

METHOD FOR IMPLEMENTING CIRCLE STORE IN THE AIR AND DEVICE THEREOF

Technical Field

The present invention relates to the e-banking field; and more particularly, the present invention relates to a method for implementing circle store in the air by means of a mobile communication device such as a mobile phone, and also relates to a key device thereof – an SIM card that supports the circle store business.

Description of Related Art

Introduction of computers and communication technologies has led to revolutionary changes in the financial sector. On basis of the banking electronization, banks now also provide their clients with various value-added financial information services, a representative one of which is digital money.

Digital money is a general term of various electronic payment means that allow for repeated value storing and prepayment, according to which a digital money holder pays traditional money to a bank, and the issuer converts information of the equivalent cash value into a digital signal to be stored in a storage medium of the holder in an electric, magnetic or optical form. Digital money has the following transaction process: a sum of money from a bank account is circle stored as digital money and transferred from the bank account to a digital money account, and then transactions can be made directly with the digital money without involvement of the bank.

Currently, the main storage media used as digital money carriers are various smart cards, such as the popular public transport IC cards, one-campus-ID cards, and dedicated PBOC electronic passbooks/electronic purses. Transactions using smart cards are very convenient, time saving and safe. However, as more and more industries and fields are adopting the smart cards, smart cards hold by users are also increasing in number, which causes inconveniences to the users in bringing so many cards with them. Furthermore, when contactless smart cards are swiped, multiple cards may enter a same radio frequency (RF) field to cause conflict

therebetween, thereby increasing the risk and convenience in use of the cards.

Mobile phones have gradually become mobile information terminals that are carried about by almost everyone. As a kind of smart cards, SIM cards within the mobile phones may be used directly to recognize users' identities. Therefore, in the future, it is possible for digital money to be integrated with such mobile communication devices as mobile phones and personal digital assistants (PDAs) to solve the cash flow problem in future e-commerce. In this way, a user only needs to carry his or her mobile phone or PDA for various transactions when going shopping, which renders the transactions safer and more convenient. Unfortunately, for reasons of safety and technologies, current mobile communication devices including mobile phones are still unable to directly implement the fundamental digital money function of implementing circle store in the air.

BRIEF SUMMARY OF THE INVENTION

An objective of the present invention is to provide a method for implementing circle store in the air by means of a mobile communication device such as a mobile phone. By implementing circle store in the air in a safe and accurate way, this method lays the foundation for using mobile communication devices such as mobile phones as a digital money tool.

Another objective of the present invention is to provide an SIM card that supports circle store businesses. This mobile phone SIM card is the key device that ensures safety of the method for implementing circle store in the air.

To this end, the present invention adopts the following technical solutions:

An SIM card for implementing circle store in the air, being characterized in that:

The SIM card has an SIM module for telecom businesses and a payment system environment module for digital money businesses, wherein the SIM module has a SIM Tool Kit (STK) function;

The payment system environment module comprises a payment system environment catalog module and at least one application definition module, wherein elementary files related to respective applications are configured in the at least one application definition module, and

information of the application definition module is stored in the payment system environment catalog module, wherein the SIM module is configured to communicate with the payment system environment module via the STK.

Preferably, the SIM card has a contact interface and a contactless interface, wherein the SIM module for telecom businesses implements telecom business communications via the contact interface, and the payment system environment module implements digital money business communications via the contactless interface.

Preferably, the application definition module at least comprises an application definition module for electronic purse/electronic passbook businesses.

Preferably, the SIM module for telecom businesses is one of a SIM card, a UIM card, a PIM card or a USIM.

A method for implementing circle store in the air, which is implemented by the aforesaid SIM card, wherein the SIM card is installed in a mobile communication terminal, the method being characterized in that:

(1) a holder of the mobile communication terminal initiates a circle store operation, inputs a transaction amount, and sends a circle store initialization instruction to a card operation system via the STK; and after the card operation system returns the corresponding data, a circle store request short message is sent by the STK to a server;

(2) after receiving the circle store request short message, the server performs an authentication, deducts the circle store fund from the corresponding account and sends a command short message of performing the circle store to the SIM card;

(3) after the SIM card receives the command short message of performing the circle store, a circle store instruction is sent by the STK to the card operation system; then the card operation system performs an authentication, adds money to the electronic purse and returns the corresponding data to the STK, which then sends a circle store result short message to the server;

(4) after receiving the circle store result short message, the server authenticates it and saves

the authentication information.

Preferably, in step (1), the circle store request short message is re-sent manually to ensure that it is received by the server.

Preferably, in step (1), when the STK is sending the circle store request short message, information of the previous circle store is added into the data so that the server can confirm the result of the last transaction.

Preferably, the information of the previous circle store comprises any of the following: the result of the last transaction, the serial number of the last on-line transaction, date and time of the last transaction, balance of the last transaction and authentication information of the last transaction.

Preferably, in step (2), if the server does not receive confirmation information from the mobile communication terminal within a predetermined time, the command short message of performing the circle store will be re-sent automatically.

Preferably, in step (2), if the server receives a repeated packet, then the server detects if a transaction status in the repeated packet indicates that the transaction has been completed. If it has not, the circle store command short message is re-sent; otherwise, the repeated packet is ignored.

Preferably, in step (4), if the server receives error information, a backoff measure will be taken to reimburse the amount deducted.

Preferably, when the card operation system is executing the instruction issued by the STK, the write operations on the non-volatile memory are either all successful or all keep the values unchanged.

Preferably, when the SIM card is performing the circle store in the air, a contactless transaction may be made in the interval between completion of step (1) and commencement of step (3), and the flow process of the circle store in the air ceases when the contactless transaction is being made.

Preferably, an MAC authentication code is calculated according to content of the

uplink/downlink short messages and a corresponding key, and the MAC authentication code is sent together with and following the short messages.

Instead of using special financial equipment such as a circle store machines located at a specific location in case of a traditional electronic passbook/electronic purse, the method for implementing circle store in the air by using a mobile communication device such as a mobile phone disclosed in the present invention may accomplish a circle store operation completely through the STK function of the mobile phone, thereby making it more convenient to use.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Hereinafter, the present invention will be described in more detail with reference to the attached drawings and embodiments thereof, wherein:

Fig. 1 is a schematic view of a basic framework of a dual interface telecom smart card with a payment function used in the present invention;

Fig. 2 is a schematic structure of another implementation of the dual interface telecom smart card shown in Fig. 1;

Fig. 3 is a basic flowchart of a circle store transaction process; and

Fig. 4 is a schematic view of a communication protection mechanism adopted in the circle store transaction process.

DETAILED DESCRIPTION OF THE INVENTION

For financial businesses, safety of transactions is always the primary concern. Therefore, mobile communication devices serving as digital money carriers shall be retrofitted in two respects: one is to enhance the safety thereof to meet the strict requirements on transaction safety when the mobile communication devices are used directly for financial businesses; the other is to simplify relevant operations in consideration of features of the circle store business, thereby facilitating implementation of the circle store in the air through limited operations.

To meet the above requirements, SIM cards of mobile phones used for the circle store in the air are in form of a dual interface telecom smart card with a payment function. The dual interface telecom smart card with the payment function, which is the key device for

implementing the circle store in the air in the present invention, has two interfaces: namely, a contact interface and a contactless interface that accomplish electrical signal connection via an antenna or contacts respectively. The contact interface may be equipped with an SIM card commonly found in current mobile phones to implement mobile communication functions including STK, while the contactless interface may be provided with a functional unit that supports digital money functions so that financial transactions such as the mobile purse and the mobile passbook can be implemented through the mobile phone.

Hereinbelow, a basic structure of the dual interface telecom smart card with the payment function will be described in detail with reference to Fig. 1. As shown in Fig. 1, to enable financial applications including the electronic purse, the dual interface telecom smart card is further provided with a payment system environment module in addition to the traditional SIM card for telecom services. The payment system environment module is just the aforesaid functional unit that supports digital money functions, and will be selected automatically by the contactless interface when the contactless interface is powered on.

In Fig. 1, the payment system environment module is separate from the MF (Main File) module used for telecom businesses, and communications therebetween may be accomplished via the STK. In the payment system environment module, a payment system environment catalogue module and a plurality of ADF (Application Definition) modules are included, in which the payment system environment catalogue module specifies what payment applications the payment system environment module can support. In the dual interface telecom smart card with the payment function, each concrete payment application is provided with one ADF module where various EFs (Elementary Files) related to the corresponding payment application are configured. Each of the ADF modules is configured in the payment system environment module, with respective information being stored in the payment system environment catalogue module.

As shown in Fig. 2, the payment system environment module also has another implementation, in which the payment system environment module is integrated with the MF

module. The payment system environment catalogue module and the ADF modules are connected with the payment system environment module respectively.

Further included in the dual interface telecom smart card are an EF_ICC module, a DF_GSM module, a DF_Telecom module, an EFKEY module and the like functional modules that support telecom businesses. These functional modules, together with the MF module, consist of a subscriber identity module for telecom businesses. As a standard communication functional module of the SIM card, this module is already well known to those of ordinary skill in the communication field, and thus will not be further described herein.

In the present invention, the respective ADF modules are configured as per the Specifications of Electronic Purses/Electronic Passbooks promulgated by the People's Bank of China (PBOC), so as to meet particular clauses in respect of implementing electronic purses/electronic passbooks in smart cards as specified in the Specifications.

The dual interface telecom smart card with the payment function may implement digital money services by way of contactless transactions or data short messages.

In case of the contactless transactions, initially, a contactless terminal accesses the card via the contactless interface of the card, and when being powered on, the card is redirected automatically to the payment system environment module DDF. Of course, the terminal may also send a Select instruction to select the payment system environment module. The terminal may determine applications supported by the card by reading the payment system environment catalogue module, and then select ADFs of different applications through the Select instruction.

If it is desired to perform the electronic purse/electronic passbook application, the contactless terminal may select this application through the electronic purse/electronic passbook ADF module. Once this application is selected, the electronic purse/electronic passbook transaction can be made, a specific transaction process of which is just the same as that specified in the PBOC Specifications of Electronic Purses/Electronic Passbooks.

Apart from performing common electronic purse/electronic passbook transactions in the contactless transaction approach as described above, the dual interface telecom smart card with

the payment function may also support the STK function in a mobile phone or transactions in the air via data short messages. Now, with the circle store in the air as an example, steps of using the dual interface telecom smart card with the payment function to implement the circle store in the air by means of data short messages will be described in detail.

As shown in Fig. 3, the whole circle store transaction process entails three short message transmissions in total.

Initially, a holder of the mobile phone initiates a circle store operation in the mobile phone and inputs a subscriber password. Subsequent to the authentication, the user inputs the transaction amount, sends a circle store initialization command to the operation system of the card by organizing relevant data via the STK, so as to initialize a circle store process. After the operation system of the card returns corresponding data, the STK organizes relevant data and sends a circle store request to the server, which is called as the first short message. During the waiting process, the user may manually re-send this short message to the server if he or she feels that the waiting time is too long.

Upon receiving the first short message from the dual interface telecom smart card with the payment function, the server validates MAC1 according to the corresponding data, generates MAC2 and deducts the circle store funds from the corresponding account. Then the server sends a command of performing the circle store to the dual interface telecom smart card with the payment function, which is called as the second short message.

The aforesaid MAC authentication code is calculated according to the content of the uplink and downlink short messages and associated keys. The authentication code is appended to the end of the data short messages to ensure accuracy and integrity of the whole data short messages. If the content of the short messages needs to be encrypted, corresponding encryption operations may also be performed on each of the short messages.

If the server fails to receive confirmation information from the mobile phone within a certain period, this short message may be re-sent several times (the number of times may depend on practical needs). In this case, a problem arises: as the first short message may have been

re-sent several times, it is highly possible that the server will receive a repeated packet within the permissible storage time (e.g., three days) in the short message center. The server shall store records of the transaction short messages for each card according to the serial numbers, and when identical transaction short messages arise, they will be considered as repeated packets, and then the server will detect if the transaction status of this transaction indicates that the transaction has been completed. If it has not, the second short message will be re-sent; otherwise, this repeated packet will be ignored.

After the dual interface telecom smart card has received the second short message, the STK organizes relevant data and sends a circle store instruction to the operation system of the card. The operation system is responsible for authentication of MAC2, incrementing the on-line serial number by 1, adding money to the electronic purse, updating a list of the transactions in the air and generating transaction authentication information. Afterwards, the operation system returns corresponding data and a status word to the STK, and the STK then organizes relevant data to send a circle store result to the terminal, which is called as the third message. As this is the last short message, the dual interface telecom smart card has no way to know if this short message is lost. To solve the problem of the short message loss on rare occasions, the STK may, when sending the circle store request (the first short message) for each transaction, add to the data the result of the last transaction, the serial number of the last on-line transaction, date and time of the last transaction, balance of the last transaction and authentication information of the last transaction. Of course, some adjustments may also be made to the aforementioned information on the result of the last circle store so that the server can confirm the result of the last transaction.

After receiving the third short message, the server authenticates and saves the transaction authentication information. If an erroneous status word is received, the server will take a corresponding backoff measure to reimburse the amount deducted.

During the circle store in the air, a contactless transaction may be made by the dual interface telecom smart card in the interval between the time when the mobile phone holder

initiates the circle store operation and the time when the dual interface telecom smart card executes the circle store command. In this case, the process of the circle store in the air ceases and, when a next circle store is initiated, the server will be notified.

As loss of short messages or communication jamming is likely to occur during the circle store process, short messages are unreliable. Hence, to ensure successful completion of transactions, a special communication protection mechanism is adopted in the present invention. As shown in Fig. 4, the communication protection mechanism primarily comprises:

1. when the circle store request is initiated, a manual re-sending approach is adopted to guarantee receipt of the request by the server;
2. when the circle store instruction is executed, confirmation information will be re-sent several times if the server fails to receive it within a certain period;
3. when the circle store result is returned, the result of the last transaction will be carried when a next transaction is initiated to conclude the last transaction.

When the operation system of the card is executing the instruction from the STK, a power-off protection mechanism shall be enabled. In other words, the write operations on the non-volatile memory (e.g., EEPROM) in this instruction are atomic operations, which are either all successful or all keep the values unchanged. The STK is only responsible for organization of data and receipt/transmission of data short messages. In this way, the circle store transactions in the air can be surely terminated in case the mobile phone is powered off or running out of power during the process of implementing the circle store in the air.

For example, in case the mobile phone is powered off after sending the first short message and execution in the server is successful, the corresponding amount will be deducted and an instruction of implementing the circle store be sent. When the mobile phone is powered on again and receives the second short message (the instruction of implementing the circle store from the server end), the operation system of the card will determine that no transaction process is under way, store an error status word and associated information (the serial number of the on-line transaction, the date and time of the transaction, and balance of the transaction) as the

last item in the transaction-in-the-air record, and returns the error status word. Then the STK sends to the server end the error status word and the transaction record, according to which the server end determines that the transaction in the dual interface telecom smart card is unsuccessful and cancels the previous deduction of the amount.

In the above embodiment, the dual interface telecom smart card with the payment function is based on the basic framework of SIM cards. However, the present invention is not merely limited thereto. When the additional payment system environment module of the present invention is used, UIM cards for CDMA systems, PIM cards for Personal Handphone Systems, USIM cards for future 3G systems and the like can all use the method disclosed in the present invention to implement the circle store in the air.

The method for implementing circle store in the air and the device thereof disclosed in the present invention have been described above in detail. For those of ordinary skill in the art, any obvious changes thereto without departing from the spirit of the present invention shall constitute infringement on the scope of the present invention and be liable to corresponding legal responsibilities.

CLAIMS

1. A subscriber identity module (SIM) card for implementing circle store in the air, characterized in that:

the SIM card has an SIM module for telecom businesses and a payment system environment module for digital money businesses, the SIM module including a SIM Tool Kit (STK) function; and

the payment system environment module comprises a payment system environment catalog module and at least one application definition module, wherein elementary files related to respective applications are configured in the at least one application definition module, and information of the at least one application definition module is stored in the payment system environment catalog module, wherein the SIM module is configured to communicate with the payment system environment module via the STK.

2. The SIM card for implementing circle store in the air as claimed in Claim 1, characterized in that:

the SIM card has a contact interface and a contactless interface, wherein the SIM module for telecom businesses implements telecom business communications via the contact interface, and the payment system environment module implements digital money business communications via the contactless interface.

3. The SIM card for implementing circle store in the air as claimed in Claim 1, characterized in that:

the application definition module at least comprises an application definition module for electronic purse/electronic passbook businesses.

4. The SIM card for implementing circle store in the air as claimed in Claim 1, characterized in that:

the SIM module is one of a SIM card, a UIM card, a PIM card or a USIM.

5. A method for implementing circle store in the air, which is implemented by the SIM card as claimed in Claim 1, wherein the SIM card is installed in a mobile communication terminal, characterized in that:

(1) a holder of the mobile communication terminal initiates a circle store operation, inputs a transaction amount, and sends a circle store initialization instruction to a card operation system via the STK; and after the card operation system returns the corresponding data, a circle store request short message is sent by the STK to a server;

(2) after receiving the circle store request short message, the server performs an authentication, deducts the circle store fund from the corresponding account and sends a command short message of performing the circle store to the SIM card;

(3) after the SIM card receives the command short message of performing the circle store, a circle store instruction is sent by the STK to the card operation system; then the card operation system performs an authentication, adds money to the electronic purse and returns corresponding data to the STK, which then sends a circle store result short message to the server;

(4) after receiving the circle store result short message, the server authenticates it and saves the authentication information.

6. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

in step (1), the circle store request short message is re-sent manually to ensure that it is received by the server.

7. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

in step (1), when the STK is sending the circle store request short message, information of the previous circle store is added into the data so that the server can confirm the result of the last transaction.

8. The method for implementing circle store in the air as claimed in Claim 7, characterized in that:

the information of the previous circle store comprises any of the following: the result of the last transaction, the serial number of the last on-line transaction, date and time of the last transaction, balance of the last transaction and authentication information of the last transaction.

9. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

in step (2), if the server does not receive confirmation information from the mobile communication terminal within a predetermined time, the command short message of performing the circle store will be re-sent automatically.

10. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

in step (2), if the server receives a repeated packet, then the server detects if a transaction status in the repeated packet indicates that the transaction has been completed; if it has not, the circle store command short message is re-sent; otherwise, the repeated packet is ignored.

11. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

in step (4), if the server receives error information, a backoff measure will be taken to reimburse the amount deducted.

12. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

when the card operation system is executing the instruction issued by the STK, the write operations on a non-volatile memory are either all successful or all keep the values unchanged.

13. The method for implementing circle store in the air as claimed in Claim 5, characterized in that:

when the SIM card is performing the circle store in the air, a contactless transaction may be made in the interval between completion of step (1) and commencement of step (3), and the flow process of the circle store in the air ceases when the contactless transaction is being made.

14. The method for implementing circle store in the air as claimed in Claim 5, characterized in

that:

an MAC authentication code is calculated according to content of the uplink/downlink short messages and a corresponding key, and the MAC authentication code is sent together with and following the short messages.