MOBILE TELEPHONE AS AN OPERATOR INDEPENDENT, SECURE MICRO-PAYMENT TOOL

Hasan AMCA* and Erbug CELEBİ**
*Electrical and Electronic Engineering Department, Eastern Mediterranean University, hasan.amca@emu.edu.tr
**Computer Science Department, Cyprus International University, ecelebi@ciu.edu.tr

ABSTRACT

With the latest advances in Information and Communication Technologies (ICT), using different technologies for electronic-payment has become a major issue in the retail market. The use of portable communication devices became particularly attractive candidates when versatility, security and simplicity considerations of payment technologies are considered.

In this paper, we investigate the use of mobile communication devices as versatile, secure and simple micro-payment tools, which satisfy the related financial, technological, computational and managerial requirements. The versatility and security of the method comes from the use of a mobile telephone and a Variable Transaction Number (VTN) in each transaction. Experimental results have shown that, the systematic requirements for the implementation of this technology are minimal and the costs involved are very much reasonable.

1. INTRODUCTION

Due to the fraudulent use, loss or damage of the card-based electronic payment (e-payment) devices such as Visa, Master-Card, Card Plus and American Express, there is a significant annual financial loss [1]. In addition, the implementation of electronic signature introduced additional security problems due to the lack of facilities to enter the Personal Identification Number (PIN) to the POS terminals. A simple but yet versatile and secure electronic payment technology could be implemented by the use of Mobile Telephones (MT), that will eliminate the security related problems due to the use of card based electronic payment devices.

MTs could be used in e-payment in several different ways. Such as, SMS, IrDa, Bluetooth, RFID [3, 16]. These methods have the common ground of charging the mobile telephone for the purchases made [4] and integrate the purchasing expenses and mobile phone bill.

Using SMS method is a premium SMS service that allows users to anonymously and securely pay for the products and services they purchased via their mobile phone by sending a text message to a premium number. The customers are then charged on their mobile phone invoice. The SMS method is designed to work in batch processing mode and therefore might take a long time to confirm the credit approval by the bank and complete the transaction [5].

Despite the well defined IrDa specifications, the relatively long setup time renders it useless for m-payment. The "express payment", designed to reduce the setup time, reduces the transaction time significantly. However, it also reduces the security of IrFM by giving the privilege to devices to bill the consumer without authentication and making them potentially vulnerable to financial fraud. It also requires an IrDA device at every merchant's counter [2,6].

Bluetooth requires a relatively long setup time before the payment process starts. Plus, it has a non-selective nature. A Bluetooth device will search for all devices within a short range. This might mean a large number of Bluetooth devices in a shopping mall [7].

The usage of RFID in m-payment could be comparable to Bluetooth and therefore is delay and complexity limited [8,9].

The method we proposed in this article uses a credit provider generated secure transaction number, unique for each transaction. This number is transformed into a barcode by the mobile terminal (MT) that can easily be read by the merchant's barcode reader. Hence, overcoming the shortcomings mentioned above in terms of latency, security and usability. The on-screen generated barcode could also be used as tickets for such places as cinema and theatre.

This method of payment could be made available in societies where Mobile Telephone usage is more widespread than the Credit Card. Most of the underdeveloped and developing countries have higher rate of mobile telephone penetration than Credit Card. Hence, m-payment in such countries can help improve on-line payment technologies as a whole by using MTs instead of CCs.

This article is organized as follows: In section 1, an introduction is made into the m-payment technologies. In section 2, a preview of online payment processing is presented. In section 3, the Variable Transaction Number Barcode (VTNB) method is described with reference to the infrastructure and security issues. Conclusions are provided in the last section.

2. ONLINE PAYMENT PROCESSING METHODS

Online payment, which may also be called electronic payment, is referred to as payment for the purchase of goods or services without using hard cash. An electronic payment solution should be secure, reliable and easy to use so that the common fraud-related risks such as product theft, identity theft and cash theft will be avoided. Electronic payment consists of 2 steps: *Authorization* and *settlement*.

Authorization verifies that the card is active and the customer has sufficient credit to make the transaction. This is shown in Figure 1. *Settlement* is the process of charging the customer's payment account and transferring money from the customer's account to the merchant's account through a transaction broker such as PayPal [14]. This is depicted in Figure 2 below.

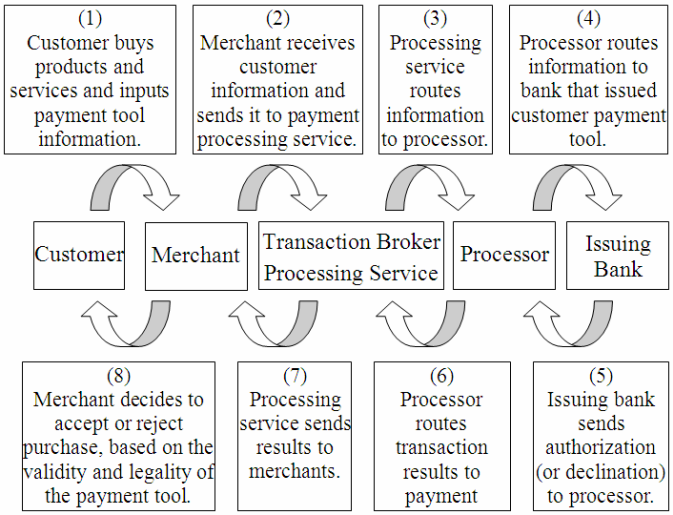

Figure 1: Payment Processing Authorization cycle.

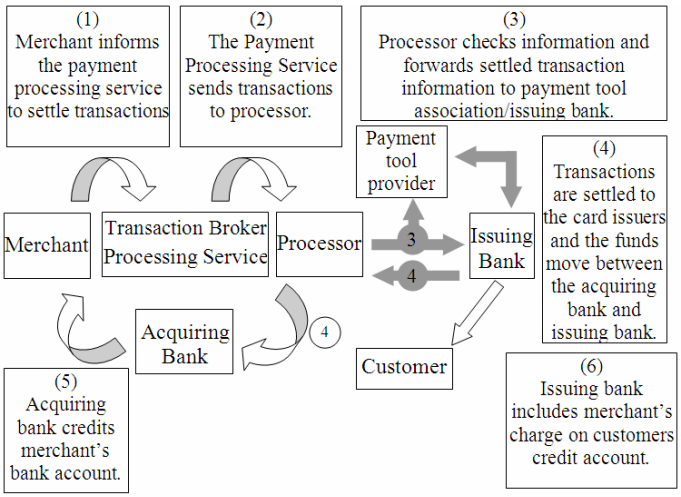

Figure 2: Payment Processing Settlement cycle.

3. THE VARIABLE TRANSACTION NUMBER BARCODE (VTNB) METHOD

The repetitive use of the fixed credit cards and the fixed verification numbers in all transactions poses a major threat on the use of the credit cards such as Visa, Master-Card and American Express, since such numbers are easy to remember and relatively easy for some attackers to steal them. Some common ways of unlawfully obtaining credit card information such as shoulder surfing, dumpster diving, packet intercepting and database stealing are presented in [2, 13]:

Due to the fraudulent use, loss or damage problems, yearly, there is a significant financial loss [2]. Not only does the credit card fraud cause money loss, but also significant worry among customers. Hence, a successful method for payment should eliminate these problems and allow customers to use the payment technique without worry.

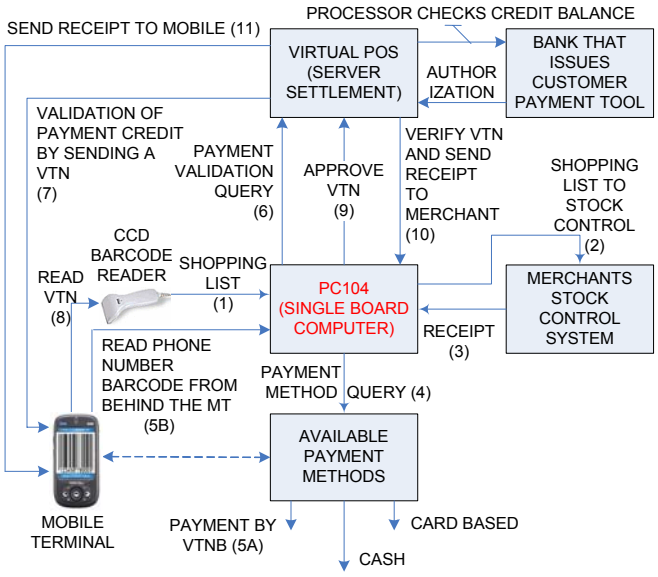

Figure 3: VTNB Payment processing system authorization cycle.

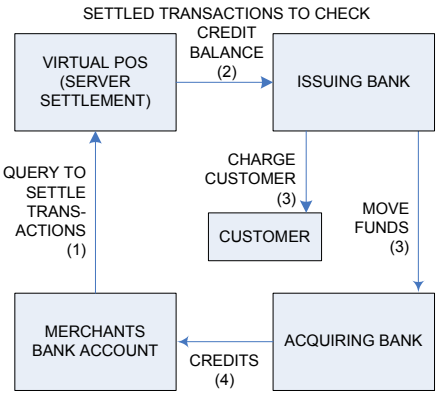

Figure 4: VTNB Payment processing system settlement cycle.

As a candidate for secure payment method, m-payment should depend on different factors such as: systematic simplicity and feasibility, open architecture, short transaction delay, ease of use by the target customers, interoperability between different vendors and security. The VTNB method will use the existing telecommunications infrastructure and satisfy all of the above criteria as follows.

3.1. Systematic Simplicity and Feasibility

The systematic simplicity and feasibility refers to the additional hardware and software required to build the VTNB over the existing payment system. The VTNB system should also be fast, traversing minimum number of proprietary networks. This way, payment of small amounts is possible since network usage is limited and the overhead is low. This can be better understood with reference to Figure 3 and Figure 4.

The VTNB method of payment is basically similar to the credit card method except that, in the former the onscreen barcode is read by the barcode reader and manipulated by the terminal device replacing the POS terminal. The terminal device is a single board computer with a GPRS support and a

USB sockets. A PC104 running on Linux could be used to produce the terminal device as shown in Figure 5.

Figure 5: A PC104 single board computer running on Linux used to produce the terminal device.

3.2. Layered Protocol Architecture

The widespread acceptance of the VTNB method depends on the choice of the architecture and the communication protocol. The architecture should support the Open System Interconnection (OSI) architecture so that different vendors could produce electronic equipment such as the VTNB processor compatible with the barcode reader and the merchants stock control system. The layers of VTNB protocol stack are shown in Figure 6 [10, 11]:

The OSI 7-Layered Architecture is preferred instead of the TCP/IP Protocol Suite due to reliability and efficiency concerns. Unlike TCP/IP, in OSI, services offered by the IP layer are reliable. TCP/IP does not provide a mechanism for secure flow control and does not guarantee delivery nor notify the end host system about packet loss due to errors or network congestion [10]. Overhead in OSI is relatively small for small packets [15]. Furthermore, since TCP was designed for wired networks, it does not perform well over wireless links where packets are frequently dropped because of bit-errors. Layer of VTNB protocol stack, are as in [10,11].

The application layer of VTNB hosts the application program responsible for receiving the VTN through the GPRS channel and performing the necessary operations. Steps 5, 7, 8 and 11 in Figure 3 are defined in the VTNB Application Layer Protocol.

After the transaction amount is displayed on the merchants terminal screen, the customer decides to pay by VTNB method. Payment is initiated by reading the barcode from the back cover of the MT, waiting for accept/reject payment response from the VPOS. Accepting the payment amount and presenting the barcode for the merchant's CCD barcode reader to finalize payment process (5-8) is followed by verification of the VTN by the VPOS (10). The on-line connection to the VPOS is provided by the module on the cash register instead of the POS device, hence eliminating the need to a number of POS devices.

An additional security level is created by introducing the entry of PIN number to the MT during the payment cycle right after step 7. Once the user accepts (by entering the PIN code on the MT) to pay the amount on the merchants screen, the payment process is completed.

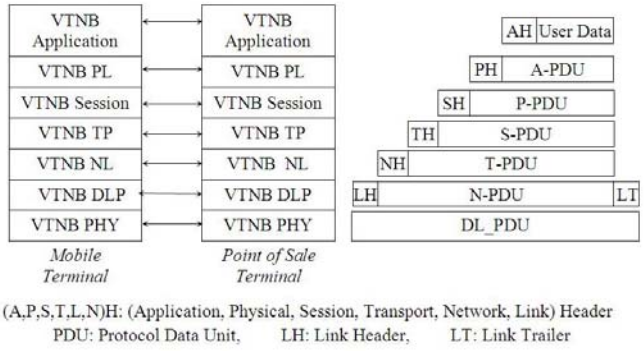

Figure 6: The 7 layer protocol stack for connection management between the MT and the POS terminal.

The VTNB payment system is suitable for other applications such as petrol stations, vending machines, buses, car parks, ATM's, cinema entrance, classroom attendance check etc.

3.3. Transaction Delay

Transaction delay is one of the most important factors for acceptability of an electronic payment system. Literature survey has shown that, ideally, such a delay should be less than 1 second [12]. The transaction delay in VTNB system is expected to be longer than that of the Bluetooth, RFID and IrDA but similar to the conventional Credit Card (CC). The delay is due to the reading of the phone number barcode, applying to the VPOS for a VTN, validation and granting VTN, reading VTN by barcode reader, verification of VTN and billing mechanism. The VTN is randomly drawn from a set with a negotiation between the financial service provider and the mobile terminal (MT), preferably as a function of the International Mobile Equipment Identity (IMEI) number of the MT. The provision of the VTN is the major challenge in the proposed method of payment and more research is to be made to eliminate delay in generating VTN without compromising security. The delays involved are presented in Figure 7.

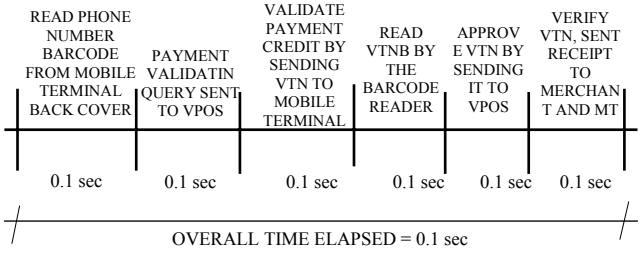

Figure 7: The delays involved in VTNB method.

Parameters effecting delay are; set-up time, connection time, data transfer time, processing time, security verification time and disconnection time. The following section clarifies the delay mechanism. The LOOP delay in VTNB Mobile Payment System includes,

1. reading and transmitting the MT number barcode from the back cover of the mobile telephone,
2. payment validation query transmitted to the VPOS
3. Validation of the payment query by sending a VTN to the MT
4. reading the VTNB
5. sending the VTNB to the VPOS for approval
6. verifying the VTN and sending the receipt to both the merchant and the customer

3.4. Ease of Use by the Target Customer

The usage of the VTNB technology is as simple as sliding a good in front of the barcode reader, basically, nothing more than using the mobile telephone as a credit card. The users are not expected to have any special skills to adapt to the method. The only requirement is the need to register for the service prior to usage. In countries where the use of credit card is not widespread but the MT penetration rate is high, the VTNB system is expected to find high level of acceptance by the public.

3.5. Interoperability between Different Vendors

A set of global foundational m-payment standards need to be agreed upon in order for content providers to reach a critical mass of paying customers who, in turn, will then have a plentiful supply of applications and services to choose from. This will enable widespread availability of m-payment and the target customer range will also increase.

For the VTNB method to pick up easily and spread all around the world, a standardized communication and interconnection standard should be adapted in order for the equipment manufacturers to produce devices that will interoperate with the, then existing, VTNB system. This requirement is satisfied by the use of OSI architecture, as described above.

3.6. Security

VTN is made random in order to avoid reproducing without the MT holders consent. VTN could be accompanied by the PIN number of the MT user. The process of entering PIN number to the POS machine could easily be replaced by entering the PIN number on your mobile, in privacy and comfort of your palm. User portability is provided by the SIM card and the MT number barcode behind the telephone.

Other security issues: The loss or theft of consumers' wallets with their physical credit cards will not be noticeable until the next time they carry out a purchase. This can occur anytime from immediately to several days later. However, the awareness of a loss or theft of one's MT can be felt immediately.

Keeping and protecting the paper receipts for future reference is also a security issue in m-payment method. Paper receipts can be lost and cause consumer inconvenience and dissatisfaction in CC payment systems. However, the storage nature of the MT helps to protect receipts and work them out easily in the electronic form.

4. CONCLUSION

The future m-payment services are expected to be simple, fast, easy to use, reliable, interoperable between different vendors, secure, and technically feasible. For such services to be successful, service provisioning by banks, operators and terminal manufacturers have to be independent from each other. Banks manage the authentication in their banking and payment services. Easy-to-use and fast-to-use services that offer value for money are the key success factors to wide-scale customer acceptance in mobile financial service area.

Due to the security gap in Credit Card usage, mobile telephones are better candidates as authentication and payment devices. The Variable Transaction Number Barcode system of m-payment is introduced as an alternative method of payment. This method is shown to be more efficient, faster and more secure than all of the other electronic payment systems

For prepaid mobile customers, the new m-payment solution will not require topping up their phone via scratch cards, credit cards, or ATM. VTNB solution delivers a high level of security as it requires a PIN for authentication of the user's identity. In addition, by providing payment direct from the user's bank account, m-payment means the spending power of users is not limited to the amount of credit available on their phone account.

5. REFERENCES

[1] Eliminating Some Credit Card Risk for E-Business, http://ecommerce.Internet.com/solutions/ec101/article/0,1467,6321_569741,00.html.

[2] Internet Usage Statistics – The Big Picture, http://www.internetworldstats.com/

[3] Pi Huang And A.C. Boucouvalas, Future Personal "E-Payment: Irfm", IEEE Wireless Communications, pp. 60-66, Feb. 2006.

[4] S. Schwiderski-Grosche and H. Knospe, "Secure Mobile Commerce", *Electronics & Communication Engineering Journal*, October 2002, pp. 228-238.

[5] S. F. Mjpllsnes and C. Rong, "On-line e-wallet system with decentralized credential keepers," *Mobile Network Applications,* vol. *8* , pp. 87--99,2003.

[6] IrDA, Infrared Financial Messaging Point and Pay Profile (IrFM), ver. 1.0, Dec. 2003.

[7] Bluetooth Core Specification, ver. 1.2+EDR, Bluetooth SIG, Nov. 2003.

[8] Weiping Z.H.U, Dong WANG and Huanye SHENG, "Mobile RFID Technology for Improving M-Commerce". Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'05), March 2005, Shanghai, China.

[9] Raj BRIDGELALL, "Enabling Mobile Commerce Through Pervasive Communications with Ubiquitous RF Tags", Wireless Communications and Networking, WCNC 2003, Volume 3, Page(s):2041 – 2046, 16-20 March 2003.

[10] William Stallings, "Data and Computer Communications, Seventh Edition", Prentice-Hall, 2004.

[11] C.D. KNUTSON and J.M. BROWN, "IrDA Principles and Protocols:" The IrDA Library, Vol.1, MCL Press, 2004.

[12] H.R. DAMON, R.J. BROWN, and L. FAULKNER, White Paper, "Creating an End-To-End Digital Payment System," *IrDA Press*, Oct. 1999.

[13] Yingjiu Li and Xinwen Zhang, "A Security-Enhanced One-Time Payment Scheme for Credit Card", Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications, RIDE-WS-ECEG'2004, Boston, USA , March 28-29, 2004.

[14] PayPal "Online Payment Processing", https://www.paypal.com/cgi-bin/webscr?cmd=_wp-pro-overview-outside.

[15] Sami IREN, Paul D. AMER and Phillip T. CONRAD, "The Transport Layer: Tutorial and Survey", *ACM Computing Surveys*, Vol. 31, No. 4, December 1999.

[16] Hasan Amca And Raygan Kansoy, "A Mobile Telephone Based, Secure Micro-Payment Technology Using The Existing ICT Infrastructure"**,** Chinacom 2007: International Conference On Communications and Networking In China, 22-24 Aug. 2007, Shanghai, China.