A Notational Payment Scheme for Mobile e-Commerce

Kou-Chen Wu

Telecommunication Laboratories,
Taoyuan, Taiwan, R.O.C.
Email:wuchris@ms.chttl.com.tw

ABSTRACT

Due to its inherent "anytime, anyplace, anywhere" convenience, mobile communication is believed going to extend the reach of e-commerce into the world of mobility. This paper proposes a notational (credit-based) payment scheme for mobile e-commerce. In our method, we define a subscriber certificate based on ITU-T X.509 recommended attribute certificate as a vehicle mainly for carrying the certificate subject (mobile user)'s maximum allowed credit amount. With subscriber certificate, a mobile user can prove his credit to the merchant server while conducting a transaction and the expenditure is added to the mobile user's monthly phone bill without the needs of paying directly to the merchant. We also describe the overall WAP (Wireless Application Protocol) network architecture as well as the application of subscriber certificates in mobile e-commerce transaction procedure. Though WAP can support the public-key cryptographic computation, the main challenge to this approach is a powerful computing capability required by the mobile terminals.

Keywords: WAP; Attribute Certificate; Mobile e-Commerce; Payment;

1. Introduction

Today, mobile phones have become a mainstream voice communication medium. A new challenge to mobile telephones is transmitting voice as well as high-speed multimedia traffic to users on the move. The technology to tackle this challenge is known as the third-generation (3G) mobile phones. The International Telecommunication Union's International Mobile Telecommunications for the year 2000 (IMT 2000) initiative for the third-generation technology declares the data rate requirement [6]. It includes: 144kb/s for user in fast moving motor vehicles, 384kb/s for pedestrians who stand still or moving slowly, and 2.048Mb/s for operations in home or offices. Besides, adaptive radio interface is another significant feature of 3G technology, which suites the high asymmetric nature of Internet communication.

Ovum report indicated that [8], by around 2003, the number of mobile devices capable of accessing the Internet will exceed the number of PCs. In order to encourage the adaptation of access to Internet based information services via wireless mobile devices, a new standard protocol, called the "Wireless Application Protocol" (WAP) was defined by a consortium, consisting of Ericsson, Motorola, Nokia, and Phone.com [7,10,11].

Due to its inherent "anytime, anyplace, anywhere" convenience, mobile communication undoubtedly will extend the reach of e-commerce into the personalized and immediate world of mobility. With public mobile network, people can access information and conduct transactions that result in the transfer of value in exchange for information, services or goods. The broad range of mobile e-commerce services may include banking, monitoring stocks and shares, ordering cinema & train tickets, playing games etc.

A key component to the success of e-commerce is a payment method, an indispensable part of a complete transaction. A lot of electronic payment systems have been proposed, such as Payme, PayWord, MicroMint, iKP, Millicent, NetBill, E-cash, NetCash, NetCheque, etc. In the following table 1 are listed some existing electronic payment systems using the Internet [2]. As Metter & Colomb indicated [7], existing HyperText Markup Language (HTML) applications can be conveyed into Wireless Markup Language (WML) applications for use on WAP-enabled devices, yet this process is not as simple as the alternation of the markup tags. With regard to conducting a transaction activity with a mobile phone, the appropriateness of the existing payment methods to mobile e-commerce deserves advanced research due to the different protocol hierarchy. We will not consider this topic further in this paper, instead, a new notational payment scheme is proposed.

Table 1. On-line payment systems [2].

On-line Payment Systems		
Cybercash	Checkfree	Digicash
Netbill Project	Intuit	Electronic Funds Clearinghouse
Netcheque	iKP protocol	Sandia's Ecash system
Net market	Netscape	Netbank
VISA/MC SET	Mondex	IBM electronic commerce
Security First Networkbank FSB	GC Tech/ GlodeD	

In practice, Sonera, the largest mobile operator in Finland, has offered a smart payment method called "Sonera Mobile Pay" for mobile user [9]. In that method, the mobile phone is used as a wallet. While a mobile user visits a vending machine, the mobile user pays products and services by calling a given phone number without the needs for cash, ticket or tokens. Though this scheme is convenient for purchases from physical vending machines, nevertheless, it does not cover the transactions occurred in the cyber world.

According to the classification scheme by Ferreira & Dahab [5], "Sonera Mobile Pay" is a kind of notational (credit-based) exchange model. Sonera server adds the transaction expenditure to the mobile subscriber's account, and the payment will be settled after the mobile user pay his phone bill. This convenience inspires our interest in designing a payment scheme for mobile e-commerce on the Wireless Application Protocol. We inherit the notational concept in our design as a valued-added service offered by the mobile operator.

In this paper, we define a particular type of attribute certificate—the subscriber certificate. A subscriber certificate is issued by the mobile operator, i.e., mobile operator is the certification authority. It declares the validity of the mobile subscriber and the maximum amount that the subject can use. Thus, a subscriber certificate represents the authorization from mobile operator, similar to the authorization from the financial institution in a general on-line credit card payment system. In other words, mobile operator offers a kind of electronic credit card service.

In addition to the basic definition of subscriber certificate, we also describe the overall WAP network architecture as well as its usage in transaction procedure.

The rest of this paper is organized as follows. In Section 2, we describe the WAP architecture and an example WAP network. In Section 3, we introduce the data structure of an attribute certificate. In Section 4, we describe the detailed format of the subscriber certificate. In the same section, we also present its usage as well as the overall network architecture. In Section 5, we consider the merits and discussion. At last, conclusion is given.

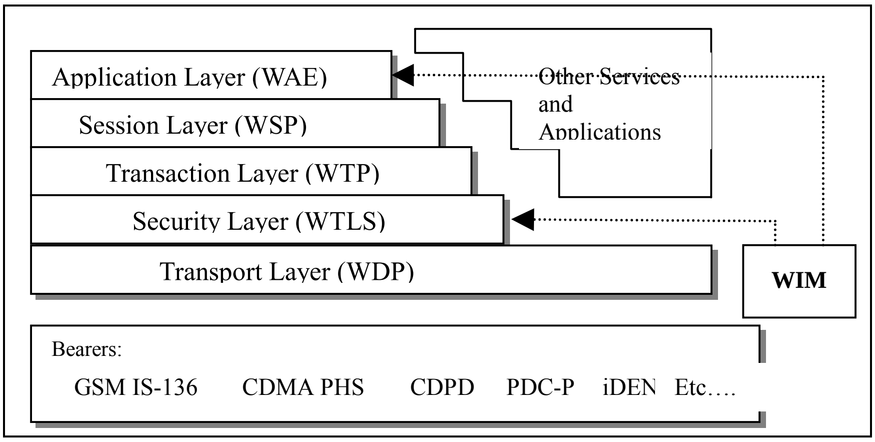

Figure 1. WAP Architecture

2. Wireless Application Protocol

The Wireless Application Protocol (WAP) is a result of the WAP forum's effort. It specifies an application framework and network protocols for wireless devices such as mobile telephones, and personal digital assistants. WAP is positioned at the convergence of wireless data and Internet, and the specifications is useful in developing new applications and services that operate over wireless communication networks.

The WAP architecture is a layered design. Each layer is accessible by the layers above, as well as by other services and applications. Figure 1 depicts the WAP architecture.

To connect between the wireless domain and the WWW, proxy technology is utilized in WAP (figure 2). The WAP proxy is typically comprised of functionality of Protocol Gateway as well as Content Encoder and Decoder. The protocol gateway translates requests from WAP protocol stack, i.e. WSP, WTP, WTLS, and WDP, to the WWW protocol stack, specifically HTTP and TCP/IP. The encoder further translates the WAP content into compact encoded format to reduce the size of data over the network.

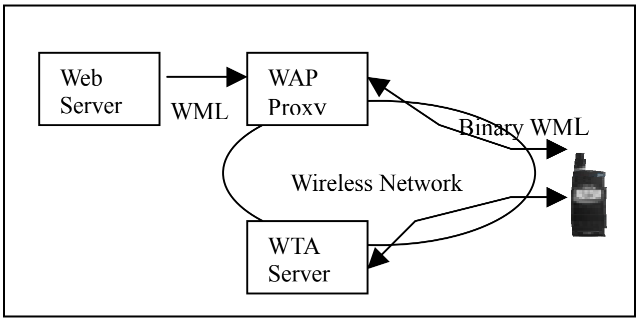

Figure 2. Example WAP Network

In the WAP protocol architecture, WIM is used in performing WTLS and application level security functions. WIM stands for WAP Identity Module, which is a tamper-resistant device. It is used to protect permanent private keys and perform cryptographic operations. It may also be used to store needed certificates: CA and user certificates. These certificates may be subject to change. So, the phone should be able to download new certificates over the air and store them itself or save them in the WIM (not necessary, but useful from the point of view of portability). The WIM functionality can be implemented on a WIM-only smart card or be implemented as part of multi-function card containing other applications, like the GSM SIM.

3. Attribute Certificate

The electronic certificates that people are familiar with are public-key certificates. The primary purpose of the public-key certificate, as indicated by the title of the X.509 standard recommendation, is entity authentication. A public-key certificate provides any recipient of a digital signature with a copy of the sender's public key, plus assurance that the public-key and the private (held by the sender) really belong to the sender. Such assurance is delivered in the form of the Certification Authority (CA's) signature on the certificate.

Though more information can be encoded into the extension fields on the public-key certificate, the use of extensions must not be extended too far. When certified attributes associated with an individual or an entity is for purpose other than authentication, we may convey these attributes in a separate structure, defined as an attribute certificate. Figure 3 shows the ASN.1 data type used to represent attribute certificate.

```
AttributeCertificateInfo::= SEQUENCE {
Version Version DEFAULT v1,
Subject CHOICE{
BaseCertificateID   [0]   IssuerSerial,
SubjectName         [1]   GeneralNames},
Issuer                    GeneralNames,
Signature                 AlgorithmIdentifier,
SerialNumber             CertificateSerialNumber,
AttrCertValidPeriod    AttCertValidityPeriod,
Attributes                SEQUENCE OF Attribute,
IssuerUniqueID           UniqueIdentifier OPTIONAL,
Extensions                     Extensions OPTIONAL }
```

Figure 3. ASN.1 representation of an attribute certificate

There are two ways to identify the subject of an attribute certificate: one is using *SubjectName*, and the other is using *baseCertificateID*. *SubjectName* is a general name of the certificate owner, and the *baseCertificateID* field associates an attribute certificate with a public-key certificate whose subject bears the attributes defined by the field *SEQUENCE OF Attributes*.

4. Our Proposed Method

4.1 Defining Subscriber Certificate based on X.509 standard

A subscriber certificate is a special attribute certificate, embedded in which are the subject's unique identity, maximum credit amount, and his/her public-key. Figure 4 depicts the deployment of a mobile subscriber's attributes in his subscriber certificate.

Subscriber Certificate Info	
Subject	Subscriber Identity
Issuer	General Name OF Mobile Operator
Signature	Algorithm Identifier
SerialNumber	Subscriber Certificate Serial Number
AttrCertValidityPeriod	Subscriber Certificate Validity Period
Subscriber Attributes	Maximum Credit Amount
	Subscriber's Public-key
Signature on the above information	

Figure 4. The contents of subscriber certificates

The subscriber's identity is the mobile subscriber's identity number. It is used to uniquely identify the mobile e-commerce consumer, and help correctly deposit each transaction record. The maximum credit amount indicates the maximum amount that can be used by the mobile subscriber during the validity period. If the cost of requested product or service exceed the mobile user's maximum credit amount, then the merchant server may deny the request or require the mobile user to pay in another way. The subscriber's public-key is correspondent to the subscriber's private key, with which he can sign a transaction description message after confirmation of the merchant's payment request.

In order to preserve the integrity and authenticity of the subscriber certificate, a signature on the certificate content is required by the mobile operator. In other words, the mobile operator is the certification authority. To issue a mobile subscriber's certificate, the mobile operator sets the validity period of the certificate, e.g. 24 hours, and calculates the maximum credit amount, also, the subscriber's public-key is embedded. At last, signature on the above attributes is made.

4.2 Overall Architecture

In our proposed payment method, mobile operator is the authority who issues subscriber certificates, and the validity period of a subscriber certificate is one day. The authority access the billing database, prepares certificates, certifies them, and issues them to mobile users. For this notational payment, mobile operator will set the monthly maximum credit value for each mobile user. This value is embedded in the first subscriber certificate issued in the beginning of every month. That is, the accumulated amount of product or service expenditure recorded in the user's mobile phone bill will not exceeds the maximum credit value set by the operator. Also, the mobile operator issues subscriber certificate on the condition that the subscriber pays his phone bill punctually. Thus, reduce the possible loss caused by bad debts.

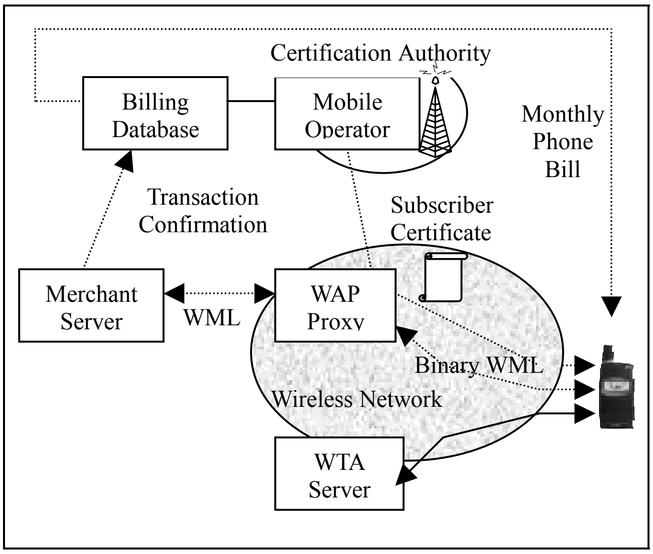

Figure 5. Overall architecture

The billing database shown in the above figure maintains the mobile subscriber's billing record. At the end of each day, the transaction confirmations generated by the subscribers during transaction processes are sent to the billing server, where each subscriber's consumption amount is accumulated and his remained available amount is calculated. Then, with the remained available amount recorded in the *maximum credit amount* field, mobile operator generates a new subscriber certificate for next day's usage.

With regard to the delivery of subscriber certificate to the mobile terminal, the mobile user can initiate a request for a subscriber certificate everyday when he first power on his handset, or the certificate can be delivered to the mobile terminal in a WAP suggested pushed-based model [[11]: p.250].

We use subscriber certificates in a mobile e-commerce environment within which a mobile phone subscriber pays the transaction cost in a notational way. Specifically, a mobile subscriber can make such a transaction as ordering a ticket or retrieving valuable information via the wireless network by adding the transaction cost to his mobile phone bill, instead of paying directly to the merchant. When the mobile user receives his phone bill and pay for it, the mobile operator will then transfer the correct amount of money to the merchants. Figure 6 depicts the transaction procedure:

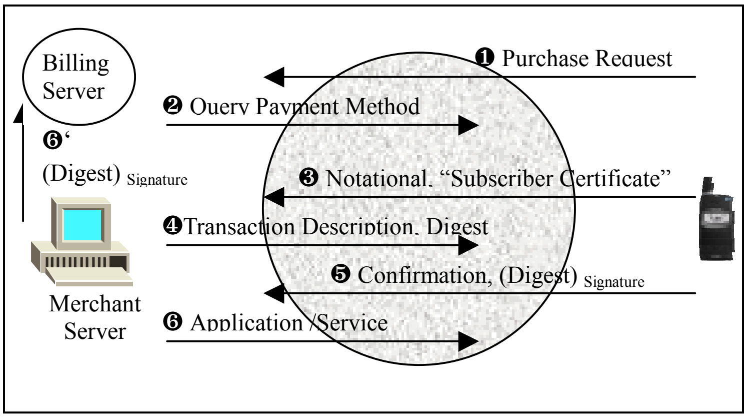

Figure 6. Transaction Procedure

Step❶: The mobile subscriber initiates a purchase request. Step❷: Merchant server queries the subscriber's preferred payment method. Step❸: Mobile subscriber chooses notational payment method, and his subscriber certificate is sent to the merchant. Step❹: Transaction description and its digest are sent to the initiator. The transaction description may include merchant identity, product/service item, time stamp, as well as cost amount. And, the digest is the hashing result of the transaction description. Step❺: The subscriber makes a signature on this description digest, and replies it to the merchant as a confirmation to this transaction. Step❻: Merchant server delivers the requested service, and in step❻': The merchant passes the mobile users' signatures on transaction digests to the mobile operator's billing server in a batch way later in that day.

Since the maximum credit amount field in the subscriber certificate indicates the maximum credit value that the subject is allowed to use during the valid period of the certificate, i.e. 24 hours in our proposed method, it restricts each transaction cost not greater than the value. Nevertheless, it can not prevent the users from conducting transactions in a day spending in a total value more than the maximum allowed credit amount. Hence, enhanced design is needed to solve this problem. Figure 7 depicts our design.

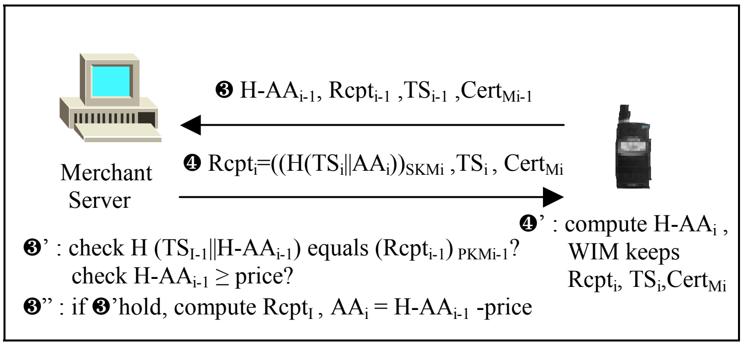
❸ $H\text{-}AA_{i-1}$, $Rcpt_{i-1}$,TS_{i-1} ,$Cert_{Mi-1}$
Merchant Server
❹ $Rcpt_i$=$((H(TS_i||AA_i))_{SKMi}$,TS_i , $Cert_{Mi}$
❹' : compute $H\text{-}AA_i$, WIM keeps $Rcpt_i$, TS_i,$Cert_{Mi}$
❸' : check H $(TS_{I-1}||H\text{-}AA_{i-1})$ equals $(Rcpt_{i-1})_{PKMi-1}$?
check $H\text{-}AA_{i-1} \geq$ price?
❸" : if ❸'hold, compute $Rcpt_I$, $AA_i = H\text{-}AA_{i-1}$ -price

Figure 7. Enhanced design of step 3 & step 4.

The notations used in figure 7 are as follows:

- Mi: Merchant, from which the mobile user purchases service in his i^{th} transaction
- AA_i: Available amount the mobile user can use in the i^{th} transaction, this is calculated by the merchant server
- $H\text{-}AA_i$: Available amount the mobile user can use in the i^{th} transaction, this is calculated by the handset
- $Rcpt_i$: Transaction receipt from the merchant in the i^{th} transaction
- TS_i: Time stamp of the i^{th} transaction
- $Cert_{Mi}$: Public-key certificate of the merchant of the i^{th} transaction
- H(): Hash computation
- $()_{PKMi}$: Public-key encryption using merchant Mi's public-key
- $()_{SKMi}$: Secret-key encryption using merchant Mi's secret-key

In step 3 of the i^{th} transaction, the mobile terminal sends the receipt, time stamp, merchant's public-key certificate of the $(i-1)^{th}$ transaction, and the remained available credit amount to the merchant server. Merchant server, then, decrypts the receipt and checks if the two remained available credit amounts, namely $H\text{-}AA_{i-1}$ from the handset and AA_{i-1} in the receipt, equal with each other. If it does, and the product price is less or equal to the remained available amount, then the merchant server accepts the mobile user's purchase request. The merchant server forms the receipt by signing the hash value of time stamp concatenating with the new remained credit amount. In step 4, the receipt of the i^{th} transaction and the merchant's public-key certificate are sent to the mobile terminal. It then computes itself the new available credit amount, and stores the receipt and public-key certificate from merchant server Mi.

5. Merits and Discussions

Notational (credit-based) payment is convenient for the consumer. The "Sonera Mobile Pay" is a successful payment method, with which the mobile phone user can purchase goods from a vending machine by adding the expenditure to his phone bill. Our proposed method, on the other hand, is suitable for the cyber world transaction, and in particular, the needed cryptographic computation in use of subscriber certificate can be supported by the WAP Identity Module.

In the usage of electronic certificates, both public-key certificates and attribute certificates, revocation of certificates is important in certificate management. The subscriber certificate in our proposed scheme is a short-lived certificate, which has a validity period of a day. Thus, the burdensome certificate management mechanism, such as certificate revocation list (CRL), for the purpose of ensuring the validity of a certificate can be avoided.

The proposed subscriber certificate is a special kind of X.509 attribute certificates. In this work, we have explained its usage in a mobile e-commerce environment. The X.509 standard does not describe how a user gets his attribute certificate from the authority, nor does the management procedure. Thus, our work supplements the X.509 standard.

The Notational (credit-based) payment offered by mobile operator is a value-added service, compared to ordinary telecommunication services. The mobile subscriber can delay payment of the purchase of information or service by transferring the expenditure to the mobile phone bill. In offering this value-added service, the mobile operator can benefit from each transaction commission.

Suitable application of the proposed payment method includes purchasing products or information, such as ordering tickets and downloading MP3 music. However, transaction of small value, e.g. reading news, may need an advanced micro-payment method, for instance, a membership account with ID and password. With that a mobile user can reach the information service with limitation on times, or the service charge can be counted based on the visiting times.

In this work, we assume that each mobile subscriber will pay his bill, thus the merchant (service provider) can correctly receive the payment. However, to put the proposed payment scheme into practice, bad debt is still an important problem that needs to be solved, for the reason that we can not assume every mobile subscriber is honest and responsible for his bill. This is common in off-line credit based payment, e.g., the work by Mu & Varadharajan [12] also meets the challenge. In our method, the maximum credit amount recorded in the subscriber certificate is a loose solution, for it is unable to thoroughly prevent the subscriber from spending more than the allowed credit amount. To conquer this problem, we enhance our method by refreshing the available credit amount each time after a transaction occurred. Detailed description is depicted in figure 7. The problem mentioned above is an interesting topic, we believed it deserves further study.

6. Conclusion

In this study, we have described the generation and usage of mobile phone subscriber certificate. A subscriber certificate is a kind of X.509 attribute certificates with the subject's maximum credit amount provided in the form of target attribute. In this work, we have explained its use in a WAP-based mobile e-commerce environment. Since the X.509 standard does not describe the procedure which a user can use to get his attribute certificate from the authority [[3]: p.49]. Our work supplements the standards though the credit amount is only a kind of attribute.

The most significant benefit of using a subscriber certificate in our notational (credit-based) payment method for mobile e-commerce is that a mobile user can request services or products from merchant servers without a need of paying directly to the merchant. This is achieved by adding the transaction expenditure to the mobile user's phone bill. Also, the user's signature on the confirmation of transaction can be a proof of his willing to conduct the transaction. In addition, the mobile telephone operator can benefit from the commission of each user's transaction.

Further research can focus on advanced electronic certificates, and electronic payment methods specific for mobile e-commerce. Firstly, The studies in electronic certificates, especially attribute certificates, are worthy of advanced exploration. Existing related studies are few, including Chaum & Pedersen's [1] work on anonymous certificate, Mu & Varadharajan's [12] credit-based payment, and Hwang, Wu & Liu's [4] work on access control with role attribute certificates. In our opinion, design of an off-line electronic certificate with a limitation on times of its usage is an interesting topic and such kind of certificate is believed to have practical applications.

Secondly, a lot of electronic payment methods using the Internet have been proposed. However, with the promising prevalence of mobile e-commerce, due to the inherently different protocol architecture, appropriateness of these existing payment methods to mobile environment, specifically WAP, deserve further study.

7. REFERENCES

[1] D.Chaum and T.P.Pedersen, "Wallet database with observers," in *Advances in Cryptology—CRYPTO '92 Proceedings*, pp.89-105, Springer-Verlag, 1992.

[2] Ioannis Mavridis, George Pangalos, Sead Muftic, "A Secure Payment for Electronic Commerce," in *Tenth International Workshop on Database and Expert Systems Applications Proceedings*, pp.832-836, 1999.

[3] ITU-T Recommendation X.509 (ISO/IEC 9594-8) Information Technology—Open Systems Interconnection—The Directory: Authentication Framework, June 1997.

[4] Jing-Jang Hwang, Kou-Chen Wu, Duen-Ren Liu, "Access Control with Role Attribute Certificates," *Computer Standards And Interfaces*, 22(1), 2000, pp.43-53.

[5] Lucas de Carvalho Ferreira, Ricardo Dahab, "A Scheme for Analyzing Electronic Payment System," in *14th Annual Computer Security Applications Conference* Proceedings, 1998, Proceedings, pp.137-146.

[6] Malcolm W. Oliphant, "The Mobile Phone Meets the Internet," *IEEE Spectrum*, August 1999, pp.20-28.

[7] Marcin Metter, Robert Colomb, "WAP enabling existing HTML applications," In *First Australasian User Interface Conference (AUIC 2000)* Proceedings, pp.49-57.

[8] Ovum, "Mobile@Ovum-Mobile e-commerce:market strategies," Ovum Ltd., February 2000.

[9] Sonera, "Sonera Mobile Pay," Sonera Ltd., URL: (http:// www.sonera.fi/english/solutions/mobilepay/)

[10] WAP Forum, "Wireless Application Protocol Architecture Specification," WAP Forum Ltd., April 30 1998. (URL: http:// www.wapforum.org)

[11] WAP Forum, "Wireless Application Environment Overview," WAP Forum Ltd., November 04 1999. (URL:http://www.wapforum.org)

[12] Yi Mu, Vijay Varadharajan, "A New Scheme of Credit Based Payment for Electronic Commerce," In *23rd Annual Conference on Local Computer Networks, (LCN'98)* Proceedings, pp.278-284, 1998.