

CLAIMS

What is claimed is:

1. A method for binding a wearable device, the method comprising:

providing, by the wearable device, device information of the wearable device to a terminal based on an established connection between the wearable device and the terminal, the device information including a device identification;

receiving, by the wearable device, a device certificate from a server, the device certificate generated by the server based on the device identification and the device certificate corresponds to a user account associated with the wearable device; and

storing, by the wearable device, the device certificate on the wearable device, the device certificate enabling the wearable device to perform a payment operation using the user account, wherein the payment operation is capable of being performed by the wearable device if the established connection between the wearable device and the terminal is not detected and wherein the payment operation comprises:

generating, by the wearable device, a transaction certificate based on the device certificate; and

providing, by the wearable device, the transaction certificate to a payee device.
2. The method according to claim 1, wherein providing device information of the wearable device to a terminal comprises displaying a two-dimensional code including the device information on a screen of the wearable device for the terminal to scan.
3. The method according to claim 1, wherein receiving a device certificate from a server comprises receiving a device certificate from the server via the connection between the wearable device and a terminal.

4. The method according to claim 1, further comprising sending, by the wearable device, an authorization request to the server, the authorization request including the device identification of the wearable device.
5. The method according to claim 1, wherein receiving a device certificate from a server comprises receiving the device certificate and a security certificate from the server, the security certificate being used for performing validation of the device certificate during the payment operation.
6. The method according to claim 1, the method further comprising:
- generating, by the wearable device, a device-side key and a server-side key used for encrypting the device certificate during transmission;
 - storing, by the wearable device, the device-side key on the wearable device, the device-side key being the same as the server-side key, or based on the server-side key;
 - transmitting, by the wearable device, the server-side key to the server; and
 - generating, by the wearable device, a decrypted device certificate by decrypting the device certificate received from the server using the device-side key, wherein the device certificate from the server is encrypted by the server using the server-side key.
7. The method according to claim 1, wherein the storing the device certificate comprises:
- encrypting, by the wearable device, the device certificate using an encryption algorithm to produce ciphertext; and
 - storing, by the wearable device, the ciphertext on the wearable device.
8. A method for binding a wearable device, the method comprising:

receiving, by a server, a binding request from the wearable device via a terminal, the binding request including a device identification of the wearable device and user account information associated with the wearable device;

generating, by the server, a device certificate of the wearable device based on the device identification, wherein the device certificate corresponds to a user account associated with the wearable device;

storing, by the server, a relationship between the device certificate and a user account associated with the wearable device; and

providing, by the server, the device certificate to the wearable device, the device certificate enabling the wearable device to perform a payment operation using the user account wherein the payment operation is capable of being performed by the wearable device if an established connection between the wearable device and the terminal is not detected.

9. The method according to claim 8, wherein the providing the device certificate comprises sending the device certificate to the wearable device via the terminal.

10. The method according to claim 9, the method further comprising generating, by the wearable device, a server-side key sent to the server, wherein the providing the device certificate to the wearable device comprises:

encrypting a device certificate using the server-side key; and

sending the encrypted device certificate to the wearable device via the terminal.

11. The method according to claim 8, the method further comprising receiving, by the server, an authorization request sent by the wearable device, the authorization request including the device identification of the wearable device, and wherein providing the device certificate to the wearable device comprises returning a response to the authorization request to the wearable device, the response including the device certificate.

12. The method according to claim 11, wherein the authorization request further includes a server-side key generated by the wearable device, and wherein the device certificate is encrypted using the server-side key.

13. The method according to claim 8, wherein providing the device certificate to the wearable device further comprises providing a security certificate to the wearable device, the security certificate used for performing validation on the device certificate during the payment operation.

14. A method for binding a wearable device, the method comprising:

establishing, by a terminal, a connection between a wearable device and the terminal;

acquiring, by the terminal, device information of the wearable device, the device information including a device identification of the wearable device;

sending, by the terminal, a binding request to a server, the binding request including the device identification of the wearable device and user account information, the binding request enabling the server to generate a device certificate corresponding to a user account associated with the wearable device and provide the device certificate to the wearable device; and

transmitting, by the terminal, the device certificate to the wearable device using the established connection, the device certificate enabling the wearable device to perform a payment operation using the user account wherein the payment operation is capable of being performed by the wearable device if the established connection between the wearable device and the terminal is not detected.

15. The method according to claim 14, the method further comprising:

receiving, by the terminal, the device certificate provided by the server; and

forwarding, by the terminal, the device certificate to the wearable device using the established connection.

16. The method according to claim 14, the method further comprising receiving, by the terminal, a server-side key from the wearable device using the established connection, the server-side key being used by the server for encrypting the device certificate for the wearable device.

17. The method according to claim 14, wherein the acquiring device information of the wearable device comprises:

scanning, by the terminal, a two-dimensional code displayed on a screen of the wearable device; and

acquiring, by the terminal, the device information of the wearable device from the scanned two-dimensional code.

18. A method for facilitating electronic payments, the method comprising:

receiving, by the wearable device, a device certificate corresponding to a user account associated with the wearable device from the terminal based on an established connection between the wearable device and the terminal;

generating, by the wearable device, a transaction certificate according to a stored device certificate for a user account associated with the wearable device, wherein the transaction certificate is capable of being generated by the wearable device if the established connection between the wearable device and a terminal is not detected; and

providing, by the wearable device, the transaction certificate to a payee device, the transaction certificate enabling the payee device to upload the transaction certificate to a server for processing a payment using the user account corresponding to the device certificate.

19. The method according to claim 18, wherein the stored device certificate is a device certificate ciphertext produced by encrypting the device certificate using an encryption algorithm, and wherein generating a transaction certificate comprises:

reading, by the wearable device, the device certificate ciphertext;

decrypting, by the wearable device, the ciphertext based on an decryption algorithm;
and

generating, by the wearable device, the transaction certificate according to the device certificate obtained from the decrypted ciphertext.

20. The method according to claim 18, wherein the wearable device further stores a security certificate corresponding to the user account, and wherein the generating a transaction certificate comprises generating a transaction certificate carrying validation information using a certificate generation algorithm, the transaction certificate based on the device certificate and the security certificate, the certificate generation algorithm corresponding to a certificate restoration algorithm adopted by the server for retrieving the device certificate and the security certificate from the transaction certificate.

21. The method according to claim 18, wherein the transaction certificate includes a two-dimensional code or a bar code.

22. A method for facilitating electronic payments, the method comprising:

receiving, by a server, a payment collection request sent by a payee device, the payment collection request including a transaction certificate generated by a wearable device and payment sum information, wherein the transaction certificate is capable of being generated by the wearable device if an available connection between the wearable device and a terminal is not detected;

restoring, by the server, a device certificate of the wearable device from the transaction certificate; and

processing, by the server, a payment according to the payment sum information using a user account corresponding to the device certificate based on a relationship between the device certificate of the wearable device and the user account stored by the server.

23. The method according to claim 22, wherein the restoring a device certificate of the wearable device from the transaction certificate further comprises

obtaining the device certificate and a security certificate of the wearable device by executing a certificate restoration algorithm on the transaction certificate, the certificate restoration algorithm corresponding to a certificate generation algorithm used by the wearable device for generating the transaction certificate, and

wherein the processing the payment further comprises performing validation on the transaction certificate using the security certificate, and, and if the validation is successful, performing a payment operation according to the payment sum information using the user account corresponding to the device certificate as payer.

24. The method according to claim 22, the method further comprising returning a result to the payee device indicating whether payment is successful.

25. A method for facilitating electronic payments, the method comprising:

acquiring, by a payee device, a transaction certificate of a wearable device, the transaction certificate generated by the wearable device according to a device certificate corresponding to a user account associated with the wearable device, wherein the transaction certificate is capable of being generated by the wearable device if an available connection between the wearable device and a terminal is not detected; and

sending, by the payee device, a payment collection request to a server, the payment collection request including the transaction certificate of the wearable device and payment sum information, the payment collection request being configured for allowing the server to restore the device certificate from the transaction certificate, and perform a payment operation according to the payment sum information using the user account corresponding to the device certificate.

26. The method according to claim 25, the method further comprising receiving, by the payee device, a result returned by the server indicating whether payment is successful.