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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2016 (15.12.2016)

WIPO | PCT

(10) International Publication Number
WO 2016/200523 A1

(51) International Patent Classification:
*G06F 21/32* (2013.01) *G06F 21/72* (2013.01)
*G06F 21/62* (2013.01)

(21) International Application Number:
PCT/US2016/031433

(22) International Filing Date:
9 May 2016 (09.05.2016)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
14/734,710 9 June 2015 (09.06.2015) US

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

(72) Inventors: **BALI, Niraj**; 260 Tuolumne Drive, Freemont, California 94539 (US). **DWARAKANATH, Kumar N.**; 421 Porter Road, Folsom, California 95630 (US). **HASKEL, Asaf**; 6 Hamarpe Street, 97774 Jerusalem (IL). **IOSAD, Gennadi**; 5, Ha-Rav Avraham Mordechai Weingarten, 9313105 Jerusalem (IL). **JAYASANKARAN, Anoop K.**; 1055 E Eveyln Ave., Apt. 51, Sunnyvale, California 94086 (US). **MOORE, Victoria C.**; 2002 E. Granite View Drive, Phoenix, Arizona 85048 (US). **NAYAGAM, Vinod Gomathi**; 4169 Blackford Circle, San Jose, California 95117 (US). **ZAHAVI, David**; 19 Eretz Binyamin St., 90618 kfar Adumim (IL).

(74) Agent: **MALONEY, Neil F.**; Finch & Maloney PLLC, c/o CPA Global, P.O. Box 52050, Minneapolis, Minnesota 55402 (US).

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

*[Continued on next page]*

(54) Title: SECURE BIOMETRIC DATA CAPTURE, PROCESSING AND MANAGEMENT

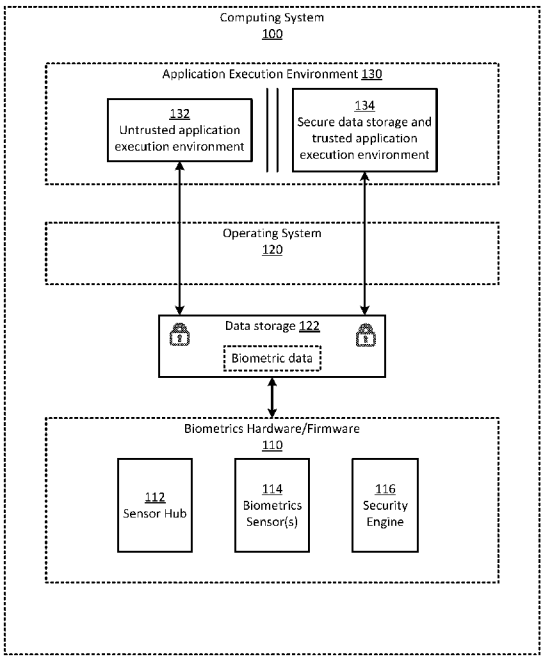


Fig. 1

(57) Abstract: A system includes one or more biometric sensors, a sensor hub and a trusted application execution environment. The sensor hub has exclusive access to the sensors and also isolates untrusted/unauthenticated portions of the operating system from direct access to unencrypted biometric data acquired by the sensors. During a biometric scan/collection process, only the sensor hub and a security engine can access the sensors and a storage component. The sensor hub reads the sensors to obtain the biometric data associated with the scan/collection process and stores the biometric data in the storage component. The security engine encrypts the biometric data before the sensor hub removes the access restrictions. Various components transfer the encrypted biometric data from the storage component to the trusted environment, which hosts algorithms for processing the biometric data.

WO 2016/200523 A1

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

**Published**:

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

# SECURE BIOMETRIC DATA CAPTURE, PROCESSING AND MANAGEMENT

## BACKGROUND

**[0001]** In the field of information security, access control includes the selective restriction of access to a protected or otherwise secure resource. Such resources may contain sensitive or confidential information. Permission to access a resource occurs upon authentication of a user's identity. Passwords, security tokens and biometrics are commonly used for such authentication. These techniques provide varying levels of security. For example, password authentication is relatively easy to implement, but passwords are easily forgotten. Further, stolen or guessed passwords permit unauthorized access to restricted resources. A security token is a type of electronic key that, when used in conjunction with a password, can provide additional security. However, unauthorized access also occurs by users who illicitly intercept security tokens. Biometrics authentication provides more security than passwords and security tokens because biometric identifiers, such as fingerprints, include distinctive and measurable physical characteristics, which are difficult to reproduce. Securing data representing biometric information reduces theft and misappropriation.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0002]** Figure 1 illustrates an example computing system configured for biometric data capture, processing and management, in accordance with an embodiment of the present disclosure.

**[0003]** Figure 2A is a flow diagram of an example methodology for biometric data capture, processing and management, in accordance with an embodiment of the present disclosure.

**[0004]** Figure 2B is a flow diagram of the example methodology of Figure 2A in further detail, in accordance with an embodiment of the present disclosure.

**[0005]** Figure 3 illustrates an example computing device configured for biometric data capture, processing and management, in accordance with an embodiment of the present disclosure.

**[0006]** Figure 4 is a flow diagram of another example methodology for biometric data capture, processing and management in a computing environment, in accordance with an embodiment of the present disclosure.

**[0007]** Figure 5 illustrates a media system configured in accordance with an embodiment of the present disclosure.

**[0008]** Figure 6 illustrates a mobile computing system configured in accordance with an embodiment of the present disclosure.

## DETAILED DESCRIPTION

**[0009]** Techniques are disclosed for biometric data capture, processing and management. In particular, according to an embodiment, a computing system, such as a smart phone, tablet or other computing device, is designed upon a framework that supports biometrics hardware, firmware, or a combination of hardware and firmware. The framework facilitates use of, among other things, an operating system, a trusted execution environment, and an untrusted execution environment. The biometrics hardware/firmware includes a sensor hub, one or more biometric sensors (e.g., fingerprint, iris, voice, to name a few), and a security engine. Each sensor captures, or scans, a biometric sample (e.g., fingerprint pattern, iris structural feature, voice pattern). Some sensors include a transducer configured to generate an electrical signal representing biometric data. The biometrics hardware/firmware includes authenticated logic or circuitry for exclusively controlling and reading the sensors, in accordance with an embodiment. In particular, the authenticated logic selectively isolates the biometrics hardware/firmware and unencrypted biometric sensor data from the remainder of the operating system and any applications, processes or components in at least the untrusted execution environment. Access to the biometric sensor(s) and the memory used to store unencrypted biometric data is limited to the sensor hub, the security engine, or both. The authenticated logic encrypts the biometric data before other components of the system transfer the data into the trusted execution environment. Further, biometric applications and data stored in the trusted execution environment are isolated from the untrusted execution environment and unauthenticated operating system processes. In this manner, only authenticated operating system processes and trusted components of the computing system

have access to the sensor(s), and at all times biometric data are either encrypted or isolated from untrusted or unauthenticated components of the computing system. Numerous variations and configurations will be apparent in light of this disclosure.

General Overview

**[0010]** Challenge-response authentication is a computer security technique in which user identity authentication occurs when the user provides a valid answer (response) to a question (challenge) posed by an authentication authority. Passwords, security tokens and biometric fingerprints are several forms of challenge-response authentication. While passwords are easily implemented, they are also easily forgotten, stolen or otherwise compromised. Likewise, security tokens are easily lost or stolen. In contrast to passwords and security tokens, biometric information is an intrinsic characteristic that is unique to each individual. As such, users cannot lose, forget or easily steal biometrics, as is the case with passwords, security tokens and other forms of challenge-response authentication. However, once collected, biometric information in electronic form must be secured to prevent unauthorized tampering, interception or theft. For instance, an unauthorized user can obtain an insecurely stored fingerprint scan, and use it for an attack in which the unauthorized user spoofs or otherwise imitates the identity of an authorized user to gain illegitimate access to a protected resource. Further, illegitimate algorithms configured to access and manipulate the fingerprint scan data can override biometric data processing algorithms, which compromises the security the biometrics authentication intends to provide.

**[0011]** Thus, the present disclosure provides a new technique for secure biometric data capture, processing and management, in accordance with various embodiments. In an embodiment, a computing system includes one or more biometric fingerprint sensors, a sensor hub, an untrusted application execution environment and a trusted application execution environment. The sensor hub has exclusive access to the sensors and also isolates untrusted or unauthenticated portions of the operating system, and other processes executing on the computing system, from direct access to unencrypted biometric data acquired by the sensors. In particular, during a fingerprint scan, the sensor hub prohibits access to the fingerprint sensors from other components of the system. The sensor hub reads the sensors to obtain the biometric data associated with the fingerprint scan and stores the biometric data in a data storage component, such as a memory stack or register. Only the sensor hub and the security engine can access the data storage component. In some embodiments, the security engine encrypts the biometric data stored in the data storage component before the sensor hub

removes the data storage and sensor access restrictions. In some embodiments, the security engine processes the biometric data associated with the fingerprint scan and transfers a verifiable result to the trusted application execution environment for additional authorization processing. Various components of the system (e.g., a native library component) can subsequently transfer the encrypted biometric data from the memory storage component to the trusted and secure application execution environment. The trusted environment hosts algorithms for processing the biometric data. Further, processes executing outside of the trusted application execution environment cannot access the biometric data or the algorithms in the trusted application execution environment. While a fingerprint sensor is used in this example embodiment, other embodiments may employ other biometric sensors or any combination of such sensors and still operate in accordance with the techniques provided herein, as will be apparent in light of this disclosure.

**[0012]** As used in this disclosure, the term "biometrics" refers to a measureable biological characteristic and a process for recognizing an individual possessing the biological characteristic. The biological characteristic is, in some cases, anatomical or physiological, including fingerprints, palm features (e.g., veins), face features, DNA, signatures, voice features, hand features (e.g., geometry), iris structure, retina features, and scent details, to name a few examples. Any such characteristics can be generally captured in the form of a biometric sample or data captured by a biometric sensor. The recognition process can include processing biometric data representing the biological characteristic to identify, and verify the identity of, an individual.

**[0013]** As used in this disclosure, the term "biometrics sensor" refers to a device configured to acquire the data needed for biometrics recognition and verification. Such devices may include, for example, fingerprint sensors, retina and iris sensors, cameras, microphones, and other such tools capable of collecting biometrics. For example, a fingerprint sensor may incorporate feature detection technologies such as optical fingerprint imaging, ultrasonic imaging, and capacitance imaging to capture details of a person's fingerprints. An iris recognition sensor may incorporate video camera technology with near infrared illumination to capture images of a person's iris structure. A face recognition sensor may incorporate high resolution video camera technology (e.g., pixel resolution, spatial resolution, spectral resolution, temporal resolution, and radiometric resolution) to capture high resolution images of a person's distinctive facial features. A voice recognition sensor may include a microphone and possibly one or more audio filters, to capture a person's

speech patterns. In some embodiments, a combination of such sensors may be used, to further increase security. In some embodiments, a sensor includes a transducer configured to generate an electrical signal representing biometric data.

**[0014]** As used in this disclosure, the term "biometric template" refers to a digital representation of one or more biometric samples. For example, a fingerprint scan obtained using a fingerprint sensor may be converted into a biometric template that uniquely corresponds to a particular individual's fingerprint. Various models and algorithms generate the biometric template and compare previously stored templates against candidate fingerprints for authentication purposes. For example, an image- or pattern-based algorithm may generate a template or compare two or more templates containing the type, size, shape and orientation of patterns that form the fingerprint.

**[0015]** As used in this disclosure, the terms "biometric verification" and "biometric authentication" refer to a process for confirming the identity of an individual by acquiring a biometric sample, such as a fingerprint scan or a voice scan or a face scan or an iris scan, and comparing the captured sample against a previously validated sample enrolled in a database. Verification or authentication results when a match between the samples occurs. A validated sample is one which has been vetted by a trusted party or otherwise considered authentic and valid by a security authority responsible for performing the verification or authentication process.

**[0016]** As used in this disclosure, the term "biometric identification" refers to a process for determining the identity of an individual by comparing a biometric sample, such as a fingerprint scan or a voice scan or a face scan or an iris scan, against one or more samples in a database to obtain a match. While in some cases verification and authentication may include identification, identification does not necessarily include a comparison with validated samples (e.g., identification may not lead to authentication).

Example System

**[0017]** Figure 1 illustrates an example computing system 100 configured for biometric data capture, processing and management, in accordance with an embodiment. The system 100 may be implemented, for example, in a smart phone, tablet computer, mobile device, desktop device, or any other suitable computing device. The system 100 generally includes a biometrics component 110, an operating system 120, and an application execution environment 130. The biometrics component 110 may include, for example, hardware,

firmware, or both (e.g., embedded code that is accessible and executable by one or more local processors of the system).

**[0018]** The biometrics component 110 includes a sensor hub 112, one or more biometrics sensors 114 (e.g., a fingerprint sensor), and a security engine 116. The sensor hub 112 includes circuitry and logic for interfacing other portions of the computing system 100 (e.g., via the operating system 120) with the biometrics sensor 114. The sensor hub 112 further includes circuitry and logic for controlling and capturing biometric samples from the biometrics sensor 114. The biometrics component 110 can operatively isolate the biometrics sensors 114 from direct access by the operating system 120 and the application execution environment 130. For example, the sensor hub 112 may include a common bus interface for communicating with the biometrics sensors 114. Examples of such a common bus interface include a serial peripheral interface (SPI) and an SPI controller (e.g., SSP6), $I^2C$ (inter-integrated circuit), universal asynchronous receiver/transmitter (UART) and Mobile Industry Processor Interface (MIPI). Examples of fingerprint biometrics sensors include, but are not limited to, capacitive sensors (Fingerprint Card 1020 Family, Synaptics 5100 family), optical (OxiTechnology all families of sensors, Authentic), and ultrasonic (UltraScan and Sonavation all families of sensors). As noted above, any of these sensors can include a transducer configured to generate an electrical signal representing biometric data. The security engine 116 may include any type of hardware or software-based security engine that provides cryptographic functionality in a secure execution environment. For example, the security engine 116 may implement defined security schemes to provide encryption and decryption capabilities for data acquired by the sensor hub 112, such as biometric data representing a fingerprint scan, and various other components of the system 100, as will be apparent in view of this disclosure.

**[0019]** The operating system 120 includes a data storage 122 (e.g., random-access memory, a data stack, or other data register). The biometrics component 110 has direct access to the data storage 122. The data storage 124 provides memory for storing biometric data received from the sensor hub 112. For example, the data storage 124 may temporarily store data representing a fingerprint scan before transfer of the data to the application execution environment 130 occurs. Further, the application execution environment 130 can access the data storage 122 via the operating system 120. However, the sensor hub 112 selectively prohibits access to the data storage from the application execution environment. For example, the sensor hub 112 may prohibit, in response to a request from the application

execution environment 130 to capture a biometric sample, access to the data storage 122 from the application execution environment 130, either directly or via the operating system 120. This, in combination with the operatively isolated biometrics component 110, serves to protect unencrypted biometric data obtained from a biometric sample from read and write access by other portions of the computing system 100, including the operating system 120 and the application execution environment 130. The security engine 116 may, for example, encrypt the biometric data. Once the biometric data is encrypted, the sensor hub 112 allows access to the data storage 122 from the operating system 120 and the application execution environment 130.

**[0020]** The application execution environment 130 includes an untrusted application execution environment 132 and a trusted application execution environment 134. The untrusted application execution environment 132 includes additional data storage that is not necessarily secure or otherwise protected from access by any process executing on the computing system 100. For example, trusted or untrusted processes executing on the computing system 100 may access data stored in the untrusted application execution environment 132. Data stored or applications executing in the untrusted application execution environment 132 may include, for example, computer viruses or malicious content. Further, unauthorized or unauthenticated users, devices or applications may access or modify data and applications in the untrusted application execution environment 132. Thus, for certain purposes, such as protecting confidential information from theft or misuse, the untrusted application execution environment 132 may not be suitable for storing or processing the biometric data.

**[0021]** By contrast, the trusted application execution environment 134 includes data storage that is isolated from memory used by unauthorized or unauthenticated processes executing outside of the trusted application execution environment 134. Further, processes executing in the trusted application execution environment 134 have exclusive access to the data stored therein, to the exclusion of all processes executing outside of the trusted application execution environment 134. In this manner, the trusted application execution environment 134 securely quarantines certain data, including biometric data, stored therein from processes executing outside of the trusted application execution environment 134 (e.g., in the operating system 120 or the untrusted application execution environment 132). In some embodiments, the memory or other data storage elements forming portions of the untrusted application execution environment 132 can be physically separate from, or integrated with, the memory

or other data storage elements forming portions of the trusted application execution environment 134, depending on the application. Further, in some cases, hardware (e.g., separate data buses, non-shared memory), firmware or software (e.g., segmentation, process isolation, virtual addressing, protection keys, privileges and permissions, address masks, etc.) can isolate one memory region of the system 100 from another.

Example Methodology

**[0022]** Figure 2A is a flow diagram of an example methodology for biometric data capture, processing and management, in accordance with an embodiment. Figure 2B is a flow diagram of the example methodology of Figure 2A in further detail, in accordance with an embodiment. An untrusted application 202 executes in a portion of a computer processing environment, such as the untrusted application execution environment 132 of Figure 1. The untrusted application 202 requests biometric authentication of a user 204. Such authentication may, for example, serve as a prerequisite for permitting the untrusted application 202 to access certain protected or secure information or perform certain functions that are restricted to authorized users. In some cases, other suitable authentication techniques, such as passwords or security tokens, may supplement biometric authentication. In response to the authentication request, a separate portion of the computer processing environment (e.g., the trusted application execution environment 134, the operating system kernel 120, the biometrics component 110, or any combination of these), which is independent of and isolated from the untrusted application 202, collects 210 biometric data (e.g., a fingerprint scan) from the user 204. Referring to Figure 2B, the secure collection of biometric data 210 can include one or more of the following: generating 212a cryptographic key, prohibiting 214 access to a data storage from the operating system, and capturing, encrypting and storing 216 biometric data in the data storage.

**[0023]** Again referring to Figure 2A, after collecting 210 the biometric data, the biometric data is transmitted 220 from one portion of the computer processing environment to another. Referring to Figure 2B, the transmission of the biometric data 220 can include one or more of the following: allowing 222 access to the data storage from the operating system, and transferring 224 the biometric data from the data storage to a trusted environment. For example, with reference to Figure 1, the biometric data may be transmitted from the biometrics component 110 to the operating system kernel 120 (e.g., the data storage 124), and further to the trusted application execution environment 134. The biometric data are

transmitted 220 securely (e.g., in an encrypted form), such that the untrusted application 202 never has access to the biometric data in an unencrypted or otherwise unsecured form.

**[0024]** Again referring to Figures 2A and 2B, processing and management 230 of the biometric data occurs in a similarly secure manner independent of and separate from the untrusted application 202. For example, decryption and processing 232 of the biometric data may occur within the trusted environment to generate a template for enrolling a fingerprint scan or for validation against a previously enrolled fingerprint scan. Any cryptographic keys used to encrypt and decrypt the biometric data are never exposed to the untrusted application 202. As such, in this example framework and methodology, the untrusted application 202 never has direct access to the biometric data in an unencrypted or otherwise unsecured form, the biometrics component, or any process or communication channel that collects, transmits, processes or manages the biometric data in an unencrypted or otherwise unsecured form.

Example Device

**[0025]** Figure 3 illustrates an example computing device 300 configured for biometric data capture, processing and management, in accordance with an embodiment. The computing device 300 includes a biometrics component 310, an operating system component 320, an untrusted environment component 330 and a trusted and secure environment component 340. The biometrics component 310 includes a sensor hub 312, one or more biometric fingerprint sensors 314, and a security engine 316. In some cases, the sensor hub 312 and the security engine 316 have exclusive access to the biometric fingerprint sensors 314 by configuring one or more access control registers (not shown) integrated into the computing device 300. The sensor hub 312 executes one or more applications or processes. These applications or processes can execute mutually exclusively of, and in isolation from, each other (e.g., no application or process on the sensor hub 312 may be aware of the presence of another, and no application or process on the sensor hub 312 may access the data of another). For example, each application or process in the sensor hub 312 may execute in a protection ring (e.g., Ring 3) architecture. The operating system component 320 includes a sensor hub inter-process communication (IPC) component 322, a data storage component 324, a security engine interface component 326, and a biometrics driver component 328. The untrusted environment 330 includes one or more of the following: an untrusted application 332, a biometrics service 334, and a biometrics service library 336. The biometrics service 334 may, for example, provide one or more application programming interfaces (APIs) for enrolling, verifying and identifying users via the biometrics hardware/firmware 310. In some

cases, the untrusted application 332 can use any standard biometrics APIs to enroll, verify and identify users. The trusted and secure environment 340 includes one or more of the following: a trusted biometrics application 342 and a trusted biometrics service 344. In some embodiments, the sensor hub 312 may include one or more of the following: a sensor processing module 350 and a sensor interface 352.

**[0026]** The computing device 300 may be implemented in one or more mobile or desktop computing devices, such as a smart phone, tablet, desktop computer, user terminal, point-of-sale terminal, automated teller machine, vending machine, airport check-in system, embedded device controller, vehicle control system, facility access control system, or other device or system or combination of devices or systems in which biometrics are utilized for user identification and authentication.

**[0027]** In general, the computing device 300 operates in the following manner, according to an embodiment. The untrusted application 332 can include any application executing on the computing device 300 that involves biometric identification or authentication of a user. An example of such an application includes an online banking application that uses biometric information to identify and authenticate the user prior to allowing the user to perform certain financial transactions. For instance, instead of, or in addition to, logging into the banking application for a financial institution using a username and password, the untrusted application 332 obtains a fingerprint scan of the user. A comparison of biometric data obtained from the fingerprint scan to known and validated biometric data determines who the user is and whether the user is permitted to perform certain functions, such as checking an account balance, withdrawing or transferring funds, making a purchase, and other types of transactions that are available only to users authorized by the financial institution. Other examples of applications where biometric-based security can be used will be apparent in light of this disclosure.

**[0028]** The device 300 does not permit applications or other processes executing in the untrusted environment 330, including the untrusted application 332, to directly access sensitive data that unauthorized users could exploit for improper purposes or otherwise misuse. As such, the device 300 does not permit the untrusted application 332 to access or otherwise intercept or manipulate biometric data, at least in an unencrypted form. Instead, the untrusted application 332 achieves biometric-based identification or authorization indirectly via a request sent to other components of the computing device 300, including but not limited to the trusted biometrics application 342, the data storage component 324, and the

biometrics component 310. In accordance with various embodiments, such other components are designed to maintain the integrity and security of biometric data, and further designed to isolate the biometrics component 310 and data storage 324 from the untrusted environment. The request may include, for example, a request to enroll a new fingerprint scan into a database or to authenticate a new fingerprint scan against a previously enrolled fingerprint scan, and to return a result of such enrollment or authentication, such as "succeed" or "fail." In some cases, the biometrics service 334 provides one or more APIs that facilitate submission of the request from the untrusted application 332 to various other components of the computing device 300, such as the sensor hub IPC 322.

**[0029]** In response to receiving a biometrics request from the untrusted application 332, the driver 328 sends a command to the trusted biometrics application 342 via the trusted biometrics service 344 to generate a cryptographic key for encrypting biometric data captured from the biometric fingerprint sensor 314. The trusted biometrics application 342 generates the cryptographic key and supplies the key to the security engine 316 via the security engine interface 326. Additionally, in response to receiving a biometrics request, the sensor hub IPC 322 sends a command to the sensor hub 312 and the fingerprint sensor 314 to capture a biometric sample. The data storage 324 is shared between the operating system 320, the sensor hub 312 and the security engine 326. The sensor hub 312 locks the data storage 324 before capturing the biometric sample to prohibit the operating system 320 from accessing the data storage 324. Next, the sensor processing module 350 uses the sensor interface 352 to acquire raw biometric data representing the biometric sample, and stores the raw biometric data in the data storage 324. The sensor processing module 350 calls the security engine 326 to encrypt the raw biometric data using the cryptographic key before sending the biometric data to the operating system 320. The sensor hub 312 unlocks access to the data storage 324 once the biometric data stored in the data storage has been encrypted.

**[0030]** Next, the sensor hub IPC 322 collects the encrypted biometric data from the data storage 324 and copies it to a buffer in the untrusted environment 330. The biometrics service library 336 then transfers the encrypted biometric data to the trusted and secure environment 340. Upon receiving the encrypted biometric data, the trusted biometrics application 342 decrypts the data using the same cryptographic key used by the security engine 316 to encrypt the biometric data. The trusted biometrics application 342 checks the biometric data for integrity and validity, pre-processes the data, extracts a biometric template, and stores the template in an encrypted form or compares the template against a previously

enrolled template. All of these functions are performed within the trusted and secure environment 340, which ensures the security of the biometric data and the templates against access from the untrusted environment 330 or the operating system 320. Another example of the operation and use of the computing device 300 is provided in further detail with respect to Figure 4.

Example Methodology

**[0031]** Figure 4 is a flow diagram of another example methodology for biometric data capture, processing and management in a computing environment, in accordance with an embodiment. For clarity, in Figure 4, various steps of the example methodology are defined with respect to the various components of the computing device of Figure 2. However, some or all of these steps may be performed by components that are different than those expressly referenced in this example embodiment, including components that are combinations of separately described components, components that are subsets of individually described components, components that are remote from the computing environment (e.g., a client-server scheme), or components located in separate computing environments or separate portions of a computing environment. Furthermore, performance of one or more of these steps may occur in different sequences than those expressly described in this example embodiment, or omitted entirely. Accordingly, the example flow diagram of Figure 4 only provides a general overview of one example methodology, and does not limit the scope of various other embodiments.

**[0032]** Generally, during a biometrics authentication session, the example methodology includes one or more of the following actions: generating a cryptographic key for encrypting and decrypting biometric data, restricting biometrics hardware/firmware access to certain components in the computing environment, capturing biometric data (e.g., a fingerprint scan), encrypting and transferring the biometric data to a trusted environment, and further processing and storing the biometric data in the trusted environment. The example methodology can further include reporting the result of such processing to applications executing in the untrusted environment. For example, the result of a fingerprint scan enrollment or authentication may be reported to an untrusted application as a success or failure. In turn, the example methodology may grant or deny access by the untrusted application to a protected resource based on the result.

**[0033]** In further detail, initially, an untrusted application, which may execute in an untrusted environment, issues 402 a biometrics authentication request. Such a request may

issue, for example, when the untrusted application needs to obtain authentication of a user for accessing a protected resource (e.g., data, services or applications) owned by the user or otherwise protected from unauthorized access on behalf of the user. Any application executing in the computing environment may issue a biometrics authentication request. Such applications are not limited to those executing in an untrusted environment and may include applications or other processes executing in other portions of the computing environment or in separate computing environments, including the trusted environment, the operating system kernel and any hardware or firmware. An untrusted biometrics service executing in the untrusted environment receives the biometrics authentication request. The untrusted biometrics service instantiates 404 a biometrics authentication session in which biometric data is captured, transmitted, processed, or managed. The biometrics authentication session may include one or more of the actions described with respect to Figure 4. In response to instantiation of the biometrics authentication session, the untrusted biometrics service calls 406 a trusted biometrics application. The trusted biometrics application executes in a trusted environment, which may include isolated memory regions or other data storage components to which access is restricted to components executing in the trusted environment.

**[0034]** In response to receiving the call from the untrusted biometrics service, the trusted biometric application generates a cryptographic key 408 via a trusted biometrics service, also within the trusted environment. The trusted biometrics service may operate in conjunction with a security engine to generate the cryptographic key. For example, the trusted biometrics service may call the security engine requesting the cryptographic key, and the security engine may generate the cryptographic key on behalf of the trusted biometrics service and return the cryptographic key to the trusted biometrics service using a secure or dedicated communication channel. The security engine may also share the cryptographic key with, for example, the sensor hub.

**[0035]** Prior to scanning a fingerprint, access to a data storage component, such as a kernel stack, is restricted to a sensor hub, a security engine, or both 410 in the hardware/firmware of the computing environment. As a result, access to the kernel stack from the untrusted environment is not permitted. Access to the kernel stack is restricted so as to prevent untrusted or unauthenticated applications or components in the computing environment from gaining access to any unencrypted or otherwise unsecured biometric data acquired during the biometrics authentication session. After kernel stack access has been so restricted, biometric data is captured 412 from a fingerprint sensor and placed 414 on the kernel stack. In some

cases, the captured biometrics sensor data can additionally or alternatively be stored in other data storage components within the hardware/firmware, kernel or trusted environment for which access is suitably restricted to authenticated or trusted components in the computing environment.

**[0036]** The sensor hub or the security engine encrypts 416 the biometric data using the cryptographic key while the biometric data resides on the kernel stack and while access to the kernel stack is restricted to the sensor hub, the security engine, or both. Subsequent to encrypting the biometric data, the sensor hub removes 418 the kernel stack access restriction, which allows access to the kernel stack from the application execution environment. The biometrics service library transfers 420 the encrypted biometric data to a trusted and secure environment, which is not directly accessible by the operating system or other untrusted processes and components of the computing environment.

**[0037]** Once the encrypted biometric data is transferred to the trusted environment, a trusted biometrics application decrypts 422 the encrypted biometric data using the cryptographic key and further processes 424 the biometric data. Such further processing may include, for example, generating a biometric template corresponding to the biometric data (e.g., fingerprint scan) or making additional authorization decisions based on the processed data received. A biometric template based on the biometrics sensor data may be stored in the trusted environment for future use during biometric validation, authentication or identification, as needed. The trusted environment provides secure data storage for the biometric template by ensuring that applications, processes or components outside of the trusted environment have no access to the biometric template. Isolated, protected or encrypted memory regions may, for example, provide secure storage of biometric data and templates. The trusted biometrics application enrolls or authenticates 426 the biometric template. For example, if a biometric sample is obtained from an individual for the first time, the resulting biometric template may be enrolled in a database for comparison with subsequently obtained samples. On the other hand, if a validated biometric template is already enrolled, the biometric template may be used for verification or authentication against the enrolled template. The untrusted application is subsequently notified of the result of the enrollment or authentication 430. For example, if the authentication results in a match between an enrolled biometric template and the current biometric template, the untrusted application may be notified that the user is authorized to access the protected resource. In some cases, the notification may include a security token or other information that the

untrusted application can use to access the protected resource. Subsequent to the notification 430, the biometrics authentication session may end, and the untrusted application notifies 432 the user of the result. In some cases, the example methodology includes notifying the user of the untrusted application of the result of the biometric authentication (e.g., via a "pass" or "fail" message or other indication). This example methodology may be repeated each time any application executing in the computing environment requests biometrics authentication.

Example System

**[0038]** Figure 5 illustrates an example system 500 that may carry out techniques for biometric data capture, processing and management, in accordance with an embodiment. In some embodiments, system 500 may be a media system although system 500 is not limited to this context. For example, system 500 may be incorporated into a personal computer (PC), laptop computer, ultra-laptop computer, tablet, touch pad, portable computer, handheld computer, palmtop computer, personal digital assistant (PDA), cellular telephone, combination cellular telephone/PDA, television, smart device (e.g., smart phone, smart tablet or smart television), mobile internet device (MID), messaging device, data communication device, set-top box, game console, or other such computing environments capable of performing graphics rendering operations.

**[0039]** In some embodiments, system 500 includes a platform 502 coupled to a display 520. Platform 502 may receive content from a content device such as content services device(s) 530 or content delivery device(s) 540 or other similar content sources. A navigation controller 550 comprising one or more navigation features may be used to interact with, for example, platform 502 and/or display 520. Each of these example components is described in more detail below.

**[0040]** In some embodiments, platform 502 includes any combination of a chipset 505, processor 510, memory 512, storage 514, graphics subsystem 515, applications 516 and/or radio 518. Chipset 505 provides intercommunication among processor 510, memory 512, storage 514, graphics subsystem 515, applications 516 and/or radio 518. For example, chipset 505 may include a storage adapter (not depicted) capable of providing intercommunication with storage 514.

**[0041]** Processor 510 may be implemented, for example, as Complex Instruction Set Computer (CISC) or Reduced Instruction Set Computer (RISC) processors, x86 instruction set compatible processors, multi-core, or any other microprocessor or central processing unit

(CPU). In some embodiments, processor 510 includes dual-core processor(s), dual-core mobile processor(s), and so forth. Memory 612 may be implemented, for instance, as a volatile memory device such as, but not limited to, a Random Access Memory (RAM), Dynamic Random Access Memory (DRAM), or Static RAM (SRAM). Storage 514 may be implemented, for example, as a non-volatile storage device such as, but not limited to, a magnetic disk drive, optical disk drive, tape drive, an internal storage device, an attached storage device, flash memory, battery backed-up SDRAM (synchronous DRAM), and/or a network accessible storage device. In some embodiments, storage 514 includes technology to increase the storage performance enhanced protection for valuable digital media when multiple hard drives are included, for example.

**[0042]** Graphics subsystem 515 may perform processing of images such as still or video for display. Graphics subsystem 515 may be a graphics processing unit (GPU) or a visual processing unit (VPU), for example. An analog or digital interface may be used to communicatively couple graphics subsystem 515 and display 520. For example, the interface may be any of a High-Definition Multimedia Interface, DisplayPort, wireless HDMI, and/or wireless HD compliant techniques. Graphics subsystem 515 can be integrated into processor 510 or chipset 505. Graphics subsystem 515 can be a stand-alone card communicatively coupled to chipset 505. The graphics and/or video processing techniques described herein may be implemented in various hardware architectures. For example, hardware assisted privilege access violation check functionality as provided herein may be integrated within a graphics and/or video chipset. Alternatively, a discrete security processor may be used. In still another embodiment, the graphics and/or video functions including hardware assist for privilege access violation checks may be implemented by a general purpose processor, including a multi-core processor.

**[0043]** Radio 518 can include one or more radios capable of transmitting and receiving signals using various suitable wireless communications techniques. Such techniques may involve communications across one or more wireless networks. Exemplary wireless networks include (but are not limited to) wireless local area networks (WLANs), wireless personal area networks (WPANs), wireless metropolitan area network (WMANs), cellular networks, and satellite networks. In communicating across such networks, radio 618 may operate in accordance with one or more applicable standards in any version.

**[0044]** In some embodiments, display 520 includes any television or computer type monitor or display. Display 520 may comprise, for example, a liquid crystal display (LCD)

screen, electrophoretic display (EPD or liquid paper display, flat panel display, touch screen display, television-like device, and/or a television. Display 520 can be digital and/or analog. In some embodiments, display 520 is a holographic or three-dimensional display. Also, display 520 can be a transparent surface that may receive a visual projection. Such projections may convey various forms of information, images, and/or objects. For example, such projections may be a visual overlay for a mobile augmented reality (MAR) application. Under the control of one or more software applications 516, platform 502 can display a user interface 522 on display 620.

**[0045]** In some embodiments, content services device(s) 530 can be hosted by any national, international and/or independent service and thus accessible to platform 502 via the Internet or other network, for example. Content services device(s) 530 can be coupled to platform 502 and/or to display 520. Platform 502 and/or content services device(s) 630 can be coupled to a network 560 to communicate (e.g., send and/or receive) media information to and from network 560. Content delivery device(s) 540 can be coupled to platform 502 and/or to display 520. In some embodiments, content services device(s) 530 includes a cable television box, personal computer, network, telephone, Internet enabled devices or appliance capable of delivering digital information and/or content, and any other similar device capable of unidirectionally or bidirectionally communicating content between content providers and platform 502 and/display 520, via network 560 or directly. It will be appreciated that the content may be communicated unidirectionally and/or bidirectionally to and from any one of the components in system 500 and a content provider via network 560. Examples of content may include any media information including, for example, video, music, graphics, text, medical and gaming content, and so forth.

**[0046]** Content services device(s) 530 receives content such as cable television programming including media information, digital information, and/or other content. Examples of content providers may include any cable or satellite television or radio or Internet content providers. The provided examples are not intended to limit the scope of the present disclosure. In some embodiments, platform 502 receives control signals from navigation controller 550 having one or more navigation features. The navigation features of controller 550 may be used to interact with user interface 522, for example. In some embodiments, navigation controller 550 can be a pointing device that may be a computer hardware component (specifically human interface device) that allows a user to input spatial (e.g., continuous and multi-dimensional) data into a computer. Many systems such as

graphical user interfaces (GUI), and televisions and monitors allow the user to control and provide data to the computer or television using physical gestures.

**[0047]** Movements of the navigation features of controller 550 can be echoed on a display (e.g., display 520) by movements of a pointer, cursor, focus ring, or other visual indicators displayed on the display. For example, under the control of software applications 516, the navigation features located on navigation controller 550 may be mapped to virtual navigation features displayed on user interface 522. In some embodiments, controller 550 is not a separate component but rather is integrated into platform 502 and/or display 520.

**[0048]** In some embodiments, drivers (not shown) include technology to enable users to instantly turn on and off platform 502 like a television with the touch of a button after initial boot-up, when enabled, for example. Program logic may allow platform 502 to stream content to media adaptors or other content services device(s) 530 or content delivery device(s) 540 when the platform is turned "off." In addition, chip set 505 may comprise hardware and/or software support for 5.1 surround sound audio and/or high definition 7.1 surround sound audio, for example. Drivers may include a graphics driver for integrated graphics platforms. In some embodiments, the graphics driver includes a peripheral component interconnect (PCI) express graphics card.

**[0049]** In various embodiments, any one or more of the components shown in system 500 can be integrated. For example, platform 502 and content services device(s) 530 may be integrated, or platform 502 and content delivery device(s) 540 may be integrated, or platform 502, content services device(s) 530, and content delivery device(s) 540 may be integrated, for example. In various embodiments, platform 502 and display 520 may be an integrated unit. Display 520 and content service device(s) 530 may be integrated, or display 520 and content delivery device(s) 540 may be integrated, for example. These examples are not meant to limit the scope of the present disclosure.

**[0050]** In various embodiments, system 500 can be implemented as a wireless system, a wired system, or a combination of both. When implemented as a wireless system, system 500 may include components and interfaces suitable for communicating over a wireless shared media, such as one or more antennas, transmitters, receivers, transceivers, amplifiers, filters, control logic, and so forth. An example of wireless shared media may include portions of a wireless spectrum, such as the RF spectrum and so forth. When implemented as a wired system, system 500 can include components and interfaces suitable for communicating over wired communications media, such as input/output (I/O) adapters,

physical connectors to connect the I/O adapter with a corresponding wired communications medium, a network interface card (NIC), disc controller, video controller, audio controller, and so forth. Examples of wired communications media include a wire, cable, metal leads, printed circuit board (PCB), backplane, switch fabric, semiconductor material, twisted-pair wire, co-axial cable, fiber optics, and so forth.

**[0051]** Platform 502 can establish one or more logical or physical channels to communicate information. The information may include media information and control information. Media information refers to any data representing content meant for consumption by a user. Examples of content include, for example, data from a voice conversation, videoconference, streaming video, email or text messages, voice mail message, alphanumeric symbols, graphics, image, video, text and so forth. Control information refers to any data representing commands, instructions or control words meant for used by an automated system. For example, control information may be used to route media information through a system, or instruct a node to process the media information in a predetermined manner (e.g., using hardware assisted for privilege access violation checks as described herein). The embodiments, however, are not limited to the elements or context shown or described in Figure 5.

**[0052]** As described above, system 500 may be embodied in varying physical styles or form factors. Figure 6 illustrates embodiments of a small form factor device 600 in which system 500 may be embodied. In some embodiments, for example, device 600 may be implemented as a mobile computing device having wireless capabilities. A mobile computing device refers to any device having a processing system and a mobile power source or supply, such as one or more batteries, for example.

**[0053]** As previously described, examples of a mobile computing device include a personal computer (PC), laptop computer, ultra-laptop computer, tablet, touch pad, portable computer, handheld computer, palmtop computer, personal digital assistant (PDA), cellular telephone, combination cellular telephone/PDA, television, smart device (e.g., smart phone, smart tablet or smart television), mobile internet device (MID), messaging device, data communication device, and so forth.

**[0054]** Examples of a mobile computing device also include computers that are arranged to be worn by a person, such as a wrist computer, finger computer, ring computer, eyeglass computer, belt-clip computer, arm-band computer, shoe computers, clothing computers, and other wearable computers. In some embodiments, for example, a mobile computing device

may be implemented as a smart phone capable of executing computer applications, as well as voice communications and/or data communications. Although some embodiments are described with a mobile computing device implemented as a smart phone, it will be appreciated that other embodiments may be implemented using other wireless mobile computing devices as well.

**[0055]** As shown in Figure 6, device 600 includes a housing 602, a display 604, an input/output (I/O) device 606, and an antenna 608. Device 600 may, for example, include navigation features 612. Display 604 includes any suitable display unit for displaying information appropriate for a mobile computing device. I/O device 606 includes any suitable I/O device for entering information into a mobile computing device. Examples for I/O device 606 include an alphanumeric keyboard, a numeric keypad, a touch pad, input keys, buttons, switches, rocker switches, microphones, speakers, voice recognition device and software, and so forth. Information may be entered into device 600 by way of microphone. Such information may be digitized by a voice recognition device.

**[0056]** Various embodiments can be implemented using hardware elements, software elements, or a combination of both. Examples of hardware elements includes processors, microprocessors, circuits, circuit elements (e.g., transistors, resistors, capacitors, inductors, and so forth), integrated circuits, application specific integrated circuits (ASIC), programmable logic devices (PLD), digital signal processors (DSP), field programmable gate array (FPGA), logic gates, registers, semiconductor device, chips, microchips, chip sets, and so forth. Examples of software may include software components, programs, applications, computer programs, application programs, system programs, machine programs, operating system software, middleware, firmware, software modules, routines, subroutines, functions, methods, procedures, software interfaces, application program interfaces (API), instruction sets, computing code, computer code, code segments, computer code segments, words, values, symbols, or any combination thereof. Whether hardware elements and/or software elements are used may vary from one embodiment to the next in accordance with any number of factors, such as desired computational rate, power levels, heat tolerances, processing cycle budget, input data rates, output data rates, memory resources, data bus speeds and other design or performance constraints.

**[0057]** Some embodiments may be implemented, for example, using a machine-readable medium or article which may store an instruction or a set of instructions that, if executed by a machine, may cause the machine to perform a method and/or operations in accordance with

an embodiment of the present disclosure. Such a machine may include, for example, any suitable processing platform, computing platform, computing device, processing device, computing system, processing system, computer, processor, or the like, and may be implemented using any suitable combination of hardware and software. The machine-readable medium or article may include, for example, any suitable type of memory unit, memory device, memory article, memory medium, storage device, storage article, storage medium and/or storage unit, for example, memory, removable or non-removable media, erasable or non-erasable media, writeable or re-writeable media, digital or analog media, hard disk, floppy disk, Compact Disk Read Only Memory (CD-ROM), Compact Disk Recordable (CD-R), Compact Disk Rewriteable (CD-RW), optical disk, magnetic media, magneto-optical media, removable memory cards or disks, various types of Digital Versatile Disk (DVD), a tape, a cassette, or the like. The instructions may include any suitable type of executable code implemented using any suitable high-level, low-level, object-oriented, visual, compiled and/or interpreted programming language.

**[0058]** Unless specifically stated otherwise, it will be appreciated that terms such as "processing," "computing," "calculating," "determining," or the like, refer to the action and/or processes of a computer or computing system, or similar electronic computing device, that manipulates and/or transforms data represented as physical quantities (e.g., electronic) within the computing system's registers and/or memories into other data similarly represented as physical quantities within the computing system's memories, registers or other such information storage, transmission or displays.

Further Example Embodiments

**[0059]** The following examples pertain to further embodiments, from which numerous permutations and configurations will be apparent.

**[0060]** Example 1 is computing system including an application execution environment, an operating system, a data storage selectively accessible from the application execution environment via the operating system, and a biometrics component having direct access to the data storage. The biometrics component is configured to selectively prohibit access to the data storage from the application execution environment.

**[0061]** Example 2 includes the subject matter of Example 1, where the biometrics component comprises a biometrics sensor, and where the biometrics component is further configured to prohibit, in response to a request from the application execution environment to

capture a biometric sample, access to the data storage from the application execution environment, capture the biometric sample with the biometrics sensor to obtain biometric data, encrypt the biometric data using a cryptographic key, store the encrypted biometric data in the data storage component, and allow access to the data storage from the application execution environment via the operating system subsequent to encrypting the biometric data.

**[0062]** Example 3 includes the subject matter of any of the above examples, where the biometrics component includes a biometrics sensor and a security engine, and where the security engine is configured to encrypt biometric data obtained from the biometrics sensor. The biometric sensor may be, for example, a fingerprint sensor, microphone, camera, or any other such tool that allows a biometric sample to be captured.

**[0063]** Example 4 includes the subject matter of any of the above examples, where the application execution environment includes an untrusted application execution environment having access to the data storage via the operating system, and a trusted application execution environment having access to the data storage via the operating system.

**[0064]** Example 5 includes the subject matter of Example 4, where the untrusted application execution environment is operatively isolated from the trusted application execution environment.

**[0065]** Example 6 includes the subject matter of any of Examples 4 and 5, where the operating system is configured to transfer the encrypted biometric data from the data storage to the trusted application execution environment.

**[0066]** Example 7 includes the subject matter of any of Examples 4, 5 and 6, where the trusted application execution environment includes a biometrics application configured to enroll a user based on biometric data obtained from a biometrics sensor, authenticate the user based the biometric data, or both.

**[0067]** Example 8 includes the subject matter of any of Examples 4, 5, 6 and 7, where the trusted application execution environment includes a biometrics application configured to decrypt encrypted biometric data obtained from a biometrics sensor using a cryptographic key.

**[0068]** Example 9 includes the subject matter of any of Example 4, 5, 6, 7 and 8, where the trusted application execution environment includes a biometrics application configured to process biometric data obtained from a biometrics sensor to generate a biometric template.

**[0069]** Example 10 is a method of capturing, processing and managing biometric data in a computing system. The method includes prohibiting, in response to a request from an application execution environment of the computing system to capture a biometric sample, access to a data storage component of the computing system from the application execution environment, capturing a biometric sample with a biometrics sensor to obtain biometric data, encrypting the biometric data using a cryptographic key, storing the encrypted biometric data in the data storage component, and allowing access to the data storage component from the application execution environment subsequent to encrypting the biometric data.

**[0070]** Example 11 includes the subject matter of Example 10, where the encrypting of the biometric data is performed by a biometrics component of the computing system independently of the operating system.

**[0071]** Example 12 includes the subject matter of any of Examples 10 and 11, where the method includes transferring, via the operating system, the encrypted biometric data from the data storage component to a trusted execution environment in the application execution environment, and where an untrusted execution environment in the application execution environment is operatively isolated from the trusted execution environment.

**[0072]** Example 13 includes the subject matter of Example 12, where the method includes generating the cryptographic key within the trusted execution environment.

**[0073]** Example 14 includes the subject matter of any of Examples 12 and 13, where the method includes decrypting the encrypted biometric data using the cryptographic key within the trusted execution environment.

**[0074]** Example 15 includes the subject matter of any of Examples 12, 13 and 14, where the method includes processing the biometric data to generate a biometric template within the trusted execution environment.

**[0075]** Example 16 includes the subject matter of any of Examples 12, 13, 14 and 15, where the method includes enrolling the user, authenticating the user based on the biometric data, or both.

**[0076]** Example 17 is a non-transient computer program product having instructions encoded thereon that when executed by one or more processors cause a process to be carried out. The process includes prohibiting, in response to a request from an application execution environment of the computing system to capture a biometric sample, access to a data storage component of the computing system from the application execution environment, capturing a

biometric sample with a biometrics sensor to obtain biometric data, encrypting the biometric data using a cryptographic key, storing the encrypted biometric data in the data storage component, and allowing access to the data storage component from the application execution environment subsequent to encrypting the biometric data.

**[0077]** Example 18 includes the subject matter of Example 17, where the encrypting of the biometric data is performed by a biometrics component of the computing system independently of the operating system.

**[0078]** Example 19 includes the subject matter of any of Examples 17 and 18, where the process includes transferring, via the operating system, the encrypted biometric data from the data storage component to a trusted execution environment in the application execution environment, and where an untrusted execution environment in the application execution environment is operatively isolated from the trusted execution environment.

**[0079]** Example 20 includes the subject matter of Example 19, where the process includes generating the cryptographic key within the trusted execution environment.

**[0080]** Example 21 includes the subject matter of any of Examples 19 and 20, where the process includes decrypting the encrypted biometric data using the cryptographic key within the trusted execution environment.

**[0081]** Example 22 includes the subject matter of any of Examples 19, 20 and 21, where the process includes processing the biometric data to generate a biometric template within the trusted execution environment.

**[0082]** Example 23 includes the subject matter of any of Examples 19, 20, 21 and 22, where the process includes enrolling the user, authenticating the user based on the biometric data, or both.

**[0083]** The foregoing description of example embodiments has been presented for the purposes of illustration and description. This description is not intended to be exhaustive or to limit the present disclosure to the precise forms disclosed. Many modifications and variations are possible in light of this disclosure. This disclosure does not intend to limit the scope of the various embodiments. Future filed applications claiming priority to this application may claim the disclosed subject matter in a different manner, and may generally include any set of one or more limitations as variously disclosed or otherwise demonstrated herein.

# CLAIMS

What is claimed is:

1. A computing system, comprising:

an application execution environment;

an operating system;

a data storage selectively accessible from the application execution environment via the operating system; and

a biometrics component having direct access to the data storage, the biometrics component configured to selectively prohibit, in response to a request to capture a biometric sample, access to the data storage from the application execution environment, so that the biometric sample is securely captured.

2. The system of claim 1, wherein the biometrics component comprises a biometrics sensor, and wherein the biometrics component is further configured to:

capture the biometric sample from a sensor to obtain biometric data;

encrypt the biometric data using a cryptographic key;

store the encrypted biometric data in the data storage component; and

allow access to the data storage from the application execution environment via the operating system subsequent to encrypting the biometric data.

3. The system of claim 1, wherein the biometrics component comprises a biometrics sensor and a security engine, and wherein the security engine is configured to encrypt biometric data obtained from the biometrics sensor.

4. The system of any of claims 1-3, wherein the application execution environment comprises:

an untrusted application execution environment having access to the data storage via the operating system; and

a trusted application execution environment having access to the data storage via the operating system.

5. The system of claim 4, wherein the untrusted application execution environment is operatively isolated from the trusted application execution environment.

6. The system of claim 4, wherein the operating system is configured to transfer the encrypted biometric data from the data storage to the trusted application execution environment.

7. The system of claim 4, wherein the trusted application execution environment comprises a biometrics application configured to at least one of enroll a user based on biometric data obtained from a biometrics sensor and authenticate the user based the biometric data.

8. The system of claim 4, wherein the trusted application execution environment comprises a biometrics application configured to decrypt encrypted biometric data obtained from a biometrics sensor using a cryptographic key.

9. The system of claim 4, wherein the trusted application execution environment comprises a biometrics application configured to process biometric data obtained from a biometrics sensor to generate a biometric template.

10. A method of capturing, processing and managing biometric data in a computing system, the method comprising:

prohibiting, in response to a request from an application execution environment of the computing system to capture a biometric sample, access to a data storage component of the computing system from the application execution environment;

capturing a biometric sample from a sensor to obtain biometric data;

encrypting the biometric data using a cryptographic key;

storing the encrypted biometric data in the data storage component; and

allowing access to the data storage component from the application execution environment subsequent to encrypting the biometric data.

11. The method of claim 10, wherein the encrypting of the biometric data is performed by a biometrics component of the computing system independently of the operating system.

12. The method of claim 10 or 11, further comprising transferring, via the operating system, the encrypted biometric data from the data storage component to a trusted execution environment in the application execution environment, wherein an untrusted execution environment in the application execution environment is operatively isolated from the trusted execution environment.

13. The method of claim 12, further comprising generating the cryptographic key within the trusted execution environment.

14. The method of claim 12, further comprising decrypting the encrypted biometric data using the cryptographic key within the trusted execution environment.

15. The method of claim 12, further comprising processing the biometric data to generate a biometric template within the trusted execution environment.

16. The method of claim 12, further comprising at least one of enrolling the user and authenticating the user based on the biometric data.

17. A non-transient computer program product having instructions encoded thereon that when executed by one or more processors cause a process to be carried out, the process comprising:

prohibiting, in response to a request to capture a biometric sample, access to a data storage component of the computing system;

capturing a biometric sample from a sensor to obtain biometric data;

encrypting the biometric data using a cryptographic key;

storing the encrypted biometric data in the data storage component; and

allowing access to the data storage component from an application execution environment only subsequent to encrypting the biometric data.

18. The computer program product of claim 17, wherein the process further comprises transferring, via the operating system, the encrypted biometric data from the data storage component to a trusted execution environment in the application execution environment, wherein an untrusted execution environment in the application execution environment is operatively isolated from the trusted execution environment.

19. The computer program product of claim 17, wherein the process further comprises generating the cryptographic key within the trusted execution environment.

20. The computer program product of claim 17, wherein the process further comprises decrypting the encrypted biometric data using the cryptographic key within the trusted execution environment.

21. The computer program product of claim 17, wherein the process further comprises processing the biometric data to generate a biometric template within the trusted execution environment.

22. The computer program product of any of claims 17-21, wherein the process further comprises at least one of enrolling the user and authenticating the user based on the biometric data.

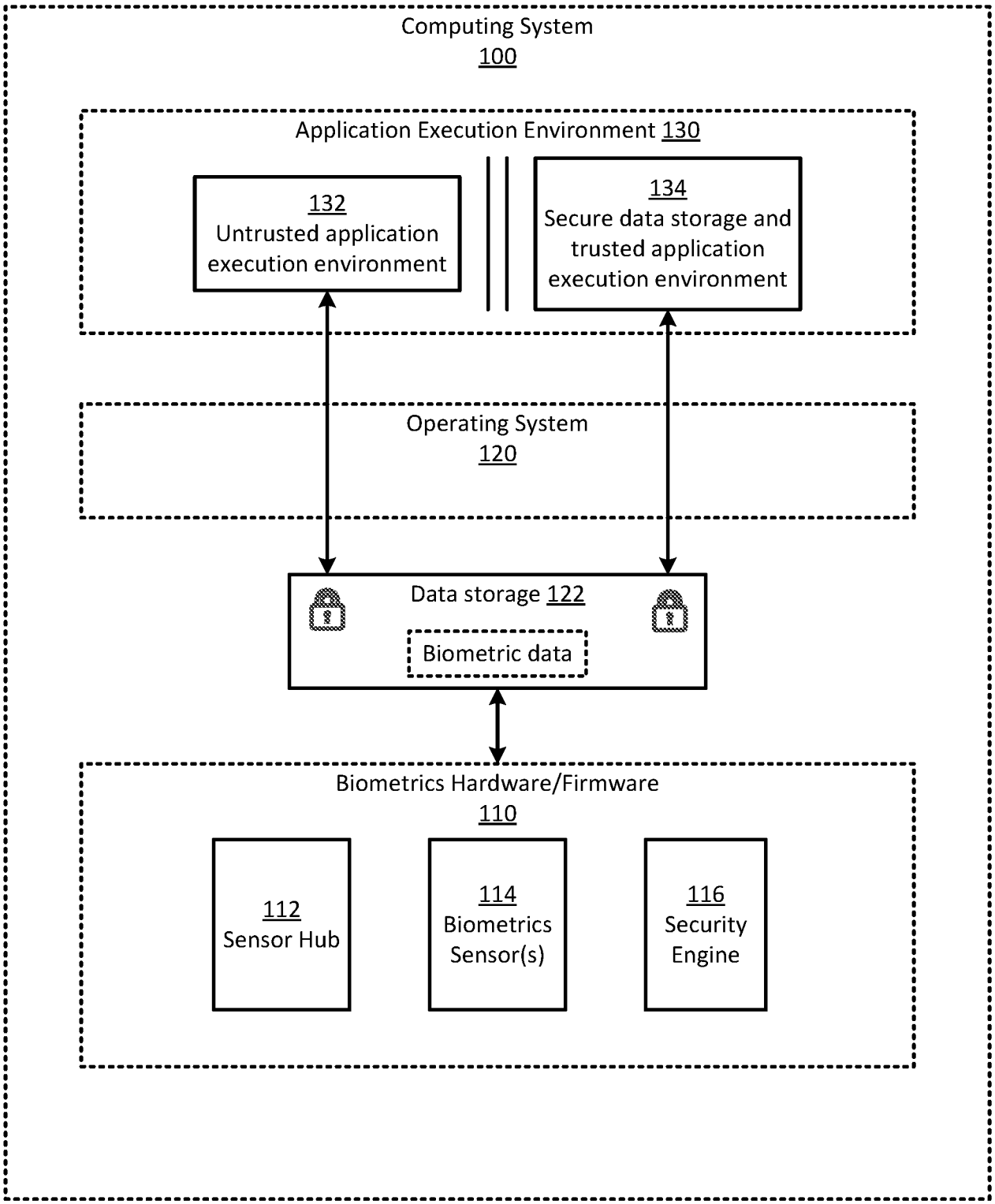
Computing System
100
Application Execution Environment 130
132
Untrusted application execution environment
134
Secure data storage and trusted application execution environment
Operating System
120
Data storage 122
Biometric data
Biometrics Hardware/Firmware
110
112
Sensor Hub
114
Biometrics Sensor(s)
116
Security Engine

Fig. 1

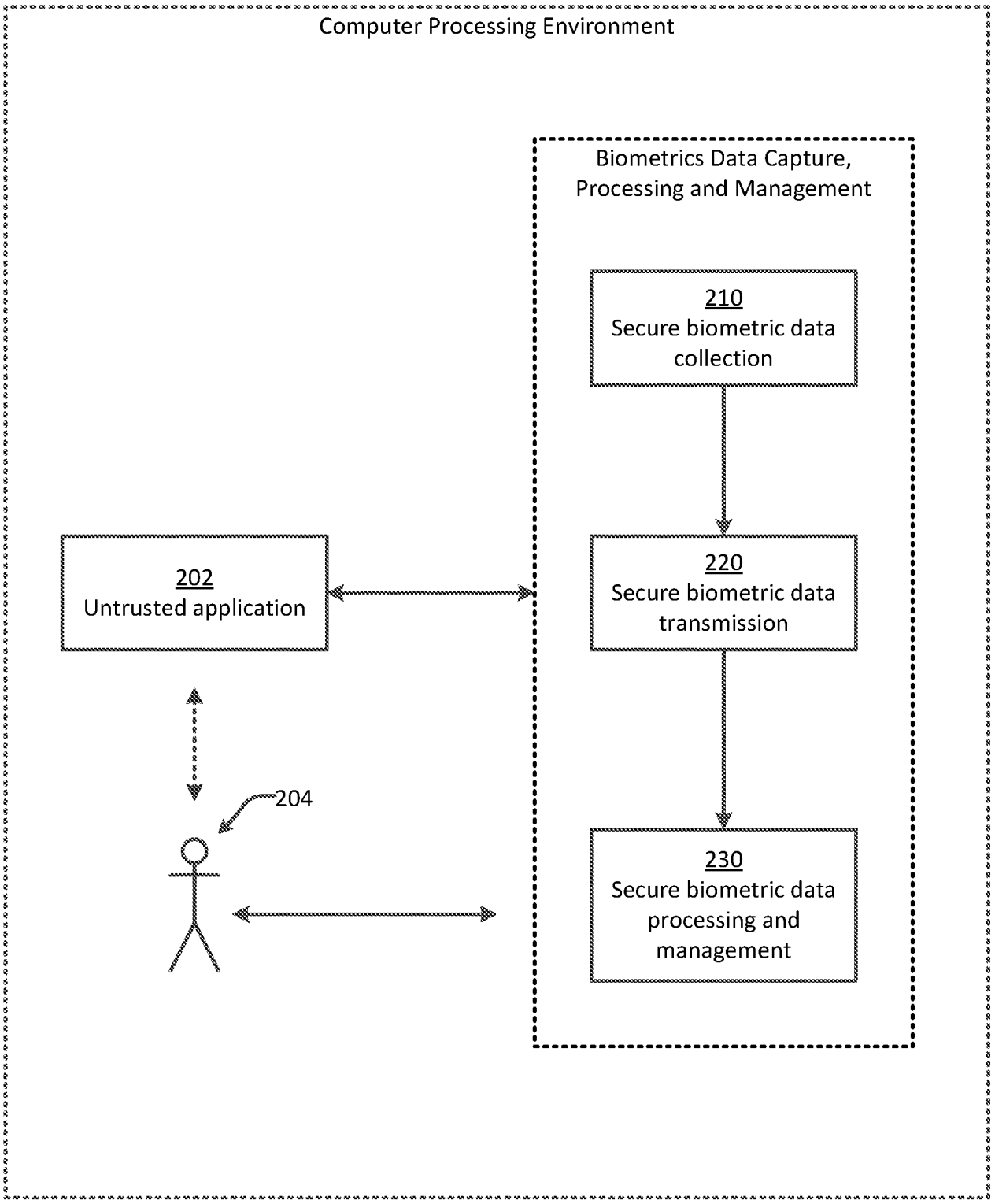
Computer Processing Environment
Biometrics Data Capture, Processing and Management
210
Secure biometric data collection
220
Secure biometric data transmission
230
Secure biometric data processing and management
202
Untrusted application
204

Fig. 2A

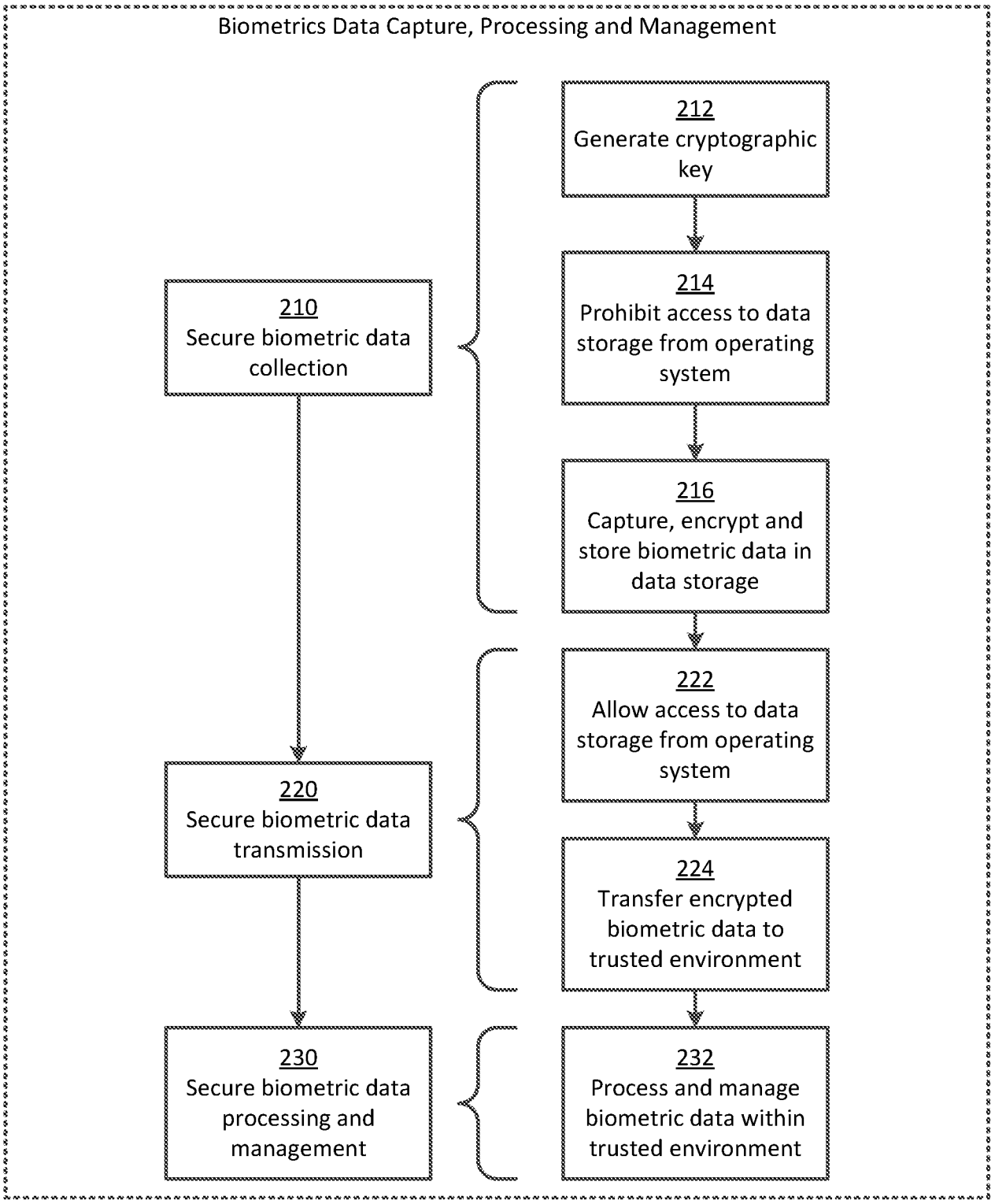
Biometrics Data Capture, Processing and Management
212
Generate cryptographic key
214
Prohibit access to data storage from operating system
216
Capture, encrypt and store biometric data in data storage
210
Secure biometric data collection
222
Allow access to data storage from operating system
220
Secure biometric data transmission
224
Transfer encrypted biometric data to trusted environment
230
Secure biometric data processing and management
232
Process and manage biometric data within trusted environment

Fig. 2B

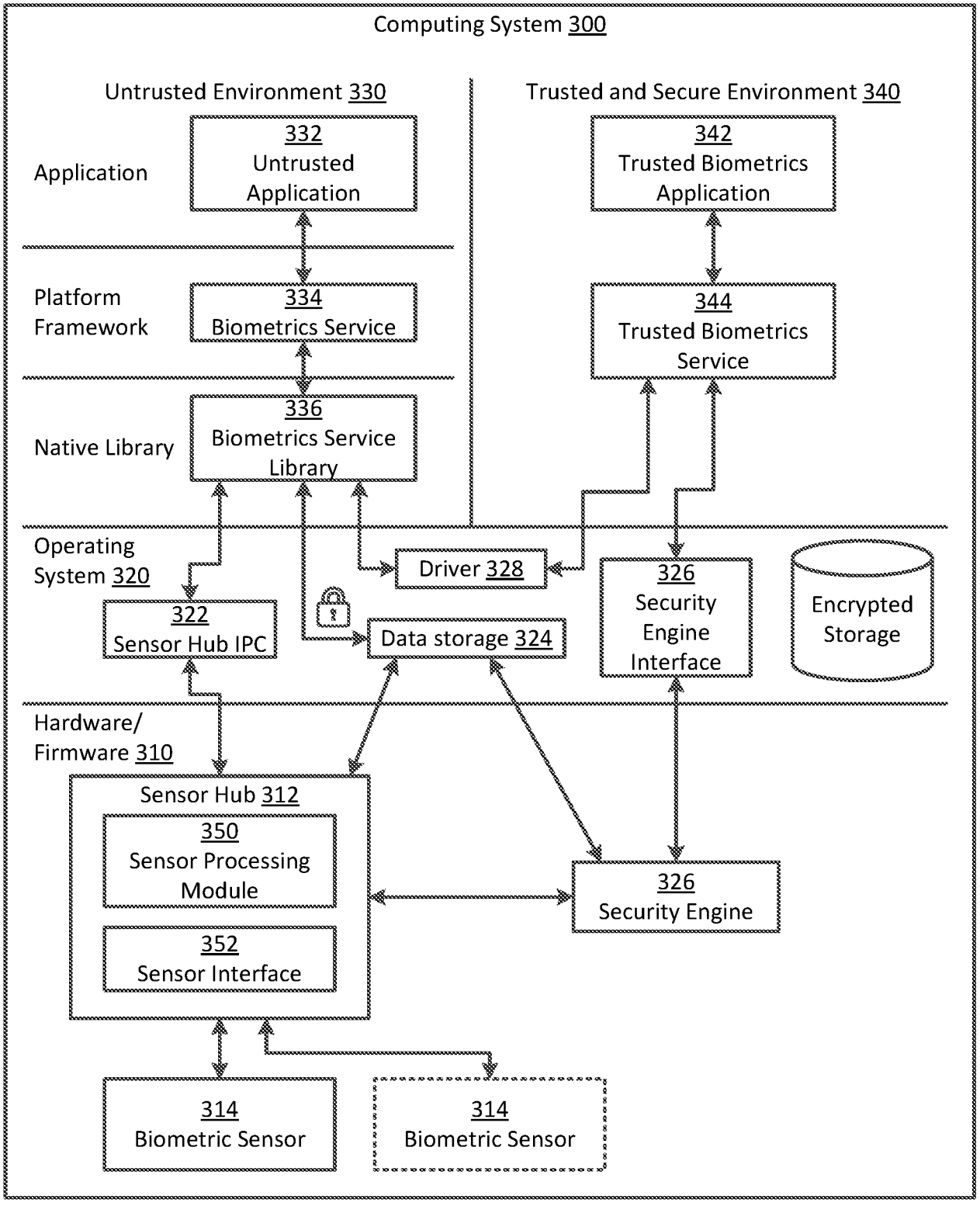
Computing System 300
Untrusted Environment 330
Trusted and Secure Environment 340
Application
332 Untrusted Application
342 Trusted Biometrics Application
Platform Framework
334 Biometrics Service
344 Trusted Biometrics Service
Native Library
336 Biometrics Service Library
Operating System 320
Driver 328
326 Security Engine Interface
Encrypted Storage
322 Sensor Hub IPC
Data storage 324
Hardware/ Firmware 310
Sensor Hub 312
350 Sensor Processing Module
352 Sensor Interface
326 Security Engine
314 Biometric Sensor
314 Biometric Sensor

Fig. 3

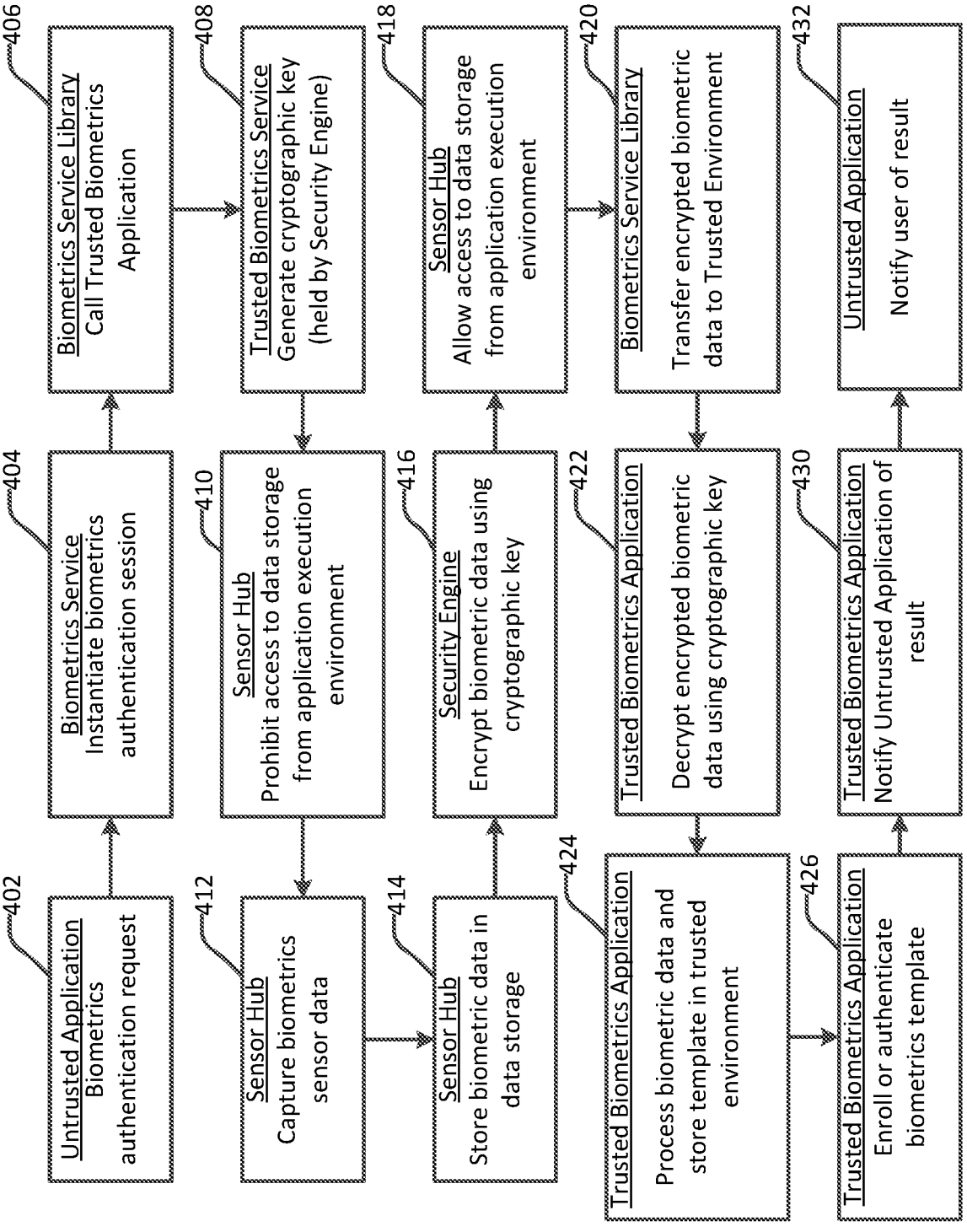
402
Untrusted Application
Biometrics authentication request
404
Biometrics Service
Instantiate biometrics authentication session
406
Biometrics Service Library
Call Trusted Biometrics Application
408
Trusted Biometrics Service
Generate cryptographic key (held by Security Engine)
410
Sensor Hub
Prohibit access to data storage from application execution environment
412
Sensor Hub
Capture biometrics sensor data
414
Sensor Hub
Store biometric data in data storage
416
Security Engine
Encrypt biometric data using cryptographic key
418
Sensor Hub
Allow access to data storage from application execution environment
420
Biometrics Service Library
Transfer encrypted biometric data to Trusted Environment
422
Trusted Biometrics Application
Decrypt encrypted biometric data using cryptographic key
424
Trusted Biometrics Application
Process biometric data and store template in trusted environment
426
Trusted Biometrics Application
Enroll or authenticate biometrics template
430
Trusted Biometrics Application
Notify Untrusted Application of result
432
Untrusted Application
Notify user of result

Fig. 4

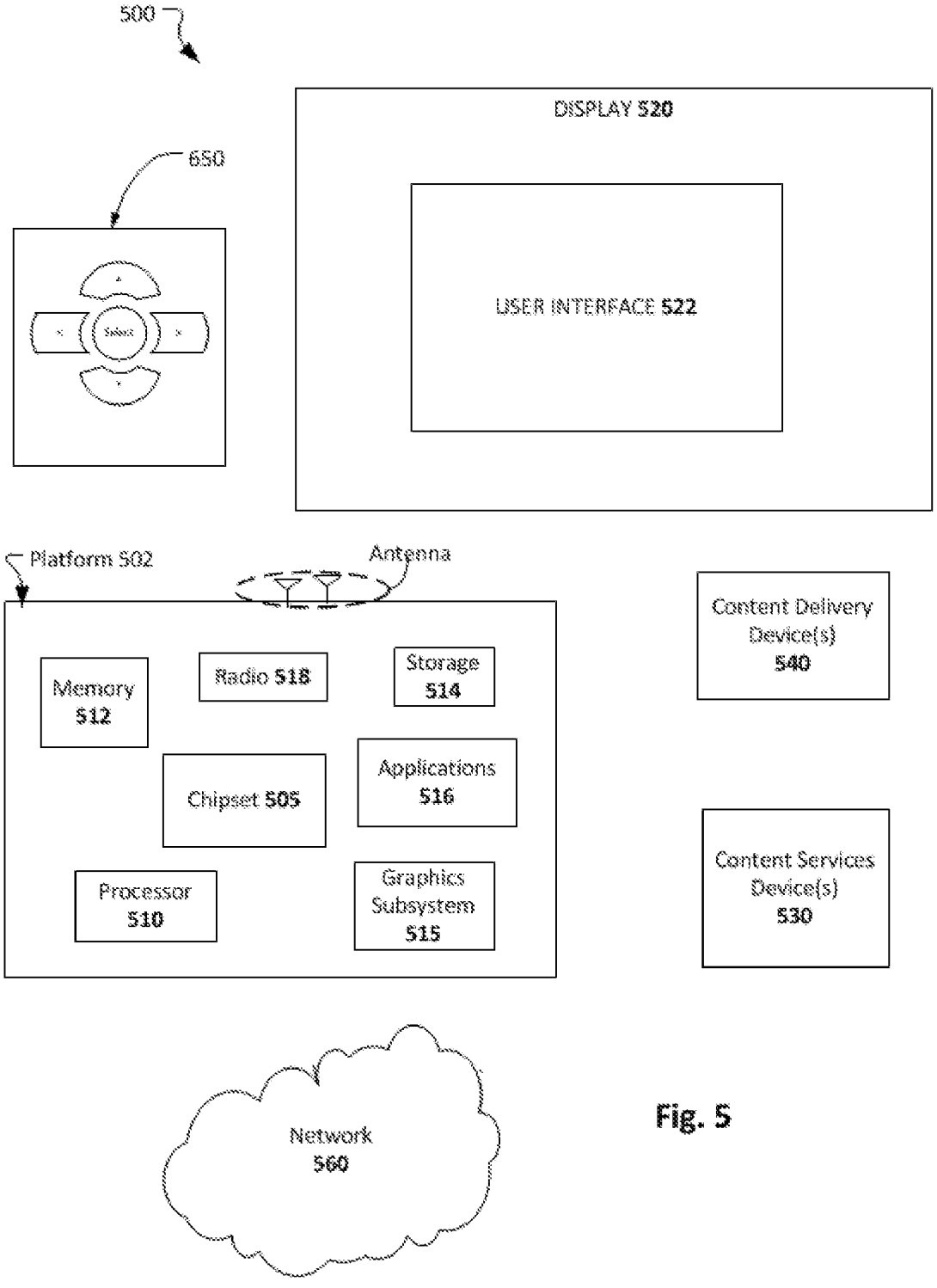
500
650
DISPLAY 520
USER INTERFACE 522
Platform 502
Antenna
Memory 512
Radio 518
Storage 514
Chipset 505
Applications 516
Processor 510
Graphics Subsystem 515
Content Delivery Device(s) 540
Content Services Device(s) 530
Network 560

Fig. 5

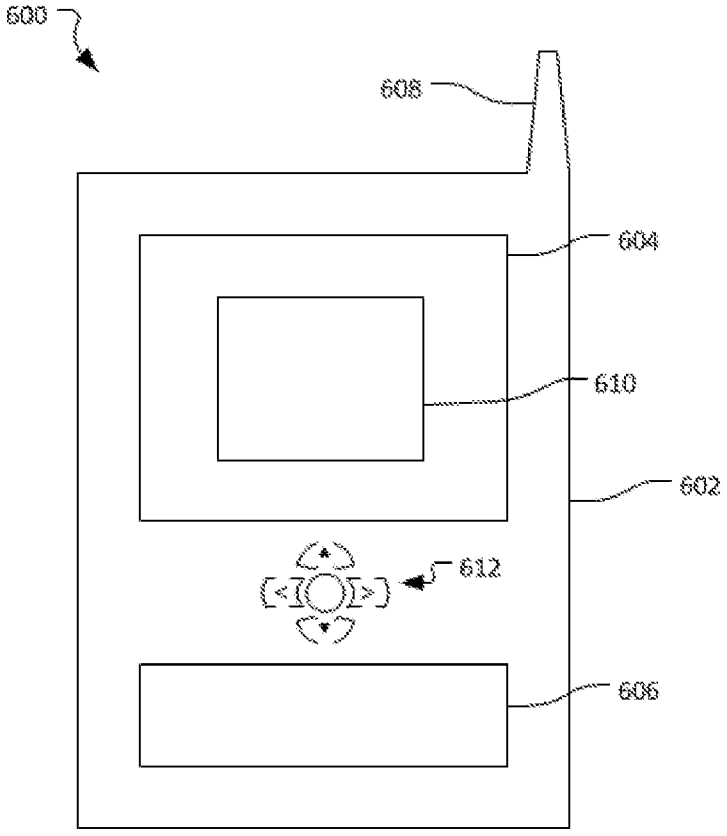


Fig. 6

**INTERNATIONAL SEARCH REPORT**

International application No.
**PCT/US2016/031433**

**A. CLASSIFICATION OF SUBJECT MATTER**

**G06F 21/32(2013.01)i, G06F 21/62(2013.01)i, G06F 21/72(2013.01)i**

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

**B. FIELDS SEARCHED**

Minimum documentation searched (classification system followed by classification symbols)
G06F 21/32; G06F 12/14; H04L 9/32; H04L 9/00; G06K 9/00; G06F 13/28; G06F 21/62; G06F 21/72

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: secure, biometric, sensor, encrypt, authorized

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | US 2009-0287895 A1 (FOLEY DENIS et al.) 19 November 2009<br>See paragraphs [0020]-[0023]; claims 1-3; and figure 2. | 1-22 |
| Y | US 2009-0164797 A1 (ALAN KRAMER) 25 June 2009<br>See paragraphs [0036]-[0037], [0040], [0042], [0046], [0050], [0053], [0065], [0077]; claims 1,3-4; and figures 3,5,6,8,11,12. | 1-22 |
| A | US 2014-0101453 A1 (MSI SECURITY, LTD.) 10 April 2014<br>See paragraphs [0029], [0041]-[0042]; claims 1-2; and figure 2. | 1-22 |
| A | US 2008-0270787 A1 (LACOUS MIRA K.) 30 October 2008<br>See paragraphs [0069]-[0071], [0077]; claims 13-15; and figures 5, 12. | 1-22 |
| A | US 2005-0244037 A1 (LI-KUO CHIU et al.) 03 November 2005<br>See claim 1; and figure 1. | 1-22 |

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

☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 17 August 2016 (17.08.2016) | **17 August 2016 (17.08.2016)** |


Name and mailing address of the ISA/KR
International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon, 35208, Republic of Korea
Facsimile No. +82-42-481-8578

Authorized officer
CHIN, Sang Bum
Telephone No. +82-42-481-8398

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International application No.

**PCT/US2016/031433**

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|---|---|---|---|
| US 2009-0287895 A1 | 19/11/2009 | None | |
| US 2009-0164797 A1 | 25/06/2009 | EP 2075730 A1 | 01/07/2009 |
| | | JP 2009-151788 A | 09/07/2009 |
| | | US 9361440 B2 | 07/06/2016 |
| US 2014-0101453 A1 | 10/04/2014 | US 9286455 B2 | 15/03/2016 |
| | | WO 2014-055792 A1 | 10/04/2014 |
| US 2008-0270787 A1 | 30/10/2008 | US 2003-0218534 A1 | 27/11/2003 |
| | | US 2007-0162739 A1 | 12/07/2007 |
| | | US 7117356 B2 | 03/10/2006 |
| | | US 7415605 B2 | 19/08/2008 |
| | | US 8214652 B2 | 03/07/2012 |
| US 2005-0244037 A1 | 03/11/2005 | TW 200535715 A | 01/11/2005 |
| | | TW I307046 B | 01/03/2009 |
| | | US 7519203 B2 | 14/04/2009 |