M-Commerce Services

Ljupco Antovski Marjan Gusev

Institute of Informatics, Faculty of Natural Sciences and Mathematics
Ss. Cyril and Methodius University, 1000 Skopje, FYRO Macedonia
Email: {anto,marjan}@ii.edu.mk
http://www.ii.edu.mk

Abstract. M-Commerce is defined as any transaction with monetary value that is conducted via a mobile telecommunications network. M-Commerce like E-Commerce can be B2B (business to business), P2P (person to person) or B2C (business to customer) oriented. The framework divides into couple sub areas based on user's distribution criterion. Mobile Ecommerce addresses electronic commerce via mobile devices, where the consumer is not in physical or eye contact 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. 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 iMS specification enables mobile payments with one button click. The purpose of this paper is to describe the factors that affect the introduction of a successful M-Payment system - and use these factors to examine whether the J2ME technology is suitable for building such successful M-Payment systems.

1 Introduction

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 hand-held 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.

2 M-Commerce Services

M-Commerce is an emerging discipline involving applications, mobile device, middleware, and wireless networks. 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)

3 Market 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 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].

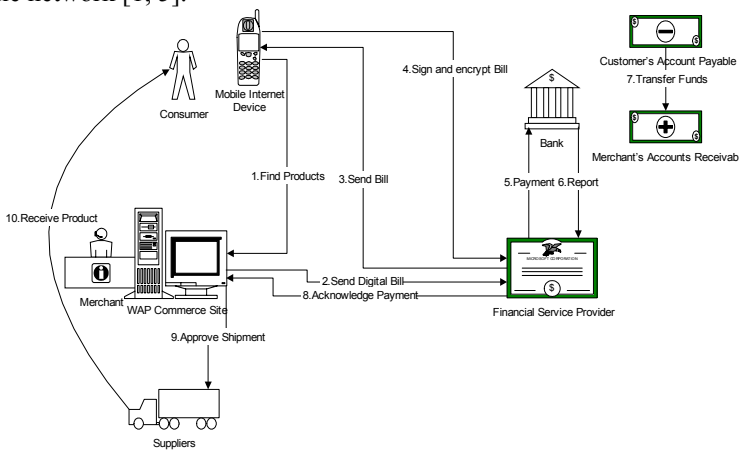

Fig. 1. Mobile E-Commerce

Mobile E-Commerce framework consists of consumer with mobile device, mobile operator that enables mobile Internet, financial service provider (FSP), bank, merchant with M-Commerce site and shipment infrastructure.

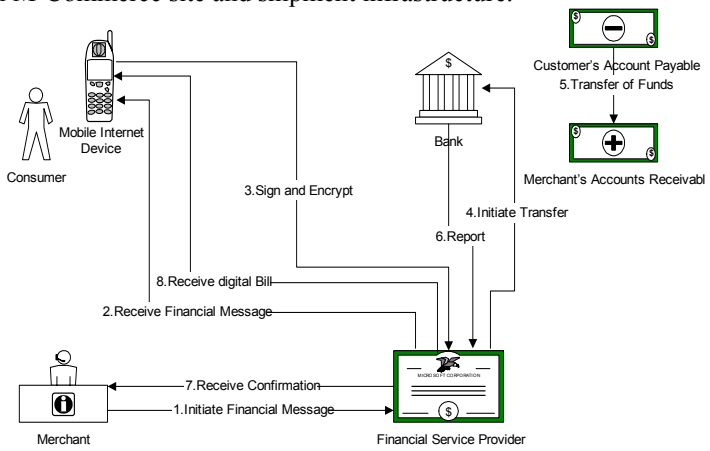

Fig. 2. M-Trade

In the M-Trade scenario presented in Fig. 2 the customer is in eye contact with the merchant. The merchant initiates the first step and prepares a financial message with predefined structure.

The digitally signed and encrypted message is sent to the FSP that decrypts and validates the message. Then it is sent back to the customer to decrypt and validate the message. His/hers role is to sign the message and return it back to FSP in encrypted form. The signing is executed in digital manner with only one button click on the mobile device. The next steps are the same as in the mobile E-Commerce scenario.

4 M-Payments Marketplace

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.

Name	Payment Service	Security aspect
Paybox & Deutsche Bank	Real and virtual POS	Cardholder authentication through the SIM card. Transmits the PIN via (DTMF).
Paiement CB & France Telecom Mobile CB	Dual slot phones with smart CB credit card.	Security lies in the credit card chip. SMS used for order confirmation.
Telia Payit	Virtual POS	Digital goods are billed either on phone bill or a Jalda pre-paid account.
Metax	Real world POS (for petrol pumps bearing the Metax brand).	Billing service validated by a PIN provided by Metax.
Sonera Mobile Pay	Real-world POS (attended & unattended).	Charged on phone bill (only low value payments), credit card.

Table 1. Mobile Payment Service Providers

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].

As presented in Table 1, 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.

5 Protocols and Technologies in Use

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 webserver. 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.

6 Success Factors

There are six main actors involved in a Mobile Payment System(MPS) [18][19]: 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.

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

Table 2. Critical Success Factors

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.

7 J2ME as Building Block

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:

Broad user experience: The J2ME™ API provides enhanced possibilities for presenting GUI's like event handling and richer graphics [20, 21].

Comprehensiveness: The details of machine architecture, operating system, and display environment are all handled transparently by the Java virtual machine (JVM). The same MIDP M-Payment client can run on all MIDP-compliant devices [21, 22]. This allows M-Payment system providers to target a wider range of end-users.

Lower network and server load: J2ME based applications can operate when disconnected and only interacts with a server when necessary. J2ME has its own runtime environment and the possibility of storing data in the mobile device.

Internet Enabled: Java is designed with a high focus on networking via HTTP or HTTPS, and Java's multi-platform capability makes it a natural choice for applications transferring data to use on the WWW.

Constant storage: The official MIDP1.0 API provides facilities for persistent storage (record store) of data [SuMIDP1]. The integrity of the record stores is kept throughout the normal use of the platform, including reboots, battery changes, etc. and is independent of any SIM/WIM [21].

There are two relevant aspects in relation to ease of use when considering the use of MIDlets. These are downloading/installing and the overall usability to carry out the transaction.A MIDlet is downloaded and installed in a single procedure. A MIDlet is

downloaded by requesting a URL directly to the specific MIDlet file (i.e. the .jad file).

Compared to WAP and SAT, the MIDP 1.0 API provides enhanced GUI and UI possibilities. Like in Java applets, MIDlets provides dynamic event handling and possibilities for graphics and dynamic image drawings, which may enhance the usability and user experience.

Apart from eventual expenditures imposed from the system providers, the only extra direct cost for the end-users is related to the airtime when downloading the MIDlet and connecting to the PSP/FSP when initiating or carrying out the payment.Besides connection fees and transfer speed, the download depends of the size of MIDlet and number and types of connections depends on the actual design of the MIDlet.

The MIDP 1.0 API does not provide official classes or packages for cryptology. There are two relevant JSRs (Java Specification Requests) in relation to cryptology and secure M-Payments according to the Java Community process(SM) Program: Mobile Information Device Profile (MIDP 2.0) and Security and Trust Services API for J2ME (JSR 177).

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].

Because MIDlets can run in any J2ME compatible device enlarges the potential target audience and opens a whole new dimension in relation to M-Payments. M-Payments with J2ME are not restricted to be carried out by mobile phones. A MIDlet can run in standalone mode, which results in fewer users accessing servers at PSP at any given time. This in turn improves performance and scalability for the payment server, and reduces demand for network bandwidth. J2ME targets a broader range of end-users via enhanced compatibility of networks and devices. These circumstances also affect the possible targeting of a wider range of PSPs and FSPs.

8 New M-Payment Method

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.

The protocol (Fig.3) 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.

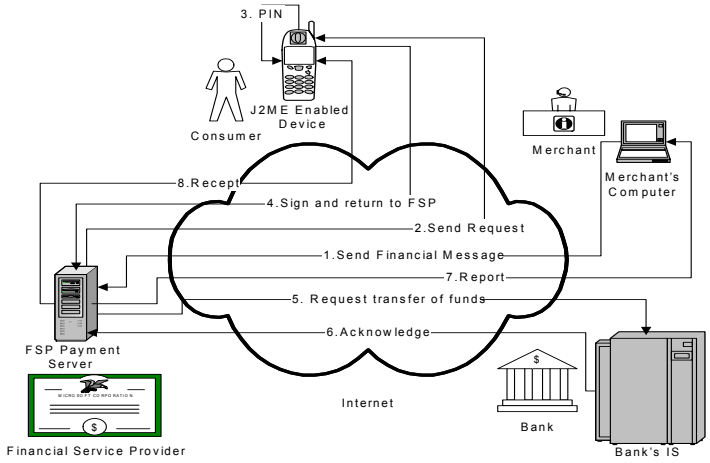

Fig. 3. New M-Payment Protocol

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.

9 Interactive Message System

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 [1]. The Extendable Markup Language (XML) is used to define the structure of the message [8].

The message is divided in three sections. The <type> section contains information about the payment procedure. The <address> section contains the information about the customer, the merchant. It also includes the signatures of the three parties included in the procedure. The <data> section contains information about the payable and receivable account, and about the amount of funds supposed to be transferred.

The Merchant fills the data for his/her identity, the customer's identity and the amount of funds. Then he/she signs the message and sends it to the FSP. The FSP fills the data for the accounts, signs and sends the message to the customer. The customer signs the message and returns it back to the FSP. The <id> fields are flexible and contain bank identification, personal identification or telephone number. It is important that there are no ambiguities and that a clear distinction exists in the format of the above mentioned identification numbers.

In accordance with the amount of money transferred, the data can be encrypted to secure the privacy of every player in the procedure of payment. Also a public key infrastructure is established [7]. The FSP stores the certificates with public keys of every merchant and customer. It also minds its own private key in a secure manner. The merchant stores its private key in a safe environment and uses it to sign the messages. It has the FSP's public key in order to encrypt the message. Only the FSP can decrypt the messages received from the merchant, customer and bank. The aspect of security procedures implemented depends on the amount of money transferred and is considered in more details in [1].

10 Conclusion and Future Work

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. The specific workflow implementation depends on user’s disposition in motion.

As a light motive, the enterprises with multi-channel infrastructure have to harmonize the security level for M-Payment and web-based security architectures for e-payment in order to protect their business and build future-proof architectures.

References

1. M. Gusev, Lj. Antovski, G. Armenski; Models of Mobile Payments; *Proceedings 2nd WSEAS International Conference on Multimedia, Internet and Video Technologies (ICOMIV),* Skiathos, (2002) pp.3581-3586

2. O. Pfaff, Identifying how WAP can be Used for Secure m-Business, *Proceedings 3rd Wireless m-business Security Forum*, Barcelona, (2002)
3. D. Amor, *The E-business Revolution*, Hewlett Packard Books, New Jersey (2002)
4. Lj. Antovski, M. Gusev, Ebanking-developing Future with Advanced Technologies. *Proceedings 2nd Conference on Informatics and IT*, Skopje, (2001), 154-164
5. D. Bulbrook, *WAP: A Beginner's Guide*, Osborne/McGraw-Hill New York (2001)
6. M. Gusev, E-Commerce, a Big Step Towards e-Business. *Proceedings 2nd SEETI Conference on Trade Initiative and Commerce*, Skopje, (2000)
7. R. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public-key Cryptosystems. *Communications of the ACM*, 21(2):120-126 (1978)
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, *Proceedings of 2002 IST Mobile & Wireless Telecommunications Summit*, (2002), pp.745-752
11. S. Pantis, N. Morphis, E. Felt, B. Reufenheuser, A. Bohm, Service Scenarios and Business Models for Mobile Commerce, *Proceedings (2002) IST Mobile & Wireless Telecommunications Summi*, (2002) 551-561
12. N. Mykkanen, Mobile Payments - a Report into the State of the Market, Commerce Net, Scandinavia, (2001)
13. European Commission DGIS, Digital Content for Global Mobile Services Final Report, Andersen, Europe (2002)
14. M. Ding, and C. Unnithan, Mobile Payments (mPayments) – an Exploratory Study of Emerging Issues and Future Trends, School Working Papers Series, Deakin Univ. (2002)
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*, 8(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"), Ver.1.0, Copyright 2000 Sun Microsystems, Inc. (2000)
22. Sun Microsystems, Inc. "Connected, Limited Device Configuration (CLDC) Specification, ver.1.0a", Sun Microsystems, Inc., (2000)
23. Mahmoud, Qusay H. "Secure Java MIDP programming using HTTPS with MIDP", http://www.wireless.java.sun (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)