MODELS OF MOBILE PAYMENTS

MARJAN GUSEV, LJUPCO ANTOVSKI, GOCE ARMENSKI
Institute of Informatics, Faculty of Natural Sciences and Mathematics
Ss. Cyril and Methodius University
Arhimedova b.b., PO Box 162, 1000 Skopje

Abstract: - Mobile phones are already approaching penetration rates of close to 80 per cent in some parts of the world. Mobile payments, or "m-payments", are expected to become an important part of retail payments. M-payments are defined as payments that are carried out via mobile phone. 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. Financial service provider is essential mediator among customers, merchants and banks. The iMS specification proposed in this paper enables mobile payments with one click of a button. Different levels of security have to be implemented for small, medium and large transaction of funds.

Key-Words: - m-payment, m-commerce, m-trade, iMS, security, transfer of funds, one click strategy, financial service provider

1 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 payment devices.

The most immediate and easy-to-implement payment system is to transform mobile phones as a means to buy goods or services either through the prepaid phone card for low-value purchases or the monthly phone bill for both low-value and larger amounts. More refined solutions include, among others, offering a real time gateway to bank transactions, a wireless internet banking service, or an additional security channel for PC-based online purchases to verify the payer's identity and confirm a transaction through his/her mobile phone [2].

Mobile payments, or "m-payments", are expected to become an important part of retail payments. M-payments are defined as payments carried out via the mobile phone. In principle, the mobile phone can be used at the real POS (point of sale), in e-commerce and in m-commerce [4].

The case for m-payments looks even more promising when one considers that the new third generation (3G) networks and applications offer the opportunity to sell completely new products such as multi-media messaging and location-based services. It is expected that these new services will strongly expand mobile commerce. M-commerce, in turn, calls for mobile payment solutions and further strengthens the case for m-payments [1].

Further the access to heterogeneous mobile networks is granted on the basis of online payment methods that are modifications of mobile payments [8].

The future is more promising because the customers want and expect to do commerce on virtually every communication device [9].

2 The Structure of M-commerce

As Fig.1 shows, the M-commerce as a wide area could be divided in two sub areas. The criterion of division is on the user's distribution. The sub structure includes the space of the mo-bile E-commerce and the M-trade area.

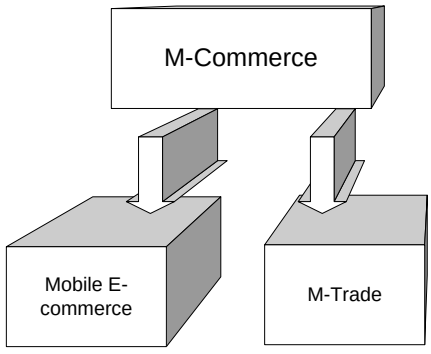

Fig.1. Basic structure of M-Commerce

More precisely, the Mobile E-commerce puts accent on the electronic commerce via the mo-bile 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 the restrictions of the mobile networks and devices. The well known scenarios in the electronic world are transferred and adapted in the mobile

world. The restrictions considered include small bandwidth, unpredictable connection, insecure transition, client mobile devices with poor processor's power and unfriendly user's interface considering the multi-click keyboard [3].

M-Trade concentrates on classic “terrestrial” shopping. This scenario includes the consumer that has eye contact with the goods, products and services that are offered. The procedure of payment is executed via the mobile network. The mobile device is used for customer's identification, payment confirmation and verification. In this scenario the mobile device plays active role in the payment process and it is a virtual digital wallet. The procedure of mobile payment is to be initialized by the consumer, or by merchant on customer's request. This is the key point in the division of the models of mobile payments that are to be analyzed in the following sections.

As discussed previously, considering the consumer and merchant's terrestrial distributions, the following models of mobile payments are identified:

- Mobile e-commerce,
- M-trade with request and
- M-trade with Interactive Message System (iMS).

3 Mobile E-Commerce Framework

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

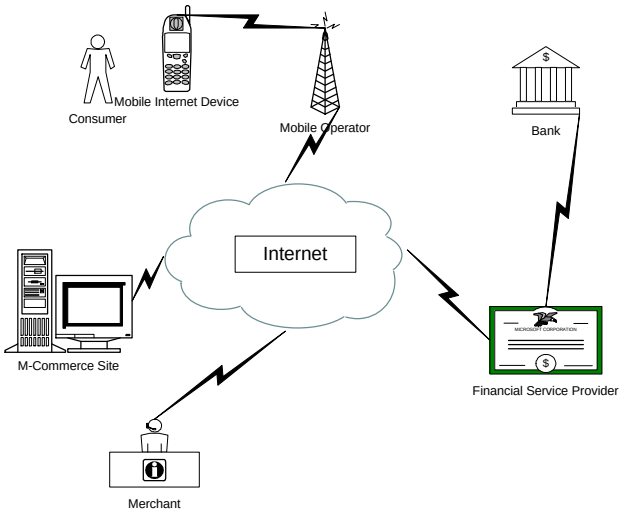

Fig.2. Mobile E-Commerce framework

In this scenario the following conditions are fulfilled. The customer is physically distributed away from the merchant and is searching for product or service over his mobile device. The mobile operator with supplied network offers the ability to use Internet while the users are in motion. The merchant has 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. All other factors in this scenario communicate among each other trough FSP. They only identify, trust and communicate with FSP, which transforms signs and sends the messages to the final point of the communication among the key factors in the scenario.

The framework architecture of the M-commerce scenario is presented in Fig.2. All key players: mobile operator, FSP and merchant are connected over the Internet.

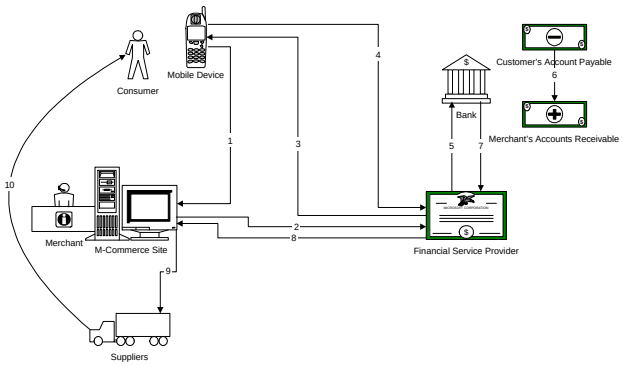

Fig.3. Mobile E-Commerce Workflow

The workflow scenario in Fig.3 is implemented considering the given framework. Its diagram consists of the following stages:

1. The consumer connects to mobile Internet, finds the appropriate site, chooses the goods and initiates the payment.
2. The merchant’s automated mobile service sends a digital bill to the Financial Service Provider.
3. The Financial Service Provider passes the financial message to the customer.
4. The Customer digitally signs, encrypts the message and returns it to the Financial Service provider.
5. The provider initiates the payment in the Bank.
6. The Bank debits the customer’s account in credit to merchant’s account.

7. The Financial Service Provider receives notification.
8. The notification is transferred back to the Customer and also to the Merchant.
9. When the Merchant receives the notification, the shipment of goods to the consumer is initiated.
10. The customer receives the chosen goods.

In more details, the customer connected over the mobile Internet, searches the Web and finds appropriate products or services, which are of his/hers interest. The information for the given products or services is stored in the shopping card. At the end of the search the customer initiates the payment procedure. As the merchant's automated service receives the information about the users shopping card, it initiates a financial message with strict predefined structure, signs and encrypts it and sends it to FSP. The FSP receives 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 user receives the message, decrypts and verifies it. After this procedure the customer signs and encrypts the financial message and returns it to the FSP. After this procedure, the FSP initiates payment procedure in the bank. The bank receives a predefined message that is signed and encrypted by the FSP. The customer's account is debited and the merchant's ac-count is credited. This procedure is executed in traditional fashion through the bank or inter-bank's payment system. The bank returns a report that is passed to the customer and the merchant. If the merchant receives a positive confirmation, the supplier is authorized to initiate shipment of products and goods to the customer. On the other hand if the customer requires a service, one is allowed to use the service.

4 M-Trade Framework

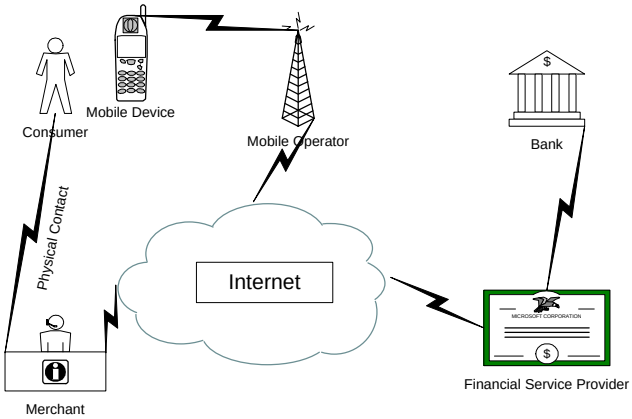

Fig.4. M-Trade framework

The M-trade framework consists of consumer with mobile device, mobile operator that enables mobile Internet, FSP, bank and merchant that uses the FSP services.

Opposite to mobile e-commerce, in this case the customer is in physical and eye contact with the merchant. The customer chooses the services and products visually. The mobile operator with the network supplied offers the users the ability to use mobile Internet. The financial ser-vice provider (FSP) is a trusted mediator among the customer, the merchant and the bank. The FSP is the authority that guarantees for the identity of the players in this scenario. It identifies the customer, the merchant and the bank. All factors in this scenario only identify, trust and communicate with the FSP.

The Fig.4 shows the framework architecture of the M-trade architecture. All key players the mobile operator, FSP and merchant are connected over the Internet. The communication between the FSP and the bank is over secured VPN network. The customer and the merchant communicate orally.

Two workflow scenarios are proposed according to the payment initialization. The first scenario examines the payment procedure where the customer requests a payment receipt.

4.1 M-trade with Request Workflow

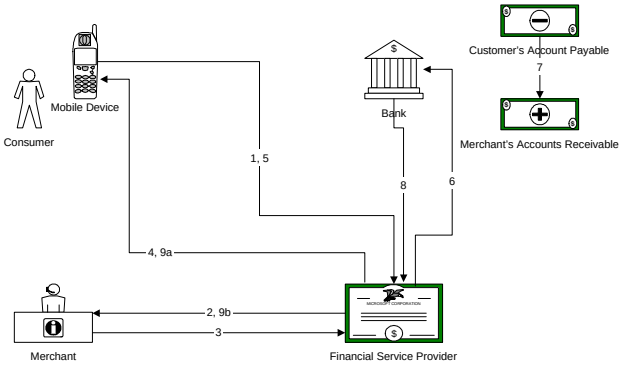

Fig.5. M-Trade with Request Workflow

This scenario called “M-Trade with request” has typical workflow given in Fig.5 and consists of the following steps:

1. The consumer chooses goods and initiates payment.
2. The Merchant receives the request.
3. The Merchant returns the financial message to the Financial Service Provider.
4. The Consumer receives a financial message.
5. The Consumer digitally signs, encrypts and sends it back to the Financial Service Provider.

6. The provider initiates the payment in the Bank.
7. The Bank debits the customer's account in credit to merchant's account.
8. The Financial Service Provider receives notification.
9. The notification is transferred back to the Customer and also to the Merchant.
10. When the Merchant receives the notification, the consumer can collect the goods.

The steps 4 to 10 are equal to the same steps in the previously given mobile e-commerce scenario. In the beginning of the procedure the customer can see and choose the products and services in traditional physical manner. After the customer decides what products and services to buy, he/she initiates the payment by request message. This message is predefined. It requires being signed and encrypted by the customer in order to fulfill the non repudiation procedure. The FSP passes through the message to the merchant. The merchant fills the necessary financial data, signs, encrypts and returns the message to the FSP. In this scenario, as in the previous one, the FSP engages the security mechanisms to authenticate and validate the customer and the merchant.

4.2 M-trade with iMS workflow

The above models of mobile payment fulfill every aspect of secure and reliable payment procedure. However, they are not proven to be user friendly. The main characteristic of the mo-bile devices is poor interface and keyboard. Every multi-click strategy is not acceptable for fast and comfortable usage.

In such a manner the M-trade procedure has to be modified to minimize the manipulation of the mobile device. The M-trade scenario enables the customer to choose the products and ser-vices physically and to demand the payment initialization procedure orally. This eases the burden of mobile devices, especially the extensive usage of its keyboard. In this case the device is only used to confirm the transfer of funds. The new proposed procedure introduces the "Interactive Message System" or iMS. The merchant initializes the financial message upon oral demand by the consumer.

The diagram in Fig.6 shows the workflow process of the M-trade with iMS.

The following steps are identified in order to successfully complete the payment procedure:

1. The Merchant initiates a financial message (iMS).

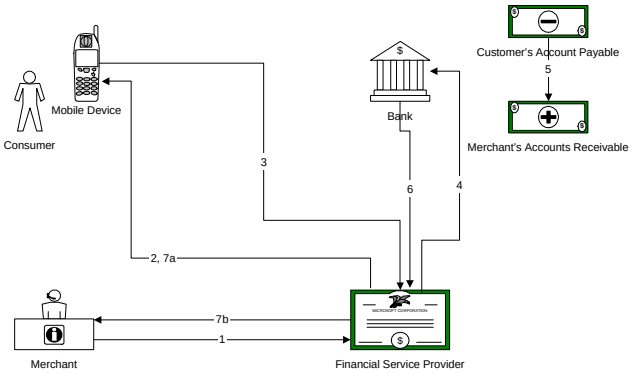

Fig.6. M-Trade with iMS Workflow

2. The Consumer receives a financial message (iMS).
3. The Consumer digitally signs the iMS, encrypts and sends it back to the Financial Service Provider.
4. The provider initiates the payment in the Bank.
5. The Bank debits the customer's account in credit to merchant's account.
6. The Financial Service Provider receives notification.
7. The notification is transferred back to the Customer, and if everything is right, also to the Merchant.
8. When the Merchant receives the notification, the consumer can collect the goods.

In more details, the merchant initiates the first step. The merchant's information system pre-pares a financial message with a strict predefined structure. The message is digitally signed, encrypted and sent to the FSP. The FSP decrypts and validates the message. It signs, encrypts and sends it to the customer. The customer receives decrypts and validates 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 click of a button on the mobile device. The steps from 4 to 8 are the same as the steps from 6 to 10 in the previous scenario.

4.3 Interactive Message System (iMS)

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

As the example in Fig.7 shows, 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.
At the beginning 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.

```
<iMS>
 <type>medium</type>
 <address>
  <from>
   <id>John.Bernard@person.xbank</id>
   <sign>abcad3456f454aabcdeehee4aed32a</sign>
  </from>
  <to>
   <id>Merkur.Trade@merchant.xbank</id>
   <sign> abcfd6fd454aabcdeehee4ead2a</sign>
  </to>
  <FSPsign>78d454aab ad345abcdeeheehe</FSPsign>
  <timestamp>27.05.2002 12:34:34</timestamp>
 </address>
 <data>
  <accountPayable>1234-56781</accountPayable>
  <accountReceivable>9876-54321</accountReceivable>
  <amount>EUR1000.00<amount>
 </data>
</iMS>
```

Fig.7. Example of non-encrypted iMS message

The <id> fields are flexible and they can contain bank identification, personal identification or telephone number. It is important that there are no ambiguities and that there is a clear distinction in the format of the above mentioned identification numbers.
During communication the data is encrypted in order to secure the privacy of every vendor in the procedure of payment. For this purpose a public key infrastructure is established [5]. 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, the customer and the bank. The customer stores his/hers private key and the procedures for encryption and signing in personal Wireless Identity Module (WIM) [6, 7].

5 User convenience and security

The models that require higher level of security always turn out to be very inconvenient for usage. There is always a balance among security and user's friendly and fast environment. The following analysis is made in order to choose appropriate model for proposed payment.
The number of steps to perform a complete payment is shown in Table 1. The “mobile e-commerce” model requires a “multi-click strategy” to find a product or service, requesting payment and confirming payment. The “m-trade with request” model requires fewer multi-clicks in order to execute payment, since it does not include process to find a product or ser-vice. The “m-trade with iMS” is a “one click strategy” that requires only one button click on the mobile device to confirm the payment. It does not include the process to find a product or service, or process to request the payment. The iMS enables mobile payments and makes the mobile devices acceptable for broad usage as digital financial terminals.
The level of security depends on the amount transferred from the customer’s to the merchant’s account. In addition the process is accelerated due to restricted security on small payments. The Table 2 examines the level of security in correlation with the amount of payment.
Small payments only require ring to a specific number or sending an SMS. Other implementations are optional and only slow down the process of payment. Interactive voice response (IVR) is also acceptable scenario for small payments.
Medium payments require higher level of security. Sufficient level of security is achieved with the usage of PIN and confirmation in combination with signing. IVR is only used in combination with the

Type	Product/service order	Payment Request	Payment Confirmation
Mobile E-Commerce	Multi	Multi	One
M-Trade with Request	No	One	One
M-Trade with iMS	No	No	One

Table 1. Number of clicks per framework

Amount/Security	Ring only	Confirm only	PIN and Confirm	PIN, Confirm and Sign	PIN, Confirm, Sign & Encrypt	Interactive Voice Response
Small Payments	Yes	Optional	Optional	Optional	Optional	Yes
Medium Payments	No	No	Yes	Yes	Optional	Combination
Large Payments	No	No	No	Yes	Yes	Combination

No- Not recommended
Yes – Preferable implementation
Optional – Recommended implementation
Combination- only with other preferable or recommended implementation

Table 2. Security implementation

mentioned methods.
Large payments require the highest level of security and protection. Every possible security mechanism is implemented including PIN, confirmation, singing, and encryption in optional combination with IVR and voice detection.
In all models the whole process must be executed in acceptable amount of time with accept-able level of security for the specific financial funds transferred.

6 Conclusion

Incorporation of wireless technology into solutions is no longer a choice. The competitors are offering wireless solutions to both their customers and staff, increasing both sales and performance. The only choice is how to implement the wireless solution.
There are many challenges involved to build an m-commerce solution, and just as many "solutions" available in today's 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.
Financial institutions are trying to influence the ongoing standardization initiatives and to circumscribe the innovation potential of mobile phone technology with a view to combining it with existing payment instruments.
The above-proposed models of mobile payments can be fully implemented in the real life considering the ability of available technology infrastructure. The models are simple, secure, scalable and future-prove. Their implementation depends on user's disposition as he/she is in motion. Mobile phones are devices that will change conventional e-Business models or trading and payment processes. With the implementation of the mobile payment models, the payment process is successfully transferred in the mobile digital world.

References:

[1] D. Amor, *The E-business Revolution*, New Jersey: Hewlett Packard Books, 2002
[2] Lj. Antovski, M. Gusev, Ebanking-developing future with advanced technologies. *Proc. of 2nd Conf. on Informatics and IT*, 2001 20-23 Dec, Bitola.
[3] D. Bulbrook, *WAP: A Beginner's Guide*, New York: Osborne/McGraw-Hill, 2001
[4] M. Gusev, E-commerce, a big step towards e-business. *Proc. of 2nd SEETI Conf. On Trade Initiative and Commerce*, 2000 Nov.8, Skopje.
[5] 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.
[6] W3C: http://www.w3.org (accessed 20.05.2002)
[7] WAP-forum: http://www.wapforum.org (accessed 15.05.2002)
[8] 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
[9] 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