CLAIMS

1. A method for credit payment, the method comprising:

sending a transaction information to a transaction terminal (S110);

receiving current payment transaction deduction information that is sent by the transaction terminal based on the transaction information (S120);

generating a payment authorization license based on the deduction information and the transaction information by using an embedded secure element (eSE) of the mobile terminal (S130); and

sending the payment authorization license to the transaction terminal, the transaction terminal being configured to complete the current payment transaction based on the received payment authorization license (S140).

2. The method according to claim 1, further comprising:

in response to sending the transaction information to the transaction terminal, receiving an application public key certificate reading instruction sent by the transaction terminal (S150); and

sending an application public key certificate to the transaction terminal based on the application public key certificate reading instruction (S160).

3. The method according to any one of claims 1 to 2, wherein generating the payment authorization license by using the embedded secure element (eSE) of the mobile terminal comprises:

generating signature data based on the deduction information by using an application private key stored on the eSE (S131);

generating a transaction authentication code (TAC) based on the deduction information and the transaction information by using a TAC sub-key that is pre-generated on the eSE (S132); and

using the signature data and the TAC as the payment authorization license (S133).

4. The method according to any one of claims 1 to 3, wherein the transaction information comprises at least one of a payment card number, an available limit, and an entrance flag or an exit flag.

5. The method according to any one of claims 1 to 4, wherein the deduction information comprises a deduction amount, a date and time of the current payment transaction, an entrance flag or an exit flag of the current payment transaction, and station information of the current payment transaction.

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

subtracting the deduction amount from the available limit in the transaction information based on the deduction amount in the current payment transaction deduction information, to obtain a current available limit (S170); and

using the current available limit as an available limit corresponding to a user in the mobile terminal (S180).

7. A credit payment method based on a mobile terminal eSE, applied to a transaction terminal, wherein the method comprises:

receiving transaction information sent by a mobile terminal;

generating current payment transaction deduction information based on the transaction information;

sending the deduction information to the mobile terminal; and

when receiving a payment authorization license, determining, based on the payment authorization license, that the current payment transaction is completed.

8. The method according to any one of claims 1 to 7, wherein the application public key certificate is verified by using a credit authorization public key locally stored on the transaction terminal (S670).

9. The method according to claim 8, wherein completing the current payment transaction comprises:

verifying the signature data by using the application public key;

generating a transaction log when the signature data is verified; and

sending the transaction log to a predetermined server, so that the predetermined server deducts a corresponding amount of money from a user account corresponding to the mobile

terminal based on the transaction log, wherein the transaction log comprises a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available limit, and a TAC.

10. The method according to any preceding claim, wherein the current payment transaction is completed offline.

11. The method according to claim 8, wherein the method is applied to payment for bus traveling; and

the transaction information comprises at least an available limit and an entrance/exit flag, and the method further comprises:

determining whether the available limit in the transaction information is greater than or equal to a predetermined threshold;

if the available limit is greater than or equal to the predetermined threshold, checking whether the entrance/exit flag in the transaction information is an exited state; and

if the entrance/exit flag in the transaction information is an exited state, performing the step of sending an application public key certificate reading instruction to the mobile terminal.

12. A method for credit payment, the method comprising:

separately generating an application public key and an application private key by using an embedded secure element (eSE) of the mobile terminal (S710);

sending the application public key to a predetermined server, so that the predetermined server signs the application public key by using a locally stored authorization private key, to generate an application public key certificate (S720);

obtaining the public key certificate sent by the predetermined server, and saving both the application public key certificate and the application private key on the eSE (S730);

sending a credit payment data obtaining request to the predetermined server (S740); and

receiving credit payment data sent by the predetermined server, and enabling a credit payment function of the mobile terminal based on the credit payment data by using the eSE (S750).

13. The method according to claim 12, further comprising:

obtaining device parameter information of the mobile terminal (S701);

sending the device parameter information to the predetermined server, so that the predetermined server determines, based on the received device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment (S702);

determining whether the credit payment enabling information sent by the predetermined server is received (S703); and

in response to determining that the credit payment enabling information sent by the predetermined server is received, determining that the mobile terminal meets the hardware condition for enabling credit payment, and performing the step of separately generating an application public key and an application private key (S710).

14. The method according to any one of claims 12 or 13, further comprising:

obtaining user identity information (S705);

sending the user identity information to the predetermined server, so that the predetermined server determines, based on the received user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment (S706);

determining whether security authentication success information sent by the predetermined server is received (S707); and

in response to determining that the security authentication success information sent by the predetermined server is received, determining that the mobile terminal meets the security authentication condition for enabling credit payment, and performing the step of separately generating an application public key and an application private key (S708).

15. The method according to any one of claims 12 to 14, further comprising:

sending a request for obtaining a predetermined installation file to the predetermined server, wherein the predetermined installation file comprises a credit payment application and a registration script (S7091);

retrieving the credit payment application and the registration script that are sent by the predetermined server (S7092);

separately installing the credit payment application and the registration script on the eSE; and

separately generating an application public key and an application private key (S7093).

16. An apparatus for credit payment, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 15.