Available online at www.sciencedirect.com
ScienceDirect
Computer Communications 30 (2007) 893–903
computer communications
www.elsevier.com/locate/comcom

Design and implementation of wireless PKI technology suitable for mobile phone in mobile-commerce

Yong Lee [a,*], Jeail Lee [a], JooSeok Song [b]

[a] Korea Information Security Agency, Seoul, Republic of Korea
[b] Yonsei University, Seoul, Republic of Korea

Received 1 May 2006; received in revised form 22 October 2006; accepted 26 October 2006
Available online 27 November 2006

Abstract

With the advent of wireless communication and internet protocol, many technologies have been developed to provide mobile phone user with the wireless internet service. Security supporting wireless internet must be guaranteed at same level as the wired security. But PKI (Public Key Infrastructure) which is used for the security of e-commerce in wired internet is not suitable for the mobile phone because of the fundamental limitation of performance such as less memory and less powerful CPU. Therefore, we need to develop a wireless PKI (WPKI) that provides the similar security level as the wired PKI supporting mobile phone. In this paper, we consider why it is difficult to apply the wired PKI technology to the mobile phone and how to cope with these problems. We propose wireless PKI technology and illustrate that implementation result of the proposed wireless PKI technology on the newest mobile phone. We minimize data sizes processed in mobile phone, and optimize protocols for the certificate management and verification between mobile phone and server. This results in the reduced module sizes to be able to install in mobile phone. Hence, the proposed WPKI technology shows that security is in the same level as the wired PKI and all PKI procedures are successfully processed in mobile phone.

Keywords: Wireless Public Key Infrastructure; Digital certificate; Mobile phone; Wireless internet

1. Introduction

As mobile user utilizes wireless internet through mobile phone, a variety of internet services supporting mobile phone have been also increasing. The wireless internet refers to accessing internet through wireless communication using mobile phone. For mobile users to successfully utilize data service and M-commerce through wireless internet, security must be guaranteed. Similar to the wired internet, for wireless internet to provide secure M-commerce service, following functions must be provided: confidentiality and integrity of data, entity authentication, and non-repudiation. Technologies that apply these security elements to mobile phones and wireless internet environment must be able to provide users with the same level of security as in the wired internet environment [1–5].

Many security protocols on internet and most security applications for e-commerce are based on public key cryptography. PKI (Public Key Infrastructure) applies a public key cryptographic method to transmit user's public key and user's identity in a secure and reliable way. Users of public key cryptography transmit their public keys to others, and must safeguard private key corresponding to the public key [6,7].

To guarantee security of M-commerce via wireless internet, public key infrastructure technology suitable for wireless environment must be required. In the wireless environment, we have two different elements from wired internet: mobile phone and wireless internet [2,8,9].

* Corresponding author. Present address: Samsung Electronics Co. Ltd., Maetan-Dong, Suwon-City 443-370, KyoungGi-Do, Republic of Korea. Tel.: +82 10 3301 6394/31 279 7536; fax: +82 31 279 5255.
E-mail address: yleehyun@gmail.com (Y. Lee).

0140-3664/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2006.10.014

Mobile phone has fundamental limitation of performance such as less memory and less powerful CPU. And wireless data network presents more constrained communication environment such as less bandwidth and has different protocol compared to wired internet protocol. Therefore, it is difficult to apply wired PKI technology for security than wired environment [3,9–13]. At first, mobile phone must generate public key pair and compute digital signature using the key. And a public key certificate could be issued to a mobile user through wireless internet. The public key certificate provides a method to bind the public key and its owner. Using the certificate, the mobile user must authenticate itself and make secure channel for internet service such as M-commerce.

In this paper, we introduce Wireless Public Key Infrastructure (WPKI) model for solving previously mentioned problems and propose optimal certificate profile, optimal certificate management protocol, and efficient certificate verification scheme. Then we show performance as module sizes and processing speed in mobile phone, and validate their security. Section 2 introduces public key infrastructure. Section 3 describes current wireless internet protocol, its problems and limitations of mobile phone and wireless network. We consider requirements for WPKI and what to be taken into consideration when the public key infrastructure is applied to mobile phone. Section 5 describes the proposed wireless PKI technology. Section 6 shows performance of wireless PKI through module size and processing speed implemented in mobile phone, and validates its security, and Section 7 concludes this paper.

2. Public key infrastructure

A PKI consists of Certification Authorities (CAs), Registration Authorities (RAs), Certificate holders, Clients, Repositories, Cryptographic Algorithms and Protocols, Policy shown as Fig. 1 [6]. The certificate binds a public key and its owner identity. PKI service scenario is followings.

(1) CA performs user identification through direct confrontation.
(2) CA provides the user with identity and password.
(3) A mobile phone generates a key pair and certificate request message.
(4) The mobile phone signs certificate request message and digital signature verification key with digital signature generation key.
(5) The mobile phone sends them to CA.
(6) CA confirms the ownership of the digital signature generation key.
(7) CA generates a certificate.
(8) CA publishes the generated certificate on a directory.
(9) CA sends the certificate information to user.
(10) The mobile phone obtains the certificate and can exchange the messages with digital signatures using the public key to another entity.

3. Characteristics of wireless internet

This section describes Wireless Application Protocol (WAP) as representative wireless internet protocol supporting mobile phone, security technologies based on the wireless internet protocols and its problems.

3.1. Wireless internet protocol

Unlike wired internet, wireless internet has many restrictions. A mobile phone does not have the same computational ability and storage capacity as a desktop computer, and wireless communication has lower transmission bandwidth than its wired counterpart. Applying wired internet protocols to mobile phone has many problems such as the limitations in screen size, computing power, and memory capacity. Wireless internet technologies have been developed to overcome these restrictions of the wireless environment.

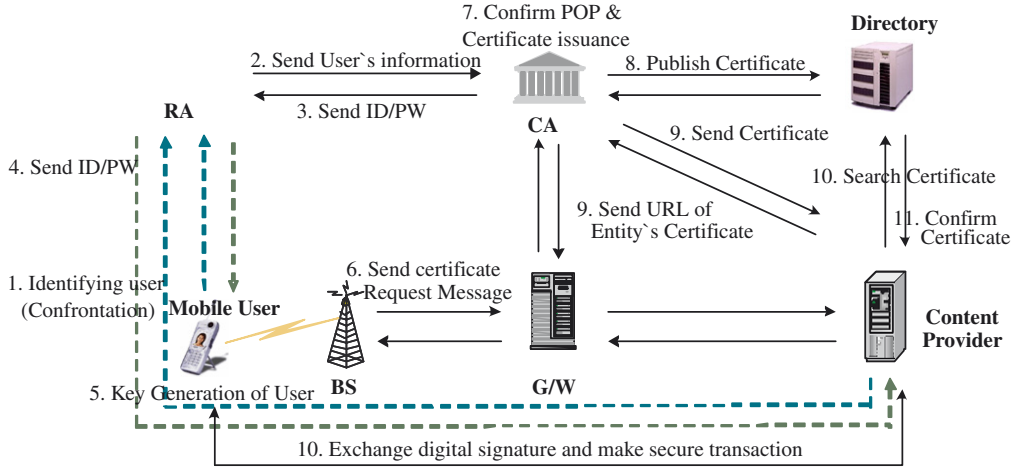

Fig. 1. PKI Model and scenario.

Currently, a representative wireless internet access supporting a mobile phone is WAP, which is not based in the wired internet protocol, HyperText Transport Protocol (HTTP) [8,9]. Although WAP 2.0 was announced as [9] following WAP 1.x, up to now, WAP 1.x has been applied to wireless internet.

In WAP 1.x, Wireless Transport Layer Security (WTLS), equivalent to Secure Socket Layer (SSL) of the wired internet, is in charge of security [3,10,14].

Though WTLS provides almost the same service as SSL, it can not support end-to-end security between mobile phone and server. Through WAP, data must go through WAP gateway, and data encrypted by WTLS is decoded by the WAP gateway before it is encrypted using SSL and transmitted to the server. Inversely, the data encrypted with SSL is decoded by the WAP gateway before it is encrypted with WTLS and sent to the mobile phone. This causes serious security problem in the gateway [3,10,14].

But certificate management protocol in WAP is based on WTLS, and hence it could not support confidentially of certificate request information.

3.2. Limitations of mobile phone and wireless network

We take into consideration limitations of the wireless communication environment when implementing wireless PKI. Compare to wired internet, there are many network problems such as less bandwidth, more latency, insecure connection and device problems such as less powerful CPU, less memory size, restricted battery power, small display and input device.

Due to these problems, it is very difficult to apply wired PKI system to the wireless environment. A mobile phone lacks computing capabilities of PKI services such as key generation, digital signature generation and verification, certificate validation, and Certificate Revocation List (CRL) verification, and memory size of storing certificate and CRL. Due to less wireless communication bandwidth, processing of CMP (Certificate Management Protocol) for certificate life cycle such as certificate issue in the mobile phone, and downloading CRL required for certificate verification must be considerable burden [3,15].

For example, CPU speed of a mobile phone with MSM3100 chip is 13.5 MHz and CPU speed in a Pentium IV with 2.8 GHz is about 200 times faster. Because memory size of a mobile phone is only 2 Mbytes, mobile user and content provider want PKI module size on mobile phone be minimized. A mobile game size on mobile phone is only 5 kbytes. But PKI module size is bigger than game. They want to load more game software to mobile phone. Hence smaller data and smaller module sizes are important issue.

4. Requirements for wireless PKI

In order to apply wireless PKI to mobile phone through wireless internet with the same level of security as that of wired internet, the following requirements must be satisfied.

- Select optimal digital signature algorithm to be calculated in mobile phone.
- Minimize data size to be stored in mobile phone and to be transmitted through wireless bandwidth.
- Optimize CMP protocol to be processed in mobile phone and through wireless bandwidth.
- Optimize certificate validation scheme.

We present the detailed requirements and problems.

4.1. Optimal digital signature algorithm in mobile phone

For digital signature, computation of public key pair generation, digital signature generation and verification in mobile phone are required.

RSA based public key cryptographic algorithm has been selected for digital signature algorithm of PKI for a long time [6]. But public key pair generation based on RSA algorithm in a mobile phone might be time consuming or be impossible due to the lack of memory and CPU performance [16,17]. Therefore we need an alternative public key algorithm to make the key generation possible in the mobile phone.

After a public key pair is generated, the mobile phone must perform computation for digital signature generation and verification, and time for digital signature operation must be acceptable to users.

4.2. Minimize data sizes

The major data storing and processing in a mobile phone are certificate and CRL.

Generally, a certificate used in PKI is ITU X.509 certificate defined by ITU [7]. This X.509 certificate has basic fields for certificate verification and many extension fields that are required for certificate path validation. These extension fields increase size of the certificate and make procedures of certificate path validation complex. We classify duplicate or unnecessary fields in the certificate. Thus, the optimization of certificate profile is required without side effect for the certificate verification and path validation.

In order to validate X.509 certificate, CRL verification is also required. To do this, a mobile phone has to download CRL from CA, and check if a certificate is in CRL. This procedure costs the mobile phone and wireless transmission considerable burden. We need a efficient and reliable method to validate X.509 certificate without direct verification of CRL in mobile phone.

4.3. Optimal certificate management protocol

Current wired CMP is based on SSL [18–20] and certificate request in WAP is based on WTLS. As previously mentioned, security protocol based on WTLS in WAP does not

support end-to-end security. In the scheme, information necessary for the certificate request could not be securely transferred to CA. Therefore, new wireless CMP (WCMP) that is based on neither SSL not WTLS and is performed by itself is required. The WCMP must guarantee the same functions as wired CMP. This protocol should be more lightweight than wired CMP, and be optimized for processing in mobile phone and through wireless transmission.

4.4. Optimal certificate validation scheme

To validate X.509 certificate, certificate chain and CRL must be acquired, and verified in mobile phone. In [6] and [7], certificate path validation scheme is much complicated and difficult for mobile phone to process. We need efficient and reliable method for certificate path validation that is possible for mobile phone to process. We have several candidates such as applying the delta CRL scheme to reduce CRL size to download [21]. Also, the certificate validation procedure might be optimized, or certificate validation scheme might be delegated to a trust system. We will consider these candidate schemes in the next section.

5. The proposed WPKI architecture

We propose a wireless PKI model that satisfies the requirements mentioned before and examine the proposed PKI model, detailed technologies, and its characteristics.

5.1. Wireless PKI model

Fig. 2 shows the proposed WPKI model and we assume the followings.

- We consider communication between mobile phone and server as content provider, and exclude communication between mobile phones.
- This model has one CA, i.e. two-level hierarchical architecture shown as Fig. 2.
- End entity such as a mobile phone or server has only one public key pair and one certificate for one purpose.
- A mobile phone and server have one unique name.
- We consider the possibility that mobile phone receives the wired X.509 certificate owned by server that was designed for wired internet.

In this model, we apply X.509 certificate as certificate of mobile phone. Because X.509 certificate owned by mobile phone is verified by server, verification of the certificate is not difficult in the server with enough performance. Even storing of a certificate is burdening to the mobile phone and mobile phone just sends it to other party without any operation for certificate. In this model, CA issues a certificate, publishes it directory, and sends only URL of the certificate to the mobile phone. When a mobile phone communicates with server, the mobile phone sends URL of the certificate to server, not the certificate itself. The server can easily access the directory and acquire the certificate. As a result, the mobile can save memory space for another use.

For server, we use X.509 and short-lived certificate [10]. If a server sends X.509 certificate to mobile phone, efficient and lightweight certificate validation scheme might be required in the mobile phone. Sometimes the mobile phone may validate X.509 certificate because it may try to connect a server that was designed for serving only wired terminal and has only X.509 certificate. We introduce Online Certificate Status Protocol (OCSP), and the mobile phone

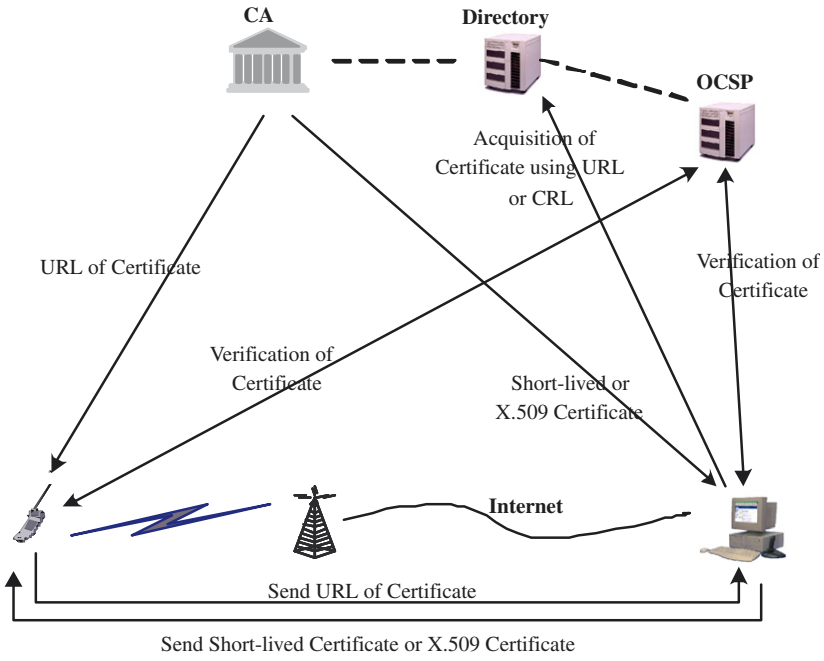

Fig. 2. Wireless PKI Model.

delegates OCSP to validate certificates rather than validation in the mobile phone by itself. In this case, the mobile phone could avoid the complicated procedure of certificate validation and acquire a result from the trusted OCSP server [22].

In [10], OMA defined WTLS-certificate as short-lived certificate for WTLS connection. Short-lived certificate does not have extensions that is used for certificate path validation and has valid period for short time. It is verified only if signature of CA and valid period for certificate validation are valid [2,10]. Therefore, mobile phone can avoid burden of CRL download and certificate path validation.

We explain the detailed components for WPKI architecture.

5.2. Digital signature algorithm

Because a mobile phone has much smaller memory and slower CPU performance than server, it is hard for mobile phone to run complex public key calculation. We consider optimal digital signature algorithm for mobile phone.

First, generation of public key pair is required for digital signature. The time that it takes to mount a brute force attack on encipher of the data is directly proportional to the key size used to encipher the data. Although the time depends on the hardware being used, it was estimated that a brute force attack on a key size of 128 bits for DES algorithm, using multi-trillion dollar specialized hardware, would still take 1011 years in 1995 [17,23]. We decide that a key size of at least 128 bits would be sufficient to protect the confidentiality of the data. Thus, we choose RSA 1024-bit key size that is at the same security level as 128 bits from [17].

From our implementation, we cannot measure the generation time of RSA 1024-bit public key pair in mobile phone, since it takes so long time and the mobile phone was down and disconnected from wireless connection. Thus, the alternative digital signature algorithm that is able to be performed in the mobile phone, with same security level is required and we choose ECC-based Elliptic Curve Digital Signature Algorithm (ECDSA) that is recommended by [3].

For ECDSA 163-bit key size, equivalent to RSA 1024-bit key size, it takes shorter time to generate public key pair in mobile phone than RSA algorithm [23]. Since ECDSA 163-bit key size is less than RSA 1024-bit key size, a certificate size including the public key could be reduced.

5.3. Certificate and CRL profiles

In this section, we describe Wireless X.509 certificate profile issuing for mobile phone and server, and short-lived certificate profile issuing for server to reduce verification load of mobile phone.

Table 1 shows the detailed fields of Wireless X.509 certificate for mobile phone in this model. X.509 certificate consists of basic field and extension field. Generation implies that a certificate has to include the specified field, and Process implies that if the specified filed is present in the certificate, the field must be examined when the certificate is verified. In basic field, subject unique identifier and issuer unique identifiers are present in the certificate to handle the possibility of reuse of subject and/or issuer names over time [6]. Our profile defines that names should not be reused for different entities and CAs conforming to this profile should not generate certificates with unique identifiers.

Table 1
Wireless X.509 certificate profile for mobile phone

	Generation	Process
Basic field		
Version	m	m
Serial number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m
Subject	m	m
Subject Public Key Info	m	m
Issuer unique identifier	x	x
Subject unique identifier	x	x
Extension field		
Authority key identifier	m	o
Subject key identifier	m	o
Key usage	m	m
Private key usage period	x	x
Certificate policy	m	m
Policy Mapping	–	–
Subject alternative names	m	m
Issuer alternative names	o	m
Subject directory attributes	x	x
Basic constraints	x	x
Name constraints	–	–
Policy constraints	–	–
Extended Key Usage	o	m
CRL distribution points	m	o
Domain information	o	o
Authority information access	m	o

m: mandatory, o: optional, x: not recommended, –: not defined.

Authority key identifier and subject key identifier are used to identify the public key where an issuer and/or subject have multiple signing keys. In the previous section, we assumed that all entities have only one signing key [6]. Thus, we define that these extensions could be processed optionally.

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than validity period of the certificate [6]. We also assume that the private key usage period is same as the validity period of the certificate and do not use this extension. Because the policy mapping extension is used in CA certificates, we do not define this extension for end entity. For the issuer alternative names extension, because we have one CA, this extension is not recommended.

The subject directory attributes extension is used to convey identification attributes (e.g., nationality) of the subject, we do not define this extension for end entity with unique identifier. Also, since the basic, name, and policy

constraints extensions are defined for CA, we do not define these extensions for end entities certificate.

The extended key usage indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. We define this extension optionally and if the extension is present, then the extension must be examined.

Since applying OCSP for certificate validation in this model, we use domain information and authority information access extension for specifying how to access of OCSP server [6,22]. For server, CRL distribution points could be used to obtain CRL information. The authority information access and the CRL distribution points extensions must be present in the certificate for certificate validation but verifier can choose a method how to validate certificate, CRL or OCSP. Table 2 shows short-lived certificate profile that does not include serial number and extension.

5.4. Wireless certificate request and management protocol

We consider how a mobile phone securely requests a certificate to CA and CA issues it to the mobile phone. The followings are requirements of certificate request protocol [18,19].

- Certificate request message is constructed at mobile phone. This value should include a public key, end-entity's reference number like as ID and password. We assume that other requested certificate fields, and additional control information related to the registration process are made in out-of-band.
- A POP (Proof of Possession) of the private key corresponding to the public key for which a certificate is being requested value is included in certificate request massage.
- Method that the certificate request message is securely communicated to a CA.

To satisfy these requirements, we designed wireless certificate management protocol and developed this protocol on mobile phone. Fig. 3 shows the detailed Wireless CMP. Since a password could be transferred to a CA by hash value, confidentiality of the password could be guaranteed. We use the public key as one time information for prevention of replay attack. POP could be accomplished in signature and verification of SignedValue. The protocol of Fig. 3 could be extended for certificate management protocol for the certificate life cycle [3,6,20].

Table 3 shows the message formats of the certificate management protocol for certificate life cycle.

Table 2
Short-lived certificate profile

Field name	Value	Generation/process
certificate_version	V1	m
signature_algorithm	ECDSA with SHA	m
issuer	⟨Text⟩	m
valid_not_before	GMT	m
valid_not_after	GMT	m
Subject	⟨Text⟩	m
public_key_type	ECDH	m
parameter_specifier	optaion	m
signature	ECDSA signature value	m

GMT: Greenwich Mean Time, ECDH : EC-based Diffie-Hellman.

5.5. Certificate validation scheme

As mentioned before, a mobile phone delegates validation authority such as OCSP to validate certificate in this model. The mobile phone can avoid burden of CRL download and storage as well as the complicated procedure to acquire and verify certificate chain.

For short-lived certificate, the mobile phone validates the certificate through verifying only signature and valid period in the certificate.

A delta CRL that lists the certificates whose revocation status has changed since the issuance of a referenced complete CRL may be used for CRL verification in mobile phone. But conformation procedure of complete CRL from delta CRL is not easy for mobile phone and requires additional module. Also the mobile phone should store the base CRL, finally complete CRL. Thus, we exclude the delta CRL-based CRL verification from our model.

Fig. 4 shows the certificate validation procedure. The server acquires a certificate from directory using URL of the certificate received from the mobile phone, and validates it using CRL or OCSP.

Inversely, the server sends mobile phone its certificate with CA's certificate and ARL (Authority Revocation List) together. Consequently, the mobile phone needs not to acquire the CA's certificate and ARL from directory as shown in Fig. 5. It reduces the number of wireless connections between mobile phone and directory.

6. Performance analysis

This section analyzes the performance of implementation by the proposed model, compared to the wired PKI. Table 4 shows WPKI test environment.

Table 5 shows the comparison of RSA algorithm that has been used in wired PKI and ECDSA algorithm calculation time in mobile phone. In the mobile phone, we could not measure RSA key generation time because the mobile phone has been down during key generation. This shows that RSA algorithm could not be applicable to even the newest mobile phone.

The running time of ECDSA key generation and signing is 1200 ms each, it is much less than RSA and acceptable to mobile user. Although the signature verification of ECDSA algorithm takes more time than RSA signature verification, this could be still acceptable to mobile user.

Fig. 6 shows an instance of Wireless X.509 in the proposed model. Wireless X.509 certificate does not have

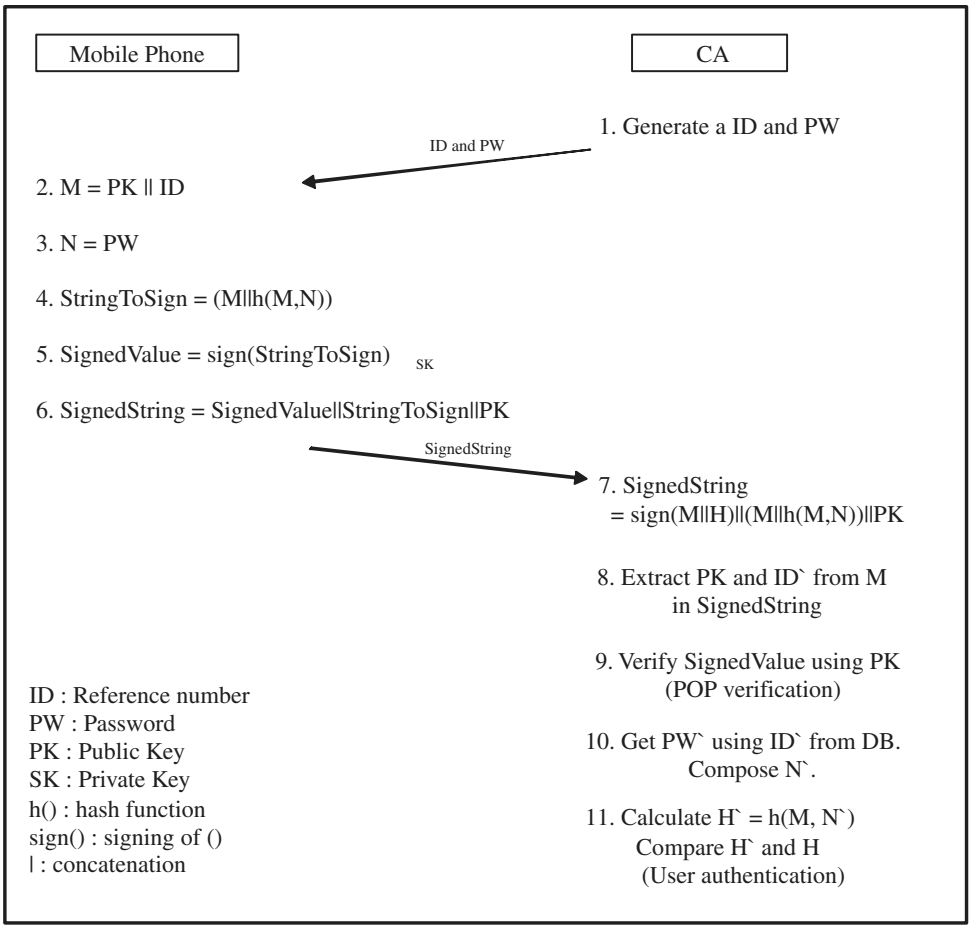

Fig. 3. Wireless Certificate Management Protocol.

Table 3
WCMP message format for certificate life cycle

Classification	Message format	StringToSign
Issue	$M = type\|PK\|ID,\ N = PW$	$M\|H(M,N)$
Rekey	$M = type\|PK_{new}\|ID_{new},\ N = PW_{new}$	$M\|H(M,N)$
Renewal	$M = type\|CN,\ N = nonce$	$M\|N$
Suspension	$M = type\|CertificateHold,\ N = nonce$	$M\|N$
Revocation	$M = type\|Reasoncode$	M

type : Initial Issue / Key pair update /Certificate update / Suspension / Revocation nonce : one time information.

any extensions defined optionally or not recommended in Table 1. Fig. 7 shows a view of the Wireless X.509 certificate that is issued through wireless CMP in mobile phone, with ECDSA public key.

In Table 6, compared to the wired certificate with RSA public key, the wireless certificate has smaller size, as 163 bit ECDSA public key in the certificate has shorter size than RSA key and several extensions are omitted. Since the short-lived certificate does not have extensions, the size of this certificate, 181 bytes is much less than X.509 certificate.

In certificate validation scheme, we designed that the server sends all information that are necessary for certificate validation to the mobile phone, the mobile phone does not need to acquire CAs certificate and ARL from directory. This reduces the number of communication between mobile phone and the wired system through wireless bandwidth. In the proposed WPKI model, the mobile phone has only three stages for certificate validation through OCSP, i.e. certificates reception from server, OCSP request and response.

Certificate validation cost of the proposed scheme is not increased, compared to the validation cost of the wired PKI. The validation cost of the wireless PKI is same as the cost of the wired PKI in the worst case as follows. In wireless PKI, certificate validation procedure is same as the wired PKI. Because communication link to user terminal for certificate validation is connected through wireless link, wireless bandwidth is required in Wireless PKI. To save the cost due to expensive wireless bandwidth, we need to optimize the certificate validation procedure in wireless link. Instead of the procedure that user terminal directly requests and download CA certificate and ARL from directory, after server requests and gets them from the directory, the server sends them to the user terminal in the proposed scheme. Therefore the CA certificate and ARL of the directory are transferred to the user terminal through the server.

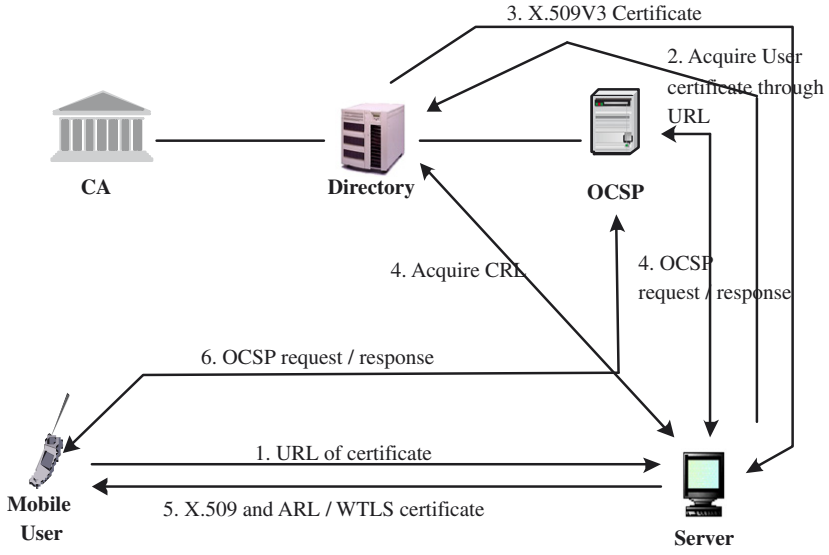

Fig. 4. Certificate validation scheme In WPKI.

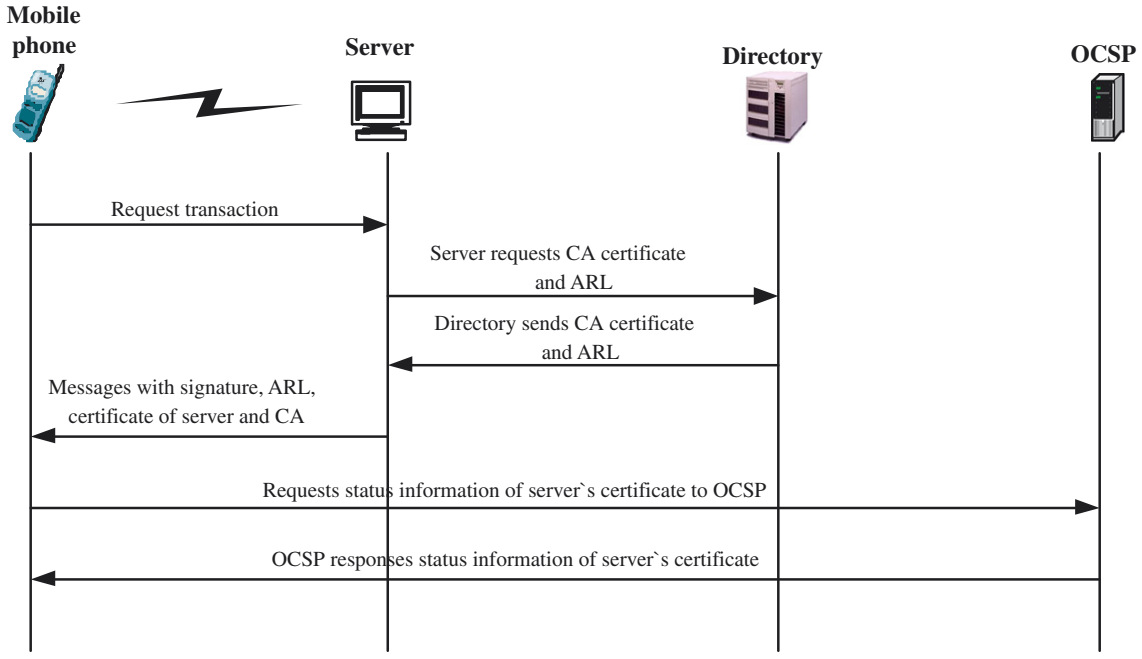

Fig. 5. OCSP procedure in mobile phone.

Table 4
WPKI test environment

Items	PC	Mobile phone
CPU	Pentium IV 700 MHz	ARM7TDMI 13.5 MHz
Memory	256 Mbyte	2Mbyte
OS	Win2000	REX

The overall certificate validation procedure is maintained as the same quality as the wired PKI and some procedures that are performed by user terminal through wireless link is reduced. Finally we can get that the cost due to wireless bandwidth utilization is reduced.

Table 5
Comparison of RSA and ECDSA processing time in mobile phone

Functions	Test Environment	
	PC	Mobile phone
ECDSA		
Key generation	3 ms	1200 ms
Digital signature generation	3 ms	1200 ms
Digital signature verification	3.6 ms	2500 ms
RSA		
Key generation	1500 ms	Cannot measure
Digital signature generation	36 ms	7000 ms
Digital signature verification	3 ms	800 ms

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 316214 (0x4d336)
    Signature Algorithm: ecdsa-with-SHA1
    Issuer: C=kr, O=kisa, OU=CA, CN=CertSIGNECDSA1
    Validity
      Not Before: Nov 11 15:00:00 2004 GMT
      Not After : Nov 11 14:59:59 2005 GMT
    Subject: C=kr, O=kisa, OU=CA, CN=test()000021420031112000653
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      04 04 df e4 6d 84 16 70 1a f3 f4 8e 80 ec ac ac f2 a3 26 b7 e0 60
        03 0e 7d 6c ba b9 3e ac 9b eb 85 13 ed 6a b9 75 5c f5 c2 02 b1
    X509v3 extensions:
      Authority Information Access:
        OCSP - URI:http://203.233.91.197:4612/
      X509v3 Authority Key Identifier:
        keyid:48:F6:C1:AA:D9:36:AD:54:01:31:E3:3D:7C:AD:EA:58:E8:5C:7A:50
      X509v3 Subject Key Identifier:
        BB:BA:B7:E1:11:1D:82:C0:81:79:A5:4E:6B:CD:7A:44:4A:F5:7F:DD
      X509v3 Key Usage: critical
        Digital Signature, Non Repudiation
      X509v3 Certificate Policies:
        Policy: 1.2.410.200005.1.2.1.1
          CPS: http://yessign.or.kr
          User Notice:
            Explicit Text: user notice
      X509v3 Subject Alternative Name:
        othername:<unsupported>
      X509v3 CRL Distribution Points:
        URI:ldap://203.233.91.197:6020cn=cdp1p1ctc214ecc1,ou=crldp,ou=CA,o=kisa,c=kr
  Signature Algorithm: ecdsa-with-SHA1
    30:2e:02:15:01:3a:07:0f:dc:e4:68:bc:c9:c1:1c:48:68:6b:
    1f:99:65:0c:b5:13:55:02:15:03:65:ac:e4:82:c2:30:42:de:
    ce:f2:49:c5:91:30:c1:90:f3:59:72:5e
```

Fig. 6. Example of wirelss X.509 certificate and short-lived certificate.

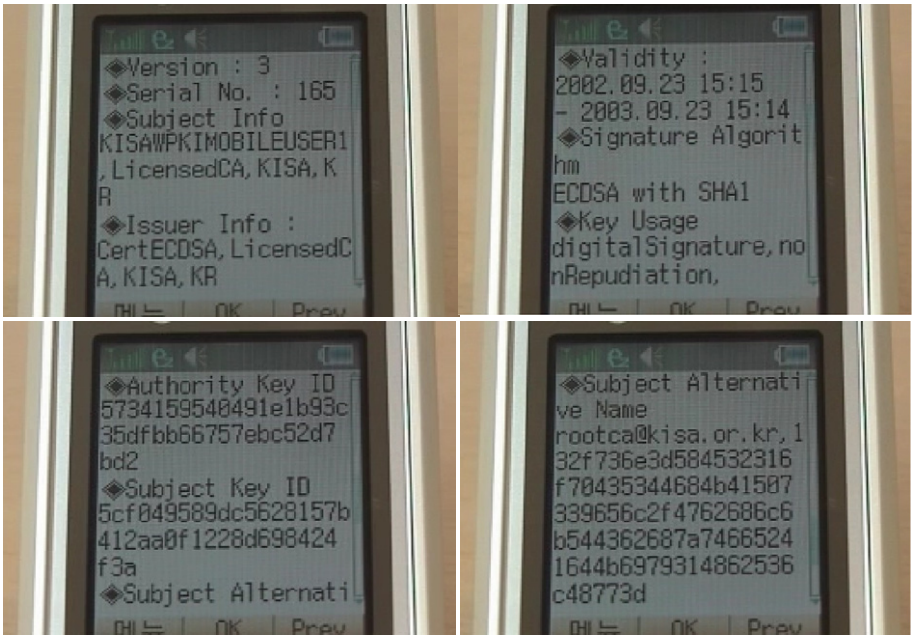

Fig. 7. View of wireless X.509 certificate in mobile phone.

Table 6
Comparison of certificate and module size

Items	Wired PKI	Wireless PKI
Certificate size		
X.509	949 byte	819 byte
Short-lived	–	181 byte
Number of communication for certificate validation	7	3
CMP module size	92 kbyte	14 kbyte
Certificate request message size	368 byte	200 byte
Total module size	1.6 Mbyte	200 kbyte

When user terminal receives CA certificate and ARL, verification method of CA certificate and ARL is performed by verification of signature that is attached to each CA certificate and ARL. The digital signature is generated by only CA. Server just forwards CA certificate and ARL to user terminal.

In OCSP scheme, user terminal delegates CRL verification procedure about server certificate to OCSP. If this is not delegated, user terminal downloads CRL from directory and performs verification procedure. Using OCSP scheme, user terminal sends server certificate to OCSP and requests verification of the certificate. OCSP downloads CRL from directory, verifies it and sends certification result to the user terminal. Thus the cost due to CRL download directly from directory in user terminal is reduced. Because OCSP request/response procedure are required, the number of the total communication is not decreased but the big size of CRL is not transferred through wireless link, the wireless bandwidth is saved. Finally, we have the additional cost that is due to two communications through wired link that is generated by the communication between server and directory instead of direct communication between user terminal and directory.

We compared to wireless CMP to RFC2511 and RFC2510 as the certificate management protocol for wired PKI and could get that module size of the WCMP is smaller than wired CMP, nevertheless having same functions. Also the wireless certificate request message size, *200 byte* is less than message by RFC2511. Total wireless PKI module size is much less than size by [6], and it is feasible to run in mobile phone.

Finally, Fig. 8 shows the signature value for payment information using ESDSA private key that is generated and stored in mobile phone. From this figure, purpose of the signature is non-repudiation of payment. Using digital signature and verification, we can securely utilize M-commerce such as mobile shopping and stocking, through mobile phone and wireless internet.

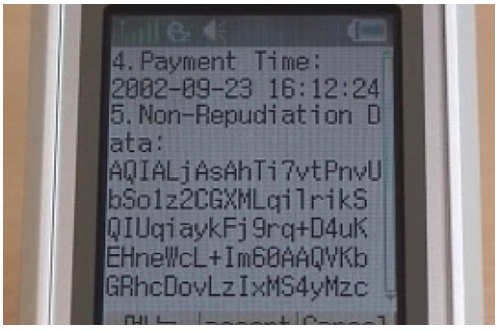

Fig. 8. Digital signature value using ESDSA private key in mobile phone.

7. Conclusion

In this paper, we proposed wireless PKI technology that provides similar security level as wired PKI supporting mobile phone. The proposed wireless PKI model aimed at secure M-commerce based on mobile phone through wireless communication. On the mobile phone with low performance, we selected ECDSA algorithm to reduce the computational complexity of public key algorithm. To reduce the complexity of certificate validation, we defined the optimal certificate profile for X.509 and short-lived certificate, which reduced the size of the certificate, and applied OCSP model to efficiently validate X.509 certificate in mobile phone. As applying short-lived certificate, the mobile phone can verify the validity of certificate without certificate path validation.

The proposed model can be utilized not only M-commerce but also diverse wireless data communication such as mobile hospital and government, based on mobile phone through wireless internet.

References

[1] K.Y. Lam, S.L. Chung, M. Gu, J.G. Sun, Performance of PKI-based security mechanisms in mobile ad hoc networks, Computer Communications 26 (2003) 2052–2060.
[2] Jaeil Lee, Yong Lee, JooSeok Song, Wireless PKI Technology in Korea, in: The First International Workshop for Asian PKI, vol. 1. Korea, 2001, pp. 145–158.
[3] OMA, Wireless Application Protocol – Wireless Public Key Infrastructure, WAP-217-WPKI, April 2001.
[4] Christian Schwingenschlogl, Stephan Eichler, Bernd Muller-Rathgeber, Performance of PKI-based security mechanisms in mobile ad hoc networks, International Journal of Electronics and Communications 60 (2006) 20–24.
[5] D. Critchlow, N. Zhang, Security enhanced accountable anonymous PKI certificates for mobile e-commerce, Computer Networks 45 (2004) 483–503.
[6] R. Housley, W. Polk, W. Ford, D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile: IETF RFC3280, IETF Network Working Group, April 2002.
[7] ITU-T Recommendation X.509(1997) — ISO/IEC 9594-8:1998, Information technology – Open Systems Interconnection – The Directory: Authentication Frame work.
[8] OMA, Wireless Application Protocol WAP2.0 Technical White Paper, April 2001.
[9] OMA, Wireless Application Protocol Architecture Specification, WAP-210-WAPArch, July 2001.
[10] OMA, Wireless Transport Layer Security, WAP-261-WTLS, April 2001.
[11] Ulrich Sax, Isaac Kohane, Jenneth D. Mandl, Wireless technology infrastructures for authentication of patients: PKI that rings, Journal of the American Medical Informatics Association 12 (3) (2005) 263–268.
[12] Alexandros Kaliontzoglou, Panagiotis Sklavos, Thanos Karantjias, Despina Polemi, A secure e-government platform architecture for small to medium sized public organizations, Electronic Commerce Research and Applications 4 (2005) 174–186.

[13] Theodosios Tsiakis, George Sthephanides, The concepts of security and trust in electronic payments, Computer and Security 24 (2005) 10–15.
[14] A. Frier, P. Karlton, P. Kocher, The SSL 3.0 Protocol, Netscape Communications Corp., November 1996.
[15] OMA, WAP Certificate and CRL, WAP-211-X.509, March 2000.
[16] M. Aydos, T. Yanik, C.K. Koc, High-speed implementation of an ECC-cased wireless authentication protocol on an ARM microprocessor, IEEE Proceedings – Communications 148 (5) (2001) 273–279.
[17] A.K. Lenstra, E.R. Verheul, Selecting cryptographic key sizes, PKC 2000, Journal of Cryptology 14 (2000) 255–293.
[18] M. Myers, C. Adams, D. Solo, D. Kemp, Internet X.509 Certificate Request Message Format: IETF RFC2511, IETF Network Working Group, March 1999.
[19] RSA Laboratories, PKCS#10: Certification Request Syntax Standard, 2000.
[20] C. Admas, S. Farrell, T. Kause, T. Mononen, Internet X.509 Certificate Management Protocols: draft-ietf-pkix-rfc2510bis-09.txt, IETF Network working Group, February 2004.
[21] T. Perlines Hormann, K. Wrona, S. Holtmanns, Evaluation of certificate validation mechanisms, Computer Communications 29 (2006) 291–305.
[22] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP): IETF RFC2560, IETF Network Working Group, June 1999.
[23] B. Schneier, Applied Cryptocgraphy, second ed., Wiley, New York, 1996.

Yong Lee received a B.S. in Food Engineering from Yonsei University, Korea, in 1988 and in Computer Science from Duksung Women's University, in 1992, an M.S and a Ph.D. in Computer Science from Yonsei University, Seoul, Korea, in 2001. She is currently a visiting scientist in the School of Electrical and Computer Engineering at Cornell University, NY, in USA. From 2001 to 2003, she worked in Korea Information Security Agency as a senior researcher, where she developed wireless public key infrastructure. Her research interests include Mobile Security, Mobile Ad Hoc Network, Mobile Network, Wireless PKI. Yong Lee is with the School of ECE, Cornell University, Ithaca, NY 14850, USA (e-mail: ylee000hanafos.com).

Jae-Il Lee received his B.S. and M.S. degrees in Computer Science and Statistics from Seoul National University, Seoul, Korea, in 1986 and 1988, respectively. He is pursuing his Ph.D. degree in Computer science at Yonsei University, Seoul, Korea. He was a Software Engineer at IBM Korea, Inc., from 1991 to 1996. He is currently a Vice President of the Korea Information Security Agency, Seoul, Korea. His research interests include information security, PKI, mobile internet security. Jae-Il Lee is with Korea Information Security Agency, Seoul, 138–803, Korea (e-mail: jilee@kisa.or.kr).

JooSeok Song received the B.S degree in electrical engineering form Seoul National University, Seoul, Korea, in 1976, and the M.S. degree in electrical engineering from KAIST, Korea, in 1979. In 1988, he received the Ph.D. degree in computer science from University of California at Berkeley. He had been an Assistant Professor of Naval Postgraduate School from 1988 to 1989. He is currently a Professor of Computer Science at Yonsei University, Seoul. Korea. His research interests include cryptography, information security, wireless communication, and mobile security. JooSoek Song is with Dept. of Computer Science, Yonsei University, Seoul, 120–749, Korea (e-mail: jssong@emerald.yonsei.ac.kr).