



(51) International Patent Classification:

G06Q 20/20 (2012.01) G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01) G06Q 20/40 (2012.01)

(21) International Application Number:

PCT/US2015/029024

(22) International Filing Date:

4 May 2015 (04.05.2015)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

14/286,520 23 May 2014 (23.05.2014) US

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

(72) Inventor: BALLESTEROS, Miguel; 8595 Morgan Creek Lane, Roseville, California 95747 (US).

(74) Agents: ROZMAN, Mark J. et al.; Trop, Pruner & Hu, P.C., 1616 S. Voss Rd., Ste. 750, Houston, Texas 77057-2631 (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, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, 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, SA, 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, ST, 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, 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).

Declarations under Rule 4.17:

- as to the identity of the inventor (Rule 4.17(i))
- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

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

(54) Title: SYSTEM AND METHODS FOR PAYMENT CREDENTIAL-BASED MOBILE COMMERCE

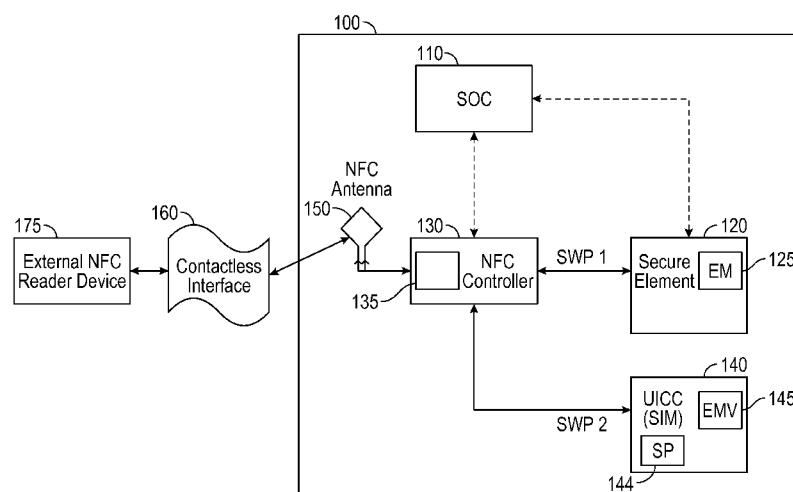


FIG. 1

(57) Abstract: In an embodiment, an apparatus comprises a security processor to perform a secure reader function to emulate an external near field communication (NFC) reader device, to obtain payment credential information of a user, a storage to store secure credential information of the user, and a NFC controller coupled to the security processor and the storage, responsive to initiation of the secure reader function, to disable a NFC contactless interface and to cause the payment credential information to be communicated to a remote system while the first contactless interface is disabled. Other embodiments are described and claimed.

SYSTEM AND METHODS FOR PAYMENT CREDENTIAL-BASED MOBILE COMMERCE

Technical Field

[0001] Embodiments relate to apparatus and techniques for secure processing of transactions.

Background

[0002] Near field communication (NFC)-based solutions are used with mobile devices to pay at a point of sale (POS) terminal as a direct replacement for a credit card or physical chip-based payment card. These solutions rely on NFC and EMV (Europay, MasterCard, Visa) technologies that are common in cellular telephones and contactless chip payment cards. EMV payment cards are recognized as a much higher security solution than traditional magnetic stripe payment cards such as a conventional credit card. While mobile devices having EMV credentials are typically used at a POS, such technologies are not readily adapted to other purchase models.

Brief Description of the Drawings

[0003] FIG. 1 is a block diagram of a portion of a device in accordance with an embodiment.

[0004] FIG. 2 is a sequence diagram for performing a mobile commerce transaction in accordance with an embodiment of the present invention.

[0005] FIG. 3 is a block diagram of a system in accordance with one embodiment of the present invention.

[0006] FIG. 4 is a flow diagram for a mobile commerce transaction method in accordance with another embodiment of the present invention.

[0007] FIG. 5 is a block diagram of a system arrangement in accordance with another embodiment of the present invention.

Detailed Description

[0008] Embodiments provide apparatus and techniques to securely and conveniently use EMV credentials available within a device such as a portable device for mobile commerce, in which a mobile device is used to access a website or

application and perform a transaction to purchase goods/services and remotely execute a payment. More specifically, embodiments enable such commerce to be performed using a device including standard-compliant EMV credentials. Stated another way, currently available EMV credentials, complying with present and future standards such as one or more EMV specifications, e.g., in accordance with the Integrated Circuit Card Specifications for Payment Systems, version 4.3 (November 2011), can be used to perform mobile commerce via a wireless device.

[0009] A mobile wallet, which includes a set of personal financial-based data and embedded technology of a mobile device, relies in part on two components of the device to perform mobile commerce as described herein. These components include a NFC device that has a card emulation mode to emulate a contactless card communications interface and a security processor, also referred to herein as a secure element (SE), that is configured to operate as a smartcard chip. Note that in general, credentials stored in a mobile wallet can only be accessed over a contactless interface (namely a NFC interface) and not from a host (namely an application processor and its software) for security reasons. EMV credentials contain both public and private data, and while the private data is secured and reserved for actual transaction operations, the public data is sensitive in nature (account number, account holder name, expiration date) and in clear text, making it an attractive target for fraudsters were it accessible from host software (e.g., via malware operating on the application processor).

[0010] In some embodiments, a basic security model for EMV payment credential access in a mobile wallet can be applied for mobile commerce by emulating access to the EMV credentials via a contactless interface of the device. To this end, embodiments may provide an internal NFC reader function (that acts as an embedded mobile POS (mPOS) terminal). This internal function may be implemented within appropriate hardware, firmware, software and/or combinations thereof. In one embodiment, the function may be implemented in a security processor of the mobile device. In different implementations, this security processor may be a standalone hardware processor, a fixed function engine such as a security

engine, or integrated within a system on chip (SoC) or other general purpose processor.

[0011] Referring now to FIG. 1, shown is a block diagram of a portion of a device in accordance with an embodiment. As shown in FIG. 1, device 100, which may be a mobile device such as smartphone, tablet computer, e-reader or other portable electronic device, includes a SoC 110 which may act as an application processor for device 100 to perform various applications on behalf of an end user. As seen, SoC 110 couples to a secure element (SE) 120, e.g., via an inter-integrated circuit (I²C) interconnect or a serial peripheral interface (SPI) interconnect. SE 120 may be a dedicated security processor. As such, this security processor may be configured as a separate component from SoC 110. In other embodiments, secure element 120 may be integrated within SoC 110.

[0012] As seen, secure element 120 includes an emulation module 125 which may be used to emulate a POS terminal. As described herein emulation module 125 may operate as a mobile POS terminal or device. In such situations, emulation module 125 performs a secure reader function to read secure information stored within device 100. In an embodiment, emulation module 125 may execute a mobile POS application that can be implemented as a collection of applets to be executed by a Java™-based operating system (OS). Of course, the mPOS device and its functionality may be performed using other combinations of hardware and software, in different embodiments.

[0013] Still referring to FIG. 1, an NFC controller 130 is further coupled both to SoC 110 and secure element 120. Although the scope of the present invention is not limited in this regard, the communication path or interconnect between SoC 110 and NFC 130 may be an I²C or SPI interconnect. NFC controller 130 may be a wireless communication interface to enable a radio frequency (RF) field to be set up to perform NFC-based wireless communications with corresponding NFC devices in close proximity to system 100. In turn, NFC controller 130 may couple to secure element 120 via a single wire protocol (SWP1) connection.

[0014] As further shown, NFC controller 130 also couples to a universal integrated circuit card (UICC) 140 (via a second SWP connection (SWP2)) which in an embodiment may comprise a subscriber identity module (SIM). As further seen, UICC 140 also includes a secure data store 145 in which EMV payment credentials may be stored. Of course understand that various other information may be stored in secure storage 145, which in various embodiments may be implemented as any desired type of non-volatile storage.

[0015] As further illustrated, UICC 140 includes a security processor logic 144, which may execute various security applications, including an EMV application (such as may be stored in non-volatile storage 145) to interact with EMV data by way of performing various cryptographic operations on the EMV data and transaction data. For example in an embodiment, the EMV application may be implemented as a collection of Java™ applets. Such EMV application may take the form, in some embodiments, of a mobile wallet that is used to interact with EMV data and transaction data, using a cryptoprocessor or other security processor of UICC 140 to perform various operations for a given transaction. As an example, the EMV data may include one or more security keys, in addition to other financial and identification information of a user. In turn, incoming transaction information, which may include a transaction identifier, merchant information, transaction amount and so forth, may be cryptographically processed using one or more of the keys to generate secure payment credential information such as a packet or digest that includes the transaction information and user (and user account) information hashed or otherwise cryptographically processed using one or more of the keys to thus generate a packet for communication to a merchant or other entity that in turn can seek to validate this message by interaction with an issuer of the keys, such as a financial institution or other card issuer that provides the EMV data for a given user/customer.

[0016] Still referring to FIG. 1, NFC controller 130 couples to an antenna 150 such as a NFC antenna that enables communication with various wireless devices. For purposes of discussion here assume that for typical contactless payment in a retail situation, mobile device 100 may be in contactless communication with an external NFC reader device 175 such as implemented within a POS terminal. As such, a

contactless interface 160 is realized between antenna 150 and external NFC reader 175. While mobile device 100 enables payment operations using EMV payment credentials stored in UICC 140 via contactless interface 160, understand that in a mobile commerce transaction in accordance with an embodiment, contactless interface 160 may be disabled, e.g., via NFC controller 130, as described further herein. Understand that these mobile commerce transactions may be online transactions between a mobile device and an online merchant, termed herein as an “online mobile transaction.”

[0017] In an embodiment, when an EMV payment credential within device 100 (e.g., embedded within UICC 140) is to be used for purposes of a NFC transaction with a locally available reader device 175 (such as a POS terminal), NFC controller 130 configures, via a router logic 135, the data flow to be between external NFC reader device 175 and UICC 140 such that on proper verification or validation, requested payment information stored in secure data storage 145 may be communicated via contactless interface 160 to external NFC reader device 175.

[0018] Instead, when the EMV payment credential is to be used for purposes of an online mobile commerce transaction, the data flow is not via this contactless interface 160, which router logic 135 disables during such mobile commerce transaction. Instead, a data flow may be between the EMV payment credential stored in UICC 140 and a remote merchant (not shown in FIG. 1). Such communication may be configured via router logic 135 of NFC controller 130 to be between UICC 140 and secure element 120, and thereafter SoC 110 and via another wireless interface of mobile device 100 (not shown for ease of illustration in FIG. 1) such as of a given cellular (e.g., 3G or 4G) or other wireless communication protocol (e.g., a wireless local area network (WLAN) in accordance with a given Institute of Electrical and Electronics Engineers (IEEE) 802.11 specification).

[0019] In this mobile commerce-based data flow, SE 120, via emulation logic 125, emulates an external NFC reader device (e.g., device 175) when secure element 120 establishes an internal NFC reader mode session terminated by UICC 140 operating in the NFC card emulation mode.

[0020] This function is equivalent to an external POS terminal and may be used to initiate an NFC reader mode session marked as internal only so that NFC controller 130 prevents contactless interface 160 from being activated. Instead, NFC controller 130, via an internal interface, routes internally to another NFC node (e.g., UICC 140) that invokes an NFC card emulation mode session. In this way, EMV payment credentials are made available for payment transactions to an internal POS device. NFC controller 130, via router logic 135, thus acts as router and connects UICC 140 to SE 120 (more specifically to enable the EMV data to be provided to emulation logic 125) as if an external NFC reader device had been detected via contactless interface 160.

[0021] Thus a mobile wallet is integrated for mobile commerce usages via an internal mPOS terminal integrated into the device itself. Stated another way, both the mobile wallet and mPOS are present within the mobile device. Assume that a merchant is an online merchant. The interactions take place between UICC 140 and SE 120 via NFC controller 130, instead of any interaction with an external POS terminal. From the integrated mPOS perspective, SE 120 invokes a NFC reader mode marked as EMULATED so that NFC controller 130 operates to detect an internal NFC node operating in the card emulation NFC mode, as opposed to an external NFC card target. As such, contactless interface 160 is not activated at any time.

[0022] Once the mobile wallet is activated and UICC 140 invokes the card emulation NFC mode, NFC controller 130 connects SE 120 and UICC 140, where the EMV credentials are stored. Thereafter, the EMV transaction begins. At the end of the EMV transaction, the SE deactivates the UICC (including the card being emulated), and terminates the NFC reader mode. Finally the online merchant and user are notified of the payment processing completion. From the mobile wallet perspective, there is no difference between an external POS case and this case.

[0023] Referring now to FIG. 2, shown is a sequence diagram for performing a mobile commerce transaction in accordance with an embodiment of the present invention. As shown in FIG. 2, sequence 200 may be used to perform a mobile commerce transaction between a merchant 180, e.g., an online merchant, and a

user 105 of a mobile device 100, which may be configured as shown in FIG. 1. Understand that while a particular information flow is shown in the illustration of FIG. 2, many variations and alternatives are possible. For the mobile commerce transaction, assume that user 105 has accessed a website of merchant 180 in order to purchase a good or service. At a checkout user interface (e.g., a graphical user interface (GUI)), user 105 is requested to input a type of payment method, such as credit card, PayPal™ account, or so forth. Assume for purposes of an embodiment an additional payment method, namely an EMV-based method such as a mobile wallet, is selected. As a result, online merchant 180 (or a payment collection service with which merchant 180 has pre-arranged for handling payment for online transactions) may issue a collect payment request (201.0). Note that as used herein, the term “remote merchant” is collectively used to identify both a remote online (or other remote merchant) as well as any third party entity with whom the merchant has engaged in a payment collection arrangement.

[0024] Upon receipt within mobile device 100, e.g., via a given wireless interface such as a 3G/4G connection or other wireless interface, the request is provided to secure element 120, and more specifically to an internal mPOS function executing within SE 120, e.g., an emulation logic 125. In turn, SE 120 generates an emulated invoke reader mode request to NFC controller 130 (201.1) and enters a wait state (201.2). Note the emulated request thus indicates to NFC controller that the transaction is to proceed internally, and as such NFC controller 130 does not enable a contactless interface of the mobile device.

[0025] Still referring to FIG. 2, as part of the mobile commerce transaction, user 105 issues a wallet activation request (201.3) to a mobile wallet 148 which may be one or a set of applications executing on hardware of mobile device 100 (e.g., executing within a cryptoprocessor of UICC 140, which further includes a data store for EMV credentials). As seen, mobile wallet 148 generates an EMV credential activation request (201.4) that in turn causes UICC 140 to invoke a card emulation mode (201.5) which in turn triggers NFC controller 130 to notify UICC 140 of a field detected event (201.6). Note that this field detected notification is a masquerade, in

that no NFC field is established due to the presence of the internal mPOS device such that no EMV data is subject to attack by NFC communication.

[0026] In turn, NFC controller 130 issues a notification of target discovery (201.7) to SE 120, which in turn generates an activate card request (201.8), which causes NFC controller 130 to generate a card activation notification to UICC 140 (201.9).

[0027] Thus a valid secure session is established between UICC 140 and SE 120 such that secure communications (generally 201.10 – 201.14) occur between these two devices to perform processing of the payment transaction including receiving transaction information, processing this information using EMV data (including a secure key) and providing secure data, e.g., a message digest to SE 120, at the end of which merchant 180 is notified of the completion of the payment cycle (201.19). Various communications to internal nodes (generally 201.15 – 201.18) may then occur to deactivate the emulated card mode and emulated NFC reader mode and communicate completion of transaction to end user 105 and remote merchant 180 (generally 201.19 – 201.22). Although shown at this high level in the embodiment of FIG. 2, understand the scope of the present invention is not limited in this regard.

[0028] Note that in other embodiments, both mobile wallet functionality and mPOS functionality may be implemented within a single component (e.g., secure element 120 or UICC 140). In such embodiments, the processing, including the appropriate coupling and NFC disabling controlled by NFC controller 130 still may occur. In still different variations of such embodiments, the component having both mobile wallet and NFC reader functionality can internally perform a mobile commerce transaction even without participation from NFC controller 130 (i.e., the EMV transaction happens directly and internally between the wallet application and mPOS without interfacing with the NFC controller).

[0029] A final end-to-end solution between a user and a remote merchant is shown in FIG. 3, which is a block diagram of a system in accordance with another embodiment. As seen, a merchant site 180 interacts with SE 120 (including an integrated mPOS implemented within emulation logic 125) to collect payment using EMV payment credentials (e.g., stored within UICC 140). The EMV credentials are

processed by SE 120 (in its emulation logic 125 mPOS function) internally over the internal emulated NFC network without activating a NFC contactless interface.

[0030] Note that in an embodiment, SE 120 (which implements the integrated mPOS terminal) utilizes a standard NFC reader mode protocol with only one exception: an indicator such as a flag is provided to indicate to NFC controller 130 that the reader mode invoked is to emulate an external NFC reader device toward internal NFC nodes. Other than that, the NFC reader mode protocol is unchanged, in an embodiment. Note that NFC controller 130 may be configured to redirect NFC traffic internally from the SE (acting as the NFC reader) and the UICC (acting as the NFC card) and vice-versa, and to disable a NFC contactless interface (e.g., by disabling NFC antenna 150).

[0031] Referring now to FIG. 4, shown is a flow diagram for a mobile commerce transaction method in accordance with another embodiment of the present invention. As shown in FIG. 4, method 300 may be performed using various hardware and logic within a mobile device, as well as backend hardware both of a remote merchant, such as an online merchant from which a user of the mobile device desires to purchase a good or service, as well as possibly a payment service provider associated with this remote merchant (and which may be coupled to hardware of the remote merchant via one more backend networks). As seen, method 300 begins by receiving a mobile commerce transaction request (block 310). This request may be triggered by a user accessing a website of the remote merchant in performing a checkout operation with a choice of payment method by mobile wallet or other mobile-based payment direction. Responsive to this request (when received in the mobile device), an emulated NFC reader mode is invoked in an internal mobile POS device (block 320). And a card emulation NFC mode of a UICC or other device that includes EMV data and an associated cryptoprocessor may be invoked as well (block 330). Responsive to these invocations, the internal mPOS device and the UICC may be coupled (block 340). By this coupling, an EMV session, which is a secure session to enable communication of transaction and EMV data, may occur. Thus at block 350 an EMV session is established between an EMV-based

application and an mPOS application (both of which may execute on various hardware of the mobile device).

[0032] Still referring to FIG. 4, responsive to this EMV session establishment and data communication between the coupled components, an authorization request may be sent to a payment service provider via a network interface (block 360). Note that this network interface may be by a given wireless interface of the mobile device such as a 3G or 4G network interface and not via a NFC interface. This authorization request may include, in an embodiment, a transaction message. More specifically, this message may be a signed message that is signed by one or more EMV credentials such as one or more public or private keys of the user provided by an issuer. Control next passes to diamond 370 to determine whether payment was successful. Such successful payment determination may occur when the payment service provider verifies the transaction message as valid using the same one or more keys used to generate the transaction message. Note that this successful validation is also predicated upon the user having a valid account as verified by the payment service provider and sufficient funds and/or credit to cover the transaction cost.

[0033] On successful payment, the emulation modes are deactivated (block 380) and the end users (namely the mobile device user and the remote merchant) are notified of the successful transaction completion such that the remote merchant may enable transfer of the goods or services. Although shown at this high level in the FIG. 4 embodiment, the scope of the present invention is not limited in this regard.

[0034] By using an embodiment of the present invention, EMV credentials stored in a mobile wallet of a mobile or other device can be conveniently and securely used for mobile commerce (such as online transactions using a mobile device). Further such EMV credentials can be used in embodiments without: reducing available security profile mechanisms for contactless EMV payment credentials; modification to existing contactless EMV standards and/or contactless EMV credential smartcard application implementations from credit card companies, banks, and other financial institutions.

[0035] Embodiments also leverage an embedded POS terminal in the device itself instead of requiring an external POS terminal device such that available EMV application/credentials need not be modified, as from the point of view of the application/credential it interacts with a POS terminal (either external or internal). As such, embodiments may seamlessly integrate use of EMV credentials already present in a mobile wallet or other wireless or other device into a mobile commerce framework, removing the limitation of in-store POS usage only. Still further, security and convenience of mobile commerce is enhanced as for an end user, it is no longer necessary to access a physical wallet to remove a payment card to complete an online transaction, while maintaining the level of security of EMV has already defined while extending it into the mobile commerce world. In this way, embodiments provide a mechanism to interface with EMV payment credentials within a mobile wallet solution in a way that is transparent to the current mobile wallet operation.

[0036] Referring now to FIG. 5, shown is a block diagram of an example system 400 with which embodiments can be used. As seen, system 400 may be a smartphone or other wireless communicator. As shown in the block diagram of FIG. 5, system 400 may include an application or baseband processor 410. In general, baseband processor 410 can perform various signal processing with regard to communications, as well as perform computing operations for the device. In turn, baseband processor 410 can couple to a user interface/display 420 which can be realized, in some embodiments by a touch screen display that can display a secure checkout webpage of a remote online merchant to enable the NFC-encrypted payment processing described herein. In addition, baseband processor 810 may couple to a memory system including, in the embodiment of FIG. 5, a non-volatile memory, namely a flash memory 430 and a system memory, namely a dynamic random access memory (DRAM) 435. As further seen, baseband processor 410 can further couple to a capture device 440 such as an image capture device that can record video and/or still images.

[0037] Still referring to FIG. 5, a UICC 440 is also coupled to baseband processor 410. As discussed herein UICC 440 may include a storage to store various secure

information of a user including secure financial information and may further include a cryptoprocessor.

[0038] Also included in system 400 is a security processor 450 that may couple to baseband processor 410. In the embodiment shown, security processor 450 is a separate component of the system, however understand that the various security operations performed by security processor 450 instead can be performed in baseband processor 410 and/or a cryptoprocessor of UICC 440. Note that in some implementations, both a mPOS device implemented using an emulated NFC reader mode function and a mobile wallet application having EMV credentials may execute wholly within security processor 450.

[0039] As further illustrated, an NFC contactless interface 460 is provided that communicates in a NFC near field via an NFC antenna 465. While separate antennae are shown in FIG. 5, understand that in some implementations one antenna or a different set of antennae may be provided to enable various wireless functionality.

[0040] To enable communications to be transmitted and received, various circuitry may be coupled between baseband processor 410 and an antenna 490. Specifically, a radio frequency (RF) transceiver 470 and a wireless local area network (WLAN) transceiver 475 may be present. In general, RF transceiver 470 may be used to receive and transmit wireless data and calls according to a given wireless communication protocol such as 3G or 4G wireless communication protocol such as in accordance with a code division multiple access (CDMA), global system for mobile communication (GSM), long term evolution (LTE) or other protocol. In addition a GPS sensor 480 may be present. Other wireless communications such as receipt or transmission of radio signals, e.g., AM/FM and other signals may also be provided. In addition, via WLAN transceiver 475, local wireless signals, such as according to a Bluetooth™ standard or an IEEE 802.11 standard such as IEEE 802.11a/b/g/n can also be realized. Note that for performing secure mobile transactions with a remote online merchant, actual communications of a financial transaction may occur via one of these transceivers 470 and 475, rather than NFC contactless interface 460, to provide enhanced security and enable such

transactions. Although shown at this high level in the embodiment of FIG. 5, understand the scope of the present invention is not limited in this regard.

[0041] The following examples pertain to further embodiments.

[0042] In Example 1, an apparatus comprises: a security processor including a first logic to perform a secure reader function to emulate an external NFC reader device, to obtain payment credential information of a user of the apparatus; a UICC including a storage to store secure credential information of the user; and a NFC controller coupled to the security processor and the UICC, responsive to initiation of the secure reader function, to disable a NFC contactless interface of the apparatus and to cause the payment credential information to be communicated to a remote system while the NFC contactless interface is disabled.

[0043] In Example 2, the apparatus of Example 1 further includes a second wireless interface to provide the payment credential information obtained from the UICC via the security processor to a remote merchant, to perform an online mobile commerce transaction.

[0044] In Example 3, the first logic is optionally to initiate the secure reader function responsive to a payment collection request from the remote merchant.

[0045] In Example 4, the first logic is optionally to set an emulation indicator to indicate to the NFC controller that the secure reader function is in an emulation mode in which the secure reader function is to be a recipient of the payment credential information.

[0046] In Example 5, the apparatus of any one of Examples 1-4 further includes a second security processor to execute a mobile wallet application stored in a storage of the apparatus and initiated by the user, wherein the mobile wallet application is to generate a request to activate a secure session responsive to the user initiation.

[0047] In Example 6, the NFC controller is to couple the UICC to the second security processor to enable the first logic to establish the secure session between the UICC and the second security processor.

[0048] In Example 7, the apparatus of one of Examples 5 and 6 comprises a system on a chip including the security processor and the second security processor.

[0049] In Example 8, the first and second security processors of one of Examples 5-7 comprise a single security processor.

[0050] In Example 9, the UICC optionally includes a secure cryptoprocessor to generate the payment credential information comprising a signed message including transaction information for the mobile commerce transaction and user financial information, and signed by at least a portion of the secure credential information, the secure credential information comprising a key stored in the UICC and provided by an issuer on behalf of the user.

[0051] In Example 10, the apparatus of Example 2 includes a display to display a GUI of the remote merchant, the GUI including a checkout area having a user-selectable area to be activated by the user to enable the online mobile commerce transaction.

[0052] In Example 11, the apparatus of Example 1 further includes the NFC contactless interface, where in a NFC mode, the NFC controller is to enable communication of the payment credential information from the UICC to an external NFC reader located in a near field with the apparatus via the NFC contactless interface.

[0053] In Example 12, at least one computer readable medium includes instructions that when execute enable a system to: receive a mobile commerce transaction request, and responsive thereto, invoke an emulated NFC reader mode in an internal mobile POS device of the system; invoke a card emulation NFC mode of a secure cryptoprocessor of the system; and couple the internal mobile POS device and the secure cryptoprocessor to enable the internal mobile POS device to participate in a secure session with the secure cryptoprocessor to receive an encrypted mobile commerce transaction packet encrypted with a secure key of secure payment credential information stored in a secure data store of the system, while a NFC contactless interface of the system is disabled.

[0054] In Example 13, the at least one computer readable medium of Example 12 includes instructions further to enable the system to communicate the encrypted mobile commerce transaction packet to a remote merchant via a wireless interface of the system.

[0055] In Example 14, the at least one computer readable medium of Example 12 further comprises instructions to enable the system to deactivate the card emulation NFC mode of the secure cryptoprocessor responsive to successful completion of the mobile commerce transaction.

[0056] In Example 15, the at least one computer readable medium of Example 14 further comprises instructions to enable the system to terminate the emulated NFC reader mode responsive to the successful completion of the mobile commerce transaction.

[0057] In Example 16, the at least one computer readable medium of Example 15 further comprises instructions to enable the system to notify a user of the system about the successful completion of the mobile commerce transaction.

[0058] In Example 17, the internal mobile POS device and secure cryptoprocessor of any one of Examples 12-16 are to execute at least some of the instructions on a processor of the system.

[0059] In Example 18, a system comprises: an application processor to execute user applications; a security processor coupled to the application processor and including an emulation logic to emulate an external NFC reader device to obtain a transaction message signed by a credential of a user of the system; a secure storage to store the credential and account information of the user with respect to at least one issuer entity; a NFC contactless interface to enable wireless communication with a NFC device in a near field with the system; a cryptographic logic coupled to the secure storage to generate the transaction message based on the credential, at least a portion of the account information, and transaction information for a mobile commerce transaction between the user and a remote entity; and a NFC controller coupled to the security processor, the secure storage, and the NFC contactless interface, responsive to initiation of the emulation logic, to

disable the NFC contactless interface and to enable the transaction message to be communicated to a remote system associated with the remote entity while the NFC contactless interface is disabled.

[0060] In Example 19, the system of Example 18 further comprises a wireless interface to provide the transaction message to the remote system, to complete the mobile commerce transaction, where the wireless interface is coupled to receive the transaction message via the application processor.

[0061] In Example 20, the emulation logic is optionally to set an emulation indicator to indicate to the NFC controller that the emulation logic is to be a recipient of the transaction message.

[0062] In Example 21, the security processor is optionally to execute a mobile wallet application to generate a request to activate a secure session using the credential.

[0063] In Example 22, in a system of any one of Examples 18-21, in a NFC mode, the NFC controller is optionally to enable communication of at least a portion of the account information to an external NFC reader device located in the near field with the system via the NFC contactless interface.

[0064] In Example 23, a system comprises: means for receiving a mobile commerce transaction request, and responsive thereto, invoking an emulated NFC reader mode in an internal mobile POS means of the system; means for invoking a card emulation NFC mode of a secure cryptoprocessor means of the system; and means for coupling the internal mobile POS means and the secure cryptoprocessor means to enable the internal mobile POS means to participate in a secure session with the secure cryptoprocessor means to receive an encrypted mobile commerce transaction packet encrypted with a secure key of secure payment credential information stored in a secure data store of the system, while a NFC contactless interface of the system is disabled.

[0065] In Example 24, the system of Example 23 further comprises means for communicating the encrypted mobile commerce transaction packet to a remote merchant via a wireless interface of the system.

[0066] In Example 25, the system of Example 24 further comprises means for deactivating the card emulation NFC mode of the secure cryptoprocessor means responsive to successful completion of the mobile commerce transaction.

[0067] In Example 26, the system of Example 24 further comprises: means for terminating the emulated NFC reader mode responsive to successful completion of the mobile commerce transaction; and means for notifying a user of the system about the successful completion of the mobile commerce transaction.

[0068] In Example 27, a method comprises: receiving a mobile commerce transaction request, and responsive thereto, invoking an emulated NFC reader mode in an internal mobile POS device of a system; invoking a card emulation NFC mode of a secure cryptoprocessor of the system; and coupling the internal mobile POS device and the secure cryptoprocessor to enable the internal mobile POS device to participate in a secure session with the secure cryptoprocessor to receive an encrypted mobile commerce transaction packet encrypted with a secure key of secure payment credential information stored in a secure data store of the system, while a NFC contactless interface of the system is disabled.

[0069] In Example 28, the method of Example 27 further comprises communicating the encrypted mobile commerce transaction packet to a remote merchant via a wireless interface of the system.

[0070] In Example 29, the method of Example 28 further comprises deactivating the card emulation NFC mode of the secure cryptoprocessor responsive to successful completion of the mobile commerce transaction.

[0071] In Example 30, the method of Example 29 further comprises terminating the emulated NFC reader mode responsive to successful completion of the mobile commerce transaction.

[0072] In Example 31, the method of Example 30 further comprises notifying a user of the system about the successful completion of the mobile commerce transaction.

[0073] In Example 32, a machine-readable storage medium includes machine-readable instructions, when executed, to implement a method of any one of Examples 27-31.

[0074] In Example 33, an apparatus comprises means to perform a method of any one of Examples 27-31.

[0075] Understand that various combinations of the above examples are possible.

[0076] Embodiments may be used in many different types of systems. For example, in one embodiment a communication device can be arranged to perform the various methods and techniques described herein. Of course, the scope of the present invention is not limited to a communication device, and instead other embodiments can be directed to other types of apparatus for processing instructions, or one or more machine readable media including instructions that in response to being executed on a computing device, cause the device to carry out one or more of the methods and techniques described herein.

[0077] Embodiments may be implemented in code and may be stored on a non-transitory storage medium having stored thereon instructions which can be used to program a system to perform the instructions. The storage medium may include, but is not limited to, any type of disk including floppy disks, optical disks, solid state drives (SSDs), compact disk read-only memories (CD-ROMs), compact disk rewritables (CD-RWs), and magneto-optical disks, semiconductor devices such as read-only memories (ROMs), random access memories (RAMs) such as dynamic random access memories (DRAMs), static random access memories (SRAMs), erasable programmable read-only memories (EPROMs), flash memories, electrically erasable programmable read-only memories (EEPROMs), magnetic or optical cards, or any other type of media suitable for storing electronic instructions.

[0078] While the present invention has been described with respect to a limited number of embodiments, those skilled in the art will appreciate numerous modifications and variations therefrom. It is intended that the appended claims cover all such modifications and variations as fall within the true spirit and scope of this present invention.

What is claimed is:

- 1 1. An apparatus comprising:
2 a security processor including a first logic to perform a secure reader function
3 to emulate an external near field communication (NFC) reader device, to obtain
4 payment credential information of a user of the apparatus;
5 a universal integrated card circuit (UICC) including a storage to store secure
6 credential information of the user; and
7 a NFC controller coupled to the security processor and the UICC, responsive
8 to initiation of the secure reader function, to disable a NFC contactless interface of
9 the apparatus and to cause the payment credential information to be communicated
10 to a remote system while the NFC contactless interface is disabled.
- 1 2. The apparatus of claim 1, further comprising a second wireless interface to
2 provide the payment credential information obtained from the UICC via the security
3 processor to a remote merchant, to perform an online mobile commerce transaction.
- 1 3. The apparatus of claim 2, wherein the first logic is to initiate the secure reader
2 function responsive to a payment collection request from the remote merchant.
- 1 4. The apparatus of claim 1, wherein the first logic is to set an emulation
2 indicator to indicate to the NFC controller that the secure reader function is in an
3 emulation mode in which the secure reader function is to be a recipient of the
4 payment credential information.
- 1 5. The apparatus of claim 1, further comprising a second security processor to
2 execute a mobile wallet application stored in a storage of the apparatus and initiated
3 by the user, wherein the mobile wallet application is to generate a request to activate
4 a secure session responsive to the user initiation.
- 1 6. The apparatus of claim 5, wherein the apparatus comprises a system on a
2 chip including the security processor and the second security processor.

1 7. The apparatus of claim 2, wherein the UICC includes a secure
2 cryptoprocessor to generate the payment credential information comprising a signed
3 message including transaction information for the mobile commerce transaction and
4 user financial information, and signed by at least a portion of the secure credential
5 information, the secure credential information comprising a key stored in the UICC
6 and provided by an issuer on behalf of the user.

1 8. The apparatus of claim 2, further comprising a display to display a graphical
2 user interface (GUI) of the remote merchant, the GUI including a checkout area
3 having a user-selectable area to be activated by the user to enable the online mobile
4 commerce transaction.

1 9. The apparatus of claim 1, further comprising the NFC contactless interface,
2 wherein in a NFC mode, the NFC controller is to enable communication of the
3 payment credential information from the UICC to an external NFC reader located in a
4 near field with the apparatus via the NFC contactless interface.

1 10. A system comprising:

2 means for receiving a mobile commerce transaction request, and responsive
3 thereto, invoking an emulated near field communication (NFC) reader mode in an
4 internal mobile point of sale (POS) means of the system;

5 means for invoking a card emulation NFC mode of a secure cryptoprocessor
6 means of the system; and

7 means for coupling the internal mobile POS means and the secure
8 cryptoprocessor means to enable the internal mobile POS means to participate in a
9 secure session with the secure cryptoprocessor means to receive an encrypted
10 mobile commerce transaction packet encrypted with a secure key of secure payment
11 credential information stored in a secure data store of the system, while a NFC
12 contactless interface of the system is disabled.

1 11. The system of claim 10, further comprising means for communicating the
2 encrypted mobile commerce transaction packet to a remote merchant via a wireless
3 interface of the system.

1 12. The system of claim 11, further comprising means for deactivating the card
2 emulation NFC mode of the secure cryptoprocessor means responsive to successful
3 completion of the mobile commerce transaction.

1 13. The system of claim 12, further comprising:
2 means for terminating the emulated NFC reader mode responsive to
3 successful completion of the mobile commerce transaction; and
4 means for notifying a user of the system about the successful completion of
5 the mobile commerce transaction.

1 14. A method comprising:
2 receiving a mobile commerce transaction request, and responsive thereto,
3 invoking an emulated near field communication (NFC) reader mode in an internal
4 mobile point of sale (POS) device of a system;
5 invoking a card emulation NFC mode of a secure cryptoprocessor of the
6 system; and
7 coupling the internal mobile POS device and the secure cryptoprocessor to
8 enable the internal mobile POS device to participate in a secure session with the
9 secure cryptoprocessor to receive an encrypted mobile commerce transaction
10 packet encrypted with a secure key of secure payment credential information stored
11 in a secure data store of the system, while a NFC contactless interface of the system
12 is disabled.

1 15. The method of claim 14, further comprising communicating the encrypted
2 mobile commerce transaction packet to a remote merchant via a wireless interface of
3 the system.

1 16. The method of claim 15, further comprising deactivating the card emulation
2 NFC mode of the secure cryptoprocessor responsive to successful completion of the
3 mobile commerce transaction.

1 17. The method of claim 16, further comprising terminating the emulated NFC
2 reader mode responsive to successful completion of the mobile commerce
3 transaction.

1 18. The method of claim 17, further comprising notifying a user of the system
2 about the successful completion of the mobile commerce transaction.

1 19. A machine-readable storage medium including machine-readable instructions,
2 when executed, to implement a method as claimed in any one of claims 14 to 18.

1 20. A system comprising:
2 an application processor to execute user applications;
3 a security processor coupled to the application processor and including an
4 emulation logic to emulate an external near field communication (NFC) reader device
5 to obtain a transaction message signed by a credential of a user of the system;
6 a secure storage to store the credential and account information of the user
7 with respect to at least one issuer entity;
8 a NFC contactless interface to enable wireless communication with a NFC
9 device in a near field with the system;
10 a cryptographic logic coupled to the secure storage to generate the
11 transaction message based on the credential, at least a portion of the account
12 information, and transaction information for a mobile commerce transaction between
13 the user and a remote entity; and
14 a NFC controller coupled to the security processor, the secure storage, and
15 the NFC contactless interface, responsive to initiation of the emulation logic, to
16 disable the NFC contactless interface and to enable the transaction message to be
17 communicated to a remote system associated with the remote entity while the NFC
18 contactless interface is disabled.

1 21. The system of claim 20, further comprising a wireless interface to provide the
2 transaction message to the remote system, to complete the mobile commerce
3 transaction, wherein the wireless interface is coupled to receive the transaction
4 message via the application processor.

1 22. The system of claim 20, wherein the emulation logic is to set an emulation
2 indicator to indicate to the NFC controller that the emulation logic is to be a recipient
3 of the transaction message.

1 23. The system of claim 20, wherein the security processor is to execute a mobile
2 wallet application, the mobile wallet application to generate a request to activate a
3 secure session using the credential.

1 24. The system of claim 20, wherein in a NFC mode, the NFC controller is to
2 enable communication of at least a portion of the account information to an external
3 NFC reader device located in the near field with the system via the NFC contactless
4 interface.

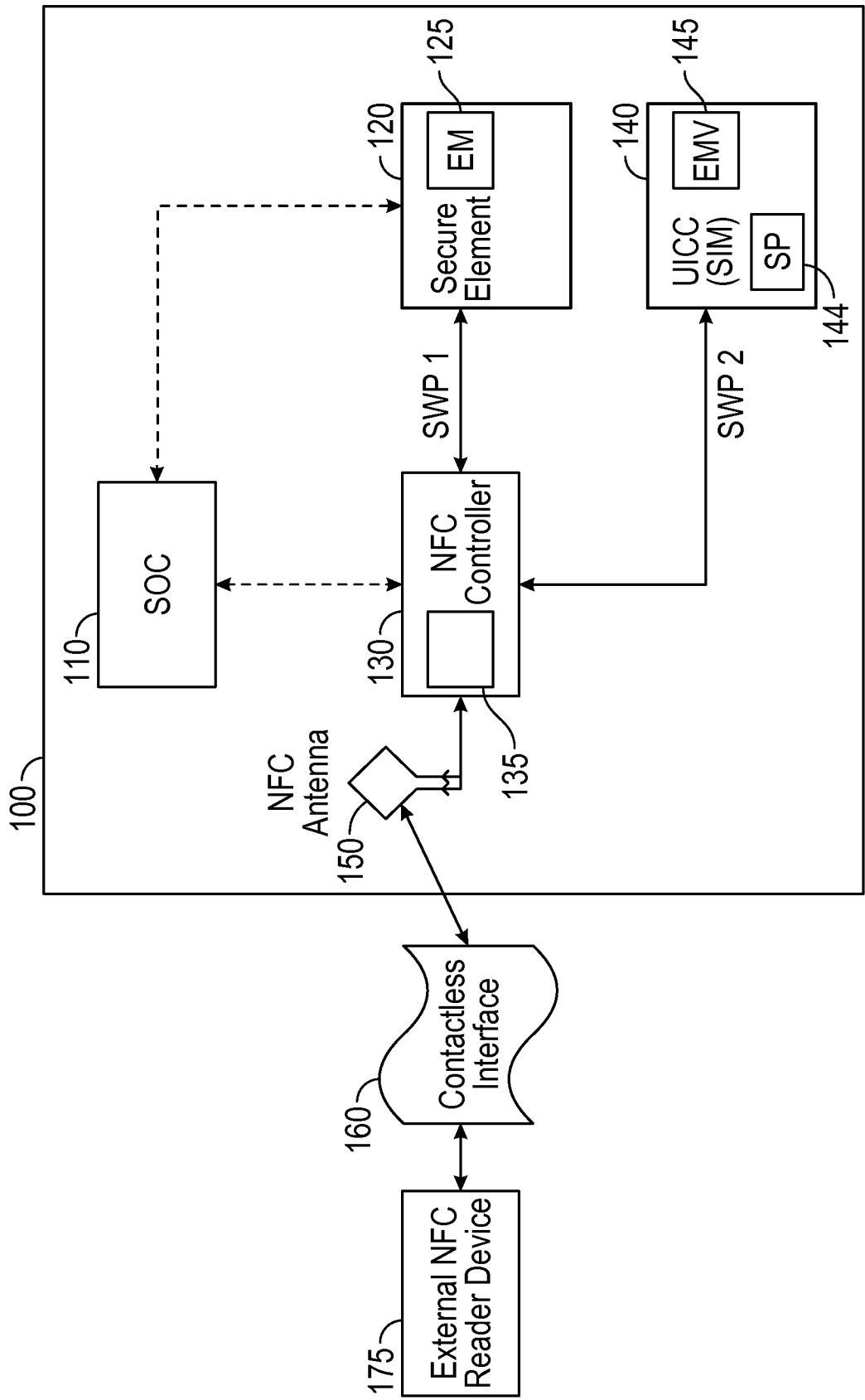
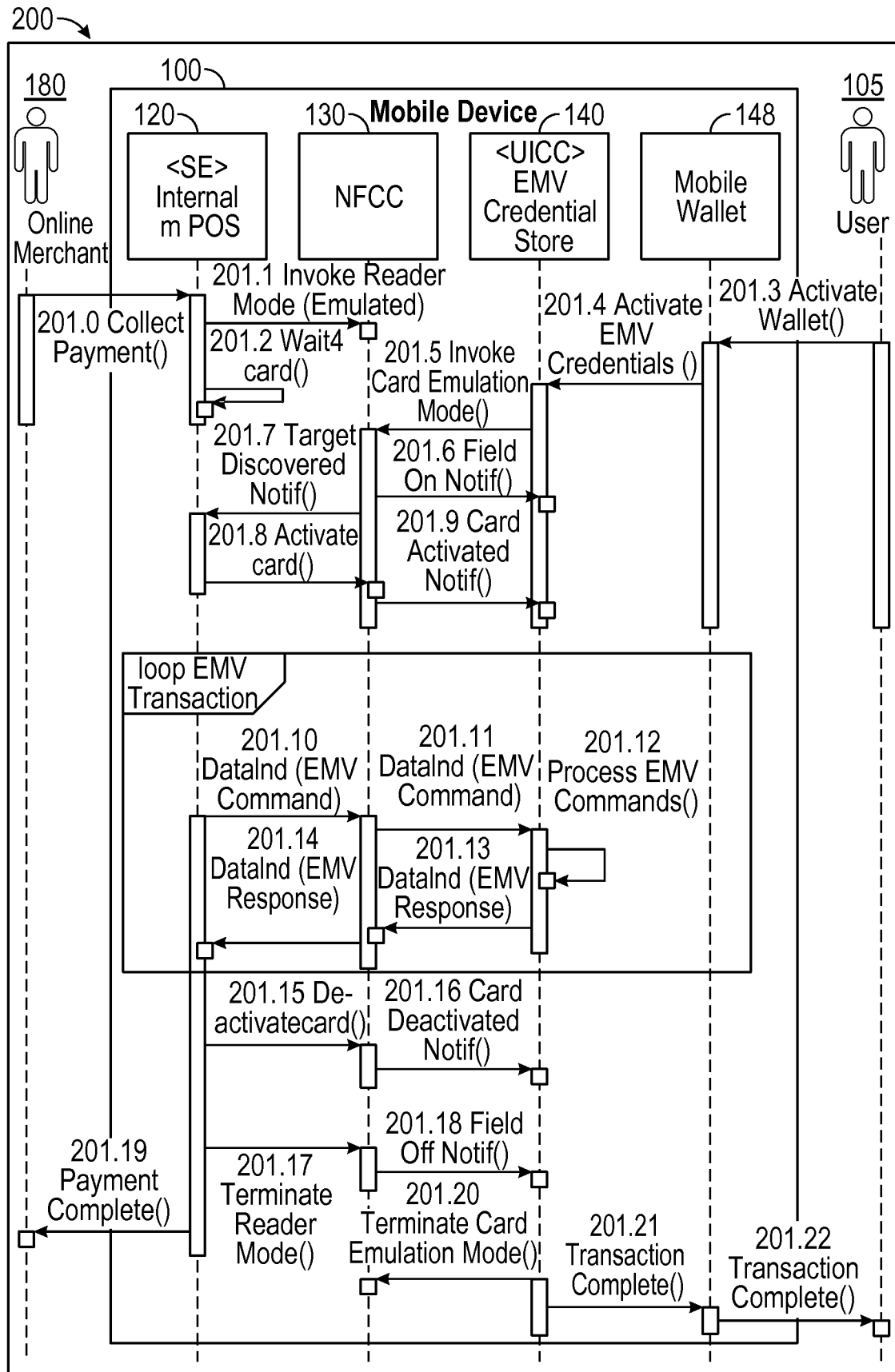


FIG. 1

2/5



3/5

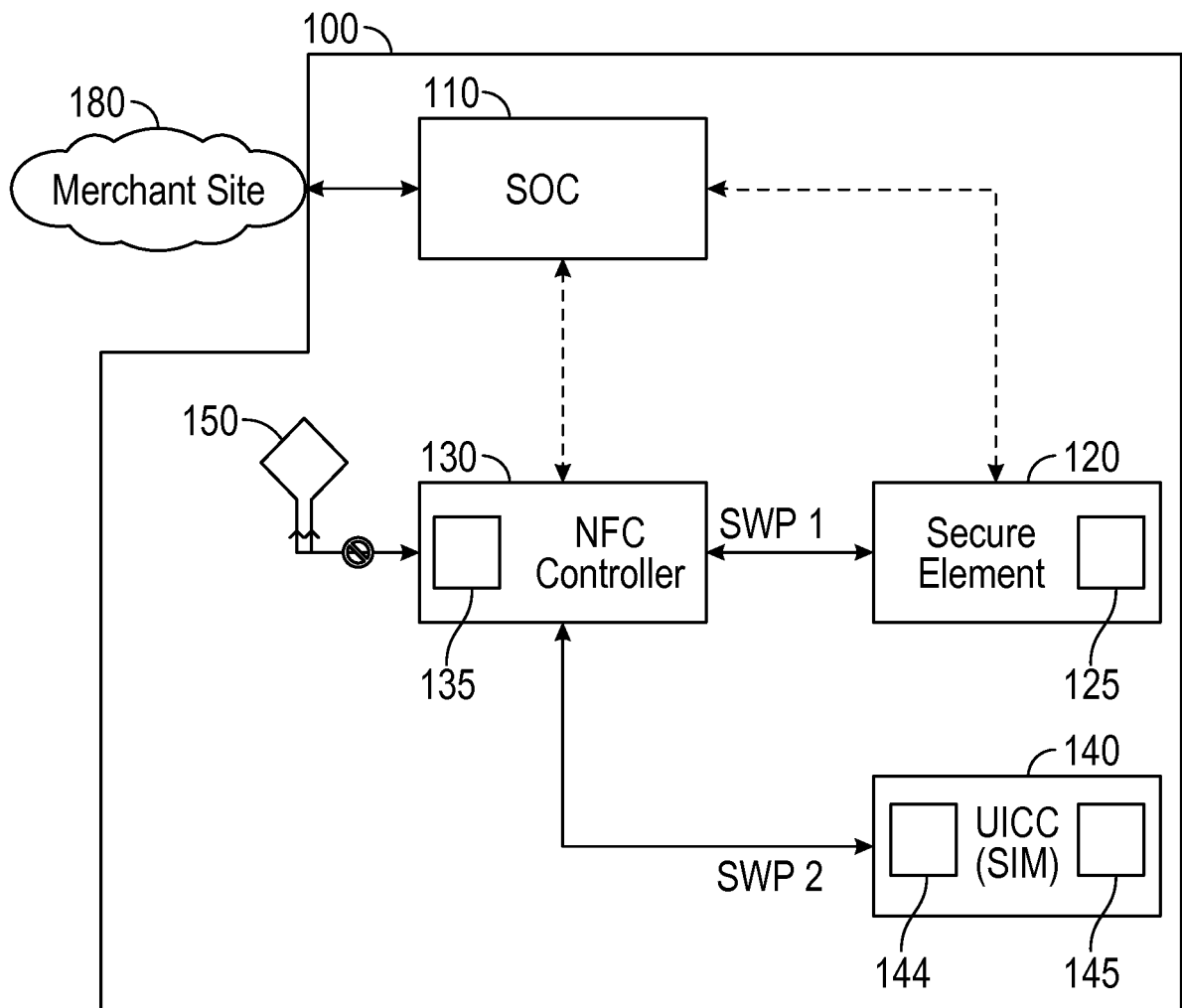


FIG. 3

4/5

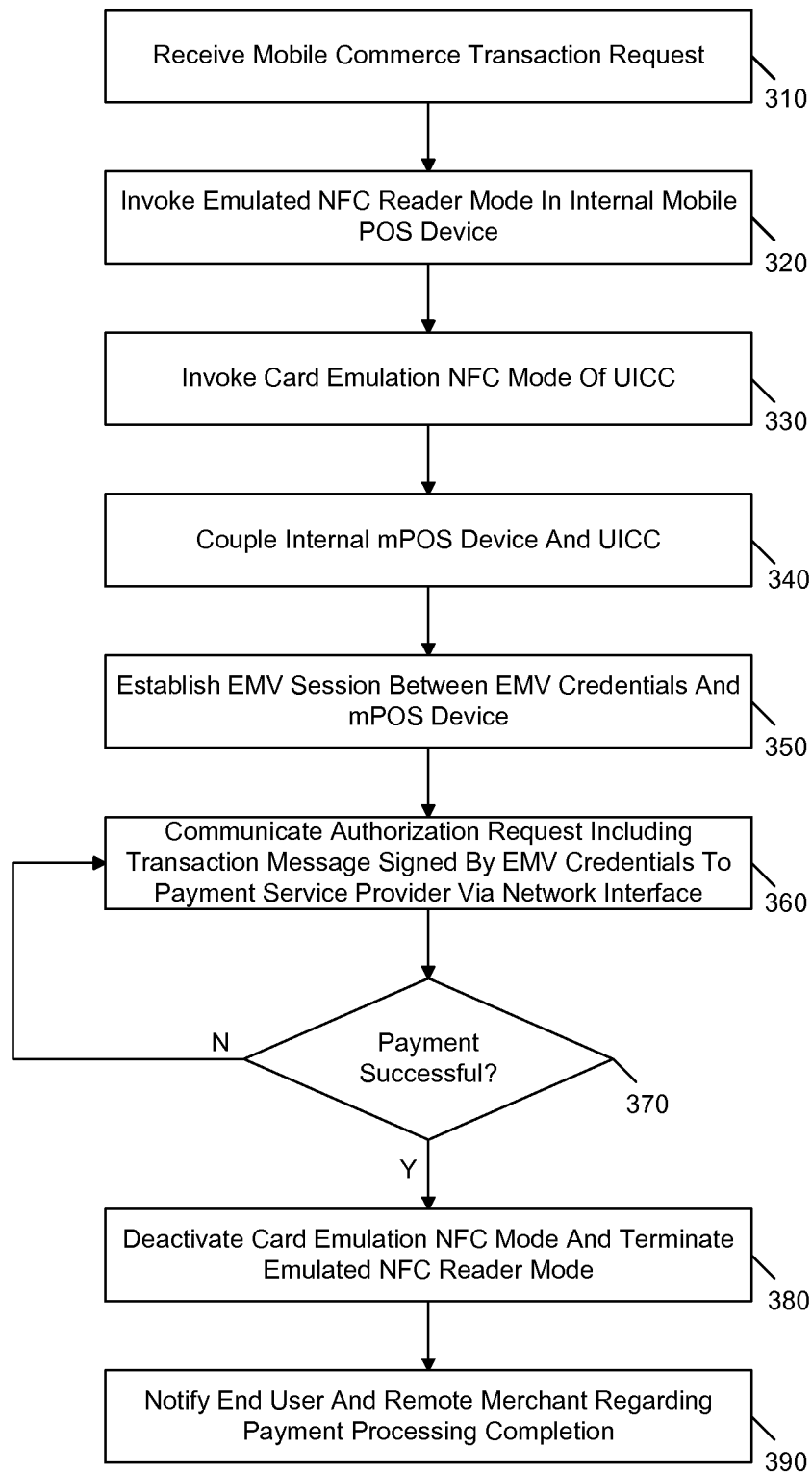
300

FIG. 4

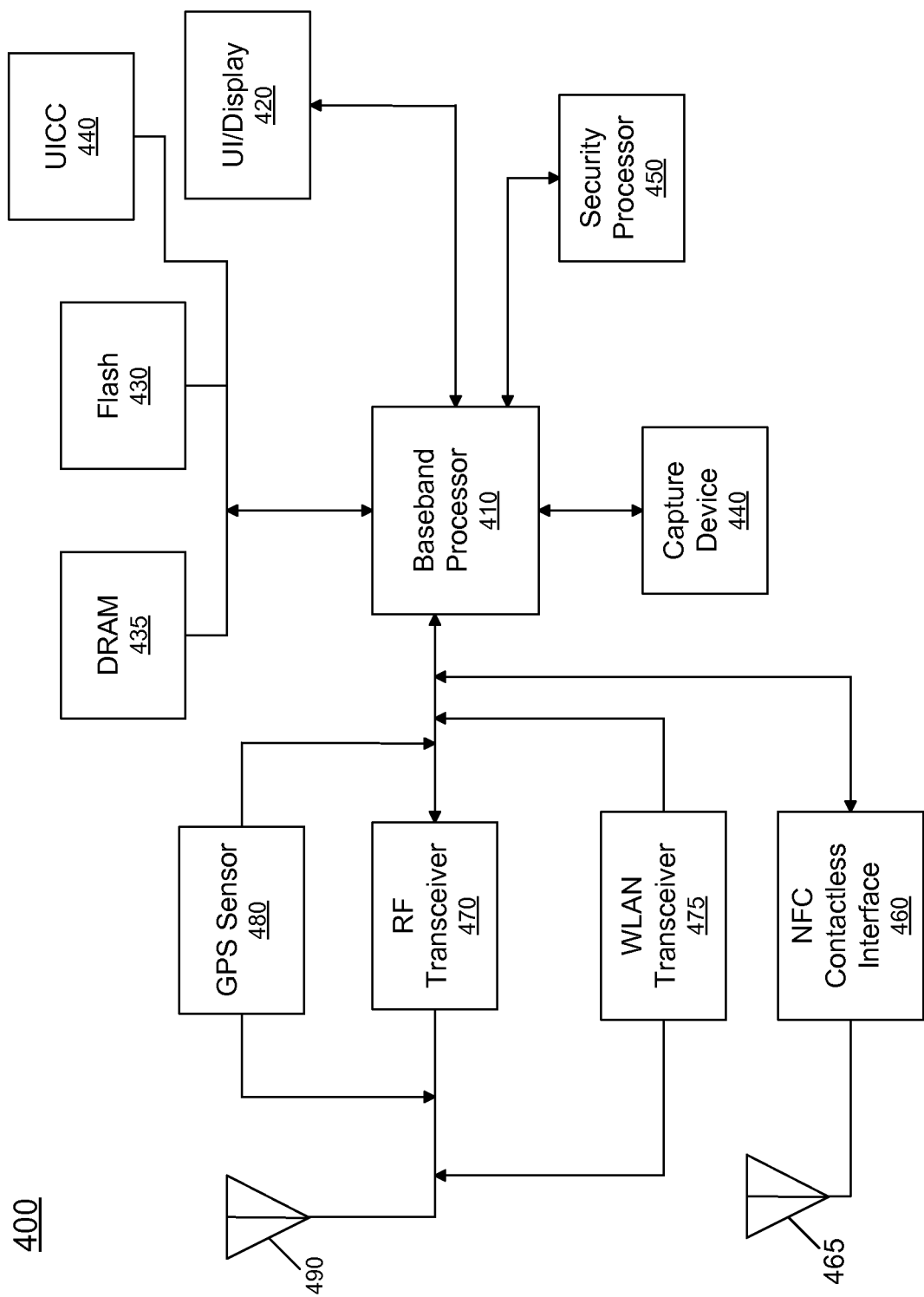


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2015/029024**A. CLASSIFICATION OF SUBJECT MATTER****G06Q 20/20(2012.01)i, G06Q 20/34(2012.01)i, G06Q 20/32(2012.01)i, G06Q 20/40(2012.01)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 20/20; G06Q 20/40; G06Q 20/24; G06Q 20/32; H04M 11/00; G06Q 20/28; G06Q 20/00; H04B 1/38; G06Q 20/34

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, emulate, payment, mobile

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2008-0071625 A1 (AVIN ARUMUGAM) 20 March 2008 See paragraphs [0016]-[0034]; and figures 1-3B.	1-24
A	US 2014-0058953 A1 ((MIROSLAV FLOREK et al.) 27 February 2014 See paragraphs [0020]-[0034]; claim 1; and figures 1-8.	1-24
A	US 2012-0030044 A1 (DOUGLAS J. HURST) 02 February 2012 See paragraphs [0074]-[0082]; and figures 8-10.	1-24
A	US 8352323 B2 (MICHELLE FISHER) 08 January 2013 See column 5, line 37 - column 7, line 10; and figures 4-5.	1-24
A	KR 10-2014-0038001 A (T-MONET CO., LTD. et al.) 28 March 2014 See paragraphs [0017]-[0035]; and figures 1-4.	1-24



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 another citation or other special reason (as specified)

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

22 July 2015 (22.07.2015)

Date of mailing of the international search report

23 July 2015 (23.07.2015)

Name and mailing address of the ISA/KR

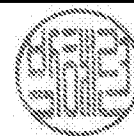
International Application Division
Korean Intellectual Property Office
189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. +82-42-472-7140

Authorized officer

PARK, Hye Lyun

Telephone No. +82-42-481-3463



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/029024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2008-0071625 A1	20/03/2008	US 7873540 B2	18/01/2011
US 2014-0058953 A1	27/02/2014	AU 2009-294209 A1	25/03/2010
		AU 2009-294210 A1	25/03/2010
		AU 2010-240543 A1	28/10/2010
		AU 2010-244100 A1	11/11/2010
		CA 2732236 A1	25/03/2010
		CA 2732238 A1	25/03/2010
		CA 2739809 A1	28/10/2010
		CA 2739858 A1	11/11/2010
		CN 102160068 A	17/08/2011
		CN 102160070 A	17/08/2011
		CN 102460520 A	16/05/2012
		CN 102460520 B	21/01/2015
		CN 102640176 A	15/08/2012
		EP 2347375 A1	27/07/2011
		EP 2350942 A1	03/08/2011
		EP 2430620 A1	21/03/2012
		EP 2449512 A2	09/05/2012
		EP 2462567 A2	13/06/2012
		EP 2561489 A1	27/02/2013
		JP 2012-503242 A	02/02/2012
		JP 2012-503243 A	02/02/2012
		JP 2012-524927 A	18/10/2012
		JP 2012-526306 A	25/10/2012
		JP 5562964 B2	30/07/2014
		JP 5562965 B2	30/07/2014
		JP 5738844 B2	24/06/2015
		KR 10-2011-0090899 A	10/08/2011
		KR 10-2011-0094176 A	22/08/2011
		KR 10-2012-0018174 A	29/02/2012
		KR 10-2012-0030408 A	28/03/2012
		MX 2011004702 A	02/09/2011
		RU 2011148267 A	10/06/2013
		TW 201205477 A	01/02/2012
		US 2010-0274677 A1	28/10/2010
		US 2010-0274726 A1	28/10/2010
		US 2011-0021175 A1	27/01/2011
		US 2011-0022482 A1	27/01/2011
		US 2011-0042456 A1	24/02/2011
		US 2011-0112968 A1	12/05/2011
		US 2011-0196796 A1	11/08/2011
		US 8406809 B2	26/03/2013
		US 8500008 B2	06/08/2013
		US 8583493 B2	12/11/2013
		US 8606711 B2	10/12/2013
		US 8799084 B2	05/08/2014
		WO 2010-032215 A1	25/03/2010
		WO 2010-032215 A4	20/05/2010

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/029024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		WO 2010-032216 A1	25/03/2010
		WO 2010-032216 A4	17/06/2010
		WO 2010-122520 A2	28/10/2010
		WO 2010-122520 A3	10/05/2012
		WO 2010-128442 A2	11/11/2010
		WO 2010-128442 A3	28/04/2011
		WO 2010-128442 A4	16/06/2011
		WO 2010-131226 A1	18/11/2010
		WO 2010-131226 A4	20/01/2011
		WO 2011-132025 A1	27/10/2011
US 2012-0030044 A1	02/02/2012	US 2009-0063312 A1	05/03/2009
		US 2012-0028612 A1	02/02/2012
US 8352323 B2	08/01/2013	US 2009-0144161 A1	04/06/2009
		US 2012-0150601 A1	14/06/2012
		US 2013-0073373 A1	21/03/2013
		US 2013-0080228 A1	28/03/2013
		US 2013-0080229 A1	28/03/2013
		US 2013-0080230 A1	28/03/2013
		US 2013-0080231 A1	28/03/2013
		US 2013-0080232 A1	28/03/2013
		US 2013-0080233 A1	28/03/2013
		US 2013-0080240 A1	28/03/2013
		US 2013-0080241 A1	28/03/2013
		US 2013-0097032 A1	18/04/2013
		US 2013-0097036 A1	18/04/2013
		US 2013-0097040 A1	18/04/2013
		US 2013-0097041 A1	18/04/2013
		US 2013-0097083 A1	18/04/2013
		US 2013-0103466 A1	25/04/2013
		US 2013-0103478 A1	25/04/2013
		US 2013-0103511 A1	25/04/2013
		US 2013-0103512 A1	25/04/2013
		US 2013-0103513 A1	25/04/2013
		US 2013-0103514 A1	25/04/2013
		US 2013-0103517 A1	25/04/2013
		US 2013-0103518 A1	25/04/2013
		US 2013-0103588 A1	25/04/2013
		US 2013-0124289 A1	16/05/2013
		US 2013-0124290 A1	16/05/2013
		US 2013-0124291 A1	16/05/2013
		US 2013-0124351 A1	16/05/2013
		US 2013-0124423 A1	16/05/2013
		US 2013-0132181 A1	23/05/2013
		US 2014-0074707 A1	13/03/2014
		US 2014-0164092 A1	12/06/2014
		US 2014-0164156 A1	12/06/2014
		US 2014-0164157 A1	12/06/2014
		US 2014-0195362 A1	10/07/2014

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2015/029024

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
		US 2014-0229259 A1	14/08/2014
		US 2014-0229276 A1	14/08/2014
		US 2014-0297518 A1	02/10/2014
		US 2014-0302824 A1	09/10/2014
		US 2014-0304073 A1	09/10/2014
		US 2014-0304082 A1	09/10/2014
		US 2014-0304095 A1	09/10/2014
		US 2014-0304159 A1	09/10/2014
		US 2014-0304160 A1	09/10/2014
		US 2014-0304161 A1	09/10/2014
		US 2014-0308934 A1	16/10/2014
		US 2014-0310161 A1	16/10/2014
		US 2014-0324560 A1	30/10/2014
		US 2014-0324574 A1	30/10/2014
		US 2014-0324635 A1	30/10/2014
		US 2014-0324697 A1	30/10/2014
		US 2014-0330626 A1	06/11/2014
		US 2015-0032524 A1	29/01/2015
		US 8332272 B2	11/12/2012
		US 8583494 B2	12/11/2013
		US 8589237 B2	19/11/2013
		US 8620754 B2	31/12/2013
		US 8630905 B2	14/01/2014
		US 8630906 B2	14/01/2014
		US 8688526 B2	01/04/2014
		US 8694380 B2	08/04/2014
		US 8725575 B2	13/05/2014
		US 8725576 B2	13/05/2014
		US 8725577 B2	13/05/2014
		US 8751313 B2	10/06/2014
		US 8751314 B2	10/06/2014
		US 8751315 B2	10/06/2014
		US 8799085 B2	05/08/2014
		US 8805726 B2	12/08/2014
		US 8818870 B2	26/08/2014
KR 10-2014-0038001 A	28/03/2014	KR 10-1459291 B1	07/11/2014