

(43) International Publication Date
24 January 2013 (24.01.2013)

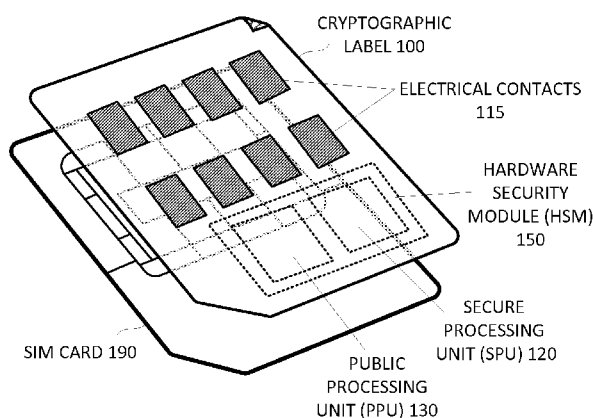
- (51) **International Patent Classification:**
H04W 12/08 (2009.01) *H04W 80/00* (2009.01)
- (21) **International Application Number:**
PCT/US2012/047693
- (22) **International Filing Date:**
20 July 2012 (20.07.2012)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (30) **Priority Data:**
61/510,023 20 July 2011 (20.07.2011) US
- (71) **Applicant (for all designated States except US):** VISA INTERNATIONAL SERVICE ASSOCIATION [US/US]; P.O. Box 8999, M1-11F, San Francisco, California 94128 (US).
- (72) **Inventor; and**
- (75) **Inventor/Applicant (for US only):** HUXHAM, Horatio Nelson [ZA/ZA]; 35 Bellwater Park, 2570 Kenridge, Capetown (ZA).
- (74) **Agents:** TSE, Michael et al.; Kilpatrick Townsend and Stockton LLP, 2 Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).

(81) **Designated States** (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, 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, 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, ML, MR, NE, SN, TD, TG).

Published:

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

(54) **Title:** CRYPTOGRAPHIC EXPANSION DEVICE AND RELATED PROTOCOLS**Fig. 1**

(57) **Abstract:** A cryptographic expansion device that can be attached to a communication component of a communication device to enable the communication device to perform cryptographic operations on communications sent to and from the communication device is described. When used with a communication device, the cryptographic expansion device enables the communication device to send and received end-to-end secure encrypted communications. The cryptographic expansion device can be used with a communication device without requiring any changes to the internal software or hardware of the communication device and without requiring any modification to the communication protocols of the communication device. In some embodiments, the end-to-end secure communications enabled by the cryptographic expansion device can be utilized by a user of the communication device to perform financial and/or banking transactions.



CRYPTOGRAPHIC EXPANSION DEVICE AND RELATED PROTOCOLS

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority from United States Provisional Patent Application No. 61/510,023, entitled “Systems and Methods for Secure Mobile Communication,” filed July 20, 2011, the contents of which is hereby incorporated in its entirety by reference for all purposes.

[0002] This application is related to commonly owned Patent Cooperation Treaty (PCT) Application No. _____, entitled “Mobile Banking System with Cryptographic Expansion Device,” filed July 20, 2012, the contents of which is hereby incorporated in its entirety by reference for all purposes.

BACKGROUND

[0003] In developing countries and rural areas, less than 10% of the population may have access to banking services from traditional brick-and-mortar banks. In such areas, a bank may be physically located too far away for a majority of the population to travel to. And even if a bank is nearby, it may be the only bank location in the vicinity of a vast region covering a large number of the population. The brick-and-mortar bank may not have the resources and capacity to adequately support such a large number of customers, resulting in long wait times and inconvenience for the bank’s customers. In most developing countries, building additional bank branches and/or installing automated teller machines (ATMs) at various locations are often not a viable solution due to the high costs of the complex infrastructure involved. Even in developed countries where there are more bank branches and ATM locations available, customers may still have limited access to banking services such as services that are not available from ATMs during non-business hours. Furthermore, certain customers such as the elderly or customers with disabilities may still have difficulty getting to the bank branches or ATM locations.

[0004] In recent years, the use of mobile devices in developed and developing countries has grown rapidly. As such, one way of providing these communities with access to banking services is to enable users of mobile devices to perform mobile banking transactions, such as making mobile payments or money transfers, or checking account balances or performing other

account related services, directly from their mobile devices. However, security concerns are often a stumbling block that hinders the wide adoption and growth of mobile banking. Most mobile devices lack the capability to securely send end-to-end encrypted communication. As a result, sensitive information, such as a Personal Identification Numbers (PINs) and Primary Account Numbers (PANs), might be sent in plaintext form, creating a vulnerability in which such sensitive information can be intercepted by malicious parties and be used for fraudulent purposes.

[0005] While some security measures can be provided by mobile network operators, for example, to provide encryption capabilities at a base station, the protection provided by such solutions is still limited because the communication is still sent in plaintext form at some point during the transmission. Other solutions require re-provisioning of users' mobile devices, for example, by over the air (OTA) provisioning, and such solutions can be costly in terms of both deployment and operating costs. Consequently, mobile operators have to either pass this cost onto their customers or absorb it themselves. Thus, the total cost of ownership (TCO) is also often a stumbling block that prevents the uptake and growth of mobile banking. Without a cost-effective and efficient way to securely send and receive communication with mobile devices, mobile banking operators are destined to incur losses or fail to roll out their mobile banking services entirely.

[0006] Embodiments of the present invention address these and other problems individually and collectively.

BRIEF SUMMARY

[0007] Embodiments of the present invention disclose a cryptographic expansion device that can be attached to a communication component of a communication device to enable the communication device to perform cryptographic operations on communications sent to and from the communication device. When used with a communication device, the cryptographic expansion device enables the communication device to send and received end-to-end secure encrypted communications. The cryptographic expansion device according to various embodiments can be used with a communication device without requiring any changes to the internal software or hardware of the communication device and without requiring any

modification to the communication protocols used by the communication device. In some embodiments, the end-to-end secure communications enabled by the cryptographic expansion device can be utilized by a user of the communication device to perform financial and/or banking transactions.

5 **[0008]** According to at least one embodiment, the cryptographic expansion device is a cryptographic label that includes a hardware security module disposed therein. The hardware security module includes a secure processing unit and a public processing unit. The cryptographic label also includes a first set of electrical contacts disposed on the top side of the cryptographic label for interfacing to a communication device, and a second set of electrical
10 contacts disposed on the bottom side of the cryptographic label for interfacing to a communication component. A coupling element is also provided to attach the cryptographic label to the communication component. In an exemplary embodiment, the communication device can be a mobile phone, the communication component can be a subscriber identity module (SIM) card, and the coupling element used for attaching the cryptographic label to the
15 communication component can be an adhesive material disposed on the cryptographic label

[0009] According to at least one embodiment, a communication system for sending secure communications includes a communication component and a cryptographic label attached to the communication component. The cryptographic label includes a cryptoprocessor disposed therein, and also a processor coupled to cryptoprocessor disposed therein. The cryptographic
20 label also includes a set of electrical contacts that electrically couples the cryptographic label to the electrical contacts of the communication component. The cryptographic label enables a mobile device equipped with the communication component and the attached cryptographic label to send encrypted data using the cryptoprocessor in the cryptographic label. In an exemplary embodiment, the communication component can be a SIM card.

25 **[0010]** According to at least one embodiment, a method for enabling the transmission of secure communications from a communication device using a cryptographic label attached to a communication component of the communication device includes receiving a message in the cryptographic label, and determining if the message is associated with a secure operation. A secure operation can include one or more of encryption, decryption, message authentication code
30 generation or verification, hash generation or verification, or other functions to be performed by

the cryptographic label. If it is determined that the message is associate with a secure operation, a cryptographic operation is performed, by a cryptographic processor disposed in the cryptographic label, on the data or information associated with the secure operation. The data encrypted by the cryptographic processor is sent from the cryptographic label to the communication device for transmission in a secure communication. If the message is determined to be associated with a non-secure operation, the message is passed through to the communication component. In an exemplary embodiment, the communication device can be a mobile phone, the communication component can be a SIM card, and the secure communication can be sent as a encrypted Short Message Service (SMS) message, an Unstructured Supplementary Service Data (USSD) message, a Near Filed Communication (NFC) communication, or a Radio Frequency (RF) communication.

[0011] These and other embodiments of the invention are described in further details below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] Fig. 1 illustrates a cryptographic expansion device and a communication component of a communication device, according to one embodiment of the present invention.

[0013] Fig. 2A illustrates a cross-sectional view of a cryptographic expansion device, according to one embodiment of the present invention.

[0014] Fig. 2B illustrates a top view of a cryptographic expansion device, according to one embodiment of the present invention.

[0015] Fig. 2C illustrates a bottom view of a cryptographic expansion device, according to one embodiment of the present invention.

[0016] Fig. 3 illustrates a block diagram of the components of a cryptographic expansion device, according to one embodiment of the present invention.

[0017] Fig. 4 illustrates a conceptual block diagram of the functional blocks of a cryptographic expansion device, according to one embodiment of the present invention.

[0018] Fig. 5 illustrates a communication system for sending and receiving secure communications using a cryptographic expansion device, according to one embodiment of the present invention.

[0019] Fig. 6 illustrates a diagram showing the process of initializing a communication component in a communication device equipped with a cryptographic expansion device, according to one embodiment of the present invention.

[0020] Fig. 7 illustrates a diagram showing the process of installing a user menu in a communication device equipped with a cryptographic expansion device, according to one embodiment of the present invention.

[0021] Fig. 8 illustrates a diagram showing the process of performing a non-secure operation in a communication device equipped with a cryptographic expansion device, according to one embodiment of the present invention.

[0022] Fig. 9 illustrates a diagram showing the process of performing a secure operation in a communication device equipped with a cryptographic expansion device, according to one embodiment of the present invention.

[0023] Fig. 10 illustrates a diagram showing the process of setting up a secure communication channel between devices using a cryptographic expansion device, according to one embodiment of the present invention.

[0024] Fig. 11 illustrates a flow diagram of performing a secure operation with a cryptographic expansion device, according to one embodiment of the present invention.

[0025] Fig. 12 illustrates a block diagram of a communication device, according to one embodiment of the present invention.

DETAILED DESCRIPTION

[0026] Embodiments of the present invention disclose a cryptographic expansion device that can be attached to a communication component of a communication device to enable the communication device to perform cryptographic operations on communications sent to and from the communication device. The cryptographic expansion device includes embedded processors

and storage capabilities that can be used to implement a Federal Information Processing Standards (FIPS) compliant hardware security module (HSM) to provide the communication device with the set of security features and functions as found in industry-standard HSMs. When used with a communication device, the cryptographic expansion device enables the

5 communication device to send and received end-to-end secure communications, and enables mobile operators to utilize their otherwise unsecure communication channels to send and receive encrypted communications. Furthermore, the cryptographic expansion device according to various embodiments can be used with a communication device without requiring any changes to the internal software or hardware of the communication device and without requiring any
10 modification to the communication protocols of the communication device. Thus, the cryptographic expansion device according to embodiments of the invention can be widely deployed in a cost-effective and efficient way. In some embodiments, the end-to-end secure communications enabled by the cryptographic expansion device can be utilized by a user of the communication device to perform financial and/or banking transactions.

15 **[0027]** Examples of the security features that the cryptographic expansion device can provide include running a secure operating system and secure key management related functions such as cryptographic key generation, configuration of security limits and capabilities of the cryptographic keys, cryptographic keys backup and recovery, secure cryptographic keys storage, and revocation and destruction of cryptographic keys. The cryptographic expansion device can
20 encrypt and decrypt data using various encryption standards and protocols including but not limited to Advance Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard/Algorithm (TDES/TDEA), Secure Socket Layer (SSL), Blowfish, Serpent, Twofish, International Data Encryption Algorithm (IDEA), Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Tiny Encryption Algorithm (TEA), extended TEA (XTEA),
25 and/or other encryption algorithms or protocols. The cryptographic expansion device can also generate and verify message authentication codes (MAC) and cryptographic hashes on communications sent to and from a communication device.

[0028] It should be appreciated that the cryptographic expansion device according to embodiments of the invention uses dedicated cryptographic hardware components provided in
30 the cryptographic expansion device to perform cryptographic operations. This is different from

software encryption technologies that use software with a general purpose processor to perform encryption, and provides enhanced security protection over such software encryption technologies. In some embodiments, the cryptographic expansion device is implemented as a dual processing units device that includes a FIPS compliant secure processing unit and a public processing unit. This division in hardware roles introduces an additional level of security by providing a physical and logical separation between interfaces that are used to communicate critical security parameters and other interfaces that are used to communicate other data. Furthermore, the cryptographic expansion device can also provide a tamper-resistant mechanism that provides a high risk of destroying components in the cryptographic expansion device and the cryptographic keys stored therein, if any attempt is made to remove or externally access the cryptographic expansion device.

[0029] As used herein, the term "secure communication" refers to a communication that includes at least some portion of the communication that is sent or received in an encrypted format. The term "secure operation" refers to a process or a function that involves performing one or more cryptographic operation. Examples of a "secure operation" can include sending or receiving of a secure or encrypted communication, or performing a financial or banking transaction with encrypted data. The term "cryptographic operation" refers to any of encryption, decryption, MAC generation or verification, hash generation or verification, and/or any of the functions provided by the cryptographic expansion device as described herein. The term "non-secure communication" refers to a communication that is sent or received in plaintext form. The term "non-secure operation" refers to a process or a function that does not involve performing a secure operation.

[0030] According to various embodiments, the cryptographic expansion device can be attached to a communication component of a communication device to enable the communication device to send and receive secure communications. A communication device is a device that is capable of sending and receiving communications with a recipient device. The communication device can be a mobile device such as a mobile phone or other types of portable communication device (e.g., a personal digital assistant, portable computing devices such as tablet computers or laptops, or portable multi-functional devices that can send and receive communications such as portable media players/readers, portable gaming devices, etc.). The recipient device that the

communication device communicates with can be another communication device, a payment device such as point-of-sale (POS) device or an automated teller machine (ATM), networking equipment, and/or telecommunication equipment of a mobile network operator. In some embodiments of the present invention, the communication device may lack the capability to perform cryptographic operations to encrypt and decrypt communications sent to and from the communication device. A cryptographic expansion device can be attached to a communication component of the communication device to provide the communication device with the capability to perform cryptographic operations. In other embodiments, the communication device may be capable of performing some cryptographic operations, for example, to encrypt or decrypt data using encryption software. In such embodiments, a cryptographic expansion device can still be used with the communication device to expand and/or enhance the cryptographic capabilities of the communication device, for example, to provide encryption algorithms that may otherwise be unavailable in the encryption software of the communication device.

[0031] According to some embodiments, the communication component that the cryptographic expansion device attaches to is a user-removable communication component of a communication device. For example, the communication component can be a subscriber identity module (SIM) card or other types of communication card that is used in conjunction with the communication device to send and receive communications. The communication component can also be other types of user-removable component of a communication device such as various types of memory card, for example, a secure digital (SD) memory card that can be used in conjunction with the communication device to send and receive communications.

[0032] The communication component of a communication device can come in various form factors. For example, in embodiments in which the communication component is a SIM card, the communication component can have a form factor according to a full-sized SIM card or a mini-SIM card as specified in the ISO/IEC 7810 standard, or a micro-SIM card or a nano-SIM card as specified in the ETSI TS 102 221 standard. In other embodiments, for example, in which the communication component is a SD memory card, the communication component can have a form factor according to a full-size SD card, a micro-SD card, or a mini-SD card as specified in the SD standard of the Secure Digital Association.

[0033] Physical Characteristics of Cryptographic Expansion Device

[0034] According to various embodiments, the cryptographic expansion device is a circuit board with integrated circuits implementing a hardware security module (HSM) disposed therein. The cryptographic expansion device can be a flexible printed circuit board in the form of a label. Fig. 1 illustrates a cryptographic expansion device and a communication component according to one embodiment of the invention. According to the embodiment as shown, the cryptographic expansion device is a cryptographic label 100 with one or more integrated circuits implementing a hardware security module (HSM) 150 disposed therein, and the communication component that the cryptographic label 100 attaches to is a SIM card 190 (e.g., a mini-SIM card as shown). It should be understood that while the description and explanation provided below are made with reference to a particular embodiment, the description and explanation provided below are applicable to and can be adapted for other embodiments, for example, embodiments in which the cryptographic expansion device is used with a SIM card with a different form factor, or in which the cryptographic expansion device is used with other types of communication component such as a memory card.

[0035] It should also be noted that although cryptographic label 100 is shown to be semi-transparent in Fig. 1, cryptographic label 100 is shown as such for illustrative purposes. Thus, in some implementations, cryptographic label 100 can be opaque, and HSM 150 and the underlying SIM card 150 may not be visible from the top of cryptographic label 100.

[0036] HSM 150 includes a public processing unit (PPU) 130 which can be implemented with one or more processors or controllers, and a secure processing unit (SPU) 120 which can be implemented with one or more cryptoprocessors. In some embodiments, HSM 150 is a packaged semiconductor chip that includes both SPU 120 and PPU 130 in a single package, but with a logical and physical separation between SPU 120 and PPU 130. In other embodiments, SPU 120 and PPU 130 can be individually packaged semiconductor chips or semiconductor dies that are coupled together in cryptographic label 100 to implement HSM 150.

[0037] Cryptographic label 100 includes a coupling element that can be used to attach cryptographic label 100 to SIM card 190. In some embodiments, the coupling element is an adhesive material 140 disposed on cryptographic label 100. Thus, cryptographic label 100 can be applied to the surface of SIM card 190 similar to an adhesive label or a sticker. In other embodiments, the coupling element can be a mechanical mechanism such as notches provided on

cryptographic label 100 or a clip that can be used to physically secure cryptographic label 100 to SIM card 190. In some embodiments, cryptographic label 100 can have a flexible or semi-flexible substrate, for example, to facilitate the application of cryptographic label 100 to the surface of SIM card 190. Cryptographic label 100 can also have a rigid or semi-rigid substrate, for example, to provide stiffness to protect the cryptographic label 100.

[0038] According to various embodiments, cryptographic label 100 can have various different form factors. The thickness of cryptographic label 100 is made to be thin enough such that when cryptographic label 100 is attached to SIM card 190, SIM card 190 can still be inserted or removed from a SIM card receiving slot of a communication device such as a mobile phone. In one embodiment, the thickness of cryptographic label 100 is less than 100 microns (um). In other embodiments, the thickness of cryptographic label 100 can be less than 150 um, 200 um, 250 um, or 300 um.

[0039] In some embodiments, cryptographic label 100 can have a form factor with planar dimensions (e.g., length and/or width) that are substantially the same as the planar dimensions of SIM card 190 as shown in Fig. 1. One or more planar dimensions of cryptographic label 100 can be within 1%, 2%, 5%, 10%, 15%, or 20% of the corresponding planar dimension of SIM card 190. For example, in a particular embodiment in which the length of SIM card 190 is 25 millimeters (mm) and the length of cryptographic label 100 is within 10% of the length of SIM card 190, the length of cryptographic label 100 can be between 22.5 mm (90% of 25 mm) and 27.5 mm (110% of 25 mm).

[0040] In other embodiments, cryptographic label 100 can have a form factor with one or more planar dimensions that is different than the corresponding planar dimension of the communication component with which cryptographic label 100 attaches to, if the size of cryptographic label 100 does not prevent the communication component from being used with a communication device. In other words, referring to the embodiment shown in Fig. 1, the planar dimensions of cryptographic label 100 should allow SIM card 190 attached with cryptographic label 100 to fit into a SIM card receiving slot of a communication device. It should be noted that this does not mean that the planar dimensions of cryptographic label 100 has to be smaller than SIM card 190. For example, in some embodiments, cryptographic label 100 can be longer than SIM card 190 and can extend out of a SIM card receiving slot of a communication device if the

communication device can tolerate such a configuration. In other embodiments in which the substrate of cryptographic label 100 is a flexible substrate, when cryptographic label 100 is applied to SIM card 190, the excess portions of cryptographic label 100 that extends over the surface of SIM card 190 can be folded over to wrap around SIM card 190.

5 [0041] Furthermore, in some embodiments, a cryptographic label with a form factor corresponding to one type of SIM card can be used with a SIM card that has a different form factor. For example, although cryptographic label 100 as shown in Fig. 1 has a form factor with planar dimensions that are substantially the same as a mini-SIM card, cryptographic label 100 can be attached to a standard SIM card instead of a mini-SIM card. Similarly, a cryptographic
10 label having a form factor with planar dimensions that are substantially the same as a micro-SIM card can be attached to a mini-SIM card instead of a micro-SIM card.

[0042] Fig. 2A illustrates a cross sectional view along the length of cryptographic label 100 according to one embodiment. Cryptographic label 100 includes a set of electrical contacts 115 disposed on the top side or on the upper surface of cryptographic label 100, a set of electrical
15 contacts 110 disposed on the bottom side or on the bottom surface of cryptographic label 100, and a hardware security module (HSM) 150 disposed in cryptographic label 100. According to some embodiments, HSM 150 can be completely embedded in the substrate of cryptographic label 100 as shown. In other words, HSM 150 does not protrude out of cryptographic label 100 and is not visible from the top or bottom of cryptographic label 100. In other embodiments,
20 HSM 150 may extend slightly over the top and/or bottom of the substrate of cryptographic label 100, creating a bump on the top and/or bottom surface of cryptographic label 100.

[0043] As mentioned above, HSM 150 can be a single packaged semiconductor chip. Alternatively, SPU 120 and PPU 130 can be individually packaged semiconductor chips or semiconductor dies that are coupled together in cryptographic label 100 to implement HSM 150.
25 While SPU 120 and PPU 130 are shown as being positioned side by side in Fig. 1, in other embodiments, SPU 120 and PPU 130 can be vertically stacked in the substrate of cryptographic label 100. Interconnects and circuits electrically coupling the various components (i.e. electrical contacts 110, electrical contacts 155, HSM 150, and/or SPU 120 and PPU 130) of cryptographic label 100 can be formed by etching the circuits into the substrate of cryptographic label 100,
30 screen-printing the circuits onto the substrate, or by providing the components of cryptographic

label 100 with solderable contacts that when heated, would bind to circuitry in the substrate to form the interconnects and circuits.

[0044] Fig. 2B illustrates a top view of cryptographic label 100 according to one embodiment.

It should be understood that HSM 150 which includes SPU 120 and PPU 130 is shown with

5 dotted lines to indicate that these components may not be visible from the top side of cryptographic label 100. The set of electrical contacts 115 on the top side of cryptographic label 100 is used for interfacing cryptographic label 100 to a communications device; that is, to electrically couple cryptographic label 100 to a SIM card reader of a communications device when a SIM card attached with cryptographic label 100 is inserted into a SIM card receiving slot
10 of the communication device. Thus, the set of electrical contacts 115 is positioned on the top side of cryptographic label 100 to align with the electrical contacts of a SIM card reader of the communication device. According to some embodiments, the set of electrical contacts 115 can have eight contact pads, as shown. In other embodiments, if some of the available signals are not used, the set of electrical contacts 115 may have less than eight contact pads, for example, six
15 contact pads.

[0045] Fig. 2C illustrates a bottom view of cryptographic label 100 according to one

embodiment. It should be understood that HSM 150 which includes SPU 120 and PPU 130 is shown with dotted lines to indicate that these components may not be visible from the bottom of

cryptographic label 100. The set of electrical contacts 110 on the bottom side of cryptographic

20 label 100 is used for interfacing cryptographic label 100 to a communications component, for example, to electrically couple cryptographic label 100 to a communication card such as SIM

card 190. Thus, the set of electrical contacts 110 is positioned on the bottom side of

cryptographic label 100 to align with the electrical contacts of the communications component

(e.g., SIM card 190) that cryptographic label 100 attaches to. According to some embodiments,

25 the set of electrical contacts 110 may have eight contact pads, as shown. In other

embodiments, if some of the available signals are not used, the set of electrical contacts 110

may have less than eight contact pads, for example, six contact pads. Furthermore, the number

of contact pads in the set of electrical contacts 110 on the bottom side of cryptographic label 100

can be different than the number of contact pads in the set of electrical contacts 115 on the top

30 side of cryptographic label 100.

[0046] According to some embodiments, an adhesive material 140 is disposed around the contact pads on the bottom side of cryptographic label 100, and may extend to the edges of the bottom surface of cryptographic label 100. The adhesive material 140 can be used to secure cryptographic label 100 to SIM card 190. In addition to securing cryptographic label 100 to SIM card 190, in one embodiment, the adhesive material 140 can also serve as a tamper-resistant mechanism to provide a high risk of destroying cryptographic label 100 if an attempt is made to remove cryptographic label 100 from SIM card 190 after cryptographic label 100 has been attached to SIM card 190. For example, after cryptographic label 100 has been applied to the surface of SIM card 190, if an attempt is made to remove cryptographic label 100 from SIM card 190 by peeling off cryptographic label 100, the adhesive material 140 may rip apart the contact pads of cryptographic label 100, and/or the interconnects and circuits electrically coupling the components of cryptographic label 100 to render cryptographic label 100 unusable. Alternatively or in addition, the adhesive material 140 may rip apart portions of SIM card 190 to render SIM card 190 unusable as well if an attempt is made to remove cryptographic label 100 from SIM card 190.

[0047] Internal Components and Features of Cryptographic Expansion Device

[0048] Fig. 3 shows a block diagram illustrating the hardware components of a cryptographic expansion device 300 (e.g., cryptographic label 100 of Figs. 1 and 2A-C), according to one embodiment. Cryptographic expansion device 300 includes a public processing unit (PPU) 330, and a secure processing unit (SPU) 320 coupled to PPU 330. It should be noted that although SPU 320 is coupled to PPU 330, cryptographic expansion device 300 provides a logical and/or physical separation between SPU 320 and PPU 330. A “physical separation” refers to some physical boundary between SPU 320 and PPU 330. For example, SPU 320 and PPU 330 can be implemented with and manufactured as separate semiconductor dies or separately packaged semiconductor chips, and the physical boundary of the dies or chips can serve as the physical separation. A “logical separation” refers to the separation of the communication interface and storage memory between SPU 320 and PPU 330. As shown in Fig. 3, SPU 320 has its own communication interfaces 340, 345, and 350, which is separate from communication interface 360 of SPU 320. PPU 330 also has its own memory 338, which is separate from secure memory 390 of SPU 320. As will be explained below, the logical and/or physical separation provided

between SPU 320 and PPU 330 creates a division in hardware roles to protect SPU 320 and the contents stored in secure memory 390 from unauthorized accesses.

[0049] According to some embodiments, PPU 330 includes processor 337, memory 338, a communication device interface 340, a communication component interface 345, and a PPU-to-SPU interface 350. Processor 337 can be implemented as one or more processors or controllers. Memory 338 is coupled to processor 337, and provides storage to store data and executable code that when executed by processor 337, causes processor 337 to run an operating system (OS) and/or applications that can be compliant with Payment Card Industry (PCI) and International Organization for Standardization (ISO) standards to manage the functionality and operations of cryptographic expansion device 300, and to process the exchange of information between the various interfaces of PPU 330.

[0050] Communication device interface 340 is coupled to a set of electrical contacts 315 that interfaces with a communication device such as a mobile device (e.g., a mobile phone), and provides a set of signals that can include a clock signal and one or more data input/output (I/O) signals to send and receive commands and information between PPU 330 and the communication device. Communication component interface 345 is coupled to a set of electrical contacts 315 that interfaces to a communication component such as a communication card (e.g., a SIM card), and provides a set of signals that can include a clock signal and one or more data input/output (I/O) signals to send and receive commands and information between PPU 330 and the communication component. PPU-to-SPU interface 350 is coupled to SPU 320, and provides a set of signals that can include a clock signal and one or more data input/output (I/O) signals to send commands and information such as encryption and decryption requests to SPU 320, and to receive commands and information such as encryption and decryption results from SPU 320. Because of the logical and physical separation between SPU 320 and PPU 330, SPU 320 is exposed to PPU 330 only, and is not accessible to the communication device or to the communication component, except through PPU 330. Hence, PPU 330 can serve as a firewall or a gatekeeper to ensure unauthorized or unwanted communications such as hacking attempts are not sent to SPU 320.

[0051] According to some embodiments, SPU 320 includes cryptoprocessor 380, secure memory 390, and SPU-to-PPU interface 360. SPU 320 can also include tamper detection

sensors 370. As mentioned above, SPU 320 is accessible from PPU 330 only, and receives commands and information from PPU 330 through SPU-to-PPU interface 360. SPU-to-PPU interface 360 provides a set of signals that can include a clock signal and one or more data input/output (I/O) signals coupled to PPU-to-SPU interface 350 that SPU 320 can use to communicate with PPU 330. In some embodiments, SPU 320 will only respond to encryption and decryption requests to perform cryptographic operations from PPU 330 received through SPU-to-PPU interface 360.

[0052] Cryptoprocessor 380 can be implemented as one or more cryptographic processors. A cryptographic processor is different from a general purpose processor in that a cryptographic processor includes dedicated circuitry and hardware such as one or more cryptographic arithmetic logic units (ALU) 382 that are optimized to perform computational intensive cryptographic functions. Cryptographic ALU 382 can include optimized pipelines and widen data buses to enable cryptoprocessor 380 to perform cryptographic operations faster and more efficiently than general purpose processors.

[0053] Secure memory 390 is coupled to cryptoprocessor 380, and can be partitioned into a cryptographic key storage 392 and a data storage 394. Data storage 394 can be read and written by cryptoprocessor 380, and provides storage memory to store user data such as data that are received on SPU-to-PPU interface 360 from PPU 330, and encryption and decryption results that are sent to PPU 330 through SPU-to-PPU interface 360. Cryptographic key storage 392 can be read-only to cryptoprocessor 380, and is used to store cryptographic keys and encryption algorithms. The cryptographic keys and algorithms stored in cryptographic key storage 392 are provisioned by the manufacturer during manufacturing of cryptographic expansion device 300, and cannot be altered by an external source without a master key that is only known to the manufacturer and/or authorized parties who are authorized to provision cryptographic expansion device 300 such as a mobile network operator or a wireless service provider. In some embodiments, the contents of cryptographic key storage 392 are never transmitted outside of SPU 320, and is inaccessible by PPU 330. The cryptographic keys and algorithms stored in cryptographic key storage 392 can be provisioned to perform various encryption standards and protocols including but not limited to Advance Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard/Algorithm (TDES/TDEA), Secure Socket

Layer (SSL), Blowfish, Serpent, Twofish, International Data Encryption Algorithm (IDEA), Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Tiny Encryption Algorithm (TEA), extended TEA (XTEA), and/or other encryption algorithms or protocols.

[0054] In some embodiments, SPU 320 may also include tamper detection sensors 370 to detect external attempts to tamper with cryptographic expansion device 300. For example, tamper detection sensors 370 may include temperature sensors to detect temperatures that may be indicative of someone attempting to desolder components of cryptographic expansion device 300, and/or mechanical sensors to sense structural changes to cryptographic expansion device 300 that may be indicative of someone attempting to dissect or cut open cryptographic expansion device 300. Tamper detection sensors 370 may also include electrical sensors to sense certain voltage, current, or impedance changes to the circuitry of cryptographic expansion device 300 that may be indicative of someone attempting to probe the components of cryptographic expansion device 300, and/or electromagnetic sensors to sense certain radiation such as X-rays that may be indicative of someone attempting to examine cryptographic expansion device 300.

In some embodiments, tamper detection sensors 370 may include circuitry that can erase and whip out the contents of secure memory 390 to render SPU 320 and/or cryptographic expansion device 300 unusable in response to detecting an attempt to tamper with cryptographic expansion device 300. Cryptographic expansion device 300 can also be configured with organic or soluble interconnects that can be dissolved by a solvent released by tamper detection sensors 370 in response to detecting an attempt to tamper with cryptographic expansion device 300.

[0055] Fig. 4 shows a conceptual block diagram illustrating the functional features of a cryptographic expansion device 400, according to one embodiment. Cryptographic expansion device 400 can be implemented with, for example, the hardware components described with reference to the cryptographic expansion device 300 of Fig. 3. PPU 430 of cryptographic expansion device 400 includes an operating system (OS) 434, a communication device application programming interface (API) 432, and a communication component API 433. OS 434, communication device API 432, and communication component API 433 together form an access layer 431, which represents the publicly accessible portion of cryptographic expansion device 400. By “publicly accessible,” it is meant that any device or components of communication device 415 (e.g., a mobile phone) that can communicate directly with

communication component 410 (e.g., a SIM card), or with a communication component reader of a communication device 415 (e.g., a SIM card reader of a mobile device), would be able to send and receive commands and information to and from access layer 431.

[0056] Communication device API 432 provides a programming interface to translate
5 commands and information received from communication device 415 into instructions and data that OS 434 can process and execute, and vice versa. For example, communication device API 432 may translate commands from communication device 415 according to a mobile phone's SIM toolkit protocol into instructions and data that OS 434 can process and execute to respond to the commands, and vice versa. Communication component API 433 provides a programming
10 interface to translate commands and information received from communication component 410 into instructions and data that OS 434 can process and execute, and vice versa. For example, communication component API 433 may translate commands from communication component 410 according to a SIM card's SIM toolkit protocol into instructions and data that OS 434 can process and execute to respond to the commands, and vice versa.

[0057] OS 434 manages the functionality and operations of cryptographic expansion device 400, and responds to commands and information from communication device 415 (e.g., a mobile device such as a mobile phone) and/or communication component 410 (e.g., a SIM card). The functionality and operations of cryptographic expansion device 400 that OS 434 can manage includes responding to user input received on communication device 415 that relates to
20 cryptographic operations, masking PIN entries on a user interface of communication device 415, creating ISO PIN blocks in SPU 420, sending encryption and decryption requests to SPU 420 for secure communications sent to and from a communication interface of communication device 415, sending requests to SPU 420 to create or verify MAC or hash values for messages or portions of messages sent to and from a communication interface of communication device 415,
25 providing certificates for HTTPS applications, storing encrypted communications history, providing basic encryption to external applications, and managing commands and information exchange through the various interfaces such as passing through commands and information between communication device 415 to communication component 410.

[0058] For example, in response to encryption and decryption commands received from
30 communication device 415 on communication device API 432, OS 434 can send encryption and

decryption requests and associated data to SPU 420. OS 434 may access and process information stored in communication component 410 in response to a command to perform as such received from communication device 415 on communication device API 432. OS 434 can also access information stored in communication component 410 and forward the information to SPU 420 in response to encryption and decryption commands involving such information. OS 434 can forward encryption and decryption results from SPU 420 to communication device 415 and/or communication component 410. OS 434 can also issue commands to communication device 415 and/or communication component 410, for example, commands to request communication device 415 to send a secure communication with data encrypted by SPU 420.

[0059] For non-secure commands and information (i.e. commands and information that do not involve cryptographic operations), OS 434 can pass through or forward the non-secure commands and information between communication device 415 and communication component 410. For example, in response to non-secure commands and information from communication device 415 intended for communication component 410 received on communication device API 432, OS 434 can pass through or forward the non-secure commands and information to communication component 410 through communication component API 433. In response to non-secure commands and information from communication component 410 intended for communication device 415 received on communication component API 433, OS 434 can pass through or forward the non-secure commands and information to communication device 415 through communication device API 432.

[0060] SPU 420 of cryptographic expansion device 400 includes a cryptographic module API 421 and cryptographic module 422. Cryptographic module API 431 provides a programming interface to translate commands and information received from OS 434 into instructions and data that cryptographic module 422 can process and execute, and vice versa. For example, OS 434 may send an encryption/decryption request to SPU 420, and cryptographic module API 431 may translate the encryption/decryption request into an encryption/decryption instruction for cryptographic module 422 to execute. In some embodiments, cryptographic module API 431 may also include, in the translated encryption/decryption instruction, which particular encryption algorithm cryptographic module 422 should use based on the particular application that is requesting the cryptographic operation.

[0061] According to various embodiments, cryptographic module 422 includes a secure application module 441, an encryption/decryption module 442, a secure key module 451, a seed key module 452, a random number generator 453, an ISO 0/1 PIN module 454, a MAC/HASH module 455, and a certificate module 456. In other embodiments, cryptographic module 422 may include additional modules to perform other cryptographic operations. Secure application module 441 can store one or more secure applications such as mobile banking applications or contactless payment applications. Secure application module 441 can process user input selecting a particular function of the secure applications stored therein, and can respond with one or more commands instructing communication device 415 to perform certain operations, for example, to send an encrypted communication or send a sequence of messages to initiate communication with another device to carry out the user selected function. Secure application module 441 can also instruct encryption/decryption module 442 to perform specific cryptographic operations depending on the user selected function.

[0062] Encryption/decryption module 442 can store and execute various encryption algorithms such as Advance Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard/Algorithm (TDES/TDEA), Blowfish, Serpent, Twofish, International Data Encryption Algorithm (IDEA), Rivest, Shamir, & Adleman (RSA), Digital Signature Algorithm (DSA), Tiny Encryption Algorithm (TEA), extended TEA (XTEA), and/or other cryptographic or encryption algorithms. In response to encryption and decryption requests from PPU 430 or from secure application module 441, encryption/decryption module 442 can look up the requested encryption algorithm, obtain any necessary keys from other modules in cryptographic module 422, perform the encryption/decryption request, and respond with the encrypted/decrypted data.

[0063] Secure key module 451 stores the set of cryptographic or encryption keys that are used in the various encryption algorithms performed by encryption/decryption module 442. The encryption keys can include symmetric keys and/or asymmetric keys. Seed key module 452 stores a set of seed keys that are used to initialize the encryption/decryption module 442 in certain encryption algorithms such as AES. Seed key module 452 also stores seed keys that are used by random number generator 453 to generate random numbers used in certain encryption algorithms such as RSA and DSA. The encryption keys stored in secure key module 451 and/or

the seed keys stored in seed key module 452 are provisioned during manufacturing, and cannot be altered by an external source without a master key that was used during manufacturing to program cryptographic module 422. The encryption keys and seed keys can also be provisioned to be specific to a particular cryptographic expansion device, and hence the encryption keys and seed keys can be user-specific and unique to the user of the cryptographic expansion device 400. One advantage of providing user-specific keys is that if the cryptographic keys stored in cryptographic module 422 is somehow compromised, the infiltration will be isolated to a single user, and the remaining user base of the mobile network will not be compromised. The affected user's keys can be changed without impacting the configuration of the remaining user base.

[0064] In some embodiments, cryptographic module 422 includes an ISO PIN module 454 to mask a user's PIN entry into the communication device 415 and to generate PIN blocks (e.g., ISO format 0/1 PINs) in accordance with ISO 9564 standard. The PIN blocks generated by ISO PIN module 454 stores PINs in an encrypted format that are used to verify a user's identity in banking transactions. The encrypted PINs stored in the PIN blocks of ISO PIN module 454 can be passed from SPU 420 to PPU 430 to be included in secure communications sent from communication device 415. It should be noted that the PINs stored in ISO PIN module 454 are never stored in plaintext form, but are instead stored in an encryption format.

[0065] Cryptographic module 422 also include Message Authentication Code (MAC) / Hash module 455 to generate and verify MACs and/or hashes for secure communications sent to and from communication device 415. A MAC or a hash can be generated for a message or a portion of the message such that the recipient can verify the message's data integrity and authenticity. Cryptographic module 422 can also include a certificate module to provide certificates such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL) certificates used to verify a user's identity in Hypertext Transfer Protocol Secure (HTTPS) applications such as web applications accessed on a web browser of communication device 415.

[0066] Functional Operations of Cryptographic Expansion Device

[0067] Fig. 5 illustrates a communication system 500 for sending and receiving secure communication according to an exemplary embodiment of the present invention.

Communication system 500 includes a cryptographic expansion device attached to a communication component installed in a communication device. In the exemplary embodiment

as shown, the cryptographic expansion device is a cryptographic label 501, the communication component is a SIM card 510, and the communication device is a mobile phone 515. It should be understood that in other embodiments, the cryptographic expansion device can be any of the embodiments described herein, communication device can be other types of communication device described above, and the communication component can be other types of user-removable communication component of a communication device such as a memory card.

[0068] In accordance with embodiments of the present invention, when mobile device 515 is equipped with cryptographic label 501, mobile device 515 can use one or more of the communication interface available in mobile device 515 to send and receive end-to-end secure communications with a recipient device. For example, cryptographic label 501 can enable mobile device 515 to send encrypted Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) messages using the cellular interface of communication device 515. In some embodiments in which mobile device 515 has a Near Field Communication (NFC) or Radio Frequency (RF) interface, cryptographic label 501 can enable mobile device 515 to send encrypted data in NFC or RF communication using the NFC or RF interface of communication device 515. Thus, cryptographic label 501 can be used with mobile device 515 to encrypt and decrypt any type of communication that mobile device 515 is capable of sending and receiving. In some embodiments, the end-to-end secure communications enabled by the cryptographic label 501 can be utilized by a user of the communication device to access mobile banking services such as managing financial accounts and performing various financial and/or banking transactions. Examples of these mobile banking services include but are not limited to making mobile payments, making mobile money transfers, buying and selling of securities, checking account balances, and or making other financial account inquiries.

[0069] When cryptographic label 501 is attached to SIM card 510 and installed in a SIM card receiving slot of mobile device 515, cryptographic label 501 can provide and/or expand the capability of mobile device 515 to perform cryptographic operations to send and receive secure communications. It should be appreciated that in various embodiments, cryptographic label 501 provides mobile device 515 with the cryptographic capabilities without requiring any modifications to the internal hardware and/or software of mobile device 515 and without requiring any modifications to the internal hardware and/or software of SIM card 510.

According to various embodiments, SIM card 510 is a standard SIM card that conforms to the ISO/IEC 7810 or ETSI TS 102 221 standards, and cryptographic label 501 can be applied to the surface of SIM card 510 without requiring any physical modifications to the SIM card itself. For example, cryptographic label 501 can be attached to a standard SIM card and be used in a mobile device without requiring the SIM card to be cut or trimmed, and without requiring any holes or openings to be formed in the SIM card.

[0070] The interactions and the exchange of commands and information between cryptographic label 501, mobile device 515, and SIM card 510 in the exemplary communication system 500 according to one embodiment will now be described in more details with reference Figs. 6-9. It should be understood that while the description and explanation provided below are made with reference to the particular embodiment shown in Fig. 5, the description and explanation provided below are applicable to and can be adapted for other embodiments, for example, embodiments in which the cryptographic expansion device is used with other types of communication component such as a memory card. Furthermore, the description and explanation provided below are made with reference to commands according to SIM toolkit (STK) protocol to illustrate that cryptographic label 501 can interoperate with mobile device 515 using the protocol that mobile device 515 uses to communicate with SIM card 510. In other embodiments in which the communication device communicates with a communication component using a different protocol, the description and explanation provided below can be adapted to use the commands in accordance with that protocol such that cryptographic label 501 can interoperate with the communication device seamlessly with requiring any modifications to the software of the communication device.

[0071] Fig. 6 illustrates an SIM card initialization sequence according to one embodiment of the invention. When mobile device 515 powers up or is turned on, mobile device 515 issues a series of select file and read commands to the SIM card reader of the mobile device to read subscriber information from a SIM card to register the SIM card with a mobile network. Because cryptographic label 510 is attached to SIM card 510 and sits between SIM card 510 and mobile device 515, when cryptographic label 510 receives these commands from mobile device 515, cryptographic label 510 passes through or forwards these commands to SIM card 510.

[0072] For example, after power up, mobile device 515 may send a select file command 602 to select a designated file in the file system of SIM card 510 that stores subscriber information or other types of SIM card related information. Upon receiving the select file command 602, cryptographic label 501 determines that the file being requested is a file in the file system of SIM card 510, and passes through or forwards the select file command 602 to SIM card 510. SIM card 510 receives the select file command 602, accesses the requested file, and sends an response 604 towards cryptographic label 501 indicating that the requested file was accessed successfully and is ready to be read. Cryptographic label 501 then passes through or forwards response 604 to mobile device 515. In response to receiving response 604 notifying mobile device 515 that the requested file is ready to be read, mobile device 515 sends a read command 610 towards SIM card 510. Upon receiving the read command 610, cryptographic label 501 passes through or forwards the read command 610 to SIM card 510. In response to the read command 610, SIM card 510 sends file content 612 of the requested file towards mobile device 515. Depending on the file being requested, file content 612 may include subscriber information, location/region information, configuration information such as language preference, and/or other types of SIM card information. Upon receiving file content 612, cryptographic label 501 passes through or forwards file content 612 to mobile device 515. The above series of commands and exchange of information may occur multiple times to allow mobile device 515 to read any information stored in SIM card 510 that mobile device 515 may use during its SIM card initialization sequence.

[0073] After mobile device 515 finishes reading the information stored in SIM card 510, mobile device 515 may send a terminal profile 614 towards SIM card 510 to inform SIM card 510 of the properties and capabilities of mobile device 515. The terminal profile may include properties of the mobile device such as the types of communication interfaces available on the mobile device. Upon receiving terminal profile 614, cryptographic label 501 may inspect terminal profile 614 to learn the properties and capabilities of mobile device 515. Cryptographic label 501 then passes through or forwards terminal profile 614 to SIM card 510. SIM card 510 may send a response 616 towards mobile device to indicate that terminal profile 614 was successfully received. Upon receiving response 616, cryptographic label 501 passes through or forwards response 616 to mobile device 515.

[0074] Next, the process of installing a user menu that lists the features of SIM card 510 and cryptographic label 501 onto mobile device 515 according to one embodiment of the invention will be described with reference to Fig 7. After the SIM card initialization sequence of Fig. 6, mobile device 515 may send a fetch command 702 towards SIM card 510 to obtain any pending
5 commands that SIM card 510 wants mobile device 515 to perform. Upon receiving fetch command 702, cryptographic label 501 may pass through or forward fetch command 702 to SIM card 510. SIM card 510 may respond with a set-up-menu command 706 that includes a list of features of SIM card 510 to be included in the user menu of mobile device 515. Upon receiving set-up-menu command 706 from SIM card 510, cryptographic label 501 can add its own list of
10 user selectable features to the features of SIM card 510 listed in set-up-menu command 706, and generates a set-up-menu command 708 that lists the features of both SIM card 510 and cryptographic label 501. The list of features added by cryptographic label 501 can include, for example, mobile banking features such as a menu selection for making mobile payments, a menu selection for making mobile money transfer, a menu selection for a financial account inquiry, a
15 menu selection for making a contactless payment, and/or other menu selections for services related to financial or banking transactions that a user can perform using mobile device 515 equipped with cryptographic label 501. Cryptographic label 501 then sends set-up-menu command 708 that includes the list of features of both SIM card 510 and cryptographic label 502 to mobile device 515. In response to receiving set-up-menu command 708, mobile device 515
20 adds the list of features of SIM card 510 and cryptographic label 501 to the user menu of mobile device 515.

[0075] Mobile device 515 can send a terminal response 710 towards SIM card 510 to indicate that the user menu is set up successfully. Upon receiving terminal response 710, cryptographic label 501 passes through or forwards terminal response 710 to SIM card 510. SIM card 510 may
25 reply with a response 712 indicating acknowledgement of terminal response 710 towards mobile device 515. Cryptographic label 501 then passes through or forwards response 712 to mobile device 515. Mobile device 515 can then display to a user the features and services that cryptographic label 501 can provide on mobile device 515, and the user can select one or more features of cryptographic label 501 from the user menu of mobile device 515 to send secure
30 communication to perform various financial and/or banking transactions. A user can also select

non-secure features of SIM card 510, for example, to send unencrypted SMS messages, from the user menu of mobile device 515.

[0076] Fig. 8 illustrates a non-secure operation being performed with mobile device 515 using SIM card 510, according to one embodiment. When a user selects a feature of SIM card 510 to perform a non-secure operation (e.g., send unencrypted SMS, or display a message stored on SIM card 510, etc.) from the user menu of mobile device 515, mobile device 515 sends a menu selection command 802 indicating the selection of the non-secure operation towards SIM card 510. Upon receiving menu selection command 802, cryptographic label 501 determines that the menu selection command 802 is requesting a feature of SIM card 510. Cryptographic label 501 then passes through or forwards menu selection command 802 to SIM card 510. In response to receiving menu selection command 802, SIM card 510 sends a response 804 towards mobile device 515 to indicate the menu selection command 802 has been received. SIM card 510 processes menu selection command 802 and prepares one or more device commands to send to mobile device 515 to carry out the non-secure operation being requested.

[0077] Upon receiving response 804 indicating menu selection command 802 has been received by SIM card 510, cryptographic label 501 passes through or forwards response 804 to mobile device 515. Mobile device 515 may then send a fetch command 806 towards SIM card 510 to obtain any pending commands that SIM card 510 wants mobile device 515 to perform to carry out the non-secure operation selected by the user. Upon receiving fetch command 806, cryptographic label 501 passes through or forwards fetch command 806 to SIM card 510. SIM card 510 responds to fetch command 806 by sending a device command 808 towards mobile device 515 to instruct mobile device 515 to perform one or more functions of mobile device 515 to carry out the non-secure operation. For example, device command 808 may instruct mobile device 515 to send an unencrypted SMS over the cellular interface of mobile device 515, or display a stored SMS message on the screen of mobile device 515. Upon receiving device command 808 from SIM card 510, cryptographic label 501 passes through or forwards device command 808 to mobile device 515. Mobile device 515 then executes device command 808 to carry out the non-secure operation requested by the user.

[0078] Fig. 9 illustrates a secure communication being sent from mobile device 515 using cryptographic label 501, according to one embodiment. When a user selects a secure application

such as a mobile banking application in cryptographic label 501 from the user menu of mobile device 515 to perform a secure operation such as a financial and/or banking transaction, for example, to make a mobile payment or to check an account balance, mobile device 515 sends a menu selection command 902 indicating the secure operation the user wants to perform to
5 cryptographic label 501. Upon receiving menu selection command 902, cryptographic label 501 determines that the menu selection command 902 is requesting a secure application of cryptographic label 501 to perform a secure operation.

[0079] Depending on the secure operation selected by the user, cryptographic label 501 may optionally retrieve information stored in cryptographic label 501 such as an encrypted PIN to
10 carry out the secure operation. In some embodiments, certain information stored in SIM card 510 may also be used to carry out the secure operation. For example, the secure operation may include sending a secure communication from mobile device 515 to a recipient device, and the unique serial number (ICCID) of SIM card 510 and/or the international mobile subscriber identity (IMSI) of SIM card 510 may be included in the secure communication to verify the
15 identity of the SIM card holder. In such embodiments, cryptographic label 501 may optionally send a select file command 904 to SIM card 510 to access the designated file storing the information in SIM card 510. In response to receiving select file command 904, SIM card 510 sends a response 906 to cryptographic label 501 indicating the designated file has been selected and is ready to be read. Cryptographic label 501 then sends a read command to 908 to SIM card
20 510 to read the information from the designated file. In response to read command 908, SIM card sends file content 910, for example, the ICCID and/or IMSI of SIM card 510, to cryptographic label 501.

[0080] Next, cryptographic label 501 sends a response 912 to mobile device 515 to acknowledge that the menu selection command 902 was received. Mobile device 515 then sends
25 a fetch command 914 to cryptographic label 501 to obtain any pending commands that cryptographic label 501 wants mobile device 515 to perform to carry out the secure operation. In some embodiments, depending on the secure operation selected by the user, in response to receiving fetch command 914, cryptographic label 501 may optionally send a display command (not shown) to mobile device 515 to instruct mobile device 515 to prompt a user for input on the
30 display screen of mobile device, for example, to prompt the user to enter a PIN, account

information, payment recipient information, or other information related to the secure operation being performed. When the user enters the requested information on the user interface of mobile device 515, mobile device 515 sends a user-input-event command (not shown) to cryptographic label 501 to notify cryptographic label 501 that user input has been received. Cryptographic label 501 can then send a get-user-input command 916 to mobile device 515 to request the user input. In response, mobile device 515 sends the user input 918 to cryptographic label 501. Cryptographic label 501 may perform cryptographic operations on the user input such as encrypting the user input using any of the encryption algorithms stored in cryptographic label 501, or generate a MAC or hash of the user input. Cryptographic label 501 sends a response 920 to mobile device acknowledging the user input has been received.

[0081] Mobile device 515 may send another fetch command (not shown) to cryptographic label 501 to obtain further device commands that cryptographic label 501 wants mobile device 515 to execute to carry out the secure operation. Thus, mobile device 515 and cryptographic label 501 can optionally exchange a series of fetch commands and device commands in response to those fetch commands to instruct mobile device 515 to perform various functions to carry out the secure operation selected by the user. Furthermore, depending on the secure operation selected by the user, the information that cryptographic label 501 may request or use to carry out the secure operation is not just limited to user input. For example, cryptographic label 501 may send commands to mobile device 515 to instruct mobile device 515 to retrieve information using any of the interfaces of mobile device 515. Cryptographic label 501 may instruct mobile device 515 to obtain location information from a global positioning system interface of mobile device 515. Cryptographic label 501 may request information received from an external NFC device through a NFC interface of mobile device 515. Cryptographic label 501 may instruct mobile device 515 to retrieved information from the internet through a wireless data interface of mobile device 515, and so on. Cryptographic label 501 may perform additional cryptographic operations on any information obtained from the various interfaces of mobile device 515.

[0082] Once cryptographic label 501 has obtained and performed the desired cryptographic operations on the information (e.g., account numbers, transaction amount, etc.) that cryptographic label 501 will use to carry out the secure operation, in response to a fetch command 922 received from mobile device 515, cryptographic label 501 can transmit a send

communication command 924 with an encrypted message that includes any of the information described above to mobile device 515. The send communication command 924 can instruct mobile device 515 to transmit an encrypted message provided by cryptographic label 501 using any of the communication interfaces available on mobile device 515. For example, the send communication command 924 may instruct mobile device 515 to send a secure SMS message with encrypted data provided by cryptographic label 501 to a server to make a mobile payment or to check account balance. The send communication command 924 may instruct mobile device 515 to send a secure USSD message with encrypted data to start a USSD two-way communication session with a banking server. The send communication command 924 may also instruct mobile device 515 to send a secure NFC or RF communication with encrypted data via the NFC or RF interface of mobile device 515 to a NFC or RF enabled recipient device such as a point-of-sale (POS) terminal. Because the information that mobile device 515 transmits out in the secure communication is provided to mobile device 515 in an encrypted format by cryptographic label 501, the secure communication is already encrypted when it leaves the communication interface of mobile device 515. In this manner, secure encrypted end-to-end communication can be maintained between mobile device 515 and a recipient device.

[0083] Referring now to Fig. 10, in some embodiments, the send communication command 924 may instruct mobile device 515 to send a series of messages to a recipient device 585 to set up a secure communication channel or tunnel. The series of messages 1012-1020 can be used to verify the identity of recipient device 585 and to verify the identity of mobile device 515 to recipient device 585. This way of verifying the identities of the communicating devices can be especially useful with NFC and/or RF communications where the identity of the recipient device 585 may not be known to mobile device 515 prior to the communication. The series of messages 1012-1020 can be a number challenge that includes a specific sequence of numbers that is only known to mobile device 515 as provided by cryptographic label 501, and only known to authorized recipient devices that are allowed to communicate with mobile device 515.

[0084] When recipient device 585 first receives message 1012, recipient device 585 does not initially respond to message 1012. Recipient device 585 will not respond until all messages 1012-1020 has been received by recipient device 585, and the number sequence transmitted in messages 1012-1020 is confirmed to be a valid and correct sequence. Thus, recipient device 585

can verify the identity of mobile device 515 based on the number challenge received in the series of messages 1012-1020. Mobile device 515 can also use the number challenge to verify the identity of recipient device 585. For example, if a recipient device response to message 1012, mobile device 515 can determine that the recipient device is not an authorized recipient device because an authorized recipient device would not respond right away to message 1012. It should be appreciated that the series of messages 1012-1020 is not limited to five messages as shown, and can include any number of messages, and that the number challenge can be any sequence of numbers, sequence of alphanumeric characters, or sequence of other types of messages. Furthermore, in other embodiments, mobile device 515 equipped with cryptographic label 501 can act as a recipient device and be on the receiving end of a number challenge.

[0085] In some embodiments, to provide an additional level of security to verify the identity of the devices, recipient device 585 can respond to the reception of a valid and correct number challenge with an encryption key challenge 1024. The encryption key challenge 1024 can be a symmetric key challenge or an asymmetric key challenge. In the encryption key challenge 1024, recipient device 585 can send a random number to mobile device 515 to request mobile device 515 to encrypt the random number with an encryption key that would only be known to an authorized device. Mobile device 515 can send the random number to cryptographic label 501 and request cryptographic label 501 to encrypt the random number using the requested encryption key stored in cryptographic label 501. Cryptographic label 501 can respond to mobile device 515 with the encrypted random number, and mobile device 515 then sends the encrypted random number to recipient device 585. Recipient device 585 then decrypts the encrypted random number with a corresponding key, which can be a symmetric key or an asymmetric key. If the decryption results in the random number that recipient device 585 has previously sent to mobile device 515, then recipient device can be further assured that mobile device 515 equipped with cryptographic label 501 is an authorized device, and a secure communication channel or tunnel can be established between mobile device 515 and recipient device 585. Exchange of sensitive information with secure communications between the two devices can then proceed.

[0086] One advantage of the being able to verify the identities of the communicating devices using cryptographic label 501 as describe above is that the number sequence of the number

challenge and the encryption key used in the encryption key challenge can be provisioned to be unique for each cryptographic label, and thus can be provisioned to be user specific. If the number sequence and/or the encryption key used in the encryption key challenge is somehow compromised, the infiltration will be isolated to a single user, and the remaining user base of the mobile network will not be compromised. The affected user's keys can be changed without impacting the configuration of the remaining user base.

[0087] Fig. 11 illustrates a flow diagram for performing a secure operation using a cryptographic expansion device (e.g., cryptographic label 501 of Fig. 5) attached to a communication component (e.g., SIM card 510 of Fig. 5) of a communication device (e.g., mobile device 515 of Fig. 5), according to various embodiments. At block 1102, the cryptographic expansion device receives a protocol message from the communication device according to a communication protocol that the communication device uses to communicate with the communication component. The protocol message can be a command or information that is associated with a secure operation to be performed by the cryptographic expansion device. For example, the protocol message can be a command associated with a request from a user to perform a financial or banking transaction using a secure application stored in the cryptographic expansion device such as a mobile banking application or a contactless payment application. The financial or banking transaction can be a mobile payment, a mobile money transfer, an account balance inquiry, or other financial or banking transactions or account inquiries, and may involve sending or receiving a secure communication. The protocol message can also be a command or information associated with a non-secure operation that is intended for the communication component of the communication device. In some embodiments, the protocol message can include a flag or a protocol identification (ID) field to indicate whether the protocol message is intended for the communication component.

[0088] At block 1104, the cryptographic expansion device determines if the protocol message is associated with a secure operation. If the cryptographic expansion device determines that the protocol message involves a secure operation to be performed by the cryptographic expansion device, for example, by examining the flag or the protocol ID of the protocol message, then at block 1106, the cryptographic expansion device processes the protocol message and performs a cryptographic operation on data or information associated with the secure operation as indicated

by the protocol message. The data or information can be data or information that is stored in the cryptographic expansion device and/or in the communication component, or data or information such as user input or other information that is obtained from an interface of the communication device. For example, to carry out a secure operation such as sending a secure communication to perform a financial or banking transaction, the cryptographic expansion device may retrieve an encrypted PIN from the cryptographic expansion device, obtain subscriber information from the communication component, and/or obtain user input from the communication device such as a PAN or a portion of a PAN entered by a user on the user interface of the communication device. The data or information associated with the secure operation can also be embedded in the protocol message received from the communication device. For example, the protocol message received from the communication device can include an encrypted communication for the cryptographic expansion device to decrypt.

[0089] To perform the cryptographic operation on data or information associated with the secure operation, the cryptographic expansion device may select a suitable encryption and/or MAC or hash algorithm stored in the cryptographic expansion device. The cryptographic expansion device then retrieves a cryptographic or encryption key associated with the selected encryption, and performs a cryptographic operation such as encrypting or decrypting the data or information associated with the secure operation using the encryption key and selected algorithm. The cryptographic expansion device may also generate or verify a MAC or hash on data or information associated with the secure operation.

[0090] Then at block 1108, the cryptographic expansion device sends a device command and/or the result of the cryptographic operation (encrypted or decrypted data) to the communication device, in accordance with the protocol of the protocol message. The device command can include commands instructing the communication device to perform certain operations to carry out the secure operation such as sending encrypted data provided by the cryptographic expansion device in a secure communication on a communication interface of the communication device. In some embodiments, the communication interface can be a cellular interface for sending SMS or USSD messages, or a NFC or RF interface for sending NFC or RF communications. In other embodiments, the communication interface can be any of the communication interfaces provided in the communication device. As another example, the

device command can instruct the communication device to display plaintext data or information to a user that the cryptographic expansion device decrypted from an encrypted message sent to the communication device. It should be understood that depending on the secure operation that is being requested or associated with the protocol message received from the communication device in block 1012, the cryptographic expansion device may send more than one device command to the communication device to carry out the secure operation, and that in some embodiments, there can be multiple iterations of protocol message and device command exchanges to carry out a secure operation.

[0091] Referring back to block 1104, if the cryptographic expansion device determines that the protocol message is associated with a non-secure operation that is intended for the communication component, then at block 1110, the cryptographic expansion device forwards or passes through the protocol message to the communication component. At block 1112, the communication component may reply to the cryptographic expansion device with a response to the protocol message. Upon receiving the response to the protocol message from the communication component, at block 114, the cryptographic expansion device forwards or passes through the response to the communication device.

[0092] It should be appreciated that while the methods and apparatuses for sending and receiving secure communications discussed above have been described with reference to performing financial and/or banking transactions from a mobile device, the methods and apparatuses discussed above can also be used to perform secure communications from a mobile device for other applications as well, such as personal or corporate secure communication (e.g., for sensitive or confidential communications to avoid industrial espionage), health care communication (e.g., for confidential medical information or electronic prescription delivery), or governmental agency communication (e.g., for law enforcement).

[0093] Fig. 12 shows a communication device 1200 according to the some of the embodiments described above. The communication device 1200 includes a communication component reader 1225 for accepting a communication component such as a SIM card that may be equipped with a cryptographic expansion device. The communication device 1200 also includes a display 1212, an input element 1214, computer readable medium 1224 such as volatile and non-volatile memory, processor 1210 and at least one antenna 1220. In addition, the communication device

1200 may include a dual interface including both contact (not shown) and contactless interface 1216 for transferring information through direct contact or through an integrated chip, which may be coupled to a second antenna. In addition, the communication device 1200 may be capable of communicating through a cellular network, such as GSM through an antenna 1220.

5 Thus, the communication device 1200 may be capable of transmitting and receiving information wirelessly through both short range NFC, radio frequency (RF) and cellular connections.

[0094] In certain implementations, individual blocks (or steps) described above with respect to the Figures may be combined, eliminated, or reordered. Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium
10 may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

[0095] The present invention can be implemented in the form of control logic in software or hardware or a combination of both. The control logic may be stored in an information storage medium as a plurality of instructions adapted to direct an information processing device to
20 perform a set of steps disclosed in embodiments of the present invention. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will appreciate other ways and/or methods to implement the present invention.

[0096] Any recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

25 [0097] The above description is illustrative and is not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

WHAT IS CLAIMED IS:

1 1. A label comprising:
2 a first set of electrical contacts disposed on a top side of the label for interfacing
3 to a communication device;
4 a second set of electrical contacts disposed on a bottom side of the label for
5 interfacing to a communication component;
6 a coupling element configured to attach the label to the communication
7 component; and
8 a hardware security module disposed in the label and coupled to the first and
9 second sets of electrical contacts, wherein the hardware security module includes a secure
10 processing unit and a public processing unit.

1 2. The label of claim 1, wherein the communication component is a
2 communication card, and the coupling element is an adhesive material disposed on the bottom
3 side of the label.

1 3. The label of claim 2, wherein the communication card is a Subscriber
2 Identity Module (SIM) card.

1 4. The label of claim 2, wherein the public processing unit comprises:
2 a communication device interface coupled to the first set of electrical contacts;
3 and
4 a communication component interface coupled to the second set of electrical
5 contacts;
6 wherein the public processing unit is configured to process messages received at
7 the communication device interface and the communication component interface.

1 5. The label of claim 4, wherein the public processing unit is configured to
2 send, to the secure processing unit, requests to perform cryptographic operations in response to
3 receiving messages on the communication device interface that are associated with secure
4 operations.

1 6. The label of claim 4 wherein the public processing unit is configured to
2 pass through messages that are associated with non-secure operations between the
3 communication device interface and the communication component interface.

1 7. The label of claim 5, wherein the secure operations include sending secure
2 communications using a communication protocol selected from a group consisting of Short
3 Message Service (SMS) protocol, Unstructured Supplementary Service Data (USSD) protocol,
4 Near Field Communication (NFC) protocol, and Radio Frequency (RF) communications
5 protocol.

1 8. The label of claim 7, wherein the secure communications are used in
2 financial transactions.

1 9. A system comprising:
2 a communication component; and
3 a label attached to the communication component, the label comprising:
4 a set of electrical contacts electrically coupled to the
5 communication component;
6 a cryptoprocessor disposed in the label; and
7 a processor disposed in the label and coupled to cryptoprocessor,
8 wherein the label enables a communication device using the communication
9 component to send encrypted data using the cryptoprocessor in the label.

1 10. The system of claim 9, wherein the communication component is a
2 communication card, and the label is attached to the communication component with an adhesive
3 material.

1 11. The system of claim 10, wherein the label is configured to render the
2 cryptoprocessor and the processor unusable when an attempt is made to remove the label from
3 the communication card.

1 12. The system of claim 10, wherein the cryptoprocessor is configured to
2 respond only to encryption and decryption requests from the processor.

1 13. The system of claim 10, wherein the encrypted data is sent using a
2 communication interface of the communication device.

1 14. The system of claim 13, wherein the communications device is a mobile
2 phone, and the communication interface is one of a cellular communications interface for
3 transmitting SMS messages, a cellular communications interface for transmitting USSD
4 messages, a NFC interface, and a RF interface.

1 15. The system of claim 13, wherein the encrypted data is associated with a
2 payment transaction.

1 16. A method for enabling transmission of secure communications from a
2 communication device using a label, wherein the label is attached to a communication
3 component of the communication device, the method comprising:
4 receiving, in the label, a first message;
5 determining that the first message is associated with a secure operation;
6 performing, by a cryptographic processor disposed in the label, a cryptographic
7 operation on data associated with the secure operation; and
8 sending the data processed by the cryptographic processor from the label to the
9 communication device for transmission in a secure communication.

1 17. The method of claim 16, further comprising:
2 sending the secure communication from the communication device in one of a
3 SMS message, a USSD message, a NFC communication, and a RF communication.

1 18. The method of claim 16, further comprising:
2 receiving, in the label, a second message;

3 determining that the second message is associated with a non-secure operation;
4 and
5 passing through the message to the communication component.

1 19. The method of claim 16, wherein the data processed by the cryptographic
2 processor is associated with a financial transaction being conducted with the communication
3 device.

1 20. The method of claim 16, wherein the cryptographic operation is performed
2 in response to an encryption or decryption request sent to the cryptographic processor from a
3 public processor disposed in the label.

1 21. The method of claim 20, wherein the cryptographic processor is accessible
2 to both the communication component and the communication device only through the public
3 processor disposed in the label.

1 22. The method of claim 16, wherein the communication component is a SIM
2 card, and the communication device is a mobile device.

1

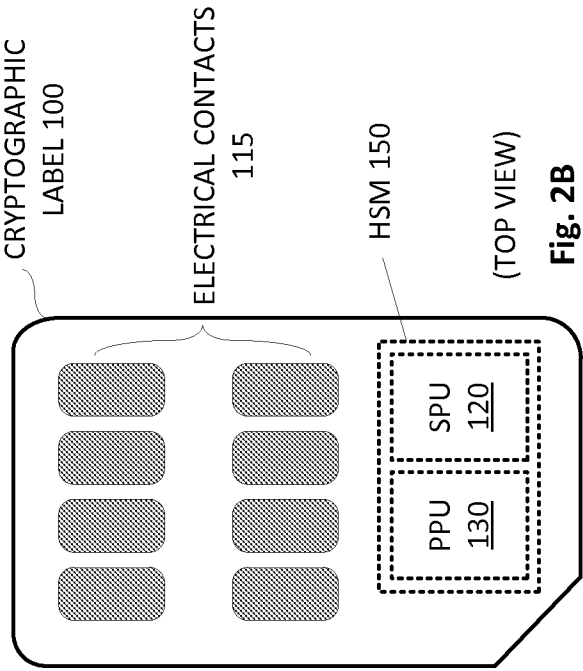


Fig. 2B

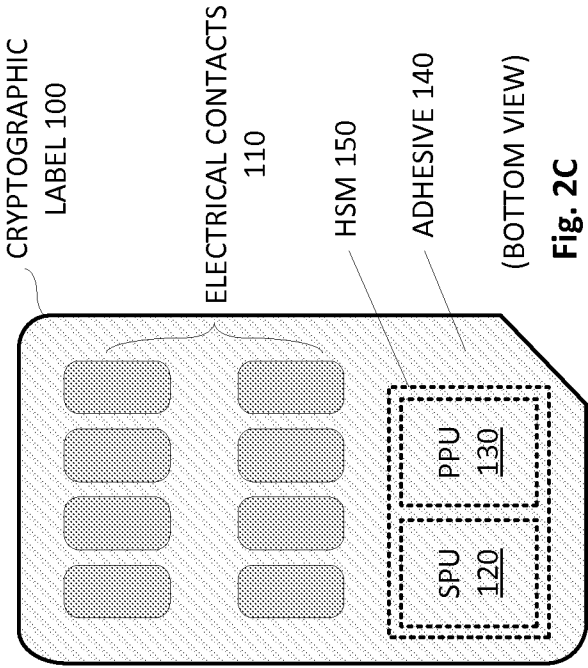


Fig. 2C

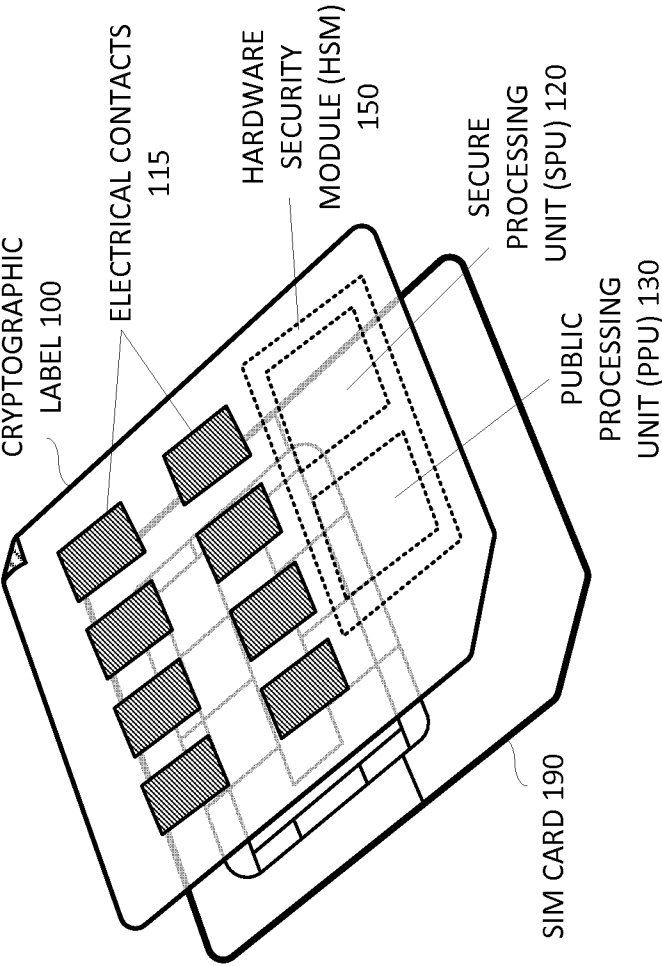


Fig. 1

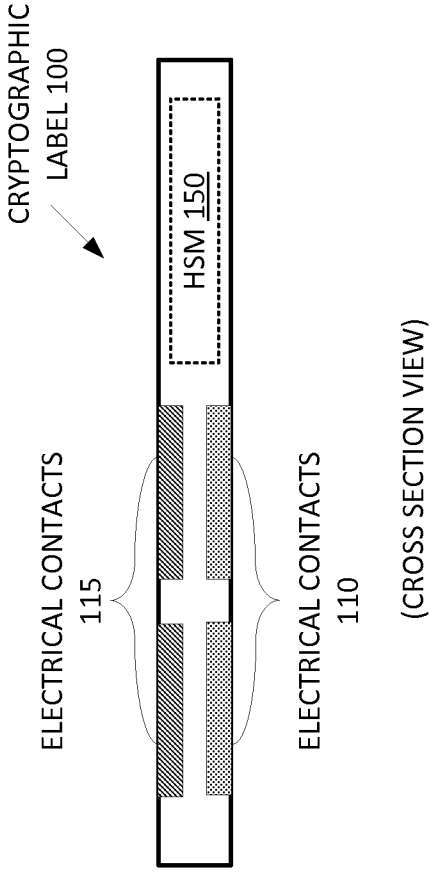


Fig. 2A

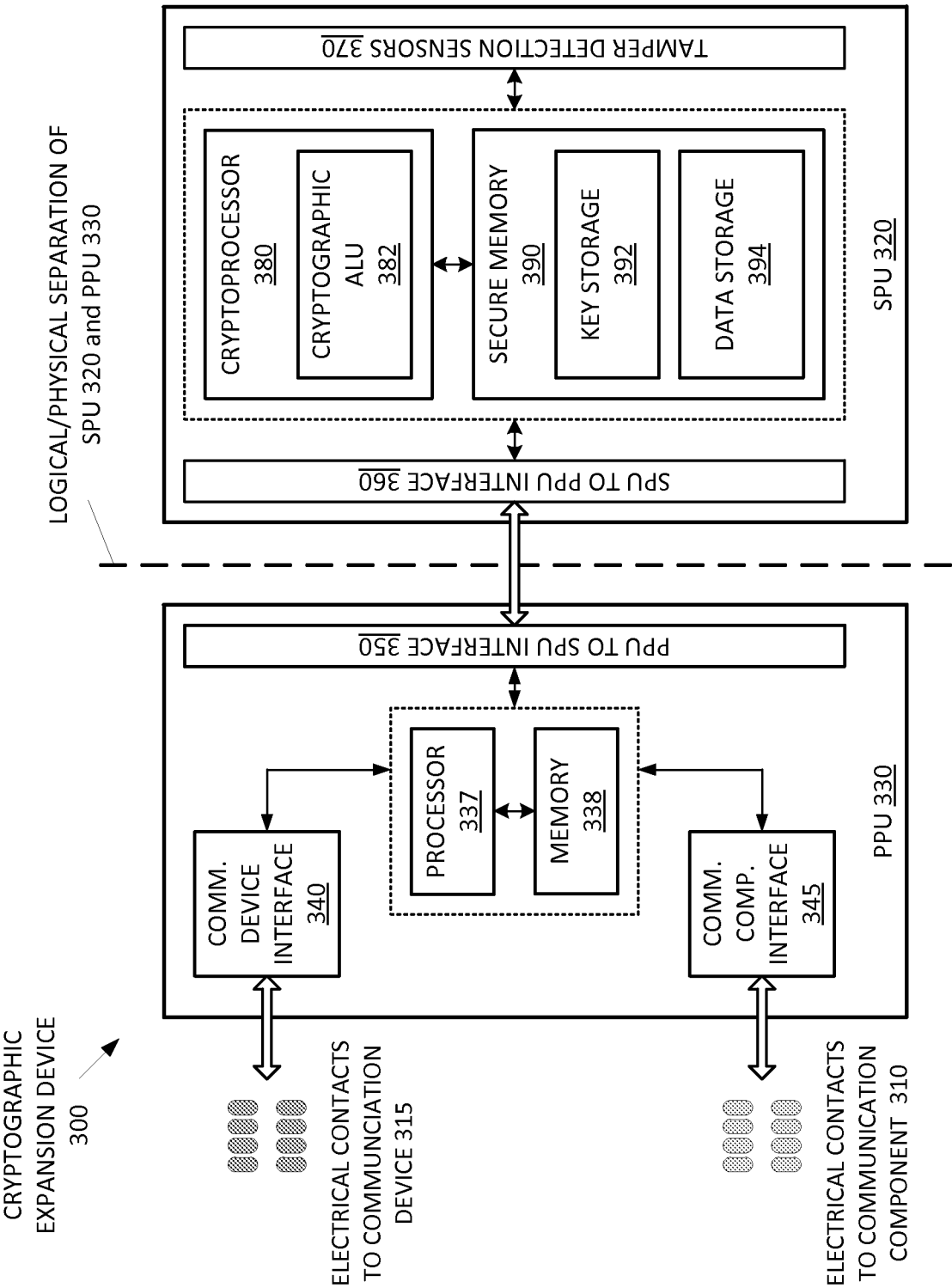


Fig. 3

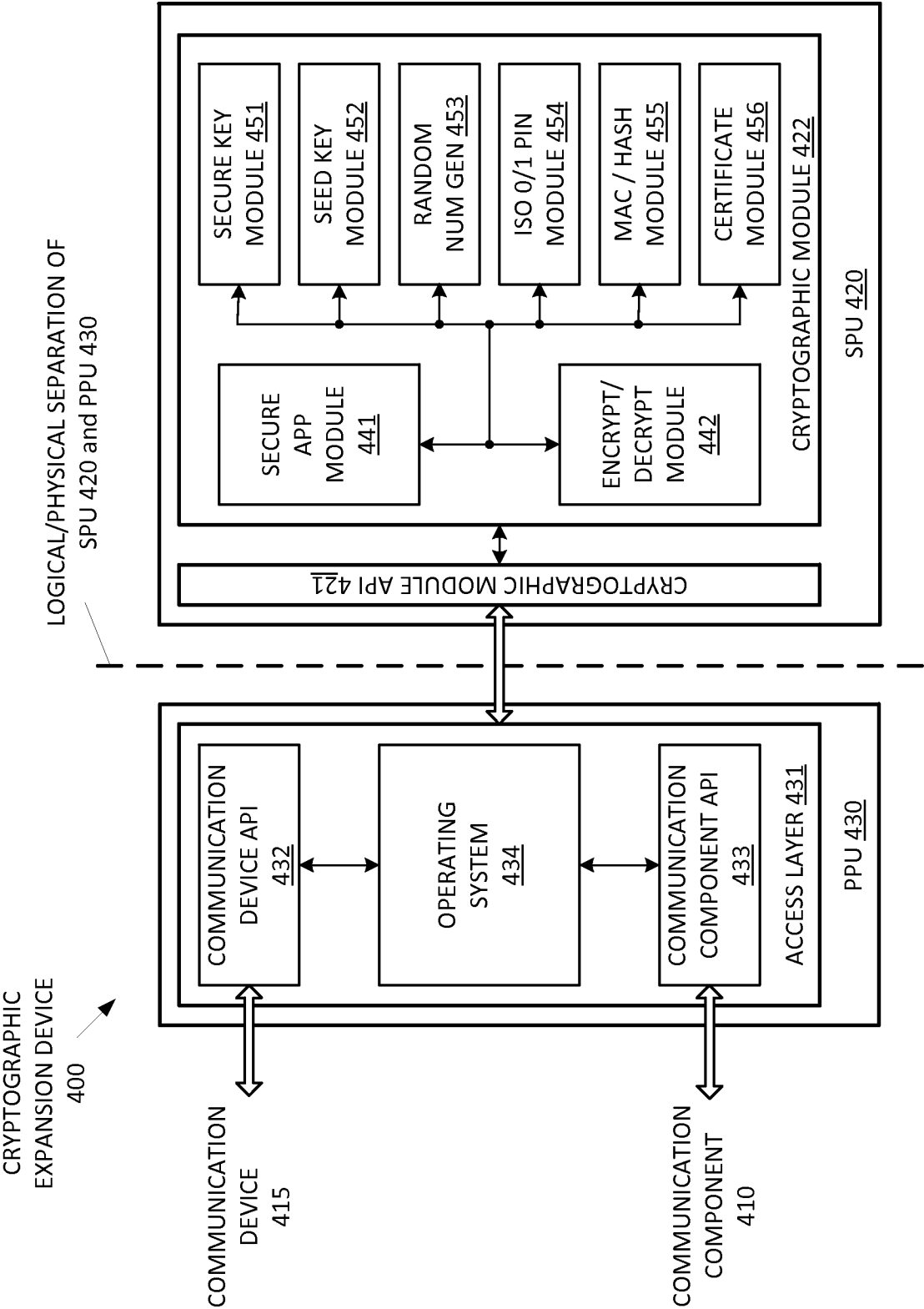


Fig. 4

4/8

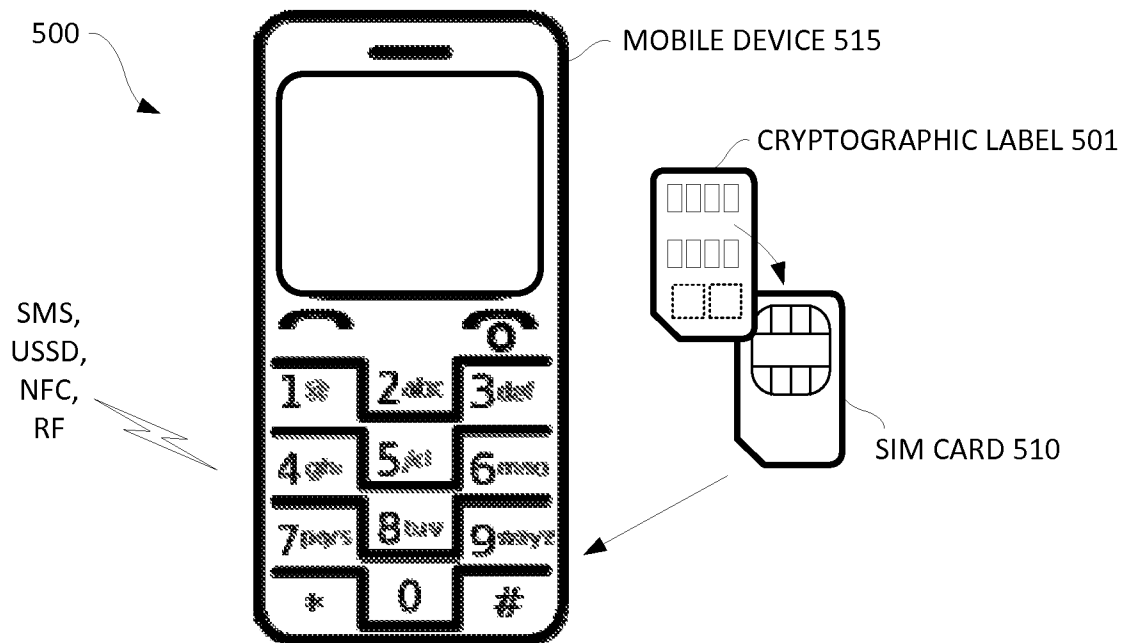


Fig. 5

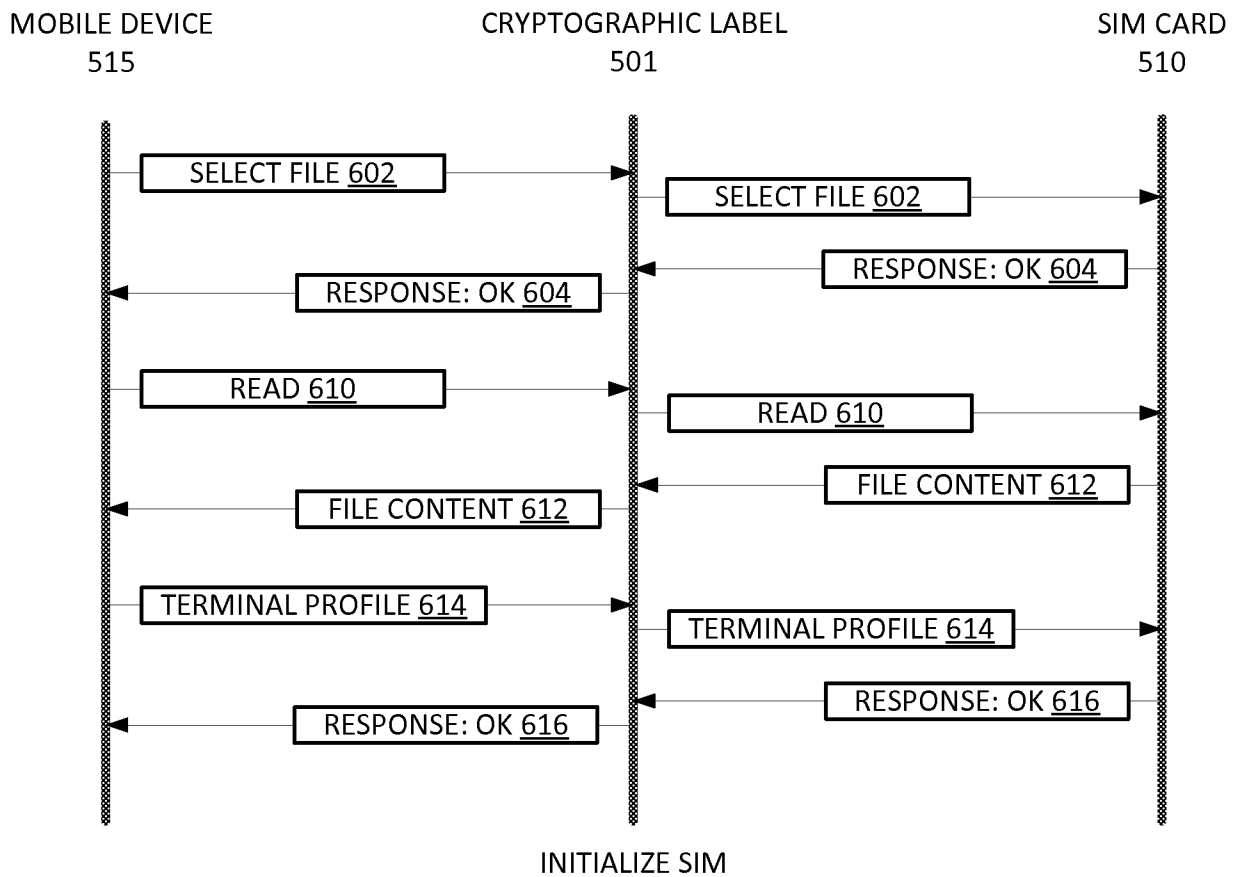


Fig. 6

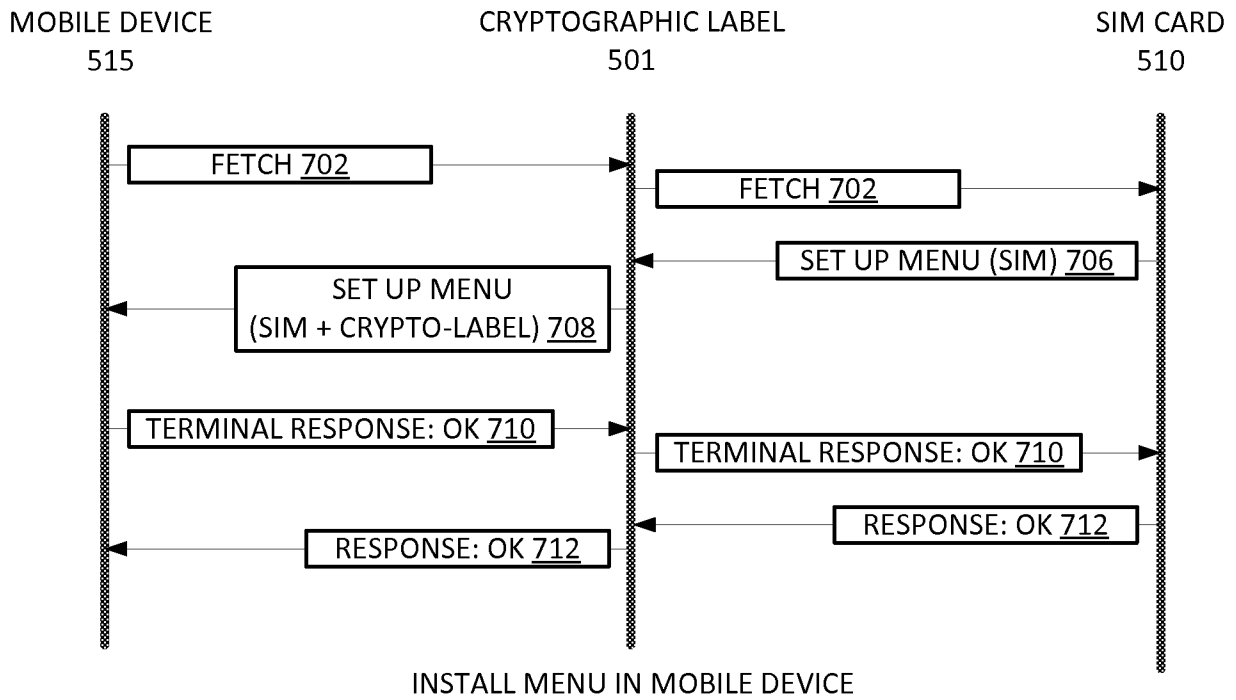


Fig. 7

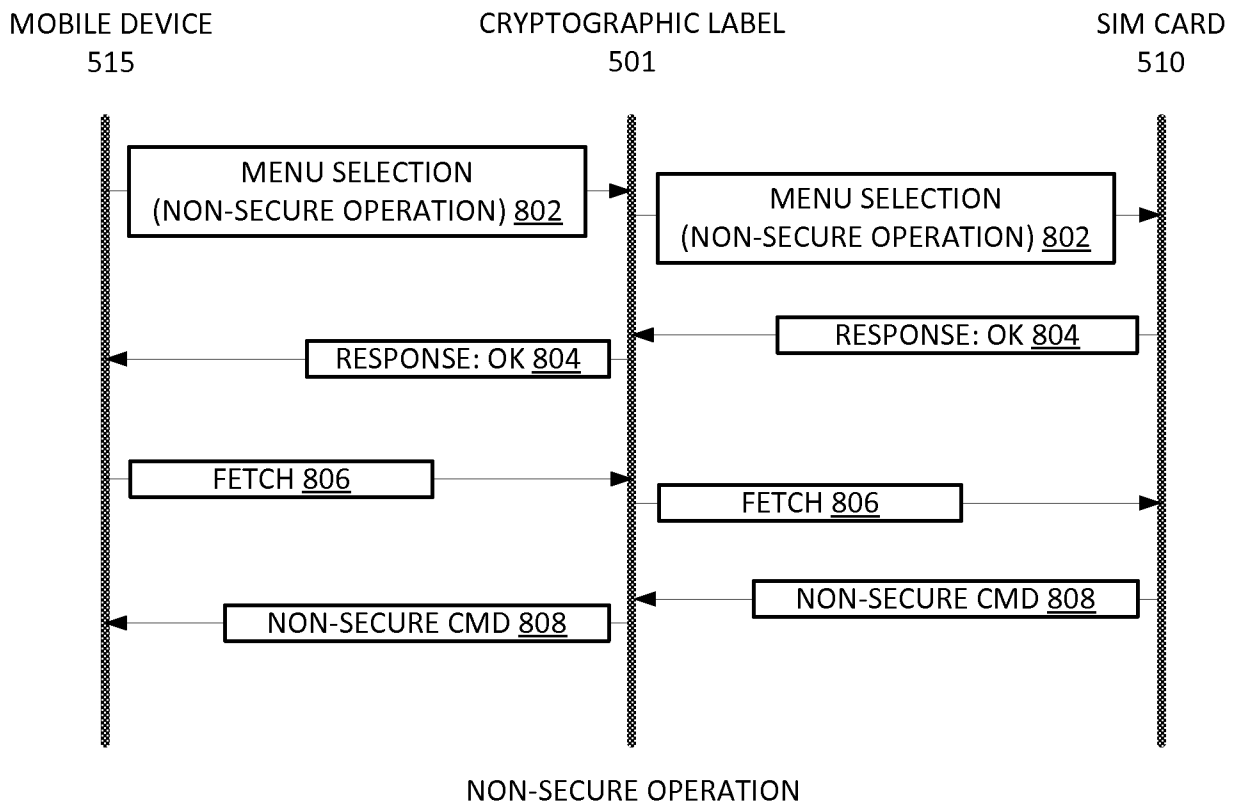


Fig. 8

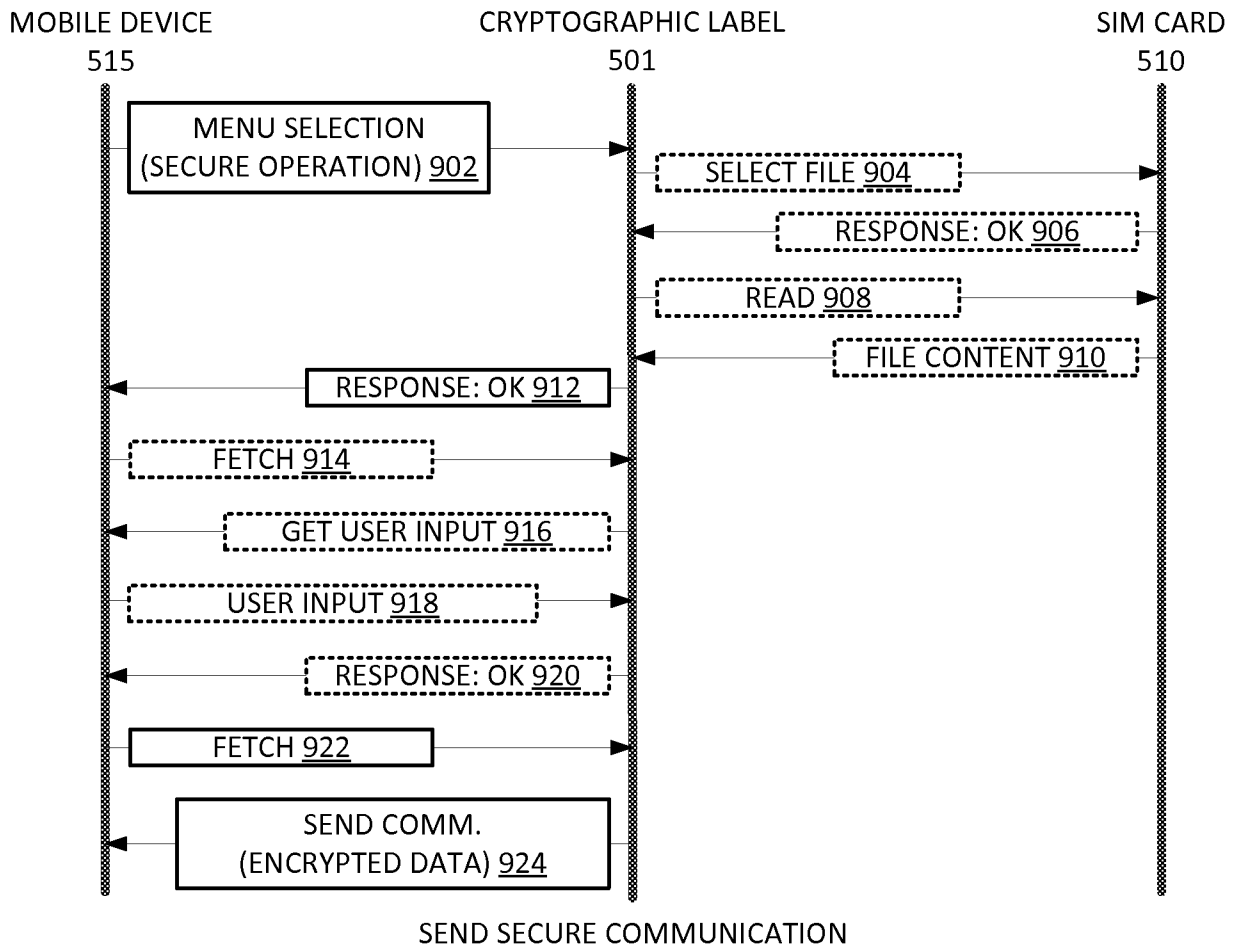


Fig. 9

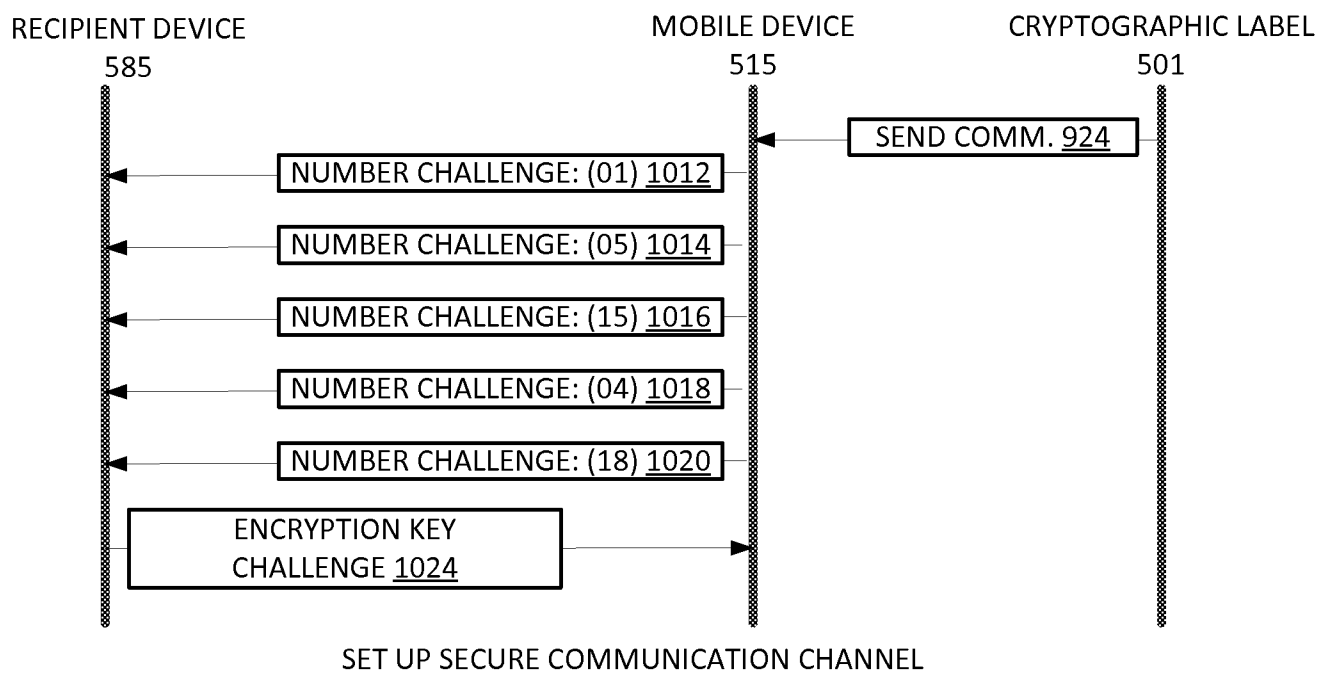


Fig. 10

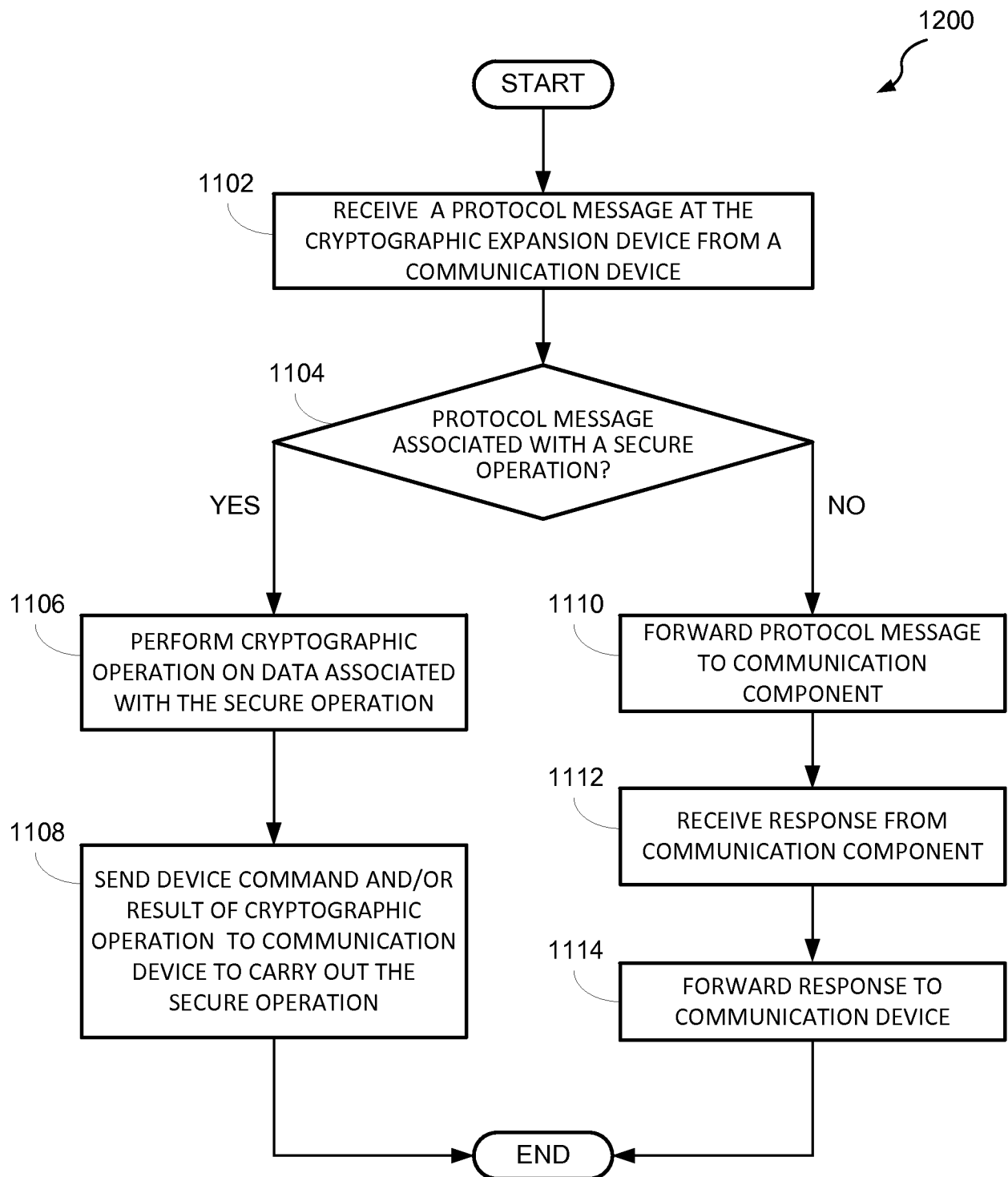
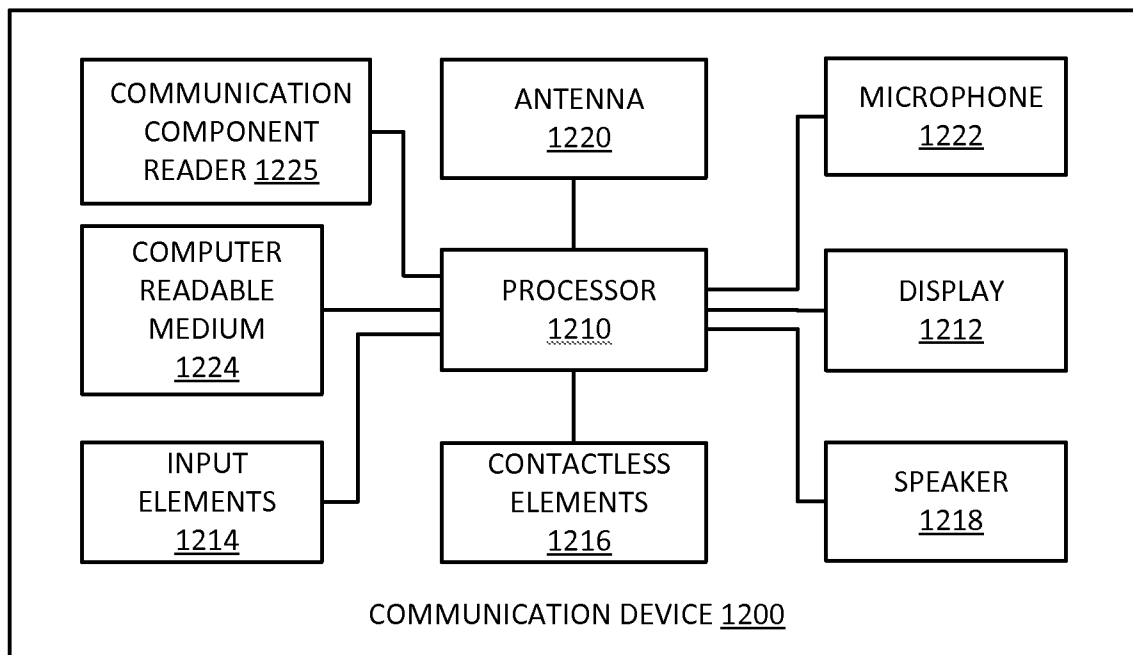


Fig. 11

**Fig. 12**