# RESEARCH AND IMPLEMENTATION OF MOBILE BANK BASED ON SSL

**Li Meihong, Zhang Qishan**
**School of Electronic Engineering, Beihang University, Beijing, P. R.China, 100083**

**Wang Jun**
**School Of Information Engineer**
**Beijing University Of Post And Telecommunication, Beijing, P.R. CHINA**

## ABSTACT

SSL protocol is one industrial standard to protect data transferred securely on Internet. Firstly SSL is analyzed, according to its characteristics, one solution plan on mobile bank based on SSL is proposed and presented, in which GPRS technology is adopted and elliptic curve algorithm is used for the session key, finally several functional modules of mobile bank are designed in details and its security is analyzed.

## KEYWORDS

SSL, Mobile Bank, GPRS, Elliptic Curve Cryptography, Certificate.

## INTRODUCTION

In recent years wireless communication boosts significantly in China. It is statistical incompletely that there are more than two hundred millions mobile subscribers, and the mobile devices with GPRS technology are invented for great convenience to connect Internet. How to implement more added-value services effectively using GPRS technology on the mobile devices has become one of most hot topics, and the solution plan on mobile bank based on SSL in this paper may bring fresh wind to us.

In this paper firstly the handshake protocol of SSL protocol is analyzed mainly, if SSL is embedded in both bank center and mobile devices, thus one secure wireless channel using GPRS is built between them, in which ECC is used to generate the session key, finally the functional modules are designed and the security of system is analyzed. Thus the users can perform transactions with bank center through the channel anytime and anywhere, this is the concept of mobile bank.

## SSL PROTOCOL

SSL protocol is short for security socket layer, which is presented by Netscape in 1995. The public key algorithm is adopted in SSL to aim at security and reliability between the two applications, now SSL is one industrial standard of secure communication.

SSL protocol comprises record protocol and handshake protocol. The format of transferred data is defined in the record protocol, and its details are ignored in the paper. Handshake protocol has two phases, one is used to build secure channel, and another optional phase is used to authentication for the customers.

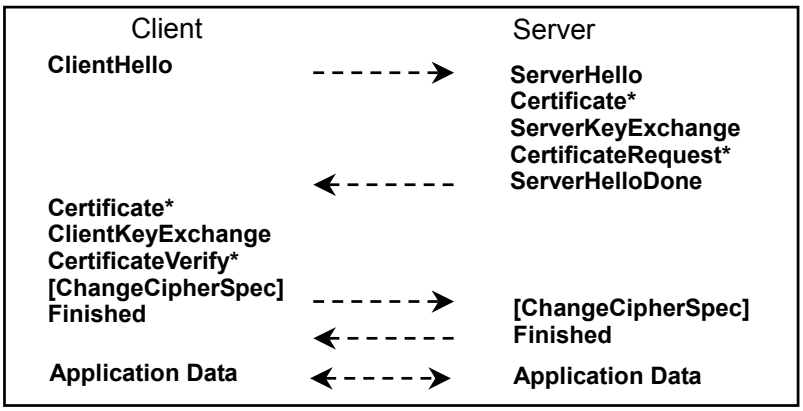


Figure 1 Flowchart of handshake protocol

Phase 1 is the initialization of communication beginning with HELLO message. HELLO message is used to determine if the new key is required or not. If not, phase 1 ends and phase 2 begin. Otherwise, the server sends the client SERVER－HELLO message to generate one new key. If one new key is generated successfully, the client will send CLIENT－MASTER－KEY message, otherwise the error message returns. At last the new key is obtained, the server sends the client SERVER－VERIFY message, the flowchart of phase 1 is showed in figure 1, in which the items with an asterisk are optional[2].

Phase 2 is the authentication for the client. The server sends the client REQUEST－CERTIFICATE message to request the authentication, then the client sends its certificate to the server. If the server authenticates the client, SERVER－FINISH message will return, otherwise the error message will return.

## TOPOLOGY STRUCTURE OF MOBILE BANK SYSTEM

The solution plan of mobile bank aims at little changes of Intranet structure in the bank center, but the indispensable components are added. Topology structure of mobile bank system is showed in figure 2, in the figure only one GPRS platform and gateway is added, which are used for data

communication between the mobile device and bank center. In addition SSL protocol is embedded in both them.

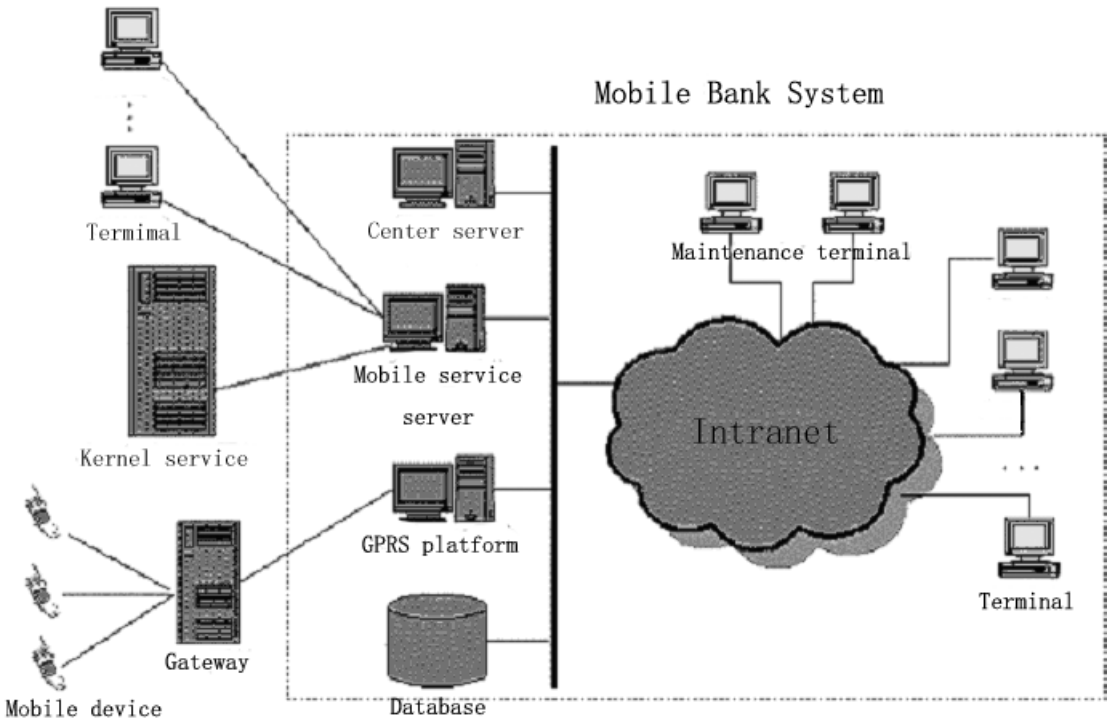


Figure 2 Topology structure of mobile bank system

## IMPLEMENTATION OF FUNCTIONAL MODULES

Functional modules are so flexible that the customers can reorganize them to save the costs to the maximum extent. The modules include two parts, one is hardware module, and another is software module. GPRS module is one new hardware module which implements wireless communication, and it is connected with GPRS gateway of communication service provider [5], the hardware frame is showed in figure 3. In which, firstly the session key is obtained by handshake between the mobile device and the bank server. After successful handshake the transaction data are partitioned, encrypted, and packaged before they are transferred securely, in addition the symmetrical key algorithm is used.

Software module comprise process of transaction, supervision and control of system, management of database, management of certificate and key, their details are as follows.

The first is process of transaction, this module includes two parts, one is the client, and another is the server.

In general the clients are mobile phone with GPRS, or other wireless devices, the below is the transaction process of the client.

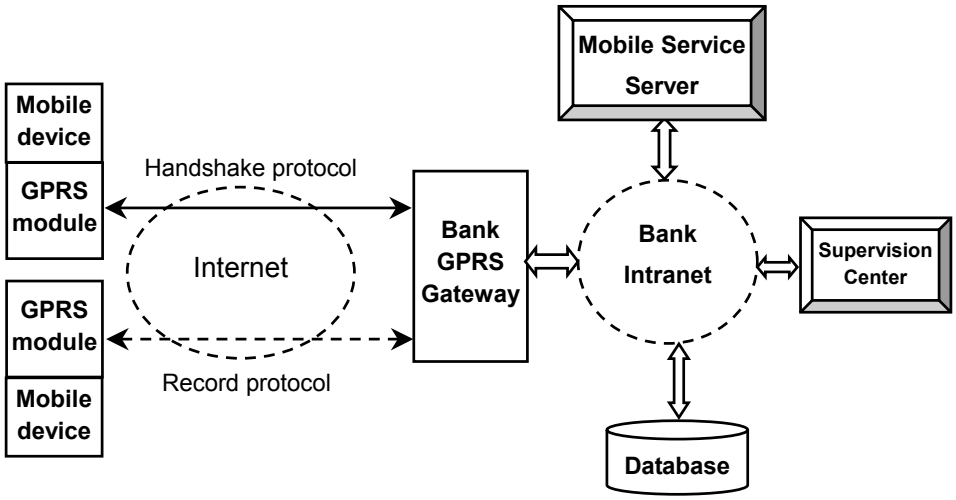


Figure 3 Frame of hardware modules

(1) Connection of GPRS: The client requests connection of GPRS, if connection fails, error will response.
(2) Negotiation of session key: The client requests to handshake with the server using SSL protocol, if handshake fails, error will response.
(3) Control of access: Control of access is required for the different accounts of user, RADIUS protocol is recommended for control of access.
(4) Preparation of transaction data: One example below is taken to describe the transaction data, and the format of data is TLV (Tag + Length + Value).
(5) After the data stream is encrypted and packaged, they will be sent to GPRS gateway.
(6) After the data received from GPRS gateway is parsed, the result of transaction returns to the user.

We suppose that the code of fund transfer is 10 (two bytes). The code of one account (AAA) is 1001, and the code of another account (BBB) is 1002, and the code of transaction amount is 1003. Now the fund of 10000$ transfers from one account AAA to another account BBB, thus we define as:

1001 03 AAA one account code＋length＋account
1002 03 BBB another account code ＋length＋account
1003 04 10000 transaction amount code＋length＋amount (four bytes)

Hence the data stream of transaction is as follows:

10 22 1001 03 AAA 1002 03 BBB 1003 04 10000

The server will process the requests from the clients such as connection of GPRS, handshake of SSL, parse of transaction data, return of results, their details are ignored.

Supervision and control of system is the second module is which is optional, this module locates in the bank network, and it aims at supervision of the mobile bank and control of behaviors of the users. Its functions can be redefined according to the customers.

The third module is management of database, which is optional, this module locates in the bank

network, and it aims at management of accounts and users of mobile bank.
The last one is management of certificate and key, in which the certificate is one entity with the signature of trustworthy authority CA (Certificate Authority), and it connects the public key and the holder. In addition the database of certificate can be created by the bank center, or apply for CA. This module aims at generation and request, download, storage, refresh of certificate and key. The generation of certificate and key should be completed in the server, and the client will download them using old expired certificate and key in cipher text.

## PUBLIC KEY ALGORITHM IN MOBILE BANK SYSTEM

Public key algorithm is used to generate the session key for encryption of transferred data. We all know that RSA is one common public key algorithm, but RSA can be attacked using the computer with high performance, thus the keys with more length are required. In the SET of e-commerce the length of key must be 1024 bits, and CA will use the key with 2048 bits, thus it will bring two problems, one is low speed of process, and another is problem of storage and management of the keys. Comparing with RSA, ECC (Elliptic Curve Cryptography) is faster in generation and authentication of digital signature, and the security of ECC with 160 bits is equivalent to the one of RSA with 1024. For these reasons, it is highly commended that ECC is adopted because of mobile device with limited resources. The differences between RSA and ECC are showed in figure 4 [6].

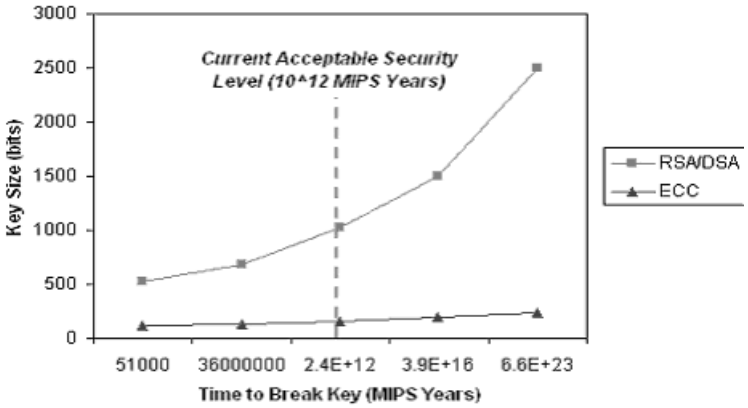


Figure 4 Comparison between RSA and ECC in security level

## ANALYSIS OF SECURITY

It is recommended that WTLS (Wireless Transport Layer Security) based on SSL is adopted because of mobile devices with limited resources. Thus there are public key of the server, private key and SSL/WTLS protocol in the client, and there are public key of the client, private key, encryption device, random number generator and SSL/WTLS etc in the server.
When the mobile device requests to the bank center, firstly the connection is performed based on

SSL/WTLS, its security subjects to the certificates and keys, the details of connection refer to handshake protocol of SSL. If the digital signature is added, the more secure level can be obtained. The digital signature can be used for the evidence of the transaction according to its characteristics. For these reasons above, there are three kinds of security mechanisms in mobile bank system. Firstly it is the authentication in two directions to protect the validity of the mobile device and the bank center, secondly it is the security that two authorized sides can access and recognize the transaction information, lastly it is the integrity that both sides can prevent the communication data from being modified.

## CONCLUSIONS

Authentication in two directions is performed using the certificates in SSL/WTLS, and the public key algorithm is adopted to generate the session key. If possible, digital signature is used to achieve the integrity. All these methods will provide the assurance of security for mobile bank system.

At present e-commerce is not true concept of mobile bank because it subjects to the fixed PC terminals, but mobile PC is likewise. The concept of mobile bank in this paper is not limited by the time and places, thus the solution plan based on SSL/WTLS must bring us extensive future of application.

## ACKNOWLEDGMENTS

First of all I am indebted to my supervisor Prof. Zhang Qishan for his valuable suggestions.

Secondly I would like to thank my close friend Wang Jun for his valuable materials and suggestions, and to my classmates and friends for their assistance.

Finally I wish to express my appreciation to my parents and my wife Zheng Xin for their endless love and unbounded understanding.

## REFERENCES

[1] Freier, Karlton, Kocher. SSL 3.0, http: //home.netscape.com/eng/ssl3/, 1996.

[2] David Wagner, Bruce Schneier. Analysis of the SSL 3.0 protocol, http: //www.counterpane.com /ssl.html, April 15, 1997

[3] T. Dierks, C. Allen. TLS 1.0, http: //www.ietf.org/rfc/rfc2246.txt, Jan 1999.

[4] Bruce Schneier, He Dequan. Application cryptography, press of machine and industry in China, 2002.

[5] Zhong Zhangdui. Mobile data service and GPRS, General package radio service, press of post and telecommunication of the people in China, 2001, 1-9.

[6] Sun Lin. Elliptic curve cryptography, http: //www.cns911.com/docs/encrypt/, Dec 2000.