International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 3, June 2012 www.ijcsn.org ISSN 2277-5420

RFID based Bill Generation and Payment through Mobile

[1]Swati R.Zope, [2]Prof. Maruti Limkar

[1]EXTC Department, Mumbai University
Terna college of Engineering,India

[2]Electronics Department, Mumbai University
Terna college of Engineering,India

Abstract

Emerging electronic commerce becomes popular together with the considerable increase of mobile device. Since mobile payments will become one of the most important mobile services. Here we are generating a bill in Super market and billing it through mobile. The most important consideration is the security of the mobile devices and the applications along with the complexity of payment process. We describe how Smart Market works and discuss related issues in detail and secure remote payment architecture based on smart card in mobile devices that simplifies the payment process and takes a finance measure to permit a more fairly allocation of risks between merchants and consumers.

Keywords: RFID tags

I. INTRODUCTION

This paper presents a new form of supermarket-Smart Market, or SMart in short. Shopping in the present day usually involves waiting in line to get your items scanned for checkout. This can result in a great deal of wasted time for customers. Furthermore, the technology currently used in checkouts barcodes - is from another era, developed in the 1970s. With the increasing prevalence and affordability of radio frequency identification (RFID) tags in everyday authentication systems, RFID holds great promise in the retail world for both customers and stores in inventory control, convenience, and cost savings.

Our project utilized these RFID tags to automate the checkout process by building a system that could read the RFID signals of all the objects that were placed in proximity to an antenna platform. This eliminated the need for barcode scanning of each individual item, making checkout a significantly faster experience. Furthermore, as each item has a unique tag, even copies of the same product contrasted to the current UPC model, much better inventory control, recall ability, and monitoring of consumer behavior trends are possible, with privacy concerns considered of course.

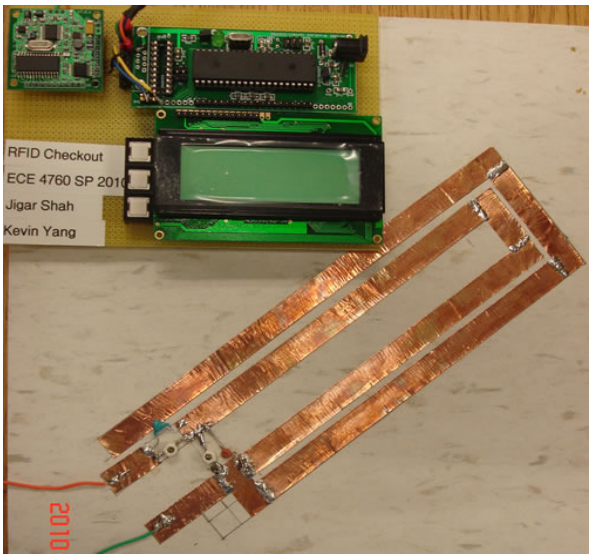

Fig 1. The Completed RFID Checkout System

II System architecture

2.1) Logical Structure:-We immediately considered RFID tags, already used heavily at Cornell for dorm access, not to mention in industry for employee authentication and credit card systems for wireless payment. For those applications, however, only one tag at a time was read, and multiple tags within the sensor read area would render the system useless, a key requirement of our checkout system. We discovered that a mainstream tag protocol had been developed at 13.56 MHz with anti-collision support, enabling simultaneous, error-free reading of all tags within the read field.

Our RFID checkout was organized around several central components. The prototype board containing the Atmel Mega 644 microcontroller received user input from the pushbuttons and outputted user feedback via the LCD. This in turn communicated with the Skyetek M1 Module which transmitted power onto RFID chips in the vicinity and received a signal back via the antenna.

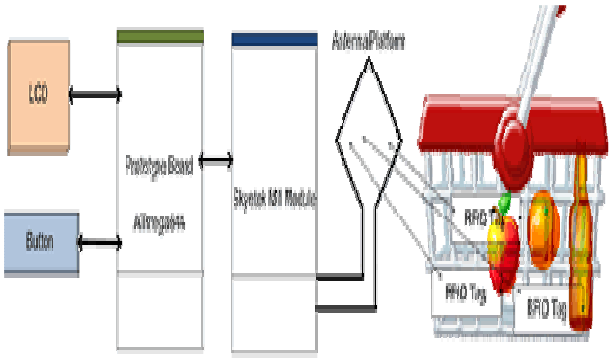

Fig 2 RFID logical structure

Multiple tags within the RFID field would not result in a problem, as each tag was told to 'stay quiet' after it had been successfully read.

2.2 System Design

The user interface for client module is a linking process between the customers and the system [6].The user interface takes all inputs for the user, and passes the information to the server to deal with database system. The sole purpose of the user can be seen in the system, and this user interface is the one module where tasks can be controlled under the server. This module is created by use of pull-down menus, buttons, tatus bars, dialog boxes, and etc. Microsoft Visual Basic 6.0 programming environment allows the programmer to easily make use of all these features without worrying about all the "behind the scenes" coding that must be done in order to make the application run in Window XP. User interface module flow chart is shown in Figure 3 .

The system design consists of customers and shop owner who owns shops. The client module contains databases which are related to category, goods, purchase details, sales details and shop owner. Figure 4 shows entity relationship diagram for shop details. Figure 5 shows the system design of flow chart. Figure 6 shows data flow diagram for the shop owner process that checks whether member or not. Figure 7 shows data flow diagram for the customer process that checks whether member or not. Figure 8 shows data flow diagram for purchasing goods process by shop owner. Figure 9shows data flow diagram for selling goods process by shop owner. Figure 10. shows data flow diagram for viewing sales details. Figure11 shows data flow diagram for purchasing items by customer. Figure 12. shows data flow diagram for viewing purchase details

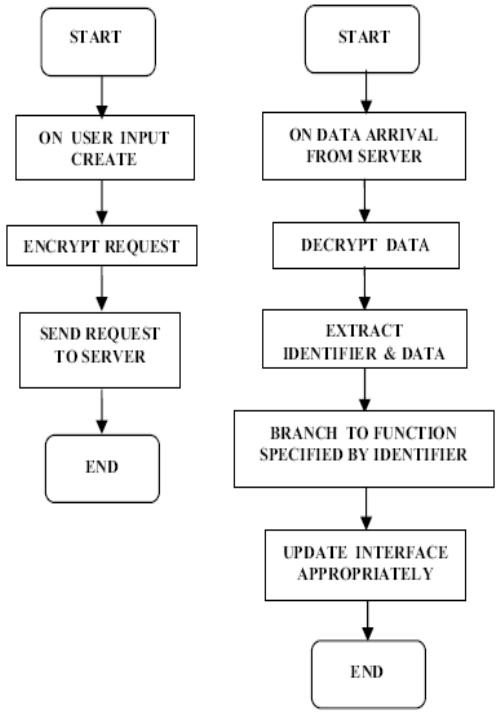

Fig.3 User Interface Module Flow Chart

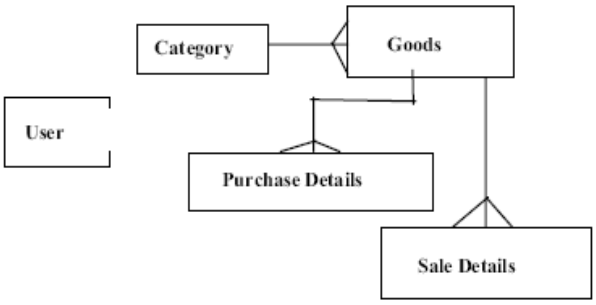

Fig 4 Entity Relationship Diagram for Shop Details

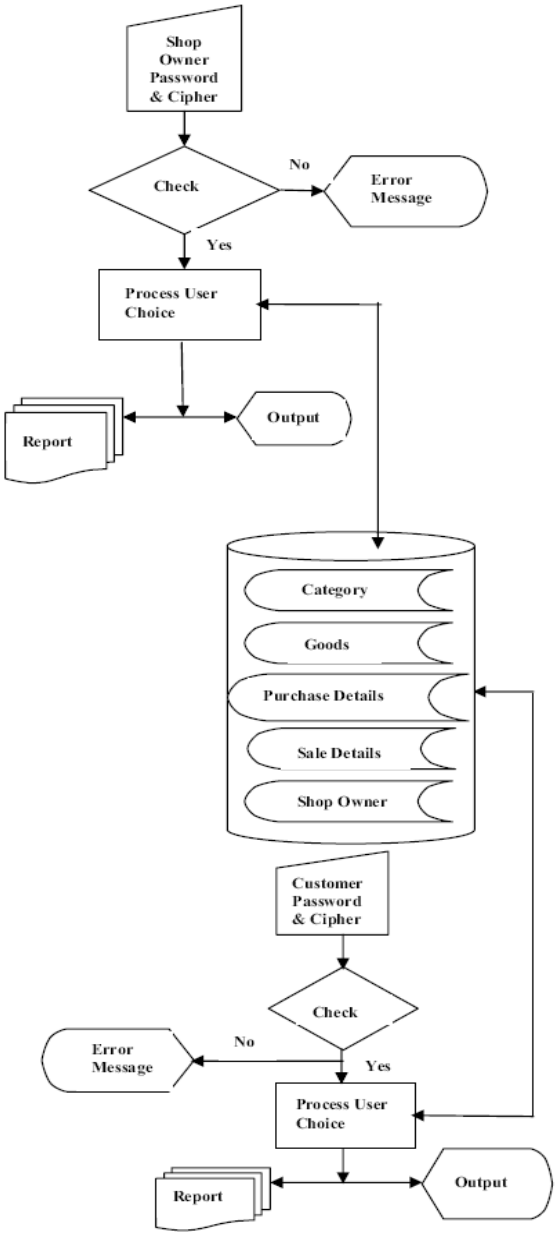

Fig.5. The System of Flow Chart

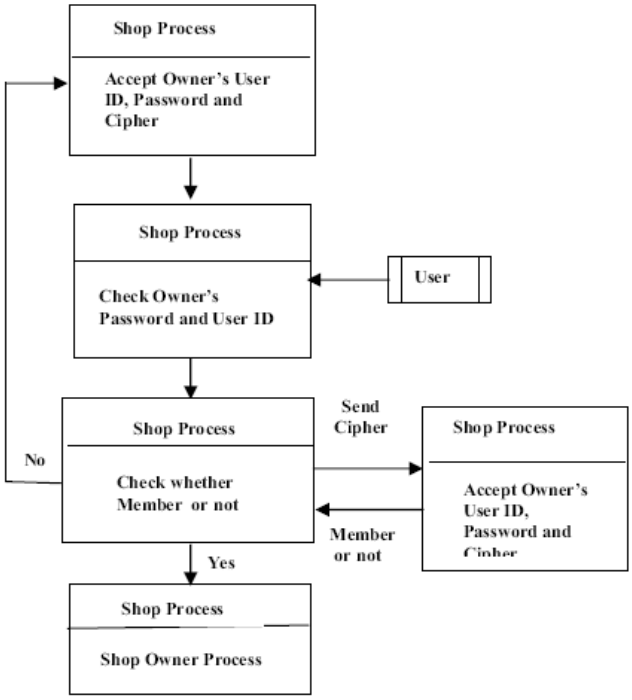

Fig.6 Data Flow Diagram for the shop Owner Process that Checks Whether Member or Not

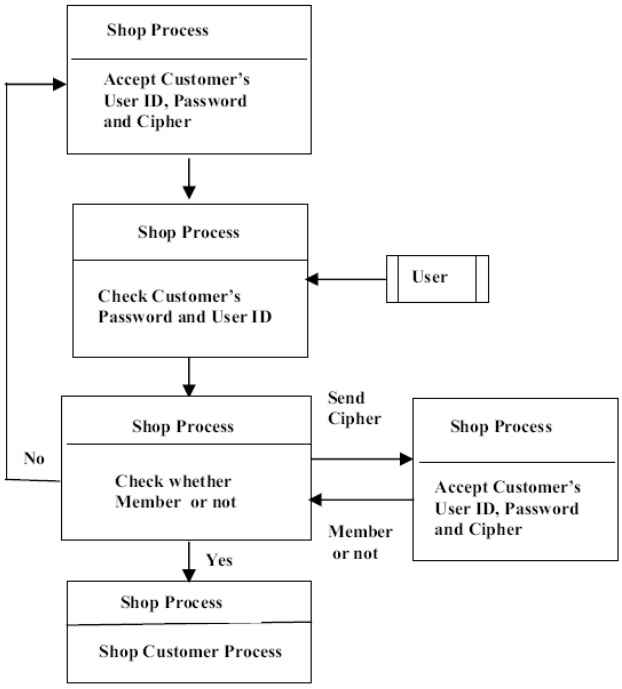

Fig. 7. Data Flow Diagram for the Customer Process that Checks Whether Member or Not

III The Secure Mobile Payment Model

The customer selects the payment method by mobile phone and submits the phone number to the merchant to terminate the negotiation phase. As soon as received the transaction order by the mobile device sent from the merchant server, the user begins with the payment one. In this phase the payment protocol is performed. The execution of the protocol involves the issuer, the acquirer, the payment gateway, the merchant and the customer. First of all, of course, mobile payment application should have been installed and initialized in smart card of user's mobile device. In order to provide the forms of remote mobile payment services, we informally assume that the user's mobile device is equipped with a smart card which has installed the secure remote mobile payment application. Furthermore, we assume that the personal mobile device is issued with a master key trusted by the user to digitally sign payment orders, and with a PIN of which the customer enters the menu of mobile payment services in mobile device. Both the master key and the PIN are stored in the smart card to physically protect them from unauthorized accesses. Finally, we assume that production, distribution, and personalization of the smart cards are securely done off-line with well known means. The money is transferred actuarially to the acquirer's accounts during the settlement phase. The acquirer requests a payment authorization to the financial network if holds related authorizations. Periodically, the merchant servers send the payment authorizations received in the payment phase to their acquirers.

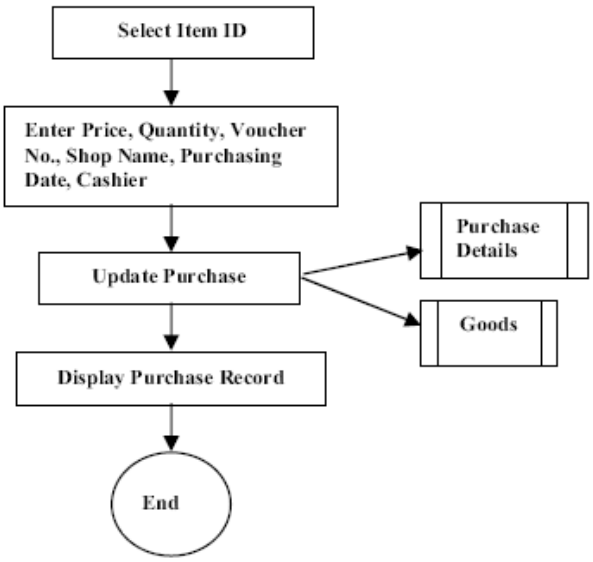

Fig.8 Data Flow Diagram for Purchasing Goods Process by Shop Owner

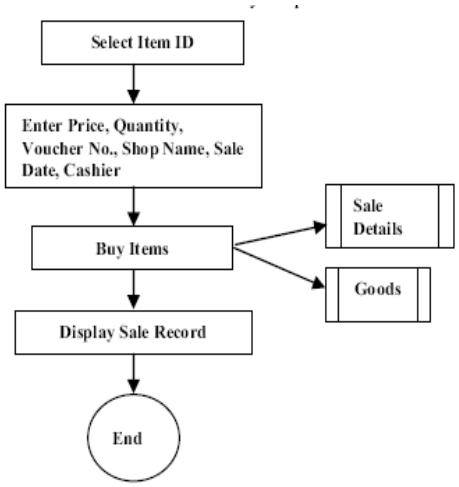

Fig.9 Data Flow Diagram for Selling Goods Process by Shop Owner

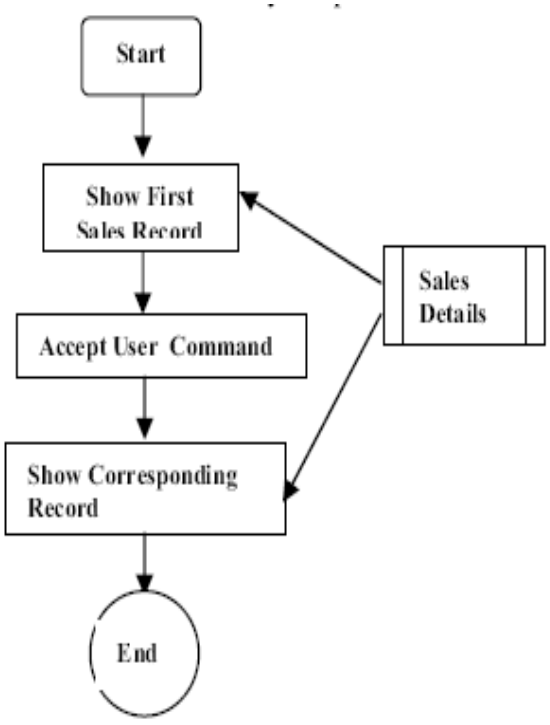

Fig.10 Data Flow Diagram for Viewing Sales Details

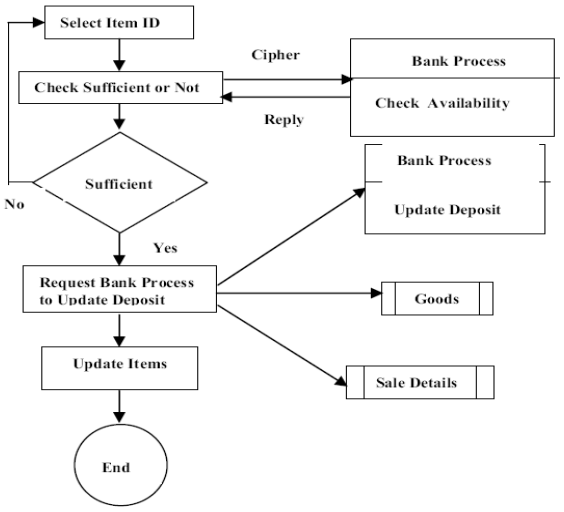

Fig. 11. Data Flow Diagram For Purchasing Items By Customer.

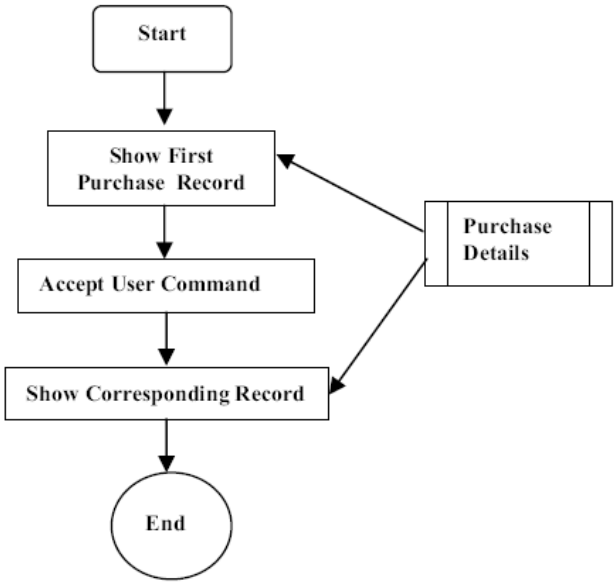

Fig. 12. Data Flow Diagram for Viewing Purchase Details

(a) Login for Shop

In this form, the user must enter the user name, user ID, password and cipher for authentication as shown in Figure13.The first user must be shop owner to access her shop. She must enter words as the cipher which can be obtained by running the RC5 encryption program for security. And then click the "OK" button. If authentication had been successful,the user can use the system. Otherwise, the system will display a message box that informs the user who is not a member. The user can quit this form by clicking the "cancel" button. After authentication has been successful, the system displays "Welcome to Shopping Center" and then secure mobile payment system window will appear.

Fig. 13. Design Window of Login for Shop

IV Secure mobile payment system

With reference to figure 14, the payment protocol consists of the following actions:

(1) The critical data are encrypted by the new session key.

(2) The mobile device sends the message with the encrypted payment data to the merchant.

(3) In the payment phase, the merchant information about the account (MerAccInfo) is necessary. So the merchant has to add the acquiring bank ID and the account info to the message before requesting for the payment authorization.

(4) The secure mobile payment message is sent to the issuer over the payment gateway.

(5) After decrypting the payment data, the issuer verifies the validity, integrity and authenticity. At the same time the system checks the balance of the user's payment account. None but all data of the message are right as well as having enough money, the issuer will perform the transaction. Otherwise the transaction cannot be completed and the message with fault information will be sent to both the user and the merchant.

(6) A request of payment confirmation is sent to the mobile device and the user gives back the answer about the payment.

(7) The payment results along with the new balance of the payment account and a new random number are sent to the mobile device. Also the authorization is sent to the merchant.

(8) The merchant gives related services or goods to the user. Periodically, the merchant submits the settlement request including payment authorizations to the acquirer to begin the settlement phase.

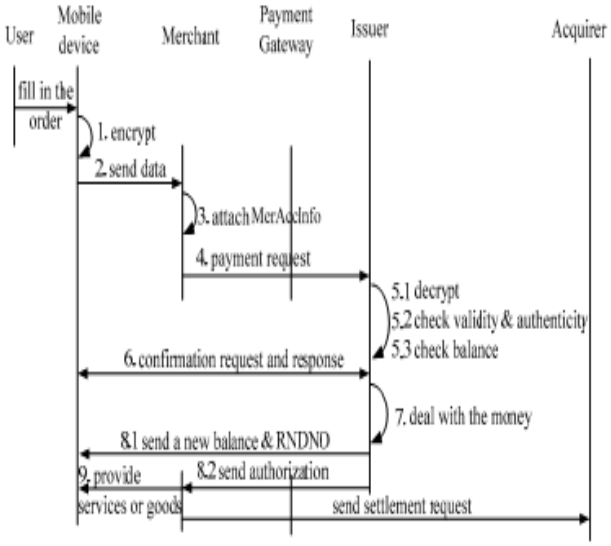

Fig 14 Secure mobile payment procedure

Security policies and implementation

In order to use the mobile payment system described in this paper over the GSM network (e.g., SMS,USSD, and future transport mechanisms), the smart card or SIM is required to contain the payment application based on the SIM Application Toolkit(SAT). The SAT is a set of commands and procedures that allow operators and other providers to create applications that reside on the SIM. SAT provides mechanisms by means of which applications can interact and operate with any compliant mobile equipment. These mechanisms include displaying text from the SIM to the mobile equipment, sending and receiving SMS messages, and initiating a dialogue with the user.
As shown in figure15, an application need to be authorized and transfer the security state of the card to another which is satisfied with the requirement of security properties before accessing the secret resource, or else COS will refuse the access. In addition, the COS system provides hardware mechanisms of tamper resistance to ensure that the platform's software stacks be not easily modified to be misbehave.

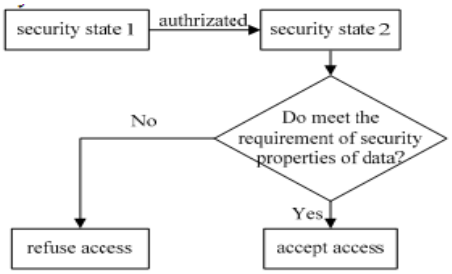

Fig 15.security state of access

The security module can be implemented by anyone of the following ways or both of them:

1) Such data as the keys, parameters, application codes, and services are written in when the card is issued.

2) The services, data and codes about applications are downloaded by OTA. It can be universal if they obey the standards and criteria of OTA which are now under enacting by related organizations.

VI Conclusion :

Some RFID tag manufacturers, like IPico, have created dual-frequency tags to combat these issues. These types of tags can achieve higher transmission rates when communication is possible at a higher frequency, yet the tag can always be read, even when placed in a glass of water because it can transmit at a lower frequency. The combined effects of easy and flexible implementation, secure transmission of account information, and reduced disputes offer the following benefits for all parties involved: 1) Increased consumer confidence, leading to increased sales. 2) Considered about the benefits of both consumers and merchants.

References

[1] G. Roussos and B. College, "Enabling Rfid in Retail", Computer, IEEE,vol. 39, no. 3, 2006, pp. 25-30.

[2] P. Kourouthanassis and G. Roussos, "Developing Consumer Friendly Pervasive Retail Systems", Pervasive computing IEEE vol. 2, no. 2,2003, pp. 32-39.

[3] S.L. Garfinkel, A. Juels and R. Pappu, "RFID Privacy: an Overview of Problems and Proposed Solutions", Security & Privacy, IEEE, vol. 3, no. 3, 2005, pp. 34-43.

[4] S.K. Misra, and N. Wickamasinghe, "Security of a mobile transaction: A trust model", Electronic Commerce Research, vol. 4, 2004, pp. 359-372.

[5] Visa International Service Association, "3-D Secure Introduction V1.0.2" , September 26, 2006.

[6] Xi Li, Hanping Hu, and Zuxi Wang. "Secure mobile payment", Application Research of Computers, 2008, vol. 25, pp. 1546-1549.