通信情報保護學會誌
第9券 第3號, 1999. 09

전자서명 인증관리센터 구축 및 운영

최 영철, 오 경희, 이 재일, 홍 기융, 이 홍섭

요 약

금년 7월 1일 전자서명법의 시행과 함께 출범한 국가최상위 인증기관(Root CA)인 전자서명 인증관리센터는 공개키기반구조(Public Key Infrastructure, PKI)에 기반한 전자서명 인증관리체계의 구축·운영, 공인인증기관에 대한 인증서 발급 및 관리 등의 인증업무를 수행함으로써 전자서명 인증관리체계의 안전·신뢰성 확보와 전자서명 인증제도 및 전자문서 이용 활성화 기반 조성에 이바지함을 주요 임무로 한다. 본 고에서는 전자서명 인증서비스, 전자서명법 제정·시행, 최상위인증기관 및 공인인증기관 구축·운영 등에 대한 국내외 현황을 분석·제시하고 국내 전자서명 인증관리체계, 전자서명 인증관리센터 구축 현황 및 운영에 대하여 기술한다.

Ⅰ. 서 론

최근 인터넷과 같은 컴퓨터 네트워크 기술이 발전함에 따라서 민간이나 정부 분야에서의 전자적 거래(Electronic transaction)가 급증하고 있다. 전자적 거래를 명확하게 정의하기는 어려우나 개념적으로 고찰하자면, 전자적 문서의 온라인 결재 또는 전자적 상행위를 위한 거래 및 이에 따른 온라인 결제 등으로 그 범주를 구분해 볼 수 있을 것이다. 컴퓨터 네트워크를 통한 원격지간의 비대면 거래 방식은 시대가 흐름에 따라 피할 수 없는 현실이 되었으며, 현재 세계 선진 각국은 이러한 현실을 직시하고 이에 대한 대비책으로서 법·제도의 제정 및 정비에 노력하고 있다. 결국, 21세기 전자적 거래의 활성화를 위해서는 기술의 지속적인 발전과 함께 범정부적 차원의 법·제도의 제정 및 정비가 반드시 필요하며, 전자서명법 제정은 이것의 한 예라고 볼 수 있다.[19]

전자서명법은 비대칭형(공개키, 이하 공개키라 칭함) 암호기술을 기반으로 하는 전자서명(Digital Signature)에 법적 인감과 동일한 효력을 부여함으로써, 컴퓨터 네트워크를 통한 온라인 전자결재(또는 전자결제) 등과 같은 전자적 거래를 촉진케 할 수 있는 제도적 기반 마련을 목적으로 한다. 이때, 사용자는 법적효력을 갖는 전자서명을 수행하기 위해서 반드시 공인인증기관으로부터 자신의 전자서명검증키에 대한 인증서를 발급받아야 한다. 전자서명법은 이러한 공인인증기관 지정·운영에 대한 내용을 포함하고 있으며, 한국정보보호센터(이하 "전자서명 인증관리센터"라고 칭함)로 하여금 공인인증기관 지정을 위한 실질심사와 지정된 공인인증기관에 대한 인증서 발급 및 관리 업무를 수행하도록 하고 있다.[24]

전자서명 인증관리센터는 최상위 인증기관(Root CA)의 역할을 수행하는 기관으로서 전자서명 인증관리체계 구축·운영 및 공인인증기관에 대한 인증서 발급 및 관리를 통하여 전자서명 인증관리체계의 안전·신뢰성 확보와 전자서명 인증제도 및 전자문서 이용 활성화 기반 조성에 이바지함을 주요 임무로 한다. 전자서명 인증관리센터의 업무를 보다 구체적으로 고찰하자면 인증관리체계 구축 및 총괄 관리, 공인인증기관에 대한 인증 업무 수행, 공인인증기관의 안전 운영 지원, 정부의 상호인정 지원 및 외국 최상위 인증기관과의 상호인증, 인증관련 기술

한국정보보호센터(Korea Information Security Agency) 최영철(ycchoi@kisa.or.kr), 오경희(khoh@kisa.or.kr), 이재일(jilee@kisa.or.kr), 홍기융(kyhong@kisa.or.kr)

개발 및 보급 등을 들 수 있다.
본 고는 전자서명법 시행을 위하여 필수적으로 구축되어야 할 전자서명 인증관리센터의 구축 및 운영을 기술적·정책적 관점에서 기술함을 목적으로 하고 있다. 전체적인 구성내용을 살펴보면 다음과 같다.

제2절은 인증 서비스에 대한 정의 및 개념을 정리하고, 현재의 국내외 현황에 대한 기술소개를 함으로써 전자서명 인증관리체계의 전반적 이해를 돕고자 한다. 제3절에서는 공인인증기관의 필요성 및 국외현황을 파악·분석하고, 공인인증기관 지정기준 등에 대한 내용을 기술한다. 제4절은 인증관리센터의 임무 및 기능, 주요 수행업무, 인증관리센터의 시스템 구축 및 운영 등에 관련된 내용을 소개하고자 한다. 마지막으로 제5절에서 결론을 맺는다.

Ⅱ. 인증(Certification) 서비스

본 절에서는 전자서명 인증관리센터의 구축 배경이 되는 인증 서비스 전반에 관한 내용을 기술하고자 한다.

1. 인증의 정의

최근 자주 언급되고 있는 인증은 일반적으로 크게 두 가지 의미로 나뉘어 사용되고 있다. 첫 번째는 전자서명을 통해 구현될 수 있는 사용자 인증이나 메시지 인증을 의미하는 「인증(Authentication)」이고, 두 번째는 공개키 암호방식에서 공개키 무결성의 보장을 의미하는 「인증(Certification)」이다. 물론 공개키에 대한 「인증(Certification)」이라는 것이 인증받고자 하는 정보(공개키의 소유자 정보, 공개키)에 대하여 제3의 신뢰기관(인증기관)이 전자서명을 함으로써 이루어지는 것이기 때문에 「인증(Authentication)」을 포함한다고 생각할 수도 있다. 일각에서는 「보증(Certification)」이라고 정의함으로써 「인증(Authentication)」과 구별을 하기도 하지만, 일반적으로 혼용되고 있는 상태이다. 본 고에서 언급하고 있는 인증 서비스는 「인증(Certification)」 서비스를 언급하는 것이며, 이것은 「인증(Authentication)」과는 다소 구분된다.

인증 서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 안전한 전자상거래 환경의 구축을 위해서는 서두에서도 언급한 바와 같이 인증, 무결성, 비밀성, 부인방지 등의 정보보호 서비스가 필요하게 되며, 인증, 무결성, 부인방지 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다.[20] 현재 안전성을 다소 정량화 시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증서비스가 필요하게 된다. 인증기관은 전자서명을 이용하고자 하는 사용자들에 대해 인증서 발급 서비스를 제공해 줌으로써 이윤을 창출하거나 기업내 안전한 전산망 구축을 담당하는 하나의 조직을 일컫는 것이며, 인증 서비스란 인증기관이 제공해주는 인증서 발급, 인증서 관리 등 일련의 인증 관련 서비스를 통칭하는 것이라고 말할 수 있다.[2]

2. 인증 서비스 분류

인증 서비스의 분류는 인증기관이 발급하는 인증서의 응용 분야에 따라서 나뉘어진다. 현재 정보통신망의 급속한 발전으로 말미암아 대부분의 영역에서 정보보호 필요성이 대두되고 있으며, 이것에 대한 해결책으로서 암호기술의 사용이 권장되고 있다. 이중에서도 공개키 암호 알고리즘을 이용한 전자서명 기술의 활용은 인증, 무결성, 부인방지 등의 정보보호 서비스를 제공해주는 효과적인 솔루션으로 자리잡고 있다. 이러한 배경으로 인하여 컴퓨터 네트워크 보안과 관련된 많은 국제 표준화 단체나 개발 업체들이 공개키 암호 기술이 적용된 프로토콜이나 제품들을 출시하고 있는 상태이며, 이것은 상업적 목적을 갖는 인증기관 탄생의 기반이 되었다.

일반적으로 인증 서비스는 두 가지 분류로 나뉘어진다. 첫 번째는 상기에서 언급한 바와 같이 범용 보안 프로토콜의 확산으로 인해 요구되는 인증 서비스로서, 이 경우 인증기관은 각 객체(Entity)들에 대해 인증서를 발급하고, 이에 대한 수수료를 받음으로써 경제적 이득을 취하게 된다. 두 번째는 안전한 인트라넷(Intranet)·익스트라넷(Extranet) 네트워크 시스템, 폐쇄(Closed) 네트워크 시스템 등의 구축을 위해 요구되는 인증 서비스로서, 이 경우 사업자는 인증서 발급에 대한 수수료를 목적으로 하는 것이 아니라 자사의 안전한 네트워크 환경 구축을 목적으로 한다.

전자의 예로는 미국의 VeriSign 인증기관, 남아프리카 공화국의 Thawte 인증기관 등에서 제공하는 S/MIME(Secure Multi-purpose Internet Mail Extension), SSL(Secure Socket Layer) 인증 서비스를 들 수 있다.[21][23]

3. 인증서비스 현황

인증 서비스는 앞 절에서 고찰한 바와 같이 크게

두 가지로 대별된다. 본 고에서는 특정 도메인에서 안전한 네트워크 환경 구축을 위해 제공되는 인증 서비스는 현황 파악에서 배제하고, 일반적인 범용 인증 서비스 제공 업체들을 중심으로 살펴본다. 표 1은 현재 세계적으로 가장 널리 알려진 VeriSign 사의 인증 서비스를 기반으로 분류한 것이다.[23]

표 1. 인증 서비스 종류

종 류	용 도
S/MIME	안전한 전자메일용(암호화 · 전자서명) 인증서
SSL	웹 보안 프로토콜인 SSL을 웹 서버에 적용하기 위해 필요한 인증서(미국외 512비트)
Global 서버 ID	미국외에서 강한 SSL을 사용하고자 하는 경우 필요한 인증서(1024비트,미국 상무부의 허가 필요, 금융권으로만 제한)
OFX를 위한 금융서버 ID	OFX 프로토콜 적용에 필요한 인증서
EDI 서버 ID	안전한 EDI 구현에 필요한 인증서
MicroSoft AuthenticCode	OCX, CLASS, CAP 등 마이크로소프트사에서 제공하는 기술을 사용하여 제작한 S/W의 온라인 판매시 사용되는 인증서
Netscape Object Signing	JavaScript, Java 등으로 제작된 S/W의 온라인 판매시 사용되는 인증서
SET	SET 프로토콜 구현에 사용되는 인증서

※ SSL(Secure Socket Layer)
S/MIME(Secure Multi-purpose Internet Mail Extension)
OFX (Open Financial Exchange)
SET(Secure Electronic Transaction)

4. 인증 관련 업체 현황

인증기관은 일반적으로 인증 서비스를 행하는 업체나 조직을 말하는 것이나, 본 고에서는 개발 업체와 서비스 업체로 분류하여 인증기관 서비스 업체 및 관련 개발 업체 등을 동시에 고찰함으로써 전체적인 현황 파악을 용이케 하고자 하였다.

최근에는 개발 업체가 서비스 업체의 역할도 수행하는 등 그 구분이 모호해지고 있으나, 현재까지는 개발 및 서비스 업체가 분류될 수 있는 상태라고 사료된다.

4.1 국내 현황

1) 국내 인증 서버 개발 업체 현황

국내 개발 업체들은 현재 SSL이나 S/MIME용 인증서 발급이 가능한 인증 서버(CA 서버)를 개발한 상태이며, 아직까지는 다양한 인증서 발급 서비스(예: IPSEC, OFX 등)들을 지원하는 인증 서버는 개발되지 않은 상태이다. 현재 국내 인증 서버 개발 현황은 시장 형성 초기 단계이며, 향후 지속적인 발전이 있을 것으로 사료된다. 표 2는 국내 인증 서버 개발업체 현황을 파악한 것이다.

표 2. 국내 인증 서버 개발 업체 현황

업체명	제품명
소프트포럼	SFCA V2.5
이니텍	이니텍 CA V2.5
장미디어 인터랙티브	JMI CA V2.0
에버 소프트	Es-CA
LG-EDS	SmarCA
삼성SDS	TrustPro
펜타시큐리티	ISSAC

2) 국내 인증 서비스 업체 현황

현재 국내에서 상업적 목적을 가지고 공식적으로 인증서 발급 서비스를 수행하고 있는 업체는 SET 지불 시스템을 구축 · 운영하고 있는 일부 업체들과 범용 인증 서비스를 제공코자 최근 사업을 개시한 몇 개 업체에 지나지 않고 있다. 특히, SET의 경우에는 일부업체가 사업을 포기하고 있는 등 SET 사업의 난항으로 인하여 현재까지 크게 활성화되고 있지는 못한 상태이다. 표 3은 현재까지의 국내 인증 서비스 업체 현황이다.

표 3. 국내 인증 서비스 제공 업체 현황

업체명	인증 서비스	인증 서버
한국통신	SET 인증서	GTE CyberTrust
커머스넷코리아 (Commerce Net Korea)	SET 인증서	IBM Registry
메타랜드	SET 인증서	자체개발
한국전자인증(주)	SSL, S/MIME 등	

4.2 국외 현황

1) 국외 인증 서버 개발 업체 현황

현재 국외에는 수 많은 개발업체들이 있으며, 이러한 업체들은 인증 서버 개발 뿐만이 아니라 공개키 기반구조(Public Key Infrastructure) 구축을 위한 토탈 솔루션을 제공하고 있다. 또한, 여러

가지 인증서 발급이 가능하도록 다양한 인증 서버들을 제공하고 있다. 표 4는 국외 인증 서버 개발 업체 현황 개요이다.

2) 국외 인증 서비스 제공 업체 현황

현재 세계 각국에 많은 인증 서비스 업체들이 존재하며, 최근 그 수가 폭발적으로 증가하고 있는 추세이다. 초기에는 SSL이나 S/MIME용 인증서 발급 서비스로 국한되던 것이 현재는 EDI, IPSEC 등 다양한 프로토콜들을 위한 인증서 발급 서비스가 제공되고 있다. 기술이나 규모면에서 가장 앞서고 있는 서비스 업체는 미국의 VeriSign사로서 다양하고 폭넓은 서비스를 제공하고 있으며, 국내에서 SSL 보안 프로토콜을 사용하는 많은 가상쇼핑몰 업체들도 VeriSign사의 인증 서비스를 활용하고 있는 상태이다.

또한, 미국의 경우 현재 유타 주 정부에서는 3개의 공인인증기관(DST,ARCANVS,USERTRUST), 워싱턴 주 정부에서는 2개의 공인인증기관(VeriSign, ID Certify), 텍사스 주 정부에서는 1개의 공인인증기관(VeriSign)을 지정한 상태이다.[30][31]

표 5는 국외 인증 서비스 현황을 요약한 것이다.

표 4. 국외 인증 서버 개발 업체 현황

국가	업체명	제품명
일본	Hitachi	Certificate Authority 01-00
	Fujitsu	CommerceSTAGE Secure Certificate Authority v1.0
캐나다	Entrust Technologies	Entrust CommerceCA WebCA
미국	GlobeSet	GlobeSet CA v1.2
	GTE Cybertrust	CyberTrust Certificate Management Systems
	IBM	IBM Registry
	Certco	Root Certauthority Commerce Certauthority

표 5. 국외 인증 서비스 제공 업체 현황

국가	회사명	특징
미국	Digital Signatur Trust Company	유타주정부 공인인증기관
	ARCANVS	유타주정부 공인인증기관
	USER TrustCompany	유타주정부 공인인증기관
	ARINC	컨설팅 및 구축 서비스
	VeriSign	인증서 발급 및 PKI 솔루션 제공
영국	Trustwise	인증서 발급 서비스
프랑스	Certplus	인증서 발급 서비스
일본	VeriSign Japan	인증서 발급 및 PKI 솔루션 제공
대만	HiTRUST	인증서 발급 서비스
남아공	SACA	인증서 발급 서비스
	Thawte	인증서 발급 서비스

Ⅲ. 인증(Certification) 서비스

본 절에서는 공인인증기관에 대한 필요성 및 역할에 관하여 고찰하고, 국외 공인인증기관에 대한 현황을 면밀히 분석함으로써 전자서명 인증관리체계에서의 공인인증기관 개념을 보다 명확히 이해할 수 있도록 한다.

1. 필요성 및 역할

1.1 필요성

앞절에서 고찰한 바와 같이 안전한 전자적 거래를 위해서는 인증 서비스가 필수적으로 요구된다. 즉, 인증기관의 인증 서비스 없이는 컴퓨터 네트워크를 통한 전자결재(또는 전자결제), 전자계약 등의 전자적 거래가 불가능할 수 밖에 없게 된다. 하지만, 이것이 단지 인증기관의 인증 서비스가 있다고 해서 모든 것이 해결되는 것만은 아니다. 현재 법률적 문서 체계에서 공식적인 법적 계약 또는 거래는 반드시 사용자의 인감을 이용하게 되어 있다. 이러한 문제는 인증 서비스에서도 동일하게 적용된다. 컴퓨터 네트워크를 이용하는 사용자들은 다양한 인증기관으로부터 인증 서비스를 받을 수 있다. 즉, 사용자들은 여러 개의 전자서명생성키와 이에 대응되는 인증서(전자서명검증키 내포)를 소유할 수 있다. 하지만, 법적으로 인정받을 수 있는 전자서명을 하기 위해서는 일반 인감과 같이 공식적으로 공인된 기관으로부터 인증 서비스를 받아야만 할 것이다. 이것은 결국 공인된 인증기관이 필요하게 되는 것을 의미하는 것

이며, 이러한 공인인증기관은 안전·신뢰성있는 서비스를 수행할 수 있는 능력을 가져야만 한다.

1.2 역할

공인인증기관은 사용자의 전자서명검증키에 대한 무결성 보장과 신분정보의 표시를 위한 인증서 발급 서비스를 제공한다. 물론 공인이 아닌 일반적인 인증기관도 이러한 역할을 수행하지만, 공인인증기관은 사용자에 대한 신원확인 방법, 인증관리체계의 안전·신뢰성 등이 보다 더 뛰어나야만 한다. 이것은 공인인증기관에서 발급한 인증서는 인감과 같은 법적효력을 같기 때문에 해당 공인인증기관은 법에서 정의하는 특별한 요구조건을 만족해야만 하기 때문이다.

공인인증기관의 주요 역할은 인증서 발급, 인증서 효력정지 및 폐지, 인증서 갱신, 인증서 공고 등 인증서 발행 및 관리에 관한 전반적인 업무를 수행하는 것이다. 여기서 공인인증기관의 특징은 인증서 발급시 철저한 사용자 신원확인을 해야 하며, 이후 법에서 정의하고 있는 안전·신뢰성있는 방법으로 인증서 관리 업무를 수행해야만 한다.

2. 국외 공인인증기관 현황

2.1 미국 유타 주 정부

1) DST(Digital Signature Trust)

DST는 유타 주 최초(세계 최초)의 공인인증기관으로서 1996년에 미국 Zions First National Bank의 자회사로 설립되었다. DST는 유타 주 정부의 전자서명법 시행을 위해 저장소(Repository) 서비스를 대행하였으며, 이후 공인인증기관과 공인 저장소로 지정되었다.[14]

2) ARCANVS

유타 주 2번째 공인인증기관으로서 초기 PGP (Pretty Good Privacy)에 대한 인증 서비스를 제공하고자 하였다. 그러나, 최근 라이센스를 갱신하면서 인증 서비스의 종류를 개인용 인증서, HIPAA (Health Insurance Portability and Accountability Act) 사용자용 인증서, 공증기관·등록기관용 인증서, 서버용 인증서를 발급해주는 인증 서비스로 그 기능을 확대하였다. 표 6은 현재 ARCANVS에서 제공하고 있는 인증 서비스를 정리한 것이며, 신청정보는 해당 인증서를 발급받기 위해 필요한 정보의 종류와 수를 의미하는 것이다. 신청정보중 공증은 레벨이 높은 인증서를 발급받는 경우 필요한 정보로서 「Crypto」는 일반 공증이 아닌 ARCANVS 에서 제공하는 「CryptoNotary」 서비스를 이용하는 것을 의미하며, 「○」는 일반 공증 서비스를 이용하는 것을 말한다.[15]

3) USERTRUST

USERTRUST 네트워크는 디지털 인증서/디지털 ID/디지털 서명과 인터넷 보안 솔루션 및 어플리케이션을 제공하기 위해 전략적 제휴로 구성되었다. 제휴 관련 회사와 각 사의 기능 및 역할은 표 7과 같다. 현재 USERTRUST 네트워크가 제공하는 인증 서비스 종류 및 가격은 다음 표 8과 같다.[16]

표 6. ARCANVS 인증 서비스 종류 및 가격

인증서 종류		신청 정보				
		Email 주소	증명서 갯수	크레디트카드 정보	생체 정보	공증
개인용	Platinum	○	3	2	○	Crypto
	Gold	○	2	2	×	Crypto
	Silver	○	1	1	×	○
	Copper	○	1	1	×	×
HIPAA 사용자용	Personal	○	2	×	×	○
	Organization	○	3	×	×	○
	Credentialed Personal	○	다양	×	×	○
	Credentialed Organization	○	다양	×	×	○
등록 기관용	CryptoNotary	○	3	×	×	○
	RA	○	3	×	×	○
서버용	Web Server	○	3	×	×	○
	HIPAA Secure Server	○	3	×	×	○

표 7. USERTRUST 컨소시움 구성표

회사명	역할 및 기능
USERTRUST	PAA(Policy Approved Authority)
USERFirst	CA, Repository
DATACorp	IA(Issuing Authority) RA(Registration Authori AA(Authenticate Author SA(Service Authority)

표 8. USERTRUST 네트워크 인증 서비스

구 분		금 액	
		인증서발급	인증서갱신
일반 사용자용 (S/MIME E-mail)	Bronze Class	$19.99/년	$19.99/년
	Silver Class (예정)	$49.99/년	$49.99/년
	Gold Class (예정)	$59.99/년	$59.99/년
	Crown Class (예정)	$69.99/년	$69.99/년
SSL 서버용		$299/개	$249/개
코드개발자용(예정)		$99/개	$59/개
Date/Time Stamp 용(예정)		$99/개	$59/개

2.2 미국 워싱턴 주 정부

1) ID Certify

ID Certyfy사는 워싱턴 주 정부 최초의 공인인증기관으로서 1998년 4월 지정되었다. ID Certify사는 가입자에게 스마트카드를 제공함으로써, 사용자의 전자서명생성키를 스마트카드에 보관케 한다. 현재, 미네소타 주의 의료 및 보건 부문에 관련된 인증서비스를 제공중이다. 주요 인증 서비스는 Global Passport Certificate, National Passport Certificate, Corporate Passport Certificate, Professional Passport Certificate, Signature Passport Certificate, Transactional Passport Certificate 발급 서비스이다.[17]

ID Certify사는 저장소를 캐나다 뱅쿠버에 두고 있으며, RA(Registration Authority)를 관련 업체에게 제공하는 방식으로서 운영된다. 전체적인 인증관리체계는 다음 그림 1과 같다.

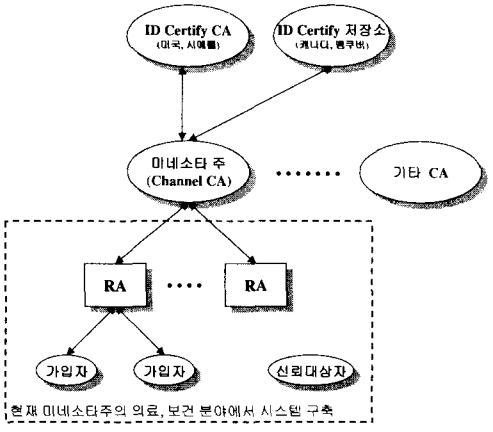

그림 1. ID Certify사 인증 서비스 체계도

2) VeriSign

VeriSign은 1995년 4월 RSA 사의 자회사로서 자본금 $22,789로 설립되었다. 초기 SSL과 S/MIME에 대한 인증 서비스를 주 사업 영역으로 하였으며, 점차적으로 인증 서비스를 다양화시켰다. VeriSign은 세계 인증 서비스를 주도하고 있는 사업체로서 전 세계에 많은 자회사 및 협력사들을 가지고 있으며, 1998년 8월 워싱턴 주 정부로부터 S/MIME Class3 (VeriSign 인증업무준칙 버전 1.2의 2.2.3)에 대해 공인 지정을 받았다. 또한, 1998년 10월에는 텍사스 주 정부로부터도 공인인증기관 지정을 받았다. VeriSign이 제공하는 인증 서비스 종류는 2절에서 설명된 표 2와 같다.

2.3 독일

1) 도이치 텔레콤 텔레섹(Deutsche Telecom Telesec)

1989년 설립된 도이치 텔레콤내 정보보호 전문조직으로 1998년 인증기관 허가를 받아 인증업무를 수행하고 있다. 조직 구조상 도이치 텔레콤내 본부의 멀티미디어 사무소 산하기관이나 인증업무의 독립성 확보를 위하여 본부조직으로 독립적으로 운영되고 있다.[18]

Ⅳ. 전자서명 인증관리센터

본 절에서는 전자서명 인증관리센터의 임무 및 역할, 관련 시스템 구축·운영 등에 대한 내용들을 기술하고자 한다.

1. 전자서명 인증관리센터 임무 및 역할

전자서명법은 법령「제25조:전자서명인증관리업무」에서 전자서명 인증관리센터의 주요 역할을 다음과 같이 규정하고 있다.

"한국정보보호센터는 전자서명을 안전하고 신뢰성 있게 이용할 수 있는 환경을 조성하고 공인인증기관을 효율적으로 관리하기 위하여 공인인증기관의 전자서명검증키에 대한 인증, 전자서명인증기술의 개발 및 취급 기타 전자서명인증과 관련된 업무를 수행한다."

상기의 전자서명법 및 하위법령을 기반으로 하여 보다 더 구체적인 전자서명 인증관리센터의 주요 임무를 도출해 보면 다음과 같이 기술할 수 있다.

⊙ 전자서명 인증관리센터는 자체 시스템을 개발하고, 이를 안전하게 운영한다. 이를 위해서 전자서명

인증관리센터는 보안통제 정책을 수립하고, 이것의 정확한 이행업무를 수행한다. 이와 관련된 세부 업무는 다음과 같다.

- 전자서명 인증관리센터 인증시스템 설계, 개발, 구축 및 운영
- 전자서명 인증관리센터 물리적 보안통제 시스템 구축 및 운영
- 전자서명 인증관리센터 인증업무준칙 개발 및 제정·시행
- 전자서명 인증관리센터 안전 운영지침 개발 및 제정·시행

⊙ 전자서명 인증관리센터는 안전한 전자서명 인증관리체계의 운영을 위하여 전자서명 인증관리센터 시스템을 구축하고, 이를 사용하여 공인인증기관에 대한 인증서 발급업무를 수행한다. 인증서 발급과 관련된 세부 업무는 다음과 같다.

- 키생성 및 관리
- 인증서, 인증서 효력정지 및 폐지목록(CSL, CRL) 생성·관리
- 디렉토리 및 웹 운영
- 인증기록 DB화 및 문서관리
- 시점확인 서비스 제공 등

⊙ 전자서명 인증관리센터는 자체 시스템 개발의 노하우를 이용하여 각종 전자서명 인증기술 개발하며, 향후 이를 산업체 기술이전이나 국가 인증기반구조 구축의 기술로 활용함으로써 국가 경쟁력 강화를 제고한다.

- 국제 호환성 보장을 위한 전자서명 알고리즘 구현기술 연구
- 국제적 상호인증을 위한 상호연동성 기술 개발
- 효율적인 공개키 기반구조 구축 기술 개발

⊙ 전자서명 인증관리센터는 정보통신부 장관의 역할에 대한 위탁을 받아 공인인증기관 지정을 위하여 신청자의 기술적 능력, 보호설비, 관리적 능력 등 세부 지정요건의 구비여부 확인을 위하여 다음과 같은 내용의 실질심사 및 평가를 수행한다.

- 시스템 안전·신뢰성 평가
  - 키 생성 시스템
  - 인증서 생성 및 관리 시스템
  - 디렉토리 시스템
  - 시점확인 시스템
  - 웹 서버 시스템
- 전자서명모듈 안전·신뢰성 평가
- 물리적 보안대책 평가
- 인적 보안대책 평가
- 관리적 보안대책 평가
- 인증업무준칙 적합성 평가
- 네트워크 보안대책 평가
- 개인정보보호 대책 평가 등

그림 2는 상기에서 설명한 전자서명 인증관리센터 업무를 전체적으로 조감하고, 국내 전자서명 인증관리체계를 보여주고 있다.

전자서명법 및 하위법령을 기반으로 한 전자서명 인증관리센터의 주요 임무 및 기능은 전자서명 인증관리체계 구축 및 총괄 관리, 공인인증기관 지정을 위한 심사 및 평가, 공인인증기관 검사 및 안전운영 지원, 전자서명 인증기술개발 및 보급, 정부의 상호인정 지원 및 외국 최상위인증기관과의 상호인증 등이다. 그림 2는 상기에서 설명한 전자서명 인증관리센터 업무를 전체적으로 조감하고, 국내 전자서명 인증관리체계를 보여주고 있다.

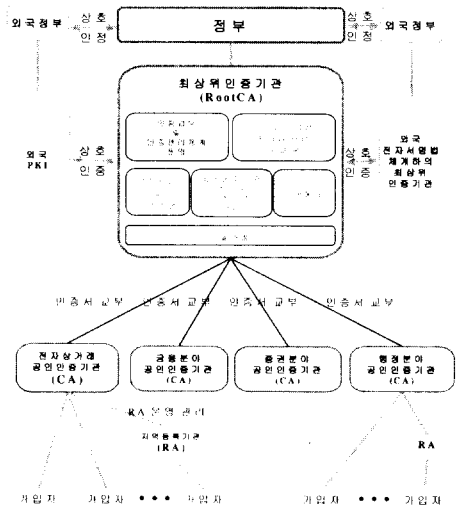

그림 2. 전자서명 인증관리체계

2. 전자서명 인증관리센터 시스템 구축

전자서명 인증관리센터 시스템 설계의 기본원칙은 안전·신뢰성의 보장이다. 전자서명 인증관리센터는 최상위 인증기관의 역할을 수행하는 인증기관으로서 공인인증기관에게 공인인증기관이 사용하는 전자서명생성키에 합치하는 전자서명검증키에 대한 인증서

를 발급해주는 업무를 수행한다. 그러므로, 전자서명 인증관리센터 시스템의 안전·신뢰성은 인증관리 체계 전반에 영향을 미칠 수 있는 중요한 요소이며, 이것은 시스템의 호환성 및 효율성 등과 더불어 중요하게 고려되어야 하는 요소이다. 다음은 인증관리센터 시스템의 안전·신뢰성을 위하여 지켜져야 할 기본원칙이다.

⊙ 엄격한 다단계 직무기반의 접근통제
  - 단독 실행이 불가능하도록 직무 분리
  - 키 생성 및 인증성 생성 업무 : 3인 이상
  - 기타 인증 업무 : 2인 이상
⊙ 네트워크 침입차단 및 침입탐지 체계 구축
⊙ 키 생성 및 관리시스템 등 중요 시스템은 오프라인 방식으로 구축
⊙ 핵심인증시스템의 이중화 운영 등

전자서명 인증관리센터 시스템은 크게 등록관리 시스템, 키 생성 시스템, 인증서 생성·관리 시스템, 디렉토리 시스템, 시점확인 시스템, 웹 서비스 시스템과 같이 분야별 주요 시스템으로 구성된다. 각 시스템별 기능은 다음 표 9와 같다.

표 9. 전자서명 인증관리센터 시스템 구성 및 기능

시스템 구성	기 능
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 자가서명 인증서(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

상기의 각 시스템은 물리적으로 서로 분리된 장소에서 운용되며, 각 시스템간의 자료 입·출력은 오프라인 방식으로 운영함으로써 전자서명 인증관리센터 시스템의 안전·신뢰성을 극대화시킨다. 각 시스템의 기능 및 논리적 구성도는 그림 3과 같다. 웹 서비스 시스템, 디렉토리 서비스 시스템, 시점확인 시스템은 외부 네트워크에 연결되어 공인인증기관이나 일반 사용자들에게 온라인 서비스를 제공하며, 나머지 시스템들은 안전·신뢰성의 향상을 위해 오프라인 방식으로 구성된다.

전자서명 인증관리센터 시스템은 각 시스템 부문별로 접근통제를 거쳐야만 동작 가능토록 운영되며, 각각의 접근통제는 철저한 역할분리 방식에 근간하여 운영된다. 또한, 각 시스템은 서로 다른 운영실에 설치·운영되고 각각의 시스템은 상호접속되지 않으며 잠금장치가 있는 보안캐비넷 내에 설치하여 물리적 및 관리적 측면에서 안전·신뢰성을 확보하고 있다. 전자서명 인증관리센터는 정책적으로 각 구역에 보안등급을 두어, 각 등급에 따라 물리적 보안 강도를 달리하여 다단계 통제가 가능토록 구축하였으며, 물리적 접근 통제방식으로서는 스마트카드 및 생체인식(지문인식 등) 기술을 이용한 접근통제 시스템을 갖추고 있다. 또한, 화재나 홍수 등과 같은 재난에 대비하여 인증서 등과 같은 중요한 데이터를 지역적으로 분리된 원격지의 안전한 저장소에 백업할 수 있는 안전·신뢰성 확보방안도 마련해 가고 있다.

3. 시스템 개발 적용기술 표준

전자서명 인증관리센터 시스템 구축에 적용된 표준들은 인증서 발행에 이용되는 전자서명 알고리즘부터 인증서나 인증서폐지목록을 저장·공고하는 디렉토리 서버까지 다양하고 광범위하게 적용되었다. 본 절에서는 전자서명 인증관리센터 시스템 구축에 적용된 전자서명 인증기술 표준에 대하여 기술함으로써, 전자서명 인증관리체계 구성의 이해를 돕고자 한다.

3.1 전자서명 알고리즘 구현 표준

인증서 발행 및 관리에 사용되는 전자서명 알고리즘은 공인인증기관들과의 상호연동성을 보장하기 위하여 RSA와 KCDSA를 사용한다. RSA 전자서명 알고리즘은 PKCS(Public Key Cryptography Standard) 표준을 준용하여 구현되었으며, KCDSA는 PKCS 구현 표준을 기반으로 하였고, 동시에 공개키와 비밀키 표현을 위하여 ASN.1을 추가적으로

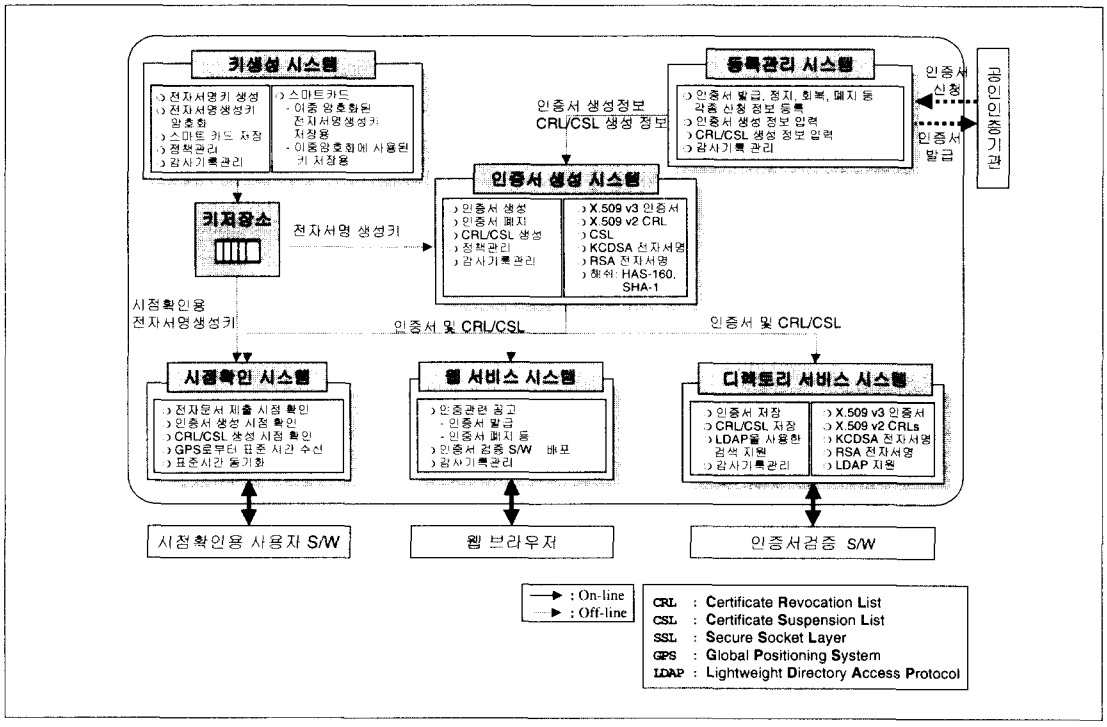

그림 3. 전자서명 인증관리센터 논리적 구성도

정의하였다. 또한, 전자서명에 사용되는 해쉬 알고리즘은 안전성을 고려하여 RSA인 경우에는 SHA-1을 사용하고, KCDSA의 경우에는 국내 단체 표준 알고리즘으로 등록된 HAS-160과 SHA-1을 사용한다. PKCS는 RSA 알고리즘의 구현방법론과 여러 가지 구문표현을 정의한 표준으로서 현재 전 세계적으로 많이 이용되고 있는 표준이다. PKCS는 1991년 3월 NIST/OSI Implementator's Workshop에서 문서 SEC-SIG-91-16으로 발표된 이후, 1993년 11월 1일 많은 수정을 거친 후 일관성 있는 문서 방식으로 개선되어 발표되었으며, 이후 지속적인 갱신과정을 거쳐 현재는 다음 표 10과 같은 현황을 가지고 있다.

표 10에서 가장 중요하게 인지되어야 할 표준은 PKCS#1, PKCS#7, PKCS#10 등이다. 여기서 PKCS#10은 공인인증기관이 인증서를 발급받고자 하는 경우 전자서명 인증관리센터에게 제출해야 하는 기본 형식이다. 다음은 PKCS 주요 표준을 구체적으로 설명한 것이다.

PKCS#1:RSA Encryption Standard

PKCS#1은 RSA 공개키를 이용해 데이터를 암호화시키는 rsaEncryption이란 방법에 대한 내용을 다루고 있다. 이러한 RSA 암호화는 PKCS#7에서 설명될 전자서명과 전자봉투(Digital Envelope)을 위해 사용된다. 또한, PKCS#1은 RSA 공개키와 비밀키를 위한 구문(syntax)을 정의하고 있다. 공개키 구문은 인증서에서 사용되며, 비밀키 구문은 일반적으로 암호화된 비밀키(PKCS#8)에 사용된다. 여기서 공개키 구문은 X.509 및 PEM에서의 구문과 동일하기 때문에 X.509/PEM RSA 키들은 PKCS#1에서도 사용될 수 있다. 또한, PKCS#1은 X.509/PEM 인증서, 인 증서폐지목록, PKCS #6의 확장된 인증서(extended certificate)를 위한 서명이나 X.400 메시지 토큰과 같은 전자서명을 위해서 세 가지의 서명 알고리즘(md2WithRSAEncryption,md4WithRSAEncryption,md5WithRSAEncryption)들을 정의하고 있다.[5]

PKCS#5:Password-Based Encryption Standard

PKCS#5는 패스워드로부터 파생된 비밀키(Secret Key)를 가지고 8진 스트링을 암호화시키는 방법을 설명한다. 이것은 PKCS#8에서 설명된 것처럼 한 컴퓨터에서 다른 컴퓨터로 비밀키들을 전송시키는

경우 그러한 키들에 대한 암호화를 응용 목적으로 한다.[6]

PKCS#6:Extended-certificate Syntax Standard
PKCS#6은 확장된 인증서들에 대한 구문을 설명한다. 확장된 인증서는 X.509 공개키 인증서와 속성들의 집합들을 포함한 서명문으로 구성된다. 이러한 확장된 인증서는 서명 검증과정을 통해 검증이 되며, PEM과 같은 응용을 위해 공개키 인증서만을 추출할 수 있다.[7]

PKCS#7:Cryptographic Mesage Syntax Standard
PKCS#7은 전자서명이나 전자봉투에 적용되는 일반적인 구문 표현에 대해 설명한다. PKCS #7은 PEM과 호환이 되며, 이것은 PKCS에서의 서명 등이 어떠한 변환 작업없이 PEM에서도 사용될 수 있다는 것을 의미한다. 물론, 이것의 역도 가능하다. 또한, PKCS#7에 따라 생성된 값들은 전형적으로 8진 스트링을 취하는 BER(Basic Encoding Rule) 인코딩이 된다.[8]

PKCS#10:Certification Request Syntax Standard
PKCS#10은 인증 요청서를 위한 구문을 정의한다. 인증 요청서는 식별자(distinguished name), 공개키, 그리고 선택사항인 속성들의 집합으로 이루어지며, 인증기관에 전송된다. PKCS#10의 초기 목적은 PKCS#7의 암호학적 메시지 지원을 위한 것이었으며, 다른 응용들도 개발될 것으로 기대된다.[9]

3.2 인증서·인증서 효력정지 및 폐지목록

전자서명 인증관리센터 시스템은 인증서 및 인증서폐지목록의 발행을 위하여 각각 X.509 버전3와 X.509 버전2를 준용한다. 인증서 형식은 1988년에 ITU-T가 X.509 버전1을 공표하고 1993년에 버전2를 공표했으며, 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동개발되어 왔다.[1] 현재에는 X.509 버전3이 제정되어 지금에 이르고 있다. 한편 IETF의 PKIX 표준화 작업의 일환으로서 인증서 및 인증서폐지목록에 대한 프로파일 표준이 올해 99년 1월 RFC 2459로 등록되었다.[2] RFC 2459는 ISO/IEC의 버전3와 거의 동일하나 인증서 확장영역 부분이 추가적으로 부가되었으며, 기타 몇 가지 ASN.1 형식도 첨가되었다. 현재 전자서명 인증관리센터는 ISO/IEC의 표준을 준용하고 있으며, 향후 RFC 2459의 인증서 확장영역도 지원해 나아갈 계획이다.

표 10. PKCS 구성 및 현황

구 분	제 목	버 전	일 시
PKCS# 1	RSA Encryption Standard	2.0	1998.10
PKCS# 3	Diffie-Hellman Key-Agreement Standard	1.4	1993.11
PKCS# 5	Password-Based Encryption Standard	2.0	1998.10
PKCS# 6	Extended-Certificate Syntax Standard	1.5	1993.11
PKCS# 7	Cryptographic Message Syntax Standard	1.5	1993.11
PKCS# 8	Private-Key Information Syntax Standard	1.2	1993.11
PKCS# 9	Selected Attribute Types	1.1	1993.11
PKCS#10	Certification Request Syntax Standard	1.0	1993.11
PKCS#11	Cryptographic Token Interface Standard	2.01	1997.12
PKCS#12	Personal Information Exchange Syntax Standard	1.0 (Draft)	1997. 4
PKCS#13	Elliptic Curve Cryptography Standard	Project	진행중
PKCS#14	Pseudorandom Generator Standard	Project	진행중

또한, 전자서명 인증관리센터는 인증서 효력정지를 위하여 인증서폐지목록을 활용한다. 즉, 인증서폐지목록의 사유코드(Reason Code) 부분중 certificate Hold 부분의 비트값을 사용함으로써 효력정지된 인증서도 인증서폐지목록에 함께 등재시킴으로써 인증서 효력정지를 수행한다. 다음 표 11, 표 12는 ISO/IEC 9594-8의 X.509 버전3 인증서, X.509 버전2 인증서폐지목록을 나타낸 것이다.

3.3 디렉토리 서비스

전자서명 인증관리센터 시스템은 인증서 및 인증서폐지목록의 공고를 위하여 디렉토리 서비스를 제공한다. 디렉토리 서비스를 위해 채택하는 표준은 X.500 디렉토리 서비스와 연동되는 LDAP (Light weight Directory Access Protocol) 기반의 디렉토리 서비스이다.[10][11][12] LDAP은 인터넷상에서의 디렉토리 서비스를 위해 개발되었으며, 현재 인터넷상의 디렉토리 서비스를 제공하는데 폭 넓게 사용되고 있다.

표 11. X.509 버전3 인증서

영역 이름	설명
version	인증서의 버전
serial number	인증서의 일련번호
signature algorithm id	인증서를 서명하는 데 사용하는 알고리즘 식별자
issuer name	인증서 발행자의 이름
validity period	인증서의 유효기간(유효 개시일과 종료일을 표시)
subject name	인증서 소유자의 이름
subject public key info	인증되는 공개키에 대한 정보(공개키가 사용될 알고리즘의 식별자와 공개키를 포함)
issuer unique identifier(선택)	발행자를 정확하게 표기하기 위해 사용되는 비트 스트링
subject unique identifier(선택)	소유자를 정확하게 표기하기 위해 사용되는 비트 스트링
extensions(선택)	표준단체나 사용자 조직에서 필요에 따라 정의할 수 있는 부분(확장영역의 이름과 critical 여부와 실질적인 값을 포함)
signature	위 영역에 대한 발행자의 서명값

표 12 X.509 버전2 인증서폐지목록

영역 이름	설명
version	CRL의 버전
signature	CRL을 서명할 알고리즘(algorithm identifier, parameters 영역을 포함)
issuer	CRL 발행자 이름으로 X.500 명명방식을 따름
this update	갱신일에 대한 타임스탬프
next update	다음 갱신일
revoked certificates	폐지된 인증서들의 목록
CRL extentions (선택)	위 영역외에 부가적인 정보를 선택적으로 기술함
issuer's signature	위 영역에 대한 발행자의 서명값

serial number	폐지된 인증서의 일련번호로 발행자에 대해 유일함
revocation date	인증서 폐지일로 UTCTime으로 표현됨
CRL entry extensions(선택)	폐지 이유등 부가적인 정보를 기술함

V. 결 론

전자서명법에 의거 전자서명 인증관리체계상 최상위 인증기관(Root CA)인 전자서명 인증관리센터는 안전한 전자서명 인증관리체계의 구축·운영 및 인증업무 수행, 전자서명 인증기술 개발 및 보급, 공인인증기관 지정을 위한 실질심사 및 평가, 공인인증기관 검사 및 안전운영 지원, 상호인정 및 상호인증체계 구축·운영 등과 같은 업무를 수행한다.

현재 전자서명 인증관리센터 시스템은 등록관리 시스템, 키 생성 시스템, 인증서 생성·관리 시스템, 디렉토리 시스템, 시점확인 시스템, 웹 서비스 시스템으로 구축·운영되고 있다. 공인인증기관에 대한 인증서 생성·발급을 위해서 국내 표준인 KCDSA 전자서명 알고리즘은 물론 국제적으로 널리 사용되고 있는 RSA를 모두 지원함으로써 다양한 인증 서비스 환경을 수용할 수 있도록 전자서명 인증관리체계를 구축하였다. 인증업무에 사용될 인증서 규격은 X.509 버전3 인증서 표준 규격을 준용하고, 인증서 효력정지 및 폐지목록은 X.509 버전2 인증서폐지목록 표준 규격을 준용하여 공인인증기관과의 상호 호환성이 보장되도록 하였다.

향후 전자서명 인증관리센터는 국내·외 전자상거래 환경 및 다양한 전자서명 인증 메커니즘·서비스들을 연계·수용하고 향후 국가간 상호인정 및 상호인증을 추진할 수 있도록 전자서명 인증관리체계를 지속적으로 운영·발전시켜 나아갈 계획이다.

참 고 문 헌

[1] ITU-T Recommandation X.509 (1997)| ISO/IEC 9594-8:1997, Information technology-Open Systems Interconnection-The Directory :Authectication Framework, 1997.

[2] RFC2459, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile",1999

[3] RFC2510,"Internet Public Key Infrastructure Certificate Management Protocol", March, 1999

[4] RFC2527, "Internet Public Key Infrastructure Certificate Policy and Cert ification Practies Framework", March, 1999

[5] PKCS#1 v2.0,"RSA Cryptography Standard",

Oct., 1998

[6] PKCS#5 v1.5,"Password-Based Encryption Standard", Nov., 1993

[7] PKCS#6 v1.5,"Extended Certificate Syntax Standard", Nov., 1993

[8] PKCS#7 v1.5,"Cryptographic Message Syntax Standard", Nov., 1993

[9] PKCS#10 v1.0,"Certification Request Syntax Format", Nov., 1993

[10] M.Wahl, T.Howes, S.Kille, "Lightweight Directory Access Protocol (v3)", RFC2251, 1997. 12.

[11] RFC2252, M.Wahl, A.Coulbeck, T.Howes, "Lightweight Directory Access Protocol(v3) :Attribute Syntax Definitions", 1997.12

[12] RFC2253, M.Wahl, S.Kille, T.Howes, "Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names", 1997. 12.

[13] American Bar Association, "Digital Signature Guidelines : Legal Infrastructure for Certification Authorities and Secure Electronic Commerce", August 1, 1996.

[14] "Digital Signature Trust Co." http:// www.arcanvs.com/arcanvsCPD.html",1999

[15] "ARCANVS",http://www.arcanvs.com, 1999

[16] "USERTRUST",http://www.usertrust.com, 1999

[17] "IDCertify",http://www.idcertify.com, 1999

[18] "도이치텔레콤",http://www.telesec.de, 1999

[19] McBride Baker & Coles, "Summary of Electronic Commerce and Digital Signature Legistration", "http://www.mbc.com/legis/"

[20] R.L. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", ACM, Vol.21, no.2, Feb. 1978, pp. 120-126

[21] "Thawte Digital Certificate Services", 1999, "http://www.thawte.com"

[22] "UMS",1998,http://www.cusys.edu/~security/users/policyhp.html

[23] "VeriSIgn", 1999, http:/www.verisign.com

[24] 법률제5792호, "전자서명법", 1999. 2. 5

[25] 덴마크 전자서명법,"Draft Bill for an act on Digital Signature", 1997, ttp:// www.fsk.dk/fsk/publ/elcom/kap02.htm

[26] 독일 전자서명법, "German Digital Signature ordinance (sigV)", July.7. 1997, http://www.kuner.com/data/sig/veroid04.htm

[27] 독일 전자서명법 시행령, "German Digital Signature ordinance (sigG)", June. 13.1997, http://www.kuner.com/data/sig/digsig4.htm

[28] 말레이시아 전자서명법, "Digital Signatu- re Bill 1997", 1997, http://www.cert.org.my/bill.html

[29] 법무부, "외국의 전자서명제도", 1997

[30] 유타주 전자서명법, "Digital Signature Administrative Rules", State of Utah, 1996, http://www.commerce.state.ut.us/web/commerce/digsig/act.htm

[31] 워싱턴주 전자서명법, "The Washington Electronic Authentication Act(EAA)", State of Washington, June 11, 1998, http://www.wa.gov/sec/ea/dsrcw.htm

[32] BSI Manual for Digital Signatures- on the basis of the Digital Signature Act(SigG) and the Digital Signature Ordinance(SigV)- Version 1.0, November 18, 1997.

著者紹介

최 영 철(Youngchul Choi) 정회원

1996년 2월 : 성균관대학교 정보공학과 학사

1998년 2월 : 성균관대학교 전기·전자·컴퓨터공학부 석사

1998년 1월~현재 : 한국정보보호센터 연구원

<관심분야> 암호학, 전자상거래 보안, 공개키기반구조

오 경 희(Kyeonghee Oh) 정회원

1988년 8월 : 서강대학교 전산학과 학사

1992년 2월 : 한국과학기술원 전산학과 석사

1992년 10월~1996년 12월 : 한국통신연구소 연구원

<관심분야> 전자상거래 보안, 공개키기반구조, 정보시스템 감사, 보안관리, 위험분석

이 재 일(Jaeill Lee) 정회원

1986년 2월 : 서울대 계산통계학과 석사
1988년 2월 : 서울대 계산통계학과 계산학전공 석사
1991년 1월~1996년 6월 : 한국IBM 연구원
1996년 7월~현재 : 한국정보보호센터 선임연구원

<관심분야> 전자상거래 보안, 전자서명 인증, 공개키기반구조, 네트워크 보안

홍 기 윰(Ki-Yoong Hong) 종신회원

1985년 2월 : 전남대학교 전자계산학과 학사
1990년 2월 : 중앙대학교 전자계산학과 석사
1996년 2월 : 아주대학교 컴퓨터공학과 박사
1994년 8월 : 정보처리기술사
1985년 9월~1995년 10월 : ETRI 선임연구원
1992년 9월~1993년 6월 : Italy Alenia Spazio사 선임연구원
1995년 10월~1996년 4월 : 한국전산원 선임연구원
1996년 4월~1999년 현재 : 한국정보보호센터 인증관리팀장

<관심분야> 컴퓨터·네트워크 보안, 정보보호시스템 평가, 정보보호표준화, 전자상거래 보안, 전자서명 인증, 공개키기반구조(PKI)

이 홍 섭(Hongsub Lee) 종신회원

한양대학교 전자공학과 학사
한양대학교 전자공학과 석사
대전대학교 컴퓨터공학 박사
1990년~1996년 : 한국전자통신연구원 실장
1996년~현재 : 한국정보보호센터 연구개발부장, 기술본부장,인증관리센터구축준비반장, 기술개발부장, 정보통신기술협회 정보보호기술위원회 의장, 한국정보통신 정보보호학회 상임이사

<관심분야> 시스템 및 네트워크 정보보호