

(51) International Patent Classification:
H04L 9/00 (2006.01)(21) International Application Number:
PCT/US2009/033789(22) International Filing Date:
11 February 2009 (11.02.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/031,864 15 February 2008 (15.02.2008) US(71) Applicant (for all designated States except US): **FIRST DATA CORPORATION** [US/US]; 6200 S. Quebec St., Suite 270, Greenwood Village, CO 80111 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **TOOMER, Christopher, L.** [US/US]; 10225 Sweet Rock Ct., Parker, CO 80134 (US). **ARTHUR, Steven, E.** [US/US]; 1895 Baguette Dr., Castle Rock, CO 80108 (US).(74) Agents: **GIBBY, Darin, J.** et al.; Townsend and Townsend and Crew LLP, 1400 Wewatta Street, Suite 600, Denver, CO 80202-5556 (US).

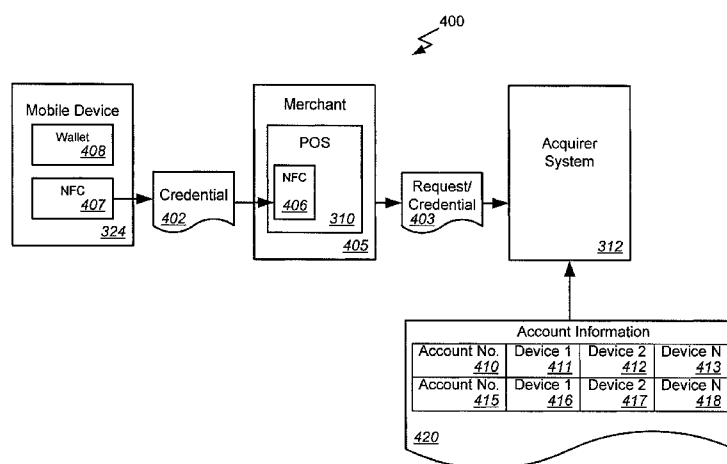
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SECURE AUTHORIZATION OF CONTACTLESS TRANSACTION

**FIG. 4**

(57) **Abstract:** Methods, systems, and machine-readable media are disclosed for securely authorizing a financial transaction utilizing an electronic payment credential. According to one embodiment, a method of authorizing a financial transaction utilizing an electronic payment credential can comprise maintaining information identifying an account associated with the electronic payment credential. The information can also identify one or more electronic devices authorized to use the electronic payment credential. A request to authorize the transaction can be received. The request can include information identifying an electronic device presenting the payment credential. The transaction can be authorized based at least in part on the information identifying the account. Authorizing can comprise determining the electronic device presenting the payment credential is one of the electronic devices authorized to use the electronic payment credential.

SECURE AUTHORIZATION OF CONTACTLESS TRANSACTION

BACKGROUND OF THE INVENTION

[0001] Embodiments of the present invention generally relate to payment systems. More specifically, embodiments of the present invention relate to securely authorizing a financial transaction utilizing an electronic payment credential.

[0002] Various forms of wireless or contactless devices have been introduced for use in various types of transactions. For example, contactless transaction initiation is often performed with a “smart” card or other device such as a key fob or a mobile device such as a cell phone or Personal Digital Assistant (PDA) containing a memory and a processor. Such a card or device typically also includes Radio-Frequency Identification (“RFID”) or Near-Field Communications (NFC) components for contactless communication with a Point-Of-Sale (POS) device. The information stored in the memory of the device and communicated via the RFID or NFC components to the POS device is generally similar or identical to the information recorded on the magnetic stripe of a card, i.e., account number etc. Thus, in some cases, such devices may be utilized instead of more conventional cards.

[0003] Conveniently, accounts represented by information stored in such electronic devices, i.e., an electronic payment credential, can be programmed or provisioned to the electronic device in many different ways. For example, the information or credential can be downloaded to the device over-the-air, e.g., via a wireless connection with a service provider's network, pre-programmed onto the device, downloaded to the device from a client computer, manually entered by a user of the device, etc. However, it is important to assure that the account information is not provisioned to or used by electronic devices which are not authorized to utilize that account information. For example, a particular electronic credential may be authorized for use on one or a small group of electronic devices. To prevent theft, fraud, or accident use of the credential on devices which are not authorized to use the credential, system and methods should be used to authorize a financial transaction utilizing the electronic payment credential and the device presenting the credential.

BRIEF SUMMARY OF THE INVENTION

[0004] Methods, systems, and machine-readable media are disclosed for securely authorizing a financial transaction utilizing an electronic payment credential. For example, the electronic payment credential can comprise a credential representing a pre-paid account such as a gift card or other account. According to one embodiment, a method of authorizing a financial transaction utilizing an electronic payment credential can comprise maintaining information identifying an account associated with the electronic payment credential. The information can also identify one or more electronic devices authorized to use the electronic payment credential. A request to authorize the transaction can be received. The request can include information identifying an electronic device presenting the payment credential. The transaction can be authorized based at least in part on the information identifying the account. Authorizing can comprise determining the electronic device presenting the payment credential is one of the electronic devices authorized to use the electronic payment credential.

[0005] In some cases, the information identifying the electronic device presenting the payment credential can comprise a unique static identifier. For example, the unique static identifier comprises a device serial number. In other cases, the information identifying the electronic device presenting the payment credential can comprise a unique dynamic identifier. In such a case, prior to receiving the request to authorize the transaction, a unique device identifier can be generated, saved in the information identifying the account, and transferred to the electronic device. Then, after authorizing the transaction, a new unique device identifier can be generated, saved in the information identifying the account, and transferred to the electronic device for use in authorizing subsequent transactions. Alternatively, the unique dynamic identifier can comprise a combination of an account number for the account and a random value. For example, the random value can comprise an elapsed time since a previous transaction, a time of occurrence of a last transaction, Greenwich Mean Time (GMT), or other value.

[0006] According to another embodiment, a system for authorizing a financial transaction utilizing an electronic payment credential can comprise a mobile electronic device adapted to maintain the electronic payment credential and initiate the financial transaction utilizing the electronic payment credential. For example, the system may include a point-of-sale device and the mobile electronic device can initiate the financial transaction by presenting the

payment credential to the point-of-sale device. The electronic payment credential can comprise, for example, a credential representing a pre-paid account such as a gift card or other account. The system can also include an acquirer system adapted to maintain information identifying an account associated with the electronic payment credential. The information can identify one or more electronic devices authorized to use the electronic payment credential. The acquirer system can receive a request to authorize the transaction, for example via the point-of-sale device, if any. The request can include information identifying the mobile electronic device initiating the financial transaction utilizing the electronic payment credential. The acquirer system can authorize the transaction based at least in part on the information identifying the account. Authorizing can comprise determining the mobile electronic device initiating the transaction is one of the electronic devices authorized to use the electronic payment credential.

[0007] In some cases, the information identifying the electronic device presenting the payment credential can comprise a unique static identifier. For example, the unique static identifier can comprise a device serial number for the mobile electronic device. In other cases, the information identifying the electronic device presenting the payment credential can comprise a unique dynamic identifier. For example, the acquirer system can be adapted to, prior to receiving the request to authorize the transaction, generate a unique device identifier, save the unique device identifier in the information identifying the account, and transfer the unique device identifier to the electronic device. The acquirer system can then, after authorizing the transaction, generate a new unique device identifier, save the new unique device identifier in the information identifying the account, and transfer the new unique device identifier to the electronic device for use in authorizing subsequent transactions. Alternatively, the unique dynamic identifier can comprise a combination of an account number for the account and a random value. For example, the random value can comprise an elapsed time since a previous transaction, a time of occurrence of a last transaction, Greenwich Mean Time (GMT), or other value.

[0008] According to yet another embodiment, a machine-readable medium can have stored thereon a series of instructions which, when executed by a processor, cause the processor to authorize a financial transaction utilizing an electronic payment credential by maintaining information identifying an account associated with the electronic payment credential, the information identifying one or more electronic devices authorized to use the electronic

payment credential, receiving a request to authorize the transaction, wherein the request includes information identifying an electronic device presenting the payment credential, and authorizing the transaction based at least in part on the information identifying the account, wherein authorizing comprises determining the electronic device presenting the payment
5 credential is one of the electronic devices authorized to use the electronic payment credential. For example, the electronic payment credential can comprise a credential representing a pre-paid account such as a gift card account. The information identifying the electronic device presenting the payment credential can comprise a unique static identifier or a unique dynamic identifier.

10

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 is a block diagram illustrating an exemplary environment in which embodiments of the present invention may be implemented.

[0010] FIG. 2 is a block diagram illustrating an exemplary computer system upon which embodiments of the present invention may be implemented.

15 [0011] FIG. 3 is block diagram illustrating, at a high level, a system for processing transactions utilizing a mobile electronic device according to one embodiment of the present invention.

[0012] FIG. 4 is a block diagram illustrating additional details of the system of FIG. 3 according to one embodiment of the present invention.

20 [0013] FIG. 5 is a block diagram illustrating components of an exemplary point of sale device that may be used with various embodiments of the present invention.

[0014] FIG. 6 is a block diagram illustrating components of an exemplary mobile device that may be used in various embodiments of the present invention.

25 [0015] FIG. 7 is a flowchart illustrating a process for authorizing a financial transaction utilizing an electronic payment credential according to one embodiment of the present invention.

[0016] FIG. 8 is a flowchart illustrating a process for implementing a unique dynamic identifier according to one embodiment of the present invention.

[0017] FIG. 9 is a flowchart illustrating a process for implementing a unique dynamic identifier according to an alternative embodiment of the present invention.

5

DETAILED DESCRIPTION OF THE INVENTION

[0018] In the following description, for the purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some of these specific details. In other instances, well-known structures and devices are shown in block diagram form.

10

[0019] Embodiments of the invention provide methods and systems for authorizing financial transactions initiated by or otherwise involving use of a contactless or mobile device. In some such embodiments, the processes are executed by an entity on behalf of one or more client organizations. The description below sometimes provides illustrations that use an example where a client organization is a financial institution, but there is no such requirement for the invention and the methods are intended also to be applicable to other types of organizations that make use of large collections of data. For example, embodiments of the invention may also be used for managing health-care documents or information.

15

[0020] The description herein sometimes refers to "clients" and to "customers." Reference to "clients" is intended to refer to persons, i.e. individuals, entities, or their agents, on whose behalf a set of information is managed. Reference to "customers" or "consumer" is intended to refer to persons, i.e. individuals, entities, or their agents, who are the subject of or related to that information. Thus, merely for purposes of illustration, in the case where the information comprises credit-card account records for a credit card issued to Mr. Jones by Bank A, Bank A corresponds to a client and Mr. Jones corresponds to a customer or consumer.

20

25

[0021] In describing embodiments of the invention, reference is sometimes made to other terms having specific intended meanings. For example, as used herein, the term "acquirer" is

used to refer to a business entity that has a business relationship with a merchant, one or more financial institutions, and other entities and handles credit card and/or other financial transactions for and/or involving those entities. In such a context, an "acquirer system" is a system operated by an acquirer that processes and authorizes credit card and/or other transactions. Acquirer systems can include those operated by credit card processing entities, such as First Data Corporation, Greenwood Village, Colorado. However, embodiments of the present invention are not limited to such financial services or payment processing. Thus, an acquirer system can be considered to be any system capable of receiving a communication from another system or entity and processing information on behalf of that entity.

[0022] The term "carrier" refers to a provider of a network and/or service for use by a mobile device. For example, a carrier can include, but is not limited to, a provider of a cellular or other wireless communications service for use by a mobile device. The terms "carrier" and "service provider" are used interchangeably herein and are intended to be synonymous. Similarly, the terms carrier network and service provider network are used interchangeably herein and are intended to be synonymous.

[0023] The term "mobile device" is used herein to refer to any small, likely handheld, electronic device that can be used to initiate or otherwise participate in a financial transaction. For example, a mobile device can include, but is not limited to, a cellular telephone, a Personal Digital Assistant (PDA), a smart card or other contactless device, etc. Exemplary devices that may be adapted for use as mobile devices in various embodiments of the present invention are described in co-pending and commonly assigned U.S. Patent Application No. 11/672,417 entitled "Contactless Electronic Wallet Payment Device" filed on February 7, 2007; U.S. Patent Application No. 11/551,063 entitled "Presentation Instrument with Non-Financial Functionality" filed on October 19, 2006; and U.S. Provisional Patent Application No. 60/833,022 entitled "Mobile Payment Device with Magnetic Stripe" filed on July 24, 2006, each of which is incorporated herein by reference in its entirety for all purposes. As used herein, the terms mobile device and contactless device are intended to be synonymous.

[0024] A "mobile wallet" or "mobile wallet application" refers to a client software application that can reside on and/or be executed by a mobile device. According to one embodiment, the mobile wallet application can be adapted to store payment vehicle information. In some cases, the mobile wallet can allow storage of multiple payment vehicles

and can provide a user interface that can be used to select a specific payment vehicle. Additionally, the mobile wallet can be adapted to provide security to deter fraudulent and unauthorized use of the payment vehicles. The terms mobile wallet and mobile wallet application are used interchangeably herein and are intended to be synonymous.

5 [0025] "Near Field Communication" (NFC) refers to short range (20cm or less) wireless technology used to facilitate communication between electronic devices in close proximity. For example, embodiments of the present invention provide for the use of NFC and/or other relatively short range communications between a mobile device and a POS device such as when a user of the mobile device scans or waves the mobile device in front of or near the
10 POS device when paying for goods or services.

[0026] A "payment network" refers herein to an infrastructure that supports the exchange of data in implementing payment transactions. It is anticipated that the data exchange typically proceeds between merchants and financial institutions. Examples of existing commercial networks that are included within the definition of "payment network" include
15 the STAR/MAC network, the NYCE® network, the VISA® network, and the MasterCard® network. Access to a network by a consumer can be achieved through entry of a secret code, such as a personal identification number ("PIN"), in combination with data extracted from the mobile device. In some embodiments, a signature of the consumer may be used in lieu of a secret code. In some instances, particularly in support of transactions having a low value, a
20 consumer might be permitted access to the payment network with only information extracted from the mobile device, without the need to provide a PIN or signature.

[0027] The term "payment vehicle" is used herein to refer to a method of payment. For example, payment vehicles can include, but are not limited to, credit, debit, stored-value, and other types of accounts. In some embodiments, a payment vehicle can include loyalty points
25 or other value accumulated, for example, under a loyalty program.

[0028] A "point-of-sale device" or "POS device" refers herein to any physical device situated at a location where a consumer may provide payment in support of a transaction. Such physical locations are typically merchant locations, such as where the POS device is operated by a clerk or is available for self-operation by the consumers, but may also be in
30 other locations. For instance, certain automatic teller machines "ATMs" may be equipped to

support transactions for the sale of movie or sporting-event tickets even remote from the merchant location. Other similar types of transactions that may be performed with a POS device at a location remote from the merchant will also be evident to those of skill in the art. In some cases, a personal computer equipped with the appropriate structure may be used as a POS device even when located on the consumer premises. Examples of POS devices thus include, without limitation, personal computers, cash registers, and any devices capable of reading a magnetic stripe, an RFID chip, NFC communications, or other information from a mobile device, contactless device, card, etc. Exemplary devices that may be adapted for use in various embodiments of the present invention are described in the following commonly assigned applications, the entire disclosures of which are incorporated herein by reference for all purposes: U.S. Provisional Patent Application No. 60/147,889, entitled "Integrated Point OF Sale Device," filed August 9, 1999 by Randy J. Templeton *et al.*; U.S. Patent Application No. 09/634,901, entitled "Point of Sale Payment System," filed August 9, 2000 by Randy J. Templeton *et al.*; U.S. Patent Application No. 10/116,689, entitled "Systems and Methods for Performing Transactions at a Point-of-Sale," filed April 3, 2002 by Earney Stoutenburg *et al.*; U.S. Patent Application No. 10/116,733, entitled "Systems and Methods for Deploying a Point-of-Sale System," filed April 3, 2002 by Earney Stoutenburg *et al.*; U.S. Patent Application No. 10/116,686, entitled "Systems and Methods for Utilizing A Point-of-Sale System," filed April 3, 2002 by Earney Stoutenburg *et al.*; and U.S. Patent Application No. 10/116,735, entitled "Systems and Methods for Configuring a Point-of-Sale System," filed April 3, 2002 by Earney Stoutenburg.

[0029] A "POS processing system" refers to a computational system used by merchants to control communications between POS devices and payment networks. Such systems may be run internally by merchants, may be run by merchant consortia, or may be outsourced to service providers in different embodiments. Some exemplary POS processing systems which may be adapted to operate with embodiments of the present invention are described in commonly assigned U.S. Patent Nos. 6,886,742, 6,827,260 and 7,086,584, the complete disclosures of which are herein incorporated by reference.

[0030] A "primary account number" or "PAN" refers to a number assigned to an account. The PAN is generally assigned by a financial institution maintaining the account. In most embodiments, it is anticipated that the PAN will identify an account associated with the wireless device and be included as data stored by the memory of the wireless device.

Identification of the PAN permits a financial institution that maintains the account to make a unique identification of the consumer initiating a payment or other transaction and determine which of potentially several accounts is to be used in supporting the transaction.

[0031] The terms "real time" or "near real time" are used herein to refer to a process or action that occurs within a relatively short time. Importantly, the terms real time and near real time are not intended to imply an immediate or instantaneous results or action. Rather, the terms are used to refer to processes or actions that can be performed relatively quickly such as within several seconds or minutes.

[0032] The term "user" refers to an entity, typically a person, that is associated with a particular mobile device. Typically, the user is the person that owns, uses, or leases the mobile device and/or controls the content and use of the payment vehicles maintained within the mobile wallet of the device.

[0033] The ensuing description provides exemplary embodiments only, and is not intended to limit the scope, applicability, or configuration of the disclosure. Rather, the ensuing description of the exemplary embodiments will provide those skilled in the art with an enabling description for implementing an exemplary embodiment. It being understood that various changes may be made in the function and arrangement of elements without departing from the spirit and scope of the invention as set forth in the appended claims.

[0034] Specific details are given in the following description to provide a thorough understanding of the embodiments. However, it will be understood by one of ordinary skill in the art that the embodiments may be practiced without these specific details. For example, circuits, systems, networks, processes, and other components may be shown as components in block diagram form in order not to obscure the embodiments in unnecessary detail. In other instances, well-known circuits, processes, algorithms, structures, and techniques may be shown without unnecessary detail in order to avoid obscuring the embodiments.

[0035] Also, it is noted that individual embodiments may be described as a process which is depicted as a flowchart, a flow diagram, a data flow diagram, a structure diagram, or a block diagram. Although a flowchart may describe the operations as a sequential process, many of the operations can be performed in parallel or concurrently. In addition, the order of

the operations may be re-arranged. A process is terminated when its operations are completed, but could have additional steps not included in a figure. A process may correspond to a method, a function, a procedure, a subroutine, a subprogram, etc. When a process corresponds to a function, its termination can correspond to a return of the function to the calling function or the main function.

[0036] The term "machine-readable medium" includes, but is not limited to, portable or fixed storage devices, optical storage devices, wireless channels, and various other mediums capable of storing, containing, or carrying instruction(s) and/or data. A code segment or machine-executable instructions may represent a procedure, a function, a subprogram, a program, a routine, a subroutine, a module, a software package, a class, or any combination of instructions, data structures, or program statements. A code segment may be coupled to another code segment or a hardware circuit by passing and/or receiving information, data, arguments, parameters, or memory contents. Information, arguments, parameters, data, etc. may be passed, forwarded, or transmitted via any suitable means including memory sharing, message passing, token passing, network transmission, etc.

[0037] Furthermore, embodiments may be implemented by hardware, software, firmware, middleware, microcode, hardware description languages, or any combination thereof. When implemented in software, firmware, middleware or microcode, the program code or code segments to perform the necessary tasks may be stored in a machine readable medium. One or more processors may perform the necessary tasks.

[0038] Embodiments of the present invention provide methods, systems, and machine-readable media for securely authorizing a financial transaction utilizing an electronic payment credential. For example, the electronic payment credential can comprise information representing an account including but not limited to a pre-paid account such as a gift card or other account. Generally speaking, a mobile device such as a cell phone, PDA, MP3 player, or other device can be adapted to maintain account information related to one or more financial accounts. For example, information such as a bank name, account number, account type, etc can be maintained in the device in and/or accessible by a mobile wallet. In other cases, identifying information other than an account number may be stored in or by the mobile wallet. For example, rather than storing an account number, the mobile wallet may

store or generate a unique identifier for use by other systems in identifying one or more accounts associated with the mobile wallet.

[0039] Regardless of the exact form or format of the information or credential, information identifying an account associated with the electronic payment credential can be maintained,,
5 for example by an acquirer system. The information can also identify one or more electronic devices authorized to use the electronic payment credential. A request to authorize the transaction can be received by the acquirer or other system. The request can include information identifying an electronic device presenting the payment credential. The transaction can be authorized based at least in part on the information identifying the account.
10 That is, authorizing the transaction can comprise determining whether the electronic device presenting the payment credential is one of the electronic devices authorized to use the electronic payment credential as identified in the account information. Additional details of the various embodiments of the present invention will be described below with reference to the figures.

[0040] FIG. 1 is a block diagram illustrating an exemplary environment in which
15 embodiments of the present invention may be implemented. In this example, the system can include one or more server computers 105, 110, 115 which can be general purpose computers and/or specialized server computers (including, merely by way of example, PC servers, UNIX servers, mid-range servers, mainframe computers rack-mounted servers, etc.). One or
20 more of the servers (*e.g.*, 130) may be dedicated to running applications, such as a business application, a web server, application server, etc. Such servers may be used to execute a plurality of processes related to financial transactions of one or more consumers on behalf of one or more client financial institutions. For example, one or more of the servers 105, 110, 115 may execute one or more processes for recording transactions on a credit card issued to
25 the consumer by the financial institution. Other processes may provide for paying a merchant for the consumer's purchase, billing the consumer, etc. The applications can also include any number of applications for controlling access to resources of the servers 105, 110, 115.

[0041] In some embodiments, the system 100 may also include a network 115. The network may can be any type of network familiar to those skilled in the art that can support
30 data communications using any of a variety of commercially-available protocols, including without limitation TCP/IP, SNA, IPX, AppleTalk, and the like. Merely by way of example,

the network 115 maybe a local area network ("LAN"), such as an Ethernet network, a Token-Ring network and/or the like; a wide-area network; a virtual network, including without limitation a virtual private network ("VPN"); the Internet; an intranet; an extranet; a public switched telephone network ("PSTN"); an infra-red network; a wireless network (*e.g.*, a
5 network operating under any of the IEEE 802.11 suite of protocols, the Bluetooth protocol known in the art, and/or any other wireless protocol); and/or any combination of these and/or other networks such as GSM, GPRS, EDGE, UMTS, 3G, 2.5 G, CDMA, CDMA2000, WCDMA, EVDO etc.

[0042] The system 100 can include one or more user computers which may be used to
10 operate a client, whether a dedicate application, web browser, etc. For example, the user computers can include a client system 125 operated by a client financial institution, a customer system 130 operated by a customer or consumer, a merchant system 135 operated by a merchant or vendor, etc. The user computers 125, 130, 135 can be general purpose personal computers (including, merely by way of example, personal computers and/or laptop
15 computers running various versions of Microsoft Corp.'s Windows and/or Apple Corp.'s Macintosh operating systems) and/or workstation computers running any of a variety of commercially-available UNIX or UNIX-like operating systems (including without limitation, the variety of GNU/Linux operating systems). These user computers 125, 130, 135 may also have any of a variety of applications, including one or more development systems, database
20 client and/or server applications, and web browser applications. Alternatively, the user computers 125, 130, 135 may be any other electronic device, such as a thin-client computer, Internet-enabled mobile telephone, and/or personal digital assistant, capable of communicating via a network (*e.g.*, the network 115 described below) and/or displaying and navigating web pages or other types of electronic documents. Although the exemplary
25 system 100 is shown with three user computers, any number of user computers may be supported.

[0043] The system 100 may also include one or more databases or repositories of enabling data 145. The database(s) of enabling data 145 may reside in a variety of locations. By way of example, a database 145 may reside on a storage medium local to (and/or resident in) one
30 or more of the computers 105, 110, 115, 125, 130. Alternatively, it may be remote from any or all of the computers 105, 110, 115, 125, 130, and/or in communication (*e.g.*, via the network 120) with one or more of these. In a particular set of embodiments, the database 145

may reside in a storage-area network ("SAN") familiar to those skilled in the art. Similarly, any necessary files for performing the functions attributed to the computers 105, 110, 115, 125, 130 may be stored locally on the respective computer and/or remotely, as appropriate. In one set of embodiments, the database 145 may be a relational database that is adapted to store, update, and retrieve data in response to SQL-formatted commands. The repository of enabling data 145 can include a wide variety of information related to financial transactions related to the consumer and/or specified by different entities such as merchants, financial institutions, third-party advertisers, etc.

[0044] FIG. 2 is a block diagram illustrating an exemplary computer system upon which various elements of the exemplary environment illustrated in Figure 1 may be implemented. The computer system 200 is shown comprising hardware elements that may be electrically coupled via a bus 255. The hardware elements may include one or more central processing units (CPUs) 205; one or more input devices 210 (*e.g.*, a scan device, a mouse, a keyboard, etc.); and one or more output devices 215 (*e.g.*, a display device, a printer, etc.). The computer system 200 may also include one or more storage device 220. By way of example, storage device(s) 220 may be disk drives, optical storage devices, solid-state storage device such as a random access memory ("RAM") and/or a read-only memory ("ROM"), which can be programmable, flash-updateable and/or the like.

[0045] The computer system 200 may additionally include a computer-readable storage media reader 225; a communications system 230 (*e.g.*, a modem, a network card (wireless or wired), an infra-red communication device, etc.); and working memory 240, which may include RAM and ROM devices as described above communicatively coupled with and readable by CPU(s) 205. In some embodiments, the computer system 200 may also include a processing acceleration unit 235, which can include a DSP, a special-purpose processor and/or the like.

[0046] The computer-readable storage media reader 225 can further be connected to a computer-readable storage medium, together (and, optionally, in combination with storage device(s) 220) comprehensively representing remote, local, fixed, and/or removable storage devices plus storage media for temporarily and/or more permanently containing computer-readable information. The communications system 230 may permit data to be exchanged with a network and/or any other computer or other type of device.

[0047] The computer system 200 may also comprise software elements, shown as being currently located within a working memory 240, including an operating system 245 and/or other code 250, such as an application program. The application programs may implement the methods of the invention as described herein. It should be appreciated that alternate
5 embodiments of a computer system 200 may have numerous variations from that described above. For example, customized hardware might also be used and/or particular elements might be implemented in hardware, software (including portable software, such as applets), or both. Further, connection to other computing devices such as network input/output devices may be employed.

10 [0048] FIG. 3 is block diagram illustrating, at a high level, a system for processing transactions utilizing a mobile electronic device according to one embodiment of the present invention. Traditionally, a credit card may be issued to a customer by a financial institution such as a bank and typically displays a logo for an association that implements rules that govern aspects of use of the card. Account information is usually printed on the face of the
15 card, specifying an account number and name of an authorized holder of the card. This information is also stored together with additional information on a magnetic stripe that is usually affixed to the back of the card. When the cardholder wishes to execute a transaction, such as a financial transaction for the purchase of goods and/or services, he presents the card 320 to a clerk at a merchant location, who swipes the card through a magnetic-stripe reader
20 comprised by a point-of-sale device 308. Multiple point-of-sale devices 308-310 may have been provided at a variety of locations by an acquirer, who acts as an intermediary between merchants and the issuer financial institutions. As an intermediary, the acquirer coordinates transaction routing and performs a variety of backend processes.

[0049] The point-of-sale device 308 typically initiates a connection to an acquirer system
25 312 through a network 304 such as the Internet or another network as described above. A packet of information that includes information read from the magnetic stripe of the card 320, a merchant identifier, the date, and transaction amount are forwarded by the point-of-sale device 308 through the network 304 to the acquirer system 312. The acquirer system 312 may store some of the information and send an authorization request, via financial network
30 313, to the issuing financial institution 316, which may be identified from a portion of the account number read from the magnetic stripe. The transaction is authorized or denied depending on such factors as the validity of the cardholder name, the validity of the card

number, the level of available credit in comparison with the transaction amount, and the like. If authorized, an authorization code is routed back through the acquirer system 312, which captures additional information and forwards the authorization code back to the originating point-of-sale device 308 so that the transaction may be completed. Periodically, such as at the end of every day, the transactions are settled by the acquirer initiating funds transfers that fund merchant bank accounts with total transaction amounts that may have resulted from multiple transactions by multiple customers.

[0050] Other types of accounts may operate with similar structures, although the details for each type of account are different. For example, use of a debit account typically requires that the customer provide a personal identification number ("PIN"), which must be validated before any authorization for the transaction can be provided. Authorization usually depends on the current level of funds actually in the identified account rather than on a credit level, and funds transfer is usually executed substantially contemporaneously with providing the authorization rather than performing periodic settlement. Other types of accounts may use arrangements that have similar differences in their particulars.

[0051] According to one embodiment, a mobile device 324 may be used in addition to or instead of a card or other token representing an account. Here, the mobile device 324 is shown for exemplary purposes in the form of a cellular telephone. However, as noted above, the mobile device 324 may be any of a variety of different mobile devices including but not limited to a PDA, MP3 player, etc. The mobile device 324 may communicate wirelessly with point-of-sale devices 314 that have been equipped for wireless communications, such as through an NFC connection.

[0052] According to one embodiment, the mobile device 324 can store and/or execute a mobile wallet application adapted to maintain account numbers and/or other information, i.e., electronic payment credentials, related to one or more financial accounts such as credit accounts, debit accounts, demand deposit accounts, stored value accounts, etc. maintained by one or more financial institutions 316-318. The mobile device 324, for example via the mobile wallet application, may allow the user to review accounts that are stored or identified in the mobile device 324 and select an account for a particular transaction such as a purchase. Upon selection of an account for use in the transaction, the user of the mobile device can scan or swipe the device 324 in front of or near the POS device 310 causing the credential of other

information related to the selected account to be read from the mobile device 324 via the NFC connection.

[0053] The credential of other information regarding the selected account can identify the account to be used in supporting transactions, for example, including an indication of the financial institution 316 where that account is maintained, an account number, etc. Such identifications may conveniently be made with numerical strings similar to card numbers that have portions that identify a financial institution and portions that identify specific accounts. Additional information may include ownership details of the account, current balance levels for the account, and the like.

[0054] The point-of-sale device 308 typically initiates a connection to an acquirer system 312 through a network 304 such as the Internet or another network as described above. A packet of information that includes information read from the mobile device 324, a merchant identifier, the date, and transaction amount are forwarded by the point-of-sale device 310 through the network 304 to the acquirer system 312. The acquirer system 312 may store some of the information and send an authorization request, via financial network 313, to the issuing financial institution 318, which may be identified from a portion of the account number read from the mobile device 324. The transaction is authorized or denied depending on such factors as the validity of the account holder name, the validity of the account number, the level of available credit in comparison with the transaction amount, and the like. As will be described in detail below, authorization can also be based at least in part on determining whether the mobile device is authorized to use the account for which the information or credential has been provided. If authorized, an authorization code is routed back through the acquirer system 312, which captures additional information and forwards the authorization code back to the originating point-of-sale device 310 so that the transaction may be completed.

[0055] FIG. 4 is a block diagram illustrating additional details of the system of FIG. 3 according to one embodiment of the present invention. In this example, the system 400 includes a mobile device 324 such as described above. The mobile device 324 can include a Near Field Communications (NFC) transponder 407 and can execute a mobile wallet application 408. The mobile device 324 can be adapted to maintain at least one set of information and/or credential related to a financial account in the mobile wallet 408 and

communicate at least a subset of the information or credential 402 via the NFC transponder 407 upon initiation of a transaction such as a purchase. In the case where the user is making a purchase, from a merchant 405, the user can use the account to pay for the purchase by swiping or passing the mobile device 324 in front of or near an NFC equipped point of sale device 310 provided by the merchant 405.

[0056] The point of sale device 310 can also include an NFC transponder 406. The point of sale device 310 can be adapted to receive the credential 402 for the financial account from the mobile device 324 via the NFC transponder 406 and send a communication or request 403 related to the transaction that includes the credential and/or other information related to the financial account. For example, in the case of a consumer making a purchase using a credit, debit, stored value, or other account, the request can be a request to authorize the transaction.

[0057] The acquirer system 312 can be adapted to maintain information 420 identifying one or more accounts 410 and 415. The information can identify one or more electronic devices authorized to use the electronic payment credential. That is, for a given account 410 and 415, the account information 420 can also include information identifying one or more devices 411-413 and 416-418 which are authorized to use the account. The acquirer system 312 can be updated upon the device information 411-413 and 416-418 upon issuance of an account, modification of an account, etc. to indicate the one or more devices which the user, acquirer, issuer, or other entity indicates to be authorized for use with that account.

[0058] As noted, the acquirer system 312 can receive the request 403 to authorize the transaction and/or the electronic payment credential, for example via the point-of-sale device 310, if any. Also as noted, the request 402 can include information identifying the mobile electronic device 324 initiating the financial transaction utilizing the electronic payment credential 402. The acquirer system 312 can authorize the transaction based at least in part on the account information 420. Authorizing can comprise determining whether the mobile electronic device 324 initiating the transaction is one of the electronic devices 411-413 authorized to use the identified account 410, i.e., authorized to use the electronic payment credential.

[0059] In some cases, the information identifying the electronic device presenting the payment credential can comprise a unique static identifier. For example, the unique static

identifier can comprise a device serial number for the mobile electronic device 324. In other cases, the information identifying the electronic device presenting the payment credential can comprise a unique dynamic identifier. For example, the acquirer system 312 can be adapted to, prior to receiving the request 403 to authorize the transaction, generate a unique device
5 identifier, save the unique device identifier in the information identifying the account 410 or 411, and transfer the unique device identifier to the electronic device 324. Transferring or provisioning the identifier to the mobile device 324 can be achieved in any of a number of different ways. Exemplary methods and systems that may be used for achieving this provisioning are described in U.S. Patent Application No. 11/830,420 filed July 30, 2007 and
10 entitled "Provisioning of a Device for Mobile Commerce", the entire disclosure of which is incorporated herein by reference for all purposes. The acquirer system 312 can then, after authorizing the transaction, generate a new unique device identifier, save the new unique device identifier in the information identifying the account, and transfer the new unique device identifier to the electronic device for use in authorizing subsequent transactions.
15 Alternatively, the unique dynamic identifier can comprise a combination of an account number for the account and a random value. For example, the random value can comprise an elapsed time since a previous transaction, a time of occurrence of a last transaction, Greenwich Mean Time (GMT), or other value known or determinable to both the mobile device 324 and the acquirer system 312.

20 **[0060]** FIG. 5 is a block diagram illustrating components of an exemplary point of sale device that may be used with various embodiments of the present invention. Operations performed by the point-of-sale device 310 are generally coordinated by a controller 504, which is provided in electrical communication with a number of components. For example, the controller 504 can comprise a microprocessor or other computing device executing
25 software stored, for example, in memory 508. Components with which the controller 504 is coupled can include an antenna 512 for transmitting and receiving electromagnetic signals and an NFC module 516 that provides instructions for implementing a communications protocol, such as an NFC protocol. The NFC module 516 performs a more active role than the antenna 512, determining what electromagnetic signals to transmit over the antenna 512
30 and/or interpreting electromagnetic signals that are received by the antenna 512. A port may be provided to permit the exchange of wired communications with the point-of-sale device 504, one example of the port being a TCP/IP port 520 that enables the point-of-sale device

504 to engage in Internet communications. A printer 524 interfaced with the controller 504 permits receipts and other documents to be printed by the point-of-sale device 504.

[0061] FIG. 6 is a block diagram illustrating components of an exemplary mobile device that may be used with various embodiments of the present invention. The mobile device 324 includes a controller 640 which can comprise a microprocessor or other computing device executing software stored, for example, in memory 644 for coordinating the functions of a variety of components. Several of the components that may be controlled by the controller 540 include components used for standard functionality of the mobile device 324. For instance, in embodiments where the mobile device 324 is a cellular telephone, the controller may be interfaced with a microphone 652, a speaker 656, and an antenna 648. The microphone 652 and speaker 656 may be used to receive and amplify voice signals that are exchanged by users of the cellular telephone. The antenna 648 may be used to transmit and receive electromagnetic signals that correspond to encoded versions of the voice signals being exchanged.

[0062] Other components may include a global positioning system 660 that may be used to locate a position of the wireless device. Such a global positioning system 660 functions by transmitting an electromagnetic signal to an orbiting satellite that identifies a relative location of the source of the signal and correlates that relative position with a geographical map of a region of the Earth. An NFC module 668 may also be provided to encode and decode transmissions sent and received electromagnetically with the point of sale device as discussed above. Because transmissions involving the account information include sensitive financial data such as account numbers, a cryptography module 672 may also be provided to allow encryption of data sent and received by the mobile device 324 via the NFC module 668.

[0063] According to one embodiment, the mobile device 324 can also include a mobile wallet module or application 676. The mobile wallet 676 can be adapted to store payment vehicle information, i.e., an electronic payment credential and/or other information identifying one or more financial accounts such as credit accounts, debit accounts, demand deposit accounts, stored value accounts, etc. In some cases, the mobile wallet 676 can allow storage of multiple payment vehicles and can provide a user interface that can be displayed on a screen or display device 680 and through which the user can select a specific payment vehicle by manipulating a keypad, wheel, touch screen, or other input device 682. The

mobile device 324, for example via the mobile wallet application 676, may allow the user to review accounts that are stored in the memory 644 of the mobile device 324 and select an account for a particular transaction such as a purchase. Upon selection of an account for use in the transaction, the user of the mobile device 324 can scan or swipe the device 624 in front of or near the POS device causing some or all of the information identifying the selected account to be read from the mobile device 324 via the NFC connection module 668.

[0064] FIG. 7 is a flowchart illustrating a process for authorizing a financial transaction utilizing an electronic payment credential according to one embodiment of the present invention. As described above, such a process may be performed by an acquirer or other such system to authorize a transaction such as a sale that may be initiated by a mobile device via a point-of-sale or other device. In this example, processing begins with receiving 705 a request to authorize the transaction. As noted above, the acquirer or other authorizing system can maintain information identifying an account associated with the electronic payment credential. The information can also identify one or more electronic devices authorized to use the electronic payment credential. Therefore, upon receiving 705 the request to authorize the transaction, the acquirer or other authorizing system can query 715 the account information or otherwise look up or read the information related to the account or credential identified by the request.

[0065] Also as noted above, the request can include information identifying an electronic device presenting the payment credential. As noted, the information identifying the electronic device that can be included in the request can be a static identifier. For example, the static identifier can comprise a serial number of the electronic device or any other static, unique, and identifiable information that can be used by the acquirer system or other authorizing system to uniquely identify the device. Alternatively, the identifying information can comprise a unique dynamic identifier. Exemplary methods for handling unique dynamic identifiers are described below with reference to FIGs. 8 and 9.

[0066] Regardless of the exact form of the identifier, a determination 720 can be made as to whether the electronic device presenting the payment credential, i.e., the device identified in the request, is one of the electronic devices authorized to use the electronic payment credential. In response to determining the device is identified in the account information as an authorized device, the transaction can be authorized 725, for example by sending an

authorization message to the requesting point-of-sale or other device. That is, the transaction can be authorized based at least in part on the information identifying the account.

[0067] FIG. 8 is a flowchart illustrating a process for implementing a unique dynamic identifier according to one embodiment of the present invention. It should become clear that this example presupposes that a unique identifier has already been provided to the mobile device for use in a request. That is, prior to receiving the request to authorize the transaction, a unique device identifier can be generated, saved in the information identifying the account, and transferred to the electronic device.

[0068] In this example, as in the previous example, processing begins with receiving 805 a request to authorize the transaction. As noted above, the acquirer or other authorizing system can maintain information identifying an account associated with the electronic payment credential. The information can also identify one or more electronic devices authorized to use the electronic payment credential. Therefore, upon receiving 805 the request to authorize the transaction, the acquirer or other authorizing system can query 815 the account information or otherwise look up or read the information related to the account identified by the request.

[0069] A determination 820 can be made as to whether the electronic device presenting the payment credential, i.e., the device identified in the request, is one of the electronic devices authorized to use the electronic payment credential. In response to determining the device is identified in the account information as an authorized device, the transaction can be authorized 825, for example by sending an authorization message to the requesting point-of-sale or other device. That is, the transaction can be authorized based at least in part on the information identifying the account. After authorizing 825 the transaction, a new unique device identifier can be generated 830, saved 835 in the information identifying the account, and transferred 840 to the electronic device for use in authorizing subsequent transactions. That is, the acquirer system or other authorizing system can provide a new unique identifier to the device for use in subsequent transactions.

[0070] FIG. 9 is a flowchart illustrating a process for implementing a unique dynamic identifier according to an alternative embodiment of the present invention. In this example, as in the previous examples, processing begins with receiving 905 a request to authorize the

transaction. As noted above, the acquirer or other authorizing system can maintain information identifying an account associated with the electronic payment credential. The information can also identify one or more electronic devices authorized to use the electronic payment credential. In this example, the information identifying the device can comprise a
5 unique dynamic identifier that comprises a combination of the account number and another random value. For example, the random value can comprise an elapsed time since a previous transaction, a time of occurrence of a last transaction, Greenwich Mean Time (GMT), or other value known and/or determinable to both the mobile device as the acquirer or other authorizing system. This random value can be combined with the account number in a
10 manner, i.e., via an algorithm, also known to both the mobile device and the acquirer or other authorizing system. Thus, upon receiving 905 the request to authorize the transaction, the acquirer or other authorizing system can determine the determine 910 the mobile device identifier based on the information receive in the request, i.e., by applying the known algorithm and the known or determinable random value.

15 [0071] The acquirer or other authorizing system can then query 915 the account information or otherwise look up or read the information related to the account identified by the request. A determination 920 can be made as to whether the electronic device presenting the payment credential, i.e., the device identified in the request, is one of the electronic devices authorized to use the electronic payment credential. In response to determining the
20 device is identified in the account information as an authorized device, the transaction can be authorized 925, for example by sending an authorization message to the requesting point-of-sale or other device. That is, the transaction can be authorized based at least in part on the information identifying the account.

[0072] In the foregoing description, for the purposes of illustration, methods were
25 described in a particular order. It should be appreciated that in alternate embodiments, the methods may be performed in a different order than that described. Additionally, the methods may contain additional or fewer steps than described above. It should also be appreciated that the methods described above may be performed by hardware components or may be embodied in sequences of machine-executable instructions, which may be used to
30 cause a machine, such as a general-purpose or special-purpose processor or logic circuits programmed with the instructions, to perform the methods. These machine-executable instructions may be stored on one or more machine readable mediums, such as CD-ROMs or

other type of optical disks, floppy diskettes, ROMs, RAMs, EPROMs, EEPROMs, magnetic or optical cards, flash memory, or other types of machine-readable mediums suitable for storing electronic instructions. Alternatively, the methods may be performed by a combination of hardware and software.

- 5 [0073] While illustrative and presently preferred embodiments of the invention have been described in detail herein, it is to be understood that the inventive concepts may be otherwise variously embodied and employed, and that the appended claims are intended to be construed to include such variations, except as limited by the prior art.

WHAT IS CLAIMED IS:

1 1. A method for authorizing a financial transaction utilizing an electronic
2 payment credential, the method comprising:

3 maintaining information identifying an account associated with the electronic
4 payment credential, the information identifying one or more electronic devices authorized to
5 use the electronic payment credential;

6 receiving a request to authorize the transaction, wherein the request includes
7 information identifying an electronic device presenting the payment credential; and

8 authorizing the transaction based at least in part on the information identifying
9 the account, wherein authorizing comprises determining the electronic device presenting the
10 payment credential is one of the electronic devices authorized to use the electronic payment
11 credential.

1 2. The method of claim 1, wherein the electronic payment credential
2 comprises a credential representing a pre-paid account.

1 3. The method of claim 2, wherein the pre-paid account comprises a gift
2 card account.

1 4. The method of claim 1, wherein the information identifying the
2 electronic device presenting the payment credential comprises a unique static identifier.

1 5. The method of claim 4, wherein the unique static identifier comprises a
2 device serial number.

1 6. The method of claim 1, wherein the information identifying the
2 electronic device presenting the payment credential comprises a unique dynamic identifier.

1 7. The method of claim 6, further comprising:
2 prior to receiving the request to authorize the transaction, generating a unique
3 device identifier;

4 saving the unique device identifier in the information identifying the account;
5 and

transferring the unique device identifier to the electronic device.

8. The method of claim 7, further comprising:

after authorizing the transaction, generating a new unique device identifier;

saving the new unique device identifier in the information identifying the

account; and

transferring the new unique device identifier to the electronic device for use in

authorizing subsequent transactions.

9. The method of claim 6, wherein the unique dynamic identifier

comprises a combination of an account number for the account and a random value.

10. The method of claim 9, wherein the random value comprises an

elapsed time since a previous transaction.

11. The method of claim 9, wherein the random value comprises a time of

occurrence of a last transaction.

12. The method of claim 9, wherein the random value comprises

Greenwich Mean Time (GMT).

13. A system for authorizing a financial transaction utilizing an electronic payment credential, the system comprising:

a mobile electronic device adapted to maintain the electronic payment

credential and initiate the financial transaction utilizing the electronic payment credential;

and

an acquirer system adapted to maintain information identifying an account

associated with the electronic payment credential, the information identifying one or more

electronic devices authorized to use the electronic payment credential, receive a request to

authorize the transaction, wherein the request includes information identifying the mobile

electronic device initiating the financial transaction utilizing the electronic payment

credential, and authorize the transaction based at least in part on the information identifying

the account, wherein authorizing comprises determining the mobile electronic device

13 initiating the transaction is one of the electronic devices authorized to use the electronic
14 payment credential.

1 14. The system of claim 13, further comprising a point-of-sale device
2 communicatively coupled with the acquirer system, wherein the mobile electronic device
3 initiates the financial transaction by presenting the payment credential to the point-of-sale
4 device and wherein the acquirer system receives the request to authorize the financial
5 transaction from the point-of-sale device.

1 15. The system of claim 13, wherein the electronic payment credential
2 comprises a credential representing a pre-paid account.

1 16. The system of claim 15, wherein the pre-paid account comprises a gift
2 card account.

1 17. The system of claim 13, wherein the information identifying the
2 electronic device presenting the payment credential comprises a unique static identifier.

1 18. The system of claim 17, wherein the unique static identifier comprises
2 a device serial number for the mobile electronic device.

1 19. The system of claim 13, wherein the information identifying the
2 electronic device presenting the payment credential comprises a unique dynamic identifier.

1 20. The system of claim 19, wherein the acquirer system is further adapted
2 to:

3 prior to receiving the request to authorize the transaction, generate a unique
4 device identifier;

5 save the unique device identifier in the information identifying the account;

6 and

7 transfer the unique device identifier to the electronic device.

1 21. The system of claim 20, wherein the acquirer system is further adapted
2 to:

3 after authorizing the transaction, generate a new unique device identifier;

4 save the new unique device identifier in the information identifying the
5 account; and
6 transfer the new unique device identifier to the electronic device for use in
7 authorizing subsequent transactions.

1 22. The system of claim 19, wherein the unique dynamic identifier
2 comprises a combination of an account number for the account and a random value.

1 23. The system of claim 22, wherein the random value comprises an
2 elapsed time since a previous transaction.

1 24. The system of claim 22, wherein the random value comprises a time of
2 occurrence of a last transaction.

1 25. The system of claim 22, wherein the random value comprises
2 Greenwich Mean Time (GMT).

1 26. A machine-readable medium having stored thereon a series of
2 instructions which, when executed by a processor, cause the processor to authorize a financial
3 transaction utilizing an electronic payment credential by:

4 maintaining information identifying an account associated with the electronic
5 payment credential, the information identifying one or more electronic devices authorized to
6 use the electronic payment credential;

7 receiving a request to authorize the transaction, wherein the request includes
8 information identifying an electronic device presenting the payment credential; and

9 authorizing the transaction based at least in part on the information identifying
10 the account, wherein authorizing comprises determining the electronic device presenting the
11 payment credential is one of the electronic devices authorized to use the electronic payment
12 credential.

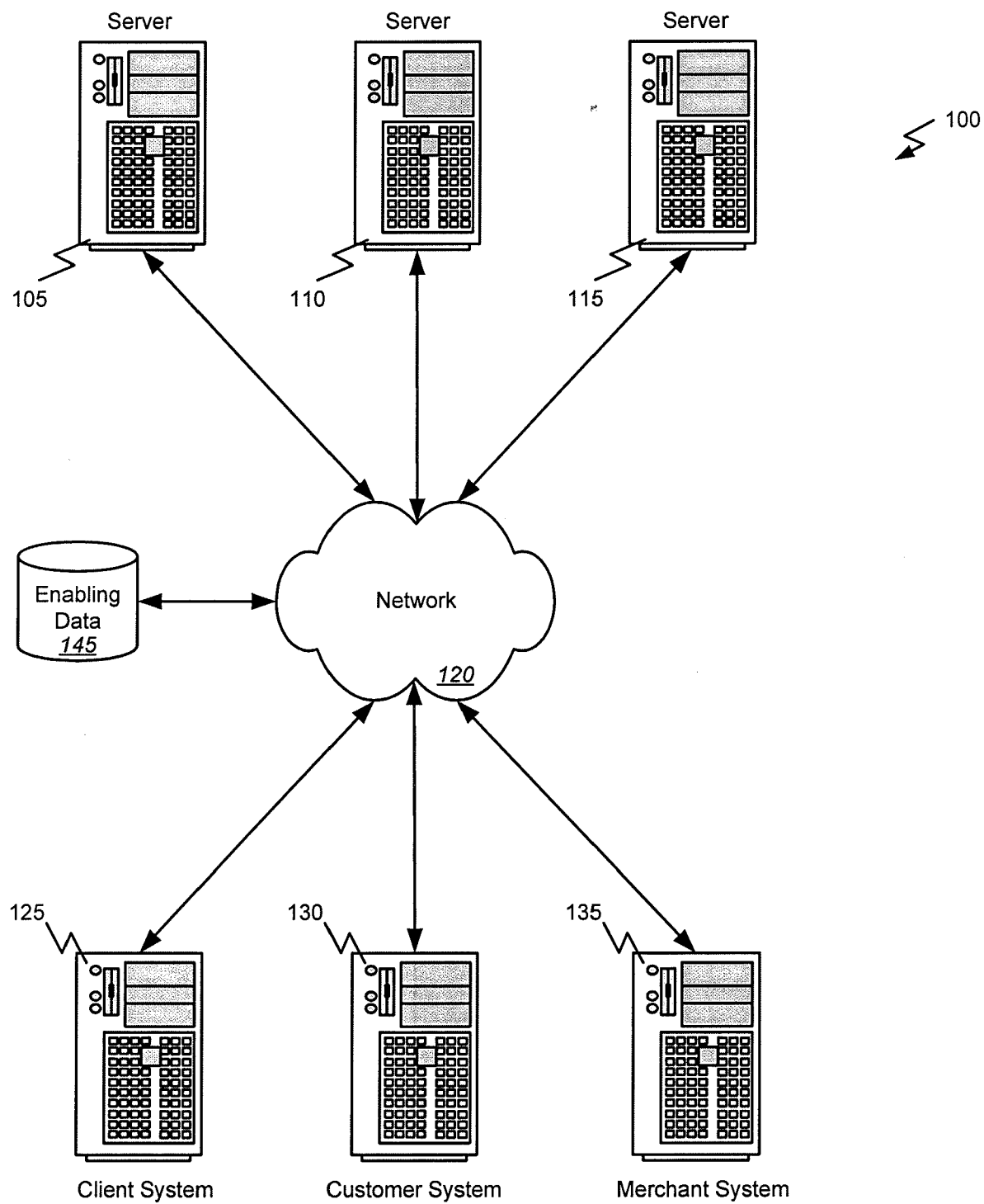
1 27. The machine-readable medium of claim 26, wherein the electronic
2 payment credential comprises a credential representing a pre-paid account.

1 28. The machine-readable medium of claim 27, wherein the pre-paid
2 account comprises a gift card account.

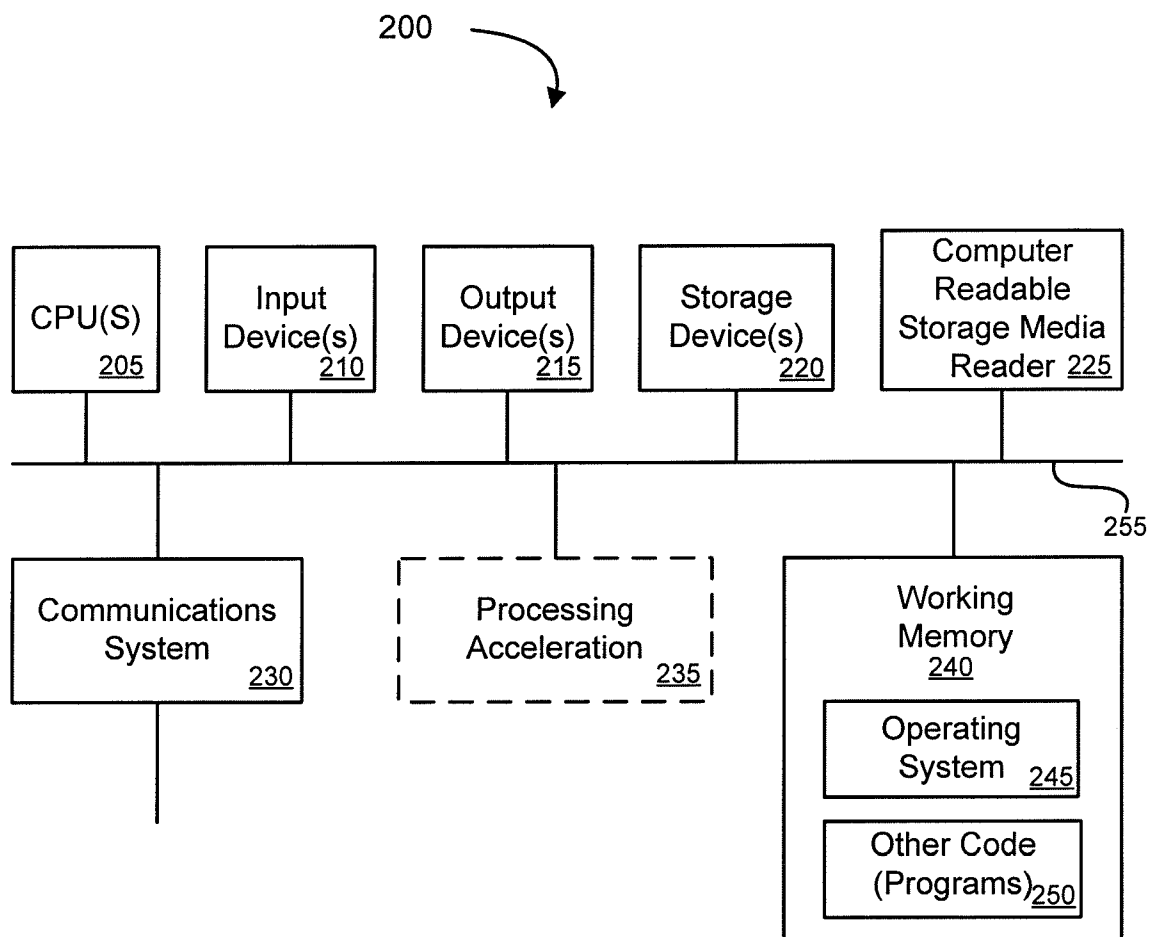
1 29. The machine-readable medium of claim 26, wherein the information
2 identifying the electronic device presenting the payment credential comprises a unique static
3 identifier.

1 30. The machine-readable medium of claim 1, wherein the information
2 identifying the electronic device presenting the payment credential comprises a unique
3 dynamic identifier.

1/9

**FIG. 1**

2/9

**FIG. 2**

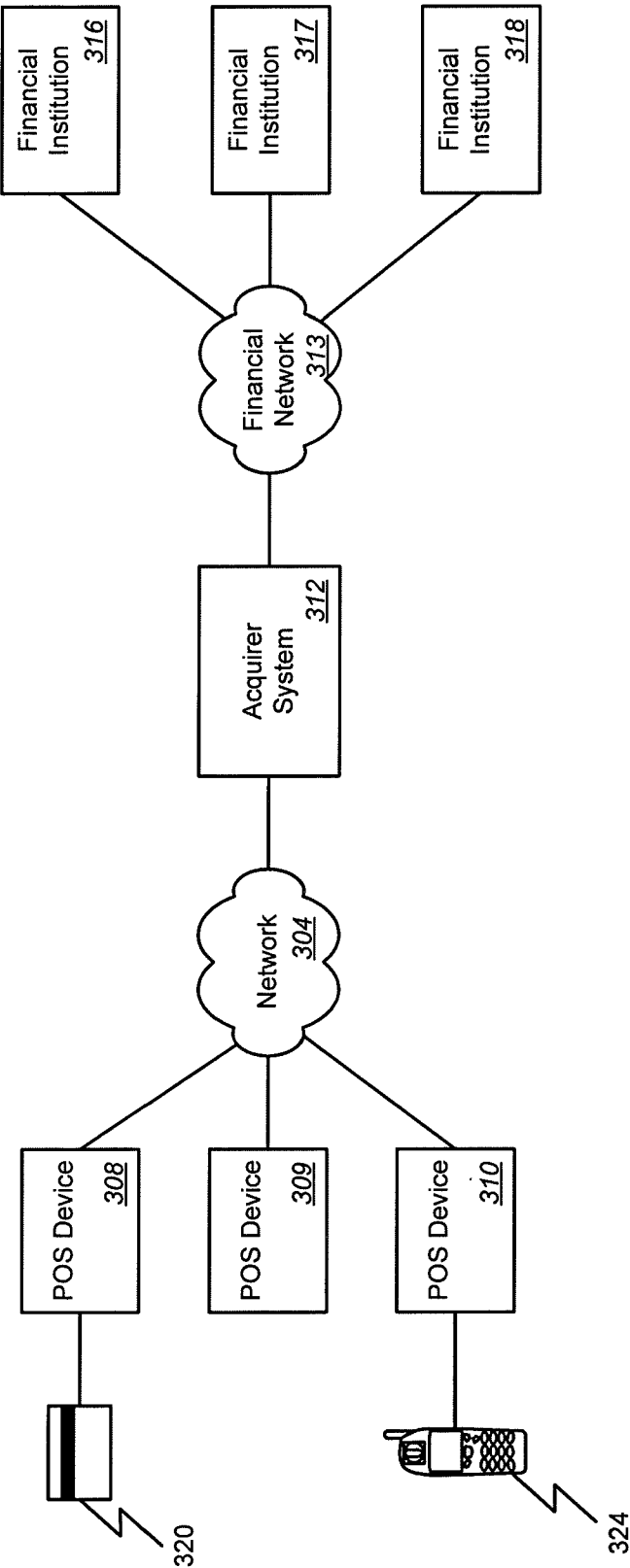


FIG. 3

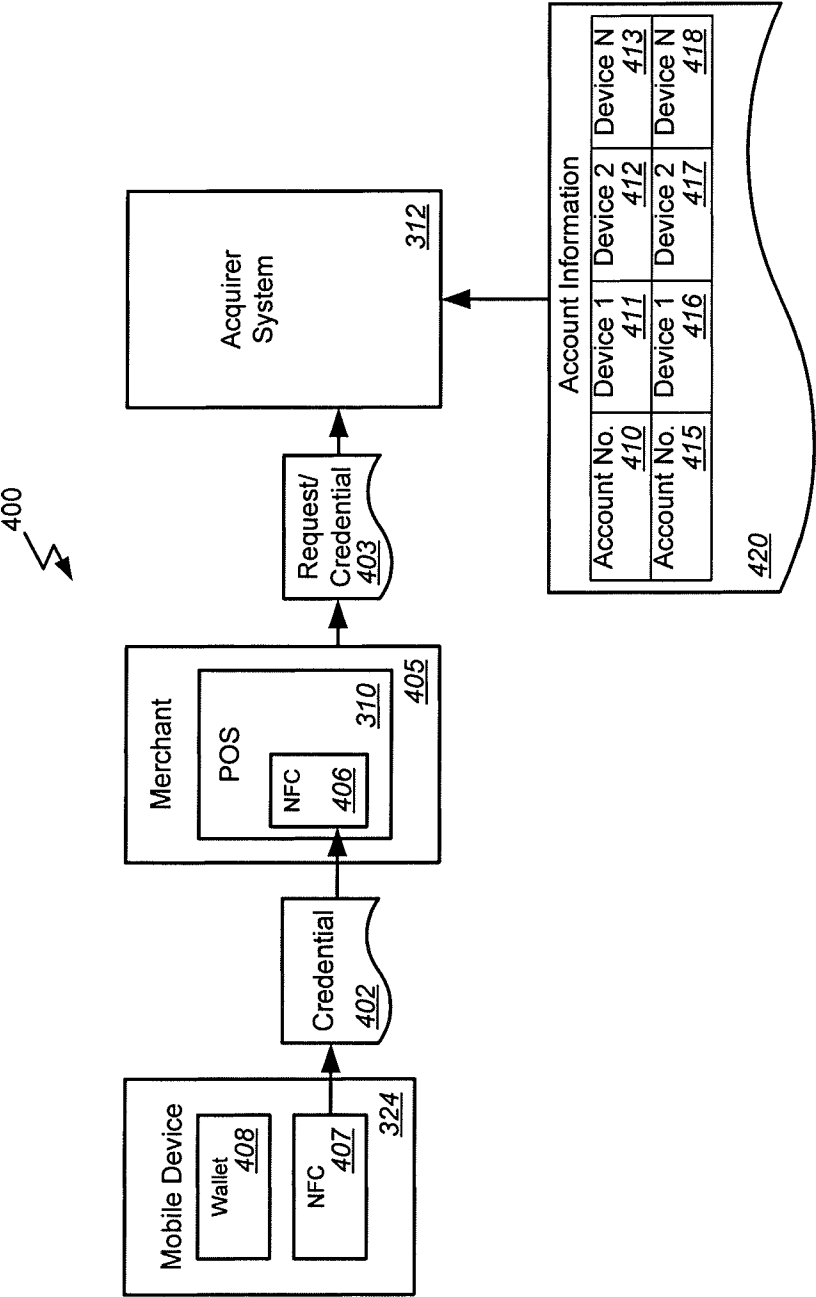
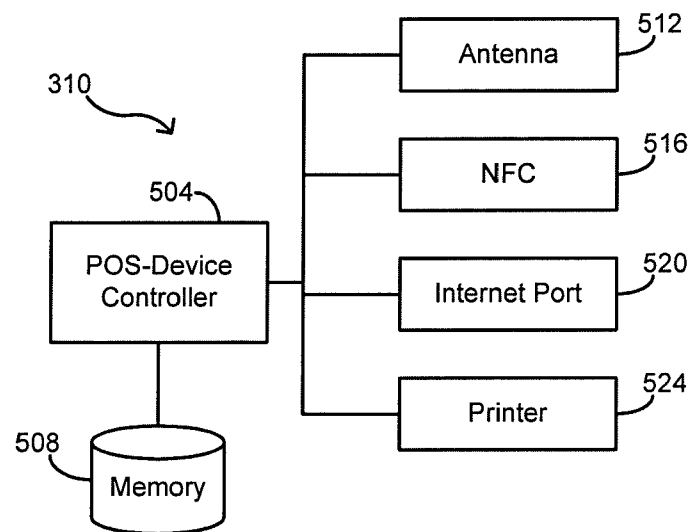
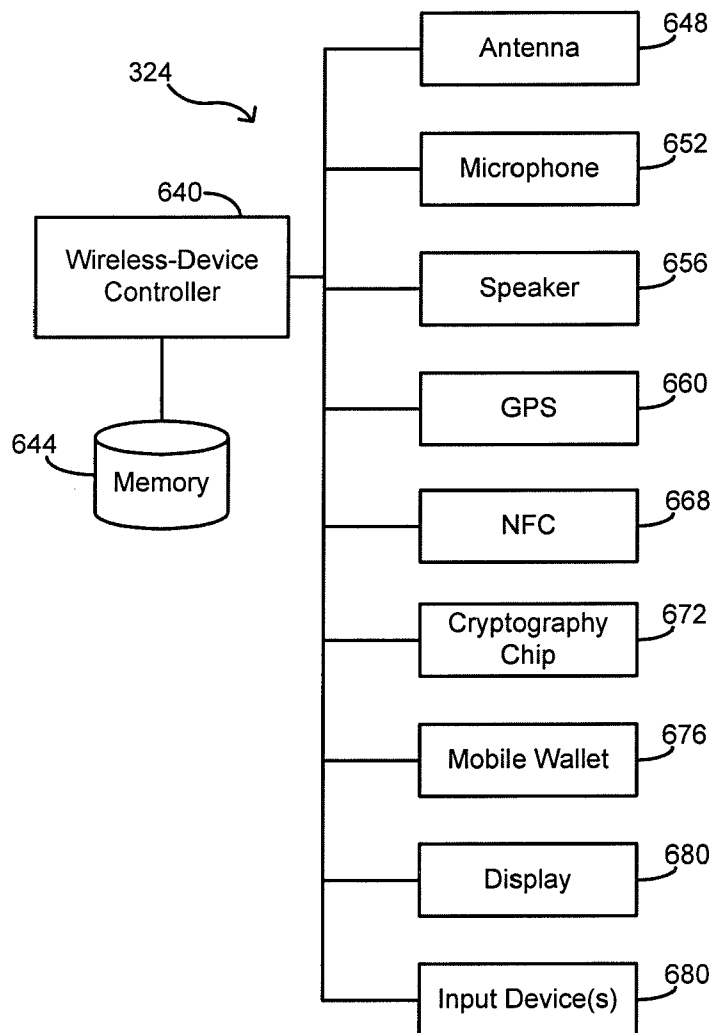


FIG. 4

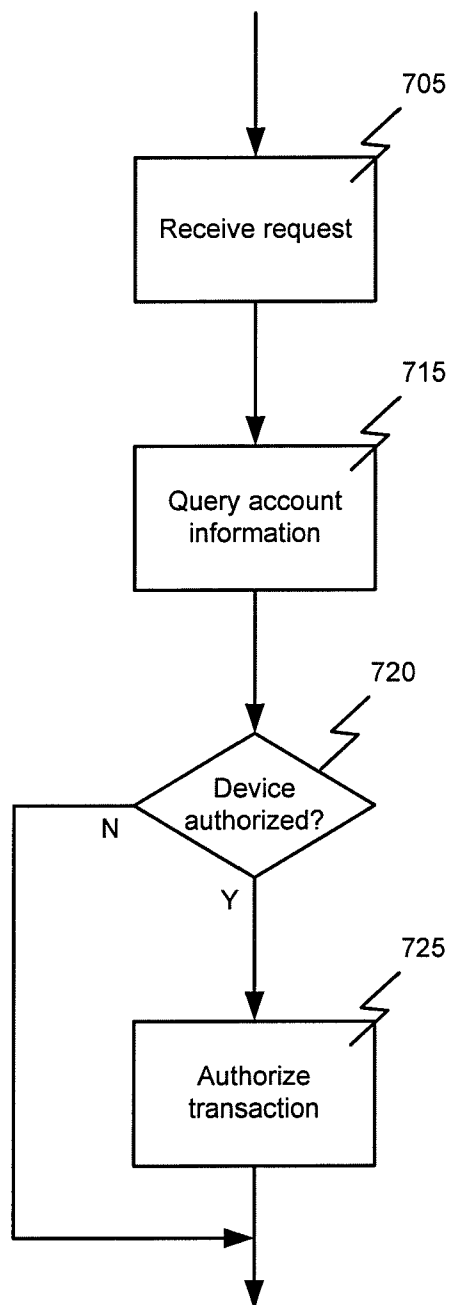
5/9

**FIG. 5**

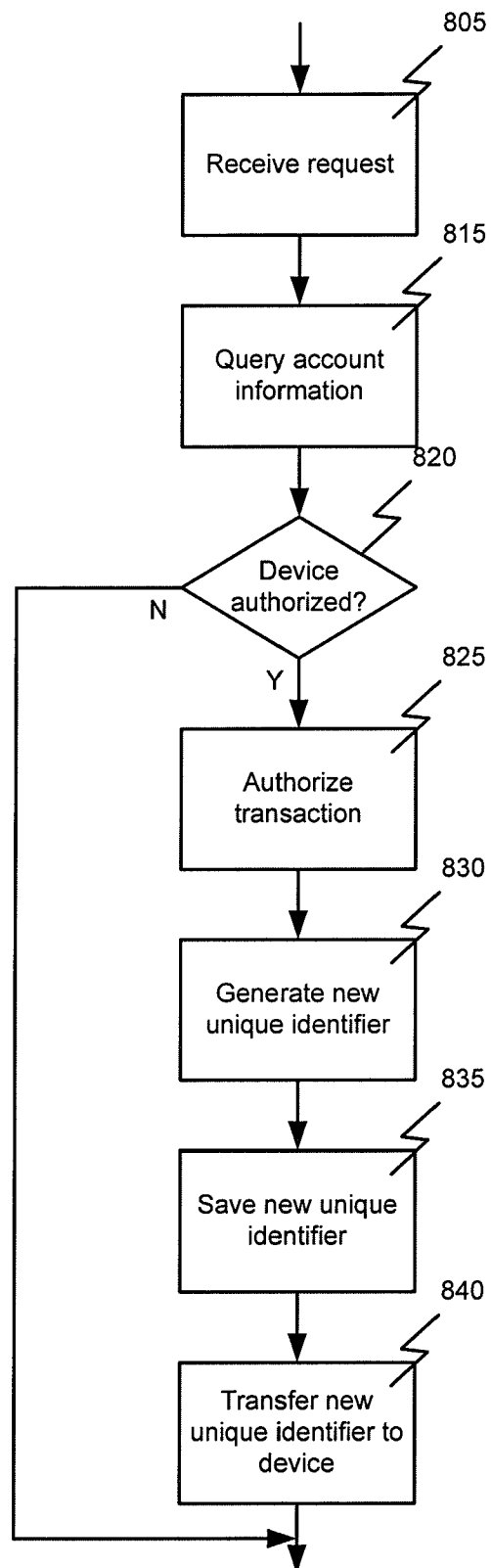
6/9

**FIG. 6**

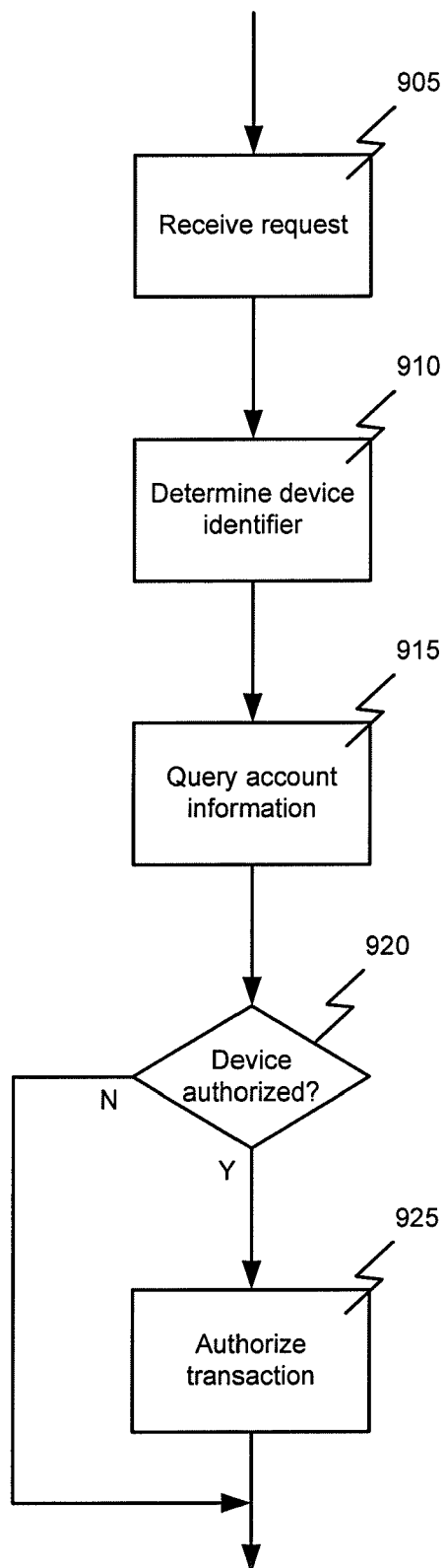
7/9

**FIG. 7**

8/9

**FIG. 8**

9/9

**FIG. 9**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US 09/33789

A. CLASSIFICATION OF SUBJECT MATTER

IPC(8) - H04L 9/00 (2009..01)

USPC - 705/65

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC(9) - H04L 9/00 (2009..01)

USPC - 705/65

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 705/64-77, 35, 39 (text search - see search terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

PubWEST(USPT,PGPB,EPAB,JPAB); USPTO; Google Patent/Scholar

search terms: mobile, wireless, contactless, payment, transaction, authorize, authenticate, identifier, key,dynamic, credential, mutating, pre-paid, gift card, random, time, GMT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2008/0010215 A1 (Rackley III, et al) 10 January 2008 (10.01.2008), FIG. 2, 10, abstract, para [0028]-[0313]	1-4, 13-17, 26-29
-----		5-12, 18-25, 30
Y		
Y	US 2007/0011099 A1 (Sheehan) 11 January 2007 (11.01.2007), para [0066]	5, 18
Y	US2007/0067833 A1 (Colnot) 22 March 2007 (22.03.2007), para [0033]-[0070]	6-12, 19-25, 30
Y	US 2003/0080183 A1 (Rajasekaran, et al) 01 May 2003 (01.05.2003), FIG. 6, claim 8, para [0039]	9-11, 22-24
Y	US 2003/0198348 A1 ((Mont, et al) 23 October 2003 (23.10.2003), para [0034]	12, 25

☐ Further documents are listed in the continuation of Box C.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

14 March 2009 (14.03.2009)

Date of mailing of the international search report

27 MAR 2009

Name and mailing address of the ISA/US

Mail Stop PCT, Attn: ISA/US, Commissioner for Patents

P.O. Box 1450, Alexandria, Virginia 22313-1450

Facsimile No. 571-273-3201

Authorized officer:

Lee W. Young

PCT Helpdesk: 571-272-4300

PCT OSP: 571-272-7774