CREDIT PAYMENT METHOD AND APPARATUS BASED ON CARD EMULATION OF MOBILE TERMINAL

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 card emulation of a mobile terminal.

BACKGROUND

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

[0003] When a user purchases a bus ticket in cash, because many buses are self-service ticketing and provide no exchange, the user needs to prepare the exact amount of fares in advance, which can be inconvenient to the user. In addition, 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 public transportation, because most current public transportation cards are usually non-contact radio frequency (RF) card, user-caused damages and wear, such as bending the card, or abrasion of the card's surface are easily made to the metro card during its normal use. When using a single-ride public transportation card, the user usually buys the single-ride public transportation card in small fares, and the staff also needs to count all the small fares.

[0004] When a user uses a reusable pre-paid card to take public transportation, because the prepaid card is not registered, its loss cannot be reported, and a great loss is caused to the user after 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 overcome problems in the existing technologies, the present disclosure provides a credit payment method and device based on card emulation of a mobile terminal.

[0006] According to a first aspect of the implementations of the present disclosure, a credit payment method based on card emulation of a mobile terminal is provided, including: sending an application authorization request to a predetermined server; receiving an application public key certificate and an application private key sent by the predetermined server; storing the application public key certificate and the application private key in a credit payment application of the mobile terminal; sending a credit payment data acquisition 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.

[0007] 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; detecting whether credit payment enablement information sent by the predetermined server is received; and when the credit payment enablement information sent by the predetermined server is received, determining that the mobile terminal meets the hardware condition for enabling credit payment, and executing the step of sending an application authorization request to a predetermined server.

[0008] 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 certification condition for enabling credit payment; detecting whether security certification success information sent by the predetermined server is received; and when the security certification success information sent by the predetermined server is received, determining that the mobile terminal meets the security certification condition for enabling credit payment, and executing the step of sending an application authorization request to a predetermined server.

[0009] 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 installation file; obtaining the predetermined installation file sent by the predetermined server; and installing the predetermined installation file on the mobile terminal, and executing the step of sending an application authorization request to a predetermined server.

[0010] Further, the credit payment data includes a payment card number, a credit limit, an available credit, and a transaction authentication code (TAC) sub-key.

[0011] According to a second aspect of the implementations of the present disclosure, a credit payment method based on card emulation of a mobile terminal is provided, including: receiving an application authorization request sent by a mobile terminal; separately generating an application public key and an application private key based on the application authorization request; signing the application public key by using a credit authorization private key stored on a predetermined server, to generate an application public key certificate; sending the application public key certificate and the application private key to the mobile terminal; receiving a credit payment data acquisition request sent by the mobile terminal; and generating credit payment data corresponding to the mobile terminal based on the credit payment data acquisition 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.

[0012] The method further includes: receiving device parameter information sent by the mobile terminal; determining, based on the apparatus 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 enablement information to the mobile terminal, and executing the step of receiving an application authorization request sent by a mobile terminal.

[0013] 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 certification condition for enabling credit payment; and when the mobile terminal meets the security certification condition for enabling credit payment, sending security certification success information to the mobile terminal, and executing the step of receiving an application authorization request sent by a mobile terminal.

[0014] The method further includes: receiving a request for obtaining a

predetermined installation file sent by the mobile terminal, where the predetermined installation file includes a credit payment installation file; and sending the predetermined installation file to the mobile terminal based on the request for obtaining a predetermined installation file, and executing the step of receiving an application authorization request sent by a mobile terminal.

[0015] According to a third aspect of the implementations of the present disclosure, a credit payment device based on card emulation of a mobile terminal is provided, including: an application authorization request sending unit, configured to send an application authorization request to a predetermined server by using a credit authorization system application on a mobile terminal; a key receiving unit, configured to receive an application public key certificate and an application private key sent by the predetermined server; a key storage unit, configured to store the application public key certificate and the application private key in a credit payment application of the mobile terminal; a credit payment data acquisition request sending unit, configured to send a credit payment data acquisition request to the predetermined server; a credit payment data receiving unit, configured to receive credit payment data sent by the predetermined server; and a credit payment completion unit, configured to enable a credit payment function of the mobile terminal based on the credit payment data.

[0016] The device 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 first detection unit, configured to detect whether credit payment enablement information sent by the predetermined server is received; and a hardware condition determining unit, configured to: when the credit payment enablement information sent by the predetermined server is received, determine that the mobile terminal meets the hardware condition for enabling credit payment.

[0017] The device 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 certification condition for enabling credit payment; a second detection unit, configured to detect whether security certification success information sent by the predetermined server is received; and a security certification condition determining unit, configured to: when the security certification success information sent by the predetermined server is received, determine that the mobile terminal meets the security certification condition for enabling credit payment.

[0018] The device further includes: a predetermined installation file acquisition 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 installation file; a predetermined installation file acquisition unit, configured to obtain the predetermined installation file sent by the predetermined server; and an installation unit, configured to install the predetermined installation file on the mobile terminal.

[0019] Further, the credit payment data includes a payment card number, a credit limit, an available credit, and a TAC sub-key.

[0020] According to a fourth aspect of the implementations of the present disclosure, a credit payment device based on card emulation of a mobile terminal is provided, including: an application authorization request receiving unit, configured to receive an application authorization request sent by a mobile terminal; a key generation unit, configured to separately generate an application public key and an application private key based on the application authorization request; an application public key certificate generation unit, configured to sign the application public key by using a credit authorization private key stored on a predetermined server, to generate an application public key certificate; a data sending unit, configured to send the application public key certificate and the application private key to the mobile terminal; a credit payment data acquisition request receiving unit, configured to receive a credit payment data acquisition request sent by the mobile terminal; a credit payment data generation unit, configured to generate credit payment data corresponding to the mobile terminal based on the credit payment data acquisition request; and a credit payment data sending unit, configured to 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.

[0021] The device further includes: a device parameter information receiving unit,

configured to receive device parameter information sent by the mobile terminal; a first 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 enablement information sending unit, configured to: when the mobile terminal meets the hardware condition for enabling credit payment, send credit payment enablement information to the mobile terminal.

[0022] The device further includes: a user identity information receiving unit, configured to receive user identity information sent by the mobile terminal; a second determining unit, configured to determine, based on the user identity information, whether the mobile terminal meets a security certification condition for enabling credit payment; and a security certification success information sending unit, configured to: when the mobile terminal meets the security certification condition for enabling credit payment, send security certification success information to the mobile terminal.

[0023] The device further includes: a predetermined installation file acquisition request receiving unit, configured to receive a request for obtaining a predetermined installation file sent by the mobile terminal, where the predetermined installation file includes a credit payment installation file; and a predetermined installation file sending unit, configured to send the predetermined installation file to the mobile terminal based on the request for obtaining a predetermined installation file.

[0024] The technical solutions provided in the implementations of the present disclosure can include the following beneficial effects:

[0025] The credit payment method and device based on card emulation of a mobile terminal provided in the present disclosure can be applied to a mobile terminal and a transaction terminal. After enabling a payment application, a user can complete offline credit payment on the transaction terminal by using the mobile terminal, to quickly and securely complete a payment transaction. Online payment is not needed. As such, unlike the existing technologies, the user can complete the payment transaction without using cash or a public transportation card when taking public transportation.

[0026] It should be understood that the previous general descriptions and the following detailed descriptions are merely an example and explanation, and cannot limit the present disclosure.

BRIEF DESCRIPTION OF DRAWINGS

[0027] The accompanying drawings here are incorporated in the specification, become a part of the specification, show implementations in accordance with the present disclosure, and are used with the specification to explain a principle of the present disclosure.

[0028] FIG. 1 is a schematic diagram illustrating a credit authorization system, according to an implementation of the present disclosure.

[0029] FIG. 2 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to an example implementation.

[0030] FIG. 3 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to another example implementation.

[0031] FIG. 4 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0032] FIG. 5 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0033] FIG. 6 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0034] FIG. 7 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0035] FIG. 8 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0036] FIG. 9 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0037] FIG. 10 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0038] FIG. 11 is a flowchart illustrating step 150 in FIG. 10.

[0039] FIG. 12 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0040] FIG. 13 is a flowchart illustrating step 460 in FIG. 12.

[0041] FIG. 14 is a flowchart illustrating a credit payment method based on card emulation of a mobile terminal, according to yet another example implementation.

[0042] FIG. 15 is a signaling diagram among a credit authorization system application, a credit payment application, and a server of a credit authorization

system.

[0043] FIG. 16 is a signaling diagram of data exchange between a mobile terminal and a bus gate.

[0044] FIG. 17 is a signaling diagram of data exchange between a bus gate and a server of a credit authorization system.

[0045] FIG. 18 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to an example implementation.

[0046] FIG. 19 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0047] FIG. 20 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0048] FIG. 21 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0049] FIG. 22 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0050] FIG. 23 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0051] FIG. 24 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

[0052] FIG. 25 is a schematic diagram illustrating a credit payment device based on card emulation of a mobile terminal, according to another example implementation.

DESCRIPTION OF IMPLEMENTATIONS

[0053] Example implementations are described in detail here, and examples of the example implementations are presented in the accompanying drawings. When the following description relates to the accompanying drawings, unless specified

otherwise, same numbers in different accompanying drawings represent the same or similar elements. Implementation methods described in the following example implementations do not represent all implementation methods consistent with the present disclosure. Instead, they are only examples of devices and methods described in the appended claims in detail and consistent with some aspects of the present disclosure.

[0054] Mobile payment is also referred to as payment with a mobile phone, and a user can pay for a purchased product or service by using a mobile terminal. The mobile terminal can communicate with a transaction terminal through near field communication (NFC), to implement a payment transaction. The NFC is also referred to as proximity-based communication:a short-distance high-frequency radio communications technology that allows non-contact point-to-point data transmission and data exchange between electronic devices. The secure nature of NFC technology shows good application prospect in fields, such as payment.

[0055] Card emulation is one of three working modes of the NFC technology. The card emulation is an integrated circuit (IC) card using a radio frequency identification (RFID) technology, and can replace a large number of IC cards (including credit cards) in most scenarios, for example, card scanning in malls, public transportation cards, access control, tickets, etc. A great advantage of the present method is that the card is powered by an RF domain of a non-contact card reader, and therefore the card can work even if a host device (such as a mobile phone) is powered off.

[0056] To facilitate better understanding and implementation of the present disclosure by a person skilled in the art, a correlation among a mobile terminal, a payment terminal, and a server in the implementations of the present disclosure is first briefly described, for example, how to transmit and process data between the previous terminals. The present disclosure can be applied to many fields 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.

[0057] As shown in FIG. 1, a credit authorization system application, according to the implementations 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 and subway system. The server

300 is a server in a credit authorization system application. 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. 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.

[0058] In the implementations of the present disclosure, two applications can be installed on the mobile terminal. One application is a credit payment application such as Applet. Sun Corporation sets the application Applet as the object running on a Java card. The other application on the mobile terminal can be a credit authorization system application. Functions of the two applications can be implemented by using one application.

[0059] The transaction terminal 200 uses a strict identity security certification mechanism to ensure that only a user passing identity security certification and having enough credit limit can enable a bus credit payment application.

[0060] The credit payment application Applet is installed on the mobile terminal 100 having an NFC function, generates an application public and private key pair during personalization, and stores an application private key in the credit payment application. The credit payment application ensures that data cannot be stolen under any condition. An application public key is signed as an application public key certificate by using a private key of the credit authorization system application, and is stored in the credit payment application. A public key of the credit authorization system application 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 mandatory security requirement needs to be imposed on the public key.

[0061] When a credit payment transaction is provided, 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 of the credit authorization system application, and restores 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 checks a security factor in the authorization license after the verification succeeds. 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 use credit, and a time interval exceeds a specified threshold, the mobile terminal needs to be connected to a network to verify user identity information, and grant authorization again.

[0062] To resolve a related technical problem, an implementation of the present disclosure first provides a credit payment method based on card emulation of a mobile terminal, applied to a process of enabling credit payment by a mobile terminal. As shown in FIG. 2, the method can include the following steps.

[0063] Step S110: Send an application authorization request to a predetermined server.

[0064] A 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.

[0065] Step S120: Receive an application public key certificate and an application private key sent by the predetermined server.

[0066] The server of the credit authorization system generates a pair of application public and private keys, that is, an application public key and an application private key based on the received application authorization request. The server signs the application public key by using a locally-stored authorized private key to generate the application public key certificate, and separately sends the obtained application public key certificate and application private key to the mobile terminal.

[0067] Step S130: Store the application public key certificate and the application private key in a credit payment application of the mobile terminal.

[0068] The mobile terminal stores the application public key certificate and the application private key sent by the server in the credit payment application of the mobile terminal.

[0069] Step S140: Send a credit payment data acquisition request to the predetermined server.

[0070] Step S150: 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.

[0071] Credit payment data can be a personalized script. The personalized script

can include a payment card number, a credit limit, an available credit, 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 credit is an amount of money that a user can currently spend. The TAC sub-key is obtained by the server of the credit authorization system through hashing based on the card number and by using a TAC parent private key.

[0072] In another implementation of the present disclosure, based on FIG. 2, as shown in FIG. 3, the method can further include the following steps before step S110.

[0073] Step S101: Obtain device parameter information of the mobile terminal.

[0074] The device parameter information of the mobile terminal can be hardware information of the mobile terminal. Whether the mobile terminal has a hardware condition for a payment transaction, for example, whether the mobile terminal has an NFC function, needs to be checked based on the device parameter information. Certainly, the device parameter information can be information such as a device model, a ROM version, a system model (such as an android version), and an application version of the mobile terminal.

[0075] Step S102: Send the device parameter information to the predetermined server.

[0076] The mobile terminal sends the obtained device parameter information to the server of the credit authorization system, so that the server determines, based on the received device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

[0077] Step S103: Check whether credit payment enablement information sent by the predetermined server is received.

[0078] If the mobile terminal meets the hardware condition for enabling credit payment, the server sends the credit payment enablement information to the mobile terminal. The credit payment enablement information can be a credit payment application enablement page.

[0079] If the mobile terminal does not meet the hardware condition for enabling credit payment, the server will not send the credit payment enablement information to the mobile terminal.

[0080] When the credit payment enablement information sent by the predetermined server is received, step S104 is performed.

[0081] Step S104: Determine that the mobile terminal meets a hardware condition

for enabling credit payment, and then perform step S110.

[0082] 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 certification condition further needs to be checked. Therefore, in another implementation of the present disclosure, the credit payment method based on card emulation of a mobile terminal according to the present disclosure can further include the following steps.

[0083] Step S105: Obtain user identity information.

[0084] The user identity information can be information such as an identity card number, a name, a bank card number, an email address, or an Alipay account of a user.

[0085] 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 certification condition for enabling credit payment.

[0086] The mobile terminal sends the user identity information to the server of the credit authorization system, so that the server verifies the user identity information, for example, verifies whether the bank card number provides service normally, and whether the user account has a poor credit transaction record.

[0087] Step S107: Check whether security certification success information sent by the predetermined server is received.

[0088] After receiving user information sent by the mobile terminal, the server checks the user information. If the security certification condition for enabling credit payment is met, the server sends the security certification success information to the mobile terminal.

[0089] When the security certification success information sent by the predetermined server is received, step S108 is performed. In step S108, determine that the mobile terminal meets the security certification condition for enabling credit payment, and then step S110 is performed.

[0090] When the mobile terminal receives the security certification success information sent by the server, it is determined that the mobile terminal meets the security certification condition for enabling credit payment.

[0091] When the mobile terminal does not receive the security certification success information sent by the server, it is determined that the mobile terminal does not meet the security certification condition for enabling credit payment.

[0092] 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 card emulation of a mobile terminal according to the present disclosure further includes the following steps.

[0093] Step S160: Send a request for obtaining a predetermined installation file to the predetermined server.

[0094] The predetermined installation file includes a credit payment installation file.

[0095] Step S170: Obtain the predetermined installation file sent by the predetermined server.

[0096] Step S180: Install the predetermined installation file on the mobile terminal. Then, step S110 is performed.

[0097] After a credit payment application and a registration script are separately installed on the mobile terminal, user personalization of the mobile terminal is competed. Then, a procedure of enabling the credit payment function on the mobile terminal is completed. Based on the previous implementations, an execution procedure on the server of the credit authorization system in which the mobile terminal enables the credit payment function is described below in detail.

[0098] In another implementation of the present disclosure, as shown in FIG. 6, an execution procedure of the credit payment method based on card emulation of a mobile terminal on a server (a server of a credit authorization system) according to the present disclosure can include the following steps.

[0099] Step S210: Receive an application authorization request sent by a mobile terminal.

[0100] Step S220: Separately generate an application public key and an application private key based on the application authorization request.

[0101] Step S230: Sign the application public key by using a credit authorization private key locally stored on a predetermined server, to generate an application public key certificate.

[0102] Step S240: Send the application public key certificate and the application private key to the mobile terminal.

[0103] The server of the credit authorization system generates a pair of application public and private keys, that is, an application public key and an application private key based on the received application authorization request. The

server signs the application public key by using a locally-stored authorized private key to generate the application public key certificate, and separately sends the obtained application public key certificate and application private key to the mobile terminal.

[0104] Step S250: Receive a credit payment data acquisition request sent by the mobile terminal.

[0105] Step S260: Generate credit payment data corresponding 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.

[0106] Credit payment data can be a personalized script. The personalized script includes a payment card number, a credit limit, an available credit, 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 credit is an amount of money that the user can currently use. The TAC sub-key is obtained by the server of the credit authorization system through hashing based on the card number hash by using a TAC parent private key.

[0107] Based on FIG. 6, as shown in FIG. 7, in another implementation of the present disclosure, the server (the server 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, the credit payment method based on card emulation of a mobile terminal according to the present implementation of the present disclosure can further include the following steps before step S210.

[0108] Step S201: Receive device parameter information sent by the mobile terminal.

[0109] In a process of enabling a credit payment function by the mobile terminal, the mobile terminal can communicate with the server of the credit authorization system (that is, the server) through a network, and the server of the credit authorization system can receive the device parameter information sent by the mobile terminal.

[0110] Step S202: Determine, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

[0111] The parameter information sent by the mobile terminal can be information

such as a device model, a ROM version, a system model (such as an android version), and an application version of the mobile terminal. The server can check, based on the previous information sent by the mobile terminal, whether the mobile terminal has an NFC function.

[0112] If the server checks that the mobile terminal meets the hardware condition for enabling credit payment, the server sends credit payment enablement information to the mobile terminal. The credit payment enablement information can be a credit payment application enablement page. A user can enter user information on the credit payment application enablement interface on the mobile terminal, and upload the user information to the server.

[0113] If the server checks that the mobile terminal does not meet the hardware condition for enabling credit payment, the server will not send credit payment enablement information to the mobile terminal.

[0114] When the mobile terminal meets the hardware condition for enabling credit payment, in step S203, credit payment enablement information is sent to the mobile terminal. Then, step S210 is performed.

[0115] In addition to the device parameter information sent by the mobile terminal, the server of the credit authorization system needs to check user identity information sent by the mobile terminal, and determines whether a user corresponding to the mobile terminal meets a security certification condition. Therefore, based on FIG. 6, as shown in FIG. 8, in a process of enabling the credit payment function by the mobile terminal, the credit payment method based on card emulation of a mobile terminal according to the present disclosure can further include the following steps before step S210.

[0116] Step S204: Receive user identity information sent by the mobile terminal.

[0117] The user identity information can be information such as an identity card number, a name, a bank card number, an email address, or an Alipay account of a user.

[0118] Step S205: Determine, based on the user identity information, whether the mobile terminal meets a security certification condition for enabling credit payment.

[0119] For example, the server can check whether a bank card number in the user identity information provides a service normally, and whether there is a poor transaction record.

[0120] If checking that the mobile terminal meets the security certification condition for enabling credit payment, the server sends security certification success

information to the mobile terminal.

[0121] When the mobile terminal meets the security certification condition for enabling credit payment, in step S206, security certification success information is sent to the mobile terminal. Then, step S210 is performed.

[0122] When enabling credit payment, the mobile terminal further needs to install a credit payment application, and these installation files need to be sent by the server of the credit payment system to the mobile terminal. Therefore, based on FIG. 6, as shown in FIG. 9, in another implementation of the present disclosure, the credit payment method based on card emulation of a mobile terminal according to the present disclosure can further include the following steps before step S210.

[0123] Step S207: Receive a request for obtaining a predetermined installation file and sent by the mobile terminal.

[0124] The predetermined installation file includes a credit payment installation file.

[0125] Step S208: Send the predetermined installation file to the mobile terminal based on the request for obtaining a predetermined installation file, and then perform step S210.

[0126] Data exchange between a mobile terminal and a transaction terminal during a payment transaction is first described below.

[0127] To resolve a related technical problem, an implementation of the present disclosure provides a credit payment method based on card emulation of a mobile terminal, applied to a mobile terminal. As shown in FIG. 10, the method can include the following steps.

[0128] Step 110: When a transaction terminal is checked, send transaction information to the transaction terminal.

[0129] For ease of description, an example that the transaction terminal is a bus gate is used for description.

[0130] When a user holding a mobile terminal approaches a bus gate to make a payment transaction, because a radio frequency field can be generated on the bus gate, the mobile terminal can detect the radio frequency field generated on the bus gate when the mobile terminal approaches the bus gate, and then can detect the bus gate. When the mobile terminal detects the bus gate, the mobile terminal sends the transaction information to the bus gate.

[0131] Step 120: Receive an application public key certificate reading instruction

sent by the transaction terminal.

[0132] 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 generated in advance and stored on the mobile terminal.

[0133] Step 130: Send an application public key certificate to the transaction terminal based on the application public key certificate reading instruction.

[0134] 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.

[0135] Step 140: Receive deduction information of a current payment transaction sent by the transaction terminal based on the transaction information.

[0136] After receiving the application public key certificate sent by the mobile terminal, the bus gate verifies the application public key certificate, generates the deduction information of the current payment transaction, and sends the deduction information to the mobile terminal. The mobile terminal receives the deduction information sent by the bus gate.

[0137] Step 150: Generate a payment authorization license based on the deduction information and the transaction information and by using a credit payment application installed on the mobile terminal.

[0138] The payment authorization license generated by the mobile terminal includes signature data and a TAC.

[0139] Step 160: 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.

[0140] After receiving the payment authorization license sent by the mobile terminal, the bus gate verifies the payment license. If the verification succeeds, it is determined that the current payment transaction is completed.

[0141] According to the credit payment method based on card emulation of a mobile terminal 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 separately sends the transaction information, the application public key certificate, and the generated payment authorization license to the transaction terminal based on related instruction information sent by the transaction terminal. The transaction terminal completes the current payment transaction based on the information sent by the mobile terminal. Unlike the existing technologies, in the credit payment method based on card emulation of a mobile terminal in the present implementation of the present disclosure, when making a transaction with the transaction terminal by using the mobile terminal, the user can make both the mobile terminal and the transaction terminal offline, and credit consumption is used for a user account of the mobile terminal. 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.

[0142] 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, based on FIG. 10, in another implementation of the present disclosure, as shown in FIG. 11, step 150 can further include the following steps.

[0143] Step 151: Generate signature data based on the deduction information and by using an application private key stored on the mobile terminal.

[0144] The application private key is generated in advance, and is 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 deduction amount, a date and time of the current payment transaction, an entry/exit sign of the current payment transaction, and station information of the current payment transaction.

[0145] Step 152: Generate a TAC based on the deduction information and the transaction information and by using a TAC sub-key generated on the mobile terminal in advance.

[0146] The credit payment application on the mobile terminal encrypts the deduction money, the date of the current payment transaction, the time of the current payment transaction, a payment card number, an available credit, and a credit limit based on the deduction information and transaction information, to generate the TAC. The credit limit is the maximum offline available money granted by the credit

authorization system to the user.

[0147] Step 153: Use both the signature data and the TAC as the payment authorization license.

[0148] The credit payment application can separately send the signature data and the TAC used as the payment authorization license to the bus gate, or can send together the signature data and the TAC used as a credit authorization license to the bus gate.

[0149] In addition, the transaction information includes a payment card number, an available credit, an entry/exit sign, and previous transaction information. 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 credit is the amount of money that the user can currently spend. The TAC sub-key is obtained by the server of the credit authorization system through hashing based on the card number and by using a TAC parent key.

[0150] Based on FIG. 10, the method can further include the following steps.

[0151] Step 11: Subtract the deduction amount from an available credit in the transaction information based on the deduction amount in the deduction information of the current pay transaction, to obtain a currently available credit.

[0152] Step 12: Use the currently available credit as an available credit corresponding to a user on the mobile terminal. Then, step S150 is performed.

[0153] 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 the credit payment method based on card emulation of a mobile terminal on the transaction terminal. As shown in FIG. 12, the method can include the following steps.

[0154] Step 410: After transaction information sent by a mobile terminal is received, send an application public key certificate reading instruction to the mobile terminal.

[0155] A bus gate receives the transaction information sent by the mobile terminal, and the transaction information includes a payment card number, an available credit, an entry/exit sign, and previous transaction information. The bus gate checks content in the transaction information, for example, checks information such as an available credit of a corresponding account of the mobile terminal and the an entry/exit sign. After the check succeeds, the bus gate sends the application public key certificate

reading instruction to the mobile terminal.

[0156] Step S420: Receive an application public key certificate sent by the mobile terminal.

[0157] 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. The bus gate receives the application public key certificate sent by the mobile terminal.

[0158] Step 430: Verify the application public key certificate by using a locally-stored credit authorization public key of a transaction terminal.

[0159] To identify 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 stored on the bus gate in advance.

[0160] Step 440: When an application public key is restored from the application public key certificate during verification, generate deduction information of a current payment transaction.

[0161] The bus gate verifies the application public key certificate sent by the mobile terminal, and if the verification fails, ends the current payment transaction. If the application public key is restored from the application public key certificate, it indicates that the verification succeeds, and the deduction information of the current payment transaction is generated. It is worthwhile to note that the deduction information of the current payment transaction can also be referred to as a deduction instruction, and intends to generate a payment authorization license after the mobile terminal receives the deduction information (the deduction instruction) sent by the bus gate.

[0162] The deduction information of the current payment transaction includes a deduction amount, a date of the current payment transaction, a time of the current payment transaction, entry/exit sign of the current payment transaction, and station information of the current payment transaction. The deduction money is calculated by the bus gate based on information such as the entry/exit sign of the current payment transaction.

[0163] Step 450: Send the deduction information to the mobile terminal.

[0164] 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 and by using the credit payment application installed on the mobile terminal.

[0165] Step 460: When a payment authorization license is received, determine that the current payment transaction is completed based on the payment authorization license.

[0166] The payment authorization license includes signature data and a TAC. The bus gate verifies the signature data in the payment authorization license, if the verification fails, ends the current payment transaction, and if the verification succeeds, records a transaction log of the current payment transaction.

[0167] To describe in detail how the transaction terminal completes the current payment transaction based on the authentication license sent by the mobile terminal in the present implementation of the present disclosure, based on FIG. 12, in another implementation of the present disclosure, as shown in FIG. 13, step 460 can further include the following steps.

[0168] Step 461: Verify the signature data by using the application public key.

[0169] The application public key is restored by the bus gate from the payment authorization license sent by the mobile terminal. The bus gate checks, by using the application public key, whether related information in the signature data matches corresponding information in the application public key, and if yes, determines that the verification succeeds.

[0170] Step 462: Generate a transaction log when the signature data is verified.

[0171] After successfully verifying the signature data, the bus gate generates the transaction log of the current payment. The transaction log includes a deduction amount, a transaction date, a transaction time, a transaction terminal ID, a payment card number, an available credit, and a TAC.

[0172] Step 463: Send the transaction log to a predetermined server, so that the predetermined server deducts corresponding money from a user account corresponding to the mobile terminal based on the transaction log.

[0173] As shown in FIG. 14, in another implementation of the present disclosure, an execution procedure of the credit payment method based on card emulation of a mobile terminal on the transaction terminal in the present implementation of the present disclosure can further include the following steps.

[0174] Step 470: Determine whether an available credit in the transaction

information is greater than or equal to a predetermined threshold.

[0175] If the available credit is greater than or equal to the predetermined threshold, step 480 is performed.

[0176] Step 480: Check whether an entry/exit sign in the transaction information is an "entered" state.

[0177] If the entry/exit sign is the "exited" state, step 410 is performed.

[0178] Step 470 is mainly used by the bus gate to check, based on the transaction information sent by the mobile terminal, whether the available credit of the user account corresponding to the mobile terminal is enough for paying for the current payment transaction. If the available credit is not enough, the current payment transaction is rejected. If the available amount is enough, the bus gate checks whether the entry/exit sign in the transaction information is 0. If the entry/exit sign is not 0, the current payment transaction is rejected. If the entry/exit sign is 0, the current payment transaction continues. It is worthwhile to note that "1" in the entry/exit sign indicates that the mobile terminal is in an "entered" state, and the current payment transaction is rejected. "0" in the entry/exit sign indicates that the mobile terminal is in an "exited" state, and the current payment transaction can be made.

[0179] The transaction information includes a payment card number, an available credit, an entry/exit sign and previous transaction information.

[0180] In another implementation, as shown in FIG. 15, the present disclosure provides a credit payment method based on card emulation of a mobile terminal. In this implementation, a mobile phone represents a mobile terminal, and a server 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 server of the credit authorization system includes the following steps:

[0181] Step 1001: Obtain device parameter information of the mobile phone.

[0182] Step 1002: Upload the device parameter information.

[0183] Step 1003: Determine whether the mobile phone meets a hardware condition for enabling credit payment.

[0184] Step 1004: Return a determining result.

[0185] Step 1005: The determining result is displaying a credit payment application interface.

[0186] Step 1006: Upload user identity information.

[0187] Step 1007: Determine whether the mobile phone meets a security certification condition for enabling credit payment.

[0188] Step 1008: Return a determining result.

[0189] Step 1009: A user chooses to enable a credit payment application.

[0190] Step 1010: Activate the credit payment application.

[0191] Step 1011: Return an activation success result.

[0192] Step 1012: Request an application private key, an application public key certificate, and credit payment data.

[0193] Step 1013: Generate a pair of public and private keys, generate an application public key certificate by using a credit authorization private key, generate a payment card number, and generate an application TAC sub-key, a sub-key, and credit payment data through hashing.

[0194] Step 1014: Return the application private key, the application public key certificate, and the credit payment data.

[0195] Step 1015: Send the application private key, the application public key certificate, and the credit payment data.

[0196] Step 1016: Store the application private key, the application public key certificate, and the credit payment data.

[0197] Step 1017: Return a personalization result.

[0198] Step 1018: Send a credit payment enablement result.

[0199] Step 1019: Record the enablement result.

[0200] Step 1020: Return a processing completion notification.

[0201] Step 1021: Notify the user that the credit payment application is successfully enabled.

[0202] In another implementation of the present disclosure, as shown in FIG. 16, the present disclosure provides a credit payment method based on card emulation. In a process in which a mobile terminal performs payment transaction, a data exchange procedure between a mobile terminal and a bus gate in a payment transaction process is as follows:

[0203] Step 2001: The bus gate selects a credit authorization system application.

[0204] Step 2002: The credit authorization system application reads data that needs to be returned.

[0205] Step 2003: The credit authorization system application returns a payment card number, an available credit, an entry/exit sign, and previous transaction

information.

[0206] Step 2004: The bus gate checks the available credit and the entry/exit sign, and if the check fails, presents rejection information.

[0207] Step 2005: The bus gate calculates deduction money.

[0208] Step 2006: The bus gate makes a deduction based on the deduction money, a transaction time, the entry/exit sign, and transaction information.

[0209] Step 2007: The credit authorization system application generates a payment authorization license that includes signature data and a TAC.

[0210] Step 2008: The credit authorization system application returns the signature data and the TAC.

[0211] Step 2009: The bus gate verifies the signature data by using an application public key, if the verification succeeds, records a transaction log, and if the verification fails, presents rejection information.

[0212] In addition, as shown in FIG. 17, the bus gate further needs to periodically upload a transaction log to the credit authorization system, and update a blacklist. In the credit payment method based on card emulation of a mobile terminal in the present disclosure, a data exchange procedure between a bus gate (a transaction terminal) and a server of a credit authorization system is as follows:

[0213] Step 3001: Periodically upload a transaction log.

[0214] Step 3002: Perform settlement, query whether a blacklist in the system is updated, and if the blacklist is updated, prepare to return the blacklist.

[0215] Step 3003: Return a transaction log receiving results and the blacklist.

[0216] Step 3004: Check whether there is the blacklist.

[0217] Step 3005: The bus gate updates the blacklist.

[0218] Step 3006: Perform updating.

[0219] Step 3007: Return an updated completion result.

[0220] Based on the previous descriptions of the 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, and can certainly be implemented by hardware, but in many circumstances, 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 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, or a network device) to perform all or some of the steps of the methods described in the implementations of the present disclosure. The storage medium includes various 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.

[0221] The implementations of the present disclosure are described above by using credit payment for a bus as an example. It can be understood that the credit payment can be applied to another payment scenario as needed, for example, a subway payment and offline shopping payment scenario. There can be different implementations in specific application scenarios.

[0222] In addition, as an implementation of the previous embodiments, an implementation of the present disclosure further provides a credit payment device based on card emulation of a mobile terminal. The device is located on a mobile terminal. As shown in FIG. 18, the device includes an application authorization request sending unit 10, a key receiving unit 20, a key storage unit 30, a credit payment data acquisition request sending unit 40, a credit payment data receiving unit 50, and a credit payment completion unit 60.

[0223] The application authorization request sending unit 10 is configured to send an application authorization request to a predetermined server by using a credit authorization system application on the mobile terminal.

[0224] The key receiving unit 20 is configured to receive an application public key certificate and an application private key sent by the predetermined server.

[0225] The key storage unit 30 is configured to store the application public key certificate and the application private key in a credit payment application of the mobile terminal.

[0226] The credit payment data acquisition request sending unit 40 is configured to send a credit payment data acquisition request to the predetermined server.

[0227] The credit payment data receiving unit 50 is configured to receive credit payment data sent by the predetermined server.

[0228] The credit payment completion unit 60 is configured to enable a credit payment function of the mobile terminal based on the credit payment data.

[0229] In another implementation of the present disclosure, based on FIG. 18, as shown in FIG. 19, the device further includes: a device parameter information acquisition unit 71, configured to obtain device parameter information of the mobile

terminal; a device parameter information sending unit 72, 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 first detection unit 73, configured to detect whether credit payment enablement information sent by the predetermined server is received; and a hardware condition determining unit 74, configured to: when the credit payment enablement information sent by the predetermined server is received, determine that the mobile terminal meets the hardware condition for enabling credit payment.

[0230] In another implementation of the present disclosure, based on FIG. 18, as shown in FIG. 20, the device further includes: a user identity information acquisition unit 75, configured to obtain user identity information; a user identity information sending unit 76, 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 certification condition for enabling credit payment; a second detection unit 77, configured to detect whether security certification success information sent by the predetermined server is received; and a security certification condition determining unit 78, configured to: when the security certification success information sent by the predetermined server is received, determine that the mobile terminal meets the security certification condition for enabling credit payment.

[0231] In another implementation of the present disclosure, based on FIG. 18, as shown in FIG. 21, the device further includes: a predetermined installation file acquisition request sending unit 81, configured to send a request for obtaining a predetermined installation file to the predetermined server, where the predetermined installation file includes a credit payment installation file; a predetermined installation file acquisition unit 82, configured to obtain the predetermined installation file sent by the predetermined server; and an installation unit 83, configured to install the predetermined installation file on the mobile terminal.

[0232] An implementation of the present disclosure further provides a credit payment device based on card emulation of a mobile terminal. The device is on a transaction terminal. As shown in FIG. 22, the device includes an application authorization request receiving unit 11, a key generation unit 12, an application public key certificate generation unit 13, a data sending unit 14, a credit payment data

acquisition request receiving unit 15, a credit payment data generation unit 16, and a credit payment data sending unit 17.

[0233] The application authorization request receiving unit 11 is configured to receive an application authorization request sent by a mobile terminal.

[0234] The key generation unit 12 is configured to separately generate an application public key and an application private key based on the application authorization request.

[0235] The application public key certificate generation unit 13 is configured to sign the application public key by using a credit authorization private key stored on a predetermined server, to generate an application public key certificate.

[0236] The data sending unit 14 is configured to send the application public key certificate and the application private key to the mobile terminal.

[0237] The credit payment data acquisition request receiving unit 15 is configured to receive a credit payment data acquisition request sent by the mobile terminal.

[0238] The credit payment data generation unit 16 is configured to generate credit payment data corresponding to the mobile terminal based on the credit payment data acquisition request.

[0239] The credit payment data sending unit 17 is configured to 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.

[0240] In another implementation of the present disclosure, based on FIG. 22, as shown in FIG. 23, the device further includes: a device parameter information receiving unit 91, configured to receive device parameter information sent by the mobile terminal; a first determining unit 92, 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 enablement information sending unit 93, configured to: when the mobile terminal meets the hardware condition for enabling credit payment, send credit payment enablement information to the mobile terminal.

[0241] In another implementation of the present disclosure, based on FIG. 22, as shown in FIG. 24, the device further includes: a user identity information receiving unit 94, configured to receive user identity information sent by the mobile terminal; a second determining unit 95, configured to determine, based on the user identity information, whether the mobile terminal meets a security certification condition for

enabling credit payment; and a security certification success information sending unit 96, configured to: when the mobile terminal meets the security certification condition for enabling credit payment, send security certification success information to the mobile terminal.

[0242] In another implementation of the present disclosure, based on FIG. 19, as shown in FIG. 25, the device further includes: a predetermined installation file acquisition request receiving unit 97, configured to receive a request for obtaining a predetermined installation file and sent by the mobile terminal, where the predetermined installation file includes a credit payment installation file; and a predetermined installation file sending unit 98, configured to send the predetermined installation file to the mobile terminal based on the request for obtaining a predetermined installation file.

[0243] Specific methods of execution operations of the modules in the device in the previous implementations are described in detail in corresponding method implementations, and details are not described here.

[0244] The credit payment method and device based on card emulation of a mobile terminal provided in the present disclosure can be applied to a mobile terminal and a transaction terminal. After enabling a payment application, a user can complete offline credit payment on the transaction terminal by using the mobile terminal, to quickly and securely complete a payment transaction. Online payment is not needed. As such, unlike the existing technologies, the user can complete the payment transaction without using cash or a public transportation card when taking a public transport vehicle.

[0245] It can be understood that the present disclosure can be applied to environments or configurations of a plurality of universal or dedicated computing systems. 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 consumer electronic device, a network PC, a minicomputer, a mainframe computer, and a distributed computing environment including any one of the previous system or device.

[0246] The present disclosure can be described in the general context of executable computer instructions executed by a computer, for example, a program module. Generally, the program unit includes a routine, a program, an object, a component, a data structure, and the like for executing a particular task or

implementing a particular abstract data type. The present disclosure can also be practiced in distributed computing environments that tasks are executed by remote processing devices 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.

[0247] It is worthwhile to note that in the present 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 any other variants mean to cover the 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 not expressly listed, or further includes elements inherent to such process, method, article, or device. An element preceded by "includes a..." does not, without more constraints, preclude the existence of additional identical elements in the process, method, article, or device that includes the element.

[0248] 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 disclosed 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 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.

[0249] It should be understood that the present disclosure is not limited to the accurate structures described in the foregoing and 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:

sending, by a mobile terminal, an application authorization request to a predetermined server (S110);

receiving, by the mobile terminal, an application public key certificate and an application private key sent by the predetermined server (S120);

storing, by the mobile terminal, the application public key certificate and the application private key in a credit payment application of the mobile terminal (S130);

sending, by the mobile terminal, a credit payment data acquisition request to the predetermined server (S140);

receiving, by the mobile terminal, credit payment data sent by the predetermined server, the credit payment data including a transaction authorization code (TAC), and enabling a credit payment function of the mobile terminal based on the credit payment data (S150); and

performing, by the mobile terminal, a payment transaction with a transaction terminal, the performing of the transaction comprising:

sending (110), by the mobile terminal, transaction information to the transaction terminal;

receiving (120), by the mobile terminal, an application public key certificate reading instruction sent by the transaction terminal;

sending (130), by the mobile terminal, an application public key certificate, stored in advance on the mobile terminal, to the transaction terminal in response to the application public key certificate reading instruction;

receiving (140), by the mobile terminal and from the transaction terminal, after the transaction terminal verifies the public key certificate, deduction information based on the transaction information;

generating (150), by the credit payment application on the mobile terminal, a payment authorization license based on the deduction information and the transaction information, including generating (151) signature data based on the deduction information and by using the application private key stored on the mobile terminal, wherein the payment authorization license generated by the mobile terminal includes the

signature data and the TAC;

sending (160), by the mobile terminal, the payment authorization license to the transaction terminal; and

verifying, by the transaction terminal, the payment authorization license, and completing the payment transaction based on the received payment authorization license.

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

retrieving device parameter information of the mobile terminal (S101);

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 (S102);

determining whether credit payment enablement information sent by the predetermined server is received (S103); and

in response to determining that the credit payment enablement information sent by the predetermined server is received, determining that the mobile terminal meets the hardware condition for enabling credit payment, and executing the step of sending an application authorization request to a predetermined server (S104).

3. The method according to any one of claims 1 to 2, further comprising:

retrieving user identity information (S105);

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 certification condition for enabling credit payment (S106);

determining whether security certification success information sent by the predetermined server is received (S107); and

in response to determining that the security certification success information sent by the predetermined server is received, determining that the mobile terminal meets the security certification condition for enabling credit payment, and executing the step of sending an application authorization request to a predetermined server (S108).

4. The method according to any one of claims 1 to 3, further comprising:

sending a request for retrieving a predetermined installation file to the predetermined server, wherein the predetermined installation file comprises a credit payment installation file (S160);

retrieving the predetermined installation file sent by the predetermined server (S170); and

installing the predetermined installation file on the mobile terminal, and executing the step of sending an application authorization request to the predetermined server (S180).

5. The method according to any one of claims 1 to 4, wherein the credit payment data comprises at least one of a payment card number, a credit limit, an available credit, and a transaction authentication code (TAC) sub-key.

6. The method according to any one of claims 1 to 5, wherein:

the credit payment enablement information is determined, based on the device parameter information, whether the mobile terminal meets a hardware condition for enabling credit payment.

7. The method according to any one of claims 1 to 6, wherein the mobile terminal comprises a card emulation to communicate with the predetermined server.

8. The method according to claim 7, wherein the card emulation enables a near field communication.

9. The method according to claim 7, wherein the card emulation is powered by a radio frequency domain of a non-contact card reader.

10. The method according to claim 7, wherein the card emulation is configured to communicate with the predetermined server when the mobile terminal is powered off.

11. An apparatus for processing credit payment, the apparatus comprising a plurality of modules configured to perform the method according to any one of claims 1 to 10.