Enabling secure e-Commerce on Mobile phones

[1] Do van Thanh & [2] Jan A. Audestad
[1] *Ericsson Norway Applied Research Center, P.O Box 34 N1361 Billingstad, Norway - etodvt@eto.ericsson.se - Tel: +47 66 84 12 00*
[2] *Telenor AS P.O Box 6701 St. Olavs plass N-0130 Oslo Norway – jan-arild.audestad@telenor.com – Tel: +47 22 77 99 52r*

Key words: Mobile e-commerce, Mobile Internet Applications, Wireless Application Protocol (WAP), Mobile security, Wireless Public Key Cryptographic

Abstract: Mobile e-commerce enables the mobile user to buy and pay for things, to pay his bill or to make a bet via his mobile phone when on the move, anywhere and at any time. It will bring convenience and contribute to improve life quality of the users. However, in order to be successful, security measures must be strong enough to protect the user from illegal abuses and to get confidence from him. Unfortunately, current security measures for mobile phones are not yet sufficient. This paper describes the mobile e-commerce activities at Ericsson, which aim at making mobile e-commerce applications secure and enabling a full-scale development and deployment of them. The paper starts with a definition of mobile e-commerce. Next are a summary of the Wireless Application Protocol (WAP) and its achievements. The Web e-commerce is briefly explained. The problems related to security in mobile e-commerce are then described. Thereafter, the solution to the problems is presented. The paper concludes with a look on the future and discussions on what can be done.

1. INTRODUCTION

The convergence of mobile communications network and Internet has paved the way for a range of brand-new applications called wireless Internet applications. Which one of them will be the killer application is still unclear. However, there is one type of wireless Internet applications that are getting

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35522-1_37

H. R. van As (ed.), *Telecommunication Network Intelligence*

more and more popular and may even surpass their counterpart in the fixed Internet. They are called mobile electronic commerce applications. They enable the user to buy small things such as soft drinks, cinema tickets, train tickets, etc. or to pay his bills via mobile devices, i.e. mobile phones, PDAs (Personal Data Assistant), palmtops, etc. In a time when people are much on the move and focus is on life quality improvement, mobile e-commerce applications will bring both convenience and save a lot of time for the mobile user. However, in order to be successful, security measures must be strong enough to protect the user from illegal abuses and to get confidence from him. Unfortunately, current security measures for mobile phones are not sufficient. This paper describes the R&D activities in mobile e-commerce at Ericsson, which aim at making mobile e-commerce applications secure and enabling a full scale development and deployment of them. The paper starts with a presentation of mobile e-commerce. Next is a summary of the Wireless Application Protocol (WAP) and its achievements. The Web e-commerce is briefly explained. The problems related to security in mobile e-commerce are then described. Therafter, the solutions to the problems are presented. The paper concludes with a look on the future and discussions on what can be done.

2. WHAT IS MOBILE E-COMMERCE?

Mobile e-commerce is e-commerce brought to mobile users via mobile devices such as palmtops, PDAs or most dominantly mobile phones. With an ever-increasing number of devices in the market, mobile phones will undoubtedly play a crucial role in promoting mobile e-commerce. Mobile e-commerce allows users to conduct e-commerce on their mobile devices: obtain marketing and sales information, receive ordering information, make a purchase decision, pay for it, obtain the service or product and finally, receive customer support required.

Mobile e-commerce is more than a mobile and wireless extension of the Web-based e-commerce. It is an entirely new sales and promotion channel, and is the enabler for a whole range of new services such as buy a Coke, pay for parking, buy train ticket, etc. via mobile phone. Most importantly it is tailored to the users in many aspects. It follows the user and is available anytime and anywhere. Although mobility is a valuable characteristic to the user in general, it is especially precious for e-commerce because it enables a key factor, which is missing in other e-commerce forms, namely the ability to adapt to the user, his humor and his demands. In fact, the essence of commerce is to be able to satisfy the demands of the users. It is important not only to be able to offer whatever the user wants but also whenever he

wants. Mobile e-commerce can also be customised such it fits the preferences of the user in combination with time and location.

Another important aspect of mobile e-commerce is the ability to mix electronic media with other media such as newspaper, TV, radio, natural communication in any of the commerce phases i.e. presentation, selection, ordering, payment, delivery and customer care. For example, the mobile user can browse on his mobile phone and obtain the location of the closest shop. He goes there and buys a Coke. In this case, the presentation and selection are done electronically via the mobile phone while the rest is done in a traditional way via natural communication. In another situation, the user buys groceries and pays via his mobile phone. The presentation, selection, ordering, delivery and customer care phases are carried out in traditional way and only the payment phase is done electronically.

3. MOBILE E-COMMERCE AND WAP

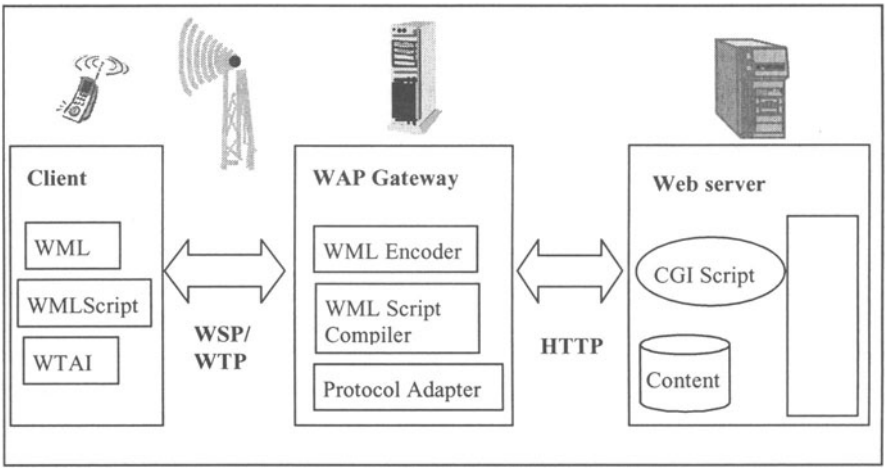

Figure 1. The Wireless Application Protocol Architecture

The *Wireless Application Protocol (WAP)* promoted by the WAP forum enables the access to the Internet for mobile devices. Taken into account the limited bandwidth of the wireless link, the limitation of mobile devices concerning processing, storage, battery life, size and weight, WAP is optimised for the wireless environment. The architecture of WAP is shown in *Figure 1*. Of course, WAP will contribute to the success of mobile e-commerce but it is worth noting that mobile e-commerce exists also without

WAP. For example, the first mobile e-commerce application in Norway,"The cinema ticket" that was jointly developed by Ericsson and Telenor Mobile is not based on WAP. It is based on SIM application toolkit where the commerce application is implemented on the SIM (Subscriber Identity Module) of the mobile phone. It is worth mentioning that WAP contains security specifications but they are not sufficient because they do not provide end-to-end security. In the future, mobile e-commerce can be extended further through the adoption of newer technology such as Bluetooth, which allows local communications between devices without the need of an on-line connection with the network.

4. SECURITY REQUIREMENTS IN E-COMMERCE

In e-commerce where the consumer and the merchant communicate indirectly via software entities and the Internet, trust must be somehow established between the two parties. In order to achieve trust the following security functions must be performed:

- **Authentication:** Each party needs to be able to authenticate its counterpart, i.e. to make sure that the counterpart is the one he claimed to be.
- **Integrity:** Each party needs to make sure that the received messages are not altered or fabricated by other than their counterpart.
- **Confidentiality:** Each party wants to keep the content of their communication secret.
- **Message authentication:** Each party wants to make sure that the received messages do really come from his counterpart.
- **Non-repudiation:** Each party wants to prevent that the counterpart later on denies the agreements that he has approved earlier.

Usually, the two parties do not and must neither know each other in order to do trading. In such a case, the *asymmetric cryptographic algorithm*, also called the *Public key algorithm* is more appropriate than the symmetric cryptographic algorithm.

Briefly, the public key algorithm uses a key pair, one private and one public for encryption and decryption. What encrypted by one key can only be decrypted by the corresponding one. It should also be practically impossible to derive one key from the other one. Confidentiality and integrity are prevailed when the sending party encrypts the message with the recipient's public key since only the later has the corresponding private key to decrypt the message. Authentication and non-repudiation are achieved when the sender encrypts the message or part of it with his private key. The receiver decrypts the message with the sender's public key and can be sure that it comes from the sender because only he is the only to have the private

key. This later encryption scheme is known as *digital signature*, which usually consists also of a message digest (hash function) to reduce the size of the message to be encrypted and to optimize the signing process. There are currently several public key algorithms such as RSA [1], Elliptic Curve [8].

The issue now is to be certain who owns what key pair. A certificate issued by a trusted authority also called *Certificate Authority* (CA) attests that a public key belongs to an entity or individual with a certain name and attributes. Both certificates and keys need to be managed, i.e. generated, revoked, updated, recovered, etc. and a *Public Key Infrastructure* (PKI) is necessary for that. Unfortunately, no such global PKI does exist yet and ad-hoc solutions as we will explain on later sections, have been adopted on web e-commerce.

5. E-COMMERCE ON THE WEB

Since our intention is not to give a deep presentation about Web e-commerce but only an elucidation necessary for the explanation of mobile e-commerce later on, only simplified views of Web shopping and Web banking are described.

5.1 Web shopping

Web shopping is getting more and more popular, especially for books, music, films, etc. The procedure varies slightly depending on the visited web site but can be summarised as follows:

1. A user visits a web site of a merchant. He browses among the offers. Up to this point, no security measure is needed since everything is public.
2. He wants to order goods or services.
3. The web server asserts its site identity by signing its server certificate and sending it together with the unsigned certificate to the browser. In this case the server must be a secure server, i.e. having a server certificate and enabled for security. The browser uses the server's public key (from the server's certificate) to verify that the owner of the certificate is the same one who signed it.
4. The browser checks if the issuing CA is one that it accepts. The trusted CAs is specified in the list of so-called trusted root certificates. Such a list is embedded in the browser. Some browser like Microsoft's Internet Explorer allows the import of new trusted root certificates. If unknown, the browser informs the user that this server certificate was issued by an unknown CA.
5. The user manually (visually) authenticates that the site's certificate was issued by a trusted third party for the exact site the user is visiting.

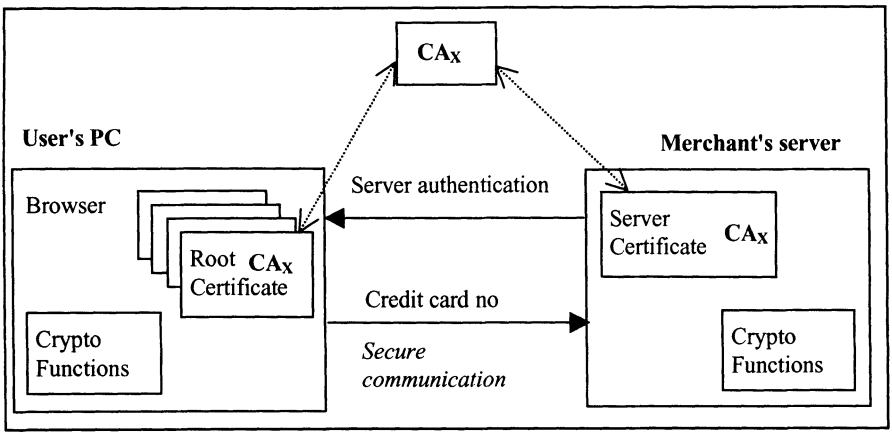

Figure 2. Web shopping

6. The browser generates a session key, encrypts this key with the server public key and sends it securely back to the server.

7. A secure channel is established, with the session key generated by the browser.

8. The user will be asked to enter his personal data, i.e. name, address, and email.

9. The user will be asked to enter his credit card number that will be charged for the purchase.

10. The server issues a receipt to the user or sends it back via email.

11. The merchant validates the credit card number and if valid ships the purchased goods to the user.

12. The transaction can be closed at this stage

The procedure to establish the secure channel described above is in accordance to the Secure Socket Layer (SSL) protocol.

The requirements on the user's side are as follows:

1. His PC must have a browser
2. The browser must be equipped with root certificates used in the authentication of the server
3. It must have access to cryptographic functions that are capable of validating server certificates and capable of encrypting and decrypting for the secure channel.

The channel is secure in the sense that confidentiality and integrity are prevailed. However, it is not a trusted channel. Neither merchant nor the user can be sure that he is dealing with the right counterpart. On the merchant side, only the web server authentication is executed but not the merchant authentication. On the user side, no user authentication is done. It is worth

noting that only the validation of the credit card number is done i.e. the credit card number is valid and can be charged for the purchase. Nothing is said about whether the user is owner of the credit card and hence is entitled to use it.

The described web shopping scheme is used widely because it is simple and does not require much infrastructure and investment. However, it has the following limitations:

- The user has to trust the merchant's site. For well-known sites with good reputation, he can do that but for unknown site he faces a lot of risks. The site may be a fake shop that collects and abuses his credit card number.
- The merchant may deal with impostors that use credit card numbers from stolen cards or valid card numbers that are generated by an illegal process. In such cases, the validation of the card number is successful and the fraud can only be discovered long after the delivery of goods. The financial institutions refuse to cover losses for such cases because the merchant has not verified that the user has a valid credit card and the signature is identical to the one on the credit card.
- The financial institutions are not very satisfied because the authentication of the user and the authentication of the merchant are skipped. The risks for frauds and the number of disputes are higher.

Visa and MasterCard have jointly developed the SET Secure Electronic Transaction protocol [1] as a method to secure payment card transactions over open networks. SET requires however investments both on the merchant and the consumer side, and is not widely used.

5.2 Web banking

Many banks in Europe have realized that by providing banking services such as paying bills, money transfer, balance check, etc. on the Web they can reduce costs at the same time as better services can be offered to customers. However, they are very concerned about security and do not find the procedure used in web shopping secure enough since no client authentication is performed. In order to remedy the situation, the banks have adopted different authentication schemes.

Authentication using a set of numerated passcodes: The user receives from the bank by post a plastic card where a series of numbered passcodes are printed on. The number of passcodes varies depending on the bank. The user is supposed to keep this card in a secure manner. When the user visits the Bank's site, a secure communication is first established between the user's computer and the bank's server. Then, the user is asked to enter his

username. The server will then ask him to enter for example passcode number n. The user consults his plastic card and enters the value of the passcode number n. If the passcode is correct, the user is authenticated.

Authentication using a passcode calculator: The user receives from the bank by post a calculator, which is capable of generating a one-time code. The calculator is secured by a PIN code chosen by the user at initialisation. When the user visits the Bank's site, a secure communication is first established between the user's computer and the bank's server. Then, the user is asked to enter his username. The server will then ask him to enter the passcode. The user enters the passcode generated by the calculator. The server has similar code generation function and does the comparison. If the passcode is correct, the user is authenticated. This method requires a synchronisation between the two calculators.

Authentication using software: Instead of a physical calculator the calculation function is delivered to the user as software in diskette or CD-ROM. The user installs it in his PC. Alternatively, the calculation function can be provided in a smart card but in this case the user must have a card reader and associated software. When the user visits the Bank's site, a secure communication is first established between the user's computer and the bank's server. Then, the user is asked to enter his username. The authentication is then carried out by the user's client program (browser) and the merchant's server without intervention of the user. The client software generates the passcode and sends it to the server. The server compares with the code it has generated. If they match, the user is authenticated.

All the three schemes described above although accepted by the banks because they provide sufficiently strong authentication still have weaknesses as follows:

- The two first schemes are not very user friendly since the user has to really concentrate in order to enter the numbers correctly.
- The user cannot be sure that the bank is performing the correct transaction that he wants.
- The bank on its side cannot prove that the user has requested a transaction and the latter one can deny it later on.

6. COMMERCE FOR THE MOBILE USER

6.1 Ideal mobile e-commerce system

At first glance, mobile e-commerce may appear to be identical to "fixed" e-commerce extended with mobile wireless access and the solutions used in

Web commerce, e.g. Web shopping, Web banking can be applied directly to mobile e-commerce. However, mobile e-commerce differs to "fixed" e-commerce in the following respects:

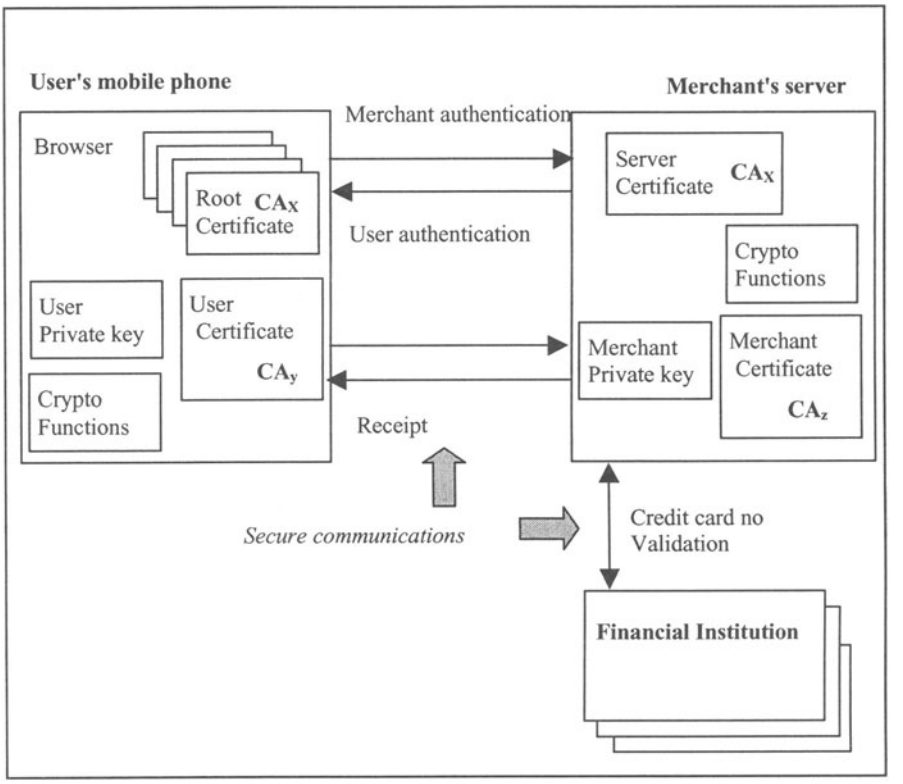

Figure 3. An ideal mobile e-commerce system

Instantaneous delivery: The mobile user is of course interested in having service like web shopping where the delivery of non-electronic goods is carried out later. But, in addition he may want to have the goods delivered to him immediately or in a short delay. For example, after paying for a Coke via his mobile phone he expects the can to run out from the Coke automate. When paying for a cinema ticket he expects to be able to collect the ticket within the same day. It is therefore necessary to have user authentication and also receipt delivery.

Micro payment: For mobile users it is also to be able to buy small things and to pay small amount of money. The fees for such payments must be small compared to the payments.

Mobile context: The mobile user in many situations must be able to operate the services with only one hand. The user may be in environments that are distracting, e.g. crowded, noisy and interactions with the e-commerce services must both simple and small in numbers. The payment scheme of Web shopping described earlier where the user has to enter his personal data and his credit card number is hence not appropriate for the mobile user. A user-friendly payment scheme is required.

An ideal mobile e-commerce as shown *Figure 3* should support the following:

- user authentication
- merchant authentication
- secure channel i.e., encrypted channel
- user friendly payment scheme supporting micro payment
- receipt delivery
- simple user interface

6.2 Limitations of the mobile phones

An ideal e-commerce system puts severe requirements that are difficult to be met by the mobile phone itself as follows:

1. It must also be equipped with a browser that has interface to the cryptographic functions.
2. It must be capable of digitally signing a message using the user private key in order to participate to the user authentication. For that, it must have public key cryptographic functions such as RSA. It must have a tamper-proof storage for storing the user's private key. It must also have enough storage for the user's certificate.
3. It must be capable of authenticating the merchant. For that, it needs to have enough storage for root certificates. It must have public key cryptographic functions.
4. It must also have symmetric cryptographic functions for the establishment of the secure channel between the mobile phone and the merchant' server.

Let us consider successively different type of mobile phones and see what capabilities they have and how to enable them to participate in mobile e-commerce.

Standard GSM phones

A GSM (Global System for Mobile communication) phone [4] [5] comprises of:

- an *ME (Mobile Equipment)* which is actually the "empty" phone with the display, keypad, microphone, speaker.

- and a *SIM (Subscriber Identity Module)* which is a removable smart card. The SIM contains *the International Mobile Subscriber Identity (IMSI)* which unambiguously identifies the subscriber. Without a valid IMSI, GSM service is not accessible. The SIM contains also the security features for subscriber authentication such as authentication algorithm (A3), subscriber authentication key (Ki), cipher key generation algorithm (A8), cipher key (Kc)

The ME is the master and initiates commands to the SIM and there is no mechanism for the SIM to initiate a communication with the ME. A standard GSM phone does not meet nay of the requirements mentioned above and is not capable to engage in mobile e-commerce.

GSM SAT enabled phones

The *SIM Application Toolkit (SAT)* provides mechanisms, which allows applications, existing in the SIM, to interact and operate with any ME supporting the specific mechanisms required by the application. A browser, the public key cryptographic functions and a user private key can be installed in the SIM. However, the SIM does not have enough storage capacity for all the certificates needed and is hence not capable of generating complete digital signature. In addition, in order to communicate with merchant's web server, the SAT phone needs assistance from an intermediary server that has similar functionality as the WAP gateway. We will not consider pure SAT phones since more powerful WAP phones have emerged.

WAP phones

The WAP phone is a mobile phone that has a WML browser and a WAP protocol stack on the ME. It is hence capable of communicating with any Web servers via the WAP gateway. The connection with the WAP gateway can be based on different bearers such as GSM circuit-switched connection, GPRS, SMS, USSD, etc.

The first version of WAP phones, called WAP 1.1 phones do not have public key cryptographic functions for digital signature. However, a combined WAP-SAT phones will both have a WML browser in the ME and public key functionality in the SIM. The only problem is the lack of the interface between the browser and the cryptographic functions on the SIM. The browser is hence not able to invoke the cryptographic functions necessary for user authentication.

In the WAP 1.2 phone, there will be a Wireless Identity Module (WIM), which incorporates both the SIM and also local memory in the ME. Public key cryptographic functions and also the user private key can both be stored in the WIM. There will also be implemented an interface, which allows the browser to communicate with the cryptographic functions. WAP 1.2 phones will be capable of generating digital signature according to the PKCS#1

standard [6], but they will not able to generate an electronic signature according to the PKCS#7 that are required in the validation process of the signature. It is possible to say that even WAP phones are not capable to participate in mobile e-commerce by themselves but they need assistance from the system.

6.3 The Mobile ePay

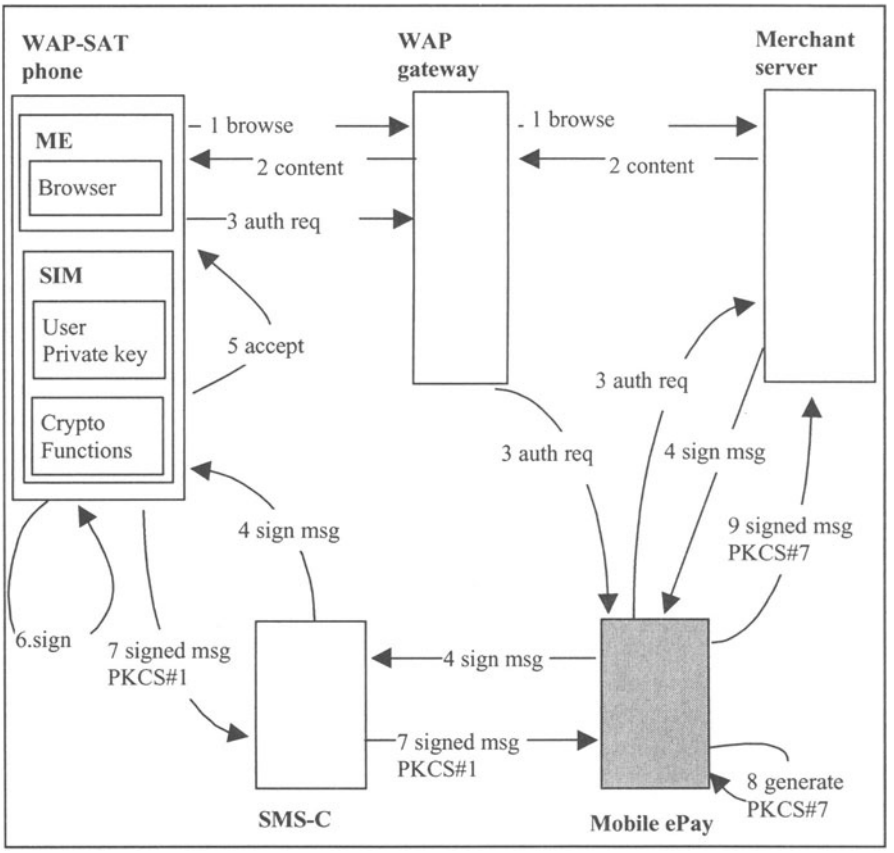

Figure 4. Mobile ePay role in the user authentication

To allow mobile phones to perform digital signature, we introduce a proxy server, called *Mobile ePay*. The Mobile ePay is responsible to perform on behalf of the mobile phones the tasks that the latter are not capable such as:

- Storing the user's certificates
- Generating electronic signature, e.g. PKCS#7 message format from digital signature, e.g. PKCS#1 format, generated by mobile phones.
- Validating of the merchant's servers

In addition to the security functions the Mobile ePay has also payment functions such as:

- Prepaid account supporting micro payment
- Interfacing with the systems of the financial institutions

To illustrate the role of the Mobile ePay in our payment system two operations namely user authentication for WAP 1.1 phones and payment from WAP 1.1 phones are described.

User authentication

The user authentication as depicted in *Figure 4* comprises of the following steps:

1. The user visits a merchant site.
2. The merchant server sends the content to the mobile phone via the WAP gateway.
3. The user wants to authenticate himself toward the merchant. The authentication request is sent to the WAP gateway, which sends to the Mobile ePay . The Mobile ePay sends it to the merchant server.
4. The merchant server generates an authentication message, e.g. a random number and sends it to the Mobile ePay, which sends to the SMS-C (Short Message Center). The SMC-C delivers it to the SIM on the mobile phone.
5. The SIM asks for permission to sign.
6. If the user accepts the SIM performs the signing, i.e. generating a digital signature in PKCI#1 format.
7. The SIM sends it back to the SMS-C, which sends it to the Mobile ePay.
8. The Mobile ePay generates an electronic signature in PKCS#7 format by using the received digital signature in PKCS#1 format.
9. The Mobile ePay sends the complete electronic signature to the merchant server.

Payment from WAP 1.1 phones

1. The user visits a merchant site.
2. The merchant server sends the content to the mobile phone via the WAP gateway.
3. The user wants to buy. The request is sent to the WAP gateway, which forwards it to the Mobile ePay. The Mobile ePay delivers it to the merchant server.
4. The merchant server sends an offer to the Mobile ePay.

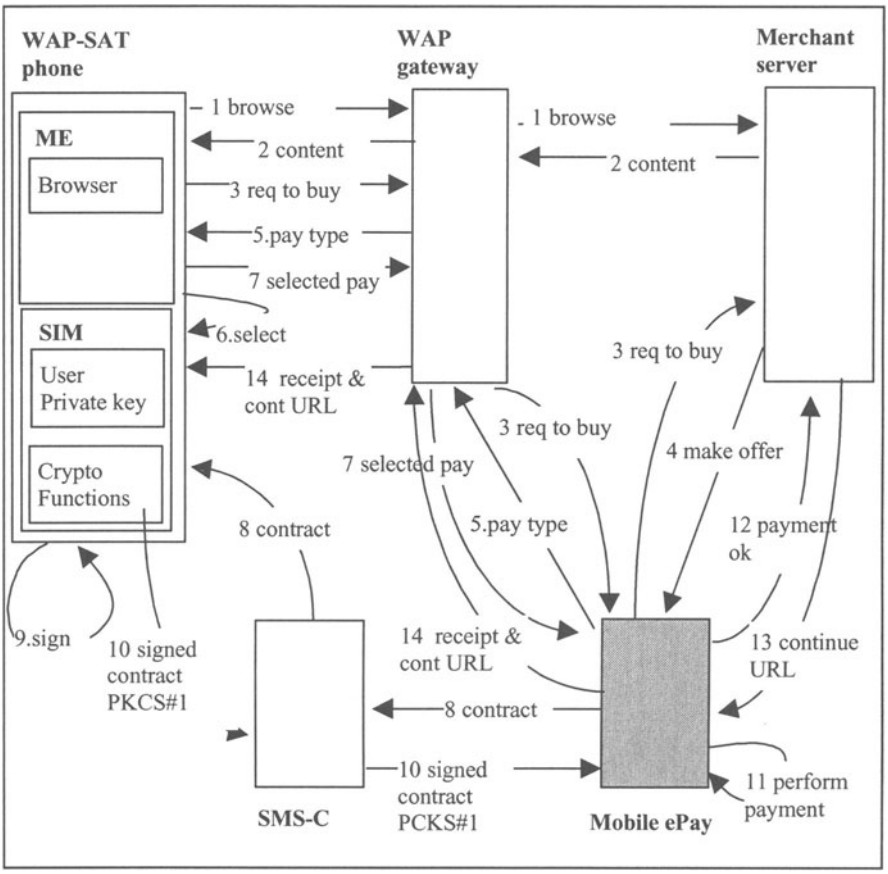

Figure 5. Payment from WAP 1.1 phones

5. The Mobile ePay sends a request for payment type to the browser via the WAP gateway

6. The user selects the payment type, e.g. prepaid account, credit cards, etc. and

7. The payment type is sent to the Mobile ePay via the WAP gateway.

8. The Mobile ePay sends the contract to the SIM via the SMS-C.

9. After asking for confirmation from the user, the SIM performs the signing

10. The SIM sends the digital signature back to the Mobile ePay via the SMS-C.

11. The Mobile ePay executes the necessary transactions according to the payment type. This may include transactions towards financial institutions in case of payment by credit card.

12. The Mobile ePay sends a confirmation to the merchant server.

13. The merchant server returns a URL for the continuation of browsing.

14. The mobile ePay generates a receipt and sends it together with the URL for continuation to the browser via the WAP gateway.

The browser can then continue with the browsing from the received URL. The shopping is hence completed.

7. CONCLUSION

In this paper a mobile e-commerce system is presented. Taking into account the physical and functional limitations that prevent mobile phones from participating to mobile e-commerce, the system introduces a proxy server that offers the necessary assistance to mobile phones. In addition to the security functions, the Mobile ePay also have payment functions such as prepaid account, interface towards financial systems. With Mobile ePay, the user can perform in a secure way any mobile e-commerce service such as doing bank transaction, buy goods or services, from mobile phones. The proposed solution is far from being perfect and quite a lot of issues remain to be done such as time stamping for electronic signature, the relation between the private public key pair and the user, i.e. how many key pair should the user have and the relation between key pair and certificates, i.e. how many certificates can be associated to a key pair

REFERENCES

[1] Visa & Master Card: SET Secure Electronic Transaction Specification - Book One: Business Description, version 1.0, May 31, 1997, http://www.setco.org/download.html/#spec

[2].Visa & Master Card: SET Secure Electronic Transaction Specification - Book Two: Programmer's Guide, version 1.0, May 31, 1997, http://www.setco.org/download.html/#spec

[3]. Visa & Master Card: SET Secure Electronic Transaction Specification - Book Three: Formal Protocol Definition, version 1.0, May 31, 1997, http://www.setco.org/download.html/#spec

[4]. ETSI: GSM 02.17 V8.0.0 Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM); Functional characteristic

[5]. ETSI: GSM 11.14 Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) Interface

[6]. RSA Laboratories. PKCS #1: RSA Encryption Standard. Version 1.5, Nov 1993

[7]. RSA Laboratories. PKCS #7: Cryptographic Message Syntax Standard. Version 1.5, Nov 1993

[8] IEEE P1363: Standard Specifications for Public-Key Cryptography.