

CLAIMS

1. ~~A computer implemented method, comprising:~~
 - ~~obtaining a biometric information verification message from a payment client of a terminal device;~~
 - 5 ~~obtaining a pre-stored digital signature certificate public key from a security server;~~
 - ~~verifying the biometric information verification message based on the pre-stored digital signature certificate public key;~~
 - ~~generating an authentication result based on verifying the biometric information verification message; and~~
 - 10 ~~sending the authentication result to the terminal device, wherein the authentication result is configured to enable the terminal device to perform a payment operation.~~An identity authentication method for authenticating of identity of a user for performing a payment operation, via a terminal device where a payment client that is packed with a security client is installed, comprising:
 - 15 generating and storing a digital signature certificate private key and a digital signature certificate public key, wherein generating and storing the digital signature certificate private key and the digital signature certificate public key comprises
 - receiving, by the terminal device, a registration request and collecting second
 - biometric authentication information of the user according to the registration request,
 - 20 when a comparison shows that the second biometric authentication information is consistent with preset biometric authentication information collected in advance by a collection module of the terminal device and capable of uniquely identifying the user, generating, by the security client, the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric authentication information, wherein the preset
 - 25 biometric authentication information is collected in advance by a collection module of the terminal device and is capable of uniquely identifying the user,
 - storing, by the security client, 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
 - 30 digital signature certificate public key, and
 - sending the registration request message to a payment server such that a security

server receives the registration request message through the payment server, wherein, after verifying and signing of the registration request message according to a first preset public key succeed, the security server stores the digital signature certificate public key, wherein the first preset private key corresponds to the first preset public key;

5 receiving (S110), by the payment client at the terminal device, a payment request by the user to perform the payment operation;

collecting (S110), by the collection module of the terminal device, first biometric authentication information of the user of the payment request to uniquely identify the user;

10 comparing (S120), by the security client, the first biometric authentication information with the preset biometric authentication information, wherein the security client is configured to store a digital signature algorithm, a security client private key, a security server public key, and the generated and stored digital signature certificate private key generated based on a registration request from the payment client;

15 reading (S120), by the security client, the digital signature certificate private key when the comparison shows that the first biometric authentication information and the preset biometric authentication information are consistent;

digitally signing (S130), by the security client, the payment request according to the stored digital signature certificate private key to generate a biometric information verification message;

20 sending (S140), by the payment client at the terminal device, the biometric information verification message to the payment server, wherein the payment server reads the stored digital signature certificate public key corresponding to the digital signature certificate private key from the security server corresponding to the security client, wherein the security server is packed in the payment server, and wherein the security server is configured to store the digital signature algorithm, a security client public key, a security server private key, a registration agreement for
25 biometric authentication, and the generated and stored digital signature certificate public key; and

returning (S140), by the payment server, after verifying and signing the biometric information verification message according to the generated and stored digital signature certificate public key, authentication result information to the terminal device to perform the payment operation at the payment client.

30

2. The method of claim 1, wherein the preset biometric authentication information is stored locally at the terminal device.

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

4. The method of claim 1, wherein generating the digital signature certificate private key and the digital signature certificate public key corresponding to the second biometric
10 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.

5. The method of claim 1, wherein receiving, by the terminal device, the registration request, and collecting second biometric authentication information of the user according to the registration request comprises:

sending, by the security client at the terminal device, the registration request to the security server;

20 receiving a response message, at the payment server, returned by the security server according to the registration request; and

verifying and signing the response message at the payment client by invoking the security client, and collecting the second biometric authentication information of the user after the verification message based on the pre-stored digital signature certificate public key
25 comprises: and signature succeeds.

6. The method of claim 1, wherein sending the registration request message to the payment server comprises:

verifying, by the terminal device, whether the user is a valid user; and

30 checking an original payment password when the user is the valid user, and sending the registration request message to the payment server when the check succeeds.

7. The method of claim 6, wherein verifying whether the user is the valid user comprises:

obtaining a mobile phone number bound to the user;

5 sending a short message to a mobile phone associated with the mobile phone number; and
receiving a message indicating acknowledgement of receiving of the short message.

8. The method of any of claims 1 and 5 to 7, wherein the method is applied to identity authentication during payment.

10

9. The method of any preceding claim, further comprising:

encrypting the payment request;

decrypting the encrypted payment request according to a preset algorithm after verifying
and signing the biometric information verification message with according to the pre-stored digital
15 signature certificate public key; and

returning result information indicating whether the authentication succeeds only after the
decryption succeeds.

20 ~~3. The method of claim 1, further comprising receiving a registration request from the terminal device.~~

~~4. The method of claim 3, further comprising:~~

25 ~~responsive to receiving the registration request from the terminal device, reading authentication challenge information by invoking the security server.~~

~~5. The method of claim 4, wherein the authentication challenge information is generated after the security server digitally signs a random character string generated for the registration request by using a preset security server private key.~~

30

~~6. The method of claim 5, wherein the random character string is generated according to a current timestamp.~~

~~7. The method of claim 4, further comprising sending a response message corresponding to the authentication challenge information to the payment client.~~

5

~~8.10. An identity authentication apparatus, the apparatus comprising a plurality of units configured to perform the method of any one of claims 1 to 7.~~

10 ~~9. A non-transitory, computer readable medium storing one or more instructions processor-executable by a computer system software modules stored in a memory of the apparatus, which when executed cause to perform operations corresponding to the method of any one of claims 1 to 7.9.~~