SYSTEMS AND METHODS FOR TOKENIZING FINANCIAL INFORMATION

Inventors: Devin Michael Cambridge, Atlanta, GA (US); Brian Kean, Missouri Valley, IA (US); Stephen M. Meyers, Omaha, NE (US); Norman Theodore Davis, JR., Elkhorn, NE (US)

Assignee: FIRST DATA CORPORATION, Greenwood Village, CO (US)

Appl. No.: 13/481,394
Filed: May 25, 2012

Related U.S. Application Data
Provisional application No. 61/490,501, filed on May 26, 2011.

Publication Classification
Int. Cl. G06Q 20/40
U.S. Cl. 705/35

Abstract
Embodiments of the invention can provide systems and methods for tokenizing financial information associated with mobile device transactions. According to one example embodiment of the invention, a method for providing tokens to devices can be provided. The method can include receiving, from a device, a request for a token to represent financial information; identifying, in response to the request, token information associated with the token; providing at least a portion of the token information to the device; and providing the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token subsequently received from one of the device or a user of the device.
FIG. 2
Start

Identify a situation in which a token will be utilized to represent information

Prepare a tokenization request and communicate the request to a tokenization service provider

Receive token information from the tokenization service provider

Token received? No
Indepedently generate a token

Yes
Identify a token to be utilized to represent the information

Provide the token to another entity or service provider in place of the information

End

FIG. 3
SYSTEMS AND METHODS FOR TOKENIZING FINANCIAL INFORMATION

RELATED APPLICATION

[0001] This application claims priority to U.S. Ser. No. 61/490,501, titled “Trusted Service Manager,” filed on May 26, 2011, the contents of which are incorporated herein by reference.

FIELD OF THE INVENTION

[0002] Embeddings of the invention relate generally to mobile device transactions, and more specifically to systems and methods for tokenizing financial information associated with mobile device transactions.

BACKGROUND OF THE INVENTION

[0003] Mobile devices, such as cell phones, personal digital assistants (“PDAs”), smart phones, and other similar devices, have increasingly been utilized to provide additional functionality beyond traditional voice communications. One component of enabling the mobile devices to support these additional functionalities includes installing software applications on the mobile devices. Mobile device applications can facilitate a variety of services performed by or with the mobile devices, including payment applications (e.g., prepaid, credit, debit, etc.), loyalty or incentive applications, transportation payment applications, access control applications, entertainment applications, and the like. Given the sensitive nature of data that may be utilized in association with these additional applications, mobile devices may make use of secure memory elements configured to store sensitive data, such as account information.

[0004] In many situations, a user of a mobile device may wish to provide sensitive data to a service provider for authentication purposes or other transaction purposes. For example, a user may wish to provide a credit card account number to a service provider during a service call. However, because the shared memory of the mobile device is inherently insecure, the sensitive data can be exposed to security attacks, such as side channel attacks, Trojan application, and/or input sniffers, if the sensitive data is moved to a shared memory of the mobile device or communicated to a service provider by the mobile device. Accordingly, there is an opportunity for improving the security of financial information and/or other sensitive data by tokenizing the data.

BRIEF DESCRIPTION OF THE INVENTION

[0005] Embeddings of the invention may provide systems and methods for tokenizing financial information associated with mobile device transactions. According to one example embodiment of the invention, a method for providing tokens to devices can be provided. The method can include receiving, from a device, a request for a token to represent financial information; identifying, in response to the request, token information associated with the token; providing at least a portion of the token information to the device; and providing the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token subsequently received from one of the device or a user of the device. In certain embodiments, one or more operations can be performed by one or more computers associated with a service provider.

[0006] According to another embodiment, a system for providing tokens to devices can be provided. The system may include at least one memory and at least one processor. The at least one memory may be configured to store computer-executable instructions. The at least one processor may be configured to receive, from a device, a request for a token to represent financial information; identify, in response to the request, token information associated with the token; provide at least a portion of the token information to the device; and provide the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token subsequently received from one of the device or a user of the device. In certain embodiments, one or more operations can be performed by one or more computers associated with a service provider.

[0007] According to yet another embodiment, a method can be provided. The method can include receiving, from a mobile device, a request for a token to represent financial information; identifying, in response to the request, token information associated with the token; providing at least a portion of the token information to the mobile device; and providing the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token received from one of the mobile device or a user of the mobile device. In certain embodiments, one or more operations can be performed by one or more computers associated with a service provider.

[0008] According to another embodiment, a system for providing tokens to devices can be provided. The system may include at least one memory and at least one processor. The at least one memory may be configured to store computer-executable instructions. The at least one processor may be configured to receive, from a mobile device, a request for a token to represent financial information; identify, in response to the request, token information associated with the token; provide at least a portion of the token information to the mobile device; and provide the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token received from one of the mobile device or a user of the mobile device. In certain embodiments, one or more operations can be performed by one or more computers associated with a service provider.

[0009] Additional systems, methods, apparatus, features, and aspects are realized through the techniques of various embodiments of the invention. Other embodiments and aspects of the invention are described in detail herein and are considered a part of the claimed invention. Other advantages and features can be understood with reference to the description and to the drawings.

BRIEF DESCRIPTION OF THE FIGURES

[0010] FIG. 1 illustrates a block diagram of an example tokenization system that may be utilized in accordance with various embodiments of the invention.

[0011] FIG. 2 illustrates a flow diagram of an example process for communicating a token to a mobile device, according to an example embodiment of the invention.

[0012] FIG. 3 illustrates a flow diagram of an example process for utilizing a token in conjunction with a mobile device, according to an example embodiment of the invention.

DETAILED DESCRIPTION

[0013] Various embodiments of the invention are directed to the tokenization of information in association with device
transactions. In other words, various embodiments of the invention are directed to the generation of tokens to represent sensitive data, such as financial account data and/or transaction data. Generated tokens may then be utilized by a device, such as a mobile device, in order to reference a transaction and/or authenticate the user. In one example embodiment of the invention, a device may identify a situation in which a token will be utilized to represent sensitive data. For example, a service call situation in which an account number is desired by a technician may be identified as a situation in which a token will be utilized to represent the account number. As other examples, a balance reporting situation or a transaction situation may be identified as situations in which tokens will be utilized. In certain embodiments, a situation may be identified by the device based upon the receipt of user input. For example, a user may request a service call. In other embodiments, a situation may be identified by the device based upon the processing of data, such as transaction data. For example, the device may identify a transaction error and automatically trigger a service call situation.

0014 Once a desired tokenization situation has been identified, a tokenization request may be prepared or generated by the device, and the tokenization request may be communicated to a tokenization service provider. A wide variety of information may be included in the request, including but not limited to, a type associated with the desired situation (e.g., a service call, a balance reporting situation, a transaction, etc.), an identifier of information to be tokenized, and/or an identifier of a service provider or other party to which a token will be communicated. The tokenization service provider may process the request in order to generate token information, and the generated token information may be provided to the device. In certain embodiments, the tokenization service provider may generate a token that is returned to the requesting device. In other embodiments, the tokenization service provider may generate a token and determine information that may be utilized by the device to independent identify or generate a token. For example, the tokenization service provider may identify an algorithm that may be utilized by the device to generate a token utilizing a wide variety of information provided by the service provider and/or device information (e.g., an identifier of a mobile device secure element, card production life cycle information, etc.). As another example, the tokenization service provider may determine a token number or other identifier and provide the identifier to a device to facilitate a device selection of a token generated by the device (e.g., a first token, a fourth token, etc.). Indeed, a wide variety of token information may be prepared by the tokenization service provider and communicated to the requesting device in order to facilitate the identification of a token by the device.

0015 In addition to returning token information to the requesting device, the tokenization service provider may additionally provide token information (e.g., a token, etc.) to another service provider or entity. For example, the tokenization service provider may provide token information to a service provider that handles technical service calls or to a transaction service provider. The recipient service provider may utilize the received token information in order to authenticate the device and/or to verify the identity of a mobile device user. For example, the recipient service provider may independently receive tokens from both the tokenization service provider and the device (or a user of the device), and the recipient service provider may compare the tokens in order to verify the identity of the device or device user. Additionally, in certain embodiments, the tokenization service provider may also communicate the sensitive data (e.g., financial account number, etc.) that is represented by the token to the recipient service provider. As desired, secure communications networks and/or other communications means may be utilized to communicate information to the recipient service provider. Once the two tokens have been matched by the recipient service provider, the received sensitive data may be utilized by the recipient service provider. As a result of this use of tokens, the storage of sensitive data on a shared or general memory of the device may be reduced and/or avoided. In this regard, security risks associated with the data may be reduced.

0016 Various embodiments of the invention utilize trusted service management functionality, which may be implemented by the tokenization service provider, to facilitate integration between multiple service providers and multiple mobile devices operating on any number of carrier networks, each operated by a different mobile network operator ("MNO"). In certain embodiments, a tokenization service provider may be a third party entity strategically positioned to provide tokenization services.

0017 Embodiments of the invention now will be described more fully hereinafter with reference to the accompanying drawings, in which embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will be thorough and complete, and will fully convey the scope of the invention to those skilled in the art. Like numbers refer to like elements throughout.

0018 FIG. 1 represents a block diagram of an example system 100 for providing tokenization services, according to one embodiment of the invention. As shown in FIG. 1, a tokenization service provider ("TSP") computer 110, multiple mobile network operator ("MNO") computers 140a, 140b, multiple mobile devices 150a, 150b; and multiple service provider computers 160 may be in communication via any number of networks 170 and/or multiple carrier networks 180a, 180b, each of the carrier networks 180a, 180b being associated with a respective MNO computer 140a, 140b. Each of these components will now be discussed in further detail.

0019 First, the TSP computer 110 may include any number of processor-driven devices, including but not limited to, a server computer, a mainframe computer, one or more networked computers, a desktop computer, a personal computer, a laptop computer, a mobile computer, or any other processor-based device. In addition to having one or more processors 116, the TSP computer 110 may further include one or more memory devices 112, input/output ("I/O") interface(s) 118, and network interface(s) 119. The memory 112 may be any computer-readable medium, coupled to the processor(s) 116, such as RAM, ROM, and/or a removable storage device for storing data files and a database management system ("DBMS") to facilitate management of data files and other data stored in the memory 112 and/or stored in one or more separate databases 138. The memory 112 may also store various program modules, such as an operating system ("OS"), a service provider interface 121, a mobile network operator interface 122, and a tokenization module 126. The OS may be, but is not limited to, Microsoft Windows®, Apple
OSX™, Unix, a mainframe computer operating system (e.g., IBM z/OS, MVS, OS/390, etc.), or a specially designed operating system. Each of the interfaces and modules 121, 122, 126 may comprise computer-executable program instructions or software, including a dedicated program, for receiving, storing, extracting, managing, processing, and analyzing communications associated with tokenization via any number of suitable networks, such as networks 170a and/or carrier networks 180a, 180b.

[0020] The tokenization module 126 may include any number of suitable software modules and/or applications that facilitate the provisioning and processing of tokenization requests. In one example operation, a tokenization request may be received from a mobile device 150a, 150b via a suitable interface or gateway, and the tokenization request may be provided to the tokenization module 126. The tokenization module 126 may process the received request in order to identify, determine, and/or generate token information (e.g., a token, a token life cycle, etc.), and the tokenization module 126 may direct the communication of at least a portion of the token information to the mobile device 150a, 150b. Additionally, the tokenization module 126 may direct provision of token information and, as desired, data represented by the token information to a service provider 160 via one or more suitable interfaces and/or gateways. In this regard, a wide variety of data (e.g., financial account data, other sensitive data, etc.) may be represented by tokens, and the tokens may be utilized by the mobile devices 150a, 150b and the service providers 160 to identify and/or access the data.

[0021] One example of the operations that may be performed by the tokenization module 126 is described in greater detail below with reference to FIG. 2.

[0022] An MNO gateway 134 and associated MNO interface 122 are operable for providing a common point of integration between the tokenization server computer 110 and the multiple MNO computers 140. According to one embodiment, the MNO interface 122 is configured to communicate with each MNO according to the same common MNO message standard, as described further herein. Moreover, according to various embodiments, the MNO gateway 134 and associated MNO interface 122 are further operable to permit the tokenization server computer 110 to communicate with mobile devices 150a via a respective carrier network operated by each MNO. In a similar manner, a service provider gateway 133 and associated service provider interface 121 are operable for providing a common point of integration between the tokenization server computer 110 and the multiple service provider computers 160.

[0023] Still referring to the TSP computer 110, the I/O interface(s) 118 may facilitate communication between the processor 116 and various I/O devices, such as a keyboard, mouse, printer, microphone, speaker, monitor, bar code reader/scanner, RFID reader, contactless reader, or Hardware Security Modules (“HSMs”) which facilitate secure key management (e.g., test key management for a variety of testing environments, etc.) and the like. The network interface(s) 119 may take any of a number of forms, such as, but not limited to, a network interface card, a modem, a wireless network card, a cellular network card, or any other means capable of facilitating communications with one or more carrier networks 180a, 180b and/or other networks 170. Indeed, the TSP computer 110 can communicate directly with mobile devices 150a, 150b via the carrier networks 180a, 180b, respectively, via network interface(s) 119 and/or via one or more of suitable Web servers 137 or the mobile network operator gateway 134. It will be appreciated that the TSP computer 110 may be implemented on a particular machine, which may include a computer that is designed, customized, configured, or programmed to perform at least one or more functions of the interfaces and modules, according to an example embodiment of the invention.

[0024] Second, the MNO computers 140a, 140b may include any number of processor-driven devices, including but not limited to, a server computer, a mainframe computer, one or more networked computers, a desktop computer, a personal computer, a laptop computer, a mobile computer, or any other processor-based device. In addition to having one or more processors 146a, 146b, each of the MNO computers 140a, 140b may further include one or more memory devices 142a, 142b, input/output ("I/O") interface(s) 148a, 148b, and network interface(s) 149a, 149b. The memory 142a, 142b may be any computer-readable medium, coupled to the processor(s) 146, such as RAM, ROM, and/or a removable storage device for storing data files and a DBMS to facilitate management of data files and other data stored in the memory 142a, 142b and/or stored in one or more separate databases. The memory 142a, 142b may also store various program modules, such as an operating system ("OS"), a communications module 144a, 144b, and an authentication module 145a, 145b. The OS may be, but is not limited to, Microsoft Windows®, Apple OSX™, Unix, a mainframe computer operating system (e.g., IBM z/OS, MVS, OS/390, etc.), or a specially designed operating system. The communications module 144a, 144b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating communications with multiple mobile devices 150a, 150b operating on the respective carrier networks 180a, 180b, and for facilitating mobile device application provisioning and management via a common MNO messaging standard as implemented by the TSP computer 110. The authentication module 145a, 145b may comprise computer-executable program instructions or software, including a dedicated program, for facilitating the authentication of mobile devices 150a, 150b and/or the establishment of secure communications channels with mobile devices 150a, 150b. A wide variety of authentication procedures may be utilized as desired by an authentication module 145a, 145b.

[0025] Still referring to each MNO computer 140a, 140b, the I/O interface(s) 148a, 148b may facilitate communication between the processors 146a, 146b and various I/O devices, such as a keyboard, mouse, printer, microphone, speaker, monitor, bar code reader/scanner, RFID reader, and the like. The network interface(s) 149a, 149b may take any of a number of forms, such as, but not limited to, a network interface card, a modem, a wireless network card, a cellular network card, or any other means capable of facilitating communications with one or more carrier networks 180a, 180b and/or other network 170. It will be appreciated that the MNO computers 140a, 140b may be implemented on a particular machine, which may include a computer that is designed, customized, configured, or programmed to perform at least one or more functions of the communications module 144a, 144b, according to an example embodiment of the invention.

[0026] Third, the mobile devices 150a, 150b may be any mobile processor-driven device, such as a mobile phone, radio, pager, laptop computer, handheld computer, PDA, and the like, or any other processor-based mobile device for facilitating communications over one or more carrier networks.
For example, each mobile device 150a, 150b may be registered with a specific MNO computer 140a, 140b for communicating via the respective carrier network 180a, 180b. In addition to having one or more processors 156a, 156b, each of the mobile devices 150a, 150b may further include one or more memory devices 152a, 152b, input/output ("I/O") interface(s) 158a, 158b, and network interface(s) 159a, 159b. The memory 152a, 152b may be any computer-readable medium, coupled to the processor(s) 156, such as RAM, ROM, and/or a removable storage device for storing data files. The memory 152a, 152b may include any number of shared or general memories (e.g., memories that may be accessed by a wide variety of applications such as a mobile wallet) and/or any number of secure elements 155a, 155b configured to maintain mobile wallet application data. In certain embodiments, a secure element 155a, 155b may be configured to store key information, as well as certain identification information for the mobile device and the secure element 155a, 155b (e.g., card production life cycle ("CPLC") information, etc.). In certain embodiments, a secure element 155a, 155b may store an authentication module or program utilized by a mobile device 150a, 150b to tag an/or encrypt communications output by the mobile device 150a, 150b and/or to decrypt communications received by the mobile device 150a, 150b. As desired, the authentication module or an application stored on shared memory may be configured to generate tokenization requests and receive token information as described in greater detail below with reference to FIG. 2.

The memory 152a, 152b may also store any number of data files 153a, 153b and/or various program modules, such as an operating system ("OS"), end user interface module(s), and a provisioning module. The OS may be any mobile operating system, including proprietary operating systems by a mobile device manufacturer or mobile network operator, or third party software vendor mobile operating system, such as, but not limited to, Microsoft Windows CE®, Microsoft Windows Mobile®, Symbian OS™, Apple iPhone™ OS, RIM BlackBerry® OS, Palm OS® by ACCESS, or Google Android™. The provisioning module may comprise computer-executable program instructions or software, including a dedicated program, for facilitating mobile device provisioning on general memory and/or the secure elements 155a, 155b. According to various embodiments, the secure elements 155a, 155b may refer to any computer-readable storage in the memory 152 and/or may refer to any secured medium having memory, such as a Universal Integrated Circuit Card ("UICC"), Subscriber Identity Module ("SIM"), and the like. In one example, the secure elements 155a, 155b may be operable with a RFID device or other NFC device associated with the mobile devices 150a, 150b. It is also appreciated that the secure elements 155a, 155b may be a separate embedded secure element (e.g., smart card chip) or a separate element (e.g., removable memory card, a key fob; connected via Bluetooth, etc.). For example, a secure element chip may be embedded in a mobile device 150a, 150b separately from a general operation chip utilized by the mobile device 150a, 150b. In certain embodiments, the secure elements 155a, 155b may include any suitable hardware and/or software, such as memory, processing components, and communications components. In certain embodiments, the secure elements 155a, 155b may be configured to communicate with other elements of the mobile devices 150a, 150b, such as a general or shared memory chip associated with the mobile devices 150a, 150b. For example, a mobile wallet may be stored in shared memory, and a secure element 155a, 155b may be accessed to encrypt and/or decrypt transactions generated by and/or received by the mobile wallet.

In certain embodiments, a mobile device 150a, 150b may be configured to generate tokenization requests that are provided to the TSP computer 110. For example, a dedicated tokenization application may be stored on a shared memory and/or the secure element 155a, 155b. As another example, the authentication application or other provisioned application may also be configured to perform tokenization functions. In operation, a tokenization situation or information to be tokenized may be identified, and a tokenization request may be prepared and communicated to the TSP computer 110. In response to the tokenization request, token information may be received from the TSP computer 110, and the token information may be utilized to identify a token to be utilized in place of information represented by the token. The token may then be utilized by the mobile device 150a, 150b or a user of the mobile device 150a, 150b to contact a service provider 160 and verify the identity of the device and/or user. In this regard, the security of the information represented by the token may be enhanced.

One example of the operations that may be performed by a mobile device 150a, 150b to facilitate tokenization is described in greater detail below with reference to FIG. 3.

Still referring to each mobile device 150a, 150b, the I/O interface(s) 158a, 158b may facilitate communication between the processors 156a, 156b and various I/O devices, such as a keypad, touch screen, keyboard, mouse, printer, microphone, speaker, screen display, RFID device, NFC device, and the like. The network interface(s) 159a, 159b may take any of a number of forms to permit wireless communications according to various communications standards, such as, but not limited to, Code Division Multiple Access ("CDMA"), Global System for Mobile Communication ("GSM"), Universal Wireless Communications ("UWC"), Universal Mobile Telecommunications System ("UMTS"), or General Packet Radio Service ("GPRS") communication standards as may be implemented by one or more carrier networks 180a, 180b. The network interfaces(s) 159a, 159b may further permit access to other networks 170, such as via one or more carrier networks 180a, 180b providing Internet or other network access, or via Wi-Fi communications onto a Wi-Fi network. It will be appreciated that the mobile devices 150a, 150b may be implemented on a particular machine, which may include a computer that is designed, customized, configured, or programmed to perform at least one or more functions of the provisioning module 154a, 154b and other mobile communications, including voice communications, data communications, short message service ("SMS"), wireless application protocol ("WAP"), multimedia message service ("MMS"), Internet communications, other wireless communications, and the like, according to an example embodiment of the invention.

Although mobile devices 150a, 150b are illustrated in FIG. 1, embodiments of the invention may be utilized in conjunction with a wide variety of other devices configured to communicate via the networks 170 and/or carrier networks 180a, 180b, such as personal computers and/or tablet computers. Indeed, embodiments of the invention are applicable to any operating environment in which sensitive data may be represented by tokens.
Fourth, the service provider computers 160 may include any number of processor-driven devices, including but not limited to, a server computer, a mainframe computer, one or more networked computers, a desktop computer, a personal computer, a laptop computer, a mobile computer, or any other processor-based device. A service provider computer 160 may be configured to provide a wide variety of services to a mobile device user, such as technical services and/or financial reporting services. In addition to having one or more processors 166, each of the service provider computers 160 may further include one or more memory devices 162, input/output ("I/O") interfaces 168, and network interface(s) 169. The memory 162 may be any computer-readable medium, coupled to the processor(s) 166, such as RAM, ROM, and/or a removable storage device for storing data files and a DBMS to facilitate management of data files and other data stored in the memory 162 and or stored in one or more separate databases 175 (e.g., a database of received token information, etc.). The memory 162 may also store various program modules, such as an operating system ("OS") and a token management module 164. The OS may be, but is not limited to, Microsoft Windows®, Apple OSX™, Unix, a mainframe computer operating system (e.g., IBM z/OS, MVS, OS/390, etc.), or a specially designed operating system. The token management module 164 may comprise computer-executable program instructions or software, including a dedicated program, for managing tokens and/or token information received from the TSP computer 110, managing information represented by tokens, managing associations between tokens and other information, processing tokens received from mobile devices 150a, 150b in order to access stored information represented by the tokens, and/or verifying identity and/or authenticating the mobile devices 150a, 150b and/or mobile device users.

Still referring to each service provider computer 160 the I/O interface(s) 168 may facilitate communication between the processors 166 and various I/O devices, such as a keyboard, mouse, printer, microphone, speaker, monitor, barcode reader/scanner, RFID reader, and the like. The network interface(s) 169 may take any of a number of forms, such as, but not limited to, a network interface card, a modem, a wireless network card, a cellular network card, or any other means operable for facilitating communications with the network 170. It will be appreciated that the service provider computer 160 may be implemented on a particular machine, which may include a computer that is designed, customized, configured, or programmed to perform at least one or more functions of token verification and/or provide other functions to a mobile device or mobile device user (e.g., technical support functions, etc.).

The network 170 may include any telecommunication and/or data network, whether public, private, or a combination thereof, including a local area network, a wide area network, an intranet, an internet, the Internet, intermediate hand-held data transfer devices, a publicly switched telephone network ("PSTN"), a cellular network, and/or any combination thereof and may be wired and/or wireless. The network 170 may also allow for real time, near real time, off-line, and/or batch transactions to be transmitted between or among the TSP computer 110, the MNO computer(s) 140a, 140b, the mobile devices 150a, 150b, and the service provider computer 160. Due to network connectivity, various methodologies as described herein may be practiced in the context of distributed computing environments. It will also be appreciated that the network 170 may include a plurality of networks, each with devices such as gateways and routers for providing connectivity between or among networks 170. Instead of, or in addition to, a network 170, dedicated communication links may be used to connect the various devices in accordance with an example embodiment.

The mobile carrier networks 180a, 180b may include any cellular telecommunications network, each operated by a respective mobile network operator. The mobile carrier networks may be implemented to operate according to one or more wireless technology formats, including, but not limited to, CDMA, GSM, UWC, UMTS, GPRS, and/or any "generation" or version thereof. Accordingly, in one embodiment, each mobile device 150a, 150b is configured to operate primarily on a certain carrier network 180a, 180b and is operated by the mobile network operator with which the mobile device end user has an agreement and with which the mobile device is registered. It is appreciated, however, that, according to various embodiments, mobile devices 150a, 150b and carrier networks 180a, 180b may be configured to permit interoperability of mobile devices on non-registered carrier networks 180a, 180b.

Generally, each of the memories and data storage devices, such as the memories 112, 142a, 142b, 152a, 152b, 162 and the databases 138, 175 and/or any other memory and data storage device, can store data and information for subsequent retrieval. In this manner, the system 100 can store various received or collected information in memory or a database associated with one or more of the TSP computer(s) 110, the MNO computer(s) 140a, 140b, the mobile devices 150a, 150b, and/or the service provider computer(s) 160. The memories and databases can be in communication with each other and/or other databases, such as a centralized database, or other types of data storage devices. When needed, data or information stored in a memory or a database may be transmitted to a centralized database capable of receiving data, information, or data records from more than one database or other data storage devices. In other embodiments, the databases shown can be integrated or distributed into any number of databases or other data storage devices.

Suitable processors, such as the processors 116, 146a, 146b, 151a, 151b, 166, may comprise a microprocessor, an application-specific integrated circuit ("ASIC"), and/or state machine. Example processors can be those provided by Intel Corporation (Santa Clara, Calif.), AMD Corporation (Sunnyvale, Calif.), and Motorola Corporation ( Schaumburg, Ill.). According to various embodiments, one or more of the computers can be configured as a multi-processor computer having multiple processors 116, 146a, 146b, 151a, 151b, 166 providing parallel and/or redundant processing capabilities. Such processors comprise, or may be in communication with, media, for example, computer-readable media, which stores instructions that, when executed by the processor, cause the processor to perform the elements described herein. Embodiments of computer-readable media include, but are not limited to, an electronic, optical, magnetic, or other storage or transmission device capable of providing a processor with computer-readable instructions. Other examples of suitable media include, but are not limited to, a floppy disk, pen drive, CD-ROM, DVD, magnetic disk, memory chip, ROM, RAM, EPROM, EEPROM, a configured processor, all optical media, all magnetic tape or other magnetic media, or any other medium from which a computer processor can read instructions. Also, various other forms of computer-readable
media may transmit or carry instructions to a computer, including a router, gateway, private or public network, or other transmission device or channel, both wired and wireless. The instructions may comprise code from any computer-programming language, including but not limited to, assembly, C, C++, C#, Visual Basic, Java, Python, Perl, JavaScript, GPSS, LISP, SAS, Parlay, JAIN, or Open Mobile Architecture.

[0038] The system 100 shown in and described with respect to FIG. 1 is provided by way of example only. Numerous other operating environments, system architectures, and device configurations are possible. Other system embodiments can include fewer or greater numbers of components and may incorporate some or all of the functionality described with respect to the system components shown in FIG. 1. Accordingly, embodiments of the invention should not be construed as being limited to any particular operating environment, system architecture, or device configuration.

[0039] According to an aspect of the invention, methods for representing data or information by tokens may be provided. In this regard, the security of sensitive data may be enhanced while tokens that represent the data are communicated. FIG. 2 illustrates a flow diagram of an example method 200 for communicating a token to a mobile device, according to an example embodiment of the invention. The method 400 may be performed by a mobile device, such as the system 100 illustrated in FIG. 1. The method 400 may begin at block 205.

[0040] At block 205, information to be represented by a token may be identified. For example, a tokenization request may be received from a mobile device, such as one of the mobile devices 150a, 150b illustrated in FIG. 1. The received tokenization request may be evaluated or analyzed in order to determine a type of tokenization situation, such as a customer support situation, a balance reporting situation, or a transaction situation, and the information to be represented by the token (e.g., financial account information, etc.) may be identified based at least in part upon the determined type of tokenization situation. As another example, an indicator of the information to be represented by a token may be included in a received tokenization request.

[0041] At block 210, a type of token for representing the information may be identified. A wide variety of different types of tokens may be utilized as desired in various embodiments of the invention. In certain embodiments, a type of token to be utilized may be determined based at least in part upon the information to be tokenized, the tokenization situation, preferences of a service provider to whom the token will be communicated, and/or preferences associated with the mobile device and/or a mobile device user. Additionally, a wide variety of suitable techniques may be utilized as desired to generate a token. For example, a token may be simply identified as a next unused sequential number. As another example, a token may be derived based upon a wide variety of combinations of base level information and/or other information, such as information associated with the mobile device (e.g., a device identifier, etc.) and/or a secure element associated with the mobile device (e.g., CPLC data, etc.).

[0042] At block 215, which may be optional in certain embodiments of the invention, a lifespan for a token may be determined. In this regard, an amount of time during which the token may be utilized and/or presented to a service provider may be limited. In certain embodiments, the type of token or tokenization situation may be taken into account when determining a token lifespan. For example, a relatively short (e.g., ten minutes, etc.) lifespan may be utilized for a transaction token while a relatively longer (e.g., one hour, one day, etc.) lifespan is utilized for a technical support process.

[0043] At block 220, a token may be generated or identified. The token may be representative of the information to be tokenized. As set forth above, a wide variety of different types of tokens and/or token generation techniques may be utilized to generate or identify a token. Once the token has been generated or identified, the token may be provided to the mobile device at block 225 in response to the tokenization request. As an alternative to communicating the token to the mobile device, base level information and/or instructions for independently identifying or generating the token may be communicated to the mobile device. For example, a base level number and/or an instruction for deriving a token utilizing the base level number and device identifying information may be communicated to the mobile device. As another example, an identifier of one of a series of tokens stored on the mobile device may be communicated.

[0044] At block 230, the token and/or the information represented by the token may be provided to another entity, such as one of the service provider computers 160 illustrated in FIG. 1. In this regard, the token and/or information represented by the token may be stored by a service provider and utilized to facilitate a subsequent authentication and/or validation of the mobile device and/or mobile device user. For example, the token may be stored for a subsequent comparison to a token received from the mobile device or mobile device user.

[0045] The method 400 may end following block 230.

[0046] FIG. 3 illustrates a flow diagram of an example method 400 for utilizing a token in conjunction with a mobile device (or other device), according to an example embodiment of the invention. The method 300 may be performed by a mobile device, such as one of the mobile devices 150a, 150b illustrated in FIG. 1. The method 300 may begin at block 305.

[0047] At block 305, a situation in which a token will be utilized to represent information (e.g., sensitive data, etc.) may be identified. In certain embodiments, a tokenization situation may be identified based upon the receipt of user input. For example, a user may request the initiation of a transaction, and a tokenization situation may be identified based upon the received request. In other embodiments, a tokenization situation may be automatically identified by a mobile device based upon the triggering of any number of predetermined criteria or conditions. For example, an error may be identified by the mobile device, and a service request tokenization situation may be identified.

[0048] Once a tokenization situation has been identified, operations may continue at block 310, and a tokenization request may be prepared or generated. The tokenization request may then be communicated to a suitable tokenization service provider, such as the TSP computer 110 illustrated in FIG. 1. A wide variety of information may be included in the tokenization request as desired in various embodiments of the invention, including but not limited to, an identifier of a type of tokenization situation, identification information for the mobile device and/or mobile device secure element, and/or any number of user preferences for generating a token or token information. The tokenization request may be processed by the TSP computer 110, and token information may be returned to the mobile device. The token information may
be received at block 315. As desired, the token information may include a wide variety of different types of information. For example, the token information may include a generated token. As another example, the token information may include an identifier of a token to be utilized by the mobile device, such as a numerical identifier of a stored token to be utilized. As yet another example, the token information may include data and/or instructions (e.g., base level data and/or algorithms, etc.) for generating or deriving a token by the mobile device.

[0049] At block 320, a determination may be made as to whether a token was received from the TSP computer 110. If it is determined at block 320 that a token has been received, then operations may continue at block 330, and the received token may be identified as a token to be utilized to represent the information. If, however, it is determined at block 320 that a token has not been received, then operations may continue at block 325, and the mobile device may independently identify, generate, or derive a token to be utilized. For example, received token information may be processed in order to derive or identify a token. Operations may then continue at block 330 and the identified or derived token may be identified as a token to be utilized to represent the information.

[0050] At block 335, the token may be provided to another entity or service provider in place of the information represented by the token. In this regard, the security of the represented information may be enhanced. A wide variety of suitable techniques may be utilized to provide the token to a service provider. For example, the mobile device may provide the token via a suitable network connection and/or via any number of suitable Web sites or graphical user interfaces hosted by the service provider. As another example, a mobile device user may provide the token to the service provider via a telephone voice connection, by entering the token via touch tone dialing or voice recognition, and/or by entering the token via a suitable Web form provided by the service provider.

[0051] Once the token has been provided by the mobile device or mobile device user to the service provider, the service provider may compare the received token to a token previously received from the TSP computer 110. In this regard, the service provider may verify the identity of the mobile device and/or user. Additionally, based upon a successful match, the service provider may access the information represented by the token (e.g., account information, etc.) without the information being communicated from the mobile device or stored on a shared memory of the mobile device. As desired, the service provider may request additional information from the mobile device or mobile device user in order to further authenticate the mobile device or mobile device user. For example, during a service call, a mobile device user may provide a service token to a service provider representative in order to facilitate the service provider representative accessing account information for the mobile device user. The service provider representative may then request additional information from the user, such as name, address, and/or security question information, in order to authenticate the user.

[0052] The method 300 may end following block 335.

[0053] The operations described and shown in the methods 200 and 300 of FIGS. 2-3 may be carried out or performed in any suitable order as desired in various embodiments of the invention. Additionally, in certain embodiments, at least a portion of the operations may be carried out in parallel. Furthermore, in certain embodiments, less than or more than the operations described in FIGS. 2-3 may be performed.

[0054] The invention is described above with reference to block and flow diagrams of systems, methods, apparatuses, and/or computer program products according to example embodiments of the invention. It will be understood that one or more blocks of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and the flow diagrams, respectively, can be implemented by computer-executable program instructions. Likewise, some blocks of the block diagrams and flow diagrams may not necessarily need to be performed in the order presented, or may not necessarily need to be performed at all, according to some embodiments of the invention.

[0055] Various block and/or flow diagrams of systems, methods, apparatus, and/or computer program products according to example embodiments of the invention are described above. It will be understood that one or more blocks of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and flow diagrams, respectively, can be implemented by computer-executable program instructions. Likewise, some blocks of the block diagrams and flow diagrams may not necessarily need to be performed in the order presented, or may not necessarily need to be performed at all, according to some embodiments of the invention.

[0056] These computer-executable program instructions may be loaded onto a special purpose computer or other particular machine, a processor, or other programmable data processing apparatus to produce a particular machine, such that the instructions that execute on the computer, processor, or other programmable data processing apparatus create means for implementing one or more functions specified in the flow diagram block or blocks. These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means that implement one or more functions specified in the flow diagram block or blocks. As an example, embodiments of the invention may provide for a computer program product, comprising a computer-readable medium having a computer-readable program code or program instructions embodied therein, said computer-readable program code adapted to be executed to implement one or more functions specified in the flow diagram block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational elements or steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions that execute on the computer or other programmable apparatus provide elements or steps for implementing the functions specified in the flow diagram block or blocks.

[0057] Accordingly, blocks of the block diagrams and flow diagrams support combinations of means for performing the specified functions, combinations of elements or steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that each block of the block diagrams and flow diagrams, and combinations of blocks in the block diagrams and flow diagrams, can be implemented by special purpose, hardware-based computer systems that perform the specified
functions, elements or steps, or combinations of special purpose hardware and computer instructions.

[0058] Many modifications and other embodiments of the invention set forth herein will be apparent having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the invention is not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

The claimed invention is:

1. A computer-implemented method for providing tokens to devices, the method comprising:
   receiving, from a device, a request for a token to represent financial information;
   identifying, in response to the request, token information associated with the token;
   providing at least a portion of the token information to the device; and
   providing the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token subsequently received from one of the device or a user of the device, wherein the above operations are performed by one or more computers associated with a tokenization service provider.

2. The computer-implemented method of claim 1, wherein the token information comprises the token.

3. The computer-implemented method of claim 1, wherein the token information comprises information that may be utilized by the device to identify or derive the token.

4. The computer-implemented method of claim 1, wherein receiving a request for a token comprises receiving a request for a token to represent a financial account number.

5. The computer-implemented method of claim 1, further comprising:
   identifying a tokenization situation associated with the request; and
   identifying the token information based at least in part upon the identified tokenization situation.

6. A system for providing tokens to devices, the system comprising:
   at least one memory configured to store computer-executable instructions; and
   at least one processor configured to access the at least one memory and execute the computer-executable instructions to:
   receive, from a device, a request for a token to represent financial information;
   identify, in response to the request, token information associated with the token;
   provide at least a portion of the token information to the device; and
   provide the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token subsequently received from one of the device or a user of the device, wherein the above operations are performed by one or more computers associated with a tokenization service provider.

7. The system of claim 6, wherein the token information comprises the token.

8. The system of claim 6, wherein the token information comprises information that may be utilized by the device to identify or derive the token.

9. The system of claim 6, wherein the computer-executable instructions to receive a request for a token comprise instructions to receive a request for a token to represent a financial account number.

10. The system of claim 6, wherein the at least one processor is further configured to execute the computer-executable instructions to:
   identify a tokenization situation associated with the request; and
   identify the token information based at least in part upon the identified tokenization situation.

11. A method comprising:
   receiving, from a mobile device, a request for a token to represent financial information;
   identifying, in response to the request, token information associated with the token;
   providing at least a portion of the token information to the mobile device; and
   providing the token to a third party entity, wherein the third party entity utilizes the received token to evaluate a second token received from one of the mobile device or a user of the mobile device, wherein the above operations are performed by one or more computers associated with a service provider.

12. The computer-implemented method of claim 11, wherein the token information comprises the token.

13. The computer-implemented method of claim 11, wherein the token information comprises information that may be utilized by the mobile device to identify or derive the token.

14. The computer-implemented method of claim 11, wherein receiving a request for a token comprises receiving a request for a token to represent a financial account number.

15. The computer-implemented method of claim 11, further comprising:
   identifying a tokenization situation associated with the request; and
   identifying the token information based at least in part upon the identified tokenization situation.