# 전자상거래에서의 인증사업 및 정책 동향

이현우, 정성영, 이상규

한국전자통신연구원

# Authentification & Certification in e-Commerce

Hyun-Woo Lee, Sung-Young Jung, Sang-Kyu Lee

ETRI

E-mail : lhwoo@etri.re.kr

## 요 약

인터넷 등 네트워크상의 거래에서의 인증은 주요한 인프라이다. 네트워크상에서의 거래에서는 일반적 대면거래에서와 달리 상대방 확인과 내용에 대한 확인을 할 수 없다. 이러한 문제점을 해결해 주는 것이 바로 인증이며 인증은 암호방식을 사용하며 신뢰받는 제3자에 의해 수행된다. 인증사업을 위한 제도적 뒷받침을 위해 각국은 디지틀서명 및 인증기관에 관한 디지틀 서명법을 제정하고 있으며, 민간부문 뿐만 아니라 공공부문을 포괄하는 상호인증을 가능케하는 국가적 차원의 공개키기반구조 확립에 주력하고 있다. 본고에서는 이러한 인증의 개념과 국내외 인증사업 및 정책에 대해 살펴보았다.

## I. 서 론

인터넷이 넓게 보급되고 있으나 아직 인터넷이 미칠 수 있는 파급효과는 이제 시작단계이다. 그러나 그중 인터넷이 우리들의 생활에 미칠 수 있는 중요 변화는 바로 경제적 변혁으로서 인터넷을 통한 네트워크상에서의 상거래, 즉 전자상거래이다. 많은 전문가들은 2000년대 초에는 전자상거래의 매출액이 연간 수천억불에 이를것으로 예측하고 있다. 미국 정부의 전자상거래 실무그룹의 1차년도 보고서(1998년 11월)에서도 향후 수십년간 인터넷과 전자상거래가 세계경제를 주도할 것으로 전망하고 있다[1]. 그러나 인터넷 등 통신네트워크상에서의 거래를 제대로 하기 위해서는 여러 가지 해결해야할 장애요인들이 산재해 있다. 그중 네트워크상의 거래에서의 근본적인 문제는 통상의 거래와 같이 대면적으로 이루어지지 않기 때문에 발생하는 문제들이다. 즉 거래시 직접 대면할 수 없기 때문에 상대방이 정말로 거래하고자 당사자인지 확인 할 수 없으며 거래내용에 대해서도 확인할 수 없다. 이러한 대면적 거래가 아니기 때문에 발생하는 문제를 네트워크상에서 해결하는 것이 바로 "인증"으로서 일반적으로 신뢰받는 제3자에 의해 행해도록 권고되고 있다.

## II. 인증의 개념

### 1. 인증의 필요성

네트워크상의 거래에서는 첫째, 거래의 상대방과 직접 대면하지 않음으로서 통신의 상대방이 정말 자신이 거래하고자 하는 사람의 본인인지 아닌지를 확인할 수 없다. 구매자의 경우 그 가상상점이 실체가 있는 회사인가, 혹은 대금을 지불하면 바로 상품이나 서비스의 제공을 해 줄 것인가에 대한 불안감을 가질 수 있으며, 판매자의 경우 주문을 한 사람의 지불 능력에 대한 확인이 곤란하다.

둘째, 거래 및 지불에 관한 통신내용에 대해 의도적인 제3자에 의해 내용이 변질되거나 불법으로 이용될 수 있을 뿐만 아니라 거래 당사자에게도 그 내용을 확인할 수 없음에 따라 오용당할 수 있다. 네트워크상의 거래의 경우 통신과정에서 글자가 깨져서 나오거나 정보의 일부 혹은 전부가 변질되어 발신자의 발신내용이 정확하게 상대방에게 전해지지 않을 가능성이 있다. 특히 인터넷 같은 개방 네트워크의 경우, 네트워크 전체의 일원적 관리자가 존재하는 것이 아니고 다양한 전기통신사업자가 관리하는 설비를 경유해 상대방에게 도착하기 때문에 통신과정에서 통신 당사자 이외의 제3자가 통신 내용을 변개시키거나 삭제할 가능성이 있다. 또한 현재의 인터넷에 있어서는 착신확인 기능이 없기 때문에 발신자가 상대의 어드레스를 잘못해 입력하므로서 의도한 상대에게 통신이 착신되지 않을 수 있다. 또한 일반

적 거래에서는 주문서, 계약서등의 교환을 문서로 하기 때문에 사후적인 확인이 용이하고, 공증인에 의하는 공증 사무나 우체국의 내용 증명우편, 도달 시각 증명 우편 등의 이용이 가능한데 비해, 네트워크상의 거래에 있어서는 기본적으로는 모든 거래과정이 네트워크상에서의 정보 전달이라고 말하는 형태로 이루어지기 때문에 거래내용이 기록에 남지 않으므로 실제로 주문 및 주문 내용이 정확하게 상대에게 전해졌는지 여부에 대한 확인이 어렵다[2].

2. 인증 기능

전술한 네트워크상 거래의 문제를 해소하는 것이 바로 인증의 기능으로서 아래와 같이 요약할 수 있다.

○ 상대방의 본인성 확인 : 네트워크를 통해서 통신 혹은 거래를 할 때에 그 통신 혹은 거래의 상대가 정말로 자신의 의도하고 있는 사람본인, 혹은 서버 등인지 아닌지의 여부를 확인하는 기능

○ 통신 내용등의 확인 : 네트워크를 통해서 통신 혹은 거래를 할 때에 그 통신 혹은 거래가 행해진 일시는 언제 였는지, 혹은 그 내용은 무엇인지를 확인하는 기능

3. 인증기술

인증은 암호기술을 이용하는 것이다. 암호화방식은 다양하지만 전자상거래에 사용되는 암호화 방식은 크게 두가지로 대별되며 그중 하나가 공통키방식이고 다른하나가 공개키방식이다. 공통키 방식은 대칭키방식이라고도 하는데 원문을 암호화하는 암호화나 암호문을 원문으로 바꾸는 복호화를 하나의 키에 의해서 한다. A가 열쇠 q를 가지고 암호화하면 B도 동일한 열쇠 q를 가지고 복호화를 할 수 있도록 하는 방식이다. 이는 양 당사자가 다른 사람에게 키를 공개하지 않으므로 비밀키방식이라고 한다.

반면에 공개키방식은 비대칭키방식이라고도 하며 "암호화키"와 이를 다시 평문으로 바꾸는 "복호키"의 서로 다른 2개의 키로 조합되어 A가 가진 비밀키q로 암호화한 경우 공개된 공개키q로 복호화를 하고 공개키로 암호화한 경우 비밀키로 복호화를 할 수 있다. 발신자A는 자신의 비밀키로 통신메시지를 암호화하여(전자서명 생성) 메시지를 B에게로 송신하면 수신자B는 발신자 A의 공개키로 메시지의 복호화를 통해 A에 의해 서명된 메시지인 것을 확인는 것으로 상대방 확인의 인증기능을 수행하며 암호화된 정보는 B의 비밀키가 아니면 복호화할 수 없고 제3자가 암호문을 입수하여도 해독이 극히 곤란하므로 내용에 대한 확인의 인증기능을 수행한다.

비밀키 방식은 하나의 키를 상대방에게 전달하고 둘이상의 당사가가 보관하는데 보안상의 허점이 생길 수 있으므로 공개된 통신망에서는 문제가 있다. 반면에 공개키방식은 두 개의 열쇠가 서로 조합이 되지 않으면 기능할 수 없기 때문에 그 중 하나의 키를 키의 생성자가 보관하므로서 키의 운반, 공개, 보관상의 허점을 제거할 수 있으므로 공개된 통신망에서의 적합하다. 그런데 일반적으로는 공통키방식과 공개키방식을 조합하여 특정의 통신의 암호화에 이용되는 공통키를 상대방의 공개키에 의해 암호화해 미리 전달한 다음 그 공통키를 이용해 암호 통신을 하는 방법이 많이 이용된다[3].

이와 같이 공개키방식의 암호는 불특정 다수자간에의 통신에 있어서의 인증에 일반적으로 이용되고 있어서 국제적으로도 공개키방식을 전제로 한 제도화를 하고 있는 예가 많으며, 세계전기통신연합전기통신표준화부문(ITU-T)의 X.509 권고, 우리나라의 전자서명법을 비롯한 미국의 유타주 디지탈 서명법, 플로리다주 전자서명법, 독일의 디지털 서명법 등은 공개키방식으로 기초를 두는 인증의 방식을 전제로 하고 있다. 그러나 향후 새로운 기술 발전이 이루어 질 것이므로 관련 주요 국제기구에서는 제도적 측면에서의 기술적 중립성을 강조하고 있다.

4. 인증의 활용 분야

현재 인증사업은 VeriSign, GTECyberTrust 등 몇몇 주요 민간사업자에 의해 주도 되고 있으며, 쇼핑몰서버 인증 그리고 전자우편 인증이 주류를 이루고 있다.그러나 향후 그 이용분야도 다양할 되고 점차 그 수요도 증가할 것으로 예상된다. 현재로서 인증이 활용될 분야를 특별히 규정하기는 곤란하나 일반적으로 다음과 같은 분야를 들 수 있다[2].

○ 기업간거래, 정보교환
○ 기업내결재, 정보교환 등
○ 가상상점 소비자 거래
○ 금융서비스
○ 원격 의료
○ 전자 공증
○ 행정 서비스
○ 우체국의 전자내용증명서비스
○ 전자 우편

## III. 인증사업 동향

1. 외국 동향

미국의 GTE는 분야에 18년의 역사를 가지고 있으며 '96년 초에 CyberTrust라는 서비스명으로 민간에 대한 서비스를 개시하였다[4]. '95년 4월에 설립된 VeriSign은 전세계적으로 75,000서버, 3백만 개인에 대해 인증서(Digital ID)를 발급하고

있다. 인증서비스의 대표적인 예가 될 수 있는 VeriSign의 서비스를 보면 (표 1)과 같다[5]. 인증서비스는 개인용과 서버용이 있으며 통합패키지 서비스가 있다. 개인용서비스의 경우 전자우편 인증과 네트워크상의 접속통제서비스를제공하고 있으며, 서버용은 이용의 90% 이상이 일반 서버 인증서비스(Secure Server Digital ID)이며, 그밖에 국제적 거래, EDI, 재무적 거래시 이용이 권장되는 서비스가 있다. 또한 부가서비스로서 CPA인증서, Seal부여 등의 여러 가지 프로그램이 있다. 또한 세계 최초로 인증에 관한 전자서명법을 제정한 미국유타주의 경우는 DST Company, Arcanvs, Inc., USERFirst 등 3개의 공인인증기관이 '97년 설립된 바 있다.

(표 1) VeriSign 서비스 현황

| 구분 | 서비스명 | 내용 | 요금 (연간) |
|---|---|---|---|
| 개인 ID | Class 1 Digital ID | e-mail | $ 9.95 |
| | Pre-Purchase Multi Digital ID | access control e-mail | |
| 서버 ID | Secure Server Digital ID | 거래, 통신 | $ 349 |
| | Global Server ID (128-bit encryption) | 국제적 영업 | $ 695 |
| | EDI Server ID | EDI | $ 995 |
| | Financial Server ID | open finantial exchange | $ 995 |
| | Web Trust Program | CPA 인증 | |
| | Web Host Program | Web Hoster가 ID획득 | $349 (13-25% 할인) |
| | Authentic Site Program | Site Seal | |
| 개발자 ID | -Marimba Castanet<br>-Microsoft Authenticode<br>-Netscape Object Signing | Download S/W 인증 | $ 400 |
| 기업 PKI Solu-tion | -VeriSign OnSite Server Certificates<br>-VeriSign OnSite IPSec Certificates<br>-Training & Consulting<br>-SET Services<br>-Government Solution | 통합 PKI Platform 제공 | |

캐나다의 경우 대표적 인증기관인 Keywitness Canada는 '95년 설립되었으며 기업과 개인에게 X.509 형태의 인증서를 발급하고 있다. 호주의 경우는 Security Domain(Zero Asia Pasific)이 선도적 사업자로서 '89년 설립되었으며 연 수익 600 백만불의 기업으로 성장하였다. 영국의 경우 BT와 VeriSign이 합작한 Trustwise가 '98년 설립되어 시범서비스를 제공하고 있으며 1등급에서 3등급의 인증서를 발급하고 있다. 일본의 경우 NTT가 3개 자회사를 통해 출자하고 있는 VeriSign Japan, Cybertrust Japan이 각각 '96년, '97년에 설립된바 있으며, '98년에는 수십개 기업이 참가한 컨소시움 형태의 일본인증주식회사가 설립되었다. 그외 BelSign은 유럽의 디지틀인증기관으로서 개인과 서버에게 인증서를 발급하고 있으며, CertCo는 금융기관에게만 인증서를 발급하고 있다.

2. 국내 동향

우리나라의 경우 아직 외국과 같은 상용서비스를 제공하는 인증전문기관은 없으므로 국내 쇼핑몰의 경우 외국 전문인증회사를 이용하고 있는 실정이며, 지불을 위한 사용자 보안수단으로는 대부분 SSL(Secure Socket Layer)를 사용하거나 보안대책도 마련되지 않은 경우가 많다. 그러나 향후 전자서명법 시행령 등 관련 제도가 정비되고 국가인증체계가 확립이 되면 공신력 있는 신뢰받는 제3자로서의 공인인증기관 및 민간인증기관 등의 설립이 시작될 것으로 기대된다. 현재의 국내 인증사업은 시험/실증단계에 있으며 주로 비자 마스터 카드사가 주축이 되어 추진되는 SET 구현의 일환으로 추진되는 경우가 많다. 국내 20여개 업체가 '97년 사단법인으로 설립한 CommerceNet Korea와 메타랜드는 SET구현의 일환으로 인증시스템 구축하고 잇으며, 한국과학기술원의 ICEC(International Center for EC)는 SET시스템 개발 및 메타랜드와 연계한 사업화 추진하고 있다. 한국통신은 마스터 카드 등 국내 10개사와 SET실험사업을 추진하고('97.6.), SET 인증기관 구축 및 실험서비스를 제공('98.11.3.)하고 있으며, 데이콤은 VISA Korea와 협력하여 SET실험사업 추진중이며, 현재 메타몰인 Interpark운영에서 SSL방식에 의한 인증서비스를 제공하고 있다. 공공부문의 경우 한국전산원의 EDI/EC지원센터는 조달 EDI 부문에서 인증서비스를 제공하고 있다[6].

## IV. 인증정책 동향

1. 전자서명법 등의 법/제도화

디지틀서명 및 인증기관과 관련하여 규정하고 있는 각국의 디지틀 서명법의 제정동향을 살펴보면 다음과 같다[2,7,10]. 먼저 미국의 경우 '955년 미국변호사협회(American Bar Association)가 디지틀서명에 관한 가이드라인을 공표하여 이것이 각주의 법률 제정의 주요 모델이 되어 왔다. 그중 유타주가 '95년 가장 일찍이 공개키기반구조(PKI

: Public Key Infrastructure)에 입각한 디지틀서명법(Digital Signature Act)을 제정하였으며('96년 개정) 여기서는 인증기관에 관한 면허제도를 제정하여 세부적 자격요건을 정하는 한편 인증기관의 의무에 대해서도 규정을 두고 있다. 유타주의 디지틀서명법에서 면허는 인증업무를 영위하기 위한 필요조건이 되고 있지는 않으나 면허를 받은 인증기관이 발행하는 증명서 등은 재판상의 추정효과가 주어지고 있다. 유타주의 디지틀서명법은 미국내외적으로 가장 포괄적이고 모델적인 법률이 되어 오고 있다. 현재 미국의 39개주가 디지틀서명법 혹은 전자서명법을 제정했거나 관련 문제에 대해 검토중이며, 그중 10개주가 공공과 일반부문에의 적용을 포괄하는 일반적인 용도의 13개 법을 제정하였고 23개주에서는 보건서비스제공자나 차량등록을 위한 전자서명의 활용과 같은 공공부문이나 민간부문에만 적용되는 특정용도의 법령 36개를 제정하였다.

독일에서는, '97년 6월 "디지탈 서명법(Gesetz zur digitalen Signatur)"이 제정되었다. 이 법 역시 미국 유타주법과 마찬가지로 공개키기반구조에 입각한 디지틀서명만을 대상으로 하고 있으며 여기에서는 디지틀서명에 관한 기본적인 요건을 명시하고 인증기관에 관한 주무관청의 허가 및 업무중지, 취소에 관한 경우에 관해 규정하고 있다. 인증 업무를 면허제로 하여 경제부의 밑에 신설되는 전기통신규제청이 규제기관이 되어 일정한 자격 심사를 하는 것과 동시에 인증 기관의 업무 운영상의 의무에 관한 규정을 정하고 있다. 또한 국외에서 작성된 디지탈 서명의 유효성에 관한 규정을 두고 있으며, 인증 기관의 개인정보 보호 의무에 관한 규정이 정해지고 있다. 디지탈 서명의 법적 효과에 관한 특별한 규정은 없으며, 인증 기관에 의하는 비밀키의 보관 등 암호 규제에 관한 문제에 대해서는 차후 검토를 한다는 전제하에 인증 기관이 고객의 비밀키를 보관하는 것을 금지하는 규정을 두고 있다.

그외, 말레이지아의 경우 '97년 "CyberBills" 내의 법률로 제정된 4가지 법률중 하나로 디지틀서명법이 제정되었는데 그 체계나 내용이 미국유타주법과 유사하다. 영국의 경우 DTI는 1997년 3월에 암호 서비스를 제공하는 Trusted Third Party (신뢰되는 제삼자 기관: TTP) 를 면허 제도의 대상으로 하는 법제를 제안하고 있다. 영국 정부의 제안에서는 TTP에 의하는 공개키의 보관과 함께 비밀키의 보관 업무도 법적 규율의 대상으로 하는 것으로 하였으며 정부기관에 의하는 인증 기관이 보유하는 비밀키에 대한 합법적 접속에 관한 규정을 두고 있으며 구체적인 면허 조건에 대해서는 향후 검토하는 것으로 되어 있다. 일본의 경우 200개 회사의 콘소시움으로 구성된 ECOM(Electronic Commerce Promotion Council of Japan)의 인증기관 검토실무반은 '97년에 "인증기관가이드라인"을, '98년에 "상호인증가이드라인"을 발표하였으며, 법무성내의 "전자거래제도에 관한 연구회"는 전자공증, 인증, 전자서명에 관한 법률 제정을 목표로 연구보고서를 작성하였으며, 이를 토대로 법무성은 관련 법규 정비를 추진중이다.

국제기구의 동향을 살펴보면, 먼저 유엔의 국제상거래법위원회(UNCITRAL)에서는 전자상거래에 관한 모델법을 '96년 6월 채택한 바 있으며 여기서는 데이터메시지와 관련한 서명의 요건을 규정하고 있다. '97년 12월 전자서명에 관한 통일규칙초안(Draft Uniform Rules on Electronic Signiture)을 발표하였으며, 여기서는 공개키암호방식을 이용한 디지틀서명을 안전한 전자서명의 하나로 간주하며, 전자서명에 대한 법적효력을 부여하고 있다. 또한 '98년 6월 전자상거래실무그룹은 제31차 위원회회의에서 전자서명과 인증기관 및 관련 법적 이슈에 관한 통일규칙을 초안을 채택하고 향후 지속적으로 보완할 예정임을 밝혔다. OECD(경제협력개발기구)에서는 '97년 3월에 "암호 정책 가이드 라인"을 공표하여 정부의 적법한 접근법을 보장하는 암호정책을 권고하고 있으며, '98년 10월 회의에서는 인증에 관한 선언문을 채택한 바 있다. EU는 '96년 3월 "역내시장에서의 암호화된 서비스에 대한 법적 보호에 관한 녹서"를 발표하고 암호화를 통한 정보유통을 적극 권장하고 있으며, '98년 5월에는 전자서명을 위한 공동틀에 대한 지침을 발표하여 인증서 및 인증기관의 요건을 규정하여 전자서명에 대해 수기서명과 동일한 효력을 보장하고 인증기관의 사전선정보다 자발적 인가의 도입을 권고 하고 있다.

국내의 경우 '99년 1월 전자거래기본법 및 공개키기반구조에 입각한 전자서명법이 제정되었으며, 동년 7월 상정될 하위법령(안)에 대한 검토가 진행중이다. 전자서명법에서는 공인인증기관을 지정사항으로 규정하고 있으며, 인증업무, 사업에 관한 규제내용이 포함되어 있으며, 상호인증에 관한 내용도 규정되어 있다. 공인인증기관의 지정요건에 관한 사항은 하위법령에서 규정될 예정이다 [8].

## 2. 인증기반구조

인증은 민간인증 뿐만 아니라 공공부문의 인증업무 및 인증기관간 상호인증이 환경이 중요하며, 이러한 측면에서 국가적 인증기반구조의 구축이 필요하다. 미국의 경우 공공부문에서의 인증업무를 효과적으로 수행하기 위해 연방정부 조직 및 기관이 참여하고 있는 연방공개키기반구조(FPKI : Federal Public Key Infrastructure) 운영위원회를 설치하여 NIST가 주도적으로 추진하고 있다. 미국의 FPKI는 PAA(Policy Approving Authority), PCA(Principal Certification Authority), CA(Certification Authority), ORA(Organizational Registration Authority) 등의 기관이 계층적 및 네트워크 구조를 동시에 가지는 혼합형을 채택하고 있다. 여기서 PAA(NIST)

는 공개키기반구조에서의 최상위 인증기관으로서 CA와 ORA를 위한 정책수립 및 감독, 공개키기반구조내의 상호인증을 위한 정책 수립 및 CA로서의 역할 등을 수행한다. PCA(국방성, 총무처, 법무성, 재무성)는 차상위 인증기관으로서 하위기관에 대한 정책조정 및 집행 그리고 CA로서의 역할을 수행한다. CA(NSA, FBI, IRS)는 공개키 인증서 발행, 배포, 취소, 보관등의 기본적인 관리기능과 CA간의 상호인증을 위한 디렉토리서버를 운영한다. ORA의 경우 등록기관으로서 인증서 신청자의 신분 및 소속 등을 증명하는 기능을 수행한다.

호주의 경우 스탠다드 · 오스트렐리아를 중심으로 하는 관민 공동의 태스크포스가 '96년 가을 인증 기관에 관한 가이드라인(PKAF 가이드라인) 으로서 "호주에서의 공개키인증프레임워크(PKAF : Public Key Authentification Framework)의 실시에 관한 전략"을 공표했다. 또한 '97년 2월에는 통신예술성이 중심이 되어 부처간의 위원회가 설치되어서 PKAF 가이드라인을 기준으로한 법제화의 검토를 시작하였다. PKAF 가이드라인에서는 상위의 단일 인증 기관으로서 정부의 통제하에 있는 PARRA(Policy and Root Registration Authority)를 설립해서 PARRA가 하위 인증 기관의 인증 및 국제간 인증을 하는 것으로 하고 있다. '98년 5월에는 GATEKEEPER라는 인증활용 전략을 발표하였으며, GATEKEEPER는 호주의 PKAF의 실행을 위한 구체적 전략을 담고 있으며 정부부문의 선도적인 수요창출을 통한 인증분야의 발전을 도모하고자 하는 것이다. 최상위인증기관인 PARRA는 아직 설치되어 있지 않다.

일본의 경우 일본정보처리개발협회는 산하기관으로서 ICAT(Initiative for Computer Authentification Technology)를 설치하고 이를 최상위인증기관으로 하여 하위 20개 기관을 시험적으로 운영하고 있다. 이는 미국의 FPKI와 유사하지만 계층구조를 채택하고 있다는 점에서 차이가 있으며, 미국의 4단계와는 달리 3단계의 구조를 가지고 있다[9].

UN은 세계무역기관네트워크(GPT-Net)를 통해 전자인증연계(SEAL)프로젝트를 진행중이며 유럽은 ICE-TEL(Interworking Public Key Certification for Europe) 프로젝트를 추진하면서 PKI 환경구축에 박차를 가하고 있다[10].

국내의 경우 정보보호센터가 전자서명법상 Root CA로서 위치를 차지하고 있으며 국내 PKI 구조에 대한 연구를 진행중에 있다.

## V. 결 론

다가올 21세기는 인터넷 전자상거래가 보편화될 전망이다. 이러한 전자상거래를 안전하고 신뢰성있게 할 수 있게 해주는 전자상거래의 인프라가 바로 인증이다. 인증사업은 한마디로 암호기술을 이용한 사업으로 볼 수 있으며 따라서 인증사업도 여러 가지 영역에서 다양한 형태로 나타날 수 있을 것이다. 미국의 예에서 볼 수 있드시 우리나라도 기업간 거래시 전자우편의 보안에 대한 인식이 증가할 것이며 쇼핑몰에 대한 확인 및 지불정보의 보안에 대한 인식과 욕구도 크게 증가할 것이다. 아직 국내에서는 인터넷상의 거래시 신용정보를 불법으로 이용한 이렇다 할 범죄는 보고 되지 않고 있으나 우리보다 훨씬 더 전자상거래가 발전될 미국의 경우 수많은 범죄 및 이에 따른 막대한 경제적 피해가 보고되고 있다. 이러한 측면에서 인증은 전자상거래 발전과 성장에 필수불가결하 하부구조일 뿐 만 아니라 네트워크상 통신 및 거래시 정보보안에 대한 필요성의 증대와 더불어 그 이용 및 시장의 확대가 크게 기대되는 분야이다.

## 참고문헌


[1] http://doc.gov.gov/ecommerce/e-comm.pdf, pp. 1-5.

[2] 일본우정성, "인증기관가이드라인, 1997.3.

[3] 황희성, 전자서명과 법률문제, 전자상거래법 제정을 위한 심포지움, pp. 11-13, 1998.

[4] http://www.bbn.com/products/security/cytrust/

[5] http://www.verisign.com

[6] 한국통신, 전자상거래 강화방안, 내부자료, pp. 25- 28, 1998.2.

[7] 신일순, 전자서명 및 인증제도의 필요성과 국내외 동향, 전자서명법 제정을 위한 대토론회, pp. 9-15, 1997. 6.18.

[8] 전자서명법, 1998.1.

[9] 정보통신정책연구원, 전자서명 및 인증제도(요약), pp. 3- 7, 1998.12.

[10]수원대학교, 주요국의 인증제도 및 인증기관에 관한 연구, 한국통신경영연구소, pp. 11-33, 1998.12.

[11]한국전산원, 전자상거래 주요 현안 및 대응방안, 내부자료, pp. 1- 13, 1998.6.