情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

국내 PKI 구축 현황 및 기술

정연호*, 최원석*, 권태경*, 이광수**

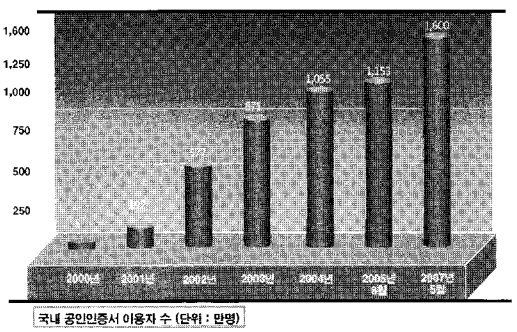
요 약

정보화 시대로써 정보의 가치가 높아지면서 이를 불법적으로 취득하려는 공격에 대응하고자 정보보호에 대한 이슈가 대두되고 있다. 이러한 정보보호 기술 중 공개키 기반구조의 암호시스템을 사용하는데 필요한 모든 서비스를 안전하게 제공할 수 있도록 하기위한 인프라를 Public Key Infrastructure 라고(이하 PKI) 한다. 이러한 PKI는 정부나 다수 기업의 공동 연합체에서 주도적인 역할을 수행해야 의미가 있다고 볼 수 있는데, 이미 선진 각국에서는 PKI 개발 및 구축 노력을 하고 있으며 이는 21세기 새로운 국가 경쟁력으로서의 중요성이 인식되어 있는 상태다. 결국 PKI를 통한 정보보호 문제의 해결은 한 차원 높은 전자 경제 활성화의 경쟁력을 갖는 주요 포인트라고 할 수 있겠고, 범 국가 적인 PKI의 구축은 세계화의 경제를 이끌 수 있는 전자 경제의 중요한 기반 기술로서 그 영향력이 매우 크다고 할 수 있으므로 본 논문에서는 이러한 PKI의 국내 구축현황 및 기술에 대하여 살펴본다.

Ⅰ. 서 론

PKI 기술은 인터넷 환경에서의 네트워크 망과 같은 정보보호기반 기술 요소로서의 인프라 개념이다. 따라서 몇몇 업체나 기관에 의해 구축되어지는 것이 아닌 정부, 정보보호 개발 업체, 서비스 업체 및 연구기관 들 다양한 분야의 기술과 정책이 어우러져야 비로소 효과를 얻을 수 있는 기술이라고 할 수 있다. 많은 선진 각국에서는 정부의 주도적인 PKI 구축 정책에 따라 많은 부분에 PKI 인프라가 구축되어졌으며 PKI 기반의 다양한 응용 서비스가 이루어지고 있다. 국내에서도 선진국에서 추진하고 있는 PKI 관련 정책 및 법 제도, 기술적 수준 등이 동등한 위치에 있거나 일부 분야는 보다 앞서고 있는 것이 사실이다. 이러한 점에서 볼 때 국내의 전자 경제화는 커다란 변화에 매우 능동적으로 대처하고 있는 것이며 차세대 세계 경제를 이끌 수 있는 좋은 소식이라고 할 수 있겠다. 또한 PKI 기술 및 구축에 있어 매우 규모가 크고 관련 요구되는 개발 업체의 끊임없는 노력과 정부의 정책적인 의지 등은 현재 국내 PKI 저변 확대 및 인프라 구축에 밝은 미래를 볼 수 있다.

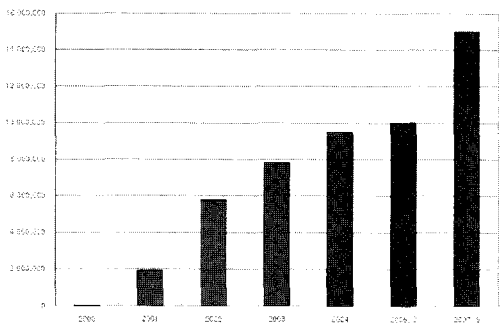
다음 [그림 1]은 공인인증서의 이용자수와 발급건수의 수요로써 PKI의 실제 사용성을 나타낸다.



〔그림 1〕 공인인증서 이용자수

이처럼 공인인증서의 실 사용율이 증가함을 근거로 PKI의 중요성을 다시한번 살펴볼 수 있다. 하위 다음 2장에서는 국내 PKI의 동향 및 구축환경에 대하여 알아보고, 3장에서 표준화 현황을 조사한 후 4장에서 국내 PKI 발전 방향으로 본 논문의 결론을 말하고자 한다.

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[IITA-2007-S-601-01, 자기통제 강화형 전자ID지갑 시스템 개발]
* 세종대학교 컴퓨터공학과 정보보호연구실({ororoyo, deabak88}@sju.ac.kr, tkwon@sejong.ac.kr)
** 숙명여자대학교 정보과학부(rhee@sm.ac.kr)



〔그림 2〕 공인인증서 발급건수

Ⅱ. 국내 PKI 동향 및 구축 환경

1. 국내 PKI 동향

현재 국내 PKI 구축 동향은 크게 대국민 서비스를 위한 정부 PKI와 공인인증 서비스를 기반으로 하는 전자서명 인증관리체계로 나뉜다.

1.1. 정부 PKI

먼저 정부 PKI는 인터넷 인프라의 확산과 인터넷 인구의 증가에 발맞춰 보다 효율적이고 국민 편의 중심의 대국민 서비스를 위한 목적으로 이루어졌다. 지난 수년간 정부의 정보화로 체질 개선을 이룬 정부는 이것을 기반으로 다양하고 복잡한 대국민 서비스를 쉽고 편하게 하기위해서 행정 자치부를 중심으로 다양한 민원 서비스를 인터넷을 활용하여 쉽게 제공 하도록 준비하고 있다. 이러한 서비스를 안전하고 신뢰성이 확보된 환경에서 제공하기 위해서는 PKI 기반의 서비스가 이루어져야 한다는 것을 알고 외국의 사례 및 국내 기술진에 의해 검토된 정부 PKI 구축이 이루어지고 있는 실정이다. 향후 정부의 서비스 범위가 세금, 자동차 관련 업무, 부동산 등으로 확대되어짐에 따라 PKI 역시 정부 내의 부서별, 분야별로 확대되어짐으로써 정부 PKI 구축 및 인증 서비스는 다양한 대국민 서비스에서의 필수적인 요소로 자리 잡고 있다.

1.1. 전자서명 인증관리체계

공인인증 서비스를 통해 사용되고 있는 전자서명 인증관리체계의 PKI는 인터넷 주식 거래 등의 증권분야, 인터넷 보험 판매 등에 대한 보험 분야, 인터넷 뱅킹 등 금융 분야, 쇼핑몰 거래 등의 전자상거래 분야, 전자세무신고, 전자입찰, 국채 매매 등의 공공분야 등에서 광범위하게 전자서명 인증 서비스가 이루어지고 있으며 그 활용 범위가 인증서 로밍 서비스나 인증서 휴대폰 저장서비스로 확대 지원되고 주민번호 대체 수단으로 사용하거나 성인인증 또는 부모동의에 공인인증서를 이용할 수 있도록 확대하고 있다[14].

2. 국내 PKI 구축 환경

현재 국내 PKI 구축 환경은 유선 PKI, 무선 PKI, Root CA 부분으로 나뉜다.

2.1. 유선 PKI

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 정의 하고 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[19, 20].

이를 위해서는 각 인증 서비스 영역 내에서의 고유한 인증서 프로파일이 요구되며 IETF에서는 인증서에 대한 프로파일에 대하여 1999년 RFC2459로 정의하여 권고하고 있다. 국내의 경우도 1999년 국제표준을 기반으로 하여 전자서명법 상에서 구축된 전자서명 인증관리체계에서 사용되는 전자서명용 인증서 프로파일에 대한 규격과 인증서효력정지 및 폐지목록(Certificate Revocation List, CRL)에 대한 규격을 제정하였다[3].

또한 인증서 및 CRL을 전자서명 인증관리체계 내에서 고유하게 식별하기 위하여 표준화된 OID(Object Identifier) 규격[13] 및 DN(Distinguished Name) 규격을 제정하여 사용하고 있으며 전자서명을 위한 KCDSA, 해쉬 알고리즘인 HAS-160, 128비트 블록암호알고리즘으로 SEED등을 국내 전자서명인증관리체계 내에 포함

시켰다[16].

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[1]) 및 SCVP(Simple Certificate Validation Protocol[2])에 대한 기술개발이 진행 중이며 공인인증기관 등에서 이러한 기술이 도입될 것으로 보인다.

2.2. 무선 PKI

무선 인터넷 시스템은 유선 인터넷 시스템과는 달리 여러 가지 제약성을 가지고 있다. 무선 시스템의 경우 네트워크의 문제(늦은 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 기반을 두지 않고 새로이 무선 인터넷 프로토콜을 개발하여 사용 중에 있다. 기존 HTTP에 기반을 두어 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. ITM-2000 및 향후 개선된 시스템에서 이 문제들의 극복이 가능하리라 보이지만 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 항태이다. 현재는 인증서 검증을 서버에서 수행하기 위한 OCSP, SCVP 등의 인증서 검증모델이 연구 진행 중이다.

2.3. Root CA

Root CA인 전자서명인증관리센터에 구축된 시스템 설계의 기본원칙은 안전·신뢰성의 보장이다. 전자서명인증관리센터의 시스템은 엄격한 직무기반 접근통제 하에 운영된다. 우선 모든 인증관련 업무는 단독 실행이 불가능하도록 직무를 분리하였다. 키 생성 업무의 경우 3인 이상이 수행하도록 구성되어 있으며 기타 인증업무의 경우 2인 이상이 함께 수행하도록 되어있다. 또한 인증 업무 기능 단위로 시스템을 분리 운영하고 있으며 오프라인 방식의 시스템으로 구축하여 외부로부터의 공격을 원천적으로 봉쇄하고 있다. 디렉토리 시스템, 웹서비스 시스템 등 오프라인 방식으로 구축하지 못하는 시스템을 위해서는 시스템의 이중화, 네트워크 침입차단, 침입탐지 시스템 수축 및 운영요원의 24시간 모니터링을 통해 안전·신뢰성을 보장하고 있다.

2.3.1 Root CA의 유선 PKI 시스템

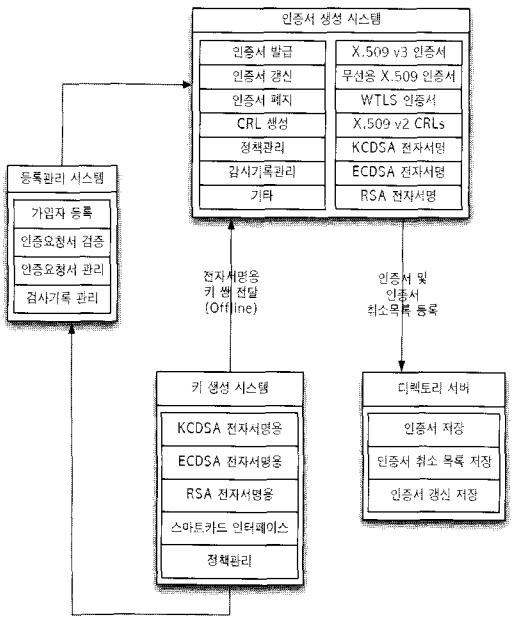
〔표 1〕 전자서명 인증관리센터 시스템 구성 및 기능

시스템 구성	기능
등록관리 시스템	·인증서 발급 요청 기관 정보 등록 및 관리 ·인증서 발급에 필요한 데이터 입력·보관
키 생성 시스템	·인증관리 센터 키 생성 ·전자서명 생성키·전자서명 검증키 ·시점확인용 전자서명 ·생성키·전자서명 검증키
인증서 생성·관리 시스템	·인증관리센터 자가 서명 ·인증서(Self-Signed Certificate) ·공인인증기관 인증서 생성 ·공인인증기관 인증서 효력정지 및 폐지목록생성
디렉토리 시스템	·인증관리센터 인증서 공고 ·공인인증기관 인증서 공고 ·공인인증기관 인증서 효력정지 및 폐지목록공고
시점확인 시스템	·공인인증기관 시점확인 요청 시 서비스 제공 ·GPS 수신방식을 통한 시간 보정
웹서비스 시스템	·전자서명법·제도 홍보 및 인증·관리센터 업무 알림 ·공인인증기관 목록 유지 ·공인인증기관 상태에 대한 정보 제공 ·인증서 검증 S/W 공고 및 인증서 상태 검증 서비스 제공 등

유선 인터넷 PKI를 위해 전자서명 인증관리센터 내에 구축된 시스템은 크게 등록관리 시스템, 키 생성 시스템, 인증서 생성·관리시스템, 디렉토리 시스템, 시점확인 시스템, 웹 서비스 시스템과 같이 분야별 주요 시스템으로 구성된다. 키 생성 시스템, 인증서 생성 시스템 및 등록관리 시스템은 오프라인으로 운영되고 있으며 웹 서비스 시스템과 디렉토리 서비스 시스템은 온라인으로 운영되고 있다. 전자서명 인증 관리 센터 내에 구축된 시스템별 주요기능은 [표 1]과 같다.

2.3.2 Root CA의 무선 PKI 시스템

Root CA의 무선용 인증서버 시스템은 무선 PKI 기술 규격을 준수하여 전자서명용 키 쌍 및 인증서 요청 양식을 생성하는 키 생성 시스템과 인증서 생성, 갱신, 재발급, 효력정지, 효력회복, 폐지 및 인증서 취소목록을 생성하는 인증서 생성 시스템, 인증요청서 및 사용자 정보를 등록 하는 등록 관리 시스템으로 구성되며 논리적 구성은 [그림 3]과 같다.



[그림 3] 전자서명 인증관리 체계

Ⅲ. 국내 PKI 관련 표준화 현황

국내 PKI 관련 표준은 IETF PKIX, ISO/IEC JTC1/SC27 등 국제 표준을 준용하거나 일부 국내 실정에 적합하게 일부 수정하여 적용하였다. 특히 국내 전자서명인증관리체계 확립을 위해 필요한 기술은 국외 전자서명 인증 서비스 기관의 기술을 다수 흡수하여 적용하였다. 국내 전자서명 인증 관리체계를 구축 하는데 요구되는 기술규격에 대한 주요 내용들을 다음과 같다[12].

- OID(Object Identifier) 기술규격
- DN(Distingguished Name) 기술규격
- X.509 v3 인증서 및 인증서 프로파일 기술규격
- X.509 v2CRL 및 CRL 확장 프로파일 기술규격
- LDAP(LightWeight Directory Access Protocol)
- SSL v3.0(Secure Socket Layer) \& TLS(Transport Layer Security)
- PKI 구성 객체 간 이용되는 프로토콜

[표 2] 국내 PKI 구축 적용 기술

구분	·한국공인인증기관용 PKI
전자서명 알고리즘	· KCDSA, RSA
해쉬 알고리즘	· HAS-160, SHA-1
키 분배 알고리즘	· Optional
암호 알고리즘	· SEED, 국가기관용 암호화 알고리즘
인증서, API 규격	· X.509 v3, PKIX-Profile(RFC2459)
인증서 효력정지 및 폐지 목록 규격	· X.509 v3, PKIX-Profile(RFC2459)
인증서, API 규격	· PKCS#10
디렉토리, API 규격	· X.500, LDAP(RFC2559)
시점확인 서비스, 프로토콜	· Optional
인증서 검증	· Optional
인증서 관리 프로토콜	· Optional
규격 표기 방식	· ASN.1

앞에서 기술한 바와 같이 PKI은 다양한 기술의 집합체라고 할 수 있다. 따라서 PKI 구축에 필요한 각 분야별 요구되는 기술은 서비스 되어지는 정책에 따라 다르게 적용될 수 있다. 상위 [표 2]는 국내외 인증 서비스에서 요구되는 기술적인 사항이다. 이어서 프로파일 기

술 규격에 대하여 좀더 자세히 알아본다. 프로파일 기술 규격은 크게 유선 PKI 인증서 기술 규격, 무선 PKI 인증서 기술 규격, 그리고 국내 전자서명 인증 관리체계의 ODI 규격으로 나뉠수 있다.

1. 유선 PKI 인증서 기술 규격

국내 전자서명 인증서 프로파일은 ITU-T위 X.509 v3 인증서 및 IETF RFC 2459를 준수하고 있다. 공인인증기관을 위한 인증서의 프로파일은 [표 3, 4]와 같고 사용자를 위한 인증서의 프로파일은 표 [5, 6]과 같다[17].

〔표 3〕 인증기관 인증서 프로파일 기본필드

기본필드	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
Extension	m	m

〔표 4〕 인증기관 인증서 프로파일 확장필드

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	n	m	m
Policy Mappings	n	o	m
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory	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	-	-	-

〔표 5〕 사용자 인증서 프로파일 기본필드

기본필드	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
Extension	m	m

전자서명 인증서 효력정지 및 폐지 목록 프로파일에 대한 내용은 [표 7~12]와 같다[18].

2. 무선 PKI 인증서 기술 규격

무선 PKI의 인증서 프로파일의 경우 WAP 포럼의 WAP-211-X.509[8]에 무선 X.509v3인증서 프로파일을 정의 하여 권고하고 있다. 국내의 경우 한국정보보호진흥원은 2001년 1월부터 공인인증기관, CA 개발업체, 이동통신사업자로 이루어진 무선 PKI 실무 작업반을 구성하고, 공인 인증 기관간의 인증서 상호 연동을 보장

〔표 6〕 사용자 인증서 프로파일 확장필드

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	n	m	m
Policy Mappings	-	-	-
Subject Alternative Names	n	m	m
Issuer Alternative Names	n	o	m
Subject Directory	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

〔표 7〕 인증기관 전자서명 인증서 효력정지 및 폐지목록(ARL) 프로파일 기본필드

기본 필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revoked Certificates	m	m
User Certificates	m	m
Revocation Date	m	m
CRL Entry Extensions	m	m
CRL Extension	m	m

〔표 8〕 인증기관 전자서명 인증서 효력정지 및 폐지목록 (ARL) 프로파일 확장필드

인증서 효력정지 및 폐지 목록 확장 필드명	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	-	-	-

〔표 9〕 인증기관 전자서명 인증서 효력정지 및 폐지목록(ARL) 프로파일 엔트리 확장필드

엔트리 확장 필드명	critical	선택여부	
		생성	처리
Reason Code	n	m	m
Hold Instruction	n	o	m
Invalidity Date	n	o	m
Certificate Issuer	c	o	m

하고 관련 제품 간의 상호환경을 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 무선 환경에 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 OCSP[6]를 사용한 검증이 용이하지 않아 WAP에서는 기존 X.509v3 인증서의 기본필드와 유사한 WTLS인증서를 정의하여 CA가 24시간마다 short-lived 형태의 WTLS 인증서를 발행하여 사용하는 것을 권고하고 있다. 또한 유선의 경우 전체 CRL을 가져와서 인증서 상태를 검증하지만 무선에서는 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 PKCD#10, RFC2511를 사용하는 것이 아니라

〔표 10〕 가입자 전자서명 인증서 효력정지 및 폐지목록 (ARL) 프로파일 기본필드

기본 필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revoked Certificates	m	m
User Certificates	m	m
Revocation Date	m	m
CRL Entry Extensions	m	m
CRL Extension	m	m

〔표 11〕 가입자 전자서명 인증서 효력정지 및 폐지목록(ARL) 프로파일 확장필드

인증서 효력정지 및 폐지목록 확장 필드명	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	m	m
Delta CRL Indicator	-	-	-

〔표 12〕 가입자 전자서명 인증서 효력정지 및 폐지목록 (ARL) 프로파일 엔트리 확장필드

엔트리 확장 필드명	critical	선택여부	
		생성	처리
Reason Code	n	m	m
Hold Instruction	n	o	m
Invalidity Date	n	o	m
Certificate Issuer	c	o	m

WAP[9]에 기반한 SignText 함수를 정의하여 무선 환경에 맞는 인증서 요청 및 관리 프로토콜 규격을 정의하여 사용을 권고하고 있다.

〔표 13〕 무선 전자서명 인증서 프로파일 기본필드

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
Extension	m	m

〔표 14〕 무선 전자서명 인증서 프로파일 확장필드

확장 필드명	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	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	o	o
Procuration	-	-	-

무선 전자서명 인증서에 프로파일은 무선 전사서명 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 13, 14]와 같다.

무선 전자서명 인증서 효력정지 및 폐지 목록은 [표 15~ 17]과 같다.

〔표 15〕 무선 전자서명 인증서 효력정지 및 폐지목록 기본필드

기본필드명	생성	처리
Version	m	m
Signature	m	m
Issuer	m	m
This Update	m	m
Next Update	m	m
Revoked Certificates	m	m
User Certificates	m	m
Revocation Date	m	m
CRL Entry Extensions	m	m
CRL Extension	m	m

〔표 16〕 무선 전자서명 인증서 효력정지 및 폐지목록 확장필드

인증서 효력정지 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

국내 무선 인증서에서 사용되는 전자서명 관련 알고리즘은 RSA, ECDSA이며 해쉬 알고리즘으로 SHA-1이 사용된다. RSA의 경우 지원하는 키의 길이는 1024비트 이상이어야 하며 ECDSA의 경우 지원하는 키의 길이는 160비트 이상이어야 한다. SHA-1해쉬 알고리즘은 기본적으로 메시지 인증에 사용되며 전자서명 알고리즘과 함께 전자서명 생성 및 검증에 사용된다[15]. 상

〔표 17〕 무선 전자서명 인증서 효력정지 및 폐지목록 엔트리 확장필드

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

〔표 18〕 인증서 유선과 무선의 차이점

엔트리 확장필드명	critical	선택여부	
		생성	처리
Authority Key Identifier	n	m	m
Reason Code	n	m	m
Hold Instruction	n	o	m
Invalidity Date	n	o	m
Certificate Issuer	c	o	m

기 내용으로 인증서 프로파일과 관련하여 유선용과 무선용의 차이를 알아보면 [표 18]과 같다.

[표 18]에서 알 수 있듯이 유선에서는 AKI와 SKI의 생성, 처리가 필수로 되어있는데 무선 단말기에서는 처리부분을 가볍게 하기 위해 두 필드에 대해서 처리부분을 선택사항으로 정의하였고 OCSP사용에 있어서도 유선에서는 Private Extension필드인 AIA필드를 사용하여 OCSP 사용을 권고하고 있는 반면 무선에서는 Domain Information 필드를 기본 확장필드로 정의하여 OCSP 사용을 권고하고 있다.

3. 국내 전자서명 인증 관리체계의 OID 규격

전자서명 인증관리체계의 기본이 되는 것은 인증서이며 인증서는 기본적으로 사용자와 사용자의 전자서명 검증키의 관계에 대한 신뢰성을 보장해주는 역할을 수행한다. 인증서 내에서는 이러한 기본적인 정보 이외에

도 기타 인증체계를 유지하기 위한 여러 가지 정보들이 포함되어 있다. 이러한 정보에는 알고리즘, 인증서 정책, 키용도, 인증서 속성 등이 포함되며 이러한 정보들이 표현하는 대상들을 객체(Object)라 하고 이러한 객체들을 유일하게 중복되지 않고 식별할 수 있는 방법이 필요하다. 이를 위해서 각 객체에 고유번호를 부여하는 방법이 사용되며 이것을 OID(Object Identifier)라 한다[13]. 본 기술규격에서는 국내 전자서명 인증관리체계에 대한 OID 규격을 제시한다[10].

(1) OID의 개요 및 구성

OID를 부여하는데 있어서 일관되고 통일된 방법이 요구되는데 이를 위해서 국제표준이 정해졌으며 이에 따라 국제단체 및 각 국의 OID 부여 권한을 가진 기관들을 통해서 OID 부여가 이루어진다. OID가 가지는 특징은 다음과 같다.

- 개방형 시스템에서 국제표준에 따라서 임의의 정보개체에 할당된 값
- 전 세계 모든 객체에 대해서 고유번호를 부여
- OID 부여권한을 가진 기관으로부터 계층적 구조에 따라서 할당

OID는 OID를 부여하는 기관에 따라서 번호체계가 달라지며 OID를 부여하는 최상위기관으로는 국제표준화기구인 ISO, ITU-T 및 JOINT-ISO -ITUT 등이 있다. 한국정보보호센터는 이중에서 IDO 체계를 따르고 있다. ISO를 통해서 OID를 부여하는 경우 기본적으로 많은 수의 객체에 대해서 일일이 ISO가 OID를 직접 발급할 수 없으므로 각 국가별로 member-body 번호를 부여하고 해당 국가에서 발생하는 OID신청에 대해서는 해당 국가의 담당기관이 부여하게 된다. 국내에서는 산업자원부가 이를 수행하고 있으며 member-body에 대한 OID는 iso(1) member-body(2) korea(410)이며 한국정보보호센터에 대한 OID는 iso(1) member-body(2) korea (410) kisa(200004)이다. 국내 전자서명 인증관리체계를 위해서는 기본적으로 알고리즘, 인증정책, 키용도, 인증속성 및 공인인증기관 객체들에 대한 정의가 필요하며 이에 따라 OID가 각각에 대해서 부여되고 이후 추가되는 사항에 대해서는 한국 정보보호센터를 기준으로 부여하게 된다.

(2) 한국정보보호센터의 OID 규격

한국정보보호센터에서는 알고리즘, 인증정책, 키용도, 인증 속성 및 공인인증기관에 대한 OID의 국내 최상위 노드로 작용하게 되며 구체적으로 다음의 체계를 갖는다.

① 알고리즘

전자서명 및 해쉬 알고리즘 등의 객체에 대한 OID를 부여한다.

② 인증정책

인증기관이 인증서 발행 시에 사용되는 인증정책에 대한 OID를 부여한다.

③ 키용도

인증서내의 KeyUsage 확장필드에서 정의하고 있는 전자서명 검증키의 용도이외의 것을 사용하고자 하는 경우 각 용도에 따라 OID를 정의한다.

④ 인증속성

인증서에서 사용되는 확장필드 중 표준에서 지원하는 것 이외에 국내 실정에 맞는 속성을 개발하여 사용하고자 하는 경우에 해당 속성에 대해서 OID를 부여한다.

⑤ 공인인증기관

한국정보보호센터로부터 인증 받은 공인인증기관에 대한 OID를 부여하며 공인인증기관이 희망하는 경우 공인인증기관에서 사용하는 객체에 대해서 OID를 부여할 수 있다.

V. 국내 PKI 발전 방향

선진 각국의 PKI 개발 및 구축 노력은 21세기 새로운 국가 경쟁력으로서의 E-Business의 중요성이 인식되어졌으며 전자 경제 활성화의 커다란 걸림돌인 정보보호 문제의 해결은 곧 한 차원 높은 경쟁력을 갖는 주요 포인트라고 할 수 있다. 따라서 범 국가 적인 PKI 구축은 세계화의 경제를 이끌 수 있는 전자 경제의 중요한 기반 기술로서 그 영향력이 매우 크다. 정부나 다수 기업의 공동 연합체에서 주도적인 역할을 수행해야 PKI 구축의 의미가 있다고 볼 수 있다.

사이버 공간상의 전자거래주체(사람, 디바이스 등 다양한 개체)에게 부여되는 다양한 신원정보를 확인 하는 Digital ID, 특정한 정보에 대한 접근, 사용 또는 변경

등의 권한 정보나 이를 표현하는 자격 등의 속성정보를 확인 하는 Digital Right, 전자거래 사실 및 내용 등을 사후에 증명할 수 있는 정보를 확보하고 보존하는 Digital Evidence의 기술들과 사용자 신원인증만을 다루고 있는 현행 전자서명법을 유비쿼터스 환경에 적합하도록 확대 개편하고 이를 위한 근거법률 및 제도가 마련되어 공인 인증이 디지털 인증으로 확대 될 것이다.

휴대폰과 같은 무선단말기를 이용한 무선인터넷 사용의 증가로 무선인터넷 뱅킹, 무선인터넷 증권거래와 인터넷쇼핑몰등 전자상거래가 확산되고 있으며 기업의 시스템도 무선시스템으로 구축되는 사례가 늘고 있어 향후에는 무선 PKI가 유선과 동일한 정보보호 서비스의 요구가 증대되어질 것으로 예상된다. 이에 따라 사용자들의 인증서 사용에 대한 편의성을 제공하기 위해서는 공인인증기관간의 인증서 상호연동이 선결되어야 하며 이를 위한 기술 규격 개발이 계속 진행되어야 한다.

참고문헌

[1] IETF PKIX draft, "Online Certificate Status Protocol, version 2", Mar. 2001.

[2] IETF PKIX draft, "Simple Certificate Validation Protocol (SCVP)", Feb. 2001.

[3] IETF RFC 2459, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", 1999.

[4] IETF RFC 2510, "Internet Public Key Infrastructure Certificate Management Protocol", Mar. 1999.

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

[6] IETF RFC 2560, "X.59 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP", Jun. 1999.

[7] ITU-T Recommendation X.509 ISO/IEC 9594-8, "Information technology-Open System Interconnection-The Directory : Authentication Framework", 1997.

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

[9] WAP Forum, "WAP-217-WPKI : WAP Public Key Infrastructure Definition", Proposed Version, Mar. 2000.

[10] 이원철, 이재일, 이홍섭, "국내 공개키 기반 구조(PKI) 구축 현황", KISA..

[11] 최영철, 오경희, 이재일, 홍기웅, "전자서명 인증관리센터 구축 및 운영", 한국정보보호 학회지 제9권 제3호, Sep. 1999.

[12] KISA, "PKI 기반 기술 및 국내외 기술 동 향", 2004. 2. 27.

[13] KISA, "전자서명 인증관리체계 OID 규격", 2001.

[14] KISA, "전자서명과 공인인증서비스", 2005. 10.

[15] TTAS.KO-12.0001/R1, "부가형 전자서명 방식 표준-제2부 : 인증서 기반 전자서명 알 고리즘", 2000.

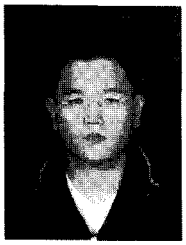
[16] TTAS.KO-12.0004, "128비트 블록암호 알고 리즘 표준", 1999.

[17] TTAS.KO-12.0012, "전자서명 인증서 프로 파일 표준", 2000.

[18] TTAS.KO-12.0013, "전자서명 인증서 효력 정지 및 폐지 목록 프로파일 표준", 2001.

[19] 법률 제5792호, "전자서명법", 1999. 2. 5.

[20] 법률 제6360호, "전자서명법 일부개정", 2000. 1. 16.



정 연 호 (Yeonho Jung)
2007년 2월 : 세종대학교 응용수학과 (학사)
2007년 ~ 현재 : 세종대학교 컴퓨터공학과 석사과정
관심분야 : 정보보호, 암호프로토콜 등

최 원 석 (wonsuk Choi)
2007년 2월 : 강남대학교 컴퓨터공학과 (학사)
2007년 ~ 현재 : 세종대학교 컴퓨터공학과 석사과정
관심분야 : 정보보호, 암호프로토콜 등

권 태 경 (Taekyoung Kwon)
종신회원
1992년 2월 : 연세대학교 컴퓨터과학과 학사
1995년 2월: 연세대학교 컴퓨터과학과 석사
1999년 8월: 연세대학교 컴퓨터과학과 박사
1999년 ~ 2000년 : U.C. Berkeley Post-Doc.
2001년 ~ 현재 : 세종대학교 컴퓨터공학과 부교수,
정보보호학회 논문지편집위원 및 이사
관심분야 : 정보보호, 암호프로토콜, 컴퓨터네트워크 등

이 광 수 (Gwangsoo Rhee)
종신회원
1981년 2월 : 서울대학교 계산통계학과 졸업
1986년 12월 : 워싱턴대학교 컴퓨터과학과 석사
1990년 5월 : 워싱턴대학교 컴퓨터과학과 박사
1990년 ~ 현재 : 숙명여자대학교 정보과학부 교수
관심분야 : 계산이론, 정보보호