Design and Implementation Mobile Payment Based on Multi-Interface of Mobile Terminal

ZHONG WAN WEIFENG YIN RONGGAO SUN
School of Computer Science and Information Technology
Zhejiang Wanli University
Ningbo, Zhejiang 315100
P. R. China
http://www.zwu.edu.cn

Abstract: - Resulting in the security of mobile payment are the two main problems of the mobile terminal itself and the process of wireless communication. As the mobile terminal's own unique portability, small size and low cost nature，it cause that the mobile terminal weak ability of computing encryption. The emergence of mobile phone virus is also a potential security threat to mobile payment. At the same time, the openness characteristic of wireless communication decide to a radio channel can be easily tapped by illegal user. Illegal user can tamper with, delete the intercepted information or pretend legal user to access communication networks to communication. This article presents a mobile payment implement solution with distributed key based on the current mobile multi-interface. Analyzes the workflow of mobile payment and the reasons that cause the security in the process of mobile payment. Uses the additional equipment to achieve the secret keys distributed storage to improve the ability of test and verify in system and enhance the computing encryption capability of mobile terminal. At the same time, based on the J2ME security architecture using the encryption methods of data encryption, digital signature, identity authentication to ensure the security of wireless communication. Gives the hardware design and software design of multi-interface data encryption equipment. And gives the some processes design of mobile client's software. This solution realizes the high security and low cost of mobile payment, has good applied value and marketable foreground.

Key-Words: - Payment Security; Mobile Payment; Data Encryption; Mobile Terminal; J2ME; Mobile interface

1 Introduction

In recent years, Mobile banking service, a kind of new comprehensive bank service that takes Mobile banking as representative, which is appearing in our life quietly, and changes our life with its powerful vitality.

People need personal financing any time and anywhere. The busy modern people have not enough time to in the area of personal financial management, and may not have enough time to line up to Handle relevance personal financial business in bank. People need the bank provide the modern trade service of "homes, self-management". This for the emergence of mobile banking provides a prerequisite of the market.

1.1 Mobile Banking Introduce

Mobile banking is also known as mobile phone bank. It is referred to as the using mobile phones for banking-related business. Mobile banking is as a channel to realize E-banking services for banks, and is a system of E-commerce services base on mobile communications network for banks.

At present, to realize mobile payment the best platform of mobile banking is mobile phone. According to the Ministry of Information Industry statistics, at the end of Nov 2006, the total number of mobile phone user is expected to reach 455,000,000 in China. Mobile banking business in such a huge user group support, if mobile banking is able to provide good financial services products, its market prospect is not in doubt. [1]

Mobile banking use the user mobile phone to connection the bank through the mobile communication network, and the use of the program that run on mobile phone to complete a variety of financial management business. Mobile banking is a product that combined with the development of electronic banking services and the development of the Internet and mobile communication technologies. From the traditional bank services at the counter to the mobile phone bank services, the application of new technologies are changing the bank's

competition rules in the banking industry. How to be able to provide customers with more convenient banking services is very important. The Bank broke through the limits of time and space using the Internet and mobile communications, and other high technologies. Not only changing the people's awareness of the bank, but also prompted the speed of bank's business innovation. Improved the service quality to customer and the convenience of services, and achieve its own development of bank.

At the same time, in accordance with the relevant survey, in the next few years later the number of the traditional bank's branch institution will significantly reduce, the number of Automatic Trader Machine (ATM) will be low growth rate. Customers need strongly the bank can be carried out the Services of detail of bank account and balance inquiries, transfers between accounts, in lieu of payment, remittance, the Securities Transfer, account management, such as foreign exchange trading using their own mobile phones anytime and anywhere. The one of the two new services that has most vitality and the future is the mobile banking. [2]

1.2 The Problems of Mobile Payment Face To

In the business spreading out of mobile banking, The security issues has become a key problem. How to protect the privacy of users and ensure the safe and reliable of transactions is very important. Mobile bank involves in a large number of financial transactions and capital flows and it has a great temptation to the malicious attacker. This attack is possible not only to caused customers of financial losses, but also to brought about the financial institutions huge economic the credibility damage.

According to the Communication Information newspaper reported in May 2005, a survey of more than 60 percent of Internet users indicated that they worry about the security of personal data and password using mobile banking. This is mainly because the mobile phone itself. With the embedded processor technology development, the handset's ability to deal with significantly strengthen. Comparing to personal computer, to mobile phone that most common user can affordable it's capacity for large number of mathematical functions handle is less. It lead to the mobile phone encryption capability is limited. So the most common mobile phones can not achieve the degree of encryption of E-banking and can not meet the requirements of financial security.

According to in the May 7, 2002 the IBM's researchers publish a report shows that a hacker use the Division of hacker attack technology can clone a mobile phone SIM card within a few minutes, and the cost which use this cloning SIM card to phone call charge to the victim's account. On the market today the SIM card skimmer known as "magic card" has been appeared, and it can copy the contents of a SIM card.[3]

With the development of the times, the mobile phone like PC is also faced with the virus threats. August 6, 2004, the Rising anti-virus global monitor network intercepted a cell phone Trojan horse virus named as "Brador"（Backdoor.Wince.Brador.a）. Using it, an attacker can steal phone numbers and e-mail that storage in mobile phone, and can run instructions to carry out remote control mobile phone. In December 2004, the virus named of "Kapoor" in Shanghai of China found that the virus will modify the smart phone system settings, automatically search next through the Bluetooth and to carry out attacks. In addition, hackers are trying to learn to understand the ecological environment of mobile. So the mobile phone viruses will become more and more serious.[4]

2 The Security Analysis of Mobile Terminal and Mobile Communication

At present, mobile payment research and development very fast. Because the mobile phone's encryption capability is limited, can not reach the level of encryption of Internet Banking, and can not meet the requirements of the financial security. At the same time as appearance the equipment of replicate SIM card and mobile phone virus, mobile banking is experiencing a serious test because it is storage secret key in SIM card (or STK card) and the mobile phone itself.

2.1 Mobile Terminal Security Analysis

To achieve mobile payment function, it must be carried out the application program that ran on mobile phone. However, due to mobile terminals must have the portability, small size and low cost characteristics, that develop application program base on the mobile terminal have the mainly restrictions in the following three aspects:

1, The power of the process chip in mobile phone is weak.

As the cost, size, weight and other factors, the mobile phone as precise electronic product is often able to use the processing power less of chip. So the

mobile phone is not suitable for the high-intensity operations.

2, The space of storage in mobile phone is small

Similarly, because of cost, space, weight, and other factors, the current mainstream mobile storage space general only has several mega bytes, and the space that assigned to the J2ME application specific storage is less.

3, The Usable memory of application is limited

Currently the memory size can be used by the J2ME application works only is 100 K ~ 200 K retinue in mainstream mobile phone. Relatively this size of memory is less for J2ME application.[5][6]

As the wireless mobile communications systems, the mobile users communicate with base station through wireless cannel. Between the wireless channel and the closure of the cable channel the most different characteristic is wireless channel is open. Anyone who has the receiving device that is work on the same frequency band can listen to the wireless channel. Comparing to the cable channel, the wireless channel is more easily eavesdropped and not to be detected. Passive attacker can tap between the base station and mobile communications. And the active attacker can intercept and capture the communication information between the base station and mobile, and can be communicate information through network by posing as legitimate users. And even come to cheat a consumer through to pretend to be the base station. So in the mobile payment system, it must be protect the security of communications and achieve the wireless transaction that no less than cable channel communications security. So we must solute the following questions.

1, Secret

The purpose of secret is to protect information not being leaked to the people who not having been authorized. And the attacker has no way to get useful information in the content from information even if the attacker knows the information form.

2, Integrity

The purpose of integrity is to protect the information that do not be deleted or replaced tampered with illegally. In trading one side must to be able to judge out whether the information had been tampered in the process of transmission after receiving information, and ensures that the data completeness and can trace in time after the data are destroyed in the process of transmission.

3, Non-repudiation

Non-repudiation is also call non-repudiation and it is important character in Electronic Commerce agreement. The purpose of non-repudiation is the transaction participant provides the evidence to the other participation in Electronic Commerce agreement ensures that the other participation's legal benefit is not infringed. The transaction participant must be responsible for himself behavior and also have no way to deny after the transaction. That use non-repudiation agreement have two reason: First, the transaction participant that send the transaction message provide the evidence to receiving participant in order to affirm the transaction participant that send the transaction message have no way to deny, and affirm message is reliability to receiving participant. Second, the transaction receiving participant is non-repudiation and provide the evidence to the transaction message that send in order to proved the receiving participant have been received the message. In order to reach the target of non-repudiation, the agreement must have two the following characteristics: The correct evidence, the equality trading.[7]

2.2 Mobile Communication Security Analysis

In mobile commerce the security problem mostly caused by mobile terminal self and the wireless communication. The specific forms are in three the following aspect:

1, Itself of mobile terminal particularity.

2, Insecure radio frequency interface.

3, The encrypted data that transfer in wireless network are easily intercepted and captured by third party.

The solution of security problem in Mobile Commerce has two methods: One method is to improve safety of mobile terminal. But mobile terminal is limited by hardware itself. So add other equipment to improve safety of mobile terminal can realize the purpose. Make use of the add equipment is to improve the data encrypt ability and use the add equipment to realize distributed storage the secret key's. The third method is to improve the security of running wireless application program on the mobile terminal. This security is ensured by the safe system structure of wireless application program exploitation environment J2ME.It can realize the security in Mobile Commerce that using data encryption, digital signature and safe communication agreement base on the two aspects.

The purpose of this research is to invent an data encryption equipment. Use it to realize security of mobile payment in mobile commerce and do not certainly need change SIM card or STK in mobile telephone.[8]

2.3 Encryption Algorithm Analysis

In order to achieve mobile payment transactions in secrecy and ensure the secrecy the most direct approach is to encrypt message. The message is complied with plaintext in changing into ciphertext with secret key. People that not have the secret key can not decrypt the message and can not know correctly content of the message. The encryption method that data encrypted can use 3DES symmetric encryption method. It can achieve secrecy among the process of transaction in wireless communications.

In order to achieve mobile payment, it is not only need to realize the data is secrecy, but also need to consider the completeness arriving at data in communication. Because the mobile communication channel is open, the message can be easily tampered with or error among transaction. In order to ensure the message completeness among transaction, the common method is add a digital digest to attach behind deferent message using Hash function to produce and As the evidence of the message to verify the integrity MD5 (Message-Digest Algorithm 5) is a single Hash Function. It produce 128-bit hash value from the input any length of the message that carry out operations with MD5. The output of the 128-bit hash value can be regard as the "message digest" of the inputted original message, if the input information of the message has changed, the output hash value of fixed-length (Summary) will change. So this method is able to guarantee data integrity that transfer in mobile communication.

As the user who use the mobile phone is uncertainty, the time and place that use mobile payment transaction is uncertainty. It is necessary to provide digital signature to ensure the safety of mobile payment. At the same time, in the bank and its customers, the bank is in a relatively strong position. In order to prevent the strong side to the malicious cheating and deny, and achieve fair trade, it is necessary to ensure that transaction between the bank and customer is equity, non-repudiation. The currently solution method is provide digital signature. Digital signature is an important tool to achieve certification, which provides authentication, data integrity, non-repudiation, and other security services. RSA public key algorithm is a recognized safe asymmetric encryption algorithm. It is the most effective security method that use for secure communication and digital signature in network. In the public key algorithm that have been putted forward, RSA is the most easy to understand and realization. RSA encryption algorithm has the better confidentiality and eliminates the exchange of secret key between the end-users. But the encryption and decryption with RSA spends time longer and speed is slow. It is suit for only a small amount of data encryption. And it can not realize the data integrity, non-repudiation. So in doer to realize security of mobile payments RSA and MD5 Hash algorithms can be used in conjunction. First of all, the data of message that will be send to process using of MD5 hash algorithms in mobile payments, generated data summary of the message. Then using RSA private key in RSA public key algorithm encrypt the data summary of the message can get the abstract data information. The abstract data information is equivalent to the user's signature, similar to the real life of the signature or seal. The receiver can verify the result to determine the validity of signature hat use his MD5 secret key after receiving the abstract data information.[9]

3 Mobile Payment Working Process With eKey

When the user apply for the mobile payment applications to the bank, He need to receive the multi-interface data encryption eKey from the bank which contains the bank 3DES encryption key. And the bank conserve it's corresponding 3DES key. At the same time the bank will apply for a legal digital certificate of MD5 and RSA from the mobile banking service providers, which includes the MD5 initialization parameters, customer RSA private key and the bank's public key, along with mobile client software downloaded to the user mobile phone. In order to provider the mobile payment to user the bank conserve the corresponding keys.

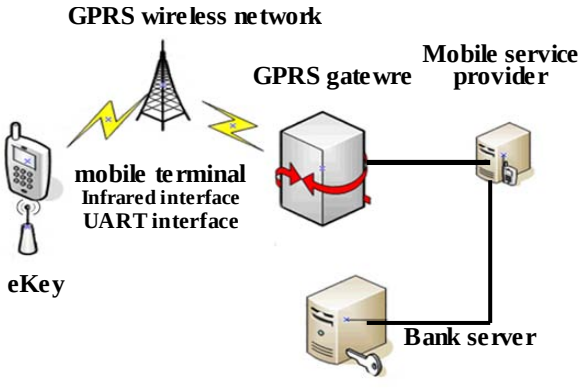

Fig.1 Mobile payment working Process with eKey

Based on additional data encryption equipment for mobile payment system, mobile phone and the bank need to communicate. The mobile phone

communicates with the multi-interface data encryption eKey through its interface (Infrared interface, or data line interface). In order to enhance the security of mobile payment, the data will be transferred to the bank server first sent to the multi-interface data encryption equipment eKey in order to use this safety equipment to encrypt data. After encrypt the received data the eKey send back the encrypted data. Mobile terminal then send out the data after encrypted data again use itself through GPRS wireless network. Pass by the GPRS gateway and mobile service provider's server the data come to bank server. The bank server can decrypt the received data. To ensure that mobile phone data from the server to the bank's end-to-end security. The mobile payment working Process with eKey shows with figure 1

3.1 The Composition of Mobile Payment System

Based on additional the multi-interface data encryption encryption for mobile payment system, it are mainly composed of the multi-interface data encryption equipment eKey and mobile phone client module that run on the mobile phone application program. The multi-interface data encryption equipment eKey main research the function of 3DES encryption/ decryption. The mobile phone client module is the base of mobile payment system. And it are composed by The following sub-module:

1, UI sub-module. It achieve the all kind of interface of the mobile payment

2, The encryption/ decryption and communication sub-module. It achieve the data digital signature, data verification and communication with the end of the bank server.

3, The eKey communication sub-module. It achieve the communication with mobile terminal through its interface (Infrared interface, or data line interface) .

4, The OTA sub-module. It achieve the function of the mobile phone client module Loading and unloading.

3.2 System Data Communication Processes

Between the mobile phone client module and the end of bank server use of Http or Socket protocol to achieve the end to end communication through GPRS. In order to ensure the security of the data transmission between the two ends, The system use 3DES, MD5 and RSA encryption for data encryption and digital signature to ensure that information not been tampered with, masqueraded and ratify the integrity of the data. At the same time ensure non-repudiation of the business transaction. The entire encryption process:

User uses the mobile phone to achieve the business transaction of mobile payment. After one transaction the mobile phone client module produce a message that should send to the end of bank server. The message is first send to the multi-interface data encryption eKey.

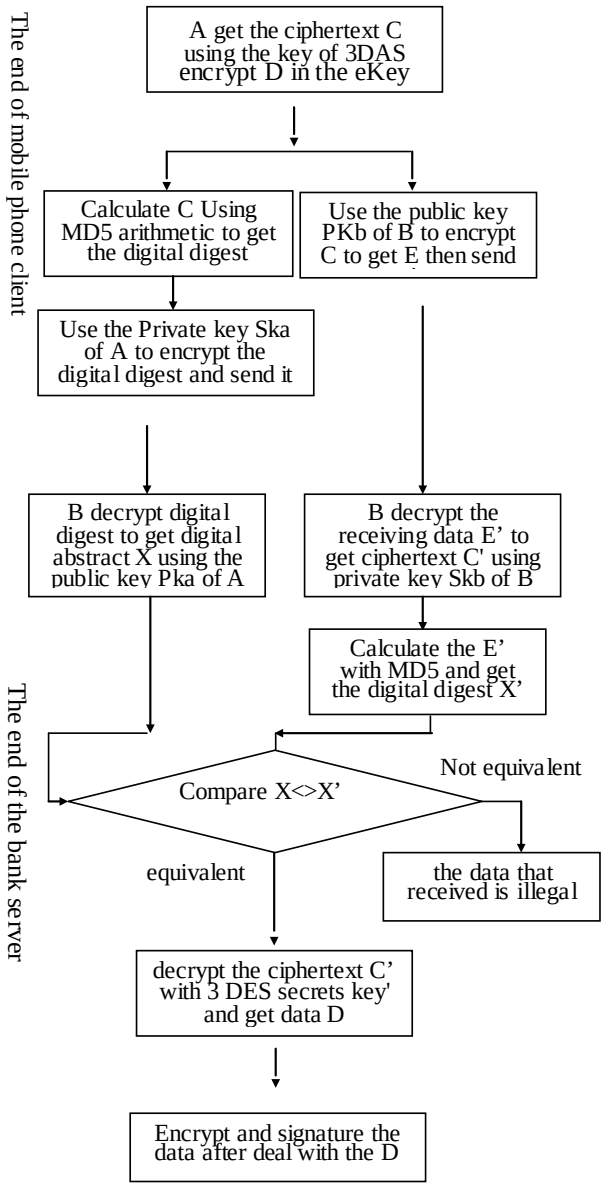

Fig. 2 Data Communication System process flowchart

After receiving the message the eKey encrypt the data with 3DES encryption key and get the ciphertext. Then the eKey sends the ciphertext back to the mobile phone client through mobile phone

interface. The mobile phone client get the data and regard as it plaintext. Then deal with the data to produce the digital digest using the MD5.Add the digital digest after the plaintext get a new message. Using the private key of the RSA to encrypt the new message to produce a new ciphertext. Final the mobile phone client send the ciphertext to the bank server through the wireless network using the Http or Socket protocol. The end of bank server receive the message from network. First the bank server decrypts the message using public key of RSA that it preserve. Take apart the message to get the digital digest and ciphertext. Then using the MD5 that preserved at end of bank server encrypt the ciphertext to get a new digital digest. The bank server can compare the new digital digest with the digital digest come from taking apart the receiving message. If the two digital digest is not the same as ,it shows that the message receiving just before has been modified or the information of the message has been lost. If the two digital digest is the same as, it shows the message receiving just before is just the user send. The bank server decrypts the ciphertext using the key of 3DES that keep in the bank server and get data. This data is the user send the message and the bank server candela with something according the means of the message and get result data message. Deal with the data message liking the mobile phone client and sent it to the user mobile phone. So the process of the data exchange between the mobile phone client and the bank server can achieve the business transaction of mobile payment.

Based on additional data encryption equipment for mobile payment system, at the end of the mobile phone client, assumption the mobile phone client is A, the private key of the RSA at the mobile phone client is Ska, the the private key of the RSA at the mobile phone client is Pka, the message that should be send to the end of bank server is D. At the end of the bank server, assumption the bank server is B,the private key of the RSA at the bank server is SKb,the public key of the RSA at the bank server is PKb. In the system, the data communication process as shown in the following figure 3. Because the secret keys of the RSA is storage at the user's mobile phone, and the secret key of the 3DES is storage at the eKey,it enhance the security of the system.

4 Mobile Payment System Design

To ensure the security of mobile payment, The Multi-interface data encryption equipment eKey must achieve 3DES 128-bit or RSA 1024-bit encryption capability in order to meet he same level of the Internet bank encryption. At the same time, low-cost solutions and low-power management must also be considered. Through the analysis, the main function of asymmetric encryption RSA 1024-bit encryption is the transmission of 3DES key, currently the eKey first achieve 3DES 128-bit encryption capability. In the experimental stage, assuming that the bank's internal security mechanism is adequate, then the issue stage, the user can be demanded to the bank to take the eKey in order to ensure of the key transmission confidentiality.

4.1 The eKey Hardware Design

Taking into account the multi-interface data encryption equipment eKey is portable and its user is target of mobile terminal, so the power supply must achieve low-power management. And low-cost solution is also need to be considered. So the figure of eKey hardware design shows as figure 3.The main controller of the multi-interface data encryption equipment eKey is chip STR711. The CPU of STR711 is an industry standard. It use a single 3.3V power supply, so it's power consumption is low; it's program memory can be encrypted to protect program, so the privacy is better; it's package use TQFP 10X10, and the package is small.[10]

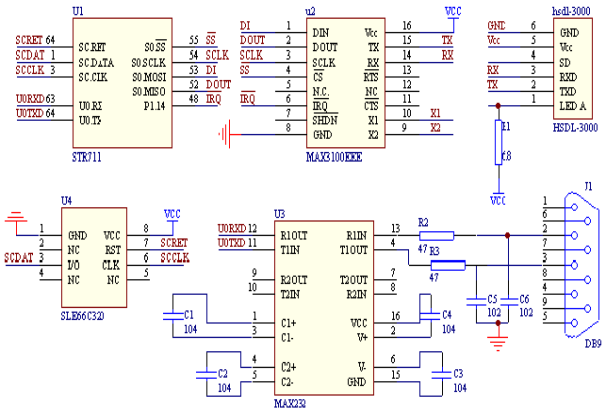

Fig.3 eKey hardware design

A UART interface of STR711 provides serial communication between STR711 and other microcontrollers, microprocessors or external peripherals. So the UART3 interface of STR711 can be used as the UART interface of eKey. UART supports full-duplex asynchronous communication, eight or nine bit data transfer, parity generation, and the number of stop bits are programmable. Parity,

framing, and overflow error detection are provided to increase the reliability of data transfers. Transmission and reception of data can simply be double-buffered, or 16-deep FIFO may be used. For multiprocessor communications, a mechanism to distinguish the address from the data bytes is included. Testing is supported by a loop-back option. A 16-bit baud rate generator provides the UART with a separate serial clock signal.

STR711 controller provides a smart card interface, the interface definition as shown in table 1.ScRST and ScDetect signal provide by the GPIO port of P0.12 and P0.10 of STR711. The two GPIO ports are controlled by software and set to suitable Multiplexing function type, in order to Respectively provide ScDataOut and ScClk signal.

The Smart Card Interface of STR711 is an extension of UART1, The Smart Card interface is designed to support asynchronous protocol SmartCards as defined in the ISO7816-3 standard. UART1 configured as eight data bits plus parity, 0.5 or 1.5 stop bits, with Smart Card mode enabled provides the UART function of the Smart Card interface. A 16 bit counter, the SmartCard clock generator, divides down the PCLK1 clock to provide the clock to the Smart Card. GPIO bits in conjunction with software are used to provide the rest of the functions required to interface to the Smart Card.[11]

Table 1. smart card interface pins

Pin	Function	In/Out	Function
Port 0.12	ScClk	out, open drain	Cards Clock for Smart Card
Port 0.10	ScDataOut	out, open drain driver	Serial data output. Open drain drive
	ScDataIn	in	Serial data input.
Any GPIO port	ScRST	out, open drain	Reset to card.
	ScDetect	in	Smart Card detect.

Now more and more mobile phone began to configure the Infrared interface. In addition to UART interface, it is necessary to develop Infrared interface in order to achieve highly adaptive. Because of it's selection of micro-controller STR711 has no internal IrDA interface, the eKey's must be consider to achieve the IrDA interface use other chip when it's hardware is designed. The MAX3100 chip is chosen to achieve the Infrared interface after comparing a lot of ways. The MAX3100 is the first universal asynchronous receiver transmitter specifically optimized for small micro-controller-based systems. Using an SPI interface for communication with the host micro-controller, and the MAX3100 comes in a compact 16-pin QSOP. It is small area and low power. The asynchronous I/O is suitable for use in RS-232, IR and opto-isolated data links. Ii is easy to achieve low-cost Infrared data communication with little power and small size.[

MAX3100 has a SPI-compatible serial interface and the STR711 has BSPI interface too, so in the eKey's system the host micro-controller STR711 use BSPI0 to connect the MAX3100. MAX3100 asynchronous receiver transmitter interface connect to HDSL-300 with the Infrared transceiver. It is a good design solution to achieve the eKey's IrDA communication.

In the multi-interface data encryption eKey equipment, the host micro-controller STR711 use the SmartCard interface to connect with the EASM security module. The EASM security module is SLE44C80S.The SLE44C80S as encryption / decryption module support for the protocols ISO7816-1 ~ 8 of the People's Bank of China, using APDU message mode communicate with the host micro-controller STR711, provide RSA, DES, MAC, Hash and other encryption methods to ensure the transfer of documents and data security and integrity, and support the encryption methods that the People's Bank of China have recognized the Single DES, Triple DES algorithm. The SLE44C80S have 8K of EEPROM, is suit to storage and management the long key, the password and file, and it's large storage space is suit to expanse of other functions too. The SLE44C80S also supports sleep mode, accord with the requirement of low-power design, reasonable in performance-price-ratio, built-in Beijing Watchdata Limited CPU card operating system TimeCOS. Support for the T = 0 (character transmission) and T = 1 (block transmission) protocol. The CPU card operting system TimeCOS accord with "China's financial integrated circuits (IC card) specification," pass the People's Bank of China detecting and accord with the ISO / IEC 7816-1/2/3/4 China's financial and integrated circuit (IC) card specification.[12]

4.2 The eKey Software Design

The software of multi-interface data encryption eKey can be divided into EASM management function module and communication management function module. The Communications management function module include communications interface management, EASM command operation and data

transmission, as well as mobile phone communication procedure; EASM management function module include EASM security module SLE 44C80S file system establishment, the accessing security attributes establishment (which key Password and encryption and decryption method can be choice, user authentication, internal and external certification), the document planning etc. The eKey software is divided into modules as shown in figure 4.

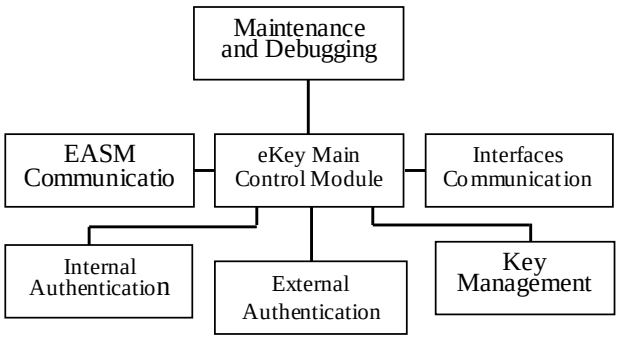

Fig.4 the eKey software system

1. The eKey Main Control Modules: This module implement the function of initializing the hardware of eKey, controlling various information distribute to proper module, coordinating all modules work, ensuring each module strict timing relationship.

2. The eKey Management: This module complete the function of planning files in EASM,loading 3DES key file in EASM, updating the 3DES keyand dealing with hash in EASM.

3. External Authentication: This module implement the fuction that the security module EASM of eKey certificate the mobile phone and the bank server.Because the bank server must certificate the eKey is legal user from a legal mobile phone before normal transaction.

4. Internal Authentication: This module implement the function that the phone certificate the communication objetc is a legal user EASM from one interface, and achieve the function of using 3DES key encrypt / decrypt the data come from mobile base on having achieved the external authentication.

5. Interfaces Communication: This module implement the function that the eKey send and receive data from mobile through UART interface or Infrared interface.

6. EASM Communication: This module implement the data communication between the main controller of STR711 and security module of SLE44C80S.

7. Maintenance and Debugging: This module implement the function of outputting debugging information, outputting log information, and receiving the maintenance order to deal with. [13]

4.3 The Software Design of Mobile Phone Client

The application of program of mobile phone client module is the basis of this mobile payment system. It is development of using the cross-platform JAVA language. So it can achieve cross-platform the as long as the mobile phone support J2ME. The following are a few key design of mobile phone client module.[14]

4.3.1 Serial Communication Design

Before developing the mobile serial communication application program base on J2ME, The program need to know the serial interface supporting in current mobile telephone and the name string of the serial first. The mobile that support the standard of MIDP 1.0 can use the Serialport.name string. The mobile that support the standard of MIDP 2.0 can use the Microedition.commports string. The concrete usage is following:

```
string propertyName=”serialport.name”;
string prorts=system.getProperty(propertyName);
```

In the packet of the MIDlet definition and the leading into, the class of GetComPortName has realized the CommandListener interface. In the mobile application program, it can first use the function getAvailableComPorts (1) to inspect the serial of MIDP1.0.If the result back is Null, it show that not inspect the serial. Then it can use the function getAvailableComPorts (2) to inspect the serial of MIDP2.0. that the following paragraph of code can gain all string of serial interface in mobile telephone. Only correctly get the string of serial interface it can use the serial interface.

```
Import java.util.Vector;
Import javax.microedition.midlet.*
Import jacax. microedition.lcdui.*;
…
public void commandAction(command command,Displayable displayable){
…
vector ports=getAvailableComPorts(1);
if(ports==null){
  ports=getAvailableComPorts(2);
}
if(ports!=null)
  for(int I=0;I<ports.size();i++){
……
```

```
form.append(ports.elementAt(i).tosString()+"\n");
    }
    }
```

Make use of CommConnection interface in javax.microedition.io packet is able to realize mobile telephone serial connection. This interface function defines a logic serial connection. A logic serial refer to a mobile telephone carry out the logical link that serial spend transfer. Logic serial is defined by OS of the mobile phone and is not the Physical RS-232 interface. Make use of the Connector.open function is able to realize the parameters setting to the serial and the serial open. the OutputStream function can realize data sending and the InputStream function can realize data receive through the serial interface.

4.3.2 Infrared Communication Design

At present the most popular technology is Bluetooth in wireless communication. It has many merit in wireless communication comparing the infrared communication. But the high hardware cost of Bluetooth limit its application in part of mobile phone. Currently most mobile phone has the infrared interface. So in order to realize the low cost point to point communication the infrared communication still is a ideal choice. And currently mostly mobile phone support the infrared interface too.

Infrared connection can carry out the data communication by logic serial. That developing the application program in mobile with the logic infrared is first get the infrared port that is supported by mobile phone. It can use the method the same as getting the mark name of serial to get the infrared port mark name. The mark form of interface ordinary is "IR # "(# is a number). After run the program that get the mark name of serial, it can get the infrared port mark name. Then it can use the following Procedure section to connect the infrared interface.

```
try{commconnection cc=(commConnection)
  Connector.open("comm.:ir1;baudrate=11500");}
```

After realizing the success of linking infrared interface, the method of Read and write infrared interface is the same as the method of serial interface.

4.3.2 Encrypting and Deciphering Designs

BouncyCastle is a safe provider of Java. the so-called safe provider is to point to realize two abstract ideas in Java safety: Engine and algorithm class. BouncyCastle is a such safe provider. It has realized the most the encrypting engine and the encrypt algorithm of Java. Though in the 1 .2 edition of J2SE later, the Java Security class has realized the encrypted engine and algorithm. During the develop program with J2ME, in the CDLC profile does not add the inherent safe mechanism of J2SE. BouncyCastle becomes the first choice safe provider to encrypting and decrypting data for his advantageous function. J2ME mobile phone can realize the signature of RSA using the BouncyCastle software package provided by the third party as long as the mobile phone apply for private key and public key certificate to CA for himself.

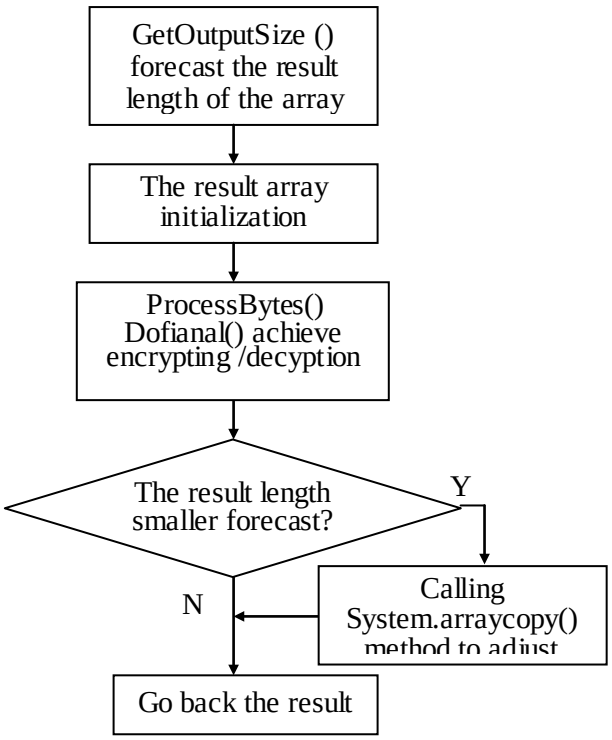

Fig.5 Basic flowchart of Encryption / decryption method

BouncyCastle API has realized the signature Encryptor class using private key. It has realized encrypted way of the RSA encrypting and the MD5 digital signature the interface through the lightweight encrypting deciphering provided Bouncy Castle. to construct its example need provide a 8 byte length data array byte[].To external class the class of Encryptor provide two method as the encrypt interface and decrypt interface.The example is following:

```
public byte[] encrypt(byte[] data)
public byte[] decrypt(byte[] data)
```

Moreover, the class of Encryptor provide two method to realize the function of formatting the input parameters and the values of bank. The example is following:

```
public byte[] encryptString(String data)
public String decryptString(byte[] data)
```

In the process of using the encrypt ()method and decrypt () method to achieve RSA encryption and decryption in class Encryptor, it need to initialize Cipher first:

Cipher.init(true,key);

The first parameter is Boolean type in initialization Cipher. It specifies the function of encryption or decryption. And true is for encryption, or false is for the decryption.

The callCipher (byte [] data) is a private method in class Encryptor. It achieve data encryption through the interface encryption and decryption of Bouncy Castle.The realization encryption / decryption process shows as Figure 5.

5 Conclusion

This article presents a mobile payment implement solution with distributed key based on the current mobile multi-interface. Analyzes the workflow of mobile payment and the reasons that cause the security in the process of mobile payment. Uses the additional equipment to achieve the secret keys distributed storage to improve the ability of test and verify in system and enhance the computing encryption capability of mobile terminal. At the same time, based on the J2ME security architecture using the encryption methods of data encryption, digital signature, identity authentication to ensure the security of wireless communication. Gives the hardware design and software design of multi-interface data encryption equipment. And gives the some processes design of mobile client's software. This solution realizes the high security and low cost of mobile payment, has good applied value and marketable foreground.

At present, most mobile phones have one or more of interface. These interface include UART interface, Infrared interface, Bluetooth interface and USB interface. The multi-interface data encryption equipment eKey has not the Bluetooth interface and USB interface currently. The eKey do not Support Bluetooth interface because of two reason. The one is that the price of Bluetooth chip is expensive for eKey currently. The other is due to the Bluetooth wireless communications, care of the wireless communication privacy concerns. So the eKey has not to design the Bluetooth interface. The USB interface on mobile electronic devices will become one of standard interface. The eKey which support USB interface can be used to PC. The eKey will expand the use to other areas and has a wider application. It is great significance that the eKey achieve communication with USB interface. So currently the eKey which support USB interface is being developed.

References:

[1] *National more than 443 million mobile phone users and an average of 3 per person have a cell* phone, *http://it.sohu.com/20061025/n245987486.shtml.*

[2] Xiaofeng Xie, JAVA technology application in the mobile value-added services,*China Data Communications*, No.5, 2002,pp.26-28

[3] Jing Ling，IBM: Hacker technology can clone mobile phone SIM card for a few minutes, *http://www.ccw.com.cn/htm/news1/net/safe/02_5_8_5.asp*

[4] Trojan Virus on Mobile phone appears and can control Mobile phone, *http://publish.it168.com/2004/0809/20040809008701.shtml*, 2004.

[5] Yang Wen.Jang Pen.etc, The flight reservation system design and implementation based on mobile phone in J2ME technology. *Application Research of Computers*,No.5,2006,pp. 166-168

[6] Ming Wu.Ping liu, Design and Implementation of mobile phone banking Based on the J2ME and J2EE, *Microcomputer Information*, ,Vol.22,No. 7,2006.pp. 294-296

[7] Xiangfeng XU. Mobile software development based on J2ME, *Microcomputer & Its Applications*,No.1,2002.pp:35-36

[8] Pei Zhang.YongPen Zhang, Mobile commerce security solutions designed based on JAVA, *Computer Engineering and Design*,Vol.27,No.5,2006,pp. 875-878

[9] RongHui Liu. Design and implementation for Micro-payment platform, Vol.30,No.2,2004,pp.171-173

[10] STMicroelectronics companies,*STR71x Pin features and packaging.pdf*, www.st.com,2005

[11] Yao Wang. EASM security module application in the card-meter. *City Gas*,Vol. 337,2003,pp17-21

[12] AiYing Wang. *Smart Card Technology*, Tsinghua University Press,2000

[13] HuiMing Chen.YangHua Li, Interface Hardware and Software Technology and applications based on MCU Control Mobile Phone, *Microcomputer Information*, ,Vol.21,No. 1,2005.pp. 139-140

[14] JianFei Zhan. *the Fine Solution of J2ME Development*. Publishing House of Electronics Industry,2006