국내 무선 PKI 기술규격 소개 및 구축 현황

(주)케이사인 장준교 · 구자동 · 홍기융*

1. 서 론

무선 인터넷의 대중화와 더불어 개인 데이터 보호 및 안전한 거래를 보장 받으려는 이동 통신 사용자들의 요구가 급속히 확산되고 있다. 이러한 요구에 이동 통신 사업자들은 서비스의 질을 차별화 하기 위한 일환으로 은행 거래 서비스 등 부분적인 서비스에 보안 모듈(종단간 보안 채널 확립)을 탑재하기 시작했으나, 궁극적인 무선 보안 서비스를 제공하기 위한 방안은 아니였다.

2000년 하반기에 무선 인터넷 환경에서의 통합 보안 솔루션 구축의 일환으로 무선 pki 개발 업체를 선정하기 시작했으며, 때를 같이하여 정부에서도 한국정보보호진흥원을 주체로 한국전자통신연구원(ETRI), 공인인증기관, 이동 통신 사업자, PKI관련 업체들을 주축으로 하는 무선 pki 실무 작업반을 구성 운영하게 되었다.

무선 pki 실무 작업반에서는 PKI관련 업체들과 연구기관, 이동 통신 3사가 각자 추진해오던 무선 pki 기술들과 현재의 무선 인터넷 기술과 단말기 제조 기술을 최대한 수용하려 노력하였고 정부의 전자서명법 그리고 정책과 기술의 상충되는 부분들을 조율하기 위해 각계 전문가들과의 의견을 수렴하여 현재와 미래에 부합되는 규격 및 기준을 만들어내기 위해 노력했다. 무선 환경에 적합한 보안 대책 수립, 공인인증기관간 인증서의 상호 연동성 보장, 제품간의 상호 호환성을 보장하기 위한 방안들도 심도 있게 논의되었다. 무선 pki 기술기준과 기술규격이 2001년 8월경에 발표되었고, 이를 기반으로 무선 공인인증기관 세부지정기준이 공시되어 무선 공인 인증 서비스를 제공할 준비를 갖추게 되었다.

무선 공인 인증 서비스를 제공하기 위한 구체적인 노력으로는 한국정보보호진흥원이 무선 pki기술작업반을 운영하면서, 2001년 3월 무선 최상위 인증기관 및 하위 공인인증기관 테스트 베드를 구축할 보안 업체를 선정하였으며, 이를 통하여 무선 인터넷 환경에 적합한 무선 최상위 인증기관을 전자서명관리센터에 구축하여 서비스 준비를 완료하였고, 무선 pki기술규격 및 기준에서 언급하고 있는 내용들이 기술적으로 또는 현실적으로 합당한지를 테스트 해보기 위해 하위 인증기관을 구축하여 최상위 인증기관과의 연동 테스트를 마무리 했으며 상용 서비스가 수행되기 전까지 지속적인 시범 테스트를 진행하고 있다. 또한 유선환경에서의 공인인증기관들도 무선 공인 인증 서비스 업체가 되기 위해 무선 공인인증기관 세부지정기준에 부합하는 시스템을 구축하는데 열을 올리고 있다. 한국정보인증은 국내 처음으로 2001년 9월경에 케이사인이 구축한 무선인증시스템을 이용하여 무선 공인인증기관 신청서를 제출하여 LG Telecom에 서비스할 계획이며, 한국증권전산은 KTF에 서비스할 인증시스템을 구축하고 공인인증기관 심사 신청서을 제출했고, 한국금융결제원도 2월 또는 3월안에 보안 업체를 선정하고 공인인증기관 심사 신청서를 제출할 계획으로 있다.

이러한 노력은 곧 무선 인터넷 환경에서 인증서를 기반으로 한 다양한 보안서비스를 사용자들이 제공받을 수 있을 것으로 전망되어지고 있다.

본 논문에서는 한국정보보호진흥원에서 발표한 무선 pki기술규격에 대해 자세히 살펴보고, 현재 규격을 따르는 무선 인증 시스템의 전체 구성도 및 구현 방안에 대해 기술한다.

2. 무선 PKI 기술규격

무선환경에 적합한 보안대책 수립, 공인인증기관

* 종신회원

표 1 무선 PKI 기술규격

규 격 명	내 용
무선 전자서명 인증서 프로파일 규격	▣ 무선 전자서명인증관리체계에서 사용되는 무선 전자서명용 X.509 V3 인증서에 대한 프로파일 규격을 정의하고 있으며 인증기관 및 응용 프로그램이 인증서를 생성 및 처리하는데 필요한 요구사항들을 명시하고 있다.
무선 WTLS 인증서 프로파일 규격	▣ 무선 전자서명인증관리체계내에서 인증서를 이용한 키분배용 무선 WTLS 인증서 프로파일 규격을 정의하고 인증기관 및 응용 프로그램의 인증서 생성 처리시 요구사항들을 명시하고 있다. ▣ 본 규격은 무선 전자서명인증관리체계내에서 무선인터넷상의 키분배를 위한 규격으로 사용될 것이다.
무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 규격	▣ 무선 전자서명인증관리체계에서 사용되는 무선 전자서명용 인증서 상태확인을 위한 인증서 효력정지 및 폐지 목록 프로파일에 대한 규격을 정의하고 있으며 인증기관과 응용 프로그램이 인증서 효력정지 및 폐지 목록을 생성 및 처리하는데 필요한 요구사항들을 명시하고 있다.
무선 전자서명 인증서 DN 규격	▣ 인증서 및 인증서 폐지 목록을 전자서명인증관리체계에서 고유하게 식별하기 위한 DN(Distinguished Name) 규격을 정의
무선 WTLS 인증서 DN 규격	▣ WTLS인증서를 무선 전자서명인증관리체계에서 고유하게 식별하기 위한 DN(Distinguished Name) 규격을 정의
무선 전자서명 알고리즘 규격	▣ 무선 전자서명인증관리체계에서 지원하는 전자서명 알고리즘, 해쉬 알고리즘에 대하여 기술하며 관련 규격을 명시한다.
무선 키분배 알고리즘 규격	▣ 본 규격에서는 키분배인증서 서명에 지원되는 알고리즘과 해쉬에 대하여 기술하며 관련 표준을 명시한다.
무선 전자서명 인증서 OID 규격	▣ 무선 전자서명인증관리체계 OID규격은 전자서명 알고리즘, 해쉬 알고리즘, 인증서 정책, 인증서 구성요소 등에 대한 OID를 체계적으로 구축하는데 활용
무선 인증서 요청형식 프로토콜 규격	▣ 무선 전자서명인증관리체계에서 사용될 전자서명 및 키분배 인증요청형식 프로토콜 규격을 정의하며 인증기관 및 응용 프로그램이 요청형식을 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다.
무선 인증서 관리 프로토콜 규격	▣ 무선 전자서명인증관리체계에서 사용될 무선 전자서명 및 키분배 인증서 재발급, 갱신, 효력정지, 효력회복시 필요한 관련규격을 정의하며 인증기관 및 응용 프로그램이 요청형식을 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다.
무선 응용계층 보안 프로토콜 규격	▣ 무선 전자서명인증관리체계에서 사용될 인증서 기반의 응용계층 프로그램간의 프로토콜이 암호화된 정보를 생성하고 처리하는데 필요한 요구사항들을 명시하고 있다.

간 인증서의 상호연동성 보장, 관련 제품간의 상호호환성을 보장하기 위해서는 관련 기술규격이 필요하다. 기술규격은 2001년 8월에 한국정보보호진흥원이 발표하였으며, 세부항목과 내용은 표 1과 같다.

무선 PKI기술규격은 총11개의 세부규격으로 나누어지며, 이들 중에 유선PKI 기술규격과 차이점을 살펴보고, 무선 전자서명 인증서 프로파일, WTLS인증서 프로파일, 무선 전자서명인증서 효력정지 및 폐지 목록 프로파일 등을 중심으로 살펴보도록 한다.

2.1 무선 PKI 기술 규격의 특징

현재 국내에서는 기존에 구축된 전자서명법에 기반을 두고 있는 전자서명인증관리체계가 존재하며, 공인인증기관을 중심으로 사용자에게 금융서비스, 전자결제 서비스, 전자상거래 서비스 등을 제공하고 있다. 그러나 무선 인터넷 환경에서 사용하기에는 시스템이 무겁고 여러가지 제약점을 가지고 있다(단말기 화면 제한, 네트워크 대역폭 제한, CPU처리속도 제한, 메모리 제한, 입력장치 제한 등). 무선 인터넷 환경에서는 이러한 제약점을 고려한 기술 규격이 필요하였으며 이를 위해 무선 PKI기술규격을 만들게 되었다.

다음은 무선 환경의 여러가지 제약사항들로 인해 무선인증시스템이 유선인증시스템과 구별되어지는 차이점들을 살펴본다.

첫번째. 인증시스템의 핵심인 공개키 암호 알고리즘으로 대표되는 RSA알고리즘은 안전성에 비해 상당한 연산을 요구한다. 특히 키 쌍 생성(공개키, 비밀키 쌍)시에는 현재 핸드폰에서 사용하고 있는 MSM3100 또는 MSM5000 칩에서는 10분 이상의 시간이 소요됨으로 인해 서비스가 불가하다. 그러나 향후 이동 단말기의 성능 향상과 유무선 통합을 고려하여 RSA공개키 알고리즘도 규격안에 포함시켰다. 현재의 기술로 구현 가능하도록 하기 위해 유선에서는 사용되지 않던 ECC알고리즘이 무선 환경을 위한 공개키 알고리즘으로 선택되었으며, RSA와 비교해 적은 키 사이즈로도 동일한 비도를 보장할 뿐만 아니라 빠른 연산속도를 보장한다.

두번째. 단말기의 CPU처리속도와 메모리 제한으로 인증서의 상태정보를 획득하기 위해 CRL을 다운로드하고 분석하는 일련의 작업이 관리되는 인증서가 많아짐에 따라 처리가 어려워진다. 이러한 문제점을 극복하기 위해 X.509v3인증서를 단순화시킨 WTLS(Short-lived)인증서를 정의하여 짧은 유효기간을 부여한다. 또한 인증시스템은 WTLS의 연장성을 보장하기위해 24시간마다 유효기간을 변경하여 발행한다. 유선의 CRL메커니즘을 Short-lived 메커니즘이 대행한다.

세번째. 이동 단말기에서 인증서 요청형식은 유선에서 사용하고 있는 PKCS#10, RFC2511을 사용하지 않고 WAP Forum에서 정의하고 있는 스크립트 함수인 signText함수를 응용하여 무선 환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 정의하여 사용하는 것을 권고하고 있다.

표 2 인증서 프로파일 비교

항 목		Critical	생성	처리
Authority Key Identifier	유선	n	m	m
	무선	n	m	o
Subject Key Identifier	유선	n	m	m
	무선	n	m	o
Domain Information	유선	n	m	m
	무선	n	m	o
Authority Information Access	유선	n	m	m
	무선	n	m	o
c : critical n : non-critical b : critical or non-critical - : not defined m : mandatory o : optional x : not recommended				

네번째. 유선용과 무선용 X.509v3인증서 프로파일에 표 2에서와 같이 차이점이 발생한다.

표 2에서 알 수 있듯이 유선에서는 AKI와 SKI의 생성, 처리가 Mandatory로 되어있는데 무선 단말기에서는 처리부분을 가볍게 하기 위해 두 필드에 대하여 처리부분은 선택사항(option)으로 정의하였고 인증서 상태검증의 방법으로 OCSP사용을 위해 DI필드와 AIA필드를 포함하였다.

2.2 무선 전자서명 인증서 프로파일

인증서의 표준은 ITU-T가 1988년 X.509를 제정한 이후로 지속적으로 개발되어 1993년 두번째 판이 개정되었으며 1997년 세 번째 판이 개정되었다. 또한 IETF에서는 인증서에 대한 프로파일에 대하여 1999년 RFC2459로 정의하여 권고하고 있다. 이에 따라 WAP 포럼에서도 WAP-211-X.509로 무선 인증서에 대한 프로파일에 대하여 무선X.509v3인증서 프로파일을 정의하여 권고하고 있다. 그림 1은 무선X.509v3 인증서 프로파일의 구성도를 나타내고 있다.

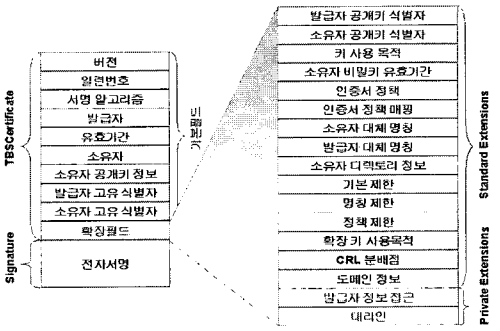


그림 1 무선 X.509v3 인증서 프로파일

2.3 WTLS인증서 프로파일

WTLS인증서 프로파일은 무선 환경의 특성을 고려하여 만들어진 간소화된 인증서의 형태이다. X.509v3인증서를 근간으로 했으며, 일련번호, 발급자 고유 식별자, 소유자 고유 식별자, 확장 필드들을 제외시켜 인증서 검증에 로드를 감소시켰다. 또한 Short-lived메커니즘을 적용 받아, 유효기간은 일반적으로 48시간으로 발행되며 폐지 사유가 발생하지 않는다면 매24시간마다 재발행되어 유효기간을 계속적으로 연장시킨다. 그림 2는 WTLS인증서 프로파일의 구성도를 표현하고 있다.

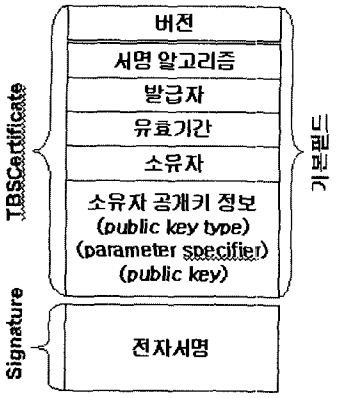


그림 2 WTLS 인증서 프로파일

2.4 무선 전자서명인증서 효력정지 및 폐지목록 프로파일

인증서 효력정지 및 폐지목록은 인증서의 효력정지 및 폐지 여부를 인증서 사용자에게 알리기 위한 수단으로 개발되었으며 ITU-T가 1993년 X.509인증서 효력정지 및 폐지 목록에 대한 첫 번째 표준을 제정한 이후로 1997년 두 번째 판이 개정되었다. 또한 IETF에서는 인증서 효력정지 및 폐지 목록에 대한 프로파일을 1999년 RFC2459로 정의하여 권고하고 있다. 무선 전자서명용 인증서 상태확인을 위한 인증서 효력정지 및 폐지 목록 프로파일에 대한 규격은 유선과 동일하게 정의한다. 그림 3은 인증서 효력정지 및 폐지 목록 프로파일에 대한 구성도를 표현하고 있다.

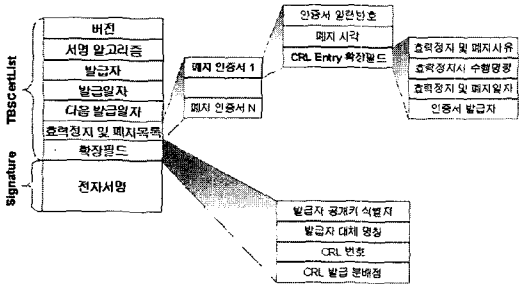


그림 3 인증서 효력정지 및 폐지 목록 프로파일

3. 구현 기술 소개

무선인터넷에서 인증서 기반의 보안서비스를 제공하기 위해 국내에서는 무선환경의 전자서명 인증관리체계를 구축하고 있다. 무선 최상위 인증기관은 한국정보보호진흥원의 전자서명인증관리센터내에 개발 완료되어 설치되었으며, 하위 인증기관들은 무선 공인인증기관이 되기 위해 시스템을 구축하고 실질심사에 임하고 있거나 이미 완료한 상태다.

특이할 사항은 유선과는 달리 무선 전자서명 인증관리체계내에서는 OCSP(On-line Certificate Status Protocol)을 기본 구성요소로 규정하였으며, OCSP서버의 인증서를 무선 최상위 인증기관에서 발급하고 관리한다.

그림 4는 최상위 인증기관과 공인인증기관과의 구성도를 표현하고 있다.

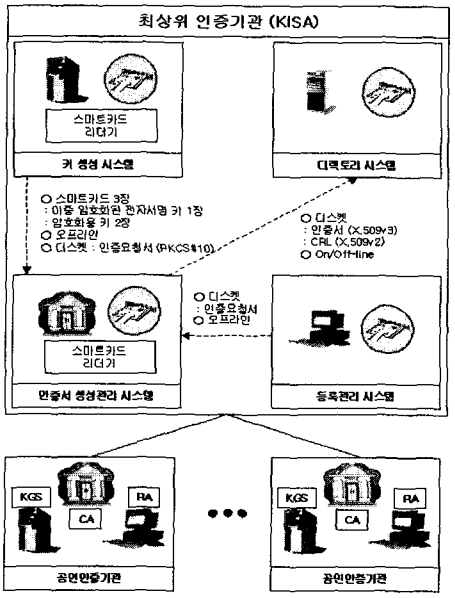


그림 4 최상위 인증기관 과 공인인증기관

3.1 인증서 발급 프로토콜

IETF PKIX Working Group RFC2510 (CMP : Certificate Management Protocol), RFC2511 (CRMF:Certificate Request Message Format)에서 정의하고 있는 인증서 관리 프로토콜과 인증서 요청 양식은 유선환경에 적합한 인증서 발급 및 관리를 위한 국제 기술 규격이다. 그러나 CPU성능 제약 등 많은 제한을 갖고 있는 무선 환경에서의 인증서 발급 및 관리 프로토콜(무선망을 사용하는 이동 단말기로 한정)로는 부적당하다. 아래의 그림 5는 무선 환경에서 인증서 발급 흐름도에 대한 구성도를 나타내고 있다.

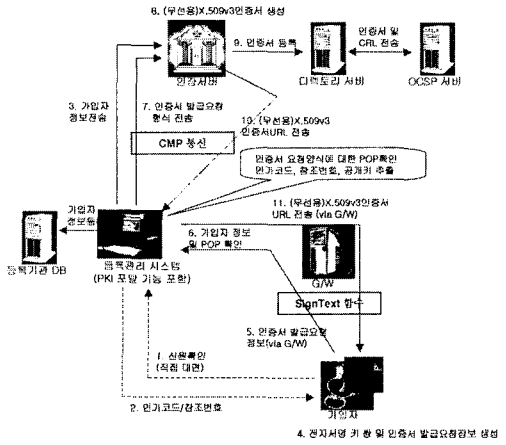


그림 5 인증서 발급 절차

국내에서 정의한 무선 PKI기술규격은 이동 단말기에서 인증서를 발급 받기 위한 인증서 발급 요청 프로토콜을 WAP 포럼에서 제안하고 있는 WML Script인 signText함수를 사용하는 것을 수용했으며, 구체적인 파라미터 세팅방안에 대해서는 보안강도와 편리성, 핸드폰의 로드 감소 차원에서 많은 논의를 거쳐 그림 6에서와 같이 인증서 발급 프로토콜을 정의했다.

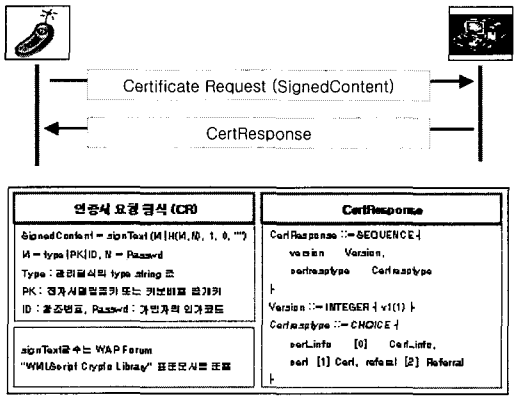


그림 6 인증서 발급 프로토콜

3.2 인증서 관리 프로토콜

인증서 관리 프로토콜은 인증서 재발급, 인증서 갱신, 인증서 효력정지, 인증서 효력회복, 인증서 폐지로 구분할 수 있다.

인증서 재발급은 가입자가 가입자의 전자서명생성키가 분실, 훼손 또는 도난, 유출되었다고 판단되는 경우를 의미하며 프로토콜은 그림 7과 같다.

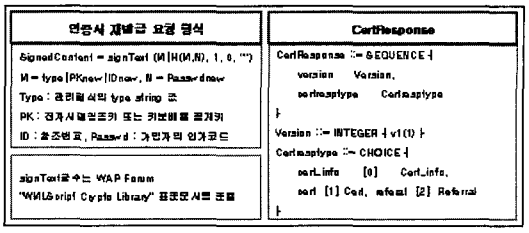


그림 7 인증서 재발급 프로토콜

인증서 갱신은 가입자가 인증서 만료 인정기간 전부터 만료일까지 가입자가 유효기간 연장을 위해 갱신발급 요청을 한 경우를 의미하며 프로토콜은 그림 8과 같다.

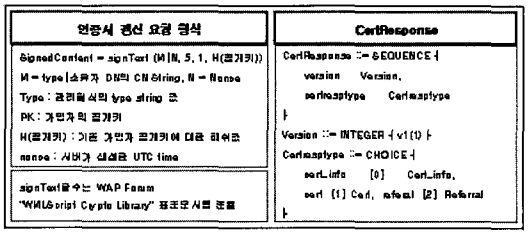


그림 8 인증서 갱신 프로토콜

인증서 효력정지/회복은 전자서명법(제17조)에 의거 가입자 또는 그 대리인의 신청이 있는 경우에는 인증서의 효력을 정지하거나 정지된 인증서를 회복하는 것을 의미하며 프로토콜은 그림 9와 같다.

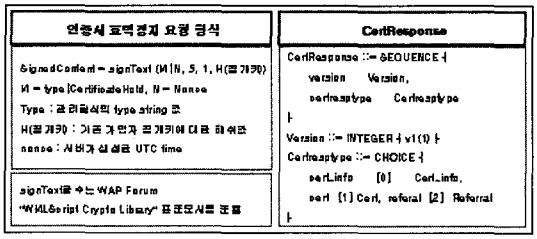


그림 9 인증서 효력정지 프로토콜

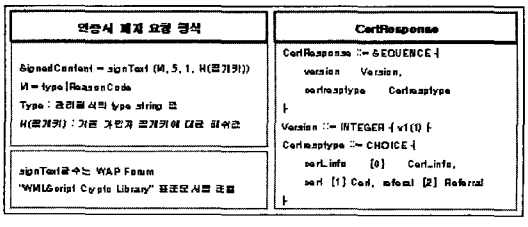


그림 10 인증서 폐지 프로토콜

인증서 폐지는 전자서명법(제18조)에 의거 가입자 또는 그 대리인이 인증서 폐지를 신청한 경우, 가입자의 전자서명생성키가 분실, 훼손 또는 도난, 유출된 사실을 인지한 경우 가입자는 공인인증기관(혹은 등록기관)에 폐지 신청을 한 경우를 의미하며 프로토콜은 그림 10과 같다.

4. 결 론

국내의 무선 인터넷 시장은 젊은층을 중심으로 확대되고 있으며, 모바일 전자상거래, 폰 뱅킹 서비스, 증권 거래 서비스 등 다양한 컨텐츠 및 서비스를 발굴하고 가입자가 믿고 사용할 수 있는 환경을 제공한다면 폭발적인 수요를 창출할 수 있을 것이다.

국내의 무선 PKI구축은 사용자의 요구에 의해 이동통신 사업자가 서비스의 질을 차별화 하기 위한 일환으로 시작됐으며, 조만간 서비스가 시작될 예정이다.

국내 이동통신 사업자인 LG Telecom은 한국정보인증에 무선 인증 시스템을 구축하고 한국정보보호진흥원으로부터 시스템 실질심사를 완료한 상태고 곧 국내 최초로 상용 서비스를 시작할 예정이며, 다른 인증기관에도 무선 인증 시스템을 구축하여 사용자에게 공인인증기관을 선택할 수 있도록 확대할 예정이다. 그리고 SK Telecom과 KTF 또한 무선 공인인증 서비스를 가입자들에게 제공하기 위해 인증 시스템 구축 및 노력을 기울이고 있다.

본 논문에서는 국내 무선 인증 관리 체계의 기술규격인 무선 PKI기술규격의 태동 배경과 내용을 살펴보았으며, 유선 PKI와 비교해 무선 환경에서 변경되어진 기술 규격 및 구현 기술들을 소개했다.

참고문헌

[1] WAP Forum Proposed Version 9-Mar-2000, WAP-211-X.509 : WAP Certificate and CRL Profile

[2] WAP Forum Proposed Version 3-Mar-2000, WAP-217-WPKI : WAP Public Key Infrastructure Definition

[3] WAP Forum Approved Version 11-July-2000, WAP Transport Layer E2E Security Specification

[4] WAP Forum Proposed Version 05-Nov-1999, WMLScript Crypto Library

[5] IETF RFC 2511, Internet X.509 Cetificate Request Message Format

[6] IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols

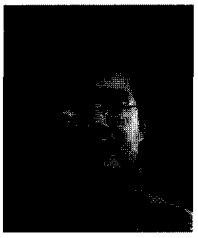
[7] ITU-T Recommendation X.509, Information technology－Open System Interconnection－The Directory : Authentication Framework

[8] IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[9] 한국정보보호진흥원, 무선 PKI기술규격 V1.21, 2001.08

[10] 한국정보보호진흥원, 무선 PKI기술기준, 2001.09

장 준 교



1997 아주대학교 컴퓨터공학과(공학사)
1999 아주대학교 컴퓨터공학과 석사과정(공학석사)
2000 아주대학교 컴퓨터공학과 박사과정 수료
2000~현재 (주)케이사인 보안기술개발부/부장
2000~2002 한국정보통신기술협회(TTA) 차세대IC카드PG 특별위원
관심분야:PKI, 네트워크 보안, 무선 보안, 암호기술 응용
E-mail:visionjk@ksign.com

구 자 동

1996 아주대학교 컴퓨터공학과(공학사)
1998 아주대학교 컴퓨터공학과 석사과정(공학석사)
1998 삼성전자 네트워크 연구소 주임연구원
1998 한국정보보호진흥원 연구원
2000~현재 ㈜케이사인 응용보안개발부 총괄 이사
관심분야:PKI, 무선 보안, 권한관리기술, 응용 보안 기술
E-mail:koojd@ksign.com

홍 기 융

1985 전남대학교 전자계산학과 졸업
1990 중앙대학교 대학원 전자계산학과 졸업(석사)
1996 아주대학교 대학원 컴퓨터공학과 졸업(박사)
1985~1995 한국전자통신연구소 선임연구원
1995~1996 한국전산원 선임연구원
1996~2000 한국정보보호진흥원 인증관리팀장
1998~현재 동국대학교 국제정보대학원 겸임교수(정보보호학과)
2000~현재 ㈜케이사인 대표이사
관심분야:PKI, 보안 커널, 네트워크 보안, 응용 보안 기술
E-mail:kyhong@ksign.com