

CLAIMS

1. A biometric feature based security verification method performed by a client device in an identity authentication system, wherein the identity authentication system further comprises a server, the security verification method comprising:

- 5 sending an authentication request to the server;
 receiving, from the server, an authentication request reply message;
 receiving a biometric feature input by a user;
 obtaining a biometric feature template ID corresponding to the biometric feature;
 comparing the obtained biometric feature template ID with a biometric feature template ID
10 included in a saved enable record, wherein the enable record is used for biometric feature verification
 and is obtained in a process of enabling biometric feature verification;
 generating an authentication response message comprising the obtained biometric feature
 template ID if the obtained biometric feature template ID and biometric feature template ID included
 in the saved enable record are consistent; and
15 sending the authentication response message to the server, so that the server receives the
 authentication response message and performs security verification.

2. The security verification method of claim 1, wherein the process of enabling the biometric feature verification comprises:

- 20 sending an enable request for enabling the biometric feature verification to the server;
 receiving an enable request reply message returned by the server;
 receiving the biometric feature used for verification and input by the user;
 obtaining the biometric feature template ID corresponding to the biometric feature used for
 verification;
25 generating and saving the enable record;
 generating an enable response message comprising the biometric feature template ID;, and
 sending the enable response message to the server, so that the server receives the enable
 response message, obtains the biometric feature template ID comprised in the message, and generates
 and saves a user record.

- 30 3. The security verification method of claim 2, wherein the server signs the authentication
 request reply message or the enable request reply message using an agreed first private key, and after
 the client device receives the authentication request reply message, the method further comprises:

verifying the received authentication request reply message using an agreed first public key, wherein a subsequent response is made only when the verification succeeds, otherwise an error is reported; and

5 after the client device receives the enable request reply message, the method further comprises:

verifying the received enable request reply message using the agreed first public key, wherein a subsequent response is made only when the verification succeeds, otherwise an error is reported.

4. The security verification method of claim 2, wherein the enable request reply message carries
10 a challenge value, and the process of enabling the biometric feature verification further comprises:

generating a user public and private key pair comprising a user private key and a user public key, and saving the user private key; and

15 selecting a signature algorithm according to the challenge value in the enable request reply message, and signing the generated enable response message using the selected signature algorithm and an agreed second private key and then sending the signed enable response message to the server, wherein the enable response message comprises the user public key, so that the server receives the enable response message and verifies the enable response message using the agreed second public key, the user public key being saved in the server; and optionally

20 wherein the authentication request reply message carries a challenge value, and the security verification method further comprises:

25 selecting a signature algorithm according to the challenge value, and signing the authentication response message using the selected signature algorithm and the user private key, so that the server also selects a signature algorithm according to the challenge value after receiving the authentication response message and verifies the authentication response message using the signature algorithm and the user public key.

5. The security verification method of claim 2, wherein the enable request reply message further comprises a user ID, and after the client device receives the enable request reply message, the method further comprises:

30 saving the user ID in the enable record, wherein the enable response message generated by the client device further comprises the user ID, so that after receiving the enable response message, the server obtains the user ID therein and saves the user ID in the user record,

optionally wherein the enable response message further comprises a client device ID, so that

after receiving the enable request reply message, the server obtains the device ID therein and saves the device ID in the user record, and

optionally wherein the authentication request reply message further comprises the user ID, and after the step of receiving a biometric feature input by a user and obtaining a biometric feature template ID corresponding to the biometric feature, the method further comprises:

searching for a corresponding enable record according to the user ID, so as to compare the obtained biometric feature template ID with the biometric feature template ID in the found enable record, wherein

the authentication response message generated by the client device further comprises the user ID, so that after receiving the authentication response message, the server obtains the user ID therein and searches for the corresponding user record according to the user ID, and optionally wherein the authentication response message further comprises the client device ID, so that after receiving the authentication response message, the server obtains the device ID therein and searches for the corresponding user record according to the device ID.

6. A biometric feature based security verification method performed by a server in an identity authentication system, wherein the identity authentication system further comprises a client device, the security verification method comprising:

receiving an authentication request from the client device;

sending an authentication request reply message to the client device;

receiving an authentication response message from the client device, wherein the authentication response message comprises a biometric feature template ID; and

performing verification by comparing the biometric feature template ID in the authentication response message with a biometric feature template ID included in a saved user record, wherein the saved user record is used for biometric feature verification and is obtained in a process of enabling the biometric feature verification, and wherein the verification succeeds if the biometric feature template ID in the authentication response message and the biometric feature template ID in the saved user record are consistent, otherwise an error is reported.

7. The security verification method of claim 6, wherein the process of enabling the biometric feature verification comprises:

receiving an enable request for enabling the biometric feature verification from the client device, and sending an enable request reply message to the client device, so that the client device

obtains, according to a biometric feature used for verification and input by a user, a biometric feature template ID corresponding to the biometric feature used for verification, and generates and saves an enable record; and

receiving an enable response message from the client device, obtaining the biometric feature
5 template ID comprised in the enable response message, and generating and saving the user record.

8. The security verification method of claim 7, wherein the security verification method further comprises:

signing the authentication request reply message or the enable request reply message using
10 an agreed first private key, so that the client device verifies the received authentication request reply message using an agreed first public key, wherein a subsequent response is made only when the verification succeeds, otherwise an error is reported; or the client device verifies the received enable request reply message using an agreed first public key, wherein a subsequent response is made only when the verification succeeds, otherwise an error is reported,

15 optionally wherein the enable request reply message carries a challenge value; the client device generates a user public and private key pair comprising a user private key and a user public key and saves the user private key; and the process of enabling the biometric feature verification further comprises:

receiving the enable response message signed by the client device using a selected signature
20 algorithm and an agreed second private key, wherein the signature algorithm is selected by the client device according to the challenge value in the enable request reply message, and the enable response message comprises a user public key; also selecting a signature algorithm according to the challenge value, and verifying the enable response message using a second public key, the user public key being saved in the server.

25

9. The security verification method of claim 8, wherein the security verification method further comprises:

receiving the authentication response message signed by the client device using a selected
signature algorithm and the user private key, wherein the signature algorithm is selected by the client
30 device according to the challenge value in the authentication request reply message; and also selecting a signature algorithm according to the challenge value, and verifying the signature on the authentication response message using the signature algorithm and the user public key.

10. The security verification method of claim 9, wherein the enable request reply message further comprises a user ID, so that the client device saves the user ID in the enable record after receiving the enable request reply message; the enable response message generated by the client device further comprises the user ID, and after the server receives the enable response message, the method further comprises:
- 5 obtaining the user ID from the enable response message, and saving the user ID in the user record.
11. The security verification method of claim 10, wherein the enable response message further comprises a client device ID, and after the server receives the enable response message, the method further comprises:
- 10 obtaining the device ID from the enable response message, and saving the device ID in the user record.
12. The security verification method of claim 10, wherein the authentication request reply message further comprises the user ID, so that the client device searches for the corresponding enable record according to the user ID, and compares the obtained biometric feature template ID with the biometric feature template ID in the found enable record; the authentication response message generated by the client device further comprises the user ID; and after the server receives the authentication response message, the method further comprises:
- 20 obtaining the user ID from the authentication response message, and searching for the corresponding user record according to the user ID.
13. The security verification method of claim 11, wherein the authentication response message further comprises the client device ID, and after the server receives the authentication response message, the method further comprises:
- 25 obtaining the device ID from the authentication response message, and searching for the corresponding user record according to the device ID.
14. A client device, applied to an identity authentication system, wherein the identity authentication system further comprises a server, the client device saves an enable record, and the enable record comprises a biometric feature template ID which is used for biometric feature verification and is obtained in a process of enabling the biometric feature verification; the client
- 30

device comprising:

multiple modules configured to perform operations according to the method of any one of claims 1 to 5.

- 5 15. A server, applied to an identity authentication system, wherein the identity authentication system further comprises a client device, the server saves a user record, and the user record comprises a biometric feature template ID which is used for biometric feature verification and is obtained in a process of enabling the biometric feature verification; the server comprising:

10 multiple modules configured to perform operations according to the method of any one of claims 6 to 13.