Mobile Payment System for Prepayment Meter

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

Abstract: - We present an approach in which the payment system of PM is enhanced by supporting mobile access without smart card. PM with embedded ESAM providing encrypting ability and protecting private data is connected to the mobile device by adaptable communication interface. MPC with GUI located on mobile device which is responsible for business initiation and the communication between the PM and PS. MPC is connected to PS by means of identification and bidirectional authentication generating different session key with timestamp every time. The cross validation among PM, MPC and PS can improve the security of mobile payment system. On the other hand, the payment information from PS can be stored in SIM or smart card plugged in another device that can communicate with mobile device when the PM is offline. SIM or smart card should insert PM to exchange information with ESAM and complete the business. In this way, the mobile payment system can reduce the cost and improve convenience of payment.

Key-Words: - mobile payment; OTA; SIM; GPRS; MIDP; IrDA

1 Introduction

Prepayment Meter (PM) is a kind of new-style meter that purchase electricity by smart card and adopt micro-electronics techniques that can help the power company to accomplish prepayment function. Both potential and realized benefits of prepayment are obviously to the power company. Since the typical PM is an offline device, customer should purchase and use a prepaid power purchase card (Smart Card) to obtain prepayment service in agency or bank in person. It’s always fussy for busy people in the current society. Recent advances to mobile communication, IrDA, Bluetooth and Radio Frequency Identification (RFID) technologies have propelled the growth of a number of mobile services, especially of mobile payment. Mobile payment raises a number of security and privacy challenges. To address this, security policies are specified to ensure controlled access to the mobile user’s bank account and personal privacy based on the mobile user’s authentication information. Considering the basic authorization specification, in a mobile environment, a mobile phone can be a subject, an object, or both to PM and PS. In this paper the main focus is to establish a set of security features, methodologies and mechanisms to build the mobile prepayment meter system architecture, which provides users a secure access to Payment Server (PS) through mobile telecommunication, network services and to PM through adaptable interface. The architecture involves the authentication and key agreement, security mode setup during connection establishment, and access link data integrity and confidentiality between PM and PS [1].

2 Mobile Prepayment Solution

The paper aims to propose a mobile payment security solution that is convenient for user to purchase power. The solution includes modules for (1) PM with embedded security access module (ESAM), and (2) Mobile payment client (MPC) with Graph User Interface (GUI) located on mobile device (e.g., mobile phone, PDA), and (3) PS which connects to bank (Fig. 1). PM connects to MPC through adaptable interface (e.g., IrDA) and MPC connects to PS through wireless network and Internet.

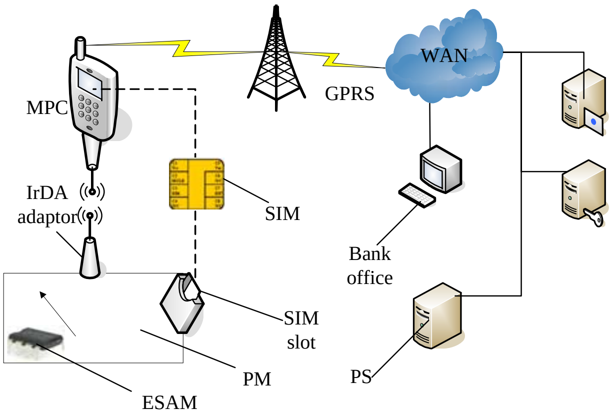

Fig. 1 Mobile Prepayment Solution Network

2.1 Mobile Prepayment Client

The development of smart phone technologies for supporting Over-The-Air (OTA) download and powerful I/O operation has been the priority of various requirements. For example, the MIDP 2.0 specification introduces optional support for serial (COMM) communication. In response to this, MPC achieves purchasing power and checking records with GUI through process bellow [4, 5].

Firstly, user takes his or her own valid ID and bank card to any agency or banking offices of bank which has contract with the power company and fills in "Personal Mobile Payment Banking Service Application Form" to apply for the service and obtain authorization code. Following the procedure stated in User's Guide, user can install MPC software on their mobile phone via IrDA, Bluetooth, high-speed data transfer line or OTA. All the signed information including MSISDN, IMSI, IMSI, user name, password, authorization code etc. is stored in PS database for future transaction verification and authentication.

Secondly, user starts MPC, selects mobile payment item, inputs contract ID (e.g., power meter id, MSISDN, bill id), selects account and confirms. In addition, password is needed for non-registered account.

Thirdly, the mutual authentication is used by prepayment applications to authenticate MPC to PS and vice versa. MPS and PS complete mutual authentication with MSISDN, IMSI, IMSI, user name, password, and authorization code used for single or crossed verification and authentication. The prepayment transaction information is transferred on SMS, MMS, socket or other channels in GSM, GPRS or CDMA mobile networks. In response to this, MPS is implemented by STK, J2ME or WAP, and connects to PM via adaptable interface such as IrDA, Bluetooth, or COMM. For the mobile phone without communication adapter, the encrypted prepayment information returned from PS is saved to Security Identification Module (SIM) with special SMS. The timestamp in the ciphertext can protect prepayment information from reply attack and digital signature for authentication is used to keep data integrity and non-reputation.

2.2 Prepayment Server

PS includes key distribution center (KDC), product distribution system (PDS) and prepayment management system (PMS). KDC is responsible for the senior management organization of power prepayment that is often the provincial power company. It generates the main control card as top key storage, and then top key generates all kinds of issuing card (e.g., PSAM, ESAM issuing card) used by junior organization such as the city power company which is responsible for initiating and changing ESAM key and generating test card for production. PMS is used by bank office that is responsible for registration, prepayment and maintenance.

PS is implemented by Visual studio 2005 developing tools with C# language. It adopts and extends ELB framework by plugging into the business application blocks (e.g. Key management block, card distribution block and prepayment block). In order to integrating with bank system and power company management system seamless, web services technology is used to complete the enterprise application integration.

PS consists of four layers vertically: business layer, security layer, transfers layer and physical layer. Business layer is responsible for registration, prepayment, changing meter, inquiry and statistic. Security layer is responsible for keys distribution and management, security process and methodology design. Transfer layer is responsible for the encapsulation of different communication ways and different drivers of Chip Operation System (COS) embedded into smart card. Physical layer is responsible for hardware interface definition and electric feature stipulation [6, 7, and 8].

2.3 Prepayment Meter

In the current PM of China, user should go to bank office to prepay the power for future requirements every time in person when the balance in the PM runs out. We design two sets of PM and relative prepayment process to support mobile prepayment. The first set (applicable to current enabling technologies and structure) consists of the following parts: offline PM with SIM adaptable interface that can be implemented by moulding board with SIM slot, MPC and PS. The second set (applicable to future enabling technologies and structure) consists of the following parts: online PM with IrDA interface, MPC and PS. Let us now use an instance to expand how the PM and relative process would work for a specific mobile prepayment application.

The first set prepayment process is as follows: firstly, mobile phone connects to bank office via GPRS and user inputs the account registered to PS. Secondly, bank office connects to PS to get the relative keys. After mutual authentication succeeds, bank office notifies user to input the prepayment amount and select prepayment ways. Thirdly, the prepayment information is encrypted by relative keys on the phone or passwords and signed by IMSI, IMEI or MSISDN etc. MPC sends the prepayment information to bank office. Fourthly, bank office processes the prepayment information and returns confirmation message that is encrypted by private key of PM in symmetric encryption Algorithms or by private key of PS in asymmetric encryption algorithms to MPS. MPS saves the confirmation message on SIM as special SMS. Finally, user Plugs SIM into PM, PM reads the SMS content and decrypts it by relative keys in ESAM, then processes the transaction and saves the prepayment information to ESAM. In fact, SIM replaces the typical prepaid power purchase card which brings the benefit of that user need not go to bank office in person to purchase power.

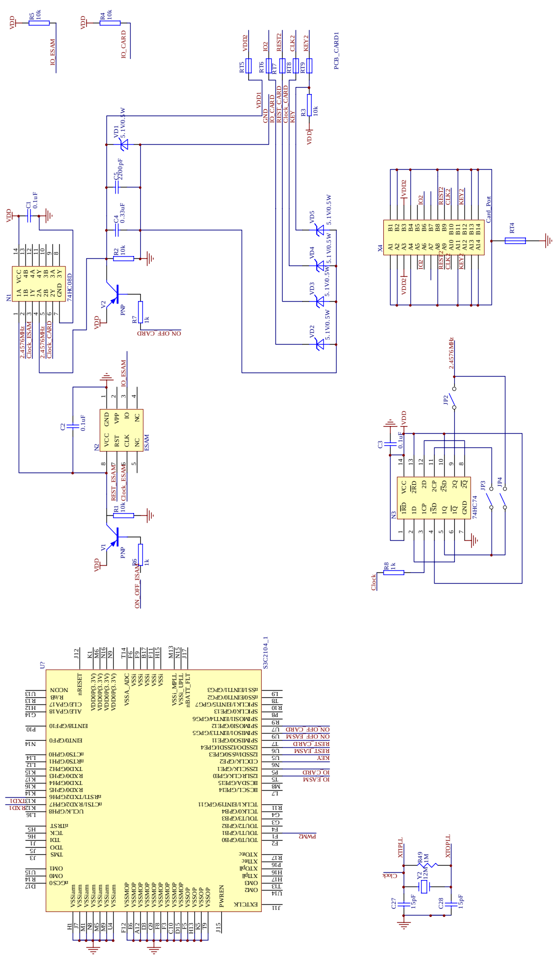

Fig. 2 PM with SIM adaptable interface

In response to the first set of prepayment process, the PM with SIM adaptable interface is designed (Fig. 2). S3C2410 is a high performance and low cost ARM9 Micro Control Unit (MCU) of Sumsung Company for PM. Its GPE0 pin conjoins with ESAM IO pin for data exchange and GPE4 pin conjoins with ESAM RST pin for resetting. 74HC08 aims to provide appropriate clock to ESAM. The similar setting applies to smart card interface for SIM. Firstly, When SIM plugs into the smart card interface, an external interrupt triggered. MCU starts a timer to meet the Element Time Unit (ETU) specification for baud rate of data exchange. Secondly, MCU reads the ciphertext from SIM and transfers it to ESAM for decryption after both the internal authentication and external authentication success. Thirdly, MCU processes the prepayment transaction and sends the confirmation information encrypted by ESAM on SIM to MPC. In the end, MPC sends the confirmation information to PS. PS decrypts the ciphertext and finishes the whole prepayment transaction.

The second set prepayment process is as follows: firstly, mobile phone connects to bank office via GPRS and connects to PM via IrDA so that PM is in online state. User inputs the account registered to PS. Secondly， bank office connects to PS to get the relative keys. After mutual authentication succeeds and session key is generated, MPC sends prepayment request to PM, PM 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 MPC. Thirdly, MPC transfers the ciphertext transparently to PS. After PS decrypts ciphertext with session key and verifies the digital signature, it processes the plaintext and returns the confirmation result which is encrypted with session key and signed with private key to MPC. Fourthly, MPC transfer the ciphertext transparently to PM. Fifthly, PM reads ciphertext and decrypts it by session key in ESAM, verifies the digital signature, process the transaction, saves the prepayment power into the ESAM, and then sends results to PS via MPC. Finally, PS deals with the results from PM and finishes the whole transaction. In fact, the typical prepaid power purchase card is omitted and user need not go to bank office in person to purchase power. MPC only provides GUI for user input and transparently communication channel between PM and PS.

In response to the second set of prepayment process, the PM with IrDA adaptable interface is designed (Fig. 3). The MCU and pin configuration is similar to that the PM with SIM shows. The difference is that IrDA interface replaces SIM interface with UART2 of S3C2410 conjoins with HDSL3208 that is an IrDA chip of HP Company. PM can communicate with MPC via IrDA interface.

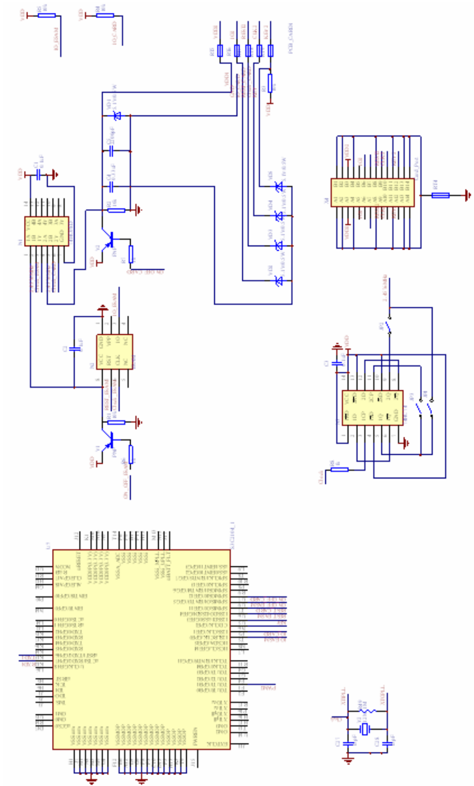

Fig. 3 PM with IrDA adaptable interface

3 Discussion

At the premises that mobile device and PM have adaptable communication interface allowed be access ed by MPC, this paper discusses the mobile prepayment architecture involves the authentication and key agreement, security mode setup during connection establishment. Business mobile phones almost all support MIDP2.0/CLPD1.1 which specifies local port access function of mobile phone.

In response to the first set of prepayment process, SIM can be replaced by any storage device such as flash disk and Secure Digital Card (SD) etc.

In response to the second set of prepayment process, IrDA can be replaced by short distance wireless communication such as Bluetooth and NFC etc.

With the developing of short distance wireless technology and the promotion of mobile device, mobile prepaymet will be the developing trend of meter.In order to improve the expensibility of PM to adapte different communiction, a necessary solution is to isolate the communication function into a subboard with standard interface specification.

In addition, the emergence of NetMetor will provide more convenient mobile prepayment solution for customers [3].

4 Conclusion

Given the interoperation between mobile device and meter is feasible, there is a new way to solve the inconvenience of the typical power prepayment system [2]. In this paper, we have presented such a mobile prepayment solution that can be used for purchasing power without going to the agency. Furthermore, we have shown the prepayment process and hardware design, a practical application.

In terms of future work, there is a need to provide prepayment gas meter with Bluetooth adaptable interface 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]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.

[5]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.

[6]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.

[7]S. Guan, T. Wang and S. Ong, Migration control for mobile agents based on passport and visa, Future Generation Computer Systems 19(2) (2003), pp.173-186.

[8]A. L. Murphy, G. P. Picco, and G.-C. Roman, LIME: A middleware for physical andlogical

mobility, in Proc. 21st Int. Conf. on Distributed Computing Systems (ICDCS-21), April 2001, Phoenix, Arizona, pp. 524-533.