通信情報保護學會誌
第9卷 第1號, 1999. 3

전자상거래와 전자서명법상 Digital Signature의 법리

Electronic Commerce and the Legal Theory of Digital Signature under the Electronic Signature Act

배 대 헌*

Ⅰ. 서 언

정보와 컴퓨터에 관한 기술의 비약적인 발전에 힘입어 얻어진 디지틀혁명(digital revolution)에 의하여 현대사회는 새로운 전기를 맞이하고 있다. 이에 터잡아 컴퓨터와 정보통신의 신기술을 통하여 얻어진 지식·정보가 정보화사회의 기반을 구축하고 있다. 이러한 것들은 정치·사회·경제·문화 전 영역에 걸쳐 근본적인 구조변화를 가져오고 있는데, 특히 Internet의 상업적 이용에 따라 경제적 측면에서 새로운 변화가 전자상거래 영역을 중심으로 뚜렷하게 드러나고 있다.

정부는 전자적 매체를 통하여 이루어지는 거래를 활성화하고, 이용의 편의를 도모하기 위하여 전자상거래기본법, 전자서명법 및 전자자금이체법 등을 1998년 중에 입법하기로 확정하였고, 그 결과로 전자서명법, 전자거래기본법의 시행을 눈앞에 두고 있다(1999년 7월 시행). 전자서명법과 전자거래기본법은 새롭게 열리고 있는 디지틀 세계에서 적용될 법·제도적 기반으로서 중요한 의미를 띠고 있다. 특히, 전자서명법은 거래법의 영역뿐만 아니라, 행정민원, 공공기관 상호간의 문서교환 등 국가 정보화를 앞당기는 중요한 계기를 마련하고 있다. 정보화에 널리 이용되는 개방체제 네트워크는 접근의 용이성이 강조되는 반면에, 보안성이 취약한 약점을 안고 있다.

이를 위하여 궁구된 것이 디지틀서명 등의 전자서명이다. 전자거래에 디지틀서명을 활용함으로써 이용자의 신뢰를 높여 전자상거래를 활성화하고, 그밖에 다른 분야로 디지틀서명의 이용범위를 확산시킬 수 있을 것이다.

이하에서 상대방의 신원확인(identification), 문서의 무결성 보장(integrity), 부인방지(non-repudiation), 개인정보의 보호(privacy protection)의 기능을 가지고 있는 디지틀서명이 가상공간상 계약체결시에 어떻게 구현되고, 이에 관한 관련입법을 검토함으로써 디지틀서명에 관한 법리를 모색하고자 한다. 여기에서 논의하는 기술내용에 있어서는 전자서명법의 입법에 반영된 디지틀서명의 PKI방식을 논의대상으로 삼고, 이와 함께 전자서명법 등의 법률규정을 검토한다.

* 계명대학교 법과대학 조교수

Ⅱ. 가상공간상 계약체결

계약은 일방의 청약과 그에 대한 상대방의 승낙 의사표시로써 체결되는데 계약자유의 원칙(freedom of contract)을 좇아 특별한 제약을 받지 않는다. 우리의 현행 계약법은 실제 환경(physical environment)에 터잡은 계약체결 및 그 이행에 관하여 규정하고 있으므로 가상적인 공간(virtual reality; cyberspace)상에서[1] 체결되는 계약의 경우에 동일하게 적용할 수 없을 것이다. 가상공간상 계약체결은 일방에 의하여 정하여진 청약내용에 대하여 상대방이 이에 합의한다는 문구("Click here if you accept ; "I accept"를 컴퓨터의 마우스나 엔터키를 통하여 표시함으로써 이루어진다. 이러한 계약체결이 외관상으로는 종래 법적 여건 하에서 형성된 법리를 좇는 것 같이 보이지만, 실제에 있어서는 전혀 다른 양상을 띠고 있다. 최근 들어 실생활에 정착되어 가고 있는 전자상거래를 살펴볼 때 여러 가지 측면에서 그 차이를 확인할 수 있다.

인터넷상 전자적 거래는 객체를 중심으로 물건의 매매와 소프트웨어 등의 이용계약의 유형으로 나누어 볼 수 있다. 후자는 주로 web wrap license(shrink wrap license에 대한 표현으로) 또는 click on contract의 명칭으로 비교적 최근 들어 논의되기 시작한 것들이다(미국 통일상법전(UCC) §2B license의 규정신설에 관한 논의[2].) 또한, 특정한 두 당사자에 한정된 거래가 이루어지는 경우와 인터넷상 쇼핑몰에서 판매할 물건을 불특정 다수인과 거래계약을 체결하는 경우로 각각 구별할 수 있다. 전자상거래는 이 경우에 후자의 주된 논의대상이다. 이 디지틀서명은 계약체결, EDI, on-line banking service, 증거법 등에 실제 활용될 수 있을 것이다.

1. 가상공간상 통상적인 계약체결

계약체결의 양 당사자인 청약자와 승낙자는 통상적으로 스스로 계약내용을 정하여 이를상대방에게 직접 전달하지만, 가상공간상 계약체결에 있어서 청약자가 일방적인 청약내용을 정하고 승낙자는 이에 합의한다는 단순한 메시지를 전송함으로써 계약이 체결된다.

전통적으로 의사표시의 전달에 있어서 민법은 도달주의 원칙을 규정하였고, 격지자간에 예외적으로 발신주의에 따른다(민법 제531조). 그런데 전자적 매체를 통하여 메시지를 전달하는 경우에 있어서, 대화자와 격지자의 구별이 모호할 뿐만 아니라, 네트워크의 물리적 고장에 의하지 않고는 거의 즉시간대(real time)에 상대방에게 의사표시가 도달된다. 또한, 종래에는 의사표시의 내용과 관련하여 법리상 청약의 유인(invitation for offer)과 청약(offer)이라는 의사표시를 구별하였지만, 가상공간상 계약체결은 이를 구별할 수 있는지에 관하여 의문이 제기될 뿐만 아니라, 구별할 실익이 있는지도 의문이다.[3] 즉, 인터넷상 가상 쇼핑몰(cyber shopping mall) 등에서 상품의 그림을 보여주고 구매를 원하는 자에게 크레딧 카드 번호를 입력함으로써 상품을 구입하는 경우에 청약과 청약의 유인을 구별하기가 어렵다. 또한, 계약체결시점을 정하는 것, 거래시 계약체결지를 확정하는 것 등 섭외사법상 관할권(jurisdiction)에 관하여 많은 논의가 진행되고 있다.[4]

전자거래상 의사표시의 전달을 위하여 인터넷 등의 컴퓨터 네트워크를 이용한 e-mail 또는 정형의 메시지 전달방식을 이용한다. 인터넷 등은 일반인에게 개방된 것이므로 제3자가 이러한 네트워크를 악용함으로써 전송한 내용이 제대로 전달되지 않거나 청약에 대한 의사표시 또는 그에 대한 승낙의 의사표시가 표의자가 행한 의사표시와 다른 내용으로 전달될 수 있다. 기망행위나 허위 의사표시의 전송은 개방형 네트워크의 문제점으로 지적되는 보안

성(security)의 취약에서 비롯된다.

보안성의 취약점을 보완하기 위하여 전송내용을 암호화하여 제3자의 악용을 막아 온전히 표의된 내용이 전달되게 하거나, 表意者를 확인할 수 있도록 하는 방법이 구체적으로 논의되고 있다. 이에 대한 대표적인 방법이 디지틀서명이다. 그밖에 결재수단에 있어서 종래에 현금 또는 크레딧 카드를 사용하였지만, 가상공간상 크레딧 카드 또는 사이버캐쉬라는 신종의 화폐를 고안하고 있으며, 분쟁해결방법으로 종래에는 주로 재판에 의하여 문제를 해결하였지만, 涉外的 去來가 빈번해짐에 따라 중재(arbitration) 등의 대체적 분쟁 해결방법이 실제 유용한 것으로 논의되고 있으며, 관할권의 문제는 계약법상 문제일 뿐만 아니라, 불법행위상 해결하기 어려운 대상으로 많은 논의를 불러오고 있다.

2. 정보이용계약(mass-market license)

프로그램을 전송받아 이용하고자 할 때에 "프로그램을 내려받거나 설치하기 전에 이용계약(license)의 내용을 읽고 클릭함으로써(click-on) 계약이 체결됩니다" 등의 문구를 접하게 된다. 전자상거래의 한 유형인 인터넷상 프로그램을 구입하는 경우에 제시된 이용계약서의 내용에 동의한다는 표시로 "I agree"또는 Yes)라는 지시문에 클릭함으로써 계약을 체결하는 결과를 가져온다. 이 정보 이용계약은 일방에 의하여 제시된 계약내용에 따라 이루어진 것으로 계약체결의 실질적 요소인 의사표시의 합치가 결여된 것으로 판단할 때에 계약법의 원칙에 비추어 많은 논의를 불러올 수 있다. 여기에서 이러한 계약이 성립된 것인지 여부, 이용계약에서 정한 내용과 같은 효력이 발생하는지 여부와 같은 의문이 제기될 수 있다.[5]

이러한 계약에 있어서 知的 産物의 이용으로부터 이용허락자의 지적 창작에 대한 권리를 보호할 필요가 있지만, 다른 한편으로 정보이용자인 소비자의 권리도 함께 보호되어야 한다.[6] 디지틀 기술이 발전·이용됨에 따라 새로운 대상이 등장하였다 하여 일방의 이익보호에 편중된 법·제도가 마련된다면, 소비자의 권리가 열악한 사정으로 빠지게 됨으로써 종국에는 정보화사회의 발전에 걸림돌로 전락하게 될 것이다. 정보유통과 관련된 규범적 영역에서 대량유통 이용계약 체결을 논의할 때에, 공급자·소비자 사이의 균형이 깨어지지 않도록 법적 방안을 강구하여야 할 것이다.

대량유통 이용계약은 정보획득의 방법에 따라 다음과 같이 두 가지로 나뉘어진다. i) shrink-wrap 이용계약과[7], ii) click-wrap 이용계약(또는 click-on contract; bootscreen license)이다. 전자상거래와 직접 관련이 있는 것은 후자이다.

click-wrap 이용계약은 온라인을 통하여 직접 소프트웨어를 내려받거나(download), 설치하기 전에 shrink-wrap 이용계약의 경우와 같이 제공자 등에 의하여 제시된 일정한 내용에 동의한다는 지시문에 클릭함으로써 체결되는 정보이용계약이다. 인터넷을 통한 전자상거래가 이용·확대됨에 따라 이러한 형태의 이용계약의 체결이 점증하고 있다. 이러한 계약의 체결은 엄격히 말하면, 당해 정보를 담은 물건을 구입하는 데에 합의하는 것이 아니라, 프로그램 등의 소프트웨어 또는 정보의 이용에 관하여 상대방의 청약에 동의(합의)한 것이다. 즉 인터넷 등에서 물건에 대한 매매계약은 통상의 경우와 본질적으로 같으나(인터넷을 통한 통신판매), 전자적 매체를 이용한 특수한 사정이 고려될 뿐이다. 그러나, 여기에서 논의하는 이용계약은 계약체결의 방식, 계약내용 및 거래대상이 통상의 매매와 현격히 구별된다.

이러한 점을 이용자의 관점에서 정리하면,

i) 계약내용으로 정하게 될 것에 대하여는 이용자가 계약체결 전에(click-wrap 이용계약의 경우에 카드의 결제 전에) 알 수 있어야 한다. ii) 승낙과 거절의 의사표시를 명백히 제시할 수 있도록 하여야 한다. 이러한 계약체결시 당사자확인 및 내용의 안전한 전송을 위하여 디지틀서명을 가지고 계약 당사자의 의사표시를 분명하게 전달할 수 있어야 한다.

통상적인 계약체결과 가상공간상 계약체결을 비교하면 다음과 같다.[8]

	가상공간상 계약체결	통상적인 계약체결
의사표시	비대면계약 전자문서에 의한 청약·승낙 의사표시 청약·청약유인 구별 모호(법리문제) 전자문서 전송(이에 관한 법리 필요)	◁ 대면계약 ◁ 직접전달, 우편 등 전통적 전달방법 ◁ 청약·청약의 유인 구별 ◁ 도달주의(원칙) (발신주의: 격지자간거래)
계약서작성 및 서 명	디지틀서명 - 인증 - 의사표시부인 방지 - 문서 진정성 확보	◁ 낙성계약(방식 불문) ◁ 날인, 서명(증거보전) ◁ 사기방지법상 500$ 이상 거래시 서명요구(미국 UCC)
대금지급 수 단	cybercash 침해방지 수단강구 credit card	◁ 현금 및 유가증권 ◁ credit card
계약형태	매매(sale) license 규정신설 (UCC §2B 신설논의)	◁ 매매가 주된 종류
거래대상 (목적물)	물건, 서비스 지적재산 (information, S/W)	◁ 주로 물건
계약이행 장애사유	외부적 요인 - 네트워크 전송장애 - Sysop의 과실	◁ 채무자의 귀책사유 (고의·과실)
분쟁해결 방 법	대체적 분쟁해결수단 재판관할권 문제	◁ 재판에 의한 분쟁해결

3. 계약체결에 있어서 기명날인·서명과 전자문서의 법적 의미

현행법상 계약체결에 있어서 계약당사자는 계약법의 일반원칙인 계약자유의 원칙에 따라 계약체결의 형식에 구애받지 아니한다. 계약서라는 일정한 형식(방식)에 의하지 아니하여도 의사표시의 합치만 있으면 계약의 효력이 생긴다. 이런 법리는 전자상거래에서도 양 당사자 사이에 일정한 형식에 의하지 아니한 채 전자적 형태로 의사표시가 합치하기만 하면 전자적 여건 하에서도 마찬가지로 적용된다. 따라서 전자적 여건 하에서 디지틀서명이 계약체결에 있어서 특별한 요구되지 않는다. 그렇지만, 서명이 일반적으로 계약체결의 요건이 되지 않는다 할지라도, 계약체결의 형식성 또는 사후의 분쟁에 대비하기 위한 증거법상 중요한 논의대상이다. 이런 점에서 계약체결상 요구되는 디지틀서명은 우리의 법체계에 비추어 검토할 때에 전자적 매체를 통한 문서의 전송에서 발생할 문제와 관련된 것이지 아래에서 설명할 미국법상 서명에 관한 법리에[9]따른 것이 아니다. 따라서 우리의 경우에 디지틀서명은 명칭에서 빚어진 잘못된 인식을 피해야 할뿐만 아니라, 그 명칭에 얽매일 것도 아니다.[10]

현행법상 통상의 계약서 등 문서는 대부분 서증으로서 증거능력이 있다. 여기에서 증거능력이란 증거조사의 대상이 될 수 있는 자격을 말한다. 당사자 사이에 작성된 계약서는 다툼의 쟁점을 밝히기 위한 중요한 증거자료다. 문제는 서면이 아닌 전자문서로 작성된 계약서에 대하여도 이와 같은 증거능력을 인정할 수 있는지의 여부이다. 또한, 증거능력이 인정되는 경우에, 그 전자문서의 증명력(증거력)을 판단하여야 한다. 이는 문서가 특정인의 의사에 기하여 작성된 것인지 여부를 먼저 검토하여야 하는데, 이를 문서의 진정성립 여부를 판단하는 것이다(문서의 형식적 증명력). 그밖에 법원은 문서성립의 진정성이 인정되면, 다툼의 쟁점을 증명하기에 적합한지를 판단하게 된다(문서의 실질적 증명력). 여기에서 특히 문제되는 것은 전자문서성립의 진정성에 관한 점이다. 일반적으로 본인이 문서를 작성했을 경우에 작성자는 기명·날인 또는 서명을 하게 된다. 이에 관하여 민사소송법상 私文書는 본인 또는 그 대리인의 서명이나 날인이 있는 때에는 진정한 것으로 추정된다.[11] 이러한 내용을 전자문서의 경우에 동일하게 적용할 수 있는가. 만약, 이러한 내용을 반영한 기술적 방법이 활용되는 경우에는 이에 관한 법리를 적용할 수 있을 것이다. 즉, 당사자의 신원을 확인할 수 있고, 거래당사자가 작성한 문서가 상대방에게 그대로 전달되어 사후에 거래내용을 부인하지 못하게 되는 방법이 이용될 때를 말한다. 이러한 디지틀서명은 신원확인·무결성·부인방지·프라이버시 보호의 기능을 가지고 있으므로 전자문서의 작성 및 전송에 있어서 문서성립의 진정성과 문서의 위조 및 변조를 막을 수 있는 개방체제 네트워크에서 정보보호를 위한 중요한 수단이다. 이에 관련하여 전자서명법 및 전자거래기본법에 디지틀서명 등 전자서명의 법적 정의와 법적 효과를 규정하고 있다.

Ⅲ. 전자상거래에 있어서 Digital Signature의 법적 효력

1. 디지틀서명의 의의

디지틀서명이라 함은 전자문서에서 수학적 조작으로 얻어진 일련의 숫자·문자로 암호화한 정보로 수기서명의 전자적인 대체물을 말한다. 기술적인 면을 중심으로 정의하면, 전자메시지에 해쉬 함수(hash function)를 적용시켜 메시지요약(message digest)을 만든 후, 이에 공개키 알고리즘과 송신자의 비밀키(전자서명법에서 정한 전자서명 생성키)를 이용하

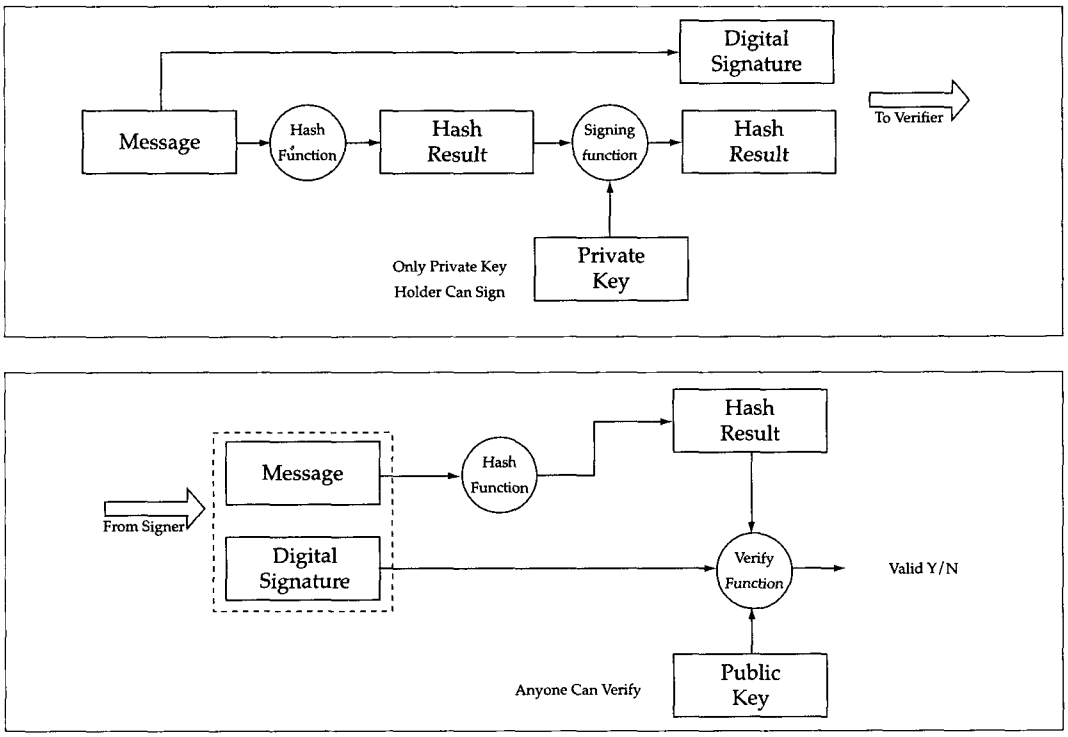
여 암호화한 비트(bits)의 조합을 말한다. 서명 작성자의 공개키(전자서명법에서 정한 전자서명 검증키)를 가지고 있는 수신자는 비트의 조합이 송신자의 공개키에 대응한 비밀키에 의하여 작성된 것인가, 메시지를 비트의 조합으로 만들어 전송된 이후에 제3자에 의하여 변경되지 아니하였는가를 확인하게 된다. 이러한 디지틀서명은 거래의 근거를 증명하고, 그 내용의 진정성을 보증하는 전자적 절차에 의한 결과이다. 이러한 디지틀서명은 비대칭형 암호방법에 의하여 만들어진 것으로 전달하는 메시지 내에 구성되어 있거나 첨부화일 또는 메시지와 분리된 파일로 전송되더라도 효력에는 아무런 영향을 미치지 아니한다. 아래 그림은 미국 ABA가 제시한 "Digital Signature Guidelines(1996)"의내용 중에서 디지틀서명이 행하여지는 과정을 설명한 것이다.[12]

이는 우리 전자서명법이 비대칭암호방법에 바탕을 두고 PKI방식을 채용했으므로 우리 법규의 관련내용을 이해하는데 직접적인 도움을 준다.

2. 전자서명법·전자거래기본법상 전자서명의 정의 및 효과

국내 전자상거래의 활성화를 도모하기 위하여 이에 관한 두 가지 법률이 제정되었다.

i) 하나는 전자거래의 기본적인 틀을 만들어 거래에 관한 법적 효력을 명확히 하여 전자적 환경 하에서 거래질서를 확립하고 전자거래를 촉진할 목적으로 입법된 전자거래기본법이고, ii) 다른 하나는 전자거래에 사용되는 전자문서의 안전성과 신뢰성을 확보하고 이를 활용하기 위한 전자서명의 기본적인 사항을 정하여 정보화를 촉진할 목적으로 입법된 전자서명법이다. 아래에서 전자서명법 및 전자



거래기본법의 전자서명의 정의와 법적 효과를 나누어 살펴보겠다.

가. 전자서명법상 전자서명의 정의

전자서명법 제2조 2호에서 "전자서명이라 함은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명생성키로 생성한 정보로서 당해 전자문서에 고유한 것을 말한다고"규정하였다. 여기에서 전자서명은 디지틀서명을 지칭하는 것으로 비대칭암호방법을 이용하여 생성된 것이다. 법률 규정상 전자서명은 법정명칭에 불과하고 실체는 법률규정 전체를 검토할 때 디지틀서명을 말한다. 전자서명법 제2조, 제3조, 제15조, 제21조, 제23조 등의 규정은 디지틀서명에 근거한 내용이다. 이 법률에서 규정한 전자서명이 디지틀서명에 한정하고 있으므로 그 실체에 따라 법률제정시 디지틀서명이라는 명칭으로 규정되지 못한 아쉬움을 남겼다. 다만, 지금까지 일반인에게 인식되었던 전자서명이라는 용어의 친숙성으로 인하여 디지틀서명이라는 명칭 대신에 전자서명이라는 용어를 채택하였다는 현실적 사정을 짐작할 수 있다. 디지틀서명에 관한 기술적인 내용을 이 법에 담아 입법하였지만, 디지틀서명을 작성하는 기술내용 예컨대, X.509라는 알고리즘을 명시한 Utah주의 경우와는[13]다르게 이를 법률에 규정하지 아니하였다. 이는 현재의 기술이 비대칭암호체계를 완벽하게 구현하고 있는 것이 아니라, 장래에 발전될 진보된 기술을 전자서명법상 디지틀서명으로 사용할 수 있는 여지를 남기고 있다는 점에서 의미를 가진다.

나. 전자거래기본법상 전자서명의 정의

전자거래기본법 제2조 5호에서 "전자서명이라 함은 전자문서를 작성한 작성자의 신원과 당해 전자문서가 그 작성자에 의하여 작성되었음을 나타내는 전자적 형태의 서명을 말한다고" 규정하였다. 이 내용은 위의 전자서명법에서 정한 디지틀서명을 지칭하지 아니할 뿐만 아니라, 실체적으로 디지틀서명이 아니더라도 수기서명의 기능을 하는 전자적 형태의 서명도 포함하는 개념이다. 즉 이는 작성자의 신원과 작성자에 의하여 작성되었다는 것을 밝힐 수 있는 정도만을 규정하고 있다. 이러한 점은 인터넷 등의 이용으로부터 등장된 가상공간의 문제점으로 대두된 네트워크 상의 보안성확보와 관련하여 검토되어야 한다. 전자거래기본법 제2조 7호는 인증기관을 규정하였고, 동 법 제2조 8호에 공인인증기관을 규정하고 있는데, 이는 전자문서 작성자의 신원과 거래와 관련된 중요사항을 확인하는 인증기관을 二元化하였다. 전자의 인증기관(비공인인증기관)은 당사자의 신청에 의하여 전자서명 사용자의 신원확인 기타 관련 업무를 취급하는 자를 말하며, 후자의 공인인증기관은 전자거래의 안전성 및 신뢰성을 확보하고 건전한 전자거래의 촉진을 위하여 전자서명법 제4조의 규정에 따라 지정된 인증기관을 말한다(전자거래기본법 제16조 1항). 그런데 이 공인인증기관도 전자문서 작성자의 신원 기타 거래와 관련된 중요사항을 확인하기 위한 인증서를 발급한다고 규정하였다(동 조 제2항). 이러한 전자서명은 전자거래에 있어서 당사자의 신원을 확인하고, 거래내용이 제3자에 의하여 변조되지 아니하였다는 내용만을 밝힐 수 있다면, 실거래계에서 추구하는 목적을 달성할 수 있다는 점에서, 다양한 형태의 전자서명 또는 디지틀서명이 사용될 수 있다는 취지는 수긍이 된다. 그렇지만, 거래 당사자는 다양한 종류의 전자서명에 대하여 사용상 혼란을 겪게 될 것으로 추단된다. 이 문제는 전자거래의 활성화가 이루어져 어느 형태로든 실거래에서 표준형태로 이용되는 시점까지 소비자에게 부담

으로 남게 될 것으로 보인다.

다. 디지틀서명, 전자서명의 효력

전자서명법에서 디지틀서명이 공인인증기관의 인증을 받은 경우에 즉, 인증서에 포함된 전자서명 검증키에 합치하는 전자서명 생성키로 생성한 디지틀서명은 법령이 정한 서명 또는 기명날인으로 본다(전자서명법 제3조 1항)고 규정하였다. 위와 같은 전자서명은 디지틀서명을 지칭하는 것으로 당해 전자서명이 당해 전자문서의 명의자의 서명 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정한다(전자서명법 제3조 2항). 또한, 전자거래기본법에서도 공인인증기관이 인증한 전자서명은 다른 법률에 그 효력을 부인하는 규정이 없는 경우를 제외하고는 관계 법률이 정한 서명 또는 기명날인으로 본다고 규정하였으며, 이러한 전자서명이 있는 전자문서는 작성자가 작성한 후 그 내용이 변경되지 아니한 것으로 추정한다고 규정함으로써(전자거래기본법 제6조) 전자서명법과 일치하는 규정을 두었다. 전자거래기본법상 전자서명에 관하여 주의할 점은 위와 같은 법적 효력이 생기는 전자서명은 전자거래기본법상 모든 전자서명이 이에 해당하는 것이 아니라, 공인인증기관에 의하여 인증된 것에 한정한다는 점이다. 따라서 전자거래에서 당사자에 의하여 사용되는 전자서명의 형태를 전자거래기본법에서 특별히 제한하지는 않지만, 거래당사자는 당해 법률상 효력을 얻기 위하여 디지틀서명을 사용하여야 한다.

한편, 디지틀서명이 아닌 전자서명을 가지고 거래한 경우에 사용된 전자문서가 다른 법률에 특별히 규정이 있는 경우를 제외하고는 전자적 형태로 되어 있다는 이유로 문서의 효력이 부인되지 아니한다고 규정하였으며, 이러한 전자문서는 재판 기타의 법적 절차에서 전자적 형태로 되어 있다는 이유로 증거능력이 부인되지 아니한다고 규정하였다(전자거래기본법 제5조, 제7조). 이는 전자문서를 통상의 종이문서와 구별하지 아니하는 취지를 직접 반영한 것으로 정보화사회의 기반을 구축하는 중요한 법과 제도의 강구에 해당한다. 다만, 전자문서가 일반 종이문서와 같은 법적 효력이 있다는 점과 그것이 무결성으로 인하여 제3자에 의하여 그 내용이 변경되었다는 것까지 추정한다거나 이를 간주하지는 아니한다는 점이다.

결론적으로, 이러한 무결성의 전자문서인지에 대한 다툼에 있어서 사용한 전자서명이 전자서명법에 정한 디지틀서명을 사용하였을 뿐만 아니라, 당해 전자문서가 공인인증기관에 의하여 인증받은 디지틀서명된 경우에 위의 법적 효력이 있다. 왜냐하면, 이 경우에 전자문서 효력은 전자서명법 제3조 2항에 따라 그 내용이 변경되지 아니하였다고 추정된다고 규정하였기 때문이다.

그 밖의 경우에 즉 디지틀서명을 사용하였지만, 공인인증기관에 의하여 인증받지 아니한 경우 또는 단순한 전자서명만을 사용한 경우 등에 거래 당사자간 다툼이 생겼다면, 거래당사자는 전자서명이 첨부되었다는 사실만을 가지고 전자문서의 효력으로부터 문서의 진정성에 해당하는 무결성까지 주장하지 못한다. 따라서 거래당사자는 사후에 발생할 수 있는 다툼을 사전에 막기 위하여, 비공인인증기관의 신뢰성 정도 또는 통상의 전자서명의 안전성이 검증되기 전까지 디지틀서명을 사용하는 것이 좋을 것이다.

3. 전자상거래에 있어서 디지틀서명의 활용

정보화시대라는 사회적 여건이 성숙되면서 공적 분야, 사적 분야를 막론하고 네트워크상 여러 가지 정보가 활발히 전파되어 널리 사용되고 있다. 특히 인터넷의 폭발적인 이용에 따라 전자거래 분야의 기술은 하루가 다르게

발전하고 있으며, 새로운 기술은 개방 네트워크의 결점인 보안성의 취약점을 극복하고 있다.

디지틀서명이 활용되는 분야는 정보화사회에서 디지틀 형태로 전달되는 정보와 대부분 직접·간접으로 관련되어 있어 어느 특정 분야에 한정되어 있다고 말할 수 없다. 따라서 종래 종이문서로 사용되던 분야가 전자문서 또는 전자적 형태로 관련내용을 대체할 수 있다면, 그와 같은 전 분야에 걸쳐 살펴보아야 할 것이다. 전자상거래, 조직내의 정보교환·결제제도, 금융서비스, 원격진료, 전자공증, 행정절차 및 우체국에서의 내용증명서비스 등 아주 다양하다. 다만, 정책의 우선순위 또는 일정한 여건이 구비된 뒤에 디지틀서명을 활용하는 시기조절의 문제만이 검토될 것이다.

전자상거래 분야에서 디지틀서명의 실제적 측면을 살펴보면 다음과 같다. 현행법상 상거래를 위한 계약체결에 있어서 계약당사자는 계약법의 일반원칙인 계약자유의 원칙에 따라 계약체결의 형식에 구애받지 아니한다. 계약서라는 일정한 형식(방식)에 의하지 아니하여도 의사표시의 합치만 되면 계약의 효력이 생긴다. 따라서 전자적 여건 하에서 디지틀서명을 계약체결에 있어서 특별한 요건으로 삼아야 하는 것은 아니다. 그렇다면, 디지틀서명이 전자상거래를 위하여 어떠한 근거에서 논의되는가. 이는 전자적 환경, 특히 인터넷이라는 개방체제의 네트워크상의 계약체결에서 빚어지는 문제와 관련하여 검토하여야 할 것이다. 개방체제의 네트워크는 안전성(security)이 취약하다는 치명적인 약점을 가지고 있다. 통상의 거래는 양 당사자가 직접 대면하여 계약을 체결함으로써 당사자의 신원을 확인할 수 있을 뿐만 아니라, 거래내용을 명확히 할 수 있는 여건이 마련되어 있기 때문에 신원확인, 당사자간 의사표시확인 및 거래내역을 분명히 파악할 수 있다.[14] 그런데, 전자적 환경 하에서 거래는 非對面이라는 여건에서 즉시에 이루어질 뿐만 아니라, 당사자의 신원확인과 의사표시의 내용을 확인하기란 현실적으로 대단히 어렵다. 이런 점에 비추어 볼 때에 이와 같은 문제점을 해결하기 위한 방법의 하나로 제시된 것이 디지틀서명이다.

디지틀서명은 위에서 살펴본 것과 같이 신원확인, 무결성 및 부인방지라는 기능을 가지고 있는데, 이를 전자상거래에 있어서 규범적인 내용으로 살펴보면, 계약당사자 확인, 계약내용의 진정성 확보 및 계약체결의 확인(또는 법률행위의 성립확인)에 해당한다. 따라서 디지틀서명은 사후에 양 당사자간 당해 거래에 관하여 다툼이 있을 경우에 중요한 증거가 될 뿐만 아니라, 디지틀서명을 붙여 작성한 전자문서는 당해 문서의 진정성을 확보하는 대단히 중요한 입증자료가 될 것이다.

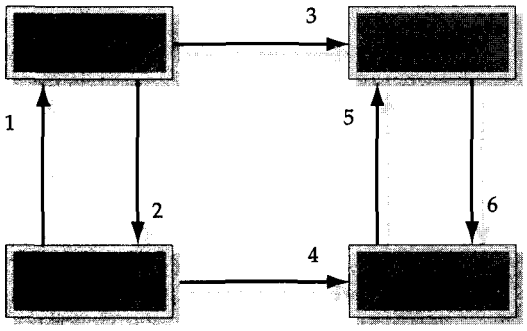
Ⅳ. 인증기관의 인증행위

인증기관의 인증행위에 관한 전반적인 면을 검토하기 위하여 다음의 세 가지로 나누어 살펴볼 수 있을 것이다. 현재 인증행위에 관하여 인증방식인 PKI방식이 가장 널리 이용되고 있는데, 이 방식에 따르면 인증기관(CA), 인증서(certificate) 및 인증서를 보관하는 보관장소(repository)을 중심으로 인증이 이루어지고 있다.

그 과정을 나누어 간략하게 살펴보면 다음과 같다. i) 가입자는 인증기관에 인증을 신청하고, ii) 인증기관은 가입자의 신원을 확인하여 인증서를 발행한다. iii) 인증기관은 인증서를 보관장소에 공개하며, iv) 가입자는 디지틀서명을 한 전자문서를 거래의 상대방(relying party)에게 전송한다. v) 상대방이 저장소(인증기관)에 대하여 가입자의 인증서 확인을 요청하면, 마지막으로 vi) 저장소(인증기관)은 가입자의 인증서가 유효하다는 내용

을 거래의 상대방에게 확인시킨다. 최종적으로 상대방은 인증서의 유효함에 터잡아 거래를 확정짓는다(전자거래의 경우에 계약체결을 완결한다).

이를 그림으로 살펴보면 아래와 같다.



〈http://www.digsigtrust.com/digital/pkiprocess.gif〉

아래에 소개하는 내용은 PKI방식에 따른 인증기관의 인증행위를 검토한 것인데, 우리의 전자서명법의 적용대상은 관계법령에 정한 일정한 요건을 구비한 경우에 인증기관이 신청에 따라 지정된 공인인증기관에 한정하고 있지만, 그렇지 아니한 경우에도 비공인인증기관도 인증업무를 수행할 수 있으므로 양자의 인증행위를 포함한다. 다만, 공인인증기관의 인증행위에 관한 내용에 대하여는 전자서명법의 관련규정을 함께 표시하여 구별하겠다.

1. (공인)인증기관

인증기관은 가입자의 신원과 그의 공개키를 확인하여 그것에 근거한 인증서를 발급하는 주된 인증업무를 수행하며, 이와 관련된 가입자의 공개키를 등록·관리, 인증기관 자신의 키를 생성·관리, 인증서의 취소, 등록·관리, 인증기관간의 상호인증·접속하는 기능을 수행한다. 이러한 인증기관은 인증업무를 수행하기 위하여 기술능력, 재정능력, 시설 및 장비 기타 필요한 사항을 구비하여야 한다. 인증기관은, 요약하면, 가입자의 신원과 가입자에 대응한 디지틀서명 생성키·검증키 한 쌍을 인증하는 신뢰받는 제3자(trusted third party; TTP)다. 이러한 인증기관이 법규에 정한 공인인증기관으로 지정받기 위하여 전자서명법 및 관련 시행령 등에서 정한 요건을 갖추어 정보통신부장관에게 지정을 신청할 수 있다(전자서명법 제2조 9호, 제4조). 이러한 공인인증기관은 인증업무를 안전하고 신뢰성 있게 수행할 수 있다는 것을 인정받은 인증기관이다.

가. 공인인증기관의 디지틀서명키 관리

공인인증기관은 인증업무를 개시하기 전에 정보화촉진법 제14조의 2의 규정에 의한 한국정보보호센타로부터 디지틀서명 검증키를 인증받아야 한다. 이 인증기관은 인증받은 디지틀서명 검증키에 합치라는 디지틀서명 생성키를 이용하여 인증업무를 수행하여야 한다(전자서명법 제8조). 이는 공인인증기관의 인증행위를 신뢰할 수 있도록 하는 방법의 구현으로 공인인증기관과 한국정보보호센타간의 인증업무의 위계성(hierarchy)을 정하고 있는 것이다(전자서명법 제3조).

공인인증기관은 자신이 이용하는 디지틀서명 생성키를 안전하게 보관·관리하여야 하며, 당해 전자서명 생성키가 분실·훼손 또는 도난·유출된 때에는 보호센터에 지체 없이 통보하고 인증업무의 안전과 신뢰상을 확보할 수 있는 대책을 강구하여야 한다(전자서명법 제21조 3항). 공인인증기관이 위의 내용을 통보하지 아니하는 경우에는 법률에서 정한 과태료 납부처분을 받게 된다(전자서명법 제34조 1항 7호).

나. 가입자의 디지틀서명 생성키의 생성 및관리

인증기관은 가입자의 신청에 따라 디지틀서명 생성키를 직접 생성하여 생성키를 가입에

게 전네주거나, 가입자에 의하여 만들어진 생성키에 대한 공개키만을 등록하여 인증업무를 수행할 수 있을 것이다. 전자의 경우에, 인증기관의 인증업무 수행과정 중 관리를 용이하게 할 수 있을 뿐만 아니라, 가입자의 키분실 등의 보안문제의 발생을 막을 수 있다는 장점이 있다. 다만, 인증기관은 가입자 개인의 디지틀서명 생성키의 보관 등에 대한 적절한 방법을 강구하여야 할 것이다. 후자의 개인이 디지틀서명 생성키를 생성하는 경우에는 가입자 개인이 자신의 생성키에 대한 보관에 철저한 주의를 기울여 제3자의 침입을 막을 수 있는 방법을 갖추어야 할 것이다. 가입자가 자신의 디지틀서명 생성키를 안전하게 보관·관리하여야 하며, 공인인증기관과 법률관계를 맺고 있는 경우에 이를 분실 또는 훼손한 때에는 공인인증기관에 통보하여야 한다(전자서명법 제21조 1항).

다. 인증업무수행(certification service)

인증기관의 인증업무수행 내용은 원칙적으로 인증기관과 가입자간의 계약내용에 따라 정해진다. 이 계약내용은 일반적으로 인증기관이 가입자와 인증행위에 관한 계약체결시 제시하게 될 인증업무준칙에서 구체적으로 명시된다. 따라서 세부적인 내용을 여기에서 명시할 수는 없지만, 법률에서 정한 내용을 중심으로 살펴볼 수 있을 것이다. 전자서명법에 정한 것은 공인인증기관에 요구한 내용으로 인증업무를 수행하려는 인증기관에게 표준적인 내용으로 검토될 수 있는 내용이다. 인증업무준칙은 계약당사자간에 있어서 잘못된 인증행위로 인하여 사후에 발생하게 되는 손해에 대한 책임과 직접적으로 관련되어 있다. 따라서 이에 관하여 사법상의 불법행위 및 이에 따르는 손해배상의 관련문제 등에 대하여 사전에 면밀히 검토하여야 할 것이다. 왜냐하면, 인증업무준칙을 양당사자가 명확히 인식할 수 있도록 명확하게 규정하지 아니할 경우에 있어서 복잡한 법률문제로 빠져들게 될 것이기 때문이다. 현재 미국의 VeriSign사의 인증업무준칙은 아주 상세할 뿐만 아니라, 여러 측면에서의 법적 검토를 마친 후 제시하고 있어 우리에게 많은 점을 시사하고 있다.[15]

전자서명법은 인증업무준칙에 관하여 공인인증기관이 인증업무를 개시하기 전에 다음 사항이 포함된 인증업무준칙을 작성하여 주무장관인 정보통신부장관에게 신고하도록 규정하고 있다.

i) 인증업무의 종류
ii) 인증업무의 수행방법 및 절차
iii) 인증역무의 이용조건 및 이용요금
iv) 기타 인증업무의 수행에 관하여 필요한 사항 등이다(전자서명법 제6조 1항).

또한, 위의 내용에 의하여 신고한 인증업무준칙의 내용이 인증업무의 안전과 신뢰성의 확보에 지장을 초래하거나, 가입자의 이익을 저해할 우려가 있다고 판단하는 경우에는 정보통신부 장관은 상당한 기간을 정하여 당해 공인인증기관에게 인증업무준칙의 변경을 명할 수 있다고 규정하였다(전자서명법 제6조 2항).

라. 잘못된 인증업무수행에 대한 법적 조치

인증업무수행에 관한 내용을 검토함에 있어서 두 가지로 나누어 살펴보아야 할 것이다. 하나는 공인인증기관·가입자간의 관계이며, 다른 하나는 비공인인증기관·가입자간의 관계이다. 전자서명법상 인증업무의 내용은 공인인증업무의 내용은 공인인증기관으로서 행하는 경우에 한정하고 있다. 비공인인증기관의 인증업무는 비공인인증기관·가입자간의 법률관계에 따라 정하여질 것이므로 이는 전적으로 사적 자치에 맡기고 있다. 여기에서 전

자서명법에 규정한 내용을 중심으로 검토하겠다. 공인인증기관이 인증행위를 함에 있어서 다음의 내용에 해당하는 사정이 생긴 경우에는 기간을 정하여 정보통신부 장관은 이에 대하여 시정조치를 명할 수 있다(전자서명법 제11조).

i) 공인인증기관의 업무수행방법이 부적합하여 전자서명의 안전과 신뢰성 확보에 지장을 줄 우려가 있는 경우
ii) 공인인증기관으로 지정을 받은 후 법규에서 정한 공인인증기관이 갖추어야 할 사항을 갖추지 아니한 경우
iii) 공인인증기관으로 지정받을 수 없는 결격사유가 있는 경우(임원이 제5조 1호 각 목에 해당하게 된 경우)
iv) 인증업무준칙(제6조)에 의한 신고 또는 변경신고를 하지아니하거나 신고한 인증업무준칙을 준수하지 아니한 경우
v) 인증역무제공(제7조)에 위반하여 인증업무의 제공을 거부하거나 가입자 또는 인증역무 이용자를 부당하게 차별한 경우
vi) 인증업무의 양수(제9조 1항)에 위반하여 인증업무의 양수나 공인인증기관 합병의 신고를 하지 아니한 경우
vii) 인증업무 휴지·폐지(제10조)에 위반하여 인증업무 휴지 또는폐지의 통보나 신고를 하지 아니하거나 인증업무 폐지시 가입자 인증서 등을 인계하지 아니한 경우
viii) 인증업무의 정지 및 지정취소규정(제12조 2항)에 위반하여 지정이 취소된 공인인증기관이 가입자인증서 등을 인계하지 아니하거나 신고하지 아니한 경우
ix) 공인인증기관에의 검사규정(제14조 1항)에 의한 자료를 제출하지 아니한 경우
x) 인증서의 효력정지규정(제17조)에 위반하여 인증서의 효력을 정지 또는 회복하지 아니하거나 그 사실을 확인할 수 있는 조치를 취하지 아니한 경우) 인증서의 폐지규정(제18조)에 위반하여 인증서를 폐지하지 아니하거나, 사실을 확인할 수 있는 조치를 취하지 아니한 경우) 개인의 디지틀서명 생성키의 보호규정(제24조 3항)에 위반하여 가입자의 개인정보 열람 또는 오류 정정에 필요한 조치를 취하지 아니한 경우 등이다.

2. 인증서

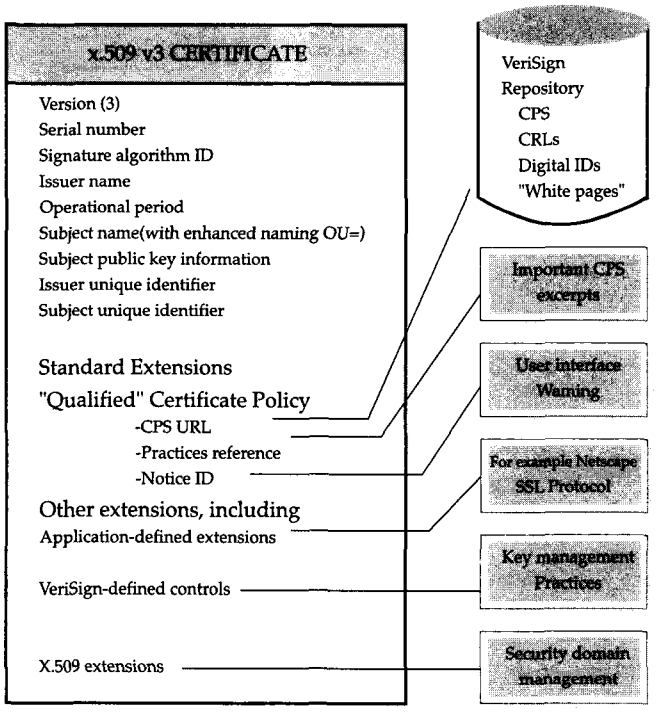
인증서는 디지틀서명을 전체적으로 조망할 때 가장 중요한 내용으로 어떠한 내용을 포함시킬 것인지 여부, 발급, 효력 등이 주된 논의 대상이다. 이에 대하여 입법된 전자서명법의 규정으로부터 공인인증기관의 인증서를 중심으로 검토하겠다.

가. 인증서 내용 및 발급

인증서를 발급받고자 하는 자는 (공인)인증기관에 대하여 인증서의 발급을 신청한다. 이때에 (공인)인증기관은 인증서의 이용범위 및 용도 등을 고려하여 그 신원을 확인하여야 한다.

공인인증기관이 발급하는 인증서에는 다음 사항이 포함되어야 한다.

i) 가입자의 이름
ii) 가입자의 전자서명 검증키
iii) 가입자와 공인인증기관이 이용하는 전자서명 방식
iv) 인증서의 일련번호
v) 인증서의 유효기간
vi) 공인인증기관의 명칭
vii) 인증서 이용범위 또는 용도를 제한하는 경우에 이에 관한 사항
viii) 가입자가 제3자를 위한 대리권 등을 갖



[국제표준 X. 509 v3의 인증서의 예시,
〈http://www.verisign.com/repository〉

는 경우에 이에 관한 사항 등이다(전자서명법 제15조 1항, 2항).

이 내용은 구체적으로 계약내용에 따라 달라질 수 있으나, PKI 방식을 중심으로 논의된 독일의 디지틀서명법 제7조에서 정한 인증서의 내용과 일치한다. 공인인증기관이 인증서를 발급하는 때에는 한국정보보호센터로부터 인증받은 디지틀서명 검증키에 합치하는 디지틀서명 생성키를 이용하여 당해 인증서에 디지틀서명을 하여야 한다. 또한, 공인인증기관은 인증서를 발급받고자 하는 자의 신청에 따라 경우에는 인증서의 이용범위 또는 용도를 제한하는 인증서를 발급할 수 있다. 이 때 공인인증기관은 인증서의 이용범위 및 용도, 이용된 기술의 안전과 신뢰성 등을 고려하여 인증서의 유효기간을 적정하게 정하여야 한다(전자서명법 제15조 3항). PKI 방식의 인증서를 예시하면 다음과 같다.

나. 인증서의 효력

1) 인증서 효력의 소멸

공인인증기관이 발급한 인증서는 다음 사유가 발생한 경우에 그 효력이 소멸된다.

i) 인증서의 유효기간이 경과한 경우
ii) 공인인증기관의 지정이 취소된 경우
iii) 인증서의 효력이 정지된 경우
iv) 인증서가 폐지된 경우
v) 한국정보보호센터가 공인인증기관에게 발급한 인증서가 폐지된 경우 등이다(전자서명법 제16조 1항). 인증업무의 안전과 신뢰성 확보를 위하여 필요한 때에는 전자서명법 제10조의 규정에 의하여 정보통신부장관은 인증업무를 휴지 또는 폐지하였거나, 제12조의 규정에 의하여 인증업무가 정지된 공인인증기관이 발급한 인증서의 효력을 정지할 수 있다. 인증서의 효력을 정지한 때에

는 한국정보보호센터로 하여금 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(전자서명법 제16조 2항).

2) 인증서 효력의 정지(Certificate Suspension) 등

공인인증기관은 가입자 또는 그 대리인의 신청이 있는 경우에는 인증서의 효력을 정지하거나 정지된 인증서의 효력을 회복하여야 한다. 이 경우 인증서 효력회복의 신청은 인증서의 효력이 정지된 날부터 6月 이내에 하여야 한다. 공인인증기관이 인증서의 효력을 정지하거나 회복한 경우에는 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(전자서명법 제17조).

3) 인증서의 폐지(Certificate Revocation)

공인인증기관은 인증서에 관하여 다음 사유가 발생한 경우에는 당해 인증서를 폐지하여야 한다.

i) 가입자 또는 그 대리인이 인증서의 폐지를 신청한 경우
ii) 가입자가 詐僞 기타 부정한 방법으로 인증서를 발급받은 사실을 인지한 경우
iii) 가입자의 사망·실종선고 또는 해산 사실을 인지한 경우
iv) 가입자의 전자서명 생성키가 분실·훼손 또는 도난·유출된 사실을 인지한 경우 등이다. 공인인증기관은 위의 내용에 의하여 인증서를 폐지한 경우에 인증관리체계에 의하여 누구든지 그 사실을 항상 확인할 수 있도록 지체없이 필요한 조치를 취하여야 한다(전자서명법 제18조).

3. 인증업무준칙

인증업무준칙(CPS)이라 함은 인증기관이 인증행위를 통하여 인증서를 발급하는데 실무상 적용되는 세부내용을 말한다. 이는 인증기관에 의하여 제시되는 것으로 인증업무의 기술적 내용 및 인증서 발급에 관한 내용을 담고 있으므로 인증기관의 인증서비스 제공에 있어서 매우 중요한 역할을 한다. 지금까지 공개된 것 중 PKI 방식을 중심으로 한 미국의 VeriSign 사의 인증업무준칙이 업계에서 하나의 표준적 지위를 점하고 있는 실정이다. 이는 VeriSign 사의 인증에 관한 기술이 해당 업계에서 뚜렷한 지위를 확보하고 있다. 그밖에 Utah주의 공인인증기관인 ARCANVS 사의 CPS도 좋은 예가 되고 있다.[16] 현재의 인증방침(certification policy)은 ITU-T X.509 표준과 직접적인 관련을 맺고 있는 것으로 기술내용과 관련하여 인증기관의 인증행위의 구체적인 내용을 정하기 위한 전체적인 지침을 말하는 것이다. 이러한 인증업무준칙은 인증방침을 근간으로 하여 인증기관과 가입자의 기술적 이용관계의 세부적인 내용을 정한 것으로 인증서를 발급을 위한 실무절차에 관한 세부규정이다. 이는 인증서를 신뢰하여 거래하는 거래의 상대방에 대하여도 일정내용이 관련되어 있으므로 인증기관과 가입자에 한정된 것이 아니라, 제3자에게도 직접적인 영향을 미친다. 이러한 점에서 인증업무준칙은 인증 서비스 제공에 관한 전반적인 사항을 규정하고 있고, 적용범위도 일반인에게 미친다는 점에서 공적 규정으로서의 성격도 가지고 있다. 물론, 규범적으로 살펴보면, 거래와 관련 있는 당사자에게 적용되는 것이지만, 향후 디지틀서명의 이용이 확대되어 디지틀서명이 일반화할 때에는 사적 계약내용으로서의 성질에서 벗어나 국가의 일정한 통제가 뒤따르게 될 것이다.

인증서는 인증방침, 가입자 인증절차, 비밀키관리절차 등이 주된 내용으로 구성되지만,

무엇보다도 중요하게 다루어지고 있는 내용으로 인증서의 발급, 취소, 중지, 재발급(재계약) 등에 대하여 명확히 하여야 할 것이다. 이 부분은 일반인에 의한 인증기관의 신뢰도를 평가하는 주요한 평가대상이 될 뿐만 아니라, 실제 인증업무수행상 발생할 수 있는 법적 다툼과 직접 관련되어 있다.

가. 인증업무준칙(CPS)과 이용계약의 관계

인증업무준칙은 인증업무의 수행이 안전하고 신뢰성을 확보할 수 있도록 법률에서 요구한 인증기관이 갖추어야 할 필요사항이다. 위에서 살펴본 전자서명법 제6에서 이를 명시하고 있다. 이런 내용은 인증기관의 인증행위가 대부분 일반인이 이해하기 어려운 기술내용에 따라 행하여지고 있으므로 이용자의 인증행위에 관한 전과정을 이해할 수 있게 할뿐만 아니라, 인증기관의 가입자정보에 대한 보안지침 등을 포함하고 있다. 예컨대, VeriSign 사의 인증업무준칙은 인증업무의 전반적인 소개, 인증업무의 기초, 인증절차, 인증서 발행, 인증서 수취, 인증서 중지·취소, 유효기간만료 및 인증기관의 의무 등을 정하고 있다. 이 인증업무준칙으로 부터 가입자와의 계약내용, 신뢰한 제3자와의 계약내용(relying party agreements), 보안방침 및 지침·기준 등의 세부내용을 이끌어내게 된다. 가입자·인증기관과의 계약은 인증업무에 관한 것으로 계약서상 이를 중심으로 한 계약내용이 정하여지겠지만, 실제로는 그 전반적인 내용을 모두 계약내용으로 적시할 수 없다. 이 때 인증기관의 적정한 인증업무의 수행 여부를 판단하기 위하여 인증업무준칙을 기준으로 삼을 수 있을 것이다. 가입자와 인증기관 모두 인증업무에 관한 법적 다툼이 생기게 될 경우에 이 인증업무준칙을 제시하여 논의하게 될 것이다. 가입자는 법률에 정한 인증업무준칙에 따른 인증업무가 행하여졌는지를 검토할 것이며, 반면에 인증기관은 인증업무준칙에 정한 내용에 따라 인증행위를 행하였다고 주장함으로써 자기의 법적 책임을 면하려 할 것이다.

이런 점에서 볼 때 인증업무준칙이 가입자·인증기관 사이의 계약내용에 명시되지 아니하였다 할지라도 계약이행 여부를 판단하는 실질적인 계약내용으로 검토된다. 따라서 인증업무준칙은 법률상 신고사항으로 중요할 뿐만 아니라, 당사자 사이에 사후 분쟁이 발생했을 경우에 법적 판단의 기준으로 규범적 성질을 띠고 있다.

나. 인증서의 분류(VeriSign의 예)

현재 VeriSign사는 가입자의 신원확인 내용 및 인증서가 사용되는 대상에 따라 세 가지 종류로 인증서를 분류하고 있는데, 각 종류를 간단히 살펴보면 다음과 같다(이면 도표 참조). 아래에 소개한 VeriSign의 인증서는 각각의 경우에 그 요건 및 효과를 구별하고 있다. 이러한 구별은 실제 가입자가 인증기관의 인증에 대하여 지급해야 하는 이용대금 및 사후에 문제되는 손해배상액과 밀접한 관련이 있다. 이는 우리에게도 좋은 검토대상이 될 것이다.

4. 인증기관의 책임

인증기관은 인증서비스의 수행으로 인하여 가입자 및 제3자에게 손해를 입혔거나, 인증서비스를 수행에 관하여 법령에 정한 내용에 따르지 아니한 경우에 그에 대한 책임을 부담한다. 이러한 책임은 민사책임과 형사책임으로 나누어 볼 수 있는데, 공인인증기관의 경우에 전자에 대하여 전자서명법 제26조에 규정하였고, 후자에 대하여 동법 제31조 이하에 자세히 규정하고 있다.

	가입자신원확인 내용	가입자의 비밀키 보호	인증서 사용 예
class 1	자동화설비로 실명 · e-mail 주소 검색 (개인에 한정)	암호화 소프트웨어(권장사항)	web-browsing, 일정한 전자우편
class 2	class 1의 내용 외에 등록정보 및 주소확인 (개인에 한정)	암호화 소프트웨어(요건)	개인 · 회사의 대내 · 외간 e-mail, 온라인 가입, 패스워드교체 등
class 3	class 1의 내용 외에 출두, 신원확인 서류 및 class 2에서 정한 개인의 신원확인 (회사: 거래실적) (개인 · 기업체 포함)	암호화 소프트웨어(요건), 하드웨어Token (권장)	E-banking, database 접근, 회원제 온라인 서비스, 전자상거래 서버 등

〈http://www.verisign.com/repository〉에서 인용

가. 민사책임

전자서명법 제26조(손해배상 규정)는 계약책임과 불법행위책임을 한 조문에 묶어 "공인인증기관은 인증업무 수행과 관련하여 가입자 또는 인증서를 신뢰한 이용자에게 손해를 입힌 때에는 그 손해를 배상하여야 한다. 다만, 그 손해가 불가항력이나 이용자의 고의 또는 과실로 인하여 발생한 경우에는 그 배상책임이 경감 또는 면제된다고" 규정하였다. 인증기관의 인증서비스가 정상적으로 행하여지지 않음으로써 가입자와 인증서를 신뢰한 거래의 상대방에게 손해가 발생하였을 경우에, 인증기관은 이들에 대하여 손해배상책임을 부담한다. 민법상 손해배상책임은 다시 두 가지로 나누어지는데 하나는 계약책임이고, 다른 하나는 불법행위책임이다. 전자는 당사자간 계약으로부터 채권을 발생시켜 채무불이행에 따른 책임을 부담하는 것이고, 후자는 손해를 입은 피해자와 가해자 사이에 아무런 법적 관계없이 발생한 손해에 대한 책임을 논의하는 것이다. 구체적으로 손해의 발생 · 손해배상의 범위 · 배상액산정 등은 당사자 사이의 약정이 있는 경우에 그 약정내용에 따르겠지만, 그렇지 아니한 불법행위책임에 있어서 전자서명법 제26조 규정해석을 통하여 얻어진 법리를 실제 사례에 적용하게 될 것이다.[17]

나. 형사책임

공인인증기관은 가입자에 대한 인증행위의 신뢰성을 확보하는 것이 대단히 중요한 것이므로 이에 배치되는 인증업무수행시 법적 제재를 받게 된다.

전자서명 생성키(비밀키)의 관리에 있어서 i) 가입자의 신청 없이 가입자의 전자서명 생성키를 보관하거나 전자서명 생성키의 보관을 신청한 가입자의 승낙 없이 이를 이용하거나 유출하는 경우, ii) 타인의 전자서명 생성키를 盜用 또는 누설한 경우, iii) 타인명의로 인증서를 발급받거나 발급받을 수 있도록 한 경우에는 3年이하의 징역 또는 3천만원 이하의 벌금에 처한다고 전자서명법 제31조에 규정하였다.

그밖에 i) 공인인증기관은 가입자의 인증서와 인증업무에 관한 기록을 보관하여야 하

는데 이를 위반한 경우, ii) 수집된 개인정보를 인증업무 외의 목적으로 이용하거나 유출한 경우, iii) 인증업무 수행상 알게 된 타인의 개인정보를 누설하거나 타인에게 제공한 경우에 있어서 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다고 전자서명법 제32조에 규정하였다. 위와 같은 내용은 법인의 대표자나 법인 또는 개인의 대리인·사용인 기타 종업원이 그 법인 또는 개인의 업무에 관하여 전자서명법 제31조 또는 제32조의 위반행위를 한 때에는 행위자를 벌하는 외에 그 법인 또는 개인에 대하여도 각 해당 조문에 정한 벌금형을 과한다고 규정하여 공인인증기관과 그 업무수행자에 대하여 묻는 엄격한 책임이다(전자서명법 제33조).

V. 결 어

전자상거래의 활성화를 위하여 무엇보다도 중요하게 다루어야 할 점은 네트워크 이용에 대한 보안성확보이다. 이를 위하여 여러 가지 방법을 논의할 수 있지만, 현재 Web에서 이루어지는 거래를 중심으로 살펴볼 때에 거래가 안전하다는 이용자의 신뢰를 쌓는 일이다. 기술내용의 진보로 인하여 종래 보다 향상된 계약체결 방법이 가상공간상 구현된다 할지라도 실제 이용자가 네트워크의 보안성을 불신할 경우에 기술의 가치를 평가할 수 없을 뿐만 아니라, 통상적인 거래방법에 대하여 우월적 지위를 확보하지도 못할 것이다. 이러한 점과 직접적인 관련을 맺고 있는 것이 위에서 논의한 디지틀서명의 실제 활용내용이다. 이는 금년 7월부터 시행될 전자서명법·전자거래기본법의 입법취지에 그대로 담겨있다. 전자서명법 등이 기술내용을 중심으로 입법되었다 하더라도, 현행법의 규범적 체계와 관련하여 모순 없이 시행될 수 있을 때에 비로소 법규정의 실효성을 발휘할 수 있을 것이다. 이런 점은 기술내용을 담은 법령의 정확한 법리를 파악함으로써 가능해질 것이다.

이러한 점을 전자상거래와 관련하여 살펴볼 때에 기술적 측면 외에 거래와 관련된 계약법적 검토를 간과하지 말아야 할 것이다. 거래에 관한 법적 문제가 사후에 발생할지라도 종래 거래방법의 이용으로부터 보호되던 이용자(소비자)의 권리가 무시되거나, 전자상거래의 기술적 측면의 지나친 강조로 인하여 이러한 법적 검토를 가볍게 다룰 경우에, 이용자(소비자)는 전자상거래의 이용으로부터 기대했던 것에 대하여 실망할게 될 것이므로 최종적으로 전자적 거래방법을 멀리하게 될 것이다. 이와 관련하여 미국 등 정보·기술선진국에서 전자상거래의 확대발전을 이루기 위하여 법률문제의 사전해결의 모색방법으로 학제간의 연구 등 다각적인 노력을 기울이고 있다. 이 분야의 활성화를 꾀하기 위한 초석을 다지고 있는 현실에 비추어 볼 때에 외국의 학제간의 연구는 우리에게 좋은 참고가 되고 있다.

참고문헌

[1] Steven E. Miller, *Civilizing Cyberspace*, ACM Press, 1996, 11 et seq; See Kahin and Nesson(ed.), *Borders in Cyberspace*, MIT Press, 1997.

[2] 미국은 1995년부터 UCC §2B 규정신설을 논의하고 있으며, 장차 세계 전자상거래에 관한 규정으로 사용할 계획을 가지고 있다. UCC §2B에 관하여 특히〈http://www.2BGuide.com〉, 〈http://www.law.uh.edu/ucc2b/〉참조.

[3] Edward A. Cavazos and Gavino Morin, *Cyberspace and the Law*, MIT Press, 1996, 35.

[4] See Kent D. Stuckey, *Internet and Online Law*, Law Journal Seminars-Press, 1996, at §1-2 et seq, §10-2 et seq.

[5] See Lance Rose, *Netlaw*, McGlaw Hill, 1995, 39 et seq.

[6] 대량유통 이용계약의 세 가지 특징은 i) 이용자의 개성무시, ii) 대량의 시장배포, iii) 시장의 다변화 등이다.

[7] shrink-wrap 이용계약이란 컴퓨터 등의 하드웨어를 구입할 때 미리 설치되었거나, 일반 상점에서 또는 주문을 통하여 소프트웨어를 구입하는 경우에 소프트웨어를 꺼내기 위하여 비닐(shrink wrap) 등으로 포장된 것을 뜯음으로써 계약이 체결된다는 지시문에 따라 동봉된 내용으로 체결되는 정보 이용계약을 말한다. 이는 프로그램 등 소프트웨어 제공자와 이용자 사이에 계약내용에 대하여 직접 합의하지 않고 체결된 것이다.

[8] 배대헌, "거래법상 디지틀서명의 효력과 입법을 위한 제언" 계명법학 제2집, 1998, 156쪽 이하

[9] Jonathan Rosenoer, *CyberLaw*, Springer, 1996, 237 et seq.

[10] 우리의 현행법상 서명이 규범적인 면에서 계약체결의 본질적인 요소가 아니라 할지라도, 미국법에서 계약내용에 따라 계약체결을 위하여 갖추어야 하는 실체법상 요건이 되기도 한다. 미국법상 계약체결시 서명을 필요로 하는 법적 근거는 통일상법전(Uniform Commercial Code; UCC) §2-201의 사기방지법(Statute of Frauds)의 규정이다. 1677년에 제정된 영국의 사기방지법에서 연원한 것이지만, 영국은 1950년에 이미 이를 폐지하였으나, UCC에 여전히 계약의 방식으로 당사자의 서명을 규정하고 있다. 이러한 서명의 요구도 본질적으로는 당사자 사이에 법률관계의 명확성을 도모하여 증거를 보전하려는 것이고, 다른 하나는 당사자로 하여금 신중함을 꾀하려는 데에 있다.

[11] 민사소송법 제329조.

[12] ABA, The Digital Signature Guidelines, 〈http://www.abanet.org/scitech/ec/isc/dsg.html〉.

[13] Utah Digital Signature Act Section 102 (3). "· · · to implement legally the general import of relevant standards, such as X.509 of the International Telecommunication Union"

[14] Terry Bernstein et al., *Internet Security for Business*, Wiley, 1996, 125 et seq.

[15] VeriSign, 〈http://www.verisign.com/repository/CPS/〉.

[16] See ARCANVS' Certification Practice Statement(Version: ACPS990206), 〈http://www.arcanvs.com/arcanvsCPS.html〉.

[17] 이에 관하여 자세히는 배대헌, 전자상거래 도입에 따른 디지틀서명의 법리와 인증기관의 민사책임에 관한 연구(정보통신학술연구과제), 1999. 3월, 65쪽 이하.

□ 著者紹介

배 대 헌

1985년 충남대학교 법학과(법학사)
1987년 충남대학교 대학원 (법학석사)
1994년 ~ 1995년 Washington University School of Law(초청연구원)
1996년 충남대학교 대학원(법학박사)
1996년 9월 ~ 현재 계명대학교 법과대학 조교수

※ 주관심분야: 민법, 지적재산권법, 전자상거래 및 디지틀서명에 관한 법률문제