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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 December 2017 (21.12.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/216796 A1

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

(21) International Application Number:
PCT/IL2017/050660

(22) International Filing Date:
14 June 2017 (14.06.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
62/350,216 15 June 2016 (15.06.2016) US

(71) Applicant: **DYADIC SECURITY LTD** [IL/IL]; 25 Efal St., 4951125 Petach Tikva (IL).

(72) Inventors: **LINDELL, Yehuda**; 13/2 Menachem Begin St., 5442111 Givat Shmuel (IL). **PE'ER, Guy**; 183 Talmey Yechiel, 79810 Talmey Yechiel (IL).

(74) Agent: **EREZ, Johnathan**; 3 Shalem St., 5221550 Ramat-Gan (IL).

(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,

(54) Title: SYSTEM AND METHODS FOR SECURING SECURITY PROCESSES WITH BIOMETRIC DATA

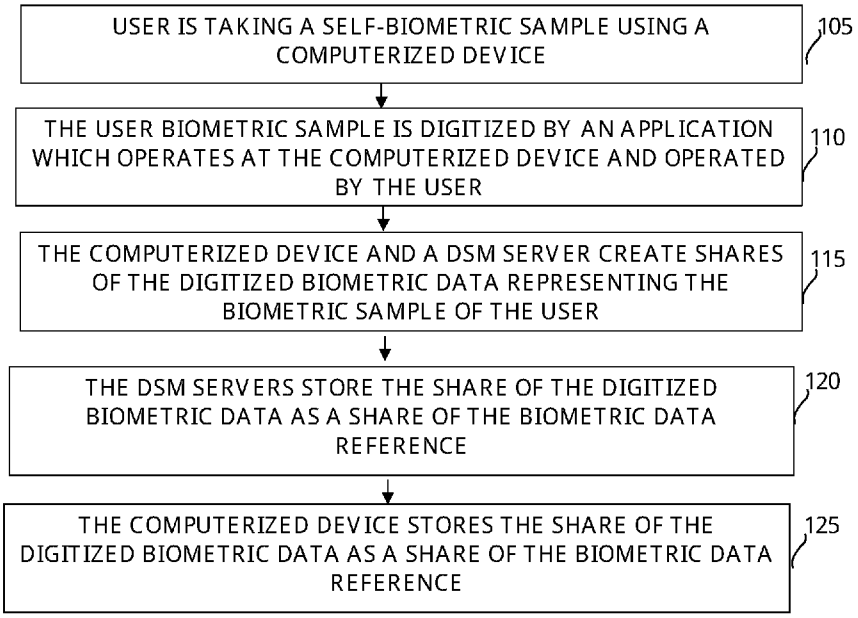


Fig. 1A

(57) Abstract: The present invention discloses a system and method designed to secure computerized security processes via an MPC based biometric comparison. Such security processes can be operated between a computerized device operated by a user and a third-party server, or a third-party application executed by a computerized device. The MPC based biometric comparison process utilized to secure the security process can be operated by at least one server and in some cases, a computerized device operated by the user. Said servers may operate a Distributed Security Module, (DSM Server), designed to participate in multi-party computation (MPC) processes. The DSM server may be configured to use the MPC based biometric comparison process to compare a biometric data sample provided by the computerized device with a biometric data reference stored in the DSM server.

WO 2017/216796 A1

[Continued on next page]

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))*

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

SYSTEM AND METHODS FOR SECURING SECURITY PROCESSES WITH BIOMETRIC DATA

FIELD OF THE INVENTION

The invention generally relates to the field of cryptography and security processes, more specifically to use biometric data for controlling the usage of cryptography secrets utilized in security processes taking place between a computerized device and a third-party application or a server.

BACKGROUND OF THE INVENTION

The extensive use of computers and the continued expansion of telecommunications networks, particularly the internet, enable businesses, governments and individuals to relocate traditional business and administration processes to the internet domain. In some cases, taking these traditional businesses and administrative processes to the internet means to relocate them into a public area and elevate the risk of exposing information to nonauthorized audience. Thus, one of the high prioritized tasks of the people who design these internet services may be to design solutions to secure these services. In many cases, authentication and authorization processes are added to the basic solutions in order to secure the services, the processes and the information thereof. The development of the technology in general and the internet technology in particular shows that the basic authentication and authorization processes do not always meet the requirements of some of the business or governmental processes and services and additional methods to secure the authorization and authentication are needed. In some cases, additional solutions are added to the basic computerized devices in order to raise the security level that these devices support. One of the solutions may be known as a Trusted Platform Module (TPM) designed to secure hardware and software processes by integrating cryptographic keys into the devices. The TPM is an internal solution which secures the computerized device by a secure crypto-processor located within each device. One of the challenges of such internal solutions is that the hardware of every computerized device is required to support such a solution.

SUMMARY OF THE INVENTION

The present invention discloses a system and method designed to secure computerized security processes via an MPC based biometric comparison. Such security processes can be operated between a computerized device operated by a user and a third-party server, or a third-party application executed by a computerized device. The security processes secured by the subject matter disclosed in the present invention can be in some cases, an authentication or ID verification processes, security processes utilizing cryptographic keys, digital signing processes, data decryption or encryption processes, multi-party authentication processes, and the like. The MPC based biometric comparison process utilized to secure the security process can be operated by at least one server and in some cases, a computerized device operated by the user. Said servers may operate a Distributed Security Module, hereinafter referred to as DSM, designed to participate in multi-party computation (MPC) processes.

The DSM server may be configured to use the MPC based biometric comparison process to compare a biometric data sample provided by the computerized device with a biometric data reference stored in the DSM server. The biometric data reference stored in the DSM server may be provided by the computerized device in advance. For example, in some cases a user may utilize a computerized device to take a biometric data sample, and then send the biometric data sample to be stored in the DSM server (or DSM servers). The biometric data sample received by the computerized device may be stored by the DSM server (or DSM servers) as a biometric data reference which can be compared with other biometric data samples provided by the user. In some cases, the biometric data reference may be split to shares and distributed between a DSM server and the computerized device. In such cases, the MPC process conducted between the DSM server and the computerized device enables performing the biometric comparison without reconstructing the biometric data reference, nor ever bringing the distributed biometric data reference shares together. Utilizing said MPC process can guarantee that the privacy of the biometric samples is preserved.

In possible embodiments of the present invention, the biometric data reference can also be split to more than two shares and distributed in the computerized device and more than one DSM server. In some cases, all the shares of the biometric data reference may be distributed and stored among more than one DSM server, wherein the computerized device may not hold any share of the

biometric data reference shares. In such cases, the MPC based comparison process may compare the biometric data reference distributed among the DSM servers and a biometric data sample provided by the computerized device. In possible embodiment of the present invention, the biometric data reference may not be split to shares. In such cases, the biometric data reference may be stored as a whole at the DSM server and the MPC based comparison process may compare a biometric data reference stored in the DSM server and a biometric data sample provided by the computerized device.

The system and method discloses in the present invention can also be configured to control a cryptographic secret which may be used in the security process. The cryptography secrets utilized in the security processes can be private or public keys, symmetric keys, a share or shares of any cryptographic key, hash result, hash function, a decryption or encryption process, and the like. Thus, in case the MPC based comparison process yields a match between the biometric data reference and biometric data sample provided by the computerized device, a second MPC process may take place in order to utilize the cryptography secrets in the security process. In some cases, the cryptography secret may be split and distributed in the DSM server or the DSM servers, and the computerize device. In some other cases, the cryptography secret may be split to shares which may be distributed between more than one DSM server, wherein no share is distributed to the computerized device.

The second MPC process enables to use the cryptography secrets without reconstructing them, nor ever bringing the distributed secret shares together. In some cases, when the MPC based biometric comparison does not yield a match between the biometric data sample provided by the computerized device and biometric data reference, the security process may abort.

In possible embodiments of the present invention, in case the process yields a match between the biometric data sample and the biometric data reference, the system may be configured to manage authorization processes in a selective manner according to the biometric information. Such a selective authorization process may be defined as granting permissions to use/access cryptographic methods, information and the like in some specific security processes

BRIEF DESCRIPTION OF THE DRAWINGS

Some embodiments of the invention are herein described, by way of example only, with reference to the accompanying drawings. With specific reference now to the drawings in detail, it

is stressed that the particulars shown are by way of example and for purposes of illustrative discussion of embodiments of the invention. In this regard, the description taken with the drawings makes apparent to those skilled in the art how embodiments of the invention may be practiced.

In the drawings:

Fig. 1A discloses a method for generating and storing a biometric data reference wherein the biometric data is split to shares which are distributed among a Distributed Security Module (DSM) server and a computerized device, according to exemplary embodiments of the present invention;

Fig. 1B discloses a method for performing a process denoted as a biometric verification designed to utilize an MPC with at least one DSM server in order to perform a biometric comparison, according to exemplary embodiments of the present invention;

Fig. 2 discloses a method of generating and storing a cryptographic secret of a user, according to exemplary embodiments of the present invention, and;

FIG. 3 discloses a system comprises of a DSM server designed to connect with a computerized device to secure security processes, according to exemplary embodiments of the present invention;

FIG. 4 discloses a method of performing a security process between a computerized device and a third-party server, according to exemplary embodiments of the present invention;

Fig. 5A discloses a method of generating and storing a biometric data reference in a Distributed Security Module (DSM) servers, according to exemplary embodiments of the present invention;

Fig. 5B discloses a method for performing another aspect of the biometric verification wherein the computerized device does not hold any shares of biometric sample, according to exemplary embodiments of the present invention, and;

FIG. 6 discloses a method of performing a security process between a computerized device and a third-party server wherein the computerized device does not hold shares of biometric reference, according to exemplary embodiments of the present invention.

DETAILED DESCRIPTION OF THE DRAWINGS

Fig. 1A discloses a method for generating and storing a biometric data reference wherein the biometric data is split to shares which are distributed among a Distributed Security Module (DSM) server and a computerized device, according to exemplary embodiments of the present invention. The generation of the biometric data reference may be performed at the first time the user approaches the DSM servers. After the generation of the biometric data reference, the DSM servers may be able to verify the user's identity in subsequent approaches to said DSM server. In some cases, the DSM servers can be a computerized device such a server, a virtual server, a computerized mobile device, a computerized device capable of executing programed applications, and the like. For example, a computerized mobile device operated by a user can operate a DSM and participate in multi-party computation (MPC) processes with the computerized device held by the user and utilized for capturing self-biometric data samples.

In step 105 a user operating a computerized device captures a self-biometric data sample. The self-biometric data sample can be taken by any computerized or mechanical device for acquiring biometric data. Such a device can comprise a scanner or a camera and application for face recognition, hand geometry readers, retina scanner, fingerprint scanner, microphone with an application for voice recording, iris scanner, and the like. In step 110, an application operates at the computerized device, receives, and in some cases, digitizes the biometric data sample. Such digitizing process may be performed in order to convert the biometric data of the user into a digital form that can be processed by a computer in MPC based biometric comparison. The digitized biometric data can be in a format of a digital file produced by a computerized device, or a computer file comprises digital representation of sound samples in any media format, or, in some cases a digital video file, digital representation of a signature, digital representation of a scanned fingerprint, or any other digital format used by a person which have ordinary skills in the art to present and store biometric data. In some cases, the computerized device utilized to capture the self-biometric data sample may be a personal device operated by the user, such as a computerized mobile telephone, a personal computer, a computer unit, a tablet personal computer and the like.

Step 115, discloses a process which takes place between the computerized device and a DSM server to generate at least two shares of the biometric sample produced in step 110. In some cases, the process for generating the at least two separate shares may be configured to utilize a Multi-Party Processing (MPC) with the DSM server. In some cases, the MPC may be operated

among the computerized device operated by the user and more than one DSM server, for example, two DSM servers, three DSM servers, or multiple DSM servers.

In step 120 the DSM server encrypts and stores the shares of the biometric data of the user, held by the DSM server, as a biometric data reference associated with the user. In possible embodiments of the present invention wherein there are more than one DSM server, other DSM servers may store shares of the biometric data reference and associated the biometric data reference with the user. For example, in case 2 DSM servers are participating in the cryptographic secret generation process, each DSM server can encrypt and store a share of the biometric data reference of the user. Similarly, the computerized device encrypts the share of the biometric data reference of the user sand store in a memory media at the computerized device.

The biometric data reference distributed and stored in the DSM server (or DSM servers) can also be associated with the computerized device operated by the user. For example, the computerized device may comprise a digital certificate utilized to provide a machine identity associated with the computerized device. In step 125 the computerized device also stores the share of the biometric data of the user, held by the computerized device, as a biometric data reference associated with the user. In some cases, once the biometric data reference shares are stored, a process of carrying out a biometric verification may take place (disclosed in Fig. 1B). In such cases, the user may provide a biometric sample and an MPC based comparison process may take place to compare between the newly acquired biometric data and the biometric data reference associated with the user (or in some cases the computerized device), without bringing the shares of the biometric data reference together.

Fig. 1B discloses a method for performing a process denoted as a biometric verification designed to utilize an MPC with at least one DSM server in order to perform a biometric comparison, according to exemplary embodiments of the present invention. In step 130, a user operating a computerized device initiates a security process with a third-party server. In some cases, the third-party server may operate an application or a computer program designed to perform the security process.

In step 135, the computerized device operated by the user may initiate a request to the DSM servers for performing biometric verification in order to be recognized and authorized to perform a security process. It should be noted that the methods disclosed in the subject matter are not limited to sharing the cryptographic key, and only limited to sharing the biometric sample. In some

cases, such a request may arrive via communication networks such a LAN, WAN, internet connections, and the like. In some embodiments of the present invention, the request to the DSM servers for performing the biometric comparison may be initiated by the third-party server. In such cases, the third-party sever may send the request to the DSM server and the DSM server may consequently initiate the process of performing the biometric comparison with the computerized device. In possible embodiments of the present invention, the third-party server may send some of the connection details of the computerized device to the DSM server. Such a connection details may be the details required for connecting with the computerized device. For example, in case the computerized device is communicating over communication networks, the connection details may comprise the Internet Protocol (IP) address of the computerized device. In some cases, the connection details may also comprise additional details such as, the Internet Protocol address of a gateway, Internet Protocol address of networking router required for accessing the computerized device, and the like.

In some cases, the DSM server and the third-party sever may hold unique IDs utilized for authentication. For example, the DSM server may hold a unique ID of the third-party server in order to authenticate the third-party and the third-party may hold a unique ID of the DSM server in order to authenticate the third-party sever. Such unique IDs can be tokens, an integer number functioning as a counter, a unique string, and the like.

In step 140 the user operating the computerized device can take a self-biometric data sample as aforementioned. In step 145 an application executed by the computerized device and operated by a user may digitize the newly acquired biometric data sample.

In step 150 the computerized device and the DSM servers, or in some cases a DSM server perform a comparison process based on MPC to compare the data of the newly acquired biometric sample, and the biometric data reference shares associated with the user. For example, in case a XOR operation is used, the DSM server and the computerized device may conduct an MPC based operation that performs a XOR function between the two shares and then operates the matching algorithm between the result and the data of the newly acquired biometric data, without ever reconstructing the biometric data in a single place.

In some cases, the comparison process may be configured to be executed by an MPC between the computerized device operated by the user and the DSM server (or DSM servers), wherein the biometric comparison process utilizes shares of the biometric data reference

distributed between the computerized device and a DSM server (or DSM servers). In some cases, the biometric comparison process may be configured to be executed by an MPC between at least two DSM servers, wherein the biometric comparison process utilizes shares of the biometric data reference distributed in at least two DSM servers.

In step 155 the computerized device and the DSM server (or servers) are ready to participate in the security process in case the MPC based biometric comparison yielded a match between the newly acquired biometric data and the distributed biometric data reference. In some cases, such a security process can be an authentication with a third-party server, conducting a digital signing procedure, and the like. In some cases, the MPC is carried out over a secure channel and the security process is carried out over the same channel. For example, in case cryptographic protocols providing communications security over a computer network such as Transport Layer Security (TLS) are used. In other cases, the server can issue a credential to the user (e.g., SAML certificate) attesting to the user identity, for the purpose of authenticating to another server or security process. In some other cases, the security process may require a cryptographic secret held by the DSM server and the computerized device. In such a case, a second MPC process may take place, in order to utilize the cryptographic secret held by the DSM serer and the computerized device (or, DSM servers).

In step 160 in case the MPC based biometric comparison does not yield a match, the biometric verification aborts. For example, in case a user seeking to access a third-party server utilizes an application to provide a fingerprint image via a mobile telephone, the application operating in the mobile telephone digitizes a biometric data sample provided by the user, connects with the DSM server and a MPC based biometric comparison takes place. In case the MPC based biometric comparison fails and there is no match between the biometric data sample provided by the user and the biometric data reference, the security process ends and the user cannot access the third-party server.

The MPC based biometric comparison can be based on diverse techniques. In some cases, such a technique may be through using homomorphic encryption to compare the distance between the newly acquired biometric data and the biometric data reference existing in the system without ever decrypting the biometric data. Another technique which may be used is representing the code comparing the newly acquired biometric data as a Boolean or Arithmetic circuit and using secure

computation based on garbled circuits or secure computation based on secret-sharing techniques to perform the comparison.

Fig. 2 discloses a method of generating and storing a cryptographic secret of a user, according to exemplary embodiments of the present invention. In some cases, the user operating the computerized device may perform a biometric verification prior the process of generating and storing the cryptographic secret. In step 230 a computerized device operated by a user may initiate a connection with a DSM server (or DSM servers). Such a connection may be via communication networks such a LAN, WAN, internet connections, and the like. In step 233 the user may utilize the computerized device to carry out a biometric verification in order to enable associating the cryptographic secret with a specific biometric data reference stored at the DSM server and at the computerized device. In some cases, the biometric verification may be configured to be executed by an MPC between the computerized device operated by the user and the DSM server (or DSM servers), wherein the biometric verification utilizes shares of the biometric data reference distributed between the computerized device and a DSM server (or DSM servers). In some cases, the biometric verification may be configured to be executed by an MPC between at least two DSM servers, wherein the biometric verification utilizes shares of the biometric data reference distributed in at least two DSM servers.

In step 235 the process halts in case the biometric verification does not yield a match between the newly acquired biometric sample and a biometric data reference.

Step 237 discloses a process which takes place in case the system is configured to store user's cryptographic secret as a whole, in a non-split format. For example, the DSM server can be configured to store the entire cryptographic secret in the DSM server. In some cases, the DSM server may also be configured to present the user's cryptographic secret to a third-party server, in case the biometric verification yielded a match between the user biometric data sample and the biometric data reference. In such cases, the cryptographic secret generated by the computerized device may not be split. In step 250 the cryptographic secret may be stored in the DSM server, and in step 255 the cryptographic secret may be encrypted by the DSM server.

Step 239, discloses a process which takes place in case the system is configured to store a cryptographic secret split to at least two separate shares. In such cases, the computerized device can generate the split cryptographic secret, wherein the cryptographic secret is being generated and split between the DSM server (or servers) and the computerized device operated by the user.

The process for generating the cryptographic secret shares may utilize a Multi-Party Computation (MPC) process with the DSM server. In some other cases, other methods or schemes, such as Proactive secret sharing, Shamir's secret-sharing scheme, Blakley's scheme, and the like may be used for splitting the cryptographic secret to cryptographic secret shares. In some cases, in which more than one DSM server is participating at the cryptographic secret generation process, the cryptographic secret may be split to multiple shares and then stored in multiple DSM servers.

Step 240 takes place in case the cryptographic secret is split to more than one share. In such cases, one cryptographic secret share can be stored in the computerized device, and another cryptographic secret share can be stored in a DSM server. In some cases, the cryptographic secret share may be associated, by the DSM server, with a user ID. In some cases, the computerized device may also associate the cryptographic secret share with the user ID. The user ID can be a unique name, a unique sequence of characters used to identify a user and utilized to associate the user operating the computerized device with the biometric data reference. In some cases, the user ID can be a digital certificate, a secret key, a digital file, a token, and the like.

The cryptographic secret can be selected from a group comprising cryptographic keys (RSA), a one-time password (OTP) seed and the like. In some cases, in which more than one DSM server is participating in the cryptographic secret splitting process, some shares may be stored in the other DSM servers. In step 245 the DSM server encrypts the share of the cryptographic secret. In some cases, in which more than one DSM server is participating in the cryptographic secret splitting process, other DSM servers may also encrypt the cryptographic secrets. In possible embodiments of the present invention, the DSM server may associate the biometric data reference with the encrypted share of the cryptographic secret generated in step 239 or 237.

Fig. 3 discloses a system comprises of a DSM server designed connect with a computerized device to secure security processes, according to exemplary embodiments of the present invention. Fig. 3 shows a system comprises a DSM server 302 designed to connect with computerized device 301 to secure the security processes which take place between the computerized device 301 and a third-party server. The DSM server 302 comprises a Server Communication Manager 335 which manages the communication with the DSM server 302 over communication networks such as internet networks local area networks, wide area networks and the like. The DSM server 302 also comprises a Secret Storage 340 for storing secretes such as cryptographic secrets utilized for the security processes, and the shares of the biometric data references. The DSM server 302 also

comprises a User Manager 352 which in some cases can be configured to associate the biometric data reference and the cryptographic secrets with the users utilizing the computerized device. In some cases, the User Manager 352 may also comprise a list of services or servers associated with the users, for the purpose of managing authorization processes with third-party services. For example, a certain user may be eligible to connect to some specific services and not be eligible to connect to other specific services. In some cases, a user may be eligible to connect some specific services of one third-party service provider and not be eligible to connect to some other specific services of the same third-party service provider. For example, a user providing biometric credentials may be eligible to utilize secret keys for preforming an authentication process with a third-party server and may be not eligible to utilize said secret key for digital signing on a document provided by the same third-party server.

DSM server 302 also comprises a Cryptographic Manager 355 designed to perform tasks and processes related to cryptography such as generating keys, decrypt and encrypt data associated with the users and the like. DSM server 302 also comprises a MPC Module 360 designed to manage the multi-party computing process as described above. In some embodiments of the present invention the DSM server 302 may be implemented on a personal computer or in some cases on a computerized device capable of operating the MPC Module 360. Such a computerized device may also comprise the Server Communication Manager 335, Secret Storage 340, User Manager 352, and the Cryptographic Manager 355.

In some cases, the DSM server 302 may also comprise a Biometric Verification Manager 365 designed to manage the type of the biometric specific verification required for the biometric data references. For example, in case a user connects to the DSM server at the first time, by a computerized device, the Biometric Verification Manager 365 may configure the biometric verification type. The types of the biometric verification can be at least one type of the following group: (i) Biometric verification wherein the biometric data reference is split to shares and the shares are shared between the DSM server 302 and the computerized device 301. (ii) Biometric verification wherein the biometric data reference is split to shares and the shares are shared between more than one DSM server, similar to DSM server 302, and the computerized device 301. (iii) Biometric verification wherein the biometric data reference is split to shares and the shares are shared between more than one DSM server similar to DSM server 302, wherein the computerized device 301 does not hold any share of the biometric data reference. (iv) Biometric

verification wherein the biometric data reference is not split to shares, and the biometric data reference is stored in the DSM server 302 as a whole in a non-split format.

The security process disclosed herein refers to an exemplary case in which both a biometric sample and a secret (for example a security key) are shared and the biometric verification performed using MPC process leads to an MPC process for verifying the secret. It should be noted that the subject matter also discloses a case in which the key is not shared, and only the biometric sample is shared and then compared with a biometric data reference, without bringing the biometric sample shares together. It should be also noted that the subject matter also discloses a case in which the biometric data reference is not split, and kept as a whole, by the DSM server. In such cases, the DSM server may require to perform an MPC to for the biometric verification. In some other cases the biometric data reference may be split and shared between the DSM servers only.

The DSM server 302 can connect with a Computerized Device 301 operated by a user and preforms the security process which utilizes a cryptographic secret. The Computerized Device 301 is also utilized in other operations of the user such as operating private applications, connecting to the internet, sharing personal information with other users using mobile devices or computers, and the like. The Computerized Device 301 comprises a Device Communication Manager 350 which manages the communication of the Computerized Device 301 over communication networks. Such communication networks may be radio frequency (RF) based communication also known in the industry as Wi-Fi, wired based communications to the internet, and the like. The Computerized Device 301 also comprises Internet Browser Application 310 for browsing the internet. The browser 310 can be any standard and commercial product for connecting to the internet or any designated software designed for a specific application of the internet, such as a news/finance mobile application. The Computerized Device 301 also comprises an MPC Module 315 designed to manage the multi-party computation process as described above.

The Computerized Device 301 also comprises User Manager 320 that associates the shares of the biometric data reference with the users utilizing the computerized device 301. In some cases, the shares of the biometric data reference may be associated with the user ID. For example, a user operating the Computerized Device 301 acquires a new biometric sample such as fingerprint image. The new biometric sample is converted to a digital file and then, split to at least two shares. The share stored by the Computerized Device 301 can be listed and associated with the user ID by

the User Manager 320. In some cases, the User manager 320 may also list multiple cryptographic secrets as described in Fig. 2 and associate the listed cryptographic secrets with the user ID. The Computerized Device 301 also comprises a Secret Storage 325 for storing secretes such as shares of the cryptographic secrets utilized for the security processes, and the shares of the biometric data references. In some cases, the Secret Storage 325 may also be configured to associate the shares of the cryptographic secrets with the shares of the biometric data reference. For example, in case a user is required to utilize a specific encryption key in a security process, the Computerized Device 301 may identify the biometric data reference associated with said specific encryption key, and utilize the biometric data reference to perform a MPC based biometric comparison with the DSM server. Then, in case the MPC based biometric comparison yields a match and the user is recognized as eligible to utilize said encryption key, a second MPC process can take place between the DSM server and the computerized device in order to utilize the encryption key. Once the second MPC is completed, the encryption key can be utilized by the Computerized Device 301 for the security process.

The Computerized Device 301 also comprises a Cryptographic Manager 330 designed to perform tasks and processes related to cryptography. For example, in case a biometric data is received and required to be digitized, the Cryptographic Manager 330 conducts the digitization process and converts the biometric data into a digital representation of the biometric data. The Cryptographic Manager 330 can also be configured to conduct the secret splitting process in order to split digital strings to multiple shares. For example, in case an MPC process is conducted by the MPC Module 315 to split a digital string to multiple shares, the Cryptographic Manager 330 preforms the secret splitting process according to instruction received from the MPC Module 315.

The Computerized Device 301 also comprises a Biometric data acquisition module 332 configured to enable the user to input biometric data into the Computerized Device 301. Such acquisition module 332 may be a camera, a pad, a scanner, and the like, to which the user can input biometric data into the Computerized Device 301. In some cases, the acquisition module 332 may be a communication port from another electronic device, for example a USB memory device.

FIG. 4 discloses a method of performing a security process between a computerized device and a third-party server, according to exemplary embodiments of the present invention. In step 405 a user operating a computerized device seeking to connect with a third-party server may be requested

to initiate a security process. In some cases, such a request may be conducted by an application operated at the computerized device. Such an application may be a dedicated application designed to connect to said third-party server, or a general application designed to utilize internet technology such as internet browser application and connect to third party servers. In step 410 the computerized device and the server perform a biometric verification. In some cases, the request to perform the biometric verification may be initiated by the computerized device, or by an application operated in the computerized device. In some other cases, the request to perform the biometric verification may be initiated by the third-party server which may send the request to the DSM server (or DSM serves) and the DSM server may consequently send the computerized device a request to initiate the biometric verification.

Step 415 takes place in case the biometric verification yields a match, and in case a split cryptographic secret is used in the security process. In some cases, the cryptographic secret may be split and distributed between the computerized device and the DSM server. In such cases, the computerized device and the DSM server can be configured to perform an MPC process, denoted as second MPC process, in order to utilize the cryptographic secret in the security process. For example, in case a private key based authentication process is requested by the third-party application or a service, the second MPC may utilize the private key for the authentication process out of the private key shares distributed in the DSM servers and the computerized device. Another example may be with a digital signing process in which the key used for signing is split between the computerized device and the DSM server. Thus, the DSM server and the computerized device may perform the second MPC to utilize the key used for signing out of the key shares distributed in the DSM servers and the computerized device. In some cases, the cryptographic secret may be for generating a one-time password, signature, decrypted information and the like.

Step 420 takes place in case the biometric verification yields a match, and a non-split cryptographic secret is used in the security process. For example, the DSM server can be configured to store the entire cryptographic secret in a non-split format and utilize the non-split cryptographic secret in the security process. In some cases, the DSM server may be also configured to present the user's cryptographic secret to the third-party server.

Step 425 takes place in case the biometric verification yields a match, and in case the security process takes place without additional cryptographic secrets, such as private keys, public keys, encryption keys, digital signatures, and the like. For example, in some cases, the biometric

verification may be utilized to verify the eligibility of a user to connect to a third-party server such as an authentication server. Such cases can be wherein the DSM server issues a credential like a SAML certificate to the user. In such case, the user can then send the certificate to the authentication server who verifies the certificate and allows the user to connect in case the certificate is valid.

In some cases, the DSM server and the computerized device may be configured to provide authorization functionality. For example, the system may approve the user ID and grant permission to utilize the user's private key to perform an authentication process and deny the permissions of using the user's private key to conduct an encryption process. In some cases, the security process with a third-party application may be an authorization process. Thus, the system may be configured to manage authorization processes in a selective manner according to the biometric information. Such selective authorization may be defined as granting permissions to use/access cryptographic methods, information and the like in some specific security processes. For example, a user providing biometric credentials may be allowed to use the private key to conduct an authentication process with a third-party server and may be refused to utilize the private key for other purposes such as digital signing, encryption processes, decryption process and the like.

Fig. 5A discloses a method of generating and storing a biometric data reference in a Distributed Security Module (DSM) servers, according to exemplary embodiments of the present invention. The generation of the biometric data reference may be performed at the first time the user approaches the DSM servers. In some cases, after the generation of the biometric data reference, the DSM servers may be able to verify the user's identity in subsequent approaches to said DSM server.

In step 505 a user operating a computerized device captures a self-biometric data sample. The self-biometric data sample can be taken by any computerized or mechanical device for acquiring biometric data. Such a device can comprise a scanner or a camera and application for face recognition, hand geometry readers, retina scanner, fingerprint scanner, microphone with an application for voice recording, iris scanner, and the like. In step 510, an application operated by the computerized device receives, and in some cases, digitizes the biometric data sample. Step 515 discloses an optional configuration of the DSM server which implements one aspect of the present invention in which the computerized device sends a non-split biometric sample as a whole to the

to the DSM server. In step 520 the DSM server may store the non-split biometric sample as a biometric data reference, and in some cases, the DSM server may encrypt the biometric data reference.

Step 525 discloses an optional configuration of the DSM server which implements another aspect of the present invention in which the computerized device sends the complete biometric sample to at least two DSM servers. In step 530 the DSM servers which receive the biometric sample, can operate a process for generating the at least two shares of the received biometric sample. In some cases, the DSM servers may be configured to utilize a Multi-Party Processing (MPC) operated among the DSM servers for creating the shares. In some other cases, the process for generating the at least two shares of the biometric sample may utilize other methods which are known to a person who has ordinary skills in the art. In some embodiments of the present invention the computerized device operated by the user may be configured to generate the biometric sample shares and then send them to the DSM server. In such cases, the computerized device may be configured to utilize methods for splitting the biometric sample to shares which are known to a person who has ordinary skills in the art

In step 535 the DSM servers may store the shares of the biometric sample as a biometric data reference, and in some cases, may also encrypt the biometric data reference. In some cases, the DSM servers may be configured to associate the biometric data reference with the user. In some other cases, the DSM servers may associate the biometric data reference with the computerized device which sent the biometric sample. In some cases, once the shares of the biometric data reference are stored, a biometric verification may take place (disclosed in Fig. 5B). In such cases, the user may provide a biometric sample and an MPC based comparison process may take place to compare between the newly provided biometric data sample and the biometric data reference associated with the user (or in some cases the computerized device), without bringing the shares of the biometric data reference together.

Fig. 5B discloses a method for performing another aspect of the biometric verification wherein the computerized device does not hold any shares of biometric sample, according to exemplary embodiments of the present invention. In step 540, a user operating a computerized device initiates a security process with a third-party server. In some cases, the third-party server may operate an application or a computer program designed to perform the security process.

In step 545, the computerized device operated by the user may initiate a request to the DSM servers for performing biometric verification in order to be recognized and authorized to perform a security process. In some cases, such a request may arrive via communication networks such a LAN, WAN, internet connections, and the like. In some embodiments of the present invention, the request to the DSM servers for performing the biometric comparison may be initiated by the third-party server. In such cases, the third-party server may send the request to the DSM server and the DSM server may consequently initiate the process of performing the biometric comparison with the computerized device. In possible embodiments of the present invention, the third-party may send to the DSM server some of the connection details of the computerized device. Such a connection details may be the details required for connecting with the computerized device. For example, in case the computerized device is communicating over communication networks, the connection details may comprise the Internet Protocol (IP) address of the computerized device. In some cases, the connection details may also comprise additional details such as, the Internet Protocol address of a gateway, Internet Protocol address of networking router required for accessing the computerized device, and the like.

In some cases, the DSM server and the third-party sever may hold unique IDs utilized for authentication. For example, the DSM server may hold a unique ID of the third-party server in order to authenticate the third-party and the third-party may hold a unique ID of the DSM server in order to authenticate the third-party sever. Such unique IDs can be tokens, an integer number functioning as a counter, a unique string, and the like. In step 547 the user operating the computerized device can take a self-biometric data sample as aforementioned. In step 550 an application executed by the computerized device and operated by a user may digitize the newly acquired biometric data sample.

Step 560 discloses a comparison process based on MPC which compares the newly acquired biometric sample, and the biometric data reference shares associated with the user. The process disclosed in step 560 takes place in case the biometric data reference is not split. In such cases, the DSM server may hold the complete biometric data references associated with the user or with the computerized device. The DSM server and the computerized device may conduct an MPC based operation that operates the matching algorithm between the result and the newly acquired biometric data. In step 565, in case the MPC based biometric comparison does not yield a match, the biometric verification aborts. Step 570 discloses an MPC based comparison process

wherein the biometric data reference is split to shares which are stored in at least two DSM servers. Step 570 shows the process designed to take place in case the computerized device operated by the user does not hold any share of the biometric data reference.

In step 575 the DSM server aborts the biometric verification in case the biometric comparison process does not yield a match between the newly acquired sample and the biometric data reference. In step 580 the computerized device and the DSM server (or servers) are ready to participate in the security process in case the MPC based biometric comparison yields a match between the newly acquired biometric data and the distributed biometric data reference. In some cases, such a security process can be an authentication with a third-party server, conducting a digital signing procedure, and the like. In some cases, the MPC is carried out over a secure channel and the security process is carried out over the same channel. For example, in case cryptographic protocols providing communications security over a computer network such as Transport Layer Security (TLS) are used. In other cases, the server can issue a credential to the user (e.g., SAML certificate) attesting to its identity, for the purpose of authenticating to another server or security process. In some cases, the security process may require a cryptographic secret held by the DSM server and the computerized device. In such a case, a second MPC process may take place, in order to utilize the cryptographic secret held by the DSM serer and the computerized device (or, DSM servers).

The MPC based biometric comparison can be based on diverse techniques. In some cases, such a technique may be through using homomorphic encryption to compare the distance between the newly acquired biometric data and the biometric data reference existing in the system without ever decrypting the biometric data. Another technique which may be used is representing the code comparing the newly acquired biometric data as a Boolean or Arithmetic circuit and using secure computation based on garbled circuits or secure computation based on secret-sharing techniques to perform the comparison.

FIG. 6 discloses a method of performing a security process between a computerized device and a third-party server wherein the computerized device does not hold shares of the biometric reference, according to exemplary embodiments of the present invention. In step 605 a user operating a computerized device seeking to connect with a third-party server may be requested to initiate a security process. In some cases, such a request may be conducted by an application

operated at the computerized device. Such an application may be a dedicated application designed to connect to said third-party server, or a general application designed to utilize internet technology such as internet browser application and connect to third party servers. In Step 607, the user operating the computerized device can take a self-biometric data sample as aforementioned. In step 608 an application executed by the computerized device and operated by a user may digitize the newly acquired biometric data sample. Step 610 discloses an optional configuration of the DSM server which implements one aspect of the present invention in which the biometric verification takes place wherein the computerized device does not hold any shares of biometric reference and the MPC takes place between the computerized device holding the biometric sample and the DSM server holding the biometric reference. In some cases, the request to perform the biometric verification wherein the computerized device does not hold shares of biometric reference may be initiated by the computerized device, or by an application operated in the computerized device. In some other cases, the request to perform the biometric verification wherein the computerized device does not hold shares of biometric sample, may be initiated by the third-party server which may send the request to the DSM server (or DSM serves) and the DSM server may consequently send the computerized device a request to initiate the biometric verification wherein the computerized device does not hold shares of biometric sample.

Step 613 discloses an optional configuration of the DSM server which implements one aspect of the present invention in which the MPC of the biometric verification involves the computerized device and the DSM servers, in an MPC based comparison process wherein the biometric data reference stored in at least two DSM servers as disclosed in step 570.

Step 615 takes place in case the biometric verification yields a match and in case a split cryptographic secret is required to be used in the security process performed between the third-party server and the computerized device. In some cases, cryptographic secret may be split and distributed between the computerized device and the DSM server. The computerized device and the DSM server may be configured to perform an MPC process, denoted as second MPC process, in order to provide the cryptographic secret to the third-party server. For example, in case a private key based authentication process is requested by the third-party application or a service, the second MPC may utilize the private key for the authentication process out of the private key shares distributed in the DSM servers and the computerized device. Another example may be with a digital signing process in which the key used for signing is split between the computerized device

and the DSM server. Thus, the DSM server and the computerized device may perform the second MPC to utilize the key used for signing out of the key shares distributed in the DSM servers and the computerized device. In some cases, the cryptographic secret may be for generating a one-time password, signature, decrypted information and the like.

Step 620 takes place in case the biometric verification yields a match, and in case a non-split cryptographic secret is used in the security process performed between the third-party server and the computerized device. In such a case, the DSM server may present the cryptographic key to the third-party server. The security process which takes place in case the system is configured to store user's cryptographic secret as whole, in a non-split format. For example, the DSM server can be configured to store the entire cryptographic secret, in a non-split format at the DSM server. In some cases, the DSM server may be also configured to present the user's cryptographic secret to a third-party server.

Step 625 takes place in case the biometric verification yields a match, and in case the security process takes place without additional cryptographic secrets, such as private keys, public keys, encryption keys, digital signatures, and the like. For example, in some cases, the biometric verification may be utilized to verify the eligibility of a user to connect, such that in case the biometric verification yields a match between the biometric sample of the user and a biometric data reference, the user may be allowed to connect to a third-party server such as an authentication server. For example, in case the DSM server issues a credential like a SAML certificate to the user. In such case, the user can then send the certificate to the authentication server who verifies the certificate and allows the user to connect in case the certificate is valid.

In some cases, the DSM server and the computerized device may be configured to provide authorization functionality. For example, the system may approve the user ID and grant permission to utilize the user's private key to perform an authentication process and deny the permissions of using the user's private key to conduct an encryption process. In some cases, the security process with a third-party application may be an authorization process. Thus, the system may be configured to manage authorization processes in a selective manner according to the biometric information. Such selective authorization may be defined as granting permissions to use/access cryptographic methods, information and the like in some specific security processes. For example, a user providing biometric credentials may be allowed to use the private key to conduct an authentication

process with a third-party server and may be refused to utilize the private key for other purposes such as digital signing, encryption processes, decryption process and the like.

While the disclosure has been described with reference to exemplary embodiments, it will be understood by those skilled in the art that various changes may be made and equivalents may be substituted for elements thereof without departing from the scope of the invention. In addition, many modifications may be made to adapt a particular situation or material to the teachings without departing from the essential scope thereof. Therefore, it is intended that the disclosed subject matter not be limited to the particular embodiment disclosed as the best mode contemplated for carrying out this invention, but only by the claims that follow.

CLAIMS

1. A method for conducting security processes between a computerized device and a third-party server, comprising:

   receiving a request, by a at least one Distributed Security Module (DSM) server, to compare a biometric sample of a user with a biometric data reference split to shares, wherein said shares are distributed and stored in the computerized device and in the at least one DSM server;

   performing a comparison process between the biometric sample of the user provided by the computerized device and the biometric data reference using a Multi-Party Computation (MPC) process between the computerized device and the at least one DSM server;

   performing a security process between the computerized device and DSM server, and the third-party server in case the comparing of the biometric sample of the user provided by the computerized device with the split biometric data reference yields a match.
2. The method of claim 1, wherein the request to compare the biometric sample of the user with the biometric data reference split to shares is received from the third-party server.
3. The method of claim 1, wherein the request to compare the biometric sample of the user with the biometric data reference split to shares is received from the computerized device.
4. The method of claim 1, wherein the security process between the computerized device and DSM server further requires a cryptography secret.
5. The method of claim 4, wherein the cryptography secret is stored in the at least one DSM server.
6. The method of claim 5, wherein the cryptography secret stored in the at least one DSM server is encrypted.
7. The method of claim 4, wherein the cryptography secret is split to more than one cryptography secret share.
8. The method of claim 7, wherein at least one of the cryptography secret shares is stored in the at least one DSM server.
9. The method of claim 8, wherein the at least one of the cryptography secret shares stored in the at least one DSM server is encrypted.

10. The method of claim 7, wherein at least one of the cryptography secret shares is stored in the computerized device.
11. The method of claim 10, wherein at least one of the cryptography secret shares stored in the computerized device is encrypted.
12. The method of claim 7, further comprises the computerized device and the at least one DSM server preforming another MPC process for utilizing the cryptography secret in a security process with the third-party.
13. The method of claim 1, further comprises capturing the biometric sample by the computerized device.
14. The method of claim 1, wherein the security process aborts in case there is no match between the biometric data reference and the biometric sample captured from the user and provided by said computerized device,
15. The method of claim 1, wherein the biometric data reference is associated with said user.
16. The method of claim 1, further comprises an enrollment phase between the computerized device and the least one DSM server, wherein the enrollment process comprises creating a biometric data reference split to shares and distributing between the computerized device and the least one DSM server.
17. The method of claim 16, wherein the enrollment phase further comprises storing at least one share of the biometric data reference shares in the least one DSM server.
18. The method of claim 16, wherein the enrollment phase further comprises storing one share of the biometric data reference shares in the computerized device.
19. The method of claim 16, wherein the enrollment phase further comprises encryption of at least one share of the biometric data reference shares stored in the least one DSM server.
20. The method of claim 16, wherein the enrollment phase further comprises encryption of the share of the biometric data reference shares stored in the computerized device.
21. The method of claim 1, wherein all the shares of the split biometric data reference are distributed and stored in more than one DSM server.
22. The method of claim 21, wherein the shares of the split biometric data reference are utilized in an MPC process which compares the shares of biometric data reference distributed and stored in more than one DSM server, with a biometric data sample of a user provided by the computerized device.

23. The method of claim 1, wherein the biometric data reference is stored as a whole in a DSM server.
24. The method of claim 23, wherein the biometric data reference stored as a whole in a DSM server is utilized in an MPC process which compares the biometric data reference with a biometric data sample provided by the computerized device.
25. A system for conducting security processes between a computerized device and a third-party server, comprising:

    at least one DSM server configured to receive a request to compare a biometric sample of a user with a biometric data reference split to shares, wherein said shares are distributed and stored in the computerized device and in the at least one DSM server;

    at least one secret storage located at the at least one DSM server designed to store shares of biometric data references;

    at least one MPC module located at the at least one DSM server designed to perform an MPC comparison process with said computerized device to compare a biometric sample of a user with biometric data reference split to shares, wherein the biometric sample is provided by said computerized device;

        and wherein the at least one DSM server is further configured to perform a security process between the computerized device and at least one DSM server, and the third-party server in case the MPC comparison process between the biometric sample of a user and the split biometric data reference, yields a match.
26. The system of claim 25, further comprises a user manager to associate the users with the biometric data references.
27. The system of claim 25, further comprises a second MPC module to perform an MPC process between the at least one DSM server and the computerized device.
28. The system of claim 25, wherein the computerized device further comprises a device for capturing a biometric data from a user.
29. The system of claim 25, wherein said shares of biometric data references are associated with users utilizing the computerized device.

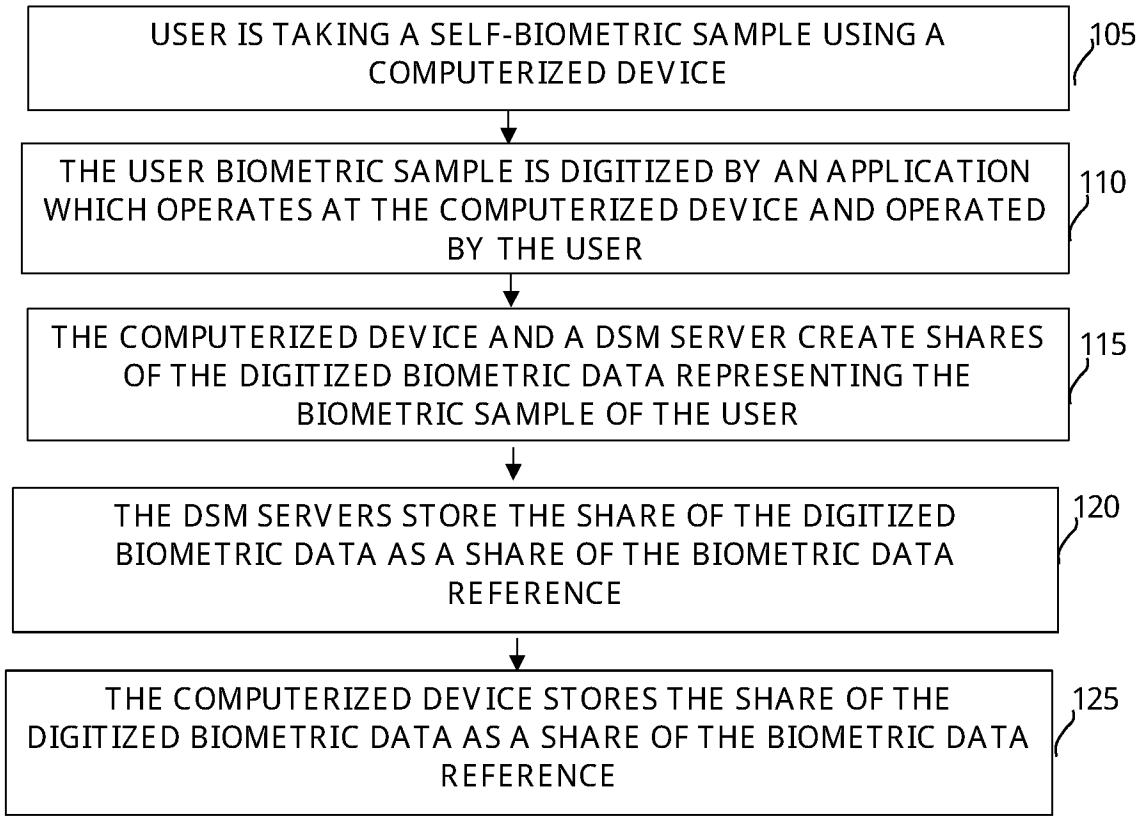

USER IS TAKING A SELF-BIOMETRIC SAMPLE USING A COMPUTERIZED DEVICE
105
THE USER BIOMETRIC SAMPLE IS DIGITIZED BY AN APPLICATION WHICH OPERATES AT THE COMPUTERIZED DEVICE AND OPERATED BY THE USER
110
THE COMPUTERIZED DEVICE AND A DSM SERVER CREATE SHARES OF THE DIGITIZED BIOMETRIC DATA REPRESENTING THE BIOMETRIC SAMPLE OF THE USER
115
THE DSM SERVERS STORE THE SHARE OF THE DIGITIZED BIOMETRIC DATA AS A SHARE OF THE BIOMETRIC DATA REFERENCE
120
THE COMPUTERIZED DEVICE STORES THE SHARE OF THE DIGITIZED BIOMETRIC DATA AS A SHARE OF THE BIOMETRIC DATA REFERENCE
125

Fig. 1A

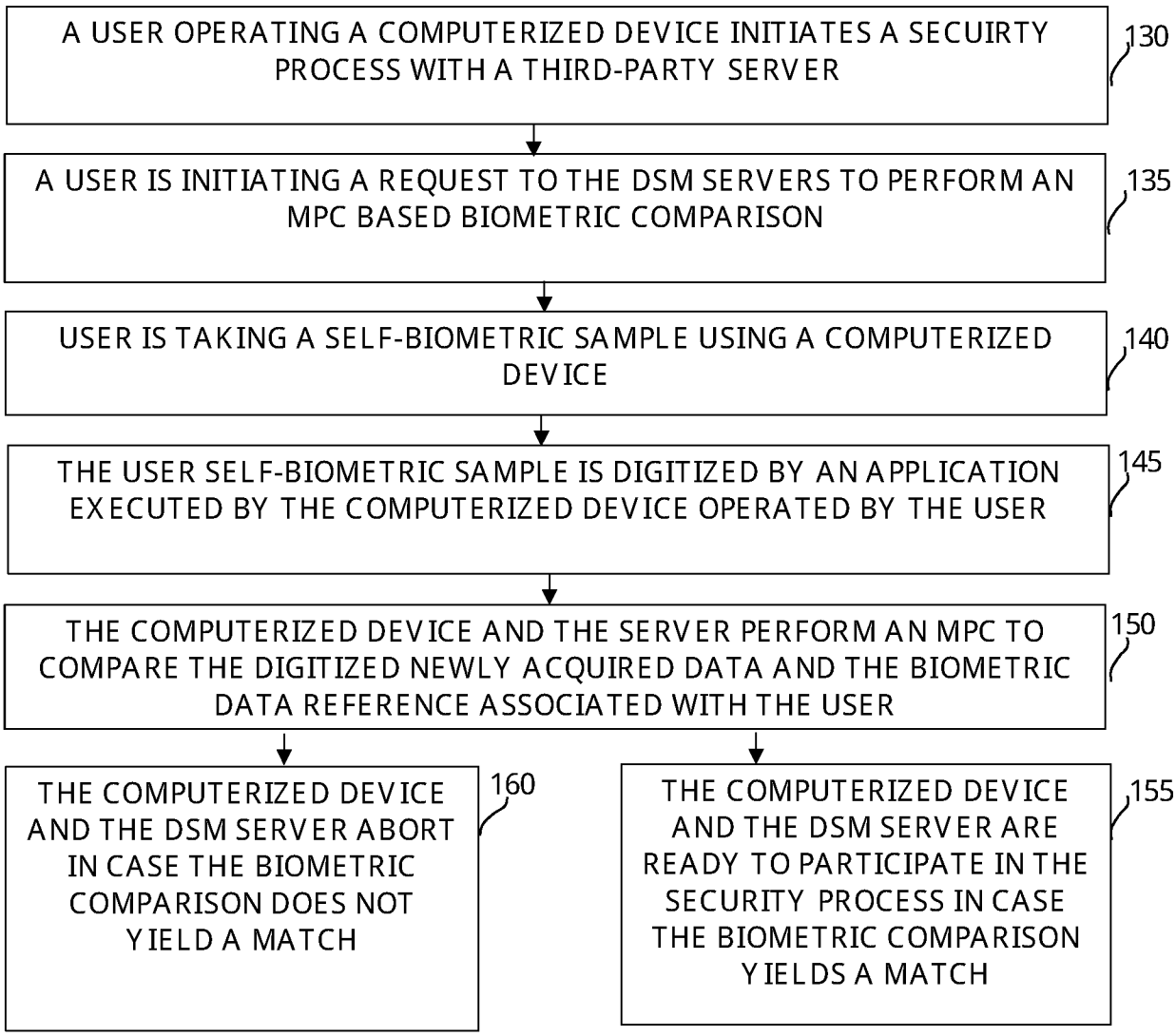

A USER OPERATING A COMPUTERIZED DEVICE INITIATES A SECUIRTY PROCESS WITH A THIRD-PARTY SERVER
130
A USER IS INITIATING A REQUEST TO THE DSM SERVERS TO PERFORM AN MPC BASED BIOMETRIC COMPARISON
135
USER IS TAKING A SELF-BIOMETRIC SAMPLE USING A COMPUTERIZED DEVICE
140
THE USER SELF-BIOMETRIC SAMPLE IS DIGITIZED BY AN APPLICATION EXECUTED BY THE COMPUTERIZED DEVICE OPERATED BY THE USER
145
THE COMPUTERIZED DEVICE AND THE SERVER PERFORM AN MPC TO COMPARE THE DIGITIZED NEWLY ACQUIRED DATA AND THE BIOMETRIC DATA REFERENCE ASSOCIATED WITH THE USER
150
THE COMPUTERIZED DEVICE AND THE DSM SERVER ABORT IN CASE THE BIOMETRIC COMPARISON DOES NOT YIELD A MATCH
160
THE COMPUTERIZED DEVICE AND THE DSM SERVER ARE READY TO PARTICIPATE IN THE SECURITY PROCESS IN CASE THE BIOMETRIC COMPARISON YIELDS A MATCH
155

Fig. 1B

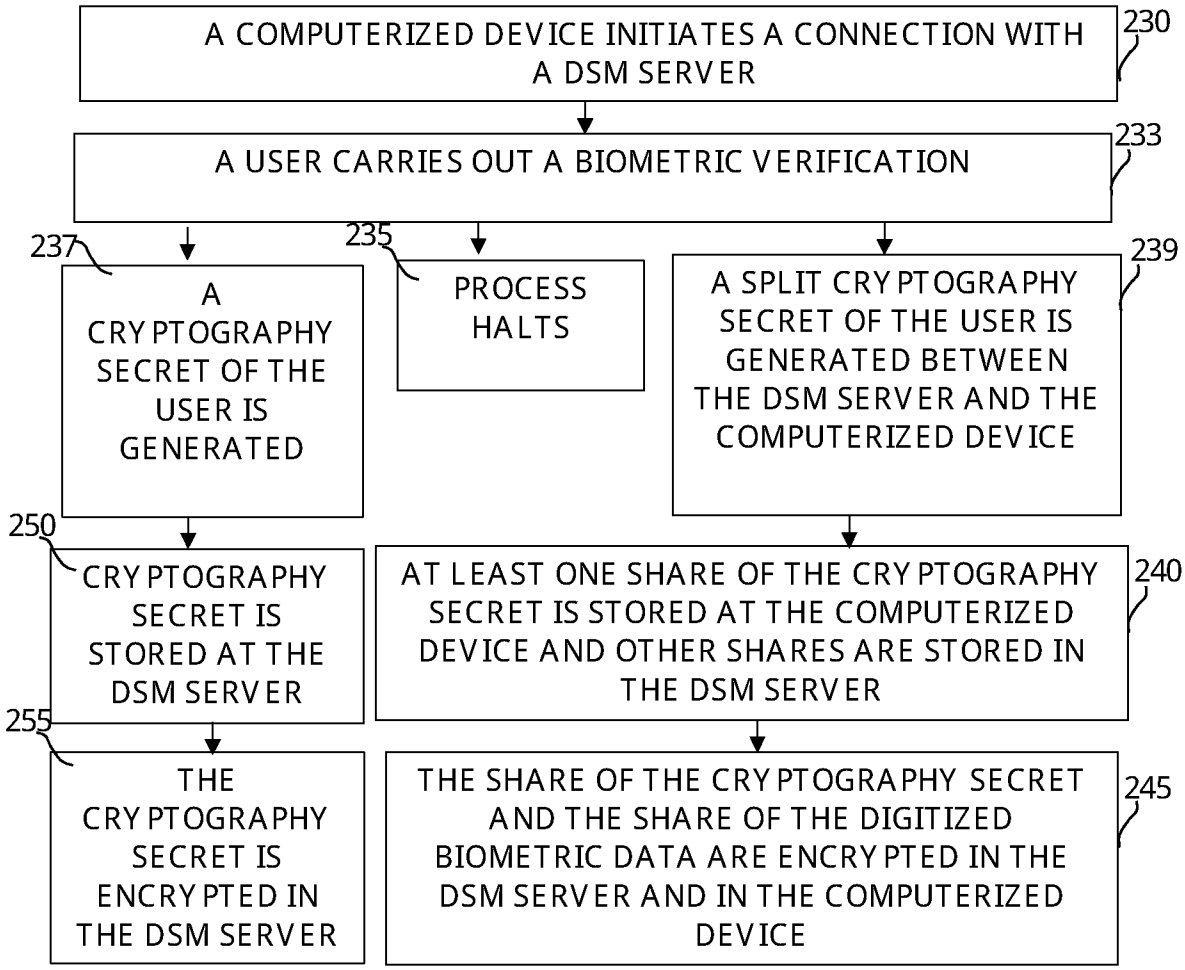

A COMPUTERIZED DEVICE INITIATES A CONNECTION WITH A DSM SERVER
230
A USER CARRIES OUT A BIOMETRIC VERIFICATION
233
237
A CRYPTOGRAPHY SECRET OF THE USER IS GENERATED
235
PROCESS HALTS
239
A SPLIT CRYPTOGRAPHY SECRET OF THE USER IS GENERATED BETWEEN THE DSM SERVER AND THE COMPUTERIZED DEVICE
250
CRYPTOGRAPHY SECRET IS STORED AT THE DSM SERVER
AT LEAST ONE SHARE OF THE CRYPTOGRAPHY SECRET IS STORED AT THE COMPUTERIZED DEVICE AND OTHER SHARES ARE STORED IN THE DSM SERVER
240
255
THE CRYPTOGRAPHY SECRET IS ENCRYPTED IN THE DSM SERVER
THE SHARE OF THE CRYPTOGRAPHY SECRET AND THE SHARE OF THE DIGITIZED BIOMETRIC DATA ARE ENCRYPTED IN THE DSM SERVER AND IN THE COMPUTERIZED DEVICE
245

Fig. 2

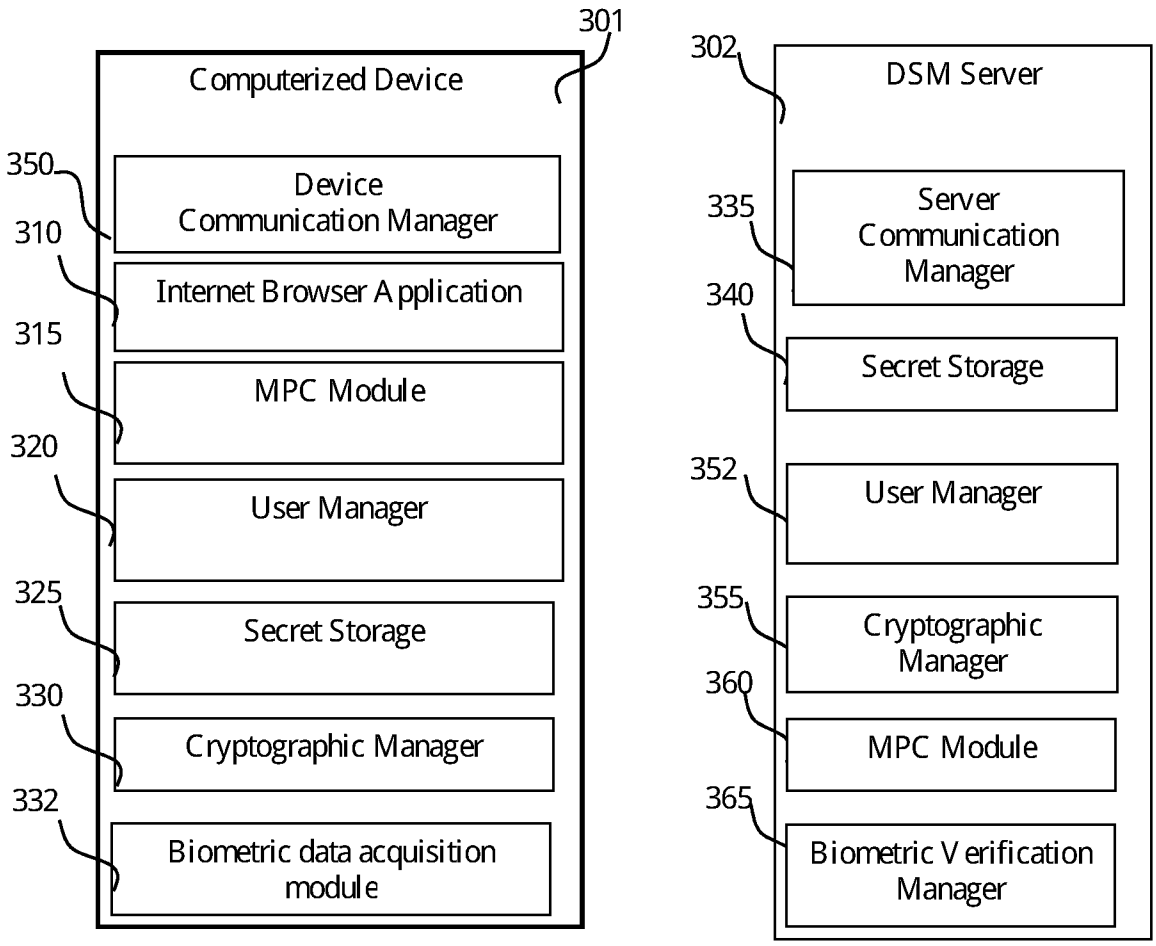

301
Computerized Device
350
Device Communication Manager
310
Internet Browser Application
315
MPC Module
320
User Manager
325
Secret Storage
330
Cryptographic Manager
332
Biometric data acquisition module
302
DSM Server
335
Server Communication Manager
340
Secret Storage
352
User Manager
355
Cryptographic Manager
360
MPC Module
365
Biometric Verification Manager

Fig. 3

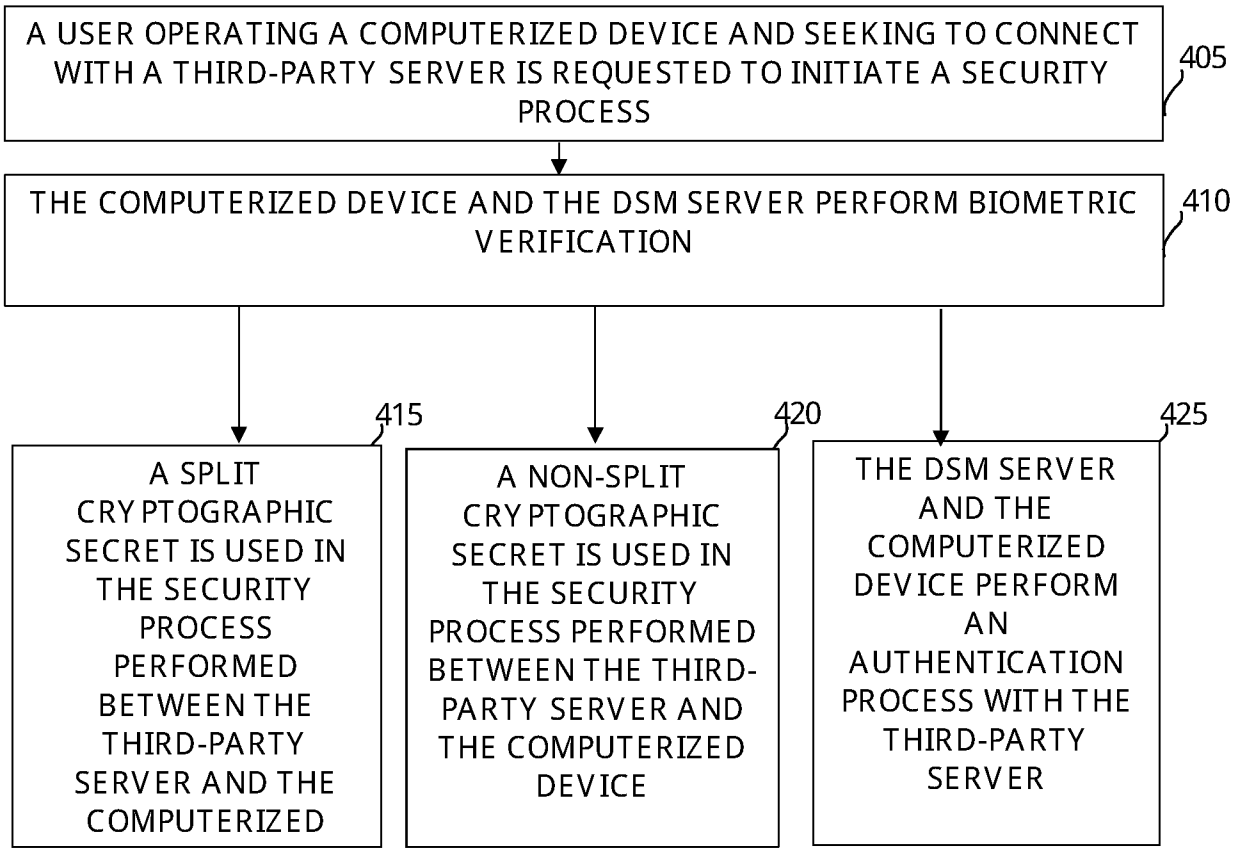

A USER OPERATING A COMPUTERIZED DEVICE AND SEEKING TO CONNECT WITH A THIRD-PARTY SERVER IS REQUESTED TO INITIATE A SECURITY PROCESS
405
THE COMPUTERIZED DEVICE AND THE DSM SERVER PERFORM BIOMETRIC VERIFICATION
410
415
A SPLIT CRYPTOGRAPHIC SECRET IS USED IN THE SECURITY PROCESS PERFORMED BETWEEN THE THIRD-PARTY SERVER AND THE COMPUTERIZED
420
A NON-SPLIT CRYPTOGRAPHIC SECRET IS USED IN THE SECURITY PROCESS PERFORMED BETWEEN THE THIRD-PARTY SERVER AND THE COMPUTERIZED DEVICE
425
THE DSM SERVER AND THE COMPUTERIZED DEVICE PERFORM AN AUTHENTICATION PROCESS WITH THE THIRD-PARTY SERVER

Fig. 4

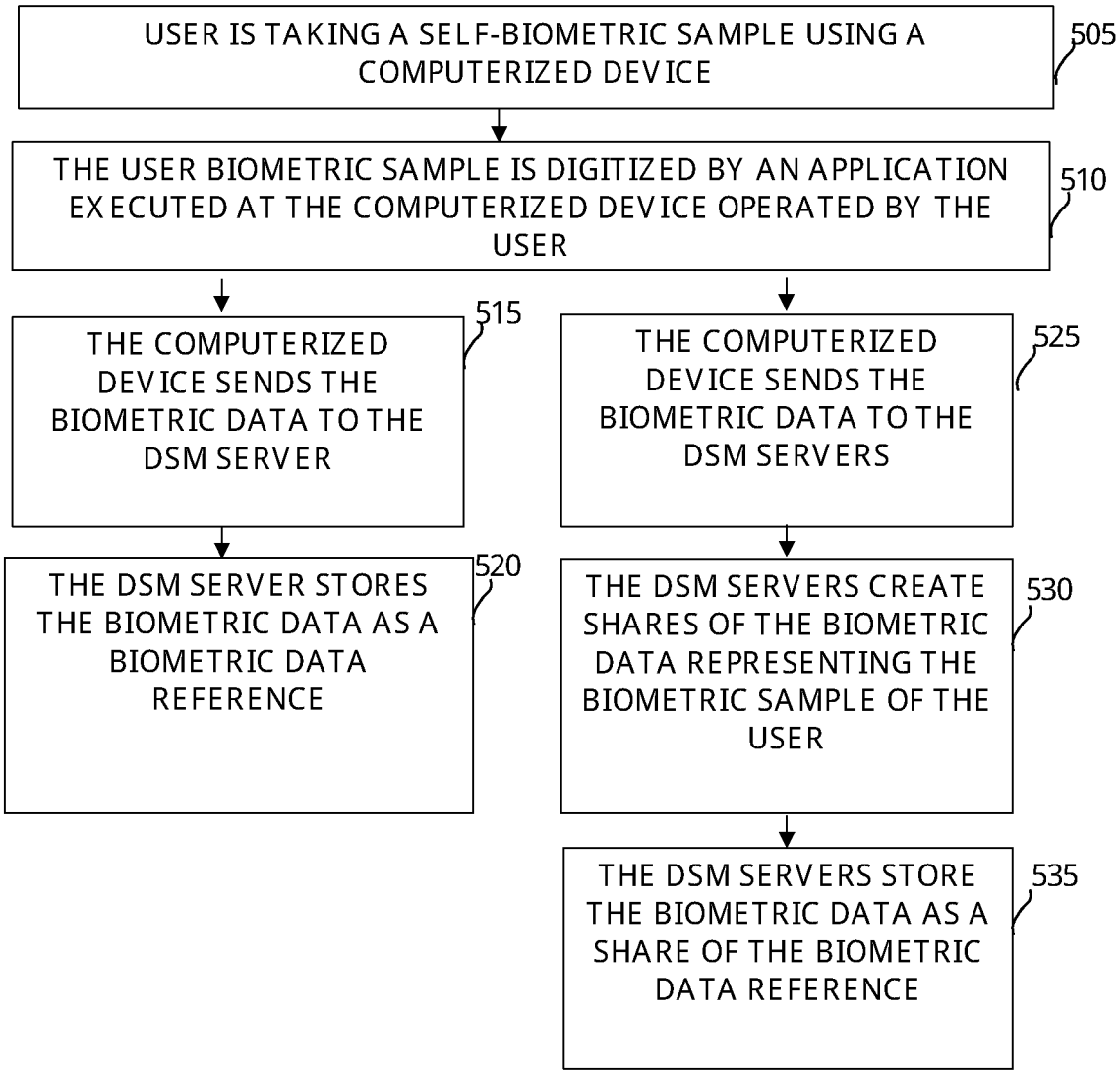

USER IS TAKING A SELF-BIOMETRIC SAMPLE USING A COMPUTERIZED DEVICE
505
THE USER BIOMETRIC SAMPLE IS DIGITIZED BY AN APPLICATION EXECUTED AT THE COMPUTERIZED DEVICE OPERATED BY THE USER
510
THE COMPUTERIZED DEVICE SENDS THE BIOMETRIC DATA TO THE DSM SERVER
515
THE DSM SERVER STORES THE BIOMETRIC DATA AS A BIOMETRIC DATA REFERENCE
520
THE COMPUTERIZED DEVICE SENDS THE BIOMETRIC DATA TO THE DSM SERVERS
525
THE DSM SERVERS CREATE SHARES OF THE BIOMETRIC DATA REPRESENTING THE BIOMETRIC SAMPLE OF THE USER
530
THE DSM SERVERS STORE THE BIOMETRIC DATA AS A SHARE OF THE BIOMETRIC DATA REFERENCE
535

Fig. 5A

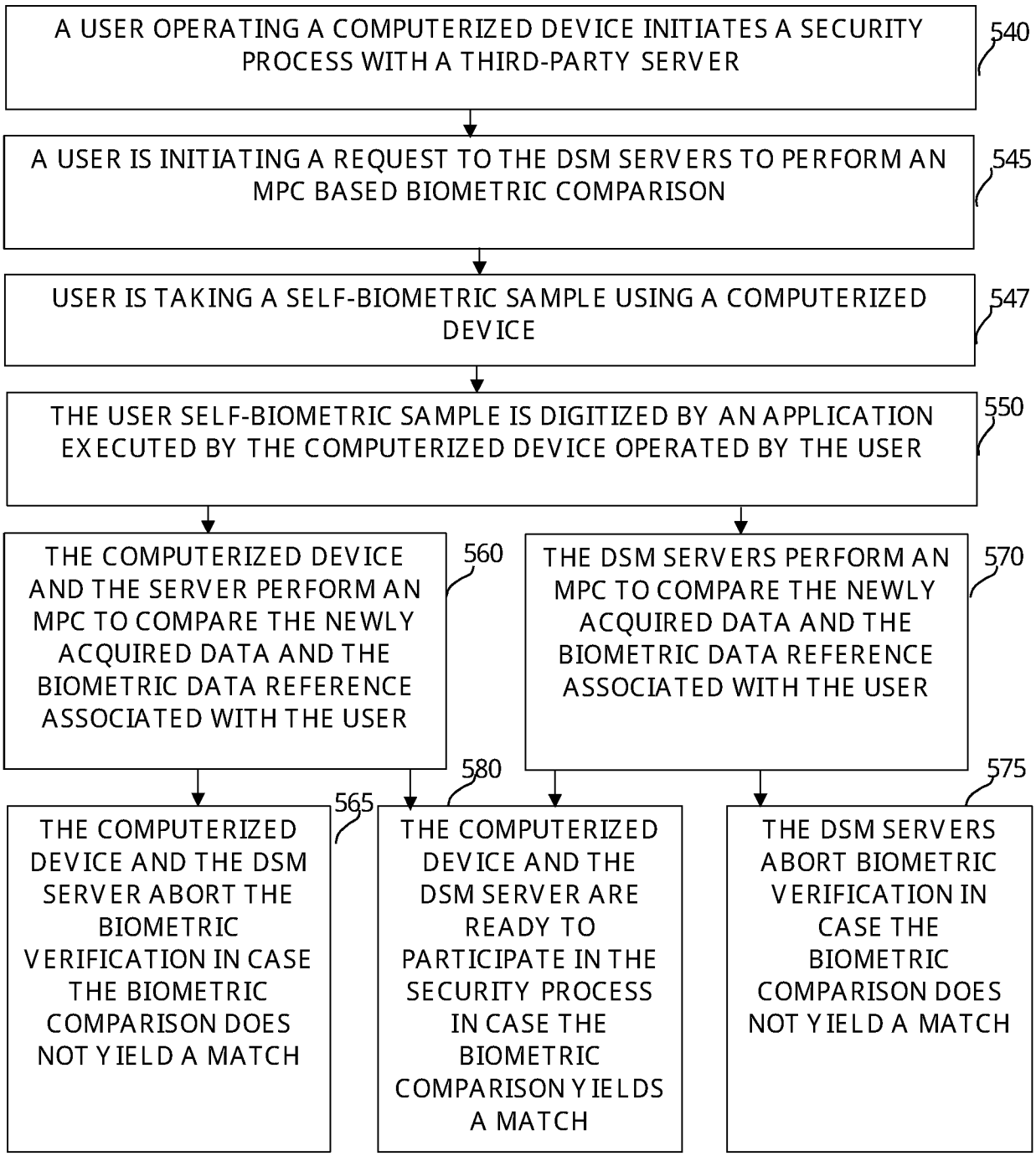

A USER OPERATING A COMPUTERIZED DEVICE INITIATES A SECURITY PROCESS WITH A THIRD-PARTY SERVER
540
A USER IS INITIATING A REQUEST TO THE DSM SERVERS TO PERFORM AN MPC BASED BIOMETRIC COMPARISON
545
USER IS TAKING A SELF-BIOMETRIC SAMPLE USING A COMPUTERIZED DEVICE
547
THE USER SELF-BIOMETRIC SAMPLE IS DIGITIZED BY AN APPLICATION EXECUTED BY THE COMPUTERIZED DEVICE OPERATED BY THE USER
550
THE COMPUTERIZED DEVICE AND THE SERVER PERFORM AN MPC TO COMPARE THE NEWLY ACQUIRED DATA AND THE BIOMETRIC DATA REFERENCE ASSOCIATED WITH THE USER
560
THE DSM SERVERS PERFORM AN MPC TO COMPARE THE NEWLY ACQUIRED DATA AND THE BIOMETRIC DATA REFERENCE ASSOCIATED WITH THE USER
570
565
THE COMPUTERIZED DEVICE AND THE DSM SERVER ABORT THE BIOMETRIC VERIFICATION IN CASE THE BIOMETRIC COMPARISON DOES NOT YIELD A MATCH
580
THE COMPUTERIZED DEVICE AND THE DSM SERVER ARE READY TO PARTICIPATE IN THE SECURITY PROCESS IN CASE THE BIOMETRIC COMPARISON YIELDS A MATCH
575
THE DSM SERVERS ABORT BIOMETRIC VERIFICATION IN CASE THE BIOMETRIC COMPARISON DOES NOT YIELD A MATCH

Fig. 5B

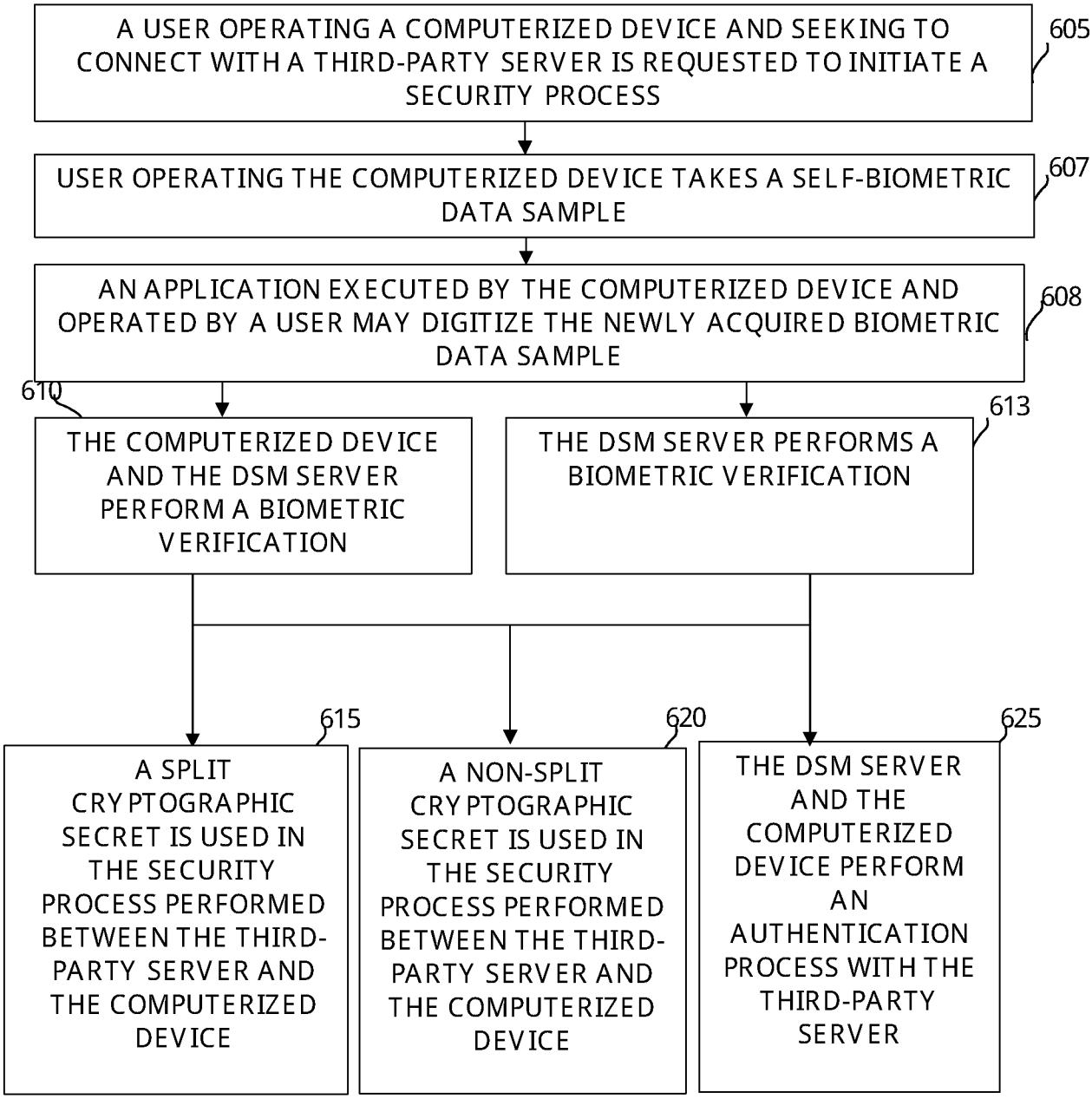

A USER OPERATING A COMPUTERIZED DEVICE AND SEEKING TO CONNECT WITH A THIRD-PARTY SERVER IS REQUESTED TO INITIATE A SECURITY PROCESS
605
USER OPERATING THE COMPUTERIZED DEVICE TAKES A SELF-BIOMETRIC DATA SAMPLE
607
AN APPLICATION EXECUTED BY THE COMPUTERIZED DEVICE AND OPERATED BY A USER MAY DIGITIZE THE NEWLY ACQUIRED BIOMETRIC DATA SAMPLE
608
610
THE COMPUTERIZED DEVICE AND THE DSM SERVER PERFORM A BIOMETRIC VERIFICATION
THE DSM SERVER PERFORMS A BIOMETRIC VERIFICATION
613
615
A SPLIT CRYPTOGRAPHIC SECRET IS USED IN THE SECURITY PROCESS PERFORMED BETWEEN THE THIRD-PARTY SERVER AND THE COMPUTERIZED DEVICE
620
A NON-SPLIT CRYPTOGRAPHIC SECRET IS USED IN THE SECURITY PROCESS PERFORMED BETWEEN THE THIRD-PARTY SERVER AND THE COMPUTERIZED DEVICE
625
THE DSM SERVER AND THE COMPUTERIZED DEVICE PERFORM AN AUTHENTICATION PROCESS WITH THE THIRD-PARTY SERVER

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2017/050660

A. CLASSIFICATION OF SUBJECT MATTER
IPC (2017.01) G06F 21/32, G06F 21/62

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 (2017.01) G06F 21/32, G06F 21/62

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Databases consulted: Esp@cenet, Google Patents

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5588061 A (GANESAN et al.) 24 Dec 1996 (1996/12/24) Entire document	1-29
Y	WO 2014108835 A2 (LINDELL) 17 Jul 2014 (2014/07/17) Entire document	1-29
A	US 8135180 B2 (BALTATU et al.) 13 Mar 2012 (2012/03/13) Entire document	1-29
A	US 9165130 B2 (MALPANI et al.) 20 Oct 2015 (2015/10/20) Entire document	1-29
P,X	WO 2016135737 A1 (PE'ER et al.) 01 Sep 2016 (2016/09/01) Entire document	1-29

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

[X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier 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
19 Oct 2017	22 Oct 2017
Name and mailing address of the ISA: Israel Patent Office Technology Park, Bldg.5, Malcha, Jerusalem, 9695101, Israel Facsimile No. 972-2-5651616	Authorized officer AKERMAN Albert Telephone No. 972-2-5651754

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL2017/050660

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	US 2017134375 A1 (WAGNER) 11 May 2017 (2017/05/11) Entire document	1-29

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2017/050660

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
US 5588061 A	24 Dec 1996	US 5588061 A	24 Dec 1996
		US 5905799 A	18 May 1999
WO 2014108835 A2	17 Jul 2014	WO 2014108835 A2	17 Jul 2014
		WO 2014108835 A3	06 Nov 2014
		EP 2904759 A2	12 Aug 2015
		EP 2904759 A4	08 Jun 2016
		IL 237990 D0	30 Nov 2015
		JP 2016502377 A	21 Jan 2016
		US 2015349958 A1	03 Dec 2015
WO 2016135737 A1	01 Sep 2016	WO 2016135737 A1	01 Sep 2016
		WO 2016135738 A1	01 Sep 2016
US 8135180 B2	13 Mar 2012	US 2008019573 A1	24 Jan 2008
		US 8135180 B2	13 Mar 2012
		BR PI0418089 A	17 Apr 2007
		EP 1697907 A1	06 Sep 2006
		JP 2007522540 A	09 Aug 2007
		JP 4869944 B2	08 Feb 2012
		JP 2012044670 A	01 Mar 2012
		JP 5470344 B2	16 Apr 2014
		KR 20060127080 A	11 Dec 2006
		KR 101226651 B1	25 Jan 2013
		WO 2005064547 A1	14 Jul 2005
US 2017134375 A1	11 May 2017	US 2017134375 A1	11 May 2017
		WO 2017083016 A1	18 May 2017
US 9165130 B2	20 Oct 2015	US 2014139318 A1	22 May 2014
		US 9165130 B2	20 Oct 2015

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IL2017/050660

Patent document cited search report	Publication date	Patent family member(s)	Publication Date
---	---	---	---