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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 September 2011 (15.09.2011)

PCT

(10) International Publication Number
WO 2011/112538 A1

(51) International Patent Classification:
G06F 21/02 (2006.01)

(21) International Application Number:
PCT/US2011/027485

(22) International Filing Date:
8 March 2011 (08.03.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
12/720,928 10 March 2010 (10.03.2010) US

(71) Applicant *(for all designated States except US)*: **SPRINT COMMUNICATIONS COMPANY L.P.** [US/US]; 6391 Sprint Parkway, Mailstop: Ksopht0101-Z2100, Overland Park, Kansas 66251-2100 (US).

(72) Inventors: **SHIPLEY, Trevor Daniel**; 13104 South Arapaho Drive, Olathe, Kansas 66062 (US). **SPANEL, Robert L.**; 7809 West 60th Terrace, Overland Park, Kansas 66202 (US).

(74) Agents: **SETTER, Michael J.** et al.; Setter Roche LLP, P.O. Box 780, Erie, Colorado 80516 (US).

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

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

Declarations under Rule 4.17:

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

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

Published:

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

[Continued on next page]

(54) Title: SECURE STORAGE OF PROTECTED DATA IN A WIRELESS COMMUNICATION DEVICE

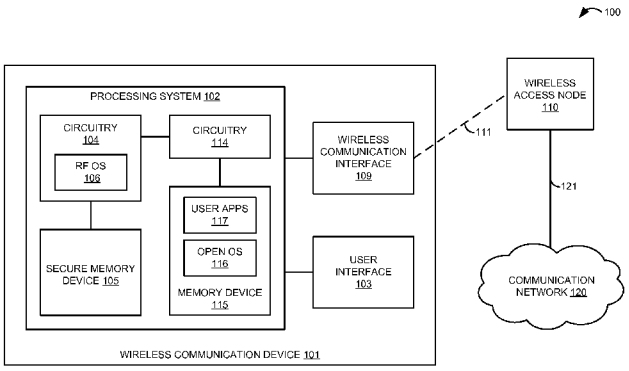

FIGURE 1

(57) Abstract: A wireless communication device (101, 302, 500) comprises first processing circuitry (104, 304, 504) configured to execute an RF operating system (106, 306, 506) and second processing circuitry (114, 314, 514) configured to execute an open operating system (116, 316, 516), wherein the first processing circuitry (104, 304, 504) is linked to a secure memory device (105, 305, 505) inaccessible to the second processing circuitry (114, 314, 514). The RF operating system (106, 306, 506) is configured to receive protected data and store the protected data in the secure memory device (105, 305, 505). The open operating system (116, 316, 516) is configured to receive a request for the protected data from one of a plurality of user applications (117, 317-318, 517) and transfer the request to the RF operating system (106, 306, 506). In response to the request for the protected data, the RF operating system (106, 306, 506) is configured to retrieve the protected data from the secure memory device (105, 305, 505), encrypt the protected data, and transfer the encrypted protected data to the open operating system (116, 316, 516) for delivery to the one of the user applications (117, 317-318, 517) associated with the request.

WO 2011/112538 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

SECURE STORAGE OF PROTECTED DATA IN A WIRELESS COMMUNICATION DEVICE

TECHNICAL BACKGROUND

[0001] Wireless communication networks typically include wireless communication devices which, via a wireless access node, communicate with further communication networks and equipment. Individuals have become increasingly reliant on wireless communication devices to send and receive information. For example, an individual may utilize a wireless communication device for voice communications, research, business, and entertainment. Typically, an operating system is installed on the wireless communication device to manage and coordinate the various functions that the device performs.

[0002] One example of an operating system for a wireless communication device is an open operating system. An open operating system has publically-disclosed source code to facilitate development of applications for the open operating system by third parties. However, due to the open source code, an open operating system may also enable third parties to write malicious applications that exploit the open operating system. In addition to an open operating system, a wireless communication device may have a second operating system for managing radio frequency (RF) communications and modem operations. This RF operating system is a separate, closed operating system that allows RF operations to execute on different circuitry than the open operating system.

[0003] Functions related to device management are typically handled by a device management client application installed on the wireless communication device. The device management client communicates with a device management server typically located in a back-office system of a wireless communication network to provide device provisioning, activation, configuration, software upgrades, and fault management. Critical parameters are

typically passed from the device management server to the device management client to support these functions using over-the-air device management protocols, such as open mobile alliance device management (OMA-DM) or over-the-air service provisioning (OTASP).

OVERVIEW

[0004] A wireless communication device comprises first processing circuitry configured to execute a radio frequency (RF) operating system and second processing circuitry configured to execute an open operating system and a plurality of user applications executing on the open operating system, wherein the first processing circuitry is linked to a secure memory device inaccessible to the second processing circuitry. The RF operating system is configured to receive protected data and unprotected data and store the protected data and the unprotected data in the secure memory device. The open operating system is configured to receive a first request for the unprotected data from one of the user applications and transfer the first request to the RF operating system. In response to the first request for the unprotected data, the RF operating system is configured to retrieve the unprotected data from the secure memory device and transfer the unprotected data to the open operating system for delivery to the one of the user applications associated with the first request. The open operating system is configured to receive a second request for the protected data from one of the user applications and transfer the second request to the RF operating system. In response to the second request for the protected data, the RF operating system is configured to retrieve the protected data from the secure memory device, encrypt the protected data, and transfer the encrypted protected data to the open operating system for delivery to the one of the user applications associated with the second request.

BRIEF DESCRIPTION OF THE DRAWINGS

[0005] Figure 1 is a block diagram that illustrates a communication system.

[0006] Figure 2 is a flow diagram that illustrates an operation of a wireless communication device in the communication system.

[0007] Figure 3 is a block diagram that illustrates a processing system of a wireless communication device in an exemplary embodiment.

[0008] Figure 4 is a sequence diagram that illustrates an operation of the processing system in an exemplary embodiment.

[0009] Figure 5 is a block diagram that illustrates a wireless communication device.

DETAILED DESCRIPTION

[0010] The following description and associated drawings teach the best mode of the invention. For the purpose of teaching inventive principles, some conventional aspects of the best mode may be simplified or omitted. The following claims specify the scope of the invention. Some aspects of the best mode may not fall within the scope of the invention as specified by the claims. Thus, those skilled in the art will appreciate variations from the best mode that fall within the scope of the invention. Those skilled in the art will appreciate that the features described below can be combined in various ways to form multiple variations of the invention. As a result, the invention is not limited to the specific examples described below, but only by the claims and their equivalents.

[0011] Figure 1 is a block diagram that illustrates communication system 100. Communication system 100 includes wireless communication device 101, wireless access

node 110, and communication network 120. Wireless communication device 101 is in communication with wireless access node 110 over wireless communication link 111. Wireless access node 110 communicates with communication network 120 over communication link 121.

[0012] Wireless communication device 101 comprises processing system 102, user interface 103, and wireless communication interface 109. Processing system 102 is linked to user interface 103 and wireless communication interface 109. Processing system 102 includes processing circuitry 104, secure memory device 105, processing circuitry 114, and memory device 115. Processing circuitry 104 includes and executes radio frequency (RF) operating system 106. Processing circuitry 104 is linked to secure memory device 105. Processing circuitry 114 is linked to processing circuitry 104 and memory device 115 that stores open operating system 116 and user application software 117.

[0013] Figure 2 is a flow diagram that illustrates an operation of wireless communication device 101 in communication system 100. The steps of the operation are indicated below parenthetically. In operation, processing circuitry 104 of wireless communication device 101 is configured to execute RF operating system 106, and processing circuitry 104 is linked to secure memory device 105 which is inaccessible to processing circuitry 114. Processing circuitry 114 is configured to execute open operating system 116 and a plurality of user applications 117 executing on open operating system 116.

[0014] In Figure 2, RF operating system 106 receives protected data and unprotected data and stores the protected data and the unprotected data in secure memory device 105 (201). The protected data could comprise any sensitive data that requires safeguarding, such as a user's personal information (a username, password, personal identification number (PIN), credit card number, or International Mobile Subscriber Identity (IMSI), for example),

identification information for device 101 (such as a telephone number, Electronic Serial Number (ESN), Mobile Station Identifier (MSID), Mobile Equipment Identifier (MEID), International Mobile Equipment Identity (IMEI), packet address, or media access control (MAC) address), or any other information that a service provider of communication network 120, a user of device 101, or a manufacturer of device 101 want to protect. Conversely, the unprotected data is any information that is not designated as protected data.

[0015] In some examples, RF operating system 106 is configured to receive the protected data through wireless communication interface 109. Also, in some examples, RF operating system 106 is configured to receive the protected data from a user through user interface 103. The protected data may also be pre-stored in secure memory device 105 by a manufacturer of wireless communication device 101, or may be received from an application 117, operating system 106 or 116, or some other internal device or process of wireless communication device 101, such as a subscriber identity module (SIM) card. If RF operating system 106 receives the protected data in an encrypted form, in some examples, RF operating system 106 may be configured to decrypt and store the protected data in secure memory device 105 without encryption.

[0016] Open operating system 116 receives a first request for the unprotected data from one of the plurality of user applications 117 and transfers the first request to RF operating system 106 (202). The user applications 117 could comprise any software installed on wireless communication device 101 that is executable by open operating system 116. For example, the user applications 117 could comprise third-party software applications installed by a user of wireless communication device 101, or could comprise an application installed by a service provider of communication network 120 or a manufacturer of device 101, such

as a device management application. RF operating system 106 is configured to receive the first request for the unprotected data from open operating system 116 in some examples.

[0017] In response to the first request for the unprotected data, RF operating system 106 retrieves the unprotected data from secure memory device 105 and transfers the unprotected data to open operating system 116 for delivery to the one of the user applications 117 associated with the first request (203). RF operating system 106 is configured to transfer the unprotected data to open operating system 116 in a clear text format (i.e., unencrypted) since the data is designated as unprotected data. The open operating system 116 typically receives the unprotected data from RF operating system 106 and forwards the unprotected data to the one of the user applications 117 associated with the first request.

[0018] Open operating system 116 receives a second request for the protected data from one of the user applications 117 and transfers the second request to RF operating system 106 (204). In response to the second request for the protected data, RF operating system 106 retrieves the protected data from secure memory device 105, encrypts the protected data, and transfers the encrypted protected data to open operating system 116 for delivery to the one of the user applications 117 associated with the second request (205). In some examples, RF operating system 106 is configured to encrypt the protected data based on receiving the second request from open operating system 116. In other words, since the second request is received from open operating system 116 and the data is designated as protected data, RF operating system 106 is configured to encrypt the protected data prior to transferring the protected data to open operating system 116. In some examples, RF operating system 106 is configured to encrypt the protected data using a shared secret key. However, in some examples, RF operating system 106 is configured to transfer the protected data without

encryption to an internal process or application executing on RF operating system 106 and/or processing circuitry 104.

[0019] Advantageously, RF operating system 106 safeguards the protected data through encryption prior to transferring the protected data to open operating system 116. In addition, since the protected data is stored in secure memory device 105, which is only accessible to RF operating system 106, a malicious user application of the applications 117 cannot access the protected data or the secure memory device 105. In this manner, if the malicious user application requests the protected data from open operating system 116, the malicious application will only receive encrypted protected data which it cannot decrypt, thereby ensuring the security of the protected data. However, genuine device management applications of the applications 117 can be entrusted with the encryption key in order to decrypt the protected data when the data must be transferred through open operating system 116 for a legitimate purpose.

[0020] Referring back to Figure 1, wireless communication device 101 may comprise any device having wireless communication connectivity with hardware and circuitry programmed to function as a telecommunications device. Wireless communication device 101 may include other well-known components such as a battery and enclosure that are not shown for clarity. Wireless communication device 101 comprises processing system 102, user interface 103, and wireless communication interface 109. Processing system 102 is linked to user interface 103 and wireless communication interface 109. Examples of wireless communication device 101 include a telephone, transceiver, mobile phone, cellular phone, smartphone, computer, personal digital assistant (PDA), e-book, game console, mobile Internet device, wireless network interface card, media player, or some other wireless communication apparatus – including combinations thereof.

[0021] Wireless communication interface 109 comprises RF communication circuitry and an antenna. The RF communication circuitry typically includes an amplifier, filter, RF modulator, and signal processing circuitry. Wireless communication interface 109 may also include a memory device, software, processing circuitry, or some other communication device. Wireless communication interface 109 may use various wireless protocols, such as Code Division Multiple Access (CDMA) 1xRTT, Global System for Mobile communications (GSM), Universal Mobile Telecommunications System (UMTS), High-Speed Packet Access (HSPA), Evolution-Data Optimized (EV-DO), EV-DO rev. A, Third Generation Partnership Project Long Term Evolution (3GPP LTE), Worldwide Interoperability for Microwave Access (WiMAX), IEEE 802.11 protocols (Wi-Fi), Bluetooth, Internet, telephony, or some other wireless communication format.

[0022] User interface 103 comprises components that interact with a user to receive user inputs and to present media and/or information. User interface 103 may include a speaker, microphone, buttons, lights, display screen, touch screen, touch pad, scroll wheel, communication port, or some other user input/output apparatus – including combinations thereof. User interface 103 may be omitted in some examples.

[0023] Processing system 102 includes processing circuitry 104, secure memory device 105, processing circuitry 114, and memory device 115. Processing circuitry 104 and 114 are typically mounted on a circuit board that may also hold secure memory device 105, memory device 115, and portions of wireless communication interface 109 and user interface 103. In some examples, processing system 102 comprises a dual-core processor, and processing circuitry 104 comprises a first core of the dual-core processor and processing circuitry 114 comprises a second core of the dual-core processor.

[0024] Processing circuitry 104 is linked to secure memory device 105. Processing circuitry 104 comprises microprocessor and other circuitry that executes RF operating system 106. Secure memory device 105 comprises a disk drive, flash drive, data storage circuitry, or some other memory apparatus. RF operating system 106 comprises computer software, firmware, or some other form of machine-readable processing instructions. RF operating system 106 may include utilities, drivers, network interfaces, applications, or some other type of software. As shown in Figure 1, RF operating system 106 is typically stored within the components of processing circuitry 104, such as on read-only memory (ROM) within circuitry 104. However, RF operating system 106 could be stored on a memory device separate from processing circuitry 104, including within secure memory device 105.

[0025] Processing circuitry 114 is linked to processing circuitry 104 and memory device 115. Processing circuitry 114 comprises microprocessor and other circuitry that executes open operating system 116. Memory device 115 comprises a disk drive, flash drive, data storage circuitry, or some other memory apparatus. Open operating system 116 and user applications 117 comprise computer software, firmware, or some other form of machine-readable processing instructions. Open operating system 116 and user applications 117 may include utilities, drivers, network interfaces, applications, or some other type of software.

[0026] Wireless access node 110 comprises RF communication circuitry and an antenna. The RF communication circuitry typically includes an amplifier, filter, RF modulator, and signal processing circuitry. Wireless access node 110 may also comprise a router, server, memory device, software, processing circuitry, cabling, power supply, network communication interface, structural support, or some other communication apparatus. Wireless access node 110 could comprise a base station, Internet access node, telephony service node, wireless data access point, or some other wireless communication system –

including combinations thereof. Some examples of wireless access node 110 include a base transceiver station (BTS), base station controller (BSC), radio base station (RBS), Node B, enhanced Node B (eNode B), and others. Wireless network protocols that may be utilized by wireless access node 110 include CDMA, GSM, UMTS, HSPA, EV-DO, EV-DO rev. A, 3GPP LTE, WiMAX, Wi-Fi, Bluetooth, Internet, telephony, or some other communication format – including combinations thereof.

[0027] Communication network 120 comprises the core network of a wireless communication provider, and could include routers, gateways, telecommunication switches, servers, processing systems, or other communication equipment and systems for providing communication and data services. Communication network 120 could comprise wireless communication nodes, telephony switches, Internet routers, network gateways, computer systems, communication links, or some other type of communication equipment – including combinations thereof. Communication network 120 may also comprise optical networks, asynchronous transfer mode (ATM) networks, packet networks, metropolitan-area networks (MAN), or other network topologies, equipment, or systems – including combinations thereof. Communication network 120 may be configured to communicate over metallic, wireless, or optical links. Communication network 120 may be configured to use time-division multiplexing (TDM), Internet Protocol (IP), Ethernet, optical networking, wireless protocols, communication signaling, or some other communication format – including combinations thereof. In some examples, communication network 120 includes further access nodes and associated equipment for providing communication services to many wireless communication devices across a large geographic region.

[0028] Wireless communication link 111 uses the air or space as the transport medium. Wireless communication link 111 may use various protocols, such as CDMA,

GSM, UMTS, HSPA, EV-DO, EV-DO rev. A, 3GPP LTE, WiMAX, Wi-Fi, Bluetooth, Internet, telephony, or some other communication format – including combinations thereof. Wireless communication link 111 may comprise many different signals sharing the same link. For example, wireless communication link 111 could include multiple signals operating in a single propagation path comprising multiple communication sessions, frequencies, timeslots, transportation ports, logical transportation links, network sockets, IP sockets, packets, or communication directions – including combinations thereof.

[0029] Communication link 121 uses metal, air, space, optical fiber such as glass or plastic, or some other material as the transport media – including combinations thereof. Communication link 121 could use various communication protocols, such as TDM, IP, Ethernet, telephony, optical networking, hybrid fiber coax (HFC), communication signaling, wireless protocols, or some other communication format – including combinations thereof. Communication link 121 may be a direct link or could include intermediate networks, systems, or devices.

[0030] Figure 3 is a block diagram that illustrates processing system 302 of a wireless communication device in an exemplary embodiment. Processing system 302 includes processing circuitry 304, secure memory device 305, processing circuitry 314, and memory device 315. Processing circuitry 304 includes and executes RF operating system 306. RF operating system 306 includes RF logic 307, input/output (I/O) interface 308, and application programming interface (API) 309. Processing circuitry 304 is linked to secure memory device 305 via I/O interface 308. Processing circuitry 314 is linked to processing circuitry 304 and memory device 315. Memory device 315 stores open operating system 316, device management client 317, and malware user application 318. Processing circuitry 314 executes

open operating system 316. In the exemplary embodiment of Figure 3, open operating system 316 comprises an android mobile operating system.

[0031] Figure 4 is a sequence diagram that illustrates an operation of processing system 302 in an exemplary embodiment. The operation depicted in Figure 4 facilitates the safeguarding and storage of critical parameters in secure memory device 305 according to an over-the-air device management protocol, such as open mobile alliance device management (OMA-DM) or over-the-air service provisioning (OTASP). To achieve this, a shared secret encryption key is hardcoded into processing system 302, typically within processing circuitry 304 as part of RF operating system 306. This shared secret key is then provided to a communication service provider for the wireless communication device.

[0032] To begin, data is received by RF logic 307. The data received by RF logic 307 includes protected data comprising critical parameters that have been encrypted by a device management server using the unique shared secret encryption key associated with the wireless communication device comprising processing system 302. RF logic 307 receives the encrypted data over-the-air through a wireless communication interface from a communication service provider operating the device management server.

[0033] RF logic 307 is configured to transfer the encrypted protected data to open operating system 316. Open operating system 316 then forwards the encrypted protected data to device management client 317. The device management client 317 may perform some operations on the encrypted protected data, including fully or partially decrypting the protected data to perform such operations. Regardless, device management client 317 transfers the encrypted protected data to open operating system 316 with a storage request to store the protected data in secure memory device 305. Open operating system 316 forwards

the encrypted protected data with the storage request to API 309 within the RF operating system 304.

[0034] API 309 receives the API call for the storage request and decrypts the protected data using the shared secret key. API 309 then transfers the decrypted protected data to I/O interface 308. I/O interface 308 stores the decrypted protected data in secure memory device 305. In this manner, malware user application 318 cannot intercept and/or modify the critical parameters or other sensitive information contained in the encrypted protected data as it is processed by device management client 317 and transferred through open operating system 316 prior to storage in secure memory device 305. For example, malware user application 318 may comprise a rogue application designed to passively monitor the protected data as it is passed through memory device 315 between the open operating system 316 and the secure memory device 305. Since the protected data is always encrypted prior to storage in secure memory device 305, malware user application 318 cannot observe the protected data.

[0035] Subsequent to storing the protected data in secure memory device 305, device management client 317 requests the protected data from open operating system 316. The data request is forwarded by open operating system 316 to API 309 in an API call for the protected data. API 309 forwards the data request to I/O interface 308 which can directly access secure memory device 305. I/O interface 308 retrieves the protected data from secure memory device 305.

[0036] I/O interface 308 transfers an API call to API 309 for encryption of protected data 309. API 309 receives the API call with the protected data and encrypts the protected data using the shared secret key. API 309 then transfers the encrypted protected data to open operating system 316. The encrypted protected data is forwarded by open operating system 316 to device management client 317. Device management client 317 can then decrypt the

encrypted protected data using the shared secret key, and process the protected data for device management purposes.

[0037] Advantageously, if malware user application 318 purports to act as a legitimate data management application and requests the protected data from open operating system 316, open operating system 316 would only receive the encrypted protected data from an API call to API 309. Thus, the malware user application 318 would also receive the protected data from open operating system 316 in an encrypted form, and would not be able to process or otherwise manipulate the protected data for malicious purposes.

[0038] Figure 5 is a block diagram that illustrates wireless communication device 500. Wireless communication device 500 provides an example of wireless communication device 101, although device 101 could use alternative configurations. Wireless communication device 500 comprises wireless communication interface 501, processing system 502, and user interface 503. Processing system 502 is linked to wireless communication interface 501 and user interface 503. Processing system 502 includes first processing circuitry 504, secure memory device 505, second processing circuitry 514, and memory device 515. Memory device 515 stores open operating system 516 and a plurality of user applications 517. Wireless communication device 500 may include other well-known components such as a battery and enclosure that are not shown for clarity. Wireless communication device 500 may comprise a telephone, computer, e-book, mobile Internet appliance, media player, game console, wireless network interface card, or some other wireless communication apparatus – including combinations thereof.

[0039] Wireless communication interface 501 comprises RF communication circuitry and an antenna. The RF communication circuitry typically includes an amplifier, filter, RF modulator, and signal processing circuitry. Wireless communication interface 501 may also

include a memory device, software, processing circuitry, or some other communication device. Wireless communication interface 501 may use various protocols, such as CDMA, GSM, UMTS, HSPA, EV-DO, EV-DO rev. A, 3GPP LTE, WiMAX, Wi-Fi, Bluetooth, Internet, telephony, or some other wireless communication format. Wireless communication interface 501 may be configured to receive protected data and unprotected data.

[0040] User interface 503 comprises components that interact with a user to receive user inputs and to present media and/or information. User interface 503 may include a speaker, microphone, buttons, lights, display screen, touch screen, touch pad, scroll wheel, communication port, or some other user input/output apparatus – including combinations thereof. User interface 503 may be configured to receive protected data and unprotected data. User interface 503 may be omitted in some examples.

[0041] First processing circuitry 504 stores RF operating system 506. First processing circuitry 504 is linked to secure memory device 505. First processing circuitry 504 comprises microprocessor and other circuitry that executes RF operating system 506. Secure memory device 505 comprises a disk drive, flash drive, data storage circuitry, or some other memory apparatus. RF operating system 506 comprises computer software, firmware, or some other form of machine-readable processing instructions. RF operating system 506 may include utilities, drivers, network interfaces, applications, or some other type of software.

[0042] When executed by processing circuitry 504, RF operating system 506 directs processing system 502 to operate wireless communication device 500 as described herein for wireless communication device 101. In particular, RF operating system 506 directs processing system 502 to receive protected data and unprotected data and store the protected data and the unprotected data in secure memory device 505. Further, RF operating system 506 directs processing system 502 to retrieve the unprotected data from secure memory

device 505 in response to a first request for the unprotected data from open operating system 516, and transfer the unprotected data to open operating system 516 for delivery to the one of the user applications 517 associated with the first request. In addition, RF operating system 506 directs processing system 502 to retrieve the protected data from secure memory device 505 in response to a second request for the protected data from open operating system 516, encrypt the protected data, and transfer the protected data to open operating system 516 for delivery to the one of the user applications 517 associated with the second request.

[0043] First processing circuitry 504 and second processing circuitry 514 are typically mounted on a circuit board that may also hold secure memory device 505, memory device 515, and portions of wireless communication interface 501 and user interface 503. Second processing circuitry 514 is linked to first processing circuitry 504 and memory device 515. Second processing circuitry 514 comprises microprocessor and other circuitry that executes open operating system 516 and user applications 517. Memory device 515 comprises a disk drive, flash drive, data storage circuitry, or some other memory apparatus. Open operating system 516 and user applications 517 comprise computer software, firmware, or some other form of machine-readable processing instructions. Open operating system 516 and user applications 517 may include utilities, drivers, network interfaces, applications, or some other type of software.

[0044] When executed by second processing circuitry 514, open operating system 516 directs processing system 502 to operate wireless communication device 500 as described herein for wireless communication device 101. In particular, open operating system 516 directs processing system 502 to receive a first request for the unprotected data from one of the user applications 517, transfer the first request to RF operating system 506, and receive the unprotected data from RF operating system 506 for delivery to the one of the user

applications 517 associated with the first request. In addition, open operating system 516 directs processing system 502 to receive a second request for the protected data from one of the user applications 517, transfer the second request to RF operating system 506, and receive encrypted protected data from RF operating system 506 for delivery to the one of the user applications 517 associated with the second request.

[0045] The above description and associated figures teach the best mode of the invention. The following claims specify the scope of the invention. Note that some aspects of the best mode may not fall within the scope of the invention as specified by the claims. Those skilled in the art will appreciate that the features described above can be combined in various ways to form multiple variations of the invention. As a result, the invention is not limited to the specific embodiments described above, but only by the following claims and their equivalents.

CLAIMS:

What is claimed is:

1. A wireless communication device comprising first processing circuitry configured to execute a radio frequency (RF) operating system, second processing circuitry configured to execute an open operating system, and a plurality of user applications executing on the open operating system, wherein the first processing circuitry is linked to a secure memory device inaccessible to the second processing circuitry, the wireless communication device characterized by:

the RF operating system configured to receive protected data and unprotected data and store the protected data and the unprotected data in the secure memory device;

the open operating system configured to receive a first request for the unprotected data from one of the user applications and transfer the first request to the RF operating system;

in response to the first request for the unprotected data, the RF operating system configured to retrieve the unprotected data from the secure memory device and transfer the unprotected data to the open operating system for delivery to the one of the user applications associated with the first request;

the open operating system configured to receive a second request for the protected data from one of the user applications and transfer the second request to the RF operating system; and

in response to the second request for the protected data, the RF operating system configured to retrieve the protected data from the secure memory device, encrypt the protected data, and transfer the encrypted protected data to the open operating system for delivery to the one of the user applications associated with the second request.

2. The wireless communication device of claim 1 wherein the RF operating system configured to encrypt the protected data comprises the RF operating system configured to encrypt the protected data based on receiving the second request from the open operating system.

3. The wireless communication device of claim 1 wherein the RF operating system configured to encrypt the protected data comprises the RF operating system configured to encrypt the protected data using a shared secret key.

4. The wireless communication device of claim 1 wherein the RF operating system configured to receive the protected data comprises the RF operating system configured to receive the protected data through a wireless communication interface.

5. The wireless communication device of claim 1 wherein the RF operating system configured to receive the protected data comprises the RF operating system configured to receive the protected data from a user through a user interface.

6. The wireless communication device of claim 1 wherein the RF operating system configured to store the protected data in the secure memory device comprises the RF operating system configured to decrypt the protected data if the protected data is encrypted and store the protected data in the secure memory device without encryption.

7. The wireless communication device of claim 1 wherein the RF operating system configured to store the protected data in the secure memory device comprises an input/output (I/O) interface of the RF operating system configured to store the protected data in the secure memory device, and wherein the RF operating system configured to retrieve the protected data from the secure memory device comprises the I/O interface configured to retrieve the protected data from the secure memory device.

8. The wireless communication device of claim 1 wherein the RF operating system is configured to receive the first request and the second request into an application programming interface (API) of the RF operating system.

9. The wireless communication device of claim 8 wherein the RF operating system configured to encrypt the protected data comprises the API configured to encrypt the protected data, and wherein the RF operating system configured to transfer the encrypted protected data to the open operating system comprises the API configured to transfer the encrypted protected data to the open operating system for delivery to the one of the user applications associated with the second request.

10. The wireless communication device of claim 1 wherein the first processing circuitry comprises a first core of a dual-core processor and wherein the second processing circuitry comprises a second core of the dual-core processor.

11. A method of operating a wireless communication device comprising first processing circuitry configured to execute a radio frequency (RF) operating system and second processing circuitry configured to execute an open operating system and a plurality of user applications executing on the open operating system, wherein the first processing circuitry is linked to a secure memory device inaccessible to the second processing circuitry, the method characterized by:

in the RF operating system, receiving protected data and unprotected data and storing the protected data and the unprotected data in the secure memory device;

in the open operating system, receiving a first request for the unprotected data from one of the user applications and transferring the first request to the RF operating system;

in the RF operating system, in response to the first request for the unprotected data, retrieving the unprotected data from the secure memory device and transferring the unprotected data to the open operating system for delivery to the one of the user applications associated with the first request;

in the open operating system, receiving a second request for the protected data from one of the user applications and transferring the second request to the RF operating system; and

in the RF operating system, in response to the second request for the protected data, retrieving the protected data from the secure memory device, encrypting the protected data, and transferring the encrypted protected data to the open operating system for delivery to the one of the user applications associated with the second request.

12. The method of claim 11 wherein encrypting the protected data comprises encrypting the protected data based on receiving the second request from the open operating system.

13. The method of claim 11 wherein encrypting the protected data comprises encrypting the protected data using a shared secret key.

14. The method of claim 11 wherein receiving the protected data comprises receiving the protected data through a wireless communication interface.

15. The method of claim 11 wherein receiving the protected data comprises receiving the protected data from a user through a user interface.

16. The method of claim 11 wherein storing the protected data in the secure memory device comprises decrypting the protected data if the protected data is encrypted and storing the protected data in the secure memory device without encryption.

17. The method of claim 11 wherein storing the protected data in the secure memory device comprises an input/output (I/O) interface of the RF operating system storing the protected data in the secure memory device, and wherein retrieving the protected data from the secure memory device comprises the I/O interface retrieving the protected data from the secure memory device.

18. The method of claim 11 further comprising receiving the first request and the second request into an application programming interface (API) of the RF operating system.

19. The method of claim 18 wherein encrypting the protected data comprises the API encrypting the protected data, and wherein transferring the encrypted protected data to the open operating system comprises the API transferring the encrypted protected data to the open operating system for delivery to the one of the user applications associated with the second request.

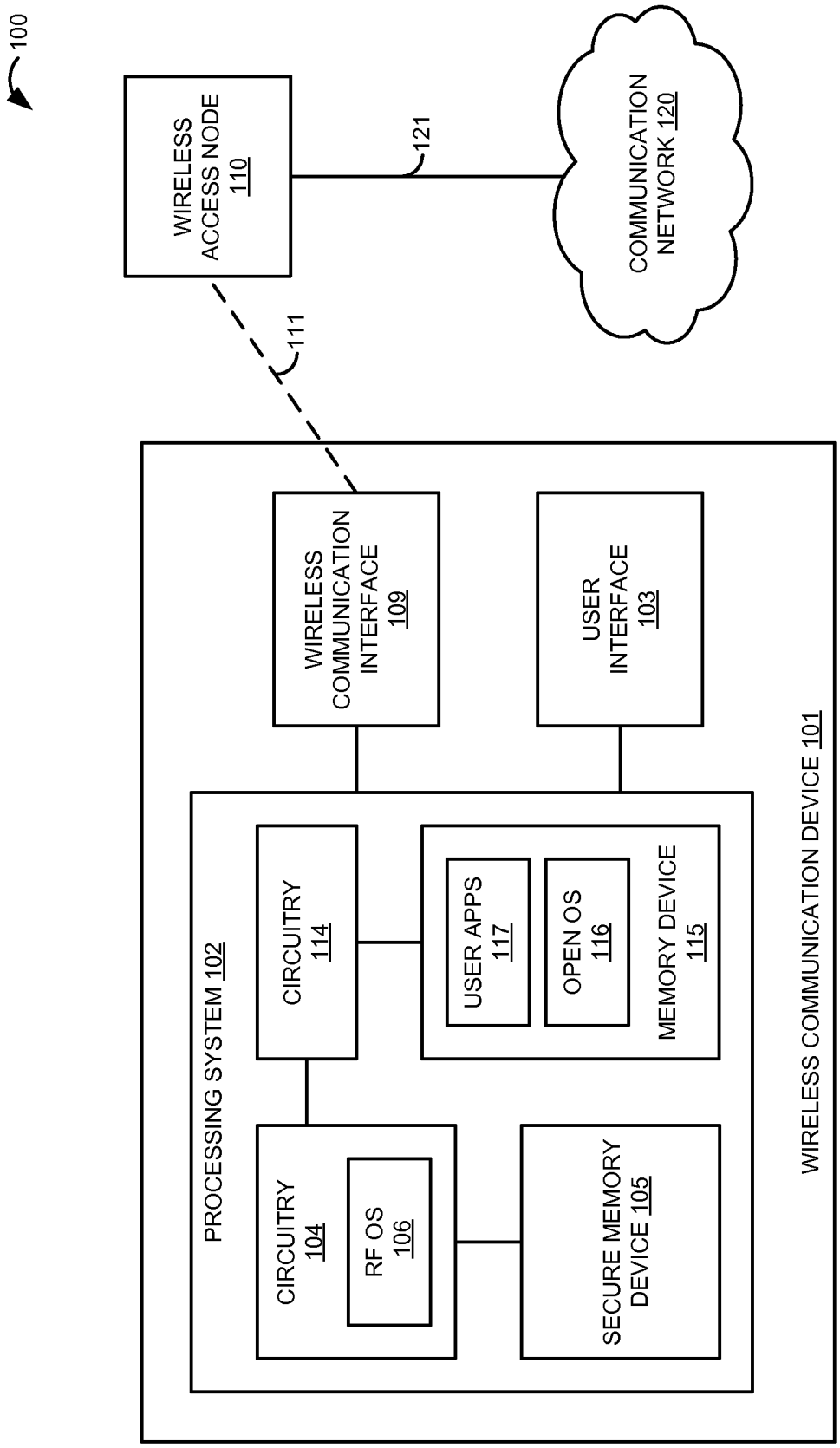
100
WIRELESS ACCESS NODE 110
121
COMMUNICATION NETWORK 120
111
WIRELESS COMMUNICATION INTERFACE 109
USER INTERFACE 103
PROCESSING SYSTEM 102
CIRCUITRY 114
USER APPS 117
OPEN OS 116
MEMORY DEVICE 115
CIRCUITRY 104
RF OS 106
SECURE MEMORY DEVICE 105
WIRELESS COMMUNICATION DEVICE 101

FIGURE 1

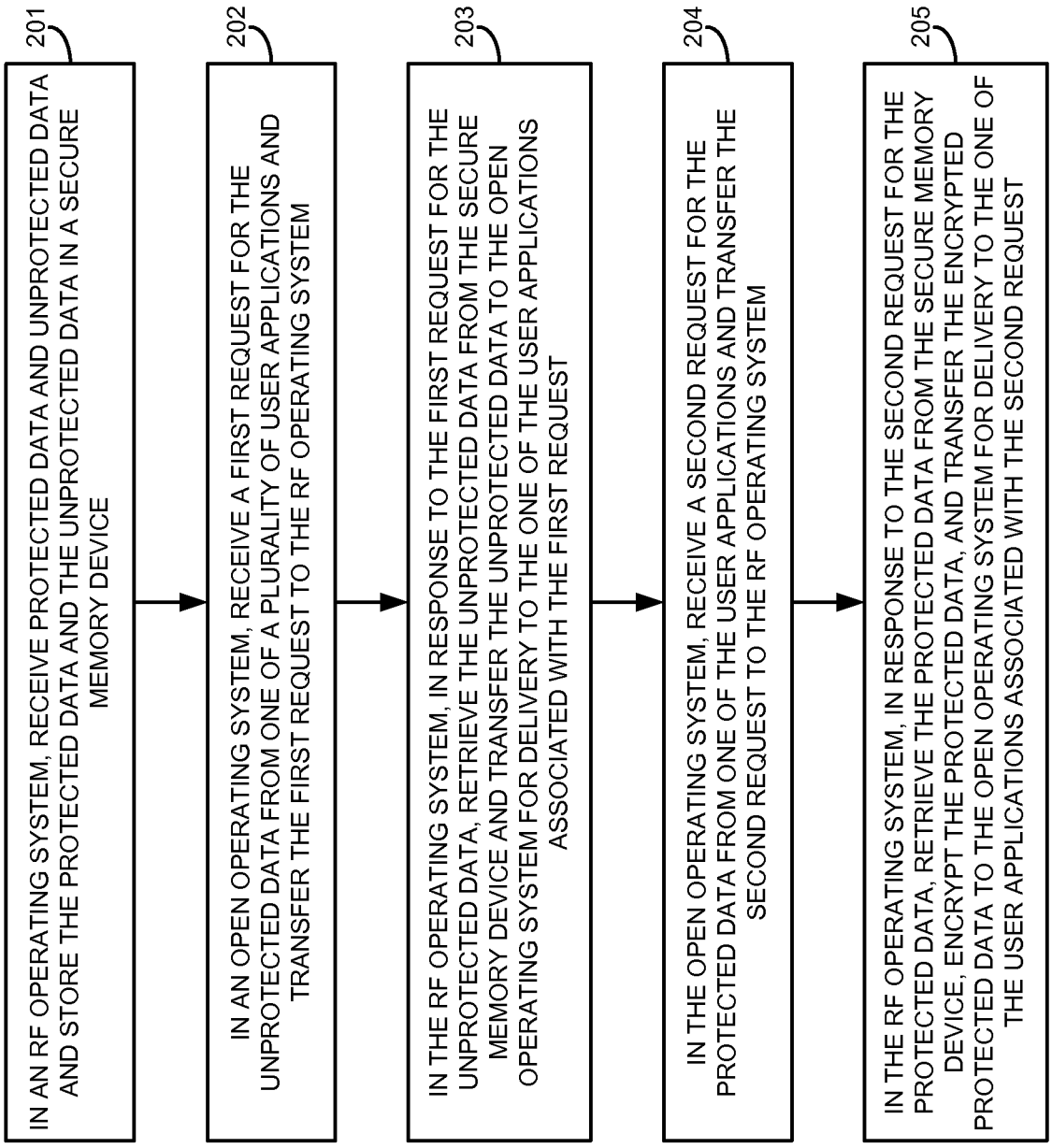
201
IN AN RF OPERATING SYSTEM, RECEIVE PROTECTED DATA AND UNPROTECTED DATA AND STORE THE PROTECTED DATA AND THE UNPROTECTED DATA IN A SECURE MEMORY DEVICE
202
IN AN OPEN OPERATING SYSTEM, RECEIVE A FIRST REQUEST FOR THE UNPROTECTED DATA FROM ONE OF A PLURALITY OF USER APPLICATIONS AND TRANSFER THE FIRST REQUEST TO THE RF OPERATING SYSTEM
203
IN THE RF OPERATING SYSTEM, IN RESPONSE TO THE FIRST REQUEST FOR THE UNPROTECTED DATA, RETRIEVE THE UNPROTECTED DATA FROM THE SECURE MEMORY DEVICE AND TRANSFER THE UNPROTECTED DATA TO THE OPEN OPERATING SYSTEM FOR DELIVERY TO THE ONE OF THE USER APPLICATIONS ASSOCIATED WITH THE FIRST REQUEST
204
IN THE OPEN OPERATING SYSTEM, RECEIVE A SECOND REQUEST FOR THE PROTECTED DATA FROM ONE OF THE USER APPLICATIONS AND TRANSFER THE SECOND REQUEST TO THE RF OPERATING SYSTEM
205
IN THE RF OPERATING SYSTEM, IN RESPONSE TO THE SECOND REQUEST FOR THE PROTECTED DATA, RETRIEVE THE PROTECTED DATA FROM THE SECURE MEMORY DEVICE, ENCRYPT THE PROTECTED DATA, AND TRANSFER THE ENCRYPTED PROTECTED DATA TO THE OPEN OPERATING SYSTEM FOR DELIVERY TO THE ONE OF THE USER APPLICATIONS ASSOCIATED WITH THE SECOND REQUEST

FIGURE 2

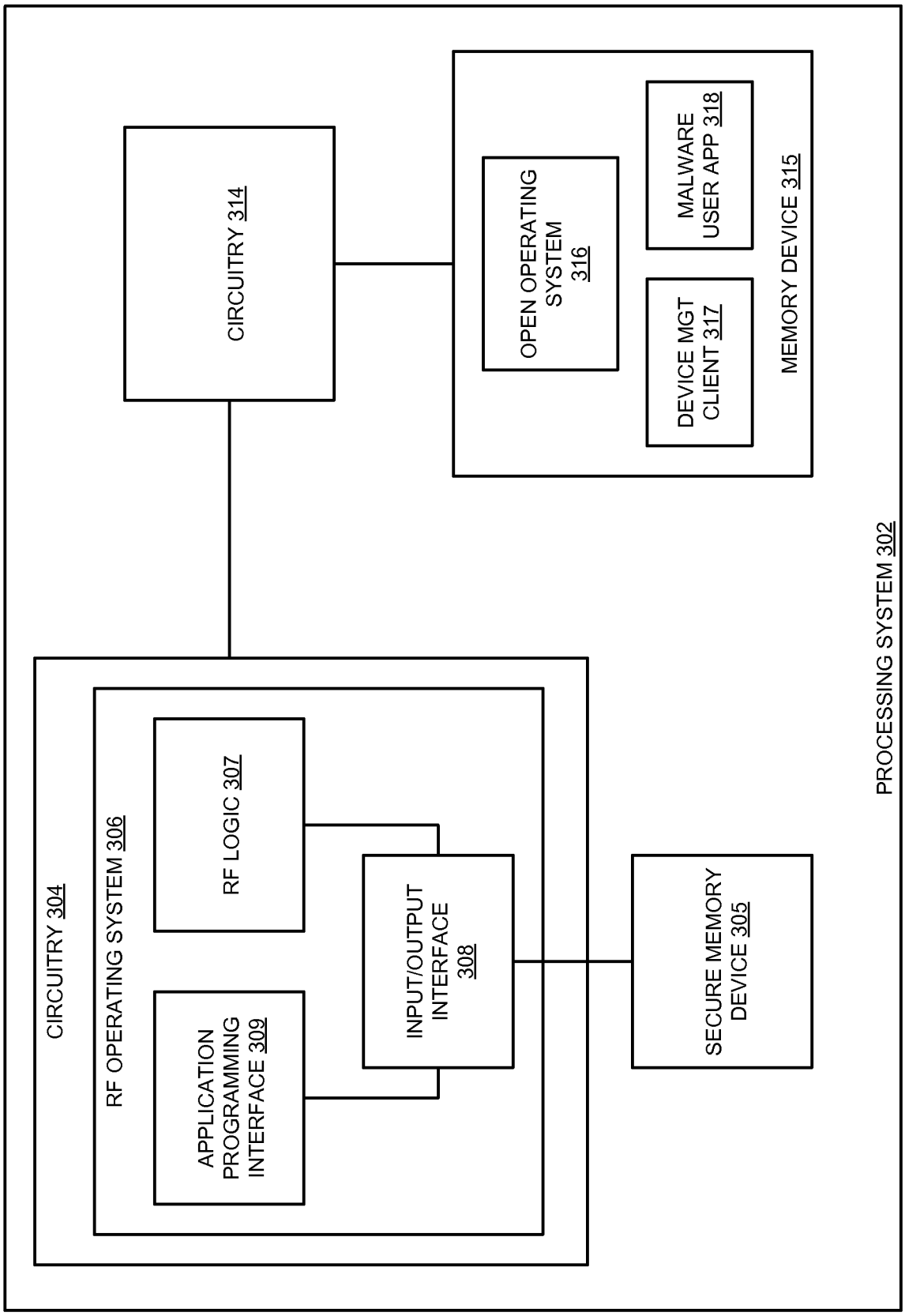
PROCESSING SYSTEM 302
CIRCUITRY 314
MEMORY DEVICE 315
OPEN OPERATING SYSTEM 316
MALWARE USER APP 318
DEVICE MGT CLIENT 317
CIRCUITRY 304
RF OPERATING SYSTEM 306
RF LOGIC 307
APPLICATION PROGRAMMING INTERFACE 309
INPUT/OUTPUT INTERFACE 308
SECURE MEMORY DEVICE 305

FIGURE 3

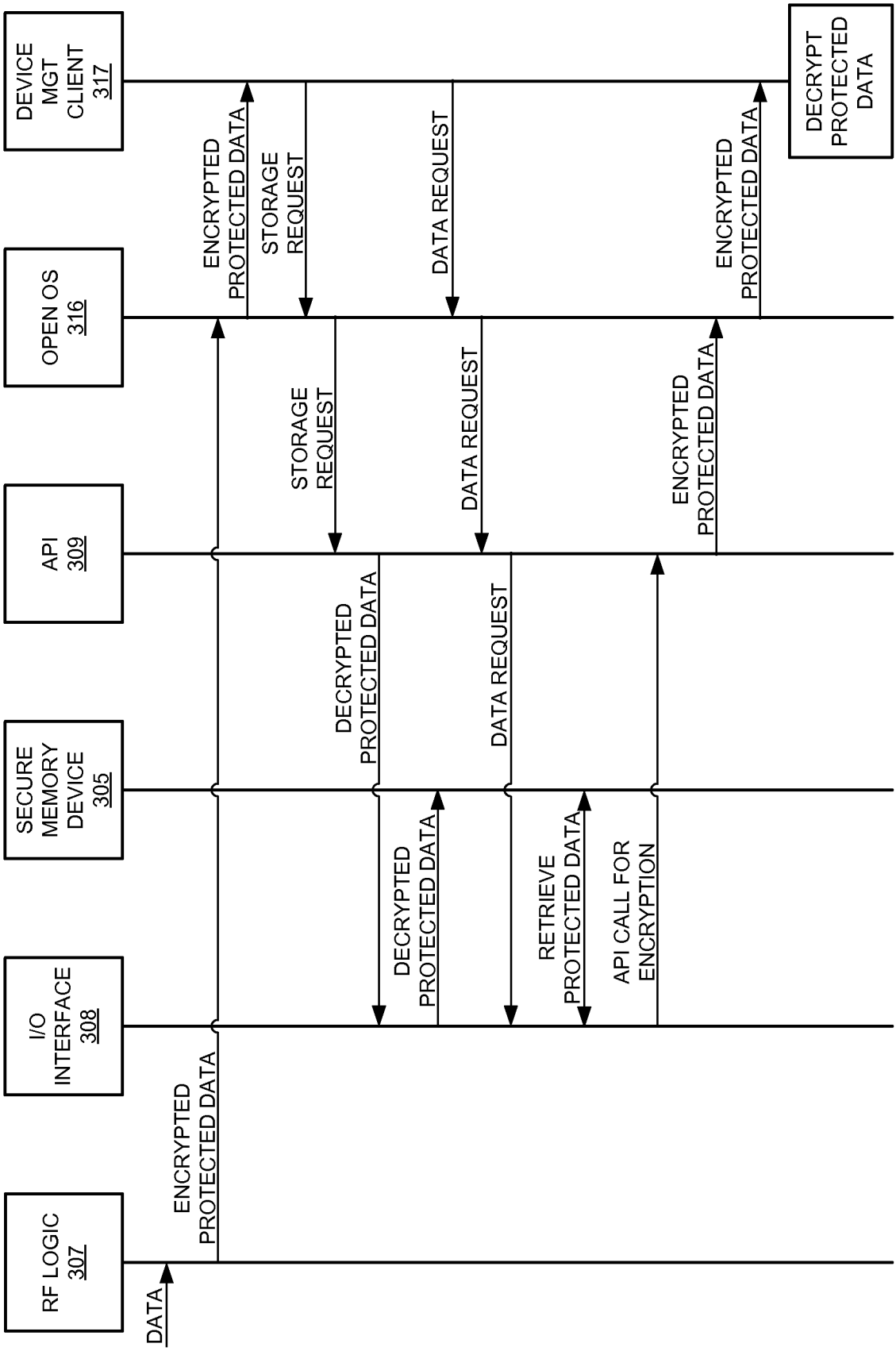
DEVICE MGT CLIENT 317
OPEN OS 316
API 309
SECURE MEMORY DEVICE 305
I/O INTERFACE 308
RF LOGIC 307
DATA
ENCRYPTED PROTECTED DATA
STORAGE REQUEST
DECRYPTED PROTECTED DATA
DATA REQUEST
RETRIEVE PROTECTED DATA
API CALL FOR ENCRYPTION
ENCRYPTED PROTECTED DATA
DATA REQUEST
ENCRYPTED PROTECTED DATA
DECRYPT PROTECTED DATA

FIGURE 4

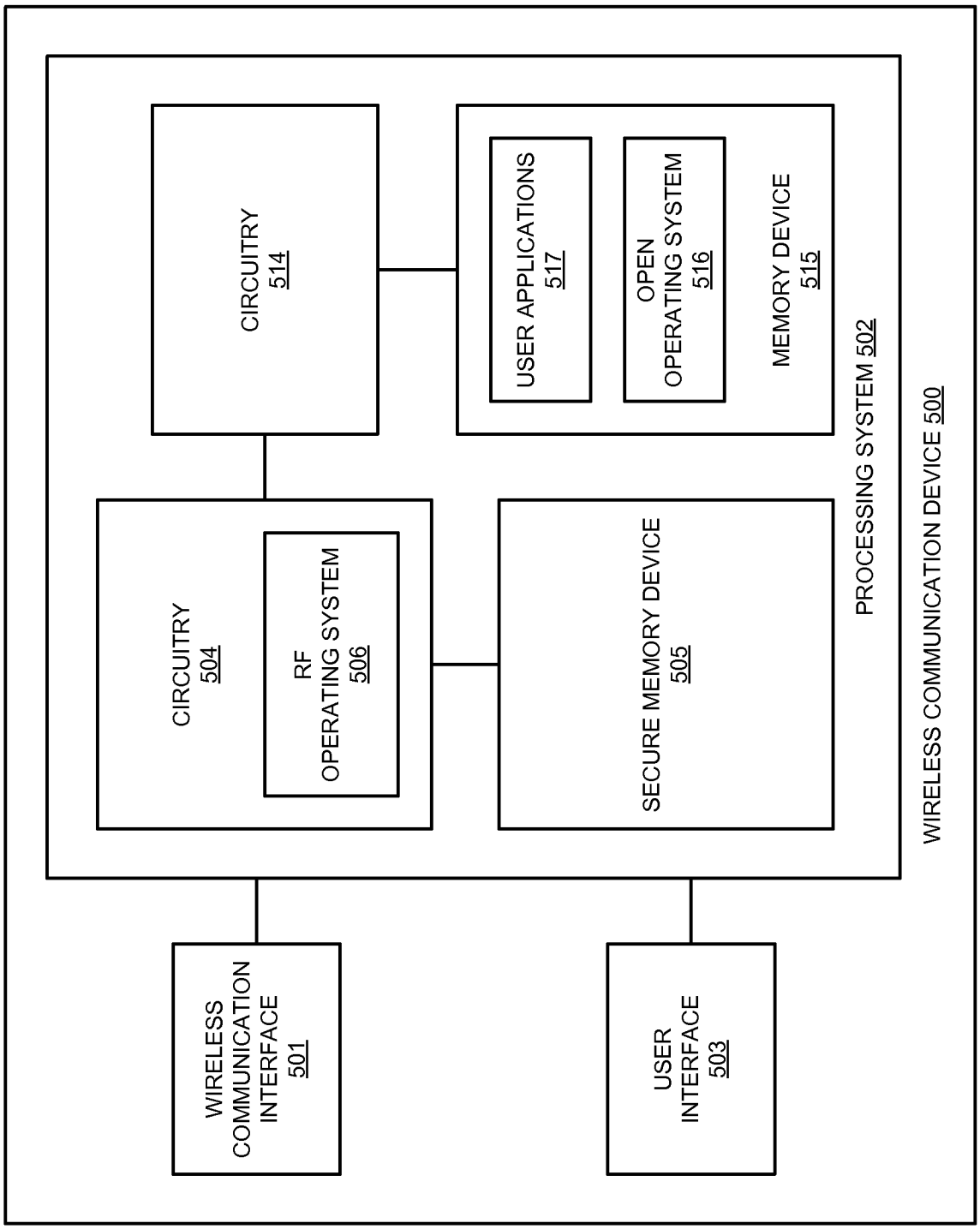
WIRELESS COMMUNICATION DEVICE 500
PROCESSING SYSTEM 502
CIRCUITRY 514
MEMORY DEVICE 515
USER APPLICATIONS 517
OPEN OPERATING SYSTEM 516
CIRCUITRY 504
RF OPERATING SYSTEM 506
SECURE MEMORY DEVICE 505
WIRELESS COMMUNICATION INTERFACE 501
USER INTERFACE 503

FIGURE 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/027485

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/02
ADD.

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)
G06F

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/199046 A1 (O'BRIEN TERENCE W [US]) 23 August 2007 (2007-08-23) paragraph [0026] - paragraph [0049]; claim 1; figure 3	1-19
X	US 2006/129848 A1 (PAKSOY ERDAL [US] ET AL) 15 June 2006 (2006-06-15) abstract paragraph [0051] - paragraph [0078]; claims 1, 2, 12, 25; figures 3, 5 paragraph [0119] paragraph [0164]	1-19

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

"E" earlier 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
11 July 2011	12/08/2011

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	Savvides, George

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/027485

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007199046 A1	23-08-2007	NONE	
US 2006129848 A1	15-06-2006	US 2011162082 A1	30-06-2011
		US 2011158407 A1	30-06-2011
		US 2011161650 A1	30-06-2011