소 특 집

국내 공개키기반구조(PKI) 구축 현황

이 원 철, 이 재 일, 이 홍 섭
한국정보보호진흥원

요 약

1999년 7월 1일 전자서명법의 시행과 더불어 국내에서는 최상위인증기관(Root CA)인 한국정보보호진흥원을 중심으로 가입자에게 전자서명 인증서비스를 제공하기 위한 공개키기반구조(Public Key Infrastructure, PKI) 구축이 진행되어 왔다. 공개키기반구조는 인터넷상에서 거래당사자에게 직접 대면에 준하는 신원확인 및 문서의 위·변조 방지, 거래사실의 부인방지 등의 기능을 제공하여 주기 때문에 전자상거래를 위한 핵심기술로 분류된다. 본 고에서는 국내 PKI 구축 현황을 파악하기 위해 현재까지 구축된 국내 PKI 체계 및 기술 현황을 기술하고 PKI 활성화를 위해 진행 중인 상호연동에 대해 알아본다. 또한 무선 인터넷환경에서 PKI 서비스를 위한 무선 PKI 기술·구축 현황에 대하여 기술한다.

I. 서 론

최근 국내·외적으로 공개키기반구조(Public Key Infrastructure, PKI)에 대한 관심이 날로 증가함에 따라 많은 e-비지니스 환경에서 PKI 서비스가 확산되고 있다. 이에 국내에서는 1999년 전자서명법을 시행하여 최상위인증기관(Root CA) 및 공인인증기관이 탄생했으며 이에 따른 본격적인 공인 인증서비스가 시행되어 왔다.

전자서명법은 비대칭형(공개키) 암호기술을 기반으로 하는 전자서명(Digital Signature)에 법적 인감과 동일한 효력을 부여함으로써, 온라인 전자결제 등과 같은 전자적 거래를 촉진케 할 수 있는 제도적 기반 마련을 목적으로 한다.

전자서명법에 의거하여 한국정보보호진흥원(KISA)내의 전자서명인증관리센터는 국내 최상위인증기관의 역할을 수행하여 전자서명인증관리체계 구축·운영 및 공인인증기관에 대한 인증서 발급 및 관리를 통하여 전자서명인증관리체계의 안전·신뢰성 확보와 전자서명 인증제도 및 전자문서 이용 활성화 기반 조성에 이바지하며 국내 PKI 구축에 앞장서 왔으며 공인인증기관은 사용자들에 대한 인증업무를 원활히 수행해 왔다.

본 고에서는 전자서명법과 함께 시작된 국내 PKI의 기술 현황과 구축 현황 등에 대해 기술하고 인증서의 상호연동 서비스를 위해 진행중인 국내 공인인증기관간의 인증서 상호연동 기술과 국가간 전자서명 상호인증과 관련한 기술을 살펴보았다. 또한 최근 급증하고 있는 무선인터넷 사용자에게 PKI 서비스를 제공하기 위한 무선 PKI 기술 규격 및 구축 현황에 대해 기술한다. 전체적인 구성내용을 살펴보면 다음과 같다. 제2절에서는 전자서명법체계에 기반을 둔 국내 공인 인증체계의 의미와 공인인증기관 지정 현황에 대해 살펴보고 제3절에서 국내 PKI의 기술현황에 대해 유·무선 PKI 부분으로 나누어 기술하였다. 제4절에서는 Root CA인 전자서명 인증관리센터의 유·무선 PKI 시스템 구축 현황에 대해 기술하였으며 제5절에서 국내 공인인증기관 등의 PKI 구축에 대해 살펴보았다. 제6절에서는 국내

에서 추진된 기술 규격과 표준화 현황에 대해서 살펴보고 제7절에서 향후 국내 PKI에 대한 전망에 대해 고찰한 뒤 제8절에서 결론을 맺는다.

II. 전자서명법에 기초한 공인 인증 체계

1999년 7월 1일 전자서명법 시행으로 정보통신망을 통한 비대면 전자문서의 교환, 전자상거래의 안전 및 신뢰성 확보를 위한 국가차원의 전자서명인증체계를 마련하였다. 전자서명법에 의해 국내 전자서명인증체계에서는 정보통신부가 공인인증기관에 대한 정책·감독 기관으로서의 기능을 수행하고, 한국정보보호진흥원내 전자서명인증관리센터가 Root CA의 역할을 담당하고 있다.

전자서명법 제25조에는 전자서명인증관리센터의 주요 역할을 규정하고 있다. Root CA는 전자서명 인증관리체계의 구축 및 총괄업무, 공인인증기관에 대한 인증 업무 수행, 공인인증기관 지정을 위한 실질심사 및 안전운영 검사, 정부의 상호인정 지원 및 외국 인증기관과의 상호인증, 인증관련 기술 개발 및 보급 등과 같은 업무를 수행한다.

국내 PKI 체계에서는 사용자에 대한 인증업무를 수행하기 위해서 Root CA로부터 실질심사를 거친 공인인증기관을 지정하여 운영하도록 하고 있다. 전자서명법에 의거 공인인증기관으로 지정된 곳은 한국정보인증(주), 한국증권전산(주), 금융결제원, 한국전산원, 한국전자인증(주)으로 모두 5곳이며 현재 한국무역정보통신에 대한 실질심사가 진행 중이다. 무선분야 서비스를 위한 공인인증기관 실질심사는 작년 8월 평가지침을 완성하였으며 현재 한국정보인증(주) 및 한국증권전산(주)에 대한 무선분야 실질심사가 진행 중이다.

국내 공인인증체계에서 전자서명법의 시행은 전자서명에 법적 인감과 동일한 효력을 부여하고 Root CA 및 공인인증기관이 인증업무를 안전하게 수행하도록 하여 사용자는 법적효력을 가진 전자서명을 이용해 안전·신뢰성 있는 PKI 서비스를 제공받을 수 있게 되었다.

III. 국내 PKI 기술 현황

1. 유선 PKI 기술

PKI의 핵심이 되는 인증서에 대한 규격은 ITU-T가 1988년 X.509를 제정한 이후로 지속적으로 개발되어 1993년에는 두 번째 판이, 1997년에는 세 번째 판이 개정되었으며 2000년 네 번째 판이 개정되었다. 인증서의 규격에서는 인증서가 지원할 수 있는 가능한 모든 정보를 표현할 수 있도록 정의하고 있으므로 이 규격을 그대로 인증 서비스 영역에 적용하여 사용하기에는 무리가 있으며 동일한 서비스 영역에서 인증서를 생성하고 사용하는 시스템들이 개별적으로 표준을 적용하여 개발되는 경우에는 전체 인증 서비스 영역 내에서의 호환성 및 연동성이 보장되지 못한다.

이를 위해서는 각 인증 서비스 영역 내에서의 고유한 인증서 프로파일이 요구되며 IETF에서는 인증서에 대한 프로파일에 대하여 1999년 RFC 2459로 정의하여 권고하고 있다. 국내의 경우도 1999년 국제표준을 기반으로 하여 전자서명법 상에서 구축된 전자서명 인증관리체계에서 사용되는 전자서명용 인증서 프로파일에 대한 규격[9]과 인증서효력정지 및 폐지목록(Certificate Revocation List, CRL)[10]에 대한 규격을 제정하였다.

또한, 인증서 및 CRL을 전자서명 인증관리체계 내에서 고유하게 식별하기 위하여 표준화된 OID(Object Identifier) 규격[11] 및 DN(Distinguished Name) 규격[12]을 제정하여 사용하고 있으며 전자서명을 위한 KCDSA, 해쉬알고리즘인 HAS-160, 128비트 블록암호알고리즘으로 SEED등을 국내 전자서명인증관리체계 내에 포함시켰다.

PKI의 구조가 복잡해지고 인증서의 검증이 복잡해짐에 따라 인증서 검증 및 획득기술과 인증서의 현재 상태 조회를 위한 인증서 상태 검증 기술 등에 대한 중요성이 증대되었다. 인증서 온라인 상태 검증을 위해 국내에서도 OCSP(Online Certificate Status Protocol) 및 SCVP (Simple Certificate Validation Protocol)에 대한 기술 개발이 진행 중이며 공인인증기관 등에도 이러한 기술이 도입될 것으로 보인다.

2. 무선 PKI 기술

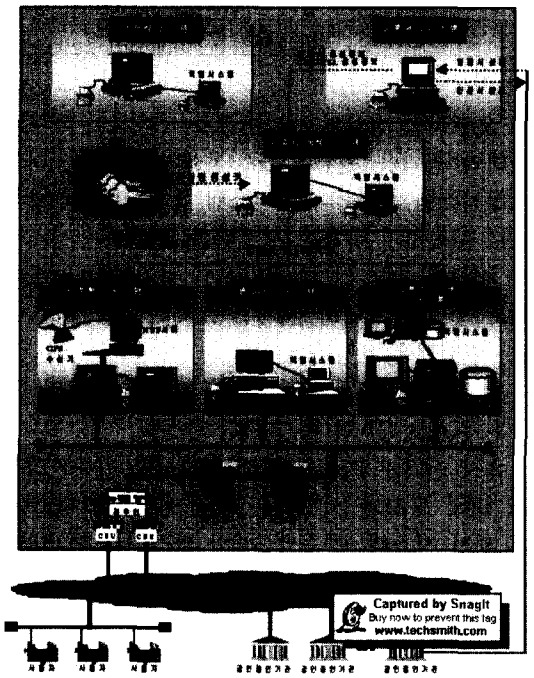
무선 인터넷 시스템은 유선 인터넷 시스템과는 달리 여러 가지 제약성을 가지고 있다. 무선 시스템의 경우 네트웍의 문제(낮은 대역폭, 시간지연, 연결의 불안전성 등) 및 디바이스의 문제(낮은 연산능력의 중앙처리장치, 적은 메모리, 배터리 시간, 작은 디스플레이, 입력장치 등)로 현재의 유선인터넷에서 이용되는 프로토콜 등을 무선단말기에 그대로 적용하기에는 많은 문제점들이 존재한다. 이러한 무선 환경의 제약성을 극복할 목적으로 무선 인터넷을 위한 새로운 기술들이 개발되었다. 현재 무선 인터넷 접속을 위한 기술은 Phone.com, Ericsson, Motorola 등이 주축인 WAP(Wireless Application Protocol)포럼에서 기존 유선 인터넷에서의 프로토콜인 HTTP에 기반하지 않고 새로이 무선 인터넷 프로토콜을 개발하여 사용 중에 있다. 기존 HTTP에 기반하여 무선 데이터 서비스를 제공하는 대표적인 기술로는 마이크로소프트사의 ME(Mobile Explorer), NTT-Docomo의 I-mode 등을 들 수 있다. 국내 무선 인터넷 접속기술로서 KTF는 ME를 SK텔레콤, LG텔레콤은 WAP을 채택하여 서비스하고 있다.

무선 단말기의 최대 단점은 낮은 대역폭과 작고 낮은 해상도의 디스플레이, 입력의 불편함을 들 수 있다. IMT-2000 및 향후 개선된 시스템에서 이 문제들의 극복이 가능하리라 보여지지만 현시점에서 많은 문제점을 안고 있는 것은 사실이다.

무선 PKI 서비스에서 가장 중요한 부분의 단말기에서 수신된 인증서의 검증부분이다. 인증서비스를 위해선 인증서를 사용하여야 하는데 현재 단말기의 성능으로는 검증이 현실적으로 어려운 상태이다. 현재는 인증서 검증을 서버에서 수행하기 위한 OCSP, SCVP 등의 인증서 검증모델이 연구 진행중이다.

Ⅳ. Root CA의 구축현황

Root CA인 전자서명인증관리센터에 구축된 시스템 설계의 기본원칙은 안전·신뢰성의 보장이다. 전자서명인증관리센터의 시스템은 엄격한 직무기반 접근통제하에 운영된다. 우선 모든 인증관련 업무는 단독 실행이 불가능하도록 직무를 분리하였다. 키 생성 업무의 경우 3인 이상이 수행하도록 구성되어있으며 기타 인증업무의 경우 2인 이상이 함께 수행하도록 되어있다. 또한 인증업무 기능 단위로 시스템을 분리 운영하고 있으



〈그림 1〉 전자서명 인증관리센터 네트워크 구성도.

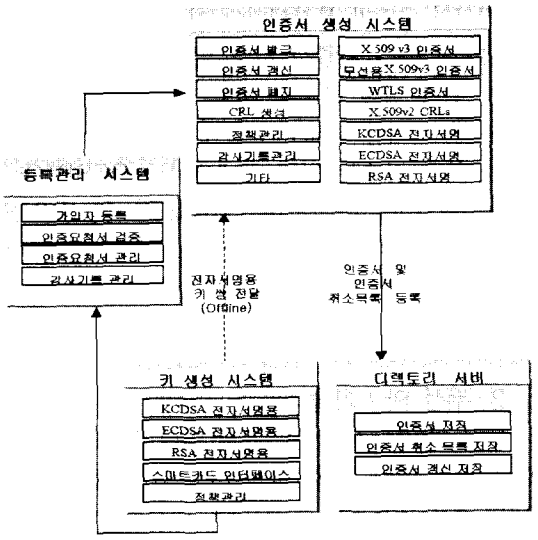
〈표 1〉 전자서명 인증관리센터 시스템 구성 및 기능

시스템 구성	기능
등록관리 시스템	· 인증서 발급 요청 기관 정보 등록 및 관리 · 인증서 발급에 필요한 데이터 입력 · 보관
키 생성 시스템	· 인증관리센터 키 생성 - 전자서명생성키 · 전자서명검증키 - 시점확인용 전자서명생성키 · 전자서명검증키
인증서 생성 · 관리 시스템	· 인증관리센터 자가서명인증서 (Self-signed Certificate) · 공인인증기관 인증서 생성 · 공인인증기관 인증서 효력정지및폐지목록 생성
디렉토리 시스템	· 인증관리센터 인증서 공고 · 공인인증기관 인증서 공고 · 공인인증기관 인증서 효력정지및폐지목록 공고
시점확인 시스템	· 공인인증기관 시점확인 요청시 서비스 제공 · GPS 수신 방식을 통한 시간 보정
웹 서비스 시스템	· 전자서명법 · 제도 홍보 및 인증관리센터 업무 알림 · 공인인증기관 목록 유지 · 공인인증기관 상태에 대한 정보 제공 · 인증서 검증 S/W 공고 및 인증서 상태 검증 서비스 제공 등

며 오프라인 방식의 시스템으로 구축하여 외부로부터의 공격을 원천적으로 봉쇄하고 있다. 디렉토리시스템, 웹 서비스 시스템 등 오프라인 방식으로 구축하지 못하는 시스템을 위해서는 시스템의 이중화, 네트워크 침입차단, 침입탐지 시스템 구축 및 운영요원의 24시간 모니터링을 통해 안전 · 신뢰성을 보장하고 있다.

1. Root CA의 유선 PKI 시스템

유선 인터넷 PKI를 위해 전자서명 인증관리센터 내에 구축된 시스템은 크게 등록관리시스템, 키 생성 시스템, 인증서 생성 · 관리 시스템, 디렉토리 시스템, 시점확인 시스템, 웹 서비스 시스템과 같이 분야별 주요 시스템으로 구성된다. 전자서명 인증관리센터의 시스템 구성도는 〈그림 1〉과 같으며 키 생성 시스템, 인증서 생성 시스템



〈그림 2〉 전자서명 인증관리센터 무선용 시스템 구성도.

및 등록관리 시스템은 오프라인으로 운영되고 있으며 웹 서비스 시스템과 디렉토리 서비스 시스템은 온라인으로 운영되고 있다.

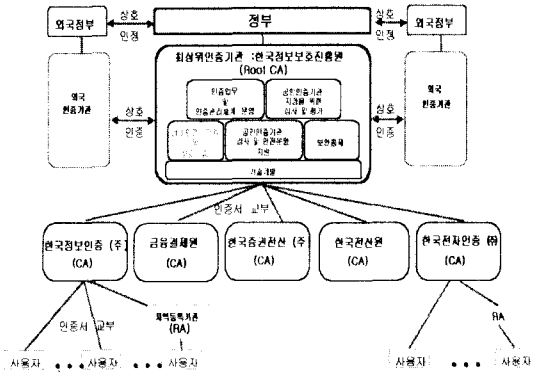
전자서명 인증관리센터 내에 구축된 시스템별 주요기능은 〈표 1〉과 같다.

2. Root CA의 무선 PKI 시스템

Root CA의 무선용 인증서버 시스템은 무선 PKI 기술 규격을 준수하여 전자서명용 키 쌍 및 인증서 요청양식을 생성하는 키 생성 시스템과 인증서 생성, 갱신, 재발급, 효력정지, 효력회복, 폐지 및 인증서 취소목록을 생성하는 인증서 생성 시스템, 인증요청서 및 사용자 정보를 등록하는 등록관리 시스템으로 구성되며 논리적 구성도는 〈그림 2〉와 같다.

V. 국내 공인인증기관의 구축 및 서비스 현황

PKI 서비스 사용자에 대한 인증업무를 수행하는 공인인증기관의 인증시스템의 경우 국내 전자서명 인증관리체계를 따르도록 구축되고 있으며



〈그림 3〉 국내 전자서명인증관리 체계도.

〈표 2〉 국내 공인인증기관 현황

구분	한국 정보인증	한국 증권전산	금융 결제원	한국 전산원	한국 전자인증
공인인증 기관지정일	2000.2	2000.2	2000.4	2001.3	2001.11
주요사업 분야	전자 상거래	사이버 증권거래	인터넷 뱅킹	공공분야	전자 상거래
웹사이트	http://www.signgate.com	http://www.signkorea.com	http://www.yessign.or.kr	http://sign.nca.or.kr	http://gca.crosscert.com

이를 Root CA에서 심사하고 평가한다. 국내 전자서명 인증관리 체계도는 〈그림 3〉과 같다.

현재까지 국내 공인인증기관으로 지정된 곳은 한국정보인증(주), 한국증권전산(주), 금융결제원, 한국전산원, 한국전자인증(주) 5곳이며 현황은 〈표 2〉와 같다.

국내에서 발급된 공인인증서는 2001년 12월 현재 150만개이상으로 인터넷 뱅킹을 위한 인증서가 많이 발행되었다. 국내 5대 공인인증기관의 인증서 발행현황을 보면 〈표 3〉과 같다. 한국전자인증의 경우 2001년 11월에 공인인증기관으로 지정된 후 2002년 1월까지 테스트를 수행하였으므로 발급된 인증서가 없는 상태이다.

무선 PKI서비스를 제공하기 위해 한국정보인증(주), 한국증권전산(주) 등에 대한 공인인증기관 실질심사가 진행 중이며 이동 통신 3개사와의 협력을 통해 곧 상용서비스를 시작할 예정이다. 각 공인인증기관 모두 Root CA의 무선 PKI 기술기준(안)과 기술규격을 준수하여 시스템을 구축하였다.

〈표 3〉 국내 공인인증기관 인증서 발급현황
(2001.12.31 기준)

구분	한국 정보 인증	한국 증권 전산	금융 결제원	한국 전산원	한국 전자 인증	계
서버 인증서	113	34	81	-	-	228
개인/법인 인증서	75,235	82,302	1,337,774	5,996	-	1,501,307
계	75,348	82,336	1,337,855	5,996	-	1,501,535

국내 이동통신사별 구축현황을 살펴보면 우선 SK텔레콤와 LG텔레콤은 WAP방식의 시스템을 적용하고 있으며, KTF는 ME방식의 시스템을 적용하고 있다. 사용자의 인증서는 X509v3을 사용하는 것으로 하나 무선단말기에 저장하는 것이 현실적으로 어려우므로 URL 전송방식을 이용한다.

Ⅳ. 국내 PKI 기술 규격 및 표준화 현황

1. 유선 PKI 인증서 기술 규격

국내 전자서명 인증서 프로파일은 ITU-T의 X.509v3인증서 및 IETF RFC 2459를 준수하고 있다. 공인인증기관을 위한 인증서의 프로파일은 〈표 4〉와 같고 사용자를 위한 인증서의 프로파일은 〈표 5〉와 같다.

〈표 4〉 인증기관 인증서 프로파일

기본필드	KISA	
	생성	처리
Version	m	m
Serial Number	m	m
Signature	m	m
Issuer	m	m
Validity	m	m

기본필드	KISA	
	생성	처리
Subject	m	m
Subject Public Key Info	m	m
Issuer Unique ID	x	x
Subject Unique ID	x	x
Extensions	m	m

확장필드명	KISA		
	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Subject Key Identifier	n	m	m
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Policies	b	m	m
Policy Mappings	n	o	m
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	m	m
Name Constraints	c	o	m
Policy Constraints	c	o	m
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	m
Authority Information Access	n	o	o
Procuration	-	-	-

c : critical
b : critical or non-critical
m : mandatory
x : not recommended
n : non-critical
- : not defined
o : optional

〈표 5〉 사용자 인증서 프로파일

기본필드명	KISA	
	생성	처리
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 ID	x	x
Subject Unique ID	x	x
Extensions	m	m

확장필드명	KISA		
	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Subject Key Identifier	n	m	m
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Policies	b	m	m
Policy Mappings	-	-	-
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	x	x
Name Constraints	-	-	-
Policy Constraints	-	-	-
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	m
Authority Information Access	n	o	o
Procuration	n	o	o

c : critical
b : critical or non-critical
m : mandatory
x : not recommended
n : non-critical
- : not defined
o : optional

전자서명 인증서 효력정지 및 폐지 목록 프로파일에 대한 내용은 〈표 6〉과 같다.

〈표 6〉 전자서명 인증서 효력정지 및 폐지 목록 프로파일

기본필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m

기본필드명	생성	처리
This Update	m	m
Next Update	m	m
Revoked Certificates	m[1)]	m
User Certificates	m[1)]	m
Revocation Date	m[1)]	m
CRL Entry Extionsions	m[1)]	m
CRL Extensions	m	m

인증서효력정지 및 폐지 목록 확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Issuer Alternative Name	n	o	m
CRL Number	n	m	m
Issuer Distribution Point	c	o	m
Delta CRL Indicator	-	-	-

엔트리 확장필드명	critical	선택여부	
		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-critical
b : critical or non-critical - : not defined
m : mandatory r : recommended
o : optional x : forbidden or not recommended
1) 효력정지 및 폐지된 인증서가 없을 경우에는 효력정지 및 폐지 목록 필드가 인증서 효력정지 및 폐지 목록에 나타나지 않음

2. 공인인증기관간 상호연동 기술 규격

국내 PKI 사용자가 공인인증기관에서 발급받은 하나의 인증서만으로 국내 모든 PKI 서비스를 이용하기 위해서는 공인인증기관간의 인증서 상호연동이 필수적이다. 이에 따라 공인인증기관간 상호연동을 위한 기술 규격[19]이 제정되었다. 이 기술 규격의 내용은 인증서 규격, 인증서 관리방식, 인증서 검증 방식, 디렉토리 서버에 관련한 사항으로 나눌 수 있다.

인증서 규격에 대한 사항의 주요내용은 〈표 7〉과 같다.

〈표 7〉 인증서 규격 관련사항

주요 항목	권고 사항
인증서 및 CRL 형식	· DER, PEM 타입의 인증서를 처리할 수 있어야 함
한글 UTF8 코딩 방식	· 인증서내 DN등에 사용되는 한글을 UTF8 형식으로 표현해야 함
인증서 DN 형식	· 사용자 소프트웨어는 인증서내 UTF 8 형식으로 표현된 한글 DN을 처리할 수 있어야 함 · 사용자 소프트웨어는 디렉토리 서버내 UTF8 형식으로 표현된 엔트리의 한글DN를 검색할 수 있어야 함
인증서 소유자 신원정보	· 인증서 소유자의 실명은 한글로 인증서내 SubjectAltName 확장필드에 UTF8 문자열로 표현해야 함 · 인증서 소유자의 주민등록번호는 인증서내 SubjectAltName 확장필드의 OtherName 속성에 전자적인 방법으로 처리한후 표현해야 함

인증서 관리방식에 관련한 사항은 〈표 8〉과 같다.

〈표 8〉 인증서 관리방식 관련사항

주요 항목	권고 사항
사용자 소프트웨어 설치	· 사용자 소프트웨어는 타 공인인증기관의 사용자 소프트웨어가 설치되는 디렉토리와 다른 위치에 생성되어야 함
전자서명키 저장 방식	· 전자서명생성키는 PKCS #5 형식으로 암호화된 후 PKCS #8 형식으로 저장되어야 함
전자서명키와 인증서 전달 방식	· 전자서명키와 인증서를 타 공인인증기관의 사용자 소프트웨어에서 Import/Export 하기 위하여 PKCS #12 형태로 생성되어야 함
신뢰당사자의 인증서 및 CRL 획득 방식	· 타 공인인증기관의 인증서를 획득하기 위해 사용자 소프트웨어는 자체적인 테이블 형태로 획득 정보를 유지하거나 인증서 확장필드의 AIA 확장필드를 사용해야 함 · 타 공인인증기관의 CRL을 획득하기 위해 사용자 소프트웨어는 CRL DP 확장필드를 처리할 수 있어야 함

인증서 검증방식과 관련된 사항은 〈표 9〉와 같다.

〈표 9〉 인증서 검증방식 관련사항

주요 항목	권고 사항
인증서 검증 방식	· 인증서 검증시에는 RFC2459의 절차를 준용하여 기본검증 및 각 확장필드가 가능해야 함 · 검증절차에는 Certificate Policies 확장필드를 무조건 검사하여 없으면 중단하는 절차를 포함하여야 함

디렉토리 서버와 관련된 사항은 〈표 10〉과 같다.

〈표 10〉 디렉토리 서버 관련사항

주요 항목	권고 사항
디렉토리 스키마	· 인증서 및 CRL 저장공간 명칭은 RFC2587를 준용하여야 함 · 인증서는 userCertificate ; binary, CRL은 certificateRevocationList ; binary에 저장하여야 함
디렉토리 DN 형식	· 디렉토리 엔트리의 DN 및 속성에 한글을 사용할 경우 한글을 UTF8 문자열로 표현해야 함

3. 무선 PKI 기술 규격

무선 PKI의 인증서 프로파일의 경우 WAP 포럼의 WAP-211-X.509에 무선 X.509V3인증서 프로파일을 정의하여 권고하고 있다. 국내의 경우 한국정보보호진흥원은 2001년 1월부터 공인인증기관, CA 개발업체, 이동통신사업자로 이루어진 무선 PKI 실무작업반을 구성하고, 공인인증기관간 인증서의 상호연동을 보장하고 관련 제품 간의 상호호환성을 확보할 수 있도록 무선 PKI 제품 개발의 가이드라인 격인 기술규격을 개발하였다. 국내의 경우 유선 인터넷의 보안을 위한 PKI 체계를 무선이라는 제한된 환경에 적용하기는 어려운 실정이다. 따라서 무선환경에 적합한 무선 PKI를 위한 기술 규격이 필요로 하였다.

알고리즘 부분의 경우 무선 단말에서는 RSA를 사용한 키 생성이 용이하지 않아 ECDSA를 사용하여 키를 생성할 수 있는 기능이 추가되었다. 현 기술로 단말기에서 CRL 혹은 OCSP를 사용한 검증이 용이하지 않아 WAP에서는 기존 X.509V3 인증서의 기본필드와 유사한 WTLS 인증서를 정의하여 CA가 24시간마다 short-lived 형태의 WTLS 인증서를 발행하여 사용하는 것을 권고하고 있다. 또한 유선의 경우 전체 CRL을 가져와서 인증서 상태를 검증하지만 무선에서는 CRL를 잘게 자른 후 최근 CRL을 가져와서 검증할 수 있는 메카니즘인 Delta CRL 사용을 선택 사항으로 추가하여 정의하였다. 인증서 요청형식의 경우 유선에서 사용되고 있는 PKCS#10, RFC2511를 사용하는 것이 아니라 WAP에 기반한 SignText 함수를 정의하여 무선환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 정의하여 사용을 권고하고 있다.

무선 전자서명 인증서 프로파일은 무선 전자서명 인증관리체계 내에서 사용되는 인증서에 대한 규격으로서 기본필드 및 확장필드 중 인증서 생성 시에 요구되는 필드의 내용과 사용자소프트웨어 등에서 인증서 처리 시에 요구되는 확장필드에 대하여 정의하고 있으며 확장필드에 대한 criticality를 정의한다. 무선 전자서명 인증서 프로파일은 〈표 11〉과 같다.

〈표 11〉 무선 전자서명인증서 프로파일

기본필드명	생성	처리
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 ID	x	x
Subject Unique ID	x	x
Extensions	m	m

확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	o
Subject Key Identifier	n	m	o
Key Usage	c	m	m
Private Key Usage Period	n	x	x
Certificate Policies	b	m	m
Policy Mappings	n	o	m
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory Attributes	n	x	x
Basic Constraints	c	m	m
Name Constraints	c	o	m
Policy Constraints	c	o	m
Extended Key Usage	b	o	m
CRL Distribution Points	n	m	o
domain information*	n	o	o
Authority Information Access	n	m	o
Procuration	-	-	-

c : critical n : non-critical
b : critical or non-critical - : not defined
m : mandatory o : optional
x : not recommended
* OCSP를 사용할 경우 DI의 사용을 적극 권고함.

무선 전자서명 인증서 효력정지 및 폐지목록은 〈표 12〉와 같다.

〈표 12〉 무선 전자서명인증서 효력정지 및 폐지목록 프로파일

기본필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revoked Certificates	m[1)]	m
User Certificates	m[1)]	m
Revocation Date	m[1)]	m
CRL Entry Extensions	m[1)]	m
CRL Extensions	m	m

인증서효력정지 및 폐지 목록 확장필드명	critical	선택여부	
		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	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
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-critical
b : critical or non-critical - : not defined
m : mandatory r : recommended
o : optional x : forbidden or not recommended
1) 효력정지 및 폐지된 인증서가 없을 경우에는 효력정지 및 폐지 목록 필드가 인증서 효력정지 및 폐지목록에 나타나지 않음

국내 무선 인증서에서 사용되는 전자서명 관련 알고리즘은 RSA, ECDSA이며 해쉬알고리즘으로 SHA-1이 사용된다. RSA의 경우 지원하는 키의 길이는 1024비트 이상이어야 하며 ECDSA의 경우 지원하는 키의 길이는 160비트 이상이어야 한다. SHA-1 해쉬알고리즘은 기본적으로 메시지 인증에 사용되며 전자서명 알고리즘과 함께 전자서명 생성 및 검증에 사용된다.

상기 내용으로 인증서 프로파일과 관련하여 유선용과 무선용의 차이를 알아보면 〈표 13〉과 같다.

〈표 13〉에서 알 수 있듯이 유선에서는 AKI와 SKI의 생성, 처리가 필수로 되어있는데 무선 단말기에서는 처리부분을 가볍게 하기 위해 두 필드에 대해서 처리부분을 선택사항으로 정의하였고 OCSP 사용에 있어서도 유선에서는 Private Extension 필드인 AIA필드를 사용하여 OCSP 사용을 권고하고 있는 반면 무선에서는 Domain

〈표 13〉 유·무선 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	-	-	-
	무선	n	o	o
Authority Information Access	유선	n	o	o
	무선	n	m	o

c : critical　　n : non-critical
- : not defined　　m : mandatory
o : optional

Information 필드를 기본 확장필드로 정의하여 OCSP 사용을 권고하고 있다.

Ⅶ. PKI의 전망

최근 인터넷 사용 인구의 폭발적인 증가로 인터넷 뱅킹, 증권거래 및 전자상거래에 대한 이용자가 급증하면서 공인인증서 발급건수는 지난해 말 150만건을 넘었다.

이와 같이 국내 PKI 서비스의 역할이 증대되면서 사용자의 편의성에 대한 관심이 집중되고 있다. 금년 공인인증기관간 인증서 상호연동을 위한 서비스가 시작되면 사용자들은 한 장의 인증서만을 가지고도 모든 PKI 서비스를 제공받을 수 있어 정부의 PKI 기반 전자민원서비스를 금년안에 시행할 예정이다.

무선 PKI의 경우, 휴대폰 등 무선단말기를 이용한 무선인터넷 사용의 증가로 무선인터넷 뱅킹, 무선인터넷 증권거래와 인터넷쇼핑몰 이용 같은 전자상거래가 확산되고 있으며 기업의 시스템도 무선시스템으로 구축하는 사례 또한 늘고 있다. 향후에는 무선인터넷 사용자 서비스가 다양해질 것으며 또한 이와 함께 유선과 동일한 정보보호 서비스의 요구가 증대되어질 것으로 예상되어진다. 그러나 기존의 유선 시스템에서 사용되던 보안 솔루션을 그대로 무선에 적용한다는 것은 아직까지 매우 어려우며, 현재는 웹 보안 프로토콜인 SSL의 사용이 증가하면서 SSL의 핵심기술인 공개키 암호방식의 기반이 되는 PKI의 중요성이 강조되고 있다.

Ⅷ. 결 론

1999년 전자서명법 시행과 함께 시작된 국내 PKI는 Root CA로 전자서명인증관리센터, 공인인증기관으로 한국정보인증(주), 한국증권전산(주), 금융결제원, 한국전산원 및 한국전자인증(주)의 5곳이 구축되어 있다. 현재 진행중인 실질심사가 완료가 된다면 유선 PKI를 지원하는 공인인증기관은 더 늘어날 것이며 금년 상반기 중으로 무선 PKI를 지원하는 공인인증기관도 구축될 것이다.

공인인증기관의 증가로 인해 사용자들의 인증서 사용에 대한 편의성을 제공하기 위해서는 공인인증기관간의 인증서 상호연동이 선결되어야 하며 이를 위한 기술 규격 개발이 계속 진행되어야 한다.

무선 PKI는 현재 WAP과 ME를 큰 축으로 양분되어 있다. 두 방식 모두 장단점을 지니고 있고 시장성에 대해서도 국내에서 검증된 바가 없기 때문에 향후 어느 방식이 주도적인 기술이 될 것이라는 판단을 내린다는 것은 매우 어렵다. 따라서 두 방식의 경쟁보다는 상호연동을 통해 두 시스템을 보완하며 발전시켜 나가는 것이 중요하다. 한국정보보호진흥원과 기타 업체들이 협의하여 내놓은 무선 PKI 기술 규격은 이러한 WAP 간의 상호연동 및 WAP과 ME 그리고, 기존의 유선인터넷을 위한 보안 기술 규격 등과 상호연동 될 수 있도록 충분히 고려되었다.

참 고 문 헌

〔1〕 ITU-T Recommendation X.509|ISO/IEC 9594-8, "Information technology-Open System Interconnection-The Directory : Authentication Framework", 1997.

〔2〕 IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999.

〔3〕 IETF RFC 2510, "Internet Public Key Infrastructure Certificate Management Protocol", Mar. 1999.

〔4〕 IETF RFC 2527, "Internet Public Key Infrastructure Certificate Policy and Certification Practies Freamework", Mar. 1999.

〔5〕 IETF RFC 2527, "Internet Public Key Infrastructure Certificate Policy and Certification Practies Freamework", Mar. 1999.

〔6〕 IETF RFC 2527, "Internet Public Key Infrastructure Certificate Policy and Certification Practies Freamework", Mar. 1999.

〔7〕 최영철, 오경희, 이재일, 홍기융, "전자서명 인증관리센터 구축 및 운영", 한국정보보호학회지 제9권 제3호, Sep. 1999.

〔8〕 박정환, "무선 PKI 기술 규격", 정보보호뉴스, Vol. 47, Aug. 2001.

〔9〕 윤재호, "국내 무선 PKI 구축 현황과 전망", 정보보호뉴스, Vol. 47, Aug. 2001.

〔10〕 TTAS.KO-12.0012, "전자서명 인증서 프로파일 표준", 2000.

〔11〕 TTAS.KO-12.0013, "전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준", 2001.

〔12〕 KISA, "전자서명 인증관리체계 OID 규격", 2001.

〔13〕 KISA, "전자서명 인증관리체계 DN 규격", 1999.

〔14〕 TTAS.KO-12.0001, "부가형 전자서명 방식 표준-제2부 : 확인서 이용 전자서명 알고리즘", 1998.

〔15〕 TTAS.KO-12.0001/R1 "부가형 전자서명 방식 표준-제2부 : 인증서 기반 전자서명 알고리즘", 2000.

〔16〕 TTAS.IT-X509/R2, "디렉토리시스템 인증 프레임워크 표준", 2000.

〔17〕 TTAS.KO-12.0011, "해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)", 1998.

〔18〕 TTAS.KO-12.0011/R1, "해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160)", 2000.

〔19〕 TTAS.KO-12.0004, "128비트 블록암호 알고리즘 표준", 1999.

〔20〕 KISA, "공인인증기관간 상호연동을 위한 기술 규격", 2000.

〔21〕 IETF RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP", Jun. 1999.

〔22〕 IETF PKIX draft, "Online Certificate Status Protocol, version 2", Mar. 2001.

〔23〕 IETF PKIX draft, "Simple Certificate Validation Protocol (SCVP)", Feb. 2001.

〔24〕 WAP Forum, "WAP-211-X.509 : WAP Certificate and CRL Profile", Proposed Version, Mar. 2000.

〔25〕 WAP Forum, "WAP-217-WPKI : WAP Public Key Infrastructure Definition", Proposed Version, Mar. 2000.

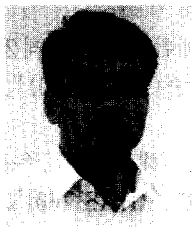
〔26〕 법률 제5792호, "전자서명법", 1999. 2. 5.

〔27〕 법률 제6360호, "전자서명법 일부개정", 2000. 1. 16.

저 자 소 개

李 杭 哲

1995년 경북대학교 전자공학과 공학사, 1997년 경북대학교 전자공학과 공학석사, 1999년 1월~2001년 6월 : (주)웰컴정보시스템 근무, 현재 한국정보보호진흥원 평가인증사업단 전자서명인증관리센터 연구원.



李 載 日

1986년 서울대학교 계산통계학 이학사, 1988년 서울대학교 계산통계학 이학사, 1991년~1996년 : 한국 IBM 소프트웨어 연구소 근무, 현재 한국정보보호진흥원 평가인증사업단 전자서명인증관리센터장

李 弘 燮

1979년 한양대학교 전자공학 공학사, 1985년 한양대학교 전자공학 공학석사, 1999년 대전대학교 컴퓨터공학 공학박사, 1980~1996년 : 한국전자통신연구원 책임연구원, 실장, 1996~현재 : 한국정보보호진흥원 연구개발부장, 기술본부장, 현 평가인증사업단 단장, 1997~2001년 : 한국정보통신기술협회 정보보호기술위원회 의장, 1999년 국가최상위인증기관 전자서명인증관리센터구축준비반장, 2000~현재 : 인터넷보안기술포럼 의장, 2001~현재 : ASIA PKI Forum Interoperability WG 공동의장, 2002~현재 : 순천향대학교 겸임교수, 2002~현재 : 한국정보보호학회 부회장.