Business Aspects of Mobile Payments

Ljupco Antovski[1], Marjan Gusev[1]

Abstract – **M-Commerce like E-Commerce can be B2B (business to business), P2P (person to person) or B2C (business to customer) oriented. No successful mobile payment system has yet lived up the different requirements from the market and thereby not been a success. A brief research on the state of the market is given to present a framework for possible solutions. The purpose of this paper is to describe the factors that affect the introduction of a successful M-Payment system.**

Keywords – **M-Commerce, J2ME, HTTPS, cryptology, FSP**

I. Introduction

Mobile phones are already approaching penetration rates higher than 80 per cent in some parts of the world. Penetration is considerably lower but growth rates are high. High market penetration and a number of technical features make mobile phones very interesting commerce devices.

With the growing momentum of wireless revolution and M-Commerce explosion, it is evident that mobile devices are becoming a critical component of the new digital economy.

The transactions are rapidly transitioning from fixed locations, to anytime, anywhere and anyone. New forms of mobile technologies are rapidly transforming the marketplace. Optimists are of the opinion that the new world economy will witness the transition of mobile devices from a simple communication device to a payments mechanism. [14]

There have been different definitions of M-Commerce. Lehman defines M-Commerce as "*the use of mobile handheld devices to communicate, inform, transact and entertain using text and data via connection to public and private networks*" [25]. Their reason for using such a broad definition is because the borders between messaging and commerce have become too blurred to separate these categories. Another definition is "finance transaction especially buying and selling: trading"[26]. Durlacher research's use a fairly broad definition as they as more distinct and is as follows: "any transaction with a monetary value that is conducted via a mobile telecommunication network" [25] M-Commerce contributes the potential to deliver most of what the internet can offer, plus the advantage of mobility. M-Commerce gives mobile communication devices as mobile phones and personal digital assistants (PDA) the ability to pay for goods and services.

II. Services

While most of existing eCommerce application can be modified to run a wireless environment, M-Commerce also involves many more new applications that become possible only due to the wireless infrastructure.

These applications include mobile financial services, user and location specific mobile advertising, mobile inventory management, wireless business re-engineering, and mobile interactive games. In addition to device and wireless constraints, M-Commerce would also be impacted by the dependability of wireless infrastructure.

M-Commerce existing and futures possible application include:

- Mobile banking service (check account information, money transfer)
- Mobile trade service (stock quotes, selling/buying)
- Credit card information (account balance)
- Life insurance account information (account information, money transfer)
- Airline (online reservation, mileage account check)
- Travel (online reservation, timetables)
- Concert ticket reservation (online or telephone booking)
- Sales (online books, CDs)
- Entertainment (games)
- News/information (headline, sports, weather, horse racing information, business,
- technology, regional)
- Database, application (yellow pages, dictionary, restaurant guide)
- Location based application (area information and guides)

III. M-Commerce Segments

M-Commerce like E-Commerce can be B2B (business to business), P2P (person to person) or B2C (business to customer) oriented. The scope of this paper is on the B2C model.

In the B2C area, M-Commerce is still in its infancy. This is due to the limitations of present, intermediate technologies such as WAP, and to the relative lack of compelling contents and services. Certain B2C services (e.g. online banking) may charge a small monthly free, but it is similar to that of comparable offline service (e.g., maintenance fee for checking accounts) and are waived under certain circumstances (e.g., if a minimum balance criterion is met), hence monetary cost is not a constraint on B2C E-Commerce acceptance [27].

The M-Commerce framework divides into couple sub areas based on user's distribution criterion. Mobile E-Commerce addresses electronic commerce via mobile devices, where the consumer is not in physical or eye contact

[1]Both authors are with the Institute of Informatics, Faculty of Natural Sciences and Mathematics, Ss. Cyril and Methodius University, Arhimedova b.b., PO Box 162, 1000 Skopje, Macedonia, Email: anto@ii.edu.mk, marjan@ii.edu.mk

with the goods that are being purchased. On the contrary in M-Trade the consumer has eye contact with offered products and services. In both cases the payment procedure is executed via the mobile network [1,5].

M-Commerce involves procedures of M-Payments (Mobile Payments) defined as payments carried out via mobile devices. The highest state of security has to be implemented in these procedures in order to ensure full reliability and trust from the customers in the system [1].

Principally, M-Payments can be used for M-Commerce, E-Commerce and in the real world. In the real world, it is the number of mobile phones that makes them a promising payment device. In 2000, trade via handy, pager and handheld has created revenues of EUR 1.3 billion in Europe and is expected to rise to EUR 3.8 billion in 2003 (BITKOM). The corresponding estimate for global M-Commerce in 2003 is USD 13 billion (Barnett/Hodges/Wilshire). By this estimates by 2005, data traffic is expected to be more important than voice traffic [12]. Similar research by Andersen [13] estimates that the European mobile content market size could range between EUR 7.8 billion to EUR 27.4 billion in 2006, with a median forecast of EUR 18.9 billion.

Many mobile operators have started offering M-Payment services. These services are in early stage and still in beta state. Several operators team up with banks while others manage M-Payment on their own [10].

There is a wide range of solutions concerning mobile payments services. The security implementation spreads from SMS messaging, PIN confirmation to financial message signing, encryption, use of tamper-resistant devices and digital certificates. Main characteristic of all this solutions is that they could only be used by limited number of users that fulfill the required technical specification.

IV. Current Protocols and Technologies

No new special network standard is needed to carry out M-Payment transactions. M-Payments are therefore carried out through existing networks, which could be Cellular networks (GSM/2,5G/3G), Wireless LAN (IEEE 802.11 protocol), Bluetooth and Infrared (irDa)

The most important technologies for M-Payment connectivity are: SIM Application Toolkit (SAT), WAP/WTLS/WIM, Voice and Manufacturer specific Applications SAT is a technology that allows configuring and programming the SIM card [15]. The SIM card contains simple application logic that is able to exchange data with the SMSC, to carry out M-Payment transactions. The specific mobile operator provides the application logic and is responsible of providing the SIM card.

Phones equipped with a WAP-browser are able to exchange data with a web server. Data is transmitted via wireless application protocol and the networks are GSM, 2.5G or 3G. WTLS is a layer in the WAP stack and is the wireless edition of the SSL 3.0 in a reduced scale. WTLS can provide secure connections for transferring confidential data [16]. WIM is a module for storing data in the mobile device and is usually used in relation to WAP transactions. WIM is used with WTLS transaction to protect permanent, typically certified, private keys. The WIM stores these keys and performs operation using these keys [17].

The end-user can via a normal phone call state his credit card number to the merchant that transfers the funds via interface provided by a PSP. A voice response system at the payment service provider can also call the end-user and guide him through a payment procedure. Voice recognition can also be used as an authentication tool for payment settlement.

The mobile phone manufacturers can chose to install native applications, which in interaction with one of the above technologies enables M-Payment opportunities.

V. Critical Success Factors

There are six main actors involved in a Mobile Payment System(MPS) [ShSw98] [Pay01]: Financial service providers (FSP), Payment service providers (PSP), Merchants, End-users, Network service Providers (NSP) and Device Manufacturers. These are further divided in users and system providers. There are different critical success factors and requirements considering the involvement of different actors.

Table 1. Critical success factors

Factor	Features
Ease of use	few clicks, intuitive, flexibility, performance, installing/download
Security	privacy, confidentiality, integrity, authentication, verification / non repudiation
Comprehensiveness	transferability, divisibility, standardization.
Expenses	set up fees, transaction fees, subscription fees
Technical Acceptability	integration effort, interoperability, scalability, remote access, performance

An important means of getting a successful MPS is obtaining acceptance from all the participants in the network and thereby achieving a critical mass. By comprehensive study from several authors [18, 19] success factors are identified: Ease of use, Security, Comprehensiveness, Expenses and Technical Acceptability. The Table 2 is an overview of the main factors features.

VI. New M-Payment Method

The foundation and ideology Java 2 Micro Edition (J2ME) brings itself a reasonable set of potentials of being a part in a MPS. There are several concrete arguments that indicate why J2ME should be considered as an interesting supplement for

M-Payments as: Broad customers experience, Comprehensiveness, Lower network and server load, Internet Enabled, Constant storage, Sun Microsystems have added an unofficial support for HTTPS (kSSL) as a part of the MIDP 1.0.3 reference implementation and the J2ME Wireless Toolkit version 1.0.3 [23]. HTTPS is not required by the MIDP 1.0 specification but if device manufactures releases devices supporting HTTPS, they will in theory be able to carry out secure transactions. In order to overcome the cryptographic gap a concrete initiative called Bouncy Castle has released a lightweight API (BC-API) with cryptology and certificate facilities, designed for J2ME. The BC-API provides a security toolbox obtained from the original Java Cryptography Architecture (JCA) and the JAVA Cryptography Extension (JCE) and has been boiled down to support the CDC and CLDC devices [24].

Considering the above exposed features of J2ME we propose a new M-Payment protocol that has the HTTP protocol as bearer. Due to the fact that SSL is still not supported in MIDP specification, the encryption, signing and certificate verification is managed at application level using the BC-API third party classes.

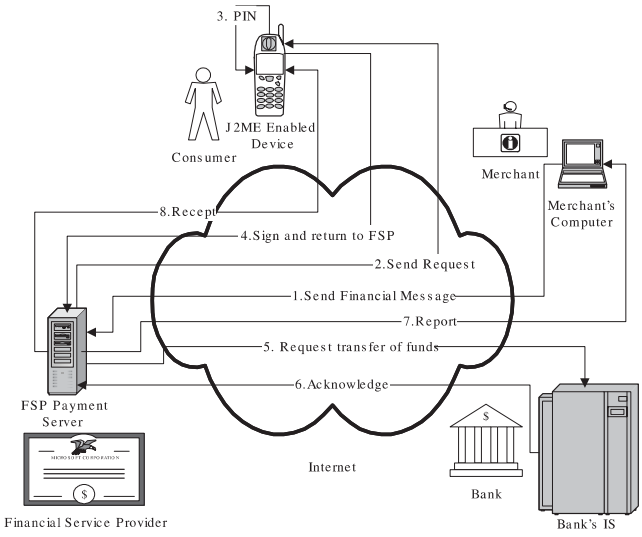

Fig. 1. M-Payment Protocol

The protocol (Fig.1) is executed in the following manner:

1. The merchant's computer issues a financial message that is encrypted and signed. Over secure Internet connection, (over SSL) the FSP receives the message.

2. The FSP verifies the source, signs, encrypts and redirects the message to the designated mobile user.

3. The user receives the message and verifies the source. If the source is the FSP gateway, the procedure continues otherwise it terminates. Afterwards the user enters PIN (or password) which is used to decrypt the encrypted private key stored in the persistent record store. Then the message is encrypted by asymmetric algorithm with session secret and sent to the FSP.

4. The encrypted message is send to the FSP. It validates the message source.

5. The FSP validates the signature. Then a request is send to the bank's information server to begin transaction from customers to merchant's account. In other scenarios the transfer of funds is from one account to another in the mobile operator's network. These accounts could be prepaid or postpaid, that involves additional procedures for validation and clearing.

6. The FSP is acknowledged after successful transfer of funds.

7. The merchant receives notification.

8. The user receives receipt in digital manner.

The procedure emphasized above addresses the M-Trade scenario. In the mobile E-Commerce scenario the procedure differs in the first steps when the user chooses the products and services and in the last steps when the merchant receives the report of successful payment and initiates shipment.

In order to lower the network load a new message system is introduced. The message transferred by the Interactive Message System (iMS) is predefined and contains financial and address data. The message represents a virtual envelope with enclosed letter. The message is divided in three sections [1]. The Extendable Markup Language (XML) is used to define the structure of the message [8].

VII. Conclusion and Future Work

It is evident that M-Payment methods are here to stay with M-Commerce gaining momentum. Lack of standards and security within devices as well as network may be pertinent issues for the future of M-Payments. A range of solutions involving financial institutions and mobile service providers seem to be in progress, and perhaps is the key to addressing these issues. The lack of standards across economies may be addressed through various consortiums, involving many economic forums, mobile operators and also financial institutions, if M-Commerce has to be diffused into the mass-market. Security has been an issue of M-Commerce development right from the start of this effort. Current infrastructures considering the limitations and enhancements, offer a comfortable environment for secure mobile payment transactions. Many challenges are involved in building an M-Commerce solution, and just as many ”solutions” available on the market. The comprehensive M-Payment suite combines strategy and analysis with rapid, fully customized technical solution development and implementation, resulting in a high return on the investments. The above proposed models of mobile payments are easy to implement considering the available technology infrastructure. The models are simple, secure and scalable.

References

[1] M. Gusev, Lj. Antovski, G. Armenski; “Models of mobile payments”, Proceedings of the 2nd WSEAS International Conference on Multimedia, Internet and Video Technologies (ICOMIV 2002), ISBN 960-8052-68-8, 25-28 September 2002, Skiathos, pp. 3581-3586

[2] O. Pfaff, Identifying how WAP can be used for secure m-business, Proc. of 3RD Wireless m-business Security Forum, 29-30 January 2002, Barcelona

[3] D. Amor, The E-business Revolution, New Jersey: Hewlett Packard Books, 2002

[4] Lj. Antovski, M. Gusev, Ebanking-developing future with advanced technologies. Proc. of 2nd Conf. on Informatics and IT, December 2001, Skopje, pp. 154-164

[5] D. Bulbrook, WAP: A Beginner's Guide, New York: Osborne/McGraw-Hill, 2001

[6] M. Gusev, E-Commerce, a big step towards e-business. Proc. of 2nd SEETI Conf. On Trade Initiative and Commerce, November 2000, Skopje

[7] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, Feb.1978 Vol.21, pp.120-126

[8] W3C: http://www.w3.org (accessed 20.10.2002)

[9] WAP-forum: http://www.wapforum.org (accessed 15.10.2002)

[10] H. Knospe, S. Schwiderski - Grosche, Online payment for access to heterogeneous mobile networks, Proc. of IST Mobile & Wireless Telecommunications Summit 2002, June 2002, pp.745-752

[11] S. Pantis, N. Morphis, E. Felt, B. Reufenheuser, A. Bohm, Service Scenarios and business models for mobile commerce, Proc. of IST Mobile & Wireless Telecommunications Summit 2002, June 2002, pp 551-561

[12] Niko Mykkanen, Mobile Payments - A report into the state of the market, Commerce Net, Scandinavia, October 2001

[13] European Commission DGIS, Digital content for global mobile services final report, Andersen, Europe, February 2002

[14] M.Ding, and C. Unnithan, Mobile Payments (mPayments) – An Exploratory Study of Emerging Issues and Future Trends, School Working Papers Series 2002, Deakin University

[15] Guthery, Scott B. & Cronin, Mary j, Mobile Application Development with SMS and the SIM Toolkit, McGraw-Hill 2002

[16] WMLScript Crypto API Library Specification, WAP-161-WML Script Crypto - 20010620-a, Version 20-Jun-2001.

[17] Wireless Application protocol Forum Ltd, "Wireless Identity Module Specification, WAP-260-WIM-20010412-1", Version 12-july-2001.

[18] Shon T.W. and Swatman P.M.C., "Effectiveness Criteria for Internet Payment Systems", Internet Research: Electronic Networking Applications and Policy, Vol. 8, No. 3, 202-218, 1998

[19] Heijden, Hans van der, "Factors affecting the successful introduction of mobile payment systems", Vrije Universiteit Amsterdam, 2002

[20] Sun Microsystems, "Designing Wireless Enterprise Applications Using java. Technology, http://java.sun.com/blueprints/, Jan 2002.

[21] Mobile Information Device Profile (MIDP) Specification ("Specification"), Version: 1.0, Release: September 15, 2000, Copyright 2000 Sun Microsystems, Inc.

[22] Sun Microsystems, Inc. "Connected, Limited Device Configuration (CLDC) Specification, version 1.0a", Sun Microsystems, Inc., may 19, 2000.

[23] Mahmoud, Qusay H. "Secure Java MIDP programming using HTTPS with MIDP", http://www.wireless.java.sun, june 2002

[24] Bouncy Castle, the Specification, http://www.bouncycastle.org, v. 1.1.4, 2002

[25] Lehman Brothers Moving in mobile media Mode (1995, p.8)

[26] Haddon, Communication on the move: the experience of mobile technology in the 1990s. COST 248, European Commission, Sweden, Telia AB, 1997.

[27] Bhattacherjee- Anol, Acceptance of E-Commerce Services: The case of Electronic Brokerage, Man and Cybernetics, 2000