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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2010 (01.04.2010)

PCT

(10) International Publication Number
WO 2010/035070 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04W 12/06* (2009.01)

(21) International Application Number:
PCT/IB2008/053962

(22) International Filing Date:
29 September 2008 (29.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA CORPORATION** [FI/FI]; Keilalahdentie 4, FIN-02150 Espoo (FI).

(71) Applicant *(for LC only)*: **NOKIA INC.** [US/US]; 6021 Connection Drive, Irving, Texas 75039 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **LINDHOLM, Rune, Adolf** [FI/FI]; Sottunga By, FIN-22720 Sottunga (FI).

(74) Agents: **LEYES, Charles, Andrew** et al.; Bank of America Plaza, 101 South Tryon Street, Suite 4000, Charlotte, North Carolina 28280-4000 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— *of inventorship (Rule 4.17(iv))*

[Continued on next page]

(54) Title: METHODS, APPARATUSES, AND COMPUTER PROGRAM PRODUCTS FOR LOCKING A REMOVEABLE DEVICE TO A SPECIFIC HOST DEVICE

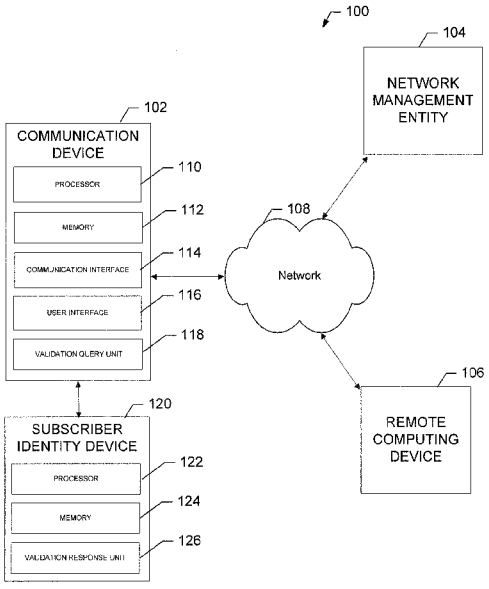

FIG. 1.

(57) Abstract: A method, apparatus, and computer program product are provided, which may lock a removable device to a specific host device. An apparatus may include a processor configured to establish a plurality of challenge-response pairings with a locked subscriber identity device. The processor may also be configured to select an unused challenge-response pairing from the plurality of challenge-response pairings. The processor may further be configured to mark the selected challenge-response pairing as used. The processor may additionally be configured to send the challenge from the selected challenge-response pairing to a connected subscriber identity device and receive a response from the connected subscriber identity device. The processor may also be configured to determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing. Corresponding methods and computer program products are also provided.

WO 2010/035070 A1

Published:

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

METHODS, APPARATUSES, AND COMPUTER PROGRAM PRODUCTS FOR LOCKING A REMOVEABLE DEVICE TO A SPECIFIC HOST DEVICE

TECHNOLOGICAL FIELD

Embodiments of the present invention relate generally to mobile communication technology and, more particularly, relate to methods, apparatuses, and computer program products for locking a removable device to a specific host device.

BACKGROUND

The modern communications era has brought about a tremendous expansion of wireline and wireless networks. Computer networks, television networks, and telephony networks are experiencing an unprecedented technological expansion, fueled by consumer demand. Wireless and mobile networking technologies have addressed related consumer demands, while providing more flexibility and immediacy of information transfer.

Current and future networking technologies as well as evolved computing devices making use of networking technologies continue to facilitate ease of information transfer and convenience to users. One area in which there is a demand to further improve the convenience to users is locking a removable device to a specific host device.

In this regard, a removable subscriber identity device that uniquely identifies a subscriber to a network operator and/or that allows for a communication device to access the operator's network may be inserted into a communication device, such as, for example, a cellular telephone. This removable subscriber identity device may, for example, be embodied as a subscriber identity module (SIM) card, a universal integrated circuit card (UICC), and/or the like.

Accordingly, communication devices may be adapted for use by different subscribers or even on different operator networks simply by swapping such a removable subscriber identity device.

However, network operators often desire to prevent device users from swapping subscriber identity devices due to the common practice of subsidizing sales of communication devices to consumers. In this regard, network operators often sell communication devices to consumers at a price below the actual cost of the communication device to the network operator in exchange for the consumer signing a service contract with the network operator. Accordingly, network operators may desire to lock the communication device to the operator, such as by locking a removable subscriber identity device to the communication device, such that the consumer is tied to using the communication device on the operator's network so that the network operator receives a return on its investment in selling the subsidized communication device.

Accordingly, it may be advantageous to provide methods, apparatuses, and computer program products for locking a removable device to a specific host device with which the removable device is intended to operate.

BRIEF SUMMARY OF SOME EXAMPLES OF THE INVENTION

A method, apparatus, and computer program product are therefore provided, which may lock a removable device to a specific host device. In particular, a method, apparatus, and computer program product may be provided to enable, for example, the locking of a subscriber identity device, such as, for example, a universal integrated circuit card, to a communication device, such as, for example, to a mobile terminal. Embodiments of the invention may provide for locking a removable device such that non-static information may be used for lock validation purposes so as to inhibit man-in-the-middle attacks attempting to gather information needed to clone the removable device so that an imposter removable device may be used.

In one exemplary embodiment, a method is provided which may include establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the subscriber

identity device. Each challenge-response pairing may comprise a challenge and a corresponding response. The method may further include selecting an unused challenge-response pairing from the plurality of challenge-response pairings. The method may also include marking the selected challenge-response pairing as used. The method may further include sending the challenge from the selected challenge-response pairing to a connected subscriber identity device. The method may additionally include receiving a response from the connected subscriber identity device. The method may also include determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

In another exemplary embodiment, a computer program product is provided. The computer program product includes at least one computer-readable storage medium having computer-readable program instructions stored therein. The computer-readable program instructions may include first, second, third, fourth, fifth, and sixth program instructions. The first program instruction is establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device. Each challenge-response pairing may comprise a challenge and a corresponding response. The second program instruction is for selecting an unused challenge-response pairing from the plurality of challenge-response pairings. The third program instruction is for marking the selected challenge-response pairing as used. The fourth program instruction is for sending the challenge from the selected challenge-response pairing to a connected subscriber identity device. The fifth program instruction is for receiving a response from the connected subscriber identity device. The sixth program instruction is for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

In another exemplary embodiment, an apparatus is provided, which may include a processor configured to establish a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device. Each challenge-response

pairing may comprise a challenge and a corresponding response. The processor may also be configured to select an unused challenge-response pairing from the plurality of challenge-response pairings. The processor may further be configured to mark the selected challenge-response pairing as used. The processor may additionally be configured to send the challenge from the selected challenge-response pairing to a connected subscriber identity device. The processor may also be configured to receive a response from the connected subscriber identity device. The processor may further be configured to determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

In another exemplary embodiment, an apparatus is provided that may include means for establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device. Each challenge-response pairing may comprise a challenge and a corresponding response. The apparatus may further include means for selecting an unused challenge-response pairing from the plurality of challenge-response pairings. The apparatus may also include means for marking the selected challenge-response pairing as used. The apparatus may further include means for sending the challenge from the selected challenge-response pairing to a connected subscriber identity device. The apparatus may additionally include means for receiving a response from the connected subscriber identity device. The apparatus may also include means for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

In still another exemplary embodiment, a method is provided which may include instructing a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device to generate a public key pair. The public key pair may be comprised of a private key and a corresponding public key and the private key may be stored in the locked subscriber identity device. The method may further include receiving the public key from the locked subscriber identity device. The method may also include sending a validation

request to a connected subscriber identity device. The method may additionally include receiving a certificate in response to the validation request from the connected subscriber identity device. The method may further include determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a validation of the received certificate using the public key. Computer program products and apparatuses corresponding to this embodiment are also provided.

The above summary is provided merely for purposes of summarizing some example embodiments of the invention so as to provide a basic understanding of some aspects of the invention. Accordingly, it will be appreciated that the above described example embodiments are merely examples and should not be construed to narrow the scope or spirit of the invention in any way. It will be appreciated that the scope of the invention encompasses many potential embodiments, some of which will be further described below, in addition to those here summarized.

BRIEF DESCRIPTION OF THE DRAWING(S)

Having thus described embodiments of the invention in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

FIG. 1 illustrates a block diagram of a system for locking a removable device to a specific host device according to an exemplary embodiment of the present invention;

FIG. 2 is a schematic block diagram of a mobile terminal according to an exemplary embodiment of the present invention; and

FIGs. 3-4 are flowcharts according to exemplary methods for locking a removable device to a specific host device according to exemplary embodiments of the present invention.

DETAILED DESCRIPTION

Some embodiments of the present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. Indeed, the invention may be embodied in many different forms and should not be construed as limited to the

embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like reference numerals refer to like elements throughout.

FIG. 1 illustrates a block diagram of a system 100 for locking a removable device to a specific host device according to an exemplary embodiment of the present invention. As used herein, "exemplary" merely means an example and as such represents one example embodiment for the invention and should not be construed to narrow the scope or spirit of the invention in any way. It will be appreciated that the scope of the invention encompasses many potential embodiments in addition to those illustrated and described herein. As such, while FIG. 1 illustrates one example of a configuration of a system for locking a removable device to a specific host device, numerous other configurations may also be used to implement embodiments of the present invention.

As used herein, "locking a removable device to a specific host device" refers to measures taken to ensure that functionality of the specific host device is limited unless the specific host device is operationally coupled to the removable device to which it is locked. In this regard, unauthorized use of the specific host device may be prevented. Accordingly, a "locked" device refers to a device which is locked to a specific host device. For example, a subscriber identity device, such as a uniform integrated circuit card (UICC), may be locked to a specific mobile communication device, such as, for example, a cellular communication device.

A "subscriber identity device" as used herein refers to a removable device and/or an application embodied on the removable device that uniquely identifies a subscriber to a network operator and/or that allows for a communication device to access an operator's network. In this regard, a subscriber identity device may be connected, such as, for example by inserting the subscriber identity device into a receptor slot, to a specific host device, such as a communication device (e.g., a mobile terminal). Although the above example describes a physical connection between a subscriber identity device and another device, it will be appreciated that in some embodiments, a subscriber identity device may be connected to another device through non-physical means, and may accordingly be connected to a specific host device through a wireless connection. The subscriber identity device

may, for example, be embodied as a subscriber identity module (SIM) card, a universal integrated circuit card (UICC), and/or the like.

Embodiments of the present invention may provide for locking a subscriber identity device or other removable device to a specific host device, such as a communication device, so as to inhibit a man-in-the-middle attack. A man-in-the-middle attack describes a situation in which a hacker may analyze communication between a communication device and a connected subscriber identity device to determine what kind of locking mechanism is used and what information is exchanged as the locking information. If a hacker determines this information, then the hacker may substitute an imposter subscriber identity device for the locked subscriber identity device simply by intercepting lock validation communications and sending back valid responses. Embodiments of the invention may prevent such attacks by using locking information that is non-static such that each response received from a connected subscriber identity device in response to a lock validation challenge may be different or at least the repetition period is long enough that it is not practical for a hacker to collect all possible combinations of challenges and responses.

Referring now to FIG. 1, the system 100 may include a communication device 102, network management entity 104, and remote computing device 106 configured to communicate over a network 108. The network management entity 104 may be embodied as any computing device or plurality of computing devices configured to provide and/or manage access to the network 108 by computing devices, such as a communication device 102. In embodiments wherein the network 108 comprises a cellular communications network, the network management entity 104 may, for example, be embodied as an access point or base station. The remote computing device 106 may be any computing device, mobile or fixed, configured to communicate with other computing devices, such as a communication device 102 or network management entity 104, over the network 108. The communication device 102 may be embodied as any computing device configured to communicate with an operationally coupled subscriber identity device 120. In an exemplary embodiment, the communication device 102 may further be configured to communicate with a network management entity 104 and/or a remote computing device 106 over the network 108. In some

embodiments, the communication device 102 and/or remote computing device 106 may be embodied as a mobile computing device, such as, for example a mobile terminal 10 depicted in FIG. 2.

In this regard, FIG. 2 illustrates a block diagram of a mobile terminal 10 representative of one embodiment of a communication device 102 and/or a remote computing device 106 in accordance with embodiments of the present invention. It should be understood, however, that the mobile terminal illustrated and hereinafter described is merely illustrative of one type of communication device 102 and/or remote computing device 106 that may benefit from embodiments of the present invention and, therefore, should not be taken to limit the scope of the present invention. While several embodiments of the electronic device are illustrated and will be hereinafter described for purposes of example, other types of electronic devices, such as mobile telephones, mobile computers, portable digital assistants (PDAs), pagers, laptop computers, desktop computers, gaming devices, televisions, and other types of electronic systems, may employ embodiments of the present invention.

As shown, the mobile terminal 10 may include an antenna 12 (or multiple antennas 12) in communication with a transmitter 14 and a receiver 16. The mobile terminal may also include a controller 20 or other processor(s) that provides signals to and receives signals from the transmitter and receiver, respectively. These signals may include signaling information in accordance with an air interface standard of an applicable cellular system, and/or any number of different wireless networking techniques, comprising but not limited to Wireless-Fidelity (Wi-Fi), wireless local access network (WLAN) techniques such as Institute of Electrical and Electronics Engineers (IEEE) 802.11, and/or the like. In addition, these signals may include speech data, user generated data, user requested data, and/or the like. In this regard, the mobile terminal may be capable of operating with one or more air interface standards, communication protocols, modulation types, access types, and/or the like. More particularly, the mobile terminal may be capable of operating in accordance with various first generation (1G), second generation (2G), 2.5G, third-generation (3G) communication protocols, fourth-generation (4G) communication protocols, and/or the like. For example, the mobile terminal may be capable of operating in accordance with 2G

wireless communication protocols IS-136 (Time Division Multiple Access (TDMA)), Global System for Mobile communications (GSM), IS-95 (Code Division Multiple Access (CDMA)), and/or the like. Also, for example, the mobile terminal may be capable of operating in accordance with 2.5G wireless communication protocols General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and/or the like. Further, for example, the mobile terminal may be capable of operating in accordance with 3G wireless communication protocols such as Universal Mobile Telecommunications System (UMTS), Code Division Multiple Access 2000 (CDMA2000), Wideband Code Division Multiple Access (WCDMA), Time Division-Synchronous Code Division Multiple Access (TD-SCDMA), and/or the like. The mobile terminal may be additionally capable of operating in accordance with 3.9G wireless communication protocols such as Long Term Evolution (LTE) or Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and/or the like. Additionally, for example, the mobile terminal may be capable of operating in accordance with fourth-generation (4G) wireless communication protocols and/or the like as well as similar wireless communication protocols that may be developed in the future.

Some Narrow-band Advanced Mobile Phone System (NAMPS), as well as Total Access Communication System (TACS), mobile terminals may also benefit from embodiments of this invention, as should dual or higher mode phones (e.g., digital/analog or TDMA/CDMA/analog phones). Additionally, the mobile terminal 10 may be capable of operating according to Wireless Fidelity (Wi-Fi) protocols.

It is understood that the controller 20 may comprise circuitry for implementing audio/video and logic functions of the mobile terminal 10. For example, the controller 20 may comprise a digital signal processor device, a microprocessor device, an analog-to-digital converter, a digital-to-analog converter, and/or the like. Control and signal processing functions of the mobile terminal may be allocated between these devices according to their respective capabilities. The controller may additionally comprise an internal voice coder (VC) 20a, an internal data modem (DM) 20b, and/or the like. Further, the controller may comprise functionality to operate one or more software programs, which may be stored in memory. For example, the controller 20 may be capable of

operating a connectivity program, such as a web browser. The connectivity program may allow the mobile terminal 10 to transmit and receive web content, such as location-based content, according to a protocol, such as Wireless Application Protocol (WAP), hypertext transfer protocol (HTTP), and/or the like. The mobile terminal 10 may be capable of using a Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit and receive web content across the internet or other networks.

The mobile terminal 10 may also comprise a user interface including, for example, an earphone or speaker 24, a ringer 22, a microphone 26, a display 28, a user input interface, and/or the like, which may be operationally coupled to the controller 20. As used herein, "operationally coupled" may include any number or combination of intervening elements (including no intervening elements) such that operationally coupled connections may be direct or indirect and in some instances may merely encompass a functional relationship between components. Although not shown, the mobile terminal may comprise a battery for powering various circuits related to the mobile terminal, for example, a circuit to provide mechanical vibration as a detectable output. The user input interface may comprise devices allowing the mobile terminal to receive data, such as a keypad 30, a touch display (not shown), a joystick (not shown), and/or other input device. In embodiments including a keypad, the keypad may comprise numeric (0-9) and related keys (#, *), and/or other keys for operating the mobile terminal.

As shown in Figure 2, the mobile terminal 10 may also include one or more means for sharing and/or obtaining data. For example, the mobile terminal may comprise a short-range radio frequency (RF) transceiver and/or interrogator 64 so data may be shared with and/or obtained from electronic devices in accordance with RF techniques. The mobile terminal may comprise other short-range transceivers, such as, for example, an infrared (IR) transceiver 66, a Bluetooth™ (BT) transceiver 68 operating using Bluetooth™ brand wireless technology developed by the Bluetooth™ Special Interest Group, a wireless universal serial bus (USB) transceiver 70 and/or the like. The Bluetooth transceiver 68 may be capable of operating according to ultra-low power Bluetooth technology (e.g., Wibree™) radio standards. In this regard, the mobile terminal 10 and, in particular, the short-range transceiver may be capable of transmitting data to and/or

receiving data from electronic devices within a proximity of the mobile terminal, such as within 10 meters, for example. Although not shown, the mobile terminal may be capable of transmitting and/or receiving data from electronic devices according to various wireless networking techniques, including Wireless Fidelity (Wi-Fi), WLAN techniques such as IEEE 802.11 techniques, and/or the like.

The mobile terminal 10 may comprise memory, such as a subscriber identity module (SIM) 38, a removable user identity module (R-UIM), a universal subscriber identity module (USIM), internet protocol multimedia services identity module (ISIM), and/or the like, which may store information elements related to and/or for validating a mobile subscriber to a network operator and/or to the mobile terminal 10 and may be embodied on a removable subscriber identity device, such as, for example, a universal integrated circuit card (UICC). In addition to the SIM, the mobile terminal may comprise other removable and/or fixed memory. The mobile terminal 10 may include volatile memory 40 and/or non-volatile memory 42. For example, volatile memory 40 may include Random Access Memory (RAM) including dynamic and/or static RAM, on-chip or off-chip cache memory, and/or the like. Non-volatile memory 42, which may be embedded and/or removable, may include, for example, read-only memory, flash memory, magnetic storage devices (e.g., hard disks, floppy disk drives, magnetic tape, etc.), optical disc drives and/or media, non-volatile random access memory (NVRAM), and/or the like. Like volatile memory 40 non-volatile memory 42 may include a cache area for temporary storage of data. The memories may store one or more software programs, instructions, pieces of information, data, and/or the like which may be used by the mobile terminal for performing functions of the mobile terminal. For example, the memories may comprise an identifier, such as an international mobile equipment identification (IMEI) code, capable of uniquely identifying the mobile terminal 10.

Returning to FIG. 1, it will be appreciated that the communication device 102 and remote computing device 106 are not limited to being embodied as a mobile terminal 10 and may be embodied as any computing device, mobile or fixed, and accordingly may be embodied as a server, desktop computer, laptop computer, mobile terminal 10, and/or the like. The network 108 may comprise one or more wireless networks, wireline networks, cellular networks, or combination

thereof and may comprise the internet. It will be appreciated that while FIG. 1 illustrates only a single network management entity 104 and remote computing device 106, the system 100 may comprise multiple network management entities 104 and/or multiple remote computing devices 106. Further, while FIG. 1 illustrates an exemplary embodiment of a system for locking a removable device to a specific host device, other embodiments are possible. For example, in another embodiment, the communication device 102 may not be configured to communicate with remote computing devices over a network 108. In such an embodiment, a subscriber identity device 120 may be locked to the communication device 102 so as to control access to subscriber services other than network communication services.

The communication device 102 may include various means, such as a processor 110, memory 112, communication interface 114, user interface 116, and validation query unit 118 for performing the various functions herein described. These means of the communication device 102 as described herein may be embodied as, for example, hardware elements (e.g., a suitably programmed processor, combinational logic circuit, and/or the like), computer code (e.g., software or firmware) embodied on a computer-readable medium (e.g. memory 112) that is executable by a suitably configured processing device (*e.g.,* the processor 110), or some combination thereof. The processor 110 may, for example, be embodied as various means including a microprocessor, a coprocessor, a controller, or various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit) or FPGA (field programmable gate array). In an exemplary embodiment, the processor 110 may be configured to execute instructions stored in the memory 112 or otherwise accessible to the processor 110. Although illustrated in FIG. 1 as a single processor, the processor 110 may comprise a plurality of general purpose and/or special purpose processors configured to operate cooperatively to provide the functionalities described herein.

The memory 112 may include, for example, volatile and/or non-volatile memory. The memory 112 may be configured to store information, data, applications, instructions, or the like for enabling communication device 102 to carry out various functions in accordance with exemplary embodiments of the

present invention. For example, the memory 112 may be configured to buffer input data for processing by the processor 110. Additionally or alternatively, the memory 112 may be configured to store instructions for execution by the processor 110. The memory 112 may comprise one or more databases that store information in the form of static and/or dynamic information. In this regard, the memory 112 may store, for example, challenge-response pairings. This stored information may be stored and/or used by the validation query unit 118 during the course of performing its functionalities.

The communication interface 114 may be embodied as any device or means embodied in hardware, software, firmware, or a combination thereof that is configured to receive and/or transmit data from/to a network, such as the network 108, and/or any other device, such as a network management entity 104 and/or remote computing device 106, in communication with the communication device 102. Additionally or alternatively, the communication interface 114 may be configured to receive and/or transmit data from/to a subscriber identity device 120 connected to the communication device 102. In one embodiment, the communication interface 114 may be at least partially embodied as or otherwise controlled by the processor 110. The communication interface 114 may include, for example, an antenna, a transmitter, a receiver, a transceiver and/or supporting hardware or software for enabling communications with other entities of the system 100, such as a network management 104 and/or remote computing device 106 via the network 108. The communication interface 114 may be configured to receive and/or transmit data using any protocol that may be used for communications between the communication device 102 and other computing devices of the system 100, such as a network management entity 104 and/or a remote computing device 106, over the network 108. The communication interface 114 may additionally be in communication with the memory 112, user interface 116, and/or validation query unit 118, such as via a bus.

The user interface 116 may be in communication with the processor 110 to receive an indication of a user input and/or to provide an audible, visual, mechanical, or other output to the user. As such, the user interface 116 may include, for example, a keyboard, a mouse, a joystick, a display, a touch screen display, a microphone, a speaker, and/or other input/output mechanisms.

However, in some embodiments of a communication device 102, elements of the user interface may be reduced or even eliminated. The user interface 116 may further be in communication with the memory 112, communication interface 116, and/or validation query unit 118, such as via a bus.

The validation query unit 118 may be embodied as various means, such as hardware, software, firmware, or some combination thereof and, in one embodiment, may be embodied as or otherwise controlled by the processor 110. In embodiments where the validation query unit 118 is embodied separately from the processor 110, the validation query unit 118 may be in communication with the processor 110. The validation query unit 118 may be configured to initiate locking of a subscriber identity device 120 to the communication device 102. The validation query unit 118 may additionally be configured to validate a connected subscriber identity device 120 as being a subscriber identity device 120 locked to the communication device 102.

In an exemplary embodiment, the validation query unit 118 may be configured to establish a plurality of challenge-response pairings with a locked subscriber identity device 120. This plurality of challenge-response pairings may comprise or otherwise be referred to as one or more lists of challenge-response pairings. However, it will be appreciated that the term list has no bearing on how the challenge-response pairings are stored or otherwise organized in memory, but rather is used herein as a way to refer to a group of challenge-response pairings. The validation query unit 118 may be configured to establish the plurality of challenge-response pairings in a secure environment during initiation of locking a subscriber identity device 120 to the communication device 102. A secure environment may be an environment in which it is known that there is no man-in-the-middle that can intercept communications passed between the communication device 102 and the locked subscriber identity device 120. Such a secure environment may be found, for example, at a site of a manufacturer or vendor of communication devices 102 where subscriber identity devices 120 may be connected to the communication devices 102. Each challenge-response pairing may comprise a challenge and a corresponding response calculated by the locked subscriber identity device 120 in response to the challenge. In this regard, a challenge may comprise any random value. For example, the challenge may

comprise a 16 byte value. The response may comprise a value calculated by the locked subscriber identity device 120 according to an authentication algorithm embodied on the locked subscriber identity device 120 based at least in part upon the challenge value. In this regard, there may be only one correct response value for any given challenge value. The validation query unit 118 may be configured to establish a list comprising a predefined number of challenge-response pairings (e.g., 20) or may be configured to establish challenge-response pairings for a duration of time, such as, for example, a predefined period of time or the duration of the initiation of locking the subscriber identity device 120 to the communication device 102.

The validation query unit 118 may establish the plurality of challenge-response pairings by generating a plurality of challenge values and sending each challenge value to the locked subscriber identity device 120. The validation query unit 118 may generate the challenge values randomly or may generate the challenge values in some predefined order, such as sequentially. The challenge value may be sent to the locked subscriber identity device 120 as a parameter of an authenticate command recognized by the subscriber identity device 120. This authenticate command may, for example, be used by a network operator and/or a network management entity 104 to validate a communication device 102 and/or a subscriber identity device 120 connected to the communication device 102 prior to providing the communication device 102 with a network communication service. The validation query unit 118 may then receive a response to the sent challenge from the locked subscriber identity device 120 and pair the received response with the sent challenge to comprise a challenge-response pairing. Since the locked subscriber identity device 120 may calculate the response according to an algorithm embodied on the locked subscriber identity device 120 such that there is only one correct response value for any given challenge, the validation query unit 118 may establish a plurality of challenge-response pairings that may be used to validate a connected subscriber identity device 120 as being the locked subscriber identity device 120 without any knowledge of the algorithm used by the locked subscriber identity device 120 to calculate a response to a received challenge. The validation query unit 120 may then store each challenge-response pairing in a memory, such as the memory 112.

Once initiation of the lock has completed and the plurality of challenge-response pairings has been established, the validation query unit 120 may be configured to validate a subscriber identity device 120 connected to the communication device 102 as being the subscriber identity device 120 which was locked to the communication device 102. In this regard, the validation query unit 118 may be configured to validate a connected subscriber identity device 120 each time the communication device 102 is powered on, when a user of the communication device 102 attempts to use a functionality of the communication device 102, and/or periodically. If the validation query unit 118 successfully validates a connected subscriber identity device 120 as being the subscriber identity device 120 that was locked to the communication device 102, then the validation query unit 118 may continue to allow full functionality and access to the communication device 102. If, however, the validation query unit 118 determines that the connected subscriber identity device 120 is not the subscriber identity device 120 that was locked to the communication device 102, the validation query unit 118 may reject the connected subscriber identity device 120 such that functionality of and/or access to the communication device 102 is limited.

In order to validate a connected subscriber identity device 120, the validation query unit 118 may be configured to select an unused challenge-response pairing from the plurality of challenge-response pairings and use the selected challenge-response pairing to validate the connected subscriber identity device 120. In this regard, each challenge-response pairing may be stored, such as in memory 112, in association with an indication of whether the challenge-response pairing has previously been used to validate a connected subscriber identity device 120. Once the validation query unit 118 has selected an unused challenge-response pairing, the validation query unit 118 may be configured to mark the selected challenge-response pairing as "used." Marking the selected challenge-response pairing as used may comprise changing the indication stored in association with the challenge-response pairing to reflect that the pairing has been used. Additionally or alternatively, marking the selected challenge-response pairing as used may comprise deleting the selected challenge-response pairing from memory such that the selected challenge-response pairing is no longer stored in the plurality of challenge-response pairings. In this regard, the challenge-

response pairing is implicitly marked as used since the pairing is no longer stored with the plurality of challenge-response pairings available for validating a connected subscriber identity device 120. Accordingly, each of the plurality of stored challenge-response pairings may be used for validation purposes only once, or if reused, the repetition period may be long enough that it is not practical for a man-in-the-middle to collect all possible combinations. In this regard, a challenge-response pairing may be reused in some circumstances, such as, for example, once all possible challenge values have been exhausted, when the unused challenge-response pairings have been exhausted, and/or in embodiments wherein used challenge-response pairings are deleted, when a challenge-response pairing comprising the particular challenge value is again established and/or collected by the validation query unit 118. However, ideally, such reuse will not occur for a period such that the repetition period is long enough that it is not practical for a man-in-the-middle to collect all combinations. Accordingly, a man-in-the-middle intercepting communications between the communication device 102 and the subscriber identity device 120 may not be able to clone a locked subscriber identity device 120 simply by sending an intercepted response in response to a received challenge.

The validation query unit 118 may be configured to send the challenge from the selected challenge-response pairing, such as in an authenticate command, to the connected subscriber identity device 120. The validation query unit 118 may further be configured to receive a response from the connected subscriber identity device in response to the sent challenge and determine whether the connected subscriber identity device 120 is the locked subscriber identity device 120 based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing. In this regard, if the received response and the response in the selected challenge-response pairing are the same, the validation query unit 118 may determine that the connected subscriber identity device 120 and the locked subscriber identity device 120 are the same. If, however, the received response is different from the response in the selected challenge-response pairing, the validation query unit 118 may determine that the connected subscriber identity device 120 is an imposter.

As it will be appreciated that the plurality of challenge-response pairings may be exhausted, the validation query unit 118 may, in an exemplary embodiment, be configured to validate a connected subscriber identity device 120 using a challenge-response pairing only after first exhausting other means of validating the connected subscriber identity device 120. In this regard, the validation query unit 118 may be configured to first validate that other locking information of a connected subscriber identity device 120 match the subscriber identity device 120 locked to the communication device 102. This other locking information may comprise static information identifying a subscriber identity device 120, such as, for example, a UICC identification value, an international mobile subscriber identity (IMSI) value, and/or the like. Thus, the validation query unit 118 may be configured to validate a connected subscriber identity device 120 using a stored challenge-response pairing only if the other locking information of the connected subscriber identity device 120 matches the locked subscriber identity device 120. If the other locking information does not match, then the validation query unit 118 may determine the connected subscriber identity device 120 is an imposter without using a challenge-response pairing from the plurality of challenge-response pairings.

The validation query unit 118 may further be configured to collect additional challenge-response pairings following locking of a subscriber identity device 120 to the communication device 102. The validation query unit 118 may be configured to collect additional pairings after a connected subscriber identity device 120 has been validated as being the locked subscriber identity device 120 so that the collected additional challenge-response pairings may be used to validate a connected subscriber identity device 120 in the future. The validation query unit 118 may be configured to collect additional challenge-response pairings by generating a challenge value, ensuring that the generated challenge value is not already represented in the plurality of challenge-response pairings, and sending the challenge to the locked subscriber identity device 120. As before, the validation query unit 120 may receive a response to the challenge from the subscriber identity device 120 and pair the received response to the sent challenge to comprise a challenge-response pairing. The validation query unit 118 may then save the

challenge-response pairing as part of the plurality of challenge-response pairings, such as in memory 112.

Additionally or alternatively, the validation query unit 118 may be configured to collect additional challenge-response pairings based at least in part upon the response of a connected subscriber identity device 120 to network authentication challenges received from a network management entity 104. In this regard, the validation query unit 118 may be configured to receive an authenticate command comprising a challenge value from a network management entity 104. The validation query unit 118 may then be configured to send the authenticate command to the connected subscriber identity device 120 and to receive a response to the authenticate command from the subscriber identity device 120. The validation query unit 118 may be configured to send the received response to the authenticate command to the network management entity 104 so that the network management entity 104 may validate the communication device 102 for access to the network 108 based at least in part upon the identity of the connected subscriber identity device 120. The validation query unit 118 may be configured to determine whether the challenge value received from the network management entity 104 is in the plurality of challenge-response pairings. If the received challenge value is not in the plurality of challenge-response pairings, the validation query unit 118 may be configured to pair the challenge received from the network management entity 104 with the response received from the connected subscriber identity device 120 to form a challenge-response pairing if the network management entity 104 validates the communication device 102. The validation query unit 118 may then save the challenge-response pairing as part of the plurality of challenge-response pairings, such as in memory 112. In some embodiments, however, the validation query unit 118 may be configured to form and/or save the challenge-response pairing only if the validation query unit 118 has independently validated the connected subscriber identity device 120 (e.g., before of the network authentication challenge or following receipt of the network authentication challenge and prior to saving the challenge-response pairing).

In an exemplary embodiment, the validation query unit 118 may be configured to collect additional challenge-response pairings if the number of unused challenge-response pairings in the plurality of challenge-response pairings

equals a first predefined number. The validation query unit 118 may be configured to continue to collect additional challenge-response pairings until the number of unused challenge-response pairings in the plurality of challenge-response pairings equals a second predefined number. For example, the first predefined number may be 15 and the second predefined number may be 20. Accordingly, when the number of unused challenge-response pairings falls to 15, the validation query unit 118 may be configured to collect additional challenge-response pairings through either or both of the above described methods until the number of unused challenge-response pairings equals 20. Even in such an embodiment, however, the validation query unit 118 may be configured to collect challenge-response pairings that may be established based at least in part upon the response of a connected subscriber identity device 120 to network authentication challenges received from a network management entity 104 regardless of the number of challenge-response pairings in the plurality of challenge-response pairings. In this regard, such pairings may be particularly trustworthy as they have been validated by the network and establishment thereof may require little computational overhead by either the validation query unit 118 or the subscriber identity device 120 since responding to the network authenticate command may be a requirement for access to the network 108 by the communication device 102.

In an exemplary embodiment, the validation query unit 118 may be configured to establish two lists of challenge-response pairings. The first list may comprise a list of more trusted challenge-response pairings that may be harder (e.g., a "hard list") for a man-in-the-middle to intercept and fake. In this regard, the first list may comprise challenge-response pairings established in a secure environment during initiation of locking a subscriber identity device 120 to the communication device 102 as these pairings should be unknown to any man-in-the-middle since they were established in a secure environment. The first list may additionally comprise challenge-response pairing collected by the validation query unit 118 through validated network authentication commands, such as described above. The second list may comprise a list of less trusted challenge-response pairings that may be somewhat easier for a man-in-the-middle to intercept and fake (e.g., a "soft list"). In this regard, the challenge-response pairings comprising the second list may be collected subsequent to locking a subscriber identity device 120

to the communication device 102. Accordingly, these pairings may comprise challenges and responses that may have been intercepted or perhaps faked by a man-in-the-middle. So as to avoid unnecessarily using a pairing from the hard list of challenge-response pairings, the validation query unit 118 may be configured to first validate a connected subscriber identity device 120 as being the locked subscriber identity device 120 using a challenge from the soft list. If there is a problem with the validation, (e.g., a predefined number of consecutive validation failures, a predefined number of validation failures over a span of time, and/or the like) the validation query unit 118 may then use a challenge from the hard list. Other criteria may also trigger the validation query unit 118 to validate a connected subscriber identity device 120 as being the locked subscriber identity device 120 when there is reason to be more cautious in validating a connected subscriber identity device 120, such as when there is cause to be suspicious that a response value from the soft list may be faked. Examples of such criteria may comprise, for example, when a communication device 102 is first powered on, following an over-the-air update of firmware on the subscriber identity device 120 and/or the communication device 102, as well as other criteria that may be established based upon the operating parameters and/or functionalities provided by a particular embodiment of the communication device 102.

Referring now to the subscriber identity device 120, may include various means, such as a processor 122, memory 124, and validation response unit 126 for performing the various functions herein described. These means of the subscriber identity device 120 as described herein may be embodied as, for example, hardware elements (e.g., a suitably programmed processor, combinational logic circuit, and/or the like), computer code (e.g., software or firmware) embodied on a computer-readable medium (e.g. memory 124) that is executable by a suitably configured processing device (*e.g.*, the processor 122), or some combination thereof. The processor 122 may, for example, be embodied as various means including a microprocessor, a coprocessor, a controller, or various other processing elements including integrated circuits such as, for example, an ASIC (application specific integrated circuit) or FPGA (field programmable gate array). In an exemplary embodiment, the processor 122 may be configured to execute instructions stored in the memory 124 or otherwise accessible to the processor 122.

Although illustrated in FIG. 1 as a single processor, the processor 122 may comprise a plurality of general purpose and/or special purpose processors configured to operate cooperatively to provide the functionalities described herein.

The memory 124 may include, for example, volatile and/or non-volatile memory. The memory 124 may be configured to store information, data, applications, instructions, or the like for enabling the subscriber identity device 120 to carry out various functions in accordance with exemplary embodiments of the present invention. For example, the memory 124 may be configured to buffer input data for processing by the processor 122. Additionally or alternatively, the memory 124 may be configured to store instructions for execution by the processor 122. The memory 124 may comprise one or more databases that store information in the form of static and/or dynamic information. In this regard, the memory 122 may store, for example, received challenges. Additionally or alternatively, the memory 122 may store algorithms, values, and/or data otherwise necessary to facilitate calculation of a response to a received authenticate command or other challenge. This stored information may be stored and/or used by the validation response unit 126 during the course of performing its functionalities.

The validation response unit 126 may be embodied as various means, such as hardware, software, firmware, or some combination thereof and, in one embodiment, may be embodied as or otherwise controlled by the processor 122. In embodiments where the validation response unit 126 is embodied separately from the processor 122, the validation response unit 126 may be in communication with the processor 122. The validation response unit 126 may be configured to receive a challenge from a connected communication device 102. The challenge, may be received, for example, as a parameter to an authenticate command. The validation response unit 126 may be configured to calculate an appropriate response to the challenge and send the calculated response to the communication device 102. Accordingly, the validation response unit 126 may be embodied as or otherwise comprise logic for implementing an algorithm to calculate responses to received challenges so that the subscriber identity device 120 may be validated by a connected communication device 102 and/or a network management entity 104.

The above embodiments have described embodiments wherein a plurality of challenge-response pairings is maintained such that a connected subscriber

identity device 120 may be validated as a locked subscriber identity device 120 in a manner to inhibit man-in-the-middle attacks. Other embodiments may additionally or alternatively utilize a public key pair to validate a connected subscriber identity device 120 as the locked subscriber identity device 120. In such embodiments, the validation query unit 118 may be configured to instruct a locked subscriber identity device 120 during initiation of locking the subscriber identity device 120 to generate a public key pair comprised of a private key and a corresponding public key. As before, the initiation of locking the subscriber identity device 120 may take place in a secure environment. The validation response unit 126 may be configured to generate the public key pair and store the private key locally, such as in the memory 124. The validation response unit 126 may be configured to send the public key to the communication device 102, where it may be received and stored in memory 112 by the validation query unit 118.

The validation query unit 118 may be configured to send a validation request to a connected subscriber identity device 120. The format of the validation request is not important so long as the subscriber identity device 120 is configured to receive the validation request and understand that the request is for information that may be used to validate the subscriber identity device 120. Accordingly, the validation response unit 126 may be configured to receive the validation request and calculate a certificate based at least in part upon the private key. The validation response unit 126 may further be configured to send the calculated certificate to the communication device 102. The validation query unit 118 may be configured to receive the certificate and determine whether the connected subscriber identity device 120 is the locked subscriber identity device 120 based at least in part upon a validation of the received certificate using the public key. Calculation and validation of the certificate may be performed in accordance with any public key cryptography protocol, such as, for example, Diffie-Hellman.

FIGs. 3-4 are flowcharts of a system, method, and computer program product according to an exemplary embodiment of the invention. It will be understood that each block or step of the flowcharts, and combinations of blocks in the flowcharts, may be implemented by various means, such as hardware, firmware, and/or software including one or more computer program instructions. For example, one or more of the procedures described above may be embodied by

computer program instructions. In this regard, the computer program instructions which embody the procedures described above may be stored by a memory device of a mobile terminal, server, or other computing device and executed by a processor in the computing device. In some embodiments, the computer program instructions which embody the procedures described above may be stored by memory devices of a plurality of computing devices. As will be appreciated, any such computer program instructions may be loaded onto a computer or other programmable apparatus to produce a machine, such that the instructions which execute on the computer or other programmable apparatus create means for implementing the functions specified in the flowchart block(s) or step(s). These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function specified in the flowchart block(s) or step(s). The computer program instructions may also be loaded onto a computer or other programmable apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer-implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block(s) or step(s).

Accordingly, blocks or steps of the flowcharts support combinations of means for performing the specified functions, combinations of steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that one or more blocks or steps of the flowcharts, and combinations of blocks or steps in the flowcharts, may be implemented by special purpose hardware-based computer systems which perform the specified functions or steps, or combinations of special purpose hardware and computer instructions.

In this regard, one exemplary method for locking a removable device to a device according to an exemplary embodiment of the present invention is illustrated in FIG. 3. The method may include the validation query unit 118 establishing a plurality of challenge-response pairings with a locked subscriber

identity device 120 in a secure environment during initiation of locking the subscriber identity device, at operation 300. Operation 310 may comprise the validation query unit 118 selecting an unused challenge-response pairing from the plurality of challenge-response pairings. The validation query unit 118 may then mark the selected challenge-response pairing as used, at operation 320. Operation 330 may comprise the validation query unit 118 sending the challenge from the selected challenge-response pairing to a connected subscriber identity device 120. The validation query unit 118 may then receive a response from the connected subscriber identity device 120, at operation 340. Operation 350 may comprise the validation query unit 118 determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

FIG. 4 illustrates another exemplary method for locking a removable device to a device according to an exemplary embodiment of the present invention. The method may include the validation query unit 118 instructing a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device 120 to generate a public key pair, at operation 400. The public key pair may comprise a private key and a corresponding public key. Operation 410 may comprise the validation query unit 118 receiving the public key from the locked subscriber identity device 120. The validation query unit 118 may then send a validation request to a connected subscriber identity device 120, at operation 420. Operation 430 may comprise the validation query unit 118 receiving a certificate in response to the validation request from the connected subscriber identity device 120. Operation 440 may comprise the validation query unit 118 determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a validation of the received certificate using the public key.

The above described functions may be carried out in many ways. For example, any suitable means for carrying out each of the functions described above may be employed to carry out embodiments of the invention. In one embodiment, a suitably configured processor may provide all or a portion of the elements of the invention. In another embodiment, all or a portion of the elements of the invention

may be configured by and operate under control of a computer program product. The computer program product for performing the methods of embodiments of the invention includes a computer-readable storage medium, such as the non-volatile storage medium, and computer-readable program code portions, such as a series of computer instructions, embodied in the computer-readable storage medium.

As such, then, some embodiments of the invention may provide several advantages to users, manufacturers, and/or vendors of a computing device, such as a mobile terminal 10. Embodiments of the invention may provide for locking a removable device to a device so as to inhibit man-in-the-middle attacks that may be used to clone the removable device so that the locked removable device may be replaced with an imposter device. In this regard, embodiments of the invention may provide for locking a removable device with non-static information such that the appropriate response by the locked removable device to each challenge is different.

Many modifications and other embodiments of the inventions set forth herein will come to mind to one skilled in the art to which these inventions pertain having the benefit of the teachings presented in the foregoing descriptions and the associated drawings. Therefore, it is to be understood that the embodiments of the invention are not to be limited to the specific embodiments disclosed and that modifications and other embodiments are intended to be included within the scope of the appended claims. Moreover, although the foregoing descriptions and the associated drawings describe exemplary embodiments in the context of certain exemplary combinations of elements and/or functions, it should be appreciated that different combinations of elements and/or functions may be provided by alternative embodiments without departing from the scope of the appended claims. In this regard, for example, different combinations of elements and/or functions than those explicitly described above are also contemplated as may be set forth in some of the appended claims. Although specific terms are employed herein, they are used in a generic and descriptive sense only and not for purposes of limitation.

WHAT IS CLAIMED IS:

1. A method comprising:

establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device, wherein each challenge-response pairing comprises a challenge and a corresponding response;

selecting an unused challenge-response pairing from the plurality of challenge-response pairings;

marking the selected challenge-response pairing as used;

sending the challenge from the selected challenge-response pairing to a connected subscriber identity device;

receiving a response from the connected subscriber identity device; and

determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

2. A method according to Claim 1, further comprising:

collecting an additional challenge-response pairing; and

adding the additional challenge-response pairing to the plurality of challenge-response pairings.

3. A method according to Claim 2, wherein collecting an additional challenge-response pairing comprises:

sending a challenge not in the plurality of challenge-response pairings to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the sent challenge with the received response.

4. A method according to Claim 2, wherein collecting an additional challenge-response pairing comprises:

receiving an authentication command comprising a challenge not in the plurality of challenge-response pairings from a network management entity;

sending the authentication command to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the received challenge with the received response.

5. A method according to Claim 2, wherein collecting an additional challenge-response pairing comprises collecting an additional challenge-response pairing if a number of unused challenge-response pairings in the plurality of challenge-response pairings equals a first predefined number and continuing to collect additional challenge-response pairings until the number of unused challenge-response pairings in the plurality of challenge-response pairings equals a second predefined number.

6. A method according to Claim 1, further comprising storing the plurality of challenge-response pairings in a memory.

7. A method according to Claim 1, wherein the locked subscriber identity device comprises a universal integrated circuit card.

8. A method according to Claim 1, further comprising:

validating the connected subscriber identity device such that a communication device is usable if it is determined that the connected subscriber identity device is the locked subscriber identity device; and

rejecting the connected subscriber identity device such that functionality of a communication device is limited if it is determined that the connected subscriber identity device is not the locked subscriber identity device.

9. A method comprising:

instructing a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device to generate a public key pair, wherein the public key pair is comprised of a private key and a corresponding public key, and wherein the private key is stored in the locked subscriber identity device;

receiving the public key from the locked subscriber identity device;

sending a validation request to a connected subscriber identity device;

receiving a certificate in response to the validation request from the connected subscriber identity device; and

determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part on validation of the received certificate using the public key.

10. A computer program product comprising at least one computer-readable storage medium having computer-readable program instructions stored therein, the computer-readable program instructions comprising:

a first program instruction for establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device, wherein each challenge-response pairing comprises a challenge and a corresponding response;

a second program instruction for selecting an unused challenge-response pairing from the plurality of challenge-response pairings;

a third program instruction for marking the selected challenge-response pairing as used;

a fourth program instruction for sending the challenge from the selected challenge-response pairing to a connected subscriber identity device;

a fifth program instruction for receiving a response from the connected subscriber identity device; and

a sixth program instruction for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

11. A computer program product according to Claim 10, further comprising:

a seventh program instruction for collecting an additional challenge-response pairing; and

an eighth program instruction for adding the additional challenge-response pairing to the plurality of challenge-response pairings.

12. A computer program product according to Claim 11, wherein the seventh program instruction includes instructions for:

sending a challenge not in the plurality of challenge-response pairings to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the sent challenge with the received response.

13. A computer program product according to Claim 11, wherein the seventh program instruction includes instructions for:

receiving an authentication command comprising a challenge not in the plurality of challenge-response pairings from a network management entity;

sending the authentication command to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the received challenge with the received response.

14. A computer program product according to Claim 11, wherein the seventh program instruction includes instructions for collecting an additional challenge-response pairing if a number of unused challenge-response pairings in the plurality of challenge-response pairings equals a first predefined number and continuing to collect additional challenge-response pairings until the number of unused challenge-response pairings in the plurality of challenge-response pairings equals a second predefined number.

15. A computer program product according to Claim 10, further comprising a seventh program instruction for storing the plurality of challenge-response pairings in a memory.

16. A computer program product according to Claim 10, wherein the locked subscriber identity device comprises a universal integrated circuit card.

17. A computer program product according to Claim 10, further comprising:

a seventh program instruction for validating the connected subscriber identity device such that a communication device is usable if it is determined that the connected subscriber identity device is the locked subscriber identity device; and

an eighth program instruction for rejecting the connected subscriber identity device such that functionality of a communication device is limited if it is determined that the connected subscriber identity device is not the locked subscriber identity device.

18. A computer program product comprising at least one computer-readable storage medium having computer-readable program instructions stored therein, the computer-readable program instructions comprising:

a first program instruction for instructing a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device to generate a public key pair, wherein the public key pair is comprised of a private key and a corresponding public key, and wherein the private key is stored in the locked subscriber identity device;

a second program instruction for receiving the public key from the locked subscriber identity device;

a third program instruction for sending a validation request to a connected subscriber identity device;

a fourth program instruction for receiving a certificate in response to the validation request from the connected subscriber identity device; and

a fifth program instruction for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part on validation of the received certificate using the public key.

19. An apparatus comprising a processor configured to:

establish a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the locked

subscriber identity device, wherein each challenge-response pairing comprises a challenge and a corresponding response;

select an unused challenge-response pairing from the plurality of challenge-response pairings;

mark the selected challenge-response pairing as used;

send the challenge from the selected challenge-response pairing to a connected subscriber identity device;

receive a response from the connected subscriber identity device; and

determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

20. An apparatus according to Claim 19, wherein the processor is configured to:

collect an additional challenge-response pairing; and

add the additional challenge-response pairing to the plurality of challenge-response pairings.

21. An apparatus according to Claim 20, wherein the processor is configured to collect an additional challenge-response pairing by:

sending a challenge not in the plurality of challenge-response pairings to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the sent challenge with the received response.

22. An apparatus according to Claim 20, wherein the processor is configured to collect an additional challenge-response pairing by:

receiving an authentication command comprising a challenge not in the plurality of challenge-response pairings from a network management entity;

sending the authentication command to the locked subscriber identity device;

receiving a response from the locked subscriber identity device; and

pairing the received challenge with the received response.

23. An apparatus according to Claim 20, wherein the processor is configured to collect an additional challenge-response pairing by collecting an additional challenge-response pairing if a number of unused challenge-response pairings in the plurality of challenge-response pairings equals a first predefined number and continuing to collect additional challenge-response pairings until the number of unused challenge-response pairings in the plurality of challenge-response pairings equals a second predefined number.

24. An apparatus according to Claim 19, further comprising a memory, and wherein the processor is further configured to store the plurality of challenge-response pairings in the memory.

25. An apparatus according to Claim 19, wherein the locked subscriber identity device comprises a universal integrated circuit card.

26. An apparatus according to Claim 19, wherein the processor is further configured to:

validate the connected subscriber identity device such that a communication device is usable if it is determined that the connected subscriber identity device is the locked subscriber identity device; and

reject the connected subscriber identity device such that functionality of a communication device is limited if it is determined that the connected subscriber identity device is not the locked subscriber identity device.

27. An apparatus comprising a processor configured to:

instruct a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device to generate a public key pair, wherein the public key pair is comprised of a private key and a corresponding public key, and wherein the private key is stored in the locked subscriber identity device;

receive the public key from the locked subscriber identity device;

send a validation request to a connected subscriber identity device;

receive a certificate in response to the validation request from the connected subscriber identity device; and

determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part on validation of the received certificate using the public key.

28. An apparatus comprising:

means for establishing a plurality of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device, wherein each challenge-response pairing comprises a challenge and a corresponding response;

means for selecting an unused challenge-response pairing from the plurality of challenge-response pairings;

means for marking the selected challenge-response pairing as used;

means for sending the challenge from the selected challenge-response pairing to a connected subscriber identity device;

means for receiving a response from the connected subscriber identity device; and

means for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing.

29. An apparatus comprising:

means for instructing a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device to generate a public key pair, wherein the public key pair is comprised of a private key and a corresponding public key, and wherein the private key is stored in the locked subscriber identity device;

means for receiving the public key from the locked subscriber identity device;

means for sending a validation request to a connected subscriber identity device;

means for receiving a certificate in response to the validation request from the connected subscriber identity device; and

means for determining whether the connected subscriber identity device is the locked subscriber identity device based at least in part on validation of the received certificate using the public key.

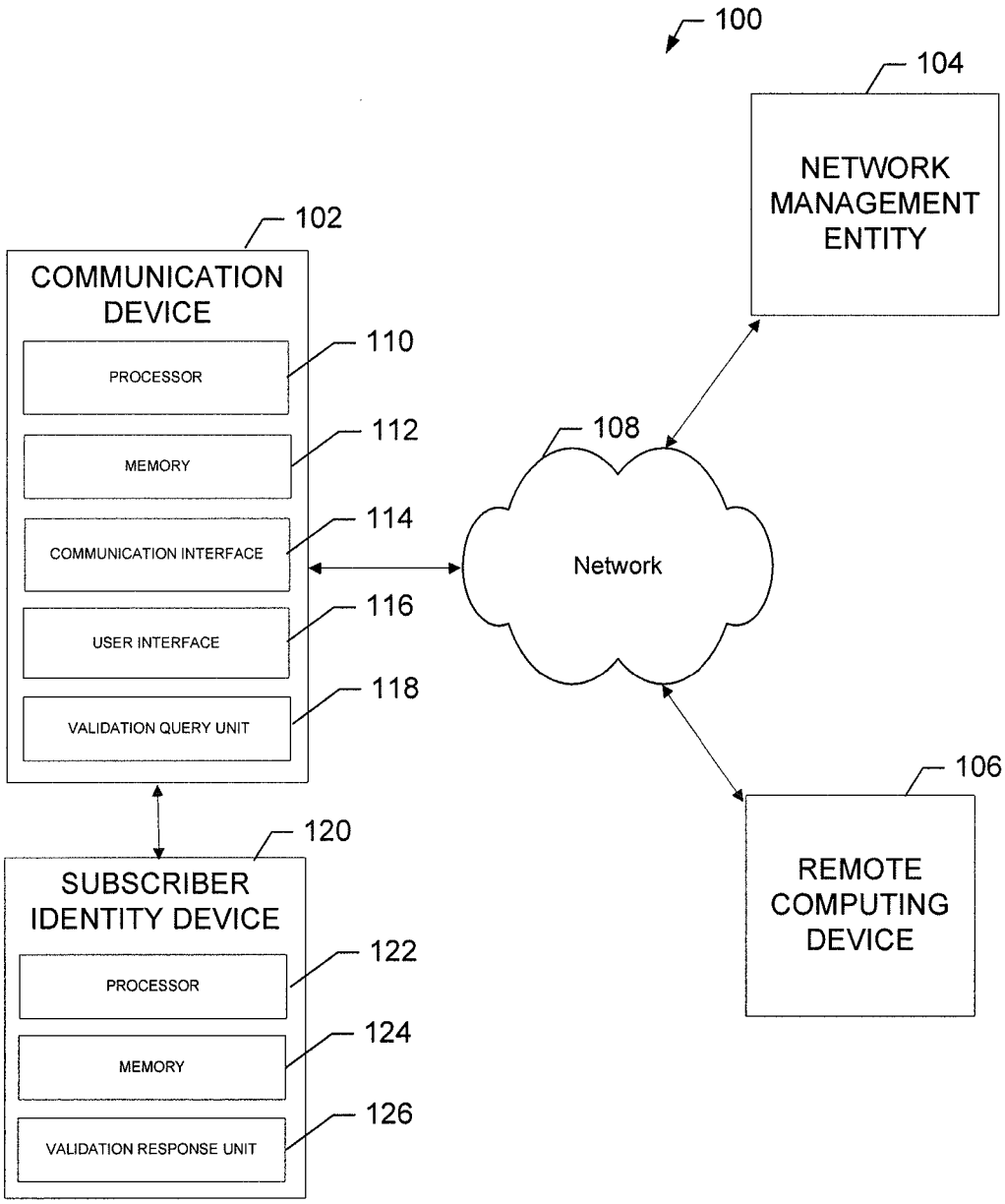
100
104
NETWORK MANAGEMENT ENTITY
102
COMMUNICATION DEVICE
110
PROCESSOR
112
MEMORY
114
COMMUNICATION INTERFACE
116
USER INTERFACE
118
VALIDATION QUERY UNIT
108
Network
106
REMOTE COMPUTING DEVICE
120
SUBSCRIBER IDENTITY DEVICE
122
PROCESSOR
124
MEMORY
126
VALIDATION RESPONSE UNIT

FIG. 1.

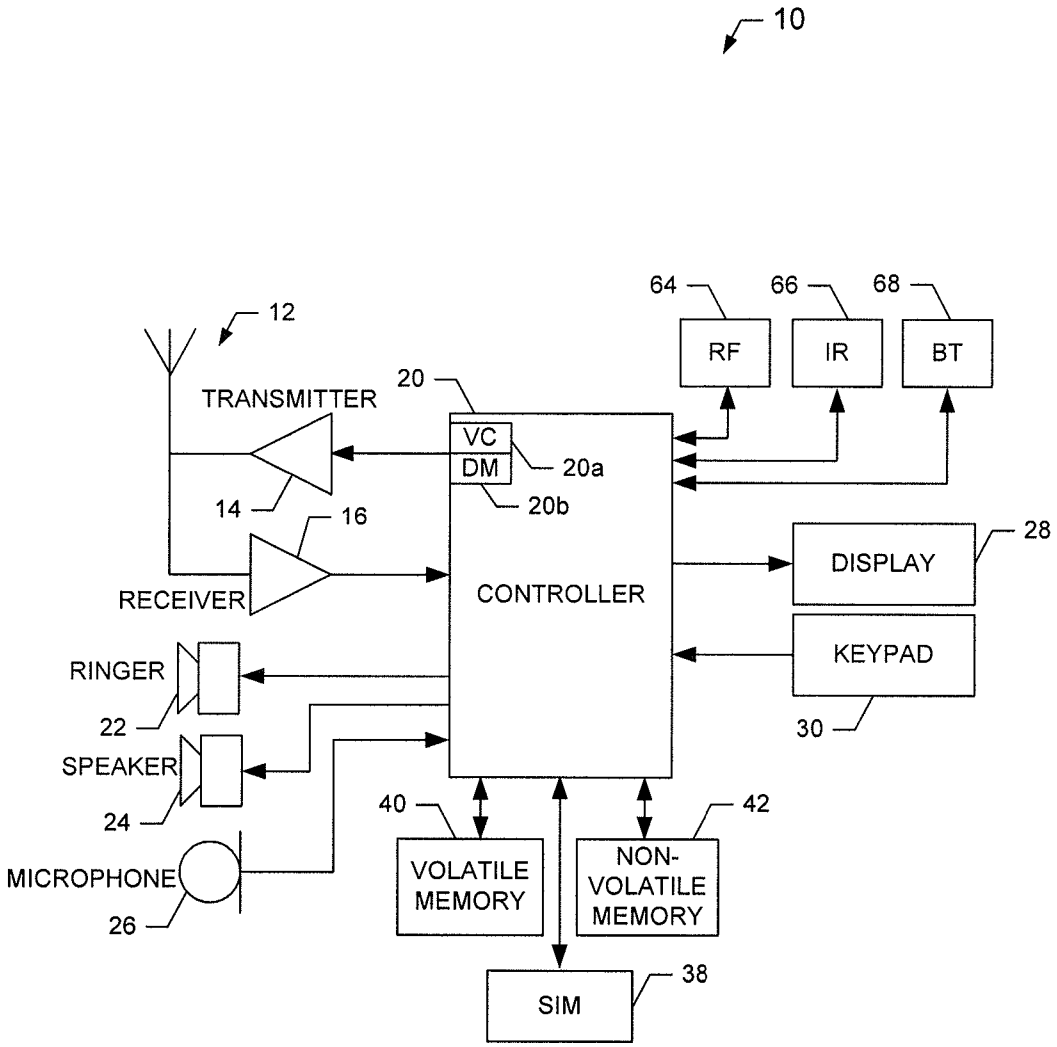
10
12
TRANSMITTER
14
16
RECEIVER
20
VC
DM
20a
20b
CONTROLLER
64
66
68
RF
IR
BT
DISPLAY
28
KEYPAD
30
RINGER
22
SPEAKER
24
MICROPHONE
26
40
VOLATILE MEMORY
42
NON-VOLATILE MEMORY
SIM
38

FIG. 2.

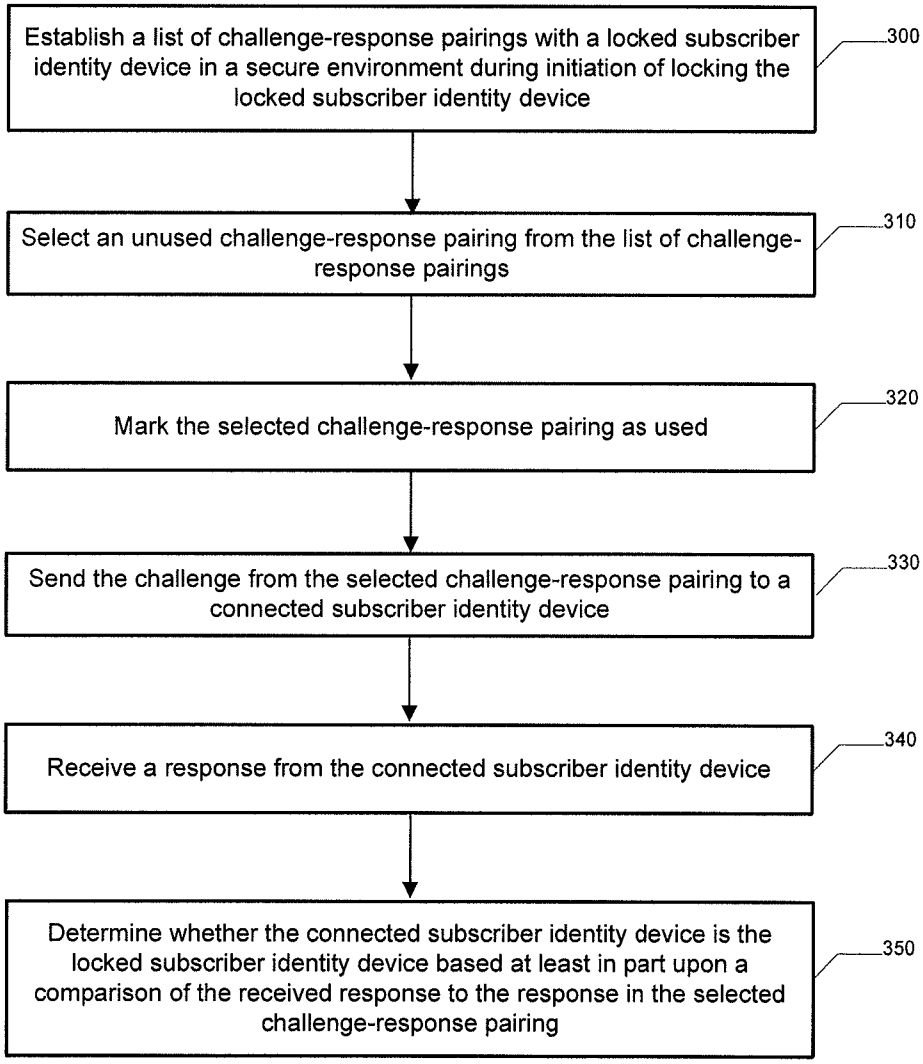
Establish a list of challenge-response pairings with a locked subscriber identity device in a secure environment during initiation of locking the locked subscriber identity device
300
Select an unused challenge-response pairing from the list of challenge-response pairings
310
Mark the selected challenge-response pairing as used
320
Send the challenge from the selected challenge-response pairing to a connected subscriber identity device
330
Receive a response from the connected subscriber identity device
340
Determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a comparison of the received response to the response in the selected challenge-response pairing
350

FIG. 3.

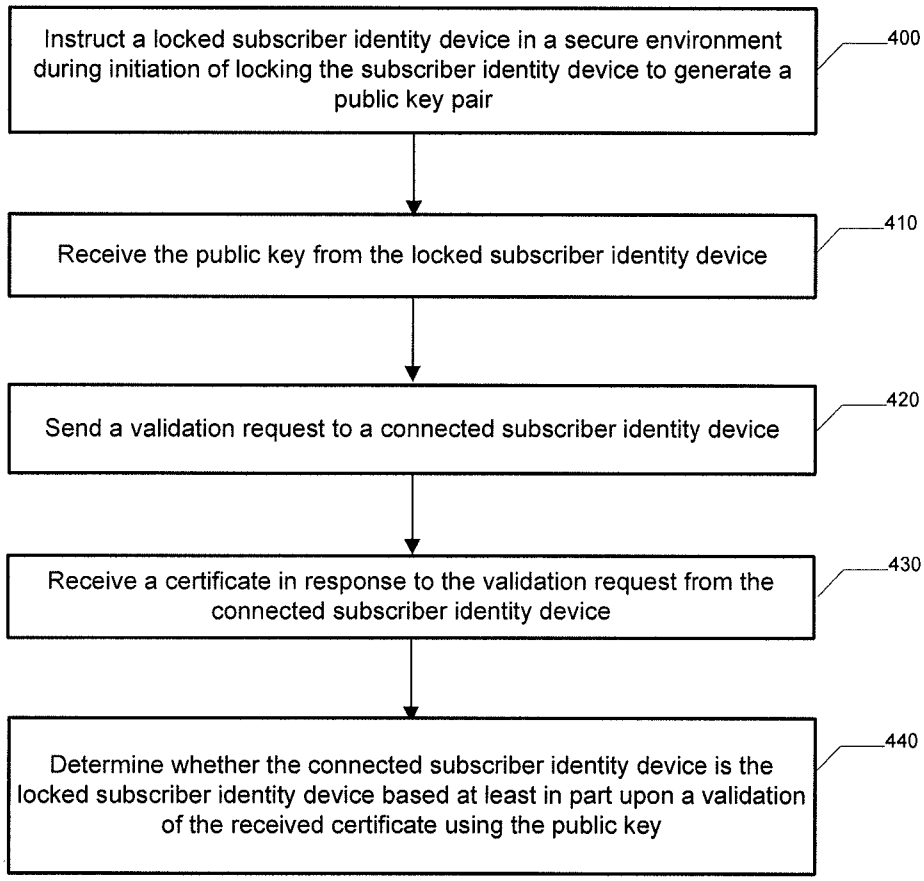
Instruct a locked subscriber identity device in a secure environment during initiation of locking the subscriber identity device to generate a public key pair
400
Receive the public key from the locked subscriber identity device
410
Send a validation request to a connected subscriber identity device
420
Receive a certificate in response to the validation request from the connected subscriber identity device
430
Determine whether the connected subscriber identity device is the locked subscriber identity device based at least in part upon a validation of the received certificate using the public key
440

FIG. 4.

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/053962

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 H04W12/06

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04Q G07F H04L G06F H04W

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 812 764 A (HEINZ SR MICHAEL WILLIAM [US]) 22 September 1998 (1998-09-22) column 4, line 19 - column 7, line 16 column 7, line 55 - column 8, line 33	1-8, 10-17, 19-26,28
X	EP 1 755 061 A (ASSA ABLOY IDENTIFICATION TECH [SE]) 21 February 2007 (2007-02-21) paragraph [0003] paragraphs [0013] - [0022] paragraphs [0034] - [0055]	1-8, 10-17, 19-26,28
A	EP 0 427 465 A (AMERICAN TELEPHONE & TELEGRAPH [US] AT & T CORP [US]) 15 May 1991 (1991-05-15) column 1, line 10 - column 4, line 21 column 5, line 4 - column 6, line 53	1-8, 10-17, 19-26,28

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 May 2009	07/07/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Olaechea, Javier

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2008/053962

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004/043792 A1 (SIMMONS CLAYTON [US]) 4 March 2004 (2004-03-04) paragraphs [0039] - [0055]	1-8, 10-17, 19-26,28
A	GB 2 335 568 A (NEC TECHNOLOGIES [GB] NEC TECHNOLOGIES [GB]; GLOBALMART LTD [GB]) 22 September 1999 (1999-09-22) page 3, paragraph 5 - page 8, paragraph 1	1-8, 10-17, 19-26,28
A	MENEZES A ET AL: "Handbook of Applied Cryptography , IDENTIFICATION AND ENTITY AUTHENTICATION" HANDBOOK OF APPLIED CRYPTOGRAPHY; [CRC PRESS SERIES ON DISCRETE MATHEMATICES AND ITS APPLICATIONS], BOCA RATON, FL, CRC PRESS.; US, 1 January 1997 (1997-01-01), pages 385-424, XP002262234 ISBN: 978-0-8493-8523-0 Section 10.2.5 "One-time passwords"	1-8, 10-17, 19-26,28
A	US 2007/286373 A1 (PAILLES JEAN-CLAUDE [FR] ET AL) 13 December 2007 (2007-12-13) paragraphs [0023] - [0039] paragraphs [0055] - [0072]	1-8, 10-17, 19-26,28

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2008/053962

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers allsearchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search reportcovers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-8, 10-17, 19-26, 28

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-8,10-17,19-26,28

Method and apparatus for determining if a locked subscriber identity module, with challenge-response pairs established during initiation of locking the locked subscriber identity module, is a correct subscriber identity module based on the comparison of the received response with one of the challenge-response pairs.

---

2. claims: 9,18,27,29

Method and apparatus for determining if a locked subscriber identity device, using a public key pair generated by the subscriber identity device during initiation of locking the locked subscriber identity device, is a correct subscriber identity device based on a validation of a received certificate using the public key of the public key pair.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2008/053962

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5812764 A	22-09-1998	NONE	
EP 1755061 A	21-02-2007	AU 2006203515 A1	01-03-2007
		CA 2556235 A1	15-02-2007
EP 0427465 A	15-05-1991	CA 2023872 A1	10-05-1991
		DE 69016589 D1	16-03-1995
		DE 69016589 T2	07-09-1995
		JP 1921556 C	07-04-1995
		JP 3158955 A	08-07-1991
		JP 6052518 B	06-07-1994
		US 5120939 A	09-06-1992
US 2004043792 A1	04-03-2004	NONE	
GB 2335568 A	22-09-1999	AU 743542 B2	31-01-2002
		AU 2124599 A	30-09-1999
		JP 11275215 A	08-10-1999
		US 6321079 B1	20-11-2001
US 2007286373 A1	13-12-2007	CN 101088249 A	12-12-2007
		EP 1815638 A1	08-08-2007
		WO 2006056669 A1	01-06-2006
		JP 2008522470 T	26-06-2008