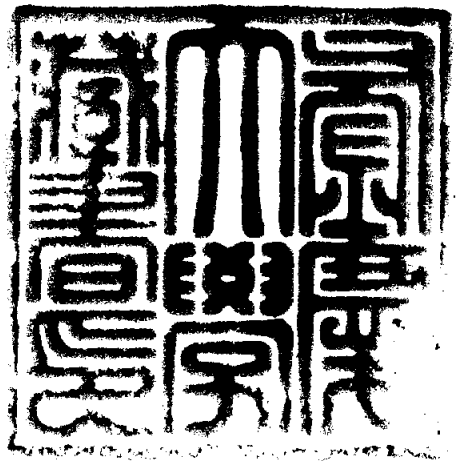
경영학석사 학위논문

전자무역결제에 있어서 전자인증제도에 관한 연구



2003년 2월

부 경 대 학 교 대 학 원

국제통상물류학과

윤 지 원

경영학석사 학위논문

전자무역결제에 있어서 전자인증제도에 관한 연구

지도교수 윤 광 운

이 논문을 경영학석사 학위논문으로 제출함

2003년 2월

부 경 대 학 교 대 학 원

국제통상물류학과

윤 지 원

윤지원의 경영학석사 학위논문을 인준함

2002년 12월

주 심 경제학박사 최 홍 석 

위 원 경영학박사 하 명 신 

위 원 경영학박사 윤 광 운 

목 차

<제목차례>

<표차례>

<그림차례>

A Study on the Electronic Certification System in the Electronic Trade Payments

Ji-Won Yun

Department of International Commerce and Logistics,

Graduate School, Pukyong National University

Abstract

This study reveals the ways of using the Electronic Certification System to support the Electronic Trade Payments.

The advances in the information technology and the use of the Internet have been changing the original style of trade into the electronic trade. However, a lot of trade companies have been faced up to some sorts of difficulties as marketing and advertisement have been going through the On-line system before signing on a contract while payments and delivery have been done on the Off-line system after the contract. Therefore, there is no doubt that the phase of payments should be carried out by the On-line system for the development of the electronic trade.

Aside from the distribution, the security problems, bringing the obstacles

of reliability, can happen. Hence, the report is not only dealing with the major international organizations and regulations related to the Electronic Trade Payments but also presenting alternatives. The Electronic Certification and the Digital Signature System are said to be the ways of settling the security and reliability problems with electronic payments system. Still, some obstacles are needed to be worked out ; there are certain differences in the regulations, the policy of the Cross Certification toward other countries' certification bodies and the implementation of the Electronic Trade Payments system among the countries.

In order to clear up these matters, some efforts are required. Firstly, reviewing the international certification organizations is essential under the institution. Secondly, the international certification bodies for the electronic payments should be founded. Finally, the Electronic Certification System should be arranged to develop the Electronic Trade Payments through reviewing international general laws.

Ⅰ. 서 론

1. 연구의 필요성과 목적

정보통신기술의 비약적인 발전과 함께 인터넷이 상용화되면서 국제무역에 있어서의 전자화는 급속한 성장세를 나타내고 있다. 이러한 전자무역[1]의 경우, 기존의 국제무역거래와 비교해 볼 때 거래절차상에서는 별다른 차이가 없지만 거래수단이나 방법에는 큰 차이가 있다.

먼저 거래처를 발굴하거나 광고 마케팅하는 방법과 상담 및 계약체결을 위한 의사교환방식도 기존과는 달리 무역거래알선사이트와 E-Mail 등을 활용하여 저렴한 비용으로 이루어지게 된다. 또한 대금결제도 전자화폐 등 전혀 다른 수단이 이용되며, 상품의 운송이나 물류도 항공운송이나 국제특송 등이 활발하게 이용된다.

하지만 무역업체들이 인터넷 등 On-Line 상에서 거래선을 발굴하고 계약을 체결한다고 하더라도 Off-Line으로 물품을 운송하고 대금결제가 이루어짐으로써 많은 불편을 느끼고 있다. 이에 능률적이고 효율적인 전자무역의 활성화를 위해서 수반되어야 하는 중요한 요소 중의 하나가 네트워크를 통한 전자무역결제와 관련된 시스템이다.

그러나 이러한 전자무역결제시스템은 네트워크에 대한 신뢰성 문제가 가장 큰 걸림돌로 작용하고 있다. GVU[2]와 Commercenet[3] 등의 조사에 의하면 전

---

1) 무역의 전부 또는 일부가 컴퓨터 등 정보처리능력을 가진 장치와 정보통신망을 이용하여 이루어지는 거래를 말한다. 대외무역법 제 2 조 제 6 항.

2) GVU(Graphics, Visualization, & Usability), "GVU's 9th WWW User Survey", http://www.cc. gatech.edu/gvu/user_surveys/ surveys-1998-04, 1998.

3) CommerceNet, "Barriers & Inhibitors to the Widespread Adoption of Internet Commerce", Research Report, http://www.commerce.net/research/free-report/, 1999.

자무역결제의 가장 큰 장애요인은 전자무역결제시스템에 대한 신뢰성 결여에서 야기되는 보안과 암호화 문제라고 지적하고 있다.

과거의 통신상 보안을 유지하는 방법은 암호방법이 주로 사용되어 왔으나 전자무역결제의 독특성 즉, 사기, 위조·변조, 거래사실의 부인 등과 같은 문제점은 기존의 암호방식으로는 해결될 수 없다는 한계점이 있다. 이러한 보안문제를 해결하기 위하여 공개키 기반구조의 전자서명과 전자인증을 통한 해결방안이 대안으로 제시되고 있다.

개방형 통신망인 인터넷 기반의 전자무역이 법적 효력을 가진 안전한 상거래가 되기 위해서 거래 양 당사자의 신원확인과 의사표시의 진위여부 등을 확인하기 위한 메카니즘을 수행할 수 있는 인증기관(CA : Certification Authority)이 필요하다. 이와 관련하여 UNCITRAL, OECD, ICC 및 WTO 등 관련 기구에서는 인증기관 관련 주요 지침을 제시하고 있으며, 미국을 비롯한 각 국에서는 이들 지침을 참고한 법제를 추진 중이다.

전자무역의 경우 인증의 문제가 국내 인증의 체계보다 훨씬 복잡한 형태를 나타낸다. 왜냐하면, 국내 인증의 경우에는 각 국가의 법제에 의하여 구체적인 형태를 구축하고 이들에 근거한 인증기관의 설립과 운용에 의해 인증의 기능을 원활히 수행할 수 있으나, 전자무역의 경우 인증기관에서 발행한 인증서의 법적 지위 등에 대하여 각 국가들의 태도가 상이하기 때문에 구체적인 해결방안이 난해한 실정이다.

이러한 문제는 상호인증을 통해 해결할 수는 있으나, 각 전자무역결제시스템 간의 인증의 신뢰성 문제, 각 국가의 인증관련 법규는 국내의 거래를 기준으로 하고 있고, 각 국가에서 실제 시행에 따른 문제점이 검증되지 않은 단계이기 때문에 인증기관의 운영이 본격화 될 경우 많은 문제점들이 파생될 수 있다.

따라서 본 연구에서는 인증기관의 필요성과 기능을 바탕으로 이와 관련한

국제적 논의 동행 및 관련 국가의 법률적·제도적 형태와 내용을 비교하고, 전자무역결제 수단별 전자인증제도 운용현황을 살펴보고 전자무역의 활성화를 위한 전자무역결제의 전자인증제도의 과제를 도출 한 후 인증기관의 위상과 신뢰성 측면에서 그 대응방안을 제시하고자 한다.

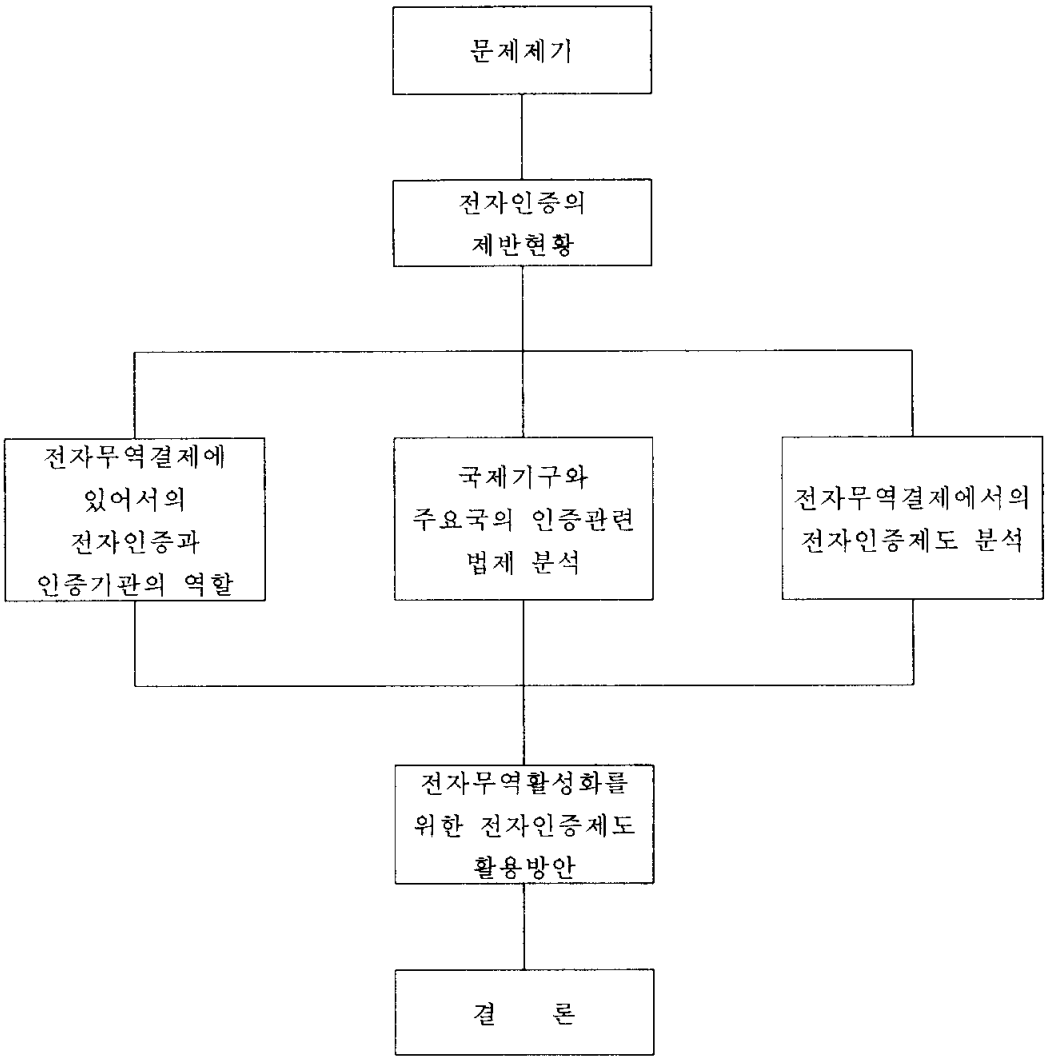
2. 연구의 범위와 방법

현재 우리나라를 비롯한 전 세계의 주요 국가들에 있어서 인증 관련 분야는 신설 분야인 동시에, 전자무역결제에서 필수적인 분야라 할 수 있다. 따라서 전 세계 각국에서는 전자무역결제시스템과 인증 관련 기술개발 노력이 치열하며, 인증 관련 법체계를 어떠한 형태로 구축할 것인가와 관련하여 주요 기구에서의 논의 또한 매우 활발하다.

따라서 본 연구는 각종 문헌과 관련 법제의 분석을 통하여 국제기구별 전자인증관련 법제현황과 주요국의 인증관련 법체계의 연구와 전자무역결제시스템의 유형별 인증체계를 비교·분석한다.

본 연구의 구성은 다음의 <그림 1-1>과 같다.

<그림 1-1> 논문의 구성도


문제제기
전자인증의 제반현황
전자무역결제에 있어서의 전자인증과 인증기관의 역할
국제기구와 주요국의 인증관련 법제 분석
전자무역결제에서의 전자인증제도 분석
전자무역활성화를 위한 전자인증제도 활용방안
결 론

Ⅱ. 전자무역결제와 전자인증에 관한 일반적 고찰

1. 전자무역결제의 개념

1) 전자무역결제의 의의

전자결제란 물품이나 서비스의 대가를 전자적 수단을 통하여 지급(payment) 및 결제(settlement)하는 것이다. 지급은 결제주체간 채권 및 채무관계에서 이루어지는 행위를 의미하고, 결제는 지급인과 수취인간의 자금이체와 같은 대금지급의 과정(process of making payment)을 의미한다.[4]

그러나 최근에는 지급수단 및 결제가 전자화됨으로 인해 지급과 결제를 엄격히 구분하기 어렵기 때문에 이를 포괄하여 결제시스템이라는 용어를 사용하고 있다. 그러한 의미에서 전자결제시스템(Electronic Payment Systems)은 전자결제수단, 운영네트워크, 그리고 이와 관련된 모든 제도적 장치를 총칭하는 개념으로 정의할 수 있으며, 그 결제과정상 지급수단(Payment Instruments), 참가기관(participants), 은행간 결제시스템(inter-bank settlement systems)이 관련되어 있다.

전자무역결제를 위해 개발된 최초의 시스템은 1977년 5월부터 가동되기 시작한 국제은행간 금융결제방식인 SWIFT(Society for Worldwide Interbank Financial Telecommunication)가 있으며, 인터넷 상에서 구현되고 있는 전자결제시스템으로서 신용카드 거래를 처리하는 신용카드 지급시스템, 인터넷에서 통용되는 화폐를 만들고 상거래에 이용하는 전자화폐시스템, 수표를 인터넷 상에서 구현한 전자수표 시스템 및 전자적 수단을 이용하여 계약이 체결되었

4) Ronald A. Anderson and Walter A. Kumpf, *Business Law*, 6th ed., South-Western Publishing Co., 1961.

을 경우에 일반 소비자에 의해서 전자적으로 직접 대금지불을 완료하거나 대금지불을 의뢰할 수 있는 전자자금이체 등이 있다.[5] 그러나 전자화폐나 신용카드를 이용한 전자결제 방식은 B to C(Business to Customers) 등 소액거래에 적합한 결제시스템으로 전자무역거래에 이용하기에는 한계가 있다. 따라서 전자무역에 적용할 수 있는 전자무역결제시스템 문제를 해결하기 위하여 전자무역의 결제를 원활히 처리하기 위해 선하증권을 포함한 무역서류 전반의 전자화를 추구함으로써 무역서류 전체의 전자화를 추진하는 Bolero와 컴퓨터의 도입으로 필요 없게 되거나 중복되는 절차를 생략하고 신용장을 개설할 필요 없이 전자통신을 통해 수출입서류 전송에서 대금결제에 이르기까지 일련의 과정을 신속하게 처리할 수 있는 TradeCard System, 그리고 무역대금결제는 물론 무역거래알선, 무역정보제공, 무역서류전송까지 원스탑 서비스를 제공하는 형태의 BeXcom 등이 추진되고 있다.

2) 전자무역결제시스템의 특징과 시행요건

(1) 전자무역결제시스템의 특징

전자무역결제를 위해 사용되고있거나 개발되고 있는 전자결제시스템들은 기존의 시스템에 비하여 다음과 같은 특성을 지닌다.

첫째, 대금지불의 편리성을 지닌다.

기존의 결제시스템이 전화나 직접지불방식을 이용하고 있는 반면, 전자결제시스템은 네트워크상에서 직접 지불하거나 신용카드를 이용해서 손쉽게 처리할 수 있다.

---

5) 윤광운, "전자상거래의 이용에 따른 전자대금결제시스템의 구축과 운용에 관한 연구", 국제상학 제 14권 제 1호, 한국국제상학회, 1999. 5.

둘째, 개인정보의 안전성을 가진다.

기존 상거래의 대금결제방식은 고객들이 상품구매에 대한 대금결제를 전화나 통신망을 이용해서 상대방에게 제공함으로써 개인의 프라이버시에 관한 정보가 유출되는 경우가 많다. 그러나 전자무역결제시스템은 국제적인 보안표준인 SET(Secure Electronic Transaction)를 적용하고 있다. SET는 인터넷과 같은 보안프로토콜로서, 일상생화에서 이용하는 신용카드거래 체계를 인터넷 상거래에서도 안전하게 이용할 수 있도록 하고 있다. 이를 위해 디지털 신원증명, 공용키 암호화, 디지털 서명과 같은 소프트웨어적 안전장치를 채택하고 있다.

셋째, 적용범위의 제한성이 있다.

인터넷 상거래에서 발생하는 보편적인 대금결제방식은 신용카드를 이용한 방식으로, 이것은 카드 소지자만이 이용할 수 있으므로 구매욕구는 강하나 적절한 신용등급을 얻지 못해 신용카드를 사용할 수 없는 계층, 예를 들면 청소년이나 실업자에 대해서는 사용을 제한하고 있다.

(2) 전자무역결제시스템의 필요조건

Off-line 상거래에서 이루어지는 대금결제는 안전성을 바탕으로 하여 은행의 지로방식이나 또는 신용카드 방식으로 이루어지고 있으며, 기업과 기업의 거래에서는 당좌계좌를 통한 지불방식이 이루어지고 있다. 또한 국제간 무역거래는 주로 외국환 거래방식으로 이루어지고 있다. 외국환에 의한 무역대금의 결제과정은 추심(Collection)과 매입(Negotiation)방법으로 대금을 결제하고 있다. 따라서 전자무역이 활성화되기 위해서는 Off-line 상거래에서 이루어지고 있는 결제방식으로는 진정한 전자거래가 성립될 수 없다.[6]

---

6) 박종돈 · 감창남 · 이제홍, "Cyber 무역의 전자결제에 관한 논의동향", 통상정보연구

전자결제시스템이 무역거래를 효율적으로 보조하기 위해서는 다음과 같은 조건들을 갖추고 있어야 한다.[7]

첫째, 정확성을 갖추고 있어야 한다. 무역에서는 신용장과 서류상호간의 일치성이 중시되는데 이러한 무역거래에서의 요구조건을 반영하고 있어야 한다.

둘째, 신속한 결제가 이루어져야 한다. 이는 결제에 필요한 서류의 전달과 검토가 신속히 이루어져야 하는 것을 전제로 하고 있다.

셋째, 소액결제를 지원할 수 있어야 하고, 처리 비용 면에서 저렴해야지만 많은 이용자를 확보할 수 있을 것이다.

넷째, 무엇보다 중요한 것으로서 안전성이 보장되어야 하는데 이러한 안전성은 시스템에 대한 보안과 관계법의 축조로 이루어질 수 있다.

이외에도 기존 결제시스템 및 거래관행과 조화를 이룰 수 있는 호환성, 사용자의 편의성, 범용성을 갖추고 있어야 한다.

<표 2-1> 전자무역결제시스템의 요건

요 건	내 용
정확성	서류작성 및 서류검토시 L/C 및 서류상호간의 일치여부
신속성	서류의 전달 및 취급상의 지연, 초고속선의 등장에 따른 B/L's Crisis 해결
경제성	종이서류 방식을 대체하기 위한 시스템 구축비용, 멤버쉽, 거래처리비용 등
안전성	시스템 보안, 법률적 보장
신뢰성	관계당사자의 신인도
호환성	기존 결제시스템 및 거래관행과의 조화
사용자 편의성	Ease of Use
범용성	이용가능 대상국, 대상품목, 거래규모 등

자료 : 송선옥, "전자무역 대금결제시스템에 관한 비교연구", 통상정보연구 제 3 권 제 1 호, 한국통상정보학회 2001. 6.

제 2권 제 1호, 한국통상정보학회, 2000. 6.

7) 문희철, " 전자무역결제시스템 관련 동향과 전망", 국제경영리뷰 제 4 권 제 2 호, 한국국제경영관리학회, 2000. 11.

(3) 전자무역결제시스템의 법적 기반

① 무역매매법규 관련규정에서의 전자무역 결제시스템의 법적 기반

가. UNCITRAL의 전자상거래에 관한 모델법(1996)

UNCITRAL(UN Commission on International Trade Law : 유엔국제거래법위원회)이 작성한 전자상거래에 관한 모델법(UNICITRAL Model Law on Electronic Commerce)은 전자상거래의 한 유형인 EDI, E-Mail 등에 의해 작성된 전자문서(data message)의 법적 효력에 대하여 규정하고 있다.

이 법은 EDI 메시지의 활용에 대한 법률적 인정에 필요한 근거조항을 마련하고 있으며, 아울러 서면을 요구하는 경우 그러한 요구를 충족한다는 조항도 마련하고 있다. 또한 서명이 요구되는 경우 전자서명을 통해 이를 충족할 수 있는 요건과 효력을 규정하고 있으며, 원본을 요구하는 경우에 대한 대비와 전자문서가 증거능력과 가치 면에서 부인되지 않도록 하는 배려도 포함하고 있다.

나. UNCITRAL의 전자서명에 관한 통일규칙 초안

UNCITRAL의 전자서명에 관한 통일규칙 초안은 전자서명기술에 대하여 중립적인 입장을 취하면서 국제적인 인증기관의 역할을 인정하는 등 전자서명의 국제적 활용에 대한 착실한 대비를 마련하고 있는 것으로 보이며, 이를 통해 전자상거래의 진정성 확보 등에 긍정적인 기여를 할 것이다.

다. 정형거래조건의 해석에 관한 국제규칙(2000)

정형거래조건의 해석에 관한 국제규칙(2000)에서는 이미 1990년 개정에서

EDI 방식에 의한 무역관습을 반영하였고, 2000년 개정에서도 이를 수용하기 위한 것임을 거듭 확인하면서, 정형거래조건을 사용하는 당사자간의 권리와 의무를 더욱 구체적으로 규정하고 있다.

따라서 정형거래조건의 해석에 관한 국제규칙(2000)에서는 EDI 방식에 의한 무역거래가 확산되면서, 이를 수용하기 위하여 매매 당사자의 합의에 의한 새로운 EDI 방식 통신문도 종래의 종이서류에 상응하는 약정품의 인도 증거 혹은 운송서류로 제공할 수 있음을 EXW를 제외한 모든 거래조건에 규정하고 있다.

라. 국제물품매매계약에 관한 UN협약(1980)

국제물품매매계약에 관한 UN협약(UN Convention on Contracts for the International Sale of Goods ; 일명 비엔나 협약 또는 CISG라고 함)의 조문은 EDI가 활성화되기 이전인 1980년에 제정되었음에도 몇몇 조항들에서 EDI방식 등 전자적 매체에 의한 거래방식을 수용할 수 있도록 하였다.

즉 계약의 충족요건으로 「서명된 서면」을 요구하는 법률적 제약에 대하여 비엔나 협약에서는 '매매계약이 서면에 의해 체결 또는 입증될 필요가 없다'고 규정하여 전자식 매체를 포함한 어떠한 방법에 대해서도 계약체결이 가능하게 하고 있다. 또 서면의 정의에 전보와 텔렉스를 포함시키고 있어 EDI 메시지도 그 범주에 포함되는 것으로 해석할 수 있다.

이러한 내용에 비추어 볼 때 비엔나 협약이 적용되는 무역매매에서도 매도인이 전자식 서류를 활용하여 자신의 의무를 이행하는 것에 별다른 문제가 발생하지 않을 것이다.

마. 전송에 의한 무역자료의 교환행위에 관한 통일규칙(1987)

1987년 UNCID(Uniform Rules of Conduct for Interchange of Trade Data

by Teletransmission)를 주도적으로 만든 국제상업회의소는 1995년 제41차 회의에서 'EDI의 국제 상업적 사용을 위한 모델 교환약정'(Model Interchange Agreement for the International Commercial Use of Electronic Data Interchange, 이하 모델 교환약정이라 함)을 채택하여 이를 UN/EDIFACT의 일부인 UN/TDID에 포함시켜 국제표준으로서 반영되도록 하였다.

요컨대 EDI를 활용한 무역매매가 원활히 이루어지기 위해 거래 당사자의 법적·기술적 문제점을 해결하기 위하여 필요한 교환약정은 UN/ECE가 주도한 UNCID와 모델 교환약정으로 표준화되었으며 이는 유엔 무역데이터 교환지침서(UNTDID)에 포함되어 메시지 표준인 UN/EDIFACT에 통합되었고 궁극적으로는 전자식 메시지의 당사자간 권리와 의무를 규율하는 근거가 되었다.

② 무역결제 관련규칙에서의 전자무역 결제시스템의 법적 기반

가. 화환신용장 통일 규칙 및 관례(1993)

신용장 통일규칙에는 전통적인 종이 서류방식의 무역관행을 존중하면서도 전자적 방식에 의한 무역거래를 수용하기 위한 조항들을 규정함으로써 새로운 무역관행을 인정하고 있는 것으로 보인다. UCP 500의 제1조, 제20조 b항, 제37조 등이 대표적인 조항들이다.

나. 국제 스탠드바이 관습(1998)

국제 스탠드바이 관습은 화환신용장이 서류를 중심으로 하는 것과 달리 유통성 서류의 제시가 요구되지 않는 것이 일반적이므로 전자 메시지 형태의 서류제시가 많을 것이라는 추측과 SWIFT가 제정과정에 참여한 것에 따른 전자적 수단 사용에 관한 규정이 포함되어 있다는 것이 특징이다. 따라서 이러한

국제 스탠드바이 관습이 물품매매에 적용된다면 전자식 선적서류의 제시가 정당한 것으로 인정받을 수 있다.

③ 국제운송법규 관련규정에서의 전자무역 결제시스템의 법적 기반

가. 해상화물운송에 대한 UN협약(1978)

해상화물운송에 관한 UN협약(UN Convention on the Carriage of Goods by Sea, 1978) 제1조에서는 전보와 텔렉스만을 서면으로 인정한다고 규정하고 있으며, 제14조에서는 선하증권이 발행되는 국가의 법률에 저촉되지 않는 한, 선하증권상의 서명이 전자적인 수단에 의해서도 가능함을 규정하고 있어 전자식 선하증권의 수용에 별 영향이 없다.

나. 국제화물복합운송에 관한 UN협약(1980)

국제화물복합운송에 관한 UN협약(UN Convention on International Multimodal Transport of Goods, 1980)은 제정과정에서 먼저 제정된 「해상화물운송에 관한 UN협약」에 상당부분 의존하였기 때문에 그 내용도 거의 흡사하다.

다만, 국제화물복합운송에 관한 UN협약은 아직 발효되지 못하고 있어, 이 협약이 적용되는 것은 사실상 어렵지만, 오늘날의 국제복합운송인과 송화인의 책임한계에 대한 중요한 해석기준으로 원용되고 있어 그 나름대로의 존재의미가 있다.

다. 전자식 선하증권에 관한 CMI규칙(1990)

1990년 6월 국제해사위원회에서 제정한 전자식 선하증권에 관한 CMI규칙(CMI Rules for electronic Bills of Lading)은 관계당사자가 이 규칙에 따라

합의한 경우에만 적용되는 임의적 규칙이다. 이 규칙은 자료전송에 따른 당사자의 행위 규범으로 ICC가 제정한 UNCID를 따르며, 전송자료는 국제표준으로 확립된 UN/EDIFACT로 작성하는 것을 원칙으로 한다. 한편 전자식 선하증권은 종이 선하증권이 포함하고 있는 것과 동일한 내용을 포함하고, 기존에 선하증권의 점유로 가능했던 물품의 청구권 및 처분권의 이전을 유효한 개인키를 가짐으로써 대신할 수 있도록 하였다.

결국 CMI가 제정한 전자식 선하증권에 대한 규칙은 전자식 선하증권의 실용을 전제로 하여 관련된 법률적 문제 및 기술적 방안을 규정한 것으로, 이전까지 문제가 되었던 권리증권적 기능의 전자화에 대하여 명확한 입장을 취하고 있으며, 전자문서 중 가장 구현이 어려운 전자식 선하증권의 실용에 있어, 이후 제정된 많은 국제규칙과 국내입법을 선도할 중요한 국제규칙으로 평가된다.

<표 2-2> 전자무역결제시스템의 법적기반

	관련 규정	주요내용
무역매매법규관련규정	UNICITRAL의 전자상거래에 관련 모델법	전자문서의 문서성 인정
	UNCITRAL의 전자서명에 관한 통일 규칙	전자서명기술에 대한 중입적 입장을 취하면서 인증기관의 역할을 인정
	정형거래조건의 해석에 관한 국제규칙	EDI 방식 통신문의 효력 부여
	국제물품매매계약에 관한 UN협약	EDI 방식 등 전자적 매체에 의한 거래방식 수용
	전송에 의한 무역자료의 교환 행위에 관한 통일 규칙	전자적 메시지의 당사자간 권리와 의무 규율

무역결제 관련 규칙	화환신용장 통일 규칙 및 관례	전자적 방식에 의한 무역거래 수용
	국제 스탠드바이 관습	전자적 선적서류 제시의 정당성 인정
국제운송법규 관련 규정	해상화물운송에 대한 UN 협약	선하증권상의 서명이 전자적 수단에 의해서도 가능함을 규정
	국제화물복합운송에 관한 UN 협약	국제복합운송증권의 서명이 전자적 수단에 의해서도 가능함을 규정
	전자식 선하증권에 관한 CMI 규칙	전자식 선하증권의 종이 선하증권과의 동일한 효력 부여

2. 전자무역결제의 유형

1) Bolero

Bolero란 "Bill of Lading Electronic Registry Organization"의 약칭[8]으로 선하증권 전자등록기구를 의미한다. 1994년 6월 홍콩, 네덜란드, 스웨덴, 영국 및 미국의 해상운송회사, 은행, 통신회사 등이 참여하여 컨소시엄 형태로 시작된 Bolero는 무역거래에 필요한 종이서류를 전자메시지로 전환하여 안전하게 교환할 수 있는 기반을 제공하는 것을 목표로 하고 있다.

무역거래 과정에서 단순히 전자식 선하증권만의 권리증권적 기능의 전자적 유통이 가능한가라는 논쟁이 무역서류 전체의 통합적인 전자화 추진에 장애요인으로 작용해 왔는데, 이에 Bolero에서는 선하증권 단독의 전자화 시도가 아닌 선하증권을 포함한 무역서류 전반의 전자화를 추구함으로써 무역서류 전체의 전자화가 상업적인 대상으로 추진되었다.

이 프로젝트는 EU가 스폰서가 되어 유통증권의 처리와 무역거래의 전자적

8) UNCTAD, Electronic Commerce Development. 2000.

관리(MANDATE)의 연구성과에 근거하여 전자선하증권을 해운실무환경에 도입하기 위해 SWIFT와 TT Club[9]의 합작투자로 운영되고 있다. 1998년 4월에 창립된 Bolero International사는 Bolero협회[10]와 함께 2년 이상의 기간동안 Bolero 서비스의 기능적·법적 가능성을 검토하는 작업을 수행하여 왔다. Bolero Project는 Deloitte & Touche Europe Services를 중심으로 결성된 컨소시엄 멤버에 의해 추진되었다. 파일럿 테스트는 영국, 스웨덴, 네덜란드, 미국 및 홍콩의 수출입업자, 운송업자, 1994년 3월 종료된 은행의 26개 조직에 의해 제1단계와 1995년 9월에 종료된 제2단계로 나누어 그 유효성을 검증하였다. 또한 1999년 1월 전 세계 18개 무역권에 대한 법률분석을 완료하고 1999년 1월에서 6월 까지의 시범서비스 기간을 거쳐 상용서비스를 출범시켰다. 국내에서는 2000년 6월 한빛은행을 시작으로 외환은행과 삼성전자가 가입한 상황이며, KTNET와의 제휴를 통해 본격적인 국내진출을 추진하고 있다.[11]

2) TradeCard System

1996년 1월 세계무역센터협회(World Trade Center Association : WTCA)가 주관이 되어 FSTS(Full Service Trade System) 프로젝트를 추진하여 1998년 미특허청(USPTA)으로부터 결제시스템에 관한 특허를 획득하였다. 1999년 2월 E.M. Warburg Pincus사의 지분참여로 TradeCard사라는 독립회사를 설립하고 2000년부터 상용서비스를 시작하였다.

TradeCard는 수입업체와 수출업체, 금융기관, 보험회사 및 화물운송업체를

9) Through Transport Club의 약칭. 해상화물운송 부문의 상호부보조직(P&I)으로 80여개국의 운송업자, 운송주선인, 항만당국 등이 회원으로 참여하고 있으며, 컨테이너 선단의 2/3, 1725개의 항만시설, 5890사의 운송업자에 대한 보험을 담당하고 있다.

10) 1995년 설립되어 수출입업자, 선사, 운송주선인. 보험회사, 상업회의소 등 약 200개 이상의 회원으로 구성된 Bolero서비스의 사용자 그룹으로서 회원의 요구에 맞는 Bolero서비스를 제공함을 목적으로 한다.

11) 한국무역협회 사이버무역부, 「사이버무역 국제동향과 성공전략」, 굿인포메이션, 2001.

연결, 수출입계약에서 무역금융, 선적 및 대금결제의 전 과정을 전자적으로 처리할 수 있게 하는 전자무역거래 및 전자금융서비스를 말한다.

신용장(L/C : Letter of Credit)은 수출상의 신용위험(Credit Risk)[12]과 수입상의 상업위험(Commercial Risk)[13]을 막기 위해 출현한 제도이자만 실제 운용에 있어서는 본래의 목적과는 달리 부정적인 부분도 적지 않다.

즉, 첫째로 신용장이 갖는 가장 중요한 기능인 지급확약에 있어서 현실적으로 신용장 조건과 일치하는 서류를 제시하였음에도 불구하고 대금의 지급이 즉각적으로 이루어지지 못하고 지연되는 경우가 적지 않아 지급수단으로서의 유용성을 떨어뜨리고 있다는 점을 들 수 있다. 또한 경미한 서류상의 결함과 오류도 하자로 취급함으로써 지급확약이 이루어지지 않는 경우도 많다.

둘째는 고비용의 문제를 들 수 있다. 즉, 은행에서 신용장방식의 선적서류를 매입할 경우 정상적으로 발생되는 비용요소 이외에도 하자 등을 이유로 높은 수수료를 요구하여 결과적으로 전체 거래비용을 높이고 있는 것은 국내외 모두에게 공통적인 현상이다. 이러한 이유 때문에 특히 자체 신용이 높은 대기업의 경우에는 신용장거래보다 추심 거래를 선호하고 있는 형편이다.

셋째는 서류심사에 소요되는 시간의 문제이다. 국제무역거래에서 일반적으로 해상운송을 선호하고 있는 것을 감안하더라도 해상을 이용한 화물운송속도가 신용장제도 탄생하고 발전했던 시기에 비하여 획기적으로 빨라진 것에 반하여 신용장방식에 의한 은행 등의 서류처리시간은 서류의 다양화 및 서류처리의 진부성에 의해 빨라지지 못함에 의해 결과적으로 물품인도가 지연되는 결과로 나타나게 되어 수입상으로서 불만의 한 요소가 되고 있다.

TradeCard는 이와 같이 무역결제상 가장 안전하고 효율적인 수단이 되어야

12) 계약에서 채무자가 지급불능 또는 지급거절에 위하여 지급이 이행되지 않는 위험을 가리킨다.
13) 대금을 지급하였음에도 불구하고 적기에 원하는 물품을 납품 받지 못하는 위험을 말한다.

할 신용장제도 조차도 의외로 적지 않은 결함들을 지니고 있음에 주목하여 이러한 결함을 제거한 새로운 결제방식이 필요하다는 주장과 함께 특히 정보통신분야의 발전된 기술을 무역거래에 수용하여 종이 서류 없이 무역거래를 실현하겠다는 배경에서 출발하고 있다.[14]

3) BeXcom

BeXcom사는 전세계 금융회사, 물류회사, 인증기관를 통합한 GTI(Global Transaction Infrastructure)를 기반으로 거래의 알선에서부터 대금결제에 이르기까지 안전성과 보안을 유지하면서 완전한 구매 프로세스를 지원하는 솔루션을 제공하기 위해 1996년 11월 Singapore에 설립되었다.

B2B 전자무역 관련 S/W와 지속적인 솔루션 개발을 목적으로 Singapore와 미국의 San-Diego에 R&D 센터를 보유하고 있으며, 전 세계 주요 무역지대(major trading zones)인 중국, 동남아시아, 북아메리카, 일본, 유럽 등에 위치해 있는 슈퍼허브(Super-hub)[15]를 운영하고 있다.

BeXcom의 핵심을 이루는 ITC(Internet Trading Center)는 전 세계 비스니스 네트워크인 GTI를 작동시키는 서버 엔진으로 자동화된 수요·공급망관리를 통해 전자무역거래의 효율성과 비용절감 매카니즘을 가능케 한다. 즉, 무역거래의 알선, 무역정보의 제공, 무역서류의 전송 및 인증, 무역거래대금의 결제에 이르기까지 전자무역거래를 통합한 완벽한 end-to end 프로세스로서 거래환경 측면에 있어서 상당한 안전성과 보안성을 강조하고 있다.

주요 결제방식은 "구좌 대 구좌로의 이전(Account-to-Account Transfer)"

---

14) 안병수, "국제결제관습상 TradeCard의 수용가능성에 관한 연구", 통상정보연구 제 2 권 제 2 호, 한국통상정보학회 2000. 11.

15) 슈퍼허브에서는 전문요원들이 관련 고객들을 상대로 주문서비스와 통합서비스를 제공하고 있으며, 또한 고객들을 상대로 교육 및 지원업무를 담당하고 있다. 이러한 서비스는 영어 혹은 특정지역의 현지어로 제공되어진다.

"은행간 지로지불 가능(Inter-bank Giro Payment)" "계좌 이체 가능(Electronic Funds Transfer)" "Physical Cheque Payment" "Bankers Cheque" "DDA(Direct Debit Authorization) on Demand" "전신환 이체" "신용카드 및 구매카드(Purchasing Card) 사용" "외환/환전" 등이다.

3. 전자무역결제에서의 전자인증의 역할

1) 전자무역결제상의 위험의 분석

전자무역결제상의 안전의 위협은 데이터의 수정, 노출, 훼손, 서비스의 거부, 혹은 사기의 형태로 네트워크 자원 혹은 상태, 환경으로 정의되어 진다.[16] 1997년 2월 컴퓨터 안전협회(Computer Security Institute : CSI)와 FBI의 배포된 자료에 의하면, 563개의 미국 조직 중 43%가 인터넷을 통해서 공격을 받았다고 나타나고 있다.[17]

전자무역의 활성화로 인한 전자결제시스템의 이용의 증대로 인하여 결제 위험 방지를 통한 결제제도의 정비가 범세계적인 과제가 되었다. 하지만 정보기술의 빠른 변화로 어떠한 위험의 내용도 완전히 없어질 수 없고 오히려 과거에 예상하지 못했던 새로운 위험의 출현 가능성이 더욱 높아졌다. 이러한 위험들은 개방네트워크에서 결제를 행할 때 전자금융뿐만 아니라 그 수단들에게도 모두 적용된다.

이들의 활동에서 나타날 수 있는 위험은 크게 운영상 위험, 사회적 위험, 법적 위험의 범주로 나눌 수 있겠다.

---

16) Kalakota, R. and Whinston, A. B. *Frontiers of Electronic Commerce.* Addison-Wesley, Reading, MA. 1996

17) Mcelroy, D. and Turban. E. "Using Smart Cards in Electronic Commerce", *International Journal of Information Management.* Vol. 18. No 1, 1998.

운영상의 위험은 시스템 확실성 또는 무결성의 중요한 결함으로 인한 손실 가능성으로부터 야기되는 보안 위험, 컴퓨터 바이러스와 고객의 실수 및 남용, 그리고 부적당하게 고안되거나 이행된 전자결제시스템으로부터 야기될 수 있는 시스템 고안 및 이행과 유지의 위험, 시스템의 부적합성 등을 들 수 있다.

사회적 위험은 금융기관 혹은 제3자의 행위에 대응해서 발생할 수 있고, 다른 위험범주에서 운영상 위험의 직접적인 결과가 될 수 있다. 사회적 위험은 기대만큼 시스템이나 결제수단이 작동하지 않아 발생할 수 있는 통신 및 컴퓨터 장애, 제3자에 의한 실수 혹은 착오, 위법행위, 사기 그리고 결제수단의 분실 등을 들 수 있다.

법적 위험은 법, 규칙, 규정 또는 규정된 관행의 위반 또는 불일치로부터 또는 어떤 거래에서의 당사자들의 법적 권리와 의무가 잘 확립되어 있지 않을 때 발생한다. 모든 거래당사자들이 거래를 행할 때 당사자들의 권리와 의무는 불확실하다. 예를 들어 전자결제에 있어 어떤 소비자 보호규칙의 적용은 명확하지 않을 수 있고 법적 위험은 전자매체를 통하여 형성된 어떤 합의의 유용성에 관한 불확실성으로부터 야기 될 수 있다. 위험의 형태로는 개인의 프라이버시 침해, 전자결제수단의 절취, 익명성 침해 등을 들 수 있다.

<표 2-3> 위험의 분석

위험의 범주	위험의 발생요인
운영상 위험	보안위험 시스템 고안 및 이행과 유지 고객의 실수 및 남용 컴퓨터 바이러스 시스템의 부적합성
사회적 위험	통신 및 컴퓨터장애 네트워크상의 악의의 제3자에 의한 부정행위 결제수단의 분실
법적 위험	개인의 프라이버시 침해 전자결제수단의 절취 익명성 침해

현재 전자무역결제의 각 위험에 대한 보안 기술은 대충 정비되었지만 어떠한 기술을 구사하더라도 100%의 안전대책은 있을 수 없다. 하지만 주로 인증과 인증기관, 인증기술과 관련된 기술을 이용되고 있다. 즉, 전자무역결제상의 위험에 대한 주요대책은 인증이다.

2) 전자서명과 전자인증의 필요성

(1) 전자서명의 의의

① 전자서명의 개념

전자서명은 전자문서에 부착되거나 논리적으로 결합된 전자적 형태의 서명, 즉 수기서명(Manual Signature)의 전자적인 대체물로서 펜 대신에 컴퓨터를

매개로 하여 생성되는 정보라고 할 수 있다. 여기서 '컴퓨터를 매개로'의 의미는 기술적으로 전송하고자 하는 전자문서의 메시지요약(message digest)을 만든 후, 이를 송신자의 전자서명 생성키(비밀키)를 이용하여 암호화(encryption)한다는 것을 의미한다. 기존의 서명이 서명자에만 의존하고 문서에 따라 변함이 없음에 비해 전자서명은 서명자뿐만 아니라 전자문서(메시지)에 따라 달라지는 디지털 정보이다. 이러한 방식으로 생성된 전자서명이 송신되면, 수신자는 송신자의 전자서명 검증키(공개키)를 이용하여 확인하게 된다. 확인이 된 경우는 전자서명의 특성상 송신자의 인증 및 문서의 무결성이 증명된 것이고, 이를 이용하여 차후에 부인방지의 기능을 할 수 있다.[18]

이러한 전자서명의 필요한 기능으로서는 첫째, 문서메시지 또는 기록에 누가 서명을 하였는가를 나타내어야 하고, 타인이 본인의 수권 없이는 생성하기 어렵다고 하는 서명자 인증, 둘째, 서명자의 서명이 기입된 문서가 서명자가 의도한 문서임을 입증하는 문서인증, 셋째, 서명을 서명자가 자신의 의사에 의한 긍정적인 행위로 행하는 확언적 행위, 넷째, 서명자인증과 문서인증 양자를 최소한의 자원비용으로 최대한 확보하는 효율성의 기능이 있다.[19]

② 전자서명의 암호화 방식

전자서명을 암호화하는 방식은 대칭키 암호방식(Symmetric Cryptosystems : 비밀키 암호방식)과 비대칭 암호방식(Asymmetric Cryptosystems : 공개키 암호방식)의 두 가지 기본적인 형태가 있다. 대칭키 암호방식은 암호화하는 키와 복호화 하는 키가 동일한 경우[20]이며, 비밀키 암호방식 또는 공통키 암

18) 김영준, "전자서명과 인증에 관한 연구", 통상정보연구 제 3권 제 1호, 한국통상정보학회, 2001. 6.
19) 손진화, "전자상거래에 대한 법적 대응", 법제연구 제 11호, 한국법제연구원, 1996.
20) Warwick Ford and Michael S. Baum, *Secure Electronic Commerce*, Prentice Hall PTR. 1997.

호방식이라고도 한다.

비대칭 암호방식은 암호화하는 키와 복호화 하는 키가 서로 다른 경우이며, 암호화하는 키 또는 복호화 하는 키를 공개하기 때문에 공개키 암호방식이라고도 한다.

대칭키 암호방식은 암호화하는 키와 복호화 하는 키가 동일한 암호방식으로서, 1970년대 초부터 상업적인 통신망에서 이용되어 왔다. 대칭키 암호방식은 동일한 키를 이용하기 때문에 처리속도가 매우 빠르며, 무엇보다도 시스템 상에서 효율성을 좌우하는 암호화 키 크기가 공개키 암호방식보다 작아 상대적으로 효과적인 암호시스템을 구축할 수 있다. 그러나 정보교환 당사자간에 같은 키를 공유해야 하므로 여러 사람과의 정보교환시한 사용자는 많은 키를 유지 관리해야 하는 어려움이 있다. 따라서 큰 네트워크 상에서 키에 대한 신뢰성을 담보하기 위해서는 믿을 만한 제3자나 인증기관을 두어야 한다.

공개키 암호방식은 대칭키 암호방식과는 달리 두개의 키를 이용한다. 즉, 모든 사용자는 각각 자신의 공개키와 비밀키 쌍을 가지고 있는데, 개인이 소지한 비밀키(Private Key)와 이에 대응하여 일반에 공개된 공개키(Public Key)가 이용된다. 공개키는 모든 사용자에게 공개되어 있으며, 비밀키는 생성자 자신만이 알 수 있다. 즉, 자신의 비밀키로 암호화환 암호메시지는 자신의 공개키로 다시 암호화하면 원래의 메시지로 복원된다.

따라서 공개 키 암호시스템의 사용자는 오직 자신의 개인 키만 보관하면 되므로, 큰 네트워크 상에서 대칭 키보다는 훨씬 적은 수의 키로도 유지될 수 있다. 현실적으로 큰 네트워크 상에서는 공개 키 관리를 위해 믿을 만한 제3자나 인증기관이 요구되지만 키 개수가 적기 때문에 훨씬 효율적인 관리를 할 수 있으며, 전자서명에 있어서도 상대적으로 효율적이고 간단한 시스템을 구축할 수 있다. 그러나 암호화를 위한 키의 크기가 상대적으로 크기 때문에 데이터 처리량이 적고, 컴퓨터 수행능력이 떨어진다.

<표 2-4> 비밀키와 공개키 암호화 방식의 장단점

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

(2) 전자인증과 인증기관의 의의

인증이란 전자서명 검정키가 자연인 또는 법인이 소유하는 전자서명 생성키에 합치한다는 사실을 확인·증명하는 행위를 말한다.[21] 인터넷을 통한 정보의 전달이나 전자무역결제가 이루어지는 상대방과 비대면 상태에서 업무를 처리하게 되므로 당사자의 신원확인 즉 진정성의 확인과 전달되는 데이터의 무결성을 확인하는 절차가 필요하게 되는데 이러한 문제를 해결하기 위하여 인증이 사용된다. 여기에는 전자서명은 전자문서를 생성한 신원과 전자문서의 변경여부를 확인할 수 있도록 비대칭 암호화 방식을 이용하여 전자서명 생성키로 생성된 정보로서 당해 전자문서에 고유한 것을 말하고[22][23], 전자서명 생성키는 전자서명 생성키는 전자서명을 생성하기 위하여 이용하는 전자적 정보를 말하며[24], 전자서명 검정키는 전자서명을 검정하기 위하여 이용하는 전자

21) 전자서명법 제 2조 6항.
22) 전자서명법 제 2조 2항.
23) 전자서명이 갖추어야 하는 요건은 첫째, 서명자의 인식이 가능하여야 하며 둘째, 문서내용의 변경여부를 확인할 수 있어야 하고, 셋째, 동일한 전자서명의 재사용이 불가능하여야 하고, 넷째, 문서작성 사실에 대한 부인을 방지할 수 있어야 한다.
24) 전자서명법 제 2조 3항.

적 정보를[25] 말한다.

즉 전자인증이란 수신자가 수취한 내용이 위조되거나 삭제되었는지의 여부를 확인하는 메시지인증(Message Authentication)과 상대방의 신분을 전자적으로 확인하는 본인인증(Entity Authentication)을 말한다.[26]

인증기관이란 네트워크를 통하여 거래당사자간에 송수신 또는 전자데이터에 첨부되어 있는 전자서명이 송신인 또는 수신인의 것인지에 대한 진정성을 확인할 수 있는 인증서[27]를 발급한 자 또는 단체를 의미한다.[28]

(3) 전자인증의 필요성과 인증기관의 역할

① 전자인증의 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 전자무역 활성화의 중요한 관건이라 할 수 있다.

전자문서의 수·발신 당사자간의 신분확인(사용자 인증 : authentication),

---

25) 전자서명법 제 2조 4항.
26) 최석범, 전게서.
27) 전자서명생성정보가 가입자에게 유일하게 속한다는 사실 등을 확인하고 이를 증명하는 전자적 정보를 말한다. 전자서명법 제 2조 7항.
28) 윤광운·장두채·김철호, 전게서.

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.

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 인증기관의 역할

앞에서 살펴본 인증의 필요성을 기초로 인증기관의 역할은 신분확인, 공개키 인증, 시간날인, 증거확보, 배달매개, 분쟁해결 등이 있는데[29], 이를 구체적으로 살펴보면 다음과 같다.

---

29) 이상규·한억수·구희조, "전자상거래 효율성 제고를 위한 공인인증체계 구축방안 연구", 한국경영정보학회 춘계학술발표대회, 한국경영정보학회, 1999.

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 한 쌍의 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) 전자인증체계

(1) 인증기관의 구성요소

인증기관을 구성하는 요소로는 인증서를 발행하고 취소하는 인증기관, 인증서 등록 및 사용자 신원확인을 대행하는 등록기관, 인증서 및 인증서 취소 목록을 저장하고 사용자에게 서비스하는 디렉토리, 그리고 인증서를 신청하고 인증서를 사용하는 사용자로 구분할 수 있다.[30]

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.[31]

가. 정책승인기관(PAA : Policy Approving Authority)

공개 키 기반 구조(PKI)의 전반적인 운용 및 관리 책임과 인증서 정책 및 인증 규정의 수립 책임이 있는 기관이다. 또한 인증서 정책과 규정의 변경 승인에 의한 PKI의 무결성의 관리 책임과 직접 하위 계층의 정책 인증 기관(PCA)에 대한 인증, 다른 기반의 PAA와의 상호 인증의 허가를 담당한다.

나. 정책인증기관(PCA : Policy Certification Authority)

정책 승인 기관(PAA)의 하위 계층으로 자체 도메인내의 사용자와 인증 기

30) 이호건 · 박승락 · 운영한, "글로벌 전자상거래를 위한 인증체계", 통상정보연구 제 2권 제 2호 한국통상정보학회, 2000. 11.
31) 김홍선, 「PKI 기반 구조의 구성요소」, 시사컴퓨터 1999.

관이 따라야 할 정책 수립과 인증을 담당하는 기관이다. PAA로부터 발급 받은 인증서를 하위 계층의 인증 기관에 보내고, 인증 기관의 공개 키를 인증하며, 인증서와 인증서 폐기 목록(CRL)를 관리하는 역할을 한다.

다. 인증기관(CA : Certification Authority)

PCA의 하위기관으로서 ㉠ 사용자의 공개키 인증서의 발급 및 취소, ㉡ 자신의 공개키와 상위 인증기관의 공개키를 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 사람뿐만 아니라, 사람이 이용하는 시스템 모두를 의미하며, ㉠ 자신의 비밀키/공개키 쌍을 생성하고, ㉡ 인증기관에 공개키 인증서를 요청하고 인증서를 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 발급 받는 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.[32] 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.

---

32) 이경구, "전자인증제도", 「전자상거래 국가전략 수립 토론회」, 한국전산원, 1998. 5.

① 순수 계층 구조 방식(Centralized Certification Infrastructure)

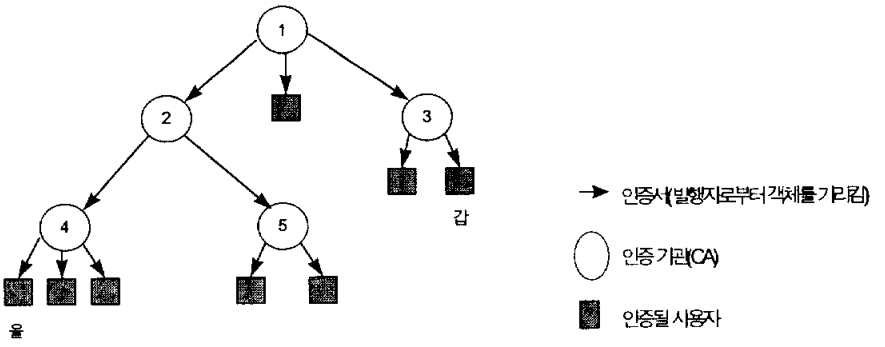
인증기관은 한 개의 루트 인증기관 하위에 계층적으로 연결되는 구조를 가지며, 각각의 인증기관은 자신의 상위 또는 하위 인증기관과 인증서를 교환한다. 즉, 아래의 그림과 같은 형식으로 구성되며, 최상위 루트 CA는 전반적인 PKI 정책을 수립하고, 제2계층의 CA를 인증하며, 제2계층 CA는 루트 CA에 의해 설정된 정책하에 자신의 정책을 수립하고, 제3계층의 CA를 인증한다. 그리고 제3계층 CA는 사용자를 인증하는 구조로 형성되어 있다.

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.

계층구조의 원하는 인증서의 획득이 용이하고, 인증경로에 대한 검증이 용이하며, 계층적인 조직에 적합하고, 루트 CA간의 상호인증을 통한 국제간 상호동작을 원활하게 하는 장점도 가지고 있다. 하지만 현실적으로 전 세계적인 구성이 불가능하고, 루트 인증기관의 비밀키 안전성이 모든 인증서의 안전성과 관계가 있는 단점이 있다.

<그림 2-1> 계층 구조



자료 : 이호건 · 박승락 · 윤영한, 전게서

② 네트워크 방식(Decentralized Certification Infrastructure)

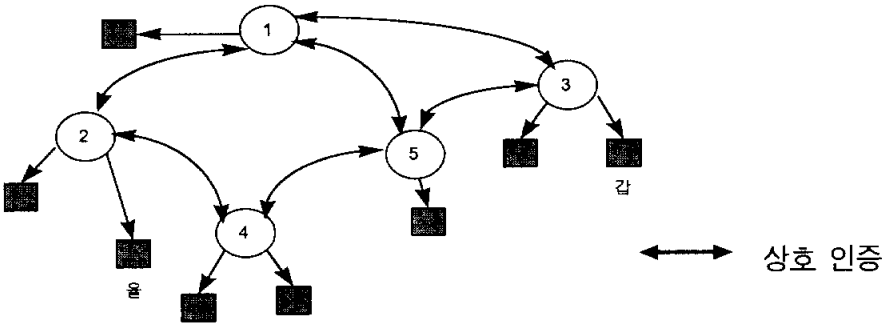
네트워크 구조는 일반적인 네트워크 환경에서 근접한 인증기관에 대해 상호 인증을 할 수 있는 구조로서 아래 그림과 같이 모든 CA가 평면적으로 구성되어 있다. 인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구조로서, 인증기관들이 상호 인증하며 인증서를 발급한다. 사용자는 인증서를 발행한 인증기관의 공개키만을 알고 있다.

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.

네트워크 구조는 인증기관간의 상호인증이 가능하고, 상업적 상호 신뢰관계의 유지가 용이하며, 유통성 있는 정책과 처리 부하의 경감, 그리고 CA의 비밀키 손상에 대한 복구가 용이한 장점이 있는 반면, 원하는 인증서를 찾기 위한 인증경로 체계와 관리가 복잡하고 단일 인증경로가 사용이 불가능하고, 모든 CA 간의 상호 인증이 허용되면, 상호인증의 수가 대폭 증가하는 단점이

있다.

<그림 2-2> 네트워크 방식



자료 : 이호건 · 박승락 · 윤영한, 전게서.

<표 2-5> 순수계층구조와 네트워크 방식의 특징 비교

	순수계층 기반구조	네트워크 기반구조
구현	· 용이하지 않음 · 전반적인 정책설정과 구성에 대한 기본 틀을 마련한 이후 구현 가능	· 용이 · 각 그룹, 조직별로 연관성 있는 시스템간의 상호인증이 가능
상호인증	· PAA를 통한 상호인증	· 하부인증기관 간에 상호인증
확장성	· 높다	· 낮다
상호 동작성	· 높다 · 일관된 보안 정책 하에 조직이 운영되므로 타 기반 시스템과의 연동성이 높다.	· 낮다 · 각 네트워크는 자신의 정책을 설정함으로써 네트워크간의 호환성을 유지하기 어렵다.

자료 : 이만영 · 김지홍 · 류재철 · 송유진 · 염홍열 · 이임영, 「전자상거래 보안기술」, 생능출판사, 1999.

③ 혼합형 방식

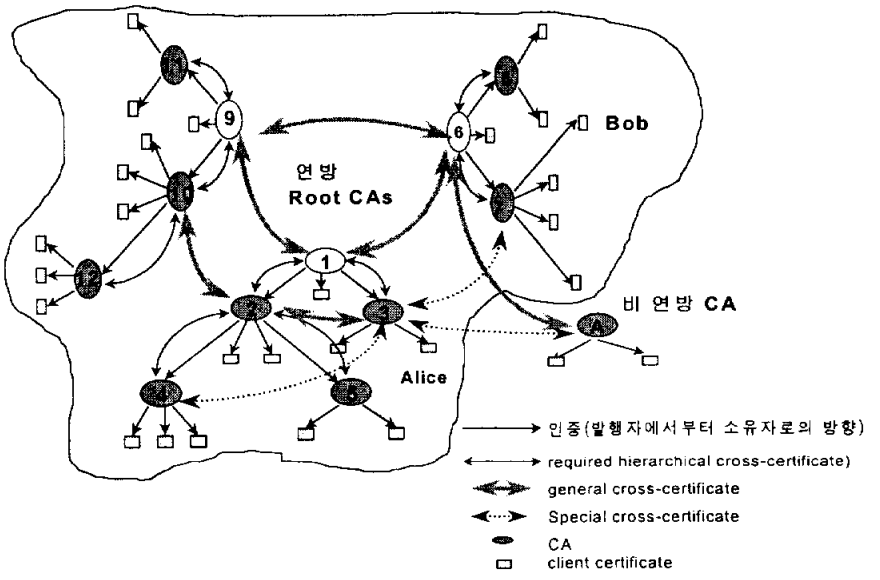
혼합형 구조는 계층구조와 네트워크 구조를 혼합한 형태이다. 구조적인 특

징으로서 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 계층 구조처럼 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 2-3> 혼합형 방식



자료 : 한국전산원, "정부전자문서를 위한 인증 소프트웨어 표준에 관한 연구", 1998. 12.

Ⅲ. 전자인증제도의 현황 및 문제점

1. 전자인증관련 법제동향

1) 주요국제기구의 법제동향

(1) UNCITRAL 전자서명 통일규칙 초안

전자거래가 범세계적으로 확산됨에 따라 이러한 입법적 차이를 다자 차원에서 해결해야 할 필요성이 시급한 과제로 대두되면서 1996년 5월에 개최된 UNCITRAL 제 29차 위원회에서 전자상거래 모델법을 채택하면서 동 위원회는 디지털 서명(Digital Signature)과 인증기관(Certification Authorities)의 문제를 차기 회의 의제로 채택하였다.[33]

UNCITRAL 제 30차 회의에서 전자상거래 실무작업반의 의견을 채택하여 전자서명과 인증기관의 법률문제에 관한 통일 규칙의 준비를 지시하였다. 이때 전자거래에서 공개키 암호의 우세에 따라 디지털서명 문제에 중점을 두되 전자상거래모델법의 매체중립원칙을 따르기로 하였으며, 기타 다양한 보안수준의 수용, 서비스의 유형에 따른 상이한 법률효과와 책임의 인정 및 국제간 상호인증을 고려한 인증기관의 최소충족요건 제시를 언급하였다.

이렇게 하여 전자상거래 실무작업반은 사무국이 마련한 시안을 토대로 제32차 회의부터 38차 회의까지 계속하여 '전자서명에 관한 통일규칙초안(Draft Uniform Rules on Electronic Signature)에 대하여 검토와 수정을 진행하여 왔다.

---

33) 정완용, "전자상거래와 전자서명법- UNCITRAL 전자서명통일규칙을 중심으로", 전자상거래와 법적 대응, 한국비교사법학회 창립 4주년 기념학술대회자료집, 1998. 10.

오스트리아 비엔나에서 개최된 제 37차 UNCITRAL 전자상거래 실무작업반회의에서는 그 때까지 작업한 통일규칙 초안의 명칭을 "전자서명모델법초안"(Draft UNCITRAL Model Law on Electronic Signatures)으로 바꾸기로 하였고 그에 대한 입법지침 초안이 논의되었다. 이로써 동 모델법의 전자상거래모델법과의 관련성이 더욱 분명하게 되었다.[34]

이 초안은 총 4장 19개 조문으로 구성되어 있으며, 이제까지의 각종 입법례와 학계의 견해를 포괄하는 것으로 전자문서와 전자서명에 대한 제반 규정이 매우 상세하고도 치밀하게 규정되어 있다.

제 37차 작업반 회의에서 집중 논의된 부분은 제2조 용어의 정의, 제 12조 외국 인증서 및 전자서명의 인정, 그리고 통일규칙의 법적 지위 등 세 가지로 요약된다. 제 2조의 a항[35]의 전자서명(Electronic signature)이라는 개념은 기술중립의 원칙, 그리고 법적 측면과 기술적 측면을 모두 포함한 것이어야 한다는 의견이 공감대를 형성하여 반영됐고, b항의 인증서(Certificate)라는 개념 또는 일반성 및 기술중립성을 포함시켜야 한다는 다수 의견에 따라 서명자와 서명생성 데이터간의 관련성을 증명하는 데이터 메시지 기타 기록으로 단순하게 정의되었다. c항의 데이터 메시지는 동 초안이 1996년 채택된 UNCITRAL 모델법 제1조의 정의와 동일성을 유지한다는 의견이 반영되어 수정되었다. 또한 f항의 신뢰당사자(relying party)라는 용어와 이를 인증서 혹은 전자서명에 의거하여 행위할 수 있는 자로 개념 정의하여 규정한 것은 신뢰당사자라는 용어가 많은 입법례에서 사용하고 있지 않으므로 이를 분명하게 해야한다는 주장이 반영되어 추가되었다.[36]

---

34) 박영우, "UNCITRAL 전자서명모델법", 인터넷 법률 제3호, 법무부, 2000. 11.

35) 전자서명(Electronic Signature)이라 함은 데이터메시지와 관련하여 서명장치 소유자(signature device holder)를 확인하고 당해 데이터메시지에 포함된 정보에 대한 서명장치 소유자의 승인을 나타내는데 이용될 수 있는 데이터 메시지에 포함, 첨부 혹은 논리적으로 결합된 전자적 형태의 데이터, 데이터 메시지와 관련된 일정한 방법을 말한다.

36) 왕상한, 「전자상거래와 국제규범」, 박영사, 2001.

초안은 미디어 중립적 접근방법에 따라서 공개키 암호화 기술에 의존하는 디지털 서명이라는 특정한 기술만을 규정하지 않고, 먼저 전자서명 및 안전한 전자서명에 대한 일반규정을 두고, 디지털 서명을 안전한 전자서명에 의한 방식으로 규정하고 있다. 그리고 인증기관은 여러 가지 전자서명 방식 가운데 디지털 서명의 안전성 및 신뢰성을 보장하기 위한 것이기 때문에 디지털 서명과 관련하여 규정하고 있다는 점에 특징이 있다. 이 초안은 기본적으로 캘리포니아주나 일리노이즈주의 디지털 서명법의 입장과 같이 전자서명과 디지털 서명을 개념적으로 구분하는 태도를 취하고 있으며, 전자서명의 효력에 관한 범세계적 해결방안을 모색하고 있다.

(2) WTO의 전자상거래 논의 동향

WTO에서 전자상거래 문제가 본격적으로 논의되기 시작한 것은 1998년 3월 WTO사무국에서 발표한 「전자상거래와 WTO의 역할」이라는 보고서가 발표되면서부터이다.[37] 동보고서에는 인터넷 접속, 시장접근 문제, GATS 체제에서의 무역자유화, 무역간소화, 전자상거래 및 공공조달, 지적재산권과 TRIPS 협정, WTO체제의 규모문제 등이 주로 언급되었다.

이후 1998년 9월 제 2차 각료회의에서 채택된 "전자상거래에 관한 각료선언(Declaration on Global electronic Commerce)"에 따라 WTO 일반이사회 특별회의에서 WTO 내에서의 작업계획(Work Program)이 수립되어 2000년 4월 현재 상품교역이사회, 서비스교역이사회, 지적재산권 이사회 및 무역개발위원회 등 해당 분야별로 논의가 진행중이다. 특히, 서비스 교역이사회에서는 이미 타결된 기본 통신서비스협정을 토대로 전자상거래 규율문제가 논의되었는데,

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

GATS의 제반규정 즉, 대상범위, 최혜국대우, 투명성, 개도국 참여, 국내규제, 경쟁관련 조항, 시장접근, 내국민 대우, 구체적 약속, 관세 분류 등에 전자상거래가 어떻게 적용될 수 있는지에 대한 논의를 정리하였다. 서비스의 전자적 전달이 GATS협정 대상이라는 점, 모든 서비스 공급방식이 적용을 받는다는 점, 기술적 중립성의 적용 등에 대하여 국가간 일반 견해를 같이 하였으나, 일부 국가는 이러한 문제가 매우 복잡하고 추가적인 검토가 필요함을 들어 반대의견을 제시하기도 하였다.

이 외에도 공급방식 분류상의 모호성, 최혜국 대우 및 내국민 대우에 대한 인터넷 망과 서비스의 접근 가능성 여부 문제, 통신부속서상의 공중통신운송망과 서비스에 대한 인터넷망과 서비스의 접근 가능성 여부 문제, 과세부과문제 등 다수 문제에 있어서 추가적 논의가 필요하다는 점이 제시되었다. 그러나, 전자인증과 관련된 구체적인 내용이 제시되지는 않고 있다.

(3) EU의 전자서명 공동체 기본 지침

EU에서 전자서명에 관한 논의는 1997년 유럽위원회가 EU내 각 기관에게 보낸 통신, "전자적 통신에서 보안 및 신뢰의 보장 : 전자서명 및 암호화를 위한 유럽기본 규칙"에서 본격적으로 시작되었다. 1997년 전자서명기본규칙은 전체 4부와 부속서로 구성되고 제2부에서 전자서명에 대한 설명과 인증기관, 법적 문제점 등을 다루고 제3부에서 암호화에 대한 규제방안을 제시하고 있으며, 마지막 4부에서 공동체 수준에서의 전자서명과 암호화에 대한 제안을 하고 있다.[38]

이어서 유럽위원회는 1997년 7월 6일 독일의 본에서 동유럽국가를 포함한

38) 박노형, "전자상거래 관련 국제규범의 제정 동향과 내용 분석", 고려대학교 통상법 연구센터, 2000. 12.

유럽 29개국이 참가한 "범세계정보망(Global Information Network)"에 관한 각료회의를 개최하고 인터넷에 대한 정부규제의 최소화, 새로운 과세 반대 등을 주요내용으로 하는 "본 선언"을 채택하였다.[39]

1999년 전자서명 공동체 기본지침[40]은 전자서명의 이용을 촉진하고, 그 법적 인정을 부여하기 위한 목적으로 채택되어 2000년 1월 19일 발효되었으며, 유럽연합 회원국들은 발효일로부터 18개월 내 즉 20001년 7월 19일까지 이 지침의 내용을 자국법에 이행하여야 한다고 규정하고 있다. 이 전자서명 공동체 기본지침의 주요내용은 다음과 같다. 우선 "전자서명"이란 첨부되어 있거나 논리적으로 다른 전자적 데이터와 연관되어 인증의 방법으로 제공되는 전자적인 형태의 데이터를 의미한다. 서명이 요구되는 요건을 충족시키는 것과 같은 형태의 전자서명은 법적 절차를 통하여 증거로서 인정을 받는다.

또한 각 회원국은 전자서명이 단지 전자적인 형태로 이루어졌다거나 기타 다른 이유로 법적 절차에서의 증거능력이나 법적 효과를 부정해서는 안 된다. 동 지침에 의할 경우, 전자서명을 광의의 전자서명(Electronic Signature)과 고급 전자서명(advanced Electronic Signature)의 두가지로 정의하며 고급의 전자서명의 경우 각 회원국은 고급 전자서명에 서면에 작성한 수기서명과 마찬가지로 유효한 것으로 자동적으로 추정되며, 또한 소송에 있어서도 증거로서 사용될 수 있다.[41]

이에 따라 고급 전자서명이 서명으로서 유효하기 위하여서는 첫째, 서명자에게 특유하게 연결되어야 하며 둘째, 서명자를 확인할 수 있어야 하고 셋째, 서명자의 독점적 지배하에 관리할 수 있는 수단을 사용하여 이루어져야 하며

---

39) 한승철, "전자서명 및 인증기관의 법적 문제", 저스티스 제 31권 제 1호, 한국법학원, 1998. 3.

40) Proposal for a European Parliment and Council Directive on Certain legal aspects of electronic commerce in the internal market, COM(1998)586final, 98/03/25(COD), 1998. 11. 18. c/30, 1999. 2

41) 배대헌, "전자서명과 인증", 인터넷 법률 제 1호, 법무부, 2000. 7.

넷째, 데이터의 변경 여부를 확인할 수 있도록 관련 데이터와 연결되어야 한다는 요건이 있다. 이 고급 전자서명은 다시 유효한 인증서에 근거하여 안전한 서명 생성장치에 의하여 이루어진 경우 문서상 데이터와 관련하여 수기서명이 서명의 법률요건을 충족시키는 것과 동일하게 전자적 형태의 데이터와 관련하여 서명의 법률요건을 충족시키고, 분쟁해결절차에서 증거능력이 있음을 인정한다.

(4) ICC의 디지털로 보장되는 국제전자상거래 일반관례

ICC는 은행, 항공운송, 육상 및 해상운송, 컴퓨터, 장거리 통신 및 정보정책, 상거래관행, 금융 서비스 및 보험 등 전자상거래와 관련된 모든 부문을 포함하는 전자상거래에 관한 국제적이고 다방면에 걸친 연구 및 활성화를 목표로 전자상거래 프로젝트를 추진한 바 있다. 이러한 과정에서 전자상거래의 법적 측면과 인증기관의 설립에 관한 국제적인 가이드라인이 있어야 한다는 점에 공감하여 1995년 11월 ICC에서는 정보보안실무작업반(information Security Working Party)을 만들고 1997년 "디지털로 보장되는 국제전자상거래 일반관례(GUIDEC : General Usage for International Digitally Ensured Commerce)"를 발표하였다.

GUIDEC의 제3편 '전자상거래와 정보 안전성(Electronic Transactions and Information Security)'의 보장과 인증기관(Ensuring and Certification Authority)'과 제 4편 '인증(Certification)'에서 유효한 인증서의 효력, 인증서 진술의 정확성, 인증기관의 신뢰도, 실행과 문제점의 통지, 재정 자원, 기록, 인증기관의 업무종료, 인증서의 효력 정치, 취소 및 이에 대한 통지 등을 언급하였다. 또한 제4편 "현행 법규와 전자거래(Existing Law and Electronic Transaction)"에서 정보의 안전성, 특히 메시지의 보장 및 인증에 관한 구체적

으로 일관되고 통일된 규제방안의 필요성을 강조하고 있다.

또한 GUIDEC는 전자상거래에 관한 중요 사항을 모아 용어의 사용기준을 제시하고 관련 문제들의 배경을 설명하고 있다. 세계적으로 널리 이용되는 공개키 암호화기법에 대한 이해를 높이고, 서로 다른 법적 전통을 조화시키기 위해 대륙법과 영미법의 처리내용을 함께 소개하고 있다. 즉, GUIDEC은 서로 다른 법제 하에서 현행법 및 관행상으로 디지털 메시지를 어떻게 보장하고 증명할 것인가에 대한 일반적인 틀을 마련하는 것을 목적으로 현재의 거래관행에 따라 거래당사자간에 위험과 책임을 공평하게 분배하고, 서명자, 인증기관 및 이에 의존하는 당사자들의 권리와 책임을 명확하게 기술하고 있다.

이를 위해 GUIDEC은 안전하게 전자거래를 할 수 있는 구체적인 거래여건의 조성, 신뢰할 수 있는 전자보장 및 증명 방법에 대한 법률상의 원칙 확립, 믿을 수 있는 보장 시스템의 개발 촉진, 전자정보 시스템 사용자들을 사기나 에러로부터 보호, 기존 정책·법률·관습·관행과 보장 기술 사이의 조화 도모, 새로 등장하는 보장 시스템에 있어서 참가자의 책임관계 명확화, 보장기술의 개발과 안전한 전자상거래와의 관련성으로 옹호하는 것 등을 기본 방침으로 하고 있다.

GUIDEC은 주로 공개키 방식의 디지털 서명을 대상으로 하지만 전통적인 문서에 의한 보장방법에도 동일하게 적용될 수 있음을 명시하고 있다. 이 보고서는 미국 변호사 협회(ABA)의 '전자서명가이드라인'을 바탕으로 국제적·상업적인 관점에서 몇 가지 개념을 강화시켰으며 UNCITRAL 모델법에 규정된 전자서명에 관한 현행 국제법상의 처리방식을 원용·확대하고 있다. 한편, ICC는 GUIDEC을 살아있는 문서(a living document)로 명명하고 업계에서 통용되는 거래용어 및 관행을 계속 적으로 반영하여 그 내용이 지속적으로 수정될 수 있음을 예정하였다.

(5) OECD의 전자상거래 인증에 관한 선언문

OECD는 80년대 초반부터 가장 먼저 전자거래에 관한 논의를 시작하였으며, 산하의 각 위원회 및 실무작업반을 통하여 조세·소비자보호·프라이버시·암호·인증·정보통신기반 등 전자거래 주요 이슈에 대한 포괄적인 논의를 계속하고 있다.

OECD에서는 1980년대이래 전자정보의 교환 등 개별문제에 대한 기본적인 논의가 진행되었으며, 전자거래에 대한 본격적인 논의는 1994년 이후부터라고 할 수 있다. 초기의 논의는 정보이동의 자유와 함께 주로 개인의 권리 보호 측면에서 소비자 보호, 인터넷의 오용 등을 중심으로 전개되었지만, 최근에는 전자거래의 유용성과 무역, 경쟁, 조세 등 국제 경제적 측면에서 역점을 두고 있는 것이 특징이다.

하지만 지금까지 전자서명 및 인증제도와 관련해서 법이나 규칙의 형태로 제시된 것은 없으며, 1998년 10월 "국경없는 세계 : 범세계적 전자상거래의 실현"을 주제로 개최된 각료회의에서 '전자상거래 인증에 관한 선언문(Declaration on Authentication for Electronic Commerce)'을 채택한 바 있다. 여기에는 인증분야에서 제기되는 다양한 이슈에 대한 검토와 함께 용어의 정의, 네트워크 상에서 인증될 수 있는 정보, OECD 각 국가의 인증문제에 대한 접근방법을 간략히 소개하고 있다.

(6) 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 전 세계의 무역기관과 무역진흥조직을 연결하는 GTPnet(Global Trade Point Network)[42]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 인터넷에서의 상거래를 보호하고 다양한 종류의 상거래 발전 유도를 목적으로 하고 있다.[43] SEAL은 현재 미국, 중국, 호주에 설치되어 있는 SEAL 허브를 상호 인증함으로서 세국가를 연결하는 안전한 전자상거래 환경을 조성에 주력하고 있다.

(6) ILPF

인터넷 법과 정책포럼(ILPF : Internet Law & Policy Forum)에서는 인증기관과 소비자간의 관계는 계약에 의해 적절하게 조화된다고 결론지으면서, 소비자가 인증기관의 수행 능력, 서비스 조건, 비용 및 기타 조건에 따라 인증기관을 선택할 수 있게 해야 한다는 주장을 하고 있다.

<표 3-1> 주요국제기구의 인증관련 논의 동향

기구	규정	논의 내용
UNCITRAL	전자서명 통일규칙초안	기술 중립적 접근방법으로 안전한 전자서명에 대한 일반규정을 두고 디지털 서명에 의한 외국 인증서 및 전자서명을 인정
WTO	-	상품교역이사회, 서비스 교역이사회, 지적재산권 이사회 및 무역개발위원회 등 해당 분야별 논의가 진행중이나 전자인증과 관련된 구체적인 내용은 제시되지 않고 있음

42) 이만영 · 김지홍 · 류재철 · 송유진 · 염홍열 · 이임영, 전게서.
43) United Nations Conference on Trade and Development, United Nations Trade Point Documentation Center, 1998. 1. 30.

EU	전자서명 공동체 기본 지침	전자서명이 요건을 충족할 때에는 수기서명과 동일한 법률 효력이 있음을 인정
ICC	디지털로 보장되는 국제 전자상거래 일반관례	신뢰할 수 있는 전자인증 및 인증방법에 대한 법률상의 원칙을 확립
OECD	전자상거래 인증에 관한 선언문	전자상거래의 유용성과 무역, 경쟁, 조세 등 국제 경제적 측면에 역점을 두어 전자서명 및 인증제도와 관련한 법이나 규칙을 제시하지 않고 있으며, 네트워크 상에서 인증될 수 있는 정보, 각 국가의 인증 문제에 대한 접근 방법만을 간략히 소개
UN	SEAL (Secure Electronic Authentication Linkages : 안전한 전자적 인증연계)	상호인증을 통하여 인터넷에서의 상거래 보호, 다양한 종류의 상거래 발전을 유도하여 안전한 전자상거래 환경을 조성에 주력
ILPF	-	소비자의 자유로운 인증기관 선택 주장

2) 주요국의 인증체계

(1) EU의 인증체계

EU는 1998년 4월 "전자서명 공동프레임 워크에 대한 유럽의회와 협의회 지침(Proposal for a European Parliament and Council Directive on a common framework for Electronic Signature)"을 마련하였다. 여기에는 첫째, 회원국은 인증서비스 제공이 사전승인에 국한되지 않도록 하여야 한다. 둘째, 인증서비스제공을 위하여 자발적인 인가계획은 도입하고 관리한다. 셋째, 모든 사항은 객관적이고 투명하며 공평하여야 한다는 의견을 천명한 바 있다.

현재 EU는 인증관련 기반 구조인 ICE-TEL PKI[44]를 구축중인데 이는 유

44) ICE(Interworking public key certification Infrastructure for Europe)는 덴마크의 Danish Computing Center for Research and Education이 주관하고 있는 EU의 최상위 인증기관으로 현재 덴마크, 독일, 이탈리아 노르웨이, 슬로베니아, 스페인, 영국 등 7개국이 참여하고 있다. http://ice-tel.uni-c.dk/ice-ca/

럽전체를 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.

또한 1999년 12월 브뤼셀에서 전자서명에 관해 역내공통규칙[45]을 마련하고 정보통신 관련 이사회에서 전자서명을 법적으로 인정하는 동시에 거래의 안전성 확보에 필요한 암호기술이나 인증기관에 대한 공통규칙을 정식으로 결정하였다.

이 공통규칙이 법제화함으로써 전자상거래에 나서는 기업 등은 EU가 정하는 기준에 따라 암호기술을 채택해야 하는데, 경우에 따라서 유력한 기술이 유럽시장으로부터 배제될 가능성도 있다. 또 공통규칙에서 전자문서의 전송처가 본인인지 여부를 확인하는 인증기관에 대해 문제가 생겼을 경우의 보상 등 소비자 대책면에서의 일정 요건을 의무화할 계획이다.

(2) 미국의 인증체계

미국은 세계 각 국이 개별적으로 인터넷 및 전자상거래 관한 비일관적인 규제체제를 구축하는 것을 사전에 방지한다는 것을 목적으로 미국 정부의 기본입장을 정리하고 있다. 미국은 지적재산권 및 특허에 관해서는 WIPO, 기본통신 및 정보내용물의 무역과 관세에 관해서는 WTO, 보안에 관해서는 OECD, 기술표준에 관해서는 G-7, OECD, ISO 및 ITU 등의 기관에 적극적으로 참여하여 전자상거래의 활성화라는 명분 하에 전자상거래와 관련한 다양한 분야에

45) Directive 1999/93/EC of European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signature.

서 미국의 국익을 관철하려는 노력을 강화해 나가고 있다. 미국은 경쟁을 바탕으로 한 급격한 정보기술의 개발은 정부의 적극적 역할이 무의미하며 오히려 장애요인이 될 수 있다는 점을 강조하고 있다.

전자인증과 전자서명에 관한 미국의 입장은 가장 앞선 기술을 보유하고 있고, 이는 암호기술과 결합되어 있기 때문에 국익차원에서 정책적으로 결정해야 할 사항을 내포하고 있다. 미국은 자국의 전자인증과 전자서명기술이 국제적인 표준으로 채택되고 전 세계적으로 널리 사용될 수 있도록 전자서명통일규칙을 매우 포괄적이고 탄력적인 것으로 만들어 나가려고 하고 있다. 실제로 미국은 다양한 전자서명 및 인증 기술을 수용할 수 있는 법제를 제정하고, 인증기관도 대부분의 주에서는 공인인증기관과 비공인인증기관을 동시에 허용하는 법제를 가지고 있다.

미국은 PKI 기반하에 공공부분 인증기관과 민간부분 인증기관으로 구분하여 연방정부와 주정부[46]의 주도 하에 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.[47]

한편 민간부분의 인증기관은 주 정부의 허가를 받아 운영하도록 되어있다.[48] 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, 진입

---

46) 1995년 유타주가 디지털 서명법(Utah Digital Signature Act) 제정후 플로리다, 일리노이, 미시시피를 제외한 대부분의 주에서 유타주의 서명법을 근간으로 입법을 완료하였거나 진행중이다.

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

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

을 시도하는 단계이다.

(3) 일본의 인증체계

일본은 민간주도의 미국과는 달리 정부의 역할이 표준화나 기초기술개발에 주도적인 역할을 수행해야 함을 강조하고 있다. 물론 민간부문의 참여를 유도하는 프로그램을 병행하고 있으나, 일본의 전자상거래 도입 및 추진은 통상산업성, 우정성, 대장성, 법무성 등 정부가 중심이 되어 추진되는 특징을 가지고 있다.

국가 공공기관의 행정서비스로 전자인증을 제도화하는 문제를 포함하여 전자서명 관련 법제 정립을 위한 논의는 1999년부터 그 움직임이 활발하다. 법무성은 기존에 담당하고 있는 법인등기와 공증제도를 기초로 한 인증을 전산망을 통하여 할 수 있도록 검토 중이며, 우정성 연구회도 네트워크상의 인증제도의 역할과 과제 등을 검토한 보고서를 정리하여 인증업무에 관한 지침을 공포하였고, 또한 대장성 연구회에서는 전자화폐 및 전자결제의 올바른 방향을 정립하기 위하여 보안성 문제를 검토하고 있으며, 향후 지방자치단체에서 주민등록정보를 기초로 한 인증이 제도화 될 것이라는 전망도 나오고 있다.

일본 정부는 전자서명의 효력에 대한 민법, 호적법, 부동산등기법, 상법 등의 기존의 법규를 토대로 "전자서명·인증법"의 골격을 발표하고 2000년 2월 10일 법무성, 통상산업성, 우정성을 중심으로 인터넷을 이용하는 전자상거래의 안전성을 확보하기 위해 전자인증제도를 도입하기로 하고 이를 골자로 한 "상업등기법" 개정안을 확정하였다. 법무성 산하 지역 사무소와 정부가 공인하는 기관들이 기업에 법인 인감격인 전자인증을 부여하고 해당 기업은 전자상거래 때 이를 사용하는 형태로 계획하고 있다. 또 공증인이 전자문서로 작성된 위임장 등을 인증할 수 있도록 전자공증제의 도입을 골자로 한 공증인법

개정안도 확정하여 2000년부터 시행중이다.

전자서명인증기관으로 인터넷정책승인인증기관(IPRA : Internet PCA Registration Authority)를 최상위 인증기관으로 인증실용화실험협의회(ICAT : Initiatives for Computer Authentication technology)가 상위인증기관(Root CA)을 구성하고 회원기관을 중심으로 상위 인증기관을 시험 운용하는 상태이며, CA는 2000년 3월 현재 ASCINET, FUJITSU, ITJ, MEIJI, NEC, INTERAUTH, JAMI PILOT 등 20개로 한정되어 있다.

(4) 독일의 인증체계

1997년 6월 13일에 연방의회에서 통과한 옴니버스형식의 법률인 정보통신서비법(IUKDG : Informations und Kommunikation Dienste Gesets)[49]의 세번째 법률로서 제정된 독일의 전자서명법은 1997년 8월 1일 부로 시행되었으며 동법 시행령은 1997년 10월 8일에 연방정부의 의결에 의해 1997년 11월 1일부로 시행되었다.[50]

독일의 인증관리체계는 최상위 인증기관의 역할을 수행하는 연방통신우편규제국이 공인인증기관의 전자서명키를 생성하며, 공인인증기관은 생성된 키를 수령 받아 인증서 발급 등의 업무에 사용한다. 독일의 인증관리체계는 전형적인 공개키 기반구조 방식으로서, 최상위 인증기관과 공인인증기관으로 이루어지는 2계층 기반 구조를 취한다. 공인인증기관은 법적 효력을 갖는 가입자 인

49) 일반적으로 멀티미디어법이라고 불리는 이 법은 통일된 단일법이 아니라 원격서비스 이용에 관한 법률, 원격서비스에서의 데이터 보호에 관한 법률, 디지털 서명법이라는 3개의 법률의 재정과 형법, 질서위반법, 청소년에게 유해한 문서의 배포에 관한 법, 저작권법, 각겨표시법 등 여섯 개의 법률의 개정을 포함하는 옴니버스법이다. 윤광운 · 장두채 · 김철호, 전게서.

50) 장휘원 · 이호용 · 이규정, "전자인증의 법적 과제-독일의 전자서명법제를 중심으로", 정보화저널 제 5권 통권 18호, 1998.

증서를 발급하기 위하여, 최상위 인증기관으로부터 발급 받은 인증서에 대응되는 전자서명 생성키를 사용해야 한다. 또한 미국의 주정부와는 달리 공인인증기관이 사용하는 인증서는 유일하게 하나가 됨으로써 서비스의 가입자나 신뢰당사자는 최상위 인증기관인 연방통신우편규제국까지 인증경로 검증과정을 거치게 된다.

(5) 영국의 인증체계

영국은 전자상거래를 위한 정부의 역할을 기업의 경쟁력을 갖출 수 있도록 안정적인 법적 기본틀을 제시하는 것으로 정의하고, 이를 위해 전자통신법(Electronic Communication Bill), 경쟁법(Competition Bill)등을 제정하였으며, OECD, WTO 등 국제협력기국에서 전자상거래 기본 틀을 마련하기 위하여 적극 활동하고 있다.

통상산업부를 중심으로 ISI(Information Society Initiative) 프로그램 등 전자상거래 관련 정책을 추진 중에 있으며, 1998년 7월에는 정부의 전략과 부처간의 정책 조율을 위해 총리실 산하에 PIU(Performance and Innovation Unit)를 구성하고, 이 PIU에서 영국의 전자상거래 활성화 방안을 수립하고 있다.

전 세계에서 가장 먼저 국가가 인증서비스를 본격적으로 시작한 영국은 1999년 3월부터 우정국에서 신뢰받는 제3자 서비스로서 우선 기업 및 정부기관을 대상으로 하는 Viacode 서비스를 개시하였다.[51]

Viacode서비스는 암호기술과 공개키 기반구조를 이용하여 인터넷 전자우편의 안전성을 보장하고 상대방의 신원을 확인할 수 있도록 하는 서비스이다. 홍콩 우정국의 경우에는 다른 인증기관들을 관리하고 직접 인증업무도 수행하

51) 정원섭, "영국의 전자인증제도 관련입법 추진동향과 시사점", 정보화동향, 한국전산원, 1998. 7.

는 최상위 인증기관을 설립할 계획이다.

(6) 우리나라의 인증체계

우리나라의 경우 전자거래기본법 제정을 시작으로, 전자서명법 등의 법안을 제정하였다. 공공부분의 경우 한국정보보호센터(KISA : Korea Information Security Agency)가 국내 모든 인증기관의 키를 관리하는 국가 Root CA의 기능을 수행하고 있으며, 산하의 전자서명 인증관리센터가 개원, 인증업무준칙을 수립한 단계이다.[52]

국내 인증기관으로는 한국정보인증(주), 한국증권전산(주), 금융결제원, 한국전산원, 한국전자인증(주), (주)한국무역정보통신(KTNET)의 6개 기관으로 한국정보인증은 주로 일반 전자상거래분야에서, 한국증권전산은 증권분야, 금융결제원은 은행분야, 한국전산원은 공공분야에 주력한 인증서비스, 한국전자인증(주)은 기업간 e비지니스 업무, (주)한국무역정보통신은 금융결제와 전자문서 표준화 및 중개분야를 중심으로 전자서명 인증서비스를 제공하고 있다.[53]

국내 전자서명법에서는 공인인증기관 지정제도를 명시하고 있다. 그러나 공인인증기관으로 지정 받지 않은 업체의 전자서명 인증 업무 자체를 금지하는 것은 아니며, 자유로운 설립을 원칙으로 하는 사적 자치의 원칙에 충실하고 있다. 따라서 전자서명법에서의 인증기관이란 공인인증기관과 비공인인증기관 모두를 포함하는 인증기관을 의미하는 것이다. 따라서 공인인증기관과 비공인인증기관이 공존하게 되는데, 이는 기술의 자유로운 발전과 인증기관의 조기 정착의 조화를 위해서도 필요하다.

공인인증기관은 디지털서명의 질과 신뢰의 확립을 최우선적으로 고려하여야

52) http://www.rootca.or.kr
53) http://www.mic.go.kr

하는데 비해, 비공인인증기관은 시장 주도적 관행을 동시에 고려하게 된다. 그러나, 현재 전자서명법에서는 공인인증기관에서만 일정한 법적 효력을 인정하고 있기 때문에, 법률관계의 명확성과 안전성 도모 차원에서 법적 근거 마련이 보다 구체화되어야 할 것이다.

<표 3-2> 주요국의 인증체계

국가	인증체계
E U	ICE-TEL을 기반으로 한 계층구조방식의 인증기관 구축 중
미 국	선진화된 기술을 바탕으로 하여 공개키 기반 공인인증기관과 민간부분의 비공인 인증기관의 이원화된 네트워크 방식의 인증체계
일 본	정부주도의 계층구조방식의 인증체계
독 일	연방통신우편규제국을 최상위 인증기관으로 하고 공개키 기반구조 방식의 공인인증기관을 두는 이계층 구조 방식
영 국	국가가 공개키 기반 구조의 Viacode 인증서비스 개시
우리나라	국가가 최상위 인증기관이 된 계층구조 방식

2. 전자무역결제시스템의 전자인증 운용현황

1) Bolero

(1) Bolero의 인증절차

Belero에서 추진하고 있는 무역서류 전체의 전자화에 따른 무역업무 처리 절차는 크게 사용자 등록절차와 무역거래 처리 절차로 나누어진다.

먼저 사용자 입장에서 사용자가 비대칭 암호화 방식의 전자서명에서 진정성을 검증하는데 활용되는 공개키(Public Key)와 자신이 작성한 문서의 진정성

과 무결성을 증명하기 위하여 활용하는 비밀키(Private Key)의 한 쌍을 작성하고 공개키를 R/A로 보낸다. P/A는 사용자 ID와 공개키를 결합시켜 이를 CA로 보낸다. 또 사용자에게는 IC카드를 발급하여 송부한다.

그러면 C/A는 R/A로부터 받은 사용자 ID와 공개키에 전자서명하여 공개키에 대한 증명으로서 S/D[54]에 보낸다. S/D는 공개키 증명서를 등록하고 저장하고, 사용자는 R/A로부터 받은 IC카드에 자신의 비밀키를 내장시킨다.[55]

한편 무역거래 처리절차는 먼저 사용자는 PC나 단말장치를 통하여 C/A 앞으로 메시지[56]를 송신한다. 이 때 비밀키가 내장된 IC카드를 사용함으로써 자동적으로 디지털 서명이 작성되어 UN/EDIFACT형태로 변환된 메시지에 첨부된다. C/A는 사용자의 공개키를 S/D상에서 찾아, 이 공개키를 사용하여 디지털 서명이 첨부된 메시지를 확인한다. 또한 공개키 증명서상의 자료에 의해 요구한 처리 내용에 대한 사용자의 자격을 확인한다. 디지털 서명이 일치하고 요구한 내용에 대한 사용자의 자격이 유효한 경우 메시지 DB의 갱신을 하고 이를 관련 당사자에게 전송한다. 또 처음 메시지를 송신한 사용자에게도 결과 메시지를 전송한다. 그 휴 사용자는 C/A로부터 온 결과 메시지를 확인한다. 이러한 메시지는 모두 송신자의 디지털 서명이 첨부되어 있으며 이를 공개키를 통해 검증하고 EDI/FACT형태의 메시지를 단말기나 PC에 맞게 변환한다.

---

54) Subscriber Directory(사용자 명부)는 사용자에 관한 모든 정보를 관리하는 DB 또는 기관이며, 무역거래의 서류를 전자화한 전자문서 DB를 관리하는 C/A와 분리되어 운영된다.

55) 사용자가 IC카드에 비밀키를 내장시킬 장비가 없는 경우에는 이를 R/A가 대신할 수도 있다.

56) 메시지에는 선복신청, 전자식 선하증권의 발행 및 권리이전, 보험증명서의 발급, 화물도착통지, 인도지시, 세관의 통관허가, 신용장 개설 신청 등이 포함된다.

(2) Bolero의 구성체계

Bolero의 구성체계는 크게 무역서류의 전자적 교환을 위한 법률적, 기반으로 구성된다. 즉 실제로 시스템을 구축·운영함과 동시에 참가자들간 법률적 계약관계를 형성한다. Bolero의 법률적 기반은 상품계약, 운송계약, 보험계약 등 자산에 대한 소유권에 관련된 문서의 전자적 교환에 필요한 법적 규정을 위해 Rule Book이라는 계약 규정집을 제정하고 있다.

Rule Book은 Bolero 서비스 참여자들간의 계약관계를 규정한 다자간 계약체계이며 Bolero 서비스에 참가하기 위해서는 의무적으로 Rule Book에 서명해야 한다. Rule Book은 18개국[57]에 대한 법률분석과 타당성 조사를 통해 만들어 졌으며, Bolero 연합회에 의해 관리되고 있다.

Bolero의 기술적 기반은 메시징구조와 안전한 전자문서의 송수신을 위한 보안 체계로 구성된다. Bolero의 메시징 시스템은 인터넷을 기반으로 하고 있으며, 전자문서 교환을 위해 SMTP/MIME과 같은 인터넷 메일 프로토콜을 사용한다. 또한 전자문서의 보안을 위해서는 공개키 암호화 기반의 디지털 서명을 사용하고 Bolero 운영자는 전자문서의 내용을 볼 수 없고 전달 역할만 수행한다. Bolero 참가자들은 Gateway방식으로 Bolero 시스템에 접속하거나 인터넷과 접속된 PC와 IC카드 Reader, IC카드 등의 단순한 시스템으로 서비스를 받을 수 있다. 다만 Bolero 참가자들은 가입비, 연회비, 수수료를 지불해야 하는데 Bolero 관계자는 Bolero 서비스를 이용하는 비용이 팩스보다 저렴할 것이라고 평가하고 있다.

57) 영국, 미국, 프랑스, 독일, 프랑스, 일본, 벨기에, 노르웨이, 스위스, 중국, 스페인, 이탈리아, 브라질, 콜롬비아, 대만, 덴마크, 싱가포르

(3) 서비스의 특징

Bolero는 글로벌한 무역문서의 전달과 전자무역 서류처리에 있어서 공동의 접근방식을 창출하기 위해 그 서비스 제공과 운영이 독특하다.

① 중립적 특성

SWIFT와 TT Club이 중심이 되어 출자한 Bolero International사는 중앙등록기관으로서 Bolero 사용자, Bolero협회, Bolero 등록기관에게 자기 자신 혹은 외부자원을 통해 상업적, 기술적 운영서비스를 제공하고 있다. 이 중앙등록기관은 중립적인 특성을 지니고 기능별로 조직을 분리함으로써 정보흐름의 독점에 따른 폐해를 예방하고 있다.

② RSA 방식의 디지털 서명, IC CARD 활용

메시지의 안전성 보장에 있어서는 현재까지 가장 안전한 방법으로 알려져 있는 RSA 방식의 디지털 서명을 메시지 전송에 채택하고 있으며, 사용자 시스템의 접속에도 IC CARD를 활용하여 그 안전성을 더욱 높이고 있다.

③ Rule Book에 의한 구속력

Bolero는 법적 공백에 대비하기 위해서 전자적 방법에 의한 거래 당사자간의 교환약정을 체결함으로써 권리의무관계를 명확히 하고 있다. 이러한 교환약정을 일대일의 관계가 아니라 다자간 관계로 전환한 "Rule Book"을 도입함으로써 실용화 가능성을 높였으며, 법률적 구속력의 적용범위는 참가자의 무

역행위 전반이 아닌 Bolero가 제공하는 서비스에 국한하고 있다.

④ 현존하는 SWIFT 금융망과 EDI와의 차별화

Bolero 서비스는 SWIFT 금융망과는 달리 플랫폼만 제공될 뿐 인턴페이스 및 접속경로는 시장에서 제3자가 제공하는 다양한 제품과 서비스 중 이용기관이 선택할 수 있도록 하고 있다. 또한 기존 EDI와는 달리 법적으로 구속력 있는 계약서를 통신상에서 전송한다.

2) TradeCard System

(1) TradeCard System의 인증절차

TradeCard System은 각국별로 몇 개의 금융기관(Funder)과 계약을 체결하여 이들로 하여금 무역업체들에게 일정한도 내에서 신용을 공여하는 구조를 가지고 있으며, 구체적인 거래절차와 구조는 다음과 같다.

① 수입업자가 자국의 금융기관인 Funder에게 신용공여를 요청한다. 이 때 Funder는 FSTS의 거래한도를 설정해주는 수입업자의 거래은행으로 FSTS와는 업무협력약정이 체결되어 있어야 한다.

② 수입업자의 신용공여를 요청받은 Funder는 담보없이 수입업체의 신용을 평가하여 거래한도를 설정하며, 그 거래한도에 관한 정보를 무역카드시스템 운영자(System Administrator : SA)에게 통보한다.

③ TradeCard System운영자는 동 거래한도 등 수입업자의 정보를 시스템에 입력함과 동시에 수입업자가 시스템을 이용할 수 있도록 승인해 준다.

④ 신용한도를 통보받은 수입업자는 시스템 운영자를 매개체로 하여 수출업

체와 무역계약을 체결한다. 이 무역계약은 FSTS에 의해 만들어진 '전자무역계약서'인 'POPFI'(Purchase Order/Pro Forma Invoice)에 의해 작성하며, 수입업자가 무역계약에 따라 POPFI에 전자서명을 한 후, 무역계약에서 정한 유효기간 내 시스템 운영자에게 전송해야 한다. 그리고 시스템 운영자는 POPFI의 기재내용과 수입업자의 신용한도 등을 검사(시스템이 자동검사)한 후 POPFI를 수출업자에게 전송하며, 수출업자가 검토한 후 전자서명을 하게 되면 무역계약이 성립하게 된다.

⑤ 무역계약이 성립되면 수출업체는 운송대리인에게 선적요청서와 POPFI를 보내야 한다.

⑥ 운송대리인은 선하증권과 보험증권 Draft를 작성하여 시스템 운영자에게 보내게 된다. 선하증권과 보험증권 Draft를 받은 시스템 운영자는 선하증권 Draft와 POPFI의 일치 여부를 검사(시스템이 자동검사)한 후,

⑦ 선하증권 Draft를 운송업체에 전송한다.

⑧ 운송업체는 수출화물을 인수한 후 선하증권에 전자서명을 하고, 이를 시스템 운영자에게 다시 돌려보낸다.

⑨ 전자선하증권을 전송 받은 시스템 운영자는 POPFI의 일치 여부를 검사한 후, 전자서명이 된 선하증권과 보험증권을 수입업자 및 운송업자에게 보내준다.

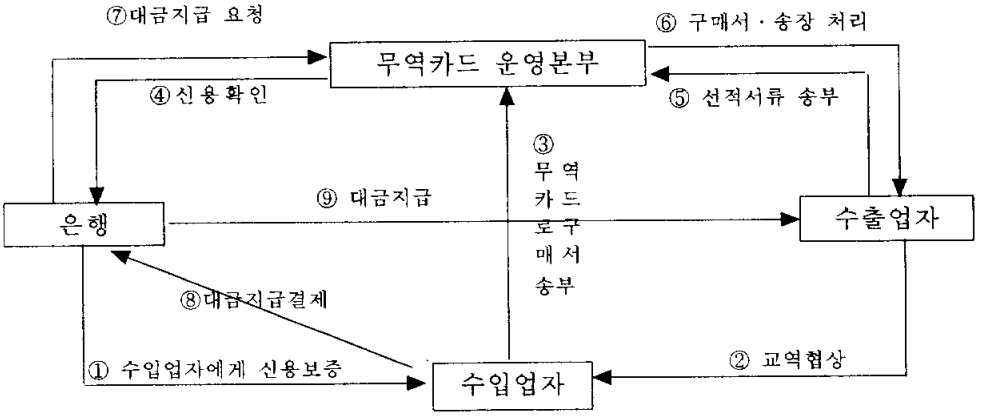
⑩ 동시에 수입업자의 거래은행인 Funder에게 대금지급을 요청하며,

⑪ 수입업자의 거래은행인 Funder가 수출업자의 거래은행에 대금을 송금하고,

⑫ 수출업자의 거래은행은 그 대금을 수출업자에게 결제하게 된다.

이 때 수입업자가 수입대금을 자신의 거래은행인 Funder에게 지급하게 되면 FSTS의 거래한도는 원래대로 회복되게 된다.

<그림 3-1> TradeCard System 서비스의 업무흐름도



자료 : 윤광운·배정한·김철호, 「사이버무역론」, 삼영사, 2001.

(2) 서비스의 특징

① 화환신용장 배제

신용장 개설은행의 서류점검에 해당하는 기능을 TradeCard 시스템 수행하며 은행은 단지 자금의 공여만을 담당하는 역할에 국한된다. 또한 운송물품을 대표하는 서류로서 선하증권은 언급되지 않고 있어 운송 중 전매를 하지 않는 소규모 제품거래를 주된 대상으로 하고 있다. 현실적으로 신용도가 높고 본지사간 거래 등이 활발한 대기업들이 신용장 방식의 결제를 회피하기 때문에 이의 수용에 소극적인 반면에 신용도가 낮아 신용장 방식의 결제에 의존하는 중소규모 수출입업체에서는 그 호응도가 상당히 높은 수준에 이를 것으로 예상된다.

② 법률적 구속력 부재

잠재적 경쟁상대인 Bolero가 18개 무역권에 대한 법률조사를 토대로 "Rule Book"을 제정, 법적 불안정성을 보완한 반면, TradeCard는 전자적 방법에 의한 거래 당사자간의 권리의무에 대한 별도의 규정을 두고 있지 않다.

③ 제휴를 통한 서비스 확대

TradeCard사는 제 관련기관과의 제휴활동을 통해 당초 TradeCard 서비스 시행과정상 드러났던 취약점들을 해결해 가고 있다. 프랑스 신용보증보험회사인 COFACE, 영국 금융회사인 Thomas Cook, 그 외에 정보기술회사인 ITPII 등과의 제휴를 통해 대금결제흐름에 관한 문제, 대금지급의 확약에 관한 문제 등 업무적용지역에서의 거래성사나 마케팅활동을 지원하는 서비스를 하고 있다.

3) BeXcom

(1) BeXcom의 인증절차

BeXcom의 주문관리(order management)는 그 프로세싱, 승인, 선적, 지불 등 거래의 모든 과정을 수입업자나 수출업자가 On-Line으로 주문상황을 감시할 수 있도록 되어있다. 시스템은 구매자와 공급자에게 On-Line 피드백을 제공하고, 사용자는 가격, 상품, 공급자의 성과를 On-Line으로 관찰할 수 있다. 시스템에서는 감사추적 보고를 목적으로 거래로그를 보유한다.

BeXcom의 전자결제시스템(payment system)은 세계적인 통화조건에 맞춰 지불이 가능하도록 하였고, On-Line으로 지불현황을 파악할 수 있도록 하고 있다. 지불방법은 ① 송장 없이도 정기적 지불을 지원하고, ② 송장에 대해 할

부를 지원, ③ On-Line 지불 서비스를 지원, 복수의 지불체계를 지원(체납, 미리 계획된 지불 등)하는 등 다양하다.

BeXcom의 승인/작업처리(Approval/Work flow)의 경우, 승인은 업무흐름에 있어 각 단계별로 위임된 임원 혹은 대리 승인자에게만 제한할 수 있다. 업무흐름에 참가하는 사용자는 미결된 승인의 상황과 의견을 검토할 수 있으며, 다양한 업무 프로세스에 따른 업무흐름을 미리 정의할 수 있다. 시스템은 임원에게 메일이나 일정표 목록을 통해 업무도착을 알릴 수 있다.

(2) 서비스 특징

① 원 스톱으로 집중화된 End-to-End 서비스

BeXcom은 거래의 알선에서부터 최종 거래대금의 결제에 이르기까지 글로벌 B2B 전자상거래시 수반되는 On-Line 주문관리, 전자결제, 승인 및 작업처리 전과정을 원 스톱으로 지원하고 있다. TradeCard나 Bolero가 그 기능적 특성으로 인해 지원서비스의 제약을 가지는 반면에, BeXcom은 End-to-End 프로세스를 통해 글로벌 B to B 전자상거래 서비스를 제공하고 있다.[58]

② 소규모 투자 및 유지·보수비용

BeXcom은 별도의 소프트웨어나 인력에 대한 과도한 투자 없이 초기의 낮은 셋업비용으로 구매/판매 종합인프라(buy/sell total infrastructure) 구현이

58) 실제로 BeXcom이 추구하는 상업화 목표도 세계 제1의 B2B 전자상거래 서비스 제공자(e-CSP: e-Commerce Service Provider)이다.(http://www.bexcom.com) BeXcom이 글로벌 B2B 전자상거래에 관련하여 최초로 원 스톱 서비스를 제공하는 업체로 주목받고 있기는 하나, 진정한 e-CSP로 자리잡기 위해서는 기본 무역거래관행과의 조화여부의 문제, 법률적 문제, 인증에 관련한 신뢰성의 문제 등의 과제가 있다.

가능하다. 전 세계 5개 슈퍼허브 담당자들이 고객(구매자/공급자)들 대상으로 시스템에 대한 교육 및 유지·보수에 관한 지원서비스를 제공하고 있어서 다른 전자결제시스템과 비교하여 비용투자가 적다.

③ 파트너쉽(partnership)을 통해 Critical Mass문제 해결

실제로 BeXcom은 뱅킹파트너(banking partner)[59]와 인증기관(certificate authorities),[60] SI사업자,[61] 물류업체[62]와 파트너쉽을 형성하고 있으며, RosettaNet, Bolero 등과 제휴파트너관계(Association Partnership)를 형성하는 등 TradeCard나 Bolero에 비해 취약한 Critital Mass문제를 보완해 나가고 있다.

<표 3-3> 전자무역결제시스템의 종합적 비교

	TradCard	BOLERO	BeXcom
메시지 표준	UN/EDTFACT	UN/EDTFACT	XML/EDI
메시지 보안	RSA방식 디지털 서명	RSA방식 디지털 서명	PKI방식 디지털 서명
상업화 목표	신용장 등 기존결제방식을 대체하는 신결제방식 제공	전자선하증권의 구현 및 무역서류의 전자적 유통	모든 지불수단이 가능하도록 은행과 인접하게 제휴한 B2B e-CSP

59) BeXcom의 뱅킹파트너로는 ABN-AMRO Bank, Development Bank of Singapore, Skura Bank, Chinatrust Commercial Bank, Frist Commercial Bank 등이 있다.

60) BeXcom의 인증기관으로는 동남아시아지역의 대표적 인증기관으로 Netrust, 타이완의 TAIWAN-CA. com Inc, 미국의 Alpha Trust 등이 있다.

61) SI는 System Integrator의 약자로 BeXcom의 ITC S/W 엔진이 잘 가동될 수 있도록 고객들에게 기술적 자문 내지 사후적 문제에 대한 고충서비스를 제공하며, 제휴업체로는 KPMG와 Semtor 등이 있다.

62) BeXcom은 세계 여러 물류업체와의 제휴를 통해 선적지시정보 및 선적화물의 위치 추적상황을 확인할 수 있도록 서비스 하고 있다. 주요 제휴업체로는 FedEx, Hsinchu Transport사, Chiao Tai Logistic사, Shuttle Service사, Ta Jung Transportation사 등이 있다.

주서비스 대상	중소무역업자	선하증권 관련 당사자	글로벌B2B거래 관련 당사자
주요 기능	계약체결 및 이행확인 대금지급 대금지급 보증	전자서명의 인증 무역서류의 관리 통신방법의 제공	무역거래알선 및 정보 제공 무역서류 전송 무역대금결제
주요 추진 주체	Warburg, WTCA, GE Information, Marsh & McLennan	SWIFT, TT Club	BeXcom, DBS Credit, ABN-ARMOBank, Sakura Bank 등
전자서류의 점검	TradCard SA의 컴퓨터에 의해 자동수행	종이출력 후 검색, 전산프로그램을 통한 자동검색	네트워크를 통한 자동검색 수행
비용절감	신용장 관련 비용 절감	선하증권 지연과 관련된 비용 절감	사업을 위한 인력 및 코스트 절감, 거래시간의 감소
서비스의 특징	무신용장 무역거래 수행	선하증권의 전자화	균일한 거래 수수료 원스톱 서비스로 비용 절감

자료 : 송선옥, 전게서.

3. 전자무역활성화를 위한 전자인증제도의 문제점

1) 각국의 법률 규정이 상이

전자무역은 그 발전의 가능성과 확산의 속도에 비해 거래에 있어서는 법적 안정성 및 신뢰의 확정성이 아직 초기 단계에 머물러 있어[63] 이에 부응하는 범세계적인 관행 및 제도의 합의가 도출되지 않고서는 소기의 성과를 달성하기 어려울 것이다. 따라서 현행 국제경제질서에 있어서 최대의 법적 과제 중 하나는 세계경제의 효율적 확대성장을 저해하지 않는 상태에서 국가간의 부와 자원의 배분적 정의를 실현할 수 있는 범세계적 전자무역관련의 법제도를 확

63) Soon-Yang Choi and Andrew B. Whinston, "The Futire of Digital Economy", *handbook on Electronic Commerce*, Sreinger, 2000.

립하는 것이라 볼 수 있겠다.[64]

국제간의 전자무역 관련 시장질서는 오랜 역사를 거듭하면서 확인되어 온 자생적 시장질서의 형태가 아니라 새롭게 생겨난 제도로서 의도적으로 산출되어 적용되어져 가는 작위적 질서에 가깝다고 볼 수 있는 측면이 있고, 더욱이 기술적인 관점에서 볼 때 그것이 활용되는 범위가 근본적으로 국경을 초월하는 초국가적 형태의 시스템 표준화를 전제함으로 거래 각 부문에 있어 범세계적인 제도의 합의가 도출되지 않고서는 거래의 실질적 권리 당사자간에 마찰과 분쟁이 발생할 가능성이 더욱 클 수 있다. 따라서 국제간 전자무역에 수반되는 문제들을 해결하기 위해 거래 주체들은 이와 관련한 거래질서를 규율해 줄 수 있는 법규범을 요구하게 된다.[65]

하지만, 인증에 관한 가장 중요한 법적, 제도적 논의의 대부분인 인증기관에 대한 각국의 법제와 국제기구의 법제가 상이한 것을 첫 번째 문제점으로 들 수 있다. 인증기관의 성격을 두고 미국은 민간자율에 맡기자는 입장인 반면, EU는 정부기관이 담당하거나 정부의 개입이 있어야 한다고 주장하여 이들의 입장이 상충되고 있다. 인증기관에 대한 제도적 태도는 그 법역 내의 인증체계와 방식을 좌우할 뿐만 아니라 범세계적인 전자상거래의 관점에서 각국의 인증체계의 조화 문제가 대두되기 때문이다.

인증기관의 문제의 핵심은 인증기관에 대하여 공적관여를 요건으로 하는가의 여부이다. 현재 전자무역 논의의 대체적인 방향은 전자무역의 발전을 저해해서는 안 된다는 것과 그것을 위해서 민간부문이 주도해야 한다는 것이라고 할 수 있다. 이는 OECD의 전자상거래 확산을 위한 10대 원칙에서도 규정되었을 뿐만 아니라 각종 전자상거래에 관한 국제 논의에서도 일반적으로 인정

64) 김기선, "전자무역 활성화를 위한 글로벌 전자무역거래법의 요건과 역할기능의 이론적 기초", 무역상무연구, 제 17권, 한국무역상무학회, 2002. 2.

65) Michael Chissick and Alistair Kelman, *Electronic Commerce : Law and Practice*, Sweet & Maxwell, 1999.

되는 바이고, 우리나라가 미국, 호주 뉴질랜드 등과 각각 발표한 "전자상거래에 관한 공동성명(Joint Statement on Electronic Commerce)" 등에서도 확인되고 있다.

우리나라의 경우 인증기관은 정부가 나서야 한다는 입장을 천명하고 있는데 이러한 주장에는 첫째 , 국가안보상, 둘째, 선진국의 공격에 대한 효과적인 방어상, 셋째, 인증기관을 민간자율에 맡겼을 경우의 혼란의 우려 등을 그 이유로 들고 있다.

그럼에도 불구하고, 인증기관에 대한 공적 관여가 바람직하다고 볼 수는 없다. 실제로 외국의 경우 대부분 민간주도의 시장 개발을 통한 인증기술의 확보 및 시장 점유라는 전략을 추진하고 있다. 즉, 정부는 민간 부분의 자율적인 기술 개발에 대한 지원을 강화하고, 민간기업의 기술개발과 이를 통한 인증기장의 성장을 위한 제도적 지원을 하는 형태로 가고 있다.

따라서 인증기관에 대한 공적 관여의 문제는 정부에서는 최소한의 개입을 하는 것이 타당하리라고 본다. 그러나 전자서명 · 인증에 대한 법적 규율이 민간의 자율을 규제하여 전자거래를 저해할 것으로 보는 시각은 일면만을 본 것으로 타당하지 못하다고 본다. 오히려 이에 대한 법적 규율을 전자서명 및 인증의 안전성과 신뢰성을 제고시켜 전자거래의 활성화를 가져올 수 있기 때문이다.

2) 국제적인 상호인정에 따른 문제

전자무역이 국제적으로 이루어지는 만큼 전자인증과 관련하여 외국의 전자인증기관이 발행한 인증서의 취급문제, 또 외국의 전자인증기관의 인정문제가 발생하게 된다.

만일, 인증체계와 관련하여 국제적으로 최상위의 전자인증기관이 존재한다

면 그에 따라 해결하면 될 문제이지만, 현 단계에서는 이러한 기관이 존재하지 않고 있기 때문에 상호인증(Cross Certification)이라는 수단을 통해 해결할 수밖에 없다. 이와 관련하여 UNCITRAL에서 발표한 전자서명법 초안인 있는데, 여기에서는 외국인증서에 대하여 국내인증기관이 직접 보증하는 '외국의 전자인증기관에 대한 국외상호인정(cross-border recognition)의 방식'과 자국이 정한 일정한 요건을 충족하거나, 국가간의 협정에 의하여 직접 외국인증서의 효력을 승인하는 '외국의 전자인증기관의 인증서 및 인증에 대한 상호인증의 방식'을 제안하고 있다.

상호인증의 경우 이용자가 누구의 인증을 더 신뢰하여 행위를 한 것인지, 어느 인증기관에 의해 손해가 발생되었는지 가리기가 어렵다는 점이다. 이 점에 대해 UNCITRAL에서는 인증기관이 시스템의 안전성에 관한 사항과 운영방침을 이용자에게 공시하는 경우 인증기관의 과실은 없는 것이기 때문에 책임도 따르지 않는다는 점을 입법화할 것을 제시하고 있다.

하지만 현재의 인증체계는 EU의 네트워크구조와 미국과 캐나다 등에서의 계층구조 및 혼합형으로 구분되어 있고, 향후 인증기관들의 구조는 정부부문에서는 미국의 사례와 같이 단일한 인증체계로 진화되고, 민간부문에서는 산업별, 거래이해집단별로 가상의 인증체계가 복합화되는 양상으로 발전할 것으로 예상된다.

현재 인증과 관련하여 깊은 관심을 표명하고 있는 전자상거래 및 국제무역 관련된 국제기구들에는 UN 산하의 UNCITRAL, ICC, WTO 등이 있으며, 이들 관련 기구들은 여러 형태의 초안(Draft), 지침서(Guideline), 및 모델 법(Model Law) 등을 통하여 여러 가지 대안을 제시하고 있다. 이들 관련 기구에서 인증과 관련된 많은 관심을 보이는 이유는 여러 가지가 있겠으나, 전자무역에서의 인증관련 중심기구로서 그 역할을 수행할 경우 가질 수 있는 기구의 위상과 경제적 이익 등도 그 가운데 하나가 될 것으로 생각된다. 이러한

문제와 관련하여 어떤 한 기구가 인증 담당 주체기구가 되어야 하는가 또는 관련 당사자들이 새로운 형태의 기구를 출범시킬 것인가라는 문제가 제기된다.

3) 전자무역결제시스템의 운영 형태의 상이

전자무역거래의 당사자간에 안정성과 신뢰성을 가지고 선택할 수 있는 전자결제시스템의 모델이 아직 정립되어 있지 않은 상태에서 전자무역결제시스템은 유형에 따라 운영의 형태가 상이한데 우선, 법적 구속력을 들 수 있다. Bolero의 경우 Rule Book을 통하여 서비스 참여자들간의 계약관계를 규정하여 상품계약, 운송계약, 보험계약 등 자산에 대한 소유권과 관련된 문서의 전자적 교환에 대하여 제정하고 있으나, TradeCard의 경우 전자적 방법에 의한 거래 당사자간의 권리의무에 대한 별도의 규정을 두고 있지 못하여 법적 구속력이 부재되어 있고 BeXcom 역시 단순한 감시만을 할 수 있게 하여 분쟁의 발생시 해결할 수 있는 방법을 제시하고 있지 못하다. 이것은 국제적인 컨소시엄 형태로 시작된 Bolero가 장기간에 걸친 법률 분석을 거치고 권리증권인 선하증권 관련 당사자 즉 선사등 대규모 기업을 서비스의 주 대상자로 하는 반면 TradeCard가 10만불 이하의 결제를 하는 중소무역업자를 BeXcom이 후발주자로서 파트너쉽에 기반하여 업무영역의 확장을 꾀하는 것에서 기인한다고 생각된다. 중소무역업자를 대상으로 하고 새로운 사업자나 사용자 그룹의 모집하여 사업의 영역을 확장하려 하는 과정에서 Rule Book과 같은 법적 구속은 장애요인이 될 수 있기 때문이다.

그리고 메시지의 암호화 방식을 들 수 있는데 TradeCard와 Bolero는 현재로서는 가장 안전한 것으로 알려진 RSA방식을 이용하는 반면 BeXcom은 PKI방식을 이용하고 있어 전자문서의 암호화 부분에서도 문제가 발생할 수

있다. 이러한 시스템 상의 호환성이 부재된 상태에서 전자무역결제의 활성화는 기대하기 어렵다고 볼 수 있다.

Ⅳ. 전자무역결제의 활성화를 위한 전자인증제도의 활용방안

1. 국제적인 인증기구의 제도적 정비

현재 인증과 관련하여 깊은 관심을 표명하고 있는 전자상거래 및 국제무역 관련된 국제기구들에는 UN 산하의 UNCITRAL, ICC, WTO 등이 있으며, 이들 관련 기구들은 여러 형태의 초안(Draft), 지침서(Guideline), 및 모델 법(Model Law) 등을 통하여 여러 가지 대안을 제시하고 있다. 이들 관련 기구에서 인증과 관련된 많은 관심을 보이는 이유는 여러 가지가 있겠으나, 전자무역에서의 인증관련 중심기구로서 그 역할을 수행할 경우 가질 수 있는 기구의 위상과 경제적 이익 등도 그 가운데 하나가 될 것으로 생각된다. 이러한 문제와 관련하여 어떤 한 기구가 인증 담당 주체기구가 되어야 하는가 또는 관련 당사자들이 새로운 형태의 기구를 출범시킬 것인가라는 문제가 제기된다.

물론, 현 단계에서는 인증과 관련된 논의는 상호인증의 단계에 머무르고 있으나, 상호인증에 대한 구체적 내용은 향후 몇 년 내에 쌍무조약 또는 다자간 조약을 통하여 문제의 해결을 시도할 것으로 판단되며, 이들 논의 가운데 최적의 대안을 중심으로 보다 구체적인 형태의 관습법적 형태의 국제규칙으로 형성될 것으로 예측할 수 있다.

전자무역을 위한 인증관련 기구에 대한 예측은 대략 다음과 같이 볼 수 있다. 첫째, 단기적으로 상호인정을 통해 인증관련 업무를 해결하고, 이것이 보편화 될 경우 공통적인 의견수렴을 거쳐 특정한 국제기구의 역할 담보 또는 새로운 국제기구의 신설 없이 단일화된 상호인증 관련 국제규칙을 생성하는

방안, 둘째, 인증관련 국제기구를 신설하고 이 기구를 통하여 제반 활동을 수행하는 방안, 셋째, WTO, OECD, ICC 등 전자상거래 관련 국제기구에서 이들 업무를 전담하는 방안으로 분류하여 생각해 볼 수 있다.

1) 상호인증의 발전을 통한 국제인증 체계의 확립

관련 당사국들의 필요성에 따라 관련 국가들간의 상호인증을 통하여 국제적 공감대를 형성하고, 상당한 시간이 경과하여 국제적인 관습으로 수용되게 하는 방법이다.

이러한 방법은 국제무역거래에서 주로 활용되는 국제무역규칙이 관습법적 성격을 가지고 있고, 서로 다른 국가들간의 유상적 거래라는 무역거래의 특징상 어떤 특정 국가의 강제적 법규가 적용되기 어려우며, '사적 당사자 자치의 원칙'이 가장 폭넓게 인정되는 특징을 고려할 때, 매우 타당하다고 본다.

그러나 상호인증을 위한 두 국가간의 쌍무협정을 체결하거나 다자간 협정을 체결할 경우, 국제인증과 관련하여 인증기관이 가장 활성화되어 있고, 전자인증에 필수적인 암호화 기술을 가지고 있는 선진제국의 이익을 반영한 형태로 타결될 가능성이 높다.

2) 인증관련 국제기구의 신설

인증관련 국제기구를 신설하고 이 기구를 통하여 제반 활동을 수행하는 방법은 기존 국제기구들의 입법 목적상 전자무역의 인증과 관련된 업무를 수행하기에는 문제가 없지 않은 것이 사실이다.

또한, 전자상거래와 관련하여 미국이 완전히 별개의 협상을 하자고 주장한 반면, EU는 별도의 전세계적 관할기관의 형성 및 논의는 반대하고, 전자상거

래를 서비스로 간주, GATS와 관련된 전반적인 검토작업을 통해 기존의 WTO 체제 내에서 다루자는 견해를 표명하였다. 이후, 미국이 EU의 주장을 받아들여 논의가 진행중이다.

미국이 인증관련 국제기구의 신설 주장을 철회한 현재, 인증관련 국제기구를 신설할 가능성은 상대적으로 희박해졌으나, 독자적인 입장표명을 하지 않은 일본과 WTO 미가입국으로서 발언권이 없던 중국 등의 국가들이 미국과 상반된 형태로 입장을 표명한다면, 상황은 달라질 수도 있을 것이다.

3) 관련 국제기구의 업무확대

마지막으로 생각해 볼 수 있는 대안은 관련된 국제기구가 그 업무영역을 확대하여 인증과 관련된 업무를 수행하는 방법이다. 현재, 국제통상과 관련된 국제기구는 WTO, OECD, ICC 등 여러 기구가 존재하며, 이들은 그 설립목적에 따라 여러 측면에서 국제통상과 관련된 업무를 수행하고 있다.

이들 가운데 가장 가능성이 크게 고려되는 기구는 전술한 바와 같이 WTO라 할 것이다. UN산하의 UNCITRAL의 경우 WTO와 함께 전자상거래 관련 최초의 법안이라 할 수 있는 전자상거래 모델법과 전자서명법 초안을 제정하는 등 여러 역할을 수행하고 있으며, 전 세계의 모든 국가들을 참여시킨다는 측면에서 WTO보다 유리한 측면이 있다.

그러나, WTO의 경우에는 설립목적상 국제통상에 직접적인 영향력을 행사할 수 있으며, 현 단계에서 EU를 중심으로 한 다수의 국가들이 WTO 내에서 논의가 되는 것을 지지하고 있으며, 미국 역시, 이들 논리를 수용하고 있는 현실을 감안한다면, 현 단계로서는 WTO가 전자인증과 관련된 논의의 중심기구가 될 가능성이 가장 크다고 볼 수 있다.

또한, 전자무역의 인증이 일종의 서비스임을 감안할 때, GATS의 분야에서

다루어져야 한다는 논리의 성립이 가능하다고 판단된다. 즉, 기존의 WTO 협상에서 결론지어졌듯이 서비스의 전자적 전달이 GATS 협정 대상이라는 점, 모든 서비스 공급방식의 적용을 받는다는 점등을 고려해 볼 때, WTO의 GATS 규율을 받을 가능성이 크다고 판단된다.

국제무역규칙들은 시대의 상황에 따라 그 형태를 달리해오고 있으며, 지속적으로 변화를 거듭하고 있다. 사실상, 국제무역규칙은 강대국의 주도하에 관련된 국제기구 및 단체들에 의해서 제정·활용되고 있음을 감안한다면, 어떤 기구가 주체가 되든 간에 이와 관련된 논의는 선진국 주도가 될 가능성이 크다. 이에 따라 우리나라로서는 유사한 상황에 처한 국가들을 중심으로 단일화된 의견 제시를 통해 대응하는 것이 필요할 것이라고 본다.

2. 국제적인 통일법제의 정비

1) 기본방향

전자무역의 법제정비의 기본적 방향은 건전한 거래질서의 확립 뿐 아니라, 정보산업의 경쟁력을 제고시키고, 국가사회의 정보화 촉진을 위해서도 매우 중요하지만, 정보통신기술의 급속한 발전은 전자무역의 법적 규율을 수립하는데 현실적으로 많은 어려움이 수반되는 것이 사실이다.

따라서 이러한 문제점을 극복하면서 발전적인 방향을 도모하기 위해서는 첫째, 최소한의 법적 조치를 취하는 것이 필요하다. 아직까지 인증업무 자체가 도입단계로서 과도한 규제는 사업발전을 저해시킬 우려가 크기 때문에 사업의 성숙도를 감안하여 적절한 시기에 필수 불가결한 분야에 한해서 법제화를 하는 것이 타당할 것이다. 또한 기존의 거래에 관한 규제와 같은 목적을 가지는 입법태도는 역시 경계되어야만 할 것이다.

둘째, 거래관계의 신속성·능률성을 도모하고자 하는 전자무역의 본질을 감안하여 민간부분의 자율성을 최대한 보장하여야 할 것이다. 물론, 인증관련 분야에 대한 공공기관의 역할이 필수적인 것은 사실이지만, 기본적으로 민간기관에 의한 자유경쟁이 여러 측면에서 바람직하다. 따라서 민간 부분에 대한 제약을 하는 형태의 법제화는 바람직하지 못하며, 자유로운 창의를 촉진하는 형식의 검토가 필요하다.

셋째, 국경을 초월하는 전자무역의 특성에 맞추어 해외 법제의 동향을 조기에 수용하여 국내법과 국제법의 일치를 도모하여야 한다.

넷째, 인증관련 분야는 정보의 기술혁신이 매우 빠른 분야이고, 사회적으로 인증관련 업무의 확대가 예상되기 때문에 기술혁신 등에 저해가 되지 않는 법제화가 필요하다. 또한, 정보기술의 진보를 적극 반영함과 동시에 정보기술의 사회적 적합성, 국내 사용자의 수용 능력 등에 대한 심도 있는 논의가 필요하다.

다섯째, 신뢰성의 확보이다. 인증업무의 보급을 확대하기 위해서는 자유로운 사업전개를 허용함과 동시에 이용자의 보호측면을 고려하여 업무의 신뢰성을 제고시키는 형식의 고려가 되어야 한다.

여섯째, 법의 예측가능성을 고려해야 할 것이다. 가능한 한 기존의 법체계를 존중하여 법적·사회적 안정성을 확보하여야 한다.

일곱째, 인증기관이 내용증명, 시간증명 등 역할 수행시 적절한 고객의 프라이버시와 관련된 정보보호가 필요하고 이에 관한 법적 조치가 필요하다.

2) 관련 법규의 정비 및 제정

국내 전자상거래 관련 법규인 전자거래기본법과 전자서명법은 상호보완적인 법이라 할 수 있는데, 그 내용상 중복적인 내용을 포함하고 있으며, 입법 취지

가 상이한 측면도 있는 것으로 판단된다. 이러한 원인은 각기 다른 부처에서 입법한 것에 기인하는 것으로 보이지만, 불합리한 요소로 지적되고 있는 것도 사실이다.

또한 기존의 전자상거래와 관련하여 여러 분야로 구분되어 있는 법을 하나의 단일한 틀 내에서 처리하는 것도 하나의 대안이 될 수 있을 것이다. 실제로 미국 등 일부국가에서는 모든 전자상거래 관련법을 대통령 직속으로 통합 연계 논의되고 있는데, 우리나라의 법 체계 상 대통령령에 의한 독립법으로 통합처리하는 것도 한가지 방법이 될 것이다.[66] 이렇게 함으로써 예산의 절감 효과는 물론 합리적인 국가차원의 정보체계 조기구축에 유리할 것이다.

또한 전자문서와 서명으로 종이문서와 서명날인을 대체하는 데 걸림돌이 됐던 법령을 발굴해 정비하는 것이 필요하다고 본다. 특히 전자거래기본법, 전자서명법을 기술적·세부적으로 새로 정비하고 공인인증기관과 관련한 제도와 비대칭 암호화에 의한 전자서명 인증제도를 보완해야 할 것이다.

이와 함께, 전통적 영업방식의 거래에 관한 기존 법제에 대한 면밀한 검토와 이에 따른 제도와 법의 정비 역시 병행되어야 할 것이다.

이들 관련 법규는 국내의 민법, 상법 등 기존 관련 법률과 전자상거래 관련 법률간의 상충 등에 대한 명확한 검토가 전제됨은 물론이며, 전자무역의 특성상 각국 동향과 국제적 규범 정비 추세 등의 고려가 필수적이다. 왜냐하면 여타 주요국가와 전혀 상이한 법안의 운용은 자칫하면 고립을 가져올 수 있기 때문이다.

---

66) 박복재, " 전자상거래 관련법 비교연구", 통상정보연구 제1권 제2호, 한국통상정보학회, 1999. 12.

V. 결 론

정보통신기술의 비약적인 발전과 함께 인터넷이 상용화되면서 국제무역의 전자화는 급속한 성장세를 나타내고 있다. 하지만 계약체결이전의 거래처 발굴과 계약체결의 단계는 On-Line으로 이루어지면서 계약이행단계의 대금결제와 국제운송은 Off-Line으로 이루어지고 있다. 현물의 장소적 이전이 이루어져야 하는 운송은 제외하더라도 네트워크를 통한 전자무역결제시스템은 전자무역의 활성화를 위한 중요한 요소라고 할 수 있다. 하지만 신뢰성의 결여에서 오는 보안문제는 전자무역결제의 장애요인으로 작용하고 있다. 이러한 보안문제의 해결방안은 공개키에 기반한 전자서명과 전자인증을 들 수 있다.

전자무역결제가 활성화되기 위한 전자인증제도의 문제점으로 첫째, 인증기관의 성격에 대한 각국의 법률 규정이 상이함을 들 수 있는데 미국은 선진화된 암호기술을 기반으로 민간자율에 맡기고 있으며, EU는 정부가 개입하여 최상위 인증기관이 되는 형태를 취하고 있다. 우리나라의 경우 국가안보상, 선진국의 공격에 대한 효과적인 방어의 목적과 인증기관을 민간에 맡겼을 경우의 혼란을 우려하여 정부가 개입하여 최상위 인증기관이 되는 EU와 같은 형태로 되어 있다. 둘째, 국제간의 거래인 전자무역의 결제과정에 각국의 다른 인증기관을 인정하는 상호인증의 문제를 들 수 있는데, 미국과 캐나다는 계층구조와 네트워크 구조의 혼합형을 택하고 있으며, EU의 경우 네트워크 구조를 취하고 있어 전자무역이 서로 다른 지역에서 일어났을 경우의 상호인증을 어렵게 하고 있다. 셋째, 전자무역결제시스템의 운영형태의 상이를 들 수 있는데, Bolero가 Rule Book에 의한 법적 구속력을 가진 반면, TradeCard System은 법적 구속력이 없으며 BeXcom의 경우 단순한 감시의 기능만을 가지고 있다. TradeCard System과 BeXcom을 사용하는 경우에 발생할 수 있는 법적 문제에 대한 대책이 마련되어 있지 못한 실정인 것이다. 또 암호화 방식도 서

로 상이하여 호환성의 문제가 발생할 수 있는데, 상호인증의 체계가 확립되더라도, Bolero와 TradeCard System이 공개키 암호화방식의 가장 안정적이라고 알려진 RSA방식의 고급 암호화 기술이 사용되고 있으나, BeXcom은 단순한 공개키 암호화방식이 사용되고 있어 서로 다른 결제수단을 사용하는 무역업자간의 거래에서 상호인증의 문제가 발생할 수 있다.

이에 대한 대책으로 첫째, 국제적인 인증기구의 제도적 정비를 위하여 전자결제에 대한 국제적 공인인증기관의 설립이 필요하다. 사이버공간에서 비대면에 의한 전자무역에서는 신용과 대금결제에 대한 확신이 무엇보다 중요한데 이를 위하여 국제적 공인인증기관의 인증서를 발급받아 거래상대방에 대한 신원확인과 대금결제의 약속을 인증받는 것이 필요하다. 이 국제적 공인인증기관의 설립을 위한 방안으로 선진제국의 영향력 하에 상호인증의 발전을 통한 국제인증체계의 확립하는 방안, 인증관련 국제기구의 신설, 관련 국제기구의 업무확대 등의 방안을 들 수 있다. 상호인증의 발전을 통한 국제인증체계를 확립하는 방안은 전세계 각국의 인증기관이 서로에 대하여 상호인증을 위한 제휴를 맺어야 가능한 것으로 많은 시간과 비용이 필요로 하기 때문에 급속도로 발전하고 있는 전자무역의 활성화를 위한 방안으로 적합하지 않은 것으로 보인다. 인증관련 국제기구의 신설은 미국이 전자상거래를 완전한 별개의 협상으로 하자고 주장하는 반면, EU는 별도의 관할기관의 형성 및 논의를 반대하고 전자상거래를 서비스로 간주하여 GATS를 통해 WTO에서 다루자는 견해를 가지고 있다. 현재 미국이 EU의 주장을 받아들여 논의 중에 있어 별도의 국제기구가 신설될 가능성도 희박해 보인다. 마지막으로 관련 국제기구의 업무확대를 통하여 인증과 관련된 업무를 수행하는 방안은 현재 국제통상과 관련된 국제기구인 WTO, OECD, ICC 등에서 다룰 수 있는데 전자상거래를 서비스로 보고 GATS를 통해 WTO 체제하에서 다루자는 주장이 가장 유력해 보인다.

둘째, 최소한의 법적조치, 민간의 자율성을 보장한 거래관계의 신속성·능률성 도모, 국제·국내법의 일치도모, 기술혁신을 저해하지 않는 법제화, 신뢰성 확보, 법의 예측가능성 고려, 프라이버시와 관련된 정보보호 등의 기본조건을 갖춘 국제적인 통일 법제의 정비를 통하여 전자무역결제의 활성화를 위한 전자인증제도가 확립되어야 할 것이다.

◆참 고 문 헌◆

[국내문헌]

강원진, "국제전자결제를 위한 SWIFT 전송신용장의 활용과 과제", 무역학회지 제 26권 제 3호, 한국무역학회, 2001. 6.

김기선, "전자무역 활성화를 위한 글로벌 전자무역거래법의 요건과 역할기능의 이론적 기초", 무역상무연구 제 17권, 한국무역상무학회, 2002. 2.

김영준, "전자서명과 인증에 관한 연구", 통상정보연구 제 3권 제 1호, 한국통상정보학회, 2001. 6.

김홍선, 「PKI 기반 구조의 구성요소」, 시사컴퓨터 1999.

문희철, " 전자무역결제시스템 관련 동향과 전망", 국제경영리뷰 제 4 권 제 2 호, 한국국제경영관리학회, 2000. 11.

박노형, "전자상거래 관련 국제규범의 제정 동향과 내용 분석", 고려대학교 통상법 연구센터, 2000. 12.

박복재, "전자상거래 관련법 비교연구", 통상정보연구 제1권 제2호, 한국통상정보학회, 1999. 12.

박영우, "UNCITRAL 전자서명모델법", 인터넷 법률 제 3 호, 법무부, 2000. 11

박종돈 · 감창남 · 이제홍, "Cyber 무역의 전자결제에 관한 논의동향", 통상정보연구 제 2권 제 1호, 한국통상정보학회, 2000. 6.

배대헌, "전자서명과 인증", 인터넷 법률 제 1호, 법무부, 2000. 7.

송선옥, "전자무역 대금결제시스템에 관한 비교연구", 통상정보연구 제 3 권 제 1 호, 한국통상정보학회 2001. 6.

손진화, "전자상거래에 대한 법적 대응", 법제연구 제 11호, 한국법제연구원, 1996.

안병수, "국제결제관습상 TradeCard의 수용가능성에 관한 연구", 통상정보연구 제 2 권 제 2 호, 한국통상정보학회 2000. 11.

왕상한, 「전자상거래와 국제규범」, 박영사, 2001.

윤광운 · 배정한 · 김철호, 「사이버무역론」, 삼영사, 2001.

윤광운 · 장두채 · 김철호, 「전자상거래론」, 삼영사, 1999.

윤광운, "전자상거래의 이용에 따른 전자대금결제시스템의 구축과 운용에 관한 연구", 국제상학 제 14권 제 1호, 한국국제상학회, 1999. 5.

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

이경구, "전자인증제도", 「전자상거래 국가전략 수립 토론회」, 한국전산원, 1998. 5.

이만영 · 김지홍 · 류재철 · 송유진 · 염홍열 · 이임영, 「전자상거래 보안기술」, 생능출판사, 1999.

이호건 · 박승락 · 윤영한, "글로벌 전자상거래를 위한 인증체계", 통상정보연구 제 2권 제 2호 한국통상정보학회, 2000. 11.

장휘원 · 이호용 · 이규정, "전자인증의 법적 과제-독일의 전자서명법제를 중심으로", 정보화저널 제 5권 통권 18호, 1998.

정완용, "전자상거래와 전자서명법- UNCITRAL 전자서명통일규칙을 중심으로", 전자상거래와 법적 대응, 한국비교사법학회 창립 4주년 기념학술대회자료집, 1998. 10.

정원섭, "영국의 전자인증제도 관련입법 추진동향과 시사점", 정보화동향, 한국전산원, 1998. 7.

정현우 · 최종수 · 윤광운, 「국제무역결제론」, 삼영사, 1998.

최경진, 「전자상거래와 법」, 현실과 미래, 1998.

최석범, "전자결제상의 위험과 인증에 관한 연구", 국제상학, 제 15권 제 1호, 한국국제상학회, 2000. 5.

한국무역협회 사이버무역부, 「사이버무역 국제동향과 성공전략」, 굿인포메이션, 2001.

한국은행 금융결제부, " 미국의 전자수표시스템 운영계획 내용", 지급결제정보, 1998.

한국전산원, "정부전자문서를 위한 인증 소프트웨어 표준에 관한 연구", 1998. 12.

한승철, "전자서명 및 인증기관의 법적 문제", 저스티스 제 31권 제 1호, 한국법학원, 1998. 3.

[외국문헌]

Directive 1999/93/EC of European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signature.

Kalakota, R. and Whinston, A. B. Frontiers of Electronic Commerce. Addison-Wesley, Reading, MA. 1996

Mcelroy, D. and Turban. E. "Using Smart Cards in Electronic Commerce", International Journal of Information Management. Vol. 18. No 1, 1998.

Proposal for a European Parliment and Council Directive on Certain legal aspects of electronic commerce in the internal market, COM(1998)586final, 98/03/25(COD), 1998. 11. 18. c/30, 1999. 2

Ronald A. Anderson and Walter A. Kumpf, Business Law, 6th ed.,

South-Western Publishing Co., 1961.

Soon-Yang Choi and Andrew B. Whinston, "The Futire of Digital Economy", handbook on Electronic Commerce, Sreinger, 2000.

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

Warwick Ford and Michael S. Baum, Secure Electronic Commerce, Prentice Hall PTR. 1997.

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

[인터넷 사이트]

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

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

http://www.cc. gatech.edu/gvu/user_surveys/ surveys-1998-04

http://www.commerce. net/research/free-report/

http://www.mic.go.kr

http://www.rootca.or.kr