논문 2008-45TC-10-11

휴대폰에서의 무선 인증서 관리 프로토콜

(Wireless Certificate Management Protocol for Mobile Phone Security)

이 용*, 이 구 연**

(Yong Lee and Goo Yeon Lee)

요 약

휴대폰에서의 제한된 메모리 용량 및 CPU 성능으로 인하여, 유선망에서의 전자상거래 보안에 사용되는 PKI를 그대로 휴대폰 보안에 사용하기는 적당치 않다. 그러므로 유선망과 비슷한 보안 기능을 제공하면서도 휴대폰에 적용할 수 있는 무선 PKI 기능을 개발할 필요가 있다. 이에 본 논문에서는 경량화되고 안전한 무선 인증서 관리 프로토콜을 제안한다. 제안한 프로토콜은 휴대폰의 제한된 통신 환경 및 성능을 고려하였다. 또한 우리는 제안된 프로토콜에 대하여 시험적으로 구현하였다. 시험 구현에서 무선 인증서 관리 프로토콜의 모듈 사이즈는 휴대폰에 탑재 할 수 있을 정도로 작게 구현되었으나, 보안 기능은 유선망의 인증서 관리 프로토콜의 경우에 비하여 비슷함을 알 수 있었다.

Abstract

PKI (Public Key Infrastructure) which is used for the security of E-commerce (Electronic-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 propose a lightweight and secure Wireless Certificate Management Protocol (WCMP) that is executable to the mobile phone that has a constrained communication environment and limitation of performance, and show the implementation results of the scheme based on the mobile phone. We minimize data sizes processed in mobile phone, and optimize protocols for the certificate management. This results in the reduced module sizes to be able to install in mobile phone and shows as the same level as the wired CMP.

Keywords: Wireless Certificate Management Protocol, Wireless Public Key Infrastructure, Digital Certificate, Mobile Phone, Wireless Internet

I. Introduction

As mobile user utilizes wireless internet through the mobile phone, a variety of internet services supporting the mobile phone have been also increasing. The wireless internet refers to accessing the internet through the wireless communication using the mobile phone. For mobile users to successfully utilize the data service and M-commerce (Mobile Commerce) through the wireless internet, security must be guaranteed. Similar to the wired internet, for the 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

* 정회원, 충주대학교 전자통신공학전공
(Dept. of Electron. and Comm., ChungJu National University)
** 정회원-교신저자, 강원대학교 컴퓨터학부
(Dept. of Computer Eng. Kangwon National University)
※ This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD) (KRF-2007-313-D00666).
접수일자: 2008년2월8일, 수정완료일: 2008년10월16일

internet environment[1~3].

Many security protocols on the internet and most security applications for M-commerce are based on the public key algorithm. PKI (Public Key Infrastructure) applies a public key algorithm to transmit the user's public key and the user's identity in a secure and reliable way. The public key certificate provides a method to bind a public key and its owner. And a public key certificate could be issued to a mobile phone user through the wireless internet in mobile phone. Using the certificate, the mobile phone user can authenticate itself and make a secure channel for transactions such as M-commerce.

In the wireless environment, we have two different elements from wired internet : mobile phone and wireless internet[2, 6~7]. Mobile phone has fundamental limitation of performance such as less memory and less powerful CPU. And wireless internet presents a more constrained communication environment such as less bandwidth and has different protocol compared to wired internet protocol. Therefore, it is difficult to apply the wired CMP(Certificate Management Protocol) technology than wired environment[3, 7~8].

Certificate management protocol is required to support on-line interactions between PKI user and management entities, and can be used to carry the user or client system registration information, or a request for revocation of a certificate. Wired certificate management protocol is not feasible for mobile phone due to its message size and unnecessary fields[3, 6, 8, 10, 14~16]. In this paper, we propose a lightweight and secure Wireless Certificate Management Protocol (WCMP) for the mobile phone and wireless internet, and show the implementation result. Section II introduces problems of mobile phone and wireless internet. Section III describes overview of certificate management protocol for life cycle of a certificate. In section IV, we consider the existing wired and wireless certificate management protocol. Section V describes the requirements for WCMP and the proposed wireless PKI technology. Section VI shows performance of wireless CMP through module size and processing speed implemented in mobile phone, and validates its security, and section VII concludes this paper.

II. Problems of Mobile Phone and Wireless Internet

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 the wired internet protocols to mobile phone has many problems such as the limitations in the screen size, computing power, and memory capacity. Wireless internet technologies have been developed to overcome these restrictions of the wireless environment.

A representative wireless internet access supporting a mobile phone is WAP (Wireless Application Protocol), which is not based in the wired internet protocol, HTTP (HyperText Transport Protocol)[6~7]. Although WAP 2.0 was announced as [7] following WAP 1.x, up to now, WAP 1.x has been applied to wireless internet.

In WAP 1.x, WTLS (Wireless Transport Layer Security), equivalent to SSL (Secure Socket Layer) of the wired internet, is in charge of security[3, 8~9].

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 the WAP gateway, and the 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, 8~9].

Even though this security problem, certificate management protocol in WAP is based on WTLS, and hence it could not support confidentially of certificate request information.

Ⅲ. Overview of Certificate Management Protocol

A certificate has a life cycle such as initial issue, renewal, revocation and suspension, and Certificate Management Protocol (CMP) manages this life cycle of the certificate from birth to death.

1. Initialization Request and Certificate Request Message Format

Basic trust of PKI starts from the certificate request, as mentioned before. The certificate request protocol is as follow.

① A person who wants to use digital signature requests a certificate for his public key to a CA (Certificate Authority).
② When the CA receives the request, CA checks the certificate request message from user.
③ CA identifies the user.
④ CA checks if the requester possesses a private key corresponding to the public key.
⑤ CA issues the certificate of the public key.

An initialization request message is intended to be used for entities when first initializing into the PKI. This message contains as the PKI body a Certificate Request Messages data structure, which specifies the requested certificate(s). Typically, Subject Public Key Information, Key Identifier, and Validity are the template fields which may be supplied for each certificate requested[15]. Also, proof of possession information is included. Checking for proof of possession (POP) of private key is to confirm and verify whether the public key for which a certificate is being requested corresponds to private key of user, and the procedure is as follow :

- User transmits the public key information and signature value for hash value of nonce which is signed by user's private key to CA.
- CA compares decoded value of the signature value by public key and hash value of nonce.
- If two hash values are same, CA confirms and verifies that there is a private key corresponding to public key transmitted by user and user possesses that key pair.

2. Key Pair Update and Certificate Update

In case that the private key has been lost, damaged, stolen or leaked, the owner fills out a key pair update request form and transmits it to CA (or through the registration authority). The owner must generate a request form including ID, Password, information for POP, and owner's public key. This form should guarantee to prevent replay attacks or message forgery/alteration, and ensuring confidentiality, and the owner should transmit the request form to CA (or through a registration authority).

Sometimes a user may want to update its certificate before an expiration date of the certificate. Certificate update may occur when the key is substituted.

3. Certificate Suspension and Revocation

When a certificate owner suspects that the private key has been lost, damaged, stolen or leaked, the owner could suspend the certificate until the owner checks the security of the certificate. If the owner realized that his private key has no problem after the owner requested the certificate suspension to CA, the certificate status can be changed by CA as valid. Therefore, the owner reuses the same public key pair and the certificate.

In case that the owner is convinced that the private key has been lost, damaged, stolen or leaked, the owner must request revocation of the certificate to CA.

Ⅳ. The Related Work

In this section, we introduce the certificate management protocols used in wired internet environment and WAP.

1. Problems of Wired Certificate Management Protocol

At first, one of the Public Key Cryptography

Standards (PKCS) about RSA public key implementation method developed by RSA Company, PKCS#10 defines the Certificate Request Syntax Standard[14].

In IETF, they have published RFC2510 (Internet X.509 Public Key Infrastructure Certificate Management Protocols) that is certificate management protocol and RFC2511 (Internet X.509 Certificate Request Message Format) that is certificate request message format. RFC2511 includes Certificate Request Message Format (CRMF) and treats the message format to request X.509 certificate in wired internet environment[5, 13].

A certificate request of PKCS#10 consists of three parts :

- Certification request information
  - The entity's distinguished name
  - A set of attributes providing other information about the entity
  - The entity's public key
- A signature algorithm identifier
- A digital signature on the certification request information

Moreover attribute type is defined in PKCS#9 (Selected Attribute Types) to provide the additional information for certificate and is composed as follows [24].

- Challenge-password attribute : it is used at certificate revocation request
- Email address : user e-mail address
- Extended-certificate-attributes : attributes which are defined in PKCS #6 (Extended-Certificate Syntax Standard)[25]

But, it is not feasible to use these additional fields in wireless internet environment with restrictions as mentioned before.

A certificate request message which is defined in RFC2511 is composed of three parts:

- Certificate request
  - Public key
  - End-entity's name
  - Other requested certificate field
- An optional proof of possession field
  - Proof of possession for the private key corresponding to the public key for which a certificate is being requested.
- An optional registration information field
  - Supplementary information related to the context of the certification request

RFC2511 also defines many optional fields to transfer additional information when a certificate revokes. Especially in the wireless PKI of WAP, because the WTLS certificate has validity during 48 hours, certificate revocation is not required and these fields are not necessary in wireless PKI[5].

As considered before, certificate management protocol used in wired PKI has some problems, and thus those are not feasible to wireless internet environment due to less wireless communication bandwidth, and processing of CMP for certificate life cycle such as certificate issue in the mobile phone must be considerable burden.

2. Wireless Certificate Request Protocol in WAP

In WAP, the wireless certificate request message for initialization request is defined in [3] based on wireless PKI environment, as follows.

$$\text{Request} = \text{Crypto.signText}(\text{nonce} + ":" + \text{Name} + ":" + \text{ID} + ":" + \text{Password}, 5, 0) \quad (1)$$

WAP defines wireless certificate request message to concatenate with nonce that is one-time information, certificate requester name, a unique identifier provided by the CA and a password to authenticate the user to the CA separated by a colon(:) and to sign on them, and then the message is securely transferred through WTLS (Wireless Transport Layer Security) using (1). But in this protocol, certificate request information with just signature is transferred to CA and the message is not encrypted. Because WTLS layer cannot provide end-to-end security[26], the protocol has problem not to guarantee security of transferred information. Thus, even though the WTLS layer is not applied, certificate request protocol must provide secure transfer functionality of certificate request information

for itself and POP functionality.

As previously mentioned, current wired CMP is based on SSL[13~15] and certificate request in WAP is based on WTLS. 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 nor 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.

V. The Proposed Wireless Certificate Management Protocol

1. Requirement of Certificate Request 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[13~14].

- Certificate request message is constructed at mobile phone. This value should include a public key, end-entity's reference number (like as ID) and authorization code (like as 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. The value is included in certificate request massage.
- Method by which the certificate request message is securely communicated to a CA.

Certificate request protocol should be configured to prevent replay attack, message counterfeiting and forging, and to guarantee confidentiality, and then request is securely delivered to a CA. Current wired CMP is based on SSL[14~16] and certificate request in WAP is based on WTLS. 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, WCMP that is based on neither SSL nor 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.

2. Symbols and Definitions

In this paper, we have the following symbols.

- h( ) : Hash function (ex. SHA1)
- PK : Public key of a user (Digital signatures verification key)
- SK : Private key of a user (Digital signature generation key)
- ID : Reference number of a user
- PW : Authorization code of a user
- $\mathrm{Sign}(\ )_{SK}$: Signature function of ( ) using SK
- $\mathrm{Verify}(\ )_{PK}$: Verification function of ( ) using PK
- || : Concatenation

3. Certificate Request Procedure

To get a certificate, a user must be identified at CA through out-of-band and the user makes the document which contains other information for certificate. Then the CA should give the user an ID and a Password for certificate request. The user generates a public key pair and makes the certificate request message.

Step 1 : Message M is composed of concatenation of the user's public key (PK) and reference number (ID).

$$M = PK \| ID \quad (2)$$

Step 2 : PW that is given by CA consists of N.

$$N = PW \quad (3)$$

Step 3 : Hash value, H is calculated by hash function from input of message M and N.

$$H = h(M, N). \quad (4)$$

Step 4 : M || H is signed by the private key corresponding to the public key for which a certificate is be requested to CA.

$$SignedValue = Sign(M \| H)_{SK} = Sign(M \| h(M,N))_{SK} \quad (5)$$

Step 5 : The user makes the certificate request message that is composed of the signed value from step 4, SignedString and delivers it to CA.

$$SignedString = SignedValue \| StringToSign \| PK \quad (6)$$

4. Certificate Request Message Verification Procedure

The CA verifies the certificate request message and responses as follows.

Step 1 : The CA gets M and H from SignedString transferred from the mobile user.
Step 2 : The CA obtains the public key (PK′) and reference number (ID′) of the user from message M.
Step 3 : The CA retrieves the authorization code (PW′) corresponding to the reference number (ID′) of Step 2 from its database and composes N′.
Step 4 : The CA calculates the hash value H′ of message M, of Step 1 and the authorization code (PW′) of Step 3.

$$H' = h(M, PW') \quad (7)$$

Step 5 : The CA compares the calculated value, H′ of Step 4 with the user's hash value, H of Step 1, identifies the user who sends the certificate request message (user authentication) and confirms the registered user information.

$$H ? = H'. \quad (8)$$

Step 6 : The CA verifies the SignedValue using the public key (PK′) of Step 2. POP is also verified through verifying the user's digital signature that is generated by the private key corresponding to the public key. If the verification succeeds, the CA issues a user's public key certificate. If the verification fails, "POP error" happens.

$$Verify(SignedValue)_{PK'} ? = StringTosign \quad (9)$$

Step 7 : The CA publishes the certificate on its directory or WEB and should give a user's certificate or certificate URL to user.

5. WCMP for Certificate Life Cycle

The management of certificates includes *Initial issue*, *Key pair update*, *Certificate update*, *Certificate suspension*, and *Certificate revocation*. Table 1 shows the message formats of wireless certificate management protocol for certificate life cycle. We can apply these formats to the wireless certificate request scheme.

표 1. 인증서에 대한 WCMC 메시지 형식
Table 1. WCMP message format for Certificate Life Cycle.

Type	Message Format	StringTo Sign
Initial issue	M = type | PK | ID, N = PW	M|H(M,N)
Key pair update	M = type | PK_{new} | ID_{new}, N = PW_{new}	M|H(M,N)
Certificate update	M = type | CN, N = one time information	M|N
Suspension	M = type | CertificateHold, N = one time information	M|N
Revocation	M = type | Reasoncode	M

VI. Results

1. Security Proof of the Proposed Protocol

First of all, CA should confirm whether the user who requests a certificate is already enrolled and authenticate the user through the ID and Password of the user. CA should also verify that the user who requests to certify his public key through the certificate request format actually possesses the private key corresponding to public key. The proposed protocol provides the method to verify POP as follows.

- Proof Of Possession : In (6), a user signs on concatenation with message M and h(M, N)

using the private key corresponding to a public key to construct a SignedValue. CA also verifies this SignedValue using the public key corresponding to the private key, in (9).

- User Authentication : The user makes the hash value, H in (4). The CA retrieves *Password* corresponding to ID from its database, and composes N. Then, the CA calculates H'= h(M, N'), where M is in the user's signed message, SignedValue. And the CA compares calculated value, H' with the user's hash value, H which is in the user's signed message to authenticate the user.
- Prevention of Replay Attack : We consider prevention of replay attack in the proposed protocol. This protocol uses public key value as one-time information to prevent the replay attack, not a separate nonce value. Every user has different value as a public key. If the same public key is applied to two users, CA which issues the public key certificate could realize it. Although an attacker does replay attack, CA could discover that a public key is used twice. Also, when an additional nonce value is used, the certificate request message becomes a little larger. But in this protocol, because public key information is used as one-time information, this problem can be solved.
- Confidentiality : In the certificate request message, password that is used to authenticate a user should guarantee confidentiality when it is transmitted to CA. In this protocol, password composes N and is concatenated with M. Then this protocol calculates hash value h(M, N) and signs on the message. Thus, the original password value is not transmitted to CA, only the hash value of password is transmitted to CA. The CA finds the password in its database through the reference number (ID), hashes it and compares the CA's calculating hash value with the certificate requester's hash value. Therefore, confidentiality of certificate request information could be guaranteed as the above.

2. Implementation and Analysis

Table 2 shows the WCMP test environment. We compared wireless CMP to RFC2511 and RFC2510 as the certificate management protocol for wired PKI and could get that module size of the WCMP is

표 2. 인증서 테스트 환경
Table 2. WCMP Test Environment.

Items	Wireless CMP (Mobile phone)	Wired CMP (PC)
CPU	ARM7TDMI 1 3.5MHz	Pentium IV 700MHz
Memory	2Mbyte	256Mbyte
OS	MUX	Win2000
CMP module size	14 Kbyte	92 Kbyte
Certificate request message size	200 byte	368 byte

type = 3 Byte (string) | req = Base64 encoded

100|BAEIKoZIzj0DAAErBAGvUnSVekH1bQj6/NK5axpbD7gKmAJ5ymwkuVjd
FOgkRD/yrMpsPmBAA==|46010|BAEIKoZIzj0DAAErBAeOR9g4L5oXa6+DHdFmSFHwnYsL7wVfcEYfgSHaimruTVMkNWpYypLbAA==|AQAAAAQmlmwHAICUoVKWJzgapOedP7NWVj6UZzBh7+E4jH9E9z1f6vJHJbzT8f1xsdys92LzCK3x4+3NQk1j19QyhycMRb4kmpHSnrXVsGPxQxciox/F4cz3cBvMoeQjDxw0AS103kO3OFnLBhLAW5EKWaUyoPjqOXoXnvXOK/EwAkeL4fHrswi9Q==|MC0CFQJKy/X4TAICg5K702/taT8QQgD2iAIUUns5DESQvNU2DVBx32l1o4Za21M=|20030117130109|AQAAAAQmlmwHAICUoVKWJzgapOedP7NWVj6UZzBhs7+E4jH9E9z1f6vJHJbzT8f1xsdys92LzCK3x4+3NQk1j19QyhycMRb4kmpHSnrXVsGPxQxciox/F4cz3cBvMoeQjDxw0AS103kO3OFnLBhLAW5EKWaUyoPjqOXoXnvXOK/EwAkeL4fHrswi9Q==|ImxHDtdvVebI4FJvGyYyp5DLVuE=

그림 1. 무선 인증서 요청 메시지의 예
Fig. 1. An example of wireless certificate request message.

그림 2. 휴대폰에서의 무선 인증서 요청 메시지 입력 화면
Fig. 2. View of Wireless Certificate Request Message input in mobile phone.

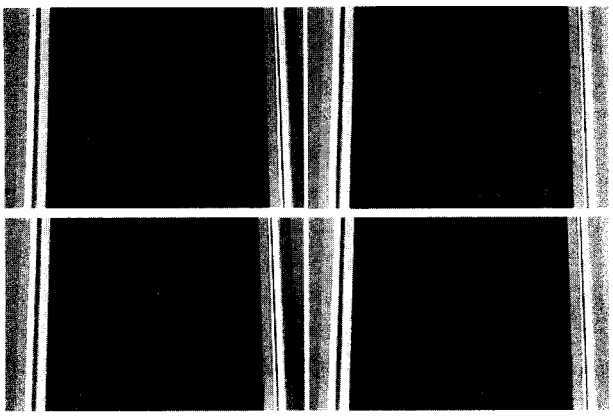


그림 3. 휴대폰에서 WCMP를 이용하여 발급된 무선 인증서

Fig. 3. Wireless certificate issued using WCMP in mobile phone.

smaller than wired CMP, nevertheless having same functions. Also the wireless certificate request message size, 200 byte is less than message by RFC2511. Fig. 1 shows an example of wireless certificate request message.

Fig. 2 shows the reference number and authentication code input procedure for WCMP and Fig. 3 shows the certificate sample that has been issued through WCMP in mobile phone.

Ⅶ. Conclusion

Even in wireless internet environment that has the characteristics such as constrained wireless bandwidth, less powerful CPU and less memory of mobile phone, security functionality is indispensable to provide secure transactions such as M-commerce. PKI aims at secure mobile commerce based on the mobile phone through wireless internet. To provide PKI service, a user should issue certificate of its public key from CA.

In this paper, we proposed the wireless certificate management protocol for mobile phone user to be securely issued public key certificate from CA. The proposed WCMP is simple and the minimum information is required for mobile phone to manage a certificate through the wireless internet for certificate life cycle. And it provides the same level of security as the wired CMP.

References

[1] Lam, K.Y., Chung, S.L., Gu,M. and Sun, J.G. : Lightweight security for mobile commerce transactions. Computer Communications, Elsevier, 26, 2052--2060 (2003).

[2] Lee, J.L., Lee, Y. and Song, J.S. : Wireless PKI Technology in Korea. In : The First International Workshop for Asian PKI, pp 145--158 (2001).

[3] Wireless Application Protocol - WirelessPublic Key Infrastructure, WAP-217-WPKI, OMA (2001).

[4] Housley, R., Polk, W., Ford, W. and Solo, D. : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile : IETF RFC3280, IETF Network Working Group (2002).

[5] ITU-T Recommendation X.509(1997) | ISO/IEC 9594-8:1998, Information technology - Open Systems Interconnection - The Directory: Authentication Frame work

[6] Wireless Application Protocol WAP2.0 Technical White Paper, OMA (2001).

[7] Wireless Application Protocol Architecture Specification, WAP-210-WAPArch, OMA (2001)

[8] Wireless Transport Layer Security, WAP-261-WTLS, OMA (2001).

[9] Frier, A., Karlton, P. and Kocher,P. : The SSL 3.0 Protocol. Netscape Communications Corp., (1996).

[10] WAP Certificate and CRL, WAP-211-X.509, OMA (2000).

[11] Aydos, M., Yanik, T. and Koc, C.K. : High-speed implementation of an ECC-cased wireless authentication protocol on an ARM microprocessor, IEEE Proceedings- Communications, Vol. 148, No. 5, pp.273 279 (2001).

[12.]Lenstra, A.K. and Verheul, E.R. : Selecting Cryptographic Key Sizes, PKC 2000, Journal of Cryptology, 14, 255--293 (2001).

[13] Myers, M., Adams, C., Solo, D. and Kemp, D. : Internet X.509 Certificate Request Message Format : IETF RFC2511, IETF Network Working Group (1999).

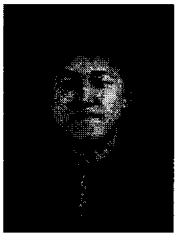
[14] PKCS#10 : Certification Request Syntax Standard, RSA Laboratories (2000).

[15] Admas, C., Farrell, S., Kause, T. and Mononen, T. : Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) : IETF RFC 2510, IETF Network working Group (2005).

[16] Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C. : X.509 Internet Public Key Infrastructure Online Certificate Status Protocol OCSP : IETF RFC2560, IETF Network Working Group (1999).
[17] Schneier, B. : Applied Cryptocgraphy, 2nd, Wiley, New York (1996).
[18] Chadwick, D. W., Mundy D. and New, J. : Experiences of using a PKI to access a hospital information system by high street opticians, Computer Communications, Elsevier, 26, 1893-1903 (2003).
[19] Morogan, M.C. and Muftic, S. : Certificate Management in Ad hoc Networks, IEEE Workshop on Security and Assurance in Ad hoc Networks, in conjunction with the 2003 International Symposium on Applications and the Internet, Orlando (2003).
[20] Dierks, T. and Allen, C. : The TLS Protocol Version 1.0 : IETF RFC2246, IETF Network Working Group (1999).
[21] WMLScript Crypto Library, WAP-161-WML ScriptCrypto, OMA (2001).
[22] Polk, W., Housley, R. and Bassham, L. : Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile : IETF RFC3279," IETF Network Working Group (2002).
[23] Digital Signature Standard (DSS) : FIPS 186-2, NIST (2000).
[24] Selected Attrubute Type Standard, RSA Laboratories PKCS#9 v1.2, (1993).
[25] Extended-Certificate Syntax Standard, RSA Laboratories PKCS#6 v2.0 (1999).
[26] WAP Transport Layer E2E Security Specification, WAP Forum Approved Version 11-July-2000, OMA (2000).

저 자 소 개

이 용(정회원)
1997년 연세대학교 컴퓨터과학과 (석사)
2001년 연세대학교 컴퓨터과학과 (박사)
1993년~1994년 디지콤정보통신 연구소
2001년~2003년 한국정보보호진흥원 선임연구원
2004년~2005년 코넬대학교 방문연구원
2005년~2007년 삼성전자 통신연구소 책임연구원
2007년~현재 충주대학교 전자통신공학전공 조교수
<주관심분야 : Mobile and Wireless Security, Ubiquitous Sensor Network, Wireless Mesh Network, Mobile Ad hoc network>



이 구 연(정회원)
1988년 KAIST 전기및전자공학과 (석사)
1993년 KAIST 전기및전자공학과 (박사)
1993년~1996년 디지콤정보통신 연구소
1996년 삼성전자
1997년~현재 강원대학교 컴퓨터학부 교수
<주관심분야 : 이동통신, 네트워크보안, 초고속통신망, ad-hoc 네트워크>