情 報 保 護 學 會 誌
第 11 券 第 4 號, 2001. 8

국내 · 외 전자서명 및 인증제도 동향 분석

이 대 기*, 김 희 선*, 조 영 섭*, 진 승 헌*, 정 교 일*, 조 현 숙**

요 약

거래를 포함한 커뮤니케이션이 효율적으로 발전함에 따라 보다 다양한 채널의 커뮤니케이션이 가능해졌으나, 신뢰 메커니즘이 아직 형성되지 못하여 불확실성과 위험 요소를 야기시킬 수 있기 때문에 정보 사회에서의 신뢰성에 대한 문제는 점점 중요한 의미를 갖게 되었다. 정보사회에서 신뢰를 형성하는 방법은 매우 다양하다. 기존에는 이용자의 경험 및 타인으로부터의 정보입수, 공급자의 신용 및 명성, 정부의 법 · 제도 등을 토대로 신뢰형성이 이루어져 왔으나, 정보사회에서는 전자서명이라는 새로운 기술과 이러한 기술을 사회적으로 이용 가능하게 하는 인증 관리 체계의 도입을 토대로 이루어지고 있다. 본 고에서는 전자서명과 인증제도의 국내 · 외적인 동향에 대해 분석하고자 한다.

Ⅰ. 서 론

인터넷의 급속한 확산과 인터넷 사용자 수의 폭발적인 증가에 따라 가상공간(cyber space)을 무대로 하는 전자거래의 규모 역시 기하급수적으로 늘어나고 있다. 이에 따라 폐쇄된 네트워크에 비해 정보 누출이 비교적 쉬운 인터넷 상에서의 안전한 전자거래를 위해서 안전한 전자서명이 상대적으로 중요시되고 있으며, 또한 최근 전자서명 기술이 발달함에 따라 기존에 널리 사용되어 오고 있는 공개키기반구조(PKI)의 디지털 서명 이외에도 지문인식, 홍채인식 및 수기서명기술 (signature dynamics) 등 다양한 전자서명 기술이 개발되어 사용되고 있고, 인증제도 역시 핵심체계로서 중요시되고 있다. 즉, 인터넷을 기반으로 한 각종 전자거래 서비스의 활성화는 비대면(非對面) 상대방에 대한 효율적인 전자서명 및 인증, 유통되는 정보의 안전성을 전제로 한다.

본 고에서는 국내 · 외 전자서명과 인증제도 동향 고찰에 있어 보편화된 세부기술 내용은 제외하고 포괄적인 내용만을 체계있게 분석한다.

Ⅱ. 필요성

컴퓨터 네트워크를 통해 거래가 이루어지게 되는 정보사회에서는 인감, 주민등록증 등과 같은 산업사회에서의 신원증명수단이 거의 무용하게 되거나, 거래는 네트워크를 통해 이루어지고 신원증명은 대면적인 수단이나 종이서류에 의한 이중 절차로 수행되는 경우가 많아진다. 이러한 거래상대방 확인수단의 미비는 익명성(anonymity)을 증가시켜 이에 따른 여러 가지 역기능을 발생시킬 수 있다.

익명성이 증가한 정보사회에서 신원확인을 위한 기술적 방법이 바로 전자서명이다. 전자서명은 서명한 메시지의 송신자 인증(authentication) 및 서명된 문서의 무결성(integrity)을 입증할 수 있기 때문에 증가된 익명성에 대응하는 효과적인 기술적 수단이다.

전자상거래(electronic commerce)가 급속한 발전을 하고 있는 가운데 당사자의 신원에 대한 불확실성은 더욱 높아질 것이고, 이에 따라 디지털서명의 필요성이 증가할 것이다.

원본과 복사본의 식별이 불가능하고 내용을 손쉽게 변조할 수 있는 전자문서는 전달된 전자문서가 의도한 바로 그 문서로서, 전자문서의 생성, 유통, 보관과정 등에서 발생할 수 있는 변조가 일어나지 않았음이 입증되는 기능을 지녀야 한다. 전자화된 정보를 이용할 경우, 정당하게 이루어진 거래 또는 계약을 부인하는 것이 용이하므로, 이를 효과적으로

* 한국전자통신연구원 정보보호기반연구부 ({ldg67063, sezsez, yscho, jinsh, kyoil} @etri.re.kr)
** 한국전자통신연구원 차세대보안응용연구부(hscho@etri.re.kr)

방지하여 거래당사자간의 분쟁을 최소화하고 전자상거래의 신뢰기반을 조성할 필요가 있으며, 전자서명된 문서의 무결성 보장을 할 수 있게 된다.

또한, 전자거래 시에 발생된 분쟁에 대해서는 인증기관이 발행한 인증서를 법원에 제출함으로써 이 인증서를 이용하여 신원확인, 자료의 무결성, 부인봉쇄 등의 증거 자료를 확보할 수 있다. 즉, 법적 분쟁 시의 증거 확보로서 필요하다.

III. 전자서명

1. 국내·외 법령체계

국내·외에서 적용되고 있는 전자서명 관련 법령의 체계 및 접근 방식은 대개 4가지 형태인 1)공개키기반구조의 디지털서명형, 2)기준 제시형, 3)유효성 인정형, 4)혼합형으로 분류해 볼 수 있다. 이들 형태에 대한 각각의 설명은 다음 표 1과 같다.

2. 전자서명법 관련 동향

2.1. 국제기구

2.1.1. 유엔국제상거래법위원회(UNCITRAL)

UNCITRAL(United Nations Commision on International Trade Law) 사무국이 전자문서 방식에 의한 국제거래가 점차 보편화됨에 따라 '84년 자동문서처리의 법적 측면(Legal Aspects of Automatic Data Processing)이라는 보고서를 작성하여, 이를 '85년 18차 위원회에 제출하였고, 이 위원회에서 컴퓨터 기록의 법적가치에 대한 검토 권고안이 채택되었다. 이 권고안 채택을 시작으로 EDI 및 관련 통신수단의 법적 측면에 대한 모델법 초안을 위한 작업반(WG)이 구성되었고, '95년 28차 위원회 작업반 회의에서 모델법 초안이 마련, '96년 6월 14일 29차 위원회에서 전자상거래에 관한 모델법(UNCITRAL Model Law on Electronic

〔표 1〕 전자서명관련 법령체계 및 접근 방식

구분	법령체계	방식개요
공개키기반 구조의 디지털서명형	Electronic/Digital Signature - 정의 - 전자/디지털서명의 적용범위 - 안전성/신뢰성을 위해 전자/디지털서명이 만족해야 하는 조건 (법적 효력을 위한 조건)	○ 공개키기반구조(PKI)방식의 디지털 서명만을 대상으로 삼고, 관련 정의와 인증기반의 인·허가 및 감독, 인·허가 중지 및 취소, 인증기관과 가입자 및 관련자간의 책임한계, 인증서의 발행·중지·폐지, 디지털서명 및 인증서의 효력, 상호인증 등과 관련 사항들을 선택적으로 규정 ○ 미국 유타주와 독일의 디지털 서명법
기준 제시형	Digital Siganture - 정의 - 인증기관 ● 인증기관의 인·허가 ● 인증서의 발행, 취소 및 정지 ● 인증기관, 가입자 및 관련 당사자의 의무 및 책임 ● 디지털서명의 인정 및 책임 - 상호 인증 및 기타	○ 전자서명에 일정한 기준을 두고, 그 기준을 만족하는 경우 법적 효력을 인정하는 방식 ○ 미국 캘리포니아주 전자서명법
유효성 인정형	Signature 정의 Electronic Signature - 정의 - 전자서명의 적용 범위 - 수기서명, 전자서명을 차별화하지 않는 조항 - 인증기관, 책임 문제 및 상호 문제는 언급되지 않고 기존의 법체계 및 시장에서 결정토록 함	○ 수기서명과 전자서명의 정의를 제시하며, 전자서명의 적용범위를 밝히고, 수기서명과 전자서명을 차별화 하지 않음을 분명히 하면서, 인증서나 인증기관, 책임문제, 상호 인증문제 등을 전혀 언급하지 않고 기존의 법체계 및 시장에서 결정하도록 함 ○ 미국 메사츄세츠주 전자서명법
혼합형	Electronic Signature 정의 Secure Elec. Sig. - effect -Digital Sig. - 정의 - 정의 - Presumption - CA - Attribution - 상호인증	○ 전자서명의 정의를 두고, 그 중에서 안전한 전자서명의 요건과 법적효력을 명기하며, 디지털서명과 관련하여 인증기관의 인·허가, 인증서의 발급·중지·폐지, 인증기관 및 사용자의 책임문제와 상호인증 문제 등을 규정 ○ UNCITRAL전자서명 통일규칙, 미국 일리노이주 전자서명법

Commerce)이 채택되고 UN총회 제51차 회의에서 통과되어 성립되었다.

이 모델법은 모든 국가들이 서류에 기초한 통신문 형식 정보자료 보관에 대한 대체 수단으로서의 전자문서의 사용을 규율하는 입법을 추진하는데 매우 중요한 도움을 줄 목적으로 제정되었으며, 전문17개조로 제1부(전자상거래일반)와 제2부(특정분야에서의 전자상거래)로 구성되어 전자상거래에서 발생하게 될 제반 법적 문제점에 대한 규정을 정하고 있다.

UNICITRAL에서는 전자상거래 모델법에서 채택한 기술 중립성의 원칙에 따라서 디지털서명과 다른 전자서명 기술의 이용을 억제하거나 제한하지 않는다는 방향에서 전자서명 모델법을 작성하였고 이 법안은 2000년 6월 전체 회의에서 채택되었다.

2.1.2. 경제협력개발기구(OECD)

OECD에서는 정보통신시스템의 안전한 운용과 전자상거래의 촉진 및 사생활 보호를 위하여 암호기법의 유용성을 인식하고 '97년 5월 OECD 암호정책지침을 제정하여 회원국에 권고하였다. OECD 암호정책의 8대 원칙은 1)암호기술의 신뢰성, 2)암호기술의 자유선택, 3)시장요구에 근거한 암호기술의 개발, 4)암호기술의 표준, 5)프라이버시와 개인정보의 확보, 6)법에 근거한 입수, 7)책무, 8)국제협력으로 제정되어 있다. 이 지침 제정 이후에도 인증제도를 전자상거래의 활성화를 위하여 필수적인 요소로 간주하고, 지난 '98년 10월에 "국경 없는 세계: 범 세계적인 전자상거래의 실현"이라는 주제하에 캐나다 오타와에서 열린 OECD 각료회의에서는 전세계 전자상거래에 대한 공동의 비전이 1) 사용자와 소비자들을 위한 신뢰 구축, 2) 디지털 시장을 위한 기본규칙 수립, 3)전자상거래를 위한 정보기반의 증진, 4) 이익의 극대화라는 사실에 합의하였다.

이를 위해, 각료회의에서는 글로벌 네트워크상에서의 사생활 보호에 관한 선언문(Declaration on Protection of Privacy on Global Network), 전자상거래 상황에서의 소비자 보호에 관한 선언문(Declaration on Consumer Protection in the Context of Electronic Commerce)과 함께 전자상거래 인증에 관한 선언문(Declaration on Authentication for Electronic Commerce)이 채택되었다.

이 외에도 OECD의 예비초안(Inventory of Approaches to Authentication and Certification in a Global Networked Society)을 작성하여, 인증분야에서 제기되는 다양한 이슈에 대한 검토와 현재 사용되는 용어의 보다 명확한 정의, 또한 네트워크 상에서 인증될 수 있는 다양한 정보와 그 사례 및 OECD 각 국가의 인증문제에 대한 접근방법을 간략히 소개하고 있다.

표 2는 OECD 암호 정책의 8대 원칙을 설명하고 있다.

2.2. 미 국

미국의 경우 이미 '95년부터 대다수의 주에서 전자문서의 안전·신뢰성 확보 방안으로 전자인증제도를 고려하고 있거나 관련 법안을 제정하였다. 2001년 6월 현재 50개 주 전체가 디지털서명법 또는 전자서명법을 제정했거나 관련 문제에 대해 연구 중이며, 공공과 일반 부문의 커뮤니케이션을 포괄하는 일반적인 용도의 법과, 보건서비스 제공자나 차량등록을 위한 전자서명의 활용 같은 공공 부분이나 제한된 민간 부문에만 적용되는 특정용도의 법령을 제정하였다.

〔표 2〕 OECD 암호 정책의 8대 원칙

원칙	요구 사항
암호기술의 신뢰성	암호기술은 이용자가 정보시스템과 통신시스템에 적용할 때에 은닉성을 확보할 수 있도록 신뢰성이 높은 것이어야 한다.
암호기술의 자유 선택	사용자는 적용되는 법률을 기준으로, 이용하는 암호기술을 자유로이 선택할 수 있어야 한다.
시장요구에 근거한 암호기술의 개발	암호기술의 개발은 개개의 사용자와 산업계, 정부의 요청에 답하는 것이어야 한다.
암호기술의 표준	암호기술에 관한 기술표준, 기준, 프로토콜은 국가 및 국제적 레벨에서 개발 및 그 적용을 추진해야 한다.
프라이버시와 개인정보의 확보	통신비밀과 개인정보의 보호를 포함한 프라이버시에 관한 개인의 기본적 권리는 국가 암호방침의 책정과 암호기술의 도입과 운용에 있어서 충분히 존중되어야 한다.
법에 근거한 입수	국가는 암호정책에 의해 암호화된 데이터의 보통 문장 또는 복호화를 위한 암호키를 법에 근거해서 입수 할 수 있다. 이 정책의 실시에 있어서는 OECD암호 정책 이외의 원칙을 충분히 배려해야 한다.
책무	암호 서비스를 제공하거나, 암호 키를 보관 또는 이용하는 개인 또는 조직에 관한 계약서가 작성되거나 규칙이 재정되는 경우는 그 책무에 대해 계약서 또는 규칙에 명기해야 한다.
국제협력	정부는 암호정책을 수행하기 위해 국제협력을 해야 한다. 이의 가시적인 수행을 위하여 정부는 무역을 저해하는 암호정책을 재정해서는 안된다. 그러한 암호정책이 존재하는 경우에는 제지해야 한다.

그 중 유타주 디지털서명법(Utah Digital Signature Act)은 '95년 10월에 발간된 미국법조협회(ABA)의 디지털서명지침(Digital Signature Guidelines)을 참고로 하여 '96년에 제정된 법령으로서 공개키기반구조에 근거한 디지털서명만을 대상으로 하는 대표적인 법률이며, 디지털서명법으로는 전세계적으로 가장 선구적이라고 할 수 있는 법이다.

유타주 디지털서명법은 명칭, 해석 및 용어 정의(제1절), 인증기관의 허가와 규제(제2절), 인증기관과 신청인의 의무(제3절), 디지털서명의 효력(제4절), 주의 역할과 저장소의 재구성(제5절) 등의 총 5절로 구성되어 있다. 유타주 디지털서명법의 특이한 점 중의 하나는 인증기관의 허가와 규제 측면이다. 상업국에서 일정요건에 해당하는 인증기관에 라이센스를 부여하도록 하였는데(제103조 및 제201조), 라이센스를 받은 공인인증기관을 통한 전자서명 및 인증서는 명확한 법적 효력을 부여받도록 하고 공인인증기관의 책임 제한규정(제309조)을 분명히 하는 등 일정한 인센티브를 공인인증기관에게 부여하고 있다. 이러한 인센티브를 통하여 자연스럽게 인증기관을 허가 쪽으로 유도하고자 하는 것이다.

이외에도 인증서, 인증기관, 저장소 등에 대하여 많은 규정이 있는데, 전자서명키 관리에 있어서 인증기관이 가입자의 비밀키를 보유하거나 사용할 수 있는 조건을 명시하고, 비밀키 관리에 있어서 신청인의 주의의무(제305조)를 명기하고 있다.

또한, 빌 클린턴 대통령이 2000년 6월 30일에 국내·외 상거래에 관한 전자서명법(The Electronic Signatures in Global and National Commerce Act : E-sign)에 서명하였다. E-sign법은 주요 정책 달성을 표방하며 전자기록과 전자거래의 법적 유효성을 확보함으로써 전자상거래를 촉진한다. 특히, 전자서명과 계약의 법적 효력의 명시, 법적으로 요구하는 통지 및 공개 사항의 전자적 전송을 인정하고, 전자적 수단을 이용하여 기록 보유 요구 사항의 충족을 고려하는 규정을 두고 있다. E-sign법은 미국 모든 주들이 각 주의 법을 통일하기 위하여 만든 전자거래 통일법(Uniform Electronic Transactions Act : UETA)을 채택한 주의 법에만 예외를 두고 있다. 실제로는 UETA 자체가 E-sign법과 거의 같은 내용을 가지고 있다.

2.3. 독 일

독일에서는 '97년 8월 1일부터 시행하고 있는 정보통신서비스 종합법 (Gesetz zur repelvng der Pahmenbendinung Fur Informations 中 Kommunikationsdienste : IuKDG) 의 제3장에 디지털서명법이 규정되어 있다.

이 법은 '97년 8월 1일부터 시행되어 오다가 2001년 5월 21일에 개정되어 전자서명의 개념을 광의로 정하고 있고, 이러한 전자서명 중에서 일정한 조건을 충족하는 것을 고급 전자서명으로 하고 다시 고급 전자서명 중에서 일정한 조건을 충족하는 것을 공인전자서명으로 정의하고 있다. 이 법은 우리나라 전자서명법의 법률 제정에 중요한 참고자료로 검토되었으며 현재 진행중인 전자서명법 개정에도 개정된 디지털서명법이 참고자료로 검토되고 있다.

2.4. 유럽연합(EU)

영국 등 15개국의 통신관련 장관 회의에서 인터넷 전자서명이 문서서명과 동일한 법적 지위를 갖도록 하는 전자서명지침(Directive 1999/93/EG of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures)이 2000년 1월 19일 발효되었으며 EU 회원국들은 발효일로부터 18개월 내에 즉, 2001년 7월 19일까지 이 지침의 내용을 자국법에 이행하여야 한다고 규정하고 있다.

미국 유타주의 디지털서명법과 유사한 법체계로 암호키 관리 및 복구 시스템으로서 정부가 인정하는 신뢰받는 제3자(TTP) 제도를 도입하고 있다.

덴마크는 '97년도에 전자서명법을 제정하여 시행하고 있다.

2.5. 일 본

200개 회사의 컨소시움으로 구성된 전자상거래실증추진위원회(Electronic Commerce Promotion Council of Japan : ECOM)와 법무성을 중심으로 전자인증 및 공증제도에 관한 연구가 진행 중인데, ECOM의 인증기관검토 실무반은 '97년 4월에 인증기관 가이드라인(알파버전)을 '98년 3월에는 상호인증가이드라인(알파버전)을 발표하였으며, 전자서명법이 2000년 5월 24일 의결되어, 2001년 4월 1일부터 시행 중에 있다. 또한 '96년 7월에 발족한 법무성 내의 전자거래제도에 관한 연구회에서는 상

업등기정보를 활용한 전자인증제도의 구축 및 거래 성립을 증명하는 전자공증제도의 창설, 전자서명에 관한 법률 제정을 목표로 한 보고서를 기초로 법무성은 시범사업에 착수하여 2001년 실용화를 목표로 민법, 상법, 민사소송법 등을 정비 작업 중이다.

2.6. 캐나다

'99년에 EU전자서명지침서(EU Directive)를 채택한 통일전자거래법(Uniform Electronic Commerce Act)을 통과시켜 각 주에 권고한 바 있다.

2.7. 호 주

'99년에 전자거래법(Electronic Transaction Act)을 제정하여 시행하고 있다.

2.8. 오스트리아

2000년부터 전자서명법(Signaturgesetz)을 시행하고 있다.

2.9. 말레이시아

'97년에 Cyberbills내의 4개의 법률(Computer Crimes Bill, Digital Signature Bill, Telemedicine Bill, Copyright(Amendent) Bill) 중의 하나로 디지털 서명법을 제정하였는데, 그 체계나 내용이 미국 유타주의 디지털서명법과 매우 유사하다.

2.10. 싱가포르

'98년에 디지털서명법을 제정하여 시행하고 있으며, 그 체계나 내용이 미국 유타주의 디지털서명법과 유사하다.

2.11. 한 국

2.11.1. 기존의 전자서명 관련 법령

전자서명과 관련된 법 조항은 국내 여러 법에서 발견되는데, 이 법들은 대부분 폐쇄망에서의 EDI 업무를 규정하기 위해 제정된 것들로 이를 위한 전자문서 및 전자서명의 효력에 대한 보장 규정이 존재한다.

현행 법률에서 다루고 있는 전자서명은 사무관리 규정 등에 나타나는 공문서에 적용되는 경우와, 정부부문의 특정사업과 관련된 특별법에서 정의된 규정으로 대별된다.

기존의 서명방식과 다른 전자서명에 대한 구체적인 정의가 나타나 있지 않으며, 인증기관에 대한 고려가 전혀 없고, 공개키방식의 전자서명을 명확히 정의하고 있지 않기 때문에, 기존 법령에 규정된 전자서명을 미국 유타주의 디지털서명법이나 독일 디지털서명법이 대상으로 하고 있는 공개키방식의 전자서명으로 간주하기 어렵다.

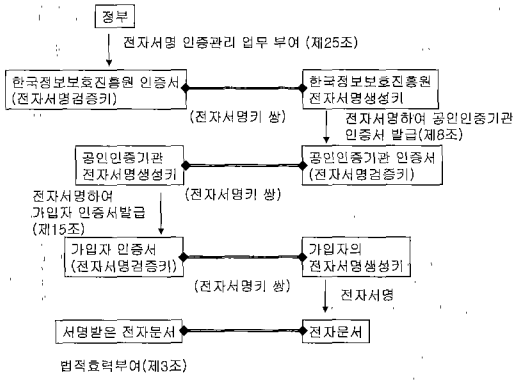
기존의 전자서명에 관한 법령은 전자상거래 활성화에 초점을 맞춘 안전하고 믿을 수 있는 전자서명 제도와 전자문서의 생성·유통·보관 과정 등에서 발생할 수 있는 내용의 위변조 및 분쟁 방지를 위한 문서내용의 인증제도로는 매우 미흡하다고 볼 수 있다.

2.11.2. 현행 전자서명법

우리나라는 정보통신망을 통하여 처리되는 전자문서의 안전성, 신뢰성을 확보하여 전자상거래를 활성화하고 전자정부 구현 및 전자화폐 이용 등 Cyber Korea21에 의한 정보화를 추진하고 국민 생활의 편익을 증진하기 위하여 법률 제5792호('99.2.5), 대통령령 제6457호('99.6.30) 및 정보통신부령 제81호('99.8.12)로 전자서명법, 동법 시행령 및 동법 시행규칙이 각각 제정되어 '99년 7월 1일부터 시행 중에 있다.

이 전자서명법에는 공개키기반의 전자서명을 적극적으로 정의하고, 전자서명과 전자문서의 법적 효력을 부여하고 있고(제3조), 안전한 전자서명의 이용기반을 조성할 수 있도록 공신력 있는 기관(공인인증기관)이 전자서명을 인증하도록 하기 위하여 공인인증기관의 지정제도를 도입하고(제4조), 공인인증업무의 적정성 및 지속성을 확보하기 위하여 필요한 규정(제6조 내지 제14조)을 두고 있다. 또한 인증서의 발급·효력정지·폐지절차 및 방법 등에 관한 세부적인 사항을 규정하고 있다(제16조 내지 제18조). 전자서명 및 전자문서의 안전한 사용 및 분쟁 발생 시에 대비하기 위하여 안전하고 신뢰성 있는 인증관리체계의 운영과 전자서명키 및 인증의무관련 기록의 안전한 관리 등 인증기관의 책임과 의무를 명확히 하고 있다(제19조, 제21조, 제22조).

전자서명의 안전성 및 신뢰성을 확보하기 위하여 전자서명법에 규정되어 있는 전자서명키의 계층구조를 정리하면 그림 1과 같다.



〔그림 1〕 전자서명법의 전자서명키 계층 구조

한편, 인증제도의 안전하고 효율적인 운용을 위해서는 전자서명키의 보호가 필수적이므로 타인의 전자서명키 도용행위, 타인의 명의로 인증서를 발급받는 행위 등을 금지하고(제23조), 이를 위반한 자는 처벌하는 규정(제30조)을 두고 있다. 한편, 인증서비스 이용증가 및 정보통신기술 발달에 따라 공인인증기관이 용이하게 수집, 처리, 보관, 유통할 수 있는 개인정보를 보호하기 위하여, 인증업무에 필요한 개인정보의 수집제한, 목적 외 이용 및 누설 금지 등을 명시한 조항(제24조)을 두고, 이를 위반한 자를 처벌하도록 하였다(제31조 및 제33조). 이와 함께, 전자서명을 안전하게 사용할 수 있는 환경 조성 및 효율적인 공인인증기관 관리를 위하여, 한국정보보호진흥원(KISA)으로 하여금 전자서명 인증관리 업무를 수행하도록 하였다(제25조). 끝으로 국가간의 전자적 거래에 대비하여 정부가 외국 인증기관이 발행한 인증서를 상호인정하는 협정을 체결할 수 있도록 규정하고 있다(제26조).

한편, 정보통신부에서 현행 전자서명법의 그 동안의 시행과정에서 제기된 문제점을 보완하고 UNCITRAL 전자서명 모델법의 전자서명 개념 확대 규정을 수용하고 다양한 전자서명 기술을 반영하고 있는 외국의 입법 동향을 수용함으로써 국가간 상호 인증과 상호 인정에도 대비할 수 있도록 법개정을 추진 중에 있다.

표 3은 국내의 전자서명법을 국외의 대표적인 전자서명법과 비교하여 나타낸 것이다.

IV. 인증제도

1. 인증의 정의

인증은 일반적으로 크게 두 가지 의미로 나뉘어 사용되고 있다. 첫째는 전자서명을 통해 구현될 수 있는 사용자 인증이나 메시지 인증을 의미하는 인증(authentication)이고, 둘째는 공개키 암호방식에서 공개키 무결성의 보장을 의미하는 인증(certification)이다. 본 고에서 언급하고 있는 인증 서비스는 certification 서비스를 언급하는 것이며, 이것은 authentication과는 다소 구분된다.

인증 서비스의 필요성은 공개키 암호 알고리즘의 사용에서부터 비롯된다. 안전한 전자상거래 환경의 구축을 위해서는 인증, 무결성, 비밀성, 부인방지 등의 정보보호 서비스가 필요하게 되며, 인증, 무결성, 부인봉쇄 등의 서비스는 전자서명 기술을 활용함으로써 해결 가능하다. 현재 안전성을 다소 정량화시킬 수 있는 공개키 암호 방식의 전자서명 기술이 가장 우수하다고 알려져 있으며, 이것이 실제 적용을 위해서는 인증 서비스가 필요하게 된다. 인증기관은 전자서명을 이용하고자 하는 사용자들에 대해 인증서 발급 서비스를 제공해 줌으로써 이윤을 창출하거나 기업 내 안전한 정보통신망 구축을 담당하는 하나의 조직을 일컫는 것이며, 인증 서비스란 인증기관이 제공해 주는 인증서 발급, 인증서 관리 등 일련의 인증 관련 서비스를 통칭하는 것이라고 말할 수 있다.

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, 부인봉쇄 등의 정보보호 서비스를 제공해 주는 효과적인 솔루션으로 자리잡고 있다. 이러한 배경으로 인하여 컴퓨터 네트워크 보안과 관련된 많은 국제 표준화 단체나 개발 업체들이 공개키 암호 기술이 적용된 프로토콜이나 제품들을 출시하고 있으며, 이것은 상업적 목적을 갖는 인증기관 탄생의 기반이 되었다.

일반적으로 인증 서비스는 두 가지 분류로 나뉘어진다.

첫째는 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. 둘째는 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, 남아

〔표 3〕 국내·외 전자서명법 비교표

항목	미국(유타주)	독일	유엔(UNCITRAL)	한국
정의	○디지털서명을 주 대상으로 하면서 40가지 용어에 대한 매우 자세한 정의 제시 (제103조)	○디지털서명을 주 대상으로 하며 용어의 정의 제시(제2조) - 디지털서명, 고급전자서명, 공인전자서명, 인증기관인증서, 시점증명	○서명, 전자서명, 안전한 전자서명(제1조), 디지털서명(제4조), 인증기관(제7조), 인증서(제8조), 인증실무준칙(제9조)	○전자서명을 주 대상으로 하면서13가지 용어의 정의 제시 (제2조)
주요대상	특정 용도에 국한없이 디지털서명이 사용되는 모든 경우에 일반적으로 적용	○일반적 용도	○일반적 용도	○일반적 용도
법적효력	○디지털서명의 요건 규정 (제401조) ○디지털서명된 메시지를 종이문서와 동일한 효력을 가진 것으로 인정할 수 있는 요건 규정(제403조) ○디지털서명과 관련된 분쟁 재판 시에 대비한 추정 규정 (제406조)	○규정없음	○정해진 요건을 모두 갖춘 디지털서명은 안전한 전자서명으로 간주 (제5조) ○안전한 전자서명으로 인증된 메시지의 경우, 메시지가 변경되지 않은 사실, 본인의 서명이라는 사실, 서명할 의사로 본인에 의해 서명된 사실 등이 추정됨 (제2조)없음	○정해진 요건을 갖춘 전자서명은 법령이 정한 서명 또는 기명날인으로 간주 (제3조) ○안전한 전자서명이 있는 경우 전자문서 명의자의 서명이라는 사실과 전자문서가 서명된 후 그 내용이 변경되지 아니한 사실이 추정됨(제3조)
인허가 수단	○라이센스(허가)	○허가	○국가 개별법의 위임	○공인인증 : 지정 기타 : 허가
인허가기관 및 이유	○상업(division) ○특별한 이유 없음	○통신법상의 규제기관 ○주무관청(authority)으로 표현	○국가 개별법에 위임	○정보통신부
개인정보 보호	○규정 없음	○서명키 소유자 등의 청구가 있는 경우 인증서에의 접근을 차단할 의무 규정 ○개인정보 수집의 가능요건 규정	○사용자 확인 정보만 청구할 수 있도록 규정 ○개인정보 이용 준칙 관련 정보 제공 의무 규정	○최소한의 정보만 수집 가능 ○본인 동의 규정 ○수집정보의 타 목적 이용 금지
상호인증 문제	○규정 없음	○동일한 보안 수준을 입증하는 경우 외국의 인증서를 동일하게 인정	○국내 인증기관이 보증하는 경우 동일하게 인정 ○외국 인증서의 승인 요건 및 법적 효력 부여 요건 규정	○외국 정부와의 협정

〔표 4〕 VeriSign사의 인증 서비스 종류

종류	용도
S/MIME	안전한 전자메일용(암호화·전자서명) 인증서
SSL	웹 보안 프로토콜인 SSL을 웹 서버에 적용하기 위해 필요한 인증서(미국의 512비트)
Global 서버 ID	미국 외에서 강한 SSL을 사용하고자 하는 경우 필요한 인증서(1024비트, 미국 상무부의 허가 필요, 금융권으로만 제한)
OFX를 위한 금융서버ID	OFX 프로토콜 적용에 필요한 인증서
EDI 서버ID	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

프러카 공화국의 Thawte 인증기관 등에서 제공하는 S/MIME, SSL 인증 서비스를 들 수 있다.

3. 인증서비스 현황

인증 서비스는 앞에서 언급한 바와 같이 두 가지로 대별된다. 여기에서는 특정 도메인에서 안전한 네트워크 환경 구축을 위해 제공되는 인증 서비스는 제외하고, 일반적인 범용 인증 서비스 제공 업체들을 중심으로 살펴본다.

표 4는 VeriSign사의 인증 서비스 종류를 나타낸 것이다.

4. 인증기관의 분류

인증기관을 분류하는 방법에는 여러 가지가 있을 수 있으나 먼저 발행하는 인증서의 이용범위에 따라 인터넷과 같은 공공망에서 사용되는 인증서를 발행하는 공적 인증기관(public CA)과 조직의 내부망 즉, 인트라넷 등에서 이용할 목적으로 사용되는 인증서를 발행하는 사적 인증기관(private CA)으로 구분할 수 있다.

또한 인증기관의 주요 기능에 따라 신원인증기관, 내용인증기관, 신용인증기관 등으로 분류해 볼 수도 있다.

인증서비스가 가장 활발하게 진행되고 있는 미국의 경우에는 이 세 가지 종류의 인증서비스가 모두 제공되고 있고, 일본의 인증기관 관련 연구는 신원인증과 내용인증 기능을 모두 포함시켜 고려하고 있다. 그러나 인증서비스가 확산, 발전해 나간다면 하나의 신원인증기관에서 부대 서비스로 내용인증의 기능을 수행하거나 다른 신용조사기관과 연계하여 신용인증 서비스를 제공할 가능성이나 필요성도 커질 것으로 예상되므로 인증기관의 다양한 기능에 대한 보다 심도있는 고려가 필요하다고 하겠다.

한편, 국내·외 전자서명 및 인증 관련 법령에 인증기관의 인가나 인정 등의 사항이 포함되어 있는 경우가 많은데, 이러한 규정에 따라 해당 법령이 정한 기관의 인가나 인정을 받은 공인인증기관과 그렇지 않은 비공인인증기관으로 분류할 수도 있다.

5. 인증기관의 역할

인증기관의 가장 핵심적인 역할은 전자적 커뮤니케이션의 상대방이 정말로 그 사람인가를 확인해주는 신원인증 업무이다. 신원인증 업무의 일환으로 인증기관은 사용자의 신원을 확인하여 인증서를 발급하고, 전자서명키를 관리하며, 인증서를 확인하고, 인증서 및 인증서의 효력 변경사항을 공개하며, 사후 분쟁에 대비하여 인증서 관련 기록을 보존하는 등의 업무를 수행한다.

5.1. 사용자 신원확인

인증기관은 인증서 발행 신청자로부터 신원과 관련된 정보를 제출 받아 이를 통해 본인 여부를 확인한다. 사용자 신원 확인의 구체적인 방법에 대해서는 인증 서비스의 수준에 따라 다를 수 있으나, 통상 개인의 경우에는 운전면허증, 여권, 주민등록증, 의료보험증, 인감 증명 등에 의한 확인방법을 사용한다. 이 외에도 신용카드 회사와 연계하여 고객의 신원을 확인하는 절차의 수준에 따라 인증서 사용용도나 요금 등 인증 서비스의 수준이 결정된다.

5.2. 인증서 발행

사용자의 신원을 확인한 후 인증기관은 전자서명 검증키를 소유하는 자의 신원을 확인하여 그 귀속관계를 증명하는 인증서를 발행한다. 인증서는 인증서 수령자가 필요로 하는 최소한의 정보가 기재되는 것이 필요하다. 구체적인 기재사항은 인증 서비스의 내용에 따라 다르지만, 기본적으로 X.509 등의 국제 표준에 따르는 것을 권고한다.

5.3. 전자서명키 관리

인증기관은 가입자의 전자서명 검증키를 인증기관의 저장소에 등록하고 이를 관리한다. 또한 가입자가 원할 경우 전자서명키를 생성하여 주거나 이를 보관, 관리한다. 인증제도의 원활한 운영을 위해서는 전자서명 생성키의 안전한 보관 및 관리가 필수적이므로, 원칙적으로 전자서명생성키는 그 소유자만이 보관하여야 하지만, 기술적인 어려움 등으로 가입자가 키를 생성하기 어려운 경우에는 가입자의 명확한 동의가 있는 경우에 한해서 인증기관이 전자서명생성키를 생성할 수 있다. 이 경우에도 가입자의 허락 없는 사용이나 유출을 엄격하게 금지하는 등 매우 신중하고 강도 높은 안전 조치의 강구가 필수적이다.

5.4. 인증서의 공개 및 효력변경 사항 통지 및 공표

인증기관은 발행한 인증서를 일정한 저장소에 등록하여 누구나 확인할 수 있도록 공개한다. 인증서를 받은 사용자는 상대방의 인증서의 진위여부를 확인하기 위하여 인증기관의 저장소에 접속하여 이를 확인한다. 인증서가 정지, 폐지 또는 효력이 회복된 경우 인증기관은 누구나 용이하게 사용할 수 있는 수단을 통해 이 사실을 확인할 수 있도록 해야 하며, 효력 변경 시점에서 뿐만 아니라 그 이후에도 참조가 가능하도록 CRL의 형태로 공표하는 것이 필요하다. 혹은, OCSP 응답자(OCSP responder)가 인증서 상태조회 서비스를 제공하는 것이 가능해야 한다.

5.5. 제3자로부터의 문의에 대한 확인

제3자가 자신의 거래 상대방인 특정 가입자의 인증서에 관한 확인을 구할 경우 인증기관은 이에 대하여 확인 회답을 한다.

5.6. 인증관련 기록의 보존

인증서의 발급에 필요한 자료, 인증서 발급 및 운영과 관련된 자료는 추후 법적인 분쟁이 발생할 경우 매우 중요한 자료로 사용되므로 인증기관은 인증관련 기록을 인증서의 효력이 소멸된 이후에도 일정기간 이상 보관해야 한다. 보존 기간은 국내·외 전자서명 관련법에서는 주로 10년 이상의 기간을 명시하고 있다.

인증기관의 업무 중 가장 핵심이 되고 현재 가장 활발하게 시행되고 있는 업무인 사용자의 신원인증 업무 이외의 주요한 업무로는 전자적 커뮤니케이션의 내용과 일시 등을 확인하는 내용인증 업무가 있다. 현재 서비스 중인 대부분의 인증기관에서는 주로 신원인증 업무만을 제공하고 있지만, 전자적인 내용인증 서비스를 상용화하여 제공하고 있는 인증기관들도 있다. 내용인증 업무에는 전자문서의 내용을 인증기관이 증명하는 내용증명, 사설증서의 전자공증, 전자문서의 보존 등이 포함된다.

또한 전자적인 커뮤니케이션이 보다 복잡해지고 응용서비스의 범위가 넓어짐에 따라, 위와 같은 신원인증과 내용인증 업무 이외에 고객의 지급능력이나 사이트를 개설한 기업의 신용도를 인증기관이나 타 기관이 보유하는 정보를 이용하여 확인, 증명하는 신용확인 업무의 필요성도 커지고 있다.

6. 인증 관련 기관 등 현황

6.1. 국내현황

국내에서는 전자서명법 시행(1999.7.1)으로 정보통신망을 통한 비대면 전자문서의 교환 및 전자상거래의 안전 및 신뢰성 확보를 위한 국가차원의 전자서명 인증제도를 마련하였다. 공개키기반구조(PKI)에 의한 국내 전자서명 인증관리체계의 구축 및 운영, 공인인증기관에 대한 인증서 발급 및 관리 등의 인증업무, 그리고 전자서명 인증기술의 개발 및 규격과 표준화를 목적으로 1999년 7월에 한국정보보호진흥원내에 전자서명인증관리센터(ROOTCA)를 설치하여 운영 중에 있다.

6.1.1. 국내 공인인증기관 현황

전자서명 인증제도에 따라 2000.2~2001.3간에 걸쳐 한국정보인증㈜, 한국증권전산㈜, 금융결제원, 한국전산원 등 4개 기관이 공인인증기관으로 지정되어 운영 중에 있다.

6.1.2. 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, OFX등)들은 지원하는 인증 서버는 개발되지 않은 상태이다. 현재 국내 인증 서버 개발 현황은 시장 형성 초기 단계이며, 향후 지속적인 발전이 있을 것으로 판단된다. 표 5는 국내 인증 서버 개발업체 현황을 나타낸 것이다.

〔표 5〕 국내 인증 서버 개발 업체 현황

업체명	제품명
소프트포럼	XecureCA
이니텍	INITECH CA
펜타씨큐리티	ISSAC-PKI
드림씨큐리티	Dream PKI
케이사인	KSignPKI

6.1.3. 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 제공하고자 최근 사업을 개시한 몇 개 업체에 지나지 않고 있다.

표 6은 국내 인증 서비스 제공 업체 현황을 나타낸 것이다.

〔표 6〕 국내 인증 서비스 제공 업체 현황

업체명	인증 서비스	인증 서버
엔트러스트코리아 (Entrustkorea.net)	웹서버인증	Entrust사 개발
㈜한국전자인증	서버인증, 전자메일인증, 개인인증	VeriSign사 개발
한국통신 커머스솔루션즈 -뱅크타운	서버인증, 전자메일인증, 개인인증, 가상 사설망 서비스 인증 및 보안	자체개발, 뱅크타운 CA
세넥스 테크놀로지 (SENEX Tech.)	서버인증, 전자메일인증, 개인인증	Digicert

6.2. 국외 현황

6.2.1. 국외 인증 서버 개발 업체 현황

현재 외국에는 수 많은 개발업체들이 있으며, 이러한 업체들은 인증 서버 개발 뿐만이 아니라 공개키기반구조(PKI) 구축을 위한 토탈 솔루션을 제공하고 있다. 또한, 여러가지 인증서 발급이 가능하도록 다양한 인증 서버들을 제공하고 있다. 표 7은 국외 인증 서버 개발 업체 현황을 나타낸 것이다.

〔표 7〕 국외 인증 서버 개발 업체 현황

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

6.2.2. 국외 인증 서비스 제공 업체 현황

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

또한, 미국의 경우 유타주에서는 3개의 공인인증기관(DST, ARCANVS, USERTRUST), 워싱턴주에서는 2개의 공인인증기관(VeriSign, ID Certify), 텍사스주에서는 1개의 공인인증기관(VeriSign)을 지정한 상태이다.

표 8은 국외 인증 서비스 제공 업체 현황을 나타낸 것이다.

〔표 8〕 국외 인증 서비스 제공 업체 현황

국가	업체명	특징
미국	Digital Signature Trust Company	유타주정부 공인인증기관
	ARCANVS	유타주정부 공인인증기관
	USER Trust Company	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

6.2.3. 국외 공인인증기관 현황

- 미국

· DST

DST는 유타주 최초(세계 최초)의 공인인증기관으로서 '96년에 미국 Zions First National Bank의 자회사로 설립되었다. DST는 유타주 정부

의 전자서명법 시행을 위해 저장소(repository) 서비스를 대행하였으며, 이후 공인인증기관과 공인저장소로 지정되었다.

· ARCANVS

유타주 2번째 공인인증기관으로서 초기 PGP에 대한 인증 서비스를 제공하고자 하였다. 그러나 최근 라이센스를 갱신하면서 인증 서비스의 종류를 개인용 인증서, HIPAA 사용자용 인증서, 공증기관·등록기관용 인증서, 서버용 인증서를 발급해주는 인증 서비스로 그 기능을 확대하였다.

· USERTRUST

USERTURST 네트워크는 디지털 인증서/디지털 ID/디지털 서명과 인터넷 보안 솔루션 및 어플리케이션을 제공하기 위해 전략적 제휴로 구성되었다.

· ID Certify

ID Certify사는 워싱턴주 정부 최초의 공인인증기관으로서 '98년 4월 지정되었다. ID Certify사는 가입자에게 스마트카드를 제공함으로써, 사용자의 전자서명생성키를 스마트카드에 보관하게 한다. 현재, 미네소타주의 의료 및 보건 부분에 관련된 인증 서비스를 제공중이다. 주요 인증 서비스는 Global Passport Certificate, National Passport Certificate, Corporate Passport Certificate, Professional Passport Certificate, Signature Passport Certificate, Transactional Passport

〔표 9〕 각국의 PKI 기술수준 비교

구분		미국(FPKI)	캐나다(GOCPKI)	한국(ETRI/PKI)
암호 라이브러리	서명 알고리즘	- RSA - DSA - EIGamal	- RSA - DSA	- RSA - DSA - KCDSA
	해쉬 함수	- MD5 - SHA - SHA-1	- MD2 - MD5 - SHA-1	- MD2/4/5 - SHA/SHA-1 - RIPEMD-160 - HAS-160
	키분배 알고리즘	- Diffie Hellman - KEA - RSA	- Diffie Hellman - RSA	- Diffie Hellman - RSA
	암호 알고리즘	- DES - SKIPJACK - IDEA - 3-DES - RC4/5	- DES - CAST - 3-DES - RC2	- DES - 3-DES - IDEA - RC2/4/5 - Blowfish - SEED
암호 API		- GSS-API - GSS-IDUP	- GSS-API - GSS-IDUP	- CSP/CDSA
디렉토리 API		- LDAP - DAP	- LDAP - DAP	- LDAP
인증서 API		- CSSM/CDSA - PKIX-Profile (RFC2459)	- PKIX-Profile (RFC2459)	- CSSM/CDSA - PKIX-Profile (RFC2459)
인코딩		ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690	ITU-T X.680 ITU-T X.690
인증서 규격		- PKIX-Profile (RFC2459) - ITU-T X.509	- PKIX-Profile (RFC2459)	- PKIX-Profile (RFC2459)
인증서 관리 프로토콜		- PKIX-CMP(RFC2510) - MISPC	- PKIX-CMP(RFC2510) - MISPC	- PKIX-CMP(RFC2510)

Certificate 발급 서비스이다.

ID Certify사는 저장소를 캐나다 뱅쿠버에 두고 있으며, RA를 관련 업체에게 제공하는 방식으로서 운영한다.

· VerySign

VerySign은 '95년 4월 RSA사의 자회사로 설립되었다. 초기 SSL과 S/MIME에 대한 인증 서비스를 주 사업 영역으로 하였으며, 점차적으로 인증 서비스를 다양화 시켰다. VeriSign은 세계 인증 서비스를 주도하고 있는 사업체로서 전 세계에 많은 자회사 및 협력사들을 가지고 있으며, '98년 8월 워싱턴주 정부로부터 S/MIME Class3(VeriSign 인증업무준칙 버전 1.2의 2.2.3)에 대해 공인 지정을 받았다. 또한, '98년 10월에는 텍사스주 정부로부터도 공인인증기관 지정을 받았다.

- 독일

· 도이치 텔레콤 텔레섹(Deutche Telecom Telesec)

'98년 설립된 도이치 텔레콤내 정보보호 전문조직으로 '98년 인증기관 허가를 받아 인증업무를 수행하고 있다. 조직 구조상 도이치 텔레콤내 본부의 멀티미디어 사무소 산하기관이지만 인증업무의 독립성 확보를 위하여 본부조직으로 독립적으로 운영되고 있다.

6.3. 각국의 공개키기반구조

공개키기반구조란 일종의 암호키 관리시스템으로서 공개키방식에 의한 서명용 키의 생성·분배·인증 등의 절차를 정하고 구현하는 기반구조를 말한다. 이 공개키기반구조는 전자서명 및 데이터 암호화 키의 생성·분배·보관 등을 관리하고, 키의 귀속관계를 인증하는 인증서의 발급, 열람, 사용, 저장, 효력중지, 취소 등의 기능을 한다.

현재 각국에서 국가적인 프로젝트차원에서 공개키기반구조 구축 및 전자서명 인증업무 관련 연구가 진행중이며, 표 9는 이에 대한 각국의 PKI 기술 수준을 비교하여 나타내었다.

V. 응용분야

1. 개방시스템의 전자거래

정보기술의 발달에 따라 전자적으로 거래를 수행하는 방식도 점차로 발전되어 왔다. 최근 인터넷 등의 공개적인 네트워크가 발전하기 이전의 단계에서 이미 전자거래가 행해졌는데, 그 대표적인 예가 EDI라고 할 수 있다. EDI는 폐쇄적인 시스템의 대표적인 응용 서비스로서 사용자가 직접 시스템에 물리적인 통제를 할 수 있고, 사전에 인가된 절차에 따라 안전한 통신을 수행하여, 사용자와 시스템 운영 책임자간에 법적 의무사항 등이 명시됨에 따라 보안성과 안정성이 쉽게 확보된다는 특징을 가지는 반면, 전자거래는 제한된 사용자가 제한된 영역으로 사용하고, 특정 거래에 참여하는 모든 당사자들의 권리와 책임이 일련의 계약을 통해 정의된다.

이에 비해 개방시스템의 전자거래는 거래당사자간에 사전적인 관계가 없는 경우에도 거래를 가능케 함으로써 거래비용을 감소시키고, 다수의 다양한 사람들에게 접근 기회를 제공하며, 시장의 범위를 전 세계로 확장하여 새로운 유형의 사업기회를 제공하고 있다. 그러나, 폐쇄적 시스템에서의 상거래에 비해 거래의 측면에서는 불확실성과 위험이 증대하며 기술적 측면에서는 보안(security)의 취약성이 크다는 단점도 지니고 있다. 이러한 문제점은 거래 당사자의 신원이나 거래 의사의 확인이 어렵고, 폐쇄 시스템에 비해 거래 당사자의 권리와 의무가 계약으로 분명하게 규정되어 있지 않다는 것과 개방시스템의 속성상 불특정 다수의 거래 참여자가 보안성이 취약한 정보통신기반을 사용하는 것에서 기인한다. 따라서, 중요한 전자문서는 이미 상호협정관계 또는 상호 신뢰가 형성된 당사자간의 폐쇄 네트워크를 통하여 교환되는 경향이 있다. 이는 개방시스템이 가져다 주는 새로운 기회를 충분히 활용하지 못함으로써 전자상거래의 활성화를 저해 시키는 요인이 된다고 볼 수 있다.

이러한 불확실성 및 위험의 증대와 보안의 취약성을 극복하기 위해 개방형 네트워크에서 전자거래에 참여하는 주체들의 요구사항은 크게 판매자와 구매자의 관점으로 구분하여 살펴볼 수 있다. 판매자는 구매자의 신원을 확인함으로써 주문과 지불을 보장받으려는 구매자 인증(authentication) 및 구매자의 상품 구매를 위한 권한 소지 여부에 대한 증명(certification)을 요구한다. 또한 대금 지불과 관련하여 판매자는 구매자가 실제로 대금을 지불했는가에 대하여 카드회사 등의 거래와 관련된 기관에서 확인(confirmation)을 하고자 하며, 구매자가 주문사실이나 상품의 배달 사실을 부인할 수 없기

(non-repudiation)를 바란다. 한편, 구매자는 구매 전에 판매자의 신원을 확인하여 상품 및 서비스를 보장 받고자 하는 판매자 인증(authentication)과 지불 및 문서전송 시의 변조로부터 보호 받고자 하는 무결성(integrity)을 요구한다.

또한 거래수행사항을 사후적으로 확인(confirmation)하기를 원하며, 특히 제3의 기관에 공개되는 구매자의 개인정보(privacy)에 대해 보호 받기를 요구한다.

이러한 요구사항을 만족시키기 위해서 전자서명 인증제도를 필요로 하게 되는데, 전자서명 인증제도는 이러한 요구사항을 모두 해결하는 것은 아니지만, 인증, 확인, 증명, 무결성 및 부인봉쇄 등의 핵심적인 부분을 해결할 수 있는 기반이 된다.

개방형 전자거래에서 전자서명이 활용되는 구체적인 예로서 인터넷 서점, 인터넷 오락, 비즈니스, 전자쇼핑, 사이버몰 및 전자증권 중개업 등에서의 대금지급과 관련하여 인터넷에서 SSL 프로토콜을 사용하는 경우가 많은데, 이 경우 선택적으로 전자서명 또는 인증서가 이용되고 있다. SSL에서 전자서명이 이용되는 것은 SSL의 handshake 프로토콜에서 살펴볼 수 있다. 지불관련 문서 등의 HTML 문서가 SSL 프로토콜을 이용할 경우 브라우저와 서버 사이에 일련의 통신 프로토콜을 통해 세션키(session key)를 생성하게 되는데, 여기에 선택적으로 브라우저 및 서버의 인증서를 요구할 수 있도록 되어 있다. 아직 서버의 인증서만이 요구되어지는 관계로 사용자 브라우저에는 자신이 인증서를 발부 받지 않는 경우에 인증서가 존재하지 않으므로, 실제적으로는 암호만이 사용된다.

전자우편의 인증은 S/MIME을 이용할 수 있는데, Netscape 또는 Explorer 등의 브라우저에 VeriSign 등의 인증기관에서 발행한 인증서를 등록한 경우에는 그 인증서를 전자우편에 부착하여 송신하고 수신자는 전자서명에 따른 송신자의 인증서와 전자서명된 문서임을 확인할 수 있다.

2. 전자지불 및 홈뱅킹

전자지불 방식은 크게 기존의 지불결제수단을 지불서비스기관(payment gateway)을 이용하여 사용하는 지불브로커형 방식과 전자화폐형이 있다. SET은 크게 고객, 상점, 지불서버(혹은 지불 게이트웨이), 인증서버 및 금융기관으로 이루어지는데, 데이터의 무결성과 송신자 확인 및 송신자의 부인봉쇄를 위해 전자서명을 사용한다. 이때, 인증서는 인증서버로부터 발급 받으며, 인증서버의 최상위는 Visa/Master 인증기관이 있고, 나라별로 지역인증기관(geographic CA)이 사용자, 상점 및 지불서버에 인증서를 교부한다. SET에서 전자서명이 사용되는 특이한 경우는 이중 전자서명(dual signature)으로 고객으로부터의 정보를 크게 지불정보(payment information)와 주문정보(order information)로 나누어 상점은 지불정보를 알 수 없고, 지불서버는 주문정보를 알 수 없게 하는 식으로 전자서명을 한다.

홈뱅킹에서 전자서명은 고객으로부터의 송금, 계좌 이체 등을 요청 받았을 경우 본인확인과 내용확인을 하는 데에 사용이 가능하다. 현재 국내에서는 홈뱅킹 뿐만 아니라 인터넷 뱅킹 또한 허용되고 있으며, 전자서명을 이용한 서비스도 제공된다. 이를 통해 잔액조회, 거래 명세 조회, 자동 이체 등의 여러 가지 은행 업무를 수행할 수 있으며, 당사자 인증과 내용 인증이 보장된다.

3. 공문서의 전자적인 신청, 발급 및 이용

3.1. 민원행정

전자서명 및 인증제도는 전자상거래 뿐 아니라, 공공기관이 발행하고 있는 등기, 호적, 주민등록등본 등의 문서들을 일반인이 네트워크를 통하여 신청하고 발급 받기 위해서도 필수적이다. 이러한 응용이 가능한 각종 신청 수속은 출생, 혼인, 사망 신고 등 각종 신고사항의 신구소속, 주민등록 및 호적등본 등 각종 증명서의 교부, 그리고 토지, 건축, 선박 등의 등기 등 현재 민간부문에서 신청하여 발부 받는 거의 모든 공문서에 해당할 것이다. 각종 신청서나 각종 증명서의 교부를 정보통신 서비스를 통해 할 경우 전자서명을 이용하여 신청자 본인 확인이나 신청 내용의 확인을 할 수 있다. 국내의 경우 공공기관 보유 데이터가 아직 완전히 디지털화되어 있지 않으나, 향후 디지털화된 문서를 네트워크를 통해 필요한 사람에게 증명하기 위해서는 인증기관의 인증이 필요할 것으로 보인다.

3.2. 정부정보의 전자적 교환

최근 들어 공공기관 내부 또는 공공기관 간에서도 업무의 효율성을 증진시키고, 보관문서의 양을 줄이

기 위해 전자문서의 사용이 확대되고 있는데, 이 경우에도 인증기관을 통한 문서의 작성자, 문서의 내용, 문서의 작성 시점 등에 인증이 필요할 것으로 보인다.

4. 전자공증 및 내용증명

전자공증제도는 전자적으로 작성된 계약서 등이 특정인에 의해서 작성되었다는 사실을 공증하고 확정일자를 붙이거나 전자적인 기록의 형태로 공증증서를 작성하는 것을 의미한다. 이 경우 공증인은 신청인으로부터 송신된 전자문서의 성립과 내용을 심사하고 공증문을 전자서명하여 신청인에게 송신하고 보관함으로써 기존의 공증을 전자화할 수 있다. 이 경우 공증인은 신원 인증에서 문서의 내용 인증 서비스를 부가적으로 제공하는 기관으로 해석되어 질 수 있으며, 전자서명 및 인증기관의 필요성은 앞서 말한 부인봉쇄를 통한 법적 안정성을 위해 매우 중요한 요소가 된다.

또한 현재 우체국에서 수행하고 있는 내용증명도 전자문서로 확대될 수 있는 바, 전자서명이 제공하는 무결성의 특징을 이용하여 인증기관 등의 객관적 제3자를 통한 전자문서의 내용증명이 가능하다. 이러한 전자문서의 교환에서 전자서명의 객관적 제3자로서의 인증기관이 시간증명과 내용증명을 수행하여 분쟁을 해결할 수 있다.

VI. 인터넷 전자상거래 정책

미국의 빌 클린턴 대통령은 '97년 7월 1일 글로벌 전자상거래 기본 계획(A Framework for Global Electronic Commerce)이라는 보고서를 통하여 인터넷을 통해 이루어지는 전자상거래에 대해서는 관세를 포함한 각종 세금을 부과하지 않고 또 정부의 개입도 최소화하겠다고 발표하였다. 또한 이를 성공적으로 추진하기 위해 세계 주요 국가와의 협상도 진행할 것이라고 밝혔다. 이 정책안의 주요 내용은 글로벌 전자상거래 발전을 위한 정부지원 차원에서의 기본원칙을 밝히고 있으며, 이들 다섯가지 기본원칙이 효과적으로 수행되어질 수 있는 환경을 구축하기 위하여 국제적으로 제시되고 논의되어야 할 아홉가지 주요 기반 과제들이 있다. 다음에서 글로벌 전자상거래 기본원칙과 국제적 주요 기반 과제에 대해 간단히 요약해 보았다.

1. 글로벌 전자상거래 기본원칙

1) 민간자율에 의해 전자상거래가 활성화되어야 한다.
2) 정부는 정부의 개입과 부적당하고 불필요한 제약들의 적용 없이 자유롭게 전자상거래가 이루어지도록 해야한다.
3) 정부는 단지 관련된 최소한의 법률을 제정하여 공정한 게임을 벌일 수 있는 환경만 만들어 제공하면 되는 것이다.
4) 정부는 인터넷의 독특한 특성(국경의 장벽이 없고 기술적 발전이 빠른 인터넷 공간의 특성)을 파악하여, 이에 알맞은 발전 방안들을 모색해야 한다.
5) 인터넷을 이용한 전자상거래를 전세계적인 차원으로 이루어져야 한다.

2. 국제적 주요 기반 과제

1) 관세와 과세(tariff and taxation)

인터넷을 통한 제품과 서비스 교역에 대해서는 관세를 부과하지 않도록 하며, 기존의 관련 과세제도 또한 국내·외로 간단하고 일률적으로 재정비되어야 한다.

2) 전자지불시스템(electronic payment systems)

상업적 기술 환경의 빠른 변화에 맞추어 전자지불 방식에 어떤 기술과 방법을 사용할 것이며 누가 개발할 것인지 분명하고 효율적인 전자지불시스템이 마련되어야 한다.

3) 전자상거래에 관한 일률적인 통상규약(uniform commercial code for EC)

인터넷 전자상거래에 이용될 일률적인 통상 규약의 개발 지원으로 효율적인 교역국간의 거래를 지원해야 한다.

4) 지적재산권의 보호(intellectual property protection)

판매자와 구매자들간, 또는 전세계적 차원의 전자상거래에서 거래되는 제품들에 대한 저작권, 특허권, 등록 상표 등의 지적재산권의 보호가 반드시 필요하다.

지적재산권을 보호하기 위해 세계 각국들은 국제지적재산권기구(WIPO)를 통하여 국제적인 합의를 이끌어낼 수 있도록 한다.

5) 프라이버시(privacy)

네트워크 환경 안에서 통신하는 개개인의 프라이버시를 보장하는 일 또한 중요하다. 특정 개인의 데이터를 이용하기 위해선 그 개인에게 어떤 데이터를 이용할 것인지, 그 데이터를 어떤 방식으로 사용할 것인지 알려주어야 하며, 이에 대한 불합리한 피해에 대해서의 보상도 고려되어야 한다. 또한, 온라인 통신망을 통해 개인정보 보호를 위한 효과적인 기술개발에 정부가 적극 지원한다.

6) 보안문제(security)

전자상거래가 이루어질 전세계적 정보 기반구조(global information infrastructure)는 반드시 완벽하게 보안이 이루어져야 하고 많은 사용자들에게 신뢰를 줄 수 있어야 한다. 미국정부는 이미 민간기업들과 힘을 합쳐 시장성 있는 공개키기반구조 구축에 전력을 다하고 있으며, 이는 사용자와 사회가 원하고 있는 안전장치의 역할을 충분히 수행할 것이다.

7) 정보통신 인프라와 정보기술(telecommunications infrastructure and information technology)

효율적인 인터넷 전자상거래가 이루어지기 위해 적합한 정보통신 인프라와 정보기술 확보가 이루어지도록 노력한다(정보통신인프라나 정보기술의 저가제공, 쉬운 사용자 접근 유도 등).

8) 내용(content)

인터넷 전자상거래를 통해 입수될 수 있는 부적절한 내용들에 대한 적절한 대책의 강구로 올바른 정보들을 접할 수 있도록 노력한다.

9) 기술적 표준(technical standards)

전자지불방식, 보안방식, 저작권 문제, 초고속 네트워크 기술, 데이터 전송방식 등 여러가지 분야에서 기술적 표준의 필요성이 많이 요구되고 있다. 이러한 기술적 표준의 개발에 관련해서 정부의 참여는 오히려 잘못된 표준을 독선적으로 선택할 확률이 높기 때문에 민간이 주도가 되어 자체적으로 경쟁적 체제하에서 해결되어야 한다.

VII. 결 론

지금까지 전자서명과 인증제도에 대한 국내·외 동향을 분석하여 보았다. 이러한 것은 자국의 현실을 반영하는 것이기는 하지만, 새로운 사회현상에 대하여 실제로는 규제하는 데 주안점을 두었다고 볼 수 있다.

그러나 디지털 환경하에서 정보화 사회의 패러다임을 구체화하기 위하여 법제화 및 체계화 되었다는 점에서는 그 의미를 달리하고 있다.

이제 기술적인 사항, 인증기관과 관련된 사항 및 제도적인 사항을 고려하여 법령과 제도가 지속적으로 보완 개선되어야 하며, 정보화 사회를 향한 비전의 제시가 형식에 머물러 이용자(소비자)의 법적 지위를 현재 보다 열악한 사정으로 추락하게 하는 결과를 가져오지 않도록 경계하여야 할 것이다.

우리나라는 이미 법령과 제도 등이 제정되어 시행중에 있다. 이는 국내인이 외국의 전자서명 인증기관을 통하여 인증받거나, 외국과 전자서명에 관한 국제 협의시에 중요하게 검토되어야 하는 대상이므로 '99년 2월에 UNCITRAL에 제시된 전자서명 통일규칙(안)에 관하여 계속적인 관심을 기울여야 할 것이다.

참 고 문 헌

[1] 법무부, "외국의 전자서명제도", 1997.

[2] 시구로 노리히코, 박춘식 역, "전자상거래", 이한출판사, 1997. 4.

[3] 한국정보보호센터, "인증분야에 대한 OECD국가의 논의사항 및 접근방법", 1998.

[4] 최인영, "전자상거래 혁명", 동일출판사, 1998. 11.

[5] 이종후, 류재철 "전자상거래에서 인증기관의 역할 및 임무", 1998. 12.

[6] 신일순, 김춘아, 박민성, "전자서명 및 인증제도", 정보통신정책연구원, 1998. 12.

[7] 이상진, 이충배, "전자상거래 이해와 활용", 두남출판사, 1999. 1.

[8] 오병철, "전자거래기본법", 법원사, 1999. 1.

[9] 정보통신부, "Cyber Korea 21", 정보통신부 고시 제 1999-29호, 1999. 4. 16.

[10] 김춘아, 강준모, "전자거래기본법, 전자서명법의 영향 및 의의", 정보통신정책연구원, 1999. 5.

[11] 김철환, 김규수, "전자상거래", 문원출판, 1999. 6.

[12] 이만영 외 5인, "전자상거래 보안기술", 생능출판사, 1999. 9.

[13] 허영국 외 4인, "전자상거래 인증기술", 한국전자거래(CALS/EC)학회, 1999. 9.

[14] 최영철, "전자서명 인증관리센터 구축 및 운영", 한국통신정보보호학회, 1999. 9.
[15] 김용준 외 4인, "전자상거래 인증서비스 체계", 한국통신정보보호학회, 1999. 9.
[16] 홍승표, 강회일, 이동일, "전자상거래 정보보호 기술 동향", ETRI 주간기술동향, 1999. 10.
[17] 정현수, 이동일, "전자거래시스템 및 관련법 분석", ETRI 전자통신동향분석, 1999. 10.
[18] 한국정보보호센터, "전자서명법 해설", 1999. 10.
[19] 배대헌, "전자서명, 인터넷법", 세창출판사, 2000. 3.
[20] 이석래 외 2인,"전자서명 인증기술 동향", 한국통신학회지, 2000. 10.
[21] 한국정보보호센터, "전자서명 인증관리센터 운영보고서", 2000. 12.
[22] 정보통신부, "전자서명법 개정 토론회", 2001. 5. 25.
[23] http://law.gov.au/aghome/advisory/eceg/summary.htm
[24] http://www.abanet.org/scitech/ec/isc/dsg.html
[25] http://www.commerce.state.ut.us/web/commerce/digsig/act.htm
[26] http://www.cse.dnd.ca/cse/english/gov8.htm
[27] http://www.doc.gov/ecommerce/E-comm.pdf
[28] http://www.e-commerce.go.kr
[29] http://www.ecommerce.gov/ecomnews/Electronic Signatures_s761.pdf
[30] http://www.iid.de/rahmen/iukdgbt.html
[31] http://www.mbc.com/commerce.html
[32] http://www.mpt.go.jp/policyreports/english/group/Internet/elec-auth2.html
[33] http://www.oecd.org/subject/e-commerce

〈著 者 紹 介〉

이 대 기 (Dai-ki Lee) 종신회원
1966년 2월 : 한양대학교 전자공학과 공학사
1987년 2월 : 한양대학교 전자공학과 공학석사
1966년 2월~1980년 3월 : 정보통신부 통신사무관
1980년 4월~1998년 7월 : 한국전자통신연구원 책임연구원, 부호기술연구부장
1998년 8월~현재 : 한국전자통신연구원 정보보호기술연구본부 초빙연구원, 프롬투정보통신㈜ 정보보호컨설팅 본부장
관심분야 : 정보보호/전자거래법·제도·정책, 네트워크보안, 정보시스템감리

김 희 선 (Hee-sun Kim) 정회원
1998년 2월 : 강원대학교 정보통신공학과 공학사
2001년 2월 : 한국정보통신대학원 대학교 공학부 공학석사
2001년 1월~현재 : 한국전자통신연구원 정보보호기술연구본부 인증기반연구팀 연구원
관심분야 : 컴퓨터/네트워크보안, 정보보호(PKI), 전자화폐

조 영 섭 (Yeong-sub Cho) 정회원
1993년 2월 : 인하대학교 전자계산공학과 공학사
1995년 2월 : 인하대학교 전자계산공학과 공학석사
1999년 2월 : 인하대학교 전자계산공학과 공학박사
1998년 12월~현재 : 한국전자통신연구원 정보보호기술연구본부 인증기반연구팀 선임연구원
관심분야 : 컴퓨터/네트워크보안, DBMS, 정보보호(PKI)

진 승 헌 (Seung-hun Jin) 정회원
1993년 2월 : 숭실대학교 전자계산공학과 공학사
1995년 2월 : 숭실대학교 전자계산공학과 공학석사
1994년 12월~1996년 4월 : 대우통신 종합연구소
1996년 5월~1999년 5월 : 삼성전자 통신연구소
1999년 6월~현재 : 한국전자통신연구원 정보보호기술연구본부 인증기반연구팀장
관심분야 : 컴퓨터/네트워크보안, 정보보호(PKI)

정 교 일 (Kyo-il Jung) 정회원

1981년 : 한양대학교 전자공학과 공학사

1983년 : 한양대학교 전자계산학과 공학석사

1997년 : 한양대학교 전자공학과 공학박사

1981년~현재 : 한국전자통신연구원 정보보호기술연구본부 정보보호기반연구부장/책임연구원

관심분야 : IC카드설계, 정보보호시스템, 주요정보통신기반보호, 신호처리

조 현 숙 (Hyun-sook Cho) 종신회원

1979년 2월 : 전남대학교 수학과 이학사

1991년 2월 : 충북대학교 전자계산학과 이학석사

2001년 2월 : 충북대학교 전자계산학과 이학박사

1982년~현재 : 한국전자통신연구원 책임연구원

1996년~1999년 1월 : 지상 S/W연구실장, 정보보호시스템연구부장

1999년 1월~2000년 5월 : 정보보호기술연구본부장

2000년 5월~현재 : 차세대보안응용연구부장

관심분야 : 컴퓨터/네트워크 보안, Conditional Access