전자서명 최근동향과 공인인증 활성화 방안

배성훈*, 한현수*, 이동근**

*한양대학교, 정보통신대학원

**국회사무처

Review on the recent trend of digital signature and policy implications for rapid propagation

Seoung-Hun Bae*, Hyun-Soo Han*, Dong-Gun Lee**

*Graduate School of Information and Communications Hanyang Univ.

**The National Assembly of R.O.K

요 약

본 연구에서는 개인용 공인인증서 활성화 방안에 대한 정책적 제안을 제시하였다. 현황 및 문제점 파악을 위하여 2003년도 정부발간자료, 통계, 과학기술정보통신위원회 국정감사 제출자료 등에서 직접 데이터를 수집하였다. 개인용 전자서명의 현황 및 문제점은 법·제도에 따른 시장 분석과 전자거래·전자문서 유통에 있어서 개인용 공인인증서의 시장독점 경향 등을 정리하였다. 이를 바탕으로 본 논문에서 제시된 활성화 방안의 초점은 전자문서 유통과 공인인증 체계의 시장 구조적 문제점 해소, 상호연동 및 유료화에 따르는 부작용 최소화에 두었다.

Ⅰ. 서론

1. 연구목적

정보통신기술의 발전과 인터넷의 급속한 확산은 인터넷 사용자의 폭발적인 증가와 우리사회의 시간적·공간적인 제약을 해소하는데 크게 기여를 하였으며, 가상공간을 무대로 하는 전자상거래라는 새로운 거래 형태를 탄생시켰다[1].

비단 전자상거래뿐만 아니라 인터넷을 통한 전자 거래는 사회 전반에 걸쳐 확산되고 있으며 개인적 차원은 물론이고 기업 내·외부적 자료의 교환, 관공서의 서류 및 민원처리에 이르기까지 다양한 차원에서 전자적 거래가 이루어지고 있다. 이에 따라 종이문서와 같은 전통적 통신방법은 점차 전자미디어로 대체되고 있는 현실이다.

그러나 이와 같은 발전의 이면에는 개방형 컴퓨터 네트워크로 인한 전자 보안의 문제가 제기되고 인터넷과 같은 경우 정보보호에 대한 요구가 크게 부각되고 있다. 또한 인터넷을 통한 전자거래는 비접촉, 비대면으로 이루어지기 때문에 거래 상대방의 신원을 확인하기 어렵고, 거래사실을 입증하기 곤란한 경우가 발생하기도 하며, 전자문서가 유통되는 과정에서 위·변조 될 가능성이 있다는 문제점이 지적되고 있다. 이와 같은 정보 교류에서의 역기능을 해소하기 위한 전자서명의 중요성이 부각되고 있다[2].

기존의 대면 거래에서는 계약서에 직접서명을 하는 수기가 이용되었지만, 전자적 거래에서는 기존의 종이로 된 계약서가 전자문서로 대체되며, 수기서명 대신 전자서명(Digital Signature)을 이용하게 된다. 이 때 전자서명은 전자적 거래에 있어서 종이문서 대신에 법적으로 구속력을 가지는 거래 집행 능력으로서 전자적 거래를 위한 중요한 단계로 인식되며, 전자서명에 대한 중요성을 인식하는 것은 세계적인 추세이다. 특히 선진국의 경우 미래 사회의 경제적구조로서 전자상거래에 대

한 중요성을 인식하고 이를 활성화하기 수단으로 공개키 암호화방식(Public Key Infrastructure : PKI) 전자서명을 활용하고자 전자서명체계를 확립하기 위한 국가적 노력을 기울이고 있다[3].

우리나라는 2000년 7월 전자서명법이 발효함으로 법·제도적 토대가 마련되었으며 2001년 12월에 전자서명법을 개정하면서 공개키 기반구조(PKI)에 대한 논의는 더욱 활성화하고 있다. 전자서명은 민간부문 중에서도 금융·증권 등을 중심으로 도입·운영되고 있으며, 점차 전자상거래의 많은 분야에서 활용가치를 넓히고 있다[4].

2000년 이후 최근 3년 동안에 국내에서 공인인증서 7,311,995장을 발급함으로서 세계 최고의 발급률과 아시아태평양지역 온라인 쇼핑 이용률 1위라는 영예에도 불구하고 전자서명 시장은 여러 가지 구조적인 문제를 나타내고 있으며[5], 공인인증서의 발급 및 관리 기관이 특별한 기능적 분담 없이 일률적으로 다수 존재한다는 사실과 영리성 여부에 따른 민간기업과 공공기관의 업무역할에 대하여 비효율적이라는 점 등이 거론되는 실정이다.

이에 본 고에서는 국내·외 전자서명의 현황을 살펴보면서 단순히 기술적인 세부사항은 별론으로 하고, 법제도에 따른 시장 분석과 전자거래·전자문서 유통에 있어서 개인용 공인인증서의 시장독점 경향과 그에 따른 구조적 문제점, 상호연동 및 유료화에 따르는 부작용을 최소화하기 위한 정책적 대안을 제시하는데 그 의의를 찾고자 한다.

2. 연구범위와 자료 수집

본 연구에서는 디지털 시대의 개인용 공인인증서 활성화 방안에 대한 연구로 전자서명의 부분적인 분야보다는 개인 공인전자서명과 관련된 전반적인 현황을 연구의 범위로 선택하였다. 전자서명의 확산에 있어서 일부의 지엽적인 요인에 의해 이루어지는 현상이 아니라 사회 전반적으로 영향을 주는 요인을 집중적으로 보고, 현황을 조사하여, 문제점과 활성화 방안을 분석 제시하고자 한다.

최근 정보통신의 기술적·사회적 변화 추이를 살펴 볼 때, 그 속도가 매우 빨라 지난 몇몇 자료들에서 언급된 각종 참고내용이 이 시점에서는 상당히 달라졌음을 전제하여 참고자료의 범위를 최근 6개월 내로 한정하였고, 본 고의 이해를 돕기 위하여 예외적으로 일부에서 지난 3년간의 통계를 예시하였다.

본 연구는 문헌조사와 조사된 통계자료를 분석하여 작성하였다. 공인인증서 확산요인에 관한 조사는 기존의 연구된 문헌을 이용하여 이론적 배경을 도출하고, 현황에 대한 자료는 각종 참고문헌과 인터넷 및 2003년 과학기술정보통신위원회 국정감사 제출자료 등을 통하여 직접 수집한 내용을 수록하였다.

Ⅱ. 전자서명의 이론적 배경

1. 전자서명의 개념

전자서명은 크게 광의의 전자서명(Electronic Signature)과 협의의 전자서명(Digital Signature)으로 나눌 수 있으며, 문서나 메시지를 보낸 사람의 신원이 사실임을 증명하기 위해 사용된다[6][7].

광의의 전자서명(Electronic Signature)은 전자펜을 이용한 그래픽 기반의 서명 방식과 수기서명을 스캐닝한 이미지, 키보드를 이용한 서명, 접근제어를 위한 비밀번호 등의 방법이 포함된다. 협의의 전자서명(Digital Signature)은 대칭키 암호로 쉽게 구성될 수 없지만, 공개키 암호 시스템에 의해서 가능한 서비스다. 전달된 메시지나 문서의 본래 내용이 변조되지 않았다는 것을 입증하기 위해 사용된다.

전자서명은 수기명의를 디지털로 대체하는 것으로서 펜 대신에 공개키 암호 시스템을 매개로 하여 생성되는 정보라 할 수 있고, 이를 사용함으로써 네트워크에서 손쉬운 전송, 부인 방지, 위·변조 방지 등의 효과를 기대할 수 있다. 즉, 전자서명은 그것이 암호화되었든 아니 되었든 간에 상관없이, 어떠한 종류의 메시지에도 사용될 수 있으므로, 메시지가 변조되지 않고 온전히 도착했다는 사실과 송신자의 신원에 대해 수신자 측에서 확신을 할 수 있게 된다. 디지털 인증서(digital certificate)는 인증서 발급기관의 전자서명을 담고 있어서, 누구라도 그 인증서가 진짜라는 사실을 확인할 수 있다[8].

우리나라를 비롯하여 홍콩, 일본 등 최근 정보화 선진을 이끄는 몇몇 국가에서 제·개정하고 있는 전자서명법에 이러한 전자서명의 개념을 법·제도적 의미로 정의하고 있으며, 주로 협의의 전자서명(Digital Signature)을 채용하고 있다. 이는 광의의 전자서명(Electronic Signature) 개념이 불명확하고 기술적 안전성면에서 신뢰하기 어렵기 때문이다.

1999년 제정된 전자서명법 제2조 제2항을 보면, '전자서명이라 함은 전자문서를 작성한 자의 신원과 전자문서의 변경 여부를 확인할 수 있도록 비대칭 암호화방식을 이용하여 전자서명 생성키로 생성한 전자문서에 대한 고유한 정보를 말한다.'로 정의하고 있으며, 입법적으로 'Digital Signature'의 개념을 명문화하고 공개키 암호화방식(PKI)을

전자서명의 기술적 기반으로 채택해 명시하고 있음을 알 수 있다.

2. 전자서명의 필요성

지금까지 인터넷을 잘 이용해 왔고 전자·금융거래에서 별달리 사고나 피해를 당한 경험도 없는데 굳이 번거로운 전자서명 절차를 밟아 이메일로 전자문서를 교류하거나 서버인증서 등 상대방을 확인해야 할 필요가 있는 것인가에 대한 의문이 있을 수 있다. 그러나 유·무선 네트워크를 기반으로 하는 월드와이드웹을 절대적이고 완전한 것으로 인정할 수 없고, 최근 디지털 콘텐츠와 관련한 저작권 문제, 해킹과 바이러스에 의한 정보 도용·훼손·누출, 개인정보 오·남용과 사이버 명예훼손, 전자상거래 사기 등에 이르기까지 정보화 역기능은 전자서명을 필요로 하는 곳곳에서 현저하게 드러나고 있음을 인식하지 않을 수 없다. 결국 네티즌은 자신과 상대방의 신원을 명확히 확인하고 비대면적인 전자교류에서 신뢰성을 확보하기 위한 수단으로 전자서명을 필요로 하게 되는 것이다.

1) 정보화 역기능 최소화 기반 제공

중요거래 및 거액의 서비스 이용에서는 금융기관에 직접 찾아가서 담당자와 상담을 하고 업무를 수행하고 있지만, 최근 몇몇 보도자료에서 국내의 많은 소비자들이 오프라인에서의 은행 거래량뿐만 아니라 인터넷뱅킹 서비스를 이용하는 증가폭이 커지고 있음을 볼 수 있다.

전자서명된 공인인증서를 설치하고 양자간에 공인인증서를 확인하면서 정보를 교류하고 전자상거래, 데이터 송·수신을 하게 되면 비대면적인 사이버 환경에서 발생되는 정보화 역기능을 어느 정도 해소할 수 있을 것이라고 예상된다.

물론, 모든 인터넷 운용과정에서 공인인증서를 필요로 하는 것은 아니지만, 전자서명은 향후 기술적·제도적으로 진실을 추구하는 이용자에게 전자거래 행위의 안전을 도모하고 궁극적으로 신뢰할 수 있는 사이버 거래 환경을 구축하기 위한 솔루션으로 자리매김할 것임에 틀림없다.

2) 전자거래 편의성 향상

현재 전자서명을 사용하는 것이 절차적으로 복잡하며 보안성에 치중하다보니 느린 속도나 과다하게 요구되는 정보로 인해 일반인의 사용의지를 적극적으로 유도하지 못하는 요인이기도 하다. 일상생활에서는 편지를 주고받고, 물건을 구입하고, 서비스를 이용하는데 대부분이 인감도장과 인감증명서를 제시할 필요가 없다. 그러나 중요한 거래관계에서는 기본적으로 인감증명서를 필요로 하듯 중요한 전자거래에서도 전자서명을 필요로 하게 된다. 인터넷 사용이 일상화되면서 공인인증서의 사용은 인감도장보다도 더 많은 기능과 필요에 따라 일반화될 것이다[9]. 편리하고 안전한 전자거래를 위한 기반이기 때문이다. 더욱이 일상과 같이 편리하고 안전하며, 빠른 교류를 위한 전제가 되어야 하는 것이 전자서명의 보급·확대다. 많이 사용할수록 장·단점이 더 많이 드러나게 되고 개발도 진척되는 것이며, 초기단계에서는 컴퓨터나 인터넷으로 전자교류를 함에 있어서 인증서를 사용하고 확인하는 절차가 번거롭게 느껴질 수밖에 없겠지만 전자서명 기술의 한계와 점차 기술적·정책적 방안이 강구되어 일상의 편리함을 제공할 것이다.

2003년 현재 우리나라의 공인인증기관은 6개이며 은행을 비롯한 지역등록기관은 수백 개가 넘는다. 전자서명이 6개 공인인증기관간의 상호연동의 확보는 물론 정부인증시스템과 연동이 되게 되면 어느 한 곳에서 발급 받은 공인인증서만으로도 인터넷 뱅킹, 사이버-트레이딩, 온라인 민원, 전자상거래 등에서 인터넷의 다양한 서비스를 손쉽게 이용할 수 있다[10].

3) 전자정부 효율성 향상 기반

우리나라는 세계 최고의 정보인프라를 구축하였고 2001년 전자정부 구현을 위한 정보화사업이 본격화되면서 국민 일상생활과 밀접한 전자정부 기반 구축이 가속화되고 있다. 이러한 전자정부에서 전자서명의 사용은 기본적이며 필수적인 전제요소다. 전자교류에서 전자서명은 본인이 진정한 정보주체임을 증명할 수 있는 결정적인 수단이고, 본인의 실체와 의사를 분명하게 표시함으로써 커뮤니케이션의 안전을 기할 수 있기 때문이다. 전자서명을 일종의 '신분증' 이라고도 하는데 정확한 표현은 아니다. 전자서명은 '사이버 도장 또는 서명' 이고 전자서명이 첨부된 '공인인증서' 가 신분증(전자신분증: e-ID) 기능을 하는 것이다. 즉, 전자정부에 대하여 개인은 전자서명된 공인인증서를 제시하고 전자정부가 제공하는 사이버 민원 서비스를 이용할 수 있으며, 전화나 우편, 방문인 경우에는 현재 상황의 민원이용과 크게 다를 바 없지만 전자정부는 편리하고 효율적으로 민원서비스를 이용케 하는 기반인 것이다.

4) 사이버범죄 대응

더 이상 우리의 삶에서 온라인·오프라인의 경계를 한정 짓기 어렵다. 인터넷은 생활의 필수적인 도구이자 사이버 환경의 근간이 되고 있다. 이러한 인터넷을 기반으로 한 각종 서비스를 이용하고 비대면으로 활동하는 사이버에서 자신의 실체를 입증할 수 있는 그 무언가가 필요한 시점이다.

현재의 사이버 활동은 비대면 교류나 전자거래가 주종을 이루기에 보안과 신뢰가 전제되어야 한다. 누군지도 명확히 알지 못하고 거래계약을 맺는다는 것은 어리석은 일임에도 불구하고 전자거래에서 신원이 불분명한 자가 개설한 웹사이트에서 무심코 동참하게 되는 우를 범하게 된다. 일정한 인터넷 도메인주소로 활동만 하고 있어도 그 사이트는 신뢰할 수 있는 사이트로 속단해 버리는 인식, 이러한 것을 교묘하게 역이용 하는 것이 바로 사이버범죄다.

사이버범죄를 예방하고 해결하기 위한 대책이 많이 강구되고 있지만 그 중 가장 기본적이고 필수적인 것이 바로 전자서명의 사용이다. 전자서명은 상대방을 믿고, 안전하게 나의 개인정보 기타 중요한 메시지를 주고받을 수 있는 판단의 근거가 되며, 전자서명은 사이버에서 정보를 주고받는 당사자간의 신원을 명확히 알 수 있도록 한다. 또한 주고받는 정보에 하자가 없음을 입증하는 무결성과 타인이 불법적으로 도·감청하지 못하도록 데이터를 암호화 해주는 기밀성, 거래이후 거래자와 거래사실을 부인하지 못하도록 봉쇄하는 부인방지 효력을 가지고 있다.

3. 전자서명의 특성

전자서명 인증의 기능(효력)은 공인인증서의 기능(효력)과 같다. 공인인증서를 사용하면 본인을 입증하고, 자료에 대한 암호화로 기밀성이 보장되며, 전송중 자료의 변조를 방지해준다. 특히 개방형 네트워크인 인터넷에서 금융기관의 뱅킹서비스를 이용하면서 공인인증서를 사용하는 경우 인터넷 뱅킹 거래의 진위여부를 법적으로 보장받을 수 있고 인터넷뱅킹 거래의 보안을 유지할 수 있으며 그 외 모든 공인인증을 지원하는 전자상거래에 있어서 본인의 실명 증표로 활용할 수 있다.

1) 본인 인증/신원확인

전자·금융거래 시 전자서명이 첨부된 공인인증서를 사용함으로써 법적으로 보장된 본인여부를 확증할 수 있다. 즉, 현금카드를 이용한 인출 시에 현금자동지급기에 사용자가 입력한 비밀번호가 은행에 미리 등록해 놓은 비밀번호와 일치하는지 확인하거나, 어떤 이용자가 특정 웹사이트의 서버인증서를 확인함으로써 특정 웹사이트가 실제로 존재하고 신뢰할 만한 객체인지를 알 수 있고, 전자메시지를 주고받는 경우 발신자가 지정된 수신자에게 자신의 존재를 알 수 있도록 하여 수신자로 하여금 믿고 열람할 수 있도록 하는 효력이 있으며, 서명자의 신원을 명확히 함으로써 거래의 안전과 신뢰할 수 있게 되는 것이다.

2) 부인 방지/봉쇄

전자서명의 부인 방지 효과는 전자문서의 송신자와 송신여부를 확인하고 수신자의 수신여부를 확인하며 전자문서 송·수신자 측의 송·수신 사실의 부인을 방지하는 것이다. 예컨대, 송신자가 송신한 사실을 부인할 때 송신자만이 알 수 있는 비밀번호로 만들어진 전자서명이 첨부되어 있으면 특별한 사정이 없는 한 송신자가 그 전자 문서를 작성하고 발신하였다고 간주할 수 있는 것이다. 공인인증기반에서는 인증서, 전자서명, 암호알고리즘의 조합으로 본인의 전자서명행위에 대한 부인을 구조적으로 차단하게 되며, 서명자는 자신의 서명행위에 대하여 부인이 불가능하다.

3) 무결성

전송되는 메시지는 일정한 형태를 유지하게 되고 어느 한 부분이라도 수정되었다면 수신자의 컴퓨터는 다른 암호방식을 생성하게 되어 경고 메시지로 나타난다. 즉 발신자와 수신자간 주고받은 정보가 발신자의 본래의도대로 전달되었다는 것을 확증하는 메시지의 무결성(Integrity) 효과는 중간에 임의의 제3자가 개입할 여지를 배제하게 되는 것이다. 전자서명된 문서 기타 데이터는 무결성 검증과정을 통해 전송중 자료가 위·변조 되지 않았음이 보장된다.

주의해야 할 것은 무결성 효과에서 임의의 제3자가 개입할 여지가 배제된다는 것이지, 자료나 서비스 이용에 대한 타인의 불법적인 접근을 방지하는 것으로서 해커 등의 침입을 접근통제(Access control)하는 기능을 수행한다는 것은 아니다.

4) 기밀성

특정한 웹서버와 이용자간에 교환된 메시지는 하나의 세션키로 암호화된다. 웹서버는 이 세션키를 공개키로 암호화하여 전송하는데 하나의 세션키는 오직 한 번, 한 사람에게만 사용되기 때문에 제3자가 중간에 메시지를 도용하거나 위·변조하는 경우 해당 메시지는 동일성을 상실하게 된다. 따라서 전자서명, 공인인증서, 자료 송수신에는 다양한 종류의 강력한 암호화 과정이 적용된다. 현재 전세계적으로 안전성이 검증된 암호알고리즘을 통하여 문서 등의 기밀성이 보장되고 있다. 다만, 기밀성(Confidentiality)은 전자서명의 본래적 기능의 범주에 해당되는 것은 아니다. 전자서명은 원문(Plain Text)을 보내면서 그 원문에 첨부되는 것으로 원문자체를 암호화(Cipher Text)하는 것이 아니기 때문에 제3자가 암호화된 전자서명 자체를 도용하여 원문에 접근할 수도 있는 것이다.

4. 전자서명 공개키 기반(PKI) 인증제도 원리

1) 공개키 기반구조 원리

공개키 기반구조(PKI)는 공개키에 대한 인증서를 기반으로 한 보안 메커니즘을 제공하는 기반구조를 말하며, 암호 알고리즘을 이용한 공개키 암호시스템은 정보 보안의 핵심기술이라고 할 수 있다[11]. 또한 공개키에 대한 인증서를 발급하는 인증기관은 복수로 존재할 수 있는데 이러한 여러 개의 인증기관에서 발행한 인증서가 한 인증기관이 발행한 것과 같은 역할을 수행할 수 있도록 하기 위해서는 인증기관들이 서로의 인증서를 자신이 발급한 것과 같이 인증해 줄 수 있는 방법이 필요하다. PKI는 이러한 작용을 위한 기반구조라고 할 수 있다. 기존의 연구에서는 PKI의 개념을 명확하게 제시하지 않고 있는데, PKI의 개념을 제시하고 있는 연구 중 한 가지를 인용하자면, "정보시스템 보안, 전자상거래, 안전한 통신 등의 여러 응용분야에서 공개키 암호기술을 사용하여 암호와 인증의 활용을 용이하도록 다양한 주체들이 정책 및 각종 기술적 수단, 도구 등을 규정하고 이에 기반을 두어 등록기관, 인증기관, 디렉토리, 사용자가 네트워크 상에서 프라이버시 보호, 접근제어, 무결성, 인증, 부인봉쇄 등의 서비스를 제공하기 위해 구조적으로 결합된 사회적 기반이다." 라고 정의하였다[12].

그 동안 연구개발 수준에서 논의되던 PKI는 증권과 금융권을 중심으로 활발히 구축되고 있으며, 공공기관과 전자상거래업체에서도 잇달아 PKI 솔루션의 도입을 검토하고 있는데, 그 이유는 기존의 키 방식인 관용키 암호 시스템이 보안 측면에 있어서 불완전했기 때문이다. 관용키 암호 시스템은 송수신자 양측에서 똑같은 비밀키를 공유하는데 반해 공개키는 암호화와 복호화 키가 다르다. 데이터를 암호화 하고 이를 다시 풀 수 있는 열쇠가 다르기 때문에 완벽한 데이터 보안이 가능하고 정보 유출의 가능성은 그만큼 적어진다. 또한 PKI는 전자적 거래나 정보 유통의 신뢰성과 안정성의 확보를 위해 공개키 암호기술을 이용하여 상대방의 신원을 확인하고 정보 내용의 변경 여부 확인과 그 내용의 비밀을 유지하는 기능을 갖고 있어서 차세대 보안키로 불릴 뿐만 아니라,전자인증 등과 관련한 가장 적합한 암호모델로 주목받고 있다.

2) 공개키 기반구조(PKI)의 구성요소

가. 인증기관(Certification Authority : CA)

사용자들의 공개키를 공식적으로 인증하는 인증서를 발급하여 주는 기관으로, 신분확인, 공개키 인증, 시간 날인(Time Stamp), 증거확보, 배달매개, 분쟁해결 등의 기능을 수행한다. 신분확인은 공개키의 인증기능을 이용하여 원래 메시지 작성자의 신분을 증명해주는 것을 말하며, 공개키 인증(Public Key Certification)은 사용자의 개인키에 대응하여 공개키가 특정인에 의해 소지되고 있음과 그 쌍의 키의 유효성을 증명해주는 것을 말한다. 시간날인이란 특정한 시간과 날짜에 메시지가 발신되었음을 증명해 주는 것을 말하며, 이는 매시지 발신자가 전자서명의 효력을 거절하지 못하게 하는 증거가 된다. 이런 증거는 인증 과정을 수행하면서 사용된 전자서명에 관한 자료를 보관함으로서 이루어진다[13].

공개키 기반구조의 인증기관은 그 역할 및 기능에 따라 3단계의 계층으로 구성되며 정책승인기관(Policy Approval Authority : PAA), 정책인증기관(Policy Certification Authority : PCA), 인증기관(CA)등의 명칭으로 불린다. 인증기관은 인증과 암호키의 생성, 관리, 폐지하는 역할 등을 한다. 인증기관은 다수가 존재할 수 있는데 그 중 공인인증기관은 관련 법률을 기준으로 한 엄정한 심사를 통해 정부가 지정하고 보증하는 기관이다. 공인인증기관이 인증한 전자서명은 법령이 정하는 기명날인 .서명과 똑같은 법적 효력을 갖는다.

나. 등록기관(Registration Authority : RA)

등록기관은 공식적인 조직이나 전자서명을 통하여 등록한 사용자들을 위해 사용되는 널리 배치된 임의의 구성요소로 전자서명과 기타 거래에 있어서 핵심적인 요소들을 확인하고 인증기관이 전자인증을 생성하도록 지도하는 기관이다.

다. 인증서 저장소(Directory)

인증서 및 CRL 등, PKI와 관련된 정보들을 논리적으로 저장하고, 요청이 있을 때 정보를 배포할 수 있는 능력을 가진 임의의 중앙 집중 데이터베이스를 의미하며, 저장 및 검색하는 장소이다[14].

라. 사용자(Client)

일반적인 사람뿐 아니라 PKI를 이용하는 시스템 전체를 포함하며, 서명 생성 및 검증, 인증서 요구생성, 인증서 취소·갱신·요구, 디렉토리로부터 인증서 및 인증서 취소목록(CRL) 획득, 인증경로 검증 등의 기능을 수행한다.

3) 공개키 기반구조의 관리대상

공개키 기반구조에서 관리해야 할 대상은 인증서(Certificate), 인증서 취소목록(CRL), 상호 인증서 쌍(Cross-Certification Pair)등이 있다.

가. 인증서(Certificate)

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성되며, 이는 사용자의 공개키가 실제로 사용자의 것임을 증명한다. PKI에서 인증서의 발행 대상은 인증기관, 사용자, 서버 등으로 인증기관에게는 상위 인증기관이 하위 인증기관의 적법성을 증명하기 위해 인증서를 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증서를 발행한다.

나. 인증서 취소목록(CRL)

인증서는 인증된 공개키에 해당하는 비밀키가 노출되거나 그 공개키의 소유자가 다른 도메인으로 옮기는 경우 등 여러 가지 이유로 유효기간이 만기되기 이전에 그 효력이 상실될 수 있다. 인증기관은 이렇게 효력이 상실된 인증서들에 대한 목록을 생성해 PKI 내에서 관리한다.

다. 상호 인증서 쌍(Cross-Certification Pair)

상호 인증서 쌍은 서로 다른 인증기관들 사이에 발행하는 상호 인증서의 쌍을 의미하는 것으로 인증기관 A에 대해 다른 인증기관에서 생성한 순방(forward)인증서와 인증기관 A가 다른 인증기관에게 생성한 역방(backward)인증서 두 가지 형태가 있다. 이것은 쌍을 이루어 각 인증기관의 엔트리로 저장소에서 관리된다.

Ⅲ. 인터넷에서의 공인인증서 현황 및 전망

1. 우리나라 인터넷 서비스 이용현황

1) 초고속 인터넷 서비스 현황 및 이용실태

우리나라의 초고속 인터넷 서비스 가입자 수는 6월말 현재 11,103,828명으로 1998년 서비스를 시작한 후 빠르게 성장하였다. 주요 통신사별 현황은 KT가 전체의 539만 명(48.6%), 하나로 통신이 296만 명(26.7%), 그리고 두루넷이 129만 명(11.6%)를 차지하고 있으며, 접속방식별로는 xDSL 가입자가 전체의 56.5%인 628만 명, CATV 방식(케이블모뎀)을 이용한 가입자가 전체의 34.5%인 383만 명으로 이들 대부분을 차지하고 있다[15].

또한 구내통신망의 고도화를 위해 1999년 4월부터 '초고속 정보통신건물 인증제도'를 시행하여 아파트, 업무용 건물의 구내통신 기반시설을 고도화한 건물에 대해 2003년 6월 현재, 총 2,275건의 인증을 부여하였다. 이를 통해 아파트 내에서 인터넷접속, 전자상거래, 커뮤니티 구성 등이 가능토록 한 '사이버 아파트' 개념을 도입하는 등 가입자망 고도화가 국내 건축문화 전반에 커다란 변화의 기틀을 제공하게 되었다[16].

2) 금융권 인터넷 서비스 이용 현황

국내 금융권별 금융서비스 채널은 지속적으로 온라인화 되고 있는 추세이며, 인터넷 뱅킹, 온라인을 통한 주식 거래 및 보험가입 등이 보편화된 금융 거래 수단으로 정착되고 있으며, 이용률도 보험관련 채널을 제외하고 전반적으로 세계 상위권을 차지하고 있다.

국내 인터넷 뱅킹 이용 현황을 보면, 2003년 9월말 기준 21개 국내 은행의 인터넷뱅킹 가입자 수는 2,126만 7,000명으로 이중 개인고객은 2,031만 7,000명으로 작년 동기대비 24%증가, 기업은 95만 명으로 74.3%가 증가했다. 그리고 2003년 9월중 인터넷뱅킹 서비스 이용건수는 2억 3,226만 6,000건으로 작년 9월의 1억 6,323만 7,000건에 비해 42.8%가 증가했다[17]. 전체 인구대비 실질 등록 고객(1,441만 명) 비율도 30.8%로 노르웨이, 스웨덴, 핀란드 등 북유럽 국가(34.2%) 및 캐나다(30.7%)와 함께 세계 최고 수준에 이르고 있다. 이에 따라 인터넷 뱅킹 이용 증가율은 점자 둔화되면서 관련 시장이 안정화 단계에 접어들고 있는 추세다[18].

<표 2> 인터넷 뱅킹 등록 고객 현황

단위 : 만명, 만개

구 분	2000년	2001년	2002년	2003년 9월
개 인	409	1,092	1,702	2,031
법 인		39	69	95
합 계	409	1,131	1,771	2,126

자료: 한국은행(2000년~2002년), 디지털타임즈(2003년10월)

3) 무선 인터넷 서비스 이용 현황

무선 인터넷 서비스는 1990년대 후반 SMS, 양방향 SMS 등을 중심으로 시작해 2000년대 접어들어 nTop, n016, ezWeb 등 본격적인 무선인터넷 브랜드 경쟁에 돌입하면서 태동하였다. 그리고 2000년 초 인터넷 프로토콜로서 SKT, LGT의 WAP, KTF의 ME 서비스 상용화로 서비스 경쟁이 가속화 되었다. 2002년 말 기준으로 우리나라 무선인터넷 단말기중 WAP방식은 66%, ME 방식이 34%를 점유하고 있다.

2001년 이후 CDMA 2000-1x 및 EV-DO 서비스의 등장으로 115kbps~600kbps 급의 고속 무선 데이터 전송이 가능하게 된 환경이 구축되었다.

이동전화의 보급·확산과 무선 인터넷 기반 강화에 따라 2000년 이후 정부, 기업부문에서의 M-commerce 수요가 점차 확대되고 있다. 또한 금융과 통신의 통합환경에 대응해 유·무선을 연

<표 3> 무선인터넷 단말기 보급현황(2002)

단위 : 명, 대

구 분	SKT	KTF	LGT	합계
총 가입자수	17,219,562	10,332,770	4,790,161	32,342,493
무선인터넷 단말기 현황	14,788,640	10,241,208	4,055,122	29,084,970
CDMA 2000-1x	9,802,028	4,821,343	1,740,399	16,363,770
CDMA EV-DO	133,700	40,277	0	173,977

동한 전자복권, 영화, 공연, 여행예약, 유·무선 통합쇼핑몰, 증권시세 등 정보제공서비스, 은행잔고조회, 계좌이체 등 모바일 뱅킹 서비스, 상품구매할인을 제공하는 모바일 쿠폰서비스 등을 경쟁적으로 도입하고 있다. 2002년 말에는 신용정보를 담은 스마트칩이 내장된 모바일 지불결제 이동전화가 출시되었으며 신용카드와 이동전화 결제를 위한 통합리더 및 이동전화 전용리더기 등을 전국 가맹점에 지속적으로 설치하고 있다. 또한 네트워크형 전자화폐(e-cash)등의 서비스가 소액결제, 이체 등을 중심으로 확산되고 있으며, 이동통신사에서는 PG(Payment Gateway)등 지불·결제 인프라를 구축했고 통신과 금융이 결합된 금융유통서비스를 위해 유·무선 통합 금융포털 구축을 추진하고 있는 등 통신과 금융의 통합을 더욱 가속화할 전망이다[19].

2. 한국의 공인인증서 현황

우리나라의 전자서명 공인인증서의 총 발급수는 2003년 6월말 현재 7311,995장으로 2000년 서비스를 시작한 후 빠르게 성장하였다. 주요 인증기관별 현황은 금융결제원이 전체의 4,901,378명 67.0%, 증권전산이 1,507,244명 20.1%, 한국전산원이 536,150명 7.3%, 그리고 한국정보인증이 342,041명 4.7%를 차지하고 있으며, 90% 이상이 개인용 공인인증서 발급수량이다.[20]

이 가운데 개인 인터넷뱅킹용 공인인증서 분야의 인터넷뱅킹의 금결원과 사이버트레이딩 분야의 증권전산이 전체 시장의 90%를 차지하고 있다.

지난 3년간 공인인증서 보급 확대 차원에서 개인인증서가 금융권에서 무료로 배포됐기 때문이며, 특히 금결원 증권전산이 관련 분야에서의 특수한 지위를 이용, 보급채널을 단일화한 것이 큰 영향을 미친 것으로 볼 수 있다.

또한 금융서비스 이외에 한국전산원에서 교육부의 위탁을 받아 교사용 공인인증서 발급 7.3%를 제외하면 타 분야의 공인인증서의 적용은 2~3% 정도로 공인인증서 활용분야 확대도 시급한 실정이며, 총 개인용 공인인증서 발급수량 중에서 증권전산 및 한국정보인증 우체국 인터넷 뱅킹용의 중복이 170만장이 예상되며 유료화 전환 시 일정 정도 감소가 예상된다.

3. 공인인증서 해외 동향

미국이나 유럽의 경우 공인인증서 개념의 전자서명 이용은 약하며 주로 사설인증서로 전자서명을 이용하고 있는 추세이며, 특히 유럽의 대표적인 공인인증 사업자인 D-trust는 1999년 2만장 발행에서 2002년말 현재 유효인증서 8천장으로 축소하였다.

아시아의 경우 일본의 공인인증기관인 JCSI도 디지털 온라인 개념이 약한 사회분위기와 관행으로 시장확산에 어려움을 겪고 있으며, 말레이지아의 MSC Trustgate는 저가정책으로 시장확산을 기대하였으나 적자누적으로 사업규모가 축소되었다.

그러나, 아시아에서는 아시아 PKI포럼을 중심으로 한 아시아 8개국의 전자서명 활성화를 위한 국

<표 4> 공인인증서 발급 현황('00~03.6)

단위 : 장

기 관 명	공 인 인 증 서					개 인 용 공인인증서	법 인 용 공인인증서
	2000년	2001년	2002년	2003.6	계	2003.6누계	2003.6누계
정보인증	5,684	69,664	178,198	88,495	342,041	250,877	91,164
증권전산	8,683	73,653	310,442	1,114,466	1,507,244	1,450,950	56,294
금융결제원	12,478	1,325,377	2,500,152	1,063,205	4,901,378	4,486,456	414,992
한국전산원	0	5,996	430,014	100,140	536,150	498,944	64,206
전자인증	0	0	13,287	9,129	22,686	1,346	21,340
무역정보통신	0	0	291	2,025	2,496	235	2,261
계	26,845	1,474,690	3,432,384	2,377,910	7,311,995	6,661,738	650,257

제회의가 활발히 진행되고 있으며, 한국과 홍콩은 가시적인 성과를 나타내고 있는 선도적 역할을 수행하고 있는 국가이다. 특히 한국은 2003년 6월 현재 공인인증서 발급 수 731만장이 넘는 세계적인 공인인증서 이용 국가로 부각 되고 있다. 일본 역시 정부 주도하에 2005년까지 전국 지방자치 단체 업무 전반에 걸쳐 공인인증서를 이용하겠다는 계획을 실행 중이다.

Ⅳ. 개인용 공인전자서명 문제점

우리나라는 전자서명 공인인증시장에서 지난 2000년 첫 서비스 이후 3년 만에 공인인증서 731만장을 발급함으로써 세계 최대 전자서명 이용국가로 급성장하였다. 그러나 이러한 성장에도 불구하고 전자서명 공인인증시장에는 몇 가지 구조적인 문제를 나타내고 있다.

첫째, 독과점 문제다. 소수 인증기관에 의한 시장독점으로 다수의 인증기관들은 인증서 수입의 감소 등 수익성 악화에 시달리고 있다. 이에 대해 대다수 인증기관들은 공인인증서 발급과정에서의 구조적인 모순으로 시장 불균형이 발생하고 있으며 이를 개선하지 않을 경우 앞으로 시장 독점이 더욱 더 가중돼 많은 소비자 피해 발생이 예상된다.

둘째, 상호연동과 유료화의 문제다. 2001년 12월에 개정된 전자서명법에 따라 공인인증서간 상호연동을 강제함으로 특정 공인인증기관의 전횡을 방지하고자 하였으나, 오히려 특정분야에서의 상호연동이 미진해 시장 활성화에 걸림돌이 되고 있다. 정부는 2003년 상반기에 상호연동 현황을 조사한 결과, 120개 전자거래 기관 중 38개 기관이 상호연동을 지키지 않는 것으로 밝혀졌다. 관련업계는 상호연동이 안될 경우 소비자가 여러 개의 공인인증서를 관리해야 하는 부담이 생기며 공인인증서 도난 등의 문제도 예상되고 있다. 정부는 당초 2003년 7월 1일부터 전면유료화를 실시하기로 했으나 상호연동 및 홍보부족을 이유로 2003년 11월 1일로 연기하였고, 다시 2004년 1월로 연기하였다[21]. 2004년 1월로 유료화가 연기된 주요 문제는 공인인증서 발급의 비용 문제이다. 인증서를 가장 많이 발급해 사실상 비용 부분의 열쇠를 쥐고 있는 금융결제원이 명확한 해답을 제시하지 않아 타 인증기관들은 금융결제원의 발표에 촉각을 세우고 있다. 이는 비용에 따라 전문인증기관들의 매출이 크게 좌우될 수 있기 때문이다.

셋째, 공인인증서의 발급과 이를 관장하는 기관의 인가 남발 문제다. 정부는 한국정보인증, 한국증권전산을 첫 공인인증기관으로 지정했고, 2000년 4월에 금융결제원, 2001년 3월과 11월에 한국전산원, 한국전자인증, 2002년 3월에 한국무역정보통신을 지정하였다. 문제는 이들 6개 공인인증기관의 성격과 추구하는 목적이 다르며, 주무부처 역시 제각각 이어서 이해관계가 복잡하다는 것이다[22]. 공인인증서 시장은 처음부터 민간 영역에서 주식회사들이 시장을 구성하는 체제였으나, 비영리법인인 금융결제원과 한국전산원이 개입되면서 시장구조 자체가 와해되고 있으며, 특정분야의 독점으로 인해 전자서명 발급수량은 많아져도 전자서명 공인인증서 활성화 및 다양한 서비스 개발에 역행하는 결과를 초래하고 있다.

넷째, 공인인증서 시장경쟁의 구조적 문제다. 공인인증서 시장은 영리를 목적으로 추구하는 일반 주식회사(한국정보인증, 한국전자인증)와 시장독점적 구조를 가지는 비영리사단법(금융결제원) 및 정부기관(한국전산원), 특수목적을 위해 비영리사단법인에서 설립한 주식회사(한국증권전산, 한국무역통신)가 혼재해 있는 시장으로 사업시작부터 공정경쟁 자체가 어려운 시장 구조로 이루어져 있는 것이다.

Ⅴ. 개인용 공인인증 활성화 방안

개방형 네트워크에서, 전자상거래, 금융거래, 교육, 의료 등의 서비스가 인터넷을 통하여 활성화하는 시점에서, 거래를 하는 상대방의 신원 확인과, 보안은 중요한 과제이다. 안전한 정보 사회의 발전을 위해서 전자서명 공인인증서의 필요성과 기반 역할이 절실하다고 판단된다. 앞에서 살펴본 바와 같이 이미 드러났거나 발생 우려가 있는 전자서명의 시장 현황과 그 문제점을 토대로 공인인증시장의 활성화 방안을 다음과 같이 다섯 가지를 제시한다.

첫째, 공인인증서 이용을 확대해야 한다. 현재 개인들의 인증서 이용분야가 주로 인터넷뱅킹, 온라인주식거래에 국한되어 이용자 증가가 둔화한 상황이며, 이를 해결하는 방안으로 스마트카드를 이용한 쇼핑몰 신용카드 결제, 사이버대학, 성인인증, 온라인 복권 구입, 온라인 주주총회, 입시원서 접수, 전자정부 민원처리 서비스 등으로 이용범위를 확대하여 개인인증서 활성화를 유도해야 한다.

둘째, 무선 공인인증서 시장의 조기정착을 서둘러야 한다. 현재 무선공인인증서 서비스는 2003년 무선망 개방에 따른 컨텐츠 공급업자(Contents Provider)들의 무선인터넷 서비스 경쟁이 심화하고 있으며, 금융권의 무선인터넷 서비스 실시로 무선 공인인증서의 수요가 폭발적으로 증가되어 무선 공인인증서를 일정한 단말기에서 사용가능하도록 휴대폰 등 정보기기의 개발·보급이 확산되고 있다[23]. 따라서 무선공인인증서 서비스를 조기에

정착하기 위해 정부 차원에서 금융기관과 통신사 등의 등록기관(RA) 등 시설 확보에 지원을 증가해야 하며, 무선망 개방에 따라 유선인터넷사업자의 무선인터넷 진출에 따른 성인인증, 금융거래와 같은 무선 공인인증서 사용 가능분야를 활성화하는 정책이 뒷받침되어야 한다.

셋째, 특화된 공인인증서를 다양하게 사용할 수 있도록 시장 확대를 꾀해야 한다. 2001년 12월 개정된 전자서명법에 따라 공인인증서간 상호연동을 강제해 특정 공인인증기관의 전횡을 방지하고 있으나 상호연동이 미진해 시장활성화의 저해요소로 작용하고 있다. 그 동안 금융권을 통해서 개인인증서를 무료로 발급·배포함으로써 어느 정도의 이용자 확대라는 성과를 거둔 것이 사실이나 그 이면에 공인인증서의 다양한 사용과 기술 개발에서는 오히려 퇴보하고 있음을 부인할 수 없다[22]. 이에 따라 현재의 단일화된 개인용 공인인증서 시장을, 신용카드 사용에서와 같이 차별화되고 특화된 기능을 서비스할 수 있도록 다양한 특수 목적용 인증서 서비스를 제안하는 바이다. 이는 개인용 공인인증서를 전자상거래용, 특정분야 상호연동용, 기타 각 인증서의 요금을 세분화하여 이용자 자신의 선택에 따라 공인인증서를 사용할 수 있도록 함으로써 공인인증서의 유료화에 대한 저항 해소와 국민 편익 차원에서 이용자의 선택의 폭을 넓힐 수 있기 때문이다. 또한 공인인증기관별로 다양한 영업정책을 펼칠 수 있어 공인인증시장의 질적 확대와 함께 경영안정화의 기대 효과도 예상할 수 있다. 그 외에도 일시적·한시적으로 사용할 수 있도록 용도와 기한을 제한하는 인증서 개발도 필요하다.

넷째, 자체 시장기반 없이 공인인증서 사업만을 위해 설립된 공인인증기관은 시장경쟁에서 처음부터 불리한 여건을 지니고 시작한 상태로 볼 수 있다. 그러므로 국가 기반인프라 사업적 성격이 강한 공인인증서 사업의 원활한 수행을 위해 안정적 수익이 실현되기 전까지 정부에서 보조금 형태의 지원이 필요하다.

다섯째, 공인인증기관들의 공정한 경쟁과 독과점 해소를 위해 현재의 법제도 개정이 필요하다. 독과점 위치의 비영리사단법인은 설립 목적에 맞게 그 영역에서의 공인인증사업을 실시하게 함으로서 전문공인인증기관들이 다양하고 특화된 서비스를 개발할 수 있도록 법·제도적 장치를 마련해야 한다.

이러한 활성화 방안은 궁극적으로 공인인증 관련 기술의 개발을 촉진하고 소비자로 하여금 저비용으로 다양한 선택의 기회를 가질 수 있게 함으로써 세계 시장을 선도하는 IT 한국의 정보화기반을 마련하는 토대가 될 것이다.

참고문헌

[1] 김희선 외 5인, 2001. "국내·외 전자서명 및 인증제도 동향 분석", 정보보호학회, 정보보호학회지 4권 11호, 2001 8.

[2] 정보통신부, "2003 정보화에 관한 연차보고서", 정보통신부, p186, 2003.

[3] 정소윤, "공개키 기반(PKI)의 전자서명 인증제도 활성화 방안 연구", 연세대학교 대학원 석사학위논문, p62, 2003.

[4] 이재일, "국내전자서명 인증 현황", 정보보호뉴스, 정보보호진흥원, p8, 2003. 6.

[5] 정보통신부, "2003년 국정감사 제출자료-공인인증서 발급 현황", 정보통신부, 2003.9.

[6] 신일순 등, "전자서명인증제도", 「연구보고」 98-09, 1998.

[7] 장기식 역, "보안을 위한 효율적인 방법 PKI", 인포북, p42. 2003.

[8] www.terms.co.kr.

[9] 정보통신부, "알기쉬운 전자상거래 http://www.kisa.or.kr/digital_signature/Frame-set.htm"

[10] 이재일, "국내전자서명 인증 현황", 정보보호뉴스, 정보보호진흥원, p13, 2003. 6.

[11] Gelbord, Boaz. "Signing your 011001010: The Problems of Digital Signatures". Communications of ACM, Vol. 43, No.12. pp27~28. 2000.

[12] 남승필, "전자서명 활성화를 위한 정부역할에 관한 연구", 중앙대학교 대학원 박사학위논문, p17, 2001.

[13] 임정미, "국내 PKI의 현황과 문제점에 대한 연구", 단국대학교 대학원 석사학위논문, pp10~11, 2002.

[14] 장기식 역, "보안을 위한 효율적인 방법 PKI", 인포북, p201, 2003.

[15] 정보통신부, "2003 전기통신에 관한 연차보고서", 정보통신부, pp105~107, 2003.

[16] 정보통신부, "2003 정보화에 관한 연차보고서", 정보통신부, pp147~148, 2003.

[17] 디지털타임즈, "인터넷 뱅킹 창구거래 눌렀다", 2003. 10. 30.

[18] 한국전산원, "국가정보화백서", 한국전산원 pp137~138. 2003.

[19] 정보통신부, "2003년도 전기통신에 관한 연차보고서", 정보통신부, pp306~308, 2003.

[20] 정보통신부, "2003년 국정감사 제출자료-공인 인증서 발급 현황", 정보통신부, 2003. 9.

[21] 디지털타임즈, "개인용 공인인증서 유료화 또 연기", 2003. 11. 3.

[22] 디지털타임즈, "공인인증서 정책 재검토 필요" 2002. 12. 6.

[23] 전자신문, "공인인증시장 왜 활성화 안되는가", 2003. 5. 20.