

CLAIMS

1. An authentication method of a biometric payment device, comprising:

acquiring, by the biometric payment device, a key pair of the biometric payment device, wherein the acquiring the key pair comprises: generating, by a secure element of the biometric payment device, a public key and a private key of the biometric payment device, and exporting the public key to a manufacturer device, the public key being uploaded to a payment authentication server by the manufacturer device, and the secure element being a hardware chip independent of a main chip of the biometric payment device;

generating, by the secure element of the biometric payment device, a signature according to the private key and device information of the biometric payment device, the signature being a ciphertext which is obtained by encrypting the device information by using the private key;

transmitting, by the biometric payment device, an authentication request to the payment authentication server, the authentication request including the device information and the signature, and instructing the payment authentication server to acquire the public key corresponding to the device information, decrypt the signature according to the public key to acquire the decrypted device information, verify the signature through verifying whether the decrypted device information is consistent with the received device information, in response to signature verification being passed, generate a verification result indicating that the signature verification is successful, and generate an authentication result indicating that authentication of the biometric payment device is successful according to the verification result;

receiving, by the biometric payment device, the authentication result returned by the payment authentication server, acquiring biometric data, and transmitting the biometric data and the device information to the payment authentication server, so that the payment authentication server matches the biometric data with feature data stored in a database and generates a payment code according to matched user account information in response to determining that the biometric payment device is an authenticated device according to the device information; and

receiving, by the biometric payment device, the payment code and initiating biometric payment to the payment authentication server according to the payment code, so that the payment authentication server performs the biometric payment.

2. The method according to claim 1, wherein acquiring the key pair comprises:

exporting, by the biometric payment device, multi-factor device information of the biometric payment device to the manufacturer device, wherein the multi-factor device information includes multiple device information and is transmitted to the payment authentication server through the manufacturer device, and the payment authentication server generates the key pair including the public key and the private key according to the multi-factor device information, stores the private key of the biometric payment device by using a dynamic link library file, and transmits the dynamic link library file storing the private key to the manufacturer device; and

locally burning, by the biometric payment device, in response to a burning instruction of the manufacturer device, the dynamic link library file returned by the payment authentication server onto the biometric payment device.

3. The method according to claim 1, wherein the generating the public key and the private key comprises: generating the public key and the private key based on a trusted execution environment (TEE); and

the generating the signature according to the private key and the device information of the biometric payment device comprises: generating the signature according to the private key and the device information based on the TEE.

4. The method according to claim 2, wherein the dynamic link library file is an obfuscated and reinforced dynamic link library file, and the generating the signature according to the private key and the device information of the biometric payment device comprises: generating the signature by encrypting the multi-factor device information according to the private key stored in the obfuscated and reinforced dynamic link library file.

5. An authentication method of a biometric payment device, comprising:

receiving, by a payment authentication server, a public key of a key pair of the biometric payment device from a manufacturer device, the key pair including the public key and a private key being generated by a secure element of the biometric payment device, the public key being exported to the manufacturer device, and the secure element being a hardware chip independent of a main chip of the biometric payment device;

receiving, by the payment authentication server, an authentication request transmitted by the biometric payment device, the authentication request including a signature and device

information of the biometric payment device, the signature being generated by the secure element of the biometric payment device according to the private key of the biometric payment device and the device information, the signature being a ciphertext which is obtained by encrypting the device information by using the private key;

acquiring, by the payment authentication server, the public key corresponding to the device information, decrypting the signature according to the public key to acquire the decrypted device information, verifying the signature through verifying whether the decrypted device information is consistent with the received device information, and in response to signature verification being passed, generating a verification result indicating that the signature verification is successful;

generating, by the payment authentication server, an authentication result indicating that authentication of the biometric payment device is successful according to the verification result; and

returning, by the payment authentication server, the authentication result to the biometric payment device, receiving biometric data and the device information from the biometric payment device, matching the biometric data with feature data stored in a database, generating a payment code according to matched user account information in response to determining that the biometric payment device is an authenticated device according to the device information, returning the payment code to the biometric payment device, and performing a biometric payment after the biometric payment device initiates the biometric payment.

6. The method according to claim 5, wherein the method further comprises:

acquiring, by the payment authentication server, multi-factor device information of the biometric payment device uploaded by the manufacturer device, wherein the multi-factor device information including multiple device information;

generating, by the payment authentication server, the key pair including the public key and the private key according to the multi-factor device information, and storing the private key of the biometric payment device by using a dynamic link library file; and

transmitting, by the payment authentication server, the dynamic link library file storing the private key to the manufacturer device, so that the biometric payment device locally burns, in response to a burning instruction of the manufacturer device, the dynamic link library file to the biometric payment device.

7. The method according to claim 6, wherein the method further comprises:

obfuscating and reinforcing the dynamic link library file storing the private key.

8. An authentication apparatus of a biometric payment device, comprising:

a key acquisition module, configured to acquire a key pair of the biometric payment device, wherein the acquiring the key pair comprises: generating, by a secure element of the biometric payment device, a public key and a private key of the biometric payment device, and exporting the public key to a manufacturer device, the public key being uploaded to a payment authentication server by the manufacturer device, and the secure element being a hardware chip independent of a main chip of the biometric payment device;

a signature module, configured to generate a signature according to the private key and device information of the biometric payment device, the signature being a ciphertext which is obtained by encrypting the device information by using the private key;

an authentication module, configured to transmit an authentication request to the payment authentication server, the authentication request including the device information and the signature, and instructing the payment authentication server to acquire the public key corresponding to the device information, decrypt the signature according to the public key to acquire the decrypted device information, verify the signature through verifying whether the decrypted device information is consistent with the received device information, in response to signature verification being passed, generate a verification result indicating that the signature verification is successful, and generate an authentication result indicating that authentication of the biometric payment device is successful according to the verification result; and

a receiving module, configured to receive the authentication result returned by the payment authentication server, acquire biometric data, and transmit the biometric data and the device information to the payment authentication server, so that the payment authentication server matches the biometric data with feature data stored in a database and generates a payment code according to matched user account information in response to determining that the biometric payment device is an authenticated device according to the device information; and receive the payment code and initiate biometric payment to the payment authentication server according to the payment code, so that the payment authentication server performs the biometric payment.

9. The apparatus according to claim 8, wherein the key acquisition module comprises:

a device information export module, configured to export multi-factor device information of the biometric payment device to the manufacturer device, wherein the multi-factor device information includes multiple device information and is transmitted to the payment authentication server through the manufacturer device, and the payment authentication server generates the key pair including the public key and the private key according to the multi-factor device information, stores the private key of the biometric payment device by using a dynamic link library file, and transmits the dynamic link library file storing the private key to the manufacturer device; and

a key import module, configured to locally burn, in response to a burning instruction of the manufacturer device, the dynamic link library file returned by the payment authentication server onto the biometric payment device.

10. The apparatus according to claim 8, wherein the key generation module is configured to generate the public key and the private key based on a trusted execution environment (TEE); and

the signature module is configured to generate the signature according to the private key and the device information based on the TEE.

11. The apparatus according to claim 9, wherein the dynamic link library file is an obfuscated and reinforced dynamic link library file, and the signature module is configured to generate the signature by encrypting the multi-factor device information according to the private key stored in the obfuscated and reinforced dynamic link library file.

12. An authentication apparatus of a biometric payment device, comprising:

an authentication acquisition module, configured to receive a public key of a key pair of the biometric payment device from a manufacturer device, the key pair including the public key and a private key being generated by a secure element of the biometric payment device, the public key being exported to the manufacturer device, and the secure element being a hardware chip independent of a main chip of the biometric payment device; receive an authentication request transmitted by the biometric payment device, the authentication request including a signature and device information of the biometric payment device, the signature being generated by the secure element of the biometric payment device according to the private key of the biometric payment device and the device information, the signature being a ciphertext which is obtained by encrypting the device information by using the private key;

a verification module, configured to acquire the public key corresponding to the device

information, decrypt the signature according to the public key to acquire the decrypted device information, verify the signature through verifying whether the decrypted device information is consistent with the received device information, and in response to signature verification being passed, generate a verification result indicating that the signature verification is successful;

an authentication module, configured to generate an authentication result indicating that authentication of the biometric payment device is successful according to the verification result; and

a transmitting module, configured to return the authentication result to the biometric payment device, receive biometric data and the device information from the biometric payment device, match the biometric data with feature data stored in a database, generate a payment code according to matched user account information in response to determining that the biometric payment device is an authenticated device according to the device information, return the payment code to the biometric payment device, and perform a biometric payment after the biometric payment device initiates the biometric payment.

13. The apparatus according to claim 12, wherein the apparatus further comprises:

a device information acquisition module, configured to acquire multi-factor device information of the biometric payment device uploaded by the manufacturer device, wherein the multi-factor device information including multiple device information;

a key generation module, configured to generate the key pair including the public key and the private key according to the multi-factor device information, and store the private key of the biometric payment device by using a dynamic link library file; and

a key transmitting module, configured to transmit the dynamic link library file storing the private key to the manufacturer device, so that the biometric payment device locally burns, in response to a burning instruction of the manufacturer device, the dynamic link library file to the biometric payment device.

14. The apparatus according to claim 13, wherein the apparatus further comprises a key processing module, configured to obfuscate and reinforce the dynamic link library file storing the private key.

15. A computer device, comprising a memory and a processor, the memory storing a computer program, and the computer program, when executed by the processor, causing the

processor to perform operations of the method according to any one of claims 1 to 7.

16. A computer-readable storage medium, storing a computer program, the computer program, when executed by a processor, causing the processor to perform operations of the method according to any one of claims 1 to 7.

17. A computer program, comprising computer instructions stored in a computer-readable storage medium, a processor of a computer device reading the computer instructions from the computer-readable storage medium, and executing the computer instructions, to cause the computer device to perform operations of the method according to any one of claims 1 to 7.