전자서명법과 전자서명 인증관리체계

한국정보보호센터 최영철 · 홍기융* · 이홍섭

1. 서 론

최근 인터넷과 같은 컴퓨터 네트워크 기술이 발전함에 따라서 민간이나 정부 분야에서의 전자적 거래(Electronic transaction)가 급증하고 있다. 컴퓨터 네트워크를 통한 원격지간의 비대면 거래 방식은 시대가 바뀜에 따라 피할 수 없는 현실이 되었으며, 현재 세계 선진 각국은 이러한 현실을 직시하고 이에 대한 대비책으로서 관련 기술개발 및 제도 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.

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. 이 때, 사용자는 법적효력을 갖는 전자서명을 수행하기 위해서 반드시 공인인증기관으로부터 자신의 전자서명검증키에 대한 인증서를 발급받아야 한다. 전자서명법은 이러한 공인인증기관 지정 · 운영에 대한 내용을 포함하고 있으며, 전자서명인증관리센터로 하여금 공인인증기관 지정을 위한 실질심사와 지정된 공인인증기관에 대한 인증서 발급 및 관리 업무를 수행하도록 하고 있다.

* 종신회원

전자서명인증관리센터는 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 개발 및 보급 등을 들 수 있다.

2. 전자서명 인증기술

2.1 전자서명의 개념

컴퓨터 네트워크를 통한 비대면 방식의 전자적 거래는 대면방식의 기존 거래 방식의 단점을 극복할 수 있게 한다. 전자적 거래는 기존 거래 방식에서 시간적 · 공간적 제약의 문제점을 해결해 줌으로써 새로운 거래 문화로서 자리잡아 가고 있다. 그러나, 전자적 거래는 많은 순기능이 있음에도 불구하고, 사용자에게 역기능을 제공할 수 있다는 문제점 때문에 보안 요구사항이 선결되어야만 전자적 거래의 활성화를 기대할 수 있을 것이다. 정보보호 역기능을 방지하기 위하여 필요한 대표적인 정보보호 서비스는 표 1과 같다.

전자서명은 상기의 보안 요구사항중 인증, 무결성, 부인방지에 대한 보안 기능을 제공해 주며, 이것은 결국 비대면 방식의 전자적 거래 환경 구

표 1 정보보호 서비스 분류

구분	내용	필요 기술
인증 (Authentication)	사용자 인증 : 정당한 사용자 메시지 인증 : 메시지 진정성	전자서명
무결성 (Integrity)	메시지 진정성	전자서명
비밀성 (Confidentiality)	정당한 사용자만이 메시지 확인 가능	암호화
부인방지 (Non-repudiation)	메시지 작성 또는 송·수신에 대한 부인 불가능	전자서명

축시 전자서명 기술이 필요하다는 것을 의미하는 것이다.

일반적으로 전자서명은 크게 두 가지 의미로 나뉘어질 수 있다. 첫 번째는 광의의 전자서명으로서 「Electronic Signature」를 의미하는 것이며, 두 번째는 협의의 전자서명으로서 「Digital Signature」를 말하는 것이다. 전자의 가장 일반적인 예는 전자펜을 이용한 그래픽 기반의 서명 방식이다. 최근 선진 각국에서 시행 또는 제정중에 있는 전자서명법은 일반적으로 후자의 개념을 법적으로 인정하고 있으며, 이것은 전자의 방식이 안전·신뢰성 측면에서 많은 취약점을 가지고 있기 때문이다. 다음 표 2는 「Electronic Signature」와 「Digital Signature」를 안전·신뢰성 측면에서 비교·분석한 것이다.

표 2 「Electronic signature」와 「Digital signature」의 비교

구분		Electronic signature	Digital signature
내용		전자펜을 이용한 수기서명 모사방식의 전자서명	공개키 암호기술을 이용한 진자서명
진정성 비교	서명자인증	불만족	만족
	위조불가	불만족	만족
	변경불가	불만족	만족
	부인불가	불만족	만족
전체적인 안전성		안전성에 대한 객관적 증명이 어려움	안전성에 대한 정량화 접근방식의 증명이 가능

2.2 전자서명 인증의 필요성

인증(Certification) 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. 현재 안전성을 정량화 시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것의 실제 적용을 위해서는 인증 서비스가 필요하게 된다.

인증기관은 전자서명을 이용하고자 하는 사용자들에 대하여 전자서명검증키(공개키)가 해당 사용자의 소유임을 증명하고 또한 해당 키가 위·변조 되지 않았다는 사실을 증명하기 위하여 전자서명검증키와 사용자 정보 등으로 구성된 데이터에 전자서명을 수행함으로써 인증서를 생성한다. 결과적으로 인증기관이라 함은 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.

3. 국내·외 전자서명 인증정책 및 법·제도 현황

3.1 국내 현황

전자서명법은 공개키 암호기술을 기반으로 하는 전자서명에 법적 인감과 동일한 효력을 부여함으로써, 컴퓨터 네트워크를 통한 온라인 전자결제(또는 전자결제) 등과 같은 전자적 거래를 촉진케 할 수 있는 제도적 기반 마련을 목적으로 한다. 이 때, 사용자는 법적효력을 갖는 전자서명을 수행하기 위해서 반드시 공인인증기관으로부터 자신의 전자서명검증키에 대한 인증서를 발급받아야 한다.

국내에서는 지난 1998년도부터 전자서명법 제정 작업이 추진되어 1999년 2월 5일자로 전자서명법이 법률 제5,792호로 공포되었으며, 동년 6월

30일에는 대통령령 제16,457호로 전자서명법 시행령이 발표되었다. 그리고, 동년 7월 1일에는 전자서명법이 시행되었으며, 7월 7일에는 전자서명법의 원활한 시행을 위하여 전자서명 인증관리센터가 한국정보보호센터내에 설립되었다.

3.2 국외 현황

미국의 유타주는 세계 최초로 1995년 전자서명법을 제정·시행하기 시작했으며, 이후 미국의 40개주, 독일('97년), 이탈리아('98년), 말레이시아('97년), 싱가폴('98년) 등이 뒤를 잇고 있다. 한편 각국 전자서명법제의 상이함으로 인하여 전자서명이 국제적으로 통합되어 사용되는데 장애가 따르므로 이를 극복키 위하여 UN산하의 UNCITRAL은 전자서명통일규칙(Uniform Rules on Electronic Signatures)의 제정을 추진 중에 있으며, EU에서도 전자서명 입법지침의 제정을 준비 중에 있다. 표 3은 국외 공인인증기관 지정·운영 현황을 나타낸 것이다.

표 3 국외 공인인증기관 지정·운영 현황

국가		공인인증기관명	비고
미국	유타주	DST	1997.11 지정
		Arcanvs	1997.12 지정
		USERTrust	1998. 6 지정
	텍사스주	Verisign	1998. 4 지정
	워싱턴주	ID Certify	1998. 4 지정
		VeriSign	1998 8 지정
		Arcanvs	1999. 4 지정
독일		도이치 텔레콤	1999. 1 지정
말레이시아		없음	
싱가포르		없음	
이탈리아		없음	

4. 전자서명 인증 서비스 현황

4.1 국내외 인증 서비스 현황

일반적으로 인증 서비스는 두 가지 분류로 나뉘어진다. 첫 번째는 범용 보안 프로토콜의 확산으로 인해 요구되는 인증 서비스이고, 두 번째는 안전한 인트라넷(Intranet)·익스트라넷(Extranet) 네트워크 시스템, 폐쇄(Closed) 네트워크 시스템 등의 구축을 위해 요구되는 인증 서비스이다. 본고에서는 전자를 범용 서비스(Public service)라고 하고, 후자를 전용 서비스(Private service)로 분류하고자 한다. 표 4는 현재 세계적으로 가장 널리 알려진 VeriSign사의 인증 서비스를 기반으로 분류한 것이다. 초기 인증 서비스 형태는 주로 S/MIME과 SSL 서버용 인증서 발급 서비스였으며, 점차적으로 전용 서비스와 새로운 범용 서비스들이 탄생하기 시작하였다.

현재 가장 폭넓게 이용되고 있는 인증 서비스 중의 하나는 가상 쇼핑몰이나 온라인 뱅킹을 구축하기 위하여 사용되고 있는 SSL 인증서 발급 서비스이다. 또한, 안전한 웹 기반의 전자우편인 S/MIME 인증서 등도 최근 많이 이용되고 있는 인증 서비스 중의 하나이다. 최근에는 인터넷을 기반으로 온라인 배포되는 S/W의 안전·신뢰성을 보장하기 위한 코드 서명용(Code singing) 인증서비스가 제공되고 있으며, 안전한 VPN(Virtual Private Network) 구축을 위하여 라우터 등에 사용되는 IPSec 인증서 발급 서비스 등도 제공되고 있다.

지금까지 고찰한 외국의 사례와는 달리 국내의 인증 서비스는 초기단계이며, 아직 다양한 인증서비스가 제공되지 않고 있다. 현재까지 국내에서 상업적 목적을 가지고 공식적으로 인증서 발급 서비스를 수행하고 있는 업체는 SET 지불 시스템을 구축·운영하고 있는 일부 업체들 외에는 거의 전무한 실정이다. 그러나 보다 엄밀히 말한다면, SET 인증 서비스는 SET 프로토콜을 위한 전용 인증 서비스이기 때문에 일반적인 인증 서비스라고 보기는 어렵다. 즉, 현재까지 일정 발급 수수료를 받고 SSL이나 S/MIME 등의 인증서를 발급해주는 국내 인증 서비스 업체는 거의 없는 실정이며, 단지 개발 업체들만의 제품 시범 서비스만이 존재할 뿐이다 그러나, 최근 공인인증기관을 준비기관들이 곧 공인인증기관으로 지정될 것으로 예상된다. 즉, 공인인증기관들의 서비스가 시작된다면 본격적인 인증 서비스가 제공될 수 있을 것이며, 이를 토대로 VeriSign사와 같은 다양한 인증 서비스가 등장하리라 예상된다.

표 4 인증 서비스 종류 및 내용

분류	서비스 종류	내용
전용 서비스	VeriSign Onsite	VeriSign사에서 제공하는 기업 전용서비스를 위한 PKI 외주 서비스
	VeriSign Onsite for Sever Certificate	서버 인증서 발행을 전담으로 하는 외주 서비스
	VeriSign Onsite for IPSec Certificate	VPN(Virtual Private Network)을 지원하기 위한 IPSec 인증서 발행을 전담으로 하는 외주 서비스
	SET Service	SET 지불시스템에서 사용되는 전용 인증서 발급 서비스
범용 서비스	Individual Certificate	안전한 전자우편 프로토콜인 S/MIME이나, 보안 프로토콜인 SSL에서 클라이언트 인증서로 사용되는 개인용 인증서 발급 서비스
	Server Digital Certificate · Secure Server Certificate · Global Server Certificate · OFX Server Certificate · EDI Server Certificate	보안 프로토콜인 SSL이나 OFX 또는 EDI 환경에서 안전한 트랜잭션을 위한 서버용 인증서 발급 서비스 · 40비트 암호화가 가능한 SSL용 인증서(Secure Server) · 128비트 암호화가 가능한 SSL용 인증서(Global Server) · 금융망 프로토콜인 OFX에서 사용되는 금융 서비용 인증서(OFX Server) · 전자데이터교환(EDI) 시스템에서 사용되는 서버용 인증서(EDI Server)
	Code Signing Certificate · Microsoft Authentication Code · Netscape Object Signing · Marimba Castanet	네트워크 상으로 S/W 모듈이나 데이터를 배포하는 경우 안전·신뢰성을 향상시키는데 사용되는 인증서 발급 서비스 · 네트워크를 통해 마이크로소프트사의 32-bit exe(PE files), .cab, .ocx .class 파일등의 S/W 모듈을 배포하는 경우 사용되는 개발자용 인증서 · 네트워크를 통해 자바, 자바스크립트, Pulg-in 등의 S/W 모듈을 배포하는 경우 사용되는 개발자용 인증서 · 네트워크를 통해 마림바社의 Push기술을 통해 데이터가 배포되는 경우 사용되는 채널 서명용 인증서

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

표 6 국내 인증 서비스 업체 현황

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

※ 상기 소개된 인증 서비스 업체는 비공인인증기관이며, 향후 공인인증기관이 곧 지정될 예정임

4.2 국내외 인증서버 개발 업체 현황

인증기관이 인증 서비스를 제공하기 위해서는 이를 지원할 수 있는 다양한 시스템들이 필요하게 된다. 가장 중요한 시스템으로서는 인증서를 발급하는 인증(Certifiaction Authority)서버이며, 발급된 인증서를 공고해주는 디렉토리 시스템, 그리고 가입자와 인증서버를 연결해 주는 등록(Registration Authority)서버 등이 있다. 인증 솔루션 개발 업체라고 하는 것은 인증서버, 등록서버 등과 같이 인증기관이나 이를 이용하는 사용자들에게 필요한 시스템을 제공하는 업체를 말하는 것이다.

표 5 국내 인증서버 개발 업체 현황

업체명	제품명
소프트포럼	SFCA V2.5
이니텍	이니텍 CA V2.5
삼성SDS	TrustPro
LG-EDS	SmartCA
장미디어인터렉티브	JMI CA
펜타시큐리티	ISSAC
세넥스	Assure Web CA
시큐어소프트	SecureCA
동진프론티어	Safe-Answer

국내 개발 업체들은 현재 SSL이나 S/MIME용 인증서 발급이 가능한 인증서버(CA서버)를 개발한 상태이며, 아직까지는 다양한 인증서 발급 서비스(예:IPSEC, OFX 등)들을 지원하는 인증 서버는 거의 없는 상태이다. 현재 국내 인증서버 개발 현황은 시장 형성 초기 단계이며, 향후 지속적인 발전이 있을 것으로 사료된다. 표 5는 현재 국내의 인증서버 개발 업체 현황을 나타낸 것이다.

국외 개발 업체들로는 인증업체 중 가장 널리 알려져 있는 캐나다의 Entrust, 영국의 Zergo사를 합병한 아일랜드의 Baltimore, 윈도우즈2000에 PKI 솔루션을 탑재시킴으로써 새로운 업체로 등장한 Microsoft, AOL사가 인수한 넷스케이프사 등이 있다. 표 6은 현재 널리 사용되고 있는 인증서버를 개발하고 있는 국외 인증서버 개발 업체 현황이다.

표 6 국외 인증서버 개발 업체 현황

업체명	제품명
Baltimore	UniCERT
CyberTrust, GTE Company	Enterprise CA and Global Provider CA
Entegrity	Notary
Entrust	Entrust PKI
Microsoft	Certificate Server 1.0/Certificate Services for Win 2000
Netscape	Certificate Server/Certificate Manager
SSE	Open Path CA
Xcert	Enterprise CA

5. 공인인증기관과 전자서명 인증관리센터

5.1 공인인증기관

앞 절에서 기술한 바와 같이 안전한 전자적 거래를 위해서는 전자서명 인증 서비스가 필수적으로 요구된다. 즉, 인증기관의 전자서명 인증 서비스 없이는 컴퓨터 네트워크를 통한 전자결재(또는 전자결재), 전자계약 등의 전자적 거래가 불가능할 수 밖에 없게 된다. 하지만, 이것이 단지 인증기관의 전자서명 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 전자서명 인증 서비스에서도 동일하게 적용된다. 컴퓨터 네트워크를 이용하는 사용자들은 다양한 인증기관으로부터 전자서명 인증 서비스를 받을 수 있다. 즉, 사용자들은 여러 개의 전자서명생성키와 이에 대응되는 인증서(전자서명검증키 내포)를 소유할 수 있다. 하지만, 법적으로 보다 확실하게 인정받을 수 있는 전자서명을 하기 위해서는 전자서명법 및 하위법령의 요구조건을 만족하고 있는 인증기관으로부터 전자서명 인증 서비스를 받아야만 할 것이다. 이것은 결국 안전·신뢰성 있는 전자서명 인증관리체계의 구축 및 운영을 위해서는 전자서명 인증관리센터로부터 공인된 인증기관이 필요하다는 것을 의미하며, 이러한 인증기관을 공인인증기관이라 한다. 공인인증기관은 사용자의 전자서명검증키에 대한 무결성 보장과 신분정보의 표시를 위하여 인증서 발급 서비스를 제공함과 동시에 인증서 관리를 위하여 인증서 효력정지 및 폐지, 인증서 갱신, 인증서 공고 등에 관한 전반적인 업무를 수행한다.

공인인증기관의 실제 운영은 전자서명 인증관리센터를 최상위 인증기관으로 하는 2단계 공개키 기반구조 형태로 이루어진다. 여기서 전자서명 인증관리센터는 공인인증기관의 안전·신뢰성 운영에 대한 검사를 실시하고, 유사시 공인인증기관의 인증서를 효력정지 또는 폐지시키는 업무를 수행한다.

5.2 전자서명인증관리센터

1999년 7월 1일 전자서명법의 시행과 함께 한국정보보호센터내에는 국가 최상위 인증기관인 전자서명 인증관리센터가 7월 7일자로 설립되었다. 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 하고 있다.

5.2.1 전자서명 인증관리센터의 임무 및 기능

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 1은 상기에서 설명한 전자서명 인증관리센터 업무를 전체적으로 조감하고, 국내 전자서명 인증관리체계를 보여주고 있다.

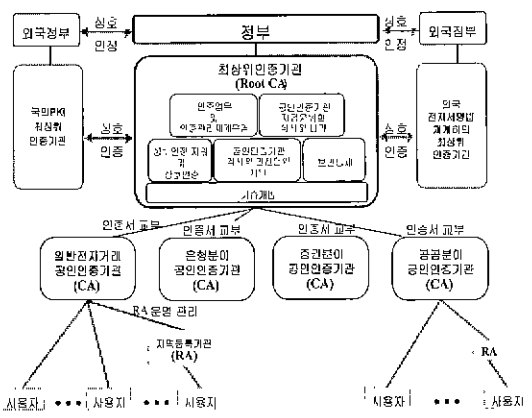


그림 1 전자서명 인증관리체계

5.2.2 전자서명 인증관리센터 시스템 개발 적용 기술 표준

전자서명 인증관리센터는 시스템 개발시 다음과 같은 기술 표준을 적용함으로써 공인인증기관과의 상호연동성을 보장할 수 있도록 하였으며, 세부 내용은 다음 표 7과 같다.

표 7 전자서명 인증관리센터 시스템 개발 적용 기술 표준

분 야	적용표준
전자서명 알고리즘	-KCDSA(TTA 정보통신 단체표준) -RSA(PKCS #1)
해쉬 알고리즘	-HAS-160(TTA 정보통신단체표준) -SHA-1(FIPS 180-1)
인증서 규격	-ISO/ITU-T X.509v3
인증서 효력정지 및 폐지목록 규격	-ISO/ITU-T X.509v2
인증서신청 요구 규격	-PKCS #10
디렉토리 규격	-LDAP(또는 X.500 기반) 디렉토리

인증서 발행 및 관리에 사용되는 전자서명 알고리즘은 공인인증기관들과의 상호연동성을 보장하기 위하여 KCDSA와 RSA를 사용한다. RSA 전자서명 알고리즘은 PKCS(Public Key Cryptography Standard) 표준을 준용하여 구현되었으며, KCDSA는 PKCS 구현 표준을 기반으로 하였으며, 동시에 전자서명검증키와 전자서명생성키 표현을 위하여 ASN.1을 추가적으로 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 거쳤다.

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. 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. RFC 2459는 ISO/IEC의 버전3와 거의 동일하나 인증서 확장영역 부분이 추가적으로 부가되었으며, 기타 몇 가지 ASN.1 형식도 참가되었다. 현재 전자서명 인증관리센터는 ISO/IEC의 표준을 준용하고 있으며, 향후 RFC 2459의 인증서 확장영역도 지원해 나아갈 계획이다. 또한, 전자서명 인증관리센터는 인증서 효력정지를 위하여 인증서폐지목록을 활용한다. 즉, 인증서폐지목록의 사유코드(Reason Code) 부분 중 certificateHold 부분의 비트값을 사용함으로써 효력정지된 인증서도 인증서폐지목록에 함께 등재시킴으로써 인증서 효력정지를 수행한다.

6. 결 론

국내 전자서명법의 제정 및 시행은 21세기 새 천년을 준비하는 시점에서 상당히 중요한 의미를 갖는다. 전자적 거래가 활성화되고 있는 현재 시점은 기존 대면 방식의 거래 문화가 컴퓨터 네트워크나 기타 통신망을 통한 비대면 방식의 거래 문화로 자리잡아 가고 있는 중요한 시점이라고 말할 수 있다. 이러한 단계에서 전자상거래의 활성화는 단지 기술적인 뒷받침만으로 이루어내기는 어려우며, 관련 정책 및 법·제도의 제정이나 보완이 반드시 병행되어야만 한다. 이러한 측면에서 우리나라의 전자서명법 제정은 21세기 전자적 거래의 활성화를 위한 제도적 기반을 마련하였다고 볼 수 있다. 또한, 전자서명법의 시행을 통한 전자서명 인증관리체계의 구축, 전자서명 인증관리센터의 구축·운영, 공인인증기관의 지정·운영 등은 전자적 거래 활성화 및 전자정부 구현에 근간이 되는 국가 공개키 기반구조 구축이라는 기술적 기반을 갖추었다는데 그 의의가 있다고 말할 수 있다 이러한 전자서명 인증관리체계의 구축은 궁극적으로 전자적 거래 활성화를 도모함과 동시에 국내 전자상거래 시장을 활성화시킬 수 있는 부가적 효과도 가질 수 있으리라 예상된다.

현재 전자서명 인증기술은 급속도로 발전하고 있다. 외국의 경우는 새로운 인증 서비스가 계속적으로 등장하고 있으며, 인증 시장 또한 급속도로 성장하고 있다. 최근에는 인증기관간 상호연동 및 상호인증이 새로운 화두로 떠오르고 있으며, 인증관련 표준화 활동도 왕성하게 진행되고 있다. 새로운 천년의 시작인 2000년부터는 국내에서도 본격적인 인증 서비스가 시작될 것이며, 이는 국내 전자서명 인증기술을 급속도로 발전시키는 새로운 계기가 될 것으로 사료된다.

참고문헌

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

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

[3] PKCS#1 v2.0, "RSA Cryptography Standard", Oct., 1998.

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

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

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

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

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

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

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

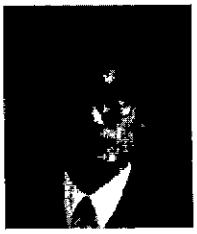
[11] McBride Baker & Coles, "Summary of Electronic Commerce and Digital Sig-

nature Legistration", "http://www.mbc.com/legis/"
[12] 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.
[13] "Thawte Digital Certificate Services", 1999, "http://www.thawte.com"
[14] "UMS", 1998, http://www.cusys.edu/~security/ users/policyhp.html
[15] "VeriSIgn", 1999, http:/www.verisign.com
[16] 법률제5792호, "전자서명법", 1999. 2. 5.
[17] 법무부, "외국의 전자서명제도", 1997.
[18] 유타주 전자서명법, "Digital Signature Administrative Rules", State of Utah, 1996, http://www.commerce.state.ut.us/web/commerce/digsig/act.htm
[19] 워싱턴주 전자서명법, "The Washington Electronic Authentication Act(EAA)", State of Washington, June 11, 1998, http://www. wa.gov/sec/ea/dsrcw.htm

최 영 철

1996.2 성균관대학교 정보공학과 학사
1998.2 성균관대학교 전기·전자·컴퓨터공학부 석사
1998.1~현재 한국정보보호센터 연구원
관심분야 : 암호이론, 전자상거래 보안, 전자서명 인증, 공개키기반구조
E-mail ycchoi@kisa.or.kr

홍 기 융



1985.2 전남대학교 전자계산학과 학사
1990.2 중앙대학교 전자계산학과 석사
1996.2 아주대학교 컴퓨터공학과 박사
1994.8 정보처리기술사
1985.9~1995.10 ETRI 선임연구원
1992.9~1993.6 Italy Alenia Spazio사 선임연구원
1995.10~1996.4 한국전산원 선임연구원
1996.4~현재 한국정보보호센터 인증관리팀장
관심분야 : 컴퓨터 · 네트워크 보안, 정보보호시스템 평가, 정보보호표준화, 전자상거래 보안, 전자서명 인증, 공개키기반구조(PKI)
E-mail: kyhong@kisa.or.kr

이 홍 섭

한양대학교 전자공학과 학사
한양대학교 전자공학과 석사
대전대학교 컴퓨터공학 박사
1990~1996 한국전자통신연구원 실장
1996~현재 한국정보보호센터 연구개발부장, 기술본부장,인증관리센터구축준비반장, 기술개발부장, 정보통신기술협회 정보보호기술위원회 의장, 한국정보통신 정보보호학회 상임이사
관심분야 : 시스템 및 네트워크 정보보호
E mail hslee@kisa.or.kr