CREDIT PAYMENT METHOD AND APPARATUS BASED ON MOBILE TERMINAL P2P

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 mobile terminal P2P.

BACKGROUND

[0002] Currently, public transportation mainly includes ground transportation and subway. 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 bus cards are non-contact radio frequency (RF) cards, user-caused damages and wears, such as bending the card, or abrasion of the card's 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 single-ride cards 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 pre-paid card is unregistered and its loss cannot be reported, a loss can be caused to the user after the reusable prepaid bus 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 overcome the problem in the related technologies, the present disclosure provides a credit payment method and apparatus based on mobile terminal P2P.

[0006] According to a first aspect of implementations of the present disclosure, a credit payment method based on mobile terminal P2P is provided, and is applied to a mobile terminal, and the method includes: receiving transaction information sent by a transaction terminal; generating transaction response information based on the transaction information, and sending the transaction response information to the transaction terminal; receiving deduction accept request information of the current payment transaction that is sent by the transaction terminal; generating an application-private-key-generated payment license in the mobile terminal based on the deduction accept request information and the transaction response information; and sending the payment license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment license.

[0007] After sending transaction information to a transaction terminal, the transaction response information that corresponds to the transaction information, the method further includes: receiving application public key certificate return request information sent by the transaction terminal; and generating application public key certificate response information for an application public key certificate in the mobile terminal based on the application public key certificate return request information, and sending the application public key certificate response information to the transaction terminal.

[0008] Further, generating an application-private-key-generated payment license in the mobile terminal includes: generating signature data based on the deduction accept request information by using an application private key stored in the mobile terminal; generating transaction authentication code (TAC) based on the deduction accept request information and the transaction response information by using a TAC sub-key pre-generated in the mobile terminal; and using the signature data and the

TAC as the payment license.

[0009] Further, the payment method is applied to public transportation payment; and the transaction response information includes a payment card number, an available limit, and an entry/exit flag.

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

[0011] Further, the method includes: subtracting the deduction amount from the available limit in the transaction response information based on the deduction amount in the deduction accept request information, to obtain a current available limit; and using the current available limit as an available limit of a user that corresponds to the mobile terminal.

[0012] According to a second aspect of the implementations of the present disclosure, a credit payment method based on mobile terminal P2P is provided, and the method includes: sending transaction information to a mobile terminal; receiving transaction response information sent by the mobile terminal; generating deduction accept request information of the current payment transaction based on the transaction response information; sending the deduction accept request information to the mobile terminal; and when receiving a payment license, determining, based on the payment license, that the current payment transaction can be completed.

[0013] After the receiving transaction response information sent by the mobile terminal, the method further includes: sending application public key certificate return request information to the mobile terminal; receiving application public key certificate response information sent by the mobile terminal; verifying a signature on an application public key certificate in the application public key certificate response information by using a credit-licensed public key in the transaction terminal; and when an application public key is restored from the application public key certificate during the signature verification process, performing the step of generating deduction accept request information of the current payment transaction.

[0014] Further, the payment method is applied to public transportation payment; and the transaction response information includes a payment card number, an available limit, an entry/exit flag, and information about a last transaction.

[0015] Further, the method includes: determining whether the payment card

number in the transaction response information is included in a predetermined blacklist; and when the payment card number in the transaction response information is not included in the predetermined blacklist, performing the step of sending application public key certificate return request information to the mobile terminal.

[0016] Further, the method includes: determining whether the available limit in the transaction response information is greater than or equal to a predetermined threshold; if the available limit is greater than or equal to the predetermined threshold, checking whether the entry/exit flag in the transaction response information is an exited state; and when the entry/exit flag is an exited state, performing the step of sending application public key certificate return request information to the mobile terminal.

[0017] Further, the payment license includes signature data and transaction authentication code (TAC), and the determining, based on the payment license, that the current payment transaction can be 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, based on the transaction log, a corresponding amount of fund from a user account that corresponds to the mobile terminal, where the transaction log includes the deduction amount, a transaction date, a transaction moment, a transaction terminal ID, a payment card number, an available limit, and the TAC.

[0018] According to a third aspect of the implementations of the present disclosure, a credit payment apparatus based on mobile terminal P2P is provided, and the apparatus includes: a first return request information receiving unit, configured to: when a transaction terminal is detected, receive transaction information sent by the transaction terminal; a transaction response information generation unit, configured to generate transaction response information based on the transaction information; an information sending unit, configured to send the transaction response information to the transaction terminal; a deduction accept request information receiving unit, configured to receive deduction accept request information of the current payment transaction that is sent by the transaction terminal; an application-private-key-generated payment license generation unit, configured to generate an application-private-key-generated payment license in the mobile terminal based on the deduction accept request information and the transaction response

information; and a payment license sending unit, configured to send the payment license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment license.

[0019] The apparatus further includes: a second return request information receiving unit, configured to receive application public key certificate return request information sent by the transaction terminal; an application public key certificate response information generation unit, configured to generate application public key certificate response information for an application public key certificate in the mobile terminal based on the application public key certificate return request information; and a public key certificate response information sending unit, configured to send the application public key certificate response information to the transaction terminal.

[0020] Further, the application-private-key-generated payment license generation unit includes: a signature data generation module, configured to generate signature data based on the deduction accept request information by using an application private key stored in the mobile terminal; an information generation module, configured to generate transaction authentication code (TAC) based on the deduction accept request information and the transaction response information by using a TAC sub-key pre-generated in the mobile terminal; and a payment license determining module, configured to use the signature data and the TAC as the payment license.

[0021] Further, the transaction response information includes a payment card number, an available limit, an entry/exit flag, and information about a last transaction.

[0022] Further, when the payment apparatus is applied to public transportation payment, the deduction accept request information includes a deduction amount, a date of the current payment transaction, a time of the current payment transaction, an entry/exit flag of the current payment transaction, and station information of the current payment transaction.

[0023] Further, the apparatus includes: a current available limit generation unit, configured to subtract the deduction amount from the available limit in the transaction response information based on the deduction amount in the deduction accept request information, to obtain a current available limit; and an available limit determining unit, configured to use the current available limit as an available limit of a user that corresponds to the mobile terminal.

[0024] According to a fourth aspect of the implementations of the present disclosure, a credit payment apparatus based on mobile terminal P2P is provided, and

the apparatus is applied to a transaction terminal and includes: a transaction information sending unit, configured to send transaction information to a mobile terminal; a transaction response information receiving unit, configured to receive transaction response information sent by the mobile terminal; a deduction unit, configured to generate deduction accept request information of the current payment transaction based on the transaction response information; a deduction accept request information sending unit, configured to send the deduction accept request information to the mobile terminal; and a current-payment-transaction complete unit, configured to: when a payment license is received, determine, based on the payment license, that the current payment transaction can be completed.

[0025] The apparatus further includes: a return request information sending unit, configured to send application public key certificate return request information to the mobile terminal; a public key certificate response information receiving unit, configured to receive application public key certificate response information sent by the mobile terminal; and a signature verification unit, configured to verify a signature on an application public key certificate in the application public key certificate response information by using a credit-licensed public key in the transaction terminal.

[0026] Further, the transaction response information includes a payment card number, an available limit, and an entry/exit flag.

[0027] Further, the apparatus includes: a blacklist determining unit, configured to determine whether the payment card number in the transaction response information is included in a predetermined blacklist; and the return request information sending unit is further configured to: when the payment card number in the transaction response information is not included in the predetermined blacklist, send the application public key certificate return request information to the mobile terminal.

[0028] Further, the apparatus includes: a threshold determining unit, configured to determine whether the available limit in the transaction response information is greater than or equal to a predetermined threshold; and a status checking unit, configured to: if the available limit is greater than or equal to the predetermined threshold, check whether the entry/exit flag in the transaction response information is an exited state.

[0029] Further, the payment license includes signature data and transaction authentication code (TAC), and the current-payment-transaction complete unit includes: a signature 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, based on the transaction log, a corresponding amount of fund from a user account that corresponds to the mobile terminal, where the transaction log includes the deduction amount, a transaction date, a transaction moment, a transaction terminal ID, a payment card number, an available limit, and the TAC.

[0030] The technical solutions provided in the implementations of the present disclosure can include the following beneficial effects:

[0031] The credit payment method and apparatus based on mobile terminal P2P that are provided in the present disclosure are applicable to the mobile terminal and the transaction terminal. After enabling a payment application, a user can complete offline credit payment with a transaction terminal by using a mobile terminal, so that a payment transaction can be fast and securely completed, and online payment is not needed. Therefore, the following situation is avoided: in the related technology, for example, when a user takes a public transport vehicle, the user can implement a payment transaction function only by using cash or a bus card.

[0032] It should be understood that the previous general descriptions and the following detailed descriptions are merely examples and explanations, and cannot limit the present disclosure.

BRIEF DESCRIPTION OF DRAWINGS

[0033] The accompanying drawings here are incorporated in the specification, become 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.

[0034] FIG. 1 is a schematic diagram illustrating a credit authorization system, according to an example implementation.

[0035] FIG. 2 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to an example implementation.

[0036] FIG. 3 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to another example implementation.

[0037] FIG. 4 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0038] FIG. 5 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0039] FIG. 6 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0040] FIG. 7 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0041] FIG. 8 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0042] FIG. 9 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0043] FIG. 10 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0044] FIG. 11 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0045] FIG. 12 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0046] FIG. 13 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0047] FIG. 14 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0048] FIG. 15 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0049] FIG. 16 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0050] FIG. 17 is a flowchart illustrating a credit payment method based on mobile terminal P2P, according to yet another example implementation.

[0051] FIG. 18 is a flowchart illustrating step S450 in FIG. 14.

[0052] FIG. 19 is a diagram illustrating a data exchange procedure between a

credit authorization system application, a credit payment application, and a serving end of a credit authorization system.

[0053] FIG. 20 is a diagram illustrating data exchange between a bus gate and a credit authorization system application.

[0054] FIG. 21 is a diagram illustrating data exchange between a bus gate and a serving end of a credit authorization system.

[0055] FIG. 22 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0056] FIG. 23 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0057] FIG. 24 is a schematic diagram illustrating an application-private-key-generated payment license generation unit in FIG. 22.

[0058] FIG. 25 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0059] FIG. 26 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0060] FIG. 27 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0061] FIG. 28 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0062] FIG. 29 is a schematic diagram illustrating a credit payment apparatus based on mobile terminal P2P, according to yet another example implementation.

[0063] FIG. 30 is a schematic diagram illustrating a current-payment-transaction complete unit in FIG. 26.

DESCRIPTION OF IMPLEMENTATIONS

[0064] Example implementations are described in detail here, and examples of the implementations are presented in the accompanying drawings. When the following description relates to the accompanying drawings, the same numbers in different accompanying drawings represent the same element or similar elements unless specified otherwise. 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 that are described in the appended claims in detail and that are consistent with some aspects of the present disclosure.

[0065] 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 complete a payment transaction. NFC, also referred to as short-distance communication, is a short distance high-frequency wireless 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 in fields such as payment.

[0066] P2P, namely, peer to peer, is one of three working modes of the NFC technology. Similar to infrared, the P2P mode can be used to exchange data. However, in the P2P mode, the transmission distance is shorter and both the transmission creation speed and the transmission speed are faster, and power consumption is lower than the infrared mode (similar to Bluetooth). Two devices with an NFC function can be wirelessly linked to each other to implement peer-to-peer data transmission; for example, music download, picture exchange, or device address book synchronization. Therefore, through NFC, data or a service can be exchanged among a plurality of devices such as a digital camera, a PDA, a computer, and a mobile phone. In the implementations of the present disclosure, the mobile terminal exchanges data with a bus gate in the P2P way of the NFC technology, to complete a credit payment transaction.

[0067] 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 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.

[0068] 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 serving 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 funds from an account that corresponds to the mobile terminal 100, and pays the amount to the bus company.

[0069] In this implementation provided in the present disclosure, two applications can be installed on the mobile terminal. One is a credit payment application, for example, a credit payment application applet. For a Java card, Sun Microsystems Inc. sets Applet as the object for running on the Java card. 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.

[0070] The transaction terminal 200 uses a strict identity security authentication mechanism, to ensure that only a user who passes identity security authentication and has an enough credit limit can enable a bus credit payment application.

[0071] The credit payment application applet is installed on the mobile terminal 100 with an NFC function. An application private-public key pair is generated during personalization. An application private key is stored in the credit payment application, and the credit payment application ensures that data of the application private key cannot be stolen in any condition. 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 in the credit payment application. 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. Since it is a public key, no

requirement is imposed on security.

[0072] 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 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 be connected to a network to verify user identity information, and grant authorization again.

[0073] To resolve a related technical problem, an implementation of the present disclosure provides a credit payment method based on mobile terminal P2P, applied to a process that enables credit payment by a mobile terminal. As shown in FIG. 2, the method can include the following steps.

[0074] In step S110, send an application authorization request to a predetermined server by using a credit authorization system application on the mobile terminal.

[0075] The credit authorization system application is installed on the mobile terminal, and the mobile terminal can send the application authorization request to a server of a credit authorization system by using the authorization system application.

[0076] In step S120, receive an application public key certificate and an application private key that are sent by the predetermined server.

[0077] Based on the received application authorization request, the server of the credit authorization system generates a pair of keys, that is, the application public key and the application private key. The server signs the application public key by using an authorized private key locally stored on the sever, to generate an application public key certificate, and sends the obtained application public key certificate and the application private key to the mobile terminal.

[0078] In step S130, store the application public key certificate and the

application private key in a credit payment application on the mobile terminal.

[0079] The mobile terminal stores, in the credit payment application on the mobile terminal, the application public key certificate and the application private key that are sent by the serving end.

[0080] In step S140, a credit payment data acquisition request is sent to the predetermined server.

[0081] In step S150, credit payment data sent by the predetermined server is received, and a credit payment function of the mobile terminal is enabled based on the credit payment data.

[0082] Credit payment data can be a personalization script, and the personalization 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 fund that the user can use currently. The TAC sub-key is obtained by the server in the credit authorization system based on the card number hash by using a TAC parent private key.

[0083] In another implementation provided in the present disclosure, based on FIG. 2, as shown in FIG. 3, before step S110, the method can further include the following steps.

[0084] In step S101, obtain device parameter information of the mobile terminal.

[0085] The device parameter information of the mobile terminal can be hardware information of the mobile terminal. It needs to be checked first, based on the device parameter information, whether the mobile terminal satisfies a hardware condition of a payment transaction, for example, whether the mobile terminal has an NFC function. Certainly, the device parameter information can also be information such as device model, a ROM version, a system model (such as, Android), an application version, etc. of the mobile terminal.

[0086] In step S102, send the device parameter information to the predetermined server.

[0087] The mobile terminal sends the obtained device parameter information of the mobile terminal to the server of the credit authorization system, so that the server determines, based on the received device parameter information, whether the mobile terminal meet a hardware condition for enabling credit payment.

[0088] In step S103, check whether credit payment enabling information sent by

the predetermined server is received.

[0089] If 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.

[0090] If 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.

[0091] When the credit payment enabling information sent by the predetermined server is received, step S104 is performed.

[0092] In step S104, determine that the mobile terminal meets the hardware condition for enabling credit payment, and step S110 is performed.

[0093] In addition to checking whether the mobile terminal meets the hardware condition for enabling credit payment, based on FIG. 2, before step S110, as shown in FIG. 4, whether the mobile terminal meets a security authentication condition further needs to be checked. Therefore, in another implementation provided in the present disclosure, the credit payment method based on mobile terminal P2P provided in the present disclosure can further include the following steps.

[0094] In step S105, obtain user identity information that corresponds to the mobile terminal.

[0095] The user identity information can be information such as an ID card number, a name, a bank card number, an email address, an Alipay account, etc. of the user.

[0096] In step S106, 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.

[0097] 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 service normally, or whether a user account has a bad-credit transaction record.

[0098] In step S107, check whether security authentication success information sent by the predetermined server is received.

[0099] After receiving the user information sent by the mobile terminal, the server

checks the user information. If the mobile terminal meets the security authentication condition for enabling credit payment, the server sends the security authentication success information to the mobile terminal.

[0100] When the security authentication success information sent by the predetermined server is received, step S108 is performed. In step S108, determine that the mobile terminal meets the security authentication condition for enabling credit payment, and step S110 is performed.

[0101] 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.

[0102] When the mobile terminal does not receive 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.

[0103] Based on FIG. 2, before step S110, as shown in FIG. 5, a related application further needs to be installed on the mobile terminal. Therefore, the credit payment method based on a mobile terminal P2P provided in the present disclosure further includes the following steps.

[0104] In step S160, send a request for obtaining predetermined installation files to the predetermined server.

[0105] The predetermined installation files includes a credit payment application.

[0106] In step S170, obtain the predetermined installation files sent by the predetermined server.

[0107] In step S180, install the predetermined installation files on the mobile terminal, step S110 is performed.

[0108] After the credit payment application and a registration script are separately installed on the mobile terminal, user personalization of the mobile terminal is completed. As such, the procedure of enabling the credit payment function on a mobile terminal is completed. 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.

[0109] In another implementation provided in the present disclosure, as shown in FIG. 6, an execution procedure of a server (a serving end of a credit authorization

system) in the credit payment method based on mobile terminal P2P provided in the present disclosure can include the following steps.

[0110] In step S210, receive an application authorization request sent by a mobile terminal is received.

[0111] In step S220, separately generate an application public key and an application private key based on the application authorization request.

[0112] In step S230, sign the application public key by using a locally stored authorization private key, to generate an application public key certificate.

[0113] In step S240, separately send the application public key certificate and the application private key to the mobile terminal.

[0114] Based on the received application authorization request, the server of the credit authorization system generates a pair of keys, that is, the application public key and the application private key. The server signs the application public key by using the locally stored authorization private key, to generate the application public key certificate, and separately sends the obtained application public key certificate and the application private key to the mobile terminal.

[0115] In step S250, receive a credit payment data acquisition request sent by the mobile terminal.

[0116] In step S260, generate credit payment data that corresponds to the mobile terminal based on the credit payment data acquisition 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.

[0117] Credit payment data can be a personalization script, and the personalization 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 fund 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.

[0118] Based on FIG. 6, as shown in FIG. 7, in another implementation provided in the present disclosure, the server (the serving 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 S210, the credit payment method based on mobile terminal P2P

provided in the implementation of the present disclosure can further include the following steps.

[0119] In step S201, receive device parameter information sent by the mobile terminal.

[0120] In a process in which the mobile terminal enables the credit payment function, the mobile terminal can communicate with the serving end (namely, the server) of the credit authorization system by using a network, etc. The serving end of the credit authorization system can receive the device parameter information sent by the mobile terminal.

[0121] In step S202 determine, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

[0122] The parameter information sent by the mobile terminal can be information such as a device model, a ROM version, a system version (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 NFC function, etc.

[0123] If the server checks 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 of the mobile terminal, and upload the user identity information to the serving end.

[0124] If the server detects that the mobile terminal does not meet the hardware condition for enabling credit payment, the server does not send credit payment enabling information to the mobile terminal.

[0125] When the mobile terminal meets the hardware condition for enabling credit payment, in step S203, send the credit payment enabling information to the mobile terminal, and step S210 is performed.

[0126] In addition to checking 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 that corresponds to the mobile terminal meets a security authentication condition. Therefore, based on FIG. 6, as shown in FIG. 8, in a process of enabling the credit

payment function of the mobile terminal, before step S210, the credit payment method based on mobile terminal P2P provided in the present disclosure can further include the following steps.

[0127] In step S204, receive user identity information sent by the mobile terminal.

[0128] The user identity information can be information such as an ID card number, a name, a bank card number, an email address, an Alipay account, etc. of the user.

[0129] In step S205, determine, based on the user identity information, whether the mobile terminal meets a security authentication condition for enabling credit payment.

[0130] For example, the server can check whether the bank card number in the user identity information provides a service normally, whether is a bad transaction record.

[0131] 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.

[0132] When the mobile terminal meets the security authentication condition for enabling credit payment, in step S206, send the security authentication success information to the mobile terminal, and step S210 is performed.

[0133] When the mobile terminal enables credit payment, a credit payment application further needs to be installed, and these installation files need to be sent to the mobile terminal by the server in a credit authorization system. Therefore, based on FIG. 6, as shown in FIG. 9, in another implementation of the present disclosure, before step S210, the credit payment method based on mobile terminal P2P provided in the present disclosure can further include the following steps.

[0134] In step S207, receive a request sent by the mobile terminal for obtaining predetermined installation files.

[0135] The predetermined installation files include the credit payment application.

[0136] In step S208, separately send the predetermined installation files to the mobile terminal based on the request for obtaining the predetermined installation files, and step S210 is performed.

[0137] The previous implementations of the present disclosure describe the process of enabling credit payment in the mobile terminal. In some scenarios, the

credit payment enabling process can be obtained in other ways, for example, is predetermined on the mobile terminal, or is obtained through a registration application to a credit payment authority. The credit payment enabling process is not limited here.

[0138] To resolve the problem in related technologies, an implementation of the present disclosure provides a credit payment method based on mobile terminal P2P, applied to a credit payment process between a mobile terminal and a transaction terminal. As shown in FIG. 10, the method can include the following steps.

[0139] In step S310, receive transaction information sent by the transaction terminal.

[0140] When a user holds the 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, that is, when the mobile terminal enters the radio frequency field generated by the bus gate, the mobile terminal can detect the radio frequency field generated by the bus gate, and the bus gate also detects the mobile terminal. In this situation, a communication connection is established between the bus gate and the mobile terminal, the bus gate sends the transaction information to the mobile terminal, and the mobile terminal receives the transaction information sent by the bus gate.

[0141] It is worthwhile to note that how to exchange an NFC data exchange format (NDEF) message is described in a P2P mode.

[0142] In step S320, generate transaction response information based on the transaction information, and send the transaction response information to the transaction terminal.

[0143] In step S330, receive deduction accept request information of the current payment transaction that is sent by the transaction terminal.

[0144] After receiving an application public key certificate sent by the mobile terminal, the bus gate performs verification of 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.

[0145] In step S340, generate an application-private-key-generated payment license in the mobile terminal based on the deduction accept request information and the transaction response information.

[0146] The payment license generated by the mobile terminal includes signature

data and a transaction authentication code (TAC).

[0147] In step S350, send the payment license to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment license.

[0148] After receiving the payment license sent by the mobile terminal, the bus gate verifies the payment license. If the license is verified. It is determined that the current payment transaction is completed.

[0149] After sensing the mobile terminal, the bus gate can ensemble an SNEP get request message and send the SNEP get request message to a bus credit payment application. The information field identifier message of the message is read card information. After receiving the SNEP get request message, the bus credit payment application assembles, into an SNEP response message, data that needs to be returned, and the SNEP response message includes a card number, an available limit, an entry/exit flag, and information about a last transaction; and returns the SNEP response message to the gate. The information about the last transaction includes station information, a transaction date, a transaction time, etc.

[0150] It is worthwhile to note that an SNEP request message is a request message sent by an SNEP client to an SNEP server in P2P. There are two types of SNEP request messages: a get message and a put message. The get message requests the server to return data, and the put message requests the server to accept data. An SNEP get request message and an SNEP put request message are distinguished in the specification. The SNEP response message is a response message returned by the SNEP server to the SNEP client in P2P. The get message requests to return data, and the put message requests to return response code indicating a success or a failure.

[0151] Return request information is equivalent to the SNEP get request message, and the transaction response information is equivalent to the SNEP response message.

[0152] In the method provided in this 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 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 provided in this 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 consumption 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.

[0153] As a refinement of the method in FIG. 10, in another implementation of the present disclosure, as shown in FIG. 11, after step S320, the method can further include the following steps.

[0154] In step S360, receive application public key certificate return request information sent by the transaction terminal.

[0155] In step S370, generate application public key certificate response information for the application public key certificate on the mobile terminal based on the application public key certificate return request information, and send the application public key certificate response information to the transaction terminal.

[0156] The application public key certificate response information corresponds to the application public key certificate return request information and meets a data transmitting and receiving format requirement.

[0157] 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. 10, in another implementation of the present disclosure, as shown in FIG. 12, step S340 can further include the following steps.

[0158] In step S361, generate signature data based on the deduction accept request information by using an application private key stored in the mobile terminal.

[0159] The application private key is pre-generated and stored on 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 deduct amount, a date and time of the current payment transaction, an entry/exit flag on the current payment transaction sign, and station information of the current payment transaction.

[0160] In step S362, generate a TAC based on the deduction accept request information and the transaction response information by using a TAC sub-key that is pre-generated on the mobile terminal.

[0161] The deduction accept request information includes the deduction information, and the transaction response information includes the transaction information. 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 the maximum available amount authorized by a credit authorization system to the user in an offline mode.

[0162] In step S363, use the signature data and the TAC as the payment authorization license.

[0163] 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.

[0164] In addition, the transaction response information includes the payment card number, the available limit, the entry/exit flag, and the information about the last transaction. The payment card number is a unique character code generated by the credit authorization system for each user's a credit payment application. The available limit is an amount of fund 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. The information about the last transaction includes the station information, the transaction date, the transaction time, etc.

[0165] Based on FIG. 10, as shown in FIG. 13, in another implementation of the present disclosure, the method can further include the following steps.

[0166] In step S380, subtract the deduction amount from the available limit in the transaction response information based on the deduction amount in the deduction accept request information, to obtain a current available limit.

[0167] In step S390, use the current available limit as an available limit that corresponds to a user on the mobile terminal.

[0168] To describe a transaction payment process between the mobile terminal and transaction terminal in detail, an implementation of the present disclosure provides a credit payment method based on mobile terminal P2P. In an execution procedure on a transaction terminal side, as shown in FIG. 14, the method can include the following steps.

[0169] In step S410, send transaction information to the mobile terminal.

[0170] In step S420, receive transaction response information sent by the mobile terminal.

[0171] In step S430, generate deduction accept request information of the current payment transaction based on the transaction response information.

[0172] In step S440, send the deduction accept request information to the mobile terminal.

[0173] In step S450, when a payment license is received, determine, based on the payment license, that the current payment transaction can be completed.

[0174] Because the method shows the execution procedure on a bus gate side in the credit payment transaction process, which corresponds to the execution procedure on the mobile terminal side in the credit payment transaction process, data exchange between the bus gate and the mobile terminal is not described here again. For details, refer to the execution procedure on the mobile terminal side in the previous implementation.

[0175] It is worthwhile to note that the transaction information, the transaction response information, the public key certificate return request information, the public key certificate response information, etc. in the implementations are used to meet a format requirement in a data exchange process. For example, the transaction response information can be understood as response information including the transaction information, and the public key certificate response information can be understood as response information including a public key certificate.

[0176] In addition, the transaction response information includes a payment card number, an available limit, an entry/exit flag, and information about a last transaction.

[0177] Based on FIG. 14, as shown in FIG. 15, in another implementation provided in the present disclosure, after step S420, the method can further include the following steps.

[0178] In step S460, send application public key certificate return request information to the mobile terminal.

[0179] In step S470, receive application public key certificate response information sent by the mobile terminal

[0180] In step S480, verify a signature on an application public key certificate in the application public key certificate response information by using a credit-licensed public key in the transaction terminal.

[0181] Because the method shows the execution procedure on a bus gate side in the credit payment transaction process, which corresponds to the execution procedure on the mobile terminal side in the credit payment transaction process, data exchange between the bus gate and the mobile terminal is not described here again. For details, refer to the execution procedure on the mobile terminal side in the previous implementation.

[0182] Based on FIG. 14, as shown in FIG. 16, in another implementation provided in the present disclosure, the method can further include the following steps.

[0183] In step S401, determine whether the payment card number in the transaction response information is included in a predetermined blacklist.

[0184] When the payment card number in the transaction response information is not included in the predetermined blacklist, step S460 is performed.

[0185] The blacklist can be predetermined in the transaction terminal, namely, the bus gate. User identity information that corresponds to the mobile terminal is compared with information in the blacklist. If the user identity information exists in the blacklist, this transaction payment procedure is stopped to avoid a malicious transaction.

[0186] Based on FIG. 14, as shown in FIG. 17, in another implementation provided in the present disclosure, the method can further include the following steps.

[0187] In step S402, determine whether the available limit in the transaction response information is greater than or equal to a predetermined threshold.

[0188] If the available limit is greater than or equal to the predetermined threshold, in step S403, check whether the entry/exit flag in the transaction response information is an exited state.

[0189] If the entrance/exit flag in the transaction information is an exited state, step S460 is performed.

[0190] The available limit of a user is checked, to determine whether the credit payment transaction needs to be continued. When the available limit of the user is less than a deduction amount of this transaction, this credit payment transaction is stopped, so that a malicious payment transaction can be avoided.

[0191] The present step is mainly used by the bus gate to check, based on the transaction response information sent by the mobile terminal, whether an available limit of a user account that corresponds 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 entry/exit flag in the transaction response information is 0. If the entry/exit flag is not 0, the current payment transaction is rejected. If the entry/exit flag is 0, the current payment transaction is continued. It is worthwhile to note that, when an entry/exit flag 1, it indicates that the user who holds the mobile terminal is in an "entered" state, and therefore the current payment transaction is rejected. When the entry/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.

[0192] Based on FIG. 14, as shown in FIG. 18, in another implementation provided in the present disclosure, step S450 can include the following steps.

[0193] In step S481, verify the signature data by using an application public key.

[0194] 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 yes, the signature verification passes.

[0195] In step S482, generate a transaction log when the signature data is verified.

[0196] 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.

[0197] In step S483, send the transaction log to a predetermined server, so that the predetermined server deducts a corresponding amount of fund from a user account that corresponds to the mobile terminal based on the transaction log.

[0198] 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. The payment license includes signature data and a TAC.

[0199] In another implementation provided in the present disclosure, as shown in FIG. 19, the present disclosure provides a credit payment method based on mobile terminal P2P. In this implementation, a mobile phone represents a mobile terminal, and a serving end of a credit authorization system represents a server. When the mobile phone enables a credit payment function, a procedure among a credit authorization system application on the mobile phone, a credit payment application on the mobile phone, and the serving end of the credit authorization system includes the following steps:

[0200] Step 1001: Obtain device parameter information of the mobile phone.

[0201] Step 1002: Upload the device parameter information.

[0202] Step 1003: Determine whether the mobile phone meets a hardware condition for enabling credit payment.

[0203] Step 1004: Return a determining result.

[0204] Step 1005: The determining result is: displaying a credit payment application enabling page.

[0205] Step 1006: Upload user identity information.

[0206] Step 1007: Determine whether the mobile phone satisfies a security authentication condition for enabling credit payment.

[0207] Step 1008: Return a determining result.

[0208] Step 1009: A user chooses to enable the credit payment application.

[0209] Step 1010: Activate the credit payment application.

[0210] Step 1011: Return an activation success result.

[0211] Step 1012: Request an application private key, an application public key certificate, and credit payment data.

[0212] Step 1013: Generate a private-public key pair, generate the application public key certificate by using a credit-authorized private key, generate a payment card number, and generate an application TAC sub-key and the credit payment data through hashing.

[0213] Step 1014: Return the application private key, the application public key certificate, and the credit payment data.

[0214] Step 1015: Send the application private key, the application public key

certificate, and the credit payment data.

[0215] Step 1016: Store the application private key, the application public key certificate, and the credit payment data.

[0216] Step 1017: Return a personalization result.

[0217] Step 1018: Send a credit payment enabling result.

[0218] Step 1019: Record the enabling result.

[0219] Step 1020: Return a processing complete notification.

[0220] Step 1021: Provide, to the user, a prompt indicating that the credit payment application is successfully enabled.

[0221] In another implementation provided in the present disclosure, as shown in FIG. 20, the present disclosure provides a credit payment method based on mobile terminal P2P. In a process in which a mobile terminal performs payment transaction, a data exchange procedure between the mobile terminal and a bus gate is as follows:

[0222] Step 2001: Send an SNEP-Request (Get [read card information]).

[0223] Step 2002: Read data that needs to be returned.

[0224] Step 2003: Return an SNEP-Response (return a payment card number, an available limit, an entry/exit flag, and information about a last transaction).

[0225] Step 2004: Perform blacklist determining; and if the payment card number exists in the blacklist, provide a prompt of rejection information.

[0226] Step 2005: Check the available limit and the entry/exit flag; and if the available limit or the entry/exit flag does not meet a predetermined condition, provide a prompt of rejection information.

[0227] Step 2006: Send an SNEP-Request (Get[read an application public key certificate]).

[0228] Step 2007: Return an SNEP-Response (the application public key certificate).

[0229] Step 2008: Read a stored public key in a credit authorization system, and verify a signature on the application public key certificate. If the signature verification fails, provide a prompt of rejection information. If the signature verification passes, obtain an application public key through parsing.

[0230] Step 2009: Calculate a deduction amount.

[0231] Step 2010: Send an SNEP-Request (Put (payment: the deduction amount, a transaction time, the entry/exit flag, and transaction information (such as a stop))).

[0232] Step 2011: Generate a payment authorization, including signature data and

TAC.

[0233] Step 2012: Return the signature data and the TAC.

[0234] Step 2013: Verify the signature data by using the application public key. If the signature verification passes, record a transaction log. If the signature verification fails, provide a prompt of rejection information.

[0235] In addition, as shown in FIG. 21, a bus gate further needs to periodically upload a transaction log to a credit authorization system, and update a blacklist. In a credit payment method based on mobile terminal P2P provided in the present disclosure, a data exchange procedure between the bus gate (a transaction terminal) and a server end of the credit authorization system is as follows:

[0236] Step 3001: Periodically upload a transaction log.

[0237] Step 3002: Perform settlement, query whether a blacklist in the system is updated, and if yes, prepare to return a blacklist.

[0238] Step 3003: Return a transaction log receiving result and the blacklist.

[0239] Step 3004: Check whether a payment card number exists in the blacklist.

[0240] Step 3005: The bus gate updates the blacklist.

[0241] Step 3006: Update.

[0242] Step 3007: Return an updated completion result.

[0243] A bus gate management system can be located in the bus gate.

[0244] The previous implementations of the present disclosure are described by using credit payment for a bus as an example. It can be understood that the previous implementations can also be applied to other scenarios, such as offline business payment and subway payment. There can be different implementations in specific application scenarios.

[0245] 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 be implemented by hardware, but in many situations, the former is a preferred 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 of the steps of the methods described in the implementations of the present disclosure. The storage medium includes any medium that can store program code, such as a read-only memory (ROM), a random access memory (RAM), a magnetic disk, or an optical disc.

[0246] In addition, as an implementation of the previous implementations, an implementation of the present disclosure further provides a credit payment apparatus based on mobile terminal P2P. The apparatus is located in a mobile terminal. As shown in FIG. 22, the apparatus includes a first return request information receiving unit 10, a transaction response information generation unit 20, an information sending unit 30, a deduction accept request information receiving unit 40, an application-private-key-generated payment authorization generation unit 50, and a payment authorization sending unit 60.

[0247] The first return request information receiving unit 10 is configured to receive transaction information sent by a transaction terminal.

[0248] The transaction response information generation unit 20 is configured to generate transaction response information based on the transaction information.

[0249] The information sending unit 30 is configured to send the transaction response information to the transaction terminal.

[0250] The deduction accept request information receiving unit 40 is configured to receive deduction accept request information of the current deduction transaction that is sent by the transaction terminal.

[0251] The application-private-key-generated payment authorization generation unit 50 is configured to generate an application-private-key-generated payment authorization in the mobile terminal based on the deduction accept request information and the transaction response information.

[0252] The payment authorization sending unit 60 is configured to send the payment authorization to the transaction terminal, so that the transaction terminal completes the current payment transaction based on the received payment authorization.

[0253] In another implementation of the present disclosure, based on FIG. 22, as

shown in FIG. 23, the apparatus further includes: a second return request information receiving unit 70, configured to receive application public key certificate return request information sent by the transaction terminal; an application public key certificate response information generation unit 80, configured to generate application public key certificate response information for an application public key certificate in the mobile terminal based on the application public key certificate return request information; and a public key certificate response information sending unit 90, configured to send the application public key certificate response information to the transaction terminal.

[0254] In another implementation of the present disclosure, based on FIG. 22, as shown in FIG. 24, the application-private-key-generated payment authorization generation unit 50 includes: a signature data generation module 51, configured to generate signature data based on the deduction accept request information by using an application private key stored in the mobile terminal; an information generation module 52, configured to generate transaction authentication code (TAC) based on the deduction accept request information and the transaction response information by using a TAC sub-key that is pre-generated on the mobile terminal; and a payment authorization determining module 53, configured to use the signature data and the TAC as the payment authorization.

[0255] In another implementation of the present disclosure, based on FIG. 22, as shown in FIG. 25, the apparatus further includes: a current available limit generation unit 91, configured to subtract the deduction amount from the available limit in the transaction information based on the deduction amount in the deduction accept request information, to obtain a current available limit; and an available limit determining unit 92, configured to use the current available limit as an available limit that corresponds to a user in the mobile terminal.

[0256] An implementation of the present disclosure further provides a credit payment apparatus based on mobile terminal P2P. The apparatus is located in a transaction terminal. As shown in FIG. 26, the apparatus includes a transaction information sending unit 11, a transaction response information receiving unit 12, a deduction unit 13, a deduction accept request information sending unit 14, and a

current-payment-transaction complete unit 15.

[0257] The transaction information sending unit 11 is configured to send transaction information to a mobile terminal.

[0258] The transaction response information receiving unit 12 is configured to receive transaction response information sent by the mobile terminal.

[0259] The deduction unit 13 is configured to generate deduction accept request information of the current payment transaction deduction based on the transaction response information.

[0260] The deduction accept request information sending unit 14 is configured to send the deduction accept request information to the mobile terminal.

[0261] The payment transaction completion unit 15 is configured to: when a payment authorization license is received, determine, based on the payment authorization license, that the current payment transaction is completed.

[0262] In another implementation of the present disclosure, based on FIG. 26, as shown in FIG. 27, the apparatus further includes: a return request information sending unit 16, configured to send application public key certificate return request information to the mobile terminal; a public key certificate response information receiving unit 17, configured to receive application public key certificate response information sent by the mobile terminal; and a signature verification unit 18, configured to verify a signature on an application public key certificate in the application public key certificate response information by using a credit-licensed public key in the transaction terminal.

[0263] In another implementation of the present disclosure, based on FIG. 26, as shown in FIG. 28, the apparatus further includes a blacklist determining unit 191.

[0264] The blacklist determining unit 191 is configured to determine whether the payment card number in the transaction response information is included in a predetermined blacklist.

[0265] The return request information sending unit 192 is further configured to: when the payment card number in the transaction response information is not included in the predetermined blacklist, send the application public key certificate return request information to the mobile terminal.

[0266] In another implementation of the present disclosure, based on FIG. 21, as shown in FIG. 29, the apparatus further includes: a threshold determining unit 193,

configured to determine whether the available limit in the transaction response information is greater than or equal to a predetermined threshold; and a status checking unit 194, configured to: if the available limit is greater than or equal to the predetermined threshold, check whether the entry/exit flag in the transaction response information is an exited state.

[0267] In still another implementation of the present disclosure, based on FIG. 26, as shown in FIG. 30, the payment authorization license includes signature data and transaction authentication code (TAC), and the current payment transaction completion unit 15 includes: a signature verification module 151, configured to verify signature data using the application public key; a transaction log generation module 152, configured to generate a transaction log when the signature data is verified; and a transaction log sending module 153, configured to send the transaction log to a predetermined server, so that the predetermined server deducts, based on the transaction log, a corresponding amount of fund from a user account that corresponds to the mobile terminal, where the transaction log includes the deduction amount, a transaction date, a transaction moment, a transaction terminal ID, a payment card number, an available limit, and the TAC.

[0268] With regard to the apparatus implementations, the specific manner each module operates has been described in detail in corresponding method implementations, and details are not repeated here for simplicity.

[0269] It can be understood that the present disclosure can be applied to many general-purpose or special purpose computer system environments or configurations. For example, a personal computer, a server computer, a handheld device or a portable device, a flat panel device, a multi-processor system, a microprocessor-based system, a set-top box, a programmable consumption electronic device, a network PC, a minicomputer, a mainframe computer, and a distributed computing environment including any one of the previous systems or devices.

[0270] The present disclosure can be described in the general context of instructions 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.

[0271] It is worthwhile to note that in the specification, relational terms such as "first" and "second" are only used to distinguish one entity or operation from another, and do not necessarily require or imply that any actual relationship or sequence exists between these entities or operations. In addition, the terms "include", "comprise", or their any other variant is intended to cover a non-exclusive inclusion, so that a process, a method, an article, 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 process, method, article, or device. An element described by "includes a…" further includes, without more constraints, another identical element in the process, method, article, or device that includes the element.

[0272] A person skilled in the art can easily figure out other implementation solutions of the present disclosure after considering the specification and practicing the present disclosure that is disclosed here. The present application is intended to cover any variation, function, or adaptive change 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 following claims.

[0273] 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 processing credit payment, the method comprising:

receiving a transaction information sent by a transaction terminal (S310);

generating a transaction response information based on the transaction information;

sending the transaction response information to the transaction terminal (S320);

in response to sending, to the transaction terminal, the transaction response information that corresponds to the transaction information, receiving application public key certificate return request information sent by the transaction terminal (S360);

generating application public key certificate response information for an application public key certificate in the mobile terminal based on the application public key certificate return request information, and sending the application public key certificate response information to the transaction terminal (S370);

receiving deduction accept request information of the current payment transaction that is sent by the transaction terminal (S330);

generating an application-private-key-generated payment authorization license in a mobile terminal based on the deduction accept request information and the transaction response information (S340); and

sending the payment authorization license to the transaction terminal, the transaction terminal being configured to complete the current payment transaction based on the received payment license (S350).

2. The method according to claim 1, wherein generating the application-private-key-generated payment license in the mobile terminal comprises:

generating signature data based on the deduction accept request information by using an application private key stored in the mobile terminal (S361);

generating transaction authentication code (TAC) based on the deduction accept request information and the transaction response information by using a TAC sub-key pre-generated in the mobile terminal (S362); and

using the signature data and the TAC as the payment authorization license (S363).

3. The method according to any one of claims 1 to 2, wherein the payment method is applied to payment for public transportation; and

the transaction response information comprises at least one of a payment card number, an available limit, and an entry flag or an exit flag.

4. The method according to any one of claims 1 to 3, wherein the deduction accept request information comprises at least one of a deduction amount, a date of the current payment transaction, a time of the current payment transaction, an entry flag or an exit flag of the current payment transaction, and station information of the current payment transaction.

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

subtracting the deduction amount from the available limit in the transaction response information based on the deduction amount in the current deduction accept request information, to obtain a current available limit (S380); and

using the current available limit as an available limit of a user that corresponds to the mobile terminal (S390).

6. A method for processing credit payment, the method comprising:

sending transaction information to a mobile terminal (S410);

receiving transaction response information sent by the mobile terminal (S420);

sending application public key certificate return request information to the mobile terminal (S460);

receiving application public key certificate response information sent by the mobile terminal (S470);

verifying a signature on an application public key certificate in the application public key certificate response information by using a credit authorization public key on the transaction terminal (S480);

in response to determining that an application public key is restored from the application public key certificate during verification, generating deduction accept request information of the current payment transaction based on the transaction response information (S430);

sending the deduction accept request information to the mobile terminal (S440); and

in response to receiving a payment authorization license, determining, based on the payment authorization license, that the current payment transaction is completed (S450).

7. The method according to claim 6, wherein the payment method is applied to public transportation payment; and

the transaction response information comprises a payment card number, an available limit, and an entry flag or an exit flag.

8. The method according to claim 7, wherein the method further comprises:

determining whether the payment card number in the transaction response information is comprised in a predetermined blacklist (S401); and

in response to determining that the payment card number in the transaction response information is not comprised in the predetermined blacklist, performing the step of sending application public key certificate return request information to the mobile terminal.

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

determining whether the available limit in the transaction response information is greater than or equal to a predetermined threshold (S402);

if the available limit is greater than or equal to the predetermined threshold, checking whether the entry flag or an exit flag in the transaction response information is an exited state (S403); and

if the entry flag or an exit flag is an exited state, performing the step of sending application public key certificate return request information to the mobile terminal (S460).

10. The method according to any one of claims 6 to 9, wherein the payment authorization license comprises signature data and transaction authentication code (TAC), and the determining, based on the payment license, that the current payment transaction can be completed comprises:

verifying the signature data by using the application public key (S481);

generating a transaction log in response to determining that the signature data is verified (S482); and

sending the transaction log to a predetermined server, so that the predetermined server

deducts, based on the transaction log, a corresponding amount of fund from a user account that corresponds to the mobile terminal, wherein the transaction log comprises the deduction amount, a transaction date, a transaction moment, a transaction terminal ID, a payment card number, an available limit, and the TAC (S483).

11. The method according to any one of claims 6 to 10, further comprising obtaining a user identity information that corresponds to the mobile terminal, the user identity comprising at least one of an identity card number, a name, a bank card number, and an email address (S105).

12. The method according to any one of claims 1 to 10, wherein the transaction terminal communicates with the mobile terminal using a peer to peer data transmission.

13. An apparatus for processing credit payment, applied to a mobile terminal, the apparatus comprising a plurality of modules configured to perform the method according to any one of claims 1 to 12.