Research of Multi- interface Data Encryption Equipment Based on 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: - Mobile payment security is one of the issues in the mobile terminal itself, this article presents a mobile payment implement solution with distributed key based on the current mobile multi-interface, analysis the mobile payment workflow, gives Multi-interface data encryption device specific hardware design and software design. 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

1 Introduction

At present, mobile payment research and development very fast. However a key factor of limits the mobile payment application is security issue. 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 phone itself[1].

The most important impact of mobile payment business development issue is in the process of mobile payment security. In the mobile payment of security problems are caused by mobile itself and by wireless communication. Therefore, mobile commerce security solutions depend on two main areas: on the one hand, the mobile terminal has the features of unique portability, small size and low cost. So it is difficult to achieve Internet Banking Encryption level with its own hardware to enhance its security. Add a addition equipment is a good solution can be achieved, and use of the addition equipment to enhance the mobile terminal equipment capacity of deal with data encryption, At the same time use of additional equipment to achieve the key distributed storage system to improve the verification mechanism and improve system security. On the other hand, the security of wireless applications running on mobile can be ensured by the J2ME security architecture. Base on these two areas, Use the data encryption, digital signature, authentication and security of wireless communication protocols can ensure the security of communication.

To enhance the ability of encryption data on mobile terminal with external encryption device can solve the problem of weak encryption capability. At present, most mobile phones have the ability to access external devices through interface, and the trend is growing significantly with the technology development. The mobile phones with Infrared interface, Bluetooth interface and data line interface has become almost standard, and with USB interface is also increasing. As a result, the use of mobile phones, SIM cards and Multi-interface data encryption equipment eKey on the cross-encryption can greatly enhance the security of mobile payment This paper is designed and implemented an Multi-interface data encryption equipment eKey, customers using the existing mobile phone without needed to replace SIM card or STK cards in the phone can achieve to meet the security requirements of mobile payments.

2 Mobile payment working Process with eKey

Based on Multi-interface data encryption equipment eKey for mobile payment systems, between mobile terminal and bank need to data communications. In order to enhance the security of communications, mobile terminals communicate with the multi-interface data encryption eKey through the Infrared interface, or data line interface, the data will transfer to the bank server first sent to the multi-interface data encryption devices 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 equipment of bank server can decrypt the received data. To ensure that mobile phone data from the server to the bank's end-to-end security[2][3]. The figure of mobile payment working process with eKey show as figure 1.

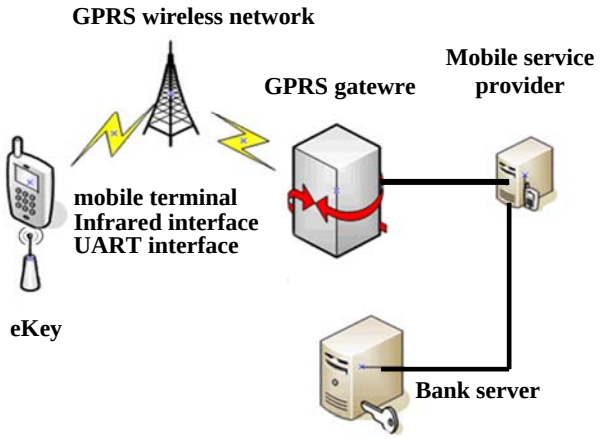

Fig.1 Mobile payment working Process with

3 eKey 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.

3.1 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 2.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[4].

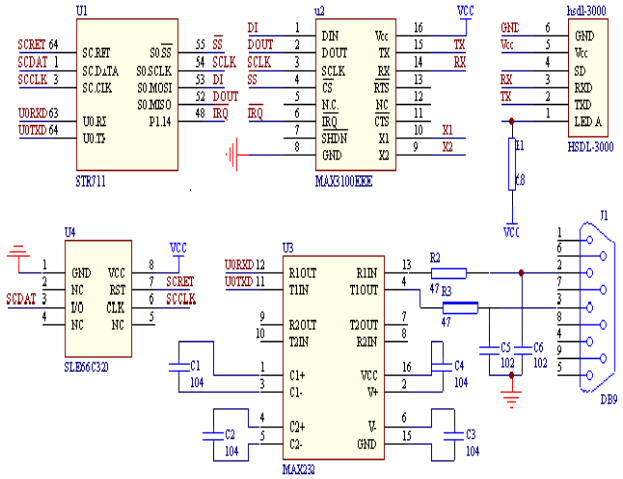

Fig.2 eKey hardware design

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.

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 [5].

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[6]. 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.

3.2 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 3.

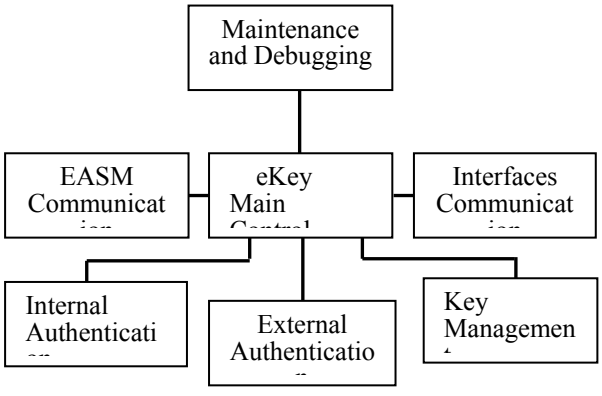

Fig.3 the eKey software

1. 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. Key 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.

4 Conclusion

This article describes the multi-interface data encryption equipment eKey which is used of the STR711 as the master controller, and gives the hardware design and software design of the eKey. The eKey use embedded security module for data encryption and decryption with 3DES and reach the level of Internet Bank, and use UART interface, or Infrared interface to communicate with mobile phones. The eKey realize the data encryption and decryption of mobile payment in practice.

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

[2] SANTOSH K.MISRA and NILMINI WICKAMASINGHE, *Security of a Mobile Transaction:A Trust Model*, Electronic Commerce Research,Vol.4, 2004, pp. 359-372

[3] Tamzin.J,*Wireless Application Protocol 2.0 Security*,http://rr.sans.org/wireless/wap2_sec.php, 2001

[4] STMicroelectronics companies,*STR71x Microcontroller Reference Manual.pdf.* www.st.com,2005.1

[5] *IrDA Object Exchange Protocol*.Infrared Data Association,1999

[6] *MAXIM3100 Data Boo*k, MAX3111E.pdf, www.maxim-ic.com, 1999