MOBILE PAYMENT'S SECURITY

Lj. Antovski, M. Gušev

Institute of Informatics, Faculty of Natural Science and Mathematics,
Ss. Cyril and Methodius University
Arhimedova b.b., PO Box 162, 1000 Skopje, Macedonia
anto@ii.edu.mk, marjan@ii.edu.mk

Abstract: Mobile payments play an important role in retail payments. M-payments are defined as payments carried out by mobile phone. This is especially promising with the third generation (3G) networks. M-commerce as a wide area could be divided into mobile E-commerce and M-trade area. Different models of mobile payments are proposed considering the physical disposition. A brief research on the state of the market is given to present a framework for possible solutions. Financial service provider is essential mediator among customers, merchants and banks. The iMS specification proposed in this paper enables mobile payments with one button click. Different levels of security have to be implemented for small, medium and large transaction of funds. The security algorithms are lightweight in correlation with the device's processing power. The proposed models are simple, secure and scalable. Future solutions would merge m-payment and e-payments infrastructures in future proof architectures.

Keywords: m-payment, m-commerce, m-trade, iMS, security, certificate, transfer of funds, FSP, WAP, WIM, WTLS

1. Introduction

There are many definitions for M-Commerce. In [6] it 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 scope of this paper is on the B2C model.

The success of M-Commerce services will largely be predicated by the customer's confidence in the security and integrity of financial transactions envisaged and the attractiveness and ease of use of service offerings. However, there are many technical, commercial and legal challenges.

The scenarios of M-Commerce involve 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].

The future of M-Payments is promising, considering the high rate of penetration of mobile devices, especially mobile phones, PDA's and other. The penetration rates in some countries are higher than 80 per cent and the growth factor is very high [4, 11].

Mobile devices have restricted capabilities: 1) low processing power, 2) small memory resources and 3) restricted network bandwidth. The procedures and security algorithms proposed in this paper are lightweight in correlation with mobile device's properties [3, 5].

2. M-Commerce Framework

M-commerce as a wide area consists of two sub areas based on user's distribution criterion including mobile E-commerce and M-trade area [1, 5].

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. This area is an extension of classic electronic commerce adapted to mobile networks and devices. The well known scenarios in the electronic world are transferred and adapted for the mobile world.

In the M-Trade scenario the consumer has eye contact with offered products and services. The payment procedure is executed via the mobile network. The mobile device is used for customer's identification, payment confirmation and verification.

2.1 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 mobile commerce site and shipment infrastructure.

The customer is physically distributed away from the merchant and is searching for product or service using his mobile device. The mobile operator with supplied network offers the ability to use mobile Internet while the users are in motion. The merchant owns m-commerce site that offers different services, products and goods. The financial service provider (FSP) is a mediator among customers, merchants and banks. The FSP is the authority that guarantees the identity of the players in this scenario. It identifies the real customer, merchant and bank.

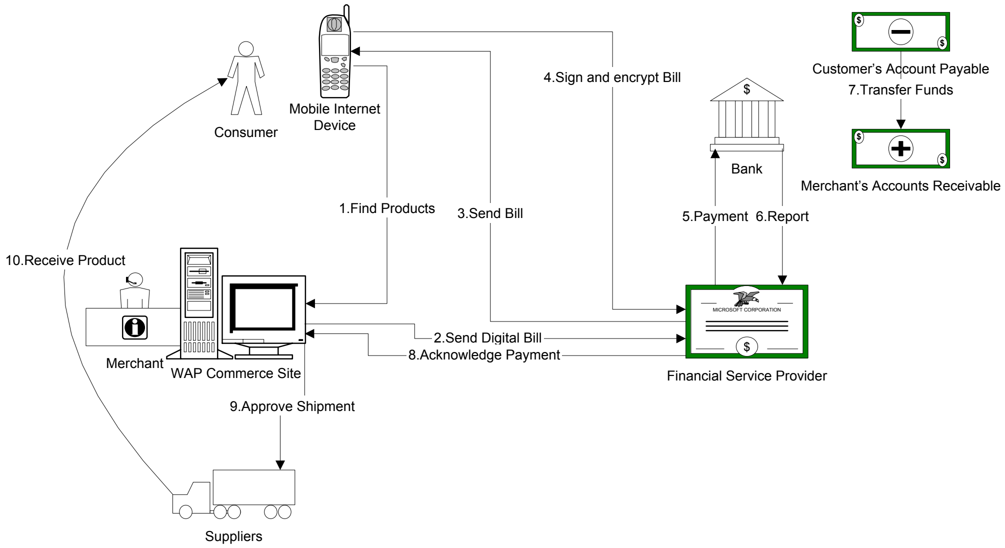

Figure 1: Mobile E-Commerce

The whole procedure given in Fig.1 is executed as follows. The customer connected over mobile Internet, searches the Web and finds products or services. The appropriate products or services are remembered in the shopping card and the customer initiates the payment procedure. The merchant's automated service receives the information from the users shopping card and initiates a financial message with strict predefined structure, signs and encrypts it and sends it to FSP. The FSP decrypts and verifies the message. With the supplied data, the FSP prepares a confirmation message, signs and encrypts it and sends it to the customer. The customer receives the message, decrypts and verifies it. Afterwards the customer signs and encrypts the financial message and returns it to the FSP. At the end the FSP initiates payment procedure in the bank. The customer's account is debited and the merchant's account is credited. This procedure is executed in traditional fashion through the bank or inter-bank's payment system. If the merchant receives a positive confirmation, the supplier is authorized to initiate shipment of products or services to the customer.

2.2 M-Trade

Opposite to mobile e-commerce, in the m-trade case the customer is in physical and eye contact with the merchant. The infrastructure includes customer with mobile device, mobile operator that enables mobile Internet, FSP, bank and merchant. The customer, bank and merchant use the FSP services.

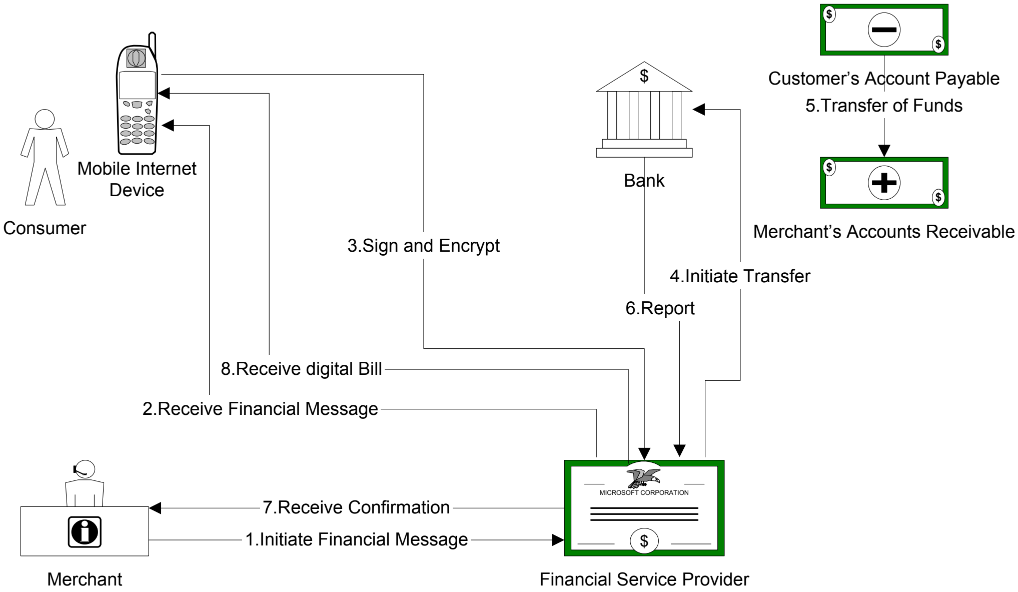

Figure 2: M-Trade

The merchant in Fig. 2 scenario 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.

3. Market Analyses

In the following section we present a brief research on the state of the market as a framework of possible solutions with different levels of security and user convenience.

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.

Numerous mobile operators have started offering m-payment services. Almost all of these services are in early stage and still testing. Some operators team up with banks while others manage m-payment on their own [10].

Name	Payment Service	Security aspect
Paybox & Deutsche Bank	Real and virtual POS	Cardholder authentication through the SIM card. Transmits the PIN via (DTMF).
Movilpago Telefonica & BBVA	Real and virtual POS. Purchases are billed on credit/debit cards or prepaid phone account.	Cardholder verification and authentication through the SIM card.
Paiement CB & France Telecom Mobile CB	Mail order and virtual POS. For dual slot phones where users insert smart CB credit card.	Security lies in the credit card chip. SMS used for order confirmation only. Also uses SIM toolkit card.
GiSMo & Millicom International Cellular Virtual POS	Payment via wallets fed by credit card or direct debit. For both micro and macro - payments.	PIN code for each transaction, sent via SMS to the Consumer's GSM Phone.
Mobilix Open Mobile Payment & France Telecom PBS & Gemplus	PIN-based credit/debit card payment over a mobile phone, initially to reload pre-paid airtime over the air.	The payment is carried out by exchange of e-payment certificates. The identity of the user is confirmed through the SIM card.
Telia Payit	Virtual POS	Digital goods are billed either on phone bill or a Jalda pre-paid account.
Sonera Mobile Pay	Real-world POS (attended & unattended).	Charged on phone bill (only low value payments), credit or debit card.

Table 1: Mobile operators that offer mobile payment service

In Table 1 we give an overview of some of the key players on the market, the type of payment implemented and the level of security required. There is a broad scope 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 given technical specification. In order to allow wider range of users to access the payment services offered, one must propose and implement a lightweight and secure procedure for mobile payments which works on variety of client devices and platforms. The following sections deal with this question.

4. Interactive Message System

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 the next section.

```
<iMS>
        <type>medium</type>
        <address>
                <from>
                        <id>John.Bernard@person.xbank</id>
                        <sign>abcad3456f454aabcdeehee4aed32a</sign>
                <from>
                <to>
                        <id>Merkur.Trade@merchant.xbank</id>
                        <sign> abc78dfd6fd454aabcdeehee4ead2a</sign>
                </to>
                <FSPsign>abc78d454aab ad345abcdeeheehe</FSPsign>
                <timestamp>27.05.2002 12:34:34</timestamp>
        </address>
        <data>
                <accountPayable>1234-5678-9abc</accountPayable>
                <accountReceivable>9876-543-21de</accountReceivable>
                <amount>EUR1000.00<amount>
        </data>
</iMS>
```

Figure 3: Non-encrypted iMS message

5. Security Procedures for Mobile Payments

Mobile devices, especially mobile (cellular) phones don't broadly support WAP 2.0 specification and have wireless identity modules in small numbers. This is the reason why we propose another secure payment procedure.

In this scenario we propose existence of trusted server, considering the fact that a prime secret as private key or password could not be stored in the temper resistant memory of the phone's SIM card. In some cases, the phone doesn't support this feature, but in most cases it is a common property of the mobile network and the SIM supplied.

The trusted server named as trusted mobile certificate server, minds all the certificates of customers with theirs respective private and public keys. It is a temper resistant area accessed only by a strict security procedure which involves a common secret as symmetric key or password.

The trusted mobile certificate server is authorized by the mobile user to execute delegate signing of financial messages on his/hers behalf in case with exact user name and PIN (or password) supplied. The trusted mobile certificate server also bears the FSP's certificate with public keys. Considering the user's mobile device restricted capabilities, the trusted mobile certificate server verifies the FSP's identity and the validity of the financial message source.

As we present in Fig. 4, the trusted mobile security server and the WAP gateway (where exists) are insourced in the demilitarized zone of the mobile internet provider's network. They can be only accessed by the mobile users and the financial service provider.

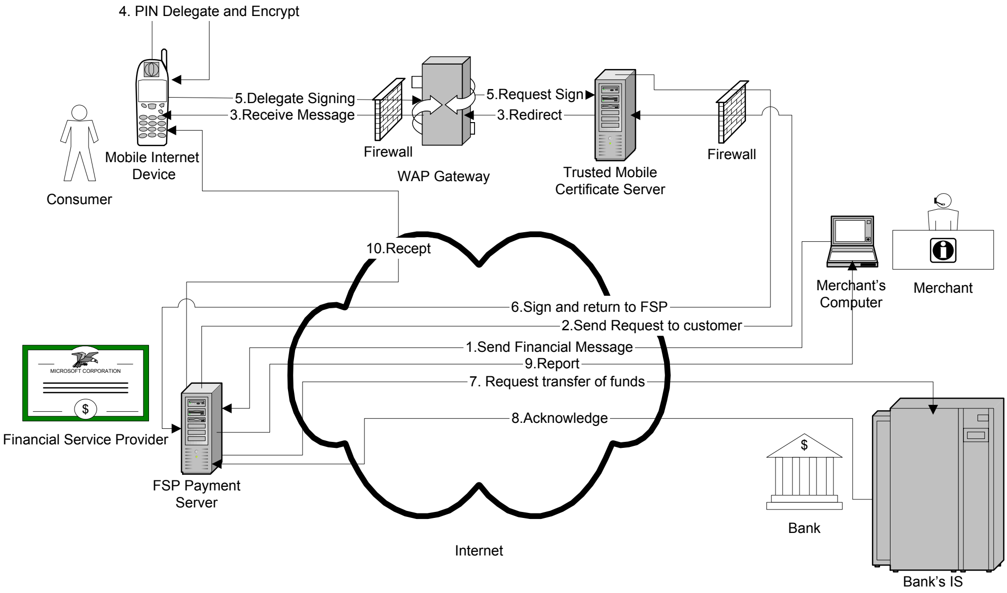

Figure 4: Security procedure for Mobile Payments

The security procedure 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, verifies the source, signs, encrypts and redirects the message to the trusted mobile certificate server.
2. The trusted mobile certificate server validates the message source and over secure communication (SSL to WAP gateway, WTLS to mobile device) sends the message to the designated mobile user.
3. The user receives the message, verifies the source (WTLS established only by server authentication). If the source is the WAP gateway in the trusted mobile provider's network, the procedure continues otherwise it terminates.
4. The user enters PIN (or password) which is encrypted by asymmetric algorithm with session secret and sends the delegate authorization to

the trusted mobile certificate server.

5. The encrypted message is send to the trusted mobile security server over secured communication.
6. The trusted mobile certificate server validates the message source, checks the PIN and if authorized, signs the financial message with the user's private key. Afterwards the message is sent to the FSP's server.
7. 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.
8. The FSP is acknowledged after successful transfer of funds.
9. The merchant receives notification.
10. 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.

6. Future Trends in Mobile Security

Even though the WAP 2.0 standard is released, it will take some time until the mobile devices supporting these features hit the market. The new specification offers numerous security enhancements. WAP 2.0 adds the feature of gateway navigation. The WAP Transport Layer E2E Security Specification supports the co-existence of mobile operator and content provider WAP gateways and mutual redirection of routing on demand [9].

The combination SSL/TLS are secure protocols that provide secure communications between clients and servers over reliable transports. WAP 2.0 adopts TLS and supports SSL/TLS tunneling trough WAP gateways by means of HTTP primitives [2].

Several features are considered in future releases as TLS extensions to support broader wireless environments, additional functions to support encryption on application level, and XML security adoption. The WIM enhancements are matter of discussion. The accent is on on-board key generation support.

The wireless public key infrastructure will support revocation. Also the goal is to integrate and facilitate the existing public key infrastructures with mobile clients in the manner of offloading certificate handling to XKMS servers.

7. Conclusion

IT-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.

There are many challenges 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 WAP based security for m-payment and web-based security architectures for e-payment in order to protect their business and build future-proof architectures.

8. 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