

METHOD AND APPARATUS FOR SERVICE IMPLEMENTATION

TECHNICAL FIELD

5 **[0001]** The present application relates to the field of communications technologies, and in particular, to a method and an apparatus for service implementation.

BACKGROUND

10 **[0002]** With the rapid development of Internet technologies, the two-dimensional code is more widely used. Through two-dimensional code scanning, information can be exchanged to implement related services. In the existing technologies, usually the two-dimensional code carries necessary information used to complete related services, such as a user account and user information. Once an unauthorized person steals the two-dimensional code, information of an authorized user can be leaked, causing losses to the authorized user.

SUMMARY

15 **[0003]** In view of this, the present application provides a method and an apparatus for service implementation.

[0004] The present application is implemented by using the following technical solutions.

20 **[0005]** A method for service implementation is applied to a client and includes: after a display instruction of a graphic code is received, obtaining a biometric feature identifier of a biometric feature that has been verified; generating a code string that carries the biometric feature identifier; and displaying a graphic code that carries the code string, so after scanning the graphic code, another terminal device sends the code string to a server, and the server identifies a binding user account based on the biometric feature identifier to complete related services.

25 **[0006]** A method for service implementation is applied to a server and includes:

receiving a code string sent by a client, where the code string is parsed out after a graphic code is scanned; parsing out a biometric feature identifier from the code string; searching for a user account binding to the biometric feature identifier; and completing related services based on the user account.

5 **[0007]** An apparatus for service implementation is applied to a client and includes: an identifier acquisition unit, configured to: after a display instruction of a graphic code is received, obtain a biometric feature identifier of a biometric feature that has been verified; a code string generation unit, configured to generate a code string that carries the biometric feature identifier; and a barcode displaying unit, configured to
10 display a graphic code that carries the code string, so after scanning the graphic code, another terminal device sends the code string to a server, and the server identifies a binding user account based on the biometric feature identifier to complete related services.

15 **[0008]** An apparatus for service implementation is applied to a server and includes: a code string receiving unit, configured to receive a code string sent by a client, where the code string is parsed out after a graphic code is scanned; an identifier parsing unit, configured to parse out a biometric feature identifier from the code string; an account searching unit, configured to search for a user account binding to the biometric feature identifier; and a service implementation unit, configured to
20 complete related services based on the user account.

25 **[0009]** It can be seen from the previous description that, in the present application, a biometric feature identifier can be bound to a user account on a server in advance. After receiving a display instruction of a graphic code, the client can display a graphic code that carries the biometric feature identifier. The server can search for the binding user account based on the biometric feature identifier to complete related services, and does not need to carry sensitive information such as a user account in the graphic code. Even if an unauthorized person steals a terminal device of the user, a service operation cannot be performed because the biometric feature does not match, thereby ensuring security of user information and property.

30 **BRIEF DESCRIPTION OF DRAWINGS**

[0010] FIG. 1 is a schematic flowchart illustrating a method for service implementation, according to an example implementation of the present application;

[0011] FIG. 2 is a schematic flowchart illustrating a method for service implementation, according to another example implementation of the present application;

5 [0012] FIG. 3 is a schematic flowchart illustrating binding a biometric feature identifier to a user account, according to an example implementation of the present application;

[0013] FIG. 4 is a schematic flowchart illustrating a method for service implementation, according to another example implementation of the present application;

10 [0014] FIG. 5 is a schematic diagram illustrating a code string, according to an example implementation of the present application;

[0015] FIG. 6 is a schematic flowchart illustrating determining a target user account, according to an example implementation of the present application;

15 [0016] FIG. 7 is a schematic structural diagram illustrating an apparatus for service implementation, according to an example implementation of the present application;

[0017] FIG. 8 is a block diagram illustrating an apparatus for service implementation, according to an example implementation of the present application;

20 [0018] FIG. 9 is a schematic structural diagram illustrating another apparatus for service implementation, according to an example implementation of the present application; and

[0019] FIG. 10 is a block diagram illustrating another apparatus for service implementation, according to an example implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

25 [0020] Example implementations are described in detail here, and examples of the example implementations are presented in the accompanying drawings. When the following description relates to the accompanying drawings, unless specified otherwise, same numbers in different accompanying drawings represent same or similar elements. Implementations described in the following example
30 implementations do not represent all implementations consistent with the present application. Instead, they are only examples of apparatuses and methods consistent with some aspects of the present application that are described in detail in the

appended claims.

[0021] The terms used in the present application are merely for illustrating specific implementations, and are not intended to limit the present application. The terms "a" and "the" of singular forms used in the present application and the appended
 5 claims are also intended to include plural forms, unless otherwise specified in the context clearly. It should be further understood that the term "and/or" used in the present specification indicates and includes any or all possible combinations of one or more associated listed items.

[0022] It should be understood that although terms "first", "second", "third", etc.
 10 can be used in the present application to describe various types of information, the information is not limited to the terms. These terms are only used to differentiate information of a same type. For example, without departing from the scope of the present application, first information can also be referred to as second information, and similarly, the second information can be referred to as the first information.
 15 Depending on the context, for example, the word "if" used here can be explained as "while", "when", or "in response to determining".

[0023] FIG. 1 is a schematic flowchart illustrating a method for service implementation, according to an example implementation of the present application.

[0024] Referring to FIG. 1, the method for service implementation can be applied
 20 to a client and includes the following steps:

[0025] Step 101: After a display instruction of a graphic code is received, obtain a biometric feature identifier of a biometric feature that has been verified.

[0026] In this implementation, the graphic code can include a barcode and a two-dimensional code. In specific application scenarios, the graphic code can be a
 25 payment code, a collection code, etc.

[0027] In an example, after receiving the display instruction of the graphic code, the client can collect a biometric feature entered by a user, and after determining that the biometric feature is verified, a terminal system or a server can return a biometric feature identifier of the biometric feature to the client. The biometric feature can be a
 30 fingerprint, a palmprint, an iris, a sclera, a face, etc. When the biometric feature is a fingerprint, the biometric feature identifier is usually generated by the terminal system when an authorized user enters a biometric feature. For example, when the user enters a fingerprint used for unlocking, the terminal system can generate a fingerprint identifier for the fingerprint. If the biometric feature is an iris, a face, etc., the

biometric feature identifier can be generated by the server when the authorized user enters a biometric feature used for identity authentication. For example, when the user enters a face image used to unlock an APP, the server generates a face image identifier for the face image entered by the user.

5 **[0028]** In another example, when an APP that displays the graphic code needs to be unlocked before being enabled, the terminal system or the server can send the biometric feature identifier of the biometric feature to the client after determining that the biometric feature of the user is verified, and the client stores the biometric feature identifier. After receiving the display instruction of the graphic code, the client can
10 obtain the stored biometric feature identifier.

[0029] Step 102: Generate a code string that carries the biometric feature identifier.

[0030] Step 103: Display a graphic code that carries the code string, so after scanning the graphic code, another terminal device sends the code string to a server,
15 and the server identifies a binding user account based on the biometric feature identifier to complete related services.

[0031] In this implementation, after scanning the graphic code displayed on the client, other terminal devices can send the parsed code string to the server, and the server can search for the binding user account based on the biometric feature
20 identifier in the code string, and complete related services based on the found user account.

[0032] FIG. 2 is a schematic flowchart illustrating another method for service implementation, according to an example implementation of the present application.

[0033] Referring to FIG. 2, the method for service implementation can be applied
25 to a server and includes the following steps:

[0034] Step 201: Receive a code string sent by a client, where the code string is parsed out after a graphic code is scanned.

[0035] Step 202: Parse out a biometric feature identifier from the code string.

[0036] Step 203: Search for a user account binding to the biometric feature
30 identifier.

[0037] In this implementation, after receiving a binding request of the client, the server can bind the biometric feature identifier carried in the binding request to the user account.

[0038] Step 204: Complete related services based on the user account.

[0039] It can be seen from the previous description that, in the present application, a biometric feature identifier can be bound to a user account on a server in advance. After receiving a display instruction of a graphic code, the client can display a graphic code that carries the biometric feature identifier. The server can search for the binding user account based on the biometric feature identifier to complete related services, and does not need to carry sensitive information such as a user account in the graphic code. Even if an unauthorized person steals the graphic code or a terminal device of a user, a service operation cannot be performed because the biometric feature does not match, thereby ensuring security of user information and property.

10 **[0040]** The following separately describes an implementation process of the present application from two aspects: user account binding and service implementation.

[0041] 1. Binding the biometric feature identifier to the user account

[0042] Referring to FIG. 3, for example, a biometric feature is a fingerprint and a graphic code is a payment code. The fingerprint is stored in a terminal device, and a process of binding a biometric feature identifier to a user account on a server can include the following steps:

[0043] Step 301: After successfully logging in to a server using the user account, collect a fingerprint of a user if the user enables a payment function in which a fingerprint identifier is used instead of a user account.

[0044] In this implementation, the user can register the user account with the server in advance. Subsequently, related services can be implemented based on the registered user account. For a specific registration procedure, references can be made to the existing technologies, and details are omitted in the present application for simplicity.

[0045] In this implementation, the user can enter a login name and a password on the login page of the client to log in to the server, or the user can log in by using an SMS message authentication code. This is not specially limited in the present application.

30 **[0046]** In this implementation, after the user successfully logs in to the server, the user can enable a payment function of adding a fingerprint identifier to the payment code to replace the user account. In actual implementations, the client can provide the user with an enabling button of the function. After detecting that the user triggers the button, the client can invoke the terminal system to perform fingerprint verification on

the user. The client can wake up a fingerprint sensor and prompt the user to perform fingerprint verification. After the fingerprint sensor collects the fingerprint of the user, the terminal system can verify the collected fingerprint to verify whether the fingerprint is a fingerprint of an authorized user stored in the system. When the collected fingerprint is a valid fingerprint, the terminal system can send the fingerprint identifier of the valid fingerprint to the client. If the collected fingerprint is not a valid fingerprint, the terminal system can return a verification failure notification to the client, and the client can further notify the user that the verification fails, or re-perform fingerprint verification.

10 **[0047]** The fingerprint identifier is generated by the terminal system when the authorized user enters the fingerprint. For example, the authorized user can enter a fingerprint on the terminal device to subsequently unlock the terminal device by using the fingerprint. After the user enters the fingerprint, the terminal device system can generate a fingerprint identifier for the fingerprint.

15 **[0048]** Step 302: A client receives a fingerprint identifier of the fingerprint that is sent by a terminal system after the terminal system determines that the fingerprint is verified.

[0049] Step 303: The client adds the fingerprint identifier to a binding request and sends the binding request to the server.

20 **[0050]** In this implementation, the binding request is used to request the server to bind a fingerprint identifier generated by the terminal system to a user account, so as to enable a payment function of adding the fingerprint identifier to a payment code to replace the user account.

[0051] Step 304: The server binds the fingerprint identifier to a currently logged-in user account.

[0052] In this implementation, after receiving the binding request, the server can extract the fingerprint identifier from the binding request, and then bind the fingerprint identifier to the user account that is currently logged in to the client.

[0053] Optionally, after binding the fingerprint identifier to the currently logged-in user account, the server can further return a binding success notification to the client, and the client can further display a prompt page indicating a function provision success to the user.

[0054] In another example, for a biometric feature that cannot be verified by the terminal system such as a face image, an iris, and a sclera, the client can add the

collected biometric feature to a binding request and send the binding request to the server. After receiving the binding request, the server can bind the biometric feature identifier of the biometric feature to the currently logged-in user account. The biometric feature identifier is generated by the server when the user enters the corresponding biometric feature. If the biometric feature carried in the binding request is not stored on the server, the server can generate a biometric feature identifier for the biometric feature, and bind the biometric feature identifier to the currently logged-in user account.

[0055] 2. Service implementation

[0056] Based on the implementation shown in FIG. 3, referring to FIG. 4, for example, a biometric feature is a fingerprint and a graphic code is a payment code. A process of using the payment code for payment can include the following steps:

[0057] Step 401: After receiving a display instruction of a payment code, a first client obtains a fingerprint identifier of a fingerprint that has been verified by a terminal system.

[0058] In this implementation, the first client is a client used by a payer. When making a payment to a payee (for example, a merchant), the payer can tap a "pay" button in the first client, and the first client can obtain the fingerprint identifier of the fingerprint that has been verified by the terminal system.

[0059] In this implementation, the first client can obtain the fingerprint identifier using the following two methods:

[0060] In an example, after receiving the display instruction of the payment code, the first client can invoke the terminal system to perform fingerprint verification on the user, and receive the fingerprint identifier of the fingerprint that is sent by the terminal system after the terminal system determines that the fingerprint of the user is verified.

[0061] As such, after the user taps the "pay" button, the first client can prompt the user to perform fingerprint verification. In addition, the first client can further invoke the terminal system to perform fingerprint verification on the user, for example, wake up a fingerprint sensor to collect the fingerprint of the user. After collecting the fingerprint entered by the user, the terminal system can verify whether the fingerprint is a fingerprint of an authorized user stored in the system. When the collected fingerprint is a valid fingerprint, the terminal system can return the fingerprint identifier of the fingerprint to the first client. When the collected fingerprint is not a

valid fingerprint, the terminal system can return a verification failure notification to the first client, and the first client can further notify the user that the verification fails, or re-perform fingerprint verification.

[0062] In another example, after receiving the display instruction of the payment code, the first client can obtain a stored fingerprint identifier. The stored fingerprint identifier is a fingerprint identifier of a fingerprint used for unlocking the first client. After the first client enables a fingerprint unlocking function, the user can unlock the first client only after passing fingerprint verification, and then tap the "pay" button. In this process, after verifying that the unlocking fingerprint of the user is a valid fingerprint, the terminal system can send the fingerprint identifier of the valid fingerprint to the first client, and the first client stores the fingerprint identifier. Subsequently, after the user taps the "pay" button, the first client can obtain the stored fingerprint identifier. It is worthwhile to note that, in such an implementation, the first client can update the stored fingerprint identifier by using a fingerprint identifier sent by the terminal system when the user unlocks the first client next time, that is, the first client stores the fingerprint identifier of the current unlocking fingerprint.

[0063] Step 402: The first client generates a code string that carries the fingerprint identifier.

[0064] Based on step 401, after obtaining the fingerprint identifier, the first client can generate a code string. Referring to FIG. 5, FIG. 5 shows a format of a code string. The first two bits are identification information of the code string, the last six bits are check information of the code string, and the middle is an encrypted fingerprint identifier.

[0065] The first client can encrypt the obtained fingerprint identifier by using a predetermined algorithm, and add the encrypted fingerprint identifier to the location following the identification information of the code string. The check information is usually a check code generated based on the predetermined algorithm. For example, the check code can be a one-time password (OTP) code.

[0066] Step 403: The first client displays a two-dimensional payment code that carries the code string.

[0067] Step 404: A second client invokes a camera to scan the two-dimensional payment code.

[0068] In this implementation, the second client is a client used by the payee, and the payee can invoke a camera to scan the two-dimensional payment code using the

second client.

[0069] Step 405: The second client sends the code string carried in the two-dimensional payment code to a server.

5 **[0070]** Step 406: The server parses out the fingerprint identifier from the code string.

[0071] Step 407: The server searches for a user account bound to the fingerprint identifier.

10 **[0072]** In this implementation, after receiving the code string, the server can parse out the encrypted fingerprint identifier and the check code. The server can decrypt the encrypted fingerprint identifier by using a predetermined algorithm, to obtain the fingerprint identifier, and then search for the user account binding to the fingerprint identifier. When the fingerprint identifier is not bound to any user account, the server can return payment failure prompt information to the second client. When the fingerprint identifier is bound to a user account, the server can further check the check code. If the check succeeds, step 408 can be performed. If the check fails, payment failure prompt information can be returned to the second client.

[0073] Step 408: Complete a payment service based on the user account.

20 **[0074]** It can be seen from the previous description that, when completing the payment service by using the two-dimensional payment code in the present application, the client can add the fingerprint identifier generated by the terminal system instead of the user account to the payment code. Even if an unauthorized person steals the payment code or the terminal device of the user, the unauthorized person cannot complete the payment operation because the fingerprint does not match, thereby ensuring property security of the user. In addition, because the two-dimensional payment code in the present application does not need to carry the user account, when the user does not log in to the user account, a payment operation can also be performed, which improves user experience.

25 **[0075]** Optionally, in another example, because the fingerprint identifier is generated by the terminal system, and a same terminal system can be loaded onto different terminal devices, terminal systems of different user terminal devices can generate a same fingerprint identifier. For example, assume that User 1 uses ANDROID mobile phone 1, User 2 uses ANDROID mobile phone 2, an ANDROID operating system of ANDROID mobile phone 1 generates fingerprint identifier 1 for a fingerprint of User 1, and a fingerprint identifier generated by an ANDROID

operating system of ANDROID mobile phone 2 for a fingerprint of User 2 can also be fingerprint identifier 1. When User 1 enables the payment function of adding a fingerprint identifier to the payment code to replace the user account, the server binds fingerprint identifier 1 to the account of User 1. When User 2 enables the payment function of adding a fingerprint identifier to the payment code to replace the user account, the server binds fingerprint identifier 1 to the account of User 2. Therefore, fingerprint identifier 1 is bound to two user accounts: the account of User 1 and the account of User 2. In this case, when determining that the fingerprint identifier is bound to multiple user accounts, the server can determine, from the multiple user accounts by using check information (for ease of differentiation, subsequently referred to as first check information) carried in a code string, the target user account for performing the payment service. Referring to FIG. 6, the server can determine the target user account by performing the following steps:

[0076] Step 601: Separately obtain, for multiple user accounts binding to a fingerprint identifier, second check information generated for the user accounts.

[0077] In this implementation, for example, the check information is an OTP code. A check rule of the OTP code is that the server and the client generate one unpredictable random code related to time every 60 seconds. For the same user account, the OTP codes generated by the server and the client are consistent and globally unique.

[0078] In this step, when finding that the fingerprint identifier is bound to multiple user accounts, the server can separately obtain a second OTP code (that is, second check information) generated for each user account.

[0079] Step 602: Determine a user account corresponding to second check information as the target user account, where the second check information is the same as the first check information.

[0080] In this implementation, the first OTP code (that is, the first check information) is an OTP code carried in the code string, and the server can sequentially compare the second OTP code with the first OTP code. When a second OTP code is the same as the first OTP code, the server can determine a user account corresponding to the second OTP code as the target user account, and subsequently complete the payment service based on the target user account.

[0081] For example, still assume that fingerprint identifier 1 is bound to two user accounts: the account of User 1 and the account of User 2, and the first OTP code

carried in the code string is 123456. If the server learns that the second OTP code generated for the account of User 1 is 456123, and the second OTP code generated for the account of User 2 is 123456, the server can determine that the account of User 2 is the target user account and can further complete the payment service based on the account of User 2.

[0082] Optionally, in another example, for a biometric feature that cannot be verified by the terminal system such as a face image, an iris, or a sclera, in step 401, the first client can send the collected biometric feature to the server for verification. After confirming that the biometric feature is verified, the server can return the biometric feature identifier of the biometric feature to the first client, so the first client generates the code string in step 402. It is worthwhile to note that, in such an implementation, because biometric feature identifiers are generated by the server, the server can generate non-repeated biometric feature identifiers, and one biometric feature identifier will not be bound to multiple user accounts.

[0083] It is worthwhile to note that, the service implementation solution provided in the present application can be applied not only to the payment service, but also to other services, such as a virtual point consumption service, an electronic coupon consumption service, and a friend addition service. This is not specially limited in the present application. The friend addition service is used as an example. When displaying a two-dimensional code of user information, a client of User A can use a biometric feature identifier to replace user account 1 of User A. After scanning the two-dimensional code, User B can send the biometric feature identifier to the server, and after identifying user account 1 bound to the biometric feature identifier, the server can add User A as a friend of User B based on user account 1. In this process, the two-dimensional code does not carry any information about user account 1. Even if an unauthorized person steals the mobile phone of User A, no service operation can be performed because the biometric feature does not match, thereby ensuring security of user information.

[0084] Corresponding to the implementations of the previous method for service implementation, the present application further provides implementations of an apparatus for service implementation.

[0085] Implementations of the apparatus for service implementation in the present application can be separately applied to a terminal device loaded with a client and a server. The apparatus implementation can be implemented by software, hardware, or a

combination of hardware and software. Software implementation is used as an example. As a logical apparatus, the apparatus is formed by reading a corresponding computer program instruction in a non-volatile memory and running the instruction in a memory by a processor in apparatus for service implementation. In terms of hardware, FIG. 7 is a structural diagram illustrating hardware of a terminal device in which the apparatus for service implementation of the present application is located. In addition to the processor, the memory, the network interface, and the nonvolatile memory shown in FIG. 7, the terminal device that the apparatus is located in this implementation usually can include other hardware based on actual functions of the terminal device. Details are omitted here for simplicity.

[0086] FIG. 8 is a block diagram illustrating an apparatus for service implementation, according to an example implementation of the present application.

[0087] Referring to FIG. 8, the apparatus 700 for service implementation can be applied to the terminal device shown in FIG. 7, including an identifier acquisition unit 701, a code string generation unit 702, a barcode displaying unit 703, a feature verification unit 704, and an account binding unit 705.

[0088] The identifier acquisition unit 701 is configured to: after a display instruction of a graphic code is received, obtain a biometric feature identifier of a biometric feature that has been verified; the code string generation unit 702 is configured to generate a code string that carries the biometric feature identifier; and the barcode displaying unit 703 is configured to display a graphic code that carries the code string, so after scanning the graphic code, another terminal device sends the code string to a server, and the server identifies a binding user account based on the biometric feature identifier to complete related services.

[0089] Optionally, after receiving the display instruction of the graphic code, the identifier acquisition unit 701 collects a biometric feature entered by a user, and receives a biometric feature identifier of the biometric feature that is sent by a terminal system or the server after determining that the biometric feature is verified.

[0090] The feature verification unit 704 is configured to: if an APP that displays the graphic code needs to be unlocked by using a biometric feature before being enabled, collect a biometric feature of a user before the APP is enabled, verify the biometric feature, and after the verification succeeds, obtain the stored biometric feature identifier.

[0091] Optionally, the graphic code is a payment code or a collection code.

[0092] Optionally, the biometric feature includes a fingerprint, a palmprint, an iris, a sclera, and a face image.

[0093] Optionally, the related services include a payment service, a virtual point consumption service, an electronic coupon consumption service, and a friend addition service.

[0094] The account binding unit 705 is configured to: when the biometric feature identifier is being bound to the user account, in a login state of the user account, if the biometric feature is stored on a terminal device, send, to the server, a binding request that carries an identifier corresponding to the biometric feature, so the server binds the identifier corresponding to the biometric feature to the user account; and if the biometric feature is stored on the server, send a binding request to the server, so the server binds the identifier corresponding to the biometric feature to the user account.

[0095] In terms of hardware, FIG. 9 is a structural diagram illustrating hardware of the server that the apparatus for service implementation of the present application is located. In addition to the processor, the memory, the network interface, and the nonvolatile memory shown in FIG. 9, the server that the apparatus is located in this implementation usually can include other hardware based on actual functions of the server. Details are omitted here for simplicity.

[0096] FIG. 10 is a block diagram illustrating an apparatus for service implementation, according to an example implementation of the present application.

[0097] Referring to FIG. 10, the apparatus 900 for service implementation can be applied to the server shown in FIG. 9, including a code string receiving unit 901, an identifier parsing unit 902, an account searching unit 903, a service implementation unit 904, a target determining unit 905, a first binding unit 906, and a second binding unit 907.

[0098] The code string receiving unit 901 is configured to receive a code string sent by a client, where the code string is parsed out after a graphic code is scanned; the identifier parsing unit 902 is configured to parse out a biometric feature identifier from the code string; the account searching unit 903 is configured to search for a user account binding to the biometric feature identifier; and the service implementation unit 904 is configured to complete related services based on the user account.

[0099] The target determining unit 905 is configured to: when the biometric feature identifier is bound to multiple user accounts, determine a target user account from the multiple user accounts based on first check information carried in the code

string, where the first check information is generated by the client; and the service implementation unit 904 is configured to complete the related services based on the target user account.

5 **[0100]** Optionally, the target determining unit 905 is configured to: separately obtain, for the multiple user accounts, second check information generated for the user accounts, and determine a user account corresponding to second check information as the target user account, where the second check information is the same as the first check information

10 **[0101]** The first binding unit 906 is configured to receive a binding request sent by the client and carrying the biometric feature identifier, and bind the biometric feature identifier to a currently logged-in user account.

[0102] The second binding unit 907 is configured to receive an account binding request sent by the client and carrying a biometric feature, and bind a biometric feature identifier of the biometric feature to a currently logged-in user account.

15 **[0103]** For an implementation process of functions and roles of each unit in the apparatus, references can be made to an implementation process of corresponding steps in the previous method. Details are omitted here for simplicity.

[0104] Because an apparatus implementation basically corresponds to a method implementation, for related parts, references can be made to related descriptions in the method implementation. The previously described apparatus implementation is merely an example. The units described as separate parts can or cannot be physically separate, and parts displayed as units can or cannot be physical units, can be located in one position, or can be distributed on a plurality of network units. Some or all of the modules or units can be selected based on actual needs to achieve the objectives of the solutions in the present application. A person of ordinary skill in the art can understand and implement the implementations of the present application without creative efforts.

25 **[0105]** The previous descriptions are merely examples of implementations of the present application, but are not intended to limit the present application. Any modification, equivalent replacement, or improvement made without departing from the spirit and principle of the present application should fall within the protection scope of the present application.

CLAIMS

What is claimed is:

1. A method for service implementation, applied to a client, wherein the method comprises:
 - 5 after a display instruction of a graphic code is received, obtaining a biometric feature identifier of a biometric feature that has been verified;
 - generating a code string that carries the biometric feature identifier; and
 - displaying a graphic code that carries the code string, so after scanning the graphic code, another terminal device sends the code string to a server, and the server
 - 10 identifies a binding user account based on the biometric feature identifier to complete related services.
 2. The method according to claim 1, wherein the obtaining a biometric feature identifier of a biometric feature that has been verified comprises:
 - after the display instruction of the graphic code is received, collecting a
 - 15 biometric feature entered by a user; and
 - receiving a biometric feature identifier of the biometric feature that is sent by a terminal system or the server after determining that the biometric feature is verified.
 3. The method according to claim 1, wherein the method further comprises:
 - if an APP that displays the graphic code needs to be unlocked by using a
 - 20 biometric feature before being enabled, collecting a biometric feature of a user before the APP is enabled, and verifying the biometric feature; and
 - after the verification succeeds, obtaining the stored biometric feature identifier.
 4. The method according to claim 1, wherein the graphic code is a payment code or a collection code.
 - 25 5. The method according to claim 1, wherein
 - the biometric feature comprises a fingerprint, a palmprint, an iris, a sclera, and a face image.
 6. The method according to claim 1, wherein
 - the related services comprise a payment service, a virtual point consumption
 - 30 service, an electronic coupon consumption service, and a friend addition service.
 7. The method according to claim 1, wherein the method further comprises:
 - when the biometric feature identifier is being bound to the user account, in a

login state of the user account, if the biometric feature is stored on a terminal device, sending, to the server, a binding request that carries an identifier corresponding to the biometric feature, so the server binds the identifier corresponding to the biometric feature to the user account; and

- 5 if the biometric feature is stored on the server, sending a binding request to the server, so the server binds the identifier corresponding to the biometric feature to the user account.

8. A method for service implementation, applied to a server, wherein the method comprises:

- 10 receiving a code string sent by a client, wherein the code string is parsed out after a graphic code is scanned;
 parsing out a biometric feature identifier from the code string;
 searching for a user account binding to the biometric feature identifier; and
 completing related services based on the user account.

- 15 9. The method according to claim 8, wherein the method further comprises:
 when the biometric feature identifier is bound to multiple user accounts, determining a target user account from the multiple user accounts based on first check information carried in the code string, wherein the first check information is generated by the client; and

- 20 the completing related services based on the user account comprises:
 completing the related services based on the target user account.

10. The method according to claim 9, wherein the determining a target user account from the multiple user accounts based on first check information carried in the code string comprises:

- 25 separately obtaining, for the multiple user accounts, second check information generated for the user accounts; and
 determining a user account corresponding to second check information as the target user account, wherein the second check information is the same as the first check information.

- 30 11. The method according to claim 8, wherein the method further comprises:
 receiving a binding request sent by the client and carrying the biometric feature identifier; and

 binding the biometric feature identifier to a currently logged-in user account.

12. The method according to claim 8, wherein the method further comprises:

receiving a binding request sent by the client and carrying a biometric feature;
and

binding a biometric feature identifier of the biometric feature to a currently
logged-in user account.

5 13. An apparatus for service implementation, applied to a client, wherein the
apparatus comprises:

an identifier acquisition unit, configured to: after a display instruction of a
graphic code is received, obtain a biometric feature identifier of a biometric feature
that has been verified;

10 a code string generation unit, configured to generate a code string that carries the
biometric feature identifier; and

a barcode displaying unit, configured to display a graphic code that carries the
code string, so after scanning the graphic code, another terminal device sends the code
string to a server, and the server identifies a binding user account based on the
15 biometric feature identifier to complete related services.

14. The apparatus according to claim 13, wherein

after receiving the display instruction of the graphic code, the identifier
acquisition unit collects a biometric feature entered by a user, and receives a biometric
feature identifier of the biometric feature that is sent by a terminal system or the
20 server after determining that the biometric feature is verified.

15. The apparatus according to claim 13, wherein the apparatus further
comprises:

a feature verification unit, configured to: if an APP that displays the graphic code
needs to be unlocked by using a biometric feature before being enabled, collect a
25 biometric feature of a user before the APP is enabled, verify the biometric feature, and
after the verification succeeds, obtain the stored biometric feature identifier.

16. The apparatus according to claim 13, wherein

the graphic code is a payment code or a collection code.

17. The apparatus according to claim 13, wherein

30 the biometric feature comprises a fingerprint, a palmprint, an iris, a sclera, and a
face image.

18. The apparatus according to claim 13, wherein

the related services comprise a payment service, a virtual point consumption
service, an electronic coupon consumption service, and a friend addition service.

19. The apparatus according to claim 13, wherein the apparatus further comprises:

an account binding unit, configured to: when the biometric feature identifier is being bound to the user account, in a login state of the user account, if the biometric feature is stored on a terminal device, send, to the server, a binding request that carries an identifier corresponding to the biometric feature, so the server binds the identifier corresponding to the biometric feature to the user account; and if the biometric feature is stored on the server, send a binding request to the server, so the server binds the identifier corresponding to the biometric feature to the user account.

20. An apparatus for service implementation, applied to a server, wherein the apparatus comprises:

a code string receiving unit, configured to receive a code string sent by a client, wherein the code string is parsed out after a graphic code is scanned;

an identifier parsing unit, configured to parse out a biometric feature identifier from the code string;

an account searching unit, configured to search for a user account binding to the biometric feature identifier; and

a service implementation unit, configured to complete related services based on the user account.

21. The apparatus according to claim 20, wherein the apparatus further comprises:

a target determining unit, configured to: when the biometric feature identifier is bound to multiple user accounts, determine a target user account from the multiple user accounts based on first check information carried in the code string, wherein the first check information is generated by the client; and

the service implementation unit is configured to complete the related services based on the target user account.

22. The apparatus according to claim 21, wherein

the target determining unit is configured to: separately obtain, for the multiple user accounts, second check information generated for the user accounts, and determine a user account corresponding to second check information as the target user account, wherein the second check information is the same as the first check information.

23. The apparatus according to claim 20, wherein the apparatus further

comprises:

a first binding unit, configured to receive a binding request sent by the client and carrying the biometric feature identifier, and bind the biometric feature identifier to a currently logged-in user account.

- 5 24. The apparatus according to claim 20, wherein the apparatus further comprises:

a second binding unit, configured to receive an account binding request sent by the client and carrying a biometric feature, and bind a biometric feature identifier of the biometric feature to a currently logged-in user account.