電子署名과 認證에 관한 硏究
A Study on the Digital Signature and Certification Authority

金榮俊(Kim, Young-Joon)*

요 약 (ABSTRACT)

전자문서를 이용한 전자거래는 비접촉, 비대면으로 이루어지기 때문에 거래당사자간에 상대방의 신원과 거래의사의 진정성 여부를 확인하기 어렵고, 타인으로 위장하여 전자문서 등을 부정하게 사용할 위험이 있다. 또한 전자문서는 유통되는 과정에서 위·변조가 용이하고, 문서작성 사실을 입증하기 곤란할 뿐만 아니라, 전송 내용의 비밀 유지가 곤란하다는 문제점이 있다.

이 같이 전자문서 및 전자거래가 가지는 문제점을 해소하기 위한 방안이 암호기술을 이용한 전자서명과 인증문제이다.

세계 각국은 전자거래에서 전자문서의 내용을 증명하고 거래의 진정성을 법적으로 확보하기 위한 관련 법제를 추진하고 있다. 우리 나라도 전자서명법을 제정하여 1999년 7월부터 시행하고 있으며, 비록 전자거래법과 같이 시행초기라서 아직 법규정이 미비하나 전자거래의 시발점을 열었다는 점에서 의의가 크다고 할 수 있다.

이와 관련하여 전자거래에서 전자서명과 인증과 관한 기술적 내용과 일반적 논의를 살펴보고, 이와 관련된 국내외 동향과 최근 제정하여 시행중인 전자거래법과 시행령·시행규칙의 주요 내용을 검토하고 이를 중심으로 향후 전자서명 인증관련 주요 과제 및 방전 방안을 검토하고자 한다.

Key Word : 암호 기술, 전자서명, 전자인증

목 차

Ⅰ. 서 론

* 同德女子大學校 經濟經營學部 講師(경영학 박사)

최근 정보통신기술의 급속한 발달과 정보통신망 확산으로 종이문서가 전자문서로 급격히 대체되고 있으며, 전자상거래,[1] 기업간 거래 및 정보교환, 전자자금이체, 행정민원 신청, 공문서 결재 및 교환 등 전자문서를 이용하는 전자적 행위가 증가일로에 있다.

이러한 전자문서 이용으로 기업이나 정부의 생산성이 향상되고 국민 개인의 생활편익이 증진되게 되었다.

그러나 전자문서교환(EDI) 방식을 이용하는 전자거래는 비접촉, 비대면으로 이루어지기 때문에 거래당사자간에 상대방의 신원과 거래의사의 진정성 여부를 확인하기 어렵고, 타인으로 위장하여 전자문서 등을 부정하게 사용할 위험이 있다. 또한 전자문서는 유통되는 과정에서 위·변조가 용이하고, 문서작성 사실을 입증하기 곤란할 뿐만 아니라, 전송 내용의 비밀 유지가 곤란하다는 문제점이 있다. 종이문서와 전자문서의 특성을 비교하면 <표1>과 같다.

<표1> 종이문서와 전자문서의 특성

구분	종이문서	전자문서
기록 매체	종이	전자기록 매체
전달방법	우편, 인편	네트워크를 통한 전송
안전·신뢰성	위·변조가 비교적 어려움 종이의 물리적 특성으로 위·변조 식별 가능	위·변조가 용이함 전자기록매체의 물리적 특성으로 위·변조 식별 불가능
진정성 증명	수기서명, 날인	전자서명

이같이 전자문서 및 전자거래가 가지는 문제점을 해소하기 위한 방안이 암호기술을 이용한 전자서명과 인증문제이다. 거래 상대방의 신원을 확인하고 전자문서의 위·변조 및 부인을 방지하기 위하여 활용하는 것이 전자서명기술이며, 신뢰할 수 있는 제3자(인증기관)가 거래당사자의 전자서명을 인증해주는 것이 전자서명 인증제도이다. 또한 전송 내용의 비밀을 유지하기 위하여 사용하는 방안이 암호기술이다.

이와 같이 전자서명과 인증의 필요성이 강조되어, 세계 각국은 전자거래에서 전자문서의 내용을 증명하고 거래의 진정성을 법적으로 확보하기 위한 관련 법제를 추진하고 있다.

우리 나라도 전자서명법을 제정하여 1999년 7월부터 시행하고 있으며, 비록 전자거래법과 같이 시행초기라서 아직 법규정이 미비하나 전자거래의 시발점을 열었다는 점에서 의의가 크다고 할 수 있다.

따라서 본고에서는 전자거래에서 전자서명과 인증과 관한 기술적 내용과 일반적 논의를 살펴보고, 이와 관련된 국내외 동향과 최근 제정하여 시행중인 전자거래법과 시행령·시행규칙의 주요 내용을 검토하고 이를 중심으로 향후 전자서명 인증관련 주요 과제 및 방전 방안을검토하고자 한다.

---

1) 인터넷을 이용한 전자상거래는 시간적 공간적 제약을 받지 않는 새로운 문화로 자리 잡아가면서 전세계적으로 비약적인 성장을 하고 있다. OECD 자료에 의하면 2003년 전자상거래 시장규모는 약 1조불로 지구상의 모든 상거래의 15%에 이를 것으로 전망하고 있다. 또 세계 인터넷 사용자의 수는 1997년 말 9천 6백만명에서 2005년에는거의 10억명에 이를 것으로 예상된다(신홍식 외1인, "전자상거래 보안과 전자인증", 정보산업 1999. 5-6월호, 「한국정보산업연합회」, 1999. 6., 52면).

Ⅱ. 전자서명과 인증의 개요

1. 기술적 개요

(1) 의의

전자서명은 전자문서에 부착되거나 논리적으로 결합된 전자적 형태의 서명, 즉 수기서명(manual signature)의 전자적인 대체물로서 펜 대신에 컴퓨터를 매개로 하여 생성되는 정보라고 할 수 있다.[2] 여기서 '컴퓨터를 매개로'의 의미는 기술적으로 전송하고자 하는 전자문서의 메시지요약(message digest)을 만든후, 이를 송신자의 전자서명생성키(비밀키)를 이용하여 암호화(encryption)한다는 것을 의미한다. 기존의 서명이 서명자에만 의존하고 문서에 따라 변함이 없음에 비해 전자서명은 서명자 뿐만 아니라 전자문서(메시지)에 따라 달라지는 디지털 정보이다. 이러한 방식으로 생성된 전자서명이 송신되면, 수신자는 송신자의 전자서명검증키(공개키)를 이용하여 확인하게 된다. 확인이 된 경우는 전자서명의 특성상 송신자의 인증 및 문서의 무결성이 증명된 것이고, 이를 이용하여 차후에 부인방지의 기능을 할 수 있다.

암호기술을 이용한 전자서명을 실제로 운용함에 있어 전자서명이 유효하기 위해서는 전자서명생성키(비밀키)가 안전하게 보관되어야 하며 전자서명검증키(공개키)와 그 키를 소유한 사람이 일치한다는 조건이 충족되어야 한다. 전자와 관련해서는 전자서명생성키(비밀키)의 분실은 인감도장의 분실과 동일한 의미이고, 후자와 관련해서는 수기서명은 서명을 기명함에 따라 서명자와 물리적인 관계가 명백하다

그러나 전자서명의 경우는 그렇지 않기 때문에 문제가 발생할 수 있다. 이러한 문제는 송신자 및 수신자 모두에 의해 신뢰받는 제3자(trusted third party)로 하여금 전자서명키와 그 키를 소유한 사람의 신원을 입증하게 함으로서 해결이 가능하다. 이러한 행위를 "인증"이라 하고, 인증을 담당하는 기관을 "인증기관(Certification Authority)"이라 하며, 인증기관은 가입자의 신원정보와 전자서명검증키가 포함된 "인증서"를 발행함에 따라 이러한 문제를 해결한다.[3] 즉, "전자서명 인증"이란 전자서명검증키(공개키)가 자연인 또는 법인이 소유하는 전자서명생성키에 합치한다는 사실을 공신력 및 전문성을 갖춘 인증기관이 확인·증명하는 행위를 말한다.[4]

(2) 암호 기술

전자서명과 인증을 이해하기 위하여는 그 전제가 되는 암호기술의 이해가 필요하다.

---

2) 전자서명법 제2조에 의하면 "전자서명이란 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 그 전자문서에 고유한 것을 말한다"고 규정하고 있다. 전자서명이 갖추어야 하는 요건은 다음과 같다. 첫째, 서명자의 인식이 가능하여야 한다. 둘째, 문서내용의 변경 여부를 확인할 수 있어야 한다. 셋째, 동일한 전자서명의 재사용이 불가능하여야 한다. 넷째, 문서작성 사실에 대한 부인을 방지할 수 있어야 한다.

3) 신일순 외1인, 「전자서명 및 인증체도」,정보통신정책연구원, 1998. 12, 24면.

4) 이러한 인증기관은 불특정다수인의 전자서명키 인증을 효율적으로 수행하고, 전자서명키 인증의 공신력을 제고하여 전자문서 이용관련 분쟁을 최소화하기 위하여는 인증기관의 존재가 필수적이다. 인증기관은 이를 위하여 서명자, 전자서명검증키 등의 정보가 포함된 전자적 인증서를 발급·정지·폐지하고, 인증관련 기록보관 등의 인증업무와 시점확인(Time Stamp), 내용증명 등의 부수업무를 수행한다.

암호기술은 크게 암호 알고리즘을 사용하는 키의 수 혹은 키의 관리방법에 따라 이를 대칭키 암호시스템과 비대칭키 암호시스템으로 구분한다.

대칭키 암호시스템은 관용키 시스템 혹은 비밀키 시스템이라고도 하는데, 이 암호기술에서 는 두 사람이 비밀리 통신하기 위해서 자신들만이 아는 공통비밀키(secret key)를 이용하여 암호화(encryption)와 복호화(decryption)를 한다. 반면에, 비대칭키 암호시스템은 공개키 암호기술이라고도 하며, 암호화에 사용하는 키와 복호화에 사용하는 서로 다른 키, 즉 비밀키(private key)와 공개키(public key)라는 두 가지 키를 이용한다. 이 중에서 비밀키는 그 키의 소유자만이 간직하고, 공개키는 그 사람과 통신하고자 하는 모든 사람에게 공개된다. 단, 공개키로부터 비밀키를 구하는 것은 어려워야 한다.[5] 전자의 대표적인 예로 RSA, ElGamal 등이 있으며, 후자의 예로 DES, SKIPJACK, IDEA 등이 있다.

공개키 암호 기술과 대칭키 암호 기술의 장단점을 살펴보면<표2>과 같다.

<표2> 대칭키와 비대칭키 암호 기술

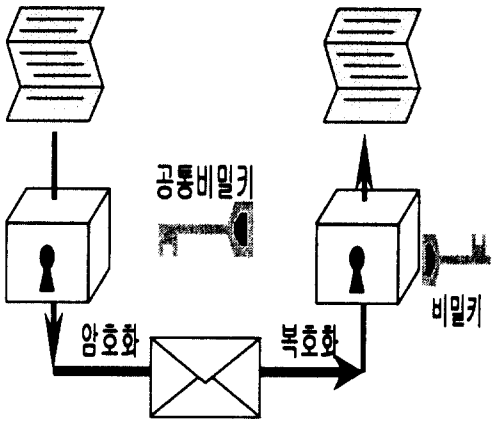
구분	대칭키 암호 기술	공개키 암호 기술
장점	- 암호화와 복호화 속도가 빠름 - 키길이가 상대적으로 김	- 키 분배가 용이함 - 상대적으로 네트워크의 사용자가 증가함에 따라 관리해야 할 키의 개수가 적음 - 상대적으로 키 변화의 빈도가 적음
단점	- 안전한 키 분배가 어려움 - 네트워크의 사용자가 증가함에 따라 관리해야 할 키의 개수가 많아짐 - 안전성을 위해 키를 자주 바꿔야 함 - 응용분야의 제약	- 암호화와 복호의 속도가 느림 - 키 길이가 상대적으로 짧음

위에서 살펴본 바와 같이 대칭키 암호 시스템은 인터넷과 같은 큰 규모의 네트워크에 이용하기에는 여러가지 제약점이 있다. 반면 공개키 암호 기술은 상대방의 공개키만을 알면 되고 그 공개키는 공개되어 있으므로, 키 관리가 대칭키 암호 기술에 비해 매우 용이하다. 그러므로 현재의 인터넷을 이용한 많은 응용 분야에서는 공개키 암호 기술을 이용하는 추세이다.

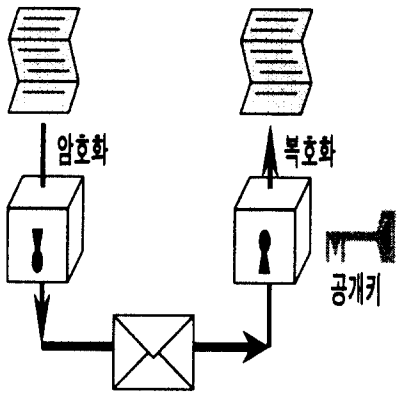
전자인증서는 공개키와 이를 소유하는 개인 또는 기관의 귀속관계등을 인증기관이 확인, 증명한 전자적 정보를 말한다. 전자인증서란 인증기관이 요청된 인감등록에 대하여 도장을 본인 확인 후 발행한 인감증명서라 할 수 있다.

인증서는 일반적으로 X.509 Certificate라는 표준을 따른다. 이 표준에 따라 인증서에는 도장의 역할을 하는 공개키에 대한 인증기관의 인증뿐만 아니라 공개키 알고리즘, 서명자, 서명방식 등의 정보가 기록되어 있다. 전자인증서에는 크게 전자문서과 암호·복호화에 사용된다.[6]

5) 백형기 외1인, 전자상거래 시대의 법, 미래와 경영, 2000.8., 185면.
6) 신홍식 외1인, 전게논문, 53면.



(그 림 1) 대칭형 암호시스템



(그림 2) 비대칭형 암호시스템

(3) 전자서명의 절차

1) 전자서명의 생성

전자서명을 사용하기 위해서는, 첫 번째 단계로 사용자는 전자서명검증키(공개키)와 전자서명생성키(비밀키) 쌍을 생성하여야 한다. 키의 생성은 자신이 가입한 인증기관에서 사용하는 공개키 알고리듬 중의 하나에 따르거나, 특정한 알고리듬에 따라서 사용자가 직접 생성한다. 비밀키는 개인이 안전한 장소에 안전한 방법으로 보관하여 다른 사람에게 공개해서는 안되며, 전자서명검증키(공개키)는 인증기관에 등록하여 일반인에게 공개한다.[7]

두 번째의 단계는 사용자가 송신할 전자문서의 메시지를 해쉬기능(Hash Function)을 통해 요약(digest)하고[8] 생성하는 단계이다.

세 번째 단계는 메시지 요약을 송신자의 전자서명생성키로 서명하여 전자서명을 생성하는 데, 보안이 필요한 경우 암호화하면 된다. 경우 전자서명은 전자서명키에 해당하고 알고리듬에 따라 생성된다.

네 번째 단계는 생성된 전자서명을 원래의 메시지에 더하여 수신자에게 전송하는 단계이다.[9]

2) 전자서명의 검증

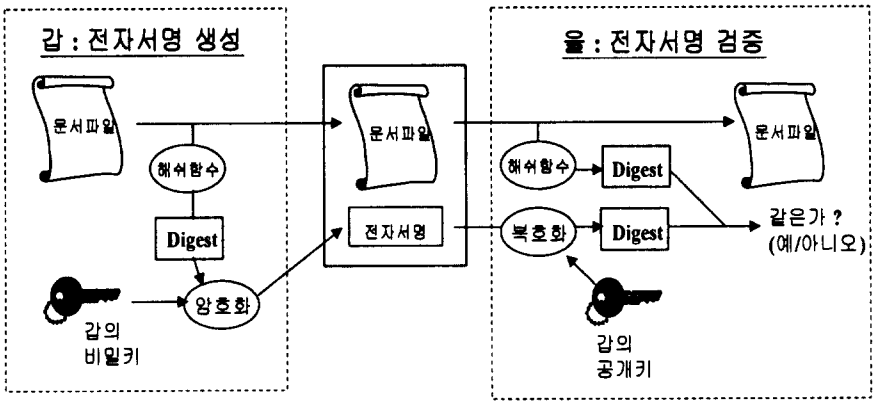
위와 같이 사용자가 생성한 전자서명을 수신자가 확인 또는 검증하는 단계를 살펴보면, 첫 번째 단계로 전자서명된 메시지(메시지와 그의 전자서명값)를 수산자가 받으면, 수신자의 컴퓨터에서 송신자의 전자서명검증키를 이용하여 송신자의 메시지 요약을 복원한다. 만일 메시지 요약이 복원되지 않으면 송신자의 전자서명검증키가 진정한 것이 아니므로 송신자의 신원확인에 실패한 것이 되고, 전자서명의 복호화(확인)가 가능하면, 송신자가 일치함을 확인(송신자의 신원확인)한다. 다음으로 수신된 메시지의 메시지요약을 만들어 이미 복원한 메시지 요약과 비교한다. 양자가 일치하게 되면,

7) 백형기 외1인, 전게서., 192면.

8) 전자문서의 메시지가 길 경우 서명을 생성하거나 확인하는데 많은 시간이 소요되므로 해쉬함수(Hash Function)를 통한 메시지 요약(message digest)이 필요하다.

9) 백형기 외1인, 전게서, 193면.

메시지가 바뀌지 않았음을 확인(메시지의 무결성 확인)한다.[10]
이상의 전자서명의 생성 및 검증의 내용을 요약하면 다음의 그림과 같이 나타나게 된다.



(그림 3) 전자서명 생성 · 검증 과정

(3) 인증절차

인증은 기술적으로는 어떠한 사람의 전자서명검증키가 그 사람의 것임을 신뢰받는(trusted) 제3자의 기관이 증명해주는 것을 의미한다. 이러한 의미에서 인증기관은 기존의 인감에 대한 인감증명기관, 인증서는 인감증명서 등에 해당된다고 이해할 수 있다. 그러나 수기서명에 비해 전자서명의 운용이 차이가 나는 것처럼 인증기관 인증서의 운용도 차별화된다.

인증을 받기 위해서, 사용자는 먼저 자신의 전자서명생성키(비밀키) 및 전자서명검증키(공개키)를 생성한다. 두 번째 단계로 사용자는 인증기관을 방문하여 자신의 신원을 증명하고, 전자서명검증키(공개키)를 제시하며, 전자서명검증키에 대응한 전자서명생성키(비밀키)를 소유하고 있는 사실을 제시한다. 세 번째 단계로 인증기관은 전자서명검증키(공개키)와 그 키에 대응하는 사람의 신원을 확인한 경우, 신원이 확인되면 인증서(certificate)[11]를 발행한다.[12]

여기서 인증서란 공개키와 신원이 증명된 사람과의 관계를 증명하는 전자적인 기록으로, 인증서에는 인증기관, 가입자, 가입자의 전자서명검증키 등의 정보를 포함하고, 인증기관의서명을 붙이는 것이 보통이다.

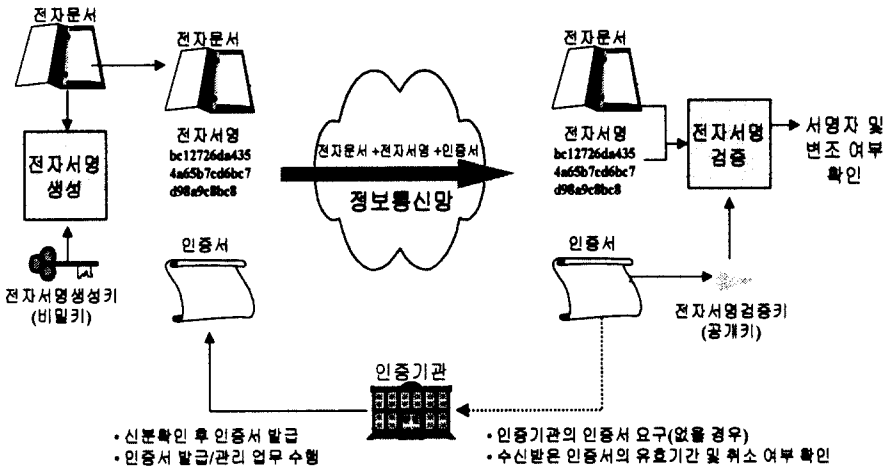
네 번째 단계로 인증기관은 가입자에게 인증서의 내용을 확인시키고, 인증기관은 인증관리체계를 통해 인증서를 모든 사람에게 접근 가능한 형태로 유지한다. 여기서 인증기관이 관리하는 인증관리체계에는 취소 또는 정지된 인증서의 목록이 포함되어야 한다.[13]

인증기관에서 인증서를 발급받으면 그 인증서를 메시지와 메시지의 전자서명에 첨부하여 송신하

10) 백형기 외1인, 전게서, 193면.
11) 인증기관은 인증서의 발급에서 취소에 대한 정책과 과정이 명시된 인증실무지침(CPS : Certification Practice Statement)을 발행하고 있다.
12) 구체적인 절차는 인증기관 및 인증서의 종류에 다라 달라질 수 있다. 예를 들어 Verisign Class 1 인증서의 경우는 신원증명을 e-mail 주소로 대신하여 직접 방문을 하지 않아도 된다.
13) 이를 인증취소목록(CRL : Certification Revolution List)이라 한다.

게 된다. 이때 수신자는 먼저 인증서를 인증기관의 전자서명검증키(공개키)를 이용하여 풀어서 송신자의 전자서명검증키를 얻고, 이 인증서가 인증취소목록에 포함되어 있는지의 여부를 확인한 후, 그렇지 않은 경우 송신자의 검증키를 이용하여 메시지요약을 생성한다.[14]

이상과 같이 인증서를 이용한 전자서명의 체계도를 살펴보면 다음의 그림과 같이 나타나게 된다.



(그림 4) 인증서를 이용한 전자서명 체계도

2. 전자서명과 인증의 필요성

(1) 전자적 컴뮤니케이션 상대방의 신원확인

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. 특히 최근 들어 급증하고 있는 기업-소비자간(business-to-consumer) 전자상거래가 본격화될 경우 사전적인 관계가 없는 상황에서 전자거래가 발생하게 되므로 당사자의 신원에 대한 불확실성은 더욱 높아질 것이고, 이에 따라 디지털서명의 필요성이 증가할 것이다.[15]

(2) 전자서명된 문서의 무결성 보장

무결성은 메시지 인증과 같이 메시지의 변조나 수정 등을 검출할 수 있는 기능을 말한다. 이것은 일반적으로 해쉬함수나 블록 암호 등을 사용함으로써 구현 가능하다.[16]

원본과 복사본의 식별이 불가능하고 내용을 손쉽게 변조할 수 있는 전자문서의 특성 상 기존의 인장이나 서명과는 다른 새로운 수단이 필요하게 된다. 전자서명과 인증은 전자서명된 문서가 서명

14) 신일순 외2인, 전게논문, 25-30면.
15) 신일순 외 2인, 전게논문, 11면.
16) 신홍식 외1인, 전게논문, 52면.

자가 의도한 바로 그 문서로서, 전자문서의 생성, 유통, 보관과정 등에서 발생할 수 있는 변조가 일어나지 않았음을 입증하는 기능을 지닌다. 또한 전자화된 정보를 이용할 경우 내용을 변조하거나, 정당하게 이루어진 거래 또는 계약을 부인하는 것이 용이하므로, 이를 효과적으로 방지하여 거래당사자간의 분쟁을 최소화하고 전자상거래의 신뢰기반을 조성할 필요가 있다. 전자서명과 인증은 이러한 신뢰기반의 중요한 요소로서 작용한다.

(3) 법적 분쟁시 증거를 위해

현재 이루어지고 있는 전자거래와 관련된 분쟁이 발생했을 때, 인증기관의 인증서를 법원에 제출해 거래 상대방을 증명할 수 있다. 즉, 디지털서명의 부인봉쇄(non-repudiation)의 기능을 통해 증거자료화할 수 있다. 여기서 고려해야 할 점은 법적 분쟁 발생시의 위험배분을 위해 인증기관의 인증을 받은 문서는 진정 성립된 것으로 추정하는 규정이 존재하여야 한다는 점이다. 만약 관련법에서 위와 같은 위험배분에 대한 추정규정을 두지 않는다거나, 관련법이 아예 제정되지 않는 경우, 또는 제정된다 하더라도 인증기관의 인증을 받은 문서에 대한 진정성립 추정이 없는 경우, 인증기관의 인증서를 이용한 법적 분쟁의히소에 한계가 있기 때문이다.[17]

3. 주요 응용분야

전자서명 및 인증제도는 주요 응용분야를 살펴보면 다음과 같다.

첫째, 개방시스템에서의 전자거래가 지니는 불확실성 및 위험의 증대와 보안의 취약성을 극복하기 위해 주로 사용될 수 있다. 전자서명 및 인증은 개방네트워크에서 전자거래에 참여하는 주체들의 다양한 요구사항들 중 인증, 확인, 증명, 무결성 및 부인봉쇄 등의 핵심적이 부분을 해결할 수 있다고 판단된다.

둘째, 전자서명은 전자지불과 홈뱅킹 시에도 필수적으로 사용될 것이다. 먼저 고객으로부터의 송금, 계좌 이체 등의 요청 받았을 경우 본인확인과 내용확인을 하는 데에 사용이 가능하며, 신규 계좌 개설, 잔액조회, 거래 명세 조회, 자동이체, 수표발행 등의 여러 가지 은행 업무를 수행할 때 당사자 인증과 내용 인증의 보장이 필수적이므로 전자서명의 이용이 불가피할 것으로 판단된다.[18]

셋째, 전자서명은 공문서의 전자적인 신청·발급 및 이용시에도 사용될 것이다.

전자상거래에서 뿐 아니라 공공기관이 발행하고 있는 등기, 호적, 주민등록등본 등의 문서들을 일반인이 네트워크를 통하여 신청하고 발급받는 민원행정업무와, 공공기관 내부 또는 공공기관간에서 업무의 효율성을 증진시키기 위해서도 전자서명은 필수적이다.

넷째, 전자공증 및 내용증명에도 사용될 수 있다.

공증인은 신청인으로부터 송신된 전자문서의 성립과 내용을 심사하고 공증문을 전자서명하여 신청인에게 송신하고 보관함으로써 기존의 공증을 전자화 할 수 있으며, 현재 우체국에서 수행하고 있는 내용증명도 전자문서로 확대될 수 있는 바, 전자서명이 제공하는 무결성의 특징을 이용하여 인증기관 등의 객관적 제3자를 통한 전자문서의 내용증명이 가능하다.[19]

---

17) 신일순 외2인, 전게논문, 13면.

18) 은행들은 자기 은행의 소개나 상품선전에 치중하고 있으며 실제로 완벽한 은행업무를 니터넷상에서 처리하는 서비스를 제공하는 은행은 극소수이다.

Ⅲ. 전자서명법 관련 입법동향

1. 외국의 입법동향

(1) 유엔상거래위원회(UNCITRAL)

전자문서방식에 의한 국제거래가 점차 보편화함에 따라 유엔상거래위원회(UNCITRAL)에서는 1992년 5월 "전자자금거래에 관한 모델법(UNCITRAL Model Law on International Credit Transfer)"[20]과 1996년 6월 전자상거래실무그룹에서 제정한 "전자상거래모델법(UNCITRAL Model Law on Electronic Commerce)"[21]을 채택하였다. 전자상거래모델법 제7조에는 데이터메시지와 관련한 서명의 요건이 규정되어 있다.

이후 UNCITRAL은 동 모델법에 포함되지 않은 전자서명과 인증에 관련된 보다 상세한 사항을 규정하기 위하여 전자서명통일규칙의 제정작업을 추진하여 1998년 6월에 "전자서명통일규칙초안(Draft Uniform Rules on Electronic Signatures)"을 채택하였다. 전자서명통일규칙초안은 국제상거래에서 사용이 증가되고 있는 전자서명을 용이하게 함을 목적으로 하며, 특히 상거래행위의 사법적인 측면에 초점을 두고 있다.

전자서명통일규칙초안은 총 4장 19개조문으로 구성되어 있는데, 제1장은 적용범위 및 일반규정, 제2장은 전자서명, 제3장은 인증기관 및 관련문제, 제4장은 외국전자서명의 승인을 각각 규정하고 있다.

(2) 미국의 입법동향

미국에서의 전자상거래는 민간중심으로 추진되고 있고, 통일법이 아닌 개별법에 의한 규제를 하고 있으며, 기술력에 우위를 바탕으로 각종 국제회의에서 자국의 이익을 관철하기 위한 영향력을 행사하고 있다.

특히, 미국은 전자서명과 관련 미국법조협회(ABA)의 정보안전위원회(Information Security Committee) 과학기술 부문에서는 국제적 법률전문가 및 기술전문가들과의 협력하에 약 4년의 기간에 걸쳐서 디지털 서명법을 연구해 왔으며, 동 위원회는 1996년 8월 1일 "디지털 서명 가이드라인(Digital Signature Guideline : 이하 ISC가이드라인이라 함)" 최종본을 발표하였다. 이 가이드라인

19) 신일순 외2인, 전게논문, 12-13면.

20) 전자자금거래에 관한 법은 전자자금이체에 관한 제반사항을 규정하고 있으며 전자상거래모델법은 법명칭과 달리 전자상거래의 구성요소중 EDI 및 그와 관련한 법률적 문제를 규율하고 있다.

21) 유엔상거래위원회(UNCITRAL)는 1993년부터 EDI모델법 제정작업을 계속해 오다가, 1996년 5월부터 6개월에 걸쳐 뉴욕에서 유엔상거래위원회 제29차 위원회를 개최하여 EDI모델법의 제목을 "전자상거래모델법(UNCITRAL Model Law on Electronec Commerce)" 으로 개칭하여 이를 최종 채택하였다. 이 모델법은 전자상거래에 관한 제도적 장애를 제거하는 것을 그 목적으로 하고 있으며, 총 17개 조문으로 구성되어 그 적용 범위와 개념 정의 및 해석 원칙, 데이터 메시지의 법적 지위 및 효율적 데이터 메시지의 교환과 관련한 법률 관련의 규율, 물품운송 분야의 특별규정 등을 규정하고 있다. ; United Nations Commission on International Trade Law("UNCITRAL"), UNCITRAL Model Law on Electronec Commerce, 1966" ; 内田 貴, 電子商取引と法 - UNCITRAL「電子商取引モデル法」および通産省「電子商取引環境整備研究會中間報告」を中心として, NBL No.601-603(1996.9.1-10.15)

은 디지털 서명을 한 쌍의 열쇠를 쓰는 방법, 즉 디지털 서명을 창설하는데 쓰이는 비밀 키(private key)와 디지털 서명의 진정성을 확인하는 공개 키(public key)에 의하는 방법을 쓰고자 한다. ISC 가이드라인은 초안 형태로 널리 배포되었으며, 유타 주가 처음으로 동 가이드라인을 상당 부분 참조하여 디지털 서명의 사용을 공식적으로 인정하는 법안을 통과시켰다. 또한 독일의 디지털 서명법 제1초안도 동 가이드라인에 기초하고 있다.[22] 이 가이드라인은 그 부재 인증기관 및 전자상거래에 관한 법적 기반에서 나타나 있는 바와 같이 전자상거래에서 필요로 되는 디지털 서명 및 인증기관에 관한 법률·제도적 검토하에서 작정된 가이드라인이다.[23] 현재는 41개 주가 Utah주('95)의 전자서명법을 근간으로 입법을 제정, 시행하고 있다.

(3) 유럽의 입법활동

1) 유럽 연합(EU)

유럽에서 전자상거래에 관한 논의는 주로 EU의 집행위원회(European Commission)을 통해서 행해지고 있으며, 1992년에는 정보 보안 문제에 관한 회원국 위원회(Committee of Member States on Information Security Issues : "SOG-IS")가 조직되었다. EC는 1994년 8월부터 인증키관리서비스를 제공하고자 유럽 전역에 걸쳐 제3차 수탁자 서비스(Europe-wide Network of Trusted Third Party Services : "ETS") Proposal을 진행시키고 있으며, 동시에 ETS 준비 프로그램으로서 제3차 수탁자(Trusted Third Parties : "TTP")에 관한 수많은 파이롯트 프로젝트를 지원하고 있다.[24] 또한, EU는 "디지털 서명의 법적 문제에 관한 연구(A Study on the Signal Aspects of Digital Signatures)" 프로젝트를 진행 중이며, 그 내용에는 회원국과 EU 주요 무역 상대국의 디지털 서명에 관한 관행, 회원국 및 EU의 주요 무역 상대국의 디지털 서명에 관한 관행, 회원국 및 ED의 정책 및 현재의 법령에 대한 전반적인 검토가 포함된다.

2) 독 일

독일에서는 1996년 12월 20일 현재 디지털 서명법 최종안이 연방의회 하원에 제출된 상태이다. 멀티미디어법 최종안과 함께 디지털 서명법은 1997년 동안 의회의 논의과정을 거쳐 1997년 8월 1일자로 법률로서 제정되었는데, 최초로 제안된 초안과는 상당한 변화 과정을 거쳐서 오늘에 이르게 되었다. 동 법은 총 16개 조문으로 구성되어 있으며, 동법 제16조의 의해서 시행령이 함께 의회에 상정되었다. 지금까지 독일에서는 디지털 서명에 관한 조항이 독일정보통신관련기본법인 정보통신서비스법(Information and Communications Services Law)에서 제외되어 있었으나, 1996년 멀티미디

22) Richard L. Field, "The electronic future of cash: survey, 1996: Survey of year's developments in electronic cash law and laws affecting eletronic banking in the United States", 46 Am. U. L. Rev. 967.

23) ISC가이드라인은 전문, 해설 등을 포함하는 것이지만, 가이드라인 본문 부분은 「제1장 정의(Definitions)」, 「제2장 일반 원칙(General Principles)」, 「제3장 인증기관(Certification Authorities)」, 「제4장 등록자(Subscribers)」, 「제5장 디지털 서명에 대한 신뢰(Relying on Digital Signatures)」의 다섯 장으로 구성되어 있다 ; 室町正實·吉田一雄, "認證機關および電子取引に關する法的基盤の整備に向けて",NBL No.593, 1996.5.15 ; American Bar Association, "Digital Signature Guideline", 1995.

24) Ian Taylor MBE MP, Minister for Science & Technology in UK, "Licensing of Trusted Third Parties for the Provision of Encryption Services(Public Consultation Paper on Detailed Proposals for Legislation)", March 1997.

어법에서 디지털서명에 관한 내용이 포함되게 되었다(멀티미디어법 제3조).[25]

3) 영 국

영국에서는 1997년 3월 19일 인증서비스 제공을 위한 제3자 수탁자 허가(Licensing of Trusted Third Parties for the Provision of Encryption Services)라는 참고안(Consultation Paper)이 영국 통상산업성에서 발표되었다. 본 참고안은 7개 부로 나뉘어지는데, 제1부에서는 본 안을 소개하고 있고, 제2부에서는 TTP에 관한 정부의 정책이 발전해 온 전체적 정책구조를 개관한다. 제3부는 TTP의 촉진을 포함하는 정보보안에 관한 EC의 국제활동을 개관한다. 제4부에서는 암호기술과 데이터의 완전성과 기밀성을 보호하기 위한 암호기술의 관점에서 TTP 네트워크의 잠재적 이익을 개관하고, TTPs가 제공하여야 할 서비스의 범주를 지시한다. 제6부에서는 정부의 Proposal의 구조를 개관하고, 입법의 기초로서 필요한 영역에 관한 논평을 시도한다. 제7부에서는 정부에서 일반인의 의견을 청취하고자 하는 주제를 특정한다.[26]

(4) 일본

일본에서는 국제적인 전자상거래 추진과 발맞춰 INGECEP(Integrated Next Generation Electronic Commerce Enveronment Project)의 추진과, BCOM(Electronic Commerce Promation Council of Japan)를 개발하여 전자상거래 추진 기반을 마련하였다. 특히 전자서명과 인증에 대하여 신뢰성 있는 인증기관의 확보와 관련하여 공공기관이 되도록 할 필요성이 제기되고 있으며, 법무성이 인증기관으로 유력시되고 있다.

한편, 민간인증의 경우 공개기반구조에 입각한 인증체계의 시험운영을 실시하고 있는데, 재단법인 정보처리개발협회 산하기관으로 인증실용화실험협의회를 설치하여 하위인증기관(20개)의 인·허가를 담당하도록 하고 있으며, 2001년 실용화를 목표로 하고 있다.

2. 전자서명법 주요 내용

(1) 개 요

정보통신망을 통하여 처리되는 전자문서의 내용을 증명하고 거래의 진정성을 확보하기 위하여 전자서명법이 1999년 1월 제정되어 동년 2월 5일 법률 제5792호로 공포되어 동년 7월 1일부터 시행되고 있다. 전자거래법과 같이 시행초기라서 아직 법규정이 미비하나 전자거래의 시발점을 열었다는 점에서 의의가 크다고 할 수 있다.

전자서명법은 대부분 인증기관과 인증서 인증업무의 안정성확보에 초점이 맞추어져 있는데, 이 법에서 전자서명을 다음과 같이 정의하고 있다. "전자서명이란 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 그 전자문서에 고유한 것을 말한다"(전자서명법 제2조 제2호).

---

25) Translation and Commentary by Christopher Kuner, Esq., Gleiss Lutz Hootz Hirsch & Partners, Frankfurt, "German Digital Signature Law" , Final Draft, December 20, 1996.

26) Ian Taylor MBE MP, Minister for Science & Technology in UK, op. cit., March 1997.

(2) 전자서명의 법적 효력

전자거래의 활성화를 위하여 공인인증기관이 인증한 전자서명에 대하여 다음과 같이 법적 효력을 부여하고 있다.

공인인증기관이 발급한 인증서에 포함된 전자서명 검증키에 합치하는 전자서명 생성키로 생성한 전자서명은 법령이 정하는 서명 또는 기명날인과 동등한 효력이 있다. 이러한 전자서명이 있는 전자문서는 전자서명된 후 문서내용이 변경이 없었던 것으로 추정하게 되는 효력이 있다(동법 제3조).

(3) 공인인증기관

공인인증기관은 국가, 지방자치단체, 법인 중 인증업무를 안전하고 신뢰성있게 수행할 능력이 있다고 인정된 기관을 대상으로 정보통신부 장관이 공인인증기관[27]으로 지정한다(동법 제4조). 이때 임원중 결격사유[28]가 있거나 인증업무의 정지 및 지정취소처분을 받은지 2년이 경과되지 않은 경우에는 공인인증기관으로 지정받을 수 없다(동법 제5조).

공인인증기관은 인증업무를 시작하기전에 인증업무의 종류, 인증업무의 수행방법 및 절차, 인증서비스의 이용조건 및 요금 등에 대한 인증업무준칙을 제정하여 정보통신부장관에게 신고하여야 한다.[29]

1) 인증기관의 업무

인증기관은 한국정보보호센터로부터 전자서명검증키를 인증받아 이에 합치하는 전자서명 생성키를 이용하여 인증업무를 수행하되, 가입자나 인증서비스이용자를 부당하게 차별하거나 정당한 사유없이 인증서비스의 제공을 거부할 수 없다(법 제8,9조).

2) 인증업무의 이전 및 폐지

공인인증기관이 다른 공인인증기관의 업무를 양수하거나 합병할 때에는 정보통신부장관에게 관련서식에 따라 신고하도록 하고 있으며, 양수 또는 합병하는 법인은 종전의 공인인증기관의 지위를 승계한다(법 제9조). 또한 공인인증기관이 업무를 일시 휴지하고자할 때는[30] 휴지하고자 하는 날의 30일전까지 가입자에게 그 사실을 통보하고 정보통신부장관에게 신고하여야 한다. 그리고 인증업무를 폐지하고자 하는 경우에도 60일전까지 가입자에게 통보하고, 역시 정보통신부장관에게 신고하여야 한다(법 제10조).[31]

---

27) 미국은 정부의 라이센스를 받은 공인인증기관제도를 도입하고 있으며, 독일은 모든 인증기관의 허가제도를 도입하였다. 미국은 정보통신을 관장하는 상무부가 허가하며, 독일은 통신법에 의한 규제기관이 허가기관이다.

28) 금치산자, 한정치산자, 복권되지 않은 파산자, 금고이상의 형의 선고를 받고 형의 집행이 면제 또는 종료된 날로부터 2년이 경과되지 않은 자. 집행유예기간중에 있는 자, 자격상실 또는 정지자, 인증업무 지정이 취소된 법인의 취소 당시 임원이었던 자로 취소된 날로부터 2년 경과되지 않은 자(전자서명법 제5조 제1호).

29) 인증업무의 내용이 변경될 때 역시 신고하여야 하며, 신고한 인증업무준칙의 내용이 인증업무의 안전과 신뢰성확보에 지장을 초래하거나 가입자이익을 저해할 우려가 있는 경우는 정통부장관은 상당한 기간을 정하여 인증업무준칙 변경을 명령할 수 있다.

30) 휴지기간은 6개월을 초과할 수 없다.

31) 이때 가입자의 인증서 등을 타 인증기관에 인계하여야 하는데, 피치못할 사정으로 인계할 수 없는 경

3) 인증기관의 감독

공인인증기관에 대한 전반적인 감독은 정보통신부에서 행하는데, 정보통신부장관은 인증업무의 안전과 신뢰성의 확보를 위해 인증기관에 자료를 제출하게 하거나 관계공무원으로 하여금 직접 공인인증기관에 출입하여 인증관리체계 등을 검사할 수 있도록 하고 있다(특법 제14조). 이때 기관의 업무수행방법이 부적절하는 등으로 인증업무에 지장을 초래할 위험이 있거나 각종 명령이나 규칙에 위반한 경우 시정명령이나 6월이내의 업무정지, 인증기관지정의 취소, 과상금을 부과시킬 수 있다(동법 제11조 내지 2조13호).

(3) 인증서

인증서란 존자서명검증키가 전자서명생성키에 합치한다는 사실등을 확인·증명하는 전자적 정보를 말한다(동법 제2조 제7호). 공인인증기관이 이러한 인증서를 발급할 때에는 법에서 정한 일정사항을 기재한 인증서[32]를 공인인증기관의 전자서명후 발급하여야 한다. 이때 발급시 발급받고자 하는 자의 신원을 확인하여야 하며, 인증서의 이용범위 또는 용도를 고려하여 거 이용등에 제한을 두거나 이용된 기술의 안전과 신뢰성 등을 고려하여 적절한 유효기간을 정하여야 한다(동법 제15조).

인증서는 i) 유효기간이 경과하거나, ii) 공인인증기관의 지정이 취소되거나, iii) 가입자 등이 인증서의 효력을 정지하거나, iv) 인증서 폐지 등의 사유가 발생한 경우 당연이 그 효력이 소멸하는데(동법 제16조), 가입자 등이 인증서의 효력을 정지하는 경우에는 공인인증기관이 효력을 정지하고, 인증업무를 휴지하는 경우와 정보통신부장관이 인증업무를 정지한 경우는 정보통신부장과이 인증서의 효력을 정지시킬 수 있다(동법 제17조).

이밖에 가입자 등이 인증서의 폐지를 신청하거나, 가입자가 사위 기타 부정한 방법으로 인증서를 발급받은 사실이나 가입자의 사망, 실종선고 또는 해산사실을 안 경우 공인인증기관은 그 밖에 가입자의 전자서명생성키(비밀키)가 분실, 훼손 또는 도난 유출된 사실을 안 경우에는 인증서를 폐지하고 인증관리체계에 의해 누구든지 확인할 수 있도록 조치해야 한다(동법 제18조).

또한 국제화시대에 걸맞게 외국정부와 전자서명의 상호인증에 관한 협정을 체결한 경우 전자서명법에 의해 인정되는 공인인증기관과 인증서와 동일한 효력을 부여할 수 있도록 인증서의 상호인정 규정을 두었다(동법 제27조).

(4) 인증업무의 운영

공인인증기관은 자신이 발급한 인증서가 유효한지 여부를 정보통신망을 통하여 항상 확인할 수 있도록 인증관리체계를 안전하게 운영하여야 하며(동법 제19조), 가입자의 인증서와 인증업무에 관한 기록을 인증서의 효력이 소멸된 날로부터 10년간, 전자서명생성키는 효력유지기간동안 안전하게 관리·보관해야 한다(동법 제22조). 전자서명생성키는 위조·도난 등의 염려가 있으므로 가입자 역

우 정보통신부장관에게 그 사실을 지체없이 신고하여 정보보호센터가 인수할 수 있도록 하여야 한다(법 제10조).

32) 일정사항을 기재한 인증서란 전자서명법 제15조 제2항 소정의 가입자이름, 전자서명검증키, 가입자와 공인인증기관이 이용하는 전자사명방식, 인증서의 일련번호 및 유효기관, 공인인증기관의 명칭, 인증서의 이용법이 또는 용도를 제한하는 경우 이에 관한 사항, 가입자가 제3자를 위한 대리권을 갖는 경우 이에 관한 사항을 기재한 인증서를 말한다.

시 안전하게 보관·관리하여야하며 분실, 훼손시 공인인증기관에 통보하도록 하고 있으며, 공인인증기관이 보관·관리하는 전자서명생성키가 분실, 훼손, 도난 유출시 지체없이 보호센터에 통보하고 인증업무의 안전과 신뢰성확보를 위한 대책을 수립하여야 한다. 이 경우 보호센터에서는 공인인증기관에게 발급한 인증서를 폐지해야 하는데, 폐지된 인증서는 폐지된 때로부터 효력을 상실하게된다.

또한 인증 공인인증기관에서는 가입자의 신청에 의해 보관하는 전자서명생성키를 가입자의 승낙없이 이용하거나 유출하여서는 안된다(동법 제21조).

이러한 인증업무수행 중 공인인증기관에서 가입자 등에게 손해를 끼치는 경우 그 손해가 불가항력적이거나 가입자등의 고의 또는 과실로 인한 경우외에는 손해배상 책임이 있다(동법 제26조). 인증약관에 의해 그 범위를 조정할 수 있으나 지나치게 그 배상의 범위나 청구를 제한하는 약관조항은 불공정약관으로 무효화 될 것이다.

그리고 인증기관이 아니더라도 거래의 안전과 진정성확보를 위해 누구든지 전자서명 생성키를 도용 또는 누설할 수 없도록하고 있으며, 타인의 명의로 인증서를 발급받을 수 없도록 규정 하고 있다(동법 제23조).

(5) 개인정보보호

이밖에 전자서명법에서는 인증업무수행시 필연적으로 채집되는 개인정보의 보호를 위해 본인의 동의없는 개인정보의 채집금지 및 필요최소한 채집의 원칙, 법률의 규정이나 본인의 동의없는 개인정보의 유용 및 유출금지, 가입자등의 개인정보에 대한 열람권 및 정정권보호, 인증업무종사자의 비밀유지의무에 관한 조항을 두고 있다(동법 제24조.)

(6)벌칙

전자서명을 위조하여 사용한 경우에는 형법에 의해 서명의 위조로 처벌될 수 있다. 그러나 전자서명을 위조하지 아니하고 전자서명을 가능하게 하는 전자서명 생성키 자체를 이용자의 승낙없이 보관, 이용, 도용, 누설한 자와 타인명의로 인증서를 발급받거나 발급받게 한 자는 바로 본법에 의해 3년이하의 징역 또는 3천만원 이하의 벌금에 처하게 된다.

4. 시행령·시행규칙의 주요내용

(1) 개 요

전자서명법 시행령 및 시행규칙은 전자서명법(1999. 7. 1시행)의 원활한 시행을 위하여 공인인증기관 지정요건, 공인인증기관 지정 절차, 기타 공인인증기관 관리에 관한 세부 사항지정절차 등 법 시행에 필요한 세부 사항을 규정하여 1999년 8월 12일 정보통신부령 제81호로 공포되었다.

(2) 공인인증기관의 지정요건

시행령은 공인인증기관 지정요건, 공인인증기관 지정절차에 대하여 규정하고 있으며, 시행규칙은 공인인증기관 세부 지정요건 및 관리에 관한 사항을 규정하고 있다.[33]

33) 전자서명법을 입법한 국가의 대부분이 공인인증기관의 안전·신뢰성 확보를 위하여 엄격한 허가요건

시행령에서는 공인인증기관의 지정요건으로 인증기관의 독립성을 보장하기 위하여 "중립적이고 신뢰할 수 있는 제3자"로 규정하고 있다. "신뢰할 수 있는 제3자"란 전자서명 인증을 이용하는 전자거래의 일방 당사자가 아닌 제3자로서 당해거래에 있어서 재정적 이해관계가 없는 자를 말한다.

시행령은 또한 공인인증기관의 재정적 요건으로 "자본금 또는 기본재산 100억 이상"으로 규정하고 있다.

한편 시행령은 기술적 능력, 보호설비, 공인인증기관 운영에 필요한 인력 및 관리적 능력을 갖출 것을 규정하고 있으며, 이와 관련하여 시행규칙에서 각 사항에 대하여 다음과 같이 구체적으로 규정하고 있다.

첫째, 기술적 능력 · 가입자 신원확인 및 등록, 전자서명키 관리, 인증서 관리, 시점확인 등 전자서명 인증업무를 안전하고 신뢰성있게 수행할 수 있는 기술적 능력을 갖추어야 한다.

둘째, 공인인증기관 운영에 필요한 인력으로, 공인인증기관의 24시간 운영체계 구축 및 기술 개발 등을 위하여 인증관리체계 운영인력, 기술개발 인력, 행정지원 인력 및 보안경비 인력을 두어야 하고, 임원(1인 이상), 인증관리체계 운영인력(15인 이상), 기술개발 인력(3인 이상), 행정지원인력(2인 이상) 및 보안경비인력을 두어야 한다.

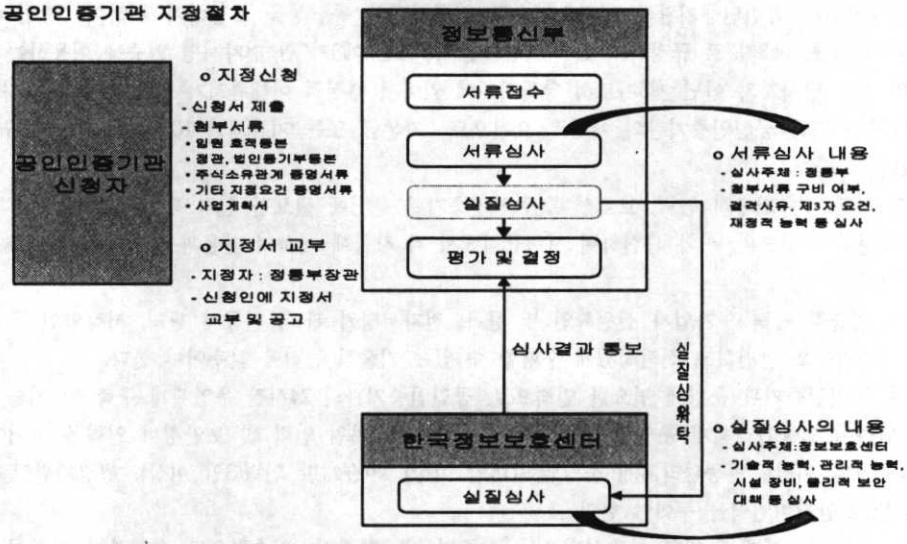
셋째, 인증관리체계에 대한 보호설비로서, 인증업무를 안정적 · 지속적으로 수행하기 위하여 출입통제 시스템, 침입탐지 및 경보 장치, 감시통제 장치 등 인증관리체계에 대한 물리적 보안설비를 갖추어야 하고, 전자서명인증 설비(Dual system), 인증관리체계에 대한 보호설비, 무정전전원공급장치, 냉각기, 화재진압 · 경보장치 및 물리적으로 분리된 이중 저장수단(Data backup) 등을 갖추어야 한다.

넷째, 관리적 능력으로, 인증업무 수행의 안전한 관리를 위하여 인증업무 관련 중요자료의 문서화, 보안감사 및 보안교육 등을 실시할 수 있는 수단을 갖추어야 하고, 인증업무관련 중요자료의 문서화, 보안교육, 인증업무 수행실태에 대한 보안감사를 실시해야 한다고 규정하고 있다.

(3) 공인인증기관의 지정절차

공인인증기관 지정에 있어서 행정절차의 투명성 및 예측가능성을 제고하기 위하여 시행령 및 시행규칙에서 공인인증기관 지정절차를 명확히 하고 있는데, 공인인증기관으로 지정 받고자 하는 자는 첨부서류를 구비하여 정보통신부장관에게 지정 신청해야 하고, 공인인증기관 지정신청자의 기술적 능력, 보호설비, 관리적 능력 등에 대한 실질심사를 거쳐 지정요건을 충족한 경우에 지정서를 교부한다고 규정하고 있다.

을 두고 있다. 특히 독일의 경우 147개의 요구조건을 두고 있다. 외국 입법례에서 공인인증기관의 허가와 관련하여 요구하는 조건을 보면 일반적으로 인증기관 운영의 독립성, 손해배상 등을 위한 재정적 능력, 2인 이상의 관리자에 의한 시스템 운영, 핵심인증시스템의 이원화, 불법침입, 화재, 홍수, 지진 등에 대비한 물리적 보안설비 등을 두고 있다.



(그림 5) 공인인증기관 지정절차도

Ⅳ. 인증체계의 발전 방안

1. 인증체계의 개요

(1) 인증기관의 인증체계와 구성요소

인증기관을 구성하는 요소는 인증서[34]를 발행하고 취소하는 인증기관, 인증서 등록 및 사용자 신원확인을 대행하는 등록기관, 인증서를 및 인증서 취소목록을 저장하고 사용자에게 서비스하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 가입자로 구분된다.[35]

1) 인증기관(CA : Certification Authority)

인증기관이란 전자서명을 위한 인증관리체계를 갖추고 정보통신망을 통하여 가입자의 비밀키를 인증하는 업무[36]를 취급하는 기관이다.

---

34) 인증서(Certification)는 CA가 최종 개체(end entity)를 인증하는 전자증명서 역할을 수행하며, 주체 사용자가 합법적인 사용자임을 입증하기 위하여 CA는 자신의 개인키를 사용하여 디지털 서명문을 생성하여 인증서를 첨부하게 된다. 보통 PKI 방식에서는 통신표준 제정기관인 ITU-T에서 제안안 형식인 X.509 certificate 라는 양식이 사용된다.

35) 이호건 외2인, "인증 관련 주요 국제기구 및 국가인증제도 현황 분석", 통상정보연구 제1권 2호, 「한국통상정보학회」, 1999.12.

36) 여기서 인증 업무란 인증서 발급 및 갱신, 취소 등의 인증절차를 정립하고 운영하는 것을 말한다. 인증기관은 인증서 발급에서 취소까지에 대한 정책과 과정이 명시되어 있는 인증실무지침(CPS : Certification Practice Statement)을 발행하여 유지하고 있다(신홍식 외1인, "전게논문", 53면).

이러한 인증기관은 역할에 따라 계층적으로 구성할 수 있는데, 특히 공인인증기관에 대한 인증서 발급 및 공인인증기관 관리 등의 전반적인 전자서명인증업무를 관리하는 최상위 인증기관(Root CA) 하에 다양한 인증기관이 존재하게 된다.[37]

이러한 인증기관의 분류하여 보면, 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 주요기능에 따라 신원인증기관과 내용인증기관, 신용인증기관 등으로 분류해볼 수도 있다. 한편, 국내외 전자서명 및 인증 관련 법령에 인증기관의 인가나 인정 등의 사항이 포함되어 있는 경우가 많은데, 이러한 규정에 따라 해당 법령이 정한 기관의 인가나 인정을 받은 "공인인증기관"[38]과 그렇지 않은 "비공인인증기관"으로 분류할 수 있다.

2) 등록기관(RA : Registration Authority)

인증기관과 물리적으로 멀리 떨어져 있는 가입자들을 위해 인증기관과 인증서 요청 객체 사이에 등록기관을 둠으로써, 가입자들의 인증서 신청시 인증기관 대신 그들의 신분과 소속의 확인 및 등록 업무를 수행한다(시행령 제3조). 지정 받지 아니한 비공인인증기관도 등록기관을 두어 같은 업무를 수행하고 있다.

3) 디렉토리(Directory)

인증서와 가입자 관련 정보, 상호 인증서 쌍 및 인증서 취소 목록 등을 저장·검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol) 또는 LDAP(Light DAP)을 이용해 X.500 디렉토리 서비스를 제공한다.

인증서와 상호 인증서 쌍은 유효기간이 경과한 후에 일정기간 동안 서명 검증의 용용을 위한 디렉토리에 저장된다.

(2) 인증기관의 주요업무

공인된 인증기관은 전자상거래, 전자정부 구현, 전자화폐 이용 등 정보화 촉진을 위하여 핵심적인 역할을 수행하게 된다. 또한 전자서명 인증을 위하여 전자거래와 관련한 중요 개인정보를 용이하게 수집할 수 있는 위치에 있게 되며, 암호기술 등 정보보호 기술의 축적이 가능하게 된다. 따라서 전자서명 인증은 향후 고도성장이 예견되는 분야라 할 수 있다.

이러한 인증기관의 가장 핵심적인 업무는 전자적 커뮤니케이션의 상대방이 정말로 그 사람인가를 확인해주는 신원인증업무이다. 신원인증업무의 일환으로 대부분의 인증기관은 사용자의 신원을 확인하여 인증서를 발급하고, 전자서명키를 관리하며, 인증서를 확인하고, 인증서 및 인증서의 효력 변경사항을 공개하며, 사후 분쟁에 대비하여 인증서관련 기록을 보존하는 등의 업무를 수행한다.[39]

37) 한국정보보호센터가 전자서명을 안전하고 신뢰성있게 이용할 수 있는 환경을 조성하고 공인인증기관을 효율적으로 관리하기 위한 최상위 인증기관으로서 역할을 수행한다(법 제25조).

38) 공인인증기관은 정보통신부장관이 지정한 기관으로 가입자에 대한 인증서 발급 등 인증업무 수행한다(법 제4조).

이외에 인증기관의 주요한 업무로는 전자적 커뮤니케이션의 내용과 일시 등을 확인하는 내용인증 업무가 있다. 내용인증업무에는 i) 계약의 신청/승락 시기가 그 계약의 성립에 영향을 주므로, 통신의 발신, 착신의 정확한 시점을 인증기관이 증명하는 시점확인표시(time stamp), ii) 우체국의 내용증명처럼 전자문서의 내용을 인증기관이 증명하는 내용증명, iii) 사서증서의 인증 등 기존의 공증업무를 전자적으로 수행하는 전자 공증, iv) 끝으로 사후 분쟁에 대비하기 위하여 과거에 증명한 전자문서를 일정기간 이상 보관하는 전자문서의 보존 등의 포함된다.

또한 전자적인 커뮤니케이션이 보다 복잡해지고 응용서비스의 범위가 넓어짐에 따라, 위와 같은 신원인증과 내용인증 업무 이외에 고객의 지급능력이나 싸이트를 개설한 기업의 신용도를 인증기관이나 타기관이 보유하는 정보를 이용하여 확인, 증명하는 신용확인업무의 필요성도 커지고 있다.

2. 국내외 인증기관 현황

(1) 외국 인증기관 현황

외국 인증기관으로는 미국의 Verisign, Cybertrust, 캐나다의 Keywitness Canada, 독일의 Deutsche Telecom 등이 대표적이며, 1~2개 주도 인증기관이 각국의 인증시장 전체를 장악하고 있다. 각국 인증기관은 인증서비스 이용자그룹과 전략적 제휴관계를 유지하고 있다. 미국은 시장주도, 유럽은 국가주도의 인증정책을 유지하고 있다.

대표적인 인증서비스 제공업체인 미국의 Veresign사의 경우, 2001년 3월 현재 지난 해와 비교하여 100% 이상의 성장을 기록하는 등, 빠른 성장세를 보이며 이미 일본과 유럽에까지 사업을 확장하고 있다. 또한 여러 종류의 CA 제품을 생산하고 있는 캐나다의 Entrust사의 경우, 1994년 처음 사업을 시작한 이래 매년 2배 이상의 빠른 성장세를 보이며 전자상거래의 기반이 되는 다양한 인증 솔루션을 제공하고 있다. 이와 같이 현재 인증서비스와 관련된 사업을 전자상거래의 확산에 따라 매우 유망한 분야의 하나로 각광 받는 분야로 떠오르고 있다.

민간상용 인증서비스 업체 이외에도 국가적인 프로젝트 차원에서도 공개키기반구조 구축 및 전자서명 인증업무 관련 연구가 진행 중인데, 그 대표적이 예로 미국의 FPKI(Federal Public Key Infrastructure), 호주의 PKAF(Public Key Authentication Framework), 일본의 ECOM(Electronic Commerce Promotion Council of Japan) 등을 들 수 있다.

이렇게 인증서비스가 가장 활발하게 이루어지고 있는 미국을 비롯해서 캐나다, 독일, 영국, 일본, 말레이시아 등 여러 나라에서 상용 서비스로서 인증기관이 운영되고 있다.

(2) 우리나라 인증기관 현황

우리 나라의 경우, 전자거래기본법(1992년 2월8일) 제정을 시작으로 전자서명법(1999년 2월5일 공포) 등의 법안을 제정하였으며, 이와 관련된 시행령 및 시행규칙(1999년 8월12일 정보통신부령 제81호로 공포)을 제정하고 한국정보보호센터 산하의 전자서명 인증관리 센터가 1999년 7월7일 개원하여 인증업무준칙을 수립한 단계이다.

이와 관련하여 공인인증기관으로서 「행정정보공동이용센터(정부전산정보관리소)」를 「정부전자서명

39) 백형기 외1인, 전게서, 191면.

인증센터」로 지정 운영하고 있다.

거래 당사자의 신원 확인 및 거래의사의 진정성을 확인해주는 신뢰받는 제3자로서의 인증서비스를 제공해주는 인증기관은 미국의 Verisign사[40]와 기술제휴를 맺고 출범한 「한국정보인증주식회사」가 설립되어 1999년 3월 국내 최초로 인증서비스를 실시중에 있으며, 기간통신사업자인 한국통신과 데이콤, 벤처기업 형태의 정보보호관련업체 등이 있고, 그 외에 이니텍, 소프트포럼 등 정보보안 전문업체 들이 인증서비스를 시험적으로 제공하고 있으며, 금융 분야는 금융결제원과 증권전산이 설립을 추진 중이고 증권거래소, 우체국, 정보전산정보관리소, 특허청 등 공공기관도 인증업무를 수행할 것으로 예견된다.[41]

이와 같이 현재 우리의 인증기관의 현황은 초기단계로서, 아직은 대부분의 전자상거래업체가 외국 인증기관을 이용하고 있으며, 일부 대기업에서는 사내 인증서비스를 제공 또는 준비중이다. 또한 정보보호업계에서 전자서명 인증 기술을 개발중에 있다.

국내 인증시장은 그 규모가 작아 초기에 적자를 볼 것으로 예상되며, 따라서 공인인증기관의 중립성 확보 및 분야별 공인인증기관을 집중 육성하는 것이 필요하다.

현재 공인인증기관 설립은 크게 공공분야와 민간분야로 나누어 추진되고 있다. 민간분야에서는 금융 및 증권 부문에서 금융결제원과 한국증권전산(주)가 각각 공인인증기관 설립을 추진하고 있으며, 그밖의 부문에서 컨소시엄 형태의 공인인증기관 설립이 추진되고 있다. 이 컨소시엄에는 현재 30여개 업체가 참여의사를 표명하였다. 주식회사 형태를 취하게 될 이 공인인증기관의 설립은 모집설립의 방법을 취하게 되며, 발기인조합 결성후 주주의 공개모집이 있을 예정이다.

3. 인증체계의 발전 방안

전자서명법의 제정으로 전자서명 및 인증제도를 위한 인프라의 첫 단계는 마련되었다고 볼 수 있다. 그러나 우리 정부의 입법은 비록 여타의 국가에 비해 앞서 제정되었지만, 입법을 뒷받침할 정부의 정책적 지원 및 업계의 대응 등은 미흡한 것으로 판단되고 있다.

전자서명법의 제정 이후의 실질적인 인증제도의 발전 방안의 논의는 크게 기술적인 사항, 인증기관과 관련한 사항 및 제도적인 사항으로 구분할 수 있다.

먼저 기술적인 사항으로 전자서명 알고리즘의 문제를 들 수 있는데, 정부부문의 전자문서의 인증을 위하여 최상위 인증기관(Root CA)이나 인증정책을 담당하는 기관이 전자서명 알고리즘의 표준을 제정하는 것이 바람직하나, 민간의 전자상거래의 활성화를 위하여는 가장 사용하기 간편하고, 확장성이 존재하는 몇가지의 알고리즘을 제시하여 그중에서 선택할 수 있도록 하며 기술적으로 전자서명 모듈화를 하여 사용할 수 있도록 하는 방법도 존재한다.

전자서명법의 제정으로 중요한 점은 전자서명 및 암호와 관련된 산업의 발전의 계기가 될 수 있도록 관련 정책 및 관련업계의 노력이 필요하다고 할 수 있다. 이를 위해 전자서명의 기초기술부터 응용기술 및 인증기관의 운영 등에 필요한 기술을 연구하고, 정책적으로 촉진하여야 할 부분이 무엇인지를 밝히는 작업이 필요하다.

---

40) 미국의 Verisign사는 인터넷과 같은 공공망에서 사용된 인증서를 발급하는 공적인증기관이다.

41) 이호건 외2인, "인증 관련 주요 국제기구 및 국가인증제도 현황 분석", 통상정보연구 제1권 2호, 「한국통상정보학회」, 1999.12., 135면.

다음으로 인증기관과 관련된 사항으로, 인증서비스가 단기간내에 활성화될 것으로 예측되는 부분을 검토하여 정책적인 지원을 강구하는 방안이 필요하다. 현재 국내의 쇼핑몰의 경우 미국의 Verisign사, Cybertrust사 등의 인증기관에 많은 비용을 지불하고 서버용 인증서를 취득하고 있는 것이 보통인데, 인터넷을 이용한 상거래에서 전자적인 지불을 위한 SSL(Secure Socket Layer), SET(Secure Electronic Transaction) 등을 사용하고 있는 해외 인증시장의 동향을 주시하면서 관련 국내 인증서비스를 활성화할 수 있도록 하는 방안이 필요하다.[42]

특히 정부의 정책적 측면으로서는 공인인증기관의 난립을 방지하고 이를 집중 육성하기 위하여 공인인증기관 지정요건을 강화하는 한편, 분야별 컨소시엄 형태로 공인인증기관을 지정할 필요가 있다. 그러나 공인인증기관의 인증업무 활성화를 위하여 비공인인증업무의 수행에 대하여는 이를 규제하는 것을 자제하는 것이 필요하다. 정부는 민간 전자상거래 부문과 전자정부 기타 공공부문을 통합하는 공개키기반구조를 구축하는 것을 최종목표로 해야 할 것이다.

마지막으로 제도적인 측면에서는 첫째, 전자상거래에서 전자적 지불을 위한 SET(Secure Electronic Transaction)에서 행하는 인증서비스처럼 전세계적으로 서비스가 이루어지는 인증의 경우, 이 업무로 인해 발생 가능한 책임의 소재가 문제된 경우 등에 우리의 전자서명법을 적용할 수 있는가의 문제 등이 존재한다. 이에 대한 연구도 필요하다. 둘째, 현재 국내 전자상거래 관련 입법은 산업자원부가 추진한 전자거래기본법과 정보통신부가 추진한 전자서명법이 그 주축을 이루고 있는데, 공인인증기관의 역할과 관리, 전자문서 및 서명의 법적 효력 등의 일부 조항에서 영역 중복의 문제가 발생하고 있다. 상호 보완적인 법률구조를 유지하기 위하여 보완대책이 필요하다.

"전자서명법"은 공인인증기관에서 인증서 발급시 신원확인 방법에 대한 규정이 미비한 반면 "금융실명거래 및 보장에 관한 법률"은 전자서명법에 의한 인증서 발급절차가 동 법률에 따른 실명확인 법적 효력이 없다고 명시해 두 법률간 상충도 문제점으로 지적되고 있다.

특히 전자서명법은 전자상거래 인증상 문제 발생시 배상책임과 한계가 불분명하며 행정자치부, 금융결제원, 민간 인증기관 간 인증업무의 차별성과 업무준칙이 명확히 구분되지 않는 등 혼돈의 소지가 있다.[43]

V. 결 론

전자서명과 인증의 문제는 전자문서를 이용한 비접촉, 비대면 거래라는 전자거래의 한계점을 극복해주는 가장 큰 해결방안이다. 전자문서의 내용을 증명하고 거래의 진정성을 확보함으로써 전자거래의 한계점을 극복하기 위하여, 전자서명법을 제정함으로써 전자서명 및 인증제도를 위한 인프라의 첫 단계는 마련되었다고 볼 수 있다.

전자서명법은 국가전체의 공개키기반구조 구축을 위한 기본적 사항을 정한 법이다. 전자서명법을 기초로 공개키기반구조가 구축되면 사회 전반의 생산력이 크게 향상되고 국민의 편익도 증진할 것이다. 따라서 전자서명법에 의한 공개키기반구조 구축은 정보화촉진의 핵심과제라 할 수 있다.

42) 신일순 외2인, 전게논문, 170 - 171면.
43) 이호건 외2인, 전게논문, 140면.

동 법에 기초하여 국내에서는 1999년 3월 한국전자인증주식회사가 설립되어 최초로 인증서비스를 시작하였으며, 앞으로 각 분야별 공인인증기관의 출현이 예상된다.

국내 전자서명 인증시장은 아직 초기 단계에 머물러 있어,[44] 대부분의 전자거래 업계들이 선진 외국의 전자서명 인증기관서비스를 이용하고 있는 실정이다. 따라서 인증서비스의 필요성과 가치에 대한 소비자의 검증이 이루어지는 처음 수년간은 인증서비스 기술 및 사업수행 상의 시행 착오로 서비스가 정착되기까지 다소 어려움을 겪을 것으로 예상된다.

현재 국제적인 차원에서 쟁점으로 떠오르고 있는 전자서명 인증기관의 허가와 공인, 상호인증, 소비자 보호, 인증실무지침에 관한 논의가 활발히 진행되고 있다. 국내 전자서명 인증기관은 시장개척과 아울러 인증기술과 정책, 표준과 직접적으로 관계된 이런 세계적인 추세에 적극적인 대응이 필요하다.

전자서명 인증사업은 전자상거래를 활성화하기 위한 필수적인 사항이지만 그 자체가 목적이 될 수 없으며, 따라서 인터넷 정책 및 전자상거래 규범, 보안기술개발 등과 연계하여 폭넓게 접근해야 할 것이다.

현재 전자서명법을 제정하여 시행중이나, 이를 뒷받침할 정부의 정책적 지원 및 업계의 대응 등은 아직 미흡한 것으로 판단된다. 비약적인 성장을 하고 있는 세계의 전자서명 인증시장에 성공적인 경쟁력을 갖추었을 때, 전자서명 인증제도는 우리의 새로운 사회적 기반으로 생산력을 크게 향상시킬 수 있는 정보화의 선구자가 될 것이다.

<參 考 文 獻>

김지연, "국외 공개키 기반구조 추진체계 분석", 한국정보보호센터, 1998. 7

백형기 · 최창렬, 「전자상거래 시대의 법」, 미래와 경영, 2000. 8

신일순 · 김춘아 · 박민성, 「전자서명 및 인증제도」,정보통신정책연구원, 1998. 12

신홍식 · 김창연, "전자상거래 보안과 전자인증", 「정보산업」, 1999. 5-6월호, 한국정보산업연합회, 1999. 6

오병철, 「전자거래법」, 법원사, 1999. 1

이경구, "전자인증제도", 한국정보보호센터,1999. 5

이규정, "전자상거래의 신뢰성 확보를 위한 법제 현황과 정비 방향", 「정보화 동향분석」, 1444호, 한국전산원, 1999. 10

이호건 · 박승락 · 윤영한, "인증 관련 주요 국제기구 및 국가인증제도 현황 분석", 「통상정보연구」, 제1권 2호, 한국통상정보학회, 1999.12.

장성수 · 김춘길, "전자상거래와 전자서명", 「정보통신연구」, 제12권 1호, 한국통신 연구개발본부, 1998. 3

44) 인증시장은 1997년 그 시장이 형성된 이후 연100% 이상 성장해 2001년에는 11억 달러에 이를 전망인데 비해, 국내시장은 초기 진입단계로 1999년의 경우에는 세계시장의 0.2% 규모이지만, 2002년에는 400억 달러에 이를 전망이다(이호건 외2인, 전게논문, 141면).

최경진, 「전자상거래와 법」, 현실과 미래, 1998.

한승철 "전자서명 및 인증기관의 법적 문제", 「저스티스」, 제31권 1호, 1998.

황희철, "전자서명과 법률문제", 「정보법학」, 제2호, 한국정보법학회, 1998.

内田 貴, 電子商取引と法 - UNCITRAL「電子商取引モデル法」および通産省「電子商取引環境整備研究 會中間報告」を中心として, NBL No.601-603(1996.9.1-10.15)

室町正實・吉田一雄, "認證機關および 電子取引に關する 法的基盤の 整備に向けて", NBL No.593, 1996. 5. 15.

American Bar Association, "Digital Signature Guideline", 1995.

Ian Taylor MBE MP, Minister for Science & Technology in UK, "Licensing of Trusted Third Parties for the Provision of Encryption Services(Public Consultation Paper on Detailed Proposals for Legislation)", March 1997.

Richard L. Field, "The electronic future of cash: survey, 1996: Survey of year's developments in electronic cash law and laws affecting eletronic banking in the United States", 46 Am. U. L. Rev. 967.

Translation and Commentary by Christopher Kuner, Esq., Gleiss Lutz Hootz Hirsch & Partners, Frankfurt, "German Digital Signature Law", Final Draft, December 20, 1996.