인증 관련 주요 국제기구 및 국가인증제도 현황 분석

Necessity for Establishing International Certification Authority System for Global Electronic Commerce

이호건(Hogun Lee)* · 박승락(Seung-Lak Park)** · 윤영한(Young-Han Yoon)***

요 약 (ABSTRACT)

전자상거래는 비대면(非對面) 거래로 모든 제반과정이 진행되기 때문에 상대에 대한 신뢰성의 문제가 크며, 거래 당사자와 거래 내역에 대한 입증을 해줄 인증기관이 필요하게 된다.

현재 미국의 베리사인 등 사설인증업체가 국내전자상거래 업체의 인증업무를 담당하고 있는 실정이다. 또한, 인증은 필연적으로 관련 기술의 표준화가 수반되는데 이에 대한 국내기술이 미흡하므로 국제동향을 고려한 국내인증기술의 개발이 시급하다.

특히, 글로벌 전자상거래에서는 인증기관에 대한 문제가 더욱 절실한데 문제는 어떠한 형태로 어떤 기관이 주축이 되어 인증체계를 구축하는가 하는 것이다. 현재, 인증체계는 네트워크 방식, 계층구조, 혼합형의 세가지가 논의되고 있으며, 각각의 장단점이 존재하므로 이에 대한 심도있는 논의가 필요하다.

이러한 체계는 국가별로 상이할 수 있지만, 문제는 글로벌 전자상거래를 활성화하기 위해서는 보다 일관된 형태의 인증체계 구축이 필요하다는 점이다. 현재까지 이와 관련한 심도있는 논의는 미흡한 실정이며, 미국 EU 등 일부국가와 UNCITRAL, OECD, ICC 등 관련 기구에서 다양한 의견을 제시하고 있는 상태이다.

이러한 문제는 단시일 내에 해결되기는 어려울 것으로 보이다. 다만, 단기적으로는 관련국가들간의 상호인증을 통한 해결이 가능할 것으로 판단되며, 이러한 상호 인증이 전세계적으로 확산되어감에 따라 글로벌 전자상거래를 위한 인증체계가 심도있게 논의될 것으로 판단된다.

이와 관련하여 상호 인증과 관련한 국내관련 법제의 보완이 필요하며, 실제로 인증을 담당할 관련 당사자들의 자구노력이 매우 시급한 시점이라 하겠다.

Key Word : CA(Certification Authority), Global Electronic Commerce, PKI(Public Key Infrastructure), Digital Signature

* 청주대학교 경상대학 경제통상학부 교수

** 청주대학교 경상대학 경제통상학부 조교수

*** 주성대학 사회문화학부 전자상거래과 전임강사

<목 차>

Ⅰ. 문제의 제기

전자상거래의 개념은 당초 인터넷과는 무관하게 정보기술에 의한 종이문서 없는 환경을 달성하기 위해 제안된 개념이었으나,[1] 1990년대 후반 폭발적으로 급증하고 있는 전자상거래의 확산은 인터넷의 보급을 그 기반으로 하고 있다.[2] 인터넷의 개방성과 글로벌한 접근성은 범세계적인 전자상거래를 촉진하는 요인으로 작용하고 있다.

그러나, 인터넷은 본질적으로 개방형 통신망을 근간으로 하고 있기 때문에 이러한 네트워크에 대한 신뢰성의 문제가 전자상거래 확산에 걸림돌로 작용하고 있는 것 또한 사실이다. 실제로 GVU와 CommerceNet 등의 조사[3]에 의하면, 전자상거래의 가장 큰 장애요인은 전자상거래에 대한 신뢰성의 결여를 그 주요 원인으로 지적하고 있다.

결국, 개방형 통신망에서 법적 효력을 갖는 안전한 상거래를 위해서 거래 양 당사자의 신원확인과 의사표시의 진위여부 등을 확인하기 위한 메커니즘 즉, 인증기관이 필요한 당위성이라 할 수 있다. 이와 관련하여 UNCITRAL, OECD, WTO 등에서는 인증기관 관련 주요 지침을 제시하고 있으며, 세계 각국에서는 이들 지침을 참고한 관련 법제를 추진중이다.

특히, 글로벌 전자상거래의 경우에는 이러한 인증의 문제가 국내인증의 체제 보다 훨씬 복잡하고 난이한 형태를 나타낼 수밖에 없다. 왜냐하면, 국내인증의 경우에는 각 국가의 법제에 의하여 구체적인 형태를 만들고 이들에 근거한 인증기관의 설립과 운용에 의해 인

1) Michael N. Gualtieri. "Turning the EC Vision into Reality", EDI World, p. 18, November 1996.
2) 1999년 12월 현재 인터넷의 사용자는 각 조사 기관에 따라 상이하지만, 대략 2억명 이상으로 추정하고 있음.(http://www.atlantistrans.com, 1999)
3) CommerceNet, "Barriers & Inhibitors to the Widespread Adoption of Internet Commerce", Research Report, http://www.commerce.net/research/free-report/97_05_r.html, 1997. ; GVU, "GVU's 9th WWW User Survey", http://www.cc.gatech.edu/gvu/user_surveys/surveys-1998-04, 1998.

증의 기능을 원활히 수행할 수 있으나, 글로벌 전자상거래의 경우 인증기관에서 발행한 인증서의 법적 지위 등에 대해서는 구체적인 해결 방안이 미흡한 실정이다. 물론, 상호 인증에 의한 해결을 할 수는 있으나, 각 국가의 인증 관련 법규는 국내의 거래를 기준으로 하고 있다는 한계점과 각 국가에서 실제 시행에 따른 문제점이 검증되지 않은 단계라서 인증기관의 운영이 본격화될 경우 파생될 문제점이 없지 않다.[4]

이러한 문제점에도 불구하고, 전자상거래는 매우 빠른 속도로 확산되고 있는 추세에 있으며, 이와 관련하여 현재 전자상거래를 운영하는 업체들은 미국의 Verisign사, 캐나다의 Entrust사 등과 같은 해외 사설 인증업체를 통한 인증 관련 문제를 해결하고 있는 실정이다. 따라서 이들 문제를 간과할 경우 향후 그 파급 효과가 매우 클 것으로 예견되는 분야에 대한 종속의 문제, 경제적 피해가 예견되는 실정이다.

따라서 본 연구에서는 인증기관의 필요성과 기능을 바탕으로 이들과 관련한 국제적 논의 동향과 우리 나라의 현황을 살펴보고, 글로벌 전자상거래를 위해 반드시 필요한 국제 인증 체계는 과연 어떠한 형태가 타당할 수 있을 것인가에 대하여 고찰해 보기로 한다.

Ⅱ. 인증에 대한 일반적 고찰

1. 인증의 의의

(1) 인증의 필요성

기존의 거래와 전자상거래와의 차이점은 여러 가지가 있으나, 가장 중요한 차이점 가운데 하나가 기존의 거래는 관련 당사자가 직접 대면으로 서면에 의한 각종 계약 및 문서의 행위를 하는 제반 업무가 컴퓨터와 같은 매체를 이용해 전자문서와 전자서명을 통하여 이루어진다는 것이다.

이와 같은 환경하에서는 가상공간이라는 환경에서 신원사칭, 전자문서의 불법 변조, 전자 문서를 이용한 계약 사실에 대한 부인 등 여러 가지 문제점이 파생된다. 따라서 이들 문제를 둘러싼 당사자들의 상이한 이해관계를 만족시킬 수 있는 환경의 제공이야말로 전자상거래 활성화의 중요한 관건이라 할 수 있다.

전자문서의 수·발신 당사자간의 신분확인(사용자 인증 : authentication), 전자문서의 변경여부의 확인(문서 인증 : integrity) 및 전자문서를 이용한 전자계약 수행사실에 대한 자의적 번복 거부(부인 봉쇄 : non-repudiation) 등의 기본적인 보안 서비스가 제공되어야 하며, 이를 구체적으로 수행할 기관이 필요한 것이다.

즉, 전자상거래에서의 인증(authentication)이란 정보의 교류 속에서 전송 받은 정보의 내용이 변조 또는 삭제되지 않았는지와 주체가 되는 송·수신자가 정당한지를 확인하는 방법이다. 보통 인증이라고 하면, 사용자 인증과 메시지 인증으로 구분하게 된다.

---

4) 이와 관련된 문제점은 여러 가지가 있을 수 있으나, 비밀키의 도용 혹은 특정 인증기관의 지위 등과 관련한 문제등이 최근 논의 시도단계이다.

사용자 인증이란, 메시지의 생성, 전송, 수신, 이용, 저장 등의 일련의 과정에 관련되어 있는 송/수신자, 전송자, 이용자, 관리자들이 제3자에게 자신이 진정한 사용자라는 것을 증명할 수 있도록 하는 기능을 의미한다. 그러나, 제3자가 위장을 통해 자신이 진정한 사용자임을 입증하는 것이 불가능해야 한다.

또한, 메시지 인증이란 전송되는 메시지의 내용이 변경이나, 수정이 되지 않고 본래의 정보를 그대로 가지고 있다는 것을 확인하는 과정을 의미한다. 즉, 수신된 메시지가 정당한 사용자로부터 전송되었고, 변경되지 않았음을 확인하는 것을 의미한다.

(2) 공개키 구조와 인증기관

전자상거래에서 거래와 관련된 자료에 대한 제3자의 침입 등 여러 가지 문제를 해결하기 위해 암호가 필요하게 된다. 암호(cryptography)란 평문(plaintext)을 해독 불가능한 암호문(ciphertext)으로 변경하거나, 암호화된 통신문을 복원 가능한 형태로 변환하는 기술을 의미한다.[5]

현재의 암호학은 크게 관용 암호 방식(대칭키 암호 방식)과 공개키 암호 방식으로 구분된다. 대칭 키 암호 방식은 암호 키와 복호 키가 일치한다는 것을 의미한다. 즉, 송신자가 수신자에게 평문을 암호화하여 메시지를 보낼 때 쓰여진 키와 수신자가 암호문을 평문으로 바꾸는데 쓰는 키가 일치한다는 의미이다.

반면, 공개키 암호 방식은 키가 다른 것을 의미한다. 송신자가 수신자의 공개키(public key)를 평문으로 암호화해서 보내면, 수신자는 자신의 비밀키(private key)로 암호문을 평문으로 복호화하게 된다. 이 특성 때문에 네트워크 상에서 누군가 암호문을 얻더라도 개인키 없이는 암호문을 복호화 할 수 없으며, 이러한 속성은 전자서명(digital signature)[6]을 가능하게 해준다.

즉, 공개키 암호 방식의 안전성을 보장하기 위해서는 공개키 쌍(공개키, 비밀키)의 안전한 보관 및 관리가 전제되어야 한다. 일반적으로 공개키 암호 방식에서 비밀키는 각 사용자가 생성 및 관리하지만, 공개키의 경우 모든 사용자에게 공개해야 하므로 공개된 키의 불법 변조, 사칭 등이 공격에 대한 안전한 관리가 필요하다.

따라서 인터넷 공간에서 이루어지는 상거래의 활성화를 위해서는 이들 관련 서비스를 제공하는 신뢰할 수 있는 제3자(TTP : Trust Third Party)로서의 인증기관(CA : Certification Authority)이 필요한 것이다. 이 기관으로 하여금 사용자들의 공개키를 공식적으로 인증하는 인증서(Certificate)를 발급하여 해당 공개키의 사용 가능 여부를 공식적으

5) 이만영 외, 「전자상거래 보안기술」, 생능 출판사, 1999. 8. p. 27.

6) 전자서명은 크게 electronic signature, secure electronic signature 및 digital signature로 구분하고 있는데, 본 논문에서는 신원확인 및 무결성 보장의 측면에서 현재까지의 기술 가운데 가장 안정하고 신뢰성이 크다고 평가받고 있으며 수기서명의 기능을 대체할 뿐만 아니라, 보다 다양한 기능을 제공한다는 평가를 받고 있는 공개키 방식의 digital signature를 전자서명으로 간주하기로 한다. (신인순 · 김춘아 · 박민성, 「전자서명 및 인증제도」, 정보통신정책연구원, 1998. 12. p. 9.)

로 증명해줌으로써 공개키 관리상의 보안 취약 요소를 해결 할 수 있는 것이다.

2. 인증기관의 역할

앞에서 살펴본 인증의 필요성을 기초로 인증기관의 역할은 신분확인, 공개키 인증, 시간날인, 증거확보, 배달매개, 분쟁해결 등이 있는데[7], 이를 구체적으로 살펴보면 다음과 같다.

첫째, 신분확인이란 원래의 메시지 작성자가 자신의 이익을 위해 메시지에 서명을 한 경우에 인증기관이 원래의 메시지 작성자의 신분을 증명하는 것을 말한다. 이러한 신분확인은 공개키의 인증기능을 통하여 이루어질 수 있다.

둘째, 공개키 인증(Public Key Certification)이란 특정 비밀키에 대응하여 특정 공개키가 특정인에 의해 소지되고 있음과 그 한쌍의 키가 특정시간에 유효함을 인증기관이 증명하는 것을 의미한다.

셋째, 시간날인이란 신뢰성 있는 게시장치를 보유한 인증기관이 특정한 시간과 날짜에 메시지가 발신되었음을 증명해주는 인증기능을 의미한다. 이처럼 시간날인이 된 경우에는 메시지 발신자가 디지털 서명의 효력을 거절하지 못하게 하는 강력한 증거를 제시해 줄 수 있다.

넷째, 증거보유는 인증기관이 인증작업을 수행하면서 각각의 디지털 서명에 관한 자료를 보관하는 것을 의미한다. 이렇게 인증기관이 디지털 서명과 관계된 자료를 보유함으로써, 실제 분쟁이 발생했을 경우, 당사자는 객관적으로 신뢰성 있는 증거를 이용할 수 있게 된다.

다섯째, 배달매개란 일정한 환경하에서 인증기관이 인증기능 뿐만 아니라, 송신자와 수신자간에 중재자 또는 배달 대리인으로서 배달매개 역할을 하는 경우를 말한다. 이러한 배달매개 기능을 통하여 송신자는 특정 메시지가 수신자에게 정확하게 배달될 것이라는 신뢰를 가지며, 수신자는 원래의 메시지 작성자로부터 온 메시지임을 확인할 수 있게 된다.

여섯째, 인증기관은 분쟁해결에 있어서 중재자로서의 역할을 수행함으로써 분쟁해결기능을 수행할 수 있다. 이러한 분쟁해결기능은 공개키 인증이나 시간날인 등과 같은 인증기관의 기술적인 역할이 아니라 법적인 측면에서 수행하는 역할이다.

3. 인증체계

(1) 인증기관의 구성요소

인증기관을 구성하는 요소로는 인증서[8]를 발행하고 취소하는 인증기관, 인증서 등록 및

7) 이상규 · 한억수 · 구회조, 「전자상거래 효율성 제고를 위한 공인인증체계 구축방안 연구」, p. 106.

8) 인증서(Certification)는 CA가 최종 개체(end entity)를 인증하는 전자증명서 역할을 수행하며, 주체(subject) 사용자가 합법적인 사용자임을 입증하기 위하여 CA는 자신의 개인키를 사용하여 디지털 서명문을 생성하여 인증서를 첨부하게 된다. 보통 PKI 방식에서는 통신표준 제정기관인

사용자 신원확인을 대행하는 등록기관, 인증서 및 인증서 취소 목록을 저장하고 사용자에게 서비스하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 구분할 수 있다.

1) 인증기관

인증기관이란 공개키 기반 구조의 핵심 객체로서 인증서 등록발급조회시 인증서의 정당성에 대한 관리를 총괄하는 시스템을 말한다. 역할에 따라 계층적으로 구성할 수 있으며, 각 계층마다 각기 다른 명칭을 부여하고 있다.[9]

① 정책승인기관(PAA : Policy Approving Authority) : PKI 전방에 사용되는 정책을 수립하고 최상위 인증기관의 역할을 수행한다.

② 정책인증기관(PCA : Policy Certification Authority) : PAA 하위 계층으로서 자체 도메인 내의 사용자와 인증기관이 따라야 할 정책을 수립하고 하위 인증기관의 공개키를 인증하며, 인증서와 인증서 취소목록(CRL : Certificate Revocation List) 등을 관리하는 역할을 수행한다.

③ 인증기관(CA : Certification Authority) : PCA의 하위기관으로서 ㉠ 사용자의 공개키 인증서의 발급 및 취소, ㉡ 자신의 공개키와 상위 인증기관의 공개캐를 사용자에게 전달, ㉢ 등록기관의 요청에 따라 인증서 발급, ㉣ 상호인증서 발급, ㉤ 인증서와 인증서 소유자의 정보 관리, ㉥ 최소한의 정책 책임을 지고, ㉦ 인증서, CRL, 감사 파일 등을 보관하게 된다.

2) 등록기관(RA : Registration Authority)

인증기관과 물리적으로 멀리 떨어져 있는 사용자들을 위해 인증기관과 인증서 요청 객체 사이에 등록기관을 둠으로써, 사용자들의 인증서 신청시 인증기관 대신 그들의 신분과 소속을 확인하는 기능을 수행한다. 조직등록기관(Organization Registration Authority)라고도 한다.

3) 디렉토리(Directory)

인증서와 사용자 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 유효기관이 경과한 후에 일정기간 동안 서명 검증의 응용을 위해 디렉토리에 저장된다.

4) 사용자(User)

PKI 내의 사용자는 사람 뿐만 아니라, 사람이 이용하는 시스템 모두를 의미하며, ㉠ 자신의 비밀키/공개키 쌍을 생성하고, ㉡ 인증기관에 공개키 인증서를 요청하고 인증서를

ITU-T에서 제안한 형식인 X.509 certificate 라는 양식이 사용된다.

9) 김홍선, 「PKI 기반 구조의 구성요소」, 시사컴퓨터 1999. 8. p. 228.

받고, ㉢ 전자서명을 생성·검증하며, ㉣ 특정 사용자의 인증서를 획득하고 그 상태를 확인하고, ㉤ 인증경로를 해석하고, ㉥ 디렉토리를 이용하여 자신의 인증서를 타 사용자에게 제공하며, ㉦ 인증서 취소목록을 이용한 인증서 상태를 검증하고, ㉧ 비밀키 손상 및 분실로 인한 긴급상황 발생시 인증기관에 인증서를 취소하고 새로운 인증서를 발급받는 등의 기능을 수행한다.

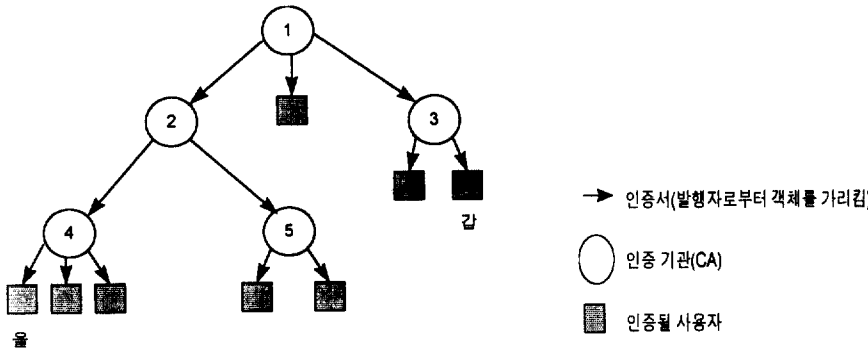
(2) 인증 체계

인증기반구조에서 통신당사자들의 신뢰는 상대방의 인증서를 전달받는 인증경로를 통해 전달된다. 신뢰가 인증경로를 따라 전달되는 방법에 따라 인증기반구조는 크게 두 가지로 구성될 수 있다.[10] 이는 최상위 인증기관인 루트 CA에 바탕을 둔 순수 계층 구조 방식(Hierarchical Infrastructure)과 모든 인증기관이 평면적으로 구성되는 네트워크 구조방식(Network Infrastructure)이 있다. 이와 함께 최근에는 이들 두 가지 형태를 혼합한 혼합형 방식(Hybrid Infrastructure)도 나타나고 있다.

1) 순수 계층 구조 방식(Centralized Certification Infrastructure)

인증기관은 한 개의 루트 인증기관 하위에 계층적으로 연결되는 구조를 가지며, 각각의 인증 기관은 자신의 상위 또는 하위 인증기관과 인증서를 교환한다. 즉, 아래의 그림과 같은 형식으로 구성되며, 최상위 루트 CA는 전반적인 PKI 정책을 수립하고, 제2계층의 CA를 인증하며, 제2계층 CA는 루트 CA에 의해 설정된 정책하에 자신의 정책을 수립하고, 제3계층의 CA를 인증한다. 그리고 제3계층 CA는 사용자를 인증하는 구조로 형성되어 있다.

<그림 - 1> 계층 구조



10) 이경구, "전자인증제도", 「전자상거래 국가전략 수립 토론회」, 한국전산원, 1998. 5. 28. pp. 249 - 260.

계층구조에서 모든 인증서 사용자는 루트 인증기관의 공개키를 소유하고 있기 때문에, 원하는 인증서가 존재할 경우 루트의 공개키로 전자서명을 검증해야만 사용자가 사용할 수 있는 인증서가 된다.

이 구조는 최상위 인증기관간의 상호 인증은 허용하지만, 하부 CA 간의 상호인증은 원칙적으로 배제한다. 그러나, 이 방식은 루트 CA간의 상호인증을 통한 국제간 상호 동작을 원활하게 하는 장점도 가지고 있다. 이 계층구조의 장단점은 아래의 도표와 같다.

<표 - 1> 계층 구조의 장단점

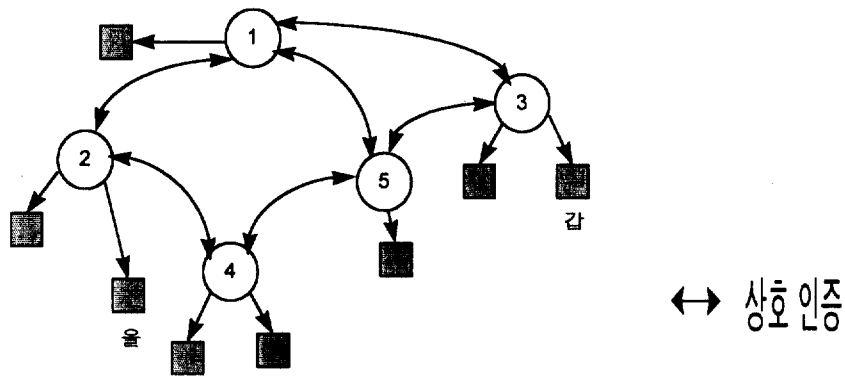
장 점	단 점
- 원하는 인증서의 획득이 용이 - 인증 경로에 대한 검증이 용이 - 계층적인 조직에 적합	- 현실적으로 전세계적인 구성이 불가능 - 루트 인증기관의 비밀키 안전성이 모든 인증서의 안전성과 관계가 있음

2) 네트워크 방식(Decentralized Certification Infrastructure)

네트워크 구조는 일반적인 네트워크 환경에서 근접한 인증기관에 대해 상호 인증을 할 수 있는 구조로서 아래 그림과 같이 모든 CA가 평면적으로 구성되어 있다. 인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구조로서, 인증기관들이 상호 인증하며 인증서를 발급한다. 사용자는 인증서를 발행한 인증기관의 공개키만을 알고 있다.

이 구조에서 인증서를 얻기 위한 인증 경로는 일반적으로 사용되는 라우팅 방법과 동일하게 최단 거리 알고리즘이 적용되며, 경로는 하나 이상이 될 수 있다. 모든 CA 간의 상호 인증을 허용한다. 그러나, 모든 CA 간의 상호 인증이 허용되면, 상호인증의 수가 대폭 증가하는 단점이 있다. 네트워크 방식의 장단점은 아래 표와 같다.

<그림 - 2> 네트워크 방식



<표 - 2> 네트워크 방식의 장단점

장 점	단 점
- 인증기관 간의 상호 인증 - 상업적 상호 신뢰관계 유리 - 융통성 있는 정책과 처리 부하 경감 - CA의 비밀키 손상에 대한 복구 용이	- 원하는 인증서를 찾기 위한 인증경로 체계와 관리의 복잡성 - 단일 인증경로 불가능

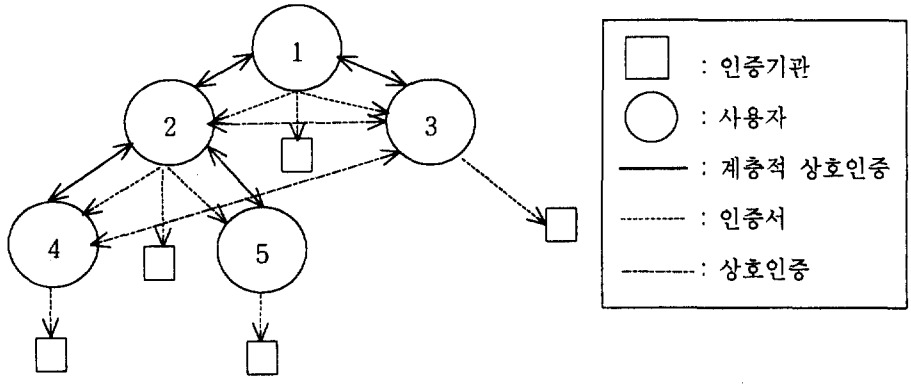
3) 혼합형 방식

혼합형 구조는 계층구조와 네트워크 구조를 혼합한 형태이다. 구조적인 특징으로서 커다란 조직에 대하여 각각 루트인 증가기관이 존재하고, 각 루트 인증기관은 자신의 하위 인증기관에 대하여 인증하며, 동일계층에 존재하는 기관은 다른 루트 인증기관과 상호 인증을 한다.

루트 인증기관의 하위 인증기관은 동일 계층의 인증기관간의 상호 인증이 가능하여 자신의 하위 및 상위 인증기관과의 인증이 가능하다. 따라서 계층구조처럼 하나의 인증서를 갖고 있으며, 다른 인증지관에 대한 인증서는 디렉토리에 저장된다. 네트워크와 계층적인 경로의 좋은 요소를 결합하여 구성되면 네트워크형과 계층구조 형의 인증경로보다 더 효율적일 수 있다.

이 상호 인증을 이용한 방식에는 혼합형 구조가 계층구조를 기본으로 하기 때문에, 아래의 그림에서와 같이 인증기관과 인증기관 사이에서처럼 같은 계층의 일반 상호 인증과 서로 다른 계층의 특별 인증이 존재할 수 있다.

<그림 - 3> 혼합형 구조



4) 시사점

이와 같은 인증기반 구조는 기본구조의 설계에 따라 인증메커니즘의 protocol과 제공되

는 서비스의 model이 분류될 수 있으므로 인증기반구조 구축시 기본구조의 설계는 신중하여야 한다.

현재 구축되고 있는 인증체계는 앞에서 언급한 바와 같이 순수계층구조와 네트워크 방식의 두가지로 구분되며, 최근 이들 두가지 형태를 혼합한 형태까지 합하면 세가지 방식의 형태가 있다고 할 수 있다.

Ⅲ. 인증관련 주요 국제기구 및 국가 인증제도 현황 분석

1. 국제기구 동향

(1) UNCITRAL

UNCITRAL에서는 이미 1985년 제18회 총회의에서 "컴퓨터 자료의 법적 가치"라는 보고서를 제출한 바 있는데, 이 보고서에서 '컴퓨터에 내장되어 있는 자료의 사용이 소송상 증거능력으로서 별 문제가 없을 뿐만 아니라, 국제거래에서 컴퓨터 및 컴퓨터를 이용하는데 매우 중요한 장애가 바로 서류의 문서성(paper form)과 수기서명(manual signature)'라고 지적한바 있다. 이후, 전자상거래에서의 인증 문제와 관련하여 1996년 11월 제정한 "전자상거래 모델법"에서 우선적인 토의 대상으로 전자서명 및 인증기관에 관련된 문제를 선정한바 있다. 이법의 제7조에는 데이터 메시지와 관련한 서명의 요건이 규정되어 있는데, 이것은 인증과 대단히 큰 관련을 가진다.[11]

이후 1997년 12월 12일에 전자서명에 관한 통일규칙초안(Draft Uniform Rules on Electronic Signature)을 발표하였다. 여기에는 인증과 관련된 여러 조항[12]들이 언급되어 있으며, 외국 전자서명의 승인이나 국제간 상호인증 요건[13]을 언급하고 있다.

다만, 국제기구의 통일규칙이라는 성격 때문에 각 국가의 상황에 따라 상이해질 수 있는 인허가제도와 관련한 사항은 언급하지 않고 있다.

(2) OECD

OECD에서 지금까지 전자서명 및 인증제도와 관련해서 법이나 규칙의 형태로 제시된 것은 없지만, 1998년 10월 "국경없는 세계 : 범세계적 전자상거래의 실현"을 주제로 개최된 각료회의에서는 '전자상거래 인증에 관한 선언문(Declaration on Authentication for Electronic Commerce)이 채택되었다.

---

11) UNCITRAL Model Law on Electronic Commerce(http://www.un.or.at/uncitral)

12) 인증기관의 개념(제7조), 인증서(제8조), 인증서의 발급에 의한 표시(제10조), 인증서 소유자에 대한 인증기관의 책임(제11조), 인증서를 신뢰한 자의 책임(제12조), 인증서의 취소와 효력 정지(제13·14조), 인증기관의 인증서에 관한 전자 등록부 작성 및 보존의무(제15조), 인증기관과 인증서 신뢰자와의 관계(제16조)

13) 외국 인증기관의 인증업무(제17조), 국내 인증기관의 보증(제18조), 외국인증서의 승인(제19조).

여기에서는 인증 분야에서 제기되는 다양한 이슈에 대한 검토와 함께 용어의 정의, 네트워크상에서 인증될 수 있는 정보, OECD 각 국가의 인증문제에 대한 접근방법을 간략히 소개하고 있다.

(3) ICC

1997년 디지털로 보장되는 국제전자상거래 일반관례(GUIDEC : General Usage for International Digitally Ensured Commerce)를 발표하였다.[14] 여기의 제Ⅲ편 '전자상거래와 정보 안전성(Electronic Transactions and Information Security)'의 4 '보장과 인증기관(Ensuring and Certification Authority)'과 제Ⅷ편 '인증(Certification)'에서 ① 유효한 인증서의 효력, ② 인증서 진술의 정확성, ③ 인증기관이 신뢰도, ④ 실행과 문제점의 통지, ⑤ 재정 자원, ⑥ 기록, ⑦ 인증기관의 업무 종료, ⑧ 인증서의 효력 정지, 취소 및 이에 대한 통지 등이 언급되었다.

(4) UN의 SEAL

글로벌 전자상거래와 관련된 인증체계와 관련된 문제로서 UN의 SEAL을 참고할 필요가 있다. 이는 UNCTAD의 TPDC(Trade Point Development Center)에서 효율성 있는 범세계적 전자상거래 시스템을 구축하기 위하여 1994년 전세계의 무역기관과 무역진흥조직을 연결하는 GTPnet(Golbal Trade Point Network)[15]을 구축하였는데, 이를 통한 완전한 전자상거래 시장을 조성하기 위하여 시작한 프로젝트가 안전한 전자적 인증 연계(SEAL : Secure Electronic Authentication Linkages)이다. SEAL Project는 몇몇 국가에 인증기관을 설립하고 상호인증을 통하여 인테넷에서의 상거래를 보호하고 다양한 종류의 상거래 발전 유도를 목적으로 하고 있다.[16] SEAL은 현재 미국, 중국, 호주에 설치되어 있는 SEAL 허브를 상호 인증함으로서 세국가를 연결하는 안전한 전자상거래 환경을 조성에 주력하고 있다.

Trade Point(TP)가 ICA(Intermediate Certification Authority)의 역할을 수행하고, 현재 125개국에 존재하며, 국내는 KOTRA가 TP 역할을 수행하고 있다.

(5) ILPF

인터넷 법과 정책포럼(ILPF : Internet Law & Policy Forum)에서는 인증기관과 소비자 간의 관계는 계약에 의해 적절하게 조화된다고 결론 지으면서, 소비자가 인증기관의 수행능력, 서비스 조건, 비용 및 기타 조건에 따라 인증기관을 선택할 수 있게 해야 한다는 주

14) http://www.iccwbo.org/Custom/html/guidec

15) 이만영 · 김지홍 · 류재철 · 송유진 · 염흥열 · 이임영, 「전자상거래 보안 기술」, 생능출판사, 1999. 9. pp. 224 - 225.

16) United Nations Conference on Trade and Development, United Nations Trade Point Documentation Center, 1998. 1. 30.

장을 하고 있다.

2. 주요 국가의 인증 제도 및 체계

(1) 미국

미국은 PKI 기반하에 공공부분 인증기관과 민간부분 인증기관으로 구분하여 연방정부와 주정부[17]의 주도하에 디렉토리 구조의 이원화된 인증체계를 확립하고 있다. 공공기관에 대해서는 국가표준업무 담당기관인 국립표준기술원(NIST : National Institute of Standard Technology)에서 연방공개키기반구조(FPKI)를 구축하면서 전자서명 인증업무를 수행하고 있다.[18]

한편 민간부분의 인증기관은 주 정부의 허가를 받아 운영하도록 되어있다.[19] 가장 앞서있는 정보관련 기술을 이용한 민간 인증기관의 움직임이 매우 활발하며, 특히 Verisign과 GTE를 비롯한 다수의 사업자가 등장하고 있으며, 행하는 업무 역시 다양하다. 이 가운데 일부는 그 영업규모를 전세계로 확대하는 실정이며, 이미 이들 민간인증기관의 상당수가 국내에 진입하거나, 진입을 시도하는 단계이다.

(2) EU

EU는 1998년 4월 전자서명 공동 프레임워크에 대한 유럽의회와 협의회 지침(Proposal for a European Parliament and Council Directive on a common framework for Electronic Signature)을 마련하였다. 여기에서 ① 회원국은 인증서비스 제공이 사전 승인에 국한되지 않도록 하여야 한다, ② 인증서비스 제공을 위하여 자발적인 인가 계획을 도입하고 관리한다, ③ 모든 사항은 객관적이고 투명하며 공평하여야 한다는 의견을 천명한바 있다.

EU의 기반 구조인 ICE-TEL PKI[20]를 구축중인데, 이는 유럽 전체를 하나의 기반 시스템으로 묶기 위한 것으로 최상위에 ICE-TEL CA와 제2계층의 PCA로 구성된다. 각국의 PCA는 각 국가마다 독자적인 이름을 가지며, ICA-TEL의 정책이 허용하는 범위 내에서 자국이 필요한 하위의 CA나 RA를 운영하거나, 소규모 기반 시스템을 운영하는 등 독자적인 정책을 시행하고 있다.

(3) 일본

1998년까지 일본은 공인인증제도에 대하여 부정적인 입장을 취하고 있었으나, 최근에 인

17) 1995년 유타주가 디지털 서명법(Utah Digital Signature Act) 제정후 플로리다, 일리노이, 미시시피를 제외한 대부분의 주에서 유타주의 서명법을 근간으로 입법을 완료하였거나 진행중이다.

18) http://csrc.nist.gov/pki/welcome.html

19) 다만, 유타주는 상무부 상업국에서, 플로리다는 주 국무장관의 허가를 득하도록 하고 있으며, 캘리포니아는 허가를 취하지 않는 인증기관의 존재를 인정하지 않고 있다.

20) http://ice-tel.uni-c.dk/ice-ca/

증의 신뢰성 확보문제와 관련하여 공공기관이 인증기관이 되도록 할 필요성에 제기되고 있으며,[21] 인증기관으로서 법무성이 유력시되고 있다.

한편, 민간 인증의 경우 공개키기반구조에 입각한 인증체계의 시험운영을 실시하고 있는데, 재단법인 정보처리개발협회 산하기관으로 인증실용화실험협의회(ICAT : Initiative for Computer Authentication Technology)를 설치하여 하위 인증기관(20개)[22]의 인·허가를 담당하도록 하고 있으며, 2001년 실용화를 목표로 민법, 상법, 민사소송법 등을 정비 작업 중이다.

3. 국내 현황

우리 나라의 경우, 전자거래기본법(1999년 2월8일) 제정을 시작으로, 전자서명법(1999년 2월 5일 공포) 등의 법안을 제정하였으며, 이와 관련된 시행령 및 시행규칙(1999년 8월 12일 정보통신부령 제81호로 공포)을 제정하고 한국정보보호센터 산하의 전자서명 인증관리센터가 개원(1999년 7월 7일)·인증업무준칙을 수립한 단계이다.

이와 관련하여 공인 CA로서 「행정정보공동이용센터(정부전산정보관리소)」를 「정부전자서명인증센터」로 지정 운영할 예정이다.

거래 당사자의 신원 확인 및 거래의사의 진정성을 확인해주는 신뢰받는 제3자로서의 인증서비스를 제공해주는 인증기관은 미국의 베리사인과 기술제휴를 맺고 출범한 「한국정보인증주식회사」가 설립 시범 운영을 실시중이며, 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.[23]

4. 시사점

외국의 경우 대부분 민간주도의 시장지향적 인증기술 개발을 통한 인증기술의 확보 및 시장 점유라는 전략을 추진하고 있다. 즉, 정부는 민간부분의 자율적인 기술개발에 대한 지원을 강화하고, 민간기업의 기술개발과 이를 통한 인증시장의 성장을 위한 제도적 지원을 하는 형태로 가고 있다.

또한, 인증기반구조 구축을 위하여 미국에서는 연방KMI, 연방PKI, 캐나다에서는 GOC PKI, 유럽연합에서는 ICE-TEL, 호주에서는 PKAF 프로젝트 수행 중에 있다. 미국의 경우는 각 주마다 다른 법률적 체계하에서 여러 개의 인증기관을 허락하고 있으며, 이들 기업은 미국내 다른 주 뿐만 아니라, 다른 국가의 CA와 상호 인증체계를 구축하여 국제적인

---

21) 日本電子商去來實證推進協議會 認證國檢討 WG, 「相互認證 Guide Line」, 「認證國 運用 Guide Line」, 「認證國の 外國の 法制度 調査報告書」, 1998.

22) CA는 현재 ASCINET, FUJITSU, ITJ, MEIJI, NEC, INTERAUTH, JAMI PILOT 등임.

23) 전자신문 각호.

기업으로 인증시장을 주도하고 있다. 한편, EU의 경우에는 기존의 영국과 독일 등 국가별로 입법되고 있는 각종 관련 법규에 대하여 상당부분 수용하면서 공통된 결론을 도출하고 있다. 또한 이들은 Task Force 또는 Working Group 등의 형태로 정부와 민간이 공동으로 각종 분야의 연구를 활발히 진행하고 있음은 주목할만하다.

또 하나의 특징은 통신사업자들이 인증사업자로서 그 영역을 넓혀가고 있다는 점이다. 미국의 GTE, AT & T, 일본의 NTT, 영국의 BT, 프랑스의 FT 등이 인증사업에 참여하고 있는 대표적인 통신사업자들이다. 우리 나라의 경우에도 대표적인 통신사업자인 한국통신이 인증사업에 적극적으로 참여하려는 움직임을 보이고 있다.

Ⅳ. 국제 인증체계 구축을 위한 제언

1. 인증 체계와 관련된 제 문제

전술한 바와 같이 인증체계는 네트워크구조와 계층구조 그리고 혼합형으로 구분할 수 있다. 미국과 캐나다의 경우는 계층구조 주축으로 하고 있으며, EU의 경우에는 네트워크 구조로 인증체계를 만들고 있는 것으로 보인다.

이들 인증체계는 아래와 같은 장·단점이 존재한다. 따라서 최근에는 순수계층기반구조와 네트워크 방식을 혼용한 형태의 복합한 형태가 주축을 이룰 것으로 전망된다.

<표 - 3> 순수계층구조와 네트워크 방식의 특징 비교

	순수계층 기반구조	네트워크 방식
구현	- 용이하지 않음 - 전반적인 정책설정과 구성에 대한 기본 틀을 마련한 이후에 구현 가능	- 용이 - 각 그룹, 조직별로 연관성 있는 시스템간의 상호 인증 가능
상호인증	- PAA를 통한 상호 인증	- 하부 인증기관 간의 상호 인증
확장성	- 높음	- 낮음
상호 동작성	- 높음 - 일관된 보안 정책 하에 조직이 운영되기 때문에 타 기반 시스템과의 연동성 높음	- 낮음 - 각 네트워크는 자신의 정책을 설정함으로써 네트워크간의 호환성을 유지하기 어려움

그러나, 이와 관련된 문제점은 글로벌 전자상거래의 특성상 여러 가지 문제점이 내포된다.

첫째, 각국에서 구축되고 있는 인증체계와 상충되지 않는 글로벌한 형태의 인증기관을 만들 수 있을 것인가? 또한 인증체계를 구축한다면, 어떠한 형태로 인증체계를 구축할 것

인가?

둘째, 인증과 관련한 주체의 문제이다. 현재, 인증과 관련하여 깊은 관심을 표명하고 있는 전자상거래 및 국제무역 관련 국제기구들이 있다. 이들 관련 기구들은 여러 형태의 지침서, 및 모델 법 등을 제시하고 있는데, 이들 기구 가운데 어떤 한 기구가 인증담당 주체기구가 되어야 하는가 또는 관련 당사자들이 새로운 형태의 기구를 출범시킬 것인가?

셋째, 인증은 필연적으로 인증관련 기술의 표준화가 수반되어야 하는데, 어떤 기구에서 여러 가지 기술 가운데 표준을 정할 것인가?

넷째, 미국의 베리사인 등 사설 인증업체와 비자, 마스터 등 결제와 관련하여 SET을 기반으로 하는 사설인증업체와 각국에서 새로이 만들어지고 있는 공인인증기관과의 업무영역문제를 인위적으로 구분할 수 있을 것인가?

다섯째, 각국의 인증 관련 법규와 관련된 문제로 대부분의 국가가 UNCITRAL의 Model Law On EC를 참고로 제정되었다고는 하지만, 각 국가의 특수한 상황을 반영한 입법이 가속화되고 있는데, 이들 법규의 충돌문제이다. 기존의 상거래의 경우 국내거래와 국제거래가 명확히 구분되기 때문에 별다른 문제가 없었지만, 전자상거래의 경우 그 문제는 대단히 복잡한 형태를 나타낼 수 있기 때문이다.

2. 향후 전망

이들 문제는 국경을 초월한 거래인데다, 가상공간을 활용한다는 여러가지의 특성상 단시일 내에 해결될 수 있는 문제는 아니라고 판단된다. 다만, 이들과 관련한 국제적 동향을 살펴봄으로서 대응전망에 갈음하고자 한다.

(1) 인증체계 및 주체

이와 관련하여 미국과 EU를 참고할 필요가 있다. 왜냐하면, 미국의 경우에는 최상위의 공인인증기관을 중심으로 상이한 주법을 허용하고 있으며, EU 역시 같은 맥락에서 파악할 수 있기 때문이다. 특히, EU의 경우 미국보다 각국의 권한을 폭넓게 허용하고 있는바, 이러한 모형은 글로벌전자상거래에서도 상당부분 참조할 수 있을 것이다.

다만, 이러한 형태가 되었을 경우, 최상위의 기관이 필요하게 되는데, 이는 WTO 등 관련기구를 중심으로 한 최상위 인증기관을 만드는 형태를 예측할 수 있을 것이다. 이러할 경우 전세계적으로 일관된 인증체계 확립을 통한 안정을 기할 수 있으나, 구체적으로 어떤 기구를 중심으로 할 것인가와 관련하여 국가간의 논쟁의 여지가 크다.

또다른 예측은 UNCITRAL에서 제시하고 있는 것처럼, 각 국가별로 상호 인증을 통한 국제인증체계를 확립하는 형태이다. 이러할 경우, 시장의 경쟁논리에 의한 인증시장이 형성될 가능성이 크지만, 상당한 시간동안 혼란을 초래할 가능성이 존재한다.[24]

24) 우리 나라의 경우에도 전자거래법 제28조에서 "정부는 전자서명의 상호인증을 위하여 외국정부와 협정을 체결할 수 있다"고 규정함서 외국과 상호인증을 통한 인증의 허용을 가능하게 하고 있으나, 구체적으로 이와 관련된 분쟁이 발생했을 경우 준거법의 문제 등 제반 내용은 구체적으

(2) 인증 관련 기술의 표준화 문제

현재 인증은 암호 기술과 매우 밀접한 관계를 맺고 있는데, 이와 관련한 최고의 기술을 보유하고 있는 국가는 미국이다. 미국은 국가보안을 이유로 암호관련 기술의 대외 유출을 통제해 왔었는데, 사실 이러한 기술의 독점은 인증관련 기술의 전세계적 종속문제를 야기시킬 수 밖에 없다. 따라서 EU 등 관련 당사국에서는 이와 관련된 기술의 허용을 주장하고 있으며, 최근 미국에서 이와 관련된 수출의 일부 허용하고 있는 것도 주목할만한 점이라 하겠다.

(3) 공인인증기관과 민간인증기관의 업무 구분

현재, 국내시장의 경우 인증과 관련해서 SET을 기반[25]으로 하는 비자, 마스타 등 세계적인 신용카드사들이 실물 환경의 안전한 결제구조를 인터넷 EC 환경에 그대로 옮겨놓은 것으로 「SETCo」가 최상위 CA를 맡고 있으며, 하부에 'Verisign' 'GTE' 등 카드사들이 브랜드 CA로서 자리잡고 있다. 이에 비해 전자서명법에서는 한국정보보호센터가 국가 최상위 CA로, 그 하부에 공이 CA 및 등록기관 RA 등을 두도록 하고 있다. 따라서 온라인 거래내용에 대한 최종적 책임도 SET에서는 SETCo가 지는데 비해 전자서명법상에서는 국가가 신뢰성을 보장한다. 물론 제공하는 인증서비스의 종류나 영역에는 차이가 없다.

따라서 근본적으로 인증서비스 영역이 공인CA 및 민간 CA로 구분되지 않기 때문에 경쟁이 불가피하며, 당분간 비대면 거래가 특성인 전자상거래에서 국가기관이 법률로 보장하는 공신력을 우선적으로 선택할 것이라는 점과, SET의 경우 신용카드 결재만이 가능한 반면, 공인 CA의 경우 자금이체(EFT), 지로 등 다양한 서비스가 가능할 것이라는 측면에서 공인 CA의 영향력이 클것이라는 전망도 있으나, 현재 국내 인증시장 자체가 극히 협소하기 때문에 공인 CA가 본격적인 영업을 시작하더라도 당장에 인증서비스를 적용할 영역이 적을 것이라는 반론도 있다.

이러한 문제는 국내의 특수한 사정으로 국한시킬 수 있는 문제라 볼 수 있으나, 인증과 관련한 세계적인 흐름은 일부 소수 국가를 제외한 대부분의 국가가 시작단계라는 점에서 우리 나라와 거의 유사한 문제와 직면할 것으로 예견된다.

결국, EC에서 인증문제는 공인인증기관과 민간인증기관과의 업무 영역을 놓고 일정부분 경쟁에 처할 것으로 판단되며, 민간인증기관에서도 베리사인 등 이미 인증시장에서 상당

로 마련되지 못한 실정이다.

25) 현재, 각 신용카드 회사에서 시행하고 있는 인증은 SET 방식이 주로 사용되지만, 본격적인 의미의 인증기관에서는 PKI 방식이 주로 사용된다. SET과 PKI방식의 차이점 중 가장 큰 것은 그 기반구조가 다르다는 것이다. SET은 신용카드 결제를 위해 고안되었기 때문에 SETCO 라는 루트 CA 밑에 Brand CA 및 지역 CA들이 연결되어 있다. 인증서 형식 면에서는 X.509 포맷을 사용하고 있는 점에서 같지만, 인증서 내에 포함되는 정보들은 다소 다를 수 밖에 없다. 현재 국내에는 SET을 정식으로 인증받아 사용하고 있는 곳이 없으며, 몇몇 쇼핑몰에서 자체적으로 SET 프로토콜에 따라 결제하는 방식을 취하고 있으므로, 은행에서 고객정보를 검토하여 인증해주는 방식을 사용하고 있지는 않다.

부분 경쟁력을 갖춘 업체와 그렇지 못한 각국의 민간업체와 경쟁 또는 제휴라는 다양한 형태의 시장 선점을 위한 노력이 증대될 것이다. 다만, 인증시장은 그 특성상 사용자의 선택이 될것으로 판단되며, 이는 글로벌 전자상거래에서도 마찬가지가 될 것이라는 전망이 크다.

(4) 각국의 법과 충돌문제

현재, 각국가의 법체계는 그 국가의 특수성을 반영하기 때문에 매우 다양하다. 전자상거래 입법과 관련하여 각국의 국내법이 전자거래를 인정하는가라는 가장 기초적인 문제에서 인정할 경우 어떠한 형태에 근거하여 인정하는가라는 문제에 이르러서는 매우 다양한 형태의 법제가 존재할 것이다. 이들 법제가 어떠한 형태로든 전세계적인 표준화된 안으로 정책되어야만 보다 안전한 글로벌 전자상거래를 할 수 있을 것으로 판단된다.

또한, 일부 국가에서 자국에서 만든 인증관련 표준을 채택할 경우, 글로벌 전자상거래와 관련해서는 상당한 저해요인으로 작용할 수 있는바, 이에 대한 심도 있는 논의를 통한 공통된 표준의 도출은 매우 절실하다. 그리고, 인증과 관련된 기술의 진보는 매우 빠른 속도로 이루어지고 있는 바, 자칫하면 제정된 법제가 기술에 종속되는 현상을 보일 수도 있기 때문에 인증관련 법제 가운데 기술과 밀접한 분야는 유연성을 가진 형태로 제정하는 방안도 고려되어야 할 것으로 판단된다.

글로벌 전자상거래는 그 특성상 관습법적 성격을 가질 수 밖에 없다. 즉, 특정 국가의 법제가 전세계적인 강제성을 가질 수 없기 때문에 이와 관련해서는 상당한 시일이 소요될 것으로 판단된다. 이러한 현실에서 최선의 해결방법은 상호 인증을 통해서 전자상거래를 확산시킬 수 있을 것이며, 이러한 상호인증이 전 세계적으로 확산될 경우 보다 구체적인 법규의 제정도 가능할 것으로 판단된다.

3. 국내 인증 현황 및 발전 방안

(1) 국내 인증체계

현재 정통부에서 발표한 공개키 기반구조 구축에 관한 계획을 보면, 최상위 인증기관으로서 한국정보보호센터(KISA)에서 인증관리센터[26]를 설립, 운영하고 그 하위 인증기관 즉, 공인인증기관들은 금융, 행정, 전자상거래 등 분야별로 두도록 되어 있다.[27]

(2) 상호인증과 관련된 국내 법규

우리 나라의 경우 전자서명법 제28조는 "정부는 전자서명의 상호인증을 위하여 외국정부와 협정을 체결할 수 있다"고 규정함으로써 전자인증제도의 국제적 협력 필요성을 인식하

26) http://www.rootca.or.kr/
27) http://webdb.mic.go.kr/BroadDir/법령/0417.htm

고 있다. 이는 UNCITRAL 여기에는 인증과 관련된 여러 조항[28]들이 언급되어 있으며, 외국 전자서명의 승인이나 국제간 상호인증 요건[29]을 언급하고 있다.

그러나, 외국 인증기관 발행의 인증서 효력의 부여문제와 만일 효력을 부여할 경우 이에 따른 책임의 문제 및 인증서 효력에 따른 손해배상책임 문제 등 매우 다양한 문제가 파생되는데, 이에 대한 해결방안은 거의 없는 실정이므로 보다 구체적인 형태의 대안 모색이 필요하다.

다만, 우리 나라가 국제적으로 통일된 전자인증제도의 혜택을 누리기 위해서는 관련 국제기관이 제정·발표한 전자인증제도 관련 원칙[30]에 대한 충분한 고려가 되어야 할 것이다.

(3) 기타

현재 국내 인증을 총괄하게 될 인증관리센터는 정보보호센터의 산하기관으로서 정보통신부의 통제하에 있다. 그런데, 이에 대하여 행정자치부, 재정경제부 등에서 반발이 클 경우 제반 효과를 발휘하기 어려울 우려가 크다. 따라서 이에 대한 각 기구가의 조정작업이 선결되어야 할 것으로 판단된다. 관련 부처들로 구성된 전자상거래 도입 전략 수립 및 전자상거래 활성화를 위한 국가차원의 일원화된 전자상거래를 위한 협의체 구성을 하는 것도 한가지 방안일 것이다.

현재, 전자상거래 관련 입법은 산업자원부가 추진한 전자거래기본법 정보통신부가 추진한 전자서명법이 그 주축을 이루고 있다. 그런데, 이들 두법의 일부 조항에서 영역 중복 문제가 발생한다는 점이다. 특히 공인인증기관의 역할과 관리, 전자문서 및 서명의 법적 효력 등 두 법률간 중복성이 있다. 따라서 상호 보완적인 법률구조를 유지하기 위한 보완대책이 강구되어야 할 것으로 판단된다.

한편, 「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.

또한 전자거래기본법의 경우 「정부는 전자상거래를 위해 노력해야 한다」는 문구 등 전체적으로 피상적인 조항이 많고 전자거래 표준 사용료를 이용자가 부담해야 하는 한편 전자상거래가 방문판매법 적용을 받아 중소기업의 세제 혜택에서 제외된 점은 법의 본래 취지에 어긋나는 것으로 판단된다. 정보통신부가 발의해 제정된 전자서명법은 전자상거래

28) 인증기관의 개념(제7조), 인증서(제8조), 인증서의 발급에 의한 표시(제10조), 인증서 소유자에 대한 인증기관의 책임(제11조), 인증서를 신뢰한 자의 책임(제12조), 인증서의 취소와 효력 정지(제13·14조), 인증기관의 인증서에 관한 전자 등록부 작성 및 보존의무(제15조), 인증기관과 인증서 신뢰자와의 관계(제16조)

29) 외국 인증기관의 인증업무(제17조), 국내 인증기관의 보증(제18조), 외국인증서의 승인(제19조).

30) 민간주도 및 시장중시원칙, 정부규제의 최소화, 정책과정의 민주성보장 등

인증상 문제 발생시 배상책임과 한계가 불분명하며 행정자치부, 금융결제원, 민간 인증기관 간 인증업무의 차별성과 업무준칙이 명확히 구분되지 않는 등 혼돈의 소지가 있다. 만일, 금융권에 온라인으로 계좌를 개설할 경우 해당기관을 일일이 방문해 실명확인을 받아야 하는 번거로움이 존재할 것으로 보인다.

V. 결론

전자상거래에서 인증의 문제는 비대면 거래라는 전자상거래의 한계점을 극복해줄 수 있는 가장 큰 해결방안이다. 또한, 국경의 개념을 초월할 수 밖에 없다는 특성상 인증의 문제는 매우 중요하며, 이러한 이유 때문에 관련 당사국과 국제 기구에서는 매우 심도있는 논의가 전개되고 있는 것이 현실이다.

실제로 인증시장은 1997년 그 시장이 형성된 이후 연 100% 이상 성장해 2001년에는 11억 달러에 이를 전망인데 비해, 국내 시장은 초기 진입단계로서 1999년의 경우에는 세계시장의 0.2% 규모이지만, 2002년에는 400억 달러에 이를 전망이다. 이러한 구체적인 액수는 논외로 하더라도 인증과 관련된 기술이 파생시키는 파급효과는 더욱더 크다는 점이다.

이러한 현실에 비해 우리 나라는 시범 사업단계를 겨우 벗어난 단계이며, 기존의 전자상거래 업계들은 선진 외국의 인증기관서비스를 이용하고 있는 실정이다. 따라서 이러한 문제를 그대로 방치할 경우 외국의 인증기관을 그대로 수용할 수 밖에 없다는 매우 절실한 문제점이 도출된다. 특히, 글로벌 전자상거래에서 인증의 문제는 더욱더 절실한 문제로 귀결될 수 밖에 없다.

매우 급속한 속도로 성장하고 있는 전자상거래의 확산은 필연적으로 인증관련 시장의 확산을 가져올 수 밖에 없으며, 글로벌 전자상거래의 경우 인증관련 체제가 어떠한 형태로 구축되는가에 따라 여러 가지 문제점을 파생시키게 된다. 기존의 국내 법제가 독립성을 가질 수 있는데 비해 글로벌 전자상거래는 해외의 관련 국가 법제와 연계성을 갖는 문제가 필연적이므로 이를 고려한 형태의 정책적 제도적 고려가 필요하다고 판단된다.

우리나라는 세계 최초로 무역자동화 관련 법안을 만든 국가이며, 세계 6번째로 전자서명법을 만든 국가이다. 하지만, 무역자동화와 관련하여 실제 사용에 있어서는 극히 떨어지고 있다.[31] 이러한 현실은 결국, 정부의 입법은 여타 국가에 비해 앞서갔지만, 입법을 뒷받침할 정부의 정책적 지원, 업계의 대응 등이 미흡하기 때문으로 판단된다.

인증과 관련한 문제에서는 무역자동화와 같은 전철을 밟지 않는 정부의 정책과 관련 당·사자들의 노력이 필요한 것이 현 시점이라 하겠다.

---

31) 실제로 1998년 「한국전산원」에서 발간한 "범 세계적 전자상거래를 위한 정책 제언"에서 EDI 활용은 매우 미흡한 것으로 나타나고 있는데, 무역/통관부문 10%, 항만부문 50%, 제조유통부문 7500개 업체에 불과한 것으로 나타나고 있다.

참고문헌

ECommerce Data from Phonezone.Com http://www.phonezone.com/data/index.htm

EITO http://www.fviteurobit.de/defeito.htm

http://webdb.mic.go.kr/BroadDir/법령/0417.htm

http://www.pca.dfn.de/eng/team/ske/pem-dok.html#CA

ICC, 「General Usage for International Digitally Ensured Commerce」, 1998.

ICC, 「ICC Electronic Commerce Project」, 1999. 4.

IITF, A Framework for Global Electronic Commerce, 1997. 7.
http://www.iitf.nist.gov/eleccomm/ecomm.htm

OECD, "OECD Ministerial Conference, A Borderless World : Realizing The Potential of Global Electronic Commerce", 1998. SG/EC (98) 3.

U.S. Government Working Group on Electronic Commerce,
http://www.doc.gov/ecommerce/e-comm.pdf

UNCITRAL, 「UNCITRAL Model Law On Electronic Commerce with Guide to Enhancement」, 1997.

United States Department of Commerce, 「The Emerging digital Economy」, 1998.

Vijay Ahuja, 「Secure Commerce on the Internet」, AP Professional, 1996.

Willian J. Clinton · Albert Gore, Jr., "A Framework For Global Electronic Commerce", 1998.

WTO, 「Electronic Commerce and The Role of the WTO」, 1998. 3.

WTO, 「Special Studies 2 : Electronic Commerce and The Role of the WTO」, 1998.

Zwass, V. "Electronic Commerce : Structures and Issues", International Journal of Electronic Commerce, Volume 1, No. 1. Fall, 1996. 3.

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

김홍선, "PKI 기반 구조의 구성 요소", 「시사 컴퓨터」, 1999. 8.

배대헌, "전자상거래와 전자서명법상 Digital Signature의 법리", 통신정보보호학회지 제9권 1호, 「한국통신정보보호학회」, 1999. 3.

송영부 · 이기영, "전자상거래를 위한 사용자 인증 시스템 구현에 관한 연구", 공학기술연구 제13권 제2호 「인하대학교 공학기술연구소」, 1998.

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.

윤광운 · 장두채 · 김철호, 「전자상거래론」, 무역경영사, 1999. 5.

이경구, "전자인증제도", 한국정보보호센터, 1998.

이경석, "전자상거래의 인증기관과 공개키 기반 구조", 산업연구원, 1998.

이규정, "전자상거래의 신뢰성 확보를 위한 법제 현황과 정비 방향", 정보화 동향분석 144호, 「한국전산원」, 1999. 10.

이만영 · 김지홍 · 류재철 · 송유진 · 염흥열 · 이임영, 「전자상거래 보안 기술」, 생능출판사, 1999. 9.

이상규 · 한억수 · 구희조, "전자상거래의 효율성 제고를 위한 공인인증체계 구축방안 연구", 한국경영정보학회 춘계학술발표대회, 「한국경영정보학회」, 1999.

이원재, "전자상거래에 관한 법적 고찰" - 전자상거래에 대한 UNCITRAL 모델법과 전자서명에 대한 통일규칙초안을 중심으로 - , 중앙대학교 대학원 석사학위 논문, 「중앙대학교」, 1998. 6.

이재규 · 최형림 · 김현수 · 이경전, 「전자상거래학 원론」, 법영사, 1999. 5.

日本電子商去來實證推進協議會 認證國檢討 WG, 「相互認證 Guide Line」, 1998. 3.

日本電子商去來實證推進協議會 認證國檢討 WG, 「認證國 運用 Guide Line」, 1998. 3.

日本電子商去來實證推進協議會 認證國檢討 WG, 「認證國の 外國の 法制度 調査報告書」, 1998.

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

정보화지원단 CALS/EC팀, "인증체계분석 및 동향 보고", 1998. 5.

주재훈, "SET 표준과 우리 나라 인증기관의 구성 방안", 한국정보시스템학회 추계학술발표논문집, 「한국정보시스템학회」, 1997. 11.

최경진, 「전자상거래와 법」, 현실과 미래, 1998.

최영철 · 오경희 · 이재일 · 홍기융 · 이홍섭, "전자서명 인증관리센터 구축 및 운영", 통신정보보호학회지 제9권 3호, 「한국통신정보보호학회」, 1999. 9.

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

허동완, "전자상거래에 관한 법적 고찰", 한국외국어 대학교 법학석사학위 논문, 「한국외국어대학교」, 1998. 9.

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