CREDIT PAYMENT METHOD AND APPARATUS BASED ON MOBILE TERMINAL ESE

TECHNICAL FIELD

[0001] The present disclosure relates to the field of communications technologies, and in particular, to a credit payment method and apparatus based on a mobile terminal eSE.

BACKGROUND

[0002] Currently, public transportation mainly includes ground transportations and subways. When users purchase public transportation tickets, they normally use cash or pre-paid cards. Cash payment is mainly used for the public transportation system, and the user can buy a ticket by inserting coins. Users can alternatively get pre-paid metro cards, and take a bus or subway by scanning the card.

[0003] When a user purchases a bus ticket in cash, because many buses are self-serving and provide no exchange, the user needs to prepare the exact amount of fares in advance, which can be inconvenient to the user. Moreover, after close of business, bus system staff needs to count all the small fares that are put in by the self-service bus users, bringing extra work to the staff. When a user uses a metro card to take the public transportation, because most current metro cards are non-contact radio frequency (RF) cards, user-caused damages and wears, such as bending the card, or abrasion of the card surface are easily made to the metro card during its normal use. When a user uses a single-ride card to take public transportation, the user normally buys the single-ride card in small fares, and the staff also needs to count the small fares.

[0004] When a user uses a reusable pre-paid card to take public transportation, because the reusable pre-paid card is unregistered and its loss cannot be reported, it can bring the user financial loss if the card is lost. The user also needs to purchase, recharge, and get a refund for the prepaid card at specified locations, which makes it inconvenient to the user.

SUMMARY

[0005] To resolve problems in related technologies, the present disclosure provides a credit payment method and apparatus based on a mobile terminal embedded secure element (eSE).

[0006] According to a first aspect of the implementations of the present disclosure, a credit payment method based on a mobile terminal eSE is provided, and is applied to a mobile terminal, and the method includes: sending transaction information to a transaction terminal; receiving current payment transaction deduction information that is sent by the transaction terminal based on the transaction information; generating a payment authorization license based on the deduction information and the transaction information by using an eSE of the mobile terminal; and sending the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license.

[0007] After sending transaction information to a transaction terminal, the method further includes: receiving an application public key certificate reading instruction sent by the transaction terminal; and sending an application public key certificate to the transaction terminal based on the application public key certificate reading instruction.

[0008] Further, generating a payment authorization license by using an eSE of the mobile terminal includes: generating signature data based on the deduction information by using an application private key stored on the eSE; 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; and using the signature data and the TAC as the payment authorization license.

[0009] Further, the payment method is applied to payment for bus traveling, and the transaction information includes a payment card number, an available limit, and an entrance/exit flag.

[0010] Further, the deduction information includes a deduction amount, a date and time of the current payment transaction, an entrance/exit flag of the current payment transaction sign, and station information of the current payment transaction.

[0011] The method further includes: 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; and using the current available limit as an available limit corresponding to a user in the mobile terminal.

[0012] According to a second aspect of the implementations of the present disclosure, a credit payment method based on a mobile terminal eSE is provided, and is applied to a transaction terminal, and the method includes: 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.

[0013] After receiving transaction information sent by a mobile terminal, the method further includes: sending an application public key certificate reading instruction to the mobile terminal; receiving an application public key certificate sent by the predetermined mobile terminal; verifying the application public key certificate by using a credit authorization public key locally stored on the transaction terminal; and when an application public key is restored from the application public key certificate during verification, performing the step of generating current payment transaction deduction information.

[0014] Further, the payment authorization license includes signature data and a TAC, and the determining, based on the payment authorization license, that the current payment transaction is completed includes: 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, where the transaction log includes a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available limit, and a TAC.

[0015] Further, the method is applied to payment for bus traveling, and the transaction information includes at least an available limit and an entrance/exit flag, and the method further includes: determining whether the available limit in the transaction information is greater than or equal to a predetermined threshold; and 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.

[0016] According to a third aspect of the implementations of the present disclosure, a credit payment method based on a mobile terminal eSE is provided, and is applied to a mobile terminal, and the method includes: separately generating an application public key and an application private key by using an eSE of the mobile terminal; 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; 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; sending a credit payment data obtaining request to the predetermined server; 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.

[0017] The method further includes: obtaining device parameter information of the mobile terminal; 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; checking whether the credit payment enabling information sent by the predetermined server is received; and when 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.

[0018] The method further includes: obtaining user identity information; 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; checking whether security authentication success information sent by the predetermined server is received; and when 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.

[0019] The method further includes: sending a request for obtaining a predetermined installation file to the predetermined server, where the predetermined installation file includes a credit payment application and a registration script; obtaining the credit payment application and the registration script that are sent by the predetermined server; and separately installing the credit payment application and the registration script on the eSE, and performing the step of separately generating an application public key and an application private key.

[0020] According to a fourth aspect of the implementations of the present disclosure, a credit payment method based on a mobile terminal eSE is provided, and is applied to a server, and the method includes: receiving an application public key sent by a mobile terminal; signing the application public key by using an authorization private key locally stored on the server to generate an application public key certificate; sending the application public key certificate to the mobile terminal, so that the mobile terminal saves the received application public key certificate on an eSE; receiving a credit payment data obtaining request sent by the mobile terminal; generating credit payment data corresponding to the mobile terminal based on the credit payment data obtaining request, and sending the credit payment data to the mobile terminal, so that the mobile terminal enables a credit payment function of the mobile terminal based on the received credit payment data.

[0021] The method further includes: receiving device parameter information sent by the mobile terminal; determining, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment; and when the mobile terminal meets the hardware condition for enabling credit payment, sending credit payment enabling information to the mobile terminal, and performing the step of receiving an application public key sent by a mobile terminal.

[0022] The method further includes: receiving user identity information sent by the mobile terminal; determining, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment; and when the mobile terminal meets the security authentication condition for enabling credit payment, sending security authentication success information to the mobile terminal, and performing the step of receiving an application public key sent by a mobile terminal.

[0023] The method further includes: receiving a request sent by the mobile terminal for obtaining a predetermined installation file, where the predetermined installation file includes a credit payment application and a registration script; and separately sending the credit payment application and the registration script to the mobile terminal based on the request for obtaining the predetermined installation file, and performing the step of receiving an application public key sent by a mobile terminal.

[0024] According to a fifth aspect of the implementations of the present disclosure, a credit payment apparatus based on a mobile terminal eSE is provided, and the apparatus includes: a transaction information sending unit, configured to send transaction information to a transaction terminal; a deduction information receiving unit, configured to receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information; a payment authorization license generation unit, configured to generate a payment authorization license based on the deduction information and the transaction information by using an eSE of the mobile terminal; and a payment authorization license sending unit, configured to send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license.

[0025] The apparatus further includes: an application public key certificate reading instruction receiving unit, configured to receive an application public key certificate reading instruction sent by the transaction terminal; and an application public key certificate sending unit, configured to send an application public key certificate to the transaction terminal based on the application public key certificate reading instruction.

[0026] Further, the payment authorization license generation unit includes: a signature data generation module, configured to generate signature data based on the deduction information by using an application private key stored on the eSE; a TAC generation module, configured to generate a TAC based on the deduction information and the transaction information by using a TAC sub-key that is pre-generated on the eSE; and a payment authorization license determining module, configured to use the signature data and the TAC as a payment authorization license.

[0027] Further, when the payment apparatus is applied to payment for bus traveling, the transaction information includes a payment card number, an available

limit, and an entrance/exit flag.

[0028] Further, the deduction information includes a deduction amount, a date and time of the current payment transaction, an entrance/exit flag of the current payment transaction sign, and station information of the current payment transaction.

[0029] The apparatus further includes: a current available limit generation unit, configured to subtract a 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; and an available limit determining unit, configured to use the current available limit as an available limit corresponding to a user in the mobile terminal.

[0030] According to a sixth aspect of the implementations of the present disclosure, a credit payment apparatus based on a mobile terminal eSE is provided, and is applied to a transaction terminal, and the apparatus includes: a transaction information receiving unit, configured to receive transaction information sent by a mobile terminal; a deduction information generation unit, configured to generate current payment transaction deduction information based on the transaction information; a deduction information sending unit, configured to send the deduction information to the mobile terminal; and a payment transaction completion determining unit, configured to: when a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed.

[0031] The apparatus further includes: an application public key certificate reading instruction sending unit, configured to send an application public key certificate reading instruction to the mobile terminal; an application public key certificate receiving unit, configured to receive an application public key certificate sent by the predetermined mobile terminal; and an application public key certificate verification unit, configured to verify the application public key certificate by using a credit authorization public key locally stored on the transaction terminal.

[0032] Further, the credit authorization license includes signature data and a TAC, and the credit transaction completion determining unit includes: a signature data verification module, configured to verify the signature data by using the application public key; a transaction log generation module, configured to generate a transaction log when the signature data is verified; and a transaction log sending module, configured to send 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, where the transaction log includes a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available limit, and a TAC.

[0033] Further, the apparatus is applied to payment for bus traveling, the transaction information includes at least an available limit and an entrance/exit flag, and the apparatus further includes a threshold determining unit and an entrance/exit flag determining unit; where the threshold determining unit is configured to determine whether the available limit in the transaction information is greater than or equal to a predetermined threshold; the entrance/exit flag determining unit is configured to: when the available limit is greater than or equal to the predetermined threshold, check whether the entrance/exit flag in the transaction information is an exited state; and the application public key certificate reading instruction sending unit is further configured to send the application public key certificate reading instruction to the mobile terminal when the entrance/exit flag in the transaction information is an exited state.

[0034] According to a seventh aspect of the implementations of the present disclosure, a credit payment apparatus based on a mobile terminal eSE is provided, and is applied to a mobile terminal, and the apparatus includes: a key generation unit, configured to separately generate an application public key and an application private key by using an eSE of the mobile terminal; an application public key sending unit, configured to send 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; a public key certificate acquisition unit, configured to obtain a public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE; a credit payment data obtaining request sending unit, configured to send a credit payment data obtaining request to the predetermined server; and a credit payment data setting unit, configured to receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data.

[0035] The apparatus further includes: a device parameter information acquisition unit, configured to obtain device parameter information of the mobile terminal; a device parameter information sending unit, configured to send 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; a credit payment enabling information check unit, configured to check whether credit payment enabling information sent by the predetermined server is received; and a credit payment hardware enabling condition, used to determine, when the credit payment enabling information sent by the predetermined server is received, that the mobile terminal meets the hardware condition for enabling credit payment.

[0036] The apparatus further includes: a user identity information acquisition unit, configured to obtain user identity information; a user identity information sending unit, configured to send 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; a security authentication success information check unit, configured to check whether security authentication success information sent by the predetermined server is received; and a hardware enabling condition confirm unit, configured to determine, when the security authentication success information sent by the predetermined server is received, that the mobile terminal meets the security authentication condition for enabling credit payment.

[0037] The apparatus further includes: a predetermined installation file obtaining a request sending unit, configured to send a request for obtaining a predetermined installation file to the predetermined server, where the predetermined installation file includes a credit payment application and a registration script; a file acquisition unit, configured to obtain the credit payment application and the registration script that are sent by the predetermined server; and a file installation unit, configured to separately install the credit payment application and the registration script on the eSE.

[0038] According to an eighth aspect of the implementations of the present disclosure, a credit payment apparatus based on a mobile terminal eSE is provided, and is applied to a server, and the apparatus includes: an application public key receiving unit, configured to receive an application public key sent by a mobile terminal; an application public key certificate generation unit, configured to sign the application public key by using an authorization private key locally stored on the server, to generate an application public key certificate; an application public key certificate sending unit, configured to send the application public key certificate to the mobile terminal, so that the mobile terminal saves the received application public key

certificate on an eSE; a credit payment data obtaining request receiving unit, configured to receive a credit payment data obtaining request sent by the mobile terminal; and a credit payment data generation unit, configured to generate credit payment data corresponding to the mobile terminal based on the credit payment data obtaining request, and send the credit payment data to the mobile terminal, so that the mobile terminal enables a credit payment function of the mobile terminal based on the received credit payment data.

[0039] The apparatus further includes: a device parameter information receiving unit, configured to receive device parameter information sent by the mobile terminal; a credit payment enabling hardware condition determining unit, configured to determine, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment; and a credit payment enabling information sending unit, configured to send credit payment enabling information to the mobile terminal when the mobile terminal meets the hardware condition for enabling credit payment.

[0040] The apparatus further includes: a user identity information receiving unit, configured to receive user identity information sent by the mobile terminal; a security authentication condition determining unit, configured to determine, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment; and a security authentication success information sending unit, configured to send security authentication success information to the mobile terminal when the user identity information meets the security authentication condition for enabling credit payment.

[0041] The apparatus further includes: a predetermined installation file obtaining request receiving unit, configured to receive a request sent by the mobile terminal for obtaining a predetermined installation file, where the predetermined installation file includes a credit payment application and a registration script; and an installation file sending unit, configured to separately send the credit payment application and the registration script to the mobile terminal based on the request for obtaining the predetermined installation file.

[0042] The technical solutions provided in the implementations of the present disclosure can include the following beneficial effects:

[0043] The credit payment method and apparatus based on a mobile terminal eSE provided in the present disclosure can be applied to a mobile terminal and a

transaction terminal. After enabling a payment application, a user can use the mobile terminal to complete offline credit payment with the transaction terminal. As such, a payment transaction can be made quickly and securely, and online payment is not required, so that a problem in related technologies that the user needs to use cash, a metro card, etc. to implement a payment transaction function when taking a public transportation vehicle can be effectively resolved.

[0044] It should be understood that the previous general description and the following detailed description are merely examples and explanations, and cannot limit the present disclosure.

BRIEF DESCRIPTION OF DRAWINGS

[0045] The accompanying drawings here are incorporated in the specification, constitute a part of the specification, show implementations that are in accordance with the present disclosure, and are used with the specification to explain a principle of the present disclosure.

[0046] FIG. 1 is a schematic diagram illustrating a credit authorization system, according to an implementation of the present disclosure.

[0047] FIG. 2 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to an example implementation.

[0048] FIG. 3 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to an example implementation.

[0049] FIG. 4 is a flowchart illustrating step S130 in FIG. 2.

[0050] FIG. 5 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to an example implementation.

[0051] FIG. 6 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0052] FIG. 7 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0053] FIG. 8 is a flowchart illustrating step S640 in FIG. 6.

[0054] FIG. 9 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0055] FIG. 10 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0056] FIG. 11 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0057] FIG. 12 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0058] FIG. 13 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0059] FIG. 14 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0060] FIG. 15 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0061] FIG. 16 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0062] FIG. 17 is a flowchart illustrating a credit payment method based on a mobile terminal eSE, according to another example implementation.

[0063] FIG. 18 is a diagram illustrating signaling among a credit authorization system application on a mobile phone, an eSE chip, and a transaction terminal, according to an implementation of the present disclosure.

[0064] FIG. 19 is a diagram illustrating signaling between a mobile terminal and a bus gate, according to an implementation of the present disclosure.

[0065] FIG. 20 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to an example implementation.

[0066] FIG. 21 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to an example implementation.

[0067] FIG. 22 is a schematic diagram illustrating a payment authorization license generation unit in FIG. 20.

[0068] FIG. 23 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to an example implementation.

[0069] FIG. 24 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0070] FIG. 25 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0071] FIG. 26 is a schematic diagram illustrating a payment transaction completion determining unit in FIG. 24.

[0072] FIG. 27 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0073] FIG. 28 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0074] FIG. 29 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0075] FIG. 30 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0076] FIG. 31 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0077] FIG. 32 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0078] FIG. 33 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0079] FIG. 34 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

[0080] FIG. 35 is a schematic diagram illustrating a credit payment apparatus based on a mobile terminal eSE, according to another example implementation.

DESCRIPTION OF IMPLEMENTATIONS

[0081] Example implementations are described in detail here, and examples of the example implementations are illustrated in the accompanying drawings. When the following description relates to the accompanying drawings, unless otherwise specified, same numbers in different accompanying drawings represent same or similar elements. Implementations described in the following example implementations do not represent all implementations consistent with the present disclosure. Instead, they are only examples of apparatuses and methods consistent with some aspects of the present disclosure that are described in detail in the appended claims.

[0082] Mobile payment is also referred to as mobile phone payment. A user can use a mobile terminal to pay for a purchased product or service. The mobile terminal can communicate with a transaction terminal through near field communication (NFC), to make a payment transaction. NFC, also referred to as short range

communication, is a short range high-frequency radio communication technology that allows electronic devices to exchange data through non-contact point-to-point data transmission. The secure nature of NFC technology shows good application prospect.

[0083] In the payment technology field, many mobile terminals with a transaction payment function have an embedded secure element (eSE) chip. The eSE chip can exist in a SIM card integrated chip, be integrated into a mobile terminal, or exist in an SD integrated chip. The eSE chip is a secured chip that is mainly responsible for data security storage, data encryption, etc. of the mobile terminal. For better description, in implementations of the present disclosure, the eSE chip is illustrated as being integrated into the mobile terminal. But it does not limit the present disclosure. The eSE on the mobile terminal is equivalent to a Java card, and complies with the JAVACARD specification and the GP specification. The Java card is an open standard formulated by Sun for a smart card development platform.

[0084] To facilitate better understanding and implementation of the present disclosure by a person skilled in the art, a correlation among a mobile terminal, a transaction terminal, and a server involved in the implementations of the present disclosure is first described briefly, such as how to transmit and process data between the terminals. Due to the wide application of the present disclosure, such as in mobile payment, for better description, the present disclosure is illustrated by a scenario where customers use mobile phone credit payment to purchase public transportation fares.

[0085] As shown in FIG. 1, a credit authorization system provided in an implementation of the present disclosure includes a mobile terminal 100, a transaction terminal 200, and a server 300. The mobile terminal 100 can be a mobile phone with a payment transaction function. The transaction terminal 200 can be a bus gate, and the bus gate is a POS terminal used in a bus system or a subway system. The server 300 is a server in a credit authorization system. Before making a payment transaction with the transaction terminal 200 by using the mobile terminal 100, a user needs to first enable a credit payment transaction function of the mobile terminal 100 by using the server 300, then can make the payment transaction with the transaction terminal 200 by using the mobile terminal 100. In addition, the transaction terminal 200 periodically uploads a transaction log of the mobile terminal 100 to the server 300, and the server 300 deducts a corresponding amount of money from an account corresponding to the mobile terminal 100, and pays the money to a bus company.

[0086] In the implementation provided in the present disclosure, two applications can be installed on the mobile terminal. One is a credit payment application which is installed on an eSE chip of the mobile terminal and can be a credit payment application applet. For a Java card, Sun sets Applet as the object for running on its platform. The other application on the mobile terminal can be a credit authorization system application. Functions of the previous two applications on the mobile terminal can be implemented by using one application. It is not limited in the present implementation.

[0087] The transaction terminal 200 uses a strict identity security authentication mechanism, to ensure that only a user who passes identity security authentication and has enough credit limit can enable a bus credit payment application.

[0088] The credit payment application applet is installed on the eSE chip of the mobile terminal 100 with an NFC function. During personalization, it generates an application public and private key pair, and saves the application private key on the eSE chip. A security mechanism of the eSE chip ensures that data of the eSE chip is not stolen in any circumstance. An application public key is signed as an application public key certificate by using a private key in the credit authorization system, and is saved on the eSE chip. A public key in the credit authorization system is provided for the transaction terminal 200, and a storage location is determined by the transaction terminal 200. Because it is a public key, no mandatory requirement is imposed on security.

[0089] When providing a credit payment transaction, after reading the application public key certificate in the credit payment application, the transaction terminal 200 verifies the application public key certificate by using the public key in the credit authorization system, to restore the application public key. The credit payment application applet on the eSE chip generates a payment authorization license by using the application private key. The transaction terminal 200 verifies the payment authorization license by using the application public key, and then checks a security factor in the authorization license after the verification passes. After confirming security, the transaction terminal 200 performs credit accounting, and then settles a corresponding credit account at a specified time. To ensure payment security, when a quantity of use times, a limit, or an interval time exceeds a specified threshold, the mobile terminal needs to connect to a network to verify user identity information, and grant authorization again.

[0090] Data interaction between the mobile terminal 100 and the transaction terminal 200 during a payment transaction is first described below.

[0091] To resolve a related technical problem, an implementation of the present disclosure provides a credit payment method based on a mobile terminal eSE, applied to a mobile terminal side. As shown in FIG. 2, the method can include the following steps:

[0092] In step S110, send transaction information to a transaction terminal.

[0093] For better description, the transaction terminal is a bus gate.

[0094] When a user holds a mobile terminal and approaches the bus gate to make a payment transaction, because the bus gate can generate a radio frequency field, when the mobile terminal approaches the bus gate, the mobile terminal can detect the radio frequency field generated by the bus gate, and then can detect the bus gate. When the mobile terminal detects the bus gate, the mobile terminal sends transaction information to the bus gate.

[0095] In step S120, receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information.

[0096] After receiving an application public key certificate sent by the mobile terminal, the bus gate verifies the application public key certificate, generates the current payment transaction deduction information, and sends the deduction information to the mobile terminal. The mobile terminal receives the deduction information sent by the bus gate.

[0097] In step S130, generate a payment authorization license based on the deduction information and the transaction information by using an eSE of the mobile terminal.

[0098] The payment authorization license generated by the mobile terminal includes: signature data and transaction authentication code (TAC).

[0099] In step S140, send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license.

[0100] After receiving the payment authorization license sent by the mobile terminal, the bus gate verifies the payment authorization license. If the license is verified, it is determined that the current payment transaction is completed.

[0101] In the credit payment method based on a mobile terminal eSE provided in the present implementation of the present disclosure, when the user makes a payment

transaction with the transaction terminal by using the mobile terminal, the mobile terminal successively sends, based on the relevant instruction information sent by the transaction terminal, the transaction information, the application public key certificate, and the generated payment authorization license to the transaction terminal, and the transaction terminal completes the current payment transaction based on the information sent by the mobile terminal. Compared with a problem in related technologies, in the credit payment method based on a mobile terminal eSE provided in the present implementation of the present disclosure, when making a transaction with the transaction terminal by using the mobile terminal, the user can separately make the mobile terminal and the transaction terminal be offline, so that credit accounting is used for a user account of the mobile terminal in a subsequent payment transaction process. The account is settled only after the user makes purchase by using the mobile terminal, so that the user can be protected from a capital loss risk caused by using cash in a transaction.

[0102] As refinement of the method in FIG. 2, in another implementation of the present disclosure, as shown in FIG. 3, after step S110, the method can further include the following steps:

[0103] In step S150, receive an application public key certificate reading instruction sent by the transaction terminal.

[0104] After the bus gate receives the transaction information sent by the mobile terminal, the bus gate sends the application public key certificate reading instruction to the mobile terminal after processing and confirming the transaction information. After the mobile terminal receives the application public key certificate reading instruction sent by the bus gate, a credit payment application on the mobile terminal reads an application public key certificate that is pre-generated and stored on the eSE of the mobile terminal.

[0105] In step S160, send an application public key certificate to the transaction terminal based on the application public key certificate reading instruction.

[0106] The credit payment application on the mobile terminal sends the read application public key certificate to the bus gate based on the application public key certificate reading instruction.

[0107] To describe in detail in the present implementation of the present disclosure, how the mobile terminal generates the payment authorization license, so

the transaction terminal can complete the current payment transaction based on the authorization license sent by the mobile terminal, as refinement of the method in FIG. 2, in another implementation of the present disclosure, as shown in FIG. 4, step S130 can further include the following steps:

[0108] In step S131, generate signature data based on the deduction information by using an application private key stored on the eSE.

[0109] The application private key is pre-generated and stored on the eSE of the mobile terminal. The credit payment application signs the deduction information by using the application private key, to generate the signature data. The deduction information includes a deduction amount, a date and time of the current payment transaction, an entrance/exit flag of the current payment transaction sign, and station information of the current payment transaction.

[0110] In step S132, generate a TAC based on the deduction information and the transaction information by using a TAC sub-key that is pre-generated on the eSE.

[0111] The credit payment application on the mobile terminal encrypts the deductible amount, the date of the current payment transaction, the time of the current payment transaction, the payment card number, the available limit, and a credit limit based on the deduction information and the transaction information, to generate the TAC. The credit limit is a maximum available amount authorized by a credit authorization system to the user in an offline mode.

[0112] The deduction information includes: the deduction amount, the date of the current payment transaction, the time of the current payment transaction, the entrance/exit flag of the current payment transaction sign, and the station information of the current payment transaction.

[0113] In step S133, use the signature data and the TAC as the payment authorization license.

[0114] The credit payment application can send the signature data and the TAC to the bus gate separately as the payment authorization license, or can send the signature data and the TAC together to the bus gate as a credit authorization license.

[0115] In addition, when the payment method is applied to payment for bus traveling, the transaction information includes a payment card number, an available limit, and an entrance/exit flag. The payment card number is a unique character code

generated by the credit authorization system for each user's credit payment application. The available limit is an amount of money that the user can use currently. The TAC sub-key is obtained by a server in the credit authorization system based on a card number hash by using a TAC parent private key.

[0116] As refinement of the method in FIG. 2, in another implementation of the present disclosure, as shown in FIG. 5, the method can further include the following steps:

[0117] In step S170, subtract 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.

[0118] In step S180, use the current available limit as an available limit corresponding to a user in the mobile terminal.

[0119] To describe a transaction payment process between the mobile terminal and the transaction terminal in detail, an implementation of the present disclosure provides an execution procedure of a credit payment method based on mobile terminal eSE on a transaction terminal side. As shown in FIG. 6, the method can include the following steps:

[0120] In step S610, receive transaction information sent by a mobile terminal.

[0121] A bus gate receives the transaction information sent by the mobile terminal. The transaction information includes a payment card number, an available limit, an entrance/exit flag, and information about a previous transaction. The bus gate checks content of the transaction information, for example, checking information such as an available limit of an account corresponding to the mobile terminal, the entrance/exit flag, etc. When the content is verified as qualified, the bus gate sends an application public key certificate reading instruction to the mobile terminal.

[0122] In step S620, generate current payment transaction deduction information based on the transaction information.

[0123] The bus gate verifies an application public key certificate sent by the mobile terminal. If the verification fails, the current payment transaction ends. If an application public key is restored from the application public key certificate, the verification succeeds, and the current payment transaction deduction information is generated. Notably, the current payment transaction deduction information can also be referred to as a deduction instruction, so the mobile terminal can generate a payment

authorization license after receiving the deduction information (deduction instruction) sent by the bus gate.

[0124] The current payment transaction deduction information includes a deduction amount, a date and time of the current payment transaction, an entrance/exit flag of the current payment transaction sign, and station information of the current payment transaction. The deduction amount is calculated by the bus gate based on information such as the entrance/exit flag of the current payment transaction.

[0125] In step S630, send the deduction information to the mobile terminal.

[0126] The bus gate sends the generated deduction information to the mobile terminal, so that after receiving the deduction information, the mobile terminal generates the payment authorization license based on the deduction information and the transaction information by using an eSE of the mobile terminal.

[0127] In step S640, when the payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed.

[0128] The payment authorization license includes: signature data and TAC. The bus gate verifies the signature data in the payment authorization license. If the verification fails, the current payment transaction ends. If the verification succeeds, a transaction log of the current payment transaction is recorded.

[0129] As refinement of the method in FIG. 6, as shown in FIG. 7, in another implementation of the present disclosure, after step S610, the method can further include the following steps:

[0130] In step S650, send an application public key certificate reading instruction to the mobile terminal.

[0131] In step S660, receive an application public key certificate sent by the predetermined mobile terminal.

[0132] After the bus gate sends the application public key certificate reading instruction to the mobile terminal, the mobile terminal sends the application public key certificate to the bus gate based on the instruction, and the bus gate receives the application public key certificate sent by the mobile terminal.

[0133] In step S670, verify the application public key certificate by using a credit authorization public key locally stored on a transaction terminal.

[0134] To determine whether the received application public key certificate is correct, and to use related information in the public key certificate, the application

public key certificate needs to be verified by using the credit authorization public key. The credit authorization public key can be pre-stored on the bus gate.

[0135] When the application public key is restored from the application public key certificate during verification, step S620 is performed.

[0136] To describe in detail how the transaction terminal completes the current payment transaction based on the authorization license sent by the mobile terminal in the present implementation of the present disclosure, as refinement of the method in FIG. 6, in another implementation of the present disclosure, as shown in FIG. 8, step S640 can further include the following steps:

[0137] In step S641, verify the signature data by using the application public key.

[0138] The application public key is restored by the bus gate from the payment authorization license sent by the mobile terminal, and the application public key checks whether related information in the signature data matches corresponding information in the application public key. If they match, the verification succeeds.

[0139] In step S642, generate a transaction log when the signature data is verified.

[0140] After the bus gate verifies the signature data, the transaction log of the current payment is generated. The transaction log includes: a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available limit, and a TAC.

[0141] In step S643, send 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.

[0142] As shown in FIG. 9, in another implementation of the present disclosure, the credit payment method based on a mobile terminal eSE provided in the implementation of the present disclosure is applied to payment for bus traveling. Before step S610, an execution procedure on the transaction terminal side can further include the following steps:

[0143] In step S691, determine whether the available limit in the transaction information is greater than or equal to a predetermined threshold.

[0144] If the available limit is greater than or equal to the predetermined threshold, step S692 is performed.

[0145] In step S692, check whether the entrance/exit flag in the transaction information is an exited state.

[0146] If the entrance/exit flag in the transaction information is an exited state,

step S610 is performed.

[0147] Step S691 is mainly to enable the bus gate to check, based on the transaction information sent by the mobile terminal, whether an available limit of a user account corresponding to the mobile terminal is enough to pay for the current payment transaction. If the available limit is insufficient, the current payment transaction is rejected. If the available limit is sufficient, the bus gate checks whether the entrance/exit flag in the transaction information is 0. If the entrance/exit flag is not 0, the current payment transaction is rejected. If the entrance/exit flag is 0, the current payment transaction is continued. Notably, when the entrance/exit flag is 1, it indicates that the user who holds the mobile terminal is in an entered state, and then the current payment transaction is rejected; when the entrance/exit flag is 0, it indicates that the user who holds the mobile terminal is in an exited state, and an account can be settled, so the current payment transaction is made.

[0148] The transaction information includes a payment card number, an available limit, an entrance/exit flag, and information about a previous transaction.

[0149] The previous implementation describes in detail the execution procedures on the mobile terminal side and the transaction terminal side in the credit payment method based on a mobile terminal eSE provided in the present disclosure during a payment transaction. Before the payment transaction is made between the mobile terminal and the transaction terminal, data needs to be interacted between the mobile terminal and a server in a credit authorization system, so as to enable a payment transaction function of the mobile terminal. Execution procedures on a mobile terminal side and a server side when a payment transaction function of the mobile terminal is enabled are described in detail below.

[0150] As shown in FIG. 10, when a mobile terminal enables a payment transaction function, an execution procedure on a mobile terminal side in a credit payment method based on a mobile terminal eSE provided in an implementation of the present disclosure can include the following steps:

[0151] In step S710, separately generate an application public key and an application private key by using an eSE of a mobile terminal.

[0152] A credit authorization system application installed on the mobile terminal sends a request to the eSE of the mobile terminal, to request the eSE to generate a pair of public key and private key, that is, the application public key and the application private key. The eSE sends the generated application public key to the credit

authorization system application on the mobile terminal.

[0153] In step S720, send 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.

[0154] After obtaining the application public key sent by the eSE, the credit authorization system application on the mobile terminal sends the application public key to the predetermined server, so that the predetermined server signs the application public key by using the locally stored authorization private key, to generate the application public key certificate. Notably, the predetermined server here can be a server in a credit authorization system.

[0155] In step S730, obtain the public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE. The eSE chip is a secure chip and mainly responsible for data security storage, data encryption, etc. of the mobile terminal, and can well store the application public key certificate and the application private key, to avoid a property loss caused to a user due to a data loss.

[0156] In step S740, send a credit payment data obtaining request to the predetermined server.

[0157] In step S750, receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data by using the eSE.

[0158] In another implementation provided in the present disclosure, as shown in FIG. 11, before step S710, the method can further include the following steps:

[0159] In step S701, obtain device parameter information of the mobile terminal.

[0160] The device parameter information of the mobile terminal can be hardware information of the mobile terminal. Because the credit payment method provided in the present disclosure is based on the mobile terminal eSE chip, whether the mobile terminal has a satisfactory eSE chip needs to be checked first. Further, whether the mobile terminal has another hardware condition required by a payment transaction, such as whether it has an NFC function, also needs to be checked based on the device parameter information. Certainly, the device parameter information can also be information such as a device model, a ROM version, a system model (such as,

Android), an application version, etc. of the mobile terminal.

[0161] In step S702, send 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.

[0162] The mobile terminal sends the obtained device parameter information of the mobile terminal to the server in the credit authorization system, so that the server determines, based on the received device parameter information, whether the mobile terminal meets the hardware condition for enabling credit payment.

[0163] In step S703, check whether credit payment enabling information sent by the predetermined server is received.

[0164] If the mobile terminal meets the hardware condition for enabling credit payment, the server end sends the credit payment enabling information to the mobile terminal. The credit payment enabling information can be a credit payment application enabling page.

[0165] If the mobile terminal does not meet the hardware condition for enabling credit payment, the server end does not send the credit payment enabling information to the mobile terminal.

[0166] When the credit payment enabling information sent by the predetermined server is received, step S704 is performed.

[0167] In step S704, determine that the mobile terminal meets the hardware condition for enabling credit payment, and step S710 is performed.

[0168] In addition to checking whether the mobile terminal meets the hardware condition for enabling credit payment, based on FIG. 10, before step S710, as shown in FIG. 12, whether the mobile terminal meets a security authentication condition further needs to be checked. Therefore, in another implementation of the present disclosure, the credit payment method based on a mobile terminal eSE provided in the present disclosure can further include the following steps:

[0169] In step S705, obtain user identity information.

[0170] The user identity information can be information such as an identity card number, a name, a bank card number, a mailbox, etc. of the user.

[0171] In step S706, send 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.

[0172] The mobile terminal sends the user identity information to the server in the credit authorization system, so that the server verifies the user identity information, for example, verifies whether the bank card number provides a service normally, whether a user account has a bad-credit transaction record, etc.

[0173] In step S707, check whether security authentication success information sent by the predetermined server is received.

[0174] After receiving the user information sent by the mobile terminal, the server end checks the user information, and if the mobile terminal meets the security authentication condition for enabling credit payment, the server end sends the security authentication success information to the mobile terminal.

[0175] When the security authentication success information sent by the predetermined server is received, step S708 is performed.

[0176] In step S708, determine that the mobile terminal meets the security authentication condition for enabling credit payment, and step S710 is performed.

[0177] When the mobile terminal receives the security authentication success information sent by the server end, the mobile terminal determines that the mobile terminal meets the security authentication condition for enabling credit payment.

[0178] When the mobile terminal does not receive the security authentication success information sent by the server end, the mobile terminal determines that the mobile terminal does not meet the security authentication condition for enabling credit payment.

[0179] Based on FIG. 10, before step S710, as shown in FIG. 13, a related application further needs to be installed on the mobile terminal. Therefore, the credit payment method based on a mobile terminal eSE provided in the present disclosure further includes the following steps:

[0180] In step S7091, send a request for obtaining a predetermined installation file to the predetermined server.

[0181] The predetermined installation file includes a credit payment application and a registration script.

[0182] In step S7092, obtain the credit payment application and the registration script that are sent by the predetermined server.

[0183] In step S7093, separately install the credit payment application and the

registration script on the eSE, and step S710 is performed.

[0184] After the credit payment application and the registration script are separately installed on the eSE chip, user personalization of the mobile terminal is completed. As such, a procedure of enabling a credit payment function on the mobile terminal side ends. Based on the previous implementations, an execution procedure on a server side of the credit authorization system in which the mobile terminal enables the credit payment function is described in detail below.

[0185] In another implementation provided in the present disclosure, as shown in FIG. 14, an execution procedure of a server (a server end of a credit authorization system) in the credit payment method based on a mobile terminal eSE provided in the present disclosure can include the following steps:

[0186] In step S810, receive an application public key sent by a mobile terminal.

[0187] After the mobile terminal generates the application public key and an application private key, it sends the application public key to a server in a credit authorization system, and the server receives the application public key sent by the mobile terminal.

[0188] In step S820, sign the application public key by using an authorization private key locally stored on the server, to generate an application public key certificate.

[0189] The credit authorization private key is a private key pre-generated in the credit authorization system, and the server signs, by using the private key, the application public key sent by the mobile terminal, to generate the application public key certificate.

[0190] In step S830, send the application public key certificate to the mobile terminal, so that the mobile terminal saves the received application public key certificate on an eSE.

[0191] After generating the application public key certificate, the server in the credit authorization system returns the application public key certificate to the mobile terminal, so that after receiving the application public key certificate sent by the server, the mobile terminal saves the application public key certificate on the eSE chip.

[0192] The server in the credit authorization system not only can return the application public key certificate to the mobile terminal, but is also responsible for checking, based on information sent by the mobile terminal, whether the mobile

terminal meets a condition for enabling credit payment.

[0193] In step S831, receive a credit payment data obtaining request sent by the mobile terminal.

[0194] Credit payment data can be a personalized script, and the personalized script includes a payment card number, a credit limit, an available limit, and a TAC sub-key. The payment card number is a unique character code generated by the credit authorization system for a credit payment application of each user. The available limit is an amount of money that the user can use currently. The TAC sub-key is obtained by the server in the credit authorization system based on a card number hash by using a TAC parent private key.

[0195] In step S832, generate credit payment data corresponding to the mobile terminal based on the credit payment data obtaining request, and send the credit payment data to the mobile terminal.

[0196] As such, the mobile terminal enables a credit payment function of the mobile terminal based on the received credit payment data.

[0197] Based on FIG. 14, as shown in FIG. 15, in another implementation provided in the present disclosure, the server (the server end of the credit authorization system) determines, based on device parameter information sent by the mobile terminal, whether the mobile terminal meets a hardware condition for enabling credit payment. Therefore, before step S810, the credit payment method based on a mobile terminal eSE provided in the implementation of the present disclosure can further include the following steps:

[0198] In step S840, receive device parameter information sent by the mobile terminal.

[0199] In a process of enabling the credit payment function, the mobile terminal can communicate with the server in the credit authorization system through a network or other similar methods, and the server in the credit authorization system can receive the device parameter information sent by the mobile terminal.

[0200] In step S850, determine, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

[0201] The parameter information sent by the mobile terminal can be information such as a device model, a ROM version, a system model (such as, Android), an application version, etc. of the mobile terminal. The server can check, based on the information sent by the mobile terminal, whether the mobile terminal has an eSE chip,

whether the mobile terminal has an NFC function, etc.

[0202] When the mobile terminal meets the hardware condition for enabling credit payment, step S860 is performed.

[0203] In step S860, send credit payment enabling information to the mobile terminal, and then step S810 is performed.

[0204] If the server detects that the mobile terminal meets the hardware condition for enabling credit payment, the server sends the credit payment enabling information to the mobile terminal. The credit payment enabling information can be a credit payment application enabling page. The user can enter user information on a credit payment application enabling interface on the mobile terminal, and upload the user information to the server.

[0205] If the server detects that the mobile terminal does not meet the hardware condition for enabling credit payment, the server does not send the credit payment enabling information to the mobile terminal.

[0206] In addition to check the device parameter information sent by the mobile terminal, the server in the credit authorization system further needs to check user identity information sent by the mobile terminal, and determine whether a user corresponding to the mobile terminal meets a security authentication condition. Therefore, based on FIG. 14, as shown in FIG. 16, in a process of enabling the credit payment function of the mobile terminal, before step S810, the credit payment method based on a mobile terminal eSE provided in the present disclosure can further include the following steps:

[0207] In step S870, receive user identity information sent by the mobile terminal.

[0208] The user identity information can be information such as an identity card number, a name, a bank card number, a mailbox, an Alipay account, etc. of the user.

[0209] In step S880, determine, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment.

[0210] For example, the server can check whether the bank card number in the user identity information provides a service normally, whether there is a bad transaction record, etc.

[0211] When the user identity information meets the security authentication condition for enabling credit payment, step S890 is performed.

[0212] In step S890, send security authentication success information to the

mobile terminal, and then step S810 is performed.

[0213] If the server detects that the mobile terminal meets the security authentication condition for enabling credit payment, the server sends the security authentication success information to the mobile terminal.

[0214] When the mobile terminal enables credit payment, a credit payment application and a registration script further need to be installed on the mobile terminal, and these installation files need to be sent to the mobile terminal by the server in a credit payment system. Therefore, based on FIG. 14, as shown in FIG. 17, in another implementation of the present disclosure, before step S810, the credit payment method based on a mobile terminal eSE provided in the present disclosure can further include the following steps:

[0215] In step S801, receive a request sent by the mobile terminal for obtaining a predetermined installation file.

[0216] The predetermined installation file includes a credit payment application and a registration script.

[0217] In step S802, separately send the credit payment application and the registration script to the mobile terminal based on the request for obtaining the predetermined installation file, and step S810 is performed.

[0218] After obtaining the credit payment application and the registration script that are sent by the server, the mobile terminal separately installs the credit payment application and the registration script on the eSE chip.

[0219] In a process used by the mobile terminal to enable a payment transaction and a repayment transaction, an execution procedure on a mobile terminal side and an execution procedure on a transaction terminal side are separately described in detail in the previous implementations. To further describe in detail how the mobile terminal enables a payment transaction, a payment transaction process, and how to exchange data between the mobile terminal and the transaction terminal, a data exchange relationship between the mobile terminal and the transaction terminal is described below by using a signaling diagram. Certainly, the transaction terminal involved in the implementation of the present disclosure can be a server in a credit authorization system, and details are not described subsequently.

[0220] In another implementation of the present disclosure, as shown in FIG. 18, in an implementation of the credit payment method based on a mobile terminal eSE provided in the present disclosure, a mobile phone represents a mobile terminal, and a

server in a credit authorization system represents a server, and when the mobile phone enables a credit payment function, a procedure among a credit authorization system application on the mobile terminal, an eSE chip, and a transaction terminal includes:

[0221] Step 1001: A credit authorization system application sends a request for obtaining device parameter information of a mobile phone.

[0222] Step 1002: An eSE returns the device parameter information of the mobile phone.

[0223] Step 1003: The credit authorization system application uploads the device parameter information.

[0224] Step 1004: A server in a credit authorization system determines whether the mobile phone meets a hardware condition for enabling credit payment.

[0225] Step 1005: Return a determination result.

[0226] Step 1006: The credit authorization system application determination result is: present a credit payment application enabling interface.

[0227] Step 1007: The credit authorization system application uploads user identity information.

[0228] Step 1008: The server in the credit authorization system determines whether the mobile phone meets a security authentication condition for enabling credit payment.

[0229] Step 1009: The server in the credit authorization system returns a determination result.

[0230] Step 1010: A user chooses to enable a credit payment application.

[0231] Step 1011: The credit authorization system application sends a credit payment application installation file request.

[0232] Step 1012: The server in the credit authorization system returns a credit payment installation file.

[0233] Step 1013: The credit authorization system application delivers the credit payment installation file.

[0234] Step 1014: The eSE installs the received credit payment installation file.

[0235] Step 1015: The eSE returns an installation result.

[0236] Step 1016: The credit authorization system application determines the installation result, and if the installation result is not a success, prompts the user.

[0237] Step 1017: The credit authorization system application sends an application public and private key generation instruction.

[0238] Step 1018: The eSE generates an application public key and an application private key, and stores the application private key.

[0239] Step 1019: The eSE returns the application private key.

[0240] Step 1020: The credit authorization system application sends the application public key and an eSE personalization request.

[0241] Step 1021: The server in the credit authorization system generates an application public key certificate and credit payment data by using a private key of the credit authorization system, and generates a TAC sub-key through hash.

[0242] Step 1022: The server in the credit authorization system returns the application public key certificate and the credit payment data.

[0243] Step 1023: The credit authorization system application sends the application public key and the credit payment data.

[0244] Step 1024: The eSE stores the application public key certificate and enables a credit payment function of the mobile terminal based on the credit payment data.

[0245] Step 1025: The eSE returns a result of enabling the credit payment function of the mobile terminal.

[0246] Step 1026: The credit authorization system application determines the result of enabling credit payment, and if there is an error, prompts the user.

[0247] Step 1027: The credit authorization system application sends the result of enabling credit payment.

[0248] Step 1028: The server in the credit authorization system records the result of enabling credit payment.

[0249] Step 1029: The server in the credit authorization system sends a processing completion result.

[0250] Step 1030: The credit authorization system application prompts the user that the credit payment application is successfully enabled.

[0251] A detailed process of mutual data exchange between the mobile terminal and the server during enabling of a payment transaction function is described in the previous implementations, and details are not described here again.

[0252] In another implementation provided in the present disclosure, as shown in FIG. 19, in the credit payment method based on a mobile terminal eSE provided in the present disclosure, in a payment transaction process of a mobile terminal, a data exchange procedure between the mobile terminal and a bus gate is as follows:

[0253] Step 2001: The bus gate selects a credit authorization system application.

[0254] Step 2002: The credit authorization system application reads data that needs to be returned.

[0255] Step 2003: The credit authorization system application returns a payment card number, an available limit, an entrance/exit flag, and information about a previous transaction.

[0256] Step 2004: The bus gate checks the available limit and the entrance/exit flag, and if the check fails, prompts rejection information.

[0257] Step 2005: The bus gate calculates a deduction amount.

[0258] Step 2006: The bus gate deducts money based on the deduction amount, transaction time, the entrance/exit flag, and transaction information.

[0259] Step 2007: The credit authorization system application generates a payment authorization license, including signature data and TAC.

[0260] Step 2008: The credit authorization system application returns the signature data and the TAC.

[0261] Step 2009: The bus gate verifies the signature data by using an application public key, and if the verification succeeds, records a transaction log, or if the verification fails, prompts rejection information.

[0262] The previous implementations of the present disclosure are described by using credit payment for a bus as an example. The technical solutions of the present application can also be applied to other scenarios, such as subway payment and offline business payment. In different application scenarios, some procedures or some data in the previous payment can be different, and it is not limited here. There can be different implementations in specific application scenarios.

[0263] By using the descriptions of the previous method implementations, a person skilled in the art can clearly understand that the present disclosure can be implemented by using software and a necessary universal hardware platform, and can certainly be implemented by hardware, but in many cases, the former is a better implementation. Based on such an understanding, the technical solutions of the present disclosure essentially or the part contributing to the existing technology can be implemented in a form of a software product. The computer software product is stored in a storage medium, and includes several instructions for instructing a computer device (which can be a personal computer, a server, a network device, etc.) to perform all or some steps of the methods described in the implementations of the present

disclosure. The storage medium includes various media that can store program code, such as a read-only memory (ROM), a random access memory (RAM), a magnetic disk, an optical disc, etc.

[0264] In addition, as an implementation of the previous implementations, an implementation of the present disclosure further provides a credit payment apparatus based on a mobile terminal eSE. The apparatus is in a mobile terminal. As shown in FIG. 20, the apparatus includes a transaction information sending unit 10, a deduction information receiving unit 20, a payment authorization license generation unit 30, and a payment authorization license sending unit 40.

[0265] The transaction information sending unit 10 is configured to send transaction information to a transaction terminal when the transaction terminal is detected.

[0266] The deduction information receiving unit 20 is configured to receive current payment transaction deduction information that is sent by the transaction terminal based on the transaction information.

[0267] The payment authorization license generation unit 30 is configured to generate a payment authorization license based on the deduction information and the transaction information by using an embedded secure element (eSE) of the mobile terminal.

[0268] The payment authorization license sending unit 40 is configured to send the payment authorization license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization license.

[0269] In another implementation of the present disclosure, based on FIG. 20, as shown in FIG. 21, the apparatus can further include: an application public key certificate reading instruction receiving unit 50, configured to receive an application public key certificate reading instruction sent by the transaction terminal; and an application public key certificate sending unit 60, configured to send an application public key certificate to the transaction terminal based on the application public key certificate reading instruction.

[0270] In another implementation of the present disclosure, based on FIG. 20, as shown in FIG. 22, the payment authorization license generation unit 30 includes: a signature data generation module 31, a TAC generation module 32, and a payment authorization license determining module 33.

[0271] The signature data generation module 31 is configured to generate signature data based on the deduction information by using an application private key stored on the eSE.

[0272] The TAC generation module 32 is configured to generate TAC based on the deduction information and the transaction information by using a transaction authentication code (TAC) sub-key that is pre-generated on the eSE.

[0273] The payment authorization license determining module 33 is configured to use the signature data and the TAC as a payment authorization license.

[0274] In another implementation of the present disclosure, based on FIG. 20, as shown in FIG. 23, the apparatus further includes a current available limit generation unit 70 and an available limit determining unit 80.

[0275] The current available limit generation unit 70 is configured to subtract a deduction amount from an available limit in the transaction information based on the deduction amount in the current payment transaction deduction information, to obtain a current available limit.

[0276] The available limit determining unit 80 is configured to use the current available limit as an available limit corresponding to a user in the mobile terminal.

[0277] An implementation of the present disclosure further provides a credit payment apparatus based on a mobile terminal eSE. The apparatus is in a transaction terminal. As shown in FIG. 24, the apparatus includes an application public key certificate reading instruction sending unit 110, a deduction information generation unit 120, a deduction information sending unit 130, and a payment transaction completion determining unit 140.

[0278] The transaction information receiving unit 110 is configured to receive transaction information sent by a mobile terminal.

[0279] The deduction information generation unit 120 is configured to generate current payment transaction deduction information based on the transaction information.

[0280] The deduction information sending unit 130 is configured to send the deduction information to the mobile terminal.

[0281] The payment transaction completion determining unit 140 is configured to: when a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed.

[0282] In another implementation of the present disclosure, based on FIG. 23, as

shown in FIG. 25, the apparatus further includes: an application public key certificate reading instruction sending unit 150, configured to send an application public key certificate reading instruction to the mobile terminal; an application public key certificate receiving unit 160, configured to receive an application public key certificate sent by the predetermined mobile terminal; and an application public key certificate verification unit 170, configured to verify the application public key certificate by using a credit authorization public key locally stored on the transaction terminal.

[0283] In another implementation of the present disclosure, based on FIG. 23, as shown in FIG. 26, the payment authorization license includes signature data and a transaction authentication code (TAC). The payment transaction completion determining unit 140 includes a signature data verification module 141, a transaction log generation module 142, and a transaction log sending module 143.

[0284] The signature data verification module 141 is configured to verify the signature data by using the application public key.

[0285] The transaction log generation module 142 is configured to generate a transaction log when the signature data is verified.

[0286] The transaction log sending module 143 is configured to send 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. The transaction log includes: a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available limit, and a TAC.

[0287] In another implementation of the present disclosure, based on FIG. 23, as shown in FIG. 27, the apparatus is applied to payment for bus traveling, the transaction information includes at least an available limit and an entrance/exit flag, and the apparatus further includes a threshold determining unit 180 and an entrance/exit flag determining unit 190.

[0288] The threshold determining unit 180 is configured to determine whether the available limit in the transaction information is greater than or equal to a predetermined threshold.

[0289] The entrance/exit flag determining unit 190 is configured to: when the available limit is greater than or equal to the predetermined threshold, check whether the entrance/exit flag in the transaction information is in an exited state.

[0290] The application public key certificate reading instruction sending unit 110 is further configured to send the application public key certificate reading instruction to the mobile terminal when the entrance/exit flag in the transaction information is in an exited state.

[0291] An implementation of the present disclosure further provides a credit payment apparatus based on a mobile terminal eSE. The apparatus is in a mobile terminal. As shown in FIG. 28, the apparatus includes a key generation unit 210, an application public key sending unit 220, a public key certificate acquisition unit 230, a credit payment data obtaining request sending unit 240, and a credit payment data setting unit 250.

[0292] The key generation unit 210 is configured to separately generate an application public key and an application private key by using an embedded secure element (eSE) of the mobile terminal.

[0293] The application public key sending unit 220 is configured to send 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.

[0294] The public key certificate acquisition unit 230 is configured to obtain a public key certificate sent by the predetermined server, and save both the application public key certificate and the application private key on the eSE.

[0295] The credit payment data obtaining request sending unit 240 is configured to send a credit payment data obtaining request to the predetermined server.

[0296] The credit payment data setting unit 250 is configured to receive credit payment data sent by the predetermined server, and enable a credit payment function of the mobile terminal based on the credit payment data.

[0297] In another implementation of the present disclosure, based on FIG. 27, as shown in FIG. 29, the apparatus further includes a device parameter information acquisition unit 260, a device parameter information sending unit 270, a credit payment enabling information check unit 280, and a credit payment hardware enabling condition 290.

[0298] The device parameter information acquisition unit 260 is configured to obtain device parameter information of the mobile terminal.

[0299] The device parameter information sending unit 270 is configured to send 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.

[0300] The credit payment enabling information check unit 280 is configured to determine whether credit payment enabling information sent by the predetermined server is received.

[0301] The credit payment hardware enabling condition 290 is used to determine, when the credit payment enabling information sent by the predetermined server is received, that the mobile terminal meets the hardware condition for enabling credit payment.

[0302] In another implementation of the present disclosure, based on FIG. 27, as shown in FIG. 30, the apparatus further includes a user identity information acquisition unit 201, a user identity information sending unit 202, a security authentication success information check unit 203, and a hardware enabling condition confirm unit 204.

[0303] The user identity information acquisition unit 201 is configured to obtain user identity information.

[0304] The user identity information sending unit 202 is configured to send 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.

[0305] The security authentication success information check unit 203 is configured to check whether security authentication success information sent by the predetermined server is received.

[0306] The hardware enabling condition confirm unit 204 is configured to determine, when the security authentication success information sent by the predetermined server is received, that the mobile terminal meets the security authentication condition for enabling credit payment.

[0307] In another implementation of the present disclosure, based on FIG. 27, as shown in FIG. 31, the apparatus further includes a predetermined installation file obtaining request sending unit 206, a file acquisition unit 207, and a file installation unit 208.

[0308] The predetermined installation file obtaining request sending unit 206 is configured to send a request for obtaining a predetermined installation file to the predetermined server.

[0309] The predetermined installation file includes a credit payment application and a registration script.

[0310] The file acquisition unit 207 is configured to obtain the credit payment application and the registration script that are sent by the predetermined server.

[0311] The file installation unit 208 is configured to separately install the credit payment application and the registration script on the eSE.

[0312] An implementation of the present disclosure further provides a credit payment apparatus based on a mobile terminal eSE. The apparatus is in a server. As shown in FIG. 32, the apparatus includes an application public key receiving unit 310, an application public key certificate generation unit 320, an application public key certificate sending unit 330, a credit payment data obtaining request receiving unit 340, and a credit payment data generation unit 350.

[0313] The application public key receiving unit 310 is configured to receive an application public key sent by a mobile terminal.

[0314] The application public key certificate generation unit 320 is configured to sign the application public key by using an authorization private key locally stored on the server, to generate an application public key certificate.

[0315] The application public key certificate sending unit 330 is configured to send the application public key certificate to the mobile terminal, so that the mobile terminal saves the received application public key certificate on an eSE.

[0316] The credit payment data obtaining request receiving unit 340 is configured to receive a credit payment data obtaining request sent by the mobile terminal.

[0317] The credit payment data generation unit 350 is configured to generate credit payment data corresponding to the mobile terminal based on the credit payment data obtaining request, and send the credit payment data to the mobile terminal, so that the mobile terminal enables a credit payment function of the mobile terminal based on the received credit payment data.

[0318] In another implementation of the present disclosure, based on FIG. 31, as shown in FIG. 33, the apparatus further includes a device parameter information receiving unit 360, a credit payment enabling hardware condition determining unit 370, and a credit payment enabling information sending unit 380.

[0319] The device parameter information receiving unit 360 is configured to receive device parameter information sent by the mobile terminal.

[0320] The credit payment enabling hardware condition determining unit 370 is

configured to determine, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

[0321] The credit payment enabling information sending unit 380 is configured to send credit payment enabling information to the mobile terminal when the mobile terminal meets the hardware condition for enabling credit payment.

[0322] In another implementation of the present disclosure, based on FIG. 31, as shown in FIG. 34, the apparatus further includes a user identity information receiving unit 301, a security authentication condition determining unit 302, and a security authentication success information sending unit 303.

[0323] The user identity information receiving unit 301 is configured to receive user identity information sent by the mobile terminal.

[0324] The security authentication condition determining unit 302 is configured to determine, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment.

[0325] The security authentication success information sending unit 303 is configured to send security authentication success information to the mobile terminal when the user identity information meets the security authentication condition for enabling credit payment.

[0326] In another implementation of the present disclosure, based on FIG. 31, as shown in FIG. 35, the apparatus further includes a predetermined installation file obtaining request receiving unit 304 and an installation file sending unit 305.

[0327] The predetermined installation file obtaining request receiving unit 304 is configured to receive a request sent by the mobile terminal for obtaining a predetermined installation file, and the predetermined installation file includes a credit payment application and a registration script.

[0328] The installation file sending unit 305 is configured to separately send the credit payment application and the registration script to the mobile terminal based on the request for obtaining the predetermined installation file.

[0329] With regard to the apparatus in the above embodiments, the specific manner in which each module performs an operation has been described in detail in the embodiment related to the method, and details are not described here.

[0330] It can be understood that the present disclosure can be applied to many general-purpose or special purpose computing system environments or configurations,

for example, a personal computer, a server computer, a handheld device or a portable device, a tablet device, a multi-processor system, a microprocessor-based system, a set top box, a programmable consumer electronic device, a network PC, a minicomputer, a mainframe computer, and a distributed computing environment including any one of the earlier described systems or devices.

[0331] The present disclosure can be described in the general context of an executable computer instruction executed by a computer, for example, a program module. Generally, the program module includes a routine, a program, an object, a component, a data structure, etc. for executing a particular task or implementing a particular abstract data type. The present disclosure can also be practiced in distributed computing environments. In the distributed computing environments, tasks are executed by remote processing devices that are connected through a communications network. In a distributed computing environment, the program module can be located in both local and remote computer storage media including storage devices.

[0332] Notably, in the present specification, relational terms such as "first", "second", etc. are merely used to distinguish one entity or operation from another entity or operation, and do not necessarily require or imply that there is any such actual relationship or sequence between these entities or operations. Moreover, the terms "include", "comprise", or their any other variant are intended to cover a non-exclusive inclusion, so that a process, a method, a product, or a device that includes a list of elements not only includes those elements but also includes other elements that are not expressly listed, or further includes elements inherent to such a process, method, product, or device. An element described by "includes a …" further includes, without more constraints, another identical element in the process, method, commodity, or device that includes the element.

[0333] A person skilled in the art can easily figure out another implementation solution of the present disclosure after considering the specification and practicing the present disclosure here. The present application is intended to cover any variations, functions, or adaptive changes of the present disclosure. These variations, functions, or adaptive changes comply with general principles of the present disclosure and include common knowledge or a commonly used technical means in the technical field that is not disclosed in the present disclosure. The specification and the implementations are merely considered as examples, and the actual scope and the

spirit of the present disclosure are pointed out by the appended claims.

[0334] It should be understood that the present disclosure is not limited to the accurate structures that are described above and that are shown in the accompanying drawings, and modifications and changes can be made without departing from the scope of the present disclosure. The scope of the present disclosure is limited only by the appended claims.

CLAIMS

1. 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).

2. The method according to claim 1, 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).

3. The method according to claim 1 or 2, 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).

4. The method according to any one of claims 1 to 3, 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).

5. An apparatus for credit payment, the apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 4.