Design and Implementation of High Security Mobile Payment System

Jian Xu1, TieJun Pan2, LeiNa Zheng3

1) Department of Information Engineering
2) Department of Computer and Information, Corresponding author

Zhejiang Wuanli University
Ningbo, Zhejiang Province, China

e-mail:960481573@qq.com, pantiejunmail@126.com, 3)mdsryx@126.com (Corresponding author)

Abstract—secure mobile payment is the most important link for a mobile phone to realize full payment. At the present stage, there are many researches about security of mobile information in the country. Those researches are mainly based on Windows Mobile, BREW or software of J2ME, and limited to specific areas. On the aspect of the hardware cryptograph, they focus on the security of computer information. There is no mature product in the mobile area basing on hardware cryptograph. Considering this situation, we refer to and compare varieties of the present payment patterns, using the JMX micro-core service as the bus structure, introducing safe technologies to design starting from the hardware unit to get security module independently. In this way, we realize the security, completeness, confidentiality, authenticity and non-repudiation of the data of mobile payment.

Keywords—mobile payment, security, encryption, hardware.

I. INTRODUCTIONS

The formal establishment of Linkage Advantageous Company in 2003 and its first cooperation with China Minsheng Bank in “mobile wallet” field in 2004 indicates that China’s mobile payment industry has already begun to display its talent. The benefit gained from mobile payments is increasing till to 2010. At the same time, because of the maturity of communication technology and the coming of 3G networks, fast and convenient mobile payment are accepted by more and more users. Many mobile communications companies have tested their ways, launching their own mobile payments. However, there is no convenient and unified method of payment adopted by the users. The information security of foreign wireless mobile terminals, basically based on specific operating system and specific hardware platform which lack of openness and portability, are not suitable to domestic handset. Taking people's livelihood into consideration, mobile security technology should be exoteric, portable, scalable and high confidential, and suitable for different business security needs. The requirement of mobile payment terminals to information security of reliability, stability, scalability, and instantaneity is higher and higher.

II. MAIN BODY

This paper puts forward a new type of mobile payment implementations which does not need to change any mobile phone hardware configuration, only with the use of some existing cutting-edge technology for mobile payments to reorganization and innovation from the model to restructuring, and optimize the allocation of the existing resources. It contains several key enabling technologies as follows:

A. EJB Technology

EJB is a server-side JAVA-based framework technology set, with which developers can easily build enterprise-class, distributed build applications. In the JAVA application server provider based on the framework of a distributed basis, developers can quickly and easily construct server-side components. EJB application can guarantee free application in any provider in the enterprise services with its first-class portability and importance.

B. Web Service Technology

Web server is a platform-neutral web services, the application of which can access the Internet through the URL specified on any services provided by a computer. Its technical features include loose decentralized structure neutral platform, no-state, providing synchronous and asynchronous procedure call, as well as easy to traverse the firewall.

C. Data Encryption Technology

In the wireless communication, radio signals related to the transmission of sensitive data are easily eavesdrop by the third party. Moreover, the wireless device itself has little capacity to support strong encryption of data communication. Therefore, in order to enable large payments through mobile banking, mobile banking software has to have adequate strength data encryption. Server-side also has to gain the ability of data encryption and decryption.

III. SYSTEM STRUCTURE

The system framework of Highly Confidential Mobile Payment is divided into three layers. They are database layer, middleware layer and the user's interface layer. The division of the three layers is very clear. The framework of the three layers will be discussed in the following section.

A. Database layer

Because of the high requirement in transaction efficiency, simultaneity and stability of database, the server port had better adopt Oracle database. Oracle is the most
popular relational object database in the current society. It is a preferred database product of both big and medium-sized management information system. In addition, it can well support Java.

Instead of the database driver from client, the method adopts intermediate layer of network - server to access a database. This type of drivers uses network protocol and pass through Java driver, providing a mechanism of calling JDBC for Java application.

The reason why we use this method is that this type of drivers is not related to platforms and it does not need the installation and management of client. As a result, it is suited for Internet application.

Since the designed wireless information mobile bank needs to record the information of registration, bill transfer, foreign exchange and SuHuiTong, when designing database, we have corresponding data table to express all the effect on the data in database.

Creating a database table should contain the following information:

- User registration form, user deletion form, payment information table, transfer information table, payment information form, remittance information table, service information table, foreign exchange business information table and securities transfer information form.

B. Mobile Information Security Middleware Facing 3G

In view of specific demand of the current mobile business information security, information security model of MIS-SDK (Mobile Information Security -Software Development Kit) will be constructed based on 3GPP security framework, to provide information security service for wireless mobile terminals. It mainly consists of two parts (as shown in figure 2):

\[\text{Figure 1. the intermediate database visits servers}\]

\[\text{Figure 2. Application Framework of MIS - SDK}\]

1) MSSClass: MS Security Service Class

It can provide API interfaces which are geared to the application layer, to realize different security service of 3GPP, such as IMR (Identity Management and Recognition), AKA (Authority and Key Agreement), DI (Data Integrity), DC (Data Confidentiality) and so on. MSSClass is constructed based on the mode of Abstract Factory, providing API interfaces which is compatible with the 3GPP security protocols. Users can flexibly configure security service and core algorithm provided by MSSClass according to their demand. MSSClass, constructed based on many-event driven model, can support CS (vehicle) and PS (Packet Switched Switched) simultaneously. Users can set priority processing mechanism (with good encapsulation and expansibility) among various events according to their different needs.

1) MSAClass: Security Algorithm Class

It can provide implementation of all sorts of encryption algorithm and Integrity algorithm of MSSClass. MSAClass enable the complete separation of interface and function which endow the whole class with good expansibility. Users can overload their own core encryption algorithm according to their demand. MSAClass also provides concrete realization of core algorithm which is clearly defined in 3GPP, including f1, f2, f3, f4, f5, f1* and f5 *in AKA; f6 and f7 in EUIC; data encryption algorithm f8 and data integrity algorithm f9. Implementation of all the algorithm is based on two core encryption units: KASUMI and AES. MSAClass optimizes the two core units and provides two different realization models. One is to give priority to speed, which needs more USIM memory space. The other one is with memory first, appropriately reducing the speed of encryption unit.

In the design of the middleware, in order to build a stable bridge between database layer and user interface layer, creating an easier condition to implement our projects under cross-platform, several key technical designs should be mentioned:

1) The design of EJB

EJB——Enterprise Java Bean, a member of JAVA technology family on the server platform released by SUN, greatly enhanced the ability of JAVA and promoted the application in enterprise JAVA applications together with other J2EE technologies.

EJB container provides an environment to maintain EJB object for the developers. As to client, EJB container provide the client view and interface for the EJB object, and realize the calling of EJB object between the EJB container and the client through a specific transport protocol. In terms of equipment and resources, EJB container can manage the database, mail server, transaction services, messaging servers and other resources, so that developers don’t have to or rarely need to relate to these resources directly. When EJB is offering such services, it ensures the stability of EJB objects, and optimized the EJB object service processing through some of the mechanisms of EJB container.

In view of the function of the system, the system uses a stateless session Bean with the client connected with session Bean. Thus the server does not need to maintain the session bean for each client, which will greatly increase the system overhead.

When Session Bean is working with Entity Bean, its calling of persistence entity Bean can enhanced system security, the realization of business logic from the session Bean methods and the implementation of database through
entity Bean.

2) The design of web services

Web Services Architecture (WSA) is the basic structure describing the Web Services standards and the core of Web Services standard. WSA stipulates the fundamental idea of Web Services and the basic structure model of architecture system, having standard awareness effect on the establishment of architecture system which complies with Web Services.

The fundamental conceptions which compose Web Services are playing different role in it.

a) Proxy and services

Service is a set of functional operations which is implemented through Service proxy. The way the Web Services system works require the proxy to realize services, request services and offer services. But the implementation of service does not depend on a certain proxy which can alter proxies while itself will not change.

b) The requester and provider

After the establishment of service, the service provider is responsible for providing services from which the service requester can send request to access to services. The process of requesting and providing requires the exchange of information through the message system between the service agent and the requests agent to complete the service process.

c) The description of the service

The description of the service, as a Web Services interface, defines the message formats, data types, transmission protocols and so on, which enables the service requester understand the service as well as its call. Here is a simple Web Services Service Description:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<deployment
  xmlns="http://xml.apache.org/axis/wsdd/
  xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance"
  xmlns:java="http://xml.apache.org/axis/wsdd/providers/java">
  <service name="MainServer3DES" provider="java:RPC">
    <parameter name="className" value="jack.j2me.ekey.MainServer3DES"/>
    <parameter name="allowedMethods" value="getMessage"/>
  </service>
</deployment>
```

WSA divides the Web Services Agreement into several levels; the relationship between the levels is shown in Figure3.

Different standards and protocols are playing different roles in the Web Services architecture, and the combination of which constitutes the technical standards of the Web Services protocol stack.

C. user interface

Highly Confidential Mobile Payment System can be divided into four parts, they are opening service, entering mobile phone bank, cancelling services and project Setting.Besides, user can develop and expand the mobile telephone interface according to their needs. Figure 4 shows the presentation of mobile phone terminal, Figure 5 system function module.

Figure3. web services protocol stack

Figure4. The process interface of payment
Figure 5. shows the presentation of mobile phone terminal

In the late stage, mobile interface can be developed and widened according to the demand, increasing new functions, new user interface and offering download service to meet the users’ need.

IV. THE DESIGN OF SAFE CORE—THE DESIGN OF ENCRYPTION MODULE

In order to guarantee the safety and reliability of the mobile’s payment information, hardware encryption device is chose to ensure users safety. Therefore, we add a high-confidential security annex (external hardware encryption device) Mkey.

Mkey (Mobile Key) is a safety encryption device separated from the information security function. Actually, it is the hardware realization of MIS-SDK to offers Mobile business information security which MIS-SDK cannot provides, such as large disposable mobile payment and bonds trading. Mkey employs hardware encryption, key diversify, adapted interface, separated mobile and card. It improves the mobile’s security and solves the problem of pretty good privacy through the outer cell phone safety encryption device. Traits are as follows:

(1) Technical skill: instead of software encryption, hardware encryption is adopted with prevention attack module or against attack circuit.

(2) Structure design: Mkey is separated from the cell phone and mobile business, but connected with cell phone by the multiple interfaces adaptor. For example, Mkey can be integrated with IF cards or RF-SIM cards, connecting with cell phone by loading process or integration.

(3) Function traits: it supports the electronic wallet and electronic passbook which is stipulated by Bank of China and the encryption algorithm which is supported by security mechanism, using flexible configuration and upgrading security algorithm rather than changing any configuration in the cell phone.

Mkey accomplishes the information secure storage and encryption functionality; while multiple interfaces adaptation technology realizes the data connection between Mkey and cell phone. There are many ways, such as NFC, RFID, SDIO, USB, Bluetooth, IrDA, Zigbee and data line. Chart 2 shows the application of Mkey in the mobile payment system. From the chart, we can see the standard configuration of smartphone--- Bluetooth headset (the enlargement of security function). Users can accomplish the identity authentication and data encryption when paying through mobile phone; the Sever can complete the data decryption and verification through Mkey; authentication is used by Mkey and the Sever.

Figure 6. the Application of MKey in Mobile business

The relationship between MIS-SDK and Mkey is relatively independent but complementary. According to the different requirements of the mobile business, MIS-SDK supplies the software encryption, and Mkey offers the hardware encryption. MIS-SDK provides Mkey with the communication interface, while Mkey provides MIS-SDK with safer place to store key. The combination of MIS-SDK and Mkey is helpful to construct a stronger mobile safety system.

Mkey can choose any external hardware equipment as its equipment among which FT card is the most suitable one because adding encryption procedure and data into TF would not change the structure configuration, saving plenty of resources.

V. THE INNOVATION AND APPLICATION OF THE SYSTEM IN THE MOBILE SERVICE FIELD

In the light of this systems technology is based on the security solution of application layer, any mobile operator, bank or the third part mobile payment facilitator, mobile service provider, terminal manufacturer can all carry on the innovative application of operating model and business model based on this technology. This benefits China where mobile messaging security standard is brewing many advantages such as easily to carry out, neatly to provide safe and reliable. For example, terminal manufacturer can develop mobile peripheral equipment (Bluetooth cellular phone) which possesses security function through this, ensuring the safety of messaging and communicating to develop mobile phone with high security. National tax department can adopt the safe Tran flash to fulfill the tax monitor of mobile commerce. Public undertakings can convert to the mobile payment which is based on RF-SIM. The bank can commence large value bank business of high security phone and the mobile operator can also commence mobile value-added service.
VI. CONCLUSION

Recently, many researches of the mobile payment software structure are focused on promoting the interaction of clients, improving the expandability of the whole structure and strengthening the security of wireless communication.

This high secure system of mobile payment does some researches in the payment structure to make out a complete structure of mobile banking software and realize the process of hardware-based cryptography.

During the research in realizing the serialization of mobile payment process, we discover that the stack model can be used well in the realization of serialization of business workflow. It is not only adaptable to mobile payment platform, but also gives us edifications about other similar platform design of business workflow. Meanwhile, the powerful compatibility and expandability of this system will make great successes in the future.

REFERENCE