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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 February 2010 (18.02.2010)

PCT

(10) International Publication Number
WO 2010/019670 A2

(51) International Patent Classification:
G06Q 40/00 (2006.01) *G06Q 20/00* (2006.01)

(21) International Application Number:
PCT/US2009/053556

(22) International Filing Date:
12 August 2009 (12.08.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/190,564 12 August 2008 (12.08.2008) US

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

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **KUMAR, Pradeep** [IN/US]; 4037 Oroville Court, Fremont, CA 94555 (US).

(74) Agent: **HUNT, Gregory, A.**; JENKINS, WILSON, TAYLOR & HUNT, P.A., 3100 Tower Boulevard - Suite 1200, University Tower, 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:

— *without international search report and to be republished upon receipt of that report (Rule 48.2(g))*

WO 2010/019670 A2

(54) **Title**: METHODS, SYSTEMS AND COMPUTER READABLE MEDIA FOR ELECTRONICALLY DELIVERING A PREPAID CARD TO A MOBILE DEVICE

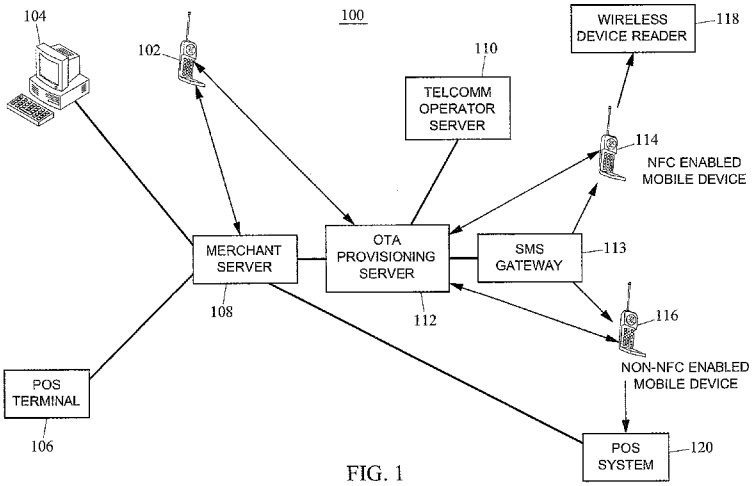

FIG. 1

(57) **Abstract**: Methods, systems, and computer readable media for electronically delivering a prepaid card to a mobile device are disclosed. According to one aspect, the method includes receiving, at a merchant server, purchase information related to the purchase of an electronic prepaid card. The method further includes receiving, from the merchant server, electronic prepaid card information derived from the purchase information. The method further includes establishing a communications link with a mobile device associated with address data included in the electronic prepaid card information. The method also includes provisioning the electronic prepaid card information on the mobile device via over the air (OTA) communications.

DESCRIPTION

METHODS, SYSTEMS AND COMPUTER READABLE MEDIA FOR ELECTRONICALLY DELIVERING A PREPAID CARD TO A MOBILE DEVICE

RELATED APPLICATIONS

This application claims the benefit of U.S. Patent Application Serial No. 12/190,564, filed August 12, 2008, the disclosure of which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

The subject matter described herein relates to electronic prepaid cards using short message service (SMS) messaging and over the air provisioning (OTA). More particularly, the subject matter described herein relates to methods, systems, and computer readable media for electronically delivering a prepaid card to a mobile device.

BACKGROUND

Currently, the primary means for purchasing prepaid cards, such as a gift card, involves a consumer visiting a brick and mortar store, selecting a physical prepaid card, and conducting a normal purchase transaction with a cashier. Alternatively, the consumer may purchase the prepaid card over the Internet by visiting the merchant's web site using a personal computer to conduct a secured electronic payment transaction using a credit card. Regardless of the manner in which the prepaid card is purchased, the end result is normally the same. Namely, the consumer physically receives a plastic prepaid card (e.g., a magnetic stripe gift card) from the cashier at the store or from the merchant via the mail. Similarly, a second party (e.g., a gift recipient) may physically receive the prepaid card either in the mail (i.e., from either the consumer, or directly from the merchant) or in person from the consumer.

Regardless of the manner in which the recipient ultimately receives the prepaid card, the prepaid card is usually provided as a tangible, physical card.

As such, the fact the prepaid card is a tangible, physical card may give rise to several problems. For instance, due to its size, the physical prepaid card may be readily misplaced, stolen, or even damaged prior to the consumer using the prepaid card. Moreover, a physical prepaid card cannot be immediately presented to a recipient as a gift if the purchaser and recipient (i.e., sender and recipient) are geographically separated. Rather the presentation of the prepaid card to the recipient is typically limited to conventional mail services.

Accordingly, there exists a need for methods, systems, and computer readable media for electronically delivering a prepaid card to a mobile device.

SUMMARY

Methods, systems, and computer readable media for electronically delivering a prepaid card to a mobile device are disclosed. According to one aspect, the method includes receiving, at a merchant server, purchase information related to the purchase of an electronic prepaid card. The method further includes receiving, from the merchant server, electronic prepaid card information derived from the purchase information. The method further includes establishing a communications link with a mobile device associated with address data included in the electronic prepaid card information. The method also includes provisioning the electronic prepaid card information on the mobile device via over the air (OTA) communications.

The subject matter described herein for electronically delivering a prepaid card to a mobile device may be implemented using a computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer 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 electronically delivering a prepaid card to a mobile device 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

The subject matter described herein will now be explained with reference to the accompanying drawings of which:

Figure 1 is a block diagram depicting an exemplary system for electronically delivering a prepaid card to a mobile device according to an embodiment of the subject matter described herein;

Figure 2 is a flow chart depicting an exemplary process for purchasing an electronic prepaid card according to an embodiment of the subject matter described herein;

Figure 3 is a flow chart depicting an exemplary process for issuing an electronic prepaid card to a near field communications (NFC) enabled mobile device according to an embodiment of the subject matter described herein; and

Figure 4 is a flow chart depicting an exemplary process for transferring an electronic prepaid card from a first near field communications (NFC) enabled mobile device to a second NFC enabled mobile device according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

In order to eliminate the need for users to carry physical cards (e.g., a credit card), card issuers have begun making softcards available to the general public. As used herein, the term "softcard" refers to a software-implemented entity for facilitating transactions, such as payment transactions. Examples of softcards include payment cards, such as credit cards, loyalty cards, member cards, identification cards, and other payment and non-payment cards that exist in an electronic or software-based format.

A softcard may be provisioned on a device with wireless communications capabilities. Devices with wireless communication capabilities are typically configured to interact with wireless readers to enable transactions involving the softcard. Examples of devices with wireless communications capabilities include mobile phones, smart phones, key fobs, physical cards, and

personal digital assistants with interfaces to local card readers. Interactions between a device and a reader may occur via an electric and/or magnetic field between the device and the reader. One type of communications channel that may be used between a device capable of supporting a softcard and a card reader for payment 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 device and the contactless card reader. Example of a contactless communications protocol that may be used in communications between a device capable of supporting a softcard and a contactless, or wireless, reader is an ISO 14443 interface.

Devices with wireless communications capabilities may also be capable of data communications with remote entities. For example, devices with wireless communications capabilities may implement HTTP over TCP/IP over-the-air interface for communicating with remote entities. 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, Bluetooth, etc.

Figure 1 is a block diagram of an exemplary system **100** for electronically delivering a prepaid card to a mobile device according to an embodiment of the subject matter described herein. In one embodiment, system **100** comprises a plurality of devices, which may include a mobile device **102**, a computer **104**, or a point of sale (POS) terminal **106**. Notably, devices **102-106** provide a sender with the necessary means to provide (e.g., purchase or forward) an electronic prepaid card to a recipient party. As used herein, the term "sender" refers to a user who purchases a prepaid card (e.g., an electronic gift card) for the benefit of a "recipient" via a merchant website, store cashier, and the like. Likewise, as used herein, the term "recipient" refers to a user that receives the electronic prepaid card in the form of a softcard (or a short message service (SMS) message containing an authorization code that may subsequently be used to obtain a physical prepaid card in an alternate embodiment). It should also be noted that the sender and recipient may be the same entity in certain scenarios.

In one embodiment, a sender uses computer **104**, which may include a personal computer (e.g., at the sender's home) or a kiosk station (e.g., positioned at or near a merchant/retail store), to access a merchant's web site. As used herein, the term "merchant" may include a seller, a retailer, or any other like entity that sells goods or services. By using the interface presented by the merchant web site, the sender may purchase an electronic prepaid card by providing various types of information. For example, one type of information may comprise recipient information. Recipient information may include the name of the recipient, the mobile phone number associated with the recipient, and even a personal message (e.g., "Happy Birthday") for the recipient. In another embodiment, a prepaid card purchase transaction described above may be conducted using a POS terminal **106** (e.g., a cash register computer, a self-checkout machine, etc.) located at the merchant store with or without the assistance of a cashier.

System **100** may also include a merchant server **108**, a telecommunications operations server **110**, and an over-the-air (OTA) provisioning server **112**. In one embodiment, merchant server **108** may comprise a backend server that is associated with a particular merchant, retailer, or Internet-based store. Telecommunications operator server **110** may include a server associated with a telecommunications service provider (e.g., a wireless phone service provider) that is capable of providing information related to a given mobile device and/or phone number. For example, server **110** may contain phone numbers and the type of mobile device associated with each phone number. OTA provisioning server **112** may include a server that is responsible for receiving and validating prepaid card information from various merchant servers (e.g., merchant server **108**) as well as issuing electronic prepaid card information to mobile devices (e.g., mobile devices **114**, **116**, as explained below) per the instructions and information received from the merchant servers. In one embodiment, the functions provided by OTA provisioning server **112** may be performed by a plurality of servers (e.g., a control server, which provides OTA administrative services for the secure element on a mobile device, and an issuer server, which provides a secure

local provisioning point for issuing softcards to a mobile device in order to allow an issuer to maintain full possession and control of softcard data).

System **100** may also include a near field communications (NFC) enabled mobile device **114**, a non-NFC enabled mobile device **116**, a wireless device reader **118**, and a POS system **120**. In one embodiment, wireless device reader **118** may be co-located and/or incorporated within POS system **120** (e.g., at the same retail store). In one embodiment, POS system **120** may include a cash register/computer operated by a cashier.

NFC enabled mobile device **114** may include a mobile phone with embedded NFC support circuitry/software, which enables a user to wirelessly communicate with wireless device reader **118**. Similarly, NFC enabled mobile device **114** may include universal subscriber identification module (USIM)/USIM integrated circuit card (UICC) NFC support circuitry/software to wirelessly communicate with the wireless device reader.

In contrast, non-NFC enabled mobile device **116** may include a cellular phone that does not include embedded NFC or USIM/UICC NFC support circuitry/software or any other means to wirelessly communicate with contactless card reader **118**. In one embodiment, wireless device reader **118** may include any reader (e.g., a wireless RFID reader or a contactless card reader) that is capable of reading wireless smart cards, NFC enabled mobile devices, or any other contactless payment type device. In one embodiment, wireless device reader **118** may wirelessly communicate with NFC-enabled mobile device **114** via an electromagnetic field.

Specifically, NFC involves communication via magnetic field induction, where two loop antennas are located within each other's near field, which effectively forms an air-core transformer. For example, an NFC enabled mobile device **114** may communicate with wireless device reader **118** via the inductive coupling of the reader's antenna to the mobile device's antenna. Wireless device reader **118** modulates the loading on its loop antenna in order to amplitude-modulate a radio frequency (RF) field/electromagnetic field. The modulations in the field are received and detected by the mobile device's antenna, thereby communicating information. In order to communicate, a transceiver module on the contactless reader may transmit a command signal

to the mobile device via the electromagnetic field (or some other energy field) powered by contactless reader. For example, by oscillating the electromagnetic field on and off very quickly, the contactless reader (via the transceiver module) is able to send a command as a string of data to mobile device **114**. Similarly, by drawing power from the electromagnetic field or using its own power source, mobile device **114** is able to send a response to contactless reader **118** by creating a short circuit on its own antenna. The short circuit produces a larger load on the reader's antenna, which is promptly detected as a communication from mobile device **114**. An example of a near-field wireless communications standard commonly used by NFC enabled mobile devices and wireless smart cards is ISO 14443.

As mentioned above, there are several ways in which a sender may electronically provide a prepaid card to the recipient. In one embodiment, the prepaid card may be purchased by a sender through a merchant's web site. For example, the sender/purchaser may log into a merchant/retailer website (e.g., using personal computer **104** or a retail kiosk) in order to select a prepaid card type (e.g., a gift card), the amount of funds to be placed on the card, and the time and date of electronic delivery of the card to the recipient (i.e., transaction information). The sender may also provide recipient information that includes the name of the intended recipient (e.g., the recipient may be the sender/purchaser himself or a second party) of the electronic prepaid card and an associated mobile device number. Likewise, the sender may also be permitted to send a message along with the electronic prepaid card information (e.g., "Happy Birthday"). After providing the above "transaction" and "recipient" information, the sender may provide the necessary "payment" information (e.g., by swiping a plastic credit card at a kiosk, entering a checking account or credit card number via a web site interface, etc.) to pay for the electronic prepaid card. In one embodiment, all of the above transaction, recipient, and payment information (i.e., collectively the "purchase data") is provided to a merchant server **108**.

In an alternate embodiment, the sender may instead purchase the electronic prepaid card at a merchant point of sale (e.g., POS terminal **106**). For example, the sender may approach the cashier at the merchant store and

select the electronic prepaid card type (e.g., a gift card), the amount, and the time and date of delivery (i.e., transaction data). The sender may then provide payment, such as cash or credit card/checking account information (i.e., payment data), for the electronic prepaid card. The sender can also provide the information associated with the recipient (i.e., recipient data), such as the recipient's name, the recipient's mobile device phone number, and a personal message (e.g., "Happy Birthday!") to the cashier. The cashier may process the transaction and present a receipt to the sender. After the purchase data (e.g., transaction information, the payment information, and recipient's information) is entered into the cash register/computer (e.g., POS terminal **106**), the data is sent to merchant server **108**.

Upon receiving the purchase data, merchant server **108** may be configured to perform a series of operations. In one embodiment, merchant server **108** sends a confirmation SMS message and/or email message to the sender. In one embodiment, the sender's contact number or email address is provided at the time the electronic prepaid card is purchased. The confirmation message may contain a purchase receipt as well as other details related to the electronic prepaid card or purchase transaction. In one embodiment, merchant server **108** may process the received purchase data from the sender. For example, merchant server **108** may generate additional prepaid card information such as the prepaid card number, the prepaid card image, a prepaid card authorization code, and the prepaid card validity information in response to receiving the purchase data. Likewise, merchant server **108** may generate personalization information using the purchase data obtained from the sender.

In one embodiment, merchant server **108** sends the above-mentioned data to OTA provisioning server **112** via a request message. For example, the request message may be embodied as a message requesting that OTA provisioning server **112** issue an electronic prepaid card (e.g., either a softcard or an SMS authorization code) to the recipient mobile phone number provided. Upon receiving the purchase data and generated electronic prepaid card data, OTA provisioning server **112** may be configured to determine if the recipient mobile device is NFC enabled (e.g., mobile device **114**) or not (e.g., mobile

device **116**). In one embodiment, OTA provisioning server **112** provides telecommunications operations server **110** with the mobile device number of a receiving party. Telecommunications operations server **110** may then access a database to obtain information relating to the type of cellular phone (e.g., NFC enabled or otherwise) that is associated with the provided mobile device number. Upon locating this device information, telecommunications operations server **110** forwards the mobile device type data to OTA provisioning server **112**.

After receiving the mobile device type information and prepaid card information, OTA provisioning server **112** is configured to deliver the prepaid card as either a softcard or an SMS message. The manner in which the electronic prepaid card is sent depends if the phone number to which the prepaid card is to be delivered is either an NFC enabled phone or non-NFC enabled phone. If the former, then OTA provisioning server **112** is configured to deliver the prepaid card as a softcard. Alternatively, if the phone number to which the prepaid card is to be delivered is associated with a non-NFC enabled phone, then OTA provisioning server **112** is configured to deliver the prepaid card as a code via an SMS message. Notably, a non-NFC enabled phone is not configured to transfer a prepaid softcard to a wireless device reader.

In the exemplary embodiment where the receiving mobile device is NFC enabled, OTA provisioning server **112** sends a control SMS message to NFC enabled mobile device **114** using the mobile phone number provided by merchant server **108**. In response, NFC enabled mobile device **114** may read the SMS control content, which triggers a wallet client application (not shown) to initiate a downloading process to receive an electronic prepaid card from OTA server **112**. NFC enabled mobile device **114** (e.g., via wallet client) may then reply to OTA provisioning sever **112** with an acknowledgement message. In one embodiment, a wallet client application may include a software application that manages multiple softcards stored on a mobile device, such as credit cards, debit cards, prepaid cards, electronic coupons, electronic tickets and the like. The wallet client may also be configured to ensure end-to-end protection of softcard data and payment applications with its interface for OTA provisioning as well as its management of the mobile device's secure element

(not shown). The secure element may include any type of hardware and/or software structure that utilizes encryption or any other means for securing sensitive data within a mobile device.

In response to the acknowledgement message, OTA provisioning server **112** may establish a secure connection using, for example, an http /https /TCP /SMS PP /CAT_TP protocol with NFC enabled mobile device **114** and provides prepaid personalization data (e.g., similar to Track 1 and Track 2 data) along with branding or issuer marketing data (e.g., branding image, customer support number, network supported, and the like). In one embodiment, the personalization data is stored on a secure element validated within mobile device **114**.

After the download process is completed, the wallet client displays the electronic prepaid card as a softcard (which visually represents the personalization data contained in the secure element). Once the downloading process is complete, OTA provisioning server **112** may then send a message instructing merchant server **108** to send an SMS message to the original purchaser **102** to notify that the delivery of the prepaid softcard was successful.

Once the prepaid softcard is stored in NFC enabled mobile device **114**, the recipient may decide to use the electronic prepaid softcard at an appropriate retail store or the like. For instance, after deciding what goods to purchase at a store, the recipient brings the merchandise to the check out station and is prompted by the cashier to provide a method of payment. The recipient may then use mobile device **114** to select the prepaid softcard. For example, the recipient may interface mobile device **114** with contactless card reader **118** via NFC communication. Personalization data associated with the prepaid softcard is then transferred to wireless device reader **118**. Namely, the transfer of this information facilitates a secure payment transaction by providing electronic funds for payment. The transaction then proceeds as normal if the funds were sufficient to cover the purchased goods, otherwise the customer is prompted to provide additional payment for the outstanding balance.

In the second embodiment mentioned above, the electronic prepaid card is provided to a non-NFC enabled phone via SMS messages. For example, mobile device **116** may receive an SMS message from OTA provisioning server

112 instead of receiving an SMS control message. The received SMS message may include a prepaid card authorization code. This authorization code is associated with a previously registered amount of funds and may be provided to a cashier at POS system **120** as detailed below.

After receiving the prepaid card authorization code, the recipient of mobile device **116** may decide to use the electronic prepaid card at a retail store or the like. For example, after selecting goods for purchase, the recipient presents the merchandise at the check out counter and may be prompted by the cashier to provide a method of payment. The recipient may then provide the prepaid card authorization code and the phone number of mobile device **116** to the cashier. The cashier may then enter the authorization code and the phone number in the POS system **120**. In one embodiment, POS system **120** validates the authorization code and phone number with merchant server **108** to ensure that the correct recipient receives the proper funds or the authorization code has not been previously used. Merchant server **108** may return information that indicates the amount of funds associated with the prepaid card if the authorization code is valid. At this point, merchant server **108** may send an SMS message and/or email message, which indicates the successful delivery of the prepaid card, to the user device (e.g., mobile device **102**) of the original purchaser/sender. The cashier may then confirm the amount of funds with the user of mobile device **116**. Once validated, the cashier will encode the dollar amount onto a plastic magnetic stripe card, which is then activated. The recipient of the plastic magnetic stripe card may then use the card for his purchase. In an alternate embodiment, the cashier may use a portion of the validated dollar amount for the purchase of the customer's merchandise and encode the outstanding dollar amount onto the plastic magnetic stripe card.

To better illustrate the communication of the components depicted in Figure 1, Figure 2 is provided to describe a purchasing transaction process using a flow diagram. Specifically, Figure 2 is a flow chart of an exemplary method **200** for purchasing an electronic prepaid card according to an embodiment of the subject matter described herein.

In block **202**, the sender logs into a merchant's website. In one embodiment, the sending party using personal computer or a kiosk computer station to gain access to the merchant's website.

In block **204**, the sender makes selections and provides recipient and payment data. In one embodiment, the sender uses the website interface to select a specific type of prepaid card, the amount of money to be placed on the prepaid card, and the date and time in which the prepaid card should be delivered to the recipient. The sender may also provide a credit card account number or the like to pay for the electronic prepaid card.

In block **206**, the sender's selections and provided data are received by a merchant server. In one embodiment, after finalizing the selections and confirming the recipient and payment data, the sender electronically submits (e.g., hits the "submit" button) the information to merchant server **108**.

In block **208**, the merchant server sends a confirmation message. In one embodiment, merchant server **108** sends an SMS or email confirmation message to the sender. The confirmation message may include a purchase receipt or some other detailed information regarding the purchase transaction.

In block **210**, the merchant server processes data and generates prepaid card data. In one embodiment, merchant server **108** processes the received purchase data from the sender (e.g., the transaction data, the recipient data, and the payment data). For example, merchant server **108** utilizes the purchase data to generate other data that is unique to the prepaid card, such as a prepaid card number, a prepaid card authorization code, a prepaid card image, prepaid card personalization information, and prepaid card validity information.

In block **212**, an OTA provisioning server receives a provisioning request message. In one embodiment, OTA provisioning server **112** receives a message from merchant server **108** to issue an electronic prepaid card to a recipient that is associated with a specific mobile phone number (i.e., the mobile phone number provided by the sender in block **204**). The request message may also include other information, such as the personal message and the prepaid card amount similarly provided in block **204**. Likewise, the

request message may also include the information generated by merchant server **108** in block **210**.

In block **214**, the OTA provisioning server requests the recipient's mobile device or handset type. In one embodiment, OTA provisioning server **112** sends a query to a telecommunications operations server **110** requesting the type of handset associated with the recipient's mobile device number.

In block **216**, a determination is made as to whether the recipient's handset is an NFC enabled mobile device or a non-NFC enabled mobile device. If OTA provisioning server **112** ascertains that the recipient's device is an NFC enabled mobile device, then method **200** continues to block **218**. Otherwise, method **200** continues to block **222** where OTA provisioning server **112** sends an authorization code message to SMS gateway **113**. In response (i.e., block **224**), SMS gateway **113** sends an SMS message embedded with the authorization code to non-NFC enabled mobile handset **116**.

In block **218**, a control short message is generated. In one embodiment, OTA provisioning server **112** generates a control (binary) short message service (SMS) message to instruct the recipient's NFC enabled mobile device to activate a wallet client application.

In block **220**, the control short message is sent to an SMS gateway. In one embodiment, SMS gateway **113** may receive the control (binary) short message and send the message to recipient mobile device **114**.

To better illustrate the issuance of an electronic prepaid card in an NFC enabled mobile device, Figure 3 is provided to depict a flow chart of an exemplary method **300** for issuing an electronic prepaid card according to an embodiment of the subject matter described herein.

In block **302**, a control short message is received by an NFC enabled handset. In one embodiment, OTA provisioning server **112** sends a control SMS message (via SMS gateway **113**) to NFC enabled mobile device **114**.

In block **304**, the NFC enabled handset processes the control SMS message. In one embodiment, a wallet client of mobile device **114** is instructed by the control short (binary) message to initiate a download process. Mobile device **114** may also send a message acknowledging receipt of the control short message to OTA provisioning server **112**.

In block **306**, the OTA provisioning server receives an acknowledgement message from the NFC enabled handset. In one embodiment, OTA provisioning server **112** receives a message acknowledging the receipt of the control message from the wallet client in mobile device **114**.

In block **308**, the OTA provisioning server creates a secured link with NFC enabled handset. In one embodiment, OTA provisioning server **112** established a secured line of communications with the wallet client and secure memory of mobile device **114**.

In block **310**, the OTA provisioning server provides personalization data over the secured link. In one embodiment, OTA provisioning server **112** uploads personalization data to the secure element in mobile device **114** over the established secured link.

In block **312**, the NFC enabled handset displays the prepaid card as a softcard. In one embodiment, the wallet client in mobile device **114** displays the electronic prepaid card, which is a graphical representation associated with the stored personalization data, as a softcard.

In block **314**, the prepaid softcard is used at a wireless device reader to make a purchase. In one embodiment, the user of mobile device **114** (i.e., the recipient) may approach a contactless reader **118** at a retail store and utilize the prepaid softcard to make a purchase. For example, the user may select the prepaid softcard from the wallet client graphical user interface (GUI) and interface NFC enabled mobile device **114** with wireless device reader **118** (e.g., bring the two devices in close proximity). By interfacing mobile device **114** with wireless device reader **118**, personalization data is provided to the wireless device reader **118**, which in turn provides the data to a cashier device (e.g., a POS system) in order to facilitate the payment transaction.

In another embodiment of the present subject matter, a sender may decide to transfer or forward an electronic prepaid card, which has been previously purchased and is stored on the sender's NFC enabled mobile device, directly to a recipient's mobile device. Figure 4 illustrates an exemplary method **400** for transferring an electronic prepaid softcard from a sender's NFC enabled mobile device (e.g., mobile device **102**) to a recipients' NFC enabled mobile device (e.g., mobile device **114**).

In block **402**, a sender selects a prepaid softcard in the sender's NFC enabled mobile device. In one embodiment, the sender may select a previously obtained prepaid card that is stored in the wallet client for transfer.

In block **404**, the sender transfers the prepaid softcard to a recipient. In one embodiment, the sender may select an option to forward the electronic prepaid softcard to a recipient's NFC enabled mobile device.

In block **406**, the sender is prompted to provide recipient information. In one embodiment, NFC enabled mobile device **102** may query the sender to provide the recipient's information, such as the recipient's name, mobile phone number, and/or a personal message.

In block **408**, the sender's NFC enabled mobile device sends a transfer request. In one embodiment, NFC enabled mobile device **102** sends a transfer request message to OTA provisioning server **112**. The transfer request message may include the recipient information obtained in block **406** as well as personalization data associated with the sender's NFC enabled mobile device (e.g., this data may only include sender's phone number, the balance of the softcard, and/or personalization data).

In block **410**, the OTA provisioning server validates the sender data. In one embodiment, OTA provisioning server **112** establishes communication with merchant server **108** in order to validate the sender's information with information stored on merchant server **108** (e.g., verify that the data from the sender's phone corresponds to the data stored in merchant server **108**). Similarly, merchant server **108** may also be provisioned with data associated with the intended recipient so as to record the transfer (i.e., the recipient is the new "owner" of the transferred electronic prepaid card).

In block **412**, the OTA provisioning server **112** sends a control short message to delete the softcard (e.g., the personalization data) from sender's NFC enabled handset. In one embodiment, OTA provisioning server **112** may conduct the transfer of the prepaid softcard by disassociating the electronic prepaid card from the sender's mobile device and subsequently associating the electronic prepaid card to the recipient's mobile device if the information in block **410** is validated. For example, OTA provisioning server **112** may send a command to disassociate, or delete, the personalization data from the sender's

NFC enabled handset client application. Similarly, OTA provisioning server **112** may then send another control short message to the recipient's NFC enabled mobile device in order to initiate the issuing of an electronic prepaid softcard. In one embodiment, OTA provisioning server **112** may transfer the "new" prepaid softcard in the manner described by method **300** in Figure 3.

In block **414**, a confirmation message is sent to the sender's mobile device. In one embodiment, OTA provisioning server **112** sends a confirmation message to mobile device **102** indicating that the transfer process was successful. The recipient may now freely use the transferred prepaid softcard utilizing the recipient mobile device (e.g., mobile device **114**).

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.

CLAIMS

What is claimed is:

1. A method for electronically delivering a prepaid card to a mobile device, the method comprising:

receiving, at a merchant server, purchase information related to the purchase of an electronic prepaid card;

receiving, from the merchant server, electronic prepaid card information derived from the purchase information;

establishing a communications link with a mobile device associated with address data included in the electronic prepaid card information; and

provisioning the electronic prepaid card information on the mobile device over the communications link via over the air (OTA) communications.

2. The method of claim 1 wherein the electronic prepaid card information includes personalization data that is used to generate a softcard prepaid card in the mobile device.

3. The method of claim 1 wherein the electronic prepaid card information comprises a prepaid card authorization code.

4. The method of claim 1 wherein establishing a communications link with a mobile device comprises:

sending a control short message service (SMS) message to the mobile device associated with the address data included in the prepaid card information; and

receiving, from the mobile device, an electronic prepaid card download request for the electronic prepaid card information.

5. The method of claim 1 further comprising:

storing the electronic prepaid card information on the mobile device as a prepaid softcard and personalization data.

6. The method of claim 5 further comprising:

storing the personalization data within a secure element in the mobile device.

7. The method of claim 1 further comprising:

sending a message to the merchant server indicating the successful delivery of the electronic prepaid information to the mobile device.

8. The method of claim 7 further comprising:

sending a message to the original purchaser of the prepaid card from the merchant server indicating a successful delivery of the electronic prepaid information to the mobile device.

9. The method of claim 1 further comprising:

transferring the personalization data to a wireless device reader in order to conduct a payment transaction.

10. A system for electronically delivering a prepaid card to a mobile device, the system comprising:

a merchant server for receiving purchase information related to the purchase of an electronic prepaid card and generating electronic prepaid card information; and

an over the air (OTA) provisioning server for receiving the electronic prepaid card information from the merchant server, establishing a communications link with a mobile device associated with address data included in the prepaid card information, and provisioning the electronic prepaid card information to the mobile device over the communications link via over the air (OTA) communications.

11. The system of claim 10 wherein the electronic prepaid card information includes personalization data that is used to generate a softcard prepaid card in the mobile device.

12. The system of claim 10 wherein the electronic prepaid card information comprises a prepaid card authorization code.

13. The system of claim 10 wherein the OTA provisioning server is further configured to send a control short message service (SMS) message to the mobile device associated with the address data included in the prepaid card information, and receive, from the mobile device, an electronic prepaid card download request for the electronic prepaid card information.

14. The system of claim 10 wherein the OTA provisioning server is further configured to upload the electronic prepaid card information to the mobile device as a prepaid softcard and personalization data.

15. The system of claim 14 wherein the personalization data is uploaded to a secure element in the mobile device.

16. The system of claim 10 wherein the OTA provisioning server is further adapted to send a message to the merchant server indicating the successful delivery of the electronic prepaid information to the mobile device.

17. The system of claim 16 wherein the merchant server is further adapted to send a message to the original purchaser of the prepaid card from the merchant server indicating a successful delivery of the electronic prepaid information to the mobile device.

18. The system of claim 1 wherein the mobile device is adapted to transfer the personalization data to a wireless device reader in order to conduct a payment transaction.

19. The system of claim 16 wherein the confirmation message includes at least one of an SMS message and an email message.

20. The system of claim 17 wherein the confirmation message includes a purchase receipt.

21. A computer readable medium having stored thereon comprising computer executable instructions that when executed by a processor of a computer performs steps comprising:

receiving, at a merchant server, purchase information related to the purchase of an electronic prepaid card;

receiving, from the merchant server, electronic prepaid card information derived from the purchase information;

establishing a communications link with a mobile device associated with address data included in the electronic prepaid card information; and

provisioning the electronic prepaid card information on the mobile device over the communications link via over the air (OTA) communications.

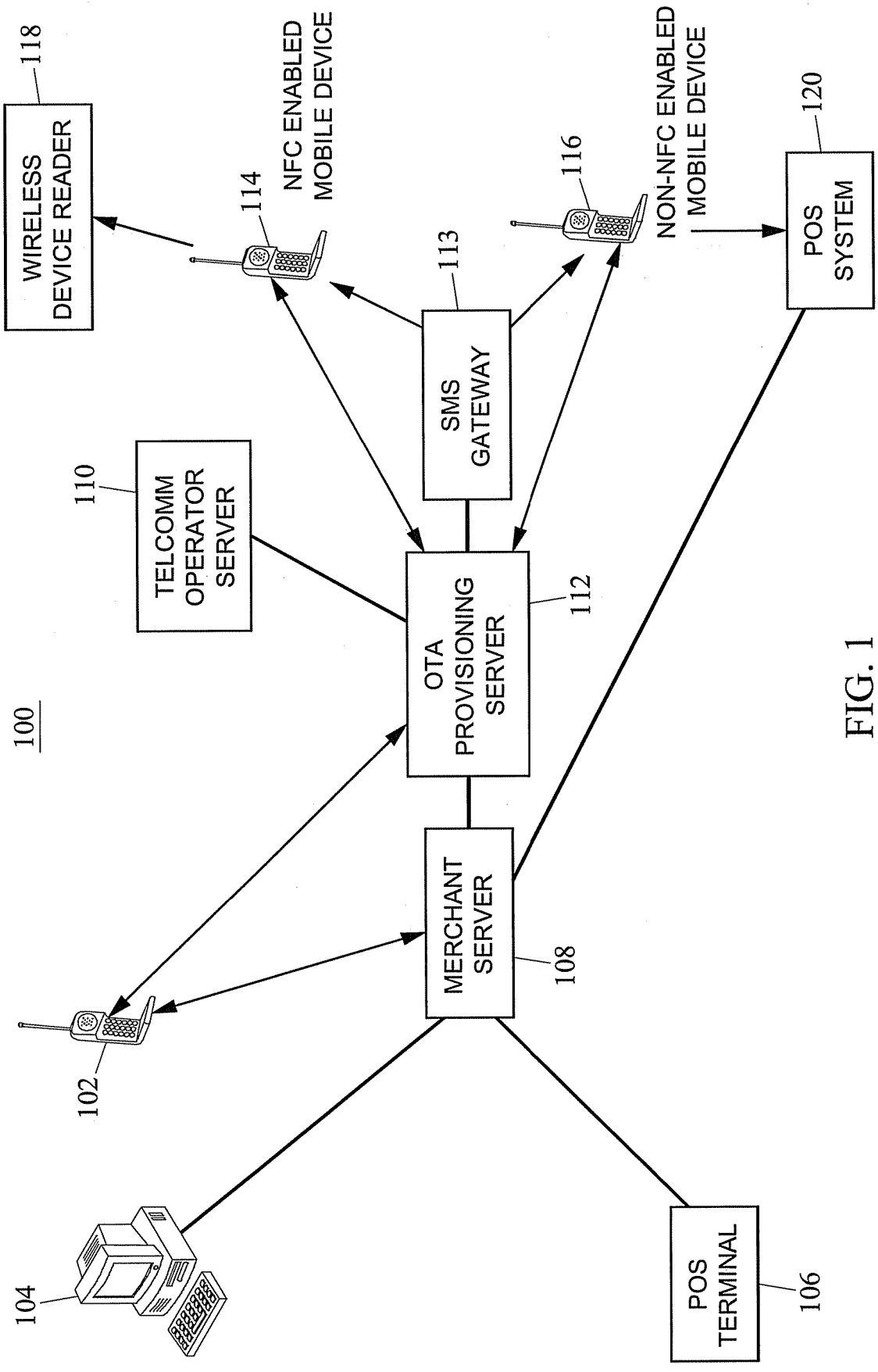
100
102
104
106
108
110
112
113
114
116
118
120
WIRELESS DEVICE READER
NFC ENABLED MOBILE DEVICE
NON-NFC ENABLED MOBILE DEVICE
POS SYSTEM
SMS GATEWAY
TELCOMM OPERATOR SERVER
OTA PROVISIONING SERVER
MERCHANT SERVER
POS TERMINAL

FIG. 1

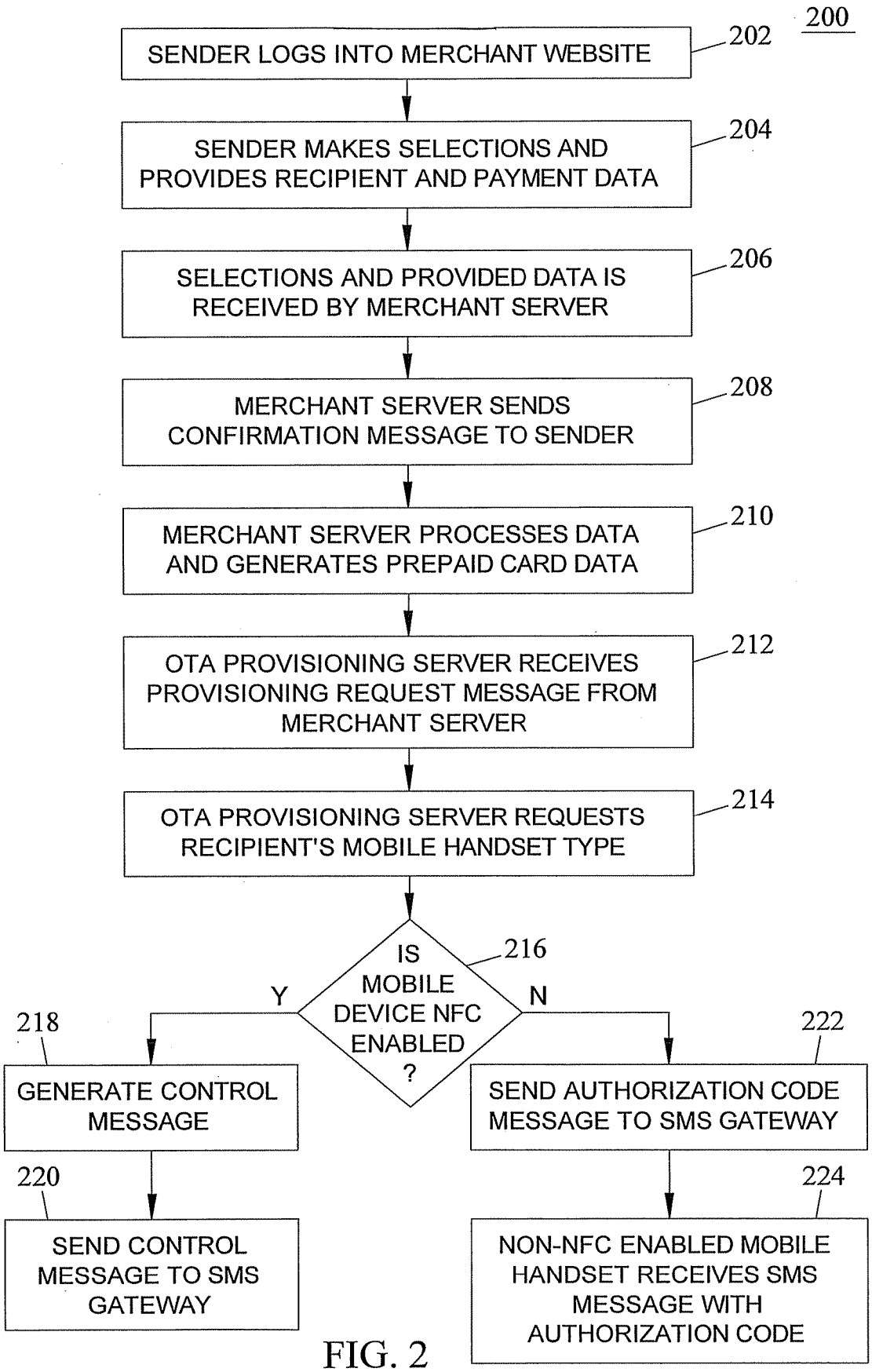
200
SENDER LOGS INTO MERCHANT WEBSITE
202
SENDER MAKES SELECTIONS AND PROVIDES RECIPIENT AND PAYMENT DATA
204
SELECTIONS AND PROVIDED DATA IS RECEIVED BY MERCHANT SERVER
206
MERCHANT SERVER SENDS CONFIRMATION MESSAGE TO SENDER
208
MERCHANT SERVER PROCESSES DATA AND GENERATES PREPAID CARD DATA
210
OTA PROVISIONING SERVER RECEIVES PROVISIONING REQUEST MESSAGE FROM MERCHANT SERVER
212
OTA PROVISIONING SERVER REQUESTS RECIPIENT'S MOBILE HANDSET TYPE
214
IS MOBILE DEVICE NFC ENABLED ?
216
Y
N
218
GENERATE CONTROL MESSAGE
220
SEND CONTROL MESSAGE TO SMS GATEWAY
222
SEND AUTHORIZATION CODE MESSAGE TO SMS GATEWAY
224
NON-NFC ENABLED MOBILE HANDSET RECEIVES SMS MESSAGE WITH AUTHORIZATION CODE

FIG. 2

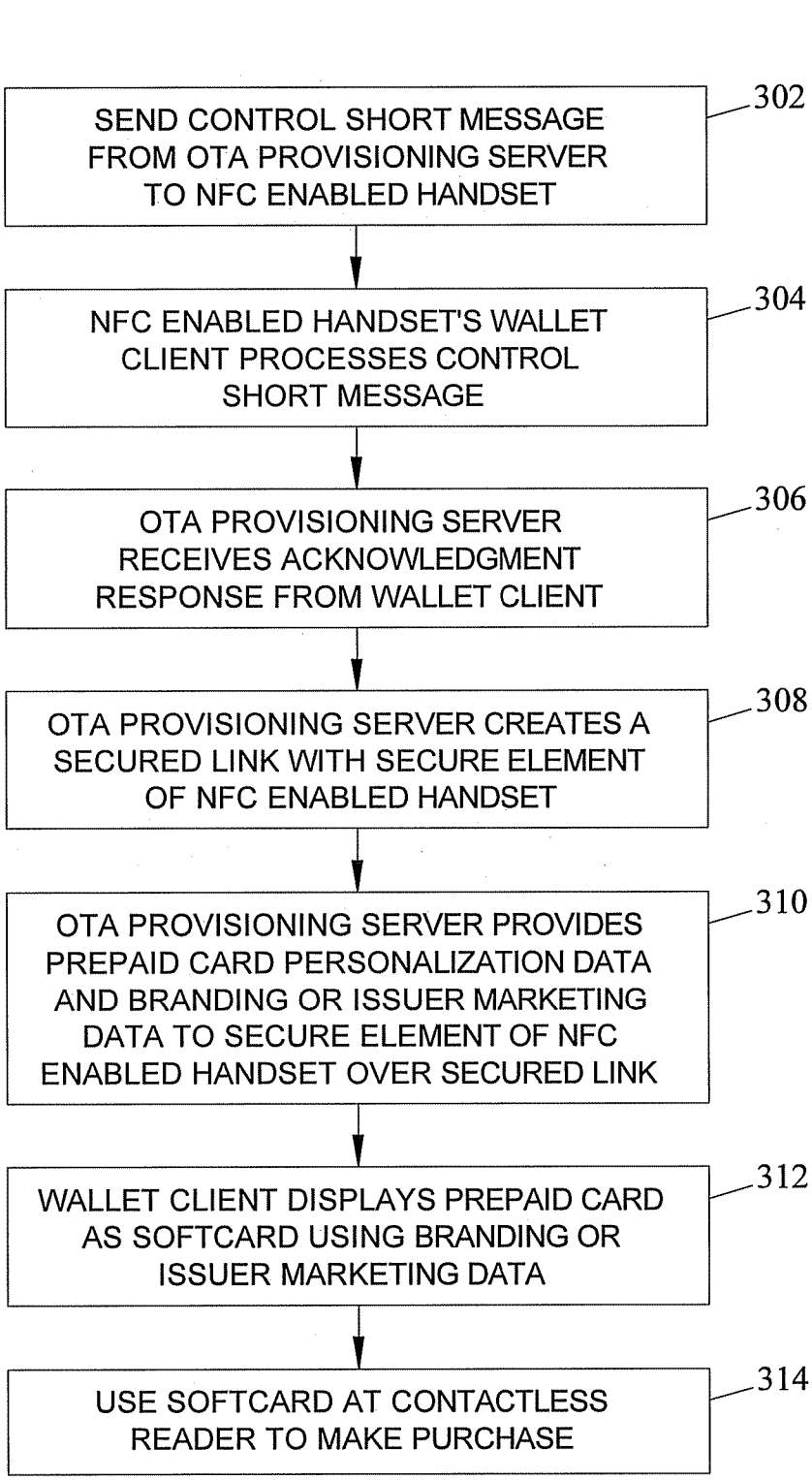
300
SEND CONTROL SHORT MESSAGE FROM OTA PROVISIONING SERVER TO NFC ENABLED HANDSET
302
NFC ENABLED HANDSET'S WALLET CLIENT PROCESSES CONTROL SHORT MESSAGE
304
OTA PROVISIONING SERVER RECEIVES ACKNOWLEDGMENT RESPONSE FROM WALLET CLIENT
306
OTA PROVISIONING SERVER CREATES A SECURED LINK WITH SECURE ELEMENT OF NFC ENABLED HANDSET
308
OTA PROVISIONING SERVER PROVIDES PREPAID CARD PERSONALIZATION DATA AND BRANDING OR ISSUER MARKETING DATA TO SECURE ELEMENT OF NFC ENABLED HANDSET OVER SECURED LINK
310
WALLET CLIENT DISPLAYS PREPAID CARD AS SOFTCARD USING BRANDING OR ISSUER MARKETING DATA
312
USE SOFTCARD AT CONTACTLESS READER TO MAKE PURCHASE
314

FIG. 3

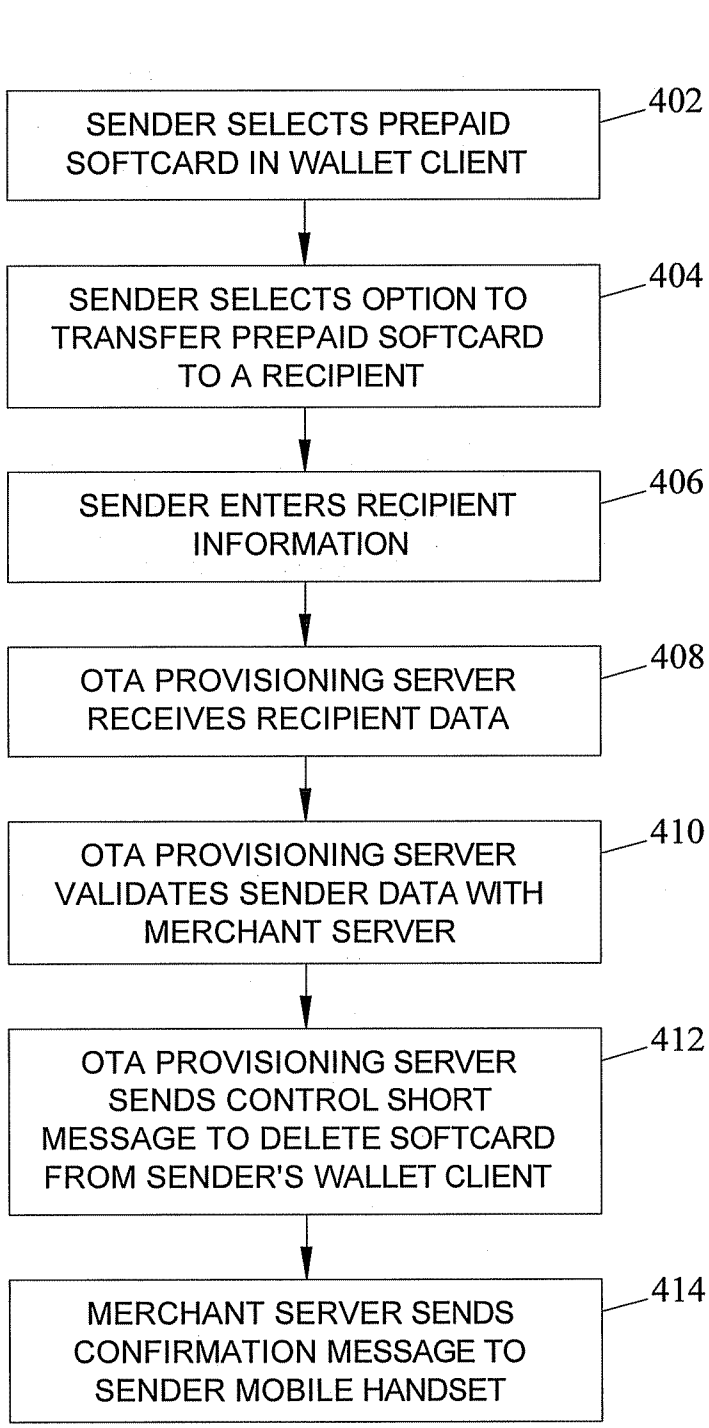
400
SENDER SELECTS PREPAID SOFTCARD IN WALLET CLIENT
402
SENDER SELECTS OPTION TO TRANSFER PREPAID SOFTCARD TO A RECIPIENT
404
SENDER ENTERS RECIPIENT INFORMATION
406
OTA PROVISIONING SERVER RECEIVES RECIPIENT DATA
408
OTA PROVISIONING SERVER VALIDATES SENDER DATA WITH MERCHANT SERVER
410
OTA PROVISIONING SERVER SENDS CONTROL SHORT MESSAGE TO DELETE SOFTCARD FROM SENDER'S WALLET CLIENT
412
MERCHANT SERVER SENDS CONFIRMATION MESSAGE TO SENDER MOBILE HANDSET
414

FIG. 4