing computer for
14 authorization, the authorizing computer using the virtual access identifier to determine a
15 primary access identifier.

1 16. The method of claim 15, wherein the user device is a mobile phone.

1 17. The method of claim 15, wherein the authorization request
2 message is received from an application computer associated with an application on the
3 user device.

1 18. The method of claim 15, wherein the authorizing computer uses the
2 primary access identifier to perform an action.

1 19. The method of claim 15, wherein the authorizing computer uses the
2 primary access identifier to perform an action, the action being allowing access to
3 secure data by the user device.

1 20. The method of claim 15, wherein the token service computer and
2 the processing computer are part of a same system.