전자상거래 신뢰서비스를 활성화시키기 위한 선진국들의 정책에 관한 비교 연구[1)]

A Comparative Study on Policies Related To Trust Services in e-Business

이정우 *, 이종성**

목 차

Key Words : trust, trust services, authentication, e-business, e-commerce

Abstract

"Trust" becomes a focal issue in e-business. Unlike traditional business environment, virtual situation requires new trust-ensuring mechanism other than face-to-face meetings and other related means of confirmation. Many countries are trying to foster trust services industry in order to increase e-business transactions and activities.

This paper compares and contrasts these countries' policies on trust services. Conclusions of this comparative research includes: (1) trust services industry will be tightly integrated horizontally and increase their scope vertically towards trust in business sense over and beyond the mere technical level trust, (2) necessity of reciprocal trust authentication exchange is calling for an international standard in a near future, and (3) two different types of policies are under development: government-led and industry-led. Advantages and disadvantages of different approaches are presented with details of legal implications and structures of operations.

1) 본 연구는 한국전자거래진흥원의 지원을 받아 연구되었음.
* 연세대학교 정보대학원 교수, jlee@yonsei.ac.kr, 011-398-7751
** 연세대학교 정보대학원 박사과정, y2k-come@yonsei.ac.kr, 011-208-4503

I. 서론

전자상거래는 기업의 생산비용을 감소시키고 소비자의 요구에 신속히 대응할 수 있는 기회를 부여할 수 있는 가능성을 열어줌으로써 생산 소비 활동의 패러다임에 커다란 변화를 일으키고 있다. 기업간에 이루어지던 기존의 상거래 또한 가상공간을 활용하기 시작하고 있으며 가상공간에서의 전자상거래 활성화 여부가 국가의 경제성장에 중요한 요소로 대두되고 있다. 한편 기존의 전통적인 상거래에서는 거래 당사자가 직접 대면을 하거나 제삼 기관의 신용도에 의뢰하던 행위들을 이제는 가상공간에서 행하여야 하는 상황이 도래하였다. 전자상거래의 활성화를 이루는데 있어 현재로써 신뢰성의 확보와 제고가 중요한 요소로 등장하고 있다.

이에 각국은 전자상거래를 활성화시키고 가상공간에서의 상거래의 위험을 최소화하기 위한 대안마련에 고심하게 되었으며 이와 관련하여 신뢰성을 고양시키기 위한 정책들을 수립하고 신뢰서비스를 산업으로 발전시키려는 움직임이 일고 있다. 일례로써 영국에서 개발되어 실행되고 있는 tScheme이라는 제도를 들 수 있는 데 영국에서는 이 제도 하에서 산업별로 기업의 이 비즈니스상의 신뢰수준을 측정하고 이를 인가해주는 비영리 기구의 설립을 추진하고 있다. 다시 말해서 전자상거래의 활성화를 위해서는 기술적인 신뢰성뿐만 아니라 제도적인 신뢰성이 확보되어야 한다는 인식이 높아지고 있고 특히 국제간 전자 거래의 확성화에는 신뢰성 확보의 기준 및 표준화, 그리고 이를 상호 인정할 수 있는 제도가 필요할 것으로 보인다.

본 연구에서는 각국에서 시행 또는 개발 중인 신뢰서비스 관련 제도와 정책을 살펴보고 비교하여 신뢰서비스산업에 관련한 정책방향의 지표를 제시하고자 하였다. 새로운 산업 분야이므로 우선 신뢰서비스 및 신뢰서비스 산업의 정의를 내리고 이 정의에 따른 신뢰서비스의 구성요소들을 살펴본 후에 선진각국에서 시행되고 있는 신뢰서비스의 활성화 방안들을 수집 분석하고 이러한 제도들을 서로 비교 분석하였다. 결론적으로 시사점을 도출하고 우리나라 신뢰서비스 산업 활성화 방안을 위한 제언을 덧붙였다.

Ⅱ. 신뢰서비스 개관

1. 신뢰서비스의 등장배경

최근 전자상거래가 시간적, 공간적 제약을 극복한 새로운 경제활동 양식으로 부각되고 있음은 주지의 사실이다. 지난 1998년에 504.3억 달러 규모로 평가되던 전자상거래 시장 규모도 오는 2003년에는 1조 3,173억 달러에 달할 것으로 전망되고 있다. 이에 따라 세계 각국은 국가경쟁력 강화를 위한 핵심수단으로 전자상거래의 활성화를 추진하고 있고, 인터넷은

'정보의 바다' 라는 개념에서 벗어나 국경 없는 '비즈니스 격전장' 으로 인식되고 있다. 정부의 국가생존 전략의 결정체인 'Cyber Korea 21' 의 중점과제에 '전자상거래 활성화' 가 포함되어 있음은 바로 이러한 추세를 반영한 결과라 할 수 있다. 아래의 표는 전 세계 인터넷 이용자수와 전자상거래 규모와 전망에 대한 자료이다.

〈표 1〉 전자상거래 규모와 전망 (1997-2003)

	단위	1997	1998	1999	2000	2001	2002	2003	성장률
인터넷 이용자수	백만	86.8	144.2	196.1	256.4	327.3	398.6	502.4	29%
전자상거래 이용자수	백만	15.0	30.8	48.0	71.5	99.7	133.9	182.6	43%
전자상거래 규모	10억US$	15.45	50.43	111.36	217.81	398.12	733.63	1,317.34	92%
1인당 전자상거래	US$	1,029	1,635	2,321	3,046	3,994	5,479	7,216	35%

* 출처 : IDC, 1999.3

이렇게 급성장해나가는 전자상거래는 새로운 비즈니스의 기회를 생산함과 더불어 규모가 커지고 물량이 많아질수록 신뢰성 확보는 필수적인 정책과제로 떠오르게 되며 국제적 거래의 빈도가 많아질수록 분쟁의 소지 또한 많아질 우려가 있다. 온라인 소비자가 믿음을 가지고 웹에서 물건을 구매할 수 없다면 건전한 전자상거래의 성장은 기대할 수 없다. 디지털 경제를 발전시키기 위해서는 통신이 안전하고, 개인정보가 보호되며, 사고자 했던 것을 확실히 받을 수 있고, 기반이 되는 인프라가 안정적이어서 인터넷상에서의 쇼핑에 문제가 없다는 것이 보장되어야 활성화가 가속될 것이며 관련된 상거래의 위험도를 낮출 수 있게 될 것이다. 전자상거래 신뢰성의 제고를 위해서는 상호협력과 공생을 위한 다각적인 정책이 요구되고 국제간 협력을 위해 관련분야의 상호 이해와 협력 필요성이 높아지고 있다. 자율 시장의 신뢰성 제고를 위한 근본적 대책 및 향후 발전을 위한 정부차원에서의 국제적 협력이 절실하여지고 있다.

2. 신뢰서비스의 개념

'인터넷' 이 20세기 말의 화두였다면 21세기는 '인터넷상의 신뢰(Trust)' 가 새로운 이슈로 떠오르고 있다. 생활의 보조수단으로 인식되던 인터넷이 이제 생활의 기본수단으로 자리 매김이 되는 사이버 사회가 도래함에 따라 이미 새로운 비즈니스 모델이 인터넷을 통해 시험되고 있으며, 온라인 사업뿐만 아니라 기존의 오프라인 산업과의 연계 등 다양한 수익기반으로써 인터넷 활용도가 점차 확대되고 있다. 초기 신뢰에 대한 요구사항은 방어적 측면에서 시스템을 보호하고 외부 침입을 감시하며 기본적인

양방향 비밀통신의 지원과 같은 기술적 개발이 주류를 이루었다. 그러나 앞으로의 신뢰 요구 사항은 기존 산업사회에서의 많은 행위들을 사이버 상으로 전이시킬 때 필요한 정책과 모델 수립을 통한 능동적 신뢰서비스의 제공이 될 것이다.

신뢰(Trust)라는 용어는 전통산업에서는 신탁행위나 기업합동을 의미하는 용어로써 쓰여 왔고 이러한 신뢰서비스는 주로 은행이나 법률 회사에서 제공을 하여 왔으나 전자상거래와 관련해서 신뢰라는 용어는 보안(security) 및 인증 서비스와 관련하여 폭 넓게 사용되고 있다. 그러나 아직까지는 보안과 신뢰의 경계가 명확하게 구분되어지고 있지 않고 더불어 신뢰 서비스라는 분야가 아직 명확히 규정되어 있지도 않은 상황이다.

Timmers는 가치 사슬에 의한 11가지 비즈니스 모델 분류에서 신뢰서비스를 인터넷상으로 공증서비스나 인증서비스를 제공하는 모델로서 수입원에는 확인서비스 수수료, 관련 소프트웨어 판매 등이 있다고 정의하고 있다(Timers,1998). 전자상거래 관련 인증서비스를 주 업무로 하고 있는 미국의 VeriSign은 Digital Trust Services를 "기업고객과 소비자들에게 안전한 전자상거래를 할 수 있는 환경을 제공해주는 것"(www.verisign.com)이라고 정의하고 세 가지 핵심 분야--Web Identity, Certification과 Payment Service--에서 서비스를 제공함으로써 인터넷상의 거래와 관련해서 신뢰 환경을 조성해 나간다고 하고 있다. 우리나라의 국가공인인증기관으로 지정받아 공공인증서비스 및 인증부가서비스를 제공하고 있는 한국정보인증(주)은 전자서명, 메시지 암호화, 전자 지불, 전자계약, 전자공증, 국제 상호 인증, Device 인증을 Total Trust Service(www.signgate.com)로 정의하고 서비스하고 있다.

이와 같은 내용들을 종합해볼 때 전자상거래와 관련해서 신뢰서비스는 단순하게는 전자통신상의 보안을 위한 기술적인 인증이나 거래상대의 Identity의 확인으로부터 지불서비스의 중개자 자격의 인증이나 더 상위 개념인 비즈니스 프로세스의 정규성을 확인하여주는 서비스까지 포함하는 개념으로서 발전되어야 할 것으로 보인다.

이러한 의미에서 *전자상거래상의 "신뢰서비스"는 인터넷상에서 기업의 기술적 상업적 제도적 신뢰도를 측정하고 이를 공인하여 일반 소비자들이나 기업들이 믿고 이용할 수 있도록 도와주는 신뢰에 관한 총체적인 서비스 관련 사업의 형태*를 총칭하는 용어로 정리할 수 있겠다.

3. 신뢰서비스와 인증

신뢰 서비스를 구성하는 요소들로서는 기술적으로 확립되어야 할 보안기제, 전자서명, 공개키구조 등이 있으나 정책적인 면에서는 이러한 기술적인 구조들과 이를 지원해주는 조직들이 필요하다. 이러한 신뢰서비스의 중심에는

총체적인 평가를 통하여 각 비즈니스의 트랜스액션마다 또는 기업단위로 신뢰성이 있다고 인증을 하여주는 포괄적인 제도가 필요하다. 여기에서는 이러한 인증의 정의와 이와 관련된 제도적인 요소들을 살펴보았다.

인증(Authentication)이란 "정보나 통신시스템에서 사용자, 주변장치, 혹은 다른 실체의 주장된 신원의 정당성을 확립하는 기능" (Recommendation of OECD Council,1997)이나 "교역항목이 원본임과 진정성이 있음을 나타내는 표시"(WordNet,1998)를 의미한다.

한편, 인증이라는 용어와 비교해서 검증(Verification)은 "주장된 신원의 검증" (Department of Trade and Industry, 1997)이나, "문제의 사용자가 이전에 등록된 사람임을 확인하는 행위. 이것은 사용자의 서명이나 사용자의 지문, 망막형태 등을 포함하는 다양한 생체적 방법을 사용하여 수행 된다" (Electronic Commerce Promotion Council of Japan(ECOM), April 1997)고 정의 되고 있다.

미국에서는 "인증하다"라는 용어는 메시지와 자신을 동일시함을 나타내는데 사용되는 반면, 유럽에서는 서명의 검증과 연관된다. 게다가, 물리적 서명과 전자적 매체를 통한 서명과는 상당한 차이가 있기 때문에 메시지를 "디지털로 서명 한다"는 개념에 기본적으로 어려움을 가지고 있다. 가장 중요한 차이점은 대부분의 디지털 서명이 메시지에 대한 "서명"을 안전하게 하기 위해 스마트카드나 다른 저장장치에 의존한다는 것이다. 이때 이 저장장치가 다른 사람에 의해 또는 소유자에 의해 접근되면, 메시지는 소유자의 동의로 혹은 동의 없이 소유자로부터 유래되었음을 나타내고 서명된다.

1) 인증서(Certificate)

인증서(Certificate)는 "인증기관의 비밀키로 위조할 수 없도록 한 데이터"를 말하며, 사용자 인증서는 "인증기관의 비밀키로 암호화하여 위조할 수 없도록 한 사용자의 공개키와 몇몇 다른 정보"를 말한다.(International Standards Organization, 1998) 현재는 다양한 종류의 인증서가 존재하며 다양한 법체계의 공증기관은 형태와 효과면 에서 다른 인증서를 발행하고 있다. 기술적 컴퓨터 표준은 인증서가 일정 시간의 유효기간을 지닌 반면, 전통적인 인증서는 거래 단위로 유효하다. 아래 정의된 공개키 인증서는 특정 형태의 인증서이기는 하지만 일반적인 정의의 범위에 해당된다. 본 정의는 인증서 개념의 심오한 차이점을 나타내기도 하지만 공통의 요지에 초점을 맞추고자 한다.

정의상으로 인증서는 의도한 효과의 범위에 대한 표시를 포함하지 않는다. 예를 들면 하나의 메시지 또는 하나의 거래에만 유효한 인증서와 특정 기간 다수의 거래에 유효한 인증서가 모두 기초적인 정의에 의하면 인증서이다. 하지만 실무적으로는 앞으로 인증서가 하나의 메시지나 하나의 거래에만 유효하다면 이를 분

명히 나타내고 그 메시지나 거래에 명확하게 연관되어야 할 것이다. 만약 인증서가 일정 기간에 제한된다면 그 기간이 인증서에 표시되어야 한다.

인증서의 내용은 인증서의 목적과 형태에 따라 다르고 법이나 관행으로 지정될 수 있는 것으로 알려져 있다(International Chamber of Commerce, 1997). 이와 관련되어 신임장(Credentials)이란 "개체의 신분을 확립하기 위해 전송되는 데이터"를 말한다(International Standards Organization, 1998).

2) 인증자 (Certifier)

인증자(Certifier)는 인증서를 발행하여, 다른 사람의 행위에 대한 법적 유효성을 위하여 어떤 사실의 정확성을 증명하는 사람을 말한다. 인증자의 예로는 공증인이나 공개키 인증기관(또는 공증인과 다른 신뢰된 개체를 포함할 수 있다), 그리고 정부 공무원 등을 들 수 있다(International Chamber of Commerce, 1997).

(1) 인증기관(Certification Authority)

인증기관(Certification Authority)은 공개키 인증서를 생성하고 할당하기 위해 신뢰되는 센터로서 선택적으로 개체에게 키를 생성하고 분배할 수 있다. 신청자의 공개키를 증명하고 이에 기초하여 인증서를 발급하고, 인증서를 양도하고, 신청자의 공개키를 등록관리하고, 인증기관 자신의 키를 생성관리하고, 취소를 등록관리하고, 상호인증을 하며, 다른 인증기관과 연결되어 있는 자연인이나 조직을 말한다.(Electronic Commerce Promotion Council of Japan(ECOM), 1997)

(2) 제삼신뢰기관 (Trusted Third Party)

제삼신뢰기관은 클라이언트에게 하나 또는 여러 가지의 암호서비스를 제공하는 조직에 대한 일반적인 용어이다(Statement on Secure Electronic Commerce, 1998). 보안관련 활동과 관련하여 다른 개체로부터 신뢰되는 보안조직, 또는 그 에이전트. 이 문맥 속에서는, 제삼신뢰기관은 발신자, 수신자 그리고/또는 부인봉쇄를 위한 전달기관 그리고 재판관과 같은 제삼자로부터 신뢰를 받는다(International Standards Organization, 1998).

(3) 등록기관 (Registration Authority: RA)

등록기관은 최종사용자(개인적 데이터, 보안데이터 등)와 관련된 정보의 등록을 수행하고, 인증서의 발행과 취소에 대해 인증기관에 요청하는 자연인이나 조직(Electronic Commerce Promotion Council of Japan(ECOM), 1997)이다.

(4) 원천인증기관(Root Certification Authority: RootCA)

원천인증기관은 공인인증기관의 구체적인 인증업무에 관하여 관리 · 감독한다. 또한 공인인증기관의 인증서에 대하여 인증을 하여주는 상위기관이다.

4. 신뢰서비스의 전망

전자상거래가 활성화되기 위해서는 신뢰성 인증제도가 지금보다 발전하여 나아가야 할 것으로 보이는 데 앞으로의 발전 방향은 두 가지로 유추할 수 있다. 하나는 수직적인 발전이고 또 하나는 수평적인 발전이다.

수평적 발전은 기술적인 통합을 의미한다. 지금까지는 주로 각 기업별로 Customized Interface에 의한 중앙집권적인 보안 기술의 운용이 주를 이루었고 더불어 특별한 업체에 의해서 개발된 인터페이스 기술이 주를 이루어 왔다. 그러나 점차로 이러한 인증과 보안 체제가 상호 인정과 통합의 형태를 이루어갈 것으로 보이며 이러한 상호 인증이 없이는 국제적인 거래가 힘들어 질 것으로 보인다. 이러한 면에서 업계의 표준이 개발되면서 총체적인 협업 시스템이 개발될 것이라는 견해이다. 인증 서비스를 포함한 전체적인 신뢰서비스는 기술적 기준의 통합을 의미하는 수평적인 통합개발과 더불어서 요즈음 부상하고 있는 웹서비스 아키텍쳐의 일부로 채택하고자 하는 움직임도 나타나고 있다. 최종적으로 웹서비스의 커뮤니티 사이에 신뢰서비스가 일부 기능으로 통합될 것이라는 발전모델이 논의가 되고 있다.

기술적 표준과 통합을 통한 상호인증의 방향을 지칭하는 수평적 통합에 비해서 신뢰서비스의 수직적인 발전은 신뢰서비스를 순수한 기술적 평가나 측정으로서 인증이 단순한 보안기술의 적용이라는 기술적인 수준을 넘어서서 보안기술의 평가위에 이를 운용하는 시스템의 평가가 이루어져야 한다는 관점을 포함하고 있다. 기술의 활용은 중립적이라는 점에서 이를 운용하는 시스템의 평가라는 개념으로 신뢰서비스를 확대 해석해야 하고 이러한 확대 해석위에 신뢰 서비스제도를 위한 정책이 자리 잡아야 한다는 관점이 수직적 발전을 의미한다.

이러한 수직적인 확대에는 신뢰 서비스 운용 인력의 평가라던가 신뢰 서비스 제공 기업이나 기관의 역량 평가까지가 포함된 신뢰서비스 관리시스템의 평가가 이루어져야 총체적인 신뢰서비스의 활성화가 이루어 질 것이라고 본다. 이러한 방향의 정책적인 움직임은 영국 전자상거래 전략지침서에서 보는 바와 같이 인증의 필수요건으로서 단순히 기술의 적용뿐만 아니라 비즈니스 측면까지 포함해서 평가하고자 한다.

Ⅲ. 신뢰서비스 지원제도의 비교 분석

본 장에서는 신뢰서비스를 활성화시키기 위한 지원제도를 비교 분석하기 위하여 각국의 신뢰서비스의 제도적 현황을 살펴보았다. 우선

입법례를 비교하고 이에 근거한 운영제도의 차이점을 비교하였다.

1. 신뢰서비스 관련 각국의 입법례 비교

각 국은 다양한 형태의 신뢰서비스 제도를 만들어 운영하고 있다. 신뢰서비스를 지원하기 위해선 제도에 맞는 법률의 형성이 필요하다. 각국은 자국에 맞게 다른 법률제도를 갖추려고 노력하고 있으나 아직은 신뢰서비스가 개발이 되어있지 않고 서로 벤치마킹하고 있는 상황이라서 혁신적으로 크게 상이한 형태는 나타나고 있지 않다.

전자상거래 관련입법에서 거래의 법적효력을 확보하는 구속력의 문제는 가장 기본적인 문제이며, 국제적으로도 이에 관련해서 가장 활발한 입법 활동을 보여준다. 이미 15개국 이상이 전자서명과 관련한 법안을 마련하였으며[1], 유럽연합은 전자서명에 관한 기본지침[2]을 제안 중이다. 유엔국제거래법위원회(UNCITRAL)는 1996년 전자상거래모델법[3]을 제정한 이후 디지털서명과 인증기관에 관한 국제규칙을 마련하고자 노력하였다.

그 결과 97년 12월 전자서명에 관한 통일규칙초안(Draft Uniform Rules on Electronic Signatures)을 발표하였다. 통일규칙이 주 대상으로 삼고 있는 전자서명은 공개키 암호방식을 이용한 디지털 서명을 안전한 전자서명의 하나로 간주하며, 안전한 전자서명에 대해서 법적 효력을 부여함으로서 기술적 중립성을 추구하는 접근방식을 채택하고 있다. 이외에도 인증서, 인증기관과 인증서 소유자 및 인증서 신뢰자간의 관계, 인증서의 취소와 효력정지, 인증서의 등록에 관한 사항을 자세하게 제시하고 있고, 외국인증서의 상호인증에 관해서도 비교적 상세하게 원칙을 제시하고 있다. 하지만, 국가의 상황에 따라 많이 달라질 수 있는 인증기관의 인허가 제도 및 인허가 기관에 관련된 사항은 명기되어 있지 않다. 경제협력개발기구(OECD) 또한 정보기술의 안전한 사용을 위한 전제조건으로 전자인증문제에 관심을 집중하고 있다.

1) McBride Baker & Coles, Hot Topics, http://www.mbc.com
2) European Commission, Proposal for European Parliament and Council Directive on a Common Framework for Electronic Signatures, 1998. 5. 13. http://www.ispo.cec.be/ief/policy/com98297.html
3) United Nations, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, http://un.or.at/uncitral/english/texts/electcom/ml-ec.html

그간 각국의 법률제정을 도표로 만들어보면 아래의 표와 같다.

〈표 2〉 인증제도에 관한 각국의 입법례 비교

입법례	인증기관에 대한 규제	법적효력 및 업무범위	비 고
한국 전자서명법	요건을 구비한 인증기관을 공인인증기관으로 지정 (공인인증기관 지정제도)	공인인증기관이 인증한 전자서명에 전자서명법상의 효력 부여	
미국 연방법	규정 없음 ※초기 주법(州法)에서 허가제도를 규정하였으나 후발 주들은 등록제 등 완화된 제도 채택	모든 전자서명에 대해 법적 효력 인정 ※주법에서 제한	구체적인 사례에 따라 상이한 법적 효력 부여
독일 디지털서명에 관한 법률	법에서 정한 요건을 구비한 인증기관이 주무관청에 신고, 주무관청의 확인 후 확인필증 수여 (임의적 공인인증기관 인정제도)	규정 없음 ※개정민법에서 공인전자서명의 효력을 인정(독일민법 제126조A)	법으로 정하지 않은 전자서명인 경우에는 그 이용이 임의적임
영국 전자통신법	인증기관에 관한 규정 없음 (자율적 비영리기구인 tScheme에 의한 자발적인 승인시스템으로 운영)	전자서명, 전자서명의 발생, 통신방법, 서명에 사용된 프로시저 등을 증명하는 선언을 한 경우, 개인의 경우에도 전자서명이 인증됨	
일본 전자서명 및 인정업무에 관한 법률	요건을 구비한 자를 특정인증업무를 수행할 수 있도록 인정 (특정인증업무자격 인정제도)	본인에 의한 전자서명이 있을 때에는 전자적 기록이 진정하게 성립된 것으로 추정함	
싱가포르 전자거래법	특정기관(CCA)이 인증기관의 자격을 주기위한 규제를 할 수 있도록 함.	ETA(Electronic Transaction Act), 다양한 형태의 허가권과 규제권 인정	
프랑스 정보기술에 의한 증거법	텔레컴 규제법 제96-650에 근거하여 인증기관을 규제	특별법 제정에 선행하여 민법전이 개정, 종이문서와 같은 효력부여	

* 이정현(2002.12), 「주요국가의 전자서명인증제도」에서 인용 및 보강

구체적으로 각국을 분석해보면, 우선 미국은 전자상거래 관련 입법이 가장 활발한 국가이다. 디지털 서명을 이용하여 서명한 아일랜드와의 공동성명(1998. 9. 4)에서 클린턴 대통령은 전자상거래 발전을 도모하는 제일의 기본원칙으로 전자서명과 인증에 관한 규칙과 지침을 마련하고자 하는 민간부문의 노력을 촉진할 것을 선언하였고, 오스트레일리아와의 공동선언(1998. 11. 30)에서도 전자서명과 인증방법에 대한 차별 없는 접근을 제안하고 있다. 유타주의 1995년 입법 이래 변호사협회(ABA)의 디지털서명지침[1]에 자극받아 거의 모든 주 또한 관련입법을 완료하였거나 진행 중이며, 연방차원의 입법도 적지 않다. 특히, 통일주법전국대의원회의(NCCUL)는 1999년 연차총회에서 통일전자거래법(Uniform Electronic Transactions Act)과 통일컴퓨터정보거래법(Uniform Computer Information Transactions Act)을 채택한 바 있다.

우리나라는 전자상거래가 활성화되고 있고 정부부문에서 전자적 문서처리(electronic data interaction)가 이루어지면서 전자서명법을 제정하게 되었다. 최근 전자정부를 천명하면서 일반 법률인 「전자정부구현을위한행정업무등의전자화촉진에관한법률」(일명 전자정부법)을 제정하였다. 이를 계기로 전자서명과 인증에 관한 제도가 활성화 될 수 있는 기반이 마련되게 된 것이다. 초기에 우리나라는 독일의 전자서명법을 인용하였다. 그러므로 많은 부분이 독일 법제와 같은 형태를 보여주고 있다. 그러나 인증의 법적효력에서 차이점을 보여준다. 우리나라는 공인인증기관이 인증한 전자서명에 대하여 전자서명법 상의 법적 효력을 부여해준다. 그러나 독일은 그런 규정이 없고 민법에서 공인전자서명의 효력을 인정하고 있다. 어느 것이 적절한 가에 대하여 민법으로 규정할 때는 일반적인 주장의 필요성이 없어지는 반면에 특별법이 부여해 줄 수 있는 강도 높은 효력이 부여될 수 없게 된다.

한편, 영국과 비교해 볼 때, 영국은 전자통신법을 가지고 있지만, 기본적인 역할에 있어 민간의 자율을 최대한 인정하고 있는 형태이다. 그러므로 법률 또한 민간의 사업에 대하여 추후 인정의 모습을 보여주고 있다. 이는 우리나라가 전자거래기본법이나 전자서명법을 근간으로 하여 인증 제도를 도입하고 있는 형태와는 다른 모습이다. 그러기에 한국은 법률적 통일성은 확보할 수 있는 반면에 영국과 같이 시장과의 정합성에 있어 문제점이 지적될 수 있다. 즉, 우리나라는 국가가 제정한 법률에 근거하여 인증제도가 정착되는 모습을 보임으로서 시장의 자율성을 침해할 수 있는 가능성이 높다는 것이다.

일본과의 차이점은 일본이 법적효력에 있어서 추정주의를 채택하고 있다는 점이다. 추정주의의 단점은 반증에 의해 계약의 성립이나 효력이 부인될 수 있다는 점이다. 이럴 경우 전

1) nformation Security Committee, Electronic Commerce Division, Digital Signature Guidelines, 1996, ABA Section of Science & Technology

자상거래라는 거래의 특성에 의하여 장점이 될 수도 있는 반면에 가뜩이나 사이버상의 거래로 인하여 발생하게 되는 신뢰성 부족을 메울 수 없다는 단점이 지적될 수 있다.

2. 신뢰서비스 운용체제의 비교

선진 각국의 신뢰서비스 운용체제의 구조 및 제도를 비교하는데 있어 가장 크게 나타난 차

〈표 4-3〉 각국의 신뢰서비스 운용 비교

	구조/제도	인증기관	인증수행기관	평가기준	관리방식
영국	정부주도 민간주도 공존	tScheme (민간) CESG (정부관련)	10여개 CA등	유럽연합의 전자서명 지침에 따른 자체 profile에 의거	행동규약가입, 승인마크 제공, 정기적 재평가, 무작위 감사
미국	정부주도 민간주도 공존 민간기업의 자생적 참여 활발 정부에서 Bridge 인증체제 도입 시도 중	브리지 인증담당: FPKIPA 각 주별 별개 민간 기업: VeriSign	30여개 민간단체	ABA (Profile) VeriSign 자체의 평가기준	-
독일	이중적인 계층구조의 정부 주도 방식이나 비공식 인증기관 설립 시 허가가 필요 없음	연방통신우편 감독청 (RegTP)	독일 텔레콤 등 16개 공인인증기관	개별 신청 -> 법적 타당성 평가 후 인정	-
일본	정부주도 특정인증업무 인증제도 (인증기관이 아닌 업무 중심 인증) 임의 인정제도	총무성, 경제산업성, 법무성의 3성에 의한 승인	8개 공인기관 8개인증 서비스 시행 중	일본품질보증기구 (JQA)가 지정조사기관	-
싱가폴	정부주도	정보통신기술부 산하 Controller of Certification Authority	Netrust ID.Safe(중단)	자체적인 허가기준	CA에 따른 구체적 기준은 없으나, 6개월 주기로 관련 보고서 제출 의무
프랑스	정부주도 (경제재무산업부)	COFRAC (프랑스 인가 위원회)에서 주도할 예정	CertPlus Thawte Francophone	수립 중으로 보임	e-Qual 프로젝트 진행 중
한국	정부주도	KISA, KICA	6개 산하기관	전자서명법에 따른 Profile	인증기관의 주기적 평가

이점은 첫째, 제도적 관점에서 관 주도로 진행이 되고 있는 지 아니면 민간 주도의 움직임에 의한 제도인지가 가장 큰 차이다. 주로 민간 주도의 경우에 제도가 유동적으로 빠르게 움직이고 있는 듯이 보이며 이러한 경우에는 민간 부분에서 다양한 서비스들이 시도되고 있는 상황이다. 다음의 표에서는 선진 5개국과 우리나라의 신뢰서비스 제도를 구조, 인증기관, 평가기준, 관리방식 등으로 나누어 비교하였다.

1) 구조 및 제도

각 국의 신뢰서비스 운용체제의 구조 및 제도를 비교해보면 각국의 정책방향에 의해 정부에 의해 주도되거나 혹은 민간 부분에서 다양한 서비스들이 시도되고 있는 상황이다.

영국에는 10여개의 인증기관이 있고, 정부부문에는 CESG (Communications and Electronic Security Group)라는 관공서에서 이용되는 정보 보증에 대한 기술적 기관이 있다. 영국 정부는 인증기관에 관한 규정이 없으며 전자서명, 전자서명의 발생, 통신방법, 서명에 사용된 프로시저 등을 증명하는 선언을 한 경우, 개인의 경우에도 전자서명이 인증될 수 있다. 영국의 민간부문은 타 국가와 다르게 계층적 인증관리체계가 없고 자율적 비영리기구인 tScheme에 의한 자발적인 승인시스템으로 운영되고 있는 것이 특징이다.

이에 반해 미국의 경우 상무부 산하 국가표준업무 담당기관인 국립표준원(NIST: National Institute of Standard Technology)은 정부기관의 안전한 통신을 위한 연방공개키기반구조(FPKI)를 구축하고 전자서명 인증업무를 운영하고 있으며 유타 주 정부에서는 4개의 공인인증기관(DST, ARCANVS, USERTrustT, VeriSign), 워싱턴 주 정부에서는 3개의 공인인증기관(VeriSign, ID Certify, ARCANVS), 텍사스 주 정부에서는 1개의 공인인증기관(VeriSign)을 지정하여 운영하고 있으며 그 외의 몇몇 주 정부에서도 공인인증기관을 운영하고 있다.

영국에서 민간조직에 의한 신뢰서비스가 제공되고 미국에서는 연방 및 주정부와 민간조직의 다양한 정책을 반영하고 있는 반면에 독일은 정부가 신뢰서비스와 관련하여 서비스를 제공하고 있고, 민간부분을 특별히 규제하지는 않는다. 독일은 디지털서명법에 의거 RegTP에 의한 전자서명이 의무화되어 있으며, 이를 통해 민간 CA들을 인증하고 있다. 밑으로 민간 CA들은 개인 이용자에게 인증서를 발급하는 이중구조로 이루어져 있지만 비공인의 일반 인증기관을 운영하기 위해서는 특별한 허가가 필요하지 않고 인증기관 운영에 필요한 사항과 법적 준수사항을 지킨다는 보장만 있으면 된다.

아시아의 경우에는 비교적 정부의 주도하에 이러한 신뢰서비스의 기초가 다져지고 있다. 가까운 일본의 경우에는 인증업무 수행과 관련한 허가제 등과 같은 규제는 없으며, 특정인증업무 인증제도로 총무성, 경제산업성, 법무성의 삼성에 인증기관 인정 권한이 주어져 있다. 이는

특정한 기관을 공인인증기관으로 지정하는 방식이 아니라 특정인증업무에 대하여 인정을 하는 방식을 의미한다. 이것은 인증과 관련하여 서로 다른 인증 영역들 간에 상호 인정하는 인증서를 이용하게 하는 것으로, 앞으로의 전자상거래에서는 인증기관들의 설립과 운영이 다양해져야 한다는 데 기초하고 있다. 하지만 이와 같은 다양한 서비스들은 기존의 상용등록 및 공증체계들에 기초해야한다고 하고 있다.

싱가포르는 Controller of CAs(CCA)가 인증기관(CA)들의 활동을 감독 및 규제하고 허가하는 역할을 한다. 현재까지 공인된 인증기관(CA)은 1997년 동남아시아 최초로 세워진 Netrust와 CCA에 의해 인증된 최초의 공인인증기관(public CA)인 ID.Safe가 있으나, 현재 ID.Safe는 서비스를 중단한 상태이다. 그리고 싱가포르는 초기단계에 해당하는 보안 및 인증산업과 전자상거래의 규제를 완화하는 방안의 일환으로 자발적인 스킴(scheme)을 통한 인가제도를 택하고 있어, 싱가포르에서 인증된 기관이 아니더라도 싱가포르의 정책과 법규를 따르고, CA의 요건을 충족시킨다면, CA로서 활동하도록 허가 받을 수 있다.

2) 인증기관

각국의 관련정책에 의거하여 설립되거나 운영되고 있는 최고인증기관과 공인인증기관 등을 살펴보면 다음과 같다.

〈표 4〉 각국의 최고인증기관 및 공인인증기관

국가	인증기관
영국	tScheme, CESG(Communications and Electronic Security Group), Endorse (Barclay Bank), BT Trustwise (Verisign International Affiliate), The Global Trust Register, Inter Clear, TrueTrust (Salford University), Globalsign UK (Globalsign Network), Viacode (Royal Mail CA), Messaging Direct Certification Products (전 Isode)
미국	ARINC, Certco, eOriginal Inc., Entegrity Soultions, Corporation, Equifax Secure Inc., Equifax Secure, Inc., GTE Cybertrust, IBM World Registry, MIT Internet PCA, Registration Authority, PenOP Signature Dynamics, Authentication Technology, Digital Signature Trust, Company, Universal Secured Encryption Repository, Company (USERFirst), Arcanvus, The Usertrust Network, Verisign, SET Certificate Authority, SUN Certification, Authorities, TradeWave Corporation Utah Digital, Signature Authority, Valicert, Verisign SET Certification Authority

국가	인증기관
독일	RegTP, Deutch Telecom Telesec, 등 16개 기관
일본	Japan Certification Services, Inc., TEIKOKU DATABANK, LTD., Japan Certification Services, Inc., Japan Digital Notarization Authority, 일본 행정 서사회 연합회, Construction-ec com Co., Ltd. SECOM Trust.net Co., Ltd, N. D. Ninsho Co., Ltd.
싱가폴	CCA(Controller of CAs), Netrust
프랑스	Certplus, Thawte Francophone
한국	한국정보보호진흥원(KISA), 한국정보인증(주), 한국증권전산(주), 금융결제원, 한국전산원, 한국전자인증(주), (주)한국무역정보통신

3) 인증평가 및 관리

영국의 민간부문에는 Root CA가 없고 tScheme의 승인을 얻은 각 산업별 인증기관이 있다. tScheme은 개방적이며 중립적인 조직으로, 트러스트 서비스 제공자, 기술제공자, 사용자, 정부, 무역협회, 소비자그룹, 재무기관, 보증기관 등 모든 종류를 고객 대상으로 한다. tScheme은 영국 전자서명규칙이 수용한 EU전자서명지침 Annex II(조건을 갖춘 인증서를 발급할 수 있는 인증기관의 요건)에 따라 tScheme이 기준을 정하고 인증기관에게 승인한 후 승인마크 사용을 허락한다. 현재 tScheme의 승인 프로파일로는 기본 승인, 등록 서비스, 인증기관, 서명키 관리, 인증 생성, 인증 보급, 인증 관리, 인증상태 비준에 대한 프로파일이 있으며 계속 확장 개발하고 있다. 관리방식을 보면, tScheme의 승인을 받은 신뢰 서비스 제공자는 tScheme의 행동 규약에 가입이 되고 승인된 서비스의 웹기반 디렉토리에 추가되어 진다. 그리고 승인 기간동안 마크를 사용할 수 있으며 이로써 사용자는 서비스에 대해 신뢰할 수 있게 된다. TSP는 tScheme의 정기적인 재평가와 무작위 감사를 받고 어떤 계약 위반이나 실패에 대해서는 즉각적인 수정이나 보상, 승인권리의 박탈 등의 권리 행사가 있을 수 있으며 tScheme측 승인 서비스로 인한 책임을 배상해야 한다.

미국의 경우에는 미국 ABA 가이드라인, 유타주 디지털 서명법이 요구하고 있는 요건들은 대체로 (1)인증기능을 수행하는데 신뢰할만한 시스템을 갖추고 있을 것 (2)재정적으로 의무를 준수하면서 지속적인 사업운영에 필요한 충분한 재원을 보유하고, 인증서 및 디지털 서명을 신뢰한 자에 대한 배상책임을 충분히 감당할 만한 재정적 능력을 갖추고 있을 것 (3)인증기관을 운영하는 주체 및 운영요원의 자격과 관련하여 일정한 지식과 기술, 범죄경력의 부재 등을 충족시킬 것 (4) 인증서의 발행 · 정지

및 취소 등과 관련된 모든 중요한 사실을 문서화하고 적절한 기간동안 이를 보관할 것 (5)인증기관 운영의 투명성 및 거래안전을 확보하기 위한 인증실무 준칙을 제정 · 공시할 것 등으로 요약할 수 있다.

독일은 공인인증기관이 되기 위해서는 주무관청에 신청하여 법령에서 정한 요건을 갖추었음을 확인받은 후 확인 필증을 교부받게 된다. 비공인인증기관의 경우 전자서명법과 시행령의 준수 사실만으로 인정을 받을 수 있으며, 2002년 3월부터 인증기관과 전자서명에 대해 식별 마크를 부여하고 있다.

일본의 경우, 심사에 관해서는 정부가 권한을 가지고 있는 것이 아니라 정부산하기관인 '재단법인 일본품질보증기구(JQA)'를 '지정조사기관'으로 지정하고 있다. 이는 특정인증업무에 대하여 전문적인 조사를 수행할 수 있는 기관을 지정하여 줌으로써 조사의 신속성과 신뢰성을 확보하려는 의도가 있는 제도이다. 현재에는 이와 관련된 인증허가 표시(마크)를 할 수 있도록 하였다.

싱가포르의 인증평가의 기준은 크게 인증기관(CA)으로서 평가받는 기준과 인증된 CA가 개인, 회사, 정부단체 등에 인증서를 발급하는 기준으로 나누어 볼 수 있다. 우선 인증기관(CAs)이 되려면 ETA와 법규, 인증실행선언문(Certificate Practice Statement; CPS), 보안가이드라인, CCA에 의한 허가기준을 준수해야 하고, 재정상태, 운영 정책 및 절차, 시스템의 보안성을 포함한 평가를 받아야 한다. 그리고 CA인 Netrust는 특정인이나 단체, 서버 등에 대한 인증의 적절성을 나타내기 위한 규칙들을 묶어서 자체적으로 인증정책(The Certificate Policy;CP)이라는 발급 기준을 정하여 준수하고 있다. 이에 대한 관리로 인증기관(CA)은 매6개월마다 일반 보안 및 네트워크 보안 감사 결과와 계획에 관한 보고서를 CCA에 제출해야 하고, 변화나 업데이트가 일어날 때마다 즉각적으로 보고해야 한다.

Ⅳ 결 론

지금까지 전자상거래에 필수적 요소인 신뢰서비스의 전반적 사항과 다른 선진 국가들의 제도적 현황을 비교 분석하였다. 개방형 정보통신망을 이용한 새로운 비즈니스인 전자 상거래에서는 전통적 거래방법 또는 폐쇄형 정보통신망과 달리 거래 상대방을 직접 확인할 수 없으므로 거래와 관련된 위험성이 높은 것으로 인식되고 있다. 전통적으로 거래당사자가 직접 상대방과 대면하여 거래하면서 확인할 수 있었던 내용을 정보공간에서는 직접 확인하기가 힘들며 또한 이러한 확인 과정 자체를 가상현실화하지 않으면 빛의 속도로 움직이는 전자상거래의 장점을 살려 나가기가 힘들게 된다.

전통적인 거래에서 사용하였던 신원확인의 수단인 기명날인, 수기서명 등의 방법은 전자상거래에서 거래 당사자를 확인하기 위한 방법

으로는 적절하지 못하다. 이런 문제점을 극복하기 위해서 고안된 것이 전자서명이다. 이러한 전자 서명을 이용함으로써 정보통신망에 의해 송신된 내용이 변경되지 않고 그대로 상대방에 수신되어 상대방이 그 내용을 신뢰할 수 있도록 만들고자 하는 것이다. 전자문서를 송 · 수신할 때 그 진위여부를 판가름하기란 쉬운 일이 아니다. 전자적 거래는 신속성, 효율성 및 경제성이라는 장점을 가지고 있지만 당사자 확인의 어려움과 거래 내용의 진정성을 확보하지 못하는 약점을 지니고 있다. 이러한 약점은 기술적 · 제도적인 방법으로 극복되어야 할 것이며 이를 위하여 인증제도들이 개발되고 있다. 이러한 의미에서 전자상거래를 촉진시키고 신뢰성을 확보하기 위한 다양한 방법을 포괄적으로 정의한 것이 신뢰서비스(Trust Service)이며 이와 관계된 산업이 신뢰서비스 산업이다. 최근 신뢰서비스 산업은 새로운 산업영역으로 떠오르고 있다.

신뢰서비스는 공공재적인 성격(비경합성, 비배제성)이 강하다. 이러한 공공성 때문에 각 국이 이를 중요한 서비스로 인식하고 신뢰서비스를 활성화시키기 위한 정책적 제도적 방안을 마련하고 있다. 선진 각국의 정책방향 및 신뢰서비스의 형태를 살펴본 결과 몇 가지 차이점들이 부각되고 있다. 특히 인증제도의 정착에 있어서 인증기관을 어떤 방식으로 구성할 것인가가 핵심문제로 떠오르는 데 크게 두 가지 측면의 접근이 사용되고 있다. 하나는 국가주도형이고 다른 하나는 민간주도형이다.

국가주도형은 신뢰성 제고와 소비자의 보호라는 명분 아래 국가의 공식인증기관 혹은 인증기관들을 감독하고 승인해주는 최 상위 인증기관을 설치하여 정부를 대표한 이 기관이 전자 서명을 비롯한 신뢰성 인증업무를 주도적으로 이끄는 형태인데 반해 민간주도형은 전자상거래가 민간의 자율적인 거래관계이니 만큼 그 인증도 민간의 자율에 맡기는 형태로서 이러한 민간 주도의 경우에 사후에 등록을 해야 하는 형태와 등록도 필요 없는 자유 방임형의 형태가 되기도 한다. 독일과 싱가포르 그리고 우리나라는 국가주도형 인증 체계를 추진하고 있고 영국과 미국은 대체적으로 민간이 주도하고 있는 형태로 볼 수 있다.

국가 주도형의 경우에 국가가 공인한 인증기관의 손해배상 등의 책임 소재가 국가 인증기관에서 책임을 지는데 반해 민간의 인증기관을 이용한 거래에서는 문제가 발생하는 경우에는 민사법에 따라 처리하도록 제도화되어 있는 것으로 보여 진다. 한편, 민간주도형 인증 체계의 경우 인증기관이 난립됨으로써 소비자들이 신뢰할 수 있는 인증기관을 선택하거나, 문제 발생시 그 구제를 받는데 어려움이 있을 수 있으며 특히, 사업자나 소비자가 모두 비대면 거래에 의해 익명성을 보장받기 어렵다는 점을 감안하고, 전자거래의 장애가 그 편리성에도 불구하고 거래의 안전성에 관한 불안에 있다는

점을 생각하면 전자거래를 활성화 시키는데 장애가 될 것으로 보인다. 이에 따라 미국, 일본, 말레이시아, 독일 등 많은 국가에서는 국가가 인증기관을 설치하거나, 민간 인증기관 중 신뢰성 있는 기관을 공식 인증기관으로 선정함으로써 국가주도형이던 아니던 정부가 어떻게든 관련하고 있는 것으로 보인다.

우리나라는 오직 한 개의 루트 인증기관만이 자체 서명한 인증서를 갖고 하위구조를 구성하는 단순계층구조를 유지하고 있는 데 이러한 체제로서는 앞으로 신뢰서비스가 산업으로 활성화되는 경우에 다양한 서비스와 복잡한 사업모델을 만족시키기에는 부족한 면이 있어 보인다. 또한 현재 여섯 개의 복수 인증기관이 탄생하였고 각자 복수개의 자체서명 인증서를 발급하고 있는 데 이로 인해 상호인증의 필요성이 대두되고 있다. 현재로서는 이러한 상호인증의 필요성은 공개키기반구조(PKI)를 사용함으로서 해결하고 있는 것으로 보인다.

나온 지 얼마 안 된 짧은 시점에 공개키기반구조는 기술적으로 상당히 발전하였고 국제적인 기준으로 참조되고 있으나 이러한 PKI는 기술적인 측면에서 상호운영성의 해결은 되었지만 확장의 문제와 짧은 수명주기, 속성타입에 대한 처리, 지정 서버, 분배스키마의 수립 및 이행 등 어려운 문제들이 많이 있고 이러한 문제들을 해결해 나가고 또한 신뢰서비스가 넓은 의미에서의 수평적 수직적 통합을 이루어 나가자면 기술적인 부분은 물론이고 비즈니스의 측면이나 제도의 측면도 함께 수정 발전해야 할 것으로 보인다.

영국의 tScheme제도는 우리나라와 다른 민간주도형의 신뢰서비스 산업의 형태를 띠고 있고 PKI에 근거한 전자서명 인증제도의 도입과정이 상위의 개념부터 정리하고 비즈니스나 평가능력의 평가까지 포함하고 그 밑에 기술적인 인프라를 승인하는 top-down의 형태로 제도가 개발된 반면 우리나라에서는 순수하게 정부주도로서 전자서명법에 근거하여 보안 기술적인 측면에 중점을 두고 상위개념의 확립이 없이 기술에 관한 승인을 위주로 시작된 bottom-up의 형태로 제도가 개발되어 온 것으로 보인다.

국가 간의 전자상거래가 급증하고 있는 시점에서 인증제도의 공고화는 앞으로 전자상거래를 활성화시키고 국가경쟁력을 확보한다는 측면에서 매우 중요한 문제이다. 영국이 취한 top-down 방식은 제도 형성의 정합성과 자율성 그리고 시장의 흐름에 대한 민첩한 대응력 등의 장점을 갖추고는 있으나 정부의 조정이 없었던 관계로 기술 표준에 있어 다양한 형태가 나타날 수 있으며 통일화 되는 과정에서 학습비용이 발생할 가능성이 있다.

이런 점에 있어서 우리나라 정부가 공인인증제도의 정착을 위해 법률적 · 제도적 그리고 기술적 개입을 하는 것은 필요하여 보이는 데 자율경쟁과 실제의 필요에 의해 형성되어가는 시장의 흐름을 막아서서는 안 될 것이다. 정부정책도 궁극적으로는 시장의 자율적인 형성을 도

와주는 형태로 진행되어야 하기 때문이다. 장기적 관점에서는 영국이나 미국처럼 자생적인 산업이 스스로 결정하고 성장해나가는 것이 바람직한 방향으로 보이나 이러한 인증제도의 문제는 단순히 기술적인 면에서 바라다보기보다는 제도적인 측면에서 다른 국가와의 정책적 공조가 필요하며 따라서 정부기관과 협력관계가 공고한 민간기구의 설립도 고려해 보아야 할 것 같아 보인다.

V. 정책적 시사점

지금까지 신뢰서비스의 개념과 각국의 현황 및 장단점을 비교해 보았다. 전자상거래가 앞으로 미래를 만들어 나갈 필연적 밑그림이고 국가 경제의 활성화를 위해서 필수불가결한 요소라면 정부의 정책적 개입 및 의지가 필요할 것으로 보이며 이를 위해서는 신뢰서비스에 관한 정책의 전개가 필수적일 것이다. 이러한 면에서 아래와 같은 정책적 시사점을 제시해 보았다.

- 앞으로 전자상거래의 활성화가 진행됨에 따라서 신뢰서비스산업의 활성화와 다각화가 전망되므로 이에 따른 다양한 인증관련 서비스가 요구될 것으로 보이며 이를 평가할 수 있는 전문 평가승인 조직설치의 필요성이 높아질 것으로 보임.

- 정부 주도형의 평가승인 조직과 병행하여 발 빠르게 변화에 대응하고 정부의 조직과 가깝게 연계하여 변화해 나갈 수 있는 민간기관을 통하여 신뢰서비스산업의 활성화가 필요한 것으로 사료됨.

- 신뢰서비스산업이 발전됨에 따라서 전통산업별로 신뢰 서비스의 필요성이 다른 양상으로 나타날 가능성이 있으며 신뢰서비스산업 자체도 서비스가 복잡해짐에 따라 신뢰서비스산업의 분류가 세분화될 가능성이 보임으로 이에 대한 지속적인 검토와 정책적 지원이 필요할 것으로 보임.

- 인증과 관련된 국제적 협력의 움직임이 점차로 활성화되고 있는 것으로 보이며 우리나라도 이러한 움직임들을 예의 주시하고 참여해야할 필요성이 있어 보임 (예를 들면 영국에서 주도하고 있는 tScheme과 같은 움직임).

- 인증기관과 관련해서 개발되는 승인 관련 프로파일들은 수평적 통합을 염두에 둔 단순기술의 응용에 대한 평가뿐만이 아니라 상위의 개념들도 포함하여 수직적인 통합을 지향하는 총체적인 프로파일들로 개발되어야 할 필요성이 대두되고 있음.

- 신뢰서비스산업의 발전과 확장이 예상되는바 이러한 승인 관련 프로파일들은 환경의 변화에 따라 지속적으로 수정, 보완 내지는 개발될 수 있는 형태로 제도화되어야 할 것으로 보임.

- 현재는 PKI등의 인증서비스와 여타 거래 관련 서비스들 - 전자신용장이나 지불시스템 등 - 이 별개로 운영되고 있으나 신뢰서비스가 넓은 의미로 정착되기 시작하면 이러한 각종 서비스들이 통합될 것으로 사료됨.

- 신뢰서비스의 기술적이고 수평적인 통합이 상위개념들을 포함하게 되는 수직적 통합과 병행하여 진행될 가능성이 보이며 동시에 국제적인 통합과 상호승인의 움직임이 있는 바 이러한 면에서 지속적인 연구개발이 필요함.

참 고 문 헌

1. 배대현, 『정보사회와 PKI』, 계명대학교 출판부, 2001.
2. 이정현, 『주요국가의 전자서명인증제도』, 해외정보보호동향 12월호, 2002.
3. 정완용, 『전자상거래법』, 법영사, 2002.
4. Article 1.1.9 Certification Authority Guideline, Alpha version, Electronic Commerce Promotion Council of Japan(ECOM), April 1997.
5. Clause 1.1.7, Certification Authority Guideline, Alpha version, Electronic Commerce Promotion Council of Japan(ECOM), April 1997.
6. Clause 1.1.8, Certification Authority Guideline, Alpha version, Electronic Commerce Promotion Council of Japan(ECOM), April 1997.
7. D. A. Garvin, "Building a Learning Organization" Harvard Business Review, 1993.
8. Dale Neef, " The Knowledge Economy", Butterworth-Heinemann, 1997.
9. Glossary of IT Security Terminology, SD6, SC 27 N 1954, International Standards Organisation, 5 March 1998.
10. H. Cleveland, "The Knowledge Dynamic", Human Valley Books, 1985.
11. Licensing of Trusted Third Parties for the Provision of Encryption Services, Consultation Paper, Department of Trade and Industry, United Kingdom, March 1997.
12. Paul Timmers, Electronic Commerce: Strategies and Models for Business-to-Business Trading, John Wiley & Sons, 1998.
13. Statement on Secure Electronic Commerce, Department of Trade and Industry, United Kingdom, 27 April, 1998.
14. The General Usage in International Digitally Ensured Commerce(GUIDEC), International Chamber of Commerce, 1997.
15. The General Usage in International Digitally Ensured Commerce(GUIDEC), International Chamber of Commerce, 1997.

참고 웹페이지

• 우리나라

· 한국전산원 (www.nca.or.kr)

· 한국정보인증(주)(www.signgate.com)

· 한국증권전산(주)(www.signkorea.com)

· 금융결제원(www.yessign.or.kr)

· 한국전자인증(주)(gca.crosscert.com),

· 한국무역정보통신 (주)(www.tradesign.net)

· 한국과학기술정보통신위원회, 전자서명법 중개정법률안, 2001. 11. 16 (search.assembly.go.kr/law/)

· 전자정부 (www.egov.go.kr)

• 일본 경제 산업성

– http://meti.go.jp

– http://www.meti.go.jp/policy/netsecurity/digisign_ninteiitiran.htm

• 독일 연방통신우편감독청

– http://www.regtp.de/behoerde/start/fs_01.html

– http://www.regtp.de/en/(영문)

• 미국

– http://www.gsa.gov/

– http://egov.gov/

– http://www.pkiforum.org/

• 일본 특정인정업무기관 URL

– http://www.jcsinc.co.jp/

– http://www.gyosei.or.jp/

– http://www.jnotary.com/

– http://www.construction-ec.com/

– http://www.ninsho.co.jp/

– http://www.secomtrust.net/

– http://www.tdb.co.jp/

– http://www.ninsho.co.jp/

• 영국

– http://www.trustuk.org.uk/

–http://www.legislation.hmso.gov.uk/

– http://www.dti.gov.uk/cii/datasecurity/index.shtml

– http://www.tscheme.org

– http://www.cesg.gov.uk

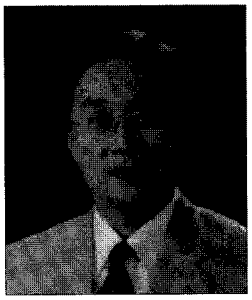
– http://www.e-envoy.gov.uk

– http://www.pki-page.org/

• Digital Signature law survey

– http://rechten.kub.nl/simone/ds-lawsu.htm

저자약력



이정우 (Jung Woo Lee)

· 1995. 8. 조지아 주립대학교 컴퓨터 정보 시스템 석사
· 1998. 12. 조지아 주립 대학교 컴퓨터 정보 시스템 박사
· 2001. 9. ~ 현재 연세대학교 정보대학원 조교수
· 관심분야 : 정보시스템 관리, 정보 품질, 중소기업 정보화, 정보시스템 부서의 역량 평가
· e-mail : jlee@yonsei.ac.kr

이종성 (Jong Sung Lee)

· 성균관대학교 정치외교학 학사
· 연세대학교 정보대학원 석사(정보통신산업 및 정책)
· 연세대학교 정보대학원 박사과정 (e-Government)
· 1981년~ 1986년 (주)워커힐 전산실대리

현재

· 연세대학교 정보대학원 정보화연구실 연구원
· 연세대학교 동서문제연구소 정보정책포럼 연구원
· 삼성경제연구소 포럼 "전자정부이야기" 총무
· 한림법학원 정보체계론 전임강사