(12) STANDARD PATENT (11) Application No. **AU 2017239211 B2**
(19) AUSTRALIAN PATENT OFFICE

(54) Title
Identity registration method and device

(51) International Patent Classification(s)
H04L 9/32 (2006.01)

(21) Application No: **2017239211** (22) Date of Filing: **2017.03.20**

(87) WIPO No: **WO17/162112**

(30) Priority Data

(31) Number	(32) Date	(33) Country
201610180030.4	**2016.03.25**	**CN**

(43) Publication Date: **2017.09.28**
(44) Accepted Journal Date: **2021.02.18**

(71) Applicant(s)
Advanced New Technologies Co., Ltd.

(72) Inventor(s)
Meng, Fei

(74) Agent / Attorney
Spruson & Ferguson, Level 24 Tower 2 Darling Park 201 Sussex Street, Sydney, NSW, 2000, AU

(56) Related Art
CN 104253818 A
US 2014/0354401 A1
US 2015/0312041 A1
US 2004/0059924 A1

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2017 年 9 月 28 日 (28.09.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/162112 A1

(51) **国际专利分类号**:
H04L 9/32 (2006.01)

(21) **国际申请号**: PCT/CN2017/077247

(22) **国际申请日**: 2017 年 3 月 20 日 (20.03.2017)

(25) **申请语言**: 中文

(26) **公布语言**: 中文

(30) **优先权**:
201610180030.4 2016 年 3 月 25 日 (25.03.2016) CN

(71) **申请人**: **阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED)** [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) **发明人**: **孟飞 (MENG, Fei)**; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) **代理人**: **北京三友知识产权代理有限公司 (BEIJING SANYOU INTELLECTUAL PROPERTY AGENCY LTD.)**; 中国北京市金融街 35 号国际企业大厦 A 座 16 层, Beijing 100033 (CN)。

(81) **指定国** (除另有指明，要求每一种可提供的国家保护): 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, 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。

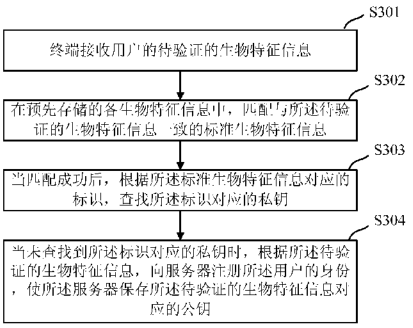
(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: IDENTITY REGISTRATION METHOD AND DEVICE

(54) **发明名称**: 一种身份注册方法及装置



S301
终端接收用户的待验证的生物特征信息
S302
在预先存储的各生物特征信息中，匹配与所述待验证的生物特征信息一致的标准生物特征信息
S303
当匹配成功后，根据所述标准生物特征信息对应的标识，查找所述标识对应的私钥
S304
当未查找到所述标识对应的私钥时，根据所述待验证的生物特征信息，向服务器注册所述用户的身份，使所述服务器保存所述待验证的生物特征信息对应的公钥

图 3

S301 A terminal receiving biometric information about a user to be verified

S302 Matching, in various pieces of pre-stored biometric information, standard biometric information consistent with the biometric information to be verified

S303 After the matching succeeds, searching for a private key corresponding to an identifier according to the identifier corresponding to the standard biometric information

S304 When the private key corresponding to the identifier is not found, registering the identity of the user to a server according to the biometric information to be verified, so that the server saves a public key corresponding to the biometric information to be verified

(57) **Abstract**: Disclosed are an identity registration method and device. The method comprises: a terminal receiving biometric information about a user to be verified, matching standard biometric information consistent with the biometric information to be verified, and when a private key corresponding to an identifier is not found according to the identifier corresponding to the standard biometric information, registering the identity of the user to a server according to the biometric information to be verified, so that the server saves a public key corresponding to the biometric information to be verified. By means of the method, no matter which biometric information is used by a user for registration, as long as the biometric information to be verified has been stored locally at the terminal, the identity of the user can be registered directly according to the biological characteristic information to be verified, so to complete service processing, bringing about great convenience to the user in using a service, and also effectively improving the success rate of using the service at the same time.

(57) **摘要**:

[见续页]

本申请公开了一种身份注册方法及装置，该方法由终端接收用户的待验证的生物特征信息，匹配与该待验证的生物特征信息一致的标准生物特征信息，当根据该标准生物特征信息对应的标识，未查找该标识对应的私钥时，根据该待验证的生物特征信息，向服务器注册该用户的身份，使服务器保存该待验证的生物特征信息对应的公钥。通过上述方法，无论用户注册时使用的生物特征信息是哪个，只要待验证的生物特征信息已经保存在终端本地，就可直接根据该待验证的生物特征信息，注册该用户的身份，进而完成业务处理，给用户使用业务带来很大的便利，同时也有效的提高了使用业务的成功率。

IDENTITY REGISTRATION METHOD AND DEVICE

[0001] The present application claims priority to Chinese Patent Application No. 201610180030.4, filed on March 25, 2016 and entitled "IDENTITY REGISTRATION METHOD AND DEVICE", which is incorporated here by reference in its entirety.

TECHNICAL FIELD

[0002] The present application relates to the field of computer technologies, and in particular, to an identity registration method and device.

BACKGROUND

[0003] With the continuous development of network technologies, using services through the network has become an integral part of people's life, for example, people use a weather forecast service through the network.

[0004] Currently, to improve information security when a user uses a service, the user needs to register a user identity in advance for the service before using the service. Later, when using the service through the network, the user identity needs to be verified. The user can use the service only after the verification succeeds. For example, if fingerprint information is used to represent the user identity, the fingerprint information of the user needs to be registered in advance.

[0005] Because fingerprint information recognition in actual applications is increasingly popular in terminal devices, for example, fingerprint information of a user is used to unlock a locked screen interface. For any service, a process in which a server of the service registers a user identity by using the fingerprint information of the user, and later verifies the user identity by using the fingerprint information of the user can be completed by using a terminal device.

[0006] Further, with the continuous improvement of the computer technologies, a plurality of fingerprint information of a user can be stored in a terminal device at the same time. For any service, when a user identity is registered by using the fingerprint information uploaded by the user, the terminal device first needs to verify whether the fingerprint information is one of the plurality of fingerprint information stored in the terminal device. If yes, the terminal device can register the user identity with a server based on the fingerprint information, and if no, the terminal device directly notifies the user that the identity registration fails.

[0007] In the existing technology, a process of registering fingerprint information of a user is shown in FIG. 1.

[0008] S101. A terminal device receives a registration operation of a user.

[0009] S102. Collect fingerprint information of the user.

[0010] S103. Determine whether the fingerprint information has been pre-stored in the terminal device, and if yes, perform S104, or otherwise, perform S105.

[0011] S104. Query an identifier corresponding to the pre-stored fingerprint information in the terminal device, generate a private key and a public key corresponding to the identifier, store a mapping relationship between the private key and the identifier corresponding to the fingerprint information in the terminal device, and send a mapping relationship between the public key and the identifier corresponding to the fingerprint information to a server for storage.

[0012] S105. Notify the user that registration fails.

[0013] Later, a process of a user using a service is shown in FIG. 2.

[0014] S201. A terminal device receives fingerprint information of a user.

[0015] S202. Match standard biometric feature information consistent with the fingerprint information.

[0016] S203. Search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information.

[0017] S204. When the private key corresponding to the identifier is identified, sign service information by using the private key, and add the signed service information and the identifier corresponding to the fingerprint information to a service processing request and send the request to a server, so the server determines a public key corresponding to the identifier included in the received service processing request and performs service processing based on the public key and the service information. Alternatively, when the private key corresponding to the identifier is not identified, notify the user that the service processing fails.

[0018] However, in actual applications, if a user forgets which fingerprint is entered, the user needs to perform fingerprint verification for a plurality of times. It causes great inconvenience to the user to use a service, and reduces the success rate of using the service. In addition, if a user's finger used for registration is injured in daily life, the user cannot be authenticated to use the service.

SUMMARY

[0018a] It is an object of the present invention to substantially overcome, or at least ameliorate, one or more disadvantages of existing arrangements.

[0019] Implementations of the present application provide an identity registration method and device, to resolve existing-technology problems: a user forgets which fingerprint is entered and consequently it causes inconvenience to the user to use a service; and if a user's finger used for registration is injured in daily life, the user cannot be authenticated to use the service.

[0019a] An implementation of the present application provides a computer-implemented method, comprising: receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request; matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier; in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user; in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises: generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user; storing a mapping relationship between the identifier and the generated private key in the terminal device; and transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

[0019b] An implementation of the present application provides a non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising: receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request; matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier; in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user; and in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises: generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user; storing a mapping relationship between the identifier and the generated private key in the terminal device; and transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

[0019c] An implementation of the present application provides a computer-implemented system, comprising: one or more computers; and one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising: receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request; matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier; in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user; and in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises: generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user; storing a mapping relationship between the identifier and the generated private key in the terminal device; and transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

[0020] An implementation of the present application provides an identity registration method, and the method includes the following: receiving, by a terminal device, biometric feature information of a user that is to be verified; matching standard biometric feature information consistent with the biometric feature information to be verified in pre-stored biometric feature information; searching for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information after the matching succeeds; and registering a user identity with a server based on the biometric feature information to be verified when the private key corresponding to the identifier is not identified, so the server stores a public key corresponding to the biometric feature information to be verified.

[0021] An implementation of the present application provides an identity registration device, and the device includes the following: a receiving module, configured to receive biometric feature information of a user that is to be verified; a matching module, configured to match standard biometric feature information consistent with the biometric feature information to be verified in pre-stored biometric feature information; a search module, configured to search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information after the matching succeeds; and a registration module, configured to register a user identity with a server based on the biometric feature information to be verified when the private key corresponding to the identifier is not identified, so the server stores a public key corresponding to the biometric feature information to be verified.

[0022] The implementations of the present application disclose an identity registration method and device. In the method, the terminal device receives the biometric feature information of the user that is to be verified, and matches the standard biometric feature information consistent with the biometric feature information to be verified. After the matching succeeds, the terminal device searches for the private key corresponding to the identifier based on the identifier corresponding to the standard biometric feature information, and registers the user identity with the server based on the biometric feature information to be verified when the private key corresponding to the identifier is not identified. As such, the server stores the public key corresponding to the biometric feature information to be verified. According to the previous method, regardless of biometric feature information used by the user for registration, provided that the terminal device can identify standard biometric feature information consistent with biometric feature information to be verified, even if a private key corresponding to an identifier is not identified in the terminal device based on the identifier corresponding to the standard biometric feature information, the terminal device can directly register the user identity based on the biometric feature information to be verified, to complete service processing, provide great convenience for the user to use a service, and also effectively improve the success rate of using the service.

BRIEF DESCRIPTION OF DRAWINGS

[0023] The accompanying drawings described here are intended to provide a further understanding of the present application, and constitute a part of the present application. The illustrative implementations of the present application and descriptions of the implementations are intended to describe the present application, and do not constitute limitations on the present application. In the accompanying drawings:

[0024] FIG. 1 is a schematic diagram illustrating a process of registering fingerprint information of a user in the existing technology, according to an implementation of the present application;

[0025] FIG. 2 is a schematic diagram illustrating a process of using a service by a user in the existing technology, according to an implementation of the present application;

[0026] FIG. 3 is a schematic diagram illustrating an identity registration process, according to an implementation of the present application; and

[0027] FIG. 4 is a schematic structural diagram illustrating an identity registration device, according to an implementation of the present application.

DESCRIPTION OF EMBODIMENTS

[0028] To make the objectives, technical solutions, and advantages of the present application clearer, the following describes the technical solutions of the present application with reference to specific implementations of the present application and corresponding accompanying drawings. Apparently, the described implementations are merely some rather than all of the implementations of the present application. Other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0029] FIG. 3 shows an identity registration process, according to an implementation of the present application. The process includes the following steps.

[0030] S301. A terminal device receives biometric feature information of a user that is to be verified.

[0031] In actual applications, to improve information security when a user uses a service, in a process of using the service, an identity of the current user first needs to be verified to confirm that the identity of the current user is valid.

[0032] Therefore, in the present application, the biometric feature information of the user that is to be verified is first received. Because biometric feature information recognition is increasingly popular in terminal devices (for example, mobile phones) in actual applications, the biometric feature information of the user that is to be verified can be received by a terminal device. After receiving the biometric feature information, the terminal device makes a corresponding response. The biometric feature information indicates a physical sign of the user, and it can be an iris of an eye or a fingerprint of a finger, and is mainly used to uniquely represent a user identity.

[0033] In addition, in actual applications, for verifying the identity of the current user, fingerprint information verification is increasingly popular and the technology is relatively mature. Therefore, that the biometric feature information is fingerprint information is used as an example for detailed description below.

[0034] For example, assume that a certain forum provides an information query service only for a user who has registered an account, and the user can log in by using fingerprint information. Therefore, when the user needs to query information in the forum, the user opens an application corresponding to the forum on a mobile phone (that is, the terminal device) and presses with a fingerprint. Later, the mobile phone (that is, the terminal device) receives the fingerprint information of the user that is to be verified, and performs step S302.

[0035] S302. Match standard biometric feature information consistent with the biometric feature information to be verified in pre-stored biometric feature information.

[0036] Because fingerprint information (that is, biometric feature information) recognition in actual applications is increasingly popular in terminal devices, for example, fingerprint information of a user is used to unlock a locked screen interface. For any service, a process in which a server of the service registers a user identity by using the fingerprint information of the user, and later verifies the user identity by using the fingerprint information of the user can be completed by using fingerprint information that has been stored in a terminal device. In other words, provided that fingerprint information is stored in a terminal device, the fingerprint information can be used to complete the entire service processing in the present application.

[0037] It is worthwhile to note here that the fingerprint information stored in the terminal device can be entered by the user when the user uses another function of the terminal device, and is not the fingerprint information used by the user for identity registration for using a service. For example, when the user uses a function of the terminal device to unlock a locked screen interface by using the fingerprint information, the terminal device can locally store the fingerprint information.

[0038] In addition, in the present application, to distinguish between the stored fingerprint information and fingerprint information received by the terminal device when the user uses the service, the stored fingerprint information can be used as standard fingerprint information (that is, standard biometric feature information), and is mainly used to check whether the user can be authenticated in a process of using the service and to provide service processing for the user.

[0039] Therefore, in the present application, after receiving the fingerprint information (that is, the biometric feature information) of the user that is to be verified, the terminal device directly matches locally stored standard fingerprint information (that is, the standard biometric feature information) consistent with the fingerprint information to be verified.

[0040] Continuing with the earlier described example, after receiving the fingerprint information of the user that is to be verified, the mobile phone matches the locally stored standard fingerprint information consistent with the fingerprint information to be verified. Assume that the standard fingerprint information consistent with the fingerprint information to be verified is identified.

[0041] S303. Search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information after the matching succeeds.

[0042] In the present application, to distinguish each piece of fingerprint information (that is, biometric feature information) that has been stored in the terminal device, the terminal device can allocate a fingerprint information identifier (that is, a biometric feature information identifier) to each piece of fingerprint information when storing the fingerprint information.

[0043] In addition, for verifying a user identity by a server corresponding to a future service, to be specific, the server corresponding to the service needs to know the user who uses the service. In the present application, a private key and a public key corresponding to an identifier need to be generated based on the identifier. The identifier is corresponding to fingerprint information used for registration. The private key and the public key represent a user identity. The generated private key is stored in the terminal device. When sending a service processing request to the server, the terminal device needs to use the private key to sign the service processing request, and sends the signed service processing request to the server.

[0044] Therefore, in the present application, after identifying the standard fingerprint information consistent with the fingerprint information to be verified, the terminal device needs to search for the private key corresponding to the identifier based on the identifier corresponding to the standard fingerprint information.

[0045] Continuing with the earlier described example, after identifying the standard fingerprint information consistent with the fingerprint information to be verified, the mobile phone searches for the private key corresponding to the identifier based on the identifier corresponding to the standard fingerprint information.

[0046] S304. Register a user identity with a server based on the biometric feature information to be verified when the private key corresponding to the identifier is not identified, so the server stores a public key corresponding to the biometric feature information to be verified.

[0047] In the present application, if the terminal device identifies the standard fingerprint information consistent with the fingerprint information to be verified in step S302, but the terminal device does not identify the private key corresponding to the identifier based on the identifier corresponding to the standard fingerprint information, it indicates that the fingerprint information to be verified belongs to the user, but is not the fingerprint information used during registration. To continue to provide the required service for the user, the user identity can be directly registered with the server based on the fingerprint information (that is, the biometric feature information) that is to be verified.

[0048] In addition, the present application provides a specific process of registering a user identity below:

[0049] The private key and the public key corresponding to the identifier are generated based on the identifier corresponding to the standard biometric feature information that matches the biometric feature information to be verified; a mapping relationship between the identifier and the generated private key is stored in the terminal device; and a mapping relationship between the identifier and the generated public key is sent to the server for storage.

[0050] It is worthwhile to note here that the standard biometric feature information uniquely corresponds to a standard biometric feature information identifier, and a standard biometric feature information identifier corresponds to a unique private key and public key. In other words, the standard biometric feature information and the standard biometric feature information identifier are in a one-to-one mapping relationship with a private key and a public key. In the present application, if the biometric feature information to be verified exists in the terminal device, in step S302, only one piece of standard biometric feature information can be identified. In other words, sending the mapping relationship between the identifier and the generated public key to the server for storage can also be storing, by the server, the public key corresponding to the biometric feature information to be verified.

[0051] Although the private key corresponding to the fingerprint information (that is, biometric feature information) is not found locally in the terminal device, the fingerprint information may not be fingerprint information of the user. To further improve information security when the user uses the service, in the present application, before the user identity is registered with the server based on the biometric feature information to be verified, the user can be prompted to enter a password for the service. When the password entered by the user is received, the terminal device verifies whether the password is correct. If the password is correct, the user identity can be registered with the server based on the biometric feature information to be verified. If the password is incorrect, the user identity is not registered with the server based on the biometric feature information to be verified, and the user is notified that service processing fails.

[0052] In addition, it is worthwhile to note here that when the terminal device does not identify the private key corresponding to the identifier, the terminal device can directly notify the user that service processing fails. In such case, the user can enter a password for the service to continue to use the service. The terminal device can receive the password entered by the user and verify whether the password is correct, and if yes, registers the user identity with the server based on the biometric feature information to be verified.

[0053] Continuing with the earlier described example, assume that the mobile phone has not identified the private key corresponding to the identifier. The mobile phone prompts the user to use a password for the information query service. Assume that the user enters the password xxxx. After receiving the password xxxx that is entered by the user, if the terminal device verifies that the password is correct, the terminal device generates the private key and the public key corresponding to the identifier, where the identifier is corresponding to the standard fingerprint information that matches the fingerprint information to be verified based on the identifier, stores a mapping relationship between the identifier and the generated private key in the mobile phone, and sends a mapping relationship between the identifier and the generated public key to the server for storage.

[0054] According to the previous method, regardless of biometric feature information used by the user for registration, provided that the terminal device can identify standard biometric feature information consistent with biometric feature information to be verified, even if a private key corresponding to an identifier is not identified in the terminal device based on the identifier corresponding to the standard biometric feature information, the terminal device can directly register the user identity based on the biometric feature information to be verified, to complete service processing, provide great convenience for the user to use a service, and also effectively improve the success rate of using the service.

[0055] Further, in actual applications, a service processing request can be sent to the server based on the biometric feature information to be verified after the user identity is registered with the server. As such, the server performs service processing based on the public key corresponding to the biometric feature information to be verified.

[0056] In step S304, the private key and the public key corresponding to the identifier of the fingerprint information (that is, the biometric feature information) have been re-generated based on the fingerprint information to be verified, and the public key is sent to the server for storage. Therefore, in a process of sending a service processing request to the server based on the fingerprint information to be verified, the present application can include the following: signing service information based on the generated private key and sending the service processing request that includes the signed service information and the identifier to the server, so the server determines the public key corresponding to the identifier included in the service processing request based on the identifier, verifies the signature of the service information included in the service processing request based on the determined public key to verify the user identity, and performs service processing on the service information.

[0057] Continuing with the earlier described example, the mobile phone signs login information based on the generated private key of the identifier, and sends a login processing request that includes the signed login information and the identifier to the server. The server identifies a public key corresponding to the identifier based on the identifier included in the login processing request, verifies the signature of the login information included in the login processing request by using the public key, and completes login of the user.

[0058] In actual applications, paying for purchased merchandise by using a payment application has become increasingly popular. In the present application, the following describes the present disclosure in detail by using an example in which a service processing request is a payment request.

[0059] For example, assume that user A has registered fingerprint information (that is, identity information) in a payment application. When user A pays for purchased merchandise by using the payment application, user A opens the payment application on the mobile phone (that is, the terminal device) and presses with a fingerprint. After receiving fingerprint information of the user that is to be verified, the mobile phone locally matches standard fingerprint information consistent with the fingerprint information to be verified. Assume that the standard fingerprint information consistent with the fingerprint information to be verified is identified. The mobile phone searches for a private key corresponding to an identifier based on the identifier corresponding to the standard fingerprint information. If the mobile phone does not identify the private key corresponding to the identifier, the mobile phone directly prompts the user to enter a payment password. The mobile phone receives the payment password cccc entered by the user and verifies whether the password is correct. If yes, the mobile phone generates the private key and a public key corresponding to an identifier, where the identifier is corresponding to the standard fingerprint information that matches the fingerprint information to be verified based on the identifier, stores a mapping relationship between the identifier and the generated private key in the mobile phone, and sends a mapping relationship between the identifier and the generated public key to the server for storage.

[0060] In a later process of processing a payment service, the mobile phone signs payment information based on the generated private key corresponding to the identifier and sends a payment processing request that includes the signed payment information and the identifier to the server. The server identifies the public key corresponding to the identifier based on the identifier included in the payment processing request, verifies the signature of the payment information by using the public key, and successfully completes payment.

[0061] What is described above is the identity registration method provided in the implementation of the present application. As shown in FIG. 4, based on the same idea, the present application further provides a corresponding identity registration device.

[0062] FIG. 4 is a schematic structural diagram illustrating an identity registration device, according to an implementation of the present application. The device includes the following: a receiving module 401, configured to receive biometric feature information of a user that is to be verified; a matching module 402, configured to match standard biometric feature information consistent with the biometric feature information to be verified in pre-stored biometric feature information; a search module 403, configured to search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information after the matching succeeds; and a registration module 404, configured to register a user identity with a server based on the biometric feature information to be verified when the search module 403 does not identify the private key corresponding to the identifier, so the server stores a public key corresponding to the biometric feature information to be verified.

[0063] The device further includes the following: a password verification module 405, configured to receive a password entered by the user and verify that the password is correct before the registration module 404 registers the user identity with the server based on the biometric feature information to be verified.

[0064] The registration module 404 is configured to generate the private key and the public key corresponding to the identifier based on the identifier corresponding to the standard biometric feature information that matches the biometric feature information to be verified; store a mapping relationship between the identifier and the generated private key in a terminal device; and send a mapping relationship between the identifier and the generated public key to the server for storage.

[0065] The device further includes the following: a processing module 406, configured to send a service processing request to the server based on the biometric feature information to be verified after the registration module 404 registers the user identity with the server, so the server performs service processing based on the public key corresponding to the biometric feature information to be verified.

[0066] The processing module 406 is configured to sign service information based on the generated private key and send the service processing request that includes the signed service information and the identifier to the server, so the server determines the public key corresponding to the identifier included in the received service processing request and performs service processing based on the determined public key and the signed service information.

[0067] The service processing request includes a payment request.

[0068] In typical configuration, a computing device includes one or more processors (CPU), an input/output interface, a network interface, and a memory.

[0069] The memory can include a non-persistent memory, a random access memory (RAM), and/or a nonvolatile memory, etc. in a computer readable medium, such as a read-only memory (ROM) or a flash memory (flash RAM). The memory is an example of the computer readable medium.

[0070] The computer readable medium includes persistent, non-persistent, movable, and unmovable media that can store information by using any method or technology. The information can be a computer readable instruction, a data structure, a program module, or other data. Examples of a computer storage medium include but are not limited to a phase change random access memory (PRAM), a static RAM (SRAM), a dynamic RAM (DRAM), a RAM of another type, a read-only memory (ROM), an electrically erasable programmable read-only memory (EEPROM), a flash memory or another memory technology, a compact disc read-only memory (CD-ROM), a digital versatile disc (DVD) or another optical storage, a magnetic tape, a magnetic disk storage, another magnetic storage device, or any other non-transmission medium. The computer storage medium can be used to store information that can be accessed by a computing device. As described in the present specification, the computer readable medium does not include transitory media, for example, a modulated data signal and a carrier.

[0071] It is worthwhile to further note that, the term "include", "contain", or any other variant is intended to cover non-exclusive inclusion so that a process, a method, a product, or a device that includes a series of elements not only includes these elements, but also includes other elements that are not expressly listed, or further includes elements inherent to such a process, method, product, or device. An element preceded by "includes a ..." does not, without more constraints, exclude the existence of additional identical elements in the process, method, product, or device that includes the element.

[0072] A person skilled in the art should understand that the implementations of the present application can be provided as a method, a system, or a computer program product. Therefore, the present application can use a form of hardware only implementations, software only implementations, or implementations with a combination of software and hardware. In addition, the present application can use a form of a computer program product implemented on one or more computer-usable storage media (including but not limited to a magnetic disk memory, a CD-ROM, and an optical memory) that include computer-usable program code.

[0073] The previous descriptions are merely implementations of the present application, and are not intended to limit the present application. A person skilled in the art can make various modifications and changes to the present application. Any modifications, equivalent replacements, improvements, etc. made within the spirit and principle of the present application shall fall within the protection scope of the claims of the present application.

CLAIMS:

1. A computer-implemented method, comprising:

receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request;

matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier;

in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user;

in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises:

generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user;

storing a mapping relationship between the identifier and the generated private key in the terminal device; and

transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and

sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

2. The computer-implemented method of claim 1, wherein, before registering the user identity with the server at which the service processing request is to be sent, the method further comprises:

prompting the user, at the terminal device, for a password to be entered by the user, the password associated with the service request;

in response to receiving the password, verifying that the password is valid; and

allowing registration of the user identity with the server at which the service processing request is to be sent.

3. The computer-implemented method of claim 1, the method further comprising:

in response to determining that a private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, determining that the user identity of the user is already registered at the server, wherein the determined private key corresponds to a public key stored at the server and associated with the identifier of the particular pre-stored biometric feature of the user.

4. The computer-implemented method of claim 5, the method further comprising:

sending the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the determined private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

5. The computer-implemented method of claim 1, wherein the service processing request comprises a payment request.

6. The computer-implemented method of claim 1, wherein the received biometric feature information of the user that is to be verified comprises a fingerprint.

7. The computer-implemented method of claim 1, wherein the pre-stored biometric feature of the user is one of a plurality of pre-stored biometric features of the user stored at the terminal device, wherein the plurality of pre-stored biometric features of the user include a plurality of different biometric feature information of the user, including at least one of a stored fingerprint, an iris pattern or visualization, a hand geometry, a retina scan, or a voice pattern.

8. A non-transitory, computer-readable medium storing one or more instructions executable by a computer system to perform operations comprising:

receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request;

matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier;

in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user; and

in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises:

generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user;

storing a mapping relationship between the identifier and the generated private key in the terminal device; and

transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and

sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

9. The non-transitory, computer-readable medium of claim 8, wherein, before registering the user identity with the server at which the service processing request is to be sent, the operations further comprising:

prompting the user, at the terminal device, for a password to be entered by the user, the password associated with the service request;

in response to receiving the password, verifying that the password is valid; and

allowing registration of the user identity with the server at which the service processing request is to be sent.

10. The non-transitory, computer-readable medium of claim 8, the operations further comprising:

in response to determining that a private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, determining that the user identity of the user is already registered at the server, wherein the determined private key corresponds to a public key stored at the server and associated with the identifier of the particular pre-stored biometric feature of the user.

11. The non-transitory, computer-readable medium of claim 10, the operations further comprising:

sending the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the determined private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

12. The non-transitory, computer-readable medium of claim 10, wherein the service processing request comprises a payment request.

13. The non-transitory, computer-readable medium of claim 10, wherein the received biometric feature information of the user that is to be verified comprises a fingerprint.

14. The non-transitory, computer-readable medium of claim 10, wherein the pre-stored biometric feature of the user is one of a plurality of pre-stored biometric features of the user stored at the terminal device, wherein the plurality of pre-stored biometric features of the user include a plurality of different biometric feature information of the user, including at least one of

a stored fingerprint, an iris pattern or visualization, a hand geometry, a retina scan, or a voice pattern.

15. A computer-implemented system, comprising:

one or more computers; and

one or more computer memory devices interoperably coupled with the one or more computers and having tangible, non-transitory, machine-readable media storing one or more instructions that, when executed by the one or more computers, perform one or more operations comprising:

receiving, by a terminal device, biometric feature information of a user that is to be verified in association with a service processing request;

matching, by the terminal device, the received biometric feature information to be verified with a particular pre-stored biometric feature of the user, wherein the particular pre-stored biometric feature of the user is stored at the terminal device, and wherein the particular pre-stored biometric feature of the user is associated with a corresponding identifier;

in response to matching the received biometric feature information to be verified to a particular pre-stored biometric feature of the user, searching a private key store for a private key associated with the identifier of the particular pre-stored biometric feature of the user; and

in response to determining that no private key in the private key store is associated with the identifier of the particular pre-stored biometric feature of the user, registering a user identity of the user with a server at which the service processing request is to be sent, wherein registering the user identity of the user with the server at which the service processing request is to be sent comprises:

generating a private key and a public key corresponding to the identifier of the particular pre-stored biometric feature of the user;

storing a mapping relationship between the identifier and the generated private key in the terminal device; and

transmitting a mapping relationship between the identifier and the generated public key to the server for storage; and

sending, after the registering, the service processing request and the identifier of the particular pre-stored biometric feature of the user to the server, wherein the terminal device signs the service processing request with a digital signature using the generated private key associated with the identifier of the particular pre-stored biometric feature of the user, and wherein the server performs the service processing associated with the service processing request after verifying the digital signature of the terminal device using the generated public key corresponding to the identifier of the particular pre-stored biometric feature of the user.

Alibaba Group Holding Limited

Patent Attorneys for the Applicant/Nominated Person

SPRUSON & FERGUSON

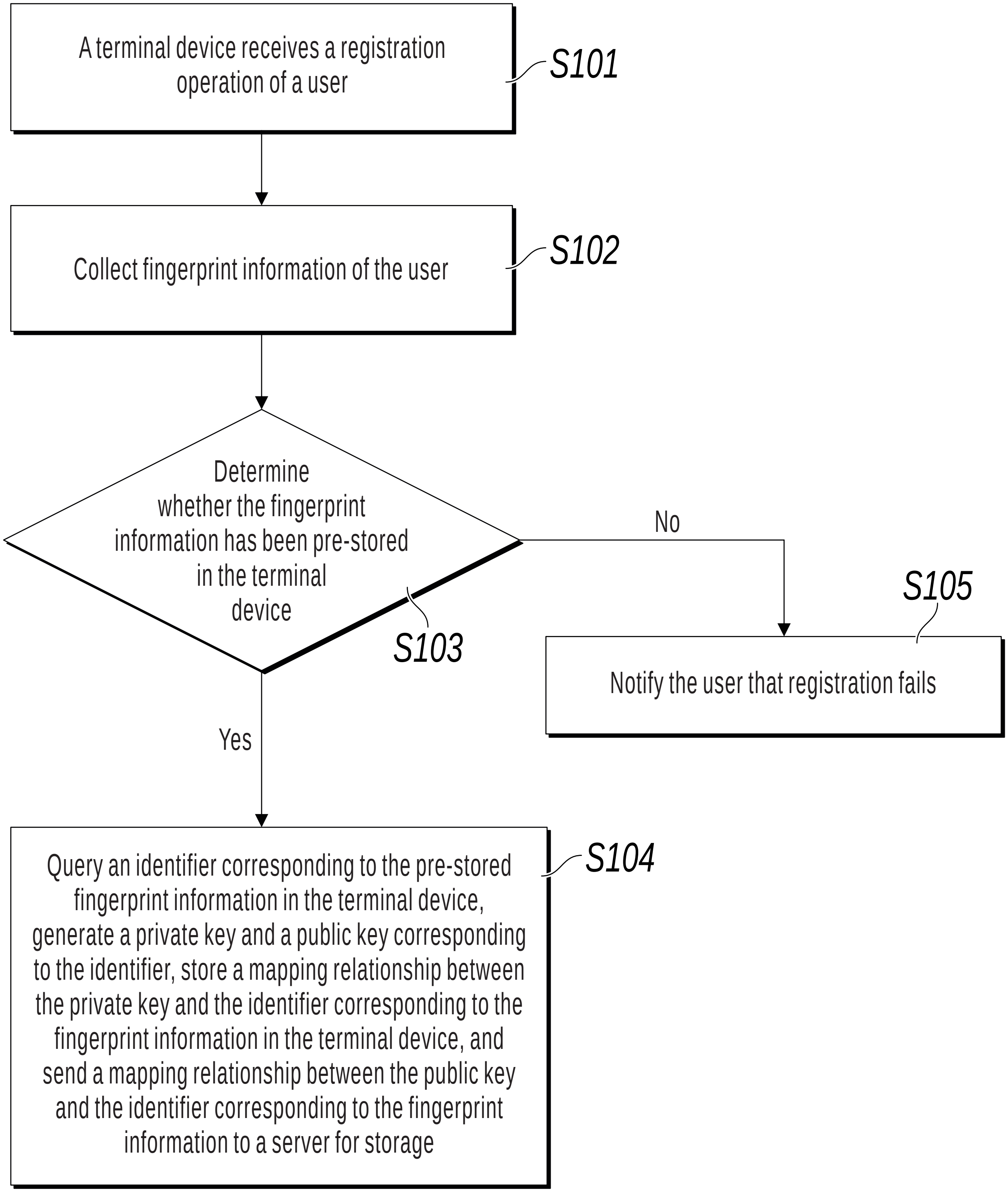

A terminal device receives a registration operation of a user
S101
Collect fingerprint information of the user
S102
Determine whether the fingerprint information has been pre-stored in the terminal device
S103
No
S105
Notify the user that registration fails
Yes
Query an identifier corresponding to the pre-stored fingerprint information in the terminal device, generate a private key and a public key corresponding to the identifier, store a mapping relationship between the private key and the identifier corresponding to the fingerprint information in the terminal device, and send a mapping relationship between the public key and the identifier corresponding to the fingerprint information to a server for storage
S104

FIG. 1

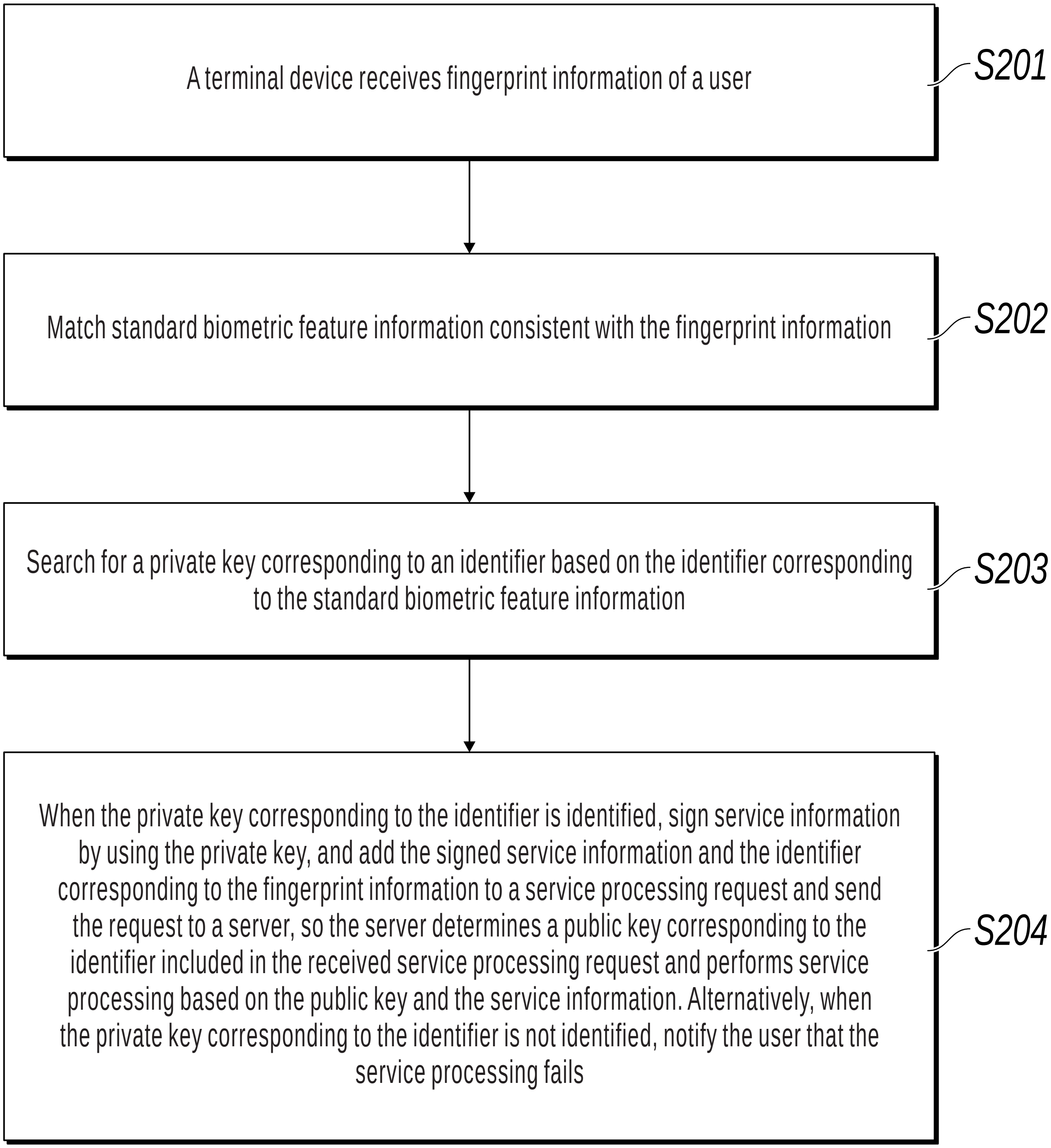

A terminal device receives fingerprint information of a user
S201
Match standard biometric feature information consistent with the fingerprint information
S202
Search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information
S203
When the private key corresponding to the identifier is identified, sign service information by using the private key, and add the signed service information and the identifier corresponding to the fingerprint information to a service processing request and send the request to a server, so the server determines a public key corresponding to the identifier included in the received service processing request and performs service processing based on the public key and the service information. Alternatively, when the private key corresponding to the identifier is not identified, notify the user that the service processing fails
S204

FIG. 2

2017239211 18 Dec 2019

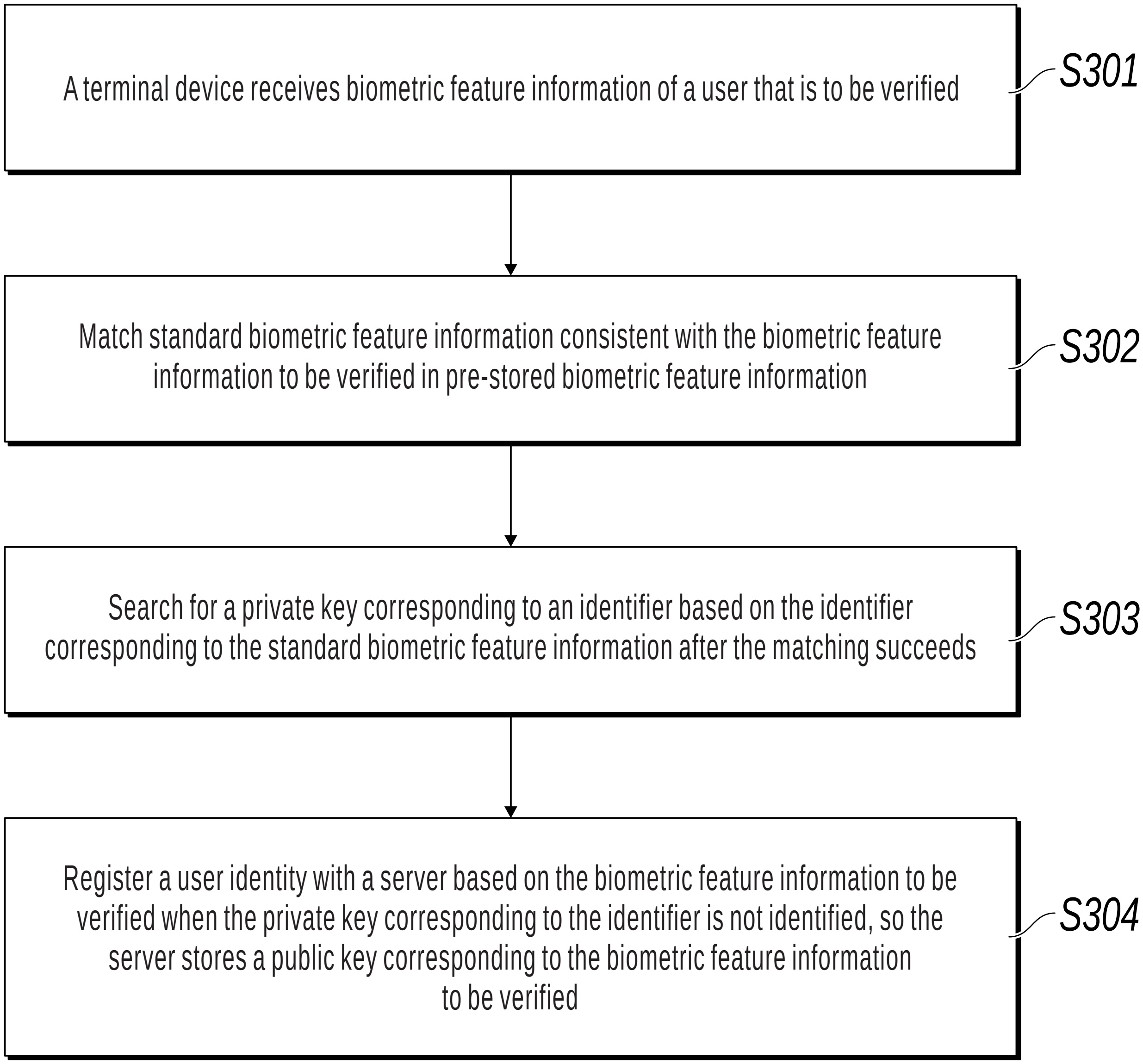

A terminal device receives biometric feature information of a user that is to be verified
S301
Match standard biometric feature information consistent with the biometric feature information to be verified in pre-stored biometric feature information
S302
Search for a private key corresponding to an identifier based on the identifier corresponding to the standard biometric feature information after the matching succeeds
S303
Register a user identity with a server based on the biometric feature information to be verified when the private key corresponding to the identifier is not identified, so the server stores a public key corresponding to the biometric feature information to be verified
S304

FIG. 3

2017239211 18 Dec 2019

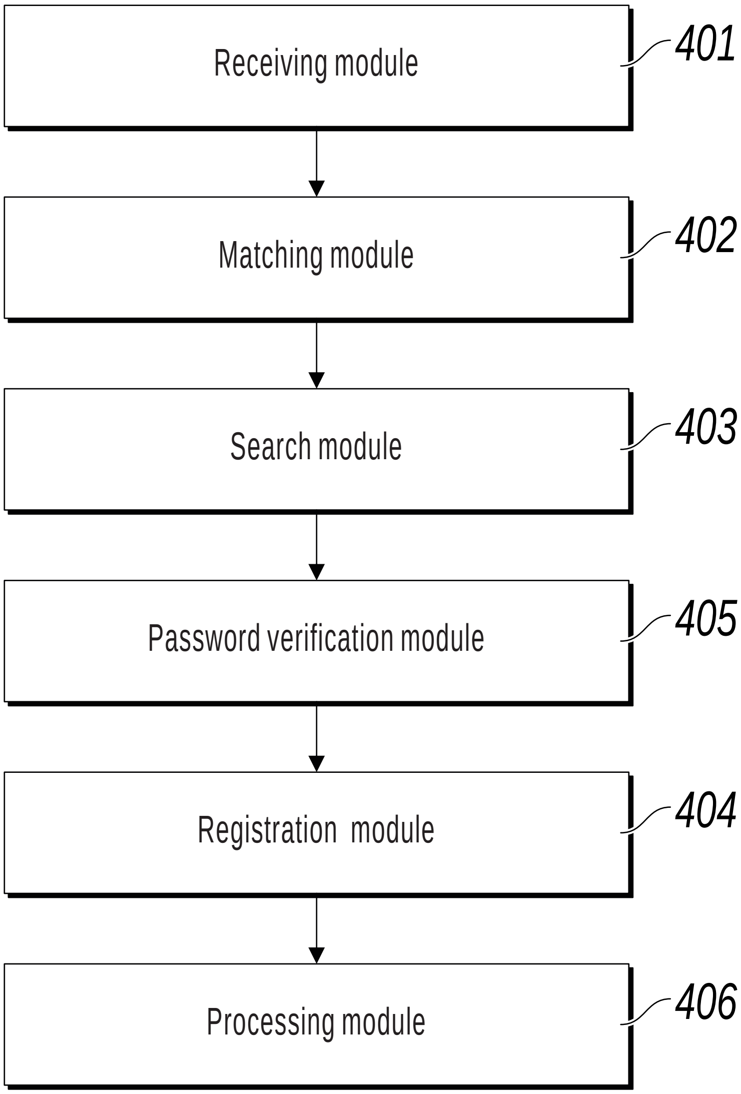


FIG. 4