(12) STANDARD PATENT (11) Application No. **AU 2009302485 C1**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Systems, methods, and computer readable media for payment and non-payment virtual card transfer between mobile devices

(51) International Patent Classification(s)
G06Q 20/00 (2012.01) ***H04W 4/00*** (2009.01)

(21) Application No: **2009302485** (22) Date of Filing: **2009.10.06**

(87) WIPO No: **WO10/042560**

(30) Priority Data

(31) Number	(32) Date	(33) Country
61/103,083	**2008.10.06**	**US**

(43) Publication Date: **2010.04.15**
(44) Accepted Journal Date: **2015.06.11**
(44) Amended Journal Date: **2015.10.22**

(71) Applicant(s)
MASTERCARD INTERNATIONAL, INC.

(72) Inventor(s)
Kumar, Pradeep;Khan, Mohammad

(74) Agent / Attorney
Griffith Hack, GPO Box 1285, Melbourne, VIC, 3001

(56) Related Art
US 2007/0255662 A1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2010 (15.04.2010)

PCT

(10) International Publication Number
WO 2010/042560 A3

(51) International Patent Classification:
G06Q 20/00 (2006.01) *H04W 4/00* (2009.01)

(21) International Application Number:
PCT/US2009/059752

(22) International Filing Date:
6 October 2009 (06.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/103,083 6 October 2008 (06.10.2008) US

(71) Applicant *(for all designated States except US)*: **VIVOTECH, INC.** [US/US]; 451 El Camino Real, 2nd Floor, Santa Clara, CA 95050 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KUMAR, Pradeep** [IN/US]; 4037 Oroville Court, Fremont, CA 94555 (US). **KHAN, Mohammad** [US/US]; 2238 Bentley Ridge Rd, San Jose, CA 95138 (US).

(74) Agent: **HUNT, Gregory, A.**; Jenkins, Wilson, Taylor & Hunt, P.A., Suite 1200, University Tower, 3100 Tower Boulevard, Durham, NC 27707 (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, CL, 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, PE, 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, SM, 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))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(88) Date of publication of the international search report:
8 July 2010

(54) Title: SYSTEMS, METHODS, AND COMPUTER READABLE MEDIA FOR PAYMENT AND NON-PAYMENT VIRTUAL CARD TRANSFER BETWEEN MOBILE DEVICES

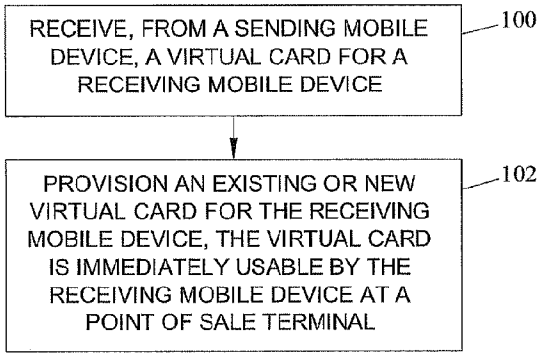

FIG. 1

(57) Abstract: The subject matter described herein includes methods, systems, and computer readable media for virtual card transfer between near field communications (NFC)-enabled mobile devices. According to one aspect, a method for over-the-air (OTA) virtual card transfer between NFC-enabled mobile devices is disclosed. The method includes receiving, at an OTA provisioning server, a virtual card, from a sending mobile device, that is intended for a receiving mobile device. The virtual card is provisioned, over the air, to the receiving mobile device, where the virtual card is immediately presentable by the receiving mobile device at a point of sale terminal.

WO 2010/042560 A3

SYSTEMS, METHODS, AND COMPUTER READABLE MEDIA FOR PAYMENT AND NON-PAYMENT VIRTUAL CARD TRANSFER BETWEEN MOBILE DEVICES

PRIORITY CLAIM

This application claims the benefit of U.S. Provisional Patent Application Serial No. 61/103,083, filed October 6, 2008; the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to virtual card transfer. More particularly, the subject matter described herein relates to payment and non-payment virtual card transfer between mobile devices.

BACKGROUND

At present, no method or process has been defined for virtual card transfer between NFC-enabled mobile devices that includes both monetary and non-monetary values such as debit, credit, rewards or loyalty points, coupons, business or personal information. Instead, various methods exist for transferring money between individuals that include transferring monetary amounts between various types of bank or credit accounts associated each individual.

Accordingly, there exists a need for a system, method, and computer product for virtual card transfer between NFC-enabled mobile devices.

SUMMARY

The subject matter described herein includes methods, systems, and computer readable media for virtual card transfer between NFC-enabled mobile devices. According to one aspect, a method for over-the-air (OTA) virtual card transfer between NFC-enabled mobile devices is disclosed. The method includes receiving, at an OTA provisioning server, a virtual card from a sending mobile device intended for a receiving mobile device. The virtual card is provisioned to the receiving mobile device, wherein the virtual card is immediately presentable by the receiving mobile device at a point of sale terminal, wherein the virtual card includes at least one of an electronic credit card, an electronic debit card, an electronic prepaid card, an electronic loyalty card, an electronic rewards card, or an electronic coupon.

In one embodiment, the method comprises receiving identification information associated with at least one of the sending mobile device and the receiving mobile device, wherein the identification information includes at least one of a phone number, a name, and an address.

Receiving a virtual card may include communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

For example, communicating over an over-the-air communications network may include communicating over one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network.

For example, over an IP-based network may include communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

In an embodiment, receiving a virtual card includes receiving an electronic, monetary deposit using at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

In an embodiment, provisioning a virtual card includes communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

For example, provisioning a virtual card may include provisioning a virtual card using at least one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network.

For example, communicating over an IP-based network may include communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

In another embodiment, provisioning a virtual card includes provisioning an electronic, monetary account using at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

Provisioning the virtual card may include initiating one of an open loop or a closed loop account.

Provisioning the virtual card may include transmitting a control short message service (cSMS) message to the receiving mobile device, the cSMS message being configured to access a wallet application associated with the receiving mobile device.

According to another aspect, the subject matter includes an over-the-air

(OTA) server for providing virtual card transfer between near field communications (NFC)-enabled mobile devices. The OTA provisioning server includes a receiving module for receiving, from a sending mobile device, a virtual card for a receiving mobile device. An account module of the server provisions the virtual card to the receiving mobile device, where the virtual card is immediately usable by the receiving mobile device at a point of sale terminal, wherein the OTA provisioning server is implemented by at least one computer having associated hardware, and the virtual card includes at least one of an electronic credit card, an electronic debit card, an electronic prepaid card, an electronic loyalty card, an electronic rewards card, or an electronic coupon.
In an embodiment, the receiving module receives identification information associated with at least one of the sending mobile device and the receiving mobile device, wherein the identification information includes at least one of a phone number, a name, and an address.

In another embodiment, the receiving module receives an electronic, monetary deposit over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

For example, the receiving module may communicate over an over-the-air communications network includes communicating over one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network.

For example, the receiving module may communicate over an IP-based network includes communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

In an embodiment, the receiving module receives a virtual card via at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

In a certain embodiment, the account module provisions the virtual card by communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

As used herein, the term “mobile device,” “NFC enabled mobile device,” “smart phone,” and “mobile handset” refer to any mobile device that is enabled with embedded or add-on capability, a secure element (e.g., a cryptographically protected smart chip), a radio frequency communications interface (e.g., contactless or NFC), and an antenna. The mobile device may comprise a mobile phone with embedded NFC support circuitry/software, which enables a user to wirelessly communicate with a contactless and/or wireless device reader.

Similarly, an NFC enabled device may include external memory-based or processor-based circuitry/software which enables a user to wirelessly communicate with contactless and/or wireless device reader. The secure element may be embedded in the mobile device, located in a SIM/USIM module, an add-on device (e.g., MicroSD card), SIM card, or processor card), or any other plug in device. The plug in device may come with antenna or utilize inbuilt phone antenna.

As used herein, the term "wallet application" refers to a software application including computer executable instructions stored in a computer readable medium, such as random access memory (RAM), flash memory or external memory that may be executed by a processor in a mobile device, where the wallet application stores information associated with one or more virtual cards. The wallet application runs on NFC-enabled mobile phones, enabling multiple payment-related and non-payment related applications managing secure data and allowing secure contactless payment. The wallet application provides the interface for provisioning data to the mobile device, as well as transmitting payment and non-payment related card or coupon information directly to POS terminals equipped with a contactless/wireless reader. A wallet application may manage multiple virtual cards stored on a mobile device. The wallet application may also be configured to ensure end-to-end protection of virtual card data and payment and non-payment related applications with its interface for OTA provisioning as well as its management of the mobile device's secure element. The secure element may include any type of hardware or combination of hardware and software that utilizes encryption or similar means for securing designated data within a mobile device.

As used herein, the term "Acceptance and issuance server" refers to a software application including computer executable instructions stored in a computer readable medium, such as random access memory (RAM) or flash memory, that may be executed by a processor in a point of sale device and/or general purpose computer system, where the acceptance and issuance server is a back-end system that indirectly supports front-end services. While front-end services are services (e.g., applications, devices, etc.) that users interact with directly and, therefore, are often located closer to a required resource and/or have the capability to communicate with the required resource (e.g., communicate via NFC with a customer's mobile device), a back-end application may interact directly with the front-end or, perhaps more typically, is a program called from an intermediate program that mediates front-end and back-end activities in order to support the front end. The acceptance and issuance server is used for authorization of card accounts, payment and non-payment card authorization, ACH processing, account validation, transaction amount processing, and loyalty, coupon or promotion processing by utilizing the

contactless interface command to read account information from handset by sending the command over the air.

As used herein, the term "OTA infrastructure software" refers to software including computer executable instructions stored in a computer readable medium, such as random access memory (RAM) or flash memory, that may be executed by a processor in an OTA provisioning server or similar computing platform, where the OTA infrastructure software enables over the air provisioning of virtual cards to wallet applications.

As used herein, the term "card" refers to a physical card, typically a magnetic stripe card, that may be drawn on an associated payment or non-payment card account. Because the person creating or issuing the card must transfer the information associated with the card, that information is immediately available to the recipient/owner/user of the card subject to various restrictions (See closed loop and open loop cards below).

As used herein, the term "virtual card account" refers to an account associated with a virtual card.

As used herein, the term "virtual card" refers to an electronic, non-physical representation of a card. A virtual card may be with or without electronic value. Virtual cards may represent credit cards, debit cards, prepaid cards, gift cards, loyalty cards, rewards card, coupon or promotion, business cards, health cards, membership cards, and other similar representations of payment and non-payment cards.

As used herein, the term "ACH" refers to Automated Clearing House Inc., a full service payment processing company offering ecommerce solutions for businesses. The ACH Network is a nationwide batch-oriented electronic funds transfer system governed by the National ACH Association (NACHA) which provides for the interbank clearing of electronic payments for participating depository financial institutions. The Federal Reserve and Electronic Payments Network act as ACH Operators, central clearing facilities through which financial institutions transmit or receive ACH entries. Exemplary types of ACH payments include: direct payroll deposit, Social Security and other government benefits, tax refunds, direct payment of consumer bills (e.g., mortgages, loans, utility bills and insurance premiums), business-to-business payments, E-checks, E-commerce payments, and federal, state and local tax payments.

As used herein, the term "value" refers to the worth of an asset, business entity, good, service, liability, or obligation. Value can be expressed in monetary terms (e.g., dollars) or in non-monetary terms. For example, a value may include an amount, (loyalty) points, rewards, coupons, personal information, or promotion values.

As used herein, the term "presentable" may refer to the characteristic of capable of being given, displayed, or offered. For example, a mobile device may

be presentable to a POS terminal in order to communicate via NFC in order to retrieve information from the mobile device. The term presentable intended to have a meaning broader in scope than associated with being solely for the purpose of conducting a payment transaction, as the information presented may include anything of value associated with a virtual card. As mentioned above, this may include non-monetary information such as coupons, loyalty points, and personal information.

The subject matter described herein for virtual card between mobile devices may be implemented using a computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps of the aforementioned method (see above). Exemplary computer readable media suitable for implementing the subject matter described herein includes disk memory devices, programmable logic devices, and application specific integrated circuits. In one implementation, the computer readable medium may include a memory accessible by a processor. The memory may include instructions executable by the processor for implementing any of the methods for virtual card transfer between mobile devices described herein. In addition, a computer readable medium that implements the subject matter described herein may be distributed across multiple physical devices and/or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

In order that the invention may be more clearly ascertained, embodiments of the subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a flowchart illustrating exemplary steps for performing a virtual card transfer between mobile devices using a virtual card according to an embodiment of the subject matter described herein;

Figure 2 is a diagram illustrating an exemplary system for transferring a virtual card between a sender and a receiver according to an embodiment of the subject matter described herein;

Figure 3 is a flowchart illustrating exemplary steps for transferring a virtual card between a sender and a receiver according to an embodiment of the subject matter described herein;

Figure 4 is a diagram illustrating an exemplary system for authorizing a virtual card from an existing account of the sender according to an embodiment of the subject matter described herein;

Figure 5 is a flowchart illustrating exemplary steps for authorizing a virtual card from an existing account of the sender according to an embodiment of the subject matter described herein;

Figure 6 is a functional block diagram of exemplary components of a mobile device suitable for performing a virtual card transfer between mobile devices according to an embodiment of the subject matter described herein; and

Figure 7 is a functional block diagram illustrating exemplary internal components of a NFC enabled mobile device suitable for performing a virtual card transfer between mobile devices according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION OF THE INVENTION

In accordance with the subject matter disclosed herein, systems, methods, and computer readable media are provided for transferring a virtual card between NFC-enabled mobile devices.

Figure 1 is a flowchart illustrating exemplary steps for performing a virtual card transfer between mobile devices according to an embodiment of the subject matter described herein. Referring to Figure 1, in step **100**, a virtual card is received from a sending mobile device for a receiving mobile device.

In step **102**, a new or existing virtual card is provisioned for the receiving mobile device, where the virtual card is immediately usable by the receiving mobile device at a point of sale terminal.

Figure 2 is a diagram illustrating an exemplary system for transferring virtual card between a sender and a receiver according to an embodiment of the subject matter described herein. Referring to Figure 2, the system may include first mobile device **200** (hereinafter, "sender"), over the air (OTA provisioning server **202**, and second mobile device **204** (hereinafter, "receiver"). Mobile devices **200** and **204** may include near field communications (NFC)-enabled or non-NFC enabled mobile devices.

As described above, an NFC enabled mobile device may comprise a mobile phone with embedded NFC support circuitry/software, which enables a user to wirelessly communicate with wireless device reader. Similarly, an NFC enabled device may include external memory-based or processor-based circuitry/software which enables a user to wirelessly communicate with contactless/wireless device reader. Similarly, an NFC enabled mobile device

may include universal subscriber identification module (USIM)/USIM integrated circuit card (UICC) NFC support circuitry/software to wirelessly communicate with the contactless/wireless device reader. For example, a POS terminal may include a contactless/wireless device reader capable of communicating with NFC-enabled mobile devices, contactless/wireless smart cards, or other contactless payment devices via a short range electromagnetic field. One type of communications channel that may be used between a device capable of supporting a virtual/soft card and a wireless device reader for payment/coupon transactions is near field communications (NFC). Near field communications typically occur at a distance of within about one wavelength of the communications frequency being used between the mobile device and the wireless device reader. An example of a contactless communications protocol that may be used in communications between a device capable of supporting a softcard and a wireless device reader is an ISO 14443 interface.

Non-NFC enabled mobile devices may include a cellular phone or other mobile device that does not include embedded NFC, external memory based NFC or USIM/UICC NFC support circuitry/software or any other means to wirelessly communicate with a POS terminal.

Additionally, mobile devices may be capable of data communications with remote entities via an OTA provisioning process. For example, devices with wireless communications capabilities may implement HTTP over TCP/IP or UDP, SMS PP, CAT_TP over-the-air interface for communicating with remote entities. The over the air interface protocol used by a device with wireless communications capabilities may vary with the device. Examples of air interface protocols that may be used include GSM, GPRS, CDMA, EDGE, 3G, Bluetooth, WIFI, WIMAX, LAN, Ethernet, etc.

Returning to Figure 2, sender **200** may transmit a request to transfer a virtual card to OTA provisioning server **202**. For example, request **206** may request transfer of a virtual card having some value (e.g., $20) to receiver **204**. In response to receiving request **206**, OTA provisioning server **202** may provision a new virtual card for receiver **204**. For example, OTA provisioning server **202** may provision $20 virtual card via message(s) **208**. Upon receiving virtual card **208**, receiver **204** may immediately use the virtual card, either to spend at a

corresponding open or closed loop merchant POS terminal, or for transferring to an existing account associated with receiver **204**.

Figure 3 is a flowchart illustrating exemplary steps for transferring a virtual card between a sender and a receiver according to an embodiment of the subject matter described herein. Referring to Figure 3, at step **300** the sender opens the wallet application on his or her mobile device. For example, the sender may utilize an interface on the mobile device (e.g., keypad or touch screen) for selecting the wallet application from among a selection of available programs and interacting with the wallet application in order to provide various information described below.

In step **302**, the sender may select an existing account used for funding the value transfer (i.e., the source). For example, sender **200** may enter or otherwise select track I and/or II data, routing number, bank account number, or ACH identifier associated with an account sender **200** wishes to use.

In step **304**, the sender may provide identification information about him or herself. For example, sender **200** may provide his or her name, address, phone number, email address, and/or password in order to uniquely identify him or herself as the sender of the virtual card.

In step **306**, the sender may provide information regarding the desired virtual card characteristics. For example, sender **200** may enter an amount to be transferred (e.g., $20) and whether the virtual card is closed loop or open loop. This may include specifying that the virtual card may only be used at Target™ stores (i.e., closed loop) or may be used anywhere Visa™ is accepted (i.e., open loop).

In step **308**, the sender may provide identification information about the intended recipient of the funds (i.e., the receiver). For example, sender **200** may provide the name, address, phone number, email address, or other information (e.g., a challenge question) that may be used to uniquely identify receiver **204** as the intended recipient of the virtual card.

In step **310**, the sender may confirm the virtual card authorization. For example, sender **200** may optionally be presented with transaction fees or other final details about the transaction, and sender **200** may accept these final conditions and initiate the value transfer.

In step **312**, OTA software application may create a new virtual card account with the requested information designating the receiver as the intended recipient using the identification information provided by the sender in step **304**. For example, the virtual card account may be either a closed loop or an open loop virtual card account. An open loop virtual card account is a virtual card account that is acceptable at multiple vendors that have a merchant agreement with the virtual card account issuer. Typically, open loop cards are branded with the identity of the card issuer, where the card issuer is a large, multi-national banking or credit institution. Examples of open loop cards include prepaid or gift cards branded with/issued by VISA™, MasterCard™, AMEX™, or Discover™ and are acceptable at any location maintaining a merchant account with one or more of those companies. A closed loop virtual card account is a virtual card account that is only accepted at the store or retail locations of the card issuer. Examples of closed loop virtual cards include prepaid / gift cards issued by Belk's™ Department store, BestBuy™, or HomeDepot™, which may only be redeemed at each of these locations, respectively.

For example, a loyalty card account may be a closed loop loyalty card account such as a Safeway™ loyalty account, Macy's™ loyalty account, or a United Loyalty™ account. Loyalty reward data may include loyalty points that are accumulated via purchases a customer makes with the associated merchant. Various rewards such as discounts, announcements, early offers for sale and the like may be exchanged for loyalty points or provided to customers with a threshold number of loyalty points in their account. For example, a coupon or promotion for a specific retailer or merchant and/or for a specific product may be an item of value that can be transferred electronically between mobile devices according to the subject matter described herein. Thus, sender **200** may have a coupon for $20 off of any TV for sale at BestBuy™ which may be transferred to receiver **204** such that receiver **204** may immediately redeem the coupon for a $20 discount on a TV purchase at a BestBuy™ location.

For example, OTA provisioning server **202** may send a control/binary SMS (cSMS) or bearer independent protocol (BIP) channel initiation or SMS point-to-point (PP) message to receiver **204**. For example, the request message may be embodied as a message requesting that OTA provisioning server **202**

issue a virtual card to the recipient mobile device number provided. Upon receiving the recipient data, OTA provisioning server **202** may be configured to determine if the recipient mobile device is NFC enabled. In one embodiment, OTA provisioning server **202** may access a database to obtain information relating to the type of mobile device (e.g., NFC enabled or otherwise) that is associated with the provided recipient number.

After receiving the mobile device type information (and virtual card information), OTA provisioning server **202** may deliver the virtual card to receiver **204**. The manner in which the virtual card may be sent depends if the recipient is an NFC enabled phone or non-NFC enabled phone. In the former case, OTA provisioning server **202** may be configured to deliver the virtual card. In one embodiment, the provisioning of a virtual card over the air interface may occur over wireless connection, for example, using HTTP and TCP protocols, SMS and CAT_TP using BIP protocol. A TCP socket may be created for the provisioning connection. The physical layer of the connection may utilize, CDMA, Bluetooth, GPRS, GSM, Wi-Fi, Wi-Max, Ethernet or LAN air interface protocols. Provisioning may occur over the Internet or over a corporate or other intranet or utilizing TCP/IP, SMS PP, CAT_TP, UDP. Provisioning may occur automatically by providing a provisioning application on a mobile device that establishes a connection with a provisioning configuration server (e.g., OTA provisioning server **202**) in response to being started or the provisioning configuration server may start the provisioning using control/binary SMS without using provisioning application on a mobile device.

Alternatively, if the receiver is a non-NFC enabled phone, then OTA provisioning server **202** may deliver the virtual card as an authorization code or a URL via an SMS message.

In the exemplary embodiment where the receiving mobile device is NFC enabled, OTA provisioning server **202** may sends a control SMS message or initiate a BIP channel using SMS PP or SMSM PP to NFC enabled mobile device **204**. In response, NFC enabled mobile device **204** may read the SMS control content, which may triggers a midlet application (e.g., a wallet client application) that initiates a downloading process to receive a virtual card from OTA provisioning server **202** or open BIP channel to receive a virtual card from

OAT provisioning server **202**. NFC enabled mobile device **204** (e.g., via the wallet client) may then reply to OTA provisioning server **202** with an acknowledgement message.

In step **314**, the receiver may then receive an indication of the virtual card provisioning and that the wallet application on the mobile device is accessed. Receiver **204** may also optionally receive a notification message from OTA infrastructure software indicating that a virtual card was available for provisioning. For example, this may include presenting receiver **204** with a message on his mobile device (e.g., "Happy Birthday John") that may indicate the reason for the money transfer.

In step **316**, the wallet application may ask the receiver to initiate the virtual card download process. For example, by clicking on a link associated with or included in the optional message, receiver **204** may access wallet application for conforming reception of the virtual card. In this way, receiver **204** may accept or deny virtual card transfers in the event that the virtual card is unsolicited (e.g., spam) or receiver **204** is not the correct intended receiver (e.g., delivery error such as transposed telephone number digits or typo in email address provided by sender **200**.)

In step **318**, the wallet application may initiate communication with the OTA infrastructure software. For example, the wallet application may request a secure communication channel with OTA provisioning server **202** that may include a communications handshake procedure between the wallet application and OTA provisioning server **202** that may conclude with the transmission of an acknowledgement message by the wallet application to OTA provisioning server **202**. In response to receiving the acknowledgement message, OTA provisioning server **202** may establish a secure connection with NFC enabled mobile device **204** and provide identification data. In one embodiment, identification data includes data that is unique to the recipient of the virtual card. In an alternate embodiment, the present subject matter may forego establishing a secure connection and the virtual card may be transmitted over an unsecured connection and stored in the mobile device's general memory.

In step **318**, OTA software infrastructure may start the virtual card provisioning process to the wallet application. For example, OTA provisioning

server may send cSMS or initiate the BIP channel to receiver's handset to initiate the download process. Once wallet is initiated or BIP channel established, OTA provisioning server create a secure channel to provision the virtual value card with account identification with or without value, branding image, welcome message and other data.

In step **320**, the provisioning process may be completed and the virtual card may be successfully downloaded to a secure element within the receiver's mobile device. The downloaded virtual card will have the requested account information available for immediate use by the receiver. For example, after receiving a $20 closed loop Target™ virtual card, receiver **204** may present the card by placing his or her NFC enabled mobile device in proximity to a contactless/wireless reader associated with a POS terminal. The contactless/wireless reader may read information from the secure element on the mobile device and deduct the amount of the desired purchase from the virtual card. The virtual card may then be reused at a Target™ location for a future use.

After the download process is completed, the wallet client may display the virtual card. After the virtual card is stored in NFC enabled mobile device **204**, the recipient may decide to use the virtual card at an appropriate retail store or the like. For instance, after deciding to purchase a particular good at a store, the recipient may bring the merchandise to the checkout register station and be prompted by the cashier to provide a method of payment. The recipient may then use mobile device **204** to select the coupon virtual/soft card to be used in the payment transaction. For example, the recipient may interface mobile device **204** with a wireless device reader via NFC communication. In one embodiment, the virtual card transaction may also be coupled with a conventional payment transaction. For example, is the virtual card is sufficient to cover the selected good(s), no other method of payment would be required. Otherwise the customer may be prompted to provide additional payment for the outstanding balance.

If a second embodiment, the virtual card may be provided to a non-NFC enabled phone via one or more SMS messages. For example, mobile device **204** may receive an SMS message from OTA provisioning server **202** instead of

receiving an SMS control message. The received SMS message may include a virtual card code. In one embodiment, the virtual card code may be associated with a designated amount that may be provided to a cashier at POS terminal. In an alternate embodiment, the SMS message may instead include a URL that is linked to a barcode image.

After receiving the virtual card, the user of mobile device **204** may decide to use the virtual card at a retail store or the like. For example, after selecting goods for purchase, the user presents the merchandise at the checkout counter and may be prompted by the cashier to provide a method of payment. The user may then provide the virtual card code to the cashier. The cashier may then enter the virtual card code in the POS terminal. In one embodiment, the POS terminal may validate the virtual card code with a merchant server to ensure that the virtual card is still valid or alternatively, that the virtual card value is sufficient to cover the transaction. The merchant server may return an acknowledgement message if the coupon code is valid. It is also appreciated that the receiver may use the received funds either by transferring it to an existing account associated with the receiver, or may re-transfer the money to a third person as a second virtual card. In the latter case, the receiver may become the sender for purposes of the second value transfer transaction, and a third party may become the receiver.

Figure 4 is a diagram illustrating an exemplary system for authorizing value from an existing account of the sender according to an embodiment of the subject matter described herein. Referring to Figure 4, wallet application **400** may be located on mobile device **200** and configured to communicate with contactless interface **402** which is associated with acceptance and issuance server **404**. Additionally, as will be described in greater detail below, acceptance and issuance server **404** may include a back-end server that may communicate electronically with one or more financial institutions **406**. In the exemplary message exchange shown, wallet application **400** may transmit request **408** for authorizing values for an existing account. In response to receiving request **408**, acceptance and issuance server **404** may return APDU command **410** requesting Track I and II (or similar) data from the secure element (not shown) securely. Wallet application **400** may provide track I and II data and a

transaction amount included in message(s) **412**. Lastly, after verification/authorization, acceptance and issuance server **404** may return a transaction approval or rejection message **414**.

Unlike a non-acceptance and issuance server system that requires integration with one or more terminals, acceptance and issuance server **404** may run on a general use computing platform, such as a personal computer. To process transactions, merchants may swipe a credit card through an attached credit card reader or accept contactless payment through an attached contactless payment reader.

Figure 5 is a flowchart illustrating exemplary steps for authorizing a virtual card of the sender. Referring to Figure 5, in step **500**, the wallet application may connect to Hosted point of sale (POS) in order to validate the virtual card information to be transferred.

In step **502**, the Acceptance and issuance server may send instructions to the wallet application to retrieve virtual card information. For example, Acceptance and issuance server **404** may send one or more application protocol data unit (APDU) commands **406** to wallet application **400** requesting Track I, Track II data, code for the virtual card account information. Alternatively, Acceptance and issuance server **404** may send one or more APDU commands **410** to wallet application **400** requesting a routing number, bank information, account number, or automated clearing house (ACH) network identifier.

In step **508**, the Acceptance and issuance server may use the information/credentials provided in steps **502-506** to request validation of the virtual card and the sender's identity.

If the transaction is approved, in step **510**, the acceptance and issuance server may complete the transaction and send a confirmation message to the sender's mobile device.

Figure 6 is a functional block diagram of exemplary components of a mobile device suitable for performing an electronic money transfer between mobile devices using a virtual card according to an embodiment of the subject matter described herein. Referring to Figure 6, OTA provisioning server **202** may include receiving module **600**, account module **602**, and transmitting module **604**. Receiving module **600** may be configured to receive, from a

sending mobile device, an electronic, monetary deposit for a predetermined amount intended for a receiving mobile device. Account module **602** may be configured to provision an electronic, monetary account in the predetermined amount. Transmitting module **604** may be configured to transmit the electronic, monetary deposit in the predetermined amount to the receiving mobile device, wherein the deposit is immediately usable by the receiving mobile device at a point of sale terminal.

Figure 7 is a functional block diagram illustrating exemplary internal components of a NFC enabled mobile device suitable for performing a virtual card transfer between mobile devices according to an embodiment of the subject matter described herein. Referring to Figure 7, mobile device **200/204** may include a baseband processor **700**, contactless chip **702**, integrated antenna **704**, secure element (external memory) **706**, integrated antenna **708**, secure element (integrated) **710**, USIM/SIM card **712**, secure element (within USIM/SIM card **712**) **714**, and phone antenna **716**. It is appreciated that the NFC components shown in Figure 7 may be embedded in circuitry within mobile handset **200/204**, integrated with SIM module, integrated with external memory, associated with phone memory, associated with external memory directly, or any other type for form factor which enables the handheld device to act as an NFC enabled handset. It is further appreciated that mobile device **200/204** may include various different form factors for secure element(s) **708**, **710**, and **714** without departing from the scope of the subject matter described herein. For example, secure element(s) **708**, **710**, and **714** may be present in combination or as a single instance (not shown).

Baseband processor (BP) **700** may include a processor that implements a wireless communications stack, such as the global system for mobile communications (GSM) stack. It may be appreciated that most smart phones, such as mobile device **200/204**, may contain two processors. The operating system (OS), user interface, and applications may run on an application processor (AP), such as an ARM-based CPU, while phone radio communications and control software may be run on BP **700**. The AP may communicate with BP **700** over a defined control link, such as a serial connection or general purpose input/output (GPIO) lines between BP **700** and

the AP. One reason for separating locating the radio functionality at BP **700** may be to protect highly timing dependent functions, such as radio control functions (e.g., signal modulation, encoding, radio frequency shifting, etc.) from less timing dependent functions. Another benefit of utilizing a BP includes that once the BP is designed and certified, it is assured to function properly regardless of application and OS changes (e.g., OS, application, and driver errors will not cause malfunctions in the phone radio).

Contactless chip **702** may be associated with integrated antenna **704** for communicating with contactless devices such as contactless payment readers or other NFC enabled mobile phones. Secure element **706** may be located in external memory (e.g., microSD or external memory) and may be device associated with integrated antenna **708**. Alternately, secure element **706** may utilize phone antenna **716**. Secure element **710** may be integrated with phone circuitry and utilize phone antenna **716** for communicating with external devices. USIM/SIM card **712** may include secure element **714** and may be integrated with phone antenna **716** for communicating wirelessly with external devices. This may include OTA provisioning server **202** via any suitable non-NFC communications protocol mentioned above. USIM **712** is an application for universal mobile telecommunications system (UMTS) mobile telephony running on a universal integrated circuit card (UICC) smart card inserted in mobile phone. It is appreciated that USIM **712** is a logical entity located on a physical UICC card, and not the physical card itself. For example, the UICC card may include physical hardware elements such as a processor, read only memory (ROM), random access memory (RAM), electronically erasable programmable read only memory (EEPROM), and input/output (I/O) circuits.

It will be understood that various details of the subject matter described herein may be changed without departing from the scope of the subject matter described herein. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation.

In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word “comprise” or variations such as “comprises” or “comprising” is used in an inclusive sense, that is, to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.

Further, any reference herein to prior art is not intended to imply that such prior art forms or formed a part of the common general knowledge in any country.

2009302485 14 May 2015

CLAIMS

1. A method for over-the-air (OTA) virtual card transfer between near field communications (NFC)-enabled mobile devices, the method comprising:
at an OTA provisioning server comprising at least one computer having associated hardware:

receiving, from a sending mobile device, a virtual card intended for a receiving mobile device; and

provisioning the virtual card to the receiving mobile device via an OTA interface, wherein the virtual card is immediately presentable by the receiving mobile device at a point of sale terminal;

wherein the virtual card includes at least one of an electronic credit card, an electronic debit card, an electronic prepaid card, an electronic loyalty card, an electronic rewards card, or an electronic coupon.

2. The method of claim 1 comprising receiving identification information associated with at least one of the sending mobile device and the receiving mobile device, wherein the identification information includes at least one of a phone number, a name, and an address.

3. The method of claim 1 wherein receiving a virtual card includes communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

4. The method of claim 3 wherein communicating over an over-the-air communications network includes communicating over one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network.

5. The method of claim 3 wherein communicating over an IP-based network includes communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

6. The method of claim 1 wherein receiving a virtual card includes receiving an electronic, monetary deposit using at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

7. The method of claim 1 wherein provisioning a virtual card includes:

i) communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network; or

ii) communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network, and provisioning a virtual card using at least one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network; or

iii) communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network, wherein communicating over an IP-based network includes communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

8. The method of claim 1 wherein provisioning a virtual card includes:

i) provisioning an electronic, monetary account using at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP);

ii) initiating one of an open loop or a closed loop account;

iii) transmitting a control short message service (cSMS) message to the receiving mobile device, wherein the cSMS message is configured to

access a wallet application associated with the receiving mobile device; and/or

iv) establishing a bearer independent protocol (BIP) using one of SMS PP and CAT_TP protocol to UICC/USIM without accessing the wallet application residing in the phone baseband memory.

9. The method of claim 1 comprising prompting the receiving mobile device to confirm the provisioning of the virtual card.

10. The method of claim 1 comprising storing the virtual card in a secure element in one of the sending mobile device and the receiving mobile device.

11. The method of claim 1 comprising encrypting at least one of the communications between the sending mobile device, the OTA provisioning server, and the receiving mobile device.

12. The method of claim 1 comprising authorizing the presentation of the virtual card.

13. The method of claim 12 wherein authorizing the virtual card transfer includes retrieving at least one of track I data, track II data, a routing number, a bank account number, a credit card number, an expiration date, a debit card number, and an automated clearing house (ACH) identifier.

14. An over-the-air (OTA) provisioning server for providing virtual card transfer between near field communications (NFC)-enabled mobile devices, the OTA provisioning server comprising:

a receiving module for receiving, from a sending mobile device, a virtual card for a receiving mobile device; and

an account module for provisioning the virtual card to the receiving mobile device, wherein the virtual card is immediately usable by the receiving mobile device at a point of sale terminal,

wherein the OTA provisioning server is implemented by at least one computer having associated hardware; and

the virtual card includes at least one of an electronic credit card, an electronic debit card, an electronic prepaid card, an electronic loyalty card, an electronic rewards card, or an electronic coupon.

15. The OTA provisioning server of claim 14 wherein the receiving module receives identification information associated with at least one of the sending mobile device and the receiving mobile device, wherein the identification information includes at least one of a phone number, a name, and an address.

16. The OTA provisioning server of claim 14 wherein the receiving module receives an electronic, monetary deposit over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

17. The OTA provisioning server of claim 16 wherein the receiving module communicates over:

i) an over-the-air communications network including communicating over one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network; or

ii) an IP-based network including communicating over one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network.

18. The OTA provisioning server of claim 14 wherein the receiving module receives a virtual card via at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

19. The OTA provisioning server of claim 14 wherein the account module provisions the virtual card by communicating over at least one of an over-the-air and an Internet protocol (IP)-based communications network.

20. The OTA provisioning server of claim 19 wherein the account module provisions a virtual card via:

i) at least one of a general packet radio service (GPRS), enhanced data rates for GSM evolution (EDGE), code division multiple access (CDMA), 3G, 4G, and long term evolution (LTE) network;

ii) an IP-based network including one of a Wi-Fi, worldwide interoperability for microwave access (Wi-Max), and an Ethernet network; or

iii) at least one of hypertext transfer protocol (HTTP), transmission control protocol (TCP), short message service (SMS), CAT_TP, code division multiple access (CDMA), Bluetooth, general packet radio service (GPRS), global system for mobile communications (GSM), Wi-Fi, SMS point-to-point (PP), Bearer Independent Protocol (BIP), and user datagram protocol (UDP).

21. The OTA provisioning server of claim 14 wherein the virtual card is one of an open loop or a closed loop virtual card.

22. The OTA provisioning server of claim 14 wherein the account module provisions the virtual card:

i) using a control short message service (cSMS) message to the receiving mobile device, wherein the cSMS message is configured to access a wallet application associated with the receiving mobile device; or

ii) by establishing a bearer independent protocol (BIP) using one of SMS PP and CAT_TP protocol to UICC/USIM without accessing the wallet application residing in the phone baseband memory.

23. The OTA provisioning server of claim 14 wherein the transmitting module

prompts the receiving mobile device to confirm the transmission of the electronic, monetary deposit.

24. A computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps comprising:

at an OTA provisioning server:

receiving, from a sending mobile device, a virtual card intended for a receiving mobile device; and

provisioning the virtual card to the receiving mobile device via an OTA interface, wherein the virtual card is immediately presentable by the receiving mobile device at a point of sale terminal;

wherein the virtual card includes at least one of an electronic credit card, an electronic debit card, an electronic prepaid card, an electronic loyalty card, an electronic rewards card, or an electronic coupon.

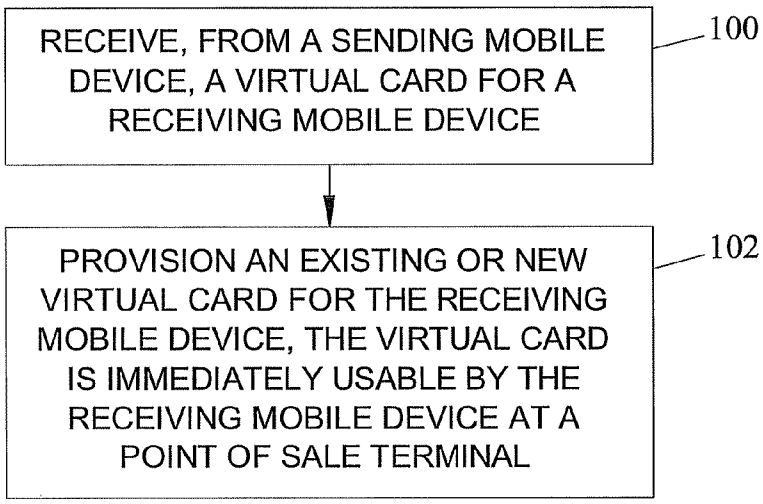
RECEIVE, FROM A SENDING MOBILE DEVICE, A VIRTUAL CARD FOR A RECEIVING MOBILE DEVICE
100
PROVISION AN EXISTING OR NEW VIRTUAL CARD FOR THE RECEIVING MOBILE DEVICE, THE VIRTUAL CARD IS IMMEDIATELY USABLE BY THE RECEIVING MOBILE DEVICE AT A POINT OF SALE TERMINAL
102

FIG. 1

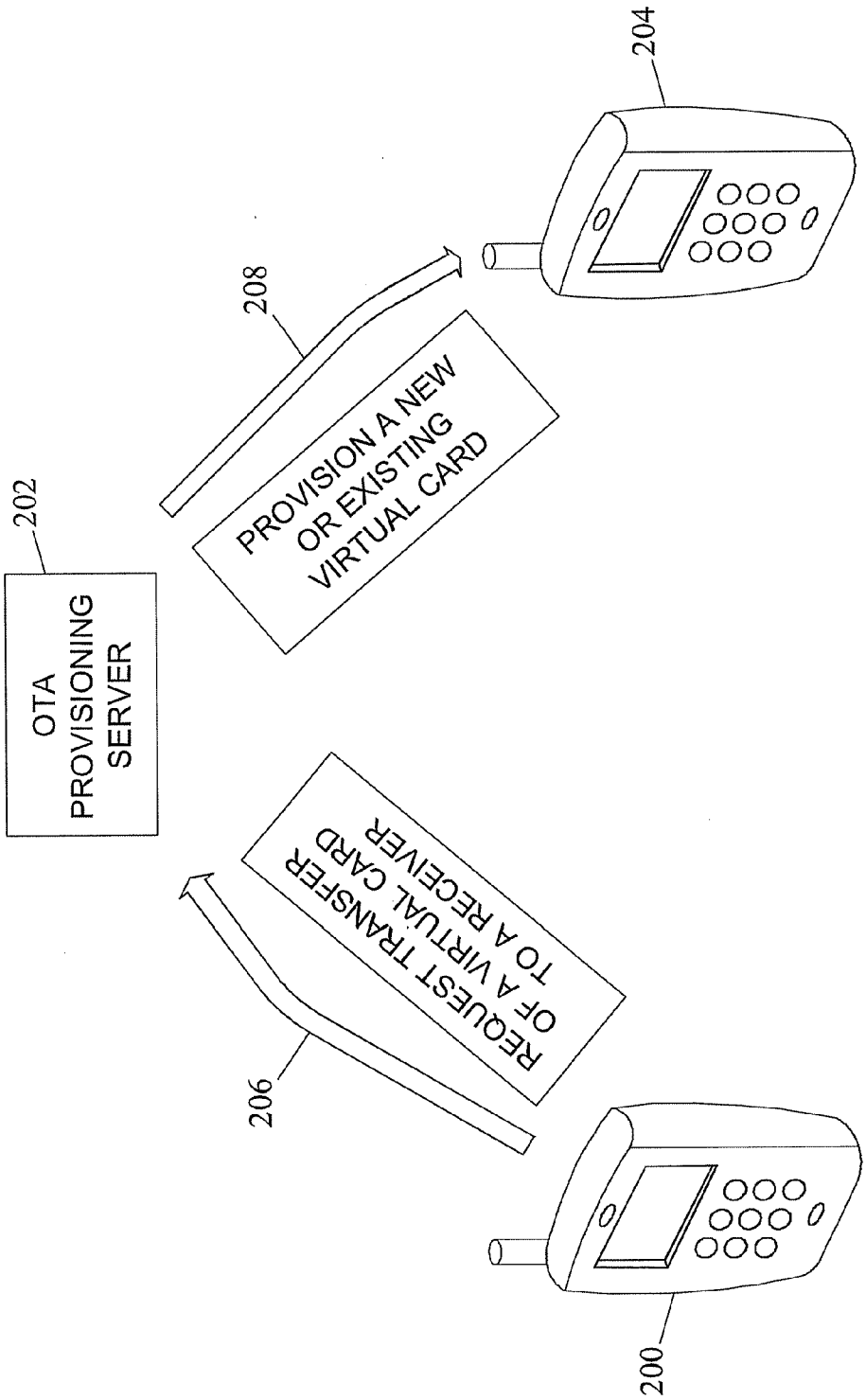
204
208
PROVISION A NEW OR EXISTING VIRTUAL CARD
202
OTA PROVISIONING SERVER
REQUEST TRANSFER OF A VIRTUAL CARD TO A RECEIVER
206
200

FIG. 2

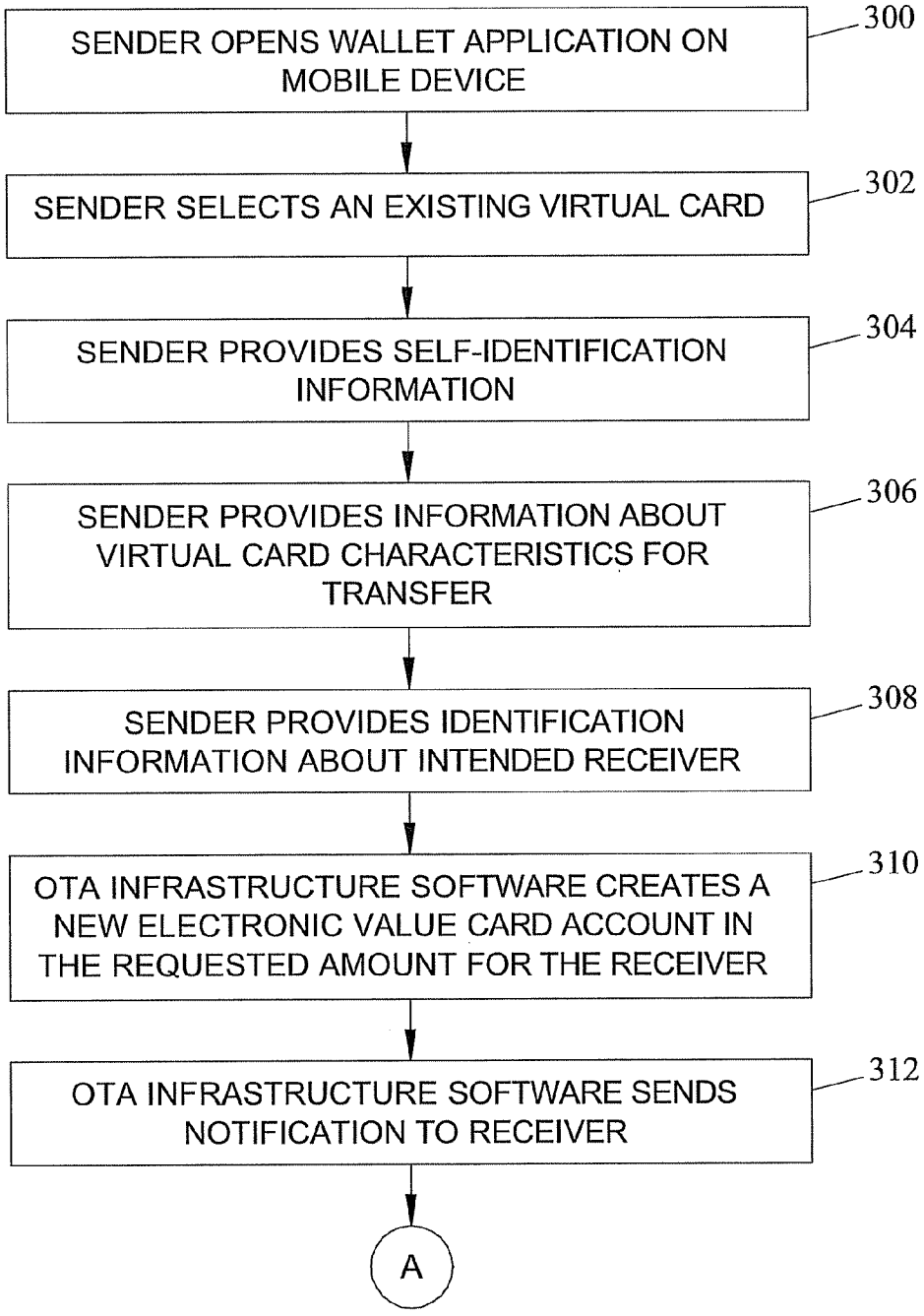
SENDER OPENS WALLET APPLICATION ON MOBILE DEVICE
300
SENDER SELECTS AN EXISTING VIRTUAL CARD
302
SENDER PROVIDES SELF-IDENTIFICATION INFORMATION
304
SENDER PROVIDES INFORMATION ABOUT VIRTUAL CARD CHARACTERISTICS FOR TRANSFER
306
SENDER PROVIDES IDENTIFICATION INFORMATION ABOUT INTENDED RECEIVER
308
OTA INFRASTRUCTURE SOFTWARE CREATES A NEW ELECTRONIC VALUE CARD ACCOUNT IN THE REQUESTED AMOUNT FOR THE RECEIVER
310
OTA INFRASTRUCTURE SOFTWARE SENDS NOTIFICATION TO RECEIVER
312
A

FIG. 3A

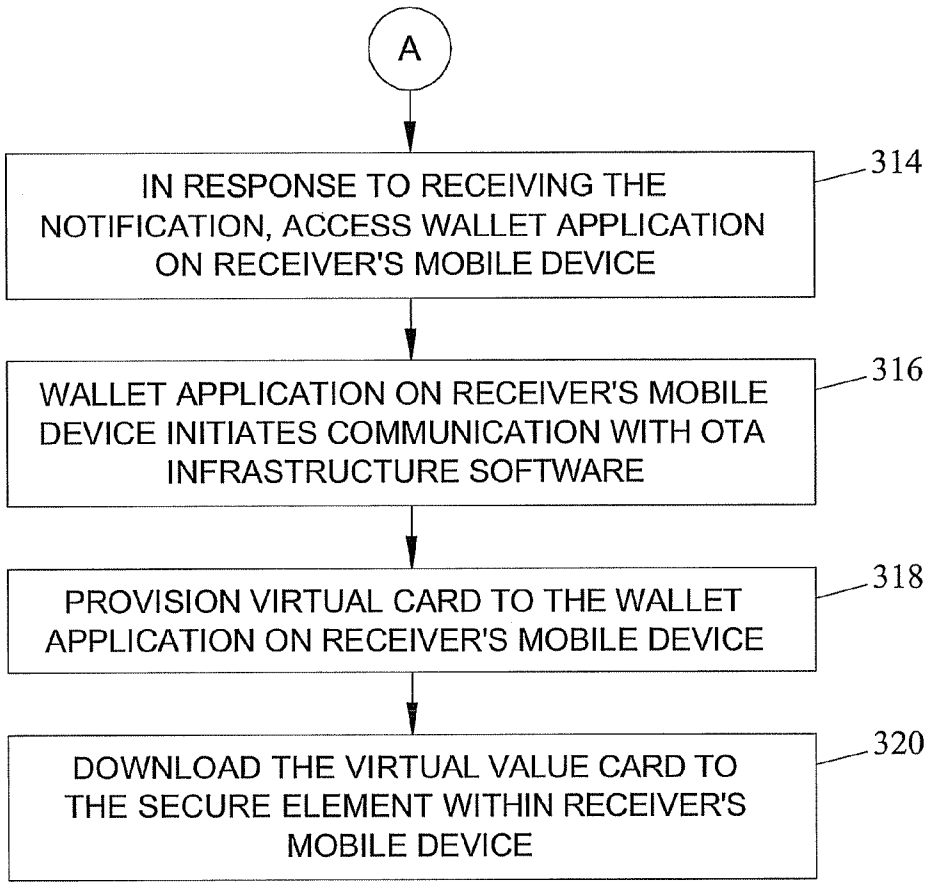
A
IN RESPONSE TO RECEIVING THE NOTIFICATION, ACCESS WALLET APPLICATION ON RECEIVER'S MOBILE DEVICE
314
WALLET APPLICATION ON RECEIVER'S MOBILE DEVICE INITIATES COMMUNICATION WITH OTA INFRASTRUCTURE SOFTWARE
316
PROVISION VIRTUAL CARD TO THE WALLET APPLICATION ON RECEIVER'S MOBILE DEVICE
318
DOWNLOAD THE VIRTUAL VALUE CARD TO THE SECURE ELEMENT WITHIN RECEIVER'S MOBILE DEVICE
320

FIG. 3B

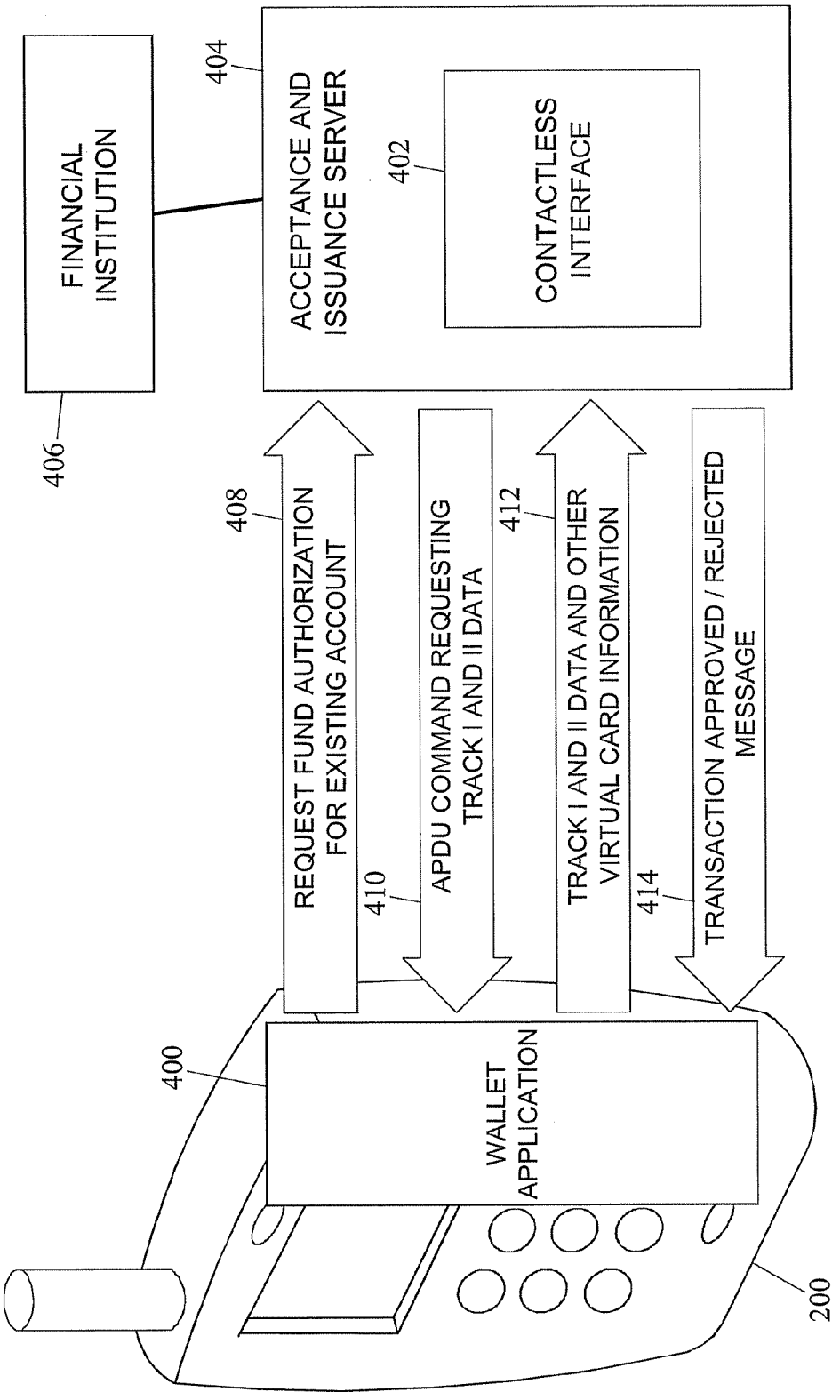
FINANCIAL INSTITUTION
406
404
ACCEPTANCE AND ISSUANCE SERVER
402
CONTACTLESS INTERFACE
408
REQUEST FUND AUTHORIZATION FOR EXISTING ACCOUNT
410
412
APDU COMMAND REQUESTING TRACK I AND II DATA
TRACK I AND II DATA AND OTHER VIRTUAL CARD INFORMATION
414
TRANSACTION APPROVED / REJECTED MESSAGE
400
WALLET APPLICATION
200

FIG. 4

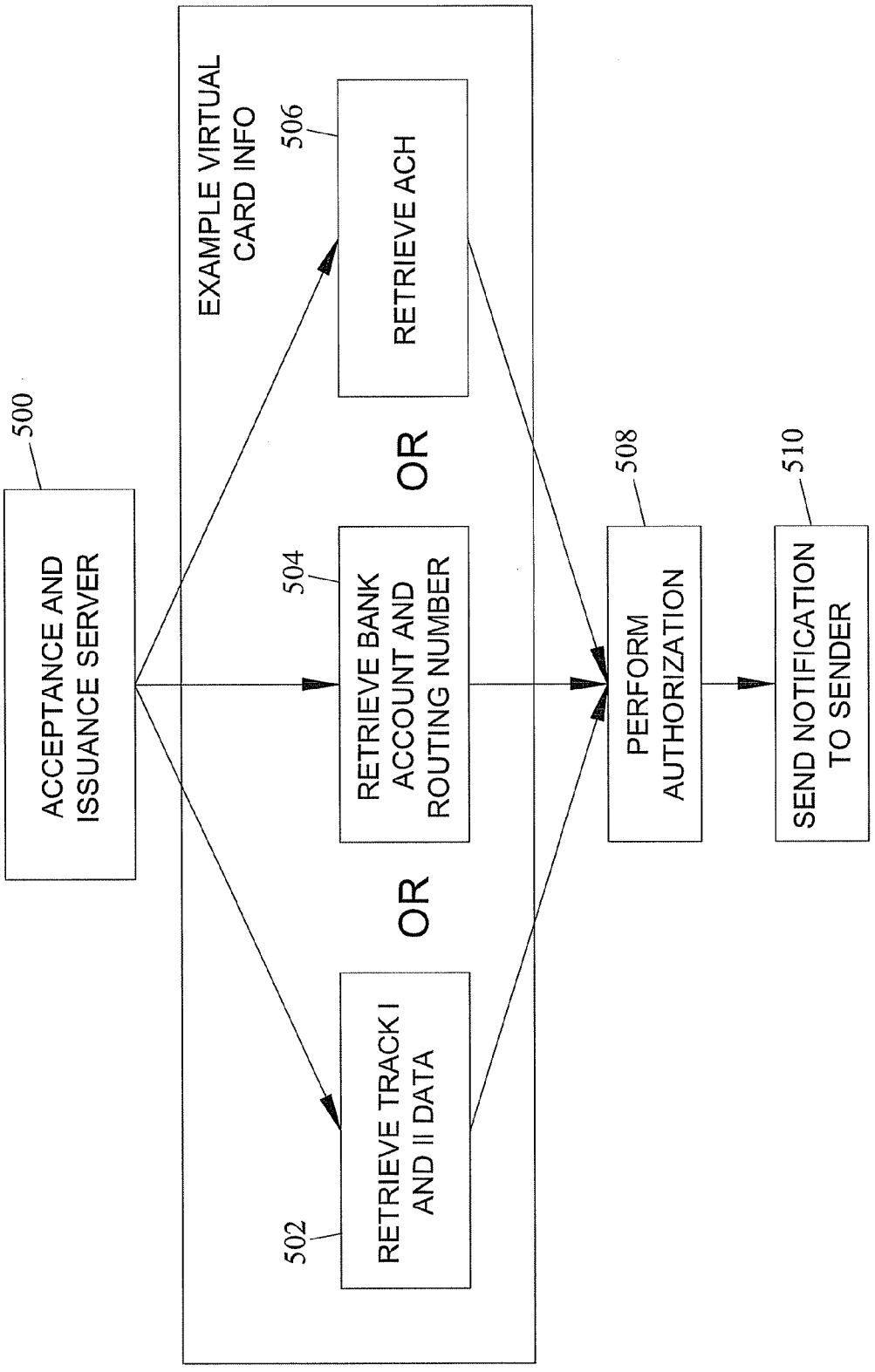
500
ACCEPTANCE AND ISSUANCE SERVER
EXAMPLE VIRTUAL CARD INFO
506
RETRIEVE ACH
OR
504
RETRIEVE BANK ACCOUNT AND ROUTING NUMBER
OR
502
RETRIEVE TRACK I AND II DATA
508
PERFORM AUTHORIZATION
510
SEND NOTIFICATION TO SENDER

FIG. 5

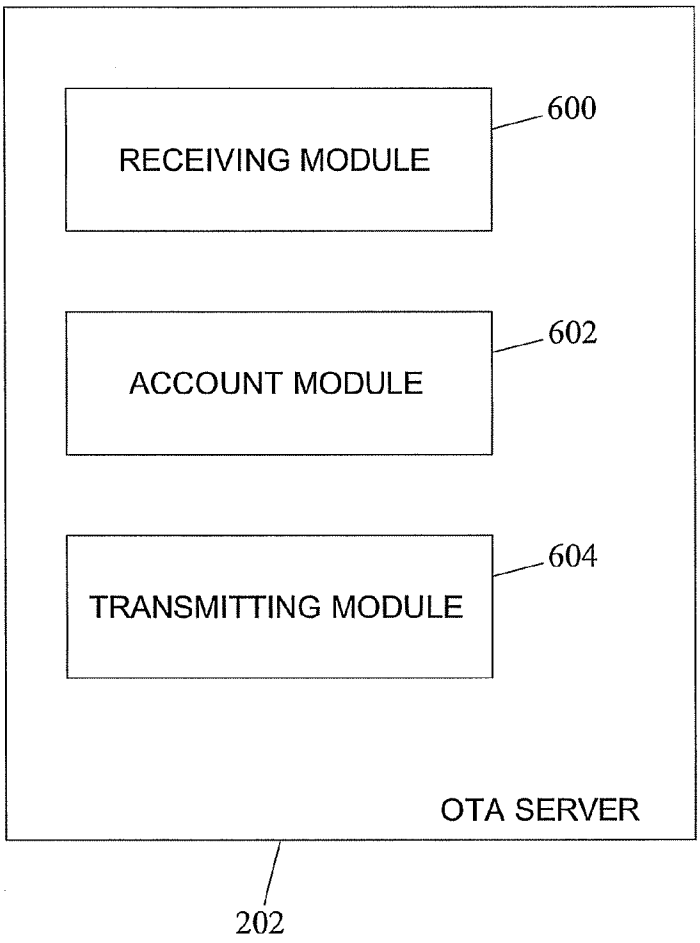
RECEIVING MODULE
600
ACCOUNT MODULE
602
TRANSMITTING MODULE
604
OTA SERVER
202

FIG. 6

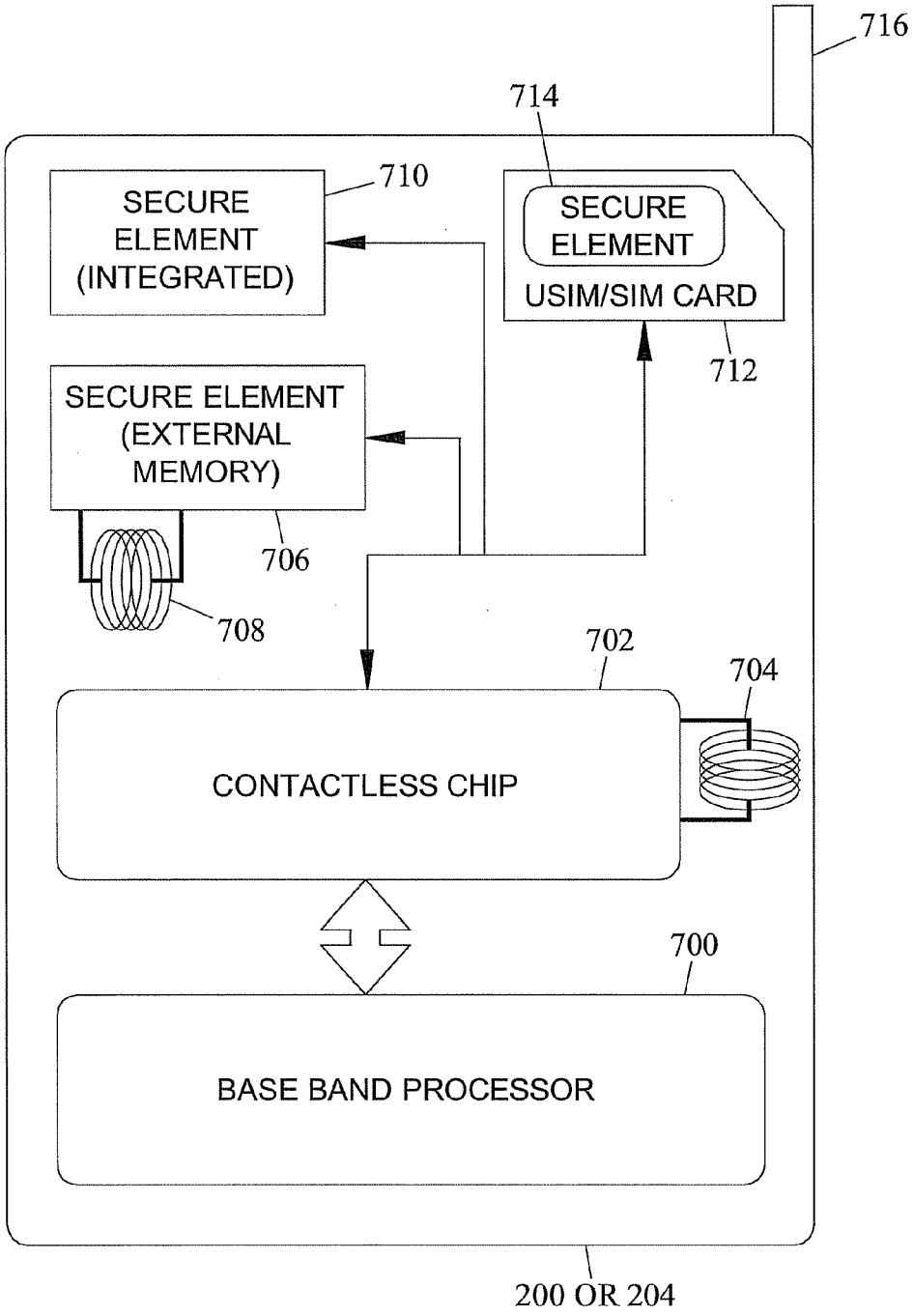
716
714
710
SECURE ELEMENT (INTEGRATED)
SECURE ELEMENT
USIM/SIM CARD
712
SECURE ELEMENT (EXTERNAL MEMORY)
706
708
702
704
CONTACTLESS CHIP
700
BASE BAND PROCESSOR
200 OR 204

FIG. 7