



(43) International Publication Date  
5 December 2013 (05.12.2013)

- (51) International Patent Classification:  
*H04W 8/00* (2009.01)
- (21) International Application Number:  
PCT/IB2013/054475
- (22) International Filing Date:  
30 May 2013 (30.05.2013)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
61/653,981 31 May 2012 (31.05.2012) US
- (71) Applicant: FUNDAMO (PTY) LTD [ZA/ZA]; 2 Strand Road, Bellville, 7530 Cape Town (ZA).
- (72) Inventors: HUXHAM, Horatio Nelson; 35 Bellwater Park, Kenridge, Bellville, 7530 Cape Town (ZA). O'REGAN, Alan Joseph; 57 Rathfelder Avenue, Constantia, 7806 Cape Town (ZA).
- (74) Agents: VON SEIDELS INTELLECTUAL PROPERTY ATTORNEYS et al.; P O Box 440 Century City, 7446 Cape Town (ZA).
- (81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,

HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

**Declarations under Rule 4.17:**

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

**Published:**

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

(54) Title: SUBSCRIBER IDENTITY MODULE CARD HOLDER FOR ENABLING A MOBILE DEVICE TO PERFORM SECURE COMMUNICATIONS

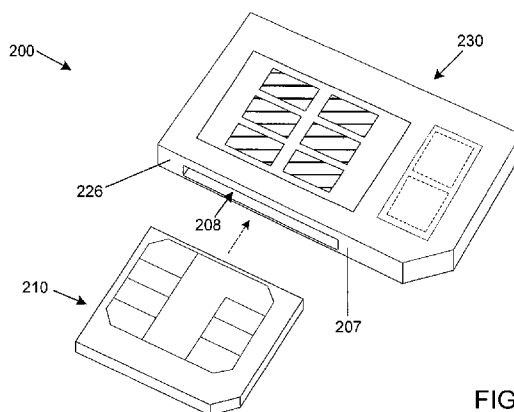


FIG. 3

(57) Abstract: A subscriber identity module (SIM) card holder for enabling a mobile device to perform secure communications is provided. The SIM card holder comprises a first set of electrical contacts disposed on a top side of the holder for interfacing to a mobile device, a hardware security module (HSM) disposed in the holder and coupled to the first set of electrical contacts, and a receiving slot configured to receive a SIM card. The receiving slot includes a second set of electrical contacts coupled to the HSM for interfacing to the SIM card.



## SUBSCRIBER IDENTITY MODULE CARD HOLDER FOR ENABLING A MOBILE DEVICE TO PERFORM SECURE COMMUNICATIONS

### CROSS-REFERENCES TO RELATED APPLICATIONS

- 5 [0001] This application claims priority from United States Provisional Patent Application No. 61/653,981 filed on 31 May 2012 entitled "Hardware Security Module in Mico-SIM Holder".

### BACKGROUND TO THE INVENTION

- 10 [0002] In developing countries and rural areas, many people may not 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. 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  
15 not have the resources and capacity to adequately support such a large number of customers, possibly resulting in long waiting 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 viable solutions due to the high costs of the complex infrastructure involved.

- 20 [0003] In recent years, the use of mobile devices in developing countries has grown rapidly. As such, one way of providing communities within these countries with access to financial and/or banking services is to enable users of mobile devices to perform mobile transactions, such as making mobile payments or money transfers, or checking account balances or performing other account related services, directly  
25 from their mobile devices. However, security concerns may often be a stumbling block that hinders the wide adoption and growth of mobile banking.

- [0004] Most mobile devices, especially older generation models that are typically used in developing countries, lack the capability to securely send end-to-end encrypted communication. As a result, sensitive information, such as a Personal  
30 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, in many cases, limited because the communication may still be 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 may be costly in terms of both deployment and operating costs. Consequently, mobile operators may have to either pass this cost onto their customers or absorb it themselves. Thus, the total cost of ownership (TCO) may be 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 may incur losses or fail to roll out their mobile banking services entirely.

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

#### BRIEF SUMMARY OF THE INVENTION

**[0007]** In accordance with the invention there is provided a subscriber identity module (SIM) card holder for enabling a mobile device to perform secure communications, the SIM card holder comprising: a first set of electrical contacts disposed on a top side of the holder for interfacing to a mobile device, a hardware security module (HSM) disposed in the holder and coupled to the first set of electrical contacts, and a receiving slot configured to receive a SIM card, wherein the receiving slot includes a second set of electrical contacts coupled to the HSM for interfacing to the SIM card.

**[0008]** Further features of the invention provide for the SIM card to be a micro-SIM card and for the SIM card holder to have substantially similar dimensions to a mini-SIM card so as to enable it to be received in a mini-SIM card reader or mini-SIM card receiving slot of a mobile device when the micro-SIM card is received in the receiving slot of the SIM card holder; alternatively for the SIM card to be a nano-SIM

card and for the SIM card holder to have substantially similar dimensions to a micro-SIM card so as to enable it to be received in a micro-SIM card reader or micro-SIM card receiving slot of a mobile device when the nano-SIM card is received in the receiving slot of the SIM card holder; further alternatively for the SIM card holder to have substantially similar dimensions to a SIM card receiving tray of a mobile device so as to act as a replacement SIM card receiving tray.

**[0009]** A further feature of the invention provides for the first set of electrical contacts and the second set of electrical contacts to be disposed in a thin film, the film optionally provided with an adhesive material disposed thereon for attachment of a SIM card to the SIM card holder.

**[0010]** Yet further features of the invention provide for the receiving slot to be defined by an opening at a bottom surface of the SIM card holder and openings or partial openings at each of a first side and a second side of the SIM card holder; for the SIM card holder to have a closed bottom provided by a thin closing integral to the SIM card holder, optionally with adhesive material disposed thereon and extending between inner surfaces of the receiving slot at a bottom side thereof so as to define the receiving slot by an opening at at least a first insertion end of the SIM card holder; and for the SIM card holder to have a closed bottom provided by a thin adhesive sticker removably attached to the SIM card holder and extending across the receiving slot on a bottom surface of the SIM card holder.

**[0011]** A further feature of the invention provides for the thin closing to be pivotally attached to a first inner surface of the receiving slot at a first end of the closing and provided with a clip formation at a second end thereof so as to enable the closing to be moved between an open position, in which it lies generally transverse to a bottom surface of the SIM card holder, to a closed position, in which it lies generally parallel to the bottom surface of the SIM card holder, and in which the clip formation is received in a corresponding receiving formation at a second, opposing inner surface of the receiving slot.

**[0012]** Still further features of the invention provide for the SIM card holder to have a thickness equal to or less than 100 microns more than the thickness of a SIM card to be received in the receiving slot; and alternatively, for the SIM card holder to have a

thickness equal to or less than 60 microns more than the thickness of a SIM card to be received in the receiving slot.

**[0013]** Further features of the invention provide for the receiving slot to be defined by a pair of thin, protruding ledges extending inwardly from opposing inner surfaces of the receiving slot such that a bottom surface of the SIM card abuts top surfaces of the ledges when the SIM card is received in the receiving slot; and for the ledges to extend from a first, insertion side of the SIM card holder and ending in one or more walls at or near a second end of the SIM card holder for receiving a SIM card.

**[0014]** Yet further features of the invention provide for branding to be provided on a surface of the SIM card holder; for the mobile device to be any one of a mobile phone, a tablet computer, a personal digital assistant, a portable digital electronic communications device, a smart phone, and a laptop computer; and for the secure communications to include one or both of financial transactions and banking transactions.

**[0015]** A further feature of the invention provides for the secure communications to be sent as encrypted Short Message Service (SMS) messages, Unstructured Supplementary Service Data (USSD) messages, Near Field Communication (NFC) communications, Radio Frequency (RF) communications, or Near Sound Communication (NSC) communications.

#### BRIEF DESCRIPTION OF THE DRAWINGS

**[0016]** FIG. 1 illustrates a three-dimensional view of a first embodiment of a SIM card holder for enabling a mobile device to perform secure communications according to the invention;

**[0017]** FIG. 2 illustrates a cross-sectional view of the SIM card holder of FIG. 1;

**[0018]** FIG. 3 illustrates a three-dimensional view of a second embodiment of a SIM card holder for enabling a mobile device to perform secure communications according to the invention;

**[0019]** FIG. 4 illustrates a cross-sectional view of the SIM card holder of FIG. 3;

**[0020]** FIG. 5 illustrates a three-dimensional view of the SIM card holder of FIG. 3, wherein a micro-SIM card is inserted in the SIM card holder;

**[0021]** FIG. 6 is a three-dimensional representation of the SIM card holder of FIG. 5, wherein a removal aperture of the SIM card holder is shown;

5 **[0022]** FIG. 7 illustrates a front view of the SIM card holder of FIG. 5;

**[0023]** FIG. 8 shows a diagrammatic illustration of a closing with a clip formation according to an embodiment of the invention;

**[0024]** FIG. 9 illustrates a three-dimensional view of a third embodiment of a SIM card holder for enabling a mobile device to perform secure communications  
10 according to the invention;

**[0025]** FIG. 10 illustrates a cross-sectional view of the SIM card holder of FIG. 9;

**[0026]** FIG. 11 illustrates a three-dimensional view of a fourth embodiment of a SIM card holder for enabling a mobile device to perform secure communications according to the invention;

15 **[0027]** FIG. 12 illustrates a cross-sectional view of the SIM card holder of FIG. 11;

**[0028]** FIG. 13 is a schematic illustration of a mobile device and SIM card along with a SIM card holder for enabling a mobile device to perform secure communications according to the invention;

**[0029]** FIG. 14 illustrates a block diagram of the components of a SIM card holder,  
20 according to one embodiment of the invention;

**[0030]** FIG. 15 illustrates a conceptual block diagram of the functional blocks of a SIM card holder, according to one embodiment of the invention;

**[0031]** FIG. 16 illustrates a diagram showing the process of initializing a SIM card in a mobile device equipped with a SIM card holder, according to one embodiment of  
25 the invention;

**[0032]** FIG. 17 illustrates a diagram showing the process of installing a user menu in a mobile device equipped with a SIM card holder, according to one embodiment of the invention;

[0033] FIG. 18 illustrates a diagram showing the process of performing a non-secure operation in a mobile device equipped with a SIM card holder, according to one embodiment of the invention;

[0034] FIG. 19 illustrates a diagram showing the process of performing a secure operation in a mobile device equipped with a SIM card holder, according to one embodiment of the invention;

[0035] FIG. 20 illustrates a diagram showing the process of setting up a secure communication channel between devices using a SIM card holder, according to one embodiment of the invention;

[0036] FIG. 21 illustrates a flow diagram of performing a secure operation with a SIM card holder, according to one embodiment of the invention; and

[0037] FIG. 22 illustrates a block diagram of an exemplary mobile device in which various embodiments of the invention can be implemented.

#### DETAILED DESCRIPTION WITH REFERENCE TO THE DRAWINGS

[0038] Embodiments of the invention disclosed herein are directed toward a subscriber identity module (SIM) card holder that has one or more integrated circuits implementing a hardware security module (HSM) disposed therein. The term "HSM" as used in this description refers to the integrated circuits disposed in the SIM card holder, which include embedded processors and storage capabilities. When used with a SIM card in a mobile device, the SIM card holder provides the mobile device with the same set of security features as found in industry-standard HSMs. The term "SIM card" as used in this description may also refer to a Universal Integrated Circuit Card (UICC).

[0039] A device with embedded processors and storage capabilities for performing HSM security features may be referred to as a cryptographic expansion device. A cryptographic expansion device is capable of running a secure operating system and provides secure key management to generate cryptographic keys, sets the capabilities and security limits of keys, implements key backup and recovery, prepares keys for storage and performs key revocation and destruction. The cryptographic expansion device can also encrypt data and user input using Data

Encryption Standard (DES), Triple Data Encryption Standard/Algorithm (TDES/TDEA), DES-X, Secure Socket Layer (SSL), Advanced Encryption Standard (AES), Blowfish, Serpent, Twofish, Threefish, 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.

**[0040]** In some embodiments, the cryptographic expansion device is implemented as a dual processor device that includes a Federal Information Processing Standards (FIPS)-compliant secure processor with storage and a public processor with storage. This division in hardware roles introduces a new 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 secure processor and storage component is inaccessible without the master key used during manufacturing.

**[0041]** An electronic device that solely uses software to encrypt communications may comply with only a security level 1 of the Federal Information Processing Standard 140-2 (FIPS 140-2), which provides only a minimum level of security to protect sensitive information. In contrast, an electronic device coupled to an HSM according to embodiments of the invention is compliant with at least a security level 2 of the FIPS 140-2 standard. More preferably, the electronic device is compliant with security level 3 or security level 4 of FIPS 140-2.

**[0042]** The HSM in embodiments of the invention uses hardware to encrypt data instead of solely performing the encryption in software. The HSM provides enhanced protection over software encryption technologies. For example, the HSM provides secure key management to generate cryptographic keys, sets the capabilities and security limits of keys, implements key backup and recovery, prepares keys for storage and performs key revocation and destruction. The HSM can also provide a tamper-proof mechanism that provides a high risk of destroying the HSM and the cryptographic keys stored therein, if any attempt is made to remove or externally access the HSM.

**[0043]** FIG. 1 illustrates a first embodiment of a SIM card holder (100) for enabling a mobile device to perform secure communications according to the invention. A

cross-sectional view taken along the length of the SIM card holder (100) is shown in FIG. 2. The SIM card holder (100) comprises a first set of electrical contacts (102) disposed on a top surface (104) of the holder for interfacing to a mobile device (not shown), an HSM (106) disposed in the holder (100) and coupled to the first set of electrical contacts (102), and a receiving slot (108) configured to receive a SIM card (110). The receiving slot (108) includes a second set of electrical contacts (112) on an inner surface (114) of the receiving slot coupled to the HSM (106), as shown in FIG. 4, for interfacing to the SIM card (110).

**[0044]** The receiving slot (108) is defined by an opening at a bottom surface (105) of the SIM card holder (100) and openings at each of a first side (107) and a second side (109) of the SIM card holder (100). The receiving slot (108) of the SIM card holder (100) of this embodiment is sized to receive a micro-SIM card. The holder (100) has substantially the same size and shape as a mini-SIM card, such that the holder (100) can be inserted into a mini-SIM card reader such as those available in many mobile devices. The receiving slot (108) is sized slightly larger than a micro-SIM card such that a micro-SIM card can be installed into the receiving slot (108).

**[0045]** The mobile device may be any appropriate mobile device, examples of which include mobile phones, tablet computers, personal digital assistants, smart phones, laptop computers, portable consumer electronic communications device with a SIM card reader, or the like. In a preferred embodiment, the mobile device is a mobile phone.

**[0046]** In embodiments of the invention the HSM (106) disposed in the SIM card holder (100) includes embedded processors (e.g., a secure processor and a public processor) and storage capabilities for performing the security features described above and other security functions enabling and/or facilitating end-to-end secure communication. The additional space provided in the SIM card holder (100) due to the size difference between a micro-SIM card and a mini-SIM card, enables the HSM (106) to be disposed in the otherwise unused region of the SIM card holder (100) that falls outside the footprint of the receiving slot (108).

**[0047]** By disposing the HSM (106) in this region, requirements on the thickness of the HSM (106) may be relaxed (i.e. the HSM (106) can be made thicker and/or have a greater total volume). This may reduce the complexity and cost of manufacturing

for a cryptographic expansion device, and a cryptographic expansion device in the form of a SIM card holder may therefore also allow more functional circuitry to be implemented in the cryptographic expansion device. For example, additional space provided in the SIM card holder (100) can be used to accommodate additional memory circuitry to expand the storage capabilities of the cryptographic expansion device.

**[0048]** It should be noted that although the SIM card holder is shown to be semi-transparent in all of the representations, the holder is shown as such for illustrative purposes. Thus, in some implementations, the HSM may not be visible from the top of the SIM card holder, as it is in FIGs. 1, 3, 5, 9 and 11.

**[0049]** FIG. 2 illustrates the first set of electrical contacts (102) on the top surface (104) of the SIM card holder (100) to enable interfacing with a mini-SIM card reader, and the second set of electrical contacts (112) on the inner surface (114) of the receiving slot (108) for interfacing with a micro-SIM card. According to some embodiments, the sets of electrical contacts (102, 112) can have six contact pads, as shown. In other embodiments, if, for example, other available signals are used, the sets of electrical contacts may have more than six contact pads, for example, eight contact pads. If some available signals are not used, the sets of electrical contacts may also have fewer than six contact pads.

**[0050]** As shown in FIG. 2, the thickness requirement of the HSM (106) can be substantially relaxed when the HSM (106) is disposed in the region outside the footprint of the receiving slot (108). For example, in an exemplary embodiment, the thickness of the HSM can be made close to 760 microns (um), which is the thickness of a standard mini-SIM card and micro-SIM card. In contrast, disposing the HSM between the electrical contact plates could, for example, limit the thickness of the HSM to 200 microns (um) or less in some implementations.

**[0051]** In embodiments of the invention, the first and second sets of electrical contacts (102, 112) are held in a thin film (116) that spans substantially across the receiving slot (108). It is envisaged that, in embodiments of the invention, some signals, such as power and ground, can have a direct connection between the first set of electrical contacts (102) on the upper surface (104) of the SIM card holder (100) and the second set of electrical contacts (112) on the inner surface (114) of the

receiving slot (108). Other signals such as data input/output (I/O) (118) which may require processing by the HSM (106) (e.g., for encryption/decryption operations) are routed (e.g., wire-bonded) from the second set of electrical contacts (112) to the HSM (106), and then from the HSM (106) to the first set of electrical contacts (102).

5   **[0052]** In other words, for signals that require processing by the HSM (106), there is, in preferred embodiments, no direct connection between the two sets of electrical contacts (102, 112). This allows the HSM (106) to intercept sensitive data that is sent from a SIM card installed in the receiving slot (108), which is a micro-SIM card in the embodiment of FIG. 1, and to encrypt the sensitive data before the data is read by  
10   the SIM card reader of a mobile device.

**[0053]** In embodiments of the invention, the SIM card holder, when a SIM card is inserted therein, has a thickness of approximately 50 microns more than the thickness of the SIM card, because the only thickness added is the thickness of the thin film (116) containing the first and second sets of electrical contacts. In  
15   alternative embodiments, the SIM card holder may have a thickness of greater than 50 microns more than the thickness of the inserted SIM card, for example, it may have a thickness of between 50 and 150 microns or a thickness of between 150 and 250 microns more than the thickness of the inserted SIM card. In even further embodiments, the SIM card holder may have a thickness of less than 50 microns  
20   more than the thickness of the inserted SIM card.

**[0054]** To install a micro-SIM card into the SIM card holder (100) of the embodiment shown in FIG. 1, the micro-SIM card is inserted into the receiving slot (108) of the SIM card holder (100). A top surface of the micro-SIM card is then pressed against the thin film (114) in which the electrical contacts (102, 112) are held. The thin film  
25   (116) includes an adhesive on the inner surface (114) thereof that attaches to the micro-SIM card to hold the micro-SIM card in place. This ensures proper electrical contact between the micro-SIM card and the second set of electrical contacts (112) of the SIM card holder (100).

**[0055]** The SIM card holder according to embodiments of the invention can also  
30   include a tamper-proof mechanism that provides a high risk of destroying the SIM card holder and the cryptographic keys stored therein or rendering the holder unusable, if any attempt is made to remove or externally access the SIM card holder

device. For example, in some embodiments of the invention, once a SIM card has been installed into the receiving slot of the holder, an attempt to externally access or remove the SIM card from the holder would render the holder unusable. In one embodiment, the thin film which holds the first and second sets of electrical contacts is designed to rip apart and destroy the electrical contacts if an installed SIM card is removed from the receiving slot. This would prevent access to the HSM or data stored thereon if an installed SIM card is ever removed. In other embodiments, removing the SIM card from the SIM card holder would render the SIM card itself unusable as well. For example, adhesive on the thin film can be designed such that the adhesive would rip out the electrical contacts on the SIM card from the SIM card when an attempt is made to detach the SIM card from the SIM card holder.

**[0056]** FIG. 3 illustrates a second embodiment of a SIM card holder (200) for enabling a mobile device to perform secure communications according to the invention. A cross-sectional view taken along the length of the SIM card holder (200) is shown in FIG. 4. A micro-SIM card (210) is shown in FIG. 3 with the broken directional arrow indicating the manner in which the micro-SIM card (210) can be inserted into a receiving slot (208) of the SIM card holder (200).

**[0057]** The SIM card holder (200) shown in FIG. 3 is similar to the SIM card holder shown in FIG. 1. However, in this embodiment the receiving slot (208) is provided with a thin closing (220) at a bottom side the SIM card holder (200). The closing (220) extends between inner surfaces of the receiving slot (208) so as to form a closed SIM card holder bottom. A bottom surface (222) of the closing (220) is substantially parallel with a bottom surface (224) of the SIM card holder, as shown in FIG. 4. The closing (220) enables the receiving slot (208) to receive a SIM card (210) without requiring an adhesive to attach the SIM card. It should, however, be noted that adhesive may still be disposed in the SIM card holder as described above in combination with the closing (220).

**[0058]** The receiving slot (208) is defined by an opening at an insertion side (207) of the SIM card holder (200), and two walls (228) are provided at a partially closed end (230) to receive the SIM card (210), the two walls (228) defining a removal aperture (332) at a partially closed end (230) of the SIM card holder (200) for removing the

SIM card (210) from the holder (200). This is more clearly illustrated in FIGs. 5 and 6.

[0059] The SIM card (210) can be inserted into the receiving slot (208) of the SIM card holder (200) at the insertion side (207) and urged through the receiving slot (208) until it engages the two walls (228). The SIM card (210) is then fully received in the receiving slot (208), with the second set of electrical contacts (212) of the SIM card holder (200) able to interface to the SIM card (210). In embodiments of the invention, the closing (220) is integral to the SIM card holder structure and made of a similar or identical material. In alternative embodiments, the closing (220) is a thin film which may have an adhesive disposed thereon for attaching a SIM card to the closing. In further embodiments, the closing is in the form of an adhesive sticker separate from the SIM card holder structure. The adhesive sticker may then be placed over a SIM card after the SIM card has been placed in the receiving slot.

[0060] FIG. 5 illustrates the SIM card holder of FIG. 3, wherein a micro-SIM card is inserted in the SIM card holder. The SIM card (210) is fully received in the receiving slot (208), with the second set of electrical contacts (212) of the SIM card holder (200) able to interface to the SIM card (210) and a bottom surface of the SIM card abutting the closing (220).

[0061] FIG. 6 is a three-dimensional view of the SIM card holder (200) of FIG. 5, wherein the removal aperture (332) of the SIM card holder (200) is more clearly shown. The HSM and electrical contacts are not shown so that the receiving slot (208), the walls (228) and the removal aperture (232) may be more clearly illustrated. The removal aperture (332) extends between the walls (228) and from the partially closed end (230) of the holder (200) through to the receiving slot (208), as illustrated by the broken lines in FIG. 6.

[0062] To remove the SIM card (210) from the SIM card holder (200), a user may urge the SIM card (210) out of the SIM card holder (200) by inserting a suitably sized elongate object into the removal aperture (332) and applying a force in the direction of the SIM card (210), thereby urging the SIM card (210), at least partially, out of the receiving slot (208). For example, a needle-like element may be used to push the SIM card (210) at the removal aperture (332) in a direction (331) towards the receiving slot (208), so that the SIM card (210) is fully removed or partially protrudes

from the receiving slot (208) after which it a protruding edge or surface may be grasped by the user to fully remove the SIM card (210). It should be appreciated that many other methods or devices, mechanical, manual or electronic, may be employed to remove a SIM card from the SIM card holder as described herein. The SIM card holder may, in various other embodiments, also be provided with a plurality of removal apertures, a single wall in the receiving slot, or more than two walls in the receiving slot. A front view of the embodiment of FIG. 5 is shown in FIG. 7.

**[0063]** In alternative embodiments, a SIM card holder closing (427) includes a protruding clip formation (429) which can be removably clipped into a corresponding receiving formation (431) at an inner wall of the receiving slot (408). The closing (427) may then be pivotally attached to an opposing inner wall (433) of the receiving slot (408) so that it can be moved from an open position, in which it lies generally transverse to the bottom surface of the SIM card holder, to a closed position, in which it lies generally parallel to the bottom surface of the SIM card holder. The closing (427) is diagrammatically illustrated in FIG. 8. This would enable a SIM card to be inserted and removed from the SIM card holder from its bottom side, without the need for removal structures such as the removal apertures described above.

**[0064]** FIG. 9 illustrates a third embodiment of a SIM card holder (500) for enabling a mobile device to perform secure communications according to the invention. A cross-sectional view taken along the length of the SIM card holder (500) is shown in FIG. 10. A micro-SIM card (510) is shown in FIG. 9, with a broken directional arrow (511) indicating the manner in which the micro-SIM card (510) can be inserted into a receiving slot (510) of the SIM card holder (500).

**[0065]** The SIM card holder (500) shown in FIG. 5 is similar to the SIM card holder shown in FIG. 3. However, in this embodiment the receiving slot (508) is defined by a pair of thin, protruding ledges (540) extending inwardly from opposing inner walls (541) of the receiving slot (508). The ledges (540) extend from the insertion side (507) of the SIM card holder (500) and end in walls (542) to define a partially closed side (530) of the SIM card holder (500). The walls (542) are illustrated in FIG. 10.

**[0066]** The SIM card (510) can be inserted into the receiving slot (508) of the SIM card holder (500) at the insertion side (507) and urged through the receiving slot (508) until it engages the walls (542). The SIM card (510) is then fully received in the

receiving slot (508), between the second set of electrical contacts (512) of the SIM card holder (500) and the ledges (540) with a bottom surface of the SIM card abutting the ledges (540), and able to interface to the SIM card (410). The ledges (540) and walls (542) are integral to the SIM card holder structure and are preferably made of a similar or identical material. In alternative embodiments, the ledges (540) may be made of a thin film which may have an adhesive disposed thereon for attaching a SIM card to the ledges (540).

**[0067]** The SIM card holder may be manufactured from any suitable material. In preferred embodiments, the card body is manufactured from stiff plastics material. To achieve the desired stiffness, polyvinyl chloride (PVC) or polyvinyl chloride acetate (PVCA) may typically be used.

**[0068]** Embodiments of the invention further provide for branding to be included on the SIM card holder. In the embodiment shown in FIG. 9, printed branding (544) is provided on the top surface (504) of the SIM card holder (500). Branding may also be applied by means of various other methods and/or devices. For example, the branding may be applied to a surface of the SIM card holder by means of an adhesive material or may be inscribed in the SIM card holder.

**[0069]** In the embodiments shown in FIGs. 3 to 10, the SIM card holder is configured to receive a micro-SIM card as specified in the ETSI TS 102 221 standard. In the embodiment shown in FIGs. 11 and 12, the SIM card holder is configured to receive a nano-SIM card as specified in the ETSI TS 102 221 standard.

**[0070]** FIG. 11 illustrates a fourth embodiment of a SIM card holder (600) for enabling a mobile device to perform secure communications according to the invention. A cross-sectional view taken along the length of the SIM card holder (600) is shown in FIG. 12. The SIM card holder (600) comprises a first set of electrical contacts (602) disposed on a top surface (604) of the holder for interfacing to a mobile device (not shown), an HSM (606) disposed in the holder (600) and coupled to the first set of electrical contacts (602), and a receiving slot (608) configured to receive a SIM card (610). The receiving slot (608) includes a second set of electrical contacts (612) on an inner surface (614) of the receiving slot coupled to the HSM (606), as shown in FIG. 12, for interfacing to the SIM card (610).

**[0071]** The receiving slot (608) is defined by an opening at a bottom surface (605) of the SIM card holder (600) and openings at each of a first side (607) and a second side (309) of the SIM card holder (600). The receiving slot (608) of the SIM card holder (600) of this embodiment is sized to receive a nano-SIM card. The holder (600) is substantially the same size as a micro-SIM card, such that the holder (600) can be inserted into a micro-SIM card reader such as those available in most mobile devices. The receiving slot (608) is sized slightly larger than a nano-SIM card such that a nano-SIM card can be installed into the receiving slot (608).

**[0072]** FIG. 12 illustrates the first set of electrical contacts (602) on the top surface (604) of the SIM card holder (600) to enable interfacing with a micro-SIM card reader, and the second set of electrical contacts (612) on the inner surface (614) of the receiving slot (608) for interfacing with a nano-SIM card.

**[0073]** As shown in FIG. 12, the thickness requirement of the HSM (606) can be substantially relaxed when the HSM (606) is disposed in the region outside the footprint of the receiving slot (608). For example, in an exemplary embodiment, the thickness of the HSM can be made close to 760 microns ( $\mu\text{m}$ ), which is the thickness of a standard micro-SIM card. Similarly to the embodiment shown in FIG. 3, the first and second sets of electrical contacts (602, 612) are held in a thin film (616) that spans substantially across the receiving slot (608).

**[0074]** The embodiments as described with reference to FIGs. 3 to 12 therefore provide a device which enables a user to insert a smaller form factor SIM card into a SIM card holder of dimensions similar to a larger form factor SIM card so that the SIM card holder can be inserted into a SIM card receiving slot or reader of a mobile device to enable the mobile device to perform secure communications. For example, a micro-SIM card can be inserted into a SIM card holder as described with reference to FIGs. 3 to 10 for insertion into a mini-SIM card reader, and a nano-SIM card can be inserted into a SIM card holder as described with reference to FIGs. 11 and 12 for insertion into a micro-SIM card reader. It should be appreciated that the invention is not limited to a SIM card holder with a receiving slot of similar dimensions to a micro-SIM card or nano-SIM card. Furthermore, any suitable form factor combination may be employed, for example, the SIM card holder may be of similar size to a mini-SIM card while the SIM card received therein is a nano-SIM card.

[0075] Alternatively, the SIM card holder may be sized substantially similar to a built-in SIM card receiving tray of a mobile device. For example, in a case where a mobile device, typically a mobile phone, includes a standard SIM card tray in which a SIM card is placed, this tray may be removed from the mobile device and replaced  
5 with an appropriately configured SIM card holder similar to those described herein. The SIM card holder with inserted SIM card is then received in the mobile device (in the original position of the SIM card tray) and interfaces to the mobile device and the SIM card to enable the mobile device to perform end-to-end secure communications.

[0076] FIG. 13 illustrates a mobile device (700), in this case a mobile phone,  
10 according to embodiments of the invention. The mobile device (700) is equipped with a SIM card holder (710) with an installed micro-SIM card (720). The SIM card holder (710) with the installed micro-SIM card (720) is inserted into the SIM card reader of the mobile device (700). The SIM card holder (710) can be any one of the embodiments of the micro-SIM holder described above and therefore represents a  
15 cryptographic expansion device which can enable the mobile device (700), or any other suitable mobile device it is installed in, to securely communicate with various other devices and hosts via a number of communication protocols.

[0077] It should be understood that the SIM card holder can be any of the embodiments described herein and that the mobile device can be other types of  
20 mobile devices as described above. A standard SIM card can be inserted into 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.

[0078] Importantly, when the mobile device is equipped with the SIM card holder, the mobile device can use the SIM card holder to send and receive end-to-end  
25 secure communications with a recipient device. For example, the SIM card holder can enable a mobile device to send encrypted Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) messages using the cellular interface of the mobile device. In some embodiments in which the mobile device has a Near Field Communication (NFC), Near Sound Communication (NSC) or Radio  
30 Frequency (RF) interface, the holder can enable the mobile device to send encrypted data in NFC, NSC or RF communication using the NFC, NSC or RF interface of the mobile device. The holder can be used with the mobile device to send and receive

encrypted data, for example, via Bluetooth or Wi-Fi networks, via 3G, 4G, Long Term Evolution (LTE) or High-Speed Downlink Packet Access (HSDPA) telecommunication networks, through Universal Mobile Telecommunications System (UMTS) data transfer, and the like. Thus, the holder can be used with a mobile device to encrypt and decrypt any type of communication that the mobile device is capable of sending and receiving.

**[0079]** In some embodiments, the end-to-end secure communications enabled by the SIM card holder can be utilized by a user of a mobile 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, creating financial accounts, buying and selling of securities, checking account balances, and or making other financial account inquiries.

**[0080]** A few of the above-mentioned communication protocols are described below for illustrative purposes. It should be appreciated that any other suitable communication protocol that the mobile device is capable of sending and receiving may be employed without departing from the scope of the invention.

**[0081]** In a first example, the SIM card holder uses the secure processor to encrypt an SMS message and then passes the message to the public processor for transmission. The public processor sends the encrypted message to a host (mobile operator). At no point is the message decrypted during transmission; full encryption is maintained point-to-point.

**[0082]** In use, the SIM card holder therefore enables mobile operators and their users to utilize the otherwise typically non-secure SMS channel to send and receive secure encrypted messages.

**[0083]** In a second example, the SIM card holder enables a mobile device to send encrypted data in NFC communication using an NFC interface of the mobile device. NFC is a "one-touch" technology that enables mobile users to exchange data and process transactions with a "touch" of their mobile device. One of the key principles behind internet and mobile network security is establishing the true identity of a transacting party. It is therefore vital that NFC users (and, for example, NSC and RF users) have a way to quickly and accurately verify the identity of the counterparts in

their transactions. In one embodiment, the NFC functionality disclosed is based on the SIM card holder as herein described. The same level of security achieved using the SIM card holder with the SMS channel is also obtainable with NFC implementations. This may enable merchants and subscribers (mobile users) to transact directly with each other using their SIM card holder-equipped mobile devices. Such secure mobile device to mobile device NFC transactions are possible due to the HSM provided by the SIM card holder.

**[0084]** In a third example, the SIM card holder enables a mobile device to send encrypted data in RF communication using an RF interface of the mobile device.

Radio-frequency identification (RFID) is a technology that relies on the use of radio waves to transfer data between a reader and an electronic tag attached to an object. It is possible for a mobile device to take on the form of an RF tag. Once again, it is important for the true identity of a transacting party to be established. In one embodiment, the RF encryption functionality disclosed is based on the SIM card holder as herein described. The same level of security achieved using the SIM card holder via the SMS channel and NFC is also obtainable for RF implementations. RF communications may thus enable a merchant and a subscriber to make and receive payments using their SIM card holder-equipped mobile devices.

**[0085]** Furthermore, while the HSM in the SIM card holder has been described as being used to enable a mobile device to send secure wireless communications (e.g., SMS, RF, or NFC), in further embodiments, the HSM in the SIM card holder may also enable an installed SIM card to be used as a Europay, MasterCard and VISA (EMV) standard smart card in both contact and contactless payment transactions.

**[0086]** FIG. 14 shows a block diagram illustrating the hardware components of a SIM card holder (800) according to one embodiment. The SIM card holder (800) includes an HSM (850) having a public processing unit (PPU) (830) and a secure processing unit (SPU) (820) coupled to the PPU (830). It should be noted that although the SPU (820) is coupled to the PPU (830), the SIM card holder (800) provides a logical and/or physical separation between the SPU (820) and the PPU (830). A "physical separation" refers to some physical boundary between the SPU (820) and the PPU (830). For example, the SPU (820) and the PPU (830) 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 the SPU (820) and the PPU (830). As shown in FIG. 14, the SPU (820) has its own communication  
5 interfaces (840, 845, 850) which are separate from a communication interface (860) of the SPU (820). The PPU (830) also has its own memory (838), which is separate from a secure memory (890) of the SPU (820). As will be explained below, the logical and/or physical separation provided between the SPU (820) and the PPU (830) creates a division in hardware roles to protect the SPU (820) and the contents  
10 stored in the secure memory (890) from unauthorized accesses.

**[0087]** According to some embodiments, the PPU (830) includes a processor (837), a memory (838), a communication device interface (840), a communication component interface (845), and a PPU-to-SPU interface (855). The processor (837) can be implemented as one or more processors or controllers. The memory (838) is  
15 coupled to the processor (837), and provides storage to store data and executable code that when executed by the processor (837), causes the processor (837) 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 the SIM card holder (800),  
20 and to process the exchange of information between the various interfaces of the PPU (830).

**[0088]** The communication device interface (840) is coupled to electrical contacts (815) that interface 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  
25 or more data input/output (I/O) signals to send and receive commands and information between the PPU (830) and the communication device. The communication component interface (845) is coupled to electrical contacts (810) 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  
30 more data input/output (I/O) signals to send and receive commands and information between the PPU (830) and the communication component. The PPU-to-SPU interface (850) is coupled to the SPU (820), 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 the SPU (820), and to receive commands and information such as encryption and decryption results from the SPU (820). Because of the logical and physical separation between the SPU (820) and the PPU (820), the SPU (820) is exposed to the PPU (830) only, and is not accessible to the communication device or to the communication component, except through the PPU (830). Hence, the PPU (830) can serve as a firewall or a gatekeeper to ensure unauthorized or unwanted communications such as hacking attempts are not sent to the SPU (820).

**[0089]** According to some embodiments, the SPU (820) includes a cryptoprocessor (880), a secure memory (890), and an SPU-to-PPU interface (860). The SPU (820) can also include tamper detection sensors (870). As mentioned above, the SPU (820) is accessible from the PPU (830) only, and receives commands and information from the PPU (830) through the SPU-to-PPU interface (860). The SPU-to-PPU interface (860) provides a set of signals that can include a clock signal and one or more data input/output (I/O) signals coupled to the PPU-to-SPU interface (855) that the SPU (820) can use to communicate with the PPU (830). In some embodiments, the SPU (820) will only respond to encryption and decryption requests to perform cryptographic operations from the PPU (830) received through the SPU-to-PPU interface (860).

**[0090]** The cryptoprocessor (880) 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 (ALUs) (882) that are optimized to perform computational intensive cryptographic functions. The cryptographic ALUs (882) can include optimized pipelines and widen data buses to enable the cryptoprocessor (880) to perform cryptographic operations faster and more efficiently than general purpose processors.

**[0091]** The secure memory (890) is coupled to the cryptoprocessor (880), and can be partitioned into a cryptographic key storage (892) and a data storage (894). The data storage (894) can be read and written by the cryptoprocessor (880), and provides storage memory to store user data such as data that are received on the SPU-to-PPU interface (860) from the PPU (830), and encryption and decryption

results that are sent to the PPU (830) through the SPU-to-PPU interface (860). The key storage (892) can be read-only to the cryptoprocessor (880), and is used to store cryptographic keys and encryption algorithms. The cryptographic keys and algorithms stored in the key storage (892) are provisioned by the manufacturer during manufacturing of the SIM card holder (800), 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 the SIM card holder (800) such as a mobile network operator or a wireless service provider. In some embodiments, the content of the key storage (892) is never transmitted outside of the SPU (820), and is inaccessible by the PPU (830). The cryptographic keys and algorithms stored in the key storage (892) can be provisioned to perform various encryption standards and protocols including but not limited to Data Encryption Standard (DES), Triple Data Encryption Standard/Algorithm (TDES/TDEA), DES-X, Secure Socket Layer (SSL), Advanced Encryption Standard (AES), Blowfish, Serpent, Twofish, Threefish, 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.

**[0092]** In some embodiments, the tamper detection sensors (870) are included to detect external attempts to tamper with the SIM card holder (800). For example, the tamper detection sensors (870) may include temperature sensors to detect temperatures that may be indicative of someone attempting to desolder components of the SIM card holder (800), and/or mechanical sensors to sense structural changes to the SIM card holder (800) that may be indicative of someone attempting to dissect or cut open the SIM card holder (800). The tamper detection sensors (870) may also include electrical sensors to sense certain voltage, current, or impedance changes to the circuitry of the SIM card holder (800) that may be indicative of someone attempting to probe the components of the SIM card holder (800), and/or electromagnetic sensors to sense certain radiation such as X-rays that may be indicative of someone attempting to examine the SIM card holder (800). In some embodiments, the tamper detection sensors (870) may include circuitry that can erase and wipe out the contents of the secure memory (890) to render the SPU (820) and/or the SIM card holder (800) unusable in response to detecting an attempt to tamper with the SIM card holder (800). The SIM card holder (800) can also be

configured with organic or soluble interconnects that can be dissolved by a solvent released by the tamper detection sensors (870) in response to detecting an attempt to tamper with the SIM card holder (800).

**[0093]** FIG. 15 shows a conceptual block diagram illustrating the functional features of a SIM card holder (900), according to one embodiment. The SIM card holder (900) can be implemented with, for example, the hardware components described with reference to the SIM card holder (800) of FIG. 14. The PPU (930) of the SIM card holder (900) includes an operating system (OS) (934), a communication device application programming interface (API) (932), and a communication component API (933). The OS (934), the communication device API (932), and the communication component API (933) together form an access layer (931), which represents the publicly accessible portion of the SIM card holder (900). By “publicly accessible,” it is meant that any device or components of a communication device (915) (e.g., a mobile phone) that can communicate directly with a communication component (910) (e.g., a SIM card), or with a communication component reader of the communication device (915) (e.g., a SIM card reader of a mobile device), would be able to send and receive commands and information to and from the access layer (931).

**[0094]** The communication device API (932) provides a programming interface to translate commands and information received from the communication device (915) into instructions and data that the OS (934) can process and execute, and vice versa. For example, the communication device API (932) may translate commands from the communication device (915) according to a mobile phone’s SIM toolkit protocol into instructions and data that the OS (934) can process and execute to respond to the commands, and vice versa. The communication component API (933) provides a programming interface to translate commands and information received from the communication component (910) into instructions and data that the OS (934) can process and execute, and vice versa. For example, the communication component API (933) may translate commands from the communication component (910) according to a SIM card’s SIM toolkit protocol into instructions and data that the OS (934) can process and execute to respond to the commands, and vice versa.

**[0095]** The OS (934) manages the functionality and operations of the SIM card holder (900), and responds to commands and information from the communication device (915) (e.g., a mobile device such as a mobile phone) and/or the communication component (910) (e.g., a SIM card). The functionality and operations of the SIM card holder (900) that the OS (934) can manage includes responding to user input received on the communication device (915) that relates to cryptographic operations, masking PIN entries on a user interface of the communication device (915), creating ISO PIN blocks in the SPU (920), sending encryption and decryption requests to the SPU (920) for secure communications sent to and from a communication interface of the communication device (915), sending requests to the SPU (920) to create or verify MAC or hash values for messages or portions of messages sent to and from a communication interface of the communication device (915), 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 the communication device (915) and the communication component (910).

**[0096]** For example, in response to encryption and decryption commands received from the communication device (915) on the communication device API (932), the OS (934) can send encryption and decryption requests and associated data to the SPU (920). The OS (934) may access and process information stored in the communication component (910) in response to a command to perform as such received from the communication device (915) on the communication device API (932). The OS (934) can also access information stored in the communication component (910) and forward the information to the SPU (920) in response to encryption and decryption commands involving such information. The OS (934) can forward encryption and decryption results from the SPU (920) to the communication device (915) and/or the communication component (910). The OS (934) can also issue commands to the communication device (915) and/or the communication component (910), for example, commands to request the communication device (915) to send a secure communication with data encrypted by the SPU (920).

**[0097]** For non-secure commands and information (i.e. commands and information that do not involve cryptographic operations), the OS (934) can pass through or

forward the non-secure commands and information between communication device (915) and the communication component (910). For example, in response to non-secure commands and information from the communication device (915) intended for the communication component (910) received on the communication device API (932), the OS (934) can pass through or forward the non-secure commands and information to the communication component (910) through the communication component API (933). In response to non-secure commands and information from the communication component (910) intended for the communication device (915) received on the communication component API (933), the OS (934) can pass through or forward the non-secure commands and information to the communication device (915) through the communication device API (932).

**[0098]** The SPU (920) of the SIM card holder (900) includes a cryptographic module API (921) and a cryptographic module (922). The cryptographic module API (931) provides a programming interface to translate commands and information received from the OS (934) into instructions and data that the cryptographic module (922) can process and execute, and vice versa. For example, the OS (934) may send an encryption/decryption request to the SPU (920), and the cryptographic module API (931) may translate the encryption/decryption request into an encryption/decryption instruction for the cryptographic module (922) to execute. In some embodiments, the cryptographic module API (931) may also include, in the translated encryption/decryption instruction, which particular encryption algorithm the cryptographic module (922) should use based on the particular application that is requesting the cryptographic operation.

**[0099]** According to various embodiments, the cryptographic module (922) includes a secure application module (941), an encryption/decryption module (942), a secure key module (951), a seed key module (952), a random number generator (953), an ISO 0/1 PIN module (954), a MAC/HASH module (955), and a certificate module (956). In other embodiments, the cryptographic module (922) may include additional modules to perform other cryptographic operations. The secure application module (941) can store one or more secure applications such as mobile banking applications or contactless payment applications. The secure application module (941) can process user input selecting a particular function of the secure applications stored therein, and can respond with one or more commands instructing the communication

device (915) 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. The secure application module (941) can also instruct the encryption/decryption module (942) to perform specific cryptographic operations depending on the user selected function.

**[0100]** The encryption/decryption module (942) can store and execute various encryption algorithms including, but not limited to, one or more of the encryption algorithms listed above. The secure key module (951) stores the set of cryptographic or encryption keys that are used in the various encryption algorithms performed by the encryption/decryption module (942). The encryption keys can include symmetric keys and/or asymmetric keys. The seed key module (952) stores a set of seed keys that are used to initialize the encryption/decryption module (942) in certain encryption algorithms, such as AES. The seed key module (952) also stores seed keys that are used by the random number generator (953) to generate random numbers used in certain encryption algorithms such as RSA and DSA. The encryption keys stored in the secure key module (951) and/or the seed keys stored in the seed key module (952) are provisioned during manufacturing, and cannot be altered by an external source without a master key that was used during manufacturing to program the cryptographic module (922). The encryption keys and seed keys can also be provisioned to be specific to a particular SIM card holder, and hence the encryption keys and seed keys can be user-specific and unique to the user of the SIM card holder (900). One advantage of providing user-specific keys is that if the cryptographic keys stored in the cryptographic module (922) are 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.

**[0101]** In some embodiments, the cryptographic module (922) includes an ISO PIN module (954) to mask a user's PIN entry into the communication device (915) and to generate PIN blocks (e.g., ISO format 0/1 PINs) in accordance with ISO 9564 standard. The PIN blocks generated by the ISO PIN module (954) 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 the ISO PIN module (954) can be passed from the SPU (920) to the PPU (930) to be included in secure

communications sent from the communication device (915). It should be noted that the PINs stored in the ISO PIN module (954) are never stored in plaintext form, but are instead stored in an encryption format.

**[0102]** The cryptographic module (922) also includes a Message Authentication Code (MAC) / Hash module (955) to generate and verify MACs and/or hashes for secure communications sent to and from the communication device (915). 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. The cryptographic module (922) 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 the communication device (915).

**[0103]** The interactions and the exchange of commands and information between the SIM card holder (710), the mobile device (700), and the SIM card (720) in FIG. 13 according to one embodiment will now be described in more detail with reference to FIGs. 16-21. It should be understood that while the description and explanation provided below are made with reference to the particular embodiment shown in FIG. 13, the description and explanation provided below are applicable to and can be adapted for other embodiments, for example, embodiments in which the SIM card holder is used with other types of communication components 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 the SIM card holder (710) can interoperate with the mobile device (700) using the protocol that the mobile device (700) uses to communicate with the SIM card (720). 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 the SIM card holder (710) can interoperate with the communication device seamlessly with requiring any modifications to the software of the communication device.

**[0104]** FIG. 16 illustrates a SIM card initialization sequence according to one embodiment of the invention. When the mobile device (700) powers up or is turned on, the mobile device (700) issues a series of select file and read commands to the SIM card reader of the mobile device (700) to read subscriber information from the SIM card (720) to register the SIM card (720) with a mobile network. Because the SIM card (720) is inserted in the SIM card holder (710) and the SIM card holder essentially sits between the SIM card (720) and the mobile device (700), when the SIM card holder (710) receives these commands from mobile device (700), the SIM card holder (710) passes through or forwards these commands to the SIM card (720).

**[0105]** For example, after power up, the mobile device (700) may send a select file command (1002) to select a designated file in the file system of the SIM card (720) that stores subscriber information or other types of SIM card related information. Upon receiving the select file command (1002), the SIM card holder (710) determines that the file being requested is a file in the file system of the SIM card (720), and passes through or forwards the select file command (1002) to the SIM card (720). The SIM card (720) receives the select file command (1002), accesses the requested file, and sends a response (1004) towards the SIM card holder (710) indicating that the requested file was accessed successfully and is ready to be read. The SIM card holder (710) then passes through or forwards the response (1004) to the mobile device (700). In response to receiving the response (1004) notifying the mobile device (700) that the requested file is ready to be read, the mobile device (700) sends a read command (1010) towards the SIM card (720). Upon receiving the read command (1010), the SIM card holder (710) passes through or forwards the read command (1010) to the SIM card (720). In response to the read command (1010), the SIM card (720) sends file content (1012) of the requested file towards the mobile device (700). Depending on the file being requested, file content (1012) may include subscriber information, location/region information, configuration information such as language preference, and/or other types of SIM card information. Upon receiving the file content (1012), the SIM card holder (710) passes through or forwards the file content (1012) to the mobile device (700). The above series of commands and exchange of information may occur multiple times to allow the

mobile device (700) to read any information stored in the SIM card (720) that the mobile device (700) may use during its SIM card initialization sequence.

**[0106]** After the mobile device (700) finishes reading the information stored in the SIM card (720), the mobile device (700) may send a terminal profile (1014) towards the SIM card (720) to inform the SIM card (720) of the properties and capabilities of the mobile device (700). The terminal profile may include properties of the mobile device such as the types of communication interfaces available on the mobile device. Upon receiving the terminal profile (1014), the SIM card holder (710) may inspect the terminal profile (1014) to learn the properties and capabilities of the mobile device (700). The SIM card holder (710) then passes through or forwards the terminal profile (1014) to the SIM card (720). The SIM card (720) may send a response (1016) towards mobile device to indicate that terminal profile (1014) was successfully received. Upon receiving the response (1016), the SIM card holder (710) passes through or forwards the response (1016) to the mobile device (700).

**[0107]** Next, the process of installing a user menu that lists the features of the SIM card (720) and the SIM card holder (710) onto the mobile device (700) according to one embodiment of the invention will be described with reference to FIG. 17. After the SIM card initialization sequence of FIG 16., the mobile device (700) may send a fetch command (1102) towards the SIM card (720) to obtain any pending commands that the SIM card (720) wants the mobile device (700) to perform. Upon receiving the fetch command (1102), the SIM card holder (710) may pass through or forward the fetch command (1102) to the SIM card (720). The SIM card (720) may respond with a set-up-menu command (1106) that includes a list of features of the SIM card (720) to be included in the user menu of the mobile device (700). Upon receiving the set-up-menu command (1106) from the SIM card (720), the SIM card holder (710) can add its own list of user selectable features to the features of the SIM card (720) listed in the set-up-menu command (1106), and generates a set-up-menu command (1108) that lists the features of both the SIM card (720) and the SIM card holder (710). The list of features added by the SIM card holder (710) 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 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 the mobile device (700) equipped with the SIM card holder (710). The SIM card holder (710) then sends the set-up-menu command (1108) that includes the list of features of both the SIM card (720) and the SIM card holder (710) to the mobile device (700). In response to receiving the set-up-menu  
5 command (1108), the mobile device (700) adds the list of features of the SIM card (720) and the SIM card holder (710) to the user menu of the mobile device (700).

**[0108]** The mobile device (700) can send a terminal response (1110) towards the SIM card (720) to indicate that the user menu is set up successfully. Upon receiving the terminal response (1110), the SIM card holder (710) passes through or forwards  
10 the terminal response (1110) to the SIM card (720). The SIM card (720) may reply with a response (1112) indicating acknowledgement of the terminal response (1110) towards the mobile device (700). The SIM card holder (710) then passes through or forwards the response (1112) to the mobile device (700). The mobile device (700) can then display to a user the features and services that the SIM card holder (710)  
15 can provide on the mobile device (700), and the user can select one or more features of the SIM card holder (710) from the user menu of the mobile device (700) to send secure communication to perform various financial and/or banking transactions. A user can also select non-secure features of the SIM card (720), for example, to send unencrypted SMS messages, from the user menu of the mobile  
20 device (700).

**[0109]** FIG. 18 illustrates a non-secure operation being performed with the mobile device (700) using the SIM card (720), according to one embodiment. When a user selects a feature of the SIM card (720) to perform a non-secure operation (e.g., send unencrypted SMS, or display a message stored on the SIM card (720), etc.) from the  
25 user menu of the mobile device (700), the mobile device (700) sends a menu selection command (1202) indicating the selection of the non-secure operation towards the SIM card (720). Upon receiving the menu selection command (1202), the SIM card holder (710) determines that the menu selection command (1202) is requesting a feature of the SIM card (720). The SIM card holder (710) then passes  
30 through or forwards the menu selection command (1202) to the SIM card (720). In response to receiving the menu selection command (1202), the SIM card (720) sends a response (1204) towards the mobile device (700) to indicate the menu selection command (1202) has been received. The SIM card (720) processes the

menu selection command (1202) and prepares one or more device commands to send to the mobile device (700) to carry out the non-secure operation being requested.

**[0110]** Upon receiving the response (1204) indicating the menu selection command (1202) has been received by the SIM card (720), the SIM card holder (710) passes through or forwards the response (1204) to the mobile device (700). The mobile device (700) may then send a fetch command (1206) towards the SIM card (720) to obtain any pending commands that the SIM card (720) wants the mobile device (700) to perform to carry out the non-secure operation selected by the user. Upon receiving the fetch command (1206), the SIM card holder (710) passes through or forwards the fetch command (1206) to the SIM card (720). The SIM card (720) responds to the fetch command (1206) by sending a device command (1208) towards the mobile device (700) to instruct the mobile device (700) to perform one or more functions of the mobile device (700) to carry out the non-secure operation. For example, the device command (1208) may instruct the mobile device (700) to send an unencrypted SMS over the cellular interface of the mobile device (700), or display a stored SMS message on the screen of the mobile device (700). Upon receiving the device command (1208) from the SIM card (720), the SIM card holder (710) passes through or forwards the device command (1208) to the mobile device (700). The mobile device (700) then executes the device command (1208) to carry out the non-secure operation requested by the user.

**[0111]** FIG. 19 illustrates a secure communication being sent from the mobile device (700) using the SIM card holder (710), according to one embodiment. When a user selects a secure application such as a mobile banking application in the SIM card holder (710) from the user menu of the mobile device (700) 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, the mobile device (700) sends a menu selection command (1302) indicating the secure operation the user wants to perform to the SIM card holder (710). Upon receiving the menu selection command (1302), the SIM card holder (710) determines that the menu selection command (1302) is requesting a secure application of the SIM card holder (710) to perform a secure operation.

**[0112]** Depending on the secure operation selected by the user, the SIM card holder (710) may optionally retrieve information stored in the SIM card holder (710) such as an encrypted PIN to carry out the secure operation. In some embodiments, certain information stored in the SIM card (720) may also be used to carry out the secure operation. For example, the secure operation may include sending a secure communication from the mobile device (700) to a recipient device, and the unique serial number (ICCID) of the SIM card (720) and/or the international mobile subscriber identity (IMSI) of the SIM card (720) may be included in the secure communication to verify the identity of the SIM card holder (710). In such embodiments, the SIM card holder (710) may optionally send a select file command (1304) to the SIM card (720) to access the designated file storing the information in the SIM card (720). In response to receiving the select file command (1304), the SIM card (720) sends a response (1306) to the SIM card holder (710) indicating the designated file has been selected and is ready to be read. The SIM card holder (710) then sends a read command (1308) to the SIM card (720) to read the information from the designated file. In response to the read command (1308), the SIM card (720) sends file content (1310), for example, the ICCID and/or IMSI of the SIM card (720), to the SIM card holder (710).

**[0113]** Next, the SIM card holder (710) sends a response (1312) to the mobile device (700) to acknowledge that the menu selection command (1302) was received. The mobile device (700) then sends a fetch command (1314) to the SIM card holder (710) to obtain any pending commands that the SIM card holder (710) wants the mobile device (700) to perform to carry out the secure operation. In some embodiments, depending on the secure operation selected by the user, in response to receiving the fetch command (1314), the SIM card holder (710) may optionally send a display command (not shown) to the mobile device (700) to instruct the mobile device (700) to prompt a user for input on the 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 the mobile device (700), the mobile device (700) sends a user-input-event command (not shown) to the SIM card holder (710) to notify the SIM card holder (710) that user input has been received. The SIM card holder (710) can then send a get-user-input

command (1316) to the mobile device (700) to request the user input. In response, the mobile device (700) sends user input (1318) to the SIM card holder (710). The SIM card holder (710) may perform cryptographic operations on the user input such as encrypting the user input using any of the encryption algorithms stored in the SIM card holder (710), or generate a MAC or hash of the user input. The SIM card holder (710) sends a response (1320) to the mobile device (700) acknowledging the user input has been received.

**[0114]** The mobile device (700) may send another fetch command (not shown) to the SIM card holder (710) to obtain further device commands that the SIM card holder (710) wants the mobile device (700) to execute to carry out the secure operation. Thus, the mobile device (700) and the SIM card holder (710) can optionally exchange a series of fetch commands and device commands in response to those fetch commands to instruct the mobile device (700) 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 the SIM card holder (710) may request or use to carry out the secure operation is not just limited to user input. For example, the SIM card holder (710) may send commands to the mobile device (700) to instruct the mobile device (700) to retrieve information using any of the interfaces of the mobile device (700). The SIM card holder (710) may instruct the mobile device (700) to obtain location information from a global positioning system interface of the mobile device (700). The SIM card holder (710) may request information received from an external NFC device or NSC device through a NFC or NSC interface of the mobile device (700). The SIM card holder (710) may instruct the mobile device (700) to retrieve information from the internet through a wireless data interface of the mobile device (700), and so on. The SIM card holder (710) may perform additional cryptographic operations on any information obtained from the various interfaces of the mobile device (700).

**[0115]** Once the SIM card holder (710) has obtained and performed the desired cryptographic operations on the information (e.g., account numbers, transaction amount, etc.) that the SIM card holder (710) will use to carry out the secure operation, in response to a fetch command (1322) received from the mobile device (700), the SIM card holder (710) can transmit a send communication command (1324) with an encrypted message that includes any of the information described

above to the mobile device (700). The send communication command (1324) can instruct the mobile device (700) to transmit an encrypted message provided by the SIM card holder (710) using any of the communication interfaces available on the mobile device (700). For example, the send communication command (1324) may instruct the mobile device (700) to send a secure SMS message with encrypted data provided by the SIM card holder (710) to a server to make a mobile payment or to check account balance. The send communication command (1324) may instruct the mobile device (700) 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 (1324) may also instruct the mobile device (700) to send a secure NFC, NSC or RF communication with encrypted data via the NFC, NSC or RF interface of the mobile device (700) to a NFC, NSC or RF enabled recipient device such as a point-of-sale (POS) terminal. Because the information that the mobile device (700) transmits out in the secure communication is provided to the mobile device (700) in an encrypted format by the SIM card holder (710), the secure communication is already encrypted when it leaves the communication interface of the mobile device (700). In this manner, secure encrypted end-to-end communication can be maintained between the mobile device (700) and a recipient device.

**[0116]** Referring now to FIG. 20, in some embodiments, the send communication command (1324) may instruct the mobile device (700) to send a series of messages to a recipient device (730) to set up a secure communication channel or tunnel. The series of messages (1412-1420) can be used to verify the identity of recipient device (730) and to verify the identity of the mobile device (700) to recipient device (730). 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 (730) may not be known to the mobile device (700) prior to the communication. The series of messages (1412-1420) can be a number challenge that includes a specific sequence of numbers that is only known to the mobile device (700) as provided by the SIM card holder (710), and only known to authorized recipient devices that are allowed to communicate with the mobile device (700).

**[0117]** When the recipient device (730) receives a first message (1412), the recipient device (730) does not initially respond. The recipient device (730) will not

respond until all messages (1412-1420) has been received and the number sequence transmitted in the messages (1412-1420) is confirmed to be a valid and correct sequence. Thus, the recipient device (730) can verify the identity of the mobile device (700) based on the number challenge received in the series of messages (1412-1420). The mobile device (700) can also use the number challenge to verify the identity of recipient device (730). For example, if a recipient device response to the first message (1412), the mobile device (700) can determine that the recipient device is not an authorized recipient device because an authorized recipient device would not respond right away to the first message (1412). It should be appreciated that the series of messages as described 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, the mobile device (700) equipped with the SIM card holder (710) can act as a recipient device and be on the receiving end of a number challenge.

**[0118]** In some embodiments, to provide an additional level of security to verify the identity of the devices, the recipient device (730) can respond to the reception of a valid and correct number challenge with an encryption key challenge (1424). The encryption key challenge (1424) can be a symmetric key challenge or an asymmetric key challenge. In the encryption key challenge (1424), the recipient device (730) can send a random number to the mobile device (700) to request the mobile device (700) to encrypt the random number with an encryption key that would only be known to an authorized device. The mobile device (700) can send the random number to the SIM card holder (710) and request the SIM card holder (710) to encrypt the random number using the requested encryption key stored in the SIM card holder (710). The SIM card holder (710) can respond to the mobile device (700) with the encrypted random number, and the mobile device (700) then sends the encrypted random number to the recipient device (730). The recipient device (730) 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 the recipient device (730) has previously sent to the mobile device (700), then the recipient device (730) can be further assured that the mobile device (700) equipped with the SIM card holder (710) is an authorized device, and a secure communication

channel or tunnel can be established between the mobile device (700) and the recipient device (730). Exchange of sensitive information with secure communications between the two devices can then proceed.

[0119] One advantage of the being able to verify the identities of the communicating devices using the SIM card holder (710) 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 SIM card holder, 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.

[0120] FIG. 21 illustrates a flow diagram for enabling transmission of secure communications from a communication device (e.g., the mobile device (700) of FIG. 13) using a SIM card holder (e.g., the SIM card holder (710) of FIG. 13) attached to a communication component (e.g., the SIM card (720) of FIG. 13) of the communication device, according to various embodiments.

[0121] At a first stage (1502), the SIM card holder 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 SIM card holder. 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 SIM card holder 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.

**[0122]** At a next stage (1504), the SIM card holder determines if the protocol message is associated with a secure operation. If the SIM card holder determines that the protocol message involves a secure operation to be performed by the SIM card holder, for example, by examining the flag or the protocol ID of the protocol message, then at a next stage (1506), using the embedded cryptographic processor, the SIM card holder 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 SIM card holder 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 SIM card holder may retrieve an encrypted PIN from the SIM card holder, 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 SIM card holder to decrypt.

**[0123]** To perform the cryptographic operation on data or information associated with the secure operation, the SIM card holder may select a suitable encryption and/or MAC or hash algorithm stored in the SIM card holder. The SIM card holder 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 SIM card holder may also generate or verify a MAC or hash on data or information associated with the secure operation.

**[0124]** Then at a next stage (1508), the SIM card holder sends a device command and/or the result of the cryptographic operation (i.e. processed data such as

encrypted or decrypted data) to the communication device in accordance with the protocol of the protocol message. The processed data or device command can be sent from the SIM card holder to the communication device, for example, via the first set of electrical contacts of the SIM card holder. The device command can include

5 commands instructing the communication device to perform certain operations to carry out the secure operation such as sending encrypted data provided by the SIM card holder 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

10 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 SIM card holder decrypted from an encrypted message sent to the communication device. It should

15 be understood that depending on the secure operation that is being requested or associated with the protocol message received from the communication device at the initial stage (1502), the SIM card holder 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

20 command exchanges to carry out a secure operation.

**[0125]** Referring back to the second stage (1504), if the SIM card holder determines that the protocol message is associated with a non-secure operation that is intended for the communication component, then at a next stage (1510), the SIM card holder forwards or passes through the protocol message to the communication component.

25 At a further stage (1512), the communication component may reply to the SIM card holder with a response to the protocol message. Upon receiving the response to the protocol message from the communication component, at a next stage (1514), the SIM card holder forwards or passes through the response to the communication device.

30 **[0126]** 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).

**[0127]** FIG. 22 shows a mobile device (1600) according to the embodiments described above. The mobile device (1600) includes a SIM card reader (1610) for accepting a SIM card that may be equipped with a SIM card holder as described herein. The mobile device (1600) also includes a display (1620), an input element (1630), computer readable medium (1640) such as volatile and non-volatile memory, a processor (1650) and at least one antenna (1660). In addition, the mobile device (1600) may include a dual interface including both a contact (not shown) and a contactless interface (1670) for transferring information through direct contact or through an integrated chip, which may be coupled to a second antenna. The mobile device (1600) may be capable of communicating through a cellular network, such as GSM through the antenna (1660). The mobile device (1600) also includes a speaker (1680) and a microphone (1690). Thus, the mobile device (1600) may be capable of transmitting and receiving information wirelessly through both short range NFC, RF and cellular connections, and through NSC. The device of FIG. 22 may include an account identifier associated with an account.

**[0128]** A SIM card holder for enabling a mobile device to perform secure communications is therefore provided. The SIM card holder acts as a housing into which a smaller SIM card fits, which can then be coupled to a mobile device.

**[0129]** The structure of the SIM card holder enables those components of a SIM card holder, such as a SIM card holder implemented as an adhesive layer, which are relatively large in size, to be moved to the periphery of the SIM card holder so as to reduce the overall thickness of such a device and SIM card when attached to each other. This may alleviate the problem of a secure element such as a cryptographic expansion device attached to a SIM card being too thick to insert into a SIM card receiving slot or a SIM card reader of a mobile device. This may also enable additional circuitry, features and/or capabilities to be included in such a secure element.

**[0130]** Furthermore, placement of a SIM card into the SIM card holder and removal of a SIM card from the holder and removal (in applicable cases) may be performed relatively easily and quickly.

**[0131]** The use of a SIM card holder may make branding easier. Whereas the color of the cheapest, most easily accessible flexible printed circuits is generally black, the SIM card holder may be of a light color. This enables conventional printing of branding on the surface of the body, and serves to make branding more visible, for example, for the purpose of marketing.

**[0132]** 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 may reside on or within a single computational apparatus, and may be present on or within different computational apparatuses within a system or network.

**[0133]** 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.

**[0134]** The foregoing description of the embodiments of the invention has been presented for the purpose of illustration; it is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Persons skilled in the relevant art can appreciate that many modifications and variations are possible in light of the above disclosure.

**[0135]** Some portions of this description describe the embodiments of the invention in terms of algorithms and symbolic representations of operations on information.

These algorithmic descriptions and representations are commonly used by those skilled in the data processing arts to convey the substance of their work effectively to others skilled in the art. These operations, while described functionally, computationally, or logically, are understood to be implemented by computer programs or equivalent electrical circuits, microcode, or the like. Furthermore, it has also proven convenient at times, to refer to these arrangements of operations as modules, without loss of generality. The described operations and their associated modules may be embodied in software, firmware, hardware, or any combinations thereof.

**[0136]** Any of the steps, operations, or processes described herein may be performed or implemented with one or more hardware or software modules, alone or in combination with other devices. In one embodiment, a software module is implemented with a computer program product comprising a computer-readable medium containing computer program code, which can be executed by a computer processor for performing any or all of the steps, operations, or processes described.

**[0137]** Finally, the language used in the specification has been principally selected for readability and instructional purposes, and it may not have been selected to delineate or circumscribe the inventive subject matter. It is therefore intended that the scope of the invention be limited not by this detailed description, but rather by any claims that issue on an application based hereon. Accordingly, the disclosure of the embodiments of the invention is intended to be illustrative, but not limiting, of the scope of the invention, which is set forth in the following claims.

WHAT IS CLAIMED IS:

1  
2  
3  
4  
5  
6  
7  
8  
9  
10

1. A subscriber identity module (SIM) card holder for enabling a mobile device to perform secure communications, the SIM card holder comprising:

a first set of electrical contacts disposed on a top side of the holder for interfacing to a mobile device;

a hardware security module (HSM) disposed in the holder and coupled to the first set of electrical contacts; and

a receiving slot configured to receive a SIM card, wherein the receiving slot includes a second set of electrical contacts coupled to the HSM for interfacing to the SIM card.

1  
2  
3  
4  
5  
6

2. The SIM card holder as claimed in claim 1 in which the SIM card is a micro-SIM card, the SIM card holder having substantially similar dimensions to a mini-SIM card so as to enable it to be received in a mini-SIM card reader or mini-SIM card receiving slot of a mobile device when the micro-SIM card is received in the receiving slot of the SIM card holder.

1  
2  
3  
4  
5  
6

3. The SIM card holder as claimed in claim 1 in which the SIM card is a nano-SIM card, the SIM card holder having substantially similar dimensions to a micro-SIM card so as to enable it to be received in a micro-SIM card reader or micro-SIM card receiving slot of a mobile device when the nano-SIM card is received in the receiving slot of the SIM card holder.

1  
2  
3  
4  
5  
6

4. The SIM card holder as claimed in claim 1 in which the SIM card is a nano-SIM card, the SIM card holder having substantially similar dimensions to a mini-SIM card so as to enable it to be received in a mini-SIM card reader or mini-SIM card receiving slot of a mobile device when the nano-SIM card is received in the receiving slot of the SIM card holder.

1  
2  
3  
4

5. A SIM card holder as claimed in claim 1 which has substantially similar dimensions to a SIM card receiving tray of a mobile device so as to act as a replacement SIM card receiving tray.

1           6.       A SIM card holder as claimed in any one of the preceding claims  
2 which has a thickness equal to or less than 120 microns more than the thickness of a  
3 SIM card to be received in the receiving slot.  
4

1           7.       A SIM card holder as claimed in any one of the preceding claims  
2 which has a thickness equal to or less than 60 microns more than the thickness of a  
3 SIM card to be received in the receiving slot.  
4

1           8.       A SIM card holder as claimed in any one of the preceding claims  
2 in which the first set of electrical contacts and the second set of electrical contacts  
3 are disposed in a thin film, the film optionally provided with an adhesive material  
4 disposed thereon to enable attachment of a SIM card to the SIM card holder.  
5

1           9.       A SIM card holder as claimed in any one of the preceding claims  
2 in which the receiving slot is defined by an opening at a bottom surface of the SIM  
3 card holder and openings or partial openings at each of a first side and a second  
4 side of the SIM card holder.  
5

1           10.      A SIM card holder as claimed in any one of claims 1 to 8 which  
2 the receiving slot is closable by a thin closing integral to the SIM card holder,  
3 optionally with adhesive material disposed thereon, and extending between inner  
4 surfaces of the receiving slot at a bottom side thereof so as to define the receiving  
5 slot by an opening at at least a first insertion end of the SIM card holder.  
6

1           11.      A SIM card holder as claimed in claim 10 in which the thin  
2 closing is pivotally attached to a first inner surface of the receiving slot at a first end  
3 of the closing and is provided with a clip formation at a second end thereof so as to  
4 enable the closing to be moved between an open position, in which it lies generally  
5 transverse to a bottom surface of the SIM card holder, to a closed position, in which  
6 it lies generally parallel to the bottom surface of the SIM card holder and in which the  
7 clip formation is received in a corresponding receiving formation at a second,  
8 opposing inner surface of the receiving slot.  
9

1           12. A SIM card holder as claimed in any one of claims 1 to 8 which  
2 has a closed bottom provided by a thin adhesive sticker removably attached to the  
3 SIM card holder and which, when attached, extends across the receiving slot on a  
4 bottom surface of the SIM card holder.  
5

1           13. A SIM card holder as claimed in any one of claims 1 to 8 in  
2 which the receiving slot is defined by a pair of thin, protruding ledges extending  
3 inwardly from opposing inner surfaces of the receiving slot such that a bottom  
4 surface of the SIM card abuts top surfaces of the ledges when the SIM card is  
5 received in the receiving slot.  
6

1           14. A SIM card holder as claimed in any one of the preceding claims  
2 which includes branding provided thereon.  
3

1           15. A SIM card holder as claimed in any one of the preceding claims  
2 in which the secure communications include sending secure communications using a  
3 communication protocol selected from a group consisting of Short Message Service  
4 (SMS) protocol, Unstructured Supplementary Service Data (USSD) protocol, Near  
5 Field Communication (NFC) protocol, Radio Frequency (RF) communications  
6 protocol, and Near Sound Communication (NSC) protocol.  
7

1           16. A SIM card holder as claimed in any one of the preceding claims  
2 in which the mobile device is a mobile phone and in which the secure  
3 communications include one or both of financial transactions and banking  
4 transactions.  
5

1           17. A system comprising:  
2 a SIM card; and  
3 a SIM card holder, the SIM card holder comprising:  
4 a first set of electrical contacts disposed on a top side of the  
5 holder for interfacing to a mobile device;  
6 a HSM disposed in the holder and coupled to the first set of  
7 electrical contacts; and  
8 a receiving slot configured to receive the SIM card, wherein the

receiving slot includes a second set of electrical contacts coupled to the HSM for interfacing to the SIM card; and

wherein the SIM card holder enables a mobile device using the SIM card to send encrypted data using the HSM disposed in the SIM card holder.

18. A system as claimed in claim 17 in which the encrypted data is sent using a communication interface of the mobile device.

19. A system as claimed in claim 17 or claim 18 in which the encrypted data is associated with one or both of a financial transaction and a banking transaction.

20. A system as claimed in any one of claims 17 to 19 in which the mobile device is a mobile phone and the communication interface is one of a cellular communications interface for transmitting SMS messages, a cellular communications interface for transmitting USSD messages, a NFC interface, a NSC interface and an RF interface.

21. A method for enabling transmission of secure communications from a mobile device using a SIM card holder having a first set of electrical contacts and a second set of electrical contacts, wherein a SIM card of the mobile device is received in a receiving slot of the SIM card holder so as to interface to the SIM card holder via the second set of electrical contacts, the method comprising:

receiving, at the SIM card holder, a first message;  
determining that the first message is associated with a secure operation;

performing, by an HSM disposed in the holder, a cryptographic operation on data associated with the secure operation; and

sending the data processed by the HSM from the SIM card holder to the mobile device via the first set of electrical contacts for transmission in a secure communication.

22. A method as claimed in claim 21, further comprising:

2 sending the secure communication from the mobile device in one of a  
3 SMS message, a USSD message, a NFC communication, a NSC communication  
4 and a RF communication.  
5

1 23. A method as claimed in claim 21 or claim 22, further comprising:  
2 receiving, in the SIM card holder, a second message;  
3 determining that the second message is associated with a non-secure  
4 operation; and  
5 passing through the message between the SIM card and the mobile  
6 device.  
7

1 24. A method as claimed in any one of claims 21 to 23 in which the  
2 mobile device is a mobile phone and in which the data processed by the HSM is  
3 associated with one or both of a financial transaction and a banking transaction  
4 being conducted with the mobile device.  
5

1 25. A method as claimed in any one of claims 21 to 24 in which the  
2 HSM includes a public processor and a cryptographic processor and in which the  
3 cryptographic processor is accessible to both the SIM card and the mobile device  
4 only through the public processor disposed in the SIM card holder.  
1

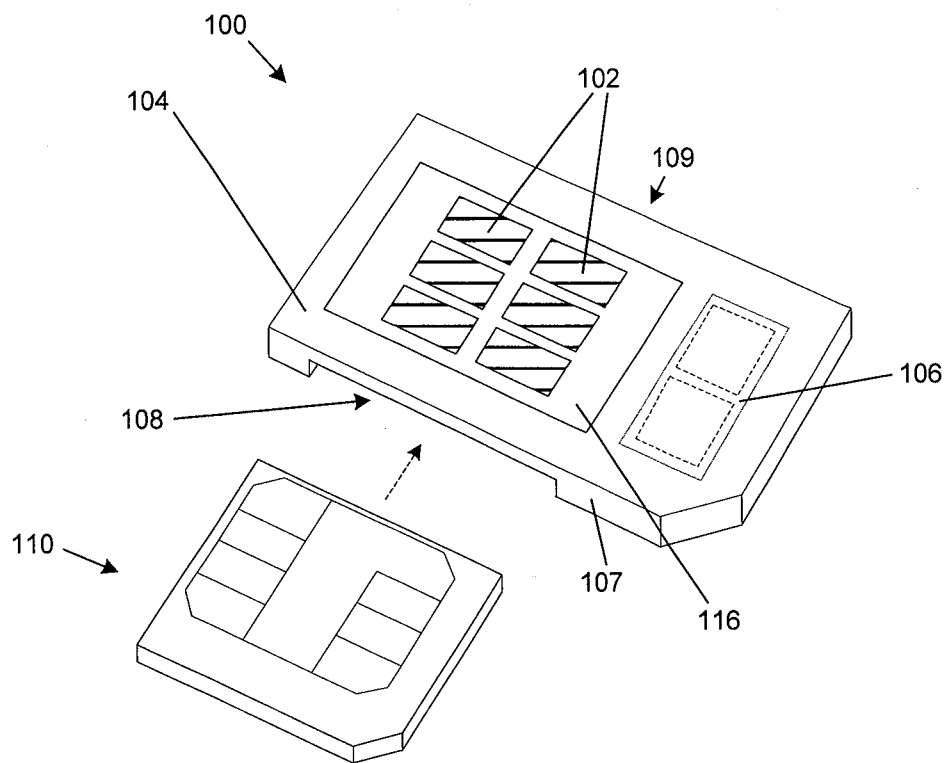


FIG. 1

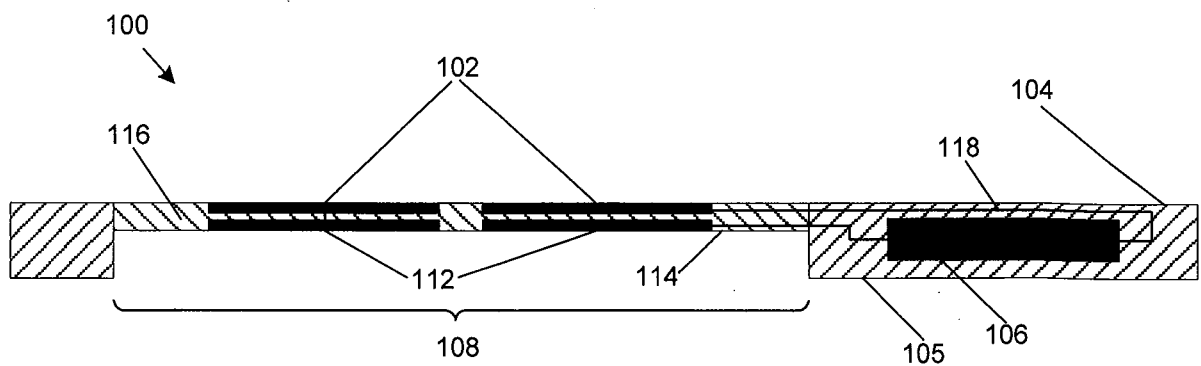


FIG. 2

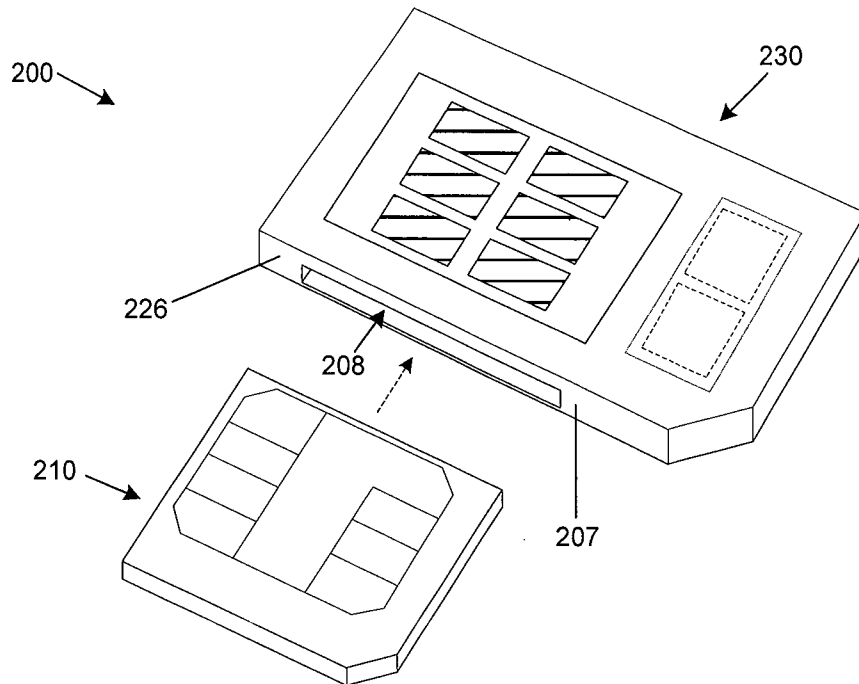


FIG. 3

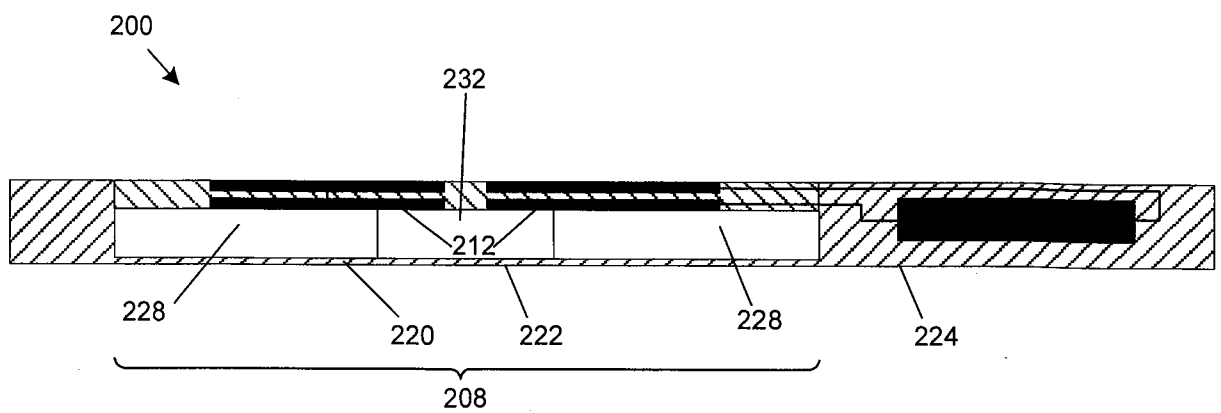


FIG. 4

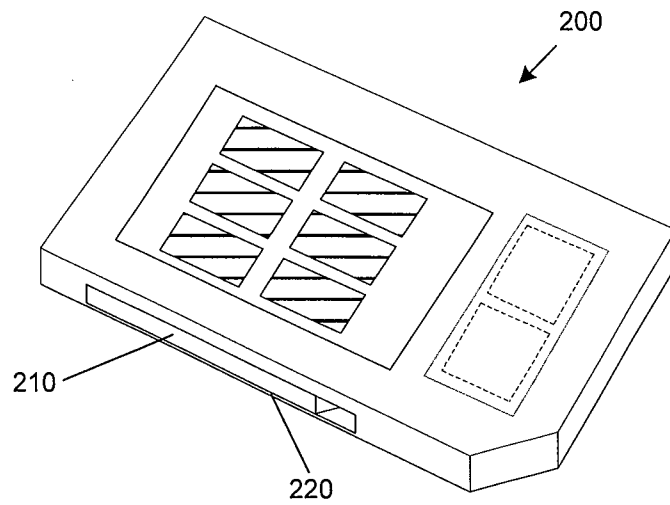


FIG. 5

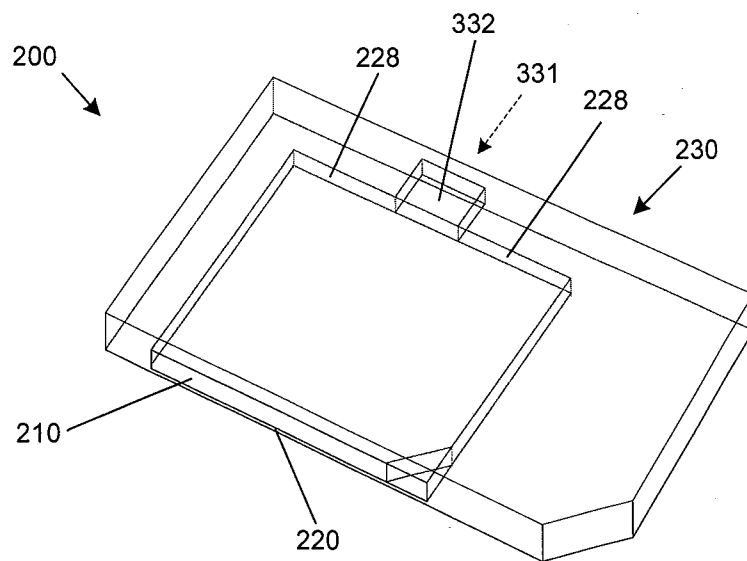


FIG. 6

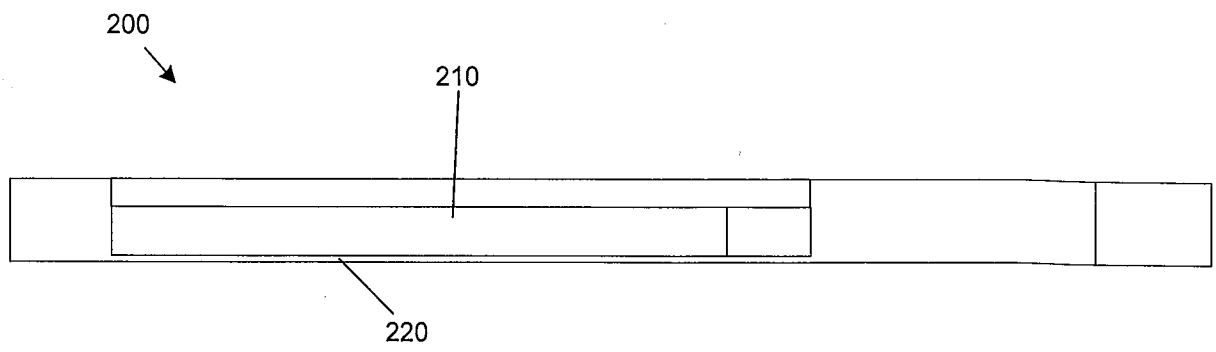


FIG. 7

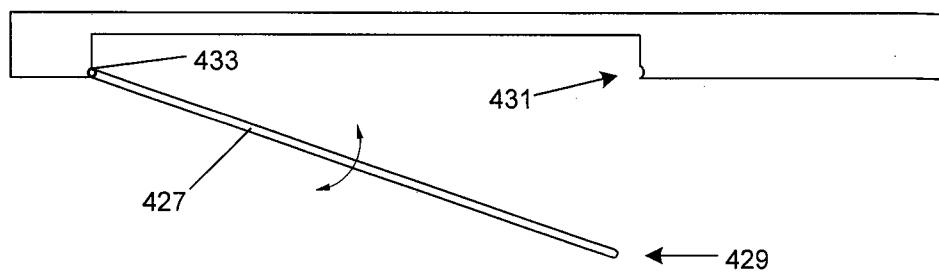


FIG. 8

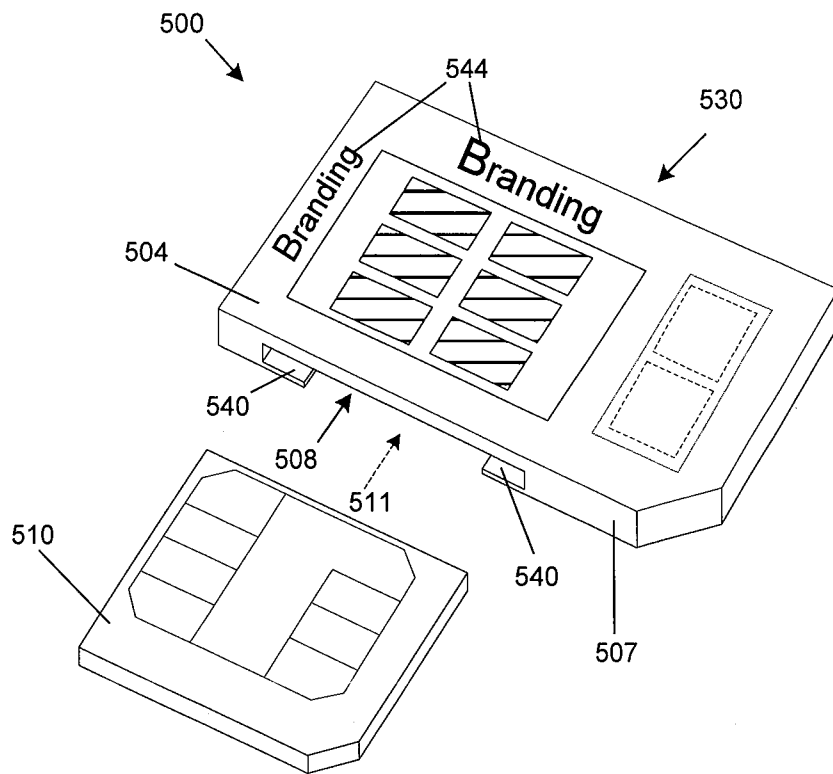


FIG. 9

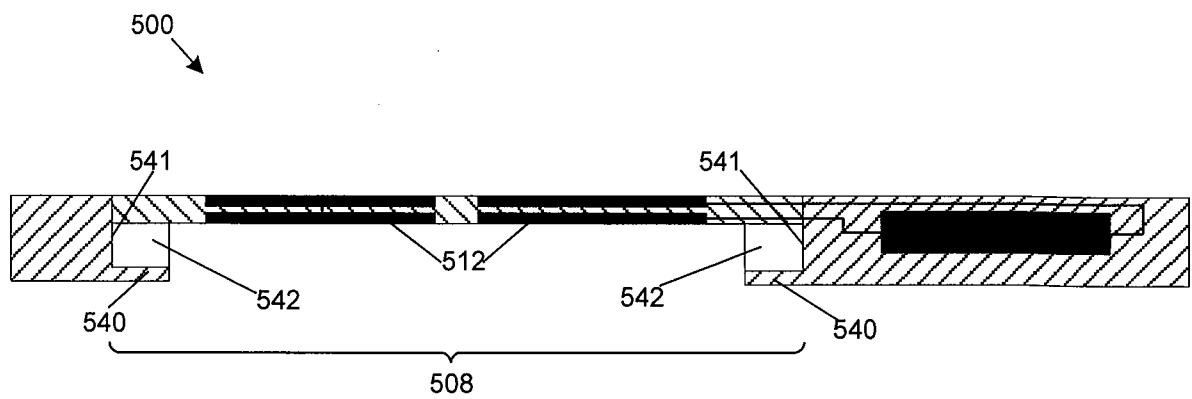


FIG. 10

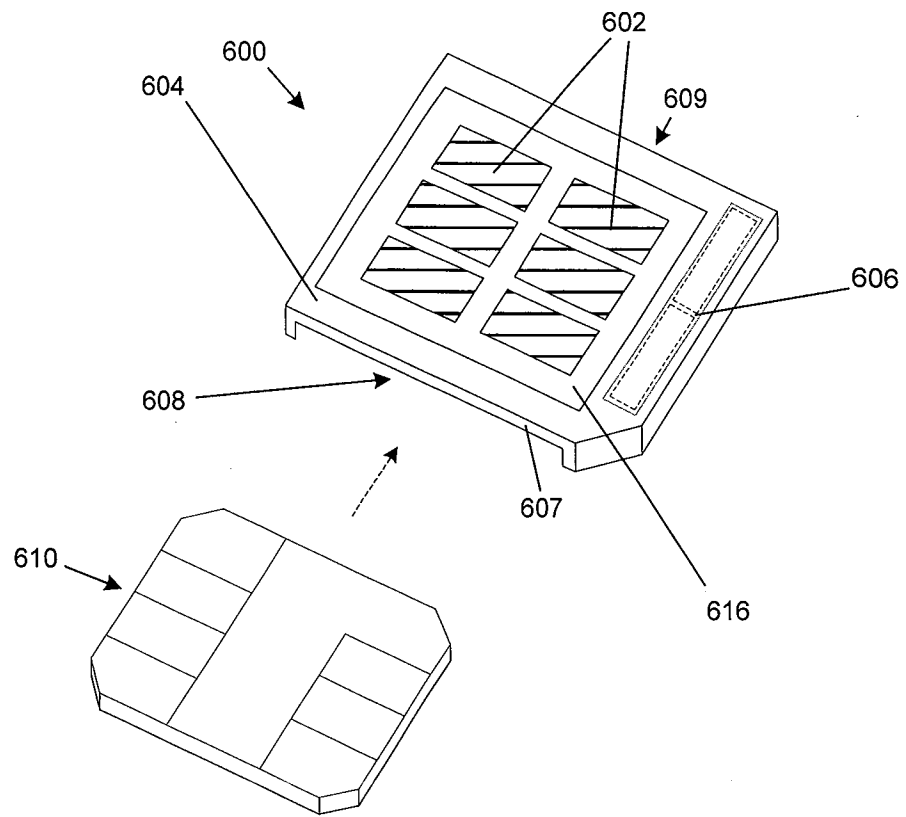


FIG. 11

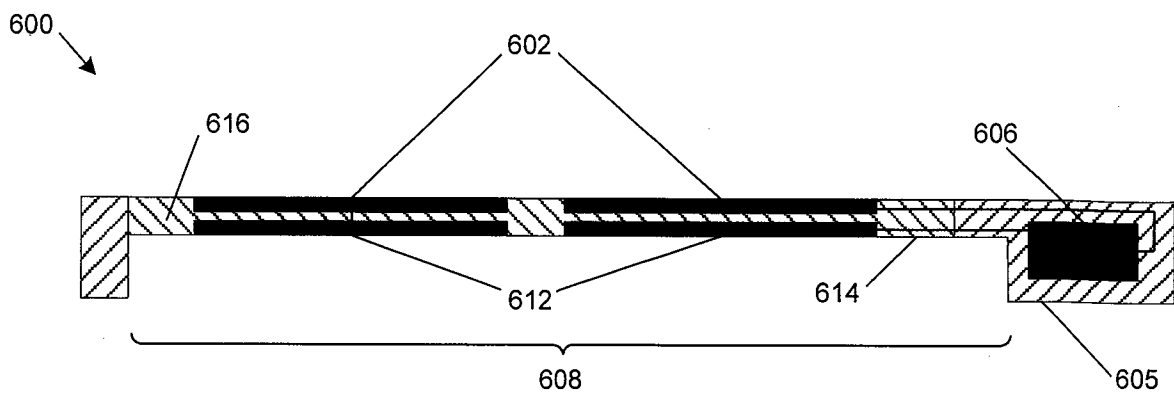


FIG. 12

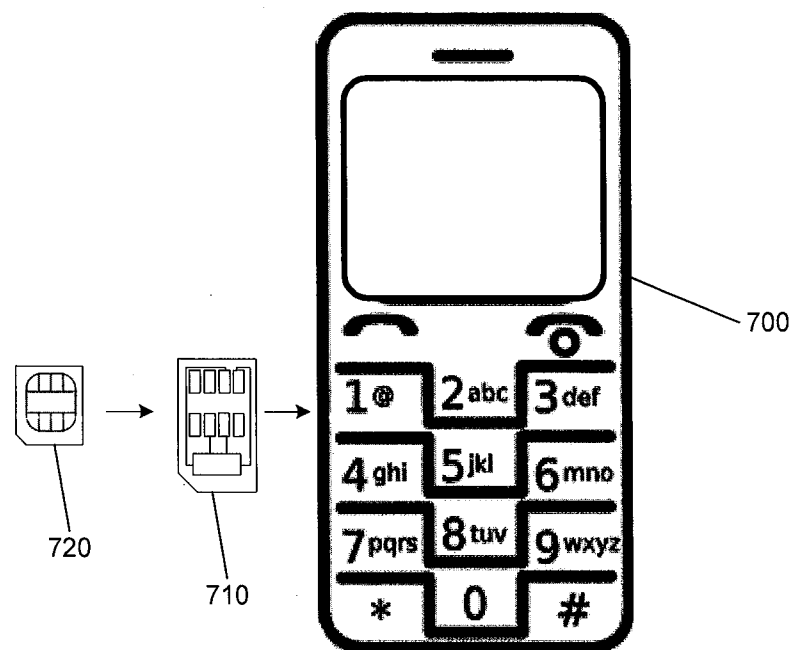


FIG. 13

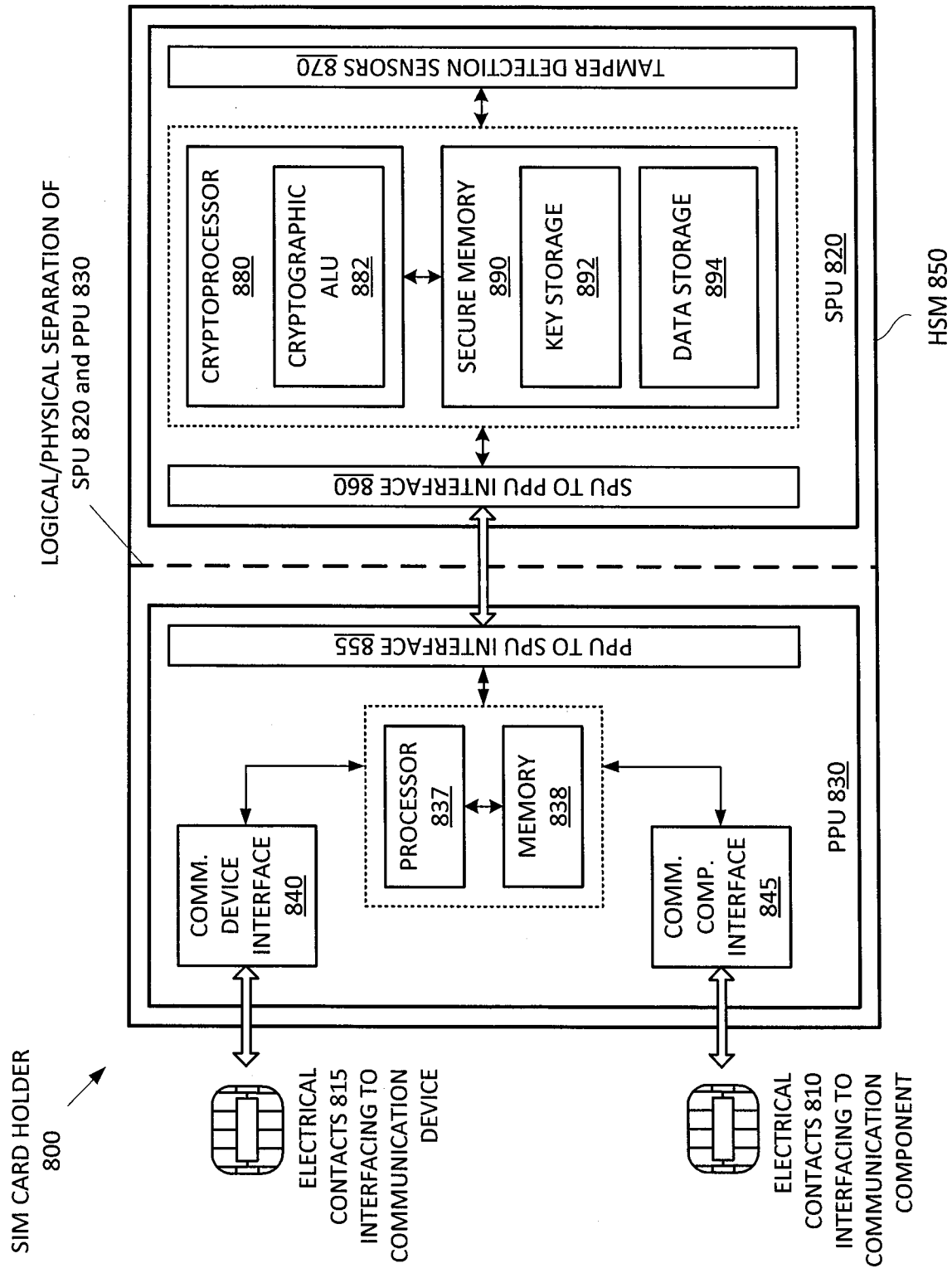


FIG. 14

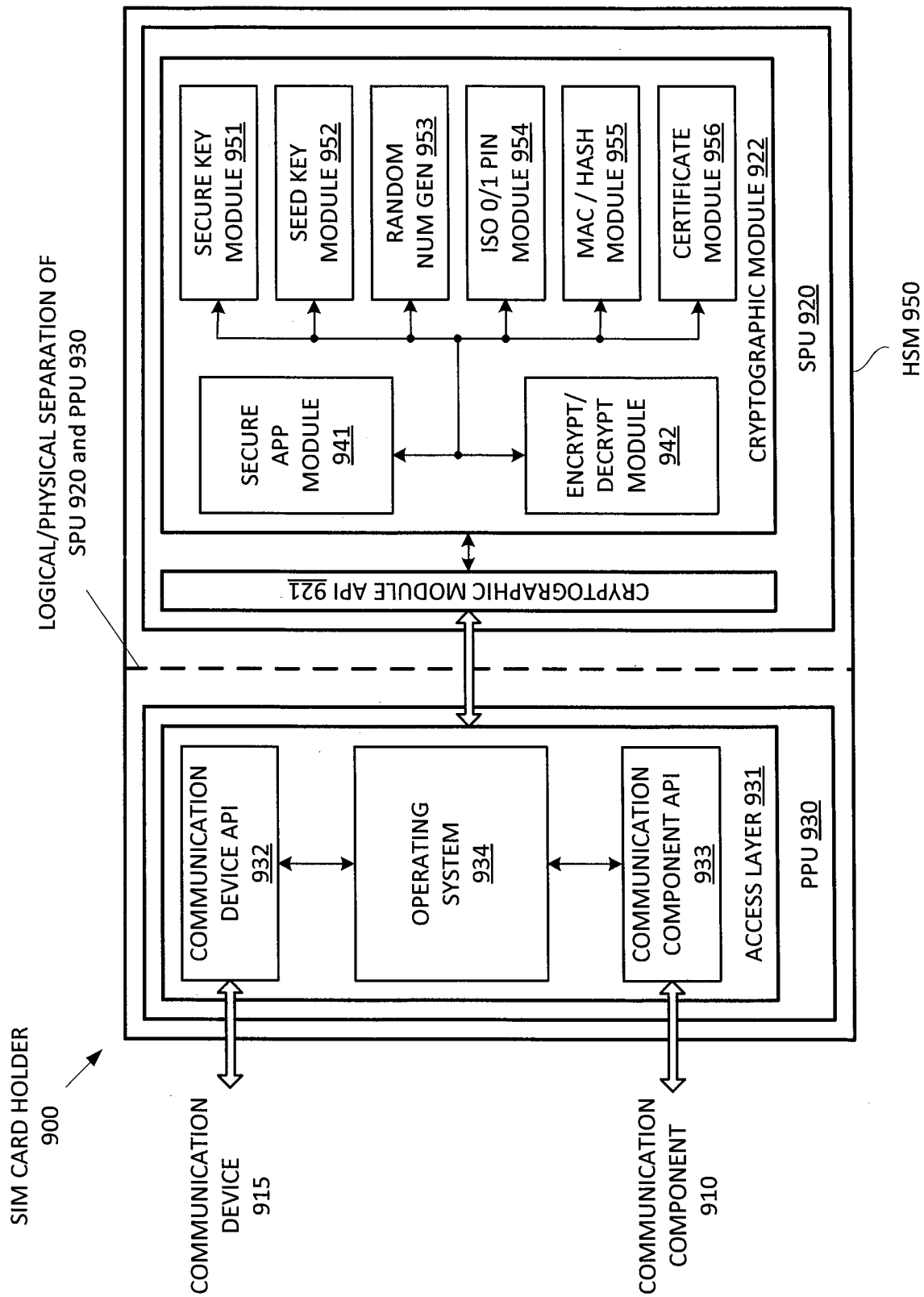


FIG. 15

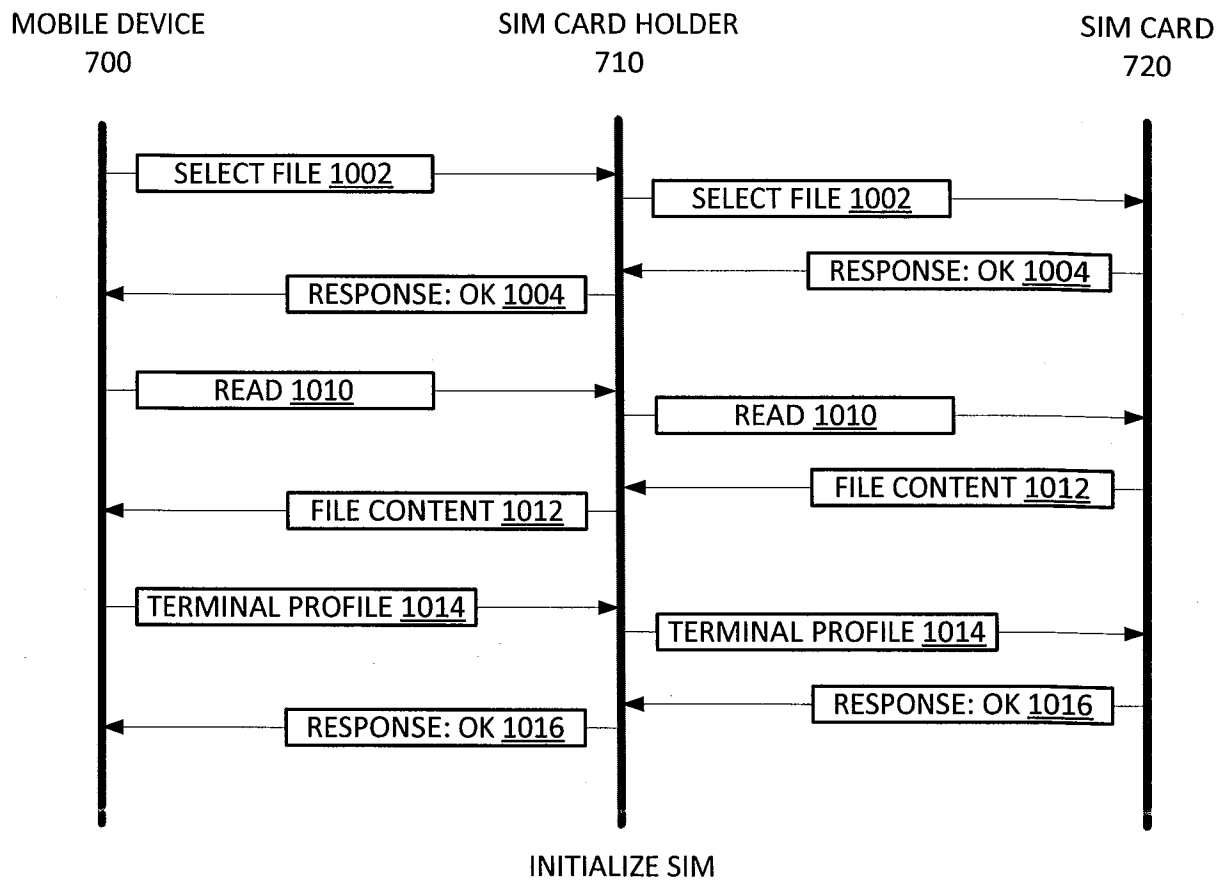


FIG. 16

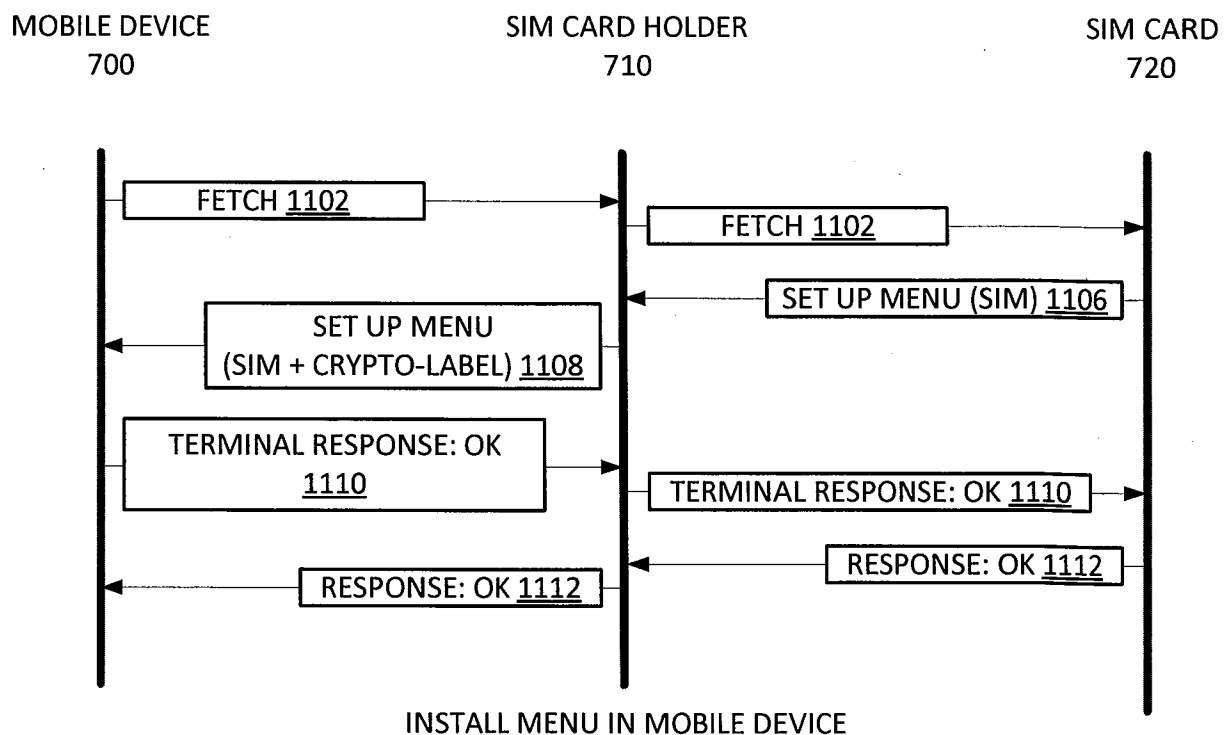


FIG. 17

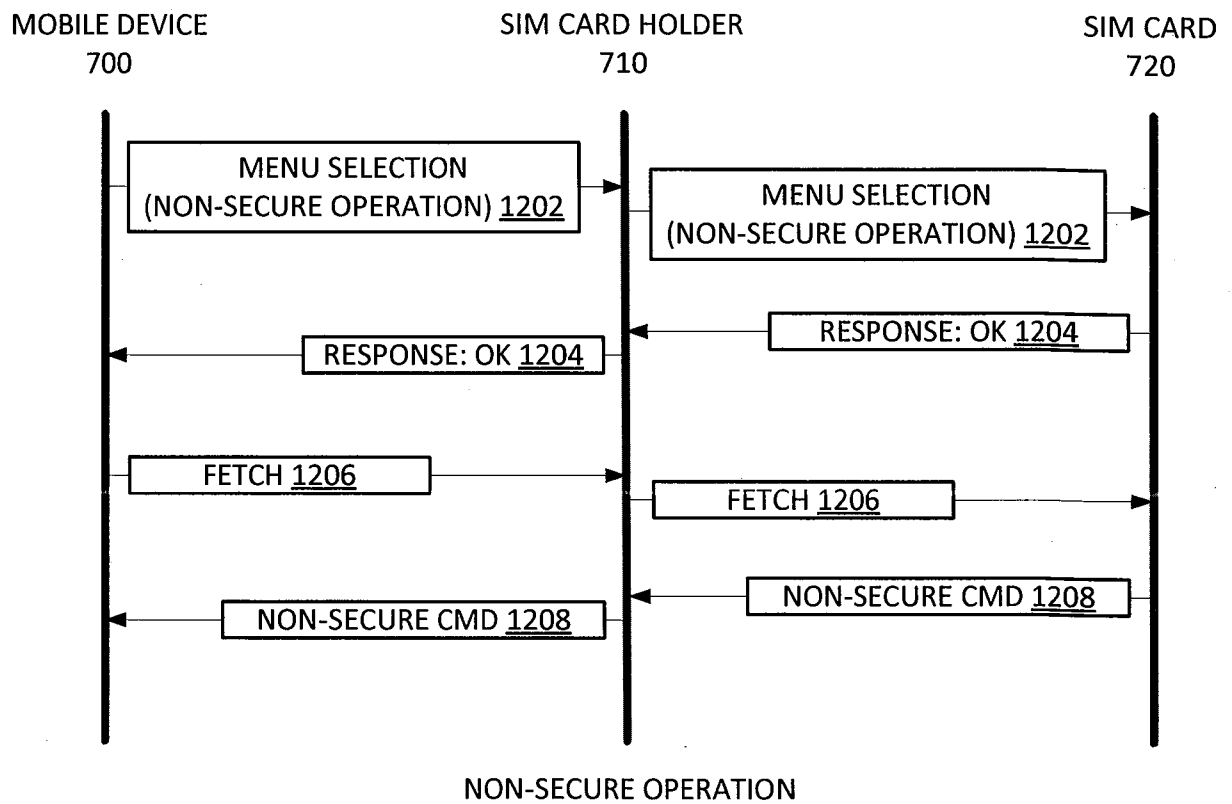


FIG. 18

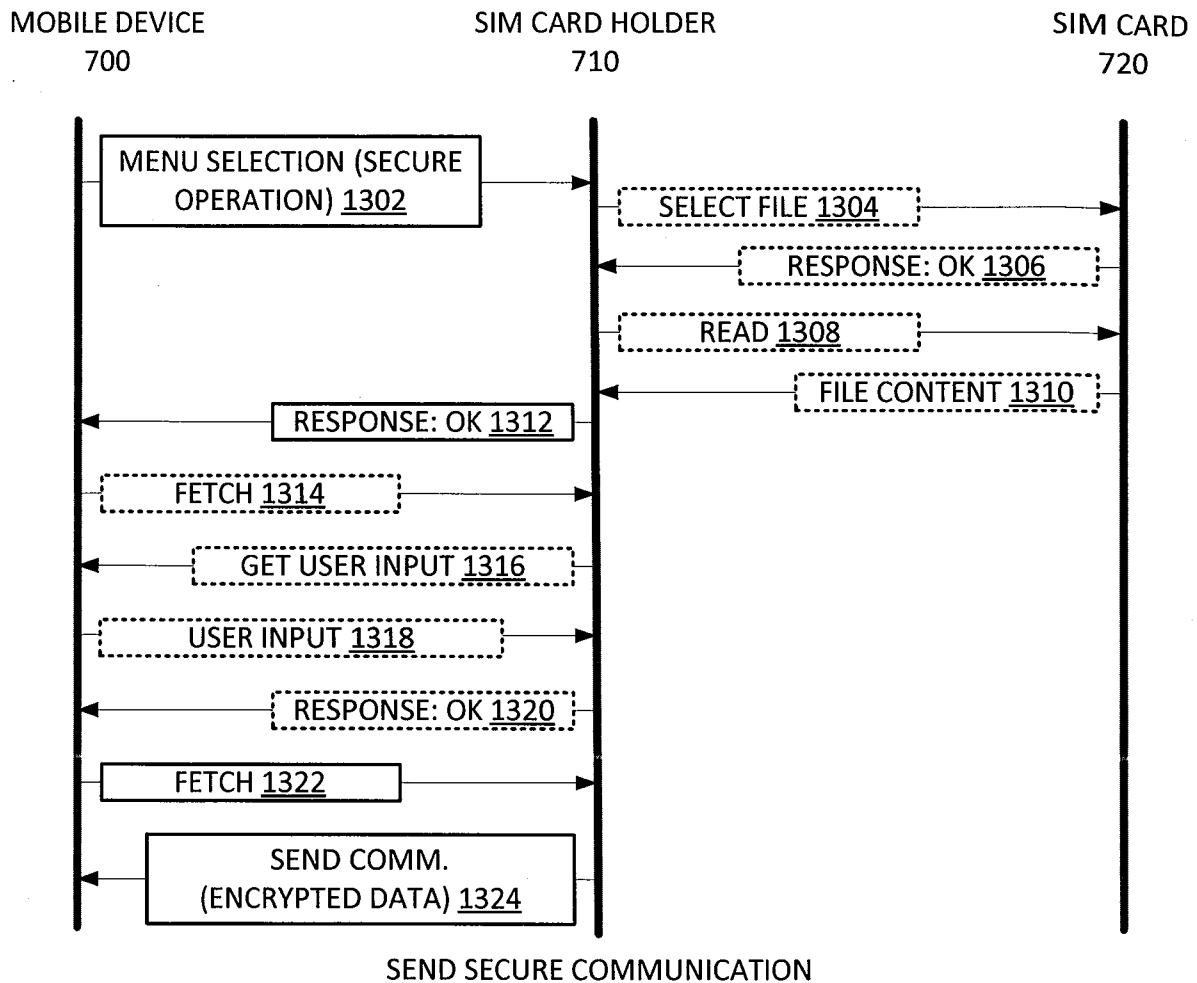


FIG. 19

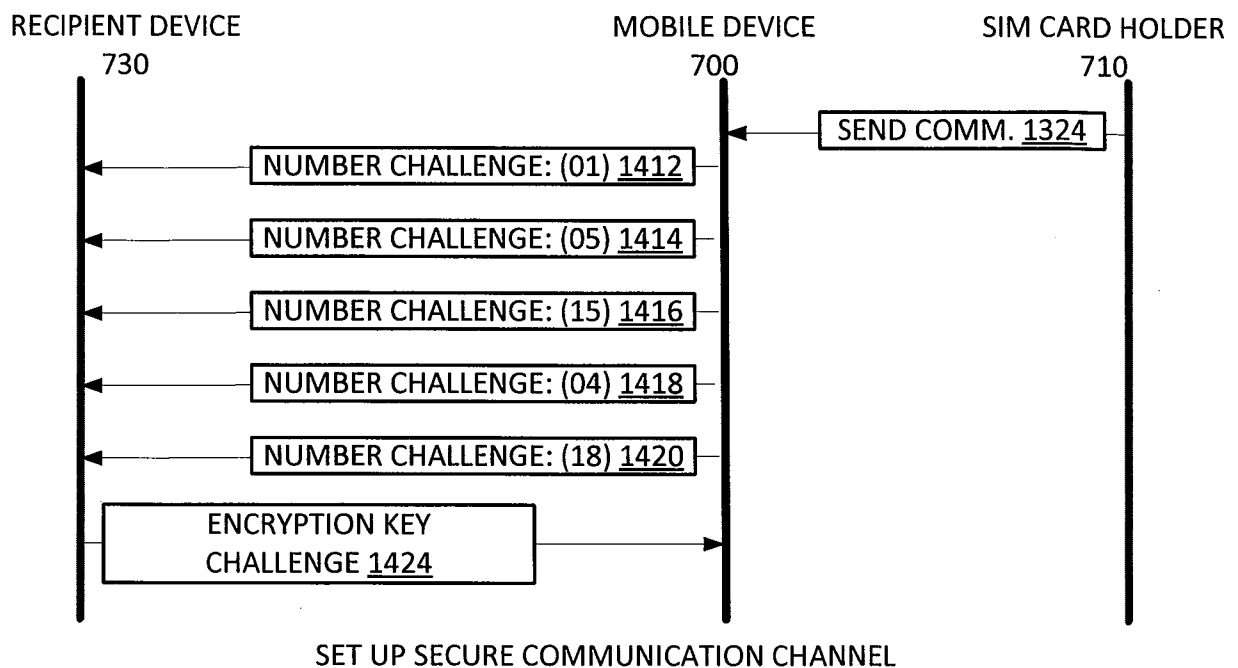


FIG. 20

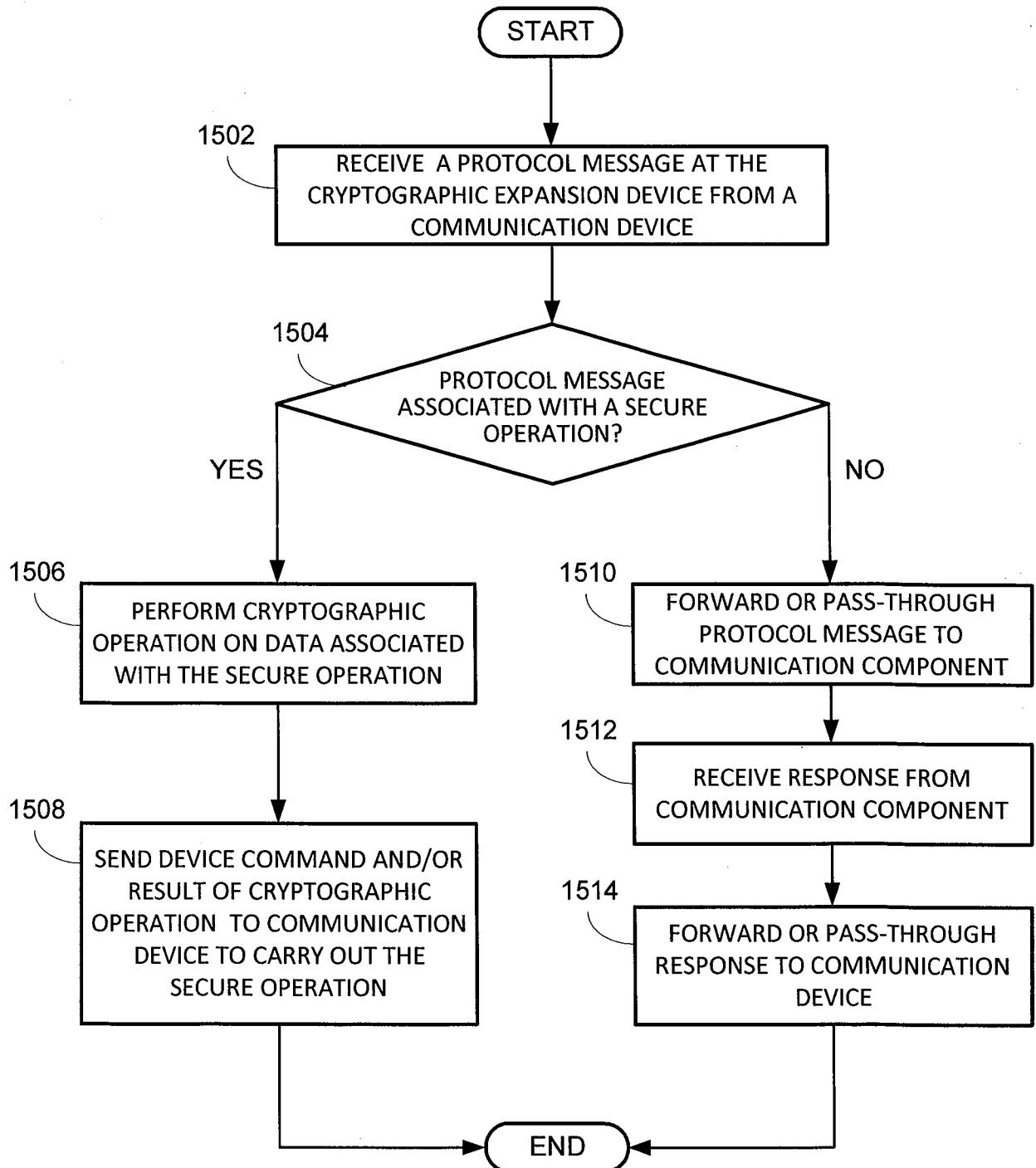


FIG. 21

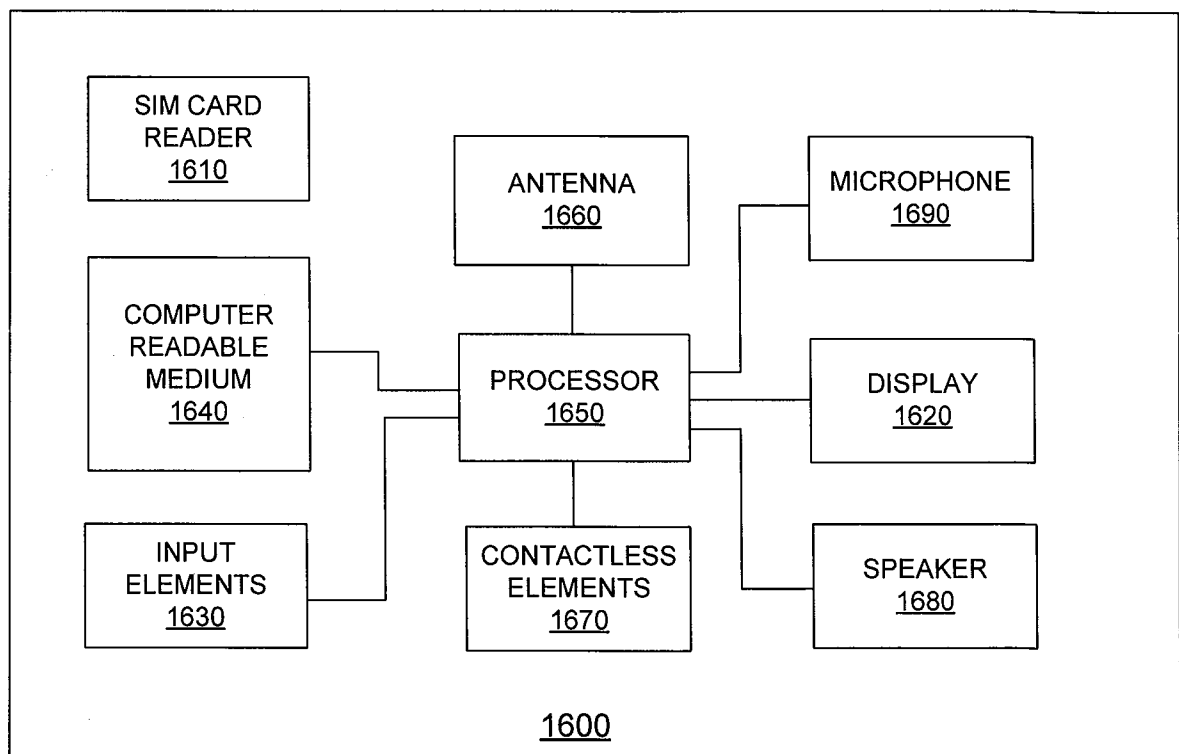


FIG. 22