

CLAIMS

What is claimed is:

1. A payment processing method, applied to an Internet of Things (IoT) device, comprising:

sending a device registration request to a first service terminal in response to a registration operation of a merchant, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant, for the first service terminal to allocate a public-private key pair to the IoT device, generate certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and validity period information of the certificate data, determine the certificate data and a private key in the public-private key pair as payment certificate information of the IoT device, and send the payment certificate information to the IoT device;

storing the received payment certificate information sent by the first service terminal;

determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user;

generating a payment request offline based on the payment information, the biometric feature information, and payment certificate information of the IoT device obtained in advance from the first service terminal, wherein the first service terminal is a service terminal corresponding to a payment application of the first user, and the payment certificate information includes certificate data and a private key;

sending the payment request to a second service terminal, for the second service terminal to send the payment request to the first service terminal, and for the first service terminal to perform payment processing based on the payment information and a payment account of the payment application in response to the first service terminal determining that the certificate data in the payment request is within a validity period and the certificate data in the payment request is consistent with certificate data of the

IoT device stored by the first service terminal, wherein the second service terminal is a service terminal of a merchant corresponding to the IoT device;

in response to determining that a validity period of the certificate data expires, sending a certificate update request to the first service terminal based on the certificate data, for the first service terminal to perform certificate update processing and send updated new certificate data to the IoT device; and

receiving the new certificate data sent by the first service terminal.

2. The method according to claim 1, wherein the generating the payment request offline based on the payment information, the biometric feature information, and the payment certificate information of the IoT device obtained in advance from the first service terminal includes:

obtaining user identification information of the first user offline based on the biometric feature information;

performing signature processing on the user identification information and time information of current time based on the private key to obtain signature data;

generating verification information to be verified based on the signature data and the certificate data; and

generating the payment request based on the verification information and the payment information.

3. The method according to claim 2, wherein the obtaining the user identification information of the first user offline based on the biometric feature information includes:

performing offline matching processing between the biometric feature information of the first user and biometric feature information stored in a first storage area; and

in response to the offline matching processing succeeding, obtaining user identification information associated with biometric feature information stored in the first storage area that matches with the biometric feature information of the first user, and determining the obtained user identification information as the user identification information of the first user.

4. The method according to claim 3, further comprising:

obtaining, from the first service terminal and at a predetermined time interval, biometric feature information and user identification information of a user who has subscribed to a biometric feature recognition payment service; and

storing, in the first storage area, the obtained biometric feature information and the obtained user identification information of the user as associated with one another.

5. The method according to claim 3, further comprising:

in response to the offline matching processing failing, displaying prompt information to prompt the first user to subscribe to a biometric feature recognition payment service for the payment account;

receiving user identification information and biometric feature information of the first user sent by the first service terminal, wherein the user identification information and the biometric feature information are determined by the first service terminal based on a request sent by the first user for subscribing to a biometric feature recognition payment service; and

storing, in the first storage area, the biometric feature information and the user identification information of the first user as associated with one another.

6. The method according to claim 1, further comprising: after the sending the payment request to the second service terminal,

receiving payment result information sent by the second service terminal, wherein the payment result information is information sent to the second service terminal after the first service terminal has performed the payment processing.

7. A payment processing method, applied to a first service terminal corresponding to a payment application, comprising:

receiving a device registration request sent by an Internet of Things (IoT) device, wherein the device registration request includes device identification information of the IoT device and merchant identification information of a merchant corresponding to the IoT device;

allocating a public-private key pair to the IoT device, and determining validity period information of certificate data to be generated;

generating the certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and the validity period information;

determining the certificate data and a private key in the public-private key pair as payment certificate information of the IoT device, and sending the payment certificate information to the IoT device;

storing, in a second storage area, the certificate data, the device identification information, and the merchant identification information as associated with one another;

receiving a payment request sent by a second service terminal, wherein the payment request is sent by the IoT device to the second service terminal; the payment request is generated offline by the IoT device in response to a payment operation of a first user based on payment information of a payment to be paid, biometric feature information of the first user, and payment certificate information of the IoT device, wherein the payment certificate information includes certificate data and a private key; the second service terminal is a service terminal of the merchant corresponding to the IoT device;

determining whether the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that the certificate data in the payment request is within a validity period and that the certificate data in the payment request is consistent with certificate data of the IoT device stored in the second storage area;

in response to the payment request satisfying the predetermined payment condition, performing payment processing based on the payment information;

receiving a certificate update request sent by the IoT device, wherein the certificate update request includes certificate data to be updated;

in response to determining that the certificate data to be updated satisfies a predetermined update condition, performing update processing to obtain new certificate data; and

sending the new certificate data to the IoT device.

8. The method according to claim 7, wherein the payment request includes verification information to be verified;

the determining whether the payment request satisfies the predetermined payment condition includes:

obtaining signature data to be verified and the certificate data from the verification information, wherein the signature data is data obtained by performing signature processing on user identification information of the first user and time information by using the private key;

obtaining a public key corresponding to the private key, validity period information of the certificate data, device identification information of the IoT device, and merchant identification information of the merchant from the certificate data;

verifying signature of the signature data by using the obtained public key;

determining whether the certificate data is within a validity period based on the validity period information;

obtaining associated certificate data from a second storage area based on the device identification information and the merchant identification information, and determining whether the obtained certificate data is consistent with the certificate data in the verification information; and

in response to the signature verification succeeding, the certificate data being within the validity period, and the obtained certificate data being consistent with the certificate data in the verification information, determining that the payment request satisfies the predetermined payment condition.

9. The method according to claim 8, wherein the performing payment processing based on the payment information includes:

determining a payment account of the first user based on the user identification information obtained through the signature verification; and

performing payment processing based on the payment information and the payment account.

10. The method according to claim 7, further comprising: after the performing the payment processing based on the payment information,

sending payment processing result information to the second service terminal, for the second service terminal to send the payment processing result information to the IoT device.

11. The method according to claim 7, further comprising:

receiving a subscription request sent by the first user, and obtaining the biometric feature information of the first user based on the subscription request;

performing subscription processing of a biometric feature recognition payment service for a corresponding payment account based on the biometric feature information; and

sending subscription success information to the first user, and sending the biometric feature information and user identification information to the IoT device, for the IoT device to store the biometric feature information and the user identification information.

12. A payment processing apparatus, applied to an IoT device, comprising:

a determination module, configured to determine payment information of a payment to be paid in response to a payment operation of a first user;

a collecting module, configured to collect to-be-verified biometric feature information of the first user;

a generating module, configured to generate a payment request offline based on the payment information, the biometric feature information, and payment certificate information of the IoT device obtained in advance from a first service terminal, wherein the first service terminal is a service terminal corresponding to a payment application of the first user, and the payment certificate information includes certificate data and a private key;

a receiving module, configured to receive the payment certificate information sent by the first service terminal; and receive new certificate data sent by the first service terminal;

a storage module, configured to store the payment certificate information; and store the new certificate data;

a sending module, configured to:

before the determination module determines the payment information of the payment to be paid in response to the payment operation of the first user, and before the collecting module collects the to-be-verified biometric feature information of the first user, send a device registration request to the first service terminal in response to a registration operation of the merchant, wherein the device registration request includes device identification information of the IoT device and merchant identification

information of the merchant, for the first service terminal to allocate a public-private key pair to the IoT device, generate the certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and validity period information of the certificate data, determine the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and send the payment certificate information to the IoT device;

in response to determining that a validity period of the certificate data expires, send a certificate update request to the first service terminal based on the certificate data, for the first service terminal to perform certificate update processing and send the new certificate data to the IoT device; and

send the payment request to a second service terminal, for the second service terminal to send the payment request to the first service terminal, and for the first service terminal to perform payment processing based on the payment information and a payment account of the payment application in response to the first service terminal determining that the certificate data in the payment request is within a validity period and that the certificate data in the payment request is consistent with certificate data of the IoT device stored by the first service terminal, wherein the second service terminal is a service terminal of a merchant corresponding to the IoT device.

13. The apparatus according to claim 12, wherein

the generating module is configured to:

obtain user identification information of the first user offline based on the biometric feature information;

perform signature processing on the user identification information and time information of current time based on the private key to obtain signature data;

generate verification information to be verified based on the signature data and the certificate data; and

generate the payment request based on the verification information and the payment information.

14. A payment processing apparatus, applied to a first service terminal corresponding to a payment application, comprising:

a receiving module, configured to receive a device registration request sent by an Internet of Things (IoT) device, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant; receive a payment request sent by a second service terminal, wherein the payment request is sent by the IoT device to the second service terminal; the payment request is generated offline by the IoT device in response to a payment operation of a first user based on payment information of a payment to be paid, biometric feature information of the first user, and payment certificate information of the IoT device, wherein the payment certificate information includes certificate data and a private key; the second service terminal is a service terminal of a merchant corresponding to the IoT device; and receive a certificate update request sent by the IoT device, wherein the certificate update request includes certificate data to be updated;

a determination module, configured to determine whether the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data in the payment request is within a validity period and is consistent with certificate data stored in a second storage area;

a processing module, configured to: allocate a public-private key pair to the IoT device, and determine validity period information of certificate data to be generated; generate the certificate data based on the device identification information, the merchant identification information, the public key in the public-private key pair, and the validity period information; determine the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and send the payment certificate information to the IoT device; store, in the second storage area, the certificate data, the device identification information, and the merchant identification information as associated with one another; in response to determining that the certificate data to be updated satisfies a predetermined update condition, perform update processing to obtain new certificate data; and send the new certificate data to the IoT device; and in response to the determination module determining that the payment request satisfies the predetermined payment condition, perform payment processing based on the payment information.

15. The apparatus according to claim 14, wherein the payment request includes verification information to be verified;

the determination module is configured to:

obtain signature data to be verified and the certificate data from the verification information, wherein the signature data is data obtained by performing signature processing on user identification information of the first user and time information by using the private key;

obtain a public key corresponding to the private key, validity period information of the certificate data, device identification information of the IoT device, and merchant identification information of the merchant from the certificate data;

verify signature of the signature data by using the obtained public key;

determine whether the certificate data is within a validity period based on the validity period information;

obtain associated certificate data from a second storage area based on the device identification information and the merchant identification information, and determine whether the obtained certificate data is consistent with the certificate data in the verification information; and

in response to the signature verification succeeding, the certificate data being within the validity period, and the obtained certificate data being consistent with the certificate data in the verification information, determine that the payment request satisfies the predetermined payment condition.

16. A payment processing system, comprising an IoT device, a first service terminal, and a second service terminal, the first service terminal being a service terminal corresponding to a payment application, and the second service terminal being a service terminal of a merchant corresponding to the IoT device;

the IoT device is configured to before determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user, send a device registration request to the first service terminal in response to a registration operation of the merchant, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant; determine payment information of a payment to be paid in response to a payment operation of a first user, and collect to-be-verified biometric feature information of the

first user; generate a payment request offline based on the payment information, the biometric feature information, and payment certificate information of the IoT device obtained in advance from the first service terminal; store the payment certificate information; in response to determining that a validity period of the certificate data expires, send a certificate update request to the first service terminal based on the certificate data; receive updated new certificate data; and send the payment request to the second service terminal, wherein the payment certificate information includes certificate data and a private key;

the second service terminal is configured to receive the payment request sent by the IoT device, and send the payment request to the first service terminal; and

the first service terminal is configured to receive the device registration request, allocate a public-private key pair to the IoT device, determine validity period information of certificate data to be generated, and generate certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and validity period information; determine the certificate data and a private key in the public-private key pair as the payment certificate information of the IoT device, and send the payment certificate information to the IoT device; store, in a second storage area, the certificate data, the device identification information, and the merchant identification information as associated with one another; receive a certificate update request including certificate data to be updated, perform update processing to obtain new certificate data, and send the new certificate data to the IoT device; determine whether the received payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data in the payment request is within a validity period and is consistent with certificate data stored in the second storage area, and in response to the payment request satisfying the predetermined payment condition, perform payment processing based on the payment information.

17. A payment processing device, applied to an Internet of Things (IoT) device, comprising:

a processor; and

a memory, configured to store a computer-executable instruction, wherein when executed, the computer-executable instruction enables the processor to perform the following operations:

before determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user, sending a device registration request to the first service terminal in response to a registration operation of the merchant, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant, for the first service terminal to allocate a public-private key pair to the IoT device, generate the certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and validity period information; determine the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and send the payment certificate information to the IoT device; storing the received payment certificate information sent by the first service terminal; in response to determining that a validity period of the certificate data expires, sending a certificate update request to the first service terminal based on the certificate data, for the first service terminal to perform certificate update processing, and send updated new certificate data to the IoT device; and receiving the new certificate data sent by the first service terminal;

determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user;

generating a payment request offline based on the payment information, the biometric feature information, and payment certificate information of an Internet of Things (IoT) device obtained in advance from a first service terminal, wherein the first service terminal is a service terminal corresponding to a payment application of the first user, and the payment certificate information includes certificate data and a private key; and

sending the payment request to a second service terminal, for the second service terminal to send the payment request to the first service terminal, and for the first service terminal to perform payment processing based on the payment information and a payment account of the payment application in response to the first service terminal determining that the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data in the payment request is within a validity period and is consistent with certificate data stored

in a second storage area, wherein the second service terminal is a service terminal of a merchant corresponding to the IoT device.

18. A payment processing device, applied to a first service terminal corresponding to a payment application, comprising:

a processor; and

a memory, configured to store a computer-executable instruction, wherein when executed, the computer-executable instruction enables the processor to perform the following operations:

receiving a device registration request sent by an Internet of Things (IoT) device, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant; allocating a public-private key pair to the IoT device, and determining validity period information of certificate data to be generated; generating the certificate data based on the device identification information, the merchant identification information, the public key in the public-private key pair, and the validity period information; determining the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and sending the payment certificate information to the IoT device; storing, in a second storage area, the certificate data, the device identification information, and the merchant identification information as associated with one another; receiving a certificate update request sent by the IoT device, wherein the certificate update request includes certificate data to be updated; in response to determining that the certificate data to be updated satisfies a predetermined update condition, performing update processing to obtain new certificate data; and sending the new certificate data to the IoT device; receiving a payment request sent by a second service terminal, wherein the payment request is sent by the IoT device to the second service terminal; the payment request is generated offline by the IoT device in response to a payment operation of a first user based on payment information of a payment to be paid, biometric feature information of the first user, and payment certificate information of the IoT device, wherein the payment certificate information includes certificate data and a private key; the second service terminal is a service terminal of a merchant corresponding to the IoT device;

determining whether the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data

in the payment request is within a validity period and is consistent with certificate data stored in the second storage area; and

in response to the payment request satisfying the predetermined payment condition, performing payment processing based on the payment information.

19. A storage medium of an Internet of Things (IoT) device, configured to store a computer-executable instruction, wherein when executed by a processor, the computer-executable instruction implements the following procedure:

before determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user, sending a device registration request to the first service terminal in response to a registration operation of the merchant, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant, for the first service terminal to allocate a public-private key pair to the IoT device, generate the certificate data based on the device identification information, the merchant identification information, a public key in the public-private key pair, and validity period information; determine the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and send the payment certificate information to the IoT device; storing the received payment certificate information sent by the first service terminal; in response to determining that a validity period of the certificate data expires, sending a certificate update request to the first service terminal based on the certificate data, for the first service terminal to perform certificate update processing, and send updated new certificate data to the IoT device; and receiving the new certificate data sent by the first service terminal;

determining payment information of a payment to be paid in response to a payment operation of a first user, and collecting to-be-verified biometric feature information of the first user;

generating a payment request offline based on the payment information, the biometric feature information, and payment certificate information of an Internet of Things (IoT) device obtained in advance from a first service terminal, wherein the first service terminal is a service terminal corresponding to a payment application of the first user, and the payment certificate information includes certificate data and a private key; and

sending the payment request to a second service terminal, for the second service terminal to send the payment request to the first service terminal, and for the first service terminal to perform payment processing based on the payment information and a payment account of the payment application in response to the first service terminal determining that the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data in the payment request is within a validity period and is consistent with certificate data stored in a second storage area, wherein the second service terminal is a service terminal of a merchant corresponding to the IoT device.

20. A storage medium of a first service terminal corresponding to a payment application, configured to store a computer-executable instruction, wherein when executed by a processor, the computer-executable instruction implements the following procedure:

receiving a device registration request sent by an Internet of Things (IoT) device, wherein the device registration request includes device identification information of the IoT device and merchant identification information of the merchant; allocating a public-private key pair to the IoT device, and determining validity period information of certificate data to be generated; generating the certificate data based on the device identification information, the merchant identification information, the public key in the public-private key pair, and the validity period information; determining the certificate data and the private key in the public-private key pair as the payment certificate information of the IoT device, and sending the payment certificate information to the IoT device; storing, in a second storage area, the certificate data, the device identification information, and the merchant identification information as associated with one another; receiving a certificate update request sent by the IoT device, wherein the certificate update request includes certificate data to be updated; in response to determining that the certificate data to be updated satisfies a predetermined update condition, performing update processing to obtain new certificate data; and sending the new certificate data to the IoT device;

receiving a payment request sent by a second service terminal, wherein the payment request is sent by an IoT device to the second service terminal; the payment request is generated offline by the IoT device in response to a payment operation of a first user based on payment information of a payment to be paid, biometric feature

information of the first user, and payment certificate information of the IoT device, wherein the payment certificate information includes certificate data and a private key; the second service terminal is a service terminal of a merchant corresponding to the IoT device;

determining whether the payment request satisfies a predetermined payment condition, wherein the predetermined payment condition comprises that certificate data in the payment request is within a validity period and is consistent with certificate data stored in the second storage area; and

in response to the payment request satisfying the predetermined payment condition, performing payment processing based on the payment information.