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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
13 September 2018 (13.09.2018)

WIPO | PCT

(10) International Publication Number
WO 2018/164630 A1

(51) International Patent Classification:
G06F 21/32 (2013.01) *G06K 9/00* (2006.01)
G06F 21/60 (2013.01)

(21) International Application Number:
PCT/SE2018/050217

(22) International Filing Date:
07 March 2018 (07.03.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/469,158 09 March 2017 (09.03.2017) US
1750330-1 20 March 2017 (20.03.2017) SE

(71) Applicant: **FINGERPRINT CARDS AB** [SE/SE]; Box 2412, 403 16 Göteborg (SE).

(72) Inventors: **WEBER, Sebastian**; Vanåsgatan 15, 216 20 MALMÖ (SE). **BURNETT, David**; 1501 Forge Road, SAN MATEO, California 94402 (US).

(74) Agent: **KRANSELL & WENNBORG KB**; Box 2096, 403 12 GÖTEBORG (SE).

(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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, 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.

(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).

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

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

(54) Title: METHODS FOR ENROLLING A USER AND FOR AUTHENTICATION OF A USER OF AN ELECTRONIC DEVICE

(57) Abstract: The present invention generally relates to methods for enrolling a user of an electronic device and authentication the user of the electronic device. The electronic device comprising a biometry sensor for acquiring sensing signals representative of a biometric feature, and a processor for computing a verification representation based on said sensing signals. The electronic device further includes a secure module isolated from said processor for computing an encrypted representation of said enrolment representation.

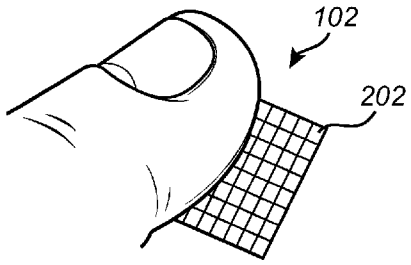

Fig. 2

WO 2018/164630 A1

Methods for enrolling a user and for authentication of a user of an electronic device

TECHNICAL FIELD

The present invention generally relates to a method for enrolling a user of an electronic device and to a method for authentication of a user of the electronic device. The invention further relates to such an electronic device.

BACKGROUND OF THE INVENTION

Various types of biometric systems are used more and more in order to provide an increased security for accessing an electronic device and at the same time keep the user convenience at an acceptable level. Such biometric systems include systems for e.g. fingerprint-based authentication, iris-based authentication, and vein-based authentication among others. In particular fingerprint sensors have been successfully integrated in such electronic devices, for example, thanks to their small form factor, high performance and user acceptance. Among the various available fingerprint sensing principles (such as capacitive, optical, thermal etc.), capacitive sensing is most commonly used, in particular in applications where size and power consumption are important.

Biometric systems rely on a computing environment which performs the processing of acquired images or other types of data indicative of a biometric feature of the user. Although spoofs are one concern for secure authentication using biometric systems, another concern is that the biometric authentication process itself may be subject to various attacks, such as for example physical tampering, compromising the security and integrity of the biometric system.

Devices that employ biometric systems for authentication of a user typically include architectural defenses to increase the difficulty of compromising the logical and physical security of the biometric authentication system. For this purpose, the biometric template extraction and matching software may be run in a more secure computing environment. In addition to providing a high level of security, the security architecture has to provide sufficiently fast authentication procedures in order to meet the market requirements with regards to processing speed.

US 2014/0210589 discloses an example of a fingerprint sensor comprising a secure microprocessor for read-out, matching and verification of fingerprint image data. Thus, if the secure element described in US 2014/0210589 is

compromised, the attacker will have access to the biometric software itself and the stored template data.

Thus, there appears to be room for improvement with regards to increasing the level of security for biometric authentication.

SUMMARY OF THE INVENTION

In view of above-mentioned and other drawbacks of the prior art, it is an object of the present invention to provide methods for biometric authentication with improved security. Another object is to provide an electronic device with improved biometric authentication security.

According to an aspect of the present invention, it is therefore provided a method for enrolling a user of an electronic device comprising: a biometry sensor for acquiring sensing signals representative of a biometric feature; a processor for computing an enrolment representation based on the sensing signals; a secure module isolated from the processor for computing an encrypted representation of the enrolment representation, wherein the method comprises: acquiring sensing signals representative of a candidate's biometric feature; based on the sensing signals, determining an enrolment representation by the processor; determining, by the secure module, an encrypted representation of the enrolment representation; storing, in the secure module, the encrypted representation; when the encrypted representation has been established, providing a success signal indicative of successful encryption to the processor, in response to receiving the success signal, storing, by the processor, the enrolment representation.

The present invention is based upon the realization that improved biometric authentication security is achieved by a layered architecture of the computing environment performing the authentication. The layered architecture may be considered to comprise multiple computing environments. It is realized that by verifying the integrity of the processor which computes the enrolment representations (and also verification representations as will be described below) in a secure module, a fast and secure way of authentication of a user is possible. With the invention, the data (e.g. biometric templates) and software used by the processor which computes enrolment representations (and verification representations) can be confirmed by the isolated secure module. Thus, the integrity of the biometric based decision of authentication is checked by the secure module operating in a separate

architectural "layer" from the processor where the decision is taken. Thereby, the overall integrity of a biometric matching event can be controlled, and "biometric non-repudiation" may be provided for the authentication process.

That the secure module is isolated should be interpreted as that the secure module is separated from the processor by being its own entity. In other words, the secure model and the processor are different hardware. Thus, the processor and the secure module operate with their own independent processing capability. However, the secure module and the processor are able to communicate with each other, i.e. the secure module may send data to the processor and receive data from the processor, and the processor may send data to the secure module and receive data from the secure module. The communication may be via e.g. a SPI-port (serial peripheral interface), or other internal or external data buses known in the art, or wireless techniques including near field communication (NFC), Bluetooth, Wifi, or other known means for communication of digital signals. The secure module may be a so-called "secure element".

The secure module may advantageously comprise a secure control unit and secure storage unit. The secure storage unit is able to store data, i.e. the secure storage unit may be a "machine-readable media".

According to one embodiment, when the encrypted representation has been determined, the enrollment representation may be discarded from the secure module. This advantageously improves the security further since the enrollment template is not stored together with the encrypted representation of the enrolment template.

In one embodiment, the secure module signs the encrypted representation with a private key unique to the electronic device. Thereby, the encrypted representation may only be used for authentication in one specific electronic device, thereby improving security further, in particular in cases when the encrypted representation is returned to the processor. Additionally, signing the encrypted representation with the private key provides improved defense against attempts to swap the entire set of enrolment templates and/or encrypted representations which may otherwise compromise the security of the authentication procedure. Furthermore, the singing with a private key provides a way to check that the encrypted representation has not been tampered with. The private key may be a digital signature attached to the encrypted representation.

Advantageously, determining the encrypted representation may comprise determining a hash representation of the enrolment representation. A hash representation is determined by applying a cryptographic hash function on the enrolment representation. The cryptographic hash function may create a bit string in a one-way manner, in other words, it is not possible to reverse the function to find out the enrolment representation. Several cryptographic hash functions exist and are as such known in the art. Exemplary cryptographic has functions include SHA-2 and SHA-3.

According to one embodiment, it may be included to send the encrypted representation to the processor, wherein the processor stores the encrypted representation as part of an enrolment template for future verification. In other words, the encrypted representation becomes part of the template such that the encrypted representation may become part of an authentication procedure.

The biometry sensor may be a fingerprint sensor whereby the biometric feature is a fingerprint pattern.

The fingerprint sensor may be implemented using any kind of current or future fingerprint sensing principle, including for example capacitive, optical, or thermal sensing technology. However, at present capacitive sensing is most preferred. Both one and two-dimensional sensors are possible and within the scope of the invention. Furthermore, the electronic device may advantageously be a mobile phone. However, other electronic devices are of course thinkable such as tablets, laptops desktop computers, etc.

With a capacitive fingerprint sensor, a measure is detected indicative of the capacitive coupling between each sensing element in an array of sensing elements and a finger surface touching the fingerprint sensor surface. Sensing elements at locations corresponding to ridges in the fingerprint will exhibit a stronger capacitive coupling to the finger than sensing elements at locations corresponding to valleys in the fingerprint. Both one and two-dimensional sensors are possible and within the scope of the invention. Furthermore, the electronic device may advantageously be a mobile phone. However, other electronic devices are of course thinkable such as tablets, a laptop computer, a desktop computer, a smart card, smart watch, etc.

According to one embodiment, the processor may be operable in a trusted execution environment. A trusted execution environment may be a secure

area of a processor, i.e. part of the processing capability of the processor is operable in a secure environment. The security of the trusted execution environment being upheld by software based protection. In other words, the processor may perform the steps of the method in a secure area of the processor, or the entire processor may operate in a trusted execution environment. The data (i.e. templates, and representations) and software in the trusted execution environment is isolated by software from the area of the processor outside the trusted execution environment. Trusted execution environments as such are known to the person skilled in the art.

According to a second aspect of the present invention, there is provided a method for authenticating a user of an electronic device comprising: a biometry sensor for acquiring sensing signals representative of a biometric feature; a processor for computing an verification representation based on the sensing signals; and, a secure module isolated from the processor for computing an encrypted representation of the enrolment representation, wherein the method comprises: acquiring sensing signals representative of a candidate's biometric feature; determining, by the processor, a verification representation based on the sensing signals; comparing, the verification representation with at least one stored enrollment representation; sending, when a match is found between the verification representation and a stored enrollment representation, the enrollment representation to the secure module; determining, by the secure module, an encrypted representation of the enrolment representation and comparing the encrypted representation with at least one stored encrypted representation; when a match is found between the encrypted representation and a stored encrypted representation, providing a pass signal indicative of successful authentication.

Advantageously, the method according to the second aspect ensures that the matched enrolment representation is known to the secure module and has not been modified since it was initially observed by the secure module in the enrolment process. The enrolment process may be as described in the first aspect.

The pass signal may be provided to the processor, or directly to a main processor of the electronic device, or for example to a terminal to which the biometric authentication allows access, i.e. a card reader for a smart card, the smart card having a biometric authentication system. Furthermore, the pass signal may be provided to an application to which the user is attempting to gain access via the biometric authentication.

According to one embodiment, the method for authenticating a user may comprise: sending, when the match is found between the verification representation and a stored enrollment representation, the enrollment representation and the verification representation to the secure module; when the match is found between the encrypted representation and the stored encrypted representation, comparing, by the secure module, the verification representation with the enrolment representation, wherein, when the verification representation is determined to match the enrolment representation, providing the pass signal indicative of successful authentication. In other words, the secure module performs another matching step between the verification representation and the enrolment representation after the encrypted enrolment representations. Thereby a higher confidence level can be asserted about the biometric authentication compared to only performing the matching in the processor.

According to one embodiment, determining an encrypted representation may comprise determining a hash representation of the enrolment representation or the verification representation.

This second aspect of the invention provides similar advantages as discussed above in relation to the first aspect of the invention.

According to third aspect of the present invention, there is provided an electronic device comprising: a biometry sensor for acquiring sensing signals representative of a biometric feature; a processor configured to compute a verification representation and an enrolment representations based on sensing signals acquired by the biometry sensor, a secure module configured to: determine encrypted representations of at least the enrolment representation, and store an encrypted enrolment representation for future authentication.

According to one embodiment, for enrolling a user of the electronic device: the processor may be configured to determine the enrollment representation, the secure module may be configured to determine and store the encrypted representation of the enrolment representation, wherein when the encrypted representation of the enrolment representation is established, the secure module may be configured to send a success signal to the processor, wherein in response to receiving the success signal the processor may be configured to store the enrolment representation for future authentication.

According to one embodiment, for authenticating a user of the electronic device the processor is configured to: determine the verification representation; compare the verification representation with at least one stored enrollment representation, and send, when a match is found between the verification representation and a stored enrollment representation, the enrollment representation to the secure module; wherein the secure module is configured to: determine an encrypted representation of the enrolment representation and compare the encrypted representation with at least one stored encrypted representation, and when a match is found between the encrypted representation and a stored encrypted representation, provide a pass signal indicative of successful authentication.

According to one embodiment, the processor may be configured to: send, when the match is found between the verification representation and a stored enrollment representation, the enrollment representation and the verification representation to the secure module, wherein the secure module is configured to: compare, when the match is found between the encrypted representation and the stored encrypted representation, the verification representation with the enrolment representation, wherein, the secure module is further configured to provide the pass signal when the verification representation matches the enrolment representation.

The electronic device may be a mobile phone such as e.g. a smartphone. However, the electronic device may equally well be a tablet, a laptop computer, a desktop computer, a smart card, smart watch, etc.

In the context of the present application, the “enrolment representation” and/or the “verification representation” of a fingerprint image may be any information extracted from the fingerprint image, which is useful for assessing the similarity between fingerprint images acquired at different times. For instance, the enrolment/verification representation of the fingerprint image may comprise descriptions of fingerprint features (such as so-called minutiae) and information about the positional relationship between the fingerprint features. Alternatively, the representation of the fingerprint image may be the image itself, or a compressed version of the image. For example, the image may be binarized and/or skeletonized. Various ways of extracting such verification representation or enrolment representation from a fingerprint image are well-known to a person of ordinary skill in the relevant art.

Authentication may comprise multiple steps, one step being the process thereof of deciding whether a biometric feature comes from the same individual as an enrolled biometric feature. This process is commonly denoted verification.

This third aspect of the invention provides similar advantages as discussed above in relation to the first aspect and the second aspect of the invention.

In summary, the present invention generally relates to methods for enrolling a user of an electronic device and authentication the user of the electronic device. The electronic device comprising a biometry sensor for acquiring sensing signals representative of a biometric feature, and a processor for computing a verification representation based on said sensing signals. The electronic device further includes a secure module isolated from said processor for computing an encrypted representation of said enrolment representation.

Further features of, and advantages with, the present invention will become apparent when studying the appended claims and the following description. The skilled addressee realize that different features of the present invention may be combined to create embodiments other than those described in the following, without departing from the scope of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The various aspects of the invention, including its particular features and advantages, will be readily understood from the following detailed description and the accompanying drawings, in which:

Figs. 1 schematically exemplify an electronic device according to the present invention, in the form of a mobile phone comprising a biometric sensor in the form of an integrated fingerprint sensor;

Fig. 2 schematically shows a fingerprint sensor array comprised in the electronic device in Fig. 1;

Fig. 3 conceptually illustrates a timing diagram according to an example embodiment;

Fig. 4 conceptually illustrates a timing diagram according to an example embodiment;

Fig. 5 conceptually an electronic device according to an embodiment of the invention;

Fig. 6 is a flow-chart of method steps according to embodiments of the invention; and

Fig. 7 is a flow-chart of method steps according to embodiments of the invention.

DETAILED DESCRIPTION

The present invention will now be described more fully hereinafter with reference to the accompanying drawings, in which currently preferred embodiments of the invention are shown. This invention may, however, be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided for thoroughness and completeness, and fully convey the scope of the invention to the skilled person. For example, the present invention will be described with reference to a fingerprint sensor, however, other biometric authentication systems are equally well applicable such as iris-based and vein-based biometric systems. Like reference characters refer to like elements throughout the drawings.

Turning now to the drawings and to Fig 1 in particular, there is schematically illustrated the electronic device according to the present invention, in the form of a mobile phone 100 with an integrated fingerprint sensor 102 and a display unit 104 with a touch screen interface 106. In this embodiment the fingerprint sensor 102 and the display unit 104 are together arranged at the front side of the mobile phone 100. The fingerprint sensor 102 may, for example, be used for unlocking the mobile phone 100 and/or for authorizing transactions carried out using the mobile phone 100, etc. The fingerprint sensor 102 may of course also be placed on the backside of the mobile phone 100.

Preferably and as is apparent for the skilled person, the mobile phone 100 shown in Fig. 1 further comprises a first antenna for WLAN/Wi-Fi communication, a second antenna for telecommunication communication, a microphone, a speaker, and a phone control unit. Further hardware elements are of course possibly comprised with the mobile phone. It should furthermore be noted that the invention may be applicable in relation to any other type of electronic device,

such as a laptop, a remote control, a tablet computer, a smart card, smart watch, or any other type of present or future similarly configured device.

With reference to Fig. 2, there is conceptually illustrated a somewhat enlarged view of the fingerprint sensor 102. The fingerprint sensor 102 is configured to comprise a large plurality of sensing elements, preferably arranged as a two-dimensional array. The two-dimensional array may have sizes depending on the planned implementation and in an embodiment 160x160 pixels are used. Other sizes are of course possible and within the scope of the invention, including two-dimensional array with less pixels as compared to the above example. A single sensing element (also denoted as a pixel) is in Fig. 2 indicated by reference numeral 202.

Now with reference to Fig. 3 conceptually illustrating a timing diagram of an enrolment procedure according to an exemplary embodiment of the invention. For initiating an enrolment process, sensing signals representative of a biometric feature of a candidate is firstly acquired by a biometry sensor such as for example a fingerprint sensor 301, in such case the sensing signals may be representative of an image of the fingerprint pattern of the candidate. The sensing signals, e.g. the fingerprint image are sent S302 to a processor (not shown) running an application 303 for computing enrolment representations. Thus, the application 303 running on the processor determines S304 an enrolment representation (i.e. an enrolment template) based on the sensing signals. A secure module 305 next receives the enrolment representation S306. The secure module 305 which is isolated from the processor, i.e. the secure module 305 comprises its own processing circuitry (see e.g. Fig. 5), computes and stores S308 an encrypted representation of the enrolment representation. Optionally, the secure module 305 discards S310 the enrollment representation. The encrypted representation of the enrolment representation may for example be a hash for the enrollment representation. When the secure module has successfully computed and stored the encrypted representation, a success signal is sent S312 to the processor running the application 303, the signal being indicative of that the encrypted representation was successfully calculated and stored. In response to the success signal, the processor stores S314 the enrolment representation as an enrolment template. The enrolment template may be used for subsequent verification. In addition, and optionally, the secure module 305 may return the encrypted representation to the processor, for example if the secure

module 305 lacks storage space to store the encrypted representation. In some embodiments, the secure module 305 stores the encrypted representation.

Fig. 4 conceptually illustrating a timing diagram of a verification procedure for authentication of a user according to an exemplary embodiment of the invention. An operating system 400, or application 400 may request a scan for a biometric feature, whereby sensing signals representative of a biometric feature of a candidate is firstly acquired S401 by a biometry sensor such as for example a finger print sensor 301, in such case an image representative of the fingerprint pattern of the candidate is acquired. The sensing signals, e.g. the fingerprint image are sent S402 to a processor (not shown) running an application 303 for computing verification representations. Thus, the application 303 determines S404 a verification representation (i.e. an enrolment template) based on the sensing signals. Next S406, the verification representation is compared with at least one stored enrolment representation (e.g. an enrolment template). If a match is found (S408) between the verification representation and an enrolment representation, the enrolment representation is sent S410 to the secure module 305. The matching (S408) may be performed by an application 303' separate from the application 303 used for creating the verification representation. Both applications 303 and 303' may be running on the processor 302.

With further reference to Fig. 4, when a match is found (S408), the enrolment representation is provided S410 to the secure module 305. The secure module 305 determines S412 an encrypted representation of the enrolment representation, for example, the encrypted representation may be a hash of the enrolment representation. Next S414, the secure module 305 attempts to match the encrypted representation of the enrolment representation with a stored encrypted enrolment representation, and if a match is found, a pass signal is provided (S418, S420, S422) indicative that the encrypted enrolment representation matches with a stored encrypted enrolment representation. Matching the encrypted representation of the enrolment representation with a stored encrypted enrolment representation ensures that the enrolment representation is known to the secure module 305 and has not been modified since initially observed by the secure module 305. The pass signal may be provided to the applications 303 or 303', or directly to the application or operating system 400. The pass signal may optionally include a digital signature (including a private key) of the electronic device.

Optionally, the processor 302 (running application 303) sends both the enrolment representation and the verification representation S410 to the secure module 305. In such case, the secure module may, subsequent to having found S414 a match between the encrypted enrolment representation and a stored encrypted enrolment representation, compare S416 the verification representation with the enrolment representation to confirm the matching result obtained by the processor 302 (e.g. application 303'). When the verification representation is determined to match (S416) the enrolment representation, the pass signal indicative of successful authentication is provided (S418, S420, S422). This provides even higher confidence level of the biometric authentication. In some embodiments, the processor running the applications 303, 303' is operative in a trusted execution environment.

Now turning to Fig. 5 conceptually illustrating an electronic device 500 comprising a biometry sensor 502 for acquiring sensing signals representative of a biometric feature, and a processor 504 configured to compute a verification representation and an enrolment representations based on sensing signals acquired by the biometry sensor 502. The processor 504 may be running one or more applications configured to compute the representations and performing biometric matching between a verification representation and an enrolment representation. The electronic device 500 further comprises a secure module 508 configured to determine encrypted representations of the enrolment representation, and store an encrypted enrolment representation for future authentication. For storing of for example encrypted representations, the secure module 508 comprises a secure storage unit 512. In addition, the secure module 508 comprises a secure control unit 510. The secure module comprises its own hardware and is thus separated from the processor 504 running the applications for computing the representations and performing biometric matching between a verification representation and an enrolment representation. The secure module 508 may receive/send data from/to the processor 504 and vice versa, but is otherwise isolated from the processor. The secure module 508 may for example be "secure element". The communication between the processor and the secure module may be via e.g. a SPI-port (serial peripheral interface), or other internal or external data buses known in the art, or wireless techniques including near field communication (NFC), Bluetooth, Wifi, or other known means for communication of digital signals.

In addition, with further reference to Fig. 5, the processor 504 may be operative in a secure environment such as a trusted execution environment 506. For example, the applications may be run in the trusted execution environment 506 for enhanced security.

Fig. 6 illustrates a flow-chart according to embodiments of the invention. The embodiments illustrated by the flow-chart in Fig. 6 relate to a method for enrolling a user of an electronic device. In a first step S602 sensing signals are acquired representative of a candidate's biometric feature. Based on the sensing signals, an enrolment representation is determined S604 by a processor (e.g. processor 302 or 504). Next S606, an encrypted representation of the enrolment representation is determined by a secure module (e.g. secure module 305 or 508). The encrypted representation is stored S610 in the secure module. When the encrypted representation has been established, a success signal indicative of successful encryption is provided S612 to the processor. In response to receiving the success signal the processor stores S614 the enrolment representation. Optionally, when the encrypted representation has been determined, the enrollment representation is discarded S608 from the secure module.

Turning now to fig. 7 which illustrates a flow-chart according to embodiments of the invention. The embodiments illustrated by the flow-chart in Fig. 7 relate to a method for authenticating a user of an electronic device. In a first step S702, sensing signals representative of a candidate's biometric feature is acquired. Next S704, a verification representation based on the sensing signals is determined by a processor. The verification representation is compared S706 with at least one stored enrolment representation. When a match is found between the verification representation and a stored enrollment representation, the enrollment representation is sent S708 to a secure module. Subsequently S710, an encrypted representation of the enrolment representation is determined by the secure module, and the encrypted representation is compared with at least one stored encrypted representation. When a match is found between the encrypted representation and a stored encrypted representation, a pass signal indicative of successful authentication is provided S712.

With further reference to Fig. 7, optionally the verification representation is also send S714 to the secure module. In such case, the verification representation may be compared S716 with the enrolment representation

subsequent to step S710. When a match is found between the encrypted representation and the stored encrypted representation, and the verification representation is determined to match the enrolment representation, the pass signal indicative of successful authentication is provided S718.

Within the context of the invention, in case of the biometric sensor being a fingerprint sensor the expression “fingerprint image” should be interpreted broadly and to include both a regular “visual image” of a fingerprint of a finger as well as a set of measurements relating to the finger when acquired using the fingerprint sensor.

A control unit of embodiment of the invention may include a microprocessor, microcontroller, programmable digital signal processor or another programmable device. The control unit may also, or instead, include an application specific integrated circuit, a programmable gate array or programmable array logic, a programmable logic device, or a digital signal processor. Where the control unit includes a programmable device such as the microprocessor, microcontroller or programmable digital signal processor mentioned above, the processor may further include computer executable code that controls operation of the programmable device. It should be understood that all or some parts of the functionality provided by means of the control unit (or generally discussed as “processing circuitry”) may be at least partly integrated with the fingerprint sensor, or may be part of the electronic device. It should also be understood that the actual implementation of such a control unit may be divided between a plurality of devices/circuits.

The control functionality of the present disclosure may be implemented using existing computer processors, or by a special purpose computer processor for an appropriate system, incorporated for this or another purpose, or by a hardwire system. Embodiments within the scope of the present disclosure include program products comprising machine-readable medium for carrying or having machine-executable instructions or data structures stored thereon. Such machine-readable media can be any available media that can be accessed by a general purpose or special purpose computer or other machine with a processor. By way of example, such machine-readable media can comprise RAM, ROM, EPROM, EEPROM, CD-ROM or other optical disk storage, magnetic disk storage or other magnetic storage devices, or any other medium which can be used to carry or store desired program code in the form of machine-executable instructions or data structures and which

can be accessed by a general purpose or special purpose computer or other machine with a processor. When information is transferred or provided over a network or another communications connection (either hardwired, wireless, or a combination of hardwired or wireless) to a machine, the machine properly views the connection as a machine-readable medium. Thus, any such connection is properly termed a machine-readable medium. Combinations of the above are also included within the scope of machine-readable media. Machine-executable instructions include, for example, instructions and data which cause a general purpose computer, special purpose computer, or special purpose processing machines to perform a certain function or group of functions.

Although the figures may show a sequence the order of the steps may differ from what is depicted. Also two or more steps may be performed concurrently or with partial concurrence. Such variation will depend on the software and hardware systems chosen and on designer choice. All such variations are within the scope of the disclosure. Likewise, software implementations could be accomplished with standard programming techniques with rule based logic and other logic to accomplish the various connection steps, processing steps, comparison steps and decision steps. Additionally, even though the invention has been described with reference to specific exemplifying embodiments thereof, many different alterations, modifications and the like will become apparent for those skilled in the art.

In addition, variations to the disclosed embodiments can be understood and effected by the skilled addressee in practicing the claimed invention, from a study of the drawings, the disclosure, and the appended claims. Furthermore, in the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality.

CLAIMS

1. A method for enrolling a user of an electronic device comprising:

a biometry sensor for acquiring sensing signals representative of a biometric feature;

a processor for computing an enrolment representation based on said sensing signals;

a secure module isolated from said processor for computing an encrypted representation of said enrolment representation, wherein said method comprises:

- acquiring sensing signals representative of a candidate's biometric feature;

- based on said sensing signals, determining an enrolment representation by said processor;

- determining, by said secure module, an encrypted representation of said enrolment representation;

- storing, in said secure module, said encrypted representation;

- when said encrypted representation has been established, providing a success signal indicative of successful encryption to said processor,

- in response to receiving the success signal, storing, by the processor, the enrolment representation.

2. The method according to claim 1, comprising:

- when said encrypted representation has been determined, discarding said enrollment representation from said secure module.

3. The method according to claim 1 or 2, further comprising:

- signing, by the secure module, said encrypted representation with a private key unique to said electronic device.

4. The method according to any one of the preceding claims, wherein determining said encrypted representation comprises determining a hash representation of said enrolment representation.

5. The method according to any one of the preceding claims, comprising:

- sending the encrypted representation to the processor, wherein the processor stores the encrypted representation as part of an enrolment template for future verification.

6. The method according to any one of the preceding claims, wherein said biometry sensor is a fingerprint sensor and said biometric feature is a fingerprint pattern.

7. The method according to any one of the preceding claims, wherein said processor is operable in a trusted execution environment.

8. A method for authenticating a user of an electronic device comprising:

a biometry sensor for acquiring sensing signals representative of a biometric feature;

a processor for computing an verification representation based on said sensing signals; and,

a secure module isolated from said processor for computing an encrypted representation of said enrolment representation, wherein said method comprises:

- acquiring sensing signals representative of a candidate's biometric feature;

- determining, by said processor, a verification representation based on said sensing signals;

- comparing, said verification representation with at least one stored enrolment representation;

- sending, when a match is found between said verification representation and a stored enrollment representation, said enrollment representation to said secure module;

- determining, by said secure module, an encrypted representation of said enrolment representation and comparing said encrypted representation with at least one stored encrypted representation;

- when a match is found between said encrypted representation and a stored encrypted representation, providing a pass signal indicative of successful authentication.

9. The method according to claim 8, comprising:

- sending, when said match is found between said verification representation and a stored enrollment representation, said enrollment representation and said verification representation to said secure module;

- when said match is found between said encrypted representation and said stored encrypted representation, comparing, by said secure module, said verification representation with said enrolment representation, wherein,

- when said verification representation matches said enrolment representation, providing said pass signal indicative of successful authentication.

10. The method according to claim 8 or 9, wherein determining an encrypted representation comprises determining a hash representation of said enrolment representation or said verification representation.

11. The method according to any one of claims 7 to 9, wherein said biometry sensor is a fingerprint sensor and said biometric feature is a fingerprint pattern.

12. The method according to any one of claims 8 to 11, wherein said processor is operable in a trusted execution environment.

13. An electronic device, comprising:

a biometry sensor for acquiring sensing signals representative of a biometric feature;

a processor configured to compute a verification representation and an enrolment representations based on sensing signals acquired by said biometry sensor,

a secure module configured to:

- determine encrypted representations of at least said enrolment representation, and

- store an encrypted enrolment representation for future authentication,

wherein for enrolling a user of said electronic device:

said processor is configured to determine said enrollment representation,

said secure module is configured to determine and store said encrypted representation of said enrolment representation, wherein

when said encrypted representation of said enrolment representation is established, said secure module is configured to send a success signal to said processor, wherein

in response to receiving the success signal the processor is configured to store the enrolment representation for future authentication.

14. An electronic device, comprising:

a biometry sensor for acquiring sensing signals representative of a biometric feature;

a processor configured to compute a verification representation and an enrolment representations based on sensing signals acquired by said biometry sensor,

a secure module configured to:

- determine encrypted representations of at least said enrolment representation, and

- store an encrypted enrolment representation for future authentication,

wherein for authenticating a user of said electronic device:

said processor is configured to:

determine said verification representation;

compare said verification representation with at least one stored enrollment representation, and

send, when a match is found between said verification representation and a stored enrollment representation, said enrollment representation to said secure module;

wherein said secure module is configured to:

determine an encrypted representation of said enrolment representation and compare said encrypted representation with at least one stored encrypted representation, and

when a match is found between said encrypted representation and a stored encrypted representation, provide a pass signal indicative of successful authentication.

15. The electronic device according to claim 14, wherein said processor is configured to:

send, when said match is found between said verification representation and a stored enrollment representation, said enrollment representation and said verification representation to said secure module, wherein said secure module is configured to:

compare, when said match is found between said encrypted representation and said stored encrypted representation, said verification representation with said enrolment representation, wherein, said secure module is further configured to

provide said pass signal when said verification representation matches said enrolment representation.

16. The electronic device according to any one of claim 13 to 15, wherein said secure module comprises a secure control unit and secure storage unit.

17. The electronic device according to any one of claims 13 to 16, wherein said encrypted representations are hash representations.

18. The electronic device according to any one of claims 13 to 17, wherein the electronic device is a mobile phone, a smart card, or a smart watch.

19. The electronic device according to any one of claims 13 to 18, wherein said processor is operable in a trusted execution environment.

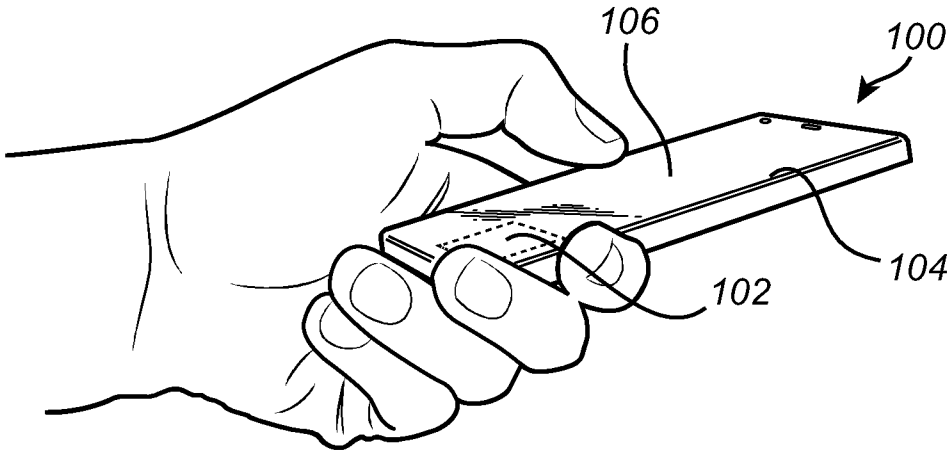

Fig. 1

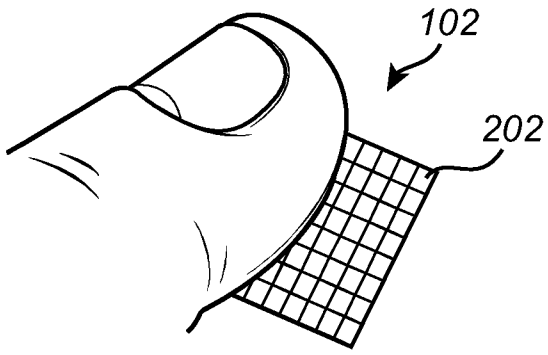

Fig. 2

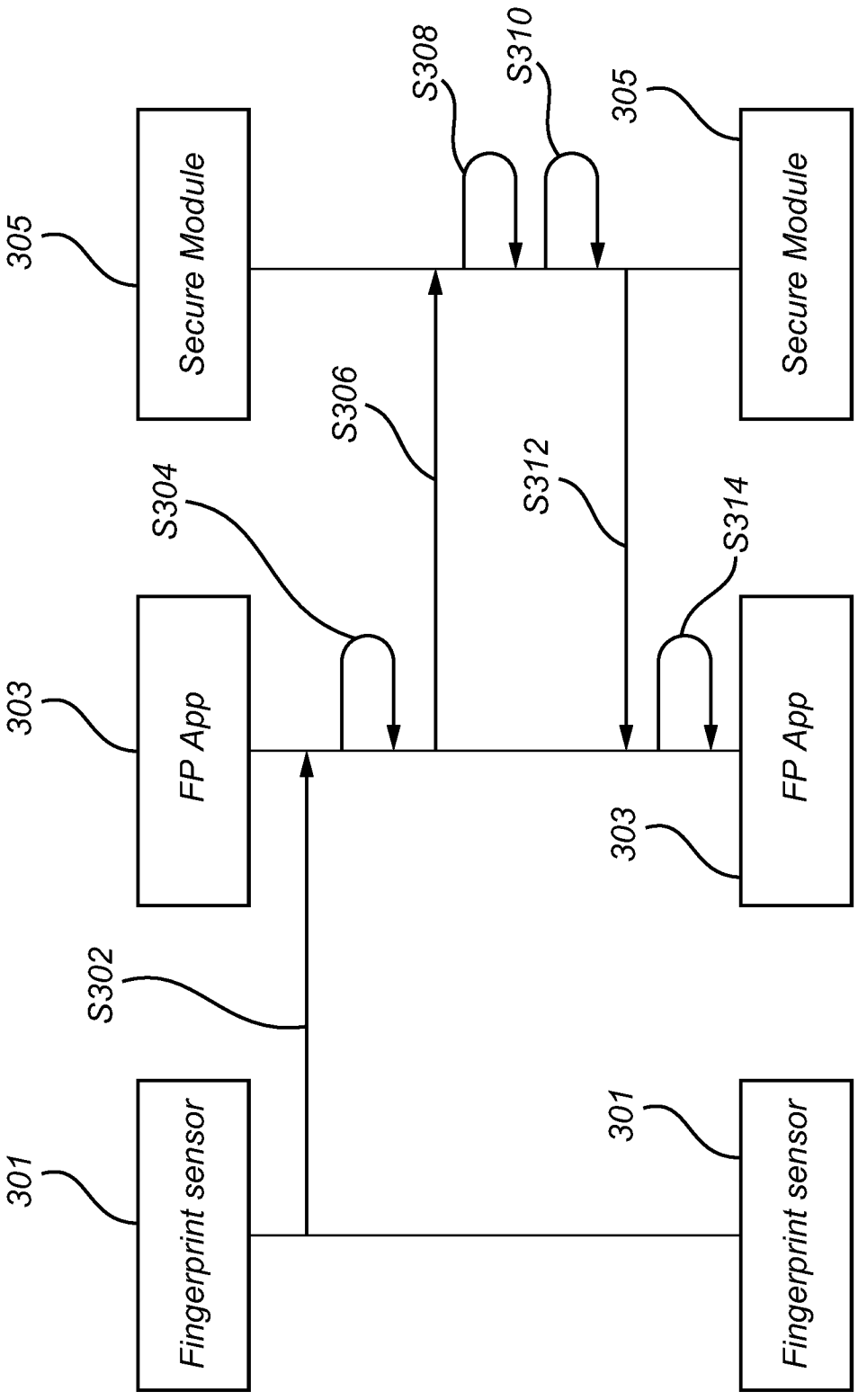
Secure Module
Secure Module
FP App
FP App
Fingerprint sensor
Fingerprint sensor
305
305
303
303
301
301
S302
S304
S306
S308
S310
S312
S314

Fig. 3

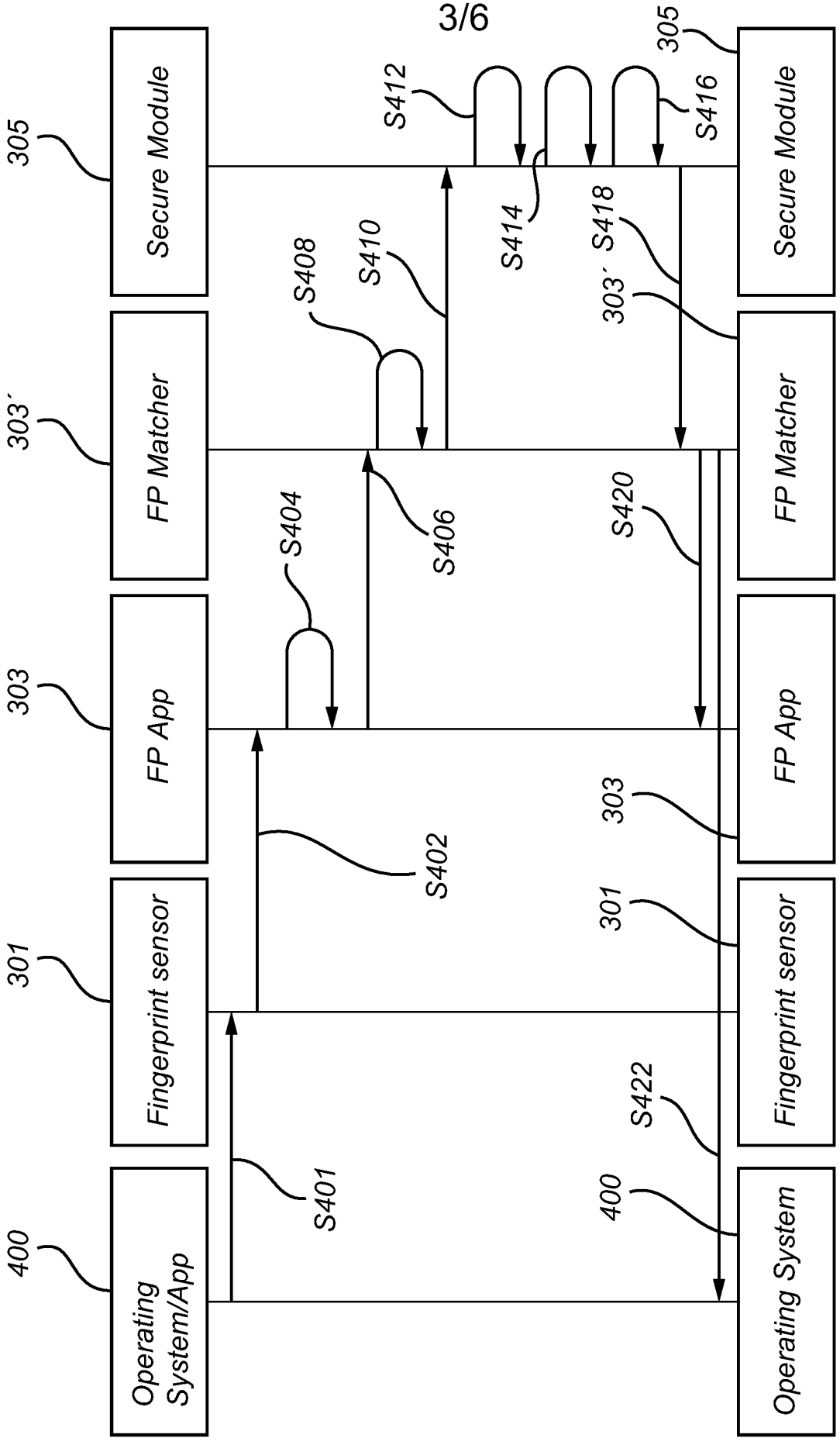
Operating System/App
400
Fingerprint sensor
301
FP App
303
FP Matcher
303´
Secure Module
305
S401
S402
S404
S406
S408
S410
S412
S414
S416
S418
S420
S422
Operating System
400
Fingerprint sensor
301
FP App
303
FP Matcher
303´
Secure Module
305

Fig. 4

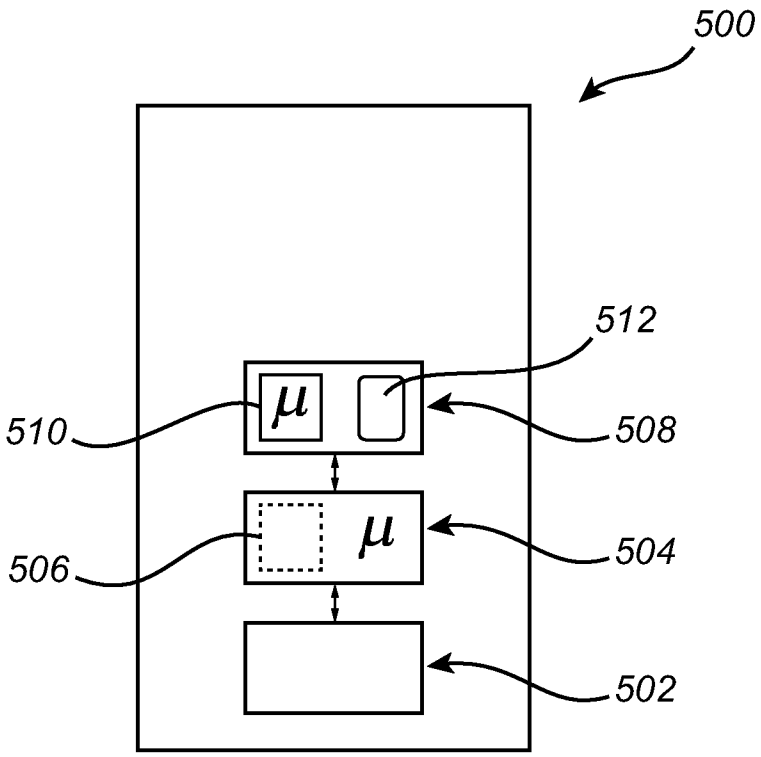

Fig. 5

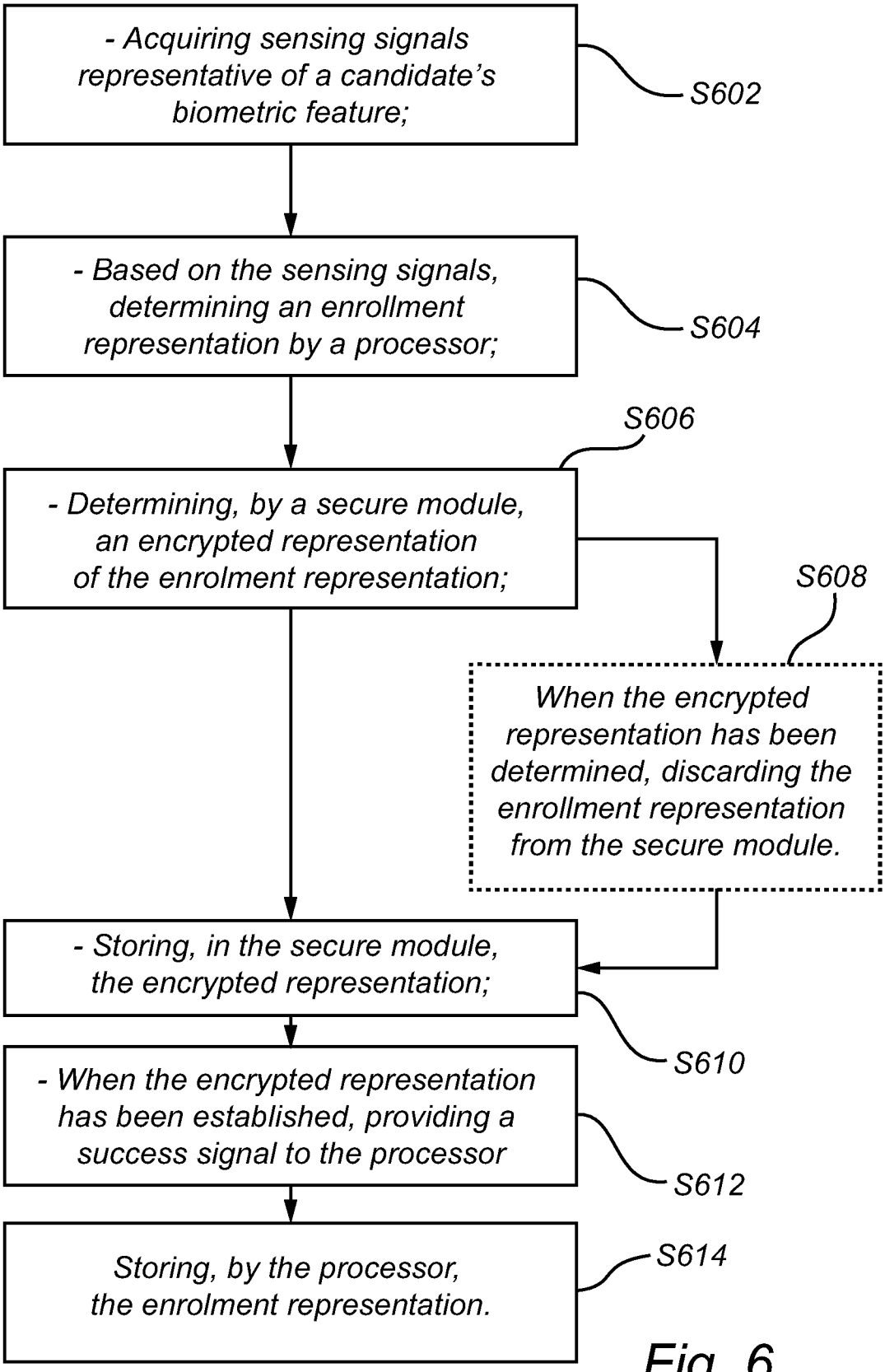
- Acquiring sensing signals representative of a candidate's biometric feature;
S602
- Based on the sensing signals, determining an enrollment representation by a processor;
S604
S606
- Determining, by a secure module, an encrypted representation of the enrolment representation;
S608
When the encrypted representation has been determined, discarding the enrollment representation from the secure module.
- Storing, in the secure module, the encrypted representation;
S610
- When the encrypted representation has been established, providing a success signal to the processor
S612
Storing, by the processor, the enrolment representation.
S614

Fig. 6

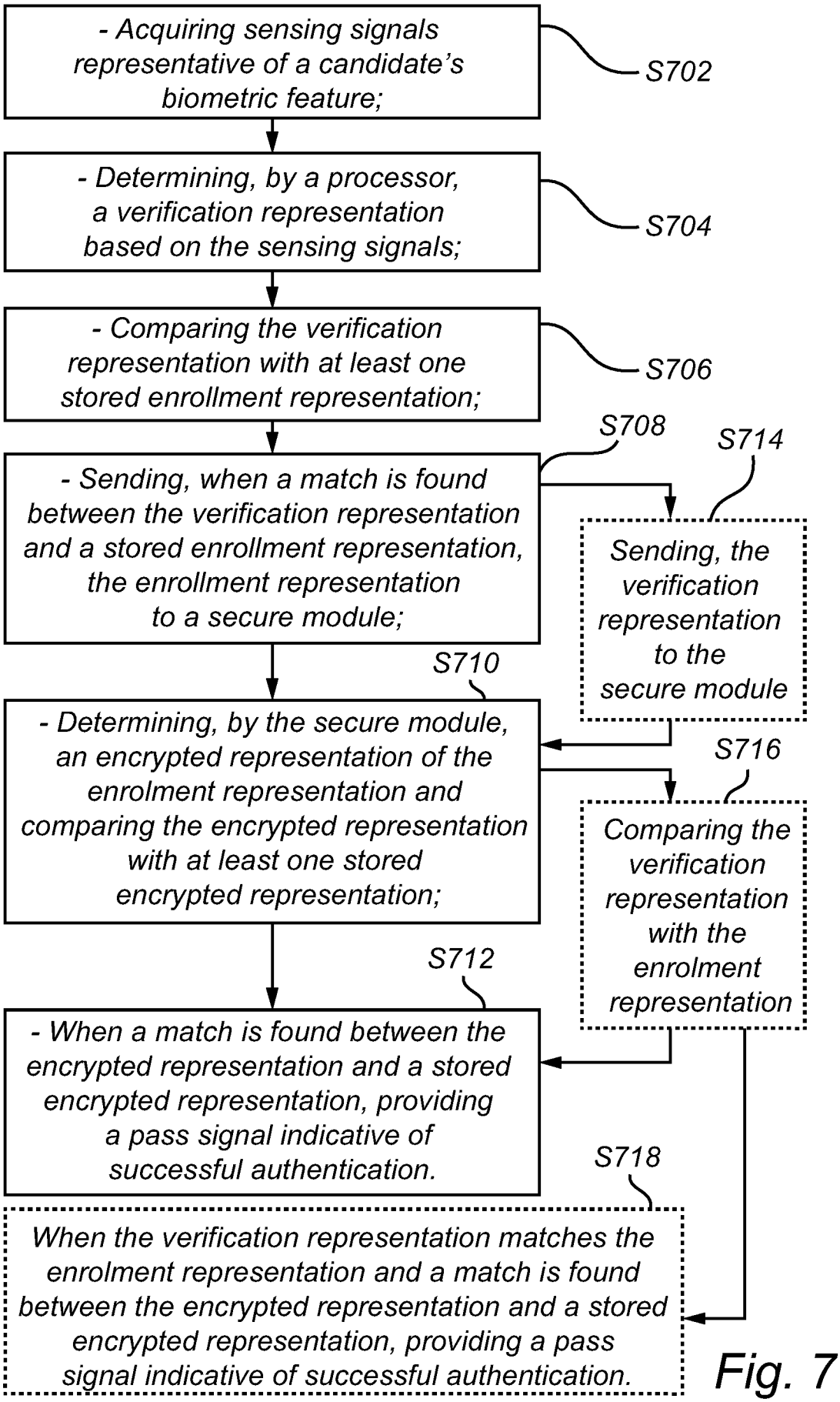
- Acquiring sensing signals representative of a candidate's biometric feature;
S702
- Determining, by a processor, a verification representation based on the sensing signals;
S704
- Comparing the verification representation with at least one stored enrollment representation;
S706
S708
S714
- Sending, when a match is found between the verification representation and a stored enrollment representation, the enrollment representation to a secure module;
Sending, the verification representation to the secure module
S710
S716
- Determining, by the secure module, an encrypted representation of the enrolment representation and comparing the encrypted representation with at least one stored encrypted representation;
Comparing the verification representation with the enrolment representation
S712
- When a match is found between the encrypted representation and a stored encrypted representation, providing a pass signal indicative of successful authentication.
S718
When the verification representation matches the enrolment representation and a match is found between the encrypted representation and a stored encrypted representation, providing a pass signal indicative of successful authentication.

Fig. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE2018/050217

A. CLASSIFICATION OF SUBJECT MATTER

IPC: see extra sheet

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)

IPC: G06F, G06K

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

SE, DK, FI, NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, PAJ, WPI data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 20130308838 A1 (WESTERMAN WAYNE C ET AL), 21 November 2013 (2013-11-21); abstract; paragraphs [0002], [0018], [0025]-[0028], [0030]; figure 5 --	1-19
A	US 9374370 B1 (BENT II BRUCE R ET AL), 21 June 2016 (2016-06-21); abstract; column 59, line 43 - column 62, line 51 --	1-19
A	US 20140344921 A1 (HAMLIN DANIEL L ET AL), 20 November 2014 (2014-11-20); abstract; paragraph [0034] -- --------	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 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
15-05-2018	15-05-2018

Name and mailing address of the ISA/SE	Authorized officer
Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. + 46 8 666 02 86	Gordana Ninkovic Telephone No. + 46 8 782 28 00

International application No.
PCT/SE2018/050217

Continuation of: second sheet

International Patent Classification (IPC)

G06F 21/32 (2013.01)
G06F 21/60 (2013.01)
G06K 9/00 (2006.01)

US	20130308838	A1	21/11/2013	US	20160012273	A1	14/01/2016
				US	9135496	B2	15/09/2015
US	9374370	B1	21/06/2016	US	9904914	B1	27/02/2018
				US	9805344	B1	31/10/2017
				US	9569773	B1	14/02/2017
				US	9483762	B1	01/11/2016
US	20140344921	A1	20/11/2014	US	20170132400	A1	11/05/2017
				US	9589121	B2	07/03/2017
				US	9230082	B2	05/01/2016
				US	20160085951	A1	24/03/2016