

CLAIMS

1. An identity authentication method, comprising:
 - receiving, by a terminal device, a service request;
 - collecting first biometric authentication information of a user associated with the service request;
 - comparing the first biometric authentication information with preset biometric authentication information;
 - when the comparison shows that the first biometric authentication information and the preset biometric authentication information are consistent reading a pre-stored digital signature certificate private key;
 - digitally signing the service request according to the digital signature certificate private key;
 - generating a biometric information verification message; and
 - sending the biometric information verification message to a server, wherein the server is configured to read a pre-stored digital signature certificate public key corresponding to the digital signature certificate private key, and
 - receiving, from the server, authentication result information after the server verifies and signs the biometric information verification message according to the digital signature certificate public key.
2. The method of claim 1, wherein the method further comprises generating and storing the digital signature certificate private key and the digital signature certificate public key, comprising:
 - receiving, by the terminal device, a registration request;
 - collecting second biometric authentication information of the user associated with the registration request;
 - when a comparison shows that the second biometric authentication information is consistent with the preset biometric authentication information generating the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric authentication information;
 - storing the digital signature certificate private key;

after the registration request is digitally signed according to a first preset private key, generating a registration request message, wherein the registration request message includes the digital signature certificate public key; and

sending the registration request message to the server, wherein the server is configured to store, after verifying and signing of the registration request message according to a first preset public key succeed, the digital signature certificate public key, wherein the first preset private key corresponds to the first preset public key.

3. The method of claim 1, wherein the method further comprises generating and storing the digital signature certificate private key and the digital signature certificate public key, comprising:

receiving, by the terminal device, a first registration request;

collecting second biometric authentication information of the user according to the first registration request;

generating the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric authentication information;

storing the digital signature certificate private key;

generating, after the registration request is digitally signed according to a first preset private key, a registration request message, wherein the registration request message carries the digital signature certificate public key; and

sending the registration request message to the server, such that the server stores, after verifying and signing of the registration request message according to a first preset public key succeed, the digital signature certificate public key, wherein the first preset private key corresponds to the first preset public key.

4. The method of claim 2 or 3, wherein the preset biometric authentication information is stored locally at the terminal device.

5. The method of any one of claims 1, 2, or 3, wherein the biometric authentication information comprises one or more of the following: fingerprint information, face image information, and voice information.

6. The method of claim 2 or 3, wherein generating the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric authentication information comprises generating the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric authentication information according to an ID of the user, an ID of the terminal device, and result information of the comparison showing consistency.
7. The method of claim 2 or 3, wherein receiving, by the terminal device, a registration request, and collecting second biometric authentication information of the user associated with the registration request comprises:
 - sending, by the terminal device, the registration request to the server;
 - receiving, from the server, a response message associated with the registration request; and
 - verifying and signing the response message;
 - after the verification and signature succeed, collecting the second biometric authentication information of the user.
8. The method of claim 2 or 3, wherein sending the registration request message to the server comprises:
 - verifying, by the terminal device, whether the user is a valid user;
 - checking an original payment password when the user is a valid user; and
 - when the check succeeds, sending the registration request message to the server.
9. The method of claim 8, wherein verifying whether the user is a valid user comprises:
 - obtaining a mobile phone number associated with the user;
 - sending a short message to a mobile phone associated with the mobile phone number; and
 - receiving, in response to sending the short message, a message acknowledging receipt of the received short message.
10. The method of any one of claims 1, 2, 3, and 6 to 9, wherein the method is applied to identity authentication during payment, and the service request is a payment request.

11. The method of any preceding claim, further comprising:
 encrypting the service request; and
 decrypting the encrypted service request according to a preset algorithm after verifying and signing the biometric information verification message according to the digital signature certificate public key; and
 returning result information indicating whether the authentication succeeds only after the decryption succeeds.
12. An identity authentication apparatus, the apparatus comprising a plurality of units configured to perform the method of any one of claims 1 to 11.