DATA INTERACTION METHOD AND DEVICE, AND OFFLINE CREDIT PAYMENT METHOD AND DEVICE

[0001] The present application claims priority to Chinese Patent Application No. 201610006675.6, filed on January 5, 2016 and entitled "Data Interaction Method and Device, and Offline Credit Payment Method and Device", which is incorporated herein by reference in its entirety.

TECHNICAL FIELD

[0002] The present application relates to the field of data interaction technologies, and in particular, to a data interaction method and device, and an offline credit payment method and device.

BACKGROUND

[0003] Conventionally, magnetic stripe credit cards are usually used for payment. However, users usually encounter problems such as skimming fraud and identity theft. At present, although some new credit cards employ smart card carriers to improve security, many transactions are still conducted by using magnetic stripe credit cards. In addition, payment limits of credit cards are usually high, and the users need to visit credit card issuers to adjust the limits. If magnetic stripe information is duplicated or credit cards are lost, the users may suffer heavy losses. Therefore, security coefficients of these magnetic stripe credit cards are relatively low. Moreover, network-based payment is usually performed through bank card (including credit card) transfer, and the user’s funds need to be processed in real time during the payment.

SUMMARY

[0004] An implementation of the present application provides a data interaction method, including: collecting authorization data for current interaction obtained by an intelligent terminal from a remote server; and recording the authorization data and data of the current interaction.

[0005] An implementation of the present application further provides a data

interaction method, including: obtaining authorization data for current interaction of a user from a remote server; and providing the authorization data for an interaction terminal, so that the interaction terminal can perform processing based on the authorization data.

[0006] An implementation of the present application further provides a data interaction method, including: obtaining an authorization request sent by a user through an intelligent terminal; and sending authorization data for current interaction of the user to the intelligent terminal based on the authorization request from the intelligent terminal.

[0007] An implementation of the present application further provides an interaction terminal, including: a collection unit, configured to collect authorization data for current interaction obtained by an intelligent terminal from a remote server; and a recording unit, configured to record the authorization data and data of the current interaction.

[0008] An implementation of the present application further provides an intelligent terminal, including: an acquisition unit, configured to obtain authorization data for current interaction of a user from a remote server; and a communication unit, configured to provide the authorization data for an interaction terminal, so that the interaction terminal can perform processing based on the authorization data.

[0009] An implementation of the present application further provides a remote server, including: an acquisition unit, configured to obtain an authorization request sent by a user through an intelligent terminal; and a processing unit, configured to send authorization data for current interaction of the user to the intelligent terminal based on the authorization request from the intelligent terminal.

[0010] An implementation of the present application further provides an offline credit payment method, including: collecting credit authorization data for a current transaction obtained by an intelligent terminal from a remote server; and recording the credit authorization data and data of the current transaction.

[0011] An implementation of the present application further provides an offline credit payment method, including: obtaining credit authorization data for a current transaction of a user from a remote server; and providing the credit authorization data for a fee deduction terminal, so that the fee deduction terminal performs processing based on the credit authorization data.

[0012] An implementation of the present application further provides an offline

payment method, including: obtaining a credit authorization request sent by a user through an intelligent terminal; and sending credit authorization data for a current transaction of the user to the intelligent terminal based on the credit authorization request from the intelligent terminal.

[0013] An implementation of the present application further provides a fee deduction terminal, including: a collection unit, configured to collect credit authorization data for a current transaction obtained by an intelligent terminal from a remote server; and a recording unit, configured to record the credit authorization data and data of the current transaction.

[0014] An implementation of the present application further provides an intelligent terminal, including: an acquisition unit, configured to obtain credit authorization data for a current transaction of a user from a remote server; and a communication unit, configured to provide the credit authorization data for a fee deduction terminal, so that the fee deduction terminal performs processing based on the credit authorization data.

[0015] An implementation of the present application further provides a remote server, including: an acquisition unit, configured to obtain a credit authorization request sent by a user through an intelligent terminal; and a processing unit, configured to send credit authorization data for a current transaction of the user to the intelligent terminal based on the credit authorization request from the intelligent terminal.

[0016] An implementation of the present application further provides an offline credit payment system, including an intelligent terminal, a remote server, and a fee deduction terminal, where the remote server is configured to send credit authorization data for a current transaction of a user to the intelligent terminal based on a credit authorization request from the intelligent terminal; the intelligent terminal is configured to obtain the credit authorization data from the remote server; and the fee deduction terminal is configured to: collect the credit authorization data from the intelligent terminal, and record the credit authorization data and data of the current transaction.

[0017] It can be seen from the technical solutions provided in the implementations of the present application that, a transaction can be processed based on authorization of the remote server to improve payment efficiency.

[0018] Certainly, products or methods that implement the present application do

not necessarily need to achieve the earlier mentioned advantages.

BRIEF DESCRIPTION OF DRAWINGS

[0019] To describe the technical solutions in the implementations of the present application or in the existing technology more clearly, the following briefly describes the accompanying drawings for illustrating the implementations or the existing technology. Apparently, the accompanying drawings in the following description merely show some implementations of the present application, and a person of ordinary skill in the art can still derive other drawings from these accompanying drawings without creative efforts.

[0020] FIG. 1 is a flowchart illustrating a data interaction method, according to an implementation of the present application.

[0021] FIG. 2 is a flowchart illustrating a data interaction method, according to an implementation of the present application.

[0022] FIG. 3 is a flowchart illustrating a data interaction method, according to an implementation of the present application.

[0023] FIG. 4 is a schematic diagram illustrating an interaction terminal, according to an implementation of the present application.

[0024] FIG. 5 is a schematic diagram illustrating an intelligent terminal, according to an implementation of the present application.

[0025] FIG. 6 is a schematic diagram illustrating a remote server, according to an implementation of the present application.

[0026] FIG. 7 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application.

[0027] FIG. 8 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application.

[0028] FIG. 9 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application.

[0029] FIG. 10 is a schematic diagram illustrating a fee deduction terminal, according to an implementation of the present application.

[0030] FIG. 11 is a schematic diagram illustrating an intelligent terminal, according to an implementation of the present application.

[0031] FIG. 12 is a schematic diagram illustrating a remote server, according to the present application.

[0032] FIG. 13 is a schematic diagram illustrating an offline credit payment system, according to an implementation of the present application.

[0033] FIG. 14 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application.

[0034] FIG. 15 is a flowchart illustrating another offline credit payment method, according to an implementation of the present application.

DESCRIPTION OF IMPLEMENTATIONS

[0035] Implementations of the present application provide a data interaction method and device, and an offline credit payment method and device.

[0036] To make a person skilled in the art better understand the technical solutions in the present application, the following clearly and completely describes the technical solutions in the implementations of the present application with reference to the accompanying drawings in the implementations of the present application. Apparently, the described implementations are merely some, but not all of the implementations of the present application. Other implementations obtained by a person of ordinary skill in the art based on the implementations of the present application without creative efforts shall fall within the protection scope of the present application.

[0037] The technical solutions provided in the present application can be used for credit payment scenarios where the payment amount is small and the payment is made frequently, such as, making payment for taking a bus, taking a subway, etc. In the technical solutions provided in the present application, during a transaction, a payment deduction can be made through the interaction between a transaction user end, such as an intelligent terminal held by a user interaction, and a transaction processing end, such as a fee deduction terminal on a bus. Further, both the transaction user end and the transaction processing end can complete the payment transaction through the interaction with a remote server. Certainly, the technical solutions provided in the present application are not limited to a payment application. For example, the technical solutions can be used to process bonus points earned by subscribers (bonus points are rewarded by merchants to the subscribers, and the subscribers can get discounts when using the bonus points to purchase certain products or services).

[0038] For conventional credit payment, that is, credit card based payment, an

online operation needs to be performed on a POS machine. In some situations, for example, when purchasing a subway ticket, the transaction time can be relatively long. The interaction method disclosed in the present application can implement offline payment, that is, the transaction processing end can process payments without accessing the real-time network, increasing an interaction speed. In addition, the mutual interaction can be implemented even when the network connection is poor, so a fee deduction can be made offline. Moreover, credit authorization data generated during each transaction can be temporary to reduce the chance that such data is reused. As such, problems existing in the current technology, such as financial losses caused by a leak of information associated with magnetic stripe bank cards can be alleviated. Certainly, the credit authorization data can be used for a longer time in some cases, for example, one year, one month, or one week. That is, the authorization data can be obtained every year, every month, or every week, instead of being generated temporarily during each transaction. When authorization fails, the user is notified to obtain new authorization data. The following describes the technical solutions of the present application in detail.

[0039] FIG. 1 is a flowchart illustrating a data interaction method, according to an implementation of the present application. The method can be applied to a transaction between a transaction user end and a transaction processing end. The transaction user end can be an intelligent terminal held by a user, such as a mobile phone, and the transaction processing terminal can be a merchant terminal. This implementation is described by using processing between the intelligent terminal held by the user and the merchant terminal. The method can include the following steps:

[0040] Step 101: Collect authorization data for current interaction obtained by an intelligent terminal from a remote server.

[0041] Step 102: Record the authorization data and data of the current interaction.

[0042] Step 101 and step 102 are performed by the merchant terminal. The merchant terminal can collect the authorization data sent by the intelligent terminal, and record the authorization data and the data of the current interaction.

[0043] In an implementation of the present application, the merchant terminal records the authorization data and the data of the current interaction, and then checks the authorization data and the data of the current interaction with the remote server at a predetermined time. That is, the merchant terminal can interact with the remote server in the back end to check the authorization data and the data of the interaction in

the current transaction, and synchronize the data with the remote server for recording and other processing.

[0044] In an implementation of the present application, the collecting authorization data for current interaction obtained by an intelligent terminal from a remote server further includes: scanning a barcode generated by the intelligent terminal based on the authorization data to obtain the authorization data; or obtaining the authorization data from the intelligent terminal through wireless communication.

[0045] In an implementation of the present application, the barcode includes a one-dimensional barcode and/or a two-dimensional barcode, and the wireless communication includes NFC or RFID.

[0046] In an implementation of the present application, after the authorization data for current interaction is obtained by an intelligent terminal from a remote server, to verify the authorization data, the method further includes performing one or more of the following operations:

comparing time information included in the authorization data with a current time, and if the current time is later than the time information included in the authorization data, determining that the authorization data has expired, and canceling the current data interaction;

determining whether a random number included in the authorization data exists in previous data interaction, and if yes, determining that the authorization data is repeatedly used, and canceling the current data interaction; and

determining whether the data of the current interaction exceeds a threshold of the authorization data, and if yes, canceling the current data interaction.

[0047] In an implementation of the present application, the collected authorization data for the current interaction obtained by the intelligent terminal from the remote server further includes signature information used by the remote server to sign the authorization data by using a private key; and after the collecting authorization data for current interaction obtained by an intelligent terminal from a remote server, but before the recording the authorization data and data of the current interaction, the method further includes:

verifying the signature information by using a public key pre-obtained from the remote server, and determining whether the authorization data is sent by the remote server, where if yes, the authorization data and the data of the current interaction are recorded.

[0048] The authorization data for the current interaction can be obtained by the intelligent terminal from the remote server in real time. Alternatively, after being obtained by the intelligent terminal from the remote server, the authorization data can be valid within a period of time, for example, one month.

[0049] In the preceding interaction process, the merchant terminal can interact with the intelligent terminal without accessing the network, and therefore a time for the merchant terminal to access the network is saved. In addition, interaction with the intelligent terminal can be successfully completed when the network is in a poor condition.

[0050] FIG. 2 is a flowchart illustrating a data interaction method, according to an implementation of the present application. A data interaction process of an intelligent terminal in the present application is illustrated in FIG. 2. The method includes the following steps:

[0051] Step 201: Obtain authorization data for current interaction of a user from a remote server.

[0052] Step 202: Provide the authorization data for an interaction terminal, so that the interaction terminal can perform processing based on the authorization data.

[0053] Sending authorization data to an interaction terminal includes presenting the authorization data to a fee deduction terminal in the form of a barcode, and further includes sending interaction data such as authorization data to the fee deduction terminal through RFID.

[0054] In an implementation of the present application, the obtaining authorization data for current interaction of a user from a remote server further includes: sending a unique identifier of the user to the remote server; and receiving authorization data that includes user information and that is generated by the remote server based on the unique identifier.

[0055] In an implementation of the present application, the authorization data further includes time information of the current authorization, a random number of the current authorization, and a threshold.

[0056] Step 201 and step 202 can implement interaction between a transaction user end and a transaction processing end in combination with step 101 and step 102. Step 201 and step 202 can be performed by the transaction user end based on a transaction request triggered by the transaction processing end.

[0057] FIG. 3 is a flowchart illustrating a data interaction method, according to an

implementation of the present application. A work process of a remote server in data interaction is illustrated in FIG. 3. The remote server generates authorization data based on a user's request and sends the authorization data to an intelligent terminal. The method includes the following steps:

[0058] Step 301: Obtain an authorization request sent by a user through an intelligent terminal.

[0059] Step 302: Send authorization data for current interaction of the user to the intelligent terminal based on the authorization request from the intelligent terminal.

[0060] In an implementation of the present application, the authorization request includes a unique identifier of the user, and the sending authorization data for current interaction of the user to the intelligent terminal includes: generating authorization data including user information based on the unique identifier, and sending the authorization data for the current interaction of the user to the intelligent terminal. The unique identifier of the user can be a user name, a device identifier of the intelligent terminal held by the user, or a combination of both. As such, security of authorization data acquisition by the user can be ensured.

[0061] In an implementation of the present application, the sending authorization data for current interaction of the user to the intelligent terminal includes: encrypting the user information, signing the authorization data by using a private key, and delivering signature information and the authorization data to the intelligent terminal by using a password.

[0062] The user information can be encrypted by using an existing encryption method, for example, by using a pair of private key and public key. Details are not described here.

[0063] In this implementation of the present application, after the remote server sends the authorization data to the intelligent terminal, the intelligent terminal can interact with the transaction processing end offline based on the authorization data.

[0064] FIG. 4 is a schematic diagram illustrating an interaction terminal, according to an implementation of the present application. Functional units in FIG. 4 can be implemented by using a logic circuit, a chip, or a high-performance computer.

[0065] The interaction terminal includes: a collection unit 401, configured to collect authorization data for current interaction obtained by an intelligent terminal from a remote server; and a recording unit 402, configured to record the authorization data and data of the current interaction.

[0066] In an implementation of the present application, the interaction terminal further includes a check unit 403, configured to check the authorization data and the data of the current interaction with the remote server at a predetermined time.

[0067] In an implementation of the present application, the collection unit further includes a scanning module 404, configured to scan a barcode generated by the intelligent terminal based on the authorization data to obtain the authorization data; or the collection unit further includes a wireless communication module 405, configured to obtain the authorization data from the intelligent terminal through wireless communication.

[0068] The barcode includes a one-dimensional barcode and/or a two-dimensional barcode, and the wireless communication includes NFC or RFID.

[0069] In an implementation of the present application, the interaction terminal further includes a verification unit 407, configured to perform one or more of the following operations to verify the authorization data:

comparing time information included in the authorization data with a current time, and if the current time is later than the time information included in the authorization data, determining that the authorization data has expired, and canceling the current data interaction;

determining whether a random number included in the authorization data exists in previous data interaction, and if yes, determining that the authorization data is repeatedly used, and canceling the current data interaction; and

determining whether the data of the current interaction exceeds a threshold of the authorization data, and if yes, canceling the current data interaction.

[0070] In an implementation of the present application, the collected authorization data for the current interaction obtained by the intelligent terminal from the remote server further includes signature information used by the remote server to sign the authorization data by using a private key, and the interaction terminal further includes:

a signature verification unit 406, configured to: verify the signature information by using a public key pre-obtained from the remote server, and determine whether the authorization data is sent by the remote server, where if yes, the recording unit records the authorization data and the data of the current interaction.

[0071] The interaction terminal in this implementation can be the previously described transaction processing end, for example, the merchant terminal, and can perform the steps in this method. Details are not described here.

[0072] FIG. 5 is a schematic diagram illustrating an intelligent terminal, according to an implementation of the present application. A structure of the intelligent terminal for implementing the data interaction in the present application is illustrated in FIG. 5. Certainly, the intelligent terminal can further include other essential parts such as a touchscreen, a battery, a memory, or a circuit board, and details are not described here. The intelligent terminal can be a smartphone, a tablet computer, an intelligent wearable device, etc.

[0073] The intelligent terminal includes: an acquisition unit 501, configured to obtain authorization data for current interaction of a user from a remote server; and a communication unit 502, configured to provide the authorization data for an interaction terminal, so that the interaction terminal can perform processing based on the authorization data.

[0074] In an implementation of the present application, the acquisition unit 501 is further configured to: send a unique identifier of the user to the remote server, and receive authorization data that includes user information and that is generated by the remote server based on the unique identifier.

[0075] In an implementation of the present application, the authorization data further includes time information of current authorization, a random number of the current authorization, and a threshold.

[0076] FIG. 6 is a schematic diagram illustrating a remote server, according to an implementation of the present application. A structure of the remote server for data interaction in the present application is illustrated in FIG. 6. Certainly, the remote server can further include other essential parts such as an input/output device, a communication unit, a power supply, a memory, or a circuit board, and details are not described here. The remote server can be a high-performance computer or a computer cluster.

[0077] The remote server includes: an acquisition unit 601, configured to obtain an authorization request sent by a user through an intelligent terminal; and a processing unit 602, configured to send authorization data for current interaction of the user to the intelligent terminal based on the authorization request from the intelligent terminal.

[0078] In an implementation of the present application, the authorization request includes a unique identifier of the user, and the processing unit is configured to: generate authorization data including user information based on the unique identifier,

and send the authorization data for the current interaction of the user to the intelligent terminal.

[0079] In an implementation of the present application, that the processing unit sends authorization data for current interaction of the user to the intelligent terminal includes: encrypting the user information, signing the authorization data by using a private key, and delivering signature information and the authorization data to the intelligent terminal by using a password.

[0080] The following describes a technical implementation process of payment in detail.

[0081] FIG. 7 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application. FIG. 7 describes a fee deduction for a user implemented by a fee deduction terminal without accessing a network, so that credit authorization data and transaction data are sent to an institute such as a bank to complete an offline fee deduction. The fee deduction terminal can be a POS machine or another fee deduction device, and needs to register with a server in advance and obtain corresponding authorization before performing a credit deduction. The fee deduction terminal records a fee deduction of the current payment transaction to complete the current payment transaction, and periodically sends fee deduction records to the server for checking, user's consumption. The method includes the following steps:

[0082] Step 701: Collect credit authorization data for a current transaction obtained by an intelligent terminal from a remote server.

[0083] Step 702: Record the credit authorization data and data of the current transaction.

[0084] In an implementation of the present application, after the credit authorization data and the data of the current transaction are recorded, the method further includes: checking the credit authorization data and the data of the current transaction with the remote server at a predetermined time.

[0085] Before the credit authorization data and the data of the current transaction are checked, the fee deduction terminal may not immediately communicate with the remote server after recording the credit authorization data and the data of the current transaction. The fee deduction terminal needs to communicate with the remote server to complete the checking. After the fee deduction terminal performs the checking twice, the fee deduction terminal can send credit authorization data generated in the

time interval between these two checks and corresponding transaction data to the remote server, saving the time needed by the fee deduction terminal to perform credit authorization communication with the remote server during each transaction. A large amount of checked data can be sent to the remote server all at once at the predetermined time. The remote server deducts a payment from an account of the user based on the credit authorization data and the transaction data.

[0086] In an implementation of the present application, the credit authorization data for the current transaction includes at least time information of the current credit authorization, a random number of the current credit authorization, user account information, and a credit limit.

[0087] The credit authorization data is obtained from the remote server, and the time information of the current credit authorization further includes a current time and valid duration of the current credit authorization. Therefore, it can be determined when the current credit authorization starts and expires. If the current time is later than a time limit of the current credit authorization, a subsequent fee deduction is not allowed. The random number of the current credit authorization is a unique identifier of the current credit authorization, that is, each time the credit authorization is independent, and a new identifier is generated during each credit authorization, therefore each credit authorization can be distinguished. The user account information can further include an account ID of the user, a bank card number (credit card number) of the user, etc. The credit limit can be used to indicate an upper limit of a deducted amount of the current transaction, and if the deducted amount exceeds the upper limit, the transaction fails.

[0088] In an implementation of the present application, the collecting credit authorization data for a current transaction obtained by an intelligent terminal from a remote server further includes: scanning a barcode generated by the intelligent terminal based on the credit authorization data, to obtain the credit authorization data; or obtaining the credit authorization data from the intelligent terminal through wireless communication.

[0089] The barcode includes a two-dimensional barcode or a one-dimensional barcode, and the wireless communication includes NFC, RFID, Bluetooth, etc.

[0090] In an implementation of the present application, after the collecting credit authorization data for a current transaction obtained by an intelligent terminal from a remote server, the method further includes: performing one or more of the following

operations to verify the credit authorization data: comparing time information included in the credit authorization data with a current time, and if the current time is later than the time information included in the credit authorization data, determining that the credit authorization data has expired, and canceling the current transaction; determining whether a random number included in the credit authorization data exists in previous transaction data; and if yes, determining that the credit authorization data is repeatedly used, and canceling the current transaction; and determining whether an amount of the current transaction exceeds a credit limit included in the credit authorization data, and if yes, canceling the current transaction.

[0091] In the previously described step, the credit authorization data can exclude time information, and the credit authorization data is obtained by the intelligent terminal all at once and can be used for a period of time, such as one week or one month. Only the credit limit needs to be verified during a fee deduction, and the credit authorization data stored in the intelligent terminal will be modified (progressively decreased) after a fee deduction (data interaction is usually performed through wireless communication, and the intelligent terminal is notified of a deducted amount). If the credit limit is reduced to 0 or lower than a threshold, the credit authorization data cannot be used for transactions.

[0092] In an implementation of the present application, the collected credit authorization data for the current transaction obtained by the intelligent terminal from the remote server further includes signature information used by the remote server to sign the credit authorization data by using a private key; and

after the collecting credit authorization data for a current transaction obtained by an intelligent terminal from a remote server, but before the recording the credit authorization data and data of the current transaction, the method further includes:

verifying the signature information by using a public key pre-obtained from the remote server, and determining whether the credit authorization data is sent by the remote server, where if yes, the credit authorization data and the data of the current transaction are recorded.

[0093] In this implementation, the authorization data obtained by the intelligent terminal from the remote server can be temporary or one-time (for example, one-time authorization that is valid for a certain period of time).

[0094] In the method in this implementation of the present application, the fee deduction terminal can quickly complete a payment transaction without accessing a

network even when a user is not using bank cards. Credit authorization data is temporarily generated during each transaction and therefore cannot be reused. As such, problems existing in the current technology, such as financial losses caused by a leak of information associated with magnetic stripe bank cards can be alleviated.

[0095] FIG. 8 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application. An offline payment process between an intelligent terminal and a fee deduction terminal after the intelligent terminal obtains credit authorization data is illustrated in FIG. 8. The method includes the following steps:

[0096] Step 801: Obtain credit authorization data for a current transaction of a user from a remote server.

[0097] Step 802: Provide the credit authorization data for a fee deduction terminal, so that the fee deduction terminal performs processing based on the credit authorization data.

[0098] In an implementation of the present application, the obtaining credit authorization data for a current transaction of a user from a remoter server further includes: sending a unique identifier of the user to the remote server; and receiving credit authorization data that includes user account information and that is generated by the remote server based on the unique identifier.

[0099] The identifier can be a user name such as a user ID, a device identifier of the intelligent terminal, or a combination of both.

[0100] In the present step, the intelligent terminal can communicate with the remote server through a network to obtain the credit authorization data that includes user account information, so that a delay of connection to the network during a transaction between the fee deduction terminal and each intelligent terminal can be reduced. The user account information included in the credit authorization data can be a bank card number, a telephone number, etc.

[0101] In an implementation of the present application, the credit authorization data can further include time information of current credit authorization, a random number of the current credit authorization, and a credit limit.

[0102] FIG. 9 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application. A work process of a remote server in the offline payment method is illustrated in FIG. 9. The method includes the following steps:

[0103] Step 901: Obtain a credit authorization request sent by a user through an intelligent terminal.

[0104] Step 902: Send credit authorization data for a current transaction of the user to the intelligent terminal based on the credit authorization request from the intelligent terminal.

[0105] In an implementation of the present application, the credit authorization request includes a unique identifier of the user, and the sending credit authorization data for a current transaction of the user to the intelligent terminal includes: generating credit authorization data including user information based on the unique identifier, and sending the credit authorization data for the current transaction of the user to the intelligent terminal.

[0106] In an implementation of the present application, the sending credit authorization data for a current transaction of the user to the intelligent terminal includes: encrypting the user information, signing the credit authorization data by using a private key, and delivering signature information and the credit authorization data to the intelligent terminal by using a password.

[0107] After the credit authorization data is signed by using the private key in the present step, the fee deduction terminal needs to verify a signature of the credit authorization data by using a public key, that is, the fee deduction terminal needs to verify whether the credit authorization data is sent by the remote server. User account information needs to be encrypted because it is insecure to store the user account information in the fee deduction terminal. For an encryption method, refer to the method in the existing technology, and details are not described here.

[0108] The steps in FIG. 7, FIG. 8, and FIG. 9 can be combined to implement credit payment. When making a payment, the process can be actively initiated by the intelligent terminal or the fee deduction terminal. For example, in a scenario where making payment for bus tickets, an NFC device of an intelligent terminal and an NFC device of a fee deduction terminal on a bus can interact with each other, and the fee deduction terminal can initiate a payment process by using the NFC device, that is, the fee deduction terminal can initiate a payment request and then obtain authorization data from the intelligent terminal to complete payment. For another example in the same scenario, the fee deduction terminal on the bus can use a barcode scanning device to scan a two-dimensional barcode displayed on the intelligent terminal held by the user to initiate a payment process.

[0109] FIG. 10 is a schematic diagram illustrating a fee deduction terminal, according to an implementation of the present application. The fee deduction terminal in FIG. 10 can include a POS machine, a smartphone, etc, and functional units of the fee deduction terminal can be implemented by using a logic circuit, a chip, or a high-performance computer.

[0110] The fee deduction terminal includes: a collection unit 1001, configured to collect credit authorization data for a current transaction obtained by an intelligent terminal from a remote server; and a recording unit 1002, configured to record the credit authorization data and data of the current transaction.

[0111] In an implementation of the present application, the fee deduction terminal further includes a check unit 1003, configured to check the credit authorization data and the data of the current transaction with the remote server at a predetermined time.

[0112] In an implementation of the present application, the credit authorization data for the current transaction includes at least time information of current credit authorization, a random number of the current credit authorization, user account information, and a credit limit.

[0113] In an implementation of the present application, the collection unit further includes a scanning module 1004, configured to scan a barcode generated by the intelligent terminal based on the credit authorization data, to obtain the credit authorization data; or the collection unit further includes a wireless communication module 1005, configured to obtain the credit authorization data from the intelligent terminal through wireless communication.

[0114] In an implementation of the present application, the barcode includes a one-dimensional barcode and/or a two-dimensional barcode, and the wireless communication includes NFC or RFID.

[0115] In an implementation of the present application, the fee deduction terminal further includes a verification unit 1007, configured to perform one or more of the following operations to verify the credit authorization data:

comparing time information included in the credit authorization data with a current time, and if the current time is later than the time information included in the credit authorization data, determining that the credit authorization data has expired, and canceling the current transaction;

determining whether a random number included in the credit authorization data

exists in previous transaction data; and if yes, determining that the credit authorization data is repeatedly used, and canceling the current transaction; and

determining whether an amount of the current transaction exceeds a credit limit included in the credit authorization data, and if yes, canceling the current transaction.

[0116] In an implementation of the present application, the collected credit authorization data for the current transaction obtained by the intelligent terminal from the remote server further includes signature information used by the remote server to sign the credit authorization data by using a private key, and the fee deduction terminal further includes: a signature verification unit 1006, configured to: verify the signature information by using a public key pre-obtained from the remote server, and determine whether the credit authorization data is sent by the remote server, where if yes, the recording unit records the credit authorization data and the data of the current transaction.

[0117] FIG. 11 is a schematic diagram illustrating an intelligent terminal, according to an implementation of the present application. A structure of the intelligent terminal for achieving the offline payment purpose of the present application is illustrated in FIG. 11. Certainly, the intelligent terminal can further include other essential parts such as a touchscreen, a battery, a memory, or a circuit board, and details are not described here. The intelligent terminal can be a smartphone, a tablet computer, an intelligent wearable device, etc.

[0118] The intelligent terminal includes: an acquisition unit 1101, configured to obtain credit authorization data for a current transaction of a user from a remote server; and a communication unit 1102, configured to provide the credit authorization data for a fee deduction terminal, so that the fee deduction terminal performs processing based on the credit authorization data.

[0119] In an implementation of the present application, the acquisition unit is further configured to: send a unique identifier of the user to the remote server, and receive credit authorization data that includes user account information and that is generated by the remote server based on the unique identifier.

[0120] In an implementation of the present application, the credit authorization data further includes time information of current credit authorization, a random number of the current credit authorization, and a credit limit.

[0121] FIG. 12 is a schematic diagram illustrating a remote server, according to the present application. A structure of the remote server for achieving the offline

payment purpose of the present application is illustrated in FIG. 12. Certainly, the remote server can further include other essential parts such as an input/output device, a communication unit, a power supply, a memory, or a circuit board, and details are not described here. The remote server can be a high-performance computer or a computer cluster.

[0122] The remote server includes: an acquisition unit 1201, configured to obtain a credit authorization request sent by a user through an intelligent terminal; and a processing unit 1202, configured to send credit authorization data for a current transaction of the user to the intelligent terminal based on the credit authorization request from the intelligent terminal.

[0123] In an implementation of the present application, the credit authorization request includes a unique identifier of the user, and the processing unit is configured to: generate credit authorization data including user information based on the unique identifier, and send the credit authorization data for the current transaction of the user to the intelligent terminal.

[0124] In an implementation of the present application, that the processing unit sends credit authorization data for a current transaction of the user to the intelligent terminal includes: encrypting the user information, signing the credit authorization data by using a private key, and delivering signature information and the credit authorization data to the intelligent terminal by using a password.

[0125] FIG. 13 is a schematic diagram illustrating an offline credit payment system, according to an implementation of the present application. A structure of the offline payment system is illustrated in FIG. 13. In this implementation, an intelligent terminal can include a smartphone, a tablet computer, etc. A fee deduction terminal can include a POS machine, a smartphone, etc. A remote server can include a high-performance computer, etc.

[0126] The offline credit payment system includes a remote server 1301, an intelligent terminal 1302, and a fee deduction terminal 1303.

[0127] The remote server 1301 is configured to send credit authorization data for a current transaction of a user to the intelligent terminal based on a credit authorization request from the intelligent terminal.

[0128] The intelligent terminal 1302 is configured to obtain the credit authorization data from the remote server.

[0129] The fee deduction terminal 1303 is configured to: collect the credit

authorization data from the intelligent terminal, and record the credit authorization data and data of the current transaction.

[0130] In the system in this implementation of the present application, the fee deduction terminal can quickly complete a fee deduction transaction without accessing a network even when a user is not using bank cards. Credit authorization data is generated temporarily during each transaction and therefore cannot be reused. As such, problems existing in the current technology, such as financial losses caused by a leak of information associated with magnetic stripe bank cards can be alleviated.

[0131] FIG. 14 is a flowchart illustrating an offline credit payment method, according to an implementation of the present application. In FIG. 14, a fee deduction terminal is a POS machine, an intelligent terminal is a mobile phone, and a remote server is a high-performance computer. The high-performance computer can generate credit authorization data and complete account reconciliation with the POS machine. Certainly, generation of the credit authorization data and the account reconciliation can be implemented by two or more high-performance computers. However, for simplicity, in this implementation, only one remote server is configured to complete the described two services. The method includes the following steps:

[0132] Step 1401: A credit payment client on a mobile phone registers with a remote server.

[0133] The registration process includes verifying a user identity, verifying a financial account, etc. For example, identity card information, credit card information, or bank card information of a user is verified. The remote server generates a private key based on the user identity or the financial account, and the private key is used to sign the credit authorization data later.

[0134] The credit payment client can be a software application, or be embedded in a security chip (for example, an eSE security chip) of the mobile phone.

[0135] The POS machine is also registered with the remote server, and the remote server delivers a public key to the POS machine. The public key is used by the POS machine to verify a signature of the credit authorization data later.

[0136] Step 1402: The credit payment client initiates a request of generating the credit authorization data to the remote server by using a radio frequency communication unit (or a WiFi network) of the mobile phone.

[0137] TOKEN (not illustrated) is used in the offline payment method described in the accompanying drawing is a token used when the mobile phone communicates

with the remote server in the existing technology.

[0138] The request can further include information such as an international mobile equipment identity (IMEI) of the mobile phone or a user identity, so that the remote server can uniquely identify a user initiating the request.

[0139] Step 1403: The remote server generates the credit authorization data based on the request.

[0140] In the present step, the remote server matches corresponding financial account information of the user based on the user identity or the IMEI in the request, and obtains user information. The financial account information can include information such as a credit limit, and the user information can include a user identity, a bank card number, a private key, etc.

[0141] The remote server generates time information included in the credit authorization data, and the time information further includes a current time, that is, a start time of the credit authorization data used during a current transaction, and obtains predetermined validity duration. The remote server further generates a random number, and the random number is used to uniquely identify the credit authorization data.

[0142] The remote server generates the credit authorization data based on the time information, the random number, and the user information and the financial account information obtained in the previous step.

[0143] The remote server can further encrypt information such as the user identity or the bank card number (or the information can be encrypted on the intelligent terminal), and use the private key to sign the credit authorization data, to ensure authenticity of the data.

[0144] In the present step, the remote server can further make a determination based on a consumption payment record and the credit limit of the user. If the consumption payment record of the user is close to or exceeds the credit limit in the financial account information, the credit authorization request is rejected, and a failure reason is fed back to the credit payment client on the mobile phone.

[0145] Step 1404: The remote server integrates the credit authorization data to the TOKEN, and delivers the TOKEN to the credit payment client on the mobile phone.

[0146] Step 1405: The credit payment client generates a two-dimensional barcode based on the credit authorization data.

[0147] The two-dimensional barcode generated in the present step can be displayed on a screen of the mobile phone, or stored in a memory of the mobile phone for use during the current transaction.

[0148] Step 1406: A scanning module of a POS machine obtains the two-dimensional barcode through scanning.

[0149] A barcode scanning device in the existing technology can be used to scan the two-dimensional barcode in the present step, and data and control interfaces of the device are connected to the POS machine, so that the POS machine can control the scanning device to complete a scanning task and return scanned barcode data.

[0150] The POS machine in the present application can be a POS machine installed with a fee deduction client, or a POS machine with a data processing capability. The fee deduction client is installed on the terminal, to perform subsequent parsing, recording, etc.

[0151] Step 1407: A fee deduction client on the POS machine parses the two-dimensional barcode to obtain the credit authorization data.

[0152] In the present step, the fee deduction client can verify the signature of the credit authorization data by using the public key, thereby verifying that the credit authorization data is from the remote server.

[0153] The fee deduction client can further parse (or decrypt) the financial account information in the credit authorization data, that is, the credit limit of the current transaction.

[0154] Step 1408: The fee deduction client processes a current payment transaction based on the credit authorization data.

[0155] The processing in the present step can include: parsing the time information in the credit authorization data, and determining whether a time of the current payment transaction is later than the current time plus the validity duration in the credit authorization data. If yes, the credit authorization data has expired and therefore cannot be used for the current payment transaction, and the credit payment client can be instructed to generate new credit authorization data for the current payment transaction.

[0156] Whether the random number in the credit authorization data has been used in a previous transaction is determined. If no, the credit authorization data is usable. If yes, duplicate payment may have occurred. Then the credit payment client can be instructed to generate new credit authorization data for the current payment

transaction.

[0157] Whether an amount of the current payment transaction exceeds the credit limit is determined. If yes, the current payment transaction fails and a failure reason is returned to the credit payment client.

[0158] The above-mentioned operations can be performed in any sequence, or only one or more of the operations can be performed, or other logical judgment or processing can be performed.

[0159] Step 1409: The fee deduction client records current fee deduction.

[0160] The fee deduction record includes the amount of the current payment transaction and the credit authorization data.

[0161] The amount of the current payment transaction and the credit authorization data recorded by the fee deduction client in the present step can be stored in the POS machine. If the POS machine includes a processing device such as a computer, the current transaction amount and the credit authorization data can be stored in a disk of the computer, or another reliable memory (for example, through network backup storage).

[0162] The recorded credit authorization data can be all information included in the previously described credit authorization data, or can be user information. In the processing step of the fee deduction client, the encrypted user information is not decrypted. Only the encrypted user information is recorded to further ensure the security of the user information.

[0163] The fee deduction record can further include content such as merchant information, for example, a merchant ID, a type of the payment transaction, or merchandise information.

[0164] In this case, the current payment transaction of the user is completed. If the POS machine is corresponding to a transportation gate, the gate can be opened to allow passengers to pass through. If the POS machine is used for consumption, it can notify the merchant that the current payment is completed. The financial account of the user does not change, the payment was made by credit payment, and the POS machine of the merchant does not need to communicate with the remote server to complete fee deduction of the current payment transaction. As such, a time of the current payment transaction between the mobile phone of the user and the POS machine can greatly be shortened, and user payment efficiency can be improved.

[0165] Step 1410: The POS machine sends the fee deduction record to the remote

server at a predetermined time for checking.

[0166] The POS machine can possibly record multiple deduction records in a certain period of time, and transfers the multiple deduction records each time when performing account reconciliation with the remote server. The predetermined time can be 00: 00 every day in this example, and 00: 00 is an idle time of the POS machine. The POS machine sends the fee deduction records to the remote server through the network (a wired or wireless network). The fee deduction record includes the user information and the payment amount described in the previous steps. The remote server decrypts the user information to obtain the user identity and the bank card number, and deducts the payment amount from the bank card account, thereby successfully completing the payment process.

[0167] FIG. 15 is a flowchart illustrating another offline credit payment method, according to an implementation of the present application. A difference between the implementation in FIG. 15 and the implementation in FIG. 14 lies in that, in this implementation in FIG. 15, a credit payment client on a mobile phone sends credit authorization data to a POS machine by using an NFC communication module, instead of generating a two-dimensional barcode. Correspondingly, an NFC communication module of the POS machine in this implementation is configured to obtain the credit authorization data sent by the mobile phone. The POS machine further has a USB interface, and the USB interface is configured to store a fee deduction record in a removable memory.

[0168] Steps same as or similar to those in the implementation in FIG. 14 are not repeated here for simplicity, and only different steps are described.

[0169] Step 1505: A credit payment client of an intelligent terminal stores credit authorization data in a local memory, so that an NFC communication module can access the credit authorization data.

[0170] In an optional implementation, the intelligent terminal end does not need to obtain credit authorization data during each time of credit payment, and the credit authorization data is stored in the credit payment client of the intelligent terminal for repeated credit payment after being generated by a remote server.

[0171] Step 1506: By using an NFC communication module, a fee deduction client of a POS machine communicates with the NFC communication module of the intelligent terminal, to obtain the credit authorization data from the credit payment client.

[0172] Step 1507: The fee deduction client parses the credit authorization data obtained by using the NFC communication module.

[0173] A signature of the received credit authorization data is verified by using a public key sent by the remote server, and the credit authorization data is obtained through decryption.

[0174] Step 1508: The fee deduction client processes a current payment transaction based on the credit authorization data.

[0175] Optionally, in the present step, the fee deduction client determines whether a credit limit included in the credit authorization data satisfies current consumption. If yes, the current consumption is subtracted from the credit limit, and a remaining credit limit is returned to the mobile phone by using the NFC communication module. The credit payment client on the mobile phone changes the credit limit included in the locally stored credit authorization data to the remaining credit limit, so that the remaining credit limit is used as a new credit limit for next credit payment.

[0176] Certainly, time information included in the credit authorization data can be deleted or can be a relatively long time, so that the credit authorization data can be used for repeated credit payment.

[0177] Step 1509: The fee deduction client records current fee deduction on a removable hard disk by using a USB interface.

[0178] The fee deduction record includes an amount of the current payment transaction and the credit authorization data.

[0179] Step 1510: The POS machine sends the fee deduction record to the remote server at a predetermined time for checking.

[0180] In the method and the system in the implementations of the present application, when a user does not use a bank card for payment, the fee deduction terminal can quickly complete a fee deduction transaction without accessing a network. Credit authorization data is temporarily generated during each transaction and therefore cannot be reused. As such, financial losses incurred by an information leak can be avoided for users who use magnetic stripe bank cards in the existing technology.

[0181] For technical improvements, one can distinguish between a hardware improvement (for example, an improvement in circuit structures of a diode, a transistor, a switch, etc.) and a software improvement (an improvement in a method

process). However, as technologies develop, improvements in many current method processes can be considered as a direct improvement in a hardware circuit structure. Almost all designers obtain corresponding hardware circuit structures by programming improved method processes to hardware circuits. Therefore, it cannot be said that the improvement in a method process cannot be implemented by using a hardware entity module. For example, a programmable logic device (PLD), such as a field programmable gate array (FPGA), is such an integrated circuit whose logic function is determined by programming a device by a user. A designer performs programming to "integrate" a digital system to a single PLD, without requiring a chip manufacturer to design and manufacture a dedicated integrated circuit chip 2. In addition, at present, instead of manually manufacturing an integrated chip, this type of programming is mostly implemented by using "logic compiler" software. The programming is similar to a software compiler used to develop and write a program. Original code needs to be written in a particular programming language for compilation. The language is referred to as a hardware description language (HDL). There are many HDLs, such as the Advanced Boolean Expression Language (ABEL), the Altera Hardware Description Language (AHDL), Confluence, the Cornell University Programming Language (CUPL), HDCal, the Java Hardware Description Language (JHDL), Lava, Lola, MyHDL, PALASM, and the Ruby Hardware Description Language (RHDL). The very-high-speed integrated circuit hardware description language (VHDL) and Verilog2 are most commonly used. It should also be clear to a person skilled in the art that a hardware circuit of a logic method process can be easily obtained by performing logic programming on the method process through several earlier described hardware description languages and programming the method process to an integrated circuit.

[0182] A controller can be implemented in any appropriate way. For example, the controller can take the form of, for example, a microprocessor or a processor and a computer-readable medium storing computer-readable program code (such as software or firmware) that can be executed by the microprocessor or the processor, a logic gate, a switch, an application specific integrated circuit (ASIC), a programmable logic controller, and an embedded microcontroller. Examples of the controller include, but are not limited to, the following microcontrollers: ARC 625D, Atmel AT91SAM, Microchip PIC18F26K20, and Silicone Labs C8051F320. A memory controller can also be implemented as a part of control logic of a memory.

[0183] A person skilled in the art also know that, in addition to implementing the controller by using the computer-readable program code, logic programming can be performed on method steps to allow the controller to implement the same function in forms of the logic gate, the switch, the programmable logic controller, the programmable logic controller, and the embedded microcontroller. Therefore, such a controller can be considered as a hardware component. An apparatus included in the controller and configured to implement various functions can be considered as a structure in the hardware component. Or, the apparatus configured to implement various functions can even be considered as both a software module implementing the method and a structure in the hardware component.

[0184] The system, apparatus, module or unit illustrated in the earlier described implementations can be implemented by a computer chip or an entity, or can be implemented by a product having a certain function.

[0185] For ease of description, the apparatus is described by dividing the functions to various units. Certainly, when the present application is implemented, the functions of all units can be implemented in one or more pieces of software and/or hardware.

[0186] It can be seen from description of the implementations that, a person skilled in the art can clearly understand that the present application can be implemented by using software in addition to a necessary universal hardware platform. Based on such an understanding, the technical solutions in the present application essentially or the part contributing to the existing technology can be implemented in a form of a software product. The software product can be stored in a storage medium, such as a ROM/RAM, a magnetic disk, or an optical disc, and includes several instructions for instructing a computer device (a personal computer, a server, or a network device) to perform the methods described in the implementations or in some parts of the implementations of the present application.

[0187] The implementations in the present specification are described in a progressive way. For same or similar parts in the implementations, reference can be made to each other. Each implementation focuses on a difference from other implementations. Particularly, a system implementation is similar to a method implementation, and therefore, is described briefly. For related parts, refer to partial descriptions in the method implementation.

[0188] The present application can be used in many general-purpose or dedicated

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 consumer digital device, a network PC, a minicomputer, a mainframe computer, and a distributed computing environment including any one of the earlier described systems or devices.

[0189] The present application can be described in the general context of an executable computer instruction executed by a computer, for example, a program module. Generally, the program module includes a routine, a program, an object, a component, a data structure, etc. for executing a particular task or implementing a particular abstract data type. The present application can also be practiced in distributed computing environments. In the distributed computing environments, tasks are performed 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.

[0190] The present application is described through implementations. However, a person of ordinary skill in the art knows that many modifications and variations of the present application can be made without departing from the spirit of the present application. It is intended that the claims include these modifications and variations without departing from the spirit of the present application.

CLAIMS

1. A method comprising the steps of:

receiving at a fee deduction terminal, credit authorization data from a mobile terminal by scanning a two-dimensional code, the credit authorization data comprising a random number, wherein the random number is a unique identifier to distinguish the credit authorization data from previous credit authorization data, and wherein the credit authorization data is generated by a remote server;

processing at the fee deduction terminal, a payment transaction based on the credit authorization data to ensure that the random number does not match that of any previous credit authorization data; and

approving offline at the fee deduction terminal, the payment transaction and recording the payment transaction at the fee deduction terminal.

2. The method of claim 1 further comprising the step of:

sending online from the fee deduction terminal to the remote server at a predetermined time, the payment transaction and the credit authorization data, so that the remote server can perform a deduction from an account of a user based on the payment transaction.

3. The method of claim 2 wherein the payment transaction and the credit authorization data, and previous payment transactions and previous credit authorization data, are periodically sent from the fee deduction terminal to the remote server in batches.

4. The method of any one of the preceding claims wherein the credit authorization data further comprises a validity period and a credit limit, and wherein the step of processing at the fee deduction terminal, a payment transaction based on the credit authorization data further comprises the steps of:-

ensuring that the validity period has not yet expired; and

ensuring that an amount of the payment transaction does not exceed the credit limit.

5. The method of any one of the preceding claims wherein the credit authorization data is signed by the remote server using a private key and wherein the step of processing at the fee deduction terminal, a payment transaction based on the credit authorization data further comprises the step of:-

verifying signature information at the fee deduction terminal, by signing the credit authorization data with a public key which matches the private key to ascertain that the credit authorization data was generated by the remote server.

6. The method of any one of the preceding claims wherein the fee deduction terminal receives the credit authorization data from the mobile terminal via wireless communication.

7. The method of claim 6 wherein the wireless communication is near field communication (NFC) or radio frequency identification (RFID) or Bluetooth.

8. An apparatus comprising a plurality of modules configured to perform the method of any one of claims 1 to 7.