

equipment needs to provide a device identity, a virtual account identity, a biometric authentication type, and a biometric feature token matching the registered information to pass authentication, greatly improving identity authentication security.

BRIEF DESCRIPTION OF DRAWINGS

- 5 **[0045]** FIG. 1 is a diagram illustrating a network structure of an application scenario, according to an implementation of the present application;
- [0046]** FIG. 2 is a flowchart illustrating a method for registering a biometric identity that applies to user equipment, according to Implementation 1 of the present application;
- [0047]** FIG. 3 is a flowchart illustrating a method for registering a biometric identity
10 that applies to an authentication server, according to Implementation 1 of the present application;
- [0048]** FIG. 4A to FIG. 4B are interaction flowcharts illustrating identity registration among user equipment, a service server, an authentication server, and a biometric authentication center server, according to Implementation 1 of the present
15 application;
- [0049]** FIG. 5 is a flowchart illustrating a method for authenticating a biometric identity that applies to user equipment, according to Implementation 2 of the present application;
- [0050]** FIG. 6 is a flowchart illustrating a method for authenticating a biometric
20 identity that applies to an authentication server, according to Implementation 2 of the present application;
- [0051]** FIG. 7A to FIG. 7B are interaction flowcharts illustrating identity authentication among user equipment, a service server, and an authentication server, according to Implementation 2 of the present application;
- 25 **[0052]** FIG. 8 is a diagram illustrating a hardware structure of user equipment or an authentication server;
- [0053]** FIG. 9 is a diagram illustrating a logical structure of a device for registering a biometric identity that applies to user equipment or a device for authenticating a biometric identity that applies to user equipment, according to Implementation 1 of the
30 present application;
- [0054]** FIG. 10 is a diagram illustrating a logical structure of a device for registering a biometric identity that applies to an authentication server, according to

registration request packet.

[0090] In an implementation including a registration verification code, an interaction process among various function modules of user equipment, a service server, an authentication server, and a biometric authentication center server are shown in FIG.

5 4A to FIG. 4B.

[0091] In Implementation 1 of the present application, a device private key and a device public key pre-stored on the user equipment are used to ensure that the user equipment is a reliable device. A server public key and a server private key are used to verify reliability of the service server. As such, a correspondence among a device
10 identity of the user equipment, a virtual account identity, a biometric authentication type, a biometric feature token, and a service public key can be securely registered in the authentication server for subsequent identity authentication, thereby improving identity registration security.

[0092] Implementation 2 of the present application describes a method for
15 authenticating a biometric identity. A process of applying the method to user equipment is shown in FIG. 5, and a process of applying the method to an authentication server is shown in FIG. 6. An identity authentication process in Implementation 2 uses the same technical means as the identity registration process in Implementation 1. The following describes only the difference between Implementation 2 and Implementation 1. For the
20 same content, reference can be made to Implementation 1. Details are omitted here for simplicity.

[0093] On the user equipment, in step 510, the service client sends a device information request to the biometric authentication middleware, the biometric authentication middleware forwards the device information request to the biometric authentication client, the biometric authentication client forwards the device
25 information request to the identity authentication detector, the identity authentication detector obtains device information of the user equipment that includes a device identity and returns a device information response that includes the device information to the biometric authentication client, the biometric authentication client returns the device
30 information response to the biometric authentication middleware, and the biometric authentication middleware returns the device information response to the service client.

[0094] When the user initiates a process of authenticating a biometric identity on the service client of the user equipment, the service client initiates a device information request to the biometric authentication middleware, the biometric authentication

service processing result.

[0114] In an implementation, the authentication server can generate an authentication verification code of a virtual account corresponding to a device identity in an authentication information request packet after receiving the authentication information request packet. The authentication server encapsulates a virtual account identity, a server public key, and the generated authentication verification code into an authentication information response packet, sends the authentication information response packet to the service server, and starts timing. When generating an authentication request packet, the identity authentication detector of the user equipment also encapsulates the authentication verification code in the authentication information response packet into the authentication request packet. The authentication server receives the authentication request packet forwarded by the service server, compares the authentication verification code in the authentication request packet with the authentication verification code generated for the virtual account in the authentication request packet, and obtains the time difference between sending the authentication information response packet and receiving the authentication request packet. If the two authentication verification codes are different or the time difference exceeds second predetermined duration, the authentication server rejects the authentication request and informs the service server, and the service server notifies the service client of the authentication failure result. If the two authentication verification codes are different, and the time difference does not exceed the second predetermined duration, the authentication server performs signature verification on the authentication request packet by using the registered service public key, and performs identity authentication on the user based on the biometric feature token in the authentication request packet and the registered biometric feature token.

[0115] In an implementation including an authentication verification code, an interaction process among various function modules of user equipment, a service server, an authentication server, and a biometric authentication center server are shown in FIG. 7A to FIG. 7B.

[0116] In Implementation 2 of the present application, a device private key and a device public key pre-stored on the user equipment are used to ensure that the user equipment is a reliable device. A server public key and a server private key are used to verify reliability of the service server. As such, a correspondence among a device identity of the user equipment, a virtual account identity, a biometric authentication