무역상무학회지 제23권
2004년 8월 pp. 291~320

논문접수일 2004. 6.29.
게재확정일 2004. 8.16.

電子貿易에서 制度上 認證시스템의 問題點에 관한 考察

오 현 석*

Ⅰ. 서론

컴퓨터 네트워크와 정보의 디지털화는 세계의 경제흐름에 큰 영향을 주고 있다. 이러한 새로운 기술과 제도의 개발 및 보급은 전자상거래라는 새로운 패러다임을 탄생시켰으며, 나아가 이국간에 거래되는 무역에도 영향을 주어 무역의 용어, 거래형태, 거래규범 등을 바꾸고 있다. 즉, IT혁명 및 글로벌 네트워크의 확산은 무역거래에도 새로운 패러다임이 적용되도록 하여 전자무역(Electronic International Commerce)이라는 새로운 용어를 탄생시켰다.[1)]

전자무역에는 네트워크(network), 데이터베이스(database), 정보처리시스템(electronic processing systems) 등 다양한 전자적 수단이 이용되어 업무를 수행하게 된다. 전자무역이 전자적 수단을 이용함에 따라 발생될 수 있는 특징으

* 영진전문대학 컴퓨터정보기술계열 전임강사
1) 대외무역법 제2조(6) ; 전자무역이라 함은 "무역의 전부 또는 일부가 컴퓨터 등 정보처리능력을 가진 장치와 정보통신망을 이용하여 이루어지는 거래"를 말한다.

로는 시·공간의 제약 극복을 통한 마케팅 대상의 확대, 무역업무의 전자화를 통한 업무의 효과증대 및 경제적 효율성, 다양한 무역정보의 획득 등이 있다.

그러나 전자적 수단이 무역에 가져다 줄 수 있는 중요한 특징들에 반하여 다양한 문제점 역시 내포되어 있는 것이 사실이다. 이러한 문제점들로서는 전자무역에 있어 계약의 성립과 관련된 다양한 규범적 문제, 재판관할권 및 준거법의 선택문제, 관세부과에 따른 형평성의 문제, 제품과 서비스의 특정에 관련된 문제 및 정보의 교환에 따른 보안문제 등이 될 것이다.

이들 중에서 무엇보다 중요하게 부각될 수 있는 것은 상거래와 관련된 당사자간에 신뢰를 부여할 수 있는 정보보안을 통한 신뢰성확보 문제라 할 수 있다. 전통적 서류거래에서 큰 논란이 없었던 인증(certification)의 문제가 전자무역에서는 선결될 필요성이 있다. 왜냐하면 인터넷 등의 컴퓨터통신을 이용한 전자무역이 급진전되고 있는 반면에 상거래 상대방의 확인수단이 불충분하고 나아가 전자정보의 변조문제 그리고 도용, 위·변조, 사칭 등의 위험이 상존하고 있다는 점 때문이다.

예컨대 한국무역협회의 2001년 '전자무역거래 실태조사'에 따르면 전자무역을 수행할 때 겪는 어려움 중 상거래 상대방의 신용도와 수출입계약 관련 내용의 진위여부 확인의 어려움이 전체 답변의 28.6%의 수위로 나타나고 있음을 참고할 수 있다.

본 연구에서는 국내에 한정된 전자상거래에서의 전자인증제도의 개념에서 벗어나 국가를 달리하는 전자무역에서 전자인증제도가 보다 활성화될 수 있도록 전자인증과 관련된 주요국제규범 및 국내법에서의 전자인증에 관한 규정들을 살펴보고 제도적 문제점을 찾는데 있다. II장에서는 전자무역의 핵심요소인 전자문서의 개념과 그 한계를 알아보고 전자인증의 당위성과 그 역할에 대해서 살펴본다. III장에서는 전자결제를 중심으로 하는 Bolero, TradeCard, SWIFT와 같은 전자결제시스템은 이전에 많은 연구가 있었기 때문에 본 논문에서는 제외하고, 전자문서의 인증시스템 측면에서 Identrus, Bolero, TEDI의 전자문서 인증부분의 구현사례에 대해서 살펴본다. IV장에서는 국가를 달리하는 전자무역에서 인증시스템이 활성화되기 위해 해결되어야할 제도상의 문제점에 대해서 살펴보며, V장에서는 본 연구의 요약 및 시사점을 기술한다.

Ⅱ. 전자문서의 한계와 전자인증의 역할

1. 전자문서의 한계

1) 전자문서의 개념

전자문서는 상인 간 또는 정부와 상인 간 통합적 자동화된 정보체계 환경을 기반으로 정보통신기술에 의한 종이문서 없는 거래환경을 달성하기 위한 목적으로 인터넷과는 무관하게 제안되어 주로 당해 상거래에 한정되어 구현되었다.

전자문서는 키보드 등 입력장치에 의해 가독문자로 입력된 언어를 컴퓨터 내부의 기계어로 변환·처리되어 저장되어 있다가 다시 모니터나 프린트 등 출력장치를 통하여 가독문자로 변환되는 형식의 기록물, 즉 컴퓨터 조직을 통하여 작성·처리되어 컴퓨터 조직의 내부기억장치 또는 외부의 보조기억장치에 존재하는 '전자적 기록물'(electronic record)을 말한다.[2)]

이러한 전자문서의 개념은 종이문서와 비교하여 편리성 면에서 우위에 있어 그 사용이 계속적으로 증가하고 있다.

전자문서와 관련하여 주요 국제기관 및 주요국의 실정법을 살펴보면 다음과 같다.

UNCITRAL 전자상거래모델법 제2조(a)에서는 전자문서 대신에 '데이터 메시지'(data messages)라는 용어를 사용하고 있다. 즉 "데이터 메시지는 특별한 제한 없이 전자문서교환(EDI), 전자우편, 텔렉스 또는 팩시밀리 등을 포함한 전자적·광학적 기타 유사한 수단으로 작성, 송·수신 또는 저장된 정보"로 규정하고 있다. 이는 특별히 컴퓨터에 의하지 아니한 텔렉스 또는 텔레카피 등에 의해서 전송되는 경우에도 이를 전자문서에 상응한 데이터 메시지의 범주에 포섭하여 두고 있어 그 수단과 방법의 다양성을 함축하고 있다는 견지에서 보다 진일보한 시각을 내포하고 있다.

---

2) 이호용 외 6명, "전자문서 이용활성화의 법적 장애요인 분석," 연구보고서, 한국전산원, 1998, p.8. ; 한삼인·김상명, "전자서명 및 전자인증의 법률문제에 관한 고찰,"「비교사법」제8권 제1호(하), 한국비교사법학회, 2000, p.1060.

또한 동 규정의 내용은 UNCITRAL의 전자계약협약예비초안, 전자서명에 관한 모델법등에서도 동일하게 규정하고 있다.[3]

ICC의 '2000년 정형거래조건의 해석에 관한 국제규칙'(International Rules for the Interpretation of Trade Terms 2000)에서는 '전자적 메시지'(electronic message)를 전자신용장통일규칙(Supplement to UCP500 for Electronic Presentation)에서는 '전자적 기록'(electronic record)의 용어를 사용하여 전자문서의 개념을 대신하고 있으며 그 내용은 UNCITRAL의 규정과 동일하다. 다만 "전자기록에 포함된 데이터의 분명한 출처, 또한 완전하고 변조되지 않았음을 확인하는 인증이 가능한 것"[4]으로 전자기록의 범위를 제한한 것이 특징이다.

미국의 'E-Sign' 역시 '전자적 기록(electronic record)[5]을 전자문서의 개념으로 대신하고 있으며 "전자적 수단에 의하여 작성, 생성, 발송, 전달, 수령 또는 저장되는 계약서나 기타 기록물"로 정의하고 있어 UNCITRAL, EU, ICC 등에서 규정하고 있는 개념과 동일하다.

한국의 전자거래기본법 제2조 1호에 의할 경우 "전자문서는 컴퓨터 등 정보처리능력을 가진 장치(이하 컴퓨터)에 의하여 전자적 형태로 작성되어 송·수신 또는 저장되는 정보를 말한다"라고 규정하고 있으며 아울러 전자서명법 제2조 1호에서 동일한 내용을 규정하고 있다.

이처럼 국제기관들과 각 국의 실정법에서는 전자문서를 데이터메시지(data message), '전자 메시지'(electronic message), '전자적 기록'(electronic record), 전자문서(electronic document), 전자정보(electronic information) 등으로 규정하고 있지만 내용 면에서 모두 전자문서를 설명하고 있는 것으로 보아야할 것이다.

2) 전자문서의 한계

(1) 전자문서의 유효성 한계

전자문서의 유효성과 관련하여 각 국의 실정법은 물론 UNCITRAL 전자상거래모델법, EU 전자상거래지침과 같은 주요 국제규범에서도 "전자문서가 단

3) 전자계약협약예비초안, 제5조(a), 'definition of data message'; UNCITRAL Model Law on Electronic Signature, Article 2(c), 'definition of data message'.

4) ICC, eUCP, Article e3(b), 'definition of electronic record'.

5) E-Sign, Section 106(4), 'definition of electronic record',

지 전자적인 형태로 되어 있다는 이유로 그 효력이 부인되지 않는다"고 규정하고 있어 전자문서의 유효성을 인정하고 있다. 특히, UNCITRAL 전자상거래 모델법에서는 컴퓨터 통신을 이용하여 교환되는 전자문서가 종이문서의 원본 서류가 아님에도 불구하고 '기능적 등가물 접근방식'(the functional-equivalent approach)에 따라 법적 지위를 동일시함으로써 전자무역에 있어서 발생할 수 있는 법적 장애와 불명확성을 극복할 수 있도록 전자문서에 '전통적 서면에 기초한 서면성'(traditional paper-based documentation)을 부여하고 있다.[6]

전자문서가 종이문서의 '기능적 등가물'(functional equivalent)[7]이 되기 위해서는 종이문서가 가지는 '정보전달 기능'(informative function), '증명적 기능'(evidential function) 및 '상징적 기능'(symbolic function)을 동일하게 수행하여야 한다.[8] 그러나 전자문서의 증명적 기능에서 종이서류가 가지고 있는 증거력을 동일하게 가질 수 있는지 문제가 된다. 동 문제는 영미법계 국가에서 전문법칙(hearsay rule)[9]이나 '최우량증거의 법칙'(best evidence rule)[10] 등을 통하여 증거허속성(admissibility)의 측면에서 증거능력에 제한을 두고 있기 때문에 전자문서의 증거능력을 인증할 수 있느냐의 문제에서 발생된 것이다.

또한 UNCITRAL 전자상거래모델법은 제8조 원본성(original) 및 제9조 '전자문서의 허용성과 증거능력'(admissibility and evidential weight of data messages)에 관해서 규정하고 있지만 전자계약협약예비초안 등은 동 규정에

---

6) UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, I, E.

7) 종래의 법적 요건에 문서(writing)와 서명(signature)을 요구하고 있는 기존의 법규가 전자상거래시대에 있어서는 거래활성화에 장애로 지적을 받고 있다. 따라서 데이터메시지(date message)가 전통적인 문서와 서명이 가지는 기능을 수행하면서 동시에 법적 효력을 갖기 위해서 어떠한 법적 환경을 제공해야하는가의 문제가 생긴다. 이것은 어떻게 문서와 서명이 종래의 전통적 기능과 디지털 시대의 전자적 환경을 지원하는 기능을 동시에 갖출 수 있는지의 문제이다. 이에 UNCITRAL은 데이터메시지도 어떤 일정한 요건을 갖춘다면 그의 법적 효력을 인정하여야 하는데 이를 '기능적 등가물'(functional equivalent)원칙이라 한다 (Guide to enactment of the UNCITRAL Model Law, I, E. 참조).

8) 노태악, "전자거래에 있어 계약의 성립을 둘러싼 몇가지 문제", 「法曹」 통권 제517호, 법체처, 1999, 10, p.137; 김은기, "전자문서의 법적 효력," 「기업법연구」 제5집, 한국기업법학회, 2000, p.473.

9) 'Hearsay is no evidence'로 표현되는 전문법칙은 영미법에서 배심제도를 보완하기 위해 발전된 것으로 알려지고 있다. 즉, 재판을 직업적으로 하지 않는 배심원들은 증거가치에 대한 판단능력이 낮을 수밖에 없으므로, 증거가치가 미약할 위험성이 있는 전문증거는 아예 증거로 사용하지 못하도록 만들자는 취지에서 비롯되었다.

10) 등본 등의 2차적 증거(secondary evidence)가 아니라 원본문서를 제출해야하는 것을 요구하는 영미법상의 증거법 준칙이다 (Benjamin Wright, The Law of Electronic Commerce, Aspen Law & Business, 1996, §10.1. 참조).

대한 명시가 없다. 또한 종이문서만을 인정하는 관습이 아직까지 존재하고 이와 관련된 규정의 보완이 없는 이상 법적 충돌의 문제점이 발생할 수 있는 한계가 있다.

한편, 전자문서의 경우 문서의 물리적 존재가 요구되는 상징적 기능은 전자문서로 대체하는데 있어 가장 많은 어려움을 야기하는 부분이다. 즉, 종이문서는 하나의 정본이 있으면 이와 똑같은 내용과 형식을 갖춘 문서를 만들더라도 정본이 될 수 없으며, 또한 정본을 복사한다 하더라도 사본일 수밖에 없다. 그러나 전자문서는 전자적인 형태로 저장된 기록을 출력함으로써 어느 때고 똑같은 문서를 얻을 수 잇기 때문에 기존의 종이문서가 지니는 상징적 기능을 전자문서로 대체하는 데에는 한계가 있다.

(2) 전자문서의 보안의 한계

전자문서에 의한 의사표시의 교환과정에 있어서 수신된 전자문서가 정당한 송신자로부터 전송된 것인지 구별하기가 어렵다. 일례로 정당한 본인이 전자문서에 의한 의사표시가 없었음에도 불구하고 위조·변조에 의해 본인이 한 것처럼 계약이 이루어질 가능성이 존재한다.[11]

또한 전자문서가 송·수신과정에서 권한 없는 자에 의해 문서의 내용이 불법적으로 위조, 변조, 도용될 수 있는 가능성 역시 존재한다.

물론 전통적인 무역거래에서 종이문서와 관련하여 거래당사자의 신원에 대한 신뢰가 항상 확실하게 존재하는 것은 아니다. 전통적인 무역거래에서도 타인명의를 도용하는 행위가 존재하였으며 또한 문서의 내용을 위조, 변조하여 거래 당사자 일방의 신뢰를 현혹하여 부당이익을 취할 수 있는 위험이 항상 존재하였다.[12] 그러나 전자문서는 네트워크에 연결된 컴퓨터에 저장되며 또한 네트워크를 통하여 송·수신되는 특징 때문에 당사자의 신원이 쉽게 도용될 수 있으며 또한 전자문서의 내용이 쉽게 해킹(hacking)당하여 위조, 변조될 수 있다. 전자문서가 위조 또는 변조되었을 경우 전자적인 형태의 특성상 진위여부의 확인이 종이문서에 비해서 어렵다.

---

11) Stephen Wilson, "Digital signatures and th future of documentation", Information Management and Computer Security, Vol. 7, No. 2, MCB University Press, 2000. p.83.

12) 오병철. 전자거래법, 법원사, 2000, p.362.

요컨대 전자문서는 보완적인 방법의 이용 없이 전자문서 그 자체로서는 종이문서와 비교하여 작성자의 신원과 전자문서의 무결성 확보가 어렵다는 한계가 있다.

2. 전자인증의 역할

1) 전자인증의 개념

인증(certification)이란 "어떠한 행위 또는 문서의 성립이나 기재가 정당한 절차로 이루어졌음을 공적기관이 증명하는 것"을 말한다.

전자인증(electronic certification)은 인증의 방법이 전자적 매체를 통하여 이루어지는 것이며, 전자서명과 당사자의 동일성 추정에 한정시킴으로써 일반적 의미의 인증과 구분할 수 있다. 따라서 전자인증은 "전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 행위"를 말한다.[13]

전자인증은 일반적으로 사용자 인증이나 메시지 인증과 관련한 시스템 보안 요건의 의미로서 'identification'[14] 및 'authentication'[15]의 개념이 있으며, 전송되는 전자문서의 무결성과 전자서명자의 진정성 보장을 위한 인증서비스 의미로서 'certification'[16]으로 상호 구분된다.

전자공증(electronic notary)은 종래 서면을 이용하여 행하던 공증사무를 전자문서 등의 전자적인 데이터에 대해서도 제공하는 것이다. 공증사무의 운영주체 및 제공서비스의 범위는 기본적으로 현재의 공증인제도에 있어서의 공증과 다를 바 없다. 공증이라는 용어는 법률상 부여된 권한에 근거하여 공적인 기관

---

13) 전자서명법, 제2조(6) (동법에서는 '인증'이라는 용어로 사용되어 있지만 전자서명법에서 전자서명의 인증과 관련되기 때문에 통상적 인증의 개념과 구분을 하기 위해서 '전자인증'의 용어로 대신한다).

14) 서버에 접속하기 위해서 암호번호나 비밀번호로 본인확인을 하는 것을 말한다.

15) 'identification'과 논리적으로 반대되는 개념으로 서버입장에서는 서버에 접속하고자 하는 이용자의 ID를 확인하는 개념으로 'authentication'이라는 용어를 사용한다.

16) 전자무역의 경우 전통적 대면에 의한 계약체결과 비교하여 본인확인 수단이 부족하므로 전자거래에서는 거래상대방을 확인하기 위한 인증을 어떻게 행하는가가 문제가 된다. 그 기술적 수단은 다양하지만 현재는 공개키 암호화방식을 이용한 전자서명이 일반적이다 (Alicia Aldridge, Michele White and Karen Forcht, "Security considerations of doing business via the Internet; cautions to be considered", Internet Research Electronic Networking Applications and Policy, Vol. 7 No. 1, MCB University Press, 1997, p.13).

이 행하는 것에 대하여 사용하는 것이고 민간주체가 제공하는 서비스에 대해서 공증이라는 용어를 사용하는 것은 적절하지 못한 듯 보이나, 실제 전자공증에서 예견되는 서비스는 종래의 공증사무 이외에도 민간주체에 의해서 제공되는 데이터의 보관이나 '일시인부'(time-stamping) 부여 등의 서비스를 포함하는 개념으로 전자공증이라는 용어를 사용하고 있는 경우가 많다.

결국 전자무역을 위한 인증시스템은 신의칙(good faith)을 기초로 진의의 의사표시를 신뢰하여 수용할 수 있는 안정적인 시스템 환경의 구축이 필수적이며 이 같은 시스템 환경은 전자무역에 있어 전자계약의 양 당사자 간 신의의 증진에 기여할 수 있는 원인일 수 있다.

2) 전자인증의 역할

(1) 진정성 보장

전자서명에 대한 전자인증은 개방형 네트워크하에서 전자무역이 가지는 불확실성 및 위험의 증대와 보안의 취약성을 극복할 수 있다. 이로 인하여, 전자무역에 참여하는 주체들의 신원을 확보함으로써 전자무역거래에서 분쟁 발생시 핵심적인 부분인 진정성(authentication) 문제를 해결할 수 있다.[17]

예컨대, 익명성이 증가한 정보사회에서 특히 국가를 달리하는 무역거래의 경우 당사자 신원확인의 문제는 매우 중요하다. 즉, 전자문서를 수신 받은 당사자가 진실로 동 전자문서가 송신자로 표시된 사람에 의해 작성되어 송신된 것임을 확인할 수 있어야 한다. 만약 누군가 송신자의 신원을 도용하여 전자문서를 발송했다면, 전자문서 수신자는 괜한 노력과 비용을 허비하게 된다.[18]

종이문서에서의 서명은 그 문서의 명의인이 누구인가를 명확히 하여 상대당사자의 신원을 확인하는 기능을 주로 하였고, 그러한 기능은 전자서명에 있어서도 마찬가지이다. 전술한 바와 같이 전자서명은 작성자에 고유한 전자서명 생성키를 이용해서 작성되며 그러한 전자서명 알고리즘은 특정인에게만 고유한 것이므로 그 알고리즘으로 인해 작성자의 신원이 명확히 확인될 수 있는 것이다.[19]

---

17) Thomas J. Smedinghoff, op. cit., pp.27~31.

18) Sanu K. Thomas, "The Protection and Promotion of E-Commerce; Should there be a Global Regulatory Scheme for Digital Signatures?", Fordham International Law Journal, Vol. 22, Fordham University School of Law, March 1999, p.1019.

(2) 무결성 보장

전자인증의 또 다른 기능은 수신된 전자문서가 전송과정에서 변조되거나 변경이 가해졌는지 아니면 불법으로 삽입된 것인가에 대한 확인할 수 있는 무결성(integrity) 확보의 기능이다.

종이문서에 행한 서명이 문서내용의 변조여부까지 담보하는 것은 아니며, 단지 그 문서의 명의인이 누구인가를 확인함으로써 위조여부의 판단기능을 한다는 점에서 전자서명은 기존의 서명에 비해 전자문서자체와 내용에 대한 신뢰성의 정도를 증가시킨다.[20]

전자문서의 무결성은 메시지 다이제스트(message digest)를 암호화하여 보냄으로써 구현할 수 있다. 메시지 다이제스트는 암호화 방법이 아니며, 일방향 해쉬함수(one-way hash function)를 이용하여 주어진 정보를 일정한 길이 내의 아주 큰 숫자(해쉬값)로 변환해 주는 것이다.[21]

이 함수는 일방향이기 때문에 주어진 정보로부터 해쉬값을 만들어 낼 수는 있어도, 반대로 이 해쉬값으로부터 원래의 정보를 복구해낼 수는 없다. 다만 정보와 함께 그 정보의 해쉬값을 받은 사람의 받은 정보의 해쉬값을 구한 후 정보화 함께 전달된 해쉬값을 비교함으로써 그 값이 같다면 정보의 전달 중에 정보가 변경되지 않았음을 확인할 수 있다. 만약 그 값이 다르다면 정보가 전달 중에 어떻게든 변경되었음을 알 수 있다. 따라서 비대면거래를 기반으로 하는 전자무역에서 사용되는 전자문서의 무결성이 확보될 수 있다.

(3) 증거력 제고 및 부인방지

전자문서는 다양한 형태를 지닐 수 있다. 즉, 디스크에 의한 저장, 컴퓨터 화면상의 가시화 및 컴퓨터를 통한 출력 등의 모습을 띄게 된다. 전자적으로 저장된 문서를 사람의 사상·관념의 표현이 포함되어 있을 수 있으나, 이것이 서면방식으로 존재하는 것은 아니다. 컴퓨터의 화면에 가시화된 문서는 전자적으로 저장된 문서의 유형화되지 아니한 재생에 지나지 않으며 또한 원본의 복사

19) Steffen Hindelang, op. cit., p.4.
20) 오병철, 전게서, p.371.
21) Steffen Hindelang, op. cit, p.6.

본을 출력한 것에 불과하다. 본래의 전자문서에 대한 컴퓨터 출력에는 작성자의 서명이 들어있지 않다.[22]

원본과 복사본의 식별이 불가능하고 내용을 손쉽게 변조할 수 있는 전자문서의 특성 상 수기서명과 인장과는 다른 새로운 수단이 필요하게 되는데, 전자서명 및 전자인증은 전자서명된 문서가 서명자가 의도한 바로 그 문서로서, 전자문서의 생성, 유통, 보관과정 등에서 발생할 수 있는 변조가 일어나지 않았음을 입증하는 역할을 한다.

한편, 종이문서에서의 서명은 작성자의 고유한 필체와 인감의 형태로 작성사실을 부인하는 것을 봉쇄할 수 있었다. 그러나 서명과 날인의 진정성은 재판과정에서 감정을 통해 법관의 심증을 형성하여 진위를 결정하게 되므로, 지극히 정교한 위조방법으로 서명이나 날인을 하는 경우에는 오히려 사실과 다른 법적 판단이 이루어 질 위험이 있다. 그러나 전자서명의 경우에는 종전의 서명과 달리 매우 과학적이고 정교한 수학적 방법을 이용하여 전자서명이 이루어지므로 사실에 부합하는 법적 효과의 귀속을 보장하는 기능을 한다.[23]

Ⅲ. 전자인증시스템 구현사례

1. Identrus

1) Identrus 개요

Identrus(IDENtification TRUSt)는 전자무역의 활성화를 위해 거래당사자의 원활한 신원인증(authentication of identity) 서비스를 목표로 금융기관(financial institutions)[24]들에 의해서 1999년 4월 설립된 인증기관이다.[25] 그 후 Identrus는

22) Sanu K. Thomas, op. cit., p.1021.

23) 오병철, 전게서, p.372.

24) Identrus 프로젝트에 참가한 금융기관들은 ABN AMRO, Bank of America, Bankers Trust, Barclays, Chase Mahattan, City Group, HypoVereinsbank 이다.

25) Bolero 서비스가 전자적 선하증권을 통하여 무역의 자동화를 목적으로 한다면, Identrus는 금융기관의 'trust community'를 통하여 전자인증 및 신용서비스를 제공하는 것을 목적으로 한다.(신동림, 신기술신경영, special report, IBM, http://www.ibm.com) visited on 2003. 10.

계속해서 새로운 금융기관들을 가입시키고 있으며 주로 거대은행만을 대상으로 하고 있다. 2003년 현재 60여 금융기관들이 Identrus 인증기관으로써 Identrus 시스템에 가입되어 있으며 이들 금융기관들은 166개국 이상의 국가들과 수백만 기업관계를 대표하는 PKI 기반의 국제금융거래를 위한 최상위 인증기관이다.[26]

전자무역거래에 있어서 당사자의 신원확보를 위해 금융기관들은 전자서명 등록기관(Register Authority) 역할 및 인증기관의 역할을 동시에 수행하며, Identrus는 최상위 인증기관(Root Certification Authority)역할을 수행한다. 또한 계층적 인증구조로 되어 있으며 최상위 인증기관과 이용자 사이에는 인증등급에 따라서 등록기관과 인증기관의 역할을 하는 1단계 금융기관(level 1 financial institutions)과 2단계 금융기관(level 2 financial institutions)이 존재한다.[27]

Identrus는 Identrus 시스템 운용의 법적 안정성을 위해 신원인증서약관(Identrus Identity Policy : IIP)과 유틸리티인증서약관(Utility Certificate Policy : UCP)을 이용하고 있다.[28] 두 약관 모두 Identrus 시스템 가입자에 한해 적용되며 시스템에 가입한 당사자간의 거래관계를 규율한다. 동 약관들은 Bolero의 Rulebook과 마찬가지로 Idenstrus 시스템의 참여자로 서명한 모든 사용자를 구속하는 다자간 교환약정의 성격을 띄고 있다. 따라서 가입자는 거래시 마다 서로간의 교환약정을 체결할 필요가 없이 Identrus가 제공하는 동 약관들에 의해 규율된다.

2) Identrus에서 전자문서 인증

Identrus 시스템은 국제적으로 다양한 서비스[29]를 제공하기 위해서 개방적

---

26) Identrus Company Overview(http://www.identrus.com/company/) visited on 2003. 10.

27) "The Opportunity for Financial Institutions in the Identrus System", Identrus LLC., 1999, p.18. (http://www.identrus.com) vistied on 2002. 10.

28) IICP와 IUCP는 모두 계정(ID)의 유효성확인 서비스에 적용되지만 IICP는 조직 인증 및 부인봉쇄와 관련된 서비스를 제공하고, 반면에 IUCP는 참여금융기관 및 그 금융기관의 고객들에게 전자문서의 기밀성 및 무결성을 제공한다.(Identrus Identity Certificate Policy IP-ICP Version 1.7, 2 및 Identrus Utility Certificate Policy IP-UCP Version 1.7, 2 참조)

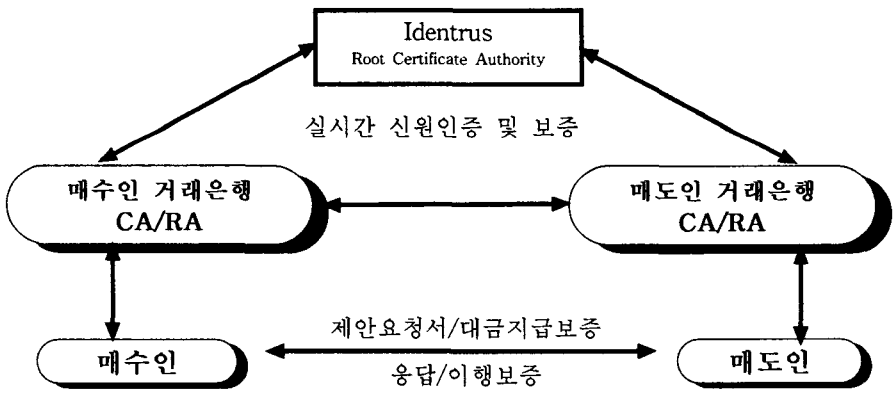
29) Identrus의 서비스로는 지급(payment), 현금관리서비스(cash management services), 보안전자우편(secure e-mail), 접근통제(access control), 메시징(messaging), PKI 서비스(PKI Services), 문서관리(document management) 등이 있다.(Identrus Trust Network; Company and Applications Overview, http://www.identrus.com) visited on 2003. 10.

그리고 기술중립적 정책을 추구한다. 특히 모든 서비스에는 글로벌 ID로 불리는 암호보안 디지털 신원확인 서비스를 제공하며, 글로벌 ID에 대한 실시간 유효성확인을 제공한다.[30]

Identrus는 DCS(Delegated Certificate Services) 시스템을 통하여 인증서비스를 제공한다. DCS 시스템은 디지털서명관리시스템(Digital Signature Management System)과 하드웨어보안모듈(Hardware Security Module)이 포함되어 있다.

DCS 시스템은 매수인, 매도인, 매수인의 거래은행 그리고 매도인의 거래은행의 관계를 통하여 인증서비스가 이루어지며 그 절차를 살펴보면 <그림 1>과 같다.

<그림 1> Identrus 인증서비스 절차



첫째, 매도인과 매수인간 계약체결 후 매도인은 자신의 거래 금융기관에게 거래당사자인 매수인이 Identrus로부터 부여받은 신원확인(글로벌 ID의 유효성확인)을 요청한다.

둘째, 매도인의 거래금융기관은 전자통신방식으로 매수인의 금융기관에 매수인의 신원확인을 요청한다.

셋째, 매수인의 금융기관은 자신의 고객인 매수인의 신원을 확인하고 DSC

30) Identrus 인증서비스는 전자서명이 유효하지 않거나 서명자가 인증서를 사용할 권한이 없을 경우 소구권을 제공하며 전 세계적으로 Identrus 인증클레임을 해결하기 위하여 간소화되고 통합된 수단을 제공한다.

시스템을 통하여 매도인 금융기관에 신원인증서를 전송한다.

넷째, 매도인 금융기관은 매도인에게 신원인증서를 통지한다.

다섯째, Identrus가 부여한 신원확인에 의존하는 매매당사자는 자신들의 금융기관을 통해 잔존위험에 대한 ID보증을 확보한다.

Identrus 시스템에서의 신원인증서의 요청 및 확인과 관련된 메시지들은 공개키 암호화방식을 따르며 그 절차는 일반적인 공개키 암호화방식의 절차와 동일하다.

2. Bolero

1) Bolero 개요

Bolero(Bill of Lading Electronic Registry Organization) 서비스는 국제물품매매, 운송, 보험, 결제 등 무역거래에 필요한 종이서류를 전자문서로 전환하고 인터넷을 통하여 안전하게 교환할 수 있는 기반을 제공하는 것을 목적으로 하고 있다.[31]

Bolero 서비스는 Bolero Project의 산물로서, 유럽에서 무역거래에 관련된 절차의 전자화를 추진하기 위해서 1994년부터 1995년까지 홍콩, 네덜란드, 스웨덴, 영국, 미국의 해상운송사, 은행, 통신회사 등이 참여하여 컨소시엄 형태로 추진된 것이다. Bolero 서비스는 SWIFT(Society for Worldwide Interbank Financial Telecommunication)와 선박·운송회사 및 항만당국이 구성한 상호보험단체인 TT(Through Transport) Club의 양 기관의 주도아래 1995년 7월부터 3개월간 법적·기술적 타당성을 검토 받은 후 1998년 6월부터 상업화를 위한 활동을 전개하였다.

Bolero 서비스는 양도성 유가증권인 선하증권 등의 선적서류를 전자화하는 것, 중앙등록기관에서 전자데이터를 일괄등록하고 인증제도에 의해 데이터의 유일성을 확보하고 보존하는 것 그리고 중앙등록기관에 의한 디지털 서명의 발행 또는 인증제도를 통한 전자적 양도 등에 의한 유가증권으로서의 선화증

31) 2003년 현재 볼레로에 가입한 업체의 수는 약 100개에 달하며 우리나라에서는 한빛은행, 외환은행, 삼성전자, 포스코, 현대상선, 한진해운, 고려해운 등이 회원으로 가입하고 있다 (양정호, "전자식 선하증권과 전통적 선하증권의 비교 연구", 성균관대학교 대학원 박사학위청구논문, 2003, p.12).

권의 유통성을 확보하는 등에 중점을 두고 있다.[32]

특히 Bolero 서비스의 신원확인과 계약의 형성 및 진행은 BAL(Bolero Association Limited)[33] 서비스계약과 그리고 BIL(Bolero International Limited)[34] 서비스계약을 통하여 이루어진다. 이와 같은 등록절차가 필요한 이유는 사용자의 신원을 확인함으로써 전자무역의 특징인 비대면에서 발생할 수 있는 신원확인불능 및 사기에 대한 위험을 경감시키기 때문이다.

Bolero 서비스의 이용자들은 Rulebook 이라는 다자간 교환약정에 서명함으로써 Bolero 서비스를 제공받을 수 있으며, 국제해사위원회(Comite Maritime International)의 해상화물운송장·전자식 B/L에 관한 CMI규칙하의 서비스와는 달리 자체적으로 신뢰할 수 있는 제3자(Trusted Third Party)로서 전자적 메시지의 송·수신을 담당하며 송신자와 발신자의 메시지는 디지털 서명(digital signature)을 통해 전자문서에 대한 진정성과 무결성을 보증 받는다.[35]

2) Bolero에서 전자문서 인증

Bolero 시스템을 사용하고자 하는 가입 희망자들은 요구되는 개인신상에 대한 충분한 정보를 제공하고 진정성을 확인 받아야 하며[36] Bolero 선하증권(Bolero Bill of Lading)의 text는 볼레로 시스템의 안전한 전자문서 전달 통로인 CMP(Core Messaging Platform)를 통하여 전송되고 권리등록시스템(title registry system)에 기록된다.

CMP는 사용자간 전자문서의 교환을 담당하면서 전자문서의 진정성과 무결

32) J. Livemore & K. Euarjai, "Electronic Bills of Lading; A Progress Report", Journal of Maritime Law and Commerce, Vol. 28. No. 1, The Jefferson Law Book Company of Baltimore, 1997, p.58.

33) BAL은 볼레로 시스템의 사용자 집단으로 시스템 운영상의 법률적 기반 구축과 지속적인 시스템 개발책임을 담당하고 있으며, 또한 BIL과 함께 볼레로규정집 개정절차(Bolero Rulebook amendment process) 및 자체 징계절차(disciplinary procedure)를 담당한다. 볼레로 시스템을 이용하기 위해서는 먼저 BAL과 서비스계약을 체결하여야 한다.

34) BIL은 SWIFT와 TT Club이 동일한 지분참여를 통하여 설립한 합작투자기업으로 Bolero.net 서비스의 운영책임을 담당하며, 'CMP', 권리등록, 인증, 보안, 사용자 및 시스템 관리 등과 같은 핵심 기술적 부분을 관장한다.

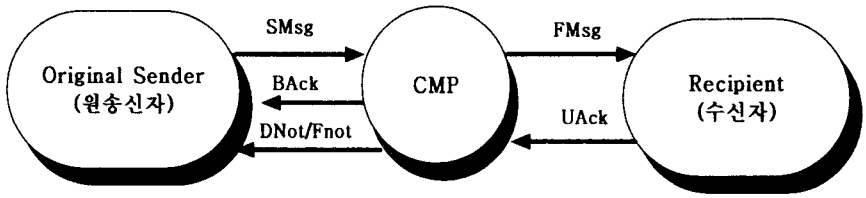
35) 안병수, "전자식 선하증권의 실용화에 따른 문제점에 관한 연구", 성균관대학교 대학원 박사학위청구논문, 1998, pp.95~96.

36) 예컨대, 기업의 경우 가입신청서, 법인증명서(certificate of incorporation)을 토대로 공증인이 작성한 보고서, 공증인이 공증을 거친 법인증명서, 관련 행정기관이 서명한 보고서를 제출하여야 한다.

성을 확인하는 인증기관의 역할을 수행한다. 이를 위해서 CMP에서는 공개키 암호화방식을 기반으로 한 디지털 서명 방식을 채택하여 사용자들의 공개키를 등록하고 인증서를 발급함으로써 송신자의 공개키를 통하여 송신자의 진정성과 전자문서의 무결성을 확인한다.[37]

CMP를 통한 전자문서의 인증절차를 살펴보면 다음과 같다.

<그림 2> Bolero 인증서비스 절차



첫째, 송신자의 컴퓨터를 통하여 CMP에 메시지를 생성하면 당해 메시지는 송신자의 디지털 서명이 첨부된 SMsg(Sent Message) 형태로 볼레로 헤더를 가지게 되며, 다음으로 선하증권의 원문을 첨부하고 이를 디지털 서명하여 CMP로 전송한다.

둘째, Bolero 시스템은 메시지를 수신한 후 서명의 적정성을 평가하고 문제가 없다면 송신자에게 메시지의 진정성과 무결성을 인정하는 BAck(Bolero Acknowledgement)를 전송한다.

셋째, 다음으로 권리등록시스템에서 송화인 또는 새로운 BBL의 양수인에게 FMsg(Forward Message)를 전송한다.

넷째, 양수인이 메시지를 수취하였음을 알리는 UAck(User Acknowledgement)를 전송한다.

마지막으로, 메시지가 예정된 수신인에게 인도된 경우 DNot(Delibery Notification)을 전송하고, 만약 그렇지 않은 경우 FNot(Fatal Notification)를 전송한다.

한편, CMP를 통한 전자문서에 첨부되기 위해 생성되는 전자서명은 공개키 암호화방식을 따르며 그 절차는 일반적인 공개키 암호화방식의 절차와 동일하다.

---

37) Diana Faber, "Electronic Bills of Lading", Lloyd's Maritime and Commercial Law Quarterly, LLP Ltd., May 1996, p.242.

3. TEDI

1) TEDI 개요

TEDI(Trade Electronic Data Interchange)는 EDEN(Electronic DElivery Negotiable Document)의 성과를 계승하여 1998년 민·관계 총 37개 기관이 참가하여 국내·외 전자문서 인증시스템 예컨대 JETRAS, NACCS, Bolero 등과의 상호 연동을 의도하고 설계되었다.[38]

제반 인증시스템과 접속을 위한 공통규약으로 첫째, 전자문서교환규약(interchanged agreement), 둘째, '전자문서 인증서비스 이용규약'(repository service terms and conditions), 셋째, '전자서명 서비스 이용규약'(electronic signature service agreement) 등을 마련하여 국제상사 관련 통일 법규범이나 국제조약과의 연계성을 확보하고 있다.

TEDI는 국제표준이용규약인 UN/EDIFACT나 'XML 문서형식'에 의해 전자문서의 송·수신 및 조회 서비스를 제공한다. 이를테면 이용자로 하여금 송·수신된 전자문서 상호 간 검색 및 조회의 편의성을 극대화하기 위해 각각의 전자문서를 개별기업 독자적으로 이용하는 전용항목과 기업 간 공통으로 이용할 수 있는 공통항목으로 구분하여 두고 있다. 또한 제반 서비스 플랫폼은 암호화 또는 전자서명에 의한 전자문서의 안전한 전송과 확인, 화물권리자의 정보 및 전자식 선하증권의 권리이전에 관한 관리, 전자문서의 이력관리를 통한 국제상거래 흐름의 신속화 및 신뢰성의 향상, 각 단계에서의 비용절감 등의 실현에 주안점을 두고 있다.

TEDI에 있어 전자문서 송·수신은 전자서명 및 전자인증이 결부된 복수의 문서를 일체화 하고 있는데 이를 자체적으로 소위 'TEDI 전자문서'라고 지칭한다. 전자문서의 송·수신자 간 본인확인을 위한 기술수준은 자체 '인증증명서', 기존의 여타 인증기관의 인증서 및 전자서명, 암호화 관련 DES[39]와 RA

---

38) 최석범, "사이버무역시대에서의 글로벌기업간 전자상거래의 모델도입현황과 문제점에 관한 연구," 「무역학회지」 제28권 2호, 한국무역학회, 2003, p.390.

39) DES(Data Encryption Standard)는 상업적으로 폭 넓게 개발된 최초의 대칭형 암호화 표준으로 1974년 미국 상무성으로부터의 공식요청에 의하여 IBM이 개발하였다. DES는 1977년에 미국 연방표준으로 1981년에는 금융산업 표준으로 채택된 바 있는데 이 표준은 비정형화 되어 있는 정부의 기록과 금융산업의 거래를 위하여

S[40]를 채택하며, 송신의 부인방지에 대해서는 전자서명, 수신의 부인방지에 관해서는 별도의 응답에 대한 서명 등을 채택하고 있다. 특별히 송·수신된 전자문서의 복제를 방지하기 위하여 '세션 ID'[41]를 결부하고 있다. 제반 전자문서 인증시스템과 연동은 수출·입 신청허가에 있어서는 JETRAS, 수출·입 통관 중계(interface)는 NACCS와의 접속이 필수적이다. Bolero와의 접속은 게이트웨이(gateway) 기능을 가져야 한다.

2) TEDI에서 전자문서 인증

무역거래의 참가자는 복수의 국가와 거래를 하기 위해 각국의 전자상거래 관련 법제도 및 가이드라인에 적합해야할 필요가 있다. TEDI는 참가 기업이 이미 이용하고 있는 인증기관의 인증서를 수용한다는 개념으로 접근하고 있으며, 인증기능, 등록기능, 참조기능이라는 세 가지 기능을 통해 인증시스템을 구현한다.

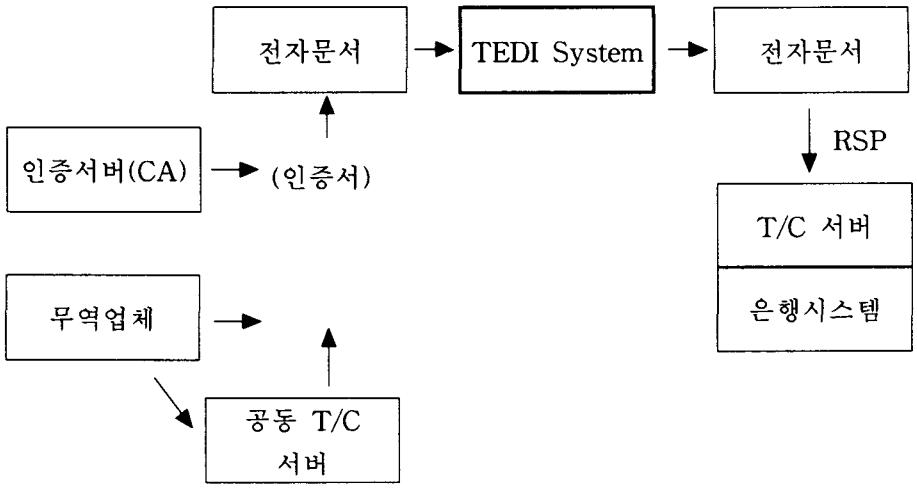
TEDI의 인증서비스절차는 크게 RSP(Repository Service Provider)센터를 경유하는 3자간 프로토콜 서비스와 RSP를 경유하지 않고 송수신자간에 전자문서를 교환하는 2자간 프로토콜 서비스가 있다. 2자간 프로토콜 서비스의 경우 당사자간에 전자문서를 교환하기 때문에 전자문서에 대한 제3자 보증기능의 서비스는 없다. 따라서 3자간 프로토콜 서비스의 인증절차를 보면 <그림 3>과 같다.

개발되었고 이후 다른 응용분야에서 폭 넓게 채택되어 왔다(Michael Brindle·et al, Law of Bank Payment, London Sweet & Maxwell, 1999, pp.221~222 참조).

40) '비대칭형 암호방식'(asymmetric cryptosystems)을 기반으로 하는 RSA(Rivest, Shamir, Adleman)는 1978년 MIT의 Rivest, Shamir, Adleman의 이름을 따서 붙여진 암호화 표준이다. RSA의 계산식은 공개키와 비밀키의 부분을 이루는 두 가지의 소수들(prime numbers)을 곱하여 얻는 부분으로 이루어지는 수 많은 공개모듈(module)을 이용한다(Smedinghoff, op. cit., pp.500~501. 참조.).

41) 데이터의 항목을 식별하거나 이름을 붙여 때로는 데이터의 성질을 나타내기 위해 사용되는 문자 또는 문자의 집합을 의미한다. 구체적으로 일련의 기록, 블록, 데이터 세트를 구별하기 위해 각각 붙여진 코드번호 또는 이름 등의 식별코드 및 파일명을 말한다. 따라서 ID코드는 비밀유지의 목적으로 비밀번호(password)와 함께 사용된다.

<그림 3> TEDI 에서 인증서비스 절차



첫째, 무역업체 및 은행시스템은 각각 인증기관 서버에 등록하여 인증서를 발행받는다.

둘째, 무역업체는 T/C서버를 통하여 전자서명이 첨부된 TEDI 전자문서(선화증권, 송장 등)을 작성하고 인증서를 첨부하여 RSP에 송부한다. RSP는 데이터베이스에 기록하는 것과 더불어 자신의 전자서명을 첨부하여 전자문서를 송부한다.

셋째, 은행은 T/C서버로 전자문서를 수취하여 조회하고 은행시스템에 데이터를 입력시킨다.

Ⅳ. 전자무역에서 제도상 인증시스템의 문제점

1. 인증기관의 신뢰성에 관한 문제

전자무역은 비대면거래를 지향하고 있기 때문에 전통적인 무역에 비해서 관련당사자의 신뢰성 문제가 더욱 부각된다. 특히 거래당사자의 신뢰성을 확보할

수 있도록 인증서비스를 제공하는 인증기관의 신뢰성은 인증제도 활성화의 가장 중요한 기반이다. 따라서 인증기관의 신뢰성이 확보될 때 거래당사자의 전자무역이용정도가 증가할 것이다.

한편, 주요 국제규범 및 국내법에서 규정한 인증기관의 신뢰성 확보를 위한 요건들을 살펴보면 다음과 같다.

첫째, UNCITRAL 전자서명모델법 제10조에서는 "인증서비스 제공자가 사용하는 시스템, 절차 및 인력이 신뢰할 수 있는지 여부와 정도로서 신뢰성을 판단할 수 있다"고 규정하고 있다. 또한 인증기관의 신뢰성 판단에 관한 세부규정으로서는 ①자산의 존재를 포함한 재정능력 및 인력, ②하드웨어 및 소프트웨어 시스템의 성능, ③인증서 처리, 인증서 신청 및 기록보존의 방법, ④인증서에 기재된 서명자 및 신뢰당사자가 될 가능성이 있는 자에 대한 정보의 획득가능성, ⑤독립된 기구에 의한 감사의 규칙성 및 정도 등이 있다. 따라서 UNCITRAL 전자서명모델법의 경우 인증기관의 신뢰성을 판단할 수 있는 요소에 대해서만 규정하고 있을 뿐 세부적 기준에 대해서는 규정하고 있지 않아 모델법(model law)으로서의 특징을 그대로 반영하고 있다.

둘째, EU 전자서명지침의 경우 '인증서비스제공자에 대한 요건'(requirements for certification-service-providers)을 부록(Annex) II에서 따로 규정하고 있다. 요컨대 인증서비스를 제공하는 데 필요한 신뢰성을 증명하기 위해서는 기술능력, 운영능력, 재정능력 등이 수반되어야 한다고 규정하고 있으며 구체적인 내용에 대해서는 언급하고 있지 않다. 이는 동 지침이 지침으로서의 역할을 수행하기 위해서이며 또한 유럽의 역내시장 내에서 각국의 자발적 인정제도의 시행을 유도하기 위해서 각국의 전자서명관련 국내법에 자유롭게 명시하도록 유도하고 있는 것으로 판단된다.

셋째, 미국의 경우 'E-Sign', UETA 등 관련 법률에서는 인증기관의 신뢰성에 관한 규정은 존재하지 않는다. 다만 ABA 가이드라인 제1조 와 제3조에서 인증기관의 신뢰성에 관한 규정을 제시하고 있다. 동 규정들에서 제안하고 있는 인증기관의 신뢰성은 ① 기술적 요건으로서 '신뢰할 만한 시스템'(trustworthy system), ② 재정적 요건으로는 사업을 운영하는데 필요한 충분한 재원의 보유와 배상책임을 충분히 감당할만한 재정적 능력, ③ 인증기관을 운영하는 주체 및 운영요원에 관한 요건으로서 일정한 지식과 기술, 범죄경력 등 반사회적 위험성, ④ 기록보존에 관한 요건으로 인증서의 발행, 정지 및 취소에 관련된 모든 중요한 사

실은 문서화하여 적절한 기간 동안 보존 ⑤ '인증실무준칙'(Certification Practice Statement : CPS)을 제정하여 공시(disclosure)를 의무화 등으로 판단된다.

넷째, 일본의 '전자서명 및 인증업무에 관한 법률'의 경우 인증기관의 신뢰성에 관하여 제5조 및 제6조에서 결격사항 및 공인의 기준으로 규정하고 있지만 구체적이지 않다.[42]

다섯째, 독일의 디지털서명법 역시 제4조 '인증기관의 자격부여'(granting of licenses for Certifiers)에서 인증기관으로서 허가받기 위한 자격요구사항(relevant legal requirements for a certifier)을 규정하고 있지만 역시 구체적이지 않다.[43]

여섯째, 우리나라 전자서명법의 경우 제4조 공인인증기관의 지정에서 규정하고 있으며, 공인인증기관으로 지정 받을 수 있는 자를 국가기관, 지방단체 또는 법인으로 제한하고 있는 것이 특징이다. 또한 공인인증기관의 결격사유에 대해서 규정하고 대통령령이 정하는 기술능력, 재정능력, 시설 및 장비에 대해서 규정[44]함으로써 인증기관의 신뢰성 기준을 대신하고 있다.

요컨대 전자인증과 관련된 주요 국제규범 및 국내법들을 비교하였을 때 인증기관의 신뢰성 확보를 위한 요건들이 상이하고 그 규정에 있어서 구체적이지 않음을 알 수 있었다. 특히 기술능력, 운영능력, 재정능력 등을 기준으로 인증기관을 평가하고 있지만 '일정한 지식', '충분한 재정적 능력' '신뢰할 만한

---

42) 예컨대 금고이상의 실형을 받은 자가 그 집행을 종료하거나 면제받은 날로부터 2년을 경과하지 아니한 자 또는 공인인증기관이 취소되고 그 취소일로부터 2년을 경과하지 않은자는 인증기관으로 지정될 수 없다. 인증과 관련된 설비기준에서는 전자서명 및 인증서 등이 위조되지 않는 적절한 설비가 마련되어 있는지, 적절한 방화벽(firewall)이 구성되어 있는지, 비상시 백업체제가 적절한지를 평가한다.('電子署名及び認證業務に關する法律' 第5條, 第6條 참조.)

43) 인증기관 신청인이 '필요한 신뢰성'(necessary reliability)을 보유한다 함은 자격소지자로서 인증기관의 업무를 수행하는데 필요한 법적 요건을 준수함을 보증할 수 있다는 것을 의미하며, 필요한 전문지식구비라 함은 인증기관에 종사하는 자가 필요한 지식, 경험 및 자격을 갖춘 경우를 말한다.(German Digital Signature Law, Article 4(3), 'granting of licenses for certifiers' 참조)

44) 기술능력요건으로는 정보통신기사, 정보처리기사 및 전자계산기조작응용기사 이상의 국가기술자격을 가진 자 또는 정보통신부장관이 정하여 고시하는 정보보호 또는 정보통신운영 및 관리 분야에서 2년 이상 근무한 경력이 있는 자로 구성된 12인 이상의 운영인력으로 판단한다. 재정능력요건으로는 자본금 80억원 이상으로 하며 국가기관 및 지방자치단체가 공인인증기관으로 지정받는 경우에는 동 규정을 적용하지 않는다. 시설 및 장비요건으로는 가입자의 신원확인 및 관리를 위한 설비, 전자서명키 관리체계를 안전하게 유지하기 위한 설비, 인증서를 안전하고 신뢰성있게 관리하기 위한 설비, 전자서명 및 시점확인을 위한 설비, 인증관리체계를 안전하게 운영하기 위한 보호설비 등이 기준이 된다.(전자서명법시행령, 제3조, '지정기준', 참조)

시스템' 등 그 내용과 구체적인 범위를 규정하고 있지 않다는 문제점이 있다. 이러한 상황은 이국간에 이루어지는 전자무역의 경우 전자인증의 활성화를 저해하는 요인이 될 수 있는 문제이다. 따라서 인증기관의 신뢰성에 관한 보다 구체적이고 객관적인 규정이 필요하다.

2. 국가간 인증법률의 조화 문제

무역거래에 적용되는 대부분의 법률은 종이서류를 기반으로 마련되어 있기 때문에 온라인 상에서 무역거래가 이루어지는 경우 예상치 못한 문제가 나타날 수밖에 없는 현실이다. 즉, 이제까지 종이서류 중심의 상관습에서 비롯된 각종법률 및 제도가 당사자들의 권리를 지켜주고 거래를 안정적으로 유지하는 역할을 수행해 왔으나, 정보통신기술의 발전과 전자무역의 확산으로 무역환경은 급속히 전자화되고, 이러한 전자환경에 부응할 수 있는 법률 및 제도가 절실히 요구되는 상황에 있다.

한편, 전자상거래와 전자무역이 제공할 수 있는 다양한 장점으로 인하여 전자상거래 및 전자무역이 전통적인 상거래와 전통적인 무역을 대체할 것이라는 기대는 확고하다. 또한 이러한 기대가 존재하였기 때문에 전자상거래와 관련된 다양한 법률 및 지침이 제정되고 제안되고 있다. 다만 전자무역과 관련된 법률 및 지침은 아직까지 전자상거래가 국제적으로 확장될 수 있는 법률적 기반이 부재하기 때문에 활성화되고 있지 않다.[45]

비록 현재까지 주요 국제기구 및 국가마다 전자상거래관련 법률 및 지침을 제정하여 사용하고 있지만 지극히 국내상황에 한정되어있다. 다만 대부분의 전자상거래관련 법률 및 지침에서는 국가간에 상호 인정될 수 있다는 규정은 포함시켜 놓고있다. 하지만 국가를 달리하는 이국간에 이루어지는 전자무역에 적용하기에는 한계가 있다. 따라서 법률의 조화가 이루어질 필요성이 있다.[46] 예컨대, 전자인증관련 법률 및 지침을 비교했을 때, 전자인증기관의 지정의 상이함, 전자서명 범위의 상이함, 관련 용어의 상이함 등 그 내용이 일치하지 않는 경우가 많다.

---

45) 이호건 외 2인, "글로벌전자상거래를 위한 인증체계," 「통상정보연구」 제2권, 한국통상정보학회, 2000, p.61.

46) Sanu K. Thomas, op. cit., p.1007.

국가마다 인증관련법률 및 지침이 상이한 이유는 전자인증기술의 발달과 방법의 다양화로 인하여 인증관련법률 및 지침이 이를 따라가지 못하기 때문에 그러하며,[47] 또한 전자인증기술에 대해서 각국의 국내법들이 아주 다양한 접근방식을 취하고 있기 때문이다. 예컨대 각 국내법에서 인정하고 있는 전자인증기술이 다양하고 그 기술이 발달할수록 다양한 문제점에 직면하게된다. 첫째, 한 국가의 특정기술이 모든 국가의 법정지에서 동일하게 인정되지 않을 것이라는 문제점이 있다. 둘째, 전자무역을 통하여 거래를 원하는 무역업자들은 무역 대상국의 전자인증기술에 의해 생성된 전자서명이 필요하며, 그 대상국이 많으면 많을수록 전자서명의 개수는 많아질 수밖에 없다는 문제점이 있다. 셋째, 국가마다 전자인증에 대한 규정의 상이함으로 인하여 거래당사자로 하여금 혼란(confusion)을 야기 시킬 수 있으며 또한 전자인증에 대한 불신(untrustworthiness)을 초래할 수 있는 문제점이 있다.[48]

모든 계약이 그러하듯 전자무역 역시 계약자유의 원칙을 따른다. 따라서 당사자 합의에 의해서 국제규범 및 국내법 중 하나를 준거법으로 선택할 자유도 있다. 그러나 어느 특정국가의 국내법을 준거법으로 한다는 것에 거래 당사자의 합의는 쉽게 이루어지지 않을 것이라는 문제점이 있다.

전자상거래 뿐만 아니라 전자인증과 관련된 다양한 국제규범 및 국내법의 상이함의 결과로 다양한 문제가 발생된다. 따라서 전자인증과 관련된 국제규범 및 각국의 국내법의 조화(harmonization) 내지는 통일화(uniform)가 필요하다.

UNCITRAL 전자서명모델법의 경우 모델법으로서의 역할을 하기 때문에 구속력이 없다. 또한 각 국의 전자서명 및 인증에 관한 법률들이 UNCITRAL 전자서명모델법을 모델로 하여 제정되었기 때문에 동 법의 제정목적에 충분히 부합되었다고 생각한다. 그러나 전자무역에 대한 작금의 상황을 생각해볼 때 새로운 전자서명 및 인증에 관한 통일법을 제정하거나 동 모델법이 구속력을 가지는 국제 협약으로 변화를 시도하여 법의 충돌 또는 혼란을 피하는 것[49]이

47) Michael J. Osty & Michael J. Pulcanio, "The Liability of Certification Authority to Relying Third Parties", The John Marshall Journal of Computer & Information Law, Vol. 17, No. 3, The John Marshall Law School, spring 1999, p.961.

48) Raneta Lawson Mack, "Digital Signatures, The Electronic Economy and The Protection of National Security; Some Distinctions with an Economic Difference", The John Marshall Journal of Computer & Information Law, Vol. 17, No. 3, The John Marshall Law School, spring 1999, p.996.

49) 이창한, "전자거래에 관한 국제기구의 논의 현황과 한국의 법제화 동향", 「인터넷법률」 제10호, 법제처, 2002. pp.181~182.

바람직하다고 판단된다.

전자무역이 활성화되기 위해서는 기술적 인프라확충과 더불어 전자무역의 안전성과 신뢰성을 확보하기 위한 법·제도적 인프라의 정비가 이루어져야 하며, 기존의 전자상거래 관련 법·제도의 기본방향은 전자상거래의 특성상 전자무역을 지향하고 있기 때문에 국제적으로 정합성을 유지하고 국내 규범과 조화를 이루는 방향으로 정비되어지는 것이 무엇보다 중요하다 할 수 있을 것이다.[50]

3. 국가간 전자인증기술의 조화문제

1) 국가간 인증기술의 범위

전자서명은 거래당사자가 인터넷을 이용하여 계약을 체결하는데 진정성과 무결성을 제공한다. 이처럼 전자서명이 전자무역거래에서 중요한 역할을 수행하기 때문에 국가적 그리고 국제적으로 전자서명에 대한 입법화를 시도하였다.[51]

전자서명의 기술적 요소와 관련하여 국제규범 및 각 국의 국내법의 입법적 기반을 살펴볼 경우 전자서명의 유효성을 입증할 수 있는 인증기술의 법률적인 채택은 '규범적 접근방식'(prescriptive approach), '이원적 접근방식'(tow-tiered approach) 또는 '최소적 접근방식'(minimalist approach)중 하나를 선택하고 있다.

첫째, 규범적 접근방식은 전자서명의 범위를 정함에 있어서 다양한 전자서명의 형태를 배제하고 디지털서명만을 유효하게 보는 입장이다. 동 접근방식은 입법과정에서 큰 고민없이 법적 유효성을 부여할 수 있다. 그러나 동 접근방식이 국제적으로 활성화되기 위해서는 두 가지 가정에 부합하여야 한다. 그 가정으로서는 세계가 하나의 정부로 구성되거나 또는 각 국은 디지털 전자서명만을 유일한 전자수명으로 규정하여야 한다. 동 접근방식에 의해서 법률적으로 전자서명의 범위를 정한 국가로는 우리나라, 독일, 이탈리아, 말레지아 등이 있다.[52]

---

50) Randy V. Sabett, "International Harmonization in Electronic Commerce and Electronic Data Interchange; A Proposed First Step Toward Signing on the Digital Dotted Line", American University Law Review, Vol. 46, Washington College of Law at the American University, 1996, p.511, 528.

51) Sanu K. Thomas, op. cit., p.1009 ; Ira H Parker, "Why Digital Signatures Matter", 1 Electronic Banking L. & Com. Rep. 2, 1997, p.24.

52) Internet Law & Policy Forum, "Survey of International Electronic Digital Signature Initiative" , <www.ilpf.org/groups/survey.htm> 참조.

둘째, 이원적 접근방식은 '기술 중립성'(technology neutrality)을 인정은 하되 디지털 서명에 대해서 보다 높은 법적 효력을 제공하는 것이다. EU 전자서명지침은 동 접근방식에 의해 제정된 국제규범이며, EU 내의 전자서명의 법적 인정을 위해서 '조화된 기반'(harmonized framework)을 획득하기 위해 채택된 것으로 판단된다.[53]

셋째, 최소적 접근방식은 어떤 전자서명의 형태도 인정하여 법적 유효성을 확보하게 하는 것이다. 동 접근 방식의 문제점으로는 다양한 전자서명기술의 개발로 상거래 각 분야마다 각기 다른 기술이 이용될 수 있어 전자서명기술의 통일화에 장애가 될 수 있다는 비판도 있다. 동 접근방식에 의해서 법률적으로 전자서명의 범위를 정한 국가는 미국이며 법률로는 'E-Sign'법이 있다.

예컨대 전자서명의 기술적 방식으로 생체인식기술에 대한 국제적 관심도가 증가하고 있다. 생체인식기술을 이용한 전자서명의 방법은 PKI 방식의 디지털 서명 및 일반전자서명에 비해서 우수한 점이 있으며, 이는 동공이나 지문과 같은 신체의 일부는 분실되거나 탈취될 위험이 없다. 또한 당사자 인증(authentication) 및 입증(verification)에서 사기에 대한 위험의 정도가 PKI 방식의 디지털서명보다 작다는 이점이 있다.

그러나 생체인식기술을 이용한 전자서명의 방법은 '원초적 프라이버시'(fundamental privacy)의 문제가 발생될 수 있다. 실무상의 문제점으로는 첫째, 생체인식기술과 관련된 장비가 너무 비싸며, 동 기술이 아직 개발단계에 있어 상용화가 아직 되어 있지 않다는 한계점이 있다. 또한 PKI 방식에서와 동일한 문제로 가로채기(interception) 및 사기의 위험에 노출되어 있으며 국가를 달리하는 당사자 각각이 사용하는 시스템의 호환성 문제가 있다.[54]

따라서 생체인식기술을 기반으로 한 전자서명은 신뢰성 및 편리성에 대한 평가가 아직까지 증명되지 않음으로서 국제적으로 널리 인정되기까지는 많은 장애요소를 극복하여야 할 것이다.[55]

---

53) Jacqueline Klosek, "EU Telecom Ministers Approve Electronic Signatures Directive", Vol. 4, No. 11, Cyberspace Lawer, Feb. 2000, p.12.

54) Klein and Koch, "Biometric Technology", Economist, Sept. 9, p.52.

55) Jennifer L. Koger, "You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures", Transnational Law & contempoary Problems, Vol. 11, University of Iowa College of Law, Fall. 2001, p.504.

2) 국가간 인증기술의 조화

암호화기술 및 인증기술에 대한 국제적인 태도는 기술중립주의를 따르는 것을 원칙으로 하고 있는 상황에 있다. 전자서명 및 인증에 관한 국제규범을 제정하기 위해 초안 또는 지침을 만들 당시에는 공개키암호화 방법을 기반으로 한 디지털 서명기술이 국제적인 표준으로 정착하였다.[56]

예컨대, 상호인증과 관련된 국제표준은 'ISO X.509'이며 대부분의 국가와 산업체들은 이 표준을 기반으로 상호인증기술을 개발하고 있다. 미국의 Xcert사는 1998년 상호인증에 관한 해결방안으로 'Cross Authentication'기술을 개발하였고, Sentry CA라고 하는 상호인증 기능과 대규모의 인증서 처리 및 저장소 관리기능을 개발하여 PKI 제품과의 상호운용성을 보장하고 있다.

그러나 특정기술(technology specific)[57]을 국제규범 또는 각 국의 실정법에 규정한다는 것은 문제가 있으며, 새로운 신기술에 대한 빠른 대응에 방해요소가 될 수 있어 일반적이며 최소요건에 적합한 기술에 대한 법률상의 언급은 하지만 기술에 대해서 특정은 하지 않고 있다.

만약 특정기술을 국제표준으로 사용하게 된다면 동 기술의 소유권을 가진 기업에 독점시장의 지배구조를 제공하는 것이므로 문제가 발생할 수 있다.

기술중립주의를 옹호할 경우 국가마다 새로운 기술을 지속적으로 개발하기 위해서 금전적, 시간적 노력이 필요하다. 또한 새로운 기술이 개발될 때마다 그에 대한 검정 없이 사용되는 우를 범할 수 있을 수 있으며, 국가마다 자국에서 개발한 기술을 사용함으로 인해 국가 간 상호연동을 추구할 때 서로 호환되지 않아 전자무역의 활성화를 저해할 수 있는 문제점이 있다.

따라서 현재의 암호화 및 인증기술 상황에서는 이원적 접근방식이 타당하다고 판단된다. 전자서명 및 인증과 관련된 국제규범 및 국내법들이 수정되기 전에는 PKI기술을 이용한 디지털 서명에 대해서만 법적 효력을 인정하였고 이에 PKI기술에 대한 연구 및 투자가 국제적으로 이루어져 기술의 고도화 및 안전

---

56) UNCITRAL, EU, ICC, OECD 등 대부분의 국제기구에서는 전자서명 및 인증기술에 대해서 기술중립주의를 따라 최초 규범 제정시 유효한 전자서명을 디지털전자서명으로 한정하였다가 현재는 안전한 전자서명 또는 고급전자서명으로 개념을 대체하였다.

57) 특정기술은 개방형 네트워크상에서 당사자의 신원을 확인하는데 '이용가능한 최상의 해결책'(best solution available)으로 제시될 수 있는 기술을 말한다.(Jane Kaufman Winn, "Open Systems, Free Markets and Regulation of Internet commerce", Tulane Law Review, Vol. 72, Tulane University Law School, 1998, p.1181)

성이 검정되어 있는 상황이다. 이러한 상황에서 또 다른 형태의 기술을 개발해서 전자무역에 사용하게 하는 것은 당사자사이에 더 큰 혼란을 야기시킬 가능성이 높다.

요컨대 특정 기술의 이용에 대해서는 법으로 규정하는 것은 피하더라도 국제기관간이라도 의견을 통일화하여 각 국에 권고하는 방법이 합당하리라 판단된다.

Ⅴ. 결론

위에서 살펴본 바와 같이, 전자무역은 전자문서를 기반으로 한다. 그러나 전자문서는 전자매체를 이용함으로써 발생되는 문제점으로 인하여 전자서명의 개념이 필요하게 되었다. 하지만 전자서명 역시 전자적 매체를 이용하기 때문에 네트워크 보안의 문제점인 진정성, 무결성, 부인 등의 문제점이 내포되어 있다. 따라서 이러한 전자문서의 문제점의 보완장치로서 전자인증제도가 활용되고 있다.

-전자결제시스템으로 또는 전자인증시스템으로 국제물품매매에 통용되고 있는 Identrus, Bolero, TEDI 등은 Rulebook, IIP(Identrus Identity Policy), UCP(Utility Certificate Policy), TEDI agreement라는 자체 규정을 가지고 있다. 그러나 이러한 자체 규정들은 각각의 기관들의 영리를 대변하며, 시스템상 표준화가 이루어져 있지 않으므로 상호연동되기가 어렵다는 단점이 있다. 또한 이들 기관이 영리를 목적으로 한다는 점에서 인증업무의 신속한 처리에서는 우위에 있을지라도 신뢰성면에서는 국가에서 인정한 공인인증기관에 비해 낮다. 따라서 전자무역 거래당사자들이 무역거래를 효과적·효율적으로 수행하기 위해서는 인증기관의 신뢰성, 이용료의 적정성, 상호연동의 가능성 등을 제시할 수 있는 국제적인 가이드라인이 필요하다.

특히, 국내 전자상거래가 아닌 전자무역에서 전자인증제도가 도입되고 활성화되기 위해서는 통일화된 법적 기준아래 인증기관이 지정·운영되어야 한다. 그러나 전자인증과 관련된 주요 국제규범과 국내법률들을 살펴본바 그 규정의 상이함이 있음을 알 수 있었다. 따라서 전자인증과 관련된 국제적 통일법의 부재가 전자무역의 활성화를 저해하는 요인이 될 수 있다.

UNCITRAL 전자서명모델법과 EU 전자서명 지침은 통일법 또는 협약으로서의 구속력을 가지는 것이 아니기 때문에 국제간 거래를 위해 기준이 될 수 있는 법률적 보완장치가 필요하다.

상기 이유로 인하여 인증과 관련된 국제통일규범이 시급히 제정되어야 하며 전자인증제도의 법적 안정성 보장을 통하여 그 지위를 확보하여야 한다. 아울러 급속하게 변화되고 있는 무역의 전자화 추이를 고려하여 필수불가결한 최소한의 규정만이라도 준비되어야 할 것이다.

參考文獻

김은기, "전자문서의 법적 효력," 「기업법연구」 제5집, 한국기업법학회, 2000.

노태악, "전자거래에 있어 계약의 성립을 둘러싼 몇가지 문제", 「法曹」 통권 제517호, 법체처, 1999, 10.

송선옥, "전자무역 대금결제시스템에 관한 비교연구", 「통상정보연구」 제3권 1호, 한국통상정보학회, 2001.

안병수, "전자식 선하증권의 실용화에 따른 문제점에 관한 연구", 성균관대학교 대학원 박사학위청구논문, 1998.

양정호, "전자식 선하증권과 전통적 선하증권의 비교 연구", 성균관대학교 대학원 박사학위청구논문, 2003.

오병철. 전자거래법, 법원사, 2000.

이창한, "전자거래에 관한 국제기구의 논의 현황과 한국의 법제화 동향", 「인터넷법률」 제10호, 법제처, 2002.

이호건 외 2인, "글로벌전자상거래를 위한 인증체계," 「통상정보연구」 제2권, 한국통상정보학회, 2000.

이호용 외 6명, "전자문서 이용활성화의 법적 장애요인 분석," 연구보고서, 한국전산원, 1998.

최석범, "사이버무역시대에서의 글로벌기업간 전자상거래의 모델도입현황과 문제점에 관한 연구," 「무역학회지」 제28권 2호, 한국무역학회, 2003.

한삼인 · 김상명, "전자서명 및 전자인증의 법률문제에 관한 고찰," 「비교사법」 제8권 제1호(하), 한국비교사법학회, 2000.

Alicia Aldridge, Michele White and Karen Forcht, "Security considerations of doing business via the Internet; cautions to be considered", Internet Research Electronic Networking Applications and Policy, Vol. 7 No. 1, MCB University Press, 1997.

Benjamin Wright, The Law of Electronic Commerce, Aspen Law & Business, 1996.

Internet Law & Policy Forum, "Survey of International Electronic Digital Signature Initiative" , <www.ilpf.org/groups/survey.htm>.

Ira H Parker, "Why Digital Signatures Matter", 1 Electronic Banking L. & Com. Rep. 2, 1997.

Jacqueline Klosek, "EU Telecom Ministers Approve Electronic Signatures Directive", Vol. 4, No. 11, Cyberspace Lawer, Feb. 2000.

Jane Kaufman Winn, "Open Systems, Free Markets and Regulation of Internet commerce", Tulane Law Review, Vol. 72, Tulane University Law School, 1998.

Jennifer L. Koger, "You Sign, E-SIGN, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures", Transnational Law & contempoary Problems, Vol. 11, University of Iowa College of Law, Fall. 2001.

Klein and Koch, "Biometric Technology", Economist, Sept. 9.

Michael Brindle · et al, Law of Bank Payment, London Sweet & Maxwell, 1999.

Michael J. Osty & Michael J. Pulcanio, "The Liability of Certification Authority to Relying Third Parties", The John Marshall Journal of Computer & Information Law, Vol. 17, No. 3, The John Marshall Law School, spring 1999.

Randy V. Sabett, "International Harmonization in Electronic Commerce and Electronic Data Interchange; A Proposed First Step Toward Signing on the Digital Dotted Line", American University Law Review, Vol. 46, Washington College of Law at the American University, 1996.

Raneta Lawson Mack, "Digital Signatures, The Electronic Economy and The Protection of National Security; Some Distinctions with an Economic Difference", The John Marshall Journal of Computer & Information Law, Vol. 17, No. 3, The John Marshall Law School, spring 1999.

Sanu K. Thomas, "The Protection and Promotion of E-Commerce; Should there be a Global Regulatory Scheme for Digital Signatures?", Fordham International Law Journal, Vol. 22, Fordham University School of Law, March 1999.

Stephen Wilson, "Digital signatures and th future of documentation", Information Management and Computer Security, Vol. 7, No. 2, MCB University Press, 2000.

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 2000.

ABSTRACT

A Study on Problems of Certification System in International Electronic Commerce

Oh, Hyon Sok

Electronic transaction using electronic documents be carried without direct person to person meeting, there is the possibility to use other's identity illegally without notice and to verity authenticity of transaction.

It is very hard to find out that the electronic documents on the process of submitting is forged documents or not and also has much difficulty in maintaining transmitting secret. Therefore, to solve such problems on electronic transactions, certification system with cryptography skill are inevitably necessary. Also there is needed legal base in the electronic document as functional equivalent of the paper document.

Recently there are so many commercial certification service provider(CPS) such as Identrus, Bolero, TEDI but their establishment of CPS, certification process, guideline and so on are different each CPS. Therefore, this kind of situation can make user confuse.

To introduce and develop the electronic certification in the international electronic commerce not domestic electronic commerce, it need to authorize and operate certification authority under the uniform regulation base. But, because the laws and guidelines that related to electronic certification system are different among the nations and international organizations, it need to compare laws and guidelines.

In conclusion, the most important thing to resolve problems surrounded certification and develope certification system in the international electronic commerce make uniform rule of international electronic certification to recognize internationally from each nation or at least, need to harmony laws and guideline in each nations.

Key Words : Certification, Electronic Document, Identrus, Bolero, TEDI