Security Key: A New Mobile Payment Solution

PAN TIE-JUN, ZHENG LEI-NA
Department of Computer and Information
Zhejiang Wanli University
NingBo 315100
CHINA

Abstract: - Mobile payment raises a number of security and privacy challenges. To address this, we present an approach in which the mobile payment security is enhanced by using external security key and specified policies. An electronic security key is connected to the mobile device by adaptable interface for enhancing the security ability and storing private data. FAM is agent software with GUI located on mobile device which is responsible for payment initiation and transparent transfers between electronic key and BAM on server. FAM connects to BAM by means of identification and mutual authentication which generates different session key with time stamp each time. The cross validation among electronic key, FAM and BAM improves the security of mobile payment system. Furthermore, comparing to keeping private data on mobile phone, the isolated key protects private data from virus attacking, enhances arithmetic expansibility and is easy to be updated. In this way, the mobile payment security problem is solved to a certain extent. As an application, we implement a mobile payment system that selects electronic key as the security module and achieves the mainstream mobile payment functions.

Key-Words: - security key; mobile payment; GPRS; MIDP; COMM; WTLS

1 Introduction

In modern mobile communications, personal privacy and security are of top concern to mobile phone subscribers on mobile payment. Yet, owing to the limit of their processing capability, mainstream mobile manufacturers are still unable to apply advanced security protocol to mobile devices [1]. Mobile payment is more than a mobile and wireless extension of the Web-based e-payment. It needs more security standard in the wireless channel. WTLS (Wireless Transport Layer Security) is spurred by the mobile phone industry's widespread support of the end-to-end security, which is based on the industry-standard TLS protocol, is optimized for use over narrow-band communication channels and is used with the WAP transport protocols [4]. STK is a security solution using SIM security. Both WTLS and STK use the security capability of mobile device that is limited by processing capability and resource. With the development of interface technology of mobile devices, rapid data interface (IrDA, Bluetooth, COMM and USB) is becoming the mainstream configuration for business mobile phone which is widely used for mobile payment. Since rapid data interface can be used for communicating with an external security device, we present an approach in which the mobile payment security is enhanced by an isolated external electronic security key with a security enhancement mechanism.

2 Mobile Payment Solution

This paper proposes an advanced security mobile payment system and related security methodology based on distribute key without changing the mobile devices hardware configuration. The system consists of the front end administration module (FAM) on mobile terminal (mobile phone and PDA), external electronic security key (eKey) with distribute key and personal privacy, CA with digital certification and backend administration module (BAM) on bank server (Fig. 1). FAM communicates with BAM and CA via GSM/GPRS mobile network and Internet. FAM communicates with eKey via adapted interface (e.g., COMM, USB, IrDA and Bluetooth).

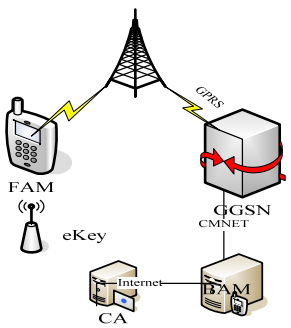

Fig.1 Mobile Payment Solution Network

The procedures of this security system service are as follows (Fig. 2):

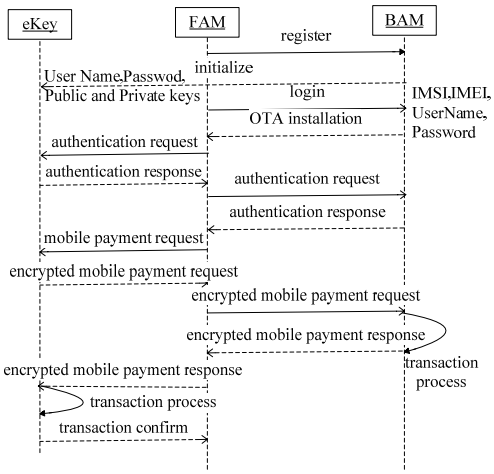

Fig.2. Mobile Payment procedure

Firstly, customer buys eKey from the authorized agency of bank or SP and signs autentication information named Mp including MSISDN, IMSI, IMSI, user name, password, authorization code etc. which is stored in BAM database for future transaction verification and authentication.

Secondly, the agency encrypts Mp into ciphertext named Mk, and writes Mk and relative security information such as PKI public key and private key in accordance with the specific encryption arithmetic ruled by China Business Security Bureau.

Thirdly, customer downloads FAM that is a mobile payment application based on MIDP or UIQ platform from specific mobile payment web site and installs it on his or her mobile phone.

Fourthly, mobile phone connects to BAM via GPRS and connects to eKey via Bluetooth so that eKey is in online state. User inputs the account registered to BAM. After mutual authentication between eKey and BAM succeeds and session key generates, FAM sends prepayment request to eKey, eKey signs prepayment request including IMSI, IMEI or MSISDN etc. with private key for verification and encrypts it with session key. The ciphertext is returned to FAM and FAM transfer the ciphertext transparently to BAM.

Next, after BAM decrypts ciphertext with session key and verifies the digital signature, it process the plaintext and return the confirmation result which is encrypted with session key and signed with private key to FAM.

Then, FAM transfers the ciphertext transparently to eKey. eKey reads the ciphertext and decrypts it by session key in eKey, verifies the digital signature, process the transaction, saves the balance, and then sends results to BAM via FAM.

Finally, BAM deals with the results from eKey, saves the transaction record into database for printing the invoice in the future and finishes the whole transaction.

In fact, eKey is an external electronic wallet enable to communicate with mobile devices. FAM only provides GUI for user input and transparently communication channel between eKey and BAM. Customer keeps the right to execute the mobile payment application or not.

3 Application Development

Mobile payment solution consists of eKey, FAM and BAM with GPRS network and internet. We have developed a practical project to explore the technology feasibility of the solution.

3.1 eKey

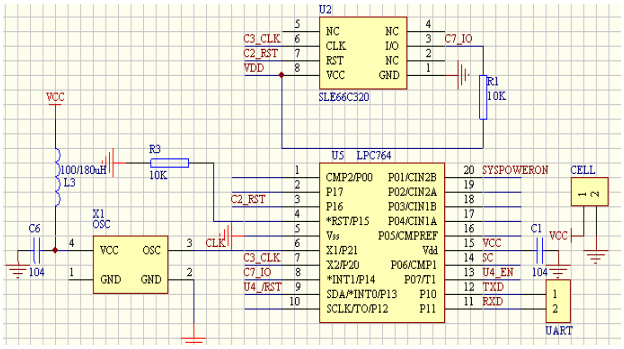

Fig.3. eKey Schematic diagram

As an external security device used for mobile phone, eKey should support Public Key Infrastructures (PKI) mechanism with Single DES, Triple DES, SHA-1, RSA arithmetic and X.509v3 certificates storage. Further, eKey should have high performance with low cost, power saving and tiny figure [4, 5]. In response to these requirements, we design the hardware solution which adopts P87LPC764 chip of Philip Company as the main MCU, Watchdata e270B embedded TimeCOS complying with Financial Integration Circuit Regulations of China as ESAM which can be replace by more powerful chip (Fig. 3), and MAX232 of Maxim Company as the interface adapted chip because eKey connects to mobile phone via COMM in our test. eKey is developed using the P87LPC764 microcontroller and a basic HW to ESAM. When smart card mode enabled, the RST, Vpp, Vcc, and Detect signals (signal for card detection) are provided by GPIO bits of the IO ports under software control. Programming the GPIO bits of the port can alternate function modes. We connect

the MCU INT1 data signal to the ESAM I/O pin with the correct driver type and the ESAM clock generator (MCU X2 pin) to the ESAM CLK pin. The X2 pin with a MCU counter provides a clock signal to the connected ESAM. The eKey uses this clock to derive the baud rate clock for the serial I/O between the ESAM and UART1. The clock is also used for the CPU in the card, if present. The ESAM Interface is an extension of UART and is designed to support asynchronous protocol smart cards as defined in the ISO7816-3 standard. With serial mode enabled, UART1 is configured as: eight data bits plus parity and 0.5 or 1.5 stop bits.

The basic payment transaction procedure is as follows: first, when FAM sends a command with ciphertext to eKey via COMM interface, an external interrupt is triggered. MCU starts a timer to meet the Element Time Unit (ETU) specification for baud rate of data exchange. Second, MCU reads the ciphertext and transfers it to ESAM for decryption after both the internal authentication and external authentication success. Third, MCU processes the payment transaction and sends the confirmation information encrypted by ESAM to FAM. Finally, FAM sends the confirmation information to BAM. BAM decrypts the ciphertext and finishes the whole payment transaction.

Embedded software is divided into following modules to achieve functions such as mutual authentication, data encryption and data storage: (1) Main control module is responsible for initializing hardware, distributing message between other modules and coordinating various modules in order to guarantee task sequence. (2) Key management module is responsible for key distribution, loading and maintenance. (3) Authentication module is responsible for encryption and authentication among eKey, FAM and BAM. (4) Communication module is responsible for data communication between COMM and ESAM. (5) Maintenance module is responsible for output of debugging information and log and maintenance command receiving and handling [6].

3.2 FAM

At present, mobile payment mainly is based on SMS, STK, USSD, WAP and J2ME in China. Each method has its own features, however, comprehensively comparing, the mobile payment based on J2ME has more advantages and can provides better value added services with rich GUI and flexible extension [7].

This system is developed by J2ME with MIDP2.0/CPLD1.1. The information model of FAM includes a main class inherited from MIDLet and implements the interface of Controller. It accomplishes screen serialization by stack technology. All the common static variables are defined in the Action and Lable class for multi-language version maintenance. Encryptor class is a light weight security provider which implements the Triple DES, RSA and digital signature function by software or eKey. Conn class implements the communication between FAM and BAM supporting Http, Socket and SMS. WelcomeScreen class implements welcome screen instance and Login class implements login screen instance, they sends and receives data by invoking Conn instance and encrypts and decrypts by invoking Encryptor instance. Wd class is an screen factory which gets all function tree model and process list and initial information from Wd_index (Fig. 4).

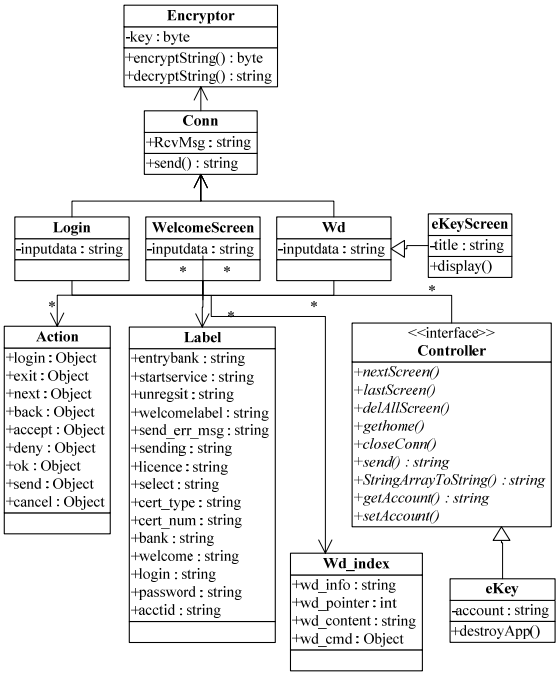

Fig. 4 Information Model of FAM

3.3 BAM

In order to keep the consistency and stability of the system, BAM adopts J2EE framework with JBOSS to be the mobile payment application server. Considering the transaction efficiency, concurrency and reliability of mobile payment, DBMS adopts Oracle 10g. We encapsulate the mobile payment business logic into EJB components using OOD thought for security and extension. For the integration requirements, we complete EAI with web services technology [8].

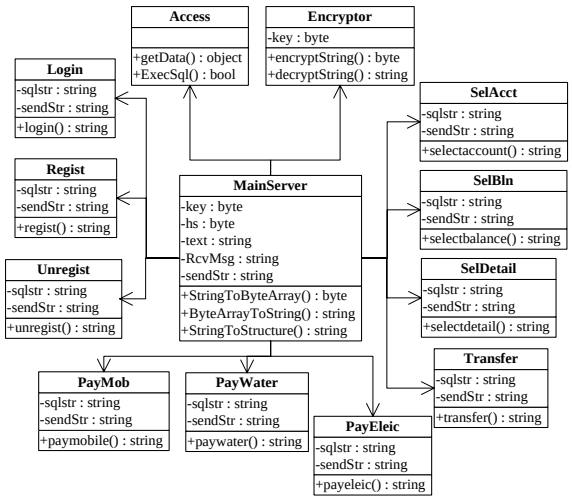

Fig.5 Information Model of BAM

In the information model of BAM (Fig. 5), firstly the MainServer initiates the entity, parses and decrypts the received messages from FAM, transfers the processed data as parameters to the function components (Regist, PayWater etc.), returns the results to FAM. The Access class is responsible for database access. The Encryptor clsss is responsible for encryption and decryption function. Others are responsible for various payment businesses.

4 Conclusion

Socket connection is more efficient than Http connection in the mobile payment data transfer. China Mobile Company provides two APN for GPRS, one is CMWAP, and the other is CMNET. Since CMWAP limits access to Socket connection, our system is designed to support both CMNET and CMWAP to keep the high stability and compatibility.

Given the interoperation between mobile device and external device is feasible, there is a new way to solve the security problem of the typical mobile prepayment system. In this paper, we have presented such a mobile payment solution that can be used for mobile payment without changing your mobile device hardware configuration by connecting to an external security device. Furthermore, we have discussed the mobile payment process and hardware design.

In terms of future work, there is a need to provide a eKey with Bluetooth, IrDA, NFC adapted interface to mobile phone in particular that will allow us to better show the applicability of our solution to a wide variety of application domains. In addition, the use of actuators will eventually improve the development of our mobile payment solution.

References:

[1]Muhammad Sher and Thomas Magedanz, Network Access Security Management (NASM) Model for Next Generation Mobile Telecommunication Networks, in Proc. of MATA 2005, 2005, pp. 263-272.

[2] Baris Kayayurt and Tugkan Tuglular, End-to-end security implementation for mobile devices using TLS protocol, Journal in Computer Virology, Vol.2, No.1, 2006, pp. 87-97.

[3]Vijayalakshmi Atluri and Heechang Shin, Efficient Enforcement of Security Policies Based on Tracking of Mobile Users, in Proc. of 20th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2006, pp. 237-251.

[4]Wong DS, Chan AH. Mutual authentication and key exchange for low power wireless communications. In: Edmonds A, Yenser G, Ferrari G, eds. Proceedings of the IEEE MILCOM 2001 Conference. Washington DC: IEEE Communication Society, 2001. pp.39~43.

[5]Jakobsson M, Pointcheval D. Mutual authentication for low-power mobile devices. In: Syverson PF, ed. Proceedings of the Financial Cryptography 2001. Heidelberg: Springer-Verlag, 2001. pp.178~195.

[6]H. Lee, J. Alves-Foss, and S. Harrison, The use of encrypted functions for mobile agent security, in Proc. 37th Annual Hawaii International Conference on System Sciences (HICSS'04), Big Island, Hawaii, 2004.

[7]G. Cabri, L. Leonardi, and F. Zambonelli, Engineering mobile agent applications via context-dependent coordination, IEEE Trans. on Software Engineering 28(11) (2002),pp. 1040-1056.

[8]S. T. Vuong and P. Fu, A security architecture and design for mobile intelligent agent systems, ACM SIGAPP Applied Computing Review 9(3) 2001, pp. 21-30.