무선 PKI 기술 표준에 관한 연구

성 연 국*, 김 현 철**, 정 진 욱***, 김 순 철****, 류 원*****
(*,**,***) 성균관대학교 정보통신공학부
(****,*****) 한국전자통신연구원

요 약

무선 인터넷에 대한 수요가 날로 증가하고 있는 가운데 무선 인터넷이 보다 활성화되기 위해서는 반드시 해결해야 될 문제가 있는데, 보안 문제가 바로 그것이다. 특히 음성 위주의 이동통신에서는 도청만이 문제가 되었지만 증권이나 뱅킹같이 단순한 정보 서비스를 뛰어넘는 상거래 활동이 이루어지는 데이터 서비스에서는 사용자 인증, 데이터 무결성 보장 등 해결해야 할 문제가 많다. 이에 무선 인터넷 환경에서 안전한 서비스를 제공하기 위해 유선 인터넷 환경에서와 같은 보안 서비스를 제공할 수 있는 무선 PKI(WPKI: Wireless Public Key Infrastructure)의 필요성이 대두되었다. 즉, 유선 인터넷 환경에서 제공되는 기밀성, 무결성, 부인봉쇄 등의 보안 서비스를 무선 인터넷 환경에서도 제공하기 위해서는, 먼저 무선 PKI가 구축되고 서비스가 활성화되어야 할 것이다. 본 논문에서는 안전한 무선 인터넷 서비스를 위한 다양한 무선 인터넷 기술들과 그에 사용되는 무선 PKI기술 그리고 이에 적용 가능한 무선 PKI 표준들에 대해 분석하였다. 본 논문의 수행 결과로는 안전한 무선 PKI 서비스의 활성화와 더불어 무선 인터넷 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등 무선 인터넷을 이용한 전자 상거래의 활성화에 기여할 것으로 기대된다.

A Study on Wireless PKI Technolngy Standard

Sung Yun Kook*, Kim Hyun Cheol**, Chung Jin Wook***, Kim Soon Choul****, Ryu Won*****

ABSTRACT

Everyday demand of wireless internet is increasing. Security problem is certainly resolved for wireless internet activation. Especially problem is only wiretap in mobile communication with voice, but problems, user authentication, data integrity guarantee etc., are resolved in data-services that have commercial transaction over simple data information service such bill, banking. Necessity of wireless PKI that can offer security service likely in wired environment is requested for offering security service in wireless environment. For offering security services, confidentiality, integrity, non-repudiation, etc, that offered in wired environment in wireless environment, first it must construct wireless PKI infrastructure and do service activity. This paper analyze various wireless internet technology for offering safe wireless internet service and wireless PKI standards. Performance Result of this paper expect activity of safe wireless PKI service and activity of electronic commercial transaction used wireless internet such banking service, bill transaction, online shopping.

1. 서 론

최근 들어 이동통신 서비스의 발전과 함께 휴대폰이나 노트북, PDA(Personal Digital Assistant)를 이용하는 무선 인터넷 사용자가 증가함에 따라, 무선 인터넷을 이용한 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등의 전자 상거래가 급속히 발전하고 있다. 이와 같이 IT 산업을 기반으로 한 신경제의 흐름은 인터넷과 이동통신이라는 거대한 두 축으로 대변될 수 있다. 급속히 성장을 거듭하고 있는 인터넷은 이미 사회, 경제, 정치적인 측면에서 인류의 삶에 깊숙이 스며들어 새로운 패러다임의 변화를 촉진하며 우리 주변의 모든 것을 바꾸어 놓고 있다.

한편 이동통신은 전 국민의 절반 이상이 단말기를 소지할 정도로 급격하게 확산되었다. 무선 인터넷은 이러한 두개의 거대한 축의 통합 과정을 통해 탄생하였다. 무선 인터넷은 인터넷이라는 네트워크의 탈 중심적, 개방적, 양방향성 등의 특성과 이동통신의 이동성, 양방향성, 개인화(Personalization)의 특성을 그대로 물려받고 있다. 즉 무선 인터넷은 사용자가 이동중 무선 네트워크(Wireless Network)를 통해 인터넷 서비스를 제공받을 수 있는 환경과 기술을 말한다. 무선 인터넷을 이용하면 이동전화나 PDA 등의 이동통신 단말기로 언제 어디서나 인터넷에 접속할 수 있으므로 다양한 정보 검색과 전자상거래 등을 이동통신 단말기를 이용해서 수행함으로써 기존의 인터넷 환경의 시간, 공간적인 제약을 극복할 수 있게 된다.

이처럼 무선 데이터 서비스, 즉 무선 인터넷에 대한 수요가 날로 증가하고 있는 가운데 무선 인터넷이 보다 활성화되기 위해서는 반드시 해결해야 될 문제가 있는데, 보안 문제가 바로 그것이다. 특히 음성 위주의 이동통신에서는 도청만이 문제가 되었지만 증권이나 뱅킹같이 단순한 정보 서비스를 뛰어넘는 상거래 활동이 이루어지는 데이터 서비스에서는 사용자 인증, 데이터 무결성 보장 등 해결해야 할 문제가 많다. 또한 이동통신에서의 보안은 무선 네트워크 환경을 충분히 고려하여 이루어져야 하며 단순히 무선 네트워크에서만 그치는 것이 아니라 유선 인터넷과의 효과적인 연동을 반드시 고려해야한다.

이에 무선 인터넷 환경에서 안전한 서비스를 제공하기 위해 유선 인터넷 환경에서와 같은 보안 서비스를 제공할 수 있는 무선 PKI(WPKI: Wireless Public Key Infrastructure)의 필요성이 대두되었다. 즉, 유선 인터넷 환경에서 제공되는 기밀성, 무결성, 부인봉쇄 등의 보안 서비스를 무선 인터넷 환경에서도 제공하기 위해서는, 먼저 무선 PKI가 구축되고 서비스가 활성화되어야 할 것이다. 현재, 국내·외에서는 무선 인터넷 환경에서 보안 서비스를 제공하기 위한 무선 PKI 제품에 대한 연구·개발이 활발히 진행 중에 있으며, 국내에서도 2002년 하반기부터는 실제로 무선 PKI 서비스가 시작될 것으로 예상된다.

본 논문에서는 무선 인터넷 기술과 그에 사용되는 무선 PKI 기술 그리고 이에 적용 가능한 무선 PKI 표준들에 대해 알아본다 .

2. 무선 인터넷 기술

2.1 WAP의 구조 및 특성

WAP 방식은 전 세계적으로 사용자 면에서 가장 많은 수를 차지하고 있으며, 공개된 표준이라는 점에서 많은 연구가 이루어지고 있으나 기존의 HTTP를 지원하는 ME 방식과는 달리 기존의 HTTP를 지원하지 않으며, 별도의 WAP 게이트웨이(Gage Way)를 필요로 하기 때문에 ME 방식에 비하여 비용이 많이 든다는 단점이 있다. 반면에, 기술적으로는 HTTP와 별

도의 WAP 프로토콜이 기존의 기술과의 호환성을 제공하고, 어플리케이션의 개발이 가능하기 때문에 다른 방식에 비하여 많은 유연성을 가지고 있고 기존의 서비스와 차별화 된 서비스를 개발하기에 유리하다는 장점을 가지고 있다. 즉, WAP에서는 표준으로 정의되지 않는 형식의 파일에 기반한 서비스나 제공되지 않는 서비스일지라도 단말기나 무선망의 성능이 보장되는 한 제공되는 프로토콜을 이용하여 구현이 가능하다. [그림 2-1]은 WAP 방식의 구조도이다.

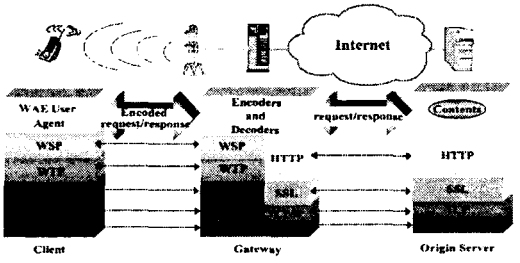

그림 2-1 WAP의 구조도

2.2 ME의 구조 및 특성

ME에서는 WAP 게이트웨이가 수행하는 작업을 무선 단말기 내의 브라우저가 수행하며, 내부적으로는 일반 인터넷 표준인 HTTP 방식과 호환 되며, HTML을 축약한 M-HTML을 사용하고 있다. ME에서의 보안 메커니즘은 HTTP에 기반하고 있으므로 유선 인터넷에서 사용되고 있는 SSL(Secure Sockets Layer) 정보보호 메커니즘의 수용이 가능하다. 또한, ME는 운영체제의 종류에 상관없이 사용 가능한 브라우저를 제공하며, 게이트웨이를 이용하지 않는다는 특징을 가진다. ME는 컨텐츠 기술 언어로 M-HTML을 사용하고 있기 때문에 이동 통신 사업자에게는 투자비를 절감할 수 있도록 해주고, 기존의 HTML 컨텐츠를 그대로 이용할 수 있다는 점에서 컨텐츠 제공자에게 편의를 제공한다는 장점이 있다. 반면에 브라우저의 오버헤드가 크며, 공개되지 않는다는 점에서 브라우저에서 지원하지 않는 파일을 이용한 서비스를 제공하지 못하는 단점을 갖는다. [그림 2-2]는 ME 방식의 구조도이다.

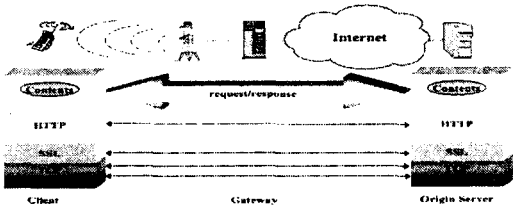

그림 2-2 ME의 구조도

3. 무선 PKI 기술

유선 인터넷 환경과 마찬가지로 무선 인터넷이 안전한 서비스를 제공하기 위해서는 기밀성, 무결성, 인증, 부인봉쇄와 같은 보안 서비스를 제공하기 위한 무선 PKI가 필요하다. 무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소한 변화시킨 것이다. 즉, WAP 게이트웨이를 통한 무선 PKI 서비스에서는 기존의 유선 환경에서 사용하는 X.509 인증서에 비해 부피가 작고 간단한 구조로 구성되어 있는 WTLS(Wireless Transport Layer Security) 인증서를 사용한다. 이는 무선 환경에서 사용하는 소용량 단말기에서 암호화 및 인증 업무를 효율적으로 수행할 수 있도록 구성되었다.

무선 PKI는 인증기관, 등록기관, 디렉토리, 사용자로 구성된다. 각 구성요소의 역할을 살펴보면, 먼저 인증기관은 공개키 기반구조를 구성하는 가장 핵심 객체로 사용자의 공개키 인증서의 발급·효력정지 및 폐지와 등록기관의 요청

에 따라 인증서를 발급하는 기능을 수행한다. 또한, 인증서와 인증서 소유자의 정보의 관리, 인증서와 그 소유자의 정보를 관리하는 데이터베이스의 관리, 인증서 효력정지 및 폐지목록, 감사 파일을 보관 등의 업무를 수행하는 핵심 기관이다.

등록기관은 인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자 사이에 설치하여 인증기관을 대신하여 사용자들의 인증서 신청 시 그들의 신분과 소속의 확인, 인증기관에 인증서 요청서 전송, 디렉토리로부터 인증서와 인증서 효력정지 및 폐지 목록 검색, 인증서 효력정지 및 폐지 요청 등의 기능을 수행한다.

디렉토리란 인증서와 사용자 관련 정보, 상호인증서 쌍 및 인증서 폐지목록의 저장 및 검색 장소로, 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol) 또는 LDAP(Lightweight DAP v2, v3)를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간 동안 디렉토리에 저장된다.

마지막으로 무선 PKI에서의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 말하며, 자신의 비밀키/공개키 쌍을 생성하고 검증, 공개키 인증서의 요청/획득, 전자 서명의 생성 및 검증, 특정 사용자의 인증서 획득 및 검증, 자신의 인증서 취소 등의 기능을 수행한다.

위에서 설명한 무선 PKI를 구성하는 4개의 중추적인 구성 요소 외에 무선 인터넷 사용자를 대신하여 인증서 상태 정보와 함께 인증 경로에 대한 검증 정보들을 제공하는 OCSP(Online Certificate Status Protocol)나, 무선 단말기의 계산 능력 저하로 인한 단점을 보완하기 위하여 사용되는 보안 모듈 등이 무선 인터넷상에서 PKI를 구성하기 위한 부수적인 구성 요소이다. 더불어, 무선 PKI는 무선 인터넷상에서 구성되어야 하므로, WAP 방식이나 ME 방식과 같은 무선 인터넷 기술 또한 중요한 구성 요소이다. 각 기술에 따라 PKI를 구성하는 인증서의 형식, 전송 포맷, 서명 알고리즘, 키분배 알고리즘 등이 각 방식에 적합하게 변형되어 사용 된다.

무선 PKI 모델에서 기본적으로 무선용 X.509 인증서를 사용하지만, 무선 CA 서버는 단말기의 검증 능력을 고려하여 WTLS 인증서를 사용하며, 무선 단말기의 저장공간의 문제를 해소하기 위해 인증서를 발급 받을 경우 인증서의 URL(Uniform Resource Locator)을 이용하기도 한다.

단말기에서 무선용 X.509 서버 인증서의 검증 메커니즘으로는 CRL(Certificate Revocation List)이나 OCSP를 사용하도록 한다. 또한 무선에서는 최신의 CRL만을 모아놓은 Delta CRL을 옵션으로 사용한다.

무선 단말기에서 RSA를 사용하여 키 생성이 용이하지 않을 경우를 고려하여 ECDSA를 사용하여 키를 생성할 수 있는 기능이 추가로 제공되며, 서명 알고리즘으로는 RSA, ECDSA가 사용되고 키분배용 알고리즘으로는 RSA, ECDH 등이 있다. [그림 3-1]은 기본적인 무선 PKI 모델에 대한 개략도이다.

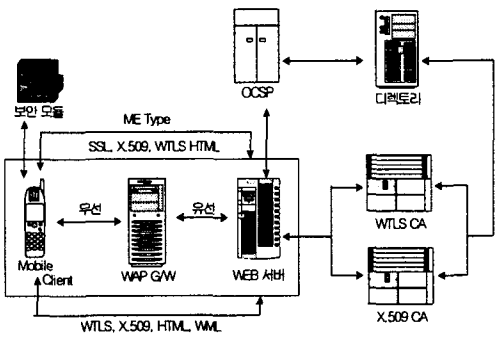

그림 3-1 무선 PKI 모델

4. 무선 PKI 기술 표준

무선 PKI 기술 표준은 무선 전자 서명 인증서 및 무선 WTLS 인증서 프로파일, 무선 전자 서명 인증서 효력정지 및 폐지목록 프로파일, 전자 서명 및 키분배 알고리즘, 무선 인증서 요청형식 프로토콜 표준 등으로 구성되어 있다. 기술 표준은 무선 인터넷 접속 기술로 사용되고 있는 WAP과 ME에 모두 적용 가능하고, 추후 유선 PKI와의 상호 연동성을 고려하여 개발되었다는 것이 특징이다. 무선 PKI 기술 표준 및 규격의 기술에 앞서 사용될 약어들에 대한 정의는 [표 4-1]과 같다.

<표 4-1> 무선 PKI 기술 표준 약어 정의

약 어	정 의
CA	Certification Authority , 인증기관
CRL	Certificate Revocation List , 인증서 효력정지 및 폐지목록
CMP	Certificate Management Protocol , 인증서 관리 프로토콜
DER	Distinguished Encoding Rules , 인코딩 규칙
HTTP	Hypertext Transfer Protocol , 인터넷 전송 프로토콜
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol, 접속 인증서 상태 프로토콜
POP	Proof of Possession , 소유 증명
PEM	Privacy Enhanced Mail, 인코딩 규칙
RA	Registration Authority , 등록기관

무선 PKI 각 표준들의 구성요소에 대해 자세히 살펴보면,

첫째, 무선 전자 서명 인증서 프로파일 표준은 WAP과 ME에 모두 적용 가능하고 이를 기반으로 무선 전자 서명 인증관리체계에서 사용되는 무선 전자 서명 X.509 v3 인증서에 대한 프로파일 표준을 정의하고 있으며, 인증기관 및 응용프로그램이 인증서를 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다. 주요 내용으로는 기본필드 및 확장필드 중 인증서 생성 시에 요구되는 필드의 내용과 사용자 소프트웨어 등에서 인증서 처리 시에 요구되는 확장필드에 대하여 정의하고 있으며 확장필드에 대한 "criticality"를 정의한다.[표 4-2]는 무선 전자 서명 인증서 프로파일을 나타낸 것이다.

<표 4-2> 무선 전자 서명 인증서 프로파일

기본 필드명	생성		처리	
	인증기관	가입자	인증기관	가입자
Version	m	m	m	m
Serial Number	m	m	m	m
signature	m	m	m	m
Issuer	m	m	m	m
Validity	m	m	m	m
Subject	m	m	m	m
Subject Public Key Info	m	m	m	m
Issuer Unique ID	x	x	x	x
Subject Unique ID	x	x	x	x
Extensions	m	m	m	m

확장 필드명	Critical		선택 여부			
			생성		처리	
	인증기관	가입자	인증기관	가입자	인증기관	가입자
Authority Key Identifier	n	n	m	m	o	o
Subject Key Identifier	n	n	m	m	o	o
Key Usage	c	c	m	m	m	m
Private Key Usage Period	n	n	x	x	x	x
Certificate Policies	b	b	m	m	m	m
Policy Mappings	n	-	o	-	m	-
Subject Alternative Names	n	n	m	m	m	m
Issuer Alternative Names	n	n	o	o	m	m

확장 필드명	Critical		선택 여부			
			생성		처리	
	인증기관	가입자	인증기관	가입자	인증기관	가입자
Subject Directory Attribute	n	n	x	x	x	x
Basic Constraints	c	c	m	x	m	x
Name Constraints	c	-	o	-	m	-
Policy Constraints	c	-	o	-	m	-
Extended Key Usage	b	b	o	o	m	m
CRL Distribution Points	n	n	m	m	o	o
Domain Information*	n	n	o	o	o	o
Authority Information Access	n	n	m	m	o	o
Procuration	-	n	-	o	-	o

c(critical) n(non-critica)l o(optional) x(not recommended)

-(not defined) m(mandatory) b(critical or non critical)

둘째, 무선 WTLS 인증서 프로파일 표준은 무선 전자 서명 인증관리체계에서 키분배용으로 사용되는 WTLS 인증서에 대한 프로파일을 정의하고 있으며, 인증기관 및 응용 프로그램이 인증서를 생성하고 처리하는데 필요한 요구 사항들을 명시한다. 무선 WTLS 인증서 프로파일은 WAP 포럼에서 제안한 WAP 인증서 및 인증서 폐지목록 프로파일, WAP-PKI, WAP-WTLS에 기반을 두고 무선 환경의 특성을 반영하여 작성되었다. 무선 키분배용 WTLS 인증서 프로파일은 [표 4-3]과 같다.

<표 4-3> 무선 WTLS 인증서 프로파일

항목	WTLS 인증서	
	서버용	인증기관용
certificate_version	V1	V1
signature_algorithm	ecdsa_sha, rsa_sha	ecdsa_sha, rsa_sha
issuer	<Text>	<Text>
valid_not_before	GMT	GMT
valid_not_after	GMT	GMT
subject	<Text>	<Text>
public_key_type	ecdh(3) rsa(2)	ecdsa(4)
parameter_specifier	option	option
publickey	ecdh 공개정보 rsa 공개정보	ecdh 공개정보
signature	ecdh 서명값, rsa 서명값	ecdh 서명값, rsa 서명값

기본 필드명	생성	처리
certificate_version	m	m
signature_algorithm	m	m
issuer	m	m
valid_not_before	m	m
valid_not_after	m	m
subject	m	m
public_key_type	m	m
parameter_specifier	m°	m°
publickey	m	m

m(mandatory) public_key_type이 타원곡선 알고리즘일 때만 사용

셋째, 무선 전자 서명 인증서 효력정지 및 폐지목록 프로파일 표준은 인증서 효력정지 및 폐지목록은 인증서의 효력정지 및 폐지 여부를 인증서 사용자에게 알리기 위한 수단으로 개발되었으며, ITU-T가 1993년 X.509 인증서 효력정지 및 폐지목록에 대한 첫 번째 표준을 제정한 이후로 1997년 두 번째 판이 개정되었다. 또한 IETF에서는 인증서 효력정지 및 폐지목록에 대한 프로파일을 1999년 RFC 2459로 정의하여 권고하고 있다. 이 표준은 전자 서명 인증관리체계에서 사용되는 무선 전자 서명용 인증서 상태확인을 위한 인증서 효력정지 및 폐지목록 프로파일에 대

한 표준을 정의하고 있으며, 인증기관과 응용 프로그램이 인증서 효력정지 및 폐지목록을 생성 및 처리하는데 필요한 요구사항들을 명시하고 있다. [표 4-4]는 무선 전자 서명 인증서 효력정지 및 폐지목록의 프로파일 규격을 나타낸다.

넷째, 무선 전자 서명 알고리즘 표준은 무선 전자 서명 인증관리체계에서 지원하는 전자 서명 알고리즘과 해쉬 알고리즘에 대하여 기술하며 관련 표준을 명시한다. 전자 서명 알고리즘은 인증기관이 인증서와 인증서 효력정지 및 폐지목록을 생성하는 경우와 전자문서에 사용자가 전자 서명을 하는 경우에 사용되며, RSA와 ECDSA를 정의하고 있다. RSA는 소인수 분해 문제의 어려움에 기반한 알고리즘으로 Rivest, Shamir 및 Adleman 등이 개발하였으며, RSA의 구현은 인증서버, CP, 단말기의 전자 서명 생성과 검증을 필수로 한다. ECDSA는 타원곡선(Elliptic Curve) 상에서 군(Group)을 정의하고, 이에 대한 이산대수 계산의 어려움에 근거를 두고 있다. 타원 곡선 상에서의 이산대수 문제는 일반적인 군에서 정의되는 이산대수 문제보다 훨씬 어려우며, 이에 따라 작은 키로도 RSA보다 높은 안전성을 유지할 수 있다. 해쉬 알고리즘은 기본적으로 메시지 인증에 사용되며 전자 서명 알고리즘과 함께 전자 서명 생성 및 검증에 사용된다. 본 표준에서는 SHA-1만을 규정하고 있다.

<표 4-4> 무선 전자 서명 인증서 효력정지 및 폐지목록 프로파일

기본 필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next UPdate	m	m
Revoke Certificate	m[1)]	m
User Certificate	m[1)]	m
Revocation Date	m[1)]	m
CRL Entry Extensions	m[1)]	m
CRL Extensions	m	m

인증서 효력정지 및 폐지목록 확장 필드명	Critical	선택 여부	
		생성	처리
Authority Key Identifier	n	m	m
Issuer Alternative Name	n	o	m
CRL Number	n	m	m
Issuing Distribution Point	c	o	m
Delta CRL Indicator	n	o	o

엔트리 확장필드명	Critical	선택 여부	
		생성	처리
Reason Code	n	m	m
Hold Instruction Code	n	o	o
Invalidity Date	n	o	o
Certificate Issuer	c	o	m

c(critical) n(non-critica)l o(optional) x(not recommended)

-(not defined) m(mandatory) b(critical or non critical)

효력정지 및 폐지된 인증서가 없을 경우에는 효력정지 및 폐지목록 필드가 인증서 효력정지 및 폐지목록에 나타나지 않음

다섯째, 무선 키분배 알고리즘 표준은 키분배 인증서 서명에 지원되는 알고리즘과 해쉬 알고리즘에 대하여 기술한다. 서명용 알고리즘은 인증기관이 키분배 인증서를 생성하는 경우에 사용되며, 전자 서명 인증관리체계에서 지원하는 키분배 인증서 서명용 알고리즘은 RSA와 ECDSA가 있다. 본 표준에서 지원하는 암호화 알고리즘은 SEED와 Triple DES가 있다. SEED는 128비트 암호키를 이용하여 메시지를 블록 단위로 암, 복호화하는 알고리즘으로 데이터의 기밀성 등과 같은 기능을 제공하기 위하여 사용된다. 해쉬 알고리즘은 기본적으로 메시지 인증에 사용되며 전자 서명 알고리즘과 함께 전자 서명 생성 및 검증에 사용된다. 본 표준에서는 SHA-1만을 규정하고 있다.

마지막으로 무선 인증서 요청형식 프로토콜 표준은 전자 서명 인증관리체계에서 사용될 전자 서명 및 키분배 인증 요청형식 프로토콜 표준을 정의하며, 인증기관 및 응용 프로그램이 요청형식을 생성하고 처리하는데 필요한 요구사항을 정의하고 있다. 무선 인증서 요청형식 프로토콜 표준은 가입자가 인증서를 요청할 때, WAP에서 정의한 signText 함수를 사용하여 인증서 요청형식을 생성한다. 가입자는 ID, Password, POP(Post Office Protocol)를 위한 방법, 가입자의 공개키를 이용하며 일회성 정보인 인증서 요청형식을 생성한다. 인증서 요청형식은 재전송 공격 및 메시지의 위·변조가 불가능하고 기밀성을 제공할 수 있는 형태로 구성한다. 인증서 요청형식은 전자 서명용 또는 키분배용 인증서 요청형식 구조와 전자 서명용 및 키분배용 인증서 요청형식 구조로 구분되어 있다.

5. 결 론

무선 인터넷 서비스와 무선 이동통신 단말기 기술의 급속한 발전으로 무선 인터넷을 이용하는 사용자가 점차적으로 증가하고 있다. 무선 인터넷 환경에서 안전한 서비스를 제공하기 위해서는 유선 인터넷 환경과 같은 사용자 정보의 보안 서비스가 요구된다. 그러므로, 유선 인터넷 환경에서와 같이 무선 인터넷 환경에서도 PKI에 기반한 암호 시스템의 응용이 필수적으로 요구된다.

본 논문에서는 먼저, 안전한 무선 인터넷 서비스를 위한 무선 인터넷 기술, 무선 PKI 기술의 개요 및 모델에 대해 알아보고, 무선 PKI 표준에 대해 분석하였다.

무선 PKI 연관돼 향후 진행될 연구로는, 무선 인터넷 환경에서의 사용자 보안 모듈에 대한 연구를 들 수 있다.

무선 인터넷 환경이 갖는 특수성과 사용하는 단말기의 여러 제약 사항으로 인해, 무선 환경에서는 유선 환경과는 달리 많은 문제점들이 존재한다. 즉, 현재 무선 인터넷 환경에서 사용하고 있는 휴대폰이나 PDA와 같은 단말기의 연산 능력으로는 전자 서명의 생성·검증이나 인증서 검증과 같이 많은 시간이 소요되는 공개키 암호 관련 연산을 수행하기 어렵다. 또한, 무선 단말기의 메모리 크기의 제한으로 인해 많은 수의 인증서를 저장하는 데에도 한계가 있으며, 단말기 분실시 인증서나 사용자의 비밀키와 같은 중요 정보를 분실할 우려도 있어 안전성 면에서도 문제점이 있다.

이러한 문제를 해결하기 위해 불법 변조 방지(tamper resistant) 특성을 갖으면서 암호 알고리즘, 사용자의 키, 인증서 및 관련 정보를 저장할 수 있는 별도의 보안 모듈의 필요성이 대두되었다.

보안 모듈이란 암호 시스템을 사용하는데 필요한 사용자의 비밀키 관련 정보나 개인 ID 등이 탑재되는 하드웨어 토큰으로, 단순히 메모리 기능만을 수행하는 것과 연산 능력이 있는 프로세서를 포함하는 것이 있다. 프로세서가 포함된 보안 모듈은 비교적 복잡한 암호 알고리즘뿐만 아니라 공개키 관련 연산과 같이 기존의 컴퓨터 플랫폼에서 수행되던 모든 암호 관련 연산을 수행하기도 한다. 보안 모듈은 무선 단말기, 노트북 및 데스크 탑 PC, 네트워크 서버 등에 설치가 가능하고 보안 시스템의 관리를 매우 효율적으로 수행할 수 있다는 장점이 있다.

아직까지는 이러한 보안 모듈이 유선 PKI 기반의 제품에서만 활용되고 있지만, 앞으로 무선 인터넷의 활성화와 함께 무선 PKI 상에서도 보안 모듈이 널리 활용될 것으로 예상된다. 또한, 2002년 하반기부터는 국내에서도 무선 PKI 서비스가 제공될 예정이므로 적절한 보안 모듈의 활용을 통해 안전한 무선 인터넷 서비스의 활성

화에 기여할 수 있을 것이다.

본 논문의 수행 결과로는 안전한 무선 PKI 서비스의 활성화와 더불어 무선 인터넷 뱅킹 서비스, 주식 거래, 온라인 쇼핑 등 무선 인터넷을 이용한 전자 상거래의 활성화에 기여할 것으로 기대된다.

참고문헌

[1] "ME를 위한 공개키 기반구조 기술 기준 (Ver 1.5) - 전자서명", 한국정보보호진흥원, 2001.8

[2] "WAP을 위한 공개키 기반구조 기술 기준 (Ver 1.5) - 전자서명", 한국정보보호진흥원, 2001.8

[3] "무선 인증서 관리 프로토콜 규격", 한국정보보호진흥원, 2001.8

[4] "무선 인증서 요청형식 표준", ISTF-017 ,한국정보보호진흥원, 2002.4

[5] "무선 WTLS 인증서 프로파일 표준", ISTF-14 ,한국정보 보호진흥원, 2002.4

[6] "무선 PKI 보고서", 성균관대학교 정보통신 보호연구실, 2002.9

[7] "무선 전자 서명 인증서 프로파일 표준", ISTF-012, 한국정보보호진흥원, 2002.4

[8] "무선 전자 서명 인증서 효력정지 및 폐지 목록 프로파일 표준", ISTF-013 ,한국정보보호진흥원, 2002.4

[9] "무선 전자 서명 알고리즘 표준", ISTF-015 ,한국정보보호진흥원, 2002.4

[10] "무선 키 분배 알고리즘 표준", ISTF-016 , 한국정보보호진흥원, 2002.4

[11] "무선 전자 서명 인증서 OID 규격",한국정보보호진흥원, 2002.4

[12] "전자 서명 인증서 프로파일 표준", TTAS.KO-12.0012, 한국정보통 신기술협회, 2000.12

[13] "전자 서명 인증서 효력정지 및 폐지 목록 프로파일 표준", TTAS.KO-12.0013 , 한국정보통신기술협회,2001.6

[14] "전자서명 인증기술", 이석래, 2001.3

[15] "무선 PKI 정책 방향", 전성배

성 연 국

2001년 성균관대학교 전기전자 및 컴퓨터 공학부(공학사)

2001년~현재 성균관대학교 정보통신공학부 석사과정

김 현 철

1990년 성균관대학교 정보공학과(공학사)

1992년 성균관대학교 정보공학과(공학석사)

1992년~2002년 2월 한국전자통신연구원 선임연구원

2002년 2월~현재 (주) 아이트로닉스 소장

정 진 욱

1974년 성균관대학교 전기공학과(공학사)

1979년 성균관대학교 전자공학(공학석사)

1991년 서울대학교 전자계산학(공학박사)

2002년~현재 한국정보처리학회 회장

1985년~현재 성균관대학교 정보통신공학부 교수

김 순 철

1998년 성균관대학교 정보공학과(공학사)
2000년 성균관대학교 대학원 전기전자컴퓨터공학부(공학석사)
2000년 1월~7월 한국정보보호센터(KISA) 개발부 연구원
2000년 8월~현재 한국전자통신연구원 연구원 유무선인터넷정합팀

류 원

1983년 부산대학교 계산통계학과(이학사)
1988년 서울대학교 대학원 계산통계학과(이학석사)
2002년 성균관대학교 대학원 정보공학과(공학박사)
1989년~현재 한국전자통신연구원 책임연구원 유무선인터넷정합팀