

電子認證制度의 問題點에 관한 研究

황 상 규*

-
- I. 序論
 - II. 電子認證의 概要
 - III. 電子認證 節次과 國內外 認證서비스 動向
 - IV. 電子認證制度의 問題點과 發展方向
 - V. 結論
-

I. 序論

최근 電子商去來의 비약적인 발전에 따라 전자상거래의 安全性 確保와 消費者保護의 필요성이 중요한 문제로 대두되고 있다. 전자문서를 이용한 電子去來는 非接觸, 非對面으로 이루어지기 때문에 거래 상대방의 신원과 거래의사의 眞正性 여부를 확인하기 어렵고, 타인으로 위장하여 부정하게 사용할 위험이 존재하게 된다.

또한 전자문서는 유통되는 과정에서 爲·變造된 문서작성 사실을 입증하기 곤란할 뿐만 아니라 전송내용의 秘密維持가 어려운 점이 있다. 이와 같이 전자문서 및 전자거래가 가지는 문제점을 해소하기 위한 방안이 暗號技術을 이용한 電子署名과 認證制度이다.

거래상대방의 신원을 확인하고 전자문서의 위·변조 및 否認防止를 위하여 활용하는 것이 전자서명기술이며, 신뢰할 수 있는 제 3자(인증기관)가 거래당사자의 전자서명을 인증해주는 것이 전자서명 인증제도이다. 또한 전송내용의 비밀을 유지하기 위하여 사용하는 방안이 암호기술이다.

* 晉州國際大學校 인터넷通商學部 助教授

전자정부 시행, 전자금융거래 등에 필요한 전자서명 이용이 활성화됨에 따라 전자인증서 발급이 확대되고, 관련 인증시장이 꾸준히 증가하고 있는 추세이다.

우리나라는 1999년 電子署名法을 제정한 이후 2001년말 개정을 통하여 2002년 4월부터 앞으로의 전자서명 및 認證技術의 발전추세에 대비하여 보다 다양한 기술을 수용할 수 있도록 전자서명의 개념을 확대하고, 국제화 시대를 맞이하여 날로 확대되는 국제거래상의 전자서명 인증문제를 해결하도록 하는 조항을 신설하는 것을 주요 골자로 하는 전자서명법이 시행중에 있다.

따라서 본고에서는 전자상거래 기반하에서의 전자인증에 대한 개념 및 필요성과 응용분야를 고찰하고 전자인증 절차 및 국내외 전자인증 서비스현황을 파악한 후, 현행 電子認證制度의 問題點과 그 發展方向을 제시하고자 한다.

II. 電子認證의 概要

1. 電子商去來와 電子認證

전자거래는 전자적 기법의 도입에 따라 서면거래와는 다른 특성을 나타내고 있다. 서면거래는 진정성(Authenticity), 무결성(Integrity), 부인봉쇄(Nonrepudiation), 서면작성(Writing)과 기밀성(Confidentiality)을 요건으로 하는 것이 보통이다.¹⁾

이러한 특성은 전자적 환경에서는 많은 변화를 초래한다. 전자상거래를 구현하기 위해서는 다양한 기술이 활용된다. 이 가운데 전자상거래가 확산될수록 그 역할과 관심이 더욱 증대되는 분야가 보안기술이라 하겠다.

전자상거래에 관련된 보안은 시스템, 네트워크, 소프트웨어 등 다양한 측면에서 논의될 수 있으나 안전한 상거래라는 측면에서는 電子署名(Digital Signature) 및 電子認證(Certification) 기술이 대표적이다.

전자인증제도가 도입될 당시에는 핵심기술인 공개키암호화기술(PKI)을 이용한 디지털서명에 한정하여 전자서명을 규정하고 있었다. 그러나 최근 전자서명 기술이 발달함에 따라서 디지털서명뿐만 아니라 指紋認識, 홍채인식, 수기서명

1) 黃希哲, 電子署名과 法律問題, 2000.12, p.3.

측정기술 등 새롭고 다양한 기술이 개발되어 전자서명에 활용될 가능성이 높아지게 되었다.

여기서 문제가 되는 것은 전자서명이 유효하기 위해서는 전자서명키와 그 키를 소유한 사람이 일치하여야 하며, 이것을 해결하기 위하여 신뢰받는 제 3자로 하여금 이들의 신원을 입증하게 함으로써 해결하여야 하는데 이러한 행위를 認證이라고 하고, 인증을 담당하는 기관을 인증기관(Certification Authority)이라고 하며, 인증기관을 가입자의 신원정보와 전자서명검증키가 포함된 인증서를 발행하게 된다.

결국 전자인증제도라는 것은 전자거래나 전자신청에 있어서 거래 또는 신청의 상대방을 특정함과 동시에 전자거래 또는 전자신청 당시에 관련된 電子情報의 작성자가 그 특정된 본인 또는 회사인가, 또 상대방이 회사인 경우에 그 대표자가 회사의 대표권을 가진 자인가 등에 관하여 증명권한을 가진 인증기관이 증명하는 것을 말한다.

따라서 이러한 인증기관은 그 신뢰성이 보장되어야 하고, 손해배상 등의 문제해결에 관한 규정이 결여되어 있으므로 損害賠償에 필요한 자금력과 신뢰성에 필요한 전문적인 인력과 정보 등을 갖추고 있어야 하며, 이를 위해 전자서명법에서는 공인인증기관의 설립 등에 관하여 규정하게 되었다.²⁾

2. 電子認證의 意義

전자인증은 거래에 참여하는 각 개체끼리 서로 상대방의 신분을 확인할 수 있도록 하는 기능으로 送信者와 受信者가 합법적인 사용자임을 증명하고, 전자서명 검증키가 자연인 또는 법인이 소유하는 전자서명 생성키에 합치한다는 사실을 확인·증명하는 行爲를 말한다.³⁾

즉 기술적으로 어떤 사람의 전자서명 검증키가 그 사람의 것이라는 것을 신뢰할 만한 제 3자 또는 제 3의 기관이 증명해 주는 것을 말한다. 또한 전자인증체계는 전자상거래의 安全性과 信賴性을 확보하기 위한 핵심기술인 전자서명기술의 안전한 운영을 위한 체계를 의미하는 것으로 현재 사용되는 전자인

2) 이정현, 주요국가의 전자서명인증제도현황, 해외정보동향 12월호, 2002.12. p.2.

3) 전자서명법 제 2조의 용어정리.

증기술은 공개키암호방식⁴⁾을 따르므로 PKI(Public Key Infrastructure) 즉 공개키기반구조를 의미한다.

전자인증은 정보의 정당성·완전성을 확보하기 위한 기술이다. 암호는 정보의 은폐를 목적으로 하는 반면 전자인증은 정보가 변경되지 않은 것을 확인하는 것을 목적으로 한다. 전자인증 자체는 암호와는 독립된 개념이지만 暗號技術을 사용함으로써 그 안전성·신뢰성을 보장한다. 인증은 정당성을 나타내야 할 대상에 따라서 메시지 인증, 사용자 인증, 단말인증, 시각인증 등으로 나뉜다.⁵⁾

일반적으로 메시지의 작성자가 자신이 그 발신자임을 나타내기 위한 전자적 데이터를 전자서명이라 부르는데 이 전자서명에 의한 인증을 사용한 制度的·法的인프라는 현재 세계적으로 급속히 정비되고 있는 추세이다.

아래의 [표-1]은 주요국가의 전자서명 인증제도에 대한 입법례를 비교분석한 것이다. 국가마다 인증기관에 대한 규제 및 법적효력 및 업무범위를 각각 달리하고 있음을 알 수 있다.

4) 공개키암호방식은 뱃색(Knapsack), 클리크(Clique), 부울대수, 모듈수학(Modular Arithmetic) 등 고도의 수학적인 이론을 응용하여 개발된 암호화방식으로 1976년 Diffie와 Hellman이 공개키 개념을 제안하였으며, Merkle와 Hellman은 뱃색방식을 개발하였다.

5) 안중호, 전자인증기술 및 서비스, 서울대학교 전자상거래지원센터, 2000.8. pp.12-13.

[표-1] 주요국가의 전자서명 인증제도 입법례 비교

| 입법례 | 인증기관에 대한 규제 | 법적효력 및 업무범위 | 비고 |
|------------------------|---|--|----------------------------------|
| 한국 전자서명법 | 요건을 구비한 인증기관을 공인인증기관으로 지정(공인인증기관지정제도) | 공인인증기관이 인증한 전자서명에 전자서명법상의 효력부여 | |
| 미국 연방법 | 규정없음 *초기 주법에 허가제도를 규정하였으나 후발주들은 등록제 등 완화된 제도 채택 | 모든 전자서명에 대해 법적 효력 인정(*주법에서 제한) | 구체적인 사례에 따라 상이한 법적 효력 부여 |
| 독일 디지털 서명에 관한 법률 | 법에서 정한 요건을 구비한 인증기관이 주무관청에 신고, 주무관청의 확인후 확인필증 수여(임의적 공인인증기관 인정제도) | 규정없음 *개정민법에서 공인전자서명의 서명으로서의 효력을 인정(독일민법 제126조A) | 법으로 정하지 않은 전자서명인 경우에는 그 이용의 임의적임 |
| 영국 전자통신법 | 인증기관에 관한 규정없음(자율적 비영리기구인 tScheme에 의한 자발적인 승인시스템으로 운영) | 전자서명, 전자서명의 발생, 통신방법, 서명에 사용된 프로시저 등을 증명하는 선언을 한 경우 개인의 경우에도 전자서명이 인정됨 | |
| 일본 전자서명 및 인정 업무에 관한 법률 | 요건을 구비한 자를 특정인증업무를 수행할 수 있도록 인정(특정인증업무자적 인증제도) | 본인에 의한 전자서명이 있을 때에는 전자적 기록이 진정하게 성립된 것으로 추정함 | |

[자료: 이정현, 주요국가의 전자서명 인증제도 현황, 2002.12. p.8.]

우리나라 개정 전자서명법 제 2조에서는 전자서명과 공인전자서명을 구분하여 전자서명이란 署名者를 확인하고 서명자가 당해 전자문서를 서명하였음을 나타내는데 이용하기 위하여 당해 電子文書에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다 고 규정하고 있으며, 공인전자서명이란 그 요건으로서 전자서명생성정보가 가입자에게 유일하게 속할 것, 서명당시 가입자가 전자서명생성정보를 지배·관리하고 있을 것, 전자서명이 있을 후에 당해 전자서명에 대한 變更與否를 확인할 수 있을 것 그리고 전자서명이 있을 후에 당해 전자문서의 변경여부를 확인할 수 있을 것 등의 요건을 갖추고 公認認證書에 기초한 전자서명을 말한다고 규정해 둬으로써 전자서명과 공인전자서명의 효력을 달리 적용하고 있다.

전자인증은 네트워크를 통해서 데이터의 교환을 하고 있는 상대가 진정으로 본인인 것 및 데이터가 변조되어 있지 않다는 것을 확인하기 위한 것이고 전자거래의 신뢰성을 확보하는데 기본적인 요소이다.

인터넷을 통한 정보의 전달이나 電子去來가 이루어지는 상대방과 비대면 상태에서 업무를 처리하게 되므로 당사자의 신원확인 즉 진정성의 확인과 전달되는 데이터의 無缺性を 확인하는 절차가 필요하게 되는데 이러한 문제들을 해결하기 위해 가입자가 인증기관에 자신의 신원을 증명할 수 있는 자료를 제출하여 가입하면 인증기관이 전자서명생성정보가 가입자에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 電子的 情報認證書を 발급한 후 가입자의 거래 상대방에게 가입자의 신원을 확인해주거나 가입자의 전자서명생성정보에 대응하는 전자서명검증정보를 제공하는 제도가 전자인증제도이다.

2. 電子認證의 必要性 및 應用分野

일반상거래와 전자상거래의 가장 뚜렷한 차이점이라면 일반상거래는 거래당사자가 직접대면하여 서면에 의한 각종 계약 및 문서의 행위를 하는 제반업무가 컴퓨터와 같은 개체를 이용해 전자문서와 전자서명을 통해 이루어진다는 것이다.

이러한 가상공간의 환경에서는 신원사칭, 전자문서의 불법변조, 전자문서를 이용한 계약 사실에 대한 부인 등 여러 가지 문제점이 발생하게 된다. 따라서 이들 문제를 둘러싼 당사자들의 상이한 利害關係를 만족시킬 수 있는 환경의 제공이야말로 電子商去來 活性化의 중요한 관건이라 할 수 있다.

전자문서의 송·수신 당사자간의 신분확인(사용자인증), 전자문서의 변경여부의 확인(문서인증) 및 전자문서를 이용한 전자계약 수행사실에 대한 자의적 번복 거부(부인봉쇄) 등의 기본적인 保安서비스가 제공되어야 하며, 이를 구체적으로 수행할 기관이 필요한 것이다. 결국 전자상거래에서의 전자인증이란 정보의 교류속에서 전송받은 정보의 내용이 변조 또는 삭제되지 않았는지와 주체가 되는 송·수신자가 정당한지를 확인하는 방법이다. 따라서 전자인증의 필요성을 요약하면 다음과 같이 정리할 수 있다.

(1) 去來相對方의 身元確認

익명성이 증가한 정보사회에서 신원확인을 위한 기술적 방법이 바로 전자서

명이다. 전자서명은 서명한 메시지의 송신자 인증(authentication) 및 서명된 문서의 無缺性(integrity)을 立證할 수 있기 때문에 증가된 익명성에 대응하는 효과적인 기술적 수단이다. 특히 최근 들어 급증하고 있는 기업-소비자간(business-to-consumer) 전자상거래가 본격화될 경우 사전적인 관계가 없는 상황에서 전자거래가 발생하게 되므로 당사자의 신원에 대한 不確實性은 더욱 높아질 것이고, 이에 따라 디지털서명의 필요성이 증가할 것이다.⁶⁾

(2) 電子署名된 文書의 무결성 보장

무결성은 메시지 인증과 같이 메시지의 變造나 修正 등을 검출할 수 있는 기능을 말한다. 이것은 일반적으로 해쉬함수(hash function)⁷⁾나 블록 암호 등을 사용함으로써 구현 가능하다. 원본과 복사본의 識別이 불가능하고 내용을 손쉽게 변조할 수 있는 전자문서의 특성 상 기존의 인장이나 서명과는 다른 새로운 수단이 필요하게 된다.

電子署名과 認證은 전자서명된 문서가 서명자가 의도한 바로 그 문서로서, 전자문서의 生成, 流通, 보관과정 등에서 발생할 수 있는 변조가 일어나지 않았음을 입증하는 기능을 지닌다. 또한 전자화된 정보를 이용할 경우 내용을 변조하거나, 정당하게 이루어진 거래 또는 계약을 부인하는 것이 용이하므로, 이를 효과적으로 방지하여 거래당사자간의 紛爭을 최소화하고 전자상거래의 신뢰기반을 조성할 필요가 있다. 전자서명과 인증은 이러한 신뢰기반의 중요한 요소로서 작용한다.

(3) 法的 紛爭時 證據資料化

현재 이루어지고 있는 전자거래와 관련된 분쟁이 발생했을 때, 인증기관의 인증서를 법원에 제출해 거래 상대방을 증명할 수 있다. 즉, 디지털서명의 쯤

6) 신일승외1인, 전자서명 및 인증제도, 정보통신정책연구원, 1998.12, pp.25-30.

7) 해쉬기능이라 함은 데이터 값을 커다란 영역으로부터 상대적으로 조그만 범위로 압축하여 모사하는 기능을 말한다. 현재 사용되고 있는 해쉬함수는 미국국립표준기술원(NIST)이 개발한 SHA(Secure Hash Algorithm)과 RSA사에서 개발한 MDRpDUF(MD2, MD4, MD5) 등이 있다.

認封鎖(non-repudiation)의 기능을 통해 증거 자료화할 수 있다.

여기서 고려해야 할 점은 법적 분쟁 발생시의 위험배분을 위해 인증기관의 인증을 받은 문서는 진정 성립된 것으로 추정하는 규정이 존재하여야 한다는 점이다. 만약 관련법에서 위와 같은 위험배분에 대한 추정규정을 두지 않는다면, 관련법이 아예 제정되지 않는 경우, 또는 제정된다 하더라도 인증기관의 인증을 받은 문서에 대한 진정성립 추정이 없는 경우, 인증기관의 認證書를 이용한 법적 분쟁의 해소에 限界가 있기 때문이다.

현재 전자상거래를 통하여 각종 정보의 교환이 활발하게 이루어지고 있으며 정보의 發信者가 정말 본인인지 혹은 정보의 내용이 변경되지 않았는지 확인하기 위하여 인증은 여러 분야에서 이용될 수 있다.⁸⁾

1) 企業間 去來나 情報交換 등에서 이용

기업간에 이루어지는 거래나 業務情報 등을 교환하는 경우 통신상대가 정말 자기가 의도하는 상대가 틀림없는지 혹은 정보의 내용이 변경되지 않았는지 인증을 이용하여 확인한다.

2) 企業內的 決濟나 情報交換 등에서 이용

기업이 회사 내의 결제나 정보교환을 하는 경우 정말 그 권한을 갖는 사람이 행사하고 있는지, 그리고 그 내용이 변경되지 않았는지를 인증을 이용하여 확인한다.

3) 消費者에 대한 販賣에 이용

네트워크 상에서 가상 점포를 개설하고 소비자에 대한 서비스나 판매를 한다든지 각종 정보를 제공할 때 그 고객이 본인인지 확인하는 것이나 주문의 내용을 확인하는데 認證을 이용한다. 그리고 소비자 측도 가상점포가 정말 존재하는지 아닌지를 확인할 때에 인증을 이용할 수 있다.

4) 金融서비스에 이용

8) 한국전산원, 인증체계분석 및 동향보고, 1998.5.

金融機關이 네트워크 등을 사용하여 고객으로부터 송금, 계좌이체 등의 주문을 받았을 때 인증을 이용하여 그 고객이 본인인지를 확인하고 상호간에 去來事實 및 內容을 확인한다.

5) 遠隔醫療에 이용

의료기관이 네트워크 등을 통해서 환자를 진단하는 원격의료서비스에서 의료기관이 환자를 확인하거나 또는 환자측이 의사의 자격유무를 확인하는데 이용한다.

6) 電子公證에 이용

금후 전자적으로 작성된 계약서 등이 특정인에 의해서 진정으로 작성됐는지 공증하거나 전자적인 형태로 증명서를 작성하여 이들 전자문서를 보존하고 그 존재, 내용 등을 증명하는 전자공증제도가 도입될 것으로 예상되는데 이러한 전자공증에 있어서도 공증을 신청하는 사람을 확인하거나 내용을 확인하는데 전자인증을 이용할 수 있다.

7) 行政手續에 이용

행정기관에 대하여 각종 신청서나 증명서의 교부를 네트워크를 통해서 행할 때 신청자의 확인이나 신청내용을 확인하는데 이용한다.

8) 그 외의 이용

개인간에 전자메일 등을 교환할 때 인증을 이용하여 상대방을 확인하거나 통신내용을 확인한다

Ⅲ. 電子認證節次와 國內外 認證서비스 動向

1. 電子認證節次

인증은 기술적으로는 어떠한 사람의 전자서명검증키가 그 사람의 것임을 신뢰받는(trusted) 제3자의 기관이 증명해주는 것을 의미한다. 이러한 의미에서 인증기관은 기존의 인감에 대한 印鑑證明機關, 인증서는 인감증명서 등에 해당된다고 이해할 수 있다. 그러나 수기서명에 비해 전자서명의 운용이 차이가 나는 것처럼 인증기관 인증서의 운용도 차별화된다.

인증을 받기 위해서, 사용자는 먼저 자신의 전자서명생성키(비밀키) 및 전자서명검증키(공개키)를 생성한다. 두 번째 단계로 사용자는 인증기관을 방문하여 자신의 신원을 증명하고, 전자서명검증키(공개키)를 제시하며, 전자서명검증키에 대응한 전자서명생성키(비밀키)를 소유하고 있는 사실을 제시한다. 세 번째 단계로 인증기관은 전자서명검증키(공개키)와 그 키에 대응하는 사람의 신원을 확인한 경우, 신원이 확인되면 認證書(certificate)를 발행한다.⁹⁾

여기서 인증서란 공개키와 신원이 증명된 사람과의 관계를 증명하는 전자적인 기록으로, 인증서에는 인증기관, 가입자, 가입자의 전자서명검증키 등의 정보를 포함하고, 인증기관의 서명을 붙이는 것이 보통이다.

네 번째 단계로 인증기관은 가입자에게 인증서의 내용을 확인시키고, 인증기관은 認證管理體系를 통해 인증서를 모든 사람에게 접근 가능한 형태로 유지한다. 여기서 인증기관이 관리하는 인증관리체계에는 취소 또는 정지된 인증서의 목록이 포함되어야 한다.¹⁰⁾

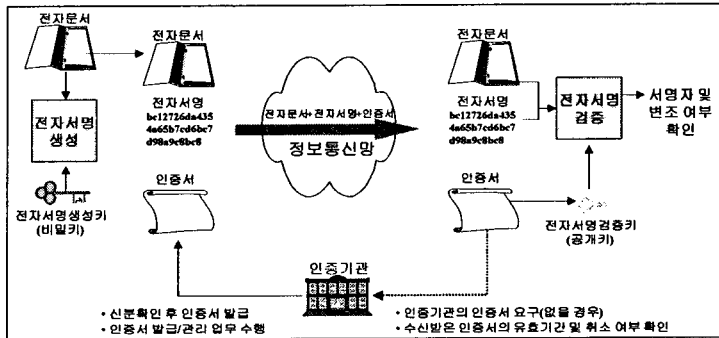
인증기관에서 인증서를 발급받으면 그 인증서를 메시지와 메시지의 전자서명에 첨부하여 송신하게 된다. 이때 수신자는 먼저 인증서를 인증기관의 전자서명검증키(공개키)를 이용하여 풀어서 송신자의 전자서명검증키를 얻고, 이

9) 구체적인 절차는 인증기관 및 인증서의 종류에 따라 달라질 수 있다. 예를 들어 Verisign Class 1 인증서의 경우는 신원증명을 e-mail 주소로 대신하여 직접 방문을 하지 않아도 된다.

10) 이를 인증취소목록(CRL : Certification Revolution List)이라한다

인증서가 認證取消目錄에 포함되어 있는지의 여부를 확인한 후, 그렇지 않은 경우 송신자의 검증키를 이용하여 메시지요약을 생성한다. 이상과 같이 인증서를 이용한 電子署名의 體系圖를 살펴보면 다음의 그림과 같이 나타나게 된다.

[그림-1] 인증서를 이용한 전자서명 체계도



2. 國內 認證機關 및 認證書 發給現況

(1) 公認認證機關 現況

1999년 7월 발효된 전자서명법상의 공인인증기관 차격 요건을 갖추고 실질 심사를 통과하여 정통부로부터 지정을 받은 기관에 한하며 2003년 1월 현재 6개 公認認證機關으로 지정되어 있다.

이중 4개기관은 인증사업을 부대사업으로 하고 있는 特殊資格의 인증기관으로 금융결제원, 한국무역정보통신, 한국전산원, 한국증권전산 등이 이에 해당한다. 그러나 전자서명 관련법령에 의거 최저자본 80억원 이상의 자본을 출자하고 실제로 인증사업 전문으로 설립된 인증기관은 현재 한국전자인증과 한국정보인증 두 군데뿐이다.

위와 같이 금융결제원과 같이 특수 목적으로 설립된 기관이 인증사업을 부가적으로 겸업하는 인증서비스 사업을 “特殊認證機關”으로, 인증서비스 전문으로 설립된 일반 사업자를 편의상 “一般認證機關” 또는 “專門認證機關”으로 구분하기로 한다.

[표-2] 국내공인인증기관 현황

| 분류 | 공인인증기관명 | 설립 일자 | 고유업무영역 | 공인지정 | 특성 |
|----|----------|----------|----------|---------|-----------------------|
| 일반 | 한국전자인증 | 1999.3 | 전문인증서비스 | 2001.11 | 일반법인 자기자본280억 원 |
| | 한국정보인증 | 1999.7 | 전문인증서비스 | 2000.2 | 일반법인 자기자본220억 원 |
| 특수 | 금융결제원 | 1989.11 | 은행간결제 | 2000.4 | 비영리기관 |
| | 한국무역정보통신 | 1991.12 | 무역EDI서비스 | 2002.3 | 한국무역협회 자회사 |
| | 한국전산원 | 1987.1 | 표준화정책기관 | 2001.3 | 국가기관 |
| | 한국증권전산 | 1977.9 | 증권업무위탁 | 2000.2 | 증권사투자법인 |

[자료 : 김정, 인증제도의 이용실태와 문제점, eBizKorea, 2003.5.]

2) 公認認證書 發給現況

공인인증기관들이 지정되기 시작한 2000년 2월 이후부터 2002년 말 현재 개인인증서 437,6만건과 법인인증서 55,7만건을 합하여 총 500만건에 육박하는 공인인증서를 발급하였으며, 이용자수로는 577만명을 상회하고 있다.

個人認證書 부문을 보면 인터넷뱅킹용이 360만건으로 84%를 점유하고 있으며 사이버증권은 현재 25만건에 불과하나, 3월부터 공인인증서를 적용하도록 되어 있어 현재 300만명에 가까운 온라인 증권사용자 중 상당수가 인증서를 사용하게 될 것으로 보인다.

이에 전자입찰조달에 4만명, 국세신고에 1,9만명, 교육공무원용 38.6만명 등이 주요 사용처로 나타나고 있다.

법인인증서의 주요 사용분야는 총 55.7만건 중 인터넷뱅킹용이 28.9만건(52%), 조달청, 공공기관 및 기업 등에서 실시한 전자입찰/조달을 위한 목적으로 21.4만건(38%)이 차지하고 있으며, 나머지는 電子稅金計算書 發行用, 國稅

申告, 教育情報用 등의 분야에서 활용되고 있다.

[표-3] 이용분야별 발급 및 이용자 현황

| 이용분야 | 서버 | 개인 | 법인 | | 계 | | 이용자 비율(%) |
|-------------|-----|-----------|---------|-----------|-----------|-----------|--------------|
| | | | 발급 | 이용자 | 발급 | 이용자 | |
| 인터넷 뱅킹 | 32 | 3,669,833 | 289,883 | 385,580 | 2,959,748 | 4,005,445 | 70.25% |
| 사이버 증권 | 57 | 250,154 | 2,464 | 9,364 | 252,675 | 259,575 | 4.49% |
| 인터넷 보험 | 32 | 6,092 | 150 | 750 | 6,274 | 6,874 | |
| 전자입찰/조 달 | 13 | 40,945 | 214,160 | 823,212 | 255,118 | 864,170 | 14.97% |
| 국세신고 | 2 | 18,938 | 7,877 | 35,119 | 26,817 | 54,059 | 0.93% |
| 국고채 매매 | 2 | 756 | 108 | 410 | 866 | 1,168 | |
| 쇼핑. 지로등 | 110 | | | | 110 | 110 | |
| VPN | | | 737 | 1,474 | 737 | 1,474 | |
| 전자지불 | 57 | | | | 57 | 57 | |
| 전자의료 | 5 | 455 | 2,579 | 9,800 | 3,039 | 10,260 | |
| 전자세금 | 32 | 67 | 20,051 | 78,615 | 20,150 | 78,714 | 1.36% |
| 전자여신 | 3 | 65 | 405 | 1,539 | 473 | 1,607 | |
| 전자문서/계 약 | 11 | 924 | 6,501 | 24,705 | 7,436 | 25,640 | |
| 전자민원 | 4 | 92 | | | 96 | 96 | |
| 전자무역 | | 8 | 67 | 201 | 75 | 209 | |
| 카드업무 | 7 | | | | 7 | 7 | |
| 공공/교육정 보 | 17 | 386,613 | 12,574 | 25,149 | 399,204 | 411,779 | 7.13% |
| E-mail용 | | 1,261 | | | 1,261 | 1,261 | |
| 계 | 84 | 4,376,203 | 557,556 | 1,395,918 | 4,934,143 | 5,772,505 | 99.13 |

[자료 : 김정, 인증제도의 이용실태와 문제점, eBizKorea, 2003.5.]

[표-4] 인증기관 연도별 인증서 발급현황

| 기관명 | 2000년도 | | | 2001년도 | | | 2002년도 | | |
|----------|--------|-------|--------|--------|---------|-----------|--------|---------|-----------|
| | 서버 | 법인 | 개인 | 서버 | 법인 | 개인 | 서버 | 법인 | 개인 |
| 한국정보인증 | 23 | 1,373 | 4,288 | 113 | 46,412 | 28,823 | 94 | 76,315 | 177,137 |
| 한국증권전산 | 7 | 6,964 | 1,712 | 34 | 71,178 | 11,124 | 101 | 127,165 | 265,512 |
| 금융결제원 | 8 | - | 12,470 | 81 | 83,871 | 1,253,903 | 166 | 291,166 | 3,546,841 |
| 한국전산원 | - | - | - | - | 5,996 | - | 19 | 49,378 | 386,613 |
| 한국전자인증 | - | - | - | - | - | - | 4 | 13,249 | 92 |
| 한국무역정보통신 | - | - | - | - | - | - | - | 283 | 8 |
| 계 | 38 | 8,337 | 18,470 | 228 | 207,457 | 1,293,850 | 384 | 557,556 | 4,376,203 |

[자료 : 김정, 인증제도의 이용실태와 문제점, eBizKorea, 2003.5.]

3. 國內外 認證서비스 現況

(1) 國外認證서비스機關 現況

대표적인 인증서비스 제공업체인 美國의 VeriSign의 경우, 인증서비스 시장의 초기 진출로 시장 선점의 이점을 누리며 빠른 성장세를 보이고 있고, 이미 일본과 유럽에까지 사업을 확장하고 있다. 또한 여러 종류의 인증 솔루션을 생산하고 있는 캐나다 Entrust의 경우, 1994년 처음 사업을 시작한 이래 매년 2배 이상의 빠른 成長勢를 보이며 전자상거래의 기반이 되는 다양한 인증 솔루션을 제공하고 있다.

① VeriSign

외국의 여러 인증기관들 중 인증서비스 시장에서 가장 높은 시장 점유율(약

70%)을 보유하고 있는 VeriSign의 사업내용을 살펴보면, 개인용 디지털 인증서 發給·管理, 서버용 디지털 인증서 발급·관리, VeriSign OnSite, V-Commerce, SET 등과 같은 기업용 인증시스템제품 및 서비스, 기타 소프트웨어 정품 인증서비스 및 고객 교육과 컨설팅 서비스가 있다.¹¹⁾

개인용 디지털 인증서는 대부분 무료이기 때문에 현재 VeriSign의 가장 큰 수입원은 서버용 디지털인증서 발급·관리부분인데 향후 전자상거래 시장이 급속히 성장할 경우 기업용 인증시스템의 판매 및 관련 서비스 제공 부분이 크게 성장할 것으로 예측된다.

② ID Certify

ID Certify는 워싱턴 주 정부 최초의 공인인증기관으로서 1998년 4월 지정되었다. ID Certify는 가입자에게 스마트카드를 제공함으로써 사용자의 전자서명 생성키를 스마트카드에 보관하도록 한다. 현재 미네소타주의 의료 및 보건 부문에 관련된 인증서비스를 제공중이다. ID Certify는 저장소(Repository)서버를 캐나다 밴쿠버에 두고 있으며 RA(Registration Authority)를 관련 업체에게 제공하는 방식으로 운영된다.

③ GTE의 Cybertrust

통신사업자인 GTE가 설립한 CyberTrust는 CA를 운영하기 위한 하드웨어와 소프트웨어를 제공하여 쉽게 인증시스템을 구축할 수 있도록 하는 사업과 함께 직접 인증서비스를 제공하고 있다. CyberTrust의 CA시스템은 SET의 상위레벨의 CA로 운영하기 위해 MasterCard가 선택한 제품이다.

④ Thawte Consulting

Thawte Consulting은 남아프리카의 온라인 서비스와 製品市場을 겨냥하여 1995년 창립된 회사로 현재 온라인 보안 및 정보보호분야에서 세계적인 제품 및 서비스 제공업체로 성장하였다. Thawte가 제공하고 있는 제품과 서비스에는 인증서 발급서비스, Extranet인증서비스, CA의 인증서비스 등이 있다.

11) 신일순·김춘아, 인증서비스사업의 발전동향과 우체국의 대응방향, 정보통신정책연구원, 1999.6.15.

⑤ NetDox

NetDox는 회계감사 부문의 세계적인 기업인 Deloitte & Touch LLP와 Thurston Group Inc.이 공동으로 1996년 설립한 회사로 Dox(Digital Box)를 이용하여 송·수신상에 특별히 보안이 요구되는 전자메시지의 경우 누가, 언제, 누구에게, 어떤 메시지를 보냈는지 등에 대한 상세하고 확실한 인증서비스를 DoxIt라는 이름으로 제공한다.

(2) 國內認證서비스 産業現況

현재 우리나라의 경우 거래 당사자의 身元 確認 및 거래의사의 진정성을 확인해주는 신뢰받는 제 3자로서의 정식으로 상용인증서비스를 제공하고 있는 認證機關은 다음과 같다.

① 한국정보인증(주)

한국정보인증주식회사는 인터넷 거래의 안전성과 신뢰성을 확보하기 위하여 첨단 전자서명 기술을 기반으로 공인인증서비스를 제공하는 국가지정 제1호 公認認證機關이다.

사이버 공간의 인터넷 전자거래에서 당사자의 신원을 보증하기 위하여 현실세계의 印鑑證明과 같은 기능을 하는 電子印鑑을 발급하고 관리하는 회사로서 1999년 7월에 시행된 電子署名法에 의거하여 고도의 안전성과 신뢰성을 보유한 인증시스템(SignGATE)을 구축하여 전자상거래에 있어 필수적이라 할 수 있는 인증서 발급 서비스를 제공하기 위하여 한국통신, 삼성SDS, SK텔레콤, LG 인터넷 등 국내 굴지의 기업들이 공동 출자하여 설립된 회사입니다. 국가 지정 제1호의 공인인증기관으로서 인터넷상에서의 각종 거래에 따른 신원확인 과 이에 대한 보증, 각종 사고 發生時 법률적으로 보호받을 수 있는 보상체계를 갖추고 있다.

② 한국증권전산(주) 공인인증센터

SignKorea는 한국증권전산이 운영하는 공인인증센터로서, 안전한 인터넷 전자거래에 필수요건인 신원확인/기밀성/ 무결성/부인방지를 보장하기 위한 고도의 電子署名技術을 기반으로 하며, 국가가 보증하는 공인인증서비스를 제공하는 공인인증기관이다.

공인인증서비스 이용의 가장 큰 특징은, 공인인증서비스를 이용한 거래는 법적인 보호를 받을 수 있다는 데 있습니다. 즉, 공인인증기관이 인증한 전자서명은 법령이 정하는 기명날인 또는 서명과 동일한 法的效力과 證據力이 있다.

SignKorea는 정부가 지정한 공인인증기관으로 공인인증서비스의 수행에 필요한 재정적 능력을 갖추고 있으며, 전자서명법 제26조(배상책임)에 의거 가입자와 이용자에 대해 SignKorea의 업무착오 및 과실에 의한 피해에 대비하여 保證 및 賠償保險에 가입하고 있으며, 향후 인증서 종류 확대, 시점확인 서비스 등 인증서가 사용되어질 수 있는 모든 분야에 전자서명을 적용하며, 더 나아가서는 일반적인 情報保護事業으로까지 영역을 확대할 예정이다.

③ 금융결제원

정보통신기술의 급속한 발달과 정보통신망 확산으로 사이버 뱅킹, 전자상거래, 전자자금이체, 행정 민원, 企業間 電子商去來 등 전자문서를 이용한 전자거래가 증가하고 있다. 그러나, 전자거래는 거래당사자와 대면거래가 아닌 통신망을 통한 거래이기 때문에 거래당사자의 신원 및 거래내용의 위·변조 여부 확인이 불가능하고 거래한 사실에 대한 부인방지 등에 곤란한 문제가 있다.

이같은 문제점은 실제 印鑑과 동일한 효력이 있는 전자서명(Digital Signature)을 사용하여 전자문서를 송·수신함으로써 해결할 수 있다. 전자서명은 암호기술을 이용하여 생성되기 때문에 사이버상의 전자거래에 안전하게 사용할 수 있다. 公認認證機關(CA: Certification Authority)은 전자서명의 주인과 전자서명에 사용하는 키(Key)의 관계를 객관적으로 검증한다는 전자증서인 공인인증서(Certificate)를 발급하는 기관으로 인감증명서를 발급하는 기관과 같은 역할을 한다.

Ⅲ. 電子認證制度 問題點과 發展方向

1. 現行 電子認證制度의 問題點

(1) 市場의 公正性 및 競爭力 確保問題

전자서명법이 제정된 이래 정부는 지난 3년간 공인인증서 확산을 위해 다각적인 노력을 기울여 왔으며, 2002년까지 1천만명이 사용자 확보라는 목표를 세우고 매진하여 2002년말 500만명 이상의 사용자를 확보하였다.¹²⁾

이렇게 된 배경에는 기존의 은행에서 인터넷뱅킹 신청을 하였거나 사설로 발급된 인증서를 가지고 있는 고객으로 하여금 공인인증서로 전환하는 형태로 하여 단기간에 급속히 확산될 수 있었는데, 이 과정에서 일부 특수 인증기관이 인증시장을 독과점하는 결과가 초래되기도 하였다.

또한 3월부터 적용된 사이버 證券分野에서 300만명의 온라인 증권사용자를 대상으로 모든 증권사는 한국증권전산만을 위한 인증서발급을 등록 및 대행하고 있으며, 당분간 상호연동에서 제외하여 증권전산 인증서 보급에 주력하고 있는 실정이다.

이와 더불어 자신들이 발급한 인증서를 無線分野, 法人認證書 등 금융 및 증권 이외의 나머지 분야로 확산시키면서 사실상 인증시장 전체를 지배할 수 있는 위치에 서게 되었다.

이는 우리나라 인증시장의 발전을 저해하는 가장 큰 문제로 부각되고 있다. 공인인증 시장의 대부분이 일부사업자에게 독점되면 나머지 사업자들은 공인기관으로서 역할이 유명무실하게 된다. 이는 당초 인증서 보급단계에서 사실상 분할된 시장규모가 사업자간의 지나친 不均衡을 초래하였다.

이렇게 되면 개인인증서 시장은 사실상 2개의 특수기관이 90%이상을 점유하면서 시장 불균형 현상이 가중될 것이다. 현재의 獨寡占的 市場 불균형 현상이 가중될 것이다. 현재의 독과점적 시장 지배를 바로 잡는 유일한 길은 인증

12) 김정, 인증제도의 이용실태와 문제점, eBizKorea, 2003.5. p.90.

기관간 시장균형을 회복하는 처방을 긴급하게 시행하고 궁극적으로는 시장을 공정한 경쟁체제로 전환하는 것이다.

(2) 消費者 中心 認證서비스 效率성과 品質改善 問題

우리나라 공인인증서비스가 단기간 내 1천만명을 넘는 사용자를 대상으로 범국민적으로 확산되면서 사용자 관점에서의 인증 서비스 안정성은 물론 便宜性和 經濟성을 비롯한 效率性 차원에서 인증 서비스의 질적 개선을 위한 노력이 절대적으로 요구된다.

그러나 소비자 관점에서 우리 공인 서비스의 실상을 좀 더 냉정하게 살펴보면 현재 공인 서비스에는 인증상품으로서의 개념이 아주 미흡하다. 최근까지 공인인증서가 무료로 배포되면서 상품으로서의 개념이 거의 발전되지 못한 것이다.

금년부터 서비스 有料化가 급진전되면 시장에서 소비자는 당연히 상품으로서의 가치를 보고 상품을 선택하게 될 것이다. 인증서비스는 돈을 주고 사용하는 소비자의 선택에 따라 발전하여 나간다는 측면에서 시장 중심의 체계적 서비스 모델 정립이 필요하다.

(3) 國家 電子認證서비스 體系의 一貫性維持問題

우리나라 전자인증 관리체계는 1999년 도입된 전자서명법에 의거한 인증관리체계와 2001년 도입된 電子政府法에 의거한 인증관리체제로 나뉘어 관리되고 있다.

전자서명법에 의거한 인증관리체계는 주로 민간섹터와 공공섹터를 관할하여, 이는 공인인증기관이 중심이 되어 서비스가 제공된다. 한편 전자정부법에 의거한 인증관리체계는 정부섹터를 관리하고 있는데 이는 주로 정부기관에 의하여 서비스가 제공된다.

금년도에는 민간부문의 공인인증서비스 범국민적으로 확산되는 동시에 전자정부의 對國民 民願서비스가 본격적으로 보급되는 올해, 전자서명법과 전자정부법으로 이원화된 법 체계를 균형과 조화를 이루는 범국민적 차원에서의 인증서비스로 변화시켜야 하는 시점이다.

(4) 國內市場 成長 한계극복 및 國際競爭力 確保

국내인증시장의 향후 성장 규모를 전망해 보면 국내인증시장은 지난해 말 현재 100억원 규모로 12억불 규모의 世界市場 對比 1%수준인 것으로 추정되고 있으나, 2005년경에 1,600억원 규모로 가파른 성장을 거듭하여 세계시장의 6%를 넘는 22억불 수준으로 발전할 것으로 보인다.

그러나 2005년이 지나면 국내 인증시장은 급격히 성장 한계에 직면하리라 예상된다. 세계인증시장은 인터넷이용자 인구 대비 인증서 숫자가 꾸준히 늘어나는 추세인 반면 國內認證市場은 유무선 인터넷이용자 인구 3,000만명 중 70%가까운 숫자가 인증서비스를 이용하게 되는 2005년이 지나면 성장세가 급격히 둔화될 것으로 전망되고 있기 때문이다.

따라서 우리나라 인증시장의 조기포화상태에 따른 인증시장의 조기노화현상에 대비하는 전략이 필요하다.

(5) 國際認證機構의 問題

현재 인증과 관련하여 깊은 관심을 표명하고 있는 전자상거래 및 국제무역 기구들에게는 UN산하의 UNCITRAL ICC, WTO 등이 있으며, 이들 관련기구들은 여러 형태의 초안(Draft), 지침서(Guideline) 및 모델법(Model Law) 등을 통하여 여러 가지 대안을 제시하고 있다.

이들 관련 기구에서 認證과 관련된 많은 관심을 보이는 이유는 여러 가지 있겠지만 電子商去來에서의 인증관련 중심기구로서 그 역할을 수행할 경우 가질 수 있는 기구의 위상과 경제적 이익 등과 그 가운데 하나가 될 것으로 생각된다.

이러한 문제와 관련하여 이들 기구 가운데 어떤 한 기구가 인증 담당 주체 기구가 되어야 하는가 또는 관련 당사자들이 새로운 형태의 기구를 출범시킬 것인가라는 문제가 제기된다.¹³⁾

(6) 認證機關의 體系와 適格性

디지털서명에 관한 認證機關을 어떻게 설정할 것인가가 문제이다. 우리나라

13) 이호건외2인, 글로벌 전자상거래를 위한 인증체계, 통상정보연구 제2권 제2호, 2000.12.15, pp.15-178.

와 같이 전자서명의 시장이 좁은 경우에 인증기관의 난립은 非經濟, 情報管理體系의 不實, 暗號化技法의 導入에 따른 외화낭비 등 여러 가지 문제가 초래될 것으로 보인다. 따라서 인증기관의 체계와 적격성이 문제가 된다.

인증기관의 체계에 관하여는 단계적으로 인증기관을 두고 인증기관 상호간에 인증서를 발급하는 일반적 계층구조, 최상위 인증기관으로부터 단계적으로 인증서를 발급하는 단계적 계층구조, 공개키사용자가 최초의 단계에서만 공개키를 일정한 조건하에 보유하고 순차적으로 일정한 조건하에 신뢰를 하되 인증을 하지는 않는 순차적 제한모델 등의 기본적 인증기관 모델이 고안되고 있다.

우리나라의 경우에는 어떠한 인증기관체계가 타당할 것인가? 인증기관에 관하여 다단계의 계층구조를 취하는 경우에는 非能率과 浪費가 초래되고, 병렬적 인증기관 상호간에만 인증서를 발급하게 하는 경우에는 인증의 신뢰성이 문제가 될 것이다. 따라서 몇 단계의 인증기관체계를 설정할 것인가, 인증기관의 신뢰성을 확보하기 위하여 어떠한 방법을 사용할 것인가 등이 앞으로 검토되어야 할 과제라고 할 것이다.

(7) 認證關聯當事者의 責任問題

전자거래는 비대면거래라는 특징 때문에 진정성 확보와 무결성 확보 그리고 상대방의 부인에 대한 대응에 대해 곤란한 문제가 발생한다. 즉 거래상대방이 현실적 존재유무 및 사칭, 電子文書의 變造, 偽造 등의 문제가 발생한다. 따라서 이러한 문제는 결국 전자인증을 활용한 공인인증기관에서 해결된다.

이러한 공인인증기관이 발행한 공인인증서에 의한 공인전자서명은 법령에서 정하는 서면요건을 확보하는 것으로 규정하고 있지만 전자서명법개정을 통해 그동안 논란이 되어 왔던 공인전자서명 외의 전자서명이 당사자간의 약정에 따른 서명, 署名捺印 또는 記名捺印으로서의 효력을 갖게 되었다.

그러나 전자인증과 관련한 인증관련당사자들의 법적 의무와 책임에 관해서는 국제적인 통일규정이 없을 뿐만 아니라 국내에서도 거의 논의된 바가 없는 실정이다.

따라서 인증기관 및 인증서비스관련당사자가 취급하는 데이터에 기인해서 예상되는 사고, 원인, 피해를 분석하고 그 중요한 사고에 대해 인증기관 및 이용자에게 어떠한 책임이 발생하는가에 대한 논의가 이루어져야 할 것이다.¹⁴⁾

(8) 國家間 電子認證書의 相互認定問題

글로벌 전자상거래는 국내에서만 이루어지는 비즈니스가 아니라, 국가간에 이루어진다는 점에서 보안 및 인증의 중요성은 크게 부각되고 있다. 그러나 각국의 認證體系는 서로 상이하며, 정책 및 법제, 그리고 기술적 환경과 비즈니스적 관계 또한 매우 상이하다고 할 수 있다. 기술적인 측면이나 정책적인 측면의 상호연동을 위한 기반확보와 함께 법적인 측면에 있어서 서로 다른 국가간의 전자서명 및 인증제도에 대한 法的 效力을 부여 하기 위해서는 국가간의 상호인정 협정 체결이 요구된다.

2. 向後 發展方向

앞으로 전자인증분야는 다양한 전자서명 관련기술의 발전 및 다양한 분야로의 전자서명 상용화가 촉진될 것으로 전망된다. 또한 전자거래 이용자의 보호 책임을 명확히 함으로써, 信賴性과 安全性 確保를 통한 국내외 전자거래 시장의 확대도 긍정적인 효과를 미칠 것이며, 또한 국경없는 전자거래의 특성에도 불구하고 명확한 원칙이 없었던 외국의 전자서명과 인증서에 관한 相互連動問題가 적극적으로 논의될 것으로 생각된다.

그러나 국내의 전자서명제도는 아직까지 걸음마 단계에 지나지 않으며, 전자서명이용의 가속화를 위해서는 전자서명이 이용가능한 시장의 활성화와 정부의 정책적 시책이 뒷받침되어야 할 것이다.

따라서 앞에서 살펴본 전자서명에 있어서의 問題點을 중심으로 향후 발전방향을 고찰해 보고자 한다.

첫째, 시장의 공정성과 경쟁력 확보방안

시장독점과 불균형을 치유하기 위한 근본적인 해결방안으로 자유롭고 공정한 인증시장 질서를 도입하고 서비스 제공자의 자유공정 경쟁을 통한 발전을 유도하여야 한다. 즉 모든 사업사자 공정한 지위에서 모든 시장에 상호 진입하여 사업을 수행하도록 하는 것이다. 특수 認證機關들이 일반 인증기관들과 공

14) 최영봉, 전자거래에 있어서 인증관련당사자의 책임에 관한 연구, 국제무역연구 제8권 제2호 2002.10. pp.310-320.

정한 환경에서 경쟁하려면 특수 목적으로 설립된 비영리기관에서 분리되어 독립적인 사업체로 認證事業을 영위하여야 한다.

둘째, 소비자 중심 인증서비스 효율성 및 품질개선방안

인증서비스라는 것이 소비자의 기호와 선택에 따라 끊임없이 발전하는 것이어서 모든 서비스를 제공하는 공인인증서의 개념은 실제 존재하지 않으며 끊임없이 신규 서비스가 생겨날 수 있다.

그러므로 무조건적인 相互連動보다는 공공성이 높은 서비스를 위주로 상호연동이 되는 서비스를 패키지화하는 것이 바람직하다. 그 외의 부가서비스는 소비자의 기호와 시장 발전에 따라 다양한 서비스가 개발되어 시장에서 통용되면 消費者는 값싸고 좋은 서비스를 선택해서 쓰는 혜택을 누리게 되며 서비스 제공자들 또한 이러한 노력을 통하여 競爭力發展을 하게 된다. 이러한 부가서비스는 특정 인증기관에서만 제공되며 상호연동서비스의 범주에 포함되지 않을 수 있다.

정부는 공인인증서비스가 소비자와 사업자간에 공정한 계약에 따라 이행되도록 감시를 철저히 하는 기능에 집중하는 한편 공인인증서가 인증기관의 전자문서에 法的效力을 부여하기 위해 고안된 것이 오히려 민간시장의 인증서비스의 발전에 저해하지 않도록 세심한 주위가 필요하다.

셋째, 국가전자인증 서비스체계의 일관성 유지방안

국가PKI와 정부PKI의 이중 認證體系로 대표되는 우리나라의 국가적인 인증체계 또한 행정부, 입법부, 사법부의 정부기관의 인증서비스를 도입 추진하는데 있어서 국가인증서비스의 발전을 위해서는 독자적인 추진보다는 일관된 국가적 인증체계하에서의 戰略을 가지고 추진할 필요가 있다. 여기서 제일 중요한 과제로 소비자를 위한 관점에서 두가지 전략적 측면이 고려되어야 한다.

그 하나는 공인인증서비스에 대한 윈스톱서비스 개념이 도입되어야 한다. 즉 電子政府法下에서 현재 공인인증서를 전자정부의 민원서비스에 활용할 수 있게 되어 있으나 공인인증서를 활용하기 위한 전제조건인 발급절차에 관하여는 전자정부의 역할이 전혀 고려되어 있지 않다. 국민적 서비스 차원의 편의성을 도모하여 전자정부의 活性化를 위한다면 공인인증서의 발급은 국가기관을 통하여 하루빨리 실현되어야 한다.

다음으로는 국민을 대상으로 하는 공인서비스와 민원서비스 사이에서 전자서명법과 전자정부법에 나타난 공인인증기관의 역할이 국민들을 상대로 한 윈

스톱서비스의 제공자로서 일관된 모습이 요구된다.

전자정부 서비스의 운영주체는 물론 정부기관이고 정부가 주관해서 전략과 사업을 펼쳐가야 할 일이지만 인증서비스 자체는 향후 기술 발전에 신속하고 효율적으로 대응하기 위한 전략으로 전자정부가 정한 諸般保安 요건을 충족한 인증기관에 운영을 위탁하는 것을 발전적으로 검토해 볼 필요가 있다.

넷째, 시장의 한계극복과 국제경쟁력 확보방안

현재 國內技術은 미국을 비롯한 선진국과 비교하면 인증기관의 출현으로 봤을 때 3-4년의 격차가 있으며 인증서비스의 기술적 수준에서나 서비스 운영 수준 등 다각적인 면에서 아직 3년 정도의 격차를 따라 잡아야 할 상황이라고 볼 수 있다.

우리나라의 認證保安技術은 역사가 매우 짧다. 한가지 경계할 점은 국내의 인증기술이 빠르게 확산되어 일방적으로 국내표준이 정착되어 국제시장 표준과의 호환성 및 해외 인증서비스와의 국제호환인증 서비스의 고립화 현상이 빚어져 인증기관의 國際競爭力 喪失로 이어지는 매우 위험한 성장이 된다.

한정된 국내시장의 한계를 극복하는 것은 적극적으로 해외시장을 개척하는 방법밖에 없다. 빠르게 확산되고 있는 국내기술이 해외기술과 균형적인 발전을 이루기 위해서는 글로벌 서비스와 상호연동전력이 요구되며 국제경쟁력 확보를 위한 전략적 포석이 절실하다.

다섯째, 정부의 실용적인 사업지원책

파급효과가 큰 공인인증 적용부문별 대표적인 업무에 대한 시범사업을 적극 발굴하여 지원하는 것은 中長期的으로 매우 중요하다. 시범사업은 적용업무개발에 한정하지 않으며, 공인인증서 기반의 업무술루선개발 지원, 비즈니스모델 개발, 해외수출지원 등으로 확대되는 것이 바람직하다. 특히 이용자에 대한 정부의 실질적인 支援策이 이루어질 수 있도록 하는 것이 바람직하다.

V. 結 論

전자상거래에서 認證問題는 전자문서를 이용한 비접촉, 비대면 거래라는 전자거래의 한계점을 극복해 주는 가장 중요한 수단이다. 이러한 전자인증은 국

내거래에 있어서도 거래의 안전성과 信賴性을 확보할 수 있는 중요한 역할을 수행하고 있지만 앞에서 살펴본 바와 같이 여전히 해결해야 할 많은 問題點을 가지고 있다.

인증제도에 있어서 市場獨寡占 및 인증사업자간 불균형현상, 국내인증시장의 성장한계 직면과 국제경쟁력 확보문제, 인증서비스의 편의성 및 효율성, 공인인증서 발급시 신원확인 수단의 효율성과 상호연동의 편의성, 경제성 및 전자서명법과 전자정부법 이원화체계 하의 대국민 인증서비스의 일관성 확보문제, 인증기관의 일관된 인증서비스 제공문제, 그리고 인증관련당사자의 責任問題 등을 해결하기 위한 노력이 있어야 할 것이다.

전자상거래의 특성상 국경을 초월한 국가간의 거래에 있어서는 더욱더 중요한 문제로 인식되고 있는바 주요국가 및 기관에서 국가간의 인증문제에 대해서 심도 있는 논의가 전개되고 있는 상황이다.

우리나라에서도 1999년 2월에 제정된 電子署名法은 지문인식기술, 홍채인식기술, 수기서명 방식의 전자서명 등 새롭고 다양한 전자서명기술을 반영하고 있는 외국의 입법동향 및 국제기구의 규범을 수용함으로써 전자서명의 國際間相互認證에 대비하는 한편, 그동안 시행과정에서 나타난 여러 가지 문제점을 보완하고 전자서명 및 인증의 활성화를 위한 시책에 대한 근거규정을 마련하는 등 보다 안전하고 신뢰할 수 있는 환경에서 전자서명의 사용이 가능하도록 法制를 정비하여 2002년 4월 일부 개정하였다.

현재 전자서명법은 시행중이지만 이를 뒷받침할 정부의 정책적 지원 및 업계의 대응 등은 아직도 미흡한 것으로 판단된다. 飛躍的인 成長을 하고 있는 세계의 電子署名 認證市場에 성공적인 競爭力을 갖추었을 때 전자서명 인증제도는 우리의 새로운 사회적 기반으로 生産力을 크게 향상시킬 수 있는 정보화의 선구자가 될 것이다.

參考文獻

- 강태욱, 인증기관의 업무와 배상책임,
김은기, 전자인증과 법률문제, 정보법학, 제 2호, 1998.
김영준, 전자서명과 인증에 관한 연구, 통상정보연구 제3권 제1호, 2001.6.
길민정, 한국,일본,미국의 전자인증 시장 비교·분석, 2003.
박재기, 아시아 주요국가의 전자서명 인증정책 및 제도조사·분석, 한국정보보호진흥원, 2002.12.
배대현, 전자서명과 인증, 인터넷법률, 창간호, 2000.
성육조, 공인인증제도와 전자서명, 한국 PKI포럼 사업분과, 2002.8.29.
신일순외 1인, 전자서명 및 인증제도, 정보통신정책연구원, 1998.12.
신홍식, 우리나라 전자인증 서비스의 균형발전 및 경쟁력 제고를 위한 건의문
안중호, 전자인증기술 및 서비스, 서울대학교 전자상거래지원센터, 2000.8
이경구, 전자인증제도, 한국정보보호센터, 1999.5.
이정현, 주요국가의 전자서명 인증제도 현황, 2003.
이호건의외2인, 글로벌 전자상거래를 위한 인증체계, 한국정보연구 제2권 제2호,
2001.11.
이호건의외2인, 인증관련 주요 국제기구 및 국가인증제도 현황분석, 통상정보연구
제 1 권 2호, 1999.12.
정완용, 유럽주요국가의 전자서명 인증정책 및 제도조사·분석, 한국정보보호진흥
원, 2002.12.
주재훈, 전자인증 서비스의 가치분석, 경영학연구 제 28권 제 2호, 1999.
최영봉, 전자거래에 있어서 인증관련당사자의 책임에 관한 연구, 국제무역연구
제 8 권 제 2호, 2002.10.
최준선, 전자서명과 전자인증의 제문제, 무역상무연구, 제 15권, 2001.2.
한승철, 전자서명 및 인증기관의 법적 문제, 저스티스 제 31권 1호, 1998.
황희철, 전자서명과 법률문제, 정보법학 제 2호, 한국정보법학회, 1998.
Draft Guide to Enactment of the UNCITRAL Model Law on Electronic
Signature, 30 January 2001. A/CN.9/WG.IV/WP.88.
CESG, Secure messaging and PKI interoperability demonstrator final report,
UK online, May 2001.
Entrust, Digital Signature -Best Practice for e-business transaction, 2001.

Roger W. Younglove, Public key infrastructure -How it works, Computing & Control Engineering Journal April 2001.

Stephen York · Kenneth Chia. E-Commerce, Butterworths, 1999.

Wright, Benjamin, The Law of Electronic Commerce, 4th(ed.), Aspen Publishers, Inc., 2000.

한국전산원(www.nca.or.kr)

한국정보보원(www.kisa.or.kr)

정보통신부(www.mic.go.kr)

산업자원부(www.mocie.go.kr)

한국정보보산업협회(www.kisia.or.kr)

한국정보인증(www.signgate.com)

전자거래진흥원(www.kiec.or.kr)

ECRC지원센터(www.ecrc-korea.or.kr)

e-비즈니스정보센터(www.kebic.or.kr)

한국PKI포럼(www.pki.or.kr)

법제처(www.moleg.go.kr)

ABSTRACT

A Study on Problems of Digital Certification System

Hwang, Sang Kyu

As a rapid development of electronic commerce transactions in these days, the security and private protection problems became more important matters under the electronic transaction base. Because electronic transaction using electronic documents be carried without direct person to person meeting, there can be the possibility to use other's identity illegally without notice, and very hard to verify authenticity of transaction as well.

In addition, it is very hard to find out that the electronic documents on the process of submitting is forged documents or not, and also have much difficulty in maintaining transmitting secret. Therefore, to solve such problems on electronic commerce transactions and electronic documents, the digital signature and certification system with cryptography skill is inevitably necessary. As the wide use of digital signature together with beginning of digital government and financial transaction, not only the issuance of electronic certification, but certification market came to gradually expand.

In Korea, after enacting digital signature act in 1999, the act contents were expanded to the wide range of contents complying with global standards from the end of 2001 to April, 2002, including the new clause of certification problems. And the act was put into operation now.

Therefore, in this paper, we'd like to suggest development scheme through the investigation on electronic certification related problems, such as, concepts, procedures, service conditions here and abroad.

Key Words : Electronic Commerce, Digital Certification