

device number, so as to implement two-way authentication between the device side and the payment system, mutually trust identities, and establish a two-way secure link.

[0005] In an actual application, it is relatively simple to use the mapping relationship between a signature and a device code for authentication. Another device may pretend to be the device for device authentication by migrating the device code and the device signature, thereby affecting the security performance of the biometric payment.

SUMMARY

[0006] According to embodiments of the present disclosure, an authentication method and apparatus of a biometric payment device, a computer device, and a storage medium are provided.

[0007] One aspect of the present disclosure provides an authentication method of a biometric payment device is provided. The method includes:

[0008] acquiring a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

[0009] generating a signature according to the key and device information;

[0010] transmitting an authentication request to the payment authentication server based on the device information and the signature, the authentication request instructing the payment authentication server to verify the signature according to the device information, and generate an authentication result of the biometric payment device according to a verification result; and

[0011] receiving the authentication result returned by the payment authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0012] Another aspect of the present disclosure provides an authentication method of a biometric payment device. The method includes:

[0013] receiving an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a payment authentication server and acquired through

communication between a manufacturer device and the payment authentication server;

[0014] verifying the signature according to the device information;

[0015] generating an authentication result of the biometric payment device according to a verification result; and

[0016] returning the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0017] Another aspect of the present disclosure provides an authentication apparatus of a biometric payment device. The apparatus includes:

[0018] a key acquisition module, configured to acquire a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

[0019] a signature module, configured to generate a signature according to the key and device information;

[0020] an authentication module, configured to transmit an authentication request to the payment authentication server based on the device information and the signature, the authentication request instructing the payment authentication server to verify the signature according to the device information, and generate an authentication result of the biometric payment device according to a verification result; and

[0021] a receiving module, configured to receive the authentication result returned by the payment authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0022] Another aspect of the present disclosure provides an authentication apparatus of a biometric payment device. The apparatus includes:

[0023] an authentication acquisition module, configured to receive an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a

payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

[0024] a verification module, configured to verify the signature according to the device information;

[0025] an authentication module, configured to generate an authentication result of the biometric payment device according to a verification result; and

[0026] a transmitting module, configured to return the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0027] Another aspect of the present disclosure provides a computer device, including 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:

[0028] acquiring a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

[0029] generating a signature according to the key and device information;

[0030] transmitting an authentication request to the payment authentication server based on the device information and the signature, the authentication request instructing the payment authentication server to verify the signature according to the device information, and generate an authentication result of the biometric payment device according to a verification result; and

[0031] receiving the authentication result returned by the payment authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0032] Another aspect of the present disclosure provides a computer device, including 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:

[0033] receiving an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a payment authentication server and acquired through

communication between a manufacturer device and the payment authentication server;

[0034] verifying the signature according to the device information;

[0035] generating an authentication result of the biometric payment device according to a verification result; and

[0036] returning the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0037] Another aspect of the present disclosure provides a computer-readable storage medium, storing a computer program, the computer program, when executed by a processor, causing the processor to perform:

[0038] acquiring a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

[0039] generating a signature according to the key and device information; transmitting an authentication request to the payment authentication server based on the signature, the authentication request carrying a device ID, and instructing the payment authentication server to verify the signature according to the device ID, and generate an authentication result of the biometric payment device according to a verification result; and

[0040] receiving the authentication result returned by the payment authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0041] Another aspect of the present disclosure provides a computer-readable storage medium, storing a computer program, the computer program, when executed by a processor, causing the processor to perform:

[0042] receiving an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a payment authentication server and acquired through

communication between a manufacturer device and the payment authentication server;

[0043] verifying the signature according to the device information;

[0044] generating an authentication result of the biometric payment device according to a verification result; and

[0045] returning the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

[0046] Another aspect of the present disclosure provides a computer program, including computer instructions, the computer instructions being stored in a computer-readable storage medium. The processor of the computer device reads the computer instructions from the computer-readable storage medium, and the processor executes the computer instructions, to cause the computer device to perform the steps in the method embodiments.

BRIEF DESCRIPTION OF THE DRAWINGS

[0047] To describe the technical solutions in the embodiments of the present disclosure or in the existing technology more clearly, the following briefly introduces the accompanying drawings required for describing the embodiments or the existing technology. Apparently, the accompanying drawings in the following description show merely some embodiments of the present disclosure, and a person of ordinary skill in the art may still derive other drawings from these accompanying drawings without creative efforts.

[0048] FIG. 1 is a diagram of an application environment of an authentication method of a biometric payment device according to an embodiment.

[0049] FIG. 2 is a schematic flowchart of an authentication method of a biometric payment device according to an embodiment.

[0050] FIG. 3 is a schematic diagram of a production environment of a biometric payment device according to an embodiment.

[0051] FIG. 4 is a schematic flowchart of an authentication process of a biometric payment device with a secure element (SE) according to an embodiment.

[0052] FIG. 5 is a schematic flowchart of an authentication process of a biometric payment device with a trusted execution environment (TEE) according to an embodiment.

CLAIMS

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

acquiring a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

generating a signature according to the key and device information;

transmitting an authentication request to the payment authentication server based on the device information and the signature, the authentication request instructing the payment authentication server to verify the signature according to the device information, and generate an authentication result of the biometric payment device according to a verification result; and

receiving the authentication result returned by the payment authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

2. The method according to claim 1, wherein acquiring the key recognized by the payment authentication server through the communication between the manufacturer device and the payment authentication server comprises:

generating a public key and a private key according to a key production instruction; and

exporting the public key to the manufacturer device, wherein the manufacturer device uploads the public key to the payment authentication server.

3. The method according to claim 1, wherein acquiring the key recognized by the payment authentication server through the communication between the manufacturer device and the payment authentication server comprises:

exporting multi-factor device information to the manufacturer device, wherein the multi-factor device information is transmitted to the payment authentication server through the manufacturer device, and the payment authentication server generates a dynamic link library file storing the key of the biometric payment device according to the multi-factor device information; and

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

4. The method according to claim 2, wherein the generating a public key and a private key according to a key production instruction comprises: controlling a secure element (SE) of the biometric payment device to generate the public key and the private key according to the key production instruction; and

the generating a signature according to the key and device information comprises: controlling the SE to generate the signature according to the private key and the device information.

5. The method according to claim 2, wherein the generating a public key and a private key according to a key production instruction comprises: generating the public key and the private key based on a trusted execution environment (TEE) according to the key production instruction; and

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

6. The method according to claim 3, wherein the dynamic link library file is an obfuscated and reinforced dynamic link library file, and the generating a signature according to the key and device information comprises: generating the signature by encrypting the device information according to the key stored in the obfuscated and reinforced dynamic link library file.

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

receiving an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

verifying the signature according to the device information;

generating an authentication result of the biometric payment device according to a verification result; and

returning the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

8. The method according to claim 7, wherein a method for acquiring the key recognized by the payment authentication server through the communication between the manufacturer device and the payment authentication server comprises:

acquiring a public key of the biometric payment device uploaded by the manufacturer device, wherein the public key and a private key corresponding to the public key are generated according to a key production instruction, and the public key is exported to the manufacturer device.

9. The method according to claim 7, wherein a method for acquiring the key recognized by the payment authentication server through the communication between the manufacturer device and the payment authentication server comprises:

acquiring multi-factor device information of the biometric payment device uploaded by the manufacturer device;

generating a dynamic link library file storing the key of the biometric payment device according to the multi-factor device information; and

transmitting the dynamic link library file to the manufacturer device, the dynamic link library file instructing the manufacturer device to burn the dynamic link library file to the biometric payment device.

10. The method according to claim 8, wherein the verifying the signature according to the device information comprises: acquiring the corresponding public key, and verifying the signature according to the device information and the public key.

11. The method according to claim 9, wherein the method further comprises:

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

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

a key acquisition module, configured to acquire a key of the biometric payment device, the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

a signature module, configured to generate a signature according to the key and device information;

an authentication module, configured to transmit an authentication request to the payment authentication server based on the device information and the signature, the authentication request instructing the payment authentication server to verify the signature according to the device information, and generate an authentication result of the biometric payment device according to a verification result; and

a receiving module, configured to receive the authentication result returned by the payment

authentication server, the authentication result causing the payment authentication server to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

13. The apparatus according to claim 12, wherein the key acquisition module comprises:

a key generation module, configured to generate a public key and a private key according to a key production instruction; and

a key export module, configured to export the public key to the manufacturer device, wherein the manufacturer device uploads the public key to the payment authentication server.

14. The apparatus according to claim 12, wherein the key acquisition module comprises:

a device information export module, configured to export multi-factor device information to the manufacturer device, wherein the multi-factor device information is transmitted to the payment authentication server through the manufacturer device, and the payment authentication server generates a dynamic link library file storing the key of the biometric payment device according to the multi-factor device information; 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.

15. The apparatus according to claim 13, wherein the key generation module is configured to control a secure element (SE) of the biometric payment device to generate the public key and the private key according to the key production instruction; and

the signature module is configured to control the SE to generate the signature according to the private key and the device information.

16. The apparatus according to claim 13, wherein the key generation module is configured to generate the public key and the private key based on a trusted execution environment (TEE) according to the key production instruction; and

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

17. The apparatus according to claim 14, 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 device information according to the key stored in the obfuscated and reinforced dynamic link library file.

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

an authentication acquisition module, configured to receive an authentication request transmitted by the biometric payment device based on a signature and device information, the signature being generated by the biometric payment device according to a key of the biometric payment device and the device information, and the key being recognized by a payment authentication server and acquired through communication between a manufacturer device and the payment authentication server;

a verification module, configured to verify the signature according to the device information;

an authentication module, configured to generate an authentication result of the biometric payment device according to a verification result; and

a transmitting module, configured to return the authentication result to the biometric payment device, to perform a biometric payment based on biometric data transmitted by the biometric payment device that have been authenticated.

19. The apparatus according to claim 18, wherein the apparatus further comprises:

a key acquisition module, configured to acquire a public key of the biometric payment device uploaded by the manufacturer device, wherein the public key and a private key corresponding to the public key are generated according to a key production instruction, and the public key is exported to the manufacturer device.

20. The apparatus according to claim 18, 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;

a key generation module, configured to generate a dynamic link library file storing the key of the biometric payment device according to the multi-factor device information; and

a key transmitting module, configured to transmit the dynamic link library file to the manufacturer device, the dynamic link library file instructing the manufacturer device to burn the dynamic link library file to the biometric payment device.

21. The apparatus according to claim 19, wherein the verification module is configured to acquire the corresponding public key, and verify the signature according to the device information and the public key.

22. The apparatus according to claim 20, wherein the apparatus further comprises a key

processing module, configured to obfuscate and reinforce the dynamic link library file storing the key.

23. 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 11.

24. 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 11.

25. 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 11.