



(51) International Patent Classification:
G06Q 20/04 (2012.01) *H04B 5/02* (2006.01)
G06Q 20/34 (2012.01)

(21) International Application Number:
PCT/US2013/047495

(22) International Filing Date:
25 June 2013 (25.06.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/621,474 17 September 2012 (17.09.2012) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, California 95054 (US).

(72) Inventors: ADRANGI, Farid; 4289 Orchard Way, Lake Oswego, Oregon 97035 (US). LORTZ, Victor B.; 7716 SW Oviatt Drive, Beaverton, Oregon 97007 (US).

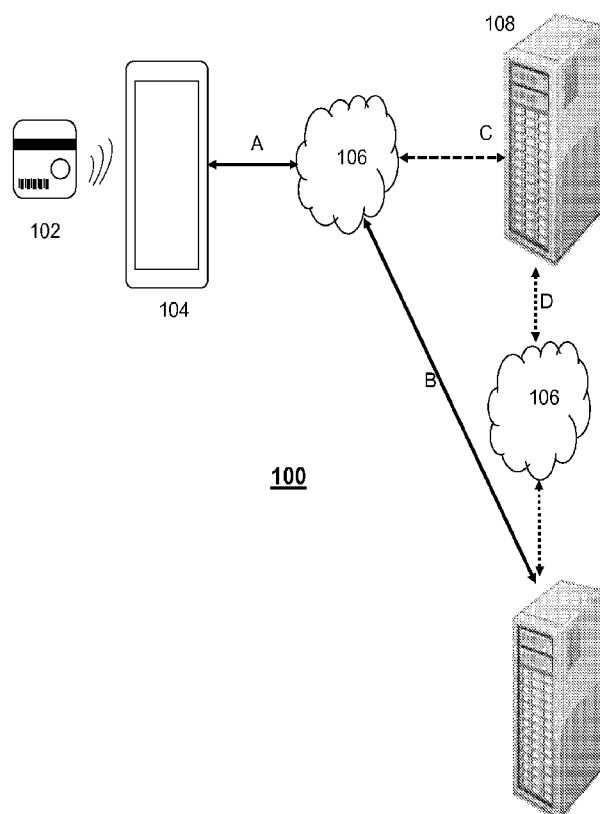
(74) Agent: HERNANDEZ, E. Rico; Pillsbury Winthrop Shaw Pittman LLP, P.O. Box 10500, McLean, Virginia 22102 (US).

(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, BN, 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, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[Continued on next page]

(54) Title: NEAR FIELD CONTACTLESS SYSTEM AND METHOD FOR ONLINE TRANSACTIONS



(57) Abstract: Systems, methods, and apparatuses are directed to conducting online transactions by virtue of a near field communication (NFC) reading mechanism configured to contactlessly read NFC-compliant provisioning information including a monetary value. Moreover, logic is configured to initiate establishment of a communication link, automatically send a request message to confirm the read provisioning information via the communication link, store at least a portion of the provisioning information in a secure memory unit, and based on the confirmation of the provisioning information, automatically present on a display unit, the monetary value, selectable transaction options, and an online information resource link to accommodate execution of a selected transaction option.



MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK,
SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ,
GW, KM, ML, MR, NE, SN, TD, TG).

— *as to the applicant's entitlement to claim the priority of
the earlier application (Rule 4.17(iii))*

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted
a patent (Rule 4.17(ii))*

Published:

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

NEAR FIELD CONTACTLESS SYSTEM AND METHOD FOR ONLINE TRANSACTIONS

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit to U.S. application no. 13/621,474 filed on September 17, 2012, the entire contents of which are incorporated herein by reference.

TECHNICAL FIELD

[0002] This disclosure relates generally to the field of data processing/communications, and in particular, to near field communications directed to online transactions.

BACKGROUND ART

[0003] Given consumer convenience, card-based currency, such as, for example, prepaid cards, gift cards, reward cards, loyalty cards, redeeming coupons, discount vouchers, etc., is fast becoming a preferred medium for consummating transactions of goods and services.

[0004] Generally, such card-based currency includes a unique identifier printed in small font on the card encoded in a barcode and/or magnetic strip. In addition, such cards may also contain a scratch-off or peel-away portion concealing a PIN code to be inputted by the consumer.

[0005] In using such a card for online transactions, users must first find, via a computer, the web page of a retailer's online store, launch the webpage, and then navigate through retailer's website to find the gift card area. To check the balance/value of the card or use the gift card online, the user must manually enter into the retailer web page, the long string of digits of the identifier printed on the gift card as well as the scratch-off/peel-away concealed PIN code.

[0006] These user steps are susceptible to errors if the user enters the online retailer Uniform Resource Locator (URL) incorrectly in addition to being susceptible to a variety phishing attacks if malware, such as, a key logger, is running in the background of the user computer.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] FIG. 1 depicts a high-level functional block diagram of an NFC contactless system conducting online transactions, in accordance with various aspects of the present disclosure.

[0008] FIG. 2 depicts a high-level functional block diagram of an NFC device, in accordance with various aspects of the present disclosure.

[0009] FIG. 3 depicts a high-level functional block diagram of an NFC-enabled reading device, in accordance with various aspects of the present disclosure.

[0010] FIG. 4 depicts a high-level flow diagram of a process for conducting online transactions based on an NFC contactless system, in accordance with various aspects of the present disclosure.

DETAILED DESCRIPTION

[0011] In the description that follows, like components have been given the same reference numerals, regardless of whether they are shown in different embodiments. To illustrate an embodiment(s) of the present disclosure in a clear and concise manner, the drawings may not necessarily be to scale and certain features may be shown in somewhat schematic form. Features that are described and/or illustrated with respect to one embodiment may be used in the same way or in a similar way in one or more other embodiments and/or in combination with or instead of the features of the other embodiments.

[0012] In accordance with various embodiments of this disclosure, what is proposed is an electronic device and system for conducting online transactions that includes a display unit, a secure memory unit, a near field communication (NFC) reading mechanism configured to contactlessly read NFC-compliant provisioning information including a monetary value and logic configured to: (a) initiate establishment of a communication link, (b) automatically send a request message to confirm the read provisioning information via the communication link, (c) store at least a portion of the provisioning information in the

secure memory unit, and (d) based on the confirmation of the provisioning information, automatically present on the display unit, the monetary value, selectable transaction options, and an online information resource link to accommodate execution of a selected transaction option.

[0013] In another embodiment, a method for conducting online transactions is presented that includes contactlessly reading near field communication (NFC)-compliant provisioning information that includes a monetary value, initiating establishment of a communication link, automatically sending a request message to confirm the read provisioning information via the communication link, storing at least a portion of the provisioning information in a secure memory unit, automatically presenting, on a display unit, the monetary value, selectable transaction options, and an online information resource interface to accommodate execution of a selected transaction option, in response to the confirmation of the provisioning information.

[0014] These and other features and characteristics, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of claims. As used in the specification and in the claims, the singular form of “a”, “an”, and “the” include plural referents unless the context clearly dictates otherwise.

[0015] FIG. 1 depicts a high-level functional block diagram of a near field communication-based (NFC) contactless system 100 for conducting online transactions, in accordance with various aspects of the present disclosure. NFC is a short-range wireless connectivity technology that provides digital communication between NFC-enabled devices by touching them together or placing them within a close proximity to each other (e.g., approximately two inches). As specified by the ISO/IEC 18092 and related standards, a

communication link is established between two NFC-capable devices when the distance between them is approximately 0-4 cm, although distances of up to about 20 cm is contemplated. NFC devices typically operate at a frequency of 13.56 MHz and may transfer data at rates up to 424 Kbs, although data transfer rates of up to 2 Mbps is contemplated.

[0016] As illustrated, system 100 includes NFC device 102, NFC reading-enabled electronic device 104 having bi-directional NFC communication capabilities, and at least one retail transaction source or provider 110. As discussed in greater detail below, system 100 is configured to provide a secure online transaction based on information provided by a contactless NFC device 102.

[0017] In the embodiment depicted in FIG. 1, NFC device 102 is in the form of a card. It will be appreciated that device 102 may equally take the form of a wristband, sticker, banner, key fob, or other suitable media, consistent with the disclosed embodiments. It will also be appreciated that NFC device 102 may operate as a prepaid card, gift card, reward card, loyalty card, coupon, discount voucher, or other redeemable certificate having an associated monetary value.

[0018] Moreover, NFC device (card) 102 is provisioned by a retail provider with a separate NFC-concealed card ID/number that is different from the NFC card number printed on NFC card 102, for security reasons. Each NFC card 102 also includes a scratch-off/peel-away concealed PIN code, which is to be used during online transactions. It will also be appreciated that a secret functionally corresponding to the concealed PIN code may be established and communicated to the user through alternative means, such as being sent in an SMS, email, or printed on a receipt when the NFC card is first activated at purchase time. The main requirement is that this additional secret "PIN" cannot be read via NFC. Furthermore, NFC cards 102 initially have zero balance until provisioned at purchase time. When the NFC card 102 is purchased, the value is credited to the account associated with the purchased NFC card 102 by storing the value in the retail provider server 110 facilities.

[0019] To this end, FIG. 2 depicts NFC device (card) 102 in greater detail, in accordance with in accordance with various aspects of the present disclosure. In particular, NFC card 102 includes NFC tag 208, scratch-off/peel-away concealed PIN code 204 and may

additionally include magnetic strip 202 and/or barcode 206. NFC tag 208 comprises a microchip including a processing device 210, a storage device 212, a transceiver device 214, and an antenna device 216. The NFC tag 208 is typically configured as a passive device (i.e., lacking its own power source) and is energized by being inductively coupled, via antenna device 216, to the magnetic field generated by the radio frequency (RF) signal transmitted by a proximally situated NFC reading device (e.g., NFC reading-enabled electronic device 104). As noted above, the RF transmitted signal may operate at 13.56 MHz in accordance with ISO/IEC 18092 standards.

[0020] The NFC processing device 210 and storage device 212 of NFC card 102 are coupled to NFC transceiver device 214. Storage device 212 may be configured as volatile or non-volatile memory and may store retailer-based transaction provisioning information, such as, for example, retailer data, URL access data, value data, NFC-concealed card ID data, security data etc. The retailer-based transaction provisioning information may be formatted in accordance with NFC standards to ensure effective recognition and interactions with retail provider server(s) 110.

[0021] NFC transceiver device 214 is configured to transmit the provisioning information from storage device 212, under the command of processing device 210, in response to establishing a communication link with a compatible NFC reading device (e.g., NFC reading-enabled electronic device 104). By way of illustration, NFC standards specify storage capacities of up to 4MBytes and as noted above, data transfer data rates up to 424 kbit/s. However, it will be appreciated that the embodiments disclosed herein are not limited to the operating parameters noted above, as the disclosed configuration may operate at RF frequencies other than 13.56 MHz, provide for storage capacities lesser than or greater than 4Mbytes, and communicate at data rates less than or greater than 424 kbit/s.

[0022] Returning back to FIG. 1, upon bringing NFC card 102 within proximity (i.e., tapping distance) of NFC reading-enabled electronic device 104, device 104 is configured to energize NFC card 102, establish a communication link with NFC card 102, and read the transaction provisioning information from NFC card 102. NFC reading-enabled electronic device 104 may represent any of a number of electronic and/or computing devices, both

wireless and wired. As such, NFC reading-enabled electronic device 104 may comprise desktops, laptops, mobile devices, smart phones, gaming devices, tablet computers, etc.

[0023] As depicted in greater detail, FIG. 3 illustrates a high-level functional block diagram of NFC reading-enabled electronic device 104, in accordance with various aspects of the present disclosure. In the illustrative example, reading-enabled electronic device 104 includes a variety of peripherals, such as, for example, display screen 304, speaker 306, microphone 308, camera 310, input devices 312, as well as memory 314, a Trusted Platform Module (TPM) chipset 315, communication module 316, antenna 318, and a system-on-chip (SoC) chipset 320. NFC reading-enabled electronic device 104 may also include a bus infrastructure and/or other interconnection means to connect and communicate information between various components of device 104.

[0024] In some embodiments, SoC 320 may be part of a core processing or computing unit of NFC reading-enabled electronic device 104, and is configured to receive and process input data and instructions, provide output and/or control other components of device 104 in accordance with embodiments of the present disclosure. SoC 320 may include a microprocessor, a memory controller, a memory and other components. The microprocessor may further include a cache memory (e.g., SRAM), which along with the memory of SoC 320 may be part of a memory hierarchy to store instructions and data. The microprocessor may also include one or more logic modules such as a field programmable gate array (FPGA) or other logic array. Communication between the SoC 320's microprocessor and memory may be facilitated by the memory controller (or chipset), which may also facilitate communication with peripheral components 302.

[0025] Memory 314 of NFC reading-enabled electronic device 104 may be a dynamic storage device coupled to the bus infrastructure and configured to store information, instructions, and programs, such as NFC device transaction manager application 325, to be executed by processors of SoC 320 and/or other processors (or controllers) associated with device 104. Some of all of memory 314 may be implemented as Dual In-line Memory Modules (DIMMs), and may be one or more of the following types of memory: Static random access memory (SRAM), Burst SRAM or SynchBurst SRAM (BSRAM), Dynamic

random access memory (DRAM), Fast Page Mode DRAM (FPM DRAM), Enhanced DRAM (EDRAM), Extended Data Output RAM (EDO RAM), Extended Data Output DRAM (EDO DRAM), Burst Extended Data Output DRAM (BEDO DRAM), Enhanced DRAM (EDRAM), synchronous DRAM (SDRAM), JEDEC SRAM, PCIOO SDRAM, Double Data Rate SDRAM (DDR SDRAM), Enhanced SDRAM (ESDRAM), SyncLink DRAM (SLDRAM), Direct Rambus DRAM (DRDRAM), Ferroelectric RAM (FRAM), or any other type of memory device. Device 104 may also include read only memory (ROM) and/or other static storage devices coupled to the bus infrastructure and configured to store static information and instructions for processors of SoC 320 and/or other processors (or controllers) associated with device 104.

[0026] Trusted Platform Module (TPM) chipset 315 comprises a security device that stores computer-generated keys for encryption. It is a hardware-based solution intended to prevent the hacking of key entries, passwords, encryption keys, and other sensitive data. TPM chipset 315 may comprise core root of trust measurement (CRTM) module, encryptor module, decryptor module, key generator, a random number generator (RNG), hash engine, and platform configuration registers (PCRs). In one embodiment, the TPM chipset 315 is coupled to associated processors, via the bus infrastructure, or may alternatively be integrated into SoC 320.

[0027] Communication module 316 includes NFC interface 317 which comprises transceiver, transponder, modulation/demodulation, and memory circuitry, configured to wirelessly communicate and transmit/receive information, via the generated RF signal, upon establishing an NFC communication link with NFC card 102. Moreover, as discussed in further detail below, upon establishing the NFC communication link, NFC interface 317 initiates the launching of NFC device transaction manager logic/application 325 which facilitates the secure online transaction based on information provided by contactless NFC card 102.

[0028] Returning to FIG. 1, upon establishing the NFC communication link between NFC card 102 and NFC reading-enabled electronic device 104, NFC reading-enabled electronic device 104 is configured to read the retailer-based transaction provisioning information stored by NFC card 102. As noted above, such provisioning information may include, for

example, formatted retailer data, retailer URL access data, value data, NFC-concealed card ID data, account data, security data, etc.

[0029] Upon reading the provisioning information stored by NFC card 102, NFC interface 317 of NFC reading-enabled electronic device 104 notifies NFC device transaction manager application 325 to initiate the launching of the application 325. NFC device transaction manager application 325 is configured to examine the formatted provisioning information and determine the nature of the transaction and identity of the retail provider. In one embodiment, for example, NFC device transaction manager application 325 examines URL data (or a portion thereof), card ID number data and/or account data contained in the read provisioning information to determine which server (i.e., secure retail transaction provider 110) to contact that is affiliated with NFC card 102 or the associated account.

[0030] The NFC device transaction manager application 325 may store the read provisioning information in memory and in some embodiments may also store provisioning information from previously-seen gift cards and additional information associated with the owner of NFC reading-enabled electronic device 104, such as user name and mailing address, that may be relevant to consummating online transactions. In some embodiments, NFC device transaction manager application 325 or other software applications on the NFC reading-enabled electronic device 104 may be pre-configured with specific base URLs of affiliated merchants so that it can appropriately respond to relevant cards while ignoring other NFC cards or devices that store URLs for purposes other than a specific online transaction (i.e., gift/loyalty card redemption).

[0031] In some embodiments, confidential or sensitive information, including some or all aspects of the combination of provisioning information and user information, may be protected by NFC processing component, such as, for example, Trusted Platform Module (TPM) chipset 315, that reads the provisioning information and stores it along with additional security information, such as a PIN code, in a protected memory region to protect the NFC card 102 ID number from exposure to any malware that might be running on NFC reading-enabled electronic device 104.

[0032] As noted above, once the NFC device transaction manager application 325 examines the read provisioning information of NFC card 102 and determines which secure retail transaction provider server 110 is associated with the information, it triggers NFC reading-enabled electronic device 104 to automatically (i.e., without user intervention) contact server 110 directly via network 106 with a request for confirmation and/or information regarding NFC card 102, as indicated by route A-B in FIG. 1. The communication mechanism and network are not intended to be limiting in any way, as the communications could be based on one or more standards and protocols including, but not limited to, Ethernet, Wi-Fi, Wi-Gi, Bluetooth, GSM, CDMA, GPRS, 3G or 4G (e.g., WiMAX, LTE) cellular standards, Wireless USB, satellite communication, etc. and the network 106 may comprise the Internet or any suitable network, such as intranets, extranets, etc. In some embodiments, for example, the request may be transmitted over an established secure communication link, such as, for example, a secure tunnel (e.g., SSL) setup between NFC card 102 and retail provider server 110.

[0033] In response to the request by NFC reading-enabled electronic device 104, retailer provider server 110 provides confirmation of the account and related information, such as the value or current balance of the account associated with NFC card 102, via the networked communications. Armed with the responsive value/balance information, NFC device transaction manager application 325 enables NFC reading-enabled electronic device 104 to display the value/balance information and retail provider's online transaction link information to the user via display screen 304. In some embodiments, NFC device transaction manager application 325 may also present user-selectable options, such as, for example: (1) go to online store, (2) add to the card balance, (3) save card information for future reference.

[0034] If the "go to online store" option is selected by the user, the NFC reading-enabled electronic device 104 opens the associated link and connects to the online portal of the retail provider, based on the read URL. In response, retail provider server 110 will open an electronic information resource interface, such as a web-page, designated for online

purchases and/or redemption and proceed with conducting a redeeming or purchase transaction.

[0035] In addition, as a user-selectable sub-option, the NFC reading-enabled electronic device 104 may also furnish the retailer web-page with the NFC card 102 number as well as the user name and address to expedite the checkout process. Furthermore, if the NFC reading-enabled electronic device 104 has any collected any digital coupons that might be relevant to that particular transaction, the digital coupon codes may be presented to the shopping portal at the same time.

[0036] To consummate the purchase/redemption transaction, at the online checkout process, the user will be able to select a gift/loyalty/coupon/voucher card payment option, as provided by the retailer web-page and enter the scratch-off/peel-away concealed PIN code 204 to confirm the transaction. It will be appreciated that, based on the disclosed configuration, there is no need for the user to enter the NFC card number since that information has been confirmed by retailer provider server 110 and may pre-populate and be displayed in a checkout form with asterisks hiding the NFC-concealed card ID data or any portion thereof. Furthermore, NFC device transaction manager application 325 may store and provide the concealed PIN code 204 for subsequent use in online checkout, so that the user will only need to enter it once on electronic device 104 for a particular NFC card.

[0037] With regard to the “add to the card balance” option, again, the initial step is to display the current card balance. To do this, the NFC manager application 325 reads the NFC card 102 number and URL access data and uses the URL to query the current card balance from the retail provider server 110. This balance can be shown to the user on a graphical display so that they can have almost instant access to this information. Because there may be no compelling need to require the user to prove knowledge of the secret PIN code for such a transaction, such a step may be optional and in accord with the retailer policies. If the user decides to add to the card balance, payment via some other means is made to the retail provider server 110. For example, a credit card, bank account, or another gift card can be used with the online connection to add value to the NFC card 102 account.

[0038] With regard to the “save card information for future reference” option, the NFC manager application 325 uses secure memory 314 or the TPM 315 to save information such as the NFC card number, URL access data, secret PIN code, and possibly the user’s personal information such as name and address. With this information saved and protected from malware, the NFC manager application 325 can display and use this information in the future without requiring the user to physically present NFC card 102 again. Thus, if NFC card 102 is lost, stolen, or destroyed for some reason, the associated value can still be preserved and used without having to explain or provide proof of purchase to the retailer.

[0039] As noted above, the NFC-concealed card ID data stored in storage device 212 of NFC card 102 differs from the numbers printed on the card or stored in the card’s magnetic strip for security reasons. It will be appreciated that once the NFC-concealed card ID/number data is stored by NFC reading-enabled electronic device 104, the user can use that stored record for subsequent online transactions or to check the card balance without having to physically touch NFC card 102 again to NFC reading-enabled electronic device 104. In some embodiments, additional options may be presented to the user, such as requests to have the balance of the NFC card 102 transferred to another card/account from the same retail provider or to a virtual card with a different gift card number. This feature allows the user to protect the NFC card 102 value in case it becomes lost or stolen.

[0040] As discussed above, based on the provisioning information, the NFC reading-enabled electronic device 104 may directly contact retail provider server 110 via network 106 with a request for confirmation and/or information, as indicated by route A-B in FIG. 1. In some embodiments, however, it may be beneficial for NFC reading-enabled electronic device 104 to first access and communicate with a trusted, intermediary, third party server 108 prior to communicating with retail provider server 110, as indicated by route A-C-D in FIG. 1.

[0041] By way of illustration, retail provider server 110 may have an arrangement with third party server 108 to provide an array of pre-specified services. The communication link between third party server 108 and retail provider server 110 will preferably be secure. As such, prior to granting access to retail provider server 110 and accepting/responding to

requests from NFC reading-enabled electronic device 104, third party server 108 may perform certain functionality, such as, for example, verifying data integrity, performing virus scans, scanning for malware, comparing security hashes, verifying sources, verifying digital signatures, ensuring database integrity, billing, collections, authenticating users, verifying user contact information, etc., thereby relieving retail provider server 110 from having to perform such functionality.

[0042] In this configuration, retail provider may incorporate NFC card 102 with URL access data to third party server 108, so that third party server 108 may directly receive confirmation/information requests from NFC reading-enabled electronic device 104. The third party server 108 will then process the NFC card 102 provisioning information and then forward the processed information to retail provider server 110 for transaction completion.

[0043] Alternatively, or in addition to, the retail provider server 110 may first receive confirmation/information requests from NFC reading-enabled electronic device 104, as discussed in the previously noted embodiments, and retail provider server 110 may then forward or “bounce” such requests to third party server 108 for processing.

[0044] FIG. 4 depicts a high-level flow diagram of process 400 for conducting online transactions based on an NFC contactless system, in accordance with various aspects of the present disclosure. In block 402, NFC card 102 is brought within proximity of NFC reading-enabled electronic device 104, which results in device 104 energizing NFC card 102 and establishing a communication link between NFC reading-enabled electronic device 104 and NFC card 102, as indicated in block 404.

[0045] In block 406, NFC reading-enabled electronic device 104 reads, via the communication link, the transaction provisioning information stored in the memory of NFC card 102. As noted above, the provisioning information may include retailer data, URL access data, value data, NFC-concealed card ID data, security data etc. In response to the reading of the provisioning information, in block 408, the NFC device transaction manager application 325 residing in NFC reading-enabled electronic device 104, examines the provisioning information that is read, determines which retail transaction provider server

110 is associated with the information, and causes NFC reading-enabled electronic device 104 to forward a request for confirmation/information to the transaction server associated with the account of NFC 102. That is, as discussed above, the provisioning information may include data indicative of contacting/communicating directly with retailer provider server 110 (i.e., provider of the NFC card) or data indicative of contacting/communicating a trusted third party intermediary server 108.

[0046] Based on the information provided in the response to the request by the transaction server, in block 410, NFC device transaction manager application 325 triggers NFC reading-enabled electronic device 104 to display the account balance associated with NFC card 102 and displays retail provider's online transaction link information. The user may also be provided with user-selectable transaction options, such as: (1) go to online store, (2) add to the card balance, (3) save card information for future reference.

[0047] In block 412, it is determined whether the user elects to conduct a purchasing transaction (or redeem) by using NFC card 102. If so, in block 414, the NFC reading-enabled electronic device 104 opens the associated link and connects to the online portal of the retail provider, based on the read URL. In response, retail provider server 110 will open an electronic information resource interface, such as a web-page, designated for online purchases and/or redemption, which is displayed by NFC reading-enabled electronic device 104 and designated for online purchases and/or redemption and provides means for conducting a redeeming or purchase transaction. In addition, as noted above, for a user-selectable transaction options, the NFC reading-enabled electronic device 104 may also furnish the retailer web-page with the NFC card 102 number as well as the user name and address to expedite the checkout process. Furthermore, if the NFC reading-enabled electronic device 104 has any collected any digital coupons that might be relevant to that particular transaction, the digital coupon codes may be presented to the shopping portal at the same time.

[0048] In block 416, to complete the purchase/redemption transaction, during the retailer online checkout process, a gift/loyalty/coupon/voucher card payment option is selected from the retailer web-page and the scratch-off/peel-away concealed PIN code 204

is entered by the user or provided by the NFC device transaction manager application 325 to confirm and complete the transaction.

[0049] Returning to block 412, if the user does not elect to conduct a purchasing transaction/redemption by using NFC card 102, then process 400 progresses to block 418 where it is determined whether the user elects to add value to NFC card 102. If so, in block 420, the user enters information from the account, such as, for example, a credit card, bank account, or another gift card, to pay for and furnish the value to be added to the NFC card 102 account. As noted above, there may be no need to require the user to prove knowledge of the secret PIN code for such a transaction, so such proof may be optional and dependent on retailer policies.

[0050] If the user does not elect to add value to NFC card 102, then process 400 determines whether to save the NFC-related information for future reference, in block 422. If so, in block 424, the NFC manager application 325 uses secure memory 314 or the TPM 315 to store information such as the NFC card 102 number, URL access data, secret PIN code, and possibly the user's personal information such as name and address. With this information saved and protected from malware, the NFC manager application 325 can display and use this information in the future without requiring the user to physically present NFC card 102 again.

[0051] Process 400 then progresses to block 426 where the transaction as well as the communication link is terminated.

[0052] By virtue of the disclosed configurations and processes, a NFC contactless online transaction is achieved that is secure, convenient, and expedient. That is, the disclosed embodiments avoid the manual entry of web addresses and card numbers to effect an online transaction.

[0053] Having thus described the basic concepts, it will be rather apparent to those skilled in the art after reading this detailed disclosure that the foregoing detailed disclosure is intended to be presented by way of example only and is not limiting. Various alterations,

improvements, and modifications will occur and are intended to those skilled in the art, though not expressly stated herein. These alterations, improvements, and modifications are intended to be suggested by this disclosure, and are within the spirit and scope of the exemplary aspects of this disclosure.

[0054] Moreover, certain terminology has been used to describe embodiments of the present disclosure. For example, the terms “one embodiment,” “an embodiment,” and/or “some embodiments” mean that a particular feature, structure or characteristic described in connection with the embodiment is included in at least one embodiment of the present disclosure. Therefore, it is emphasized and should be appreciated that two or more references to “an embodiment” or “one embodiment” or “an alternative embodiment” in various portions of this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures or characteristics may be combined as suitable in one or more embodiments of the present disclosure. In addition, the term “logic” is representative of hardware, firmware, software (or any combination thereof) to perform one or more functions. For instance, examples of “hardware” include, but are not limited to, an integrated circuit, a finite state machine, or even combinatorial logic. The integrated circuit may take the form of a processor such as a microprocessor, an application specific integrated circuit, a digital signal processor, a micro-controller, or the like.

[0055] Furthermore, the recited order of method, processing elements, or sequences, or the use of numbers, letters, or other designations therefore, is not intended to limit the claimed processes and methods to any order except as can be specified in the claims. Although the above disclosure discusses through various examples what is currently considered to be a variety of useful aspects of the disclosure, it is to be understood that such detail is solely for that purpose, and that the appended claims are not limited to the disclosed aspects, but, on the contrary, are intended to cover modifications and equivalent arrangements that are within the spirit and scope of the disclosed aspects.

[0056] Similarly, it should be appreciated that in the foregoing description of embodiments of the present disclosure, various features are sometimes grouped together

in a single embodiment, figure, or description thereof for the purpose of streamlining the disclosure aiding in the understanding of one or more of the various inventive aspects. This method of disclosure, however, is not to be interpreted as reflecting an intention that the claimed subject matter requires more features than are expressly recited in each claim. Rather, as the following claims reflect, inventive aspects lie in less than all features of a single foregoing disclosed embodiment. Thus, the claims following the detailed description are hereby expressly incorporated into this detailed description.

CLAIMS

What Is Claimed Is:

1. An electronic device, comprising:
 - a display unit;
 - a secure memory unit;
 - a near field communication (NFC) reading mechanism configured to contactlessly read NFC-compliant provisioning information including a monetary value; and
 - logic configured to:
 - initiate establishment of a communication link,
 - automatically send a request message to confirm the read provisioning information via the communication link,
 - store at least a portion of the provisioning information in the secure memory unit, and
 - based on the confirmation of the provisioning information, automatically present on the display unit, the monetary value, selectable transaction options, and an online information resource link to accommodate execution of a selected transaction option.
2. The electronic device of claim 1, further comprising an input device configured to enter a selection of a transaction option and a PIN code.
3. The electronic device of claim 1, wherein the NFC-compliant provisioning information comprises one or more of the following: concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, user contact information.

4. The electronic device of claim 3, wherein the NFC-compliant provisioning information is stored in a card, a wristband, sticker, banner, or key fob.

5. The electronic device of claim 1, wherein the secure memory unit comprises a trusted platform module (TPM).

6. The electronic device of claim 1, further comprising a microprocessor, memory controller, and memory integrated on a system-on-chip (SoC) module.

7. The electronic device of claim 1, wherein the selectable transaction options comprise one or more of the following: conducting a purchase transaction, conducting a redemption transaction, adding monetary value to account, saving NFC information for future transactions, application of coupons or vouchers.

8. The electronic device of claim 7 wherein, upon selection of the purchase transaction or redemption transaction, the online information resource link is activated to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the purchase or redemption transaction.

9. The electronic device of claim 7 wherein, upon selection of the adding monetary value to account transaction, the online information resource link is activated to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the adding monetary value transaction.

10. The electronic device of claim 7 wherein, upon selection of the saving NFC information for future transactions, one or more of the concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, user contact information is stored in secure memory to automate subsequent transactions.

11. A system comprising:

a near field communication (NFC) device, including:

a transceiver and antenna, and
a memory device configured to store NFC-compliant provisioning information including a monetary value; and
an electronic device, including:
a display unit;
a secure memory unit;
an NFC reading mechanism configured to contactlessly read NFC-compliant provisioning information including a monetary value from the NFC device; and
logic configured to:
initiate establishment of a communication link,
automatically send a request message to confirm the read provisioning information via the communication link,
store at least a portion of the provisioning information in the secure memory unit, and
based on the confirmation of the provisioning information, automatically present on the display unit, the monetary value, selectable transaction options, and an online information resource interface link to accommodate execution of a selected transaction option.

12. The system of claim 10, further comprising an input device configured to enter a selection of a transaction option and a PIN code.

13. The system of claim 10, wherein the NFC-compliant provisioning information comprises one or more of the following: concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, user contact information.

14. The system of claim 10, wherein the NFC device comprises one of the following: a card, wristband, sticker, banner, or key fob.

15. The system of claim 10, wherein the secure memory unit comprises a trusted platform module (TPM).

16. The system of claim 10, further comprising a microprocessor, memory controller, and memory integrated on a system-on-chip (SoC) module.

17. The system of claim 10, wherein the selectable transaction options comprise one or more of the following: conducting a purchase transaction, conducting a redemption transaction, adding monetary value to account, saving NFC information for future transactions, application of coupons or vouchers.

18. The system of claim 10 wherein, upon selection of the purchase transaction or redemption transaction, the online information resource link is activated to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the purchase or redemption transaction.

19. The system of claim 10 wherein, upon selection of the adding monetary value to account transaction, the online information resource link is activated to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the adding monetary value transaction.

20. The system of claim 10 wherein, upon selection of the saving NFC information for future transactions, one or more of the concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, user contact information is stored in secure memory to automate subsequent transactions.

21. A method comprising:
contactlessly reading near field communication (NFC)-compliant provisioning information that includes a monetary value;
initiating establishment of a communication link;

automatically sending a request message to confirm the read provisioning information via the communication link;

storing at least a portion of the provisioning information in a secure memory unit;

automatically presenting, on a display unit, the monetary value, selectable transaction options, and an online information resource interface link to accommodate execution of a selected transaction option, in response to the confirmation of the provisioning information.

22. The method of claim 21, wherein the NFC-compliant provisioning information comprises one or more of the following: concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, user contact information.

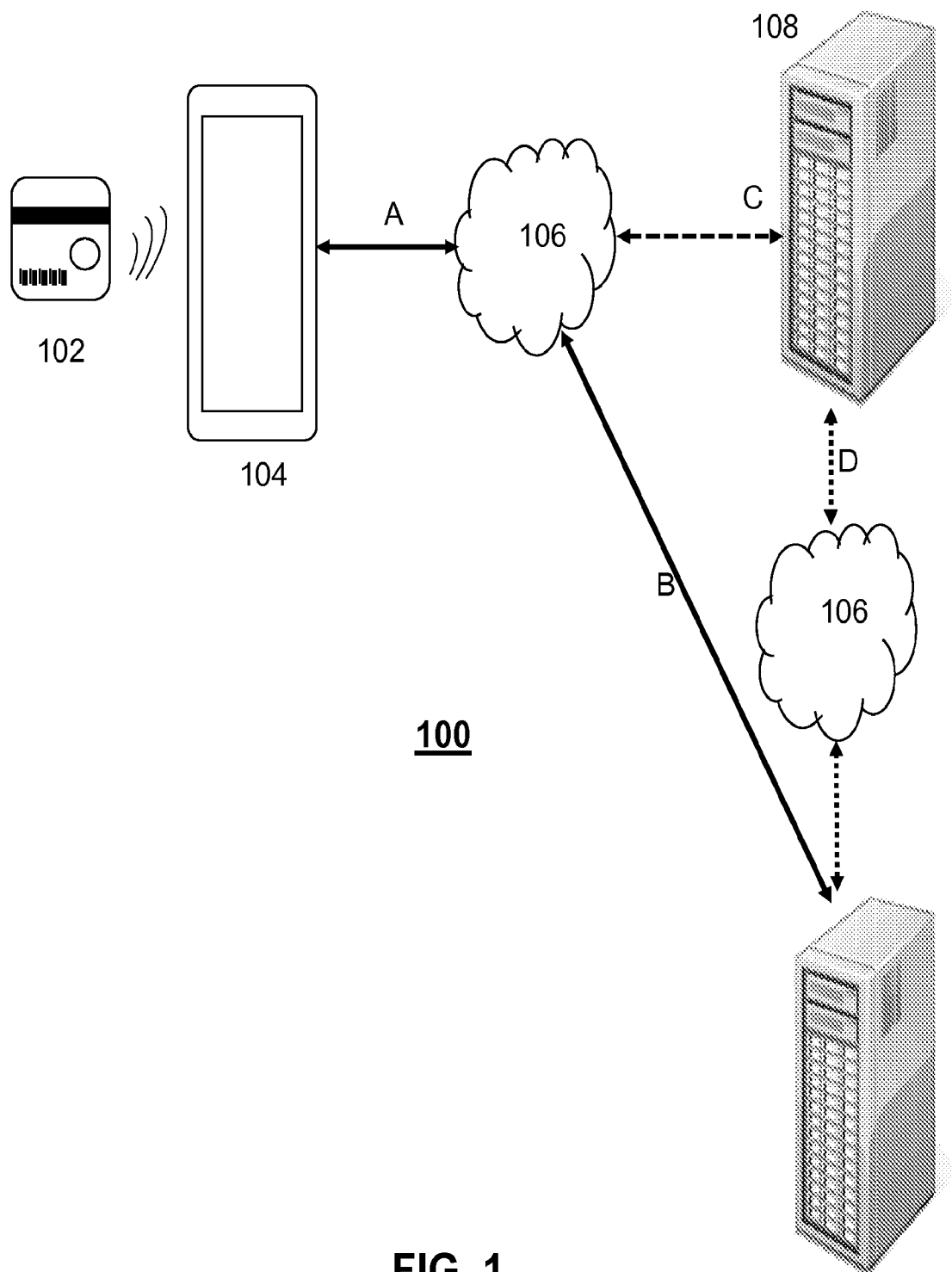
23. The method of claim 21, wherein the selectable transaction options comprise one or more of the following: conducting a purchase transaction, conducting a redemption transaction, adding monetary value to account, saving NFC information for future transactions, application of coupons or vouchers.

24. The method of claim 23, further comprising inputting a selection of a transaction option and a PIN code via an input device.

25. The method of claim 21 wherein, upon selecting the purchase transaction or redemption transaction, activating the online information resource link to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the purchase or redemption transaction.

26. The method of claim 21 wherein, upon selecting the adding monetary value to account transaction, activating the online information resource link to launch a retailer online interface, corresponding to the retailer data of the provisioning information, to accommodate execution of the adding monetary value transaction.

27. The method of claim 21 wherein, upon selecting the saving NFC information for future transactions, storing in secure memory one or more of the concealed NFC ID data, retailer data, retailer URL access data associated with the online information resource interface, monetary value data, account data, security data, secret data, user personal information, to automate subsequent transactions.

**FIG. 1**

102

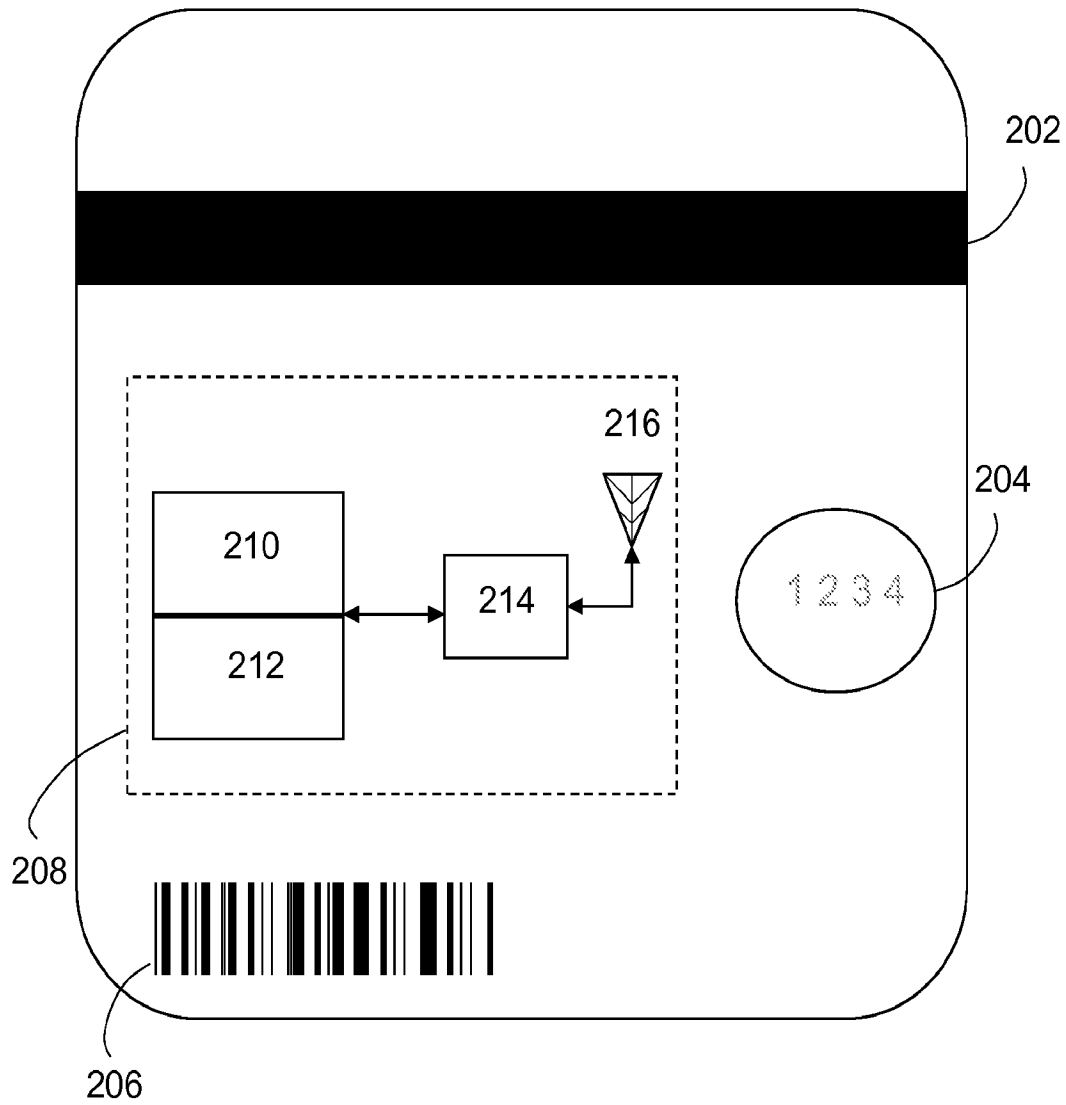
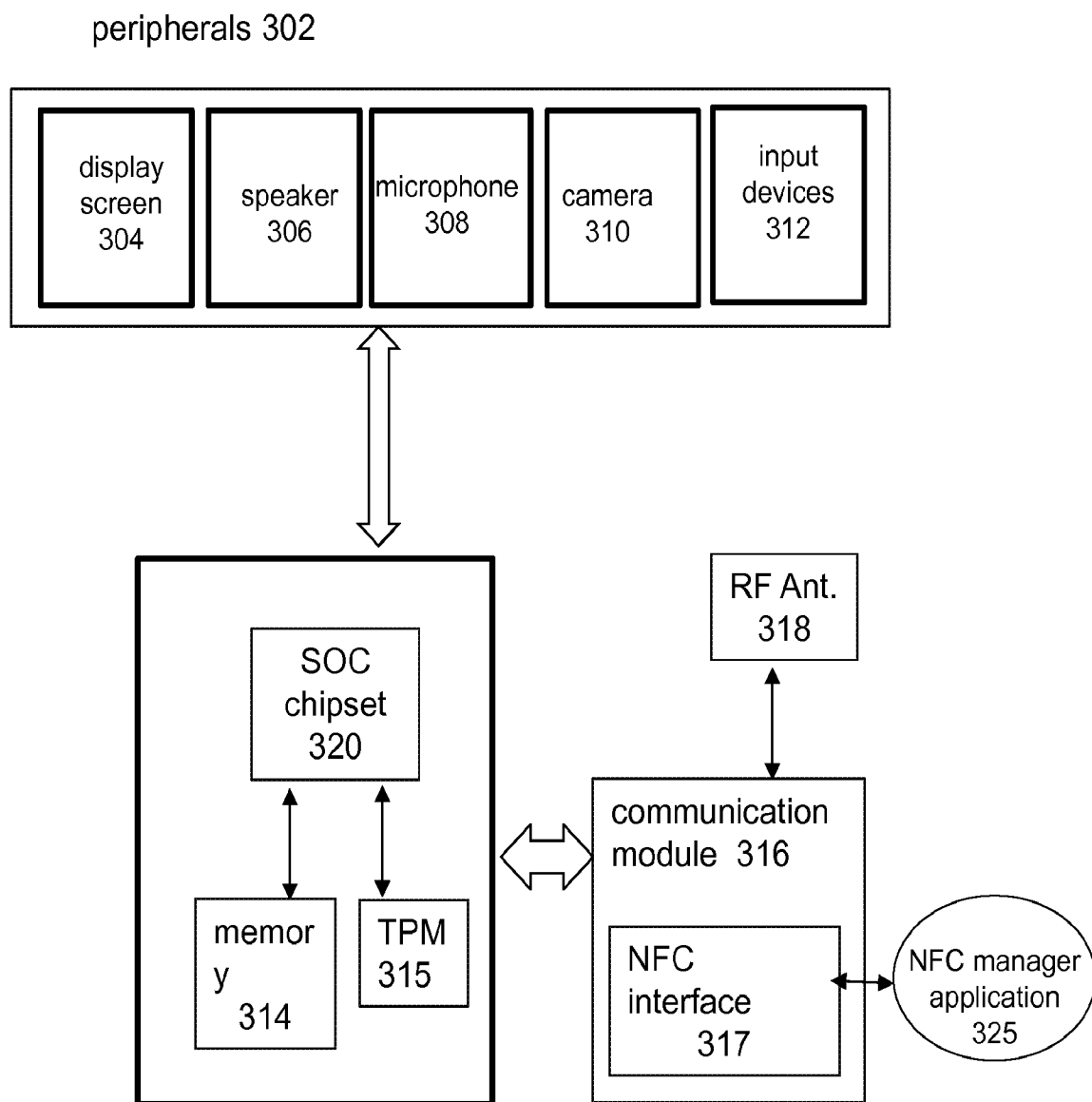


FIG.2

104**FIG. 3**

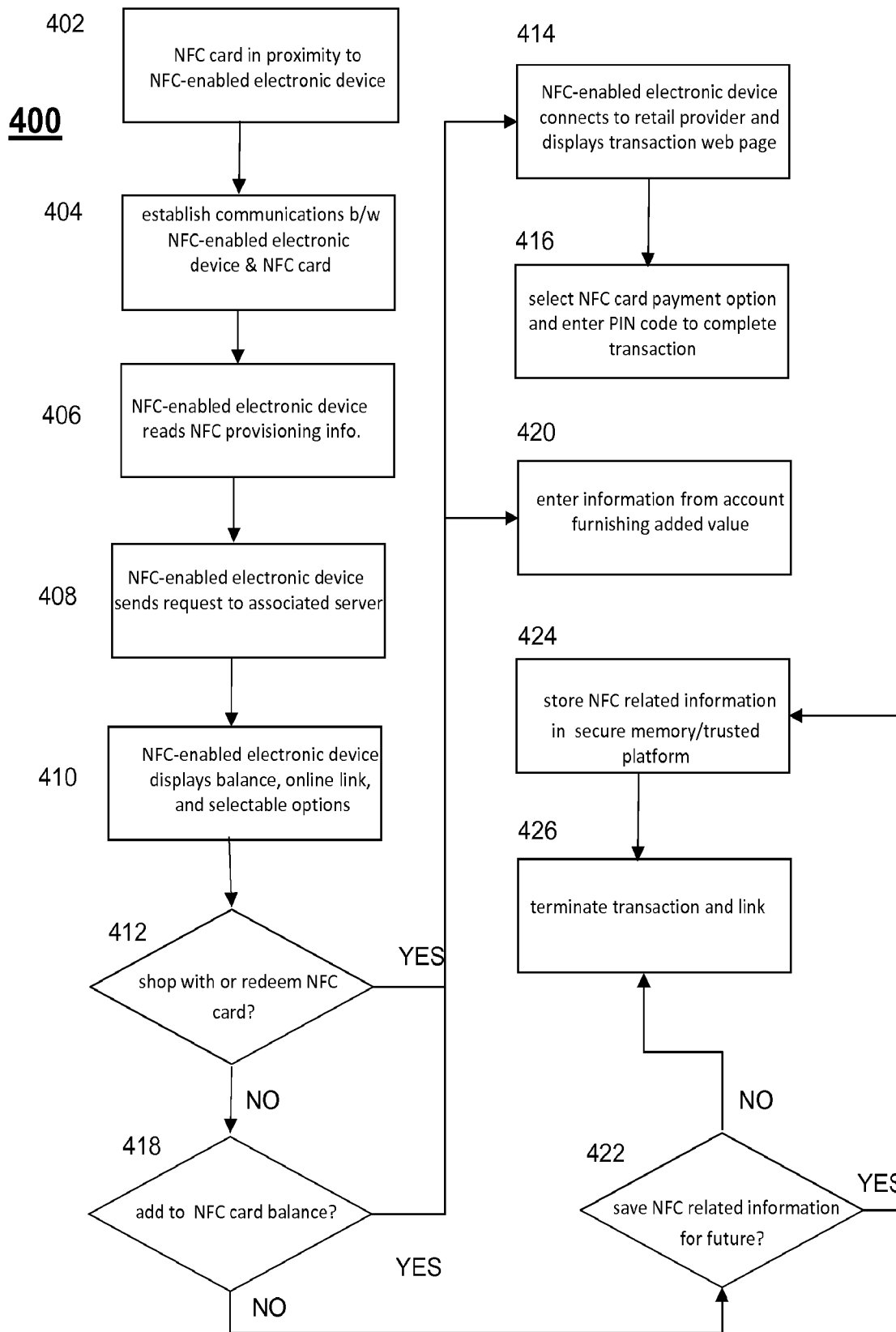


FIG. 4

A. CLASSIFICATION OF SUBJECT MATTER**G06Q 20/04(2012.01)i, G06Q 20/34(2012.01)i, H04B 5/02(2006.01)i**

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q 20/04; G06K 5/00; H04B 5/00; H04W 4/12; G07F 19/00; H04W 4/00; G06K 19/00; G06Q 50/00; H04B 1/40; G06Q 20/34; H04B 5/02

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models

Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: NFC, monetary, transaction, options, link, automatically, display

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2011-0165896 A1 (RUSSEL M. STROMBERG et al.) 07 July 2011 See paragraphs [0021],[0030]-[0031],[0084],[0104], claims 1,16 and figures 1-2.	1-27
Y	KR 10-2008-0073098 A (LG N SYS INC.) 08 August 2008 See paragraph [0056], claims 1,6-7 and figures 1-2,4c.	1-27
Y	US 2010-0294835 A1 (AJAY BAM et al.) 25 November 2010 See abstract, paragraph [0080] and figure 10.	1-27
Y	KR 10-2009-0050437 A (CURRENT NETWORKS INC.) 20 May 2009 See paragraph [0017], claims 1,8 and figures 1,3.	7-10,17-20,23-27
A	US 2009-0170432 A1 (VICTOR LORTZ) 02 July 2009 See abstract, claims 1-6 and figures 3-4.	1-27



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

27 September 2013 (27.09.2013)

Date of mailing of the international search report

30 September 2013 (30.09.2013)

Name and mailing address of the ISA/KR

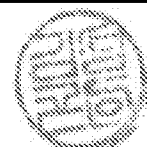
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City,
302-701, Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

KIM Sung Gon

Telephone No. +82-42-481-8746



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2013/047495

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0165896 A1	07/07/2011	WO 2011-084963 A2 WO 2011-084963 A3	14/07/2011 20/10/2011
KR 10-2008-0073098 A	08/08/2008	None	
US 2010-0294835 A1	25/11/2010	CN 102439616 A RU 2011151786 A WO 2010-133753 A1	02/05/2012 27/06/2013 25/11/2010
KR 10-2009-0050437 A	20/05/2009	None	
US 2009-0170432 A1	02/07/2009	CN 101478332 A EP 2077652 A2 EP 2077652 A3 JP 2009-188984 A US 2011-287716 A1 US 8014720 B2 US 8483610 B2	08/07/2009 08/07/2009 18/01/2012 20/08/2009 24/11/2011 06/09/2011 09/07/2013

Referring to the description, it is understood that claims 12-20 are dependent on claim 11. Accordingly, this ISR has been established on the assumption that claims 12-20 refer to claim 11.