主題

국내 전자서명인증기술 이용 현황 및 전망

한국정보보호진흥원 평가인증사업단장 이 홍 섭

차 례

1. 개 요

최근 인터넷을 이용한 전자상거래가 급속히 증가하면서 인터넷에서의 정보보호에 대한 필요성이 높아지고 있다. 전자상거래와 같은 응용 분야에서 요구되는 다양한 정보보호 기술로는 상대방에 대한 인증, 전송하는 메시지에 대한 무결성 보장 및 부인방지 제공기술 등이 있다. 현재 인터넷을 통하여 거래하는 거래 당사자들에게 신뢰를 제공하는 대표적인 기반기술로 공개키 암호방식의 전자서명 기술이 있다. 공개키 암호 방식의 전자서명 기술에서는 각 사용자의 공개키에 대한 정당성을 검증할 수 있는 메커니즘이 필요하며, 이에 대한 해결 방안이 바로 공개키 기반 구조라 할 수 있다.

공개키 기반구조를 이용하여 전자상거래가 안정적으로 활성화될 수 있도록 하기 위해서는 서로 믿고 거래할 수 있는 기술적·제도적 장치가 우선적으로 구축되어야만 한다. 이를 위해 세계 각 국에서는 전자서명인증기술의 도입 및 전자서명법 제정 등을 통해 전자상거래 활성화를 위한 기반을 구축하고 있다.

국내에서도 1999년 2월 전자서명법을 제정하고 이에 따라 공인인증기관을 지정하는 등 전자서명인증체계 구축에 만전을 기하고 있다. 최근 정부를 중심으로 인터넷을 통한 민원서류 발급 서비스 등 효율적인 전자정부구축에 박차를 가하고 있으며, 아울러 민간분야에서도 전자서명인증 기반의 인터넷 뱅킹, 사이버 증권거래 등 전자서명인증서비스의 활용범위가 점차 넓어지고 있다.

본고에서는 이와 같이 인터넷의 핵심 요소로 자리를 잡아가고 있는 전자서명인증서비스와 관련하여 국내 관련 법·제도 및 전자서명인증관리체계의 동향을 살펴보고 관련 서비스의 국내 구축 및 이용현황 그리고 국가간 전자서명 상호인증 추진 현황을 분석하여 향후 전자서명인증체계에 필요한 연구분야 및 발전 방향들을 짚어보고자 한다.

2. 전자서명 인증기술

2.1 전자서명의 개념

현대사회는 신뢰를 기반으로 하는 고도의 지식정보화 사회로 급변하고 있으며, 이에 따라 인터넷상에

서 유통되는 정보의 가치 또한 커지고 있다. 특히, 인터넷상에서 이루어지는 증권거래나 인터넷 뱅킹 등과 같은 전자거래는 온라인으로 수행된다는 특성으로 인하여 거래하는 상대방을 확인할 수 없고, 전송되는 메시지의 위·변조 위협이 항상 존재하게 된다. 이는 신뢰를 기반으로 하는 전자상거래의 발전을 크게 저해하는 요소로 작용되고 있으며, 이를 해결하기 위한 방법으로 공개키 암호방식의 사용이 널리 확대되고 있다.

공개키 암호방식은 비밀키를 공유해서 사용하는 비밀키 암호방식과 달리, 수학적으로 연관된 서로 다른 공개키·개인키쌍을 생성하여 공개키를 공개함으로써 송·수신자간에 비밀키의 교환 없이도 공개된 키를 이용한 암호화가 가능하다. 특히, 공개키 암호방식은 기존의 비밀키 암호방식이 제공하는 기밀성 및 무결성 뿐만 아니라, 인증 및 부인방지의 기능도 제공한다.

전자서명은 공개키 암호방식의 한 응용으로 전자문서에 수기서명과 같은 서명효과를 부여하는 전자적 서명 방식으로, 서명에 참여한 사용자에 대한 인증과 서명 대상인 전자문서에 대한 인증을 수행한다. 또한, 서명의 검증자 또는 제삼자에 의한 서명의 위·변조 및 서명자에 의한 서명문 전송 행위 부인과 같은 형태의 부정 행위를 방지할 수 있다. 그러므로 전자서명을 이용하여 원본과 사본의 구별이 불가능하고, 위·변조가 용이한 전자문서에 대한 부정 행위를 방지할 수 있다.

전자서명이 위와 같은 기능을 제공하기 위해서는 정당한 서명자만이 전자서명을 생성할 수 있어야 하고, 누구든지 전자서명의 서명자를 검증할 수 있어야 하며, 서명자는 서명한 사실을 부인할 수 없어야 한다. 또한, 서명한 문서의 내용은 변경할 수 없어야 하며, 해당 문서의 서명을 다른 문서의 서명으로 재사용하는 것이 불가능해야 한다.

전자서명의 절차는 일반적으로 다음과 같다. 먼저, 전자서명을 사용하기 위해서 사용자는 자신의 공개키와 개인키 쌍을 생성하여야 한다. 이후, 서명자는 자신의 개인키로 서명하고자 하는 메시지의 해쉬값에 전자서명하고, 메시지와 해당 메시지의 전자서명을 검증자에게 전송한다. 검증자는 서명자의 공개키를

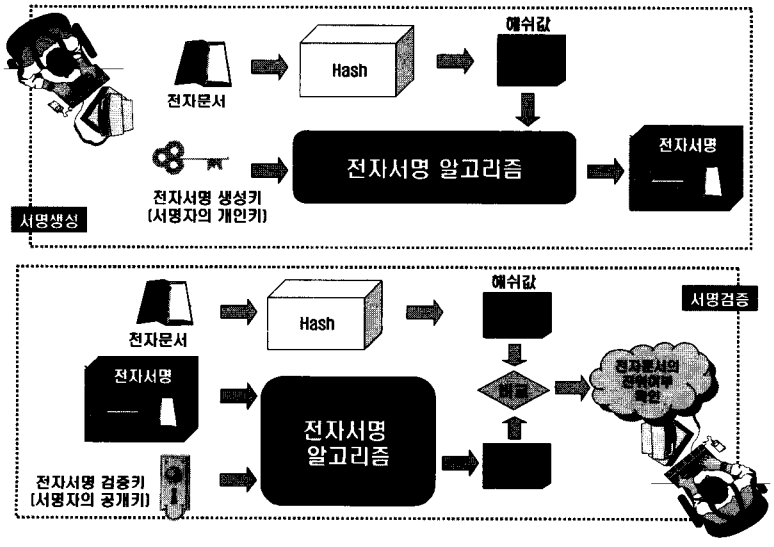

그림 1. 전자서명의 생성과 검증

이용하여 수신한 전자서명에서 서명자가 생성한 메시지의 해쉬값을 구한 후, 함께 수신된 메시지에 대해 해쉬값을 생성하여 서로 비교함으로써 서명을 검증할 수 있다.

2.2 공개키 기반구조(PKI)

전자상거래의 정착을 위한 선결요건으로 전자서명을 바탕으로 하는 안전한 전자상거래 환경 구축이 필요한데 공개키 기반구조(Public Key Infrastructure, PKI)는 이러한 목적을 달성하기 위한 기반기술로써 공개키 암호기술을 이용하고 있다.

일반적으로 공개키 기반구조를 구성하는 최소 객체로는 (그림 2)와 같이 인증기관과 등록기관, 디렉토리, 사용자가 있다. 인증기관(Certification Authority, CA)은 어떤 정보가 거래당사자와 연관되어 있음을 검증할 수 있게 해주는 신뢰할 만한 기관으로 독립된 신뢰기관 역할을 수행한다.

인증기관은 역할 및 기능에 따라 계층적 또는 네트워크 관계로 구성될 수 있는데, 국내에서는 한국정보보호진흥원에서 운영하고 있는 최상위인증기관이 신뢰의 정점역할을 수행하고 하위에 공인인증기관이 존재하는 계층적인 구조를 택하고 있다. 등록기관(Registration Authority, RA)은 사용자가 인증기관과 지역적으로 멀리 떨어져 있거나 인증기관 업무의 효율적인 분산을 위해 사용자들의 인증서 발급 신청시 인증기관 대신 그들의 신원과 소속을 확인해 주는 기관이다. 등록기관이 사용자의 신원확인후 인증서 발급신청을 인증기관에게 제출하면 인증기관은 등록기관의 인증과정을 거쳐 사용자의 인증서를 발급하고 이를 사용자에게 전달하게 된다. 디렉토리(Directory)는 인증서와 인증서 폐지목록(CRL)의 가용성을 제공하기 위해 사용자 관련정보, 인증서, 인증서 폐지목록 등을 저장하거나 검색할 수 있는 장소이다. 마지막으로 공개키 기반구조의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미

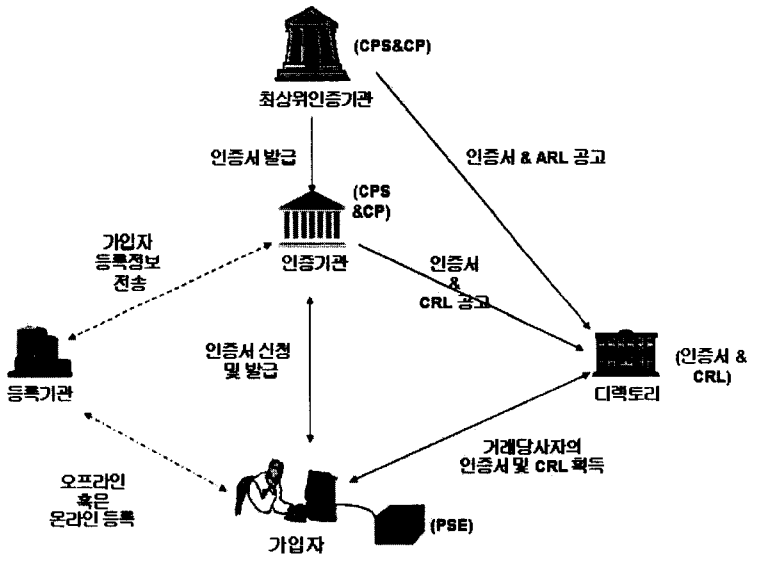

그림 2. 공개키 기반구조

한다.

공개키 기반구조의 기술적 메커니즘은 크게 X.509 기반의 인증서 프로파일, 인증서와 인증서 폐지목록의 발급, 공고 등을 위한 표준 프로토콜과 이들의 유효성을 검증하는 프로토콜 등으로 구성되어 있다. 이러한 기술의 표준화는 국제표준화 단체인 ITU-T의 X.509나 IETF의 PKIX 워킹그룹에서 활발히 진행 중에 있다.

3. 국외 동향

전자서명인증체계의 구축이 각 국가마다 최대의 현안으로 떠오르고 있는 것은 주지의 사실이며 여기서는 주요 국가에서 추진하고 있는 전자서명인증관련 기반법, 전자서명인증체계, 인증기관 현황 등에 대하여 살펴보고자 한다.

3.1 미국

미국은 1995년에 유타주를 시작으로 모든 주에서 전자서명에 대한 법률을 제정하였으며, 연방 차원에서 2000년 「국제 및 국내 전자상거래에서의 전자서명법」 (Electronic signatures in Global and National Commerce Act : 통칭 연방 전자서명법, E-sign법)을 제정(2000. 10. 1 시행)하였다. 연방 전자서명법에서는 인증기관의 허가·감독에 관하여 규정하지 않으며, 각 주의 전자서명법에서 이를 규율하도록 하였다. 미국의 주요 공인인증기관으로는 Verisign이 있다. Verisign은 세계 최대의 인증서비스를 제공하는 업체로서 Web Site Trust Services, Payment Processing 등의 인증, 검증, 지불서비스, 도메인명 등록서비스를 업체 및 고객에게 제공하고 있다.

3.2 독일

독일은 1997년 8월 「디지털서명에관한법률」을 제정·시행하고, 유럽연합의 전자서명지침에 합치되도록 2001년 5월 이를 개정하였다. 개정법에서는 법에서 정한 요건을 충족하는 공인인증서를 기반으로한 공인전자서명에 대하여 수기서명과 동등한 법적효력을 부여하였으며, 공인전자서명의 법적효력에 대해서만 민법, 행정절차법 등에서 별도로 규정하는 형식을 취하였다. 독일의 PKI에서는 독일연방통신우편국(RegTP)이 최상위인증기관의 역할을 담당하고 있으며 그 밑에 공인인증기관으로 연결되는 2계층의 구조를 가지고 있다. 공인인증기관은 법적 효력을 갖는 가입자 인증서를 발급하기 위하여, 최상위인증기관으로부터 발급받은 인증서에 대응되는 전자서명 생성키를 사용해야 한다.

3.3 일본

일본은 「전자서명및인증업무에관한법률」을 제정(2000년)하여 2001년 4월부터 시행하고 있다. 일본은 인증업무 수행과 관련한 허가제 등과 같은 규제는 없으며 다만, 특정인증업무를 수행하고자 하는 자는 주무대신의 인증을 받을 수 있도록 하는 특정인증업무 인정제도를 도입하고 있다. 이는 한 기관을 공인인증기관으로 지정하는 방식이 아니라 특정인증업무에 대하여 인정하는 방식을 의미한다. 일본의 경우 중앙부처 PKI를 GPKI(Government PKI)라 부르고 지방자치단체 PKI를 LGPKI라 부른다. 민간인증기관이 전자서명법에 의해 공인인증기관으로 허가를 받을 경우 BCA(Bridge CA)를 통하여 정부인증기관과 상호연동할 수 있으며, 이때 법적 효력을 갖는 인증서를 법인 및 민간인에게 발급할 수 있다. 일본 정부의 각 부처들은 독자적으로 인증기관을 운영하고, 정부부처 인증기관간의 상호연동을 위하여 BCA를 둘 예정이다.

3.4 호주

호주의 전자서명 관련 법률은 Electronic Transaction Act(ETA)로서 2001년 7월 시행되었다. 주요 관련 부서로는 NOIE(National Office for the Information Economy)가 있다. 과거 호주의 PKI 공공부문(Public Sector)은 OGO (Office of Government Online)가 담당하고 민간부문(Private Sector)은 NOIE에서 담당하였으나, 현재 OGO의 기능이 NOIE로 통합되어 NOIE에서 민간부문과 공공부문 PKI를 통합하여 운영하고 있다. 예를 들어 민간인증기관인 eSign에서는 공공부문인 Victoria 주정부를 하부인증기관으로 두고 인증서를 발행할 수 있으며 Victoria 주정부에서는 eSign에서 발행받은 인증서를 바탕으로 공공부문 인증서를 발행할 수 있다. 주요 인증기관은 Full Accreditation인 ATO(Australian Taxation CAPL(Certification Australia Pty. Entry-level Accreditation인 eSign Australia 이 있다.

4. 국내 현황

4.1 국내 공인인증체계

전자서명 인증제도의 구축·추진을 목적으로, 공개키 암호기술에 기반한 전자서명에 대하여 법적인 효력을 부여하는 전자서명법이 1999년 2월 제정되어 동년 7월부터 시행되어 오고 있으며 이를 근간으로 공개키기반구조에 기반한 국내 전자서명인증체계가 구축되었다. 이후 전자서명의 기본적인 요건을 갖춘 경우에는 서명의 법적 효력을 인정하는 등 기술중립적인 사항들을 새로 명시하여 2001년 12월 전자서명법을 개정하였다.

국내 공인인증체계는 한국정보보호진흥원이 최상위인증기관의 역할을 담당하고, 전자서명법에 의하여 지정된 6개의 공인인증기관이 일반 사용자를 대상으로 인증서비스를 제공하는 형태로 구성되어 있으며 정부를 포함한 각 기관별 역할은 (그림 3)과 같다.

2000년 2월, 한국정보인증㈜과 한국증권전산㈜이 공인인증기관으로 지정된 이후 동년 4월 금융결제

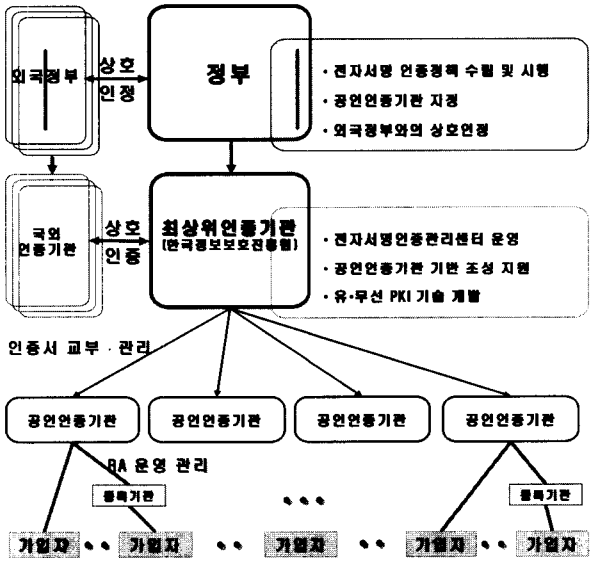

그림 3. 국내 전자서명 인증관리체계도

표 1. 공인인증기관 현황

구분	[illegible]	[illegible]	금융결제원	[illegible]	한국전자인증㈜	㈜한국무역정보통신
영문명	SignGATE	SignKorea	yessign	NCASign	CrossCert	TRADESIGN
지정일	2000년 2월	2000년 2월	2000년 4월	2001년 3월	2001년 11월	2002년 3월
웹주소	www.signgate.com	www.signkorea.com	www.yessign.or.kr	sign.nca.or.kr	www.koreacert.com	www.tradesign.net

원이, 2001년 3월과 11월에 각각 한국전산원과 한국전자인증㈜이 공인인증기관으로 지정되었고, 2002년 3월 ㈜한국무역정보통신이 지정되어 총 6개 기관에 이르게 되었다.

4.2 전자서명인증서 이용 현황

2000년 조달 분야를 시작으로 하여 첫 공인인증서비스가 도입된 이후 인터넷 뱅킹, 사이버 증권, 전자민원서비스 등 전자서명인증서 이용 분야는 지금도 꾸준히 늘어나고 있는 추세이다. 공인인증서 이용자수는 서비스가 제공된 첫해인 2000년에는 5만여명, 2001년에는 190여만명에 지나지 않았으나, 2002년도에는 전자민원서비스와 인터넷 뱅킹, 교육행정정보시스템, 전자 조달 등 인터넷을 이용한 각 종 서비스의 활성화로 인하여 580여만명으로 크게 증가하였다.

표 2. 연도별 공인인증서 이용자수 현황

구 분	2000. 12.	2001. 12.	2002. 12.
인증서 이용자수	51,836	1,917,638	5,772,505

표 3. 종류별 공인인증서 이용자수 현황

구 분	2000.12.	2001.12.	2002.11.
서버용 인증서	38	228	348
법인용 인증서	33,328	623,560	1,343,322
개인용 인증서	18,470	1,293,850	3,878,342

현재 전자서명인증서 이용이 가장 활성화 된 분야는 인터넷 뱅킹 분야로서 21개 시중은행이 전자금융거래의 안전성 및 신뢰성 확보를 위해 자사 고객을 대상으로 전자서명을 이용한 인터넷 뱅킹 서비스를 제공 중에 있다. 2000년 1만여명에 불과하던 인터넷 뱅킹 인증서 이용자 수는 정부의 적극적인 공인인증서 보급 정책에 힘입어 2002년에는 350여만명으로 급증하였다. 금융감독원의 전자금융거래지침에 의해 사설인증서가 공인인증서로 전환되는 2003년 5월부터는 그 이용자 수가 급격히 늘어날 것으로 예상된다.

사이버 증권 분야는 인터넷 뱅킹에 비해 다소 준비가 늦었지만, 2002년 상반기부터 신영, 교보 등 4개 증권사를 중심으로 전자서명 이용서비스를 제공하기 시작한 바 있다. 2002년 12월부터 세계 최초로 휴대폰을 이용한 공인전자서명인증 서비스를 사이버 증권 분야에서 제공 중에 있으며, 2003년 1월부터는 대부분의 증권사에서 전자서명을 이용한 사이버 증권 서비스를 제공할 계획이다. 2002년 말 현재 사이버 증권 분야의 인증서 이용자 수는 20만 여명에 달하고 있다.

한편 정부는 인터넷을 통한 전자민원처리시 민원인의 신원확인, 관련정보의 비밀성 등을 제공하여 행정기관 방문이 필요없는 One-Stop/Non-stop 민원행정서비스기반 구축을 추진하여 왔다. 그 결과로 2002년 상반기 첨부서류가 없고, 본인확인이 필요한 업무부터 우선적으로 전자서명을 적용하여 민원업무를 인터넷으로 처리하고 있으며, 현재 그 적용 대상 분야를 계속적으로 확대하고 있다.

앞으로도 전자서명 이용은 대학의 학사행정, 기업

간의 전자계약 솔류션, 기업 내부의 PC 보안 및 그룹웨어, 의료, 무역, 무선 전자거래 등으로 그 분야가 크게 늘어날 것으로 보이며, 이에 따라 그 이용자도 급격히 증가할 것으로 예상된다. 특히 무선 인증서비스가 본격화 될 것으로 예상되는 2003년 이후에는 그 수요가 더욱 더 늘어날 것으로 기대된다.

4.3 무선 공인인증 서비스

최근 휴대폰 등 무선 단말기를 이용한 인터넷 사용이 급증하면서 무선 분야에서의 인터넷 뱅킹, 사이버 증권, 인터넷쇼핑몰 이용 등 무선 전자거래 역시 확산되고 있다. 이에 따라 무선 인터넷에서도 유선과 동일한 수준의 정보보호 서비스가 요구되고 있다. 그러나, 기존의 유선 시스템에서 사용하던 보안 솔루션을 그대로 무선에 적용한다는 것은 아직까지 매우 어려운 일이다. 따라서 무선 데이터 통신환경에서 사용할 수 있는 무선 PKI 기술 개발의 중요성이 점차 부각되고 있다.

무선 PKI란 기존의 유선 PKI의 구성요소를 그대로 이용하며, 무선환경에 적합하도록 기능을 최소화하여 변화시킨 것이다. 무선 PKI 기술을 개발하기 위해서는 유선과 달리 무선 단말기와 서버간의 제한된 대역폭, 무선 단말기의 처리능력 및 제한된 메모리 등을 고려해야 한다.

국내 무선 전자서명인증체계를 구축하기 위해서는 관련 기술규격 및 표준, 제도 및 절차, 공인인증기관 평가기술 및 운용기술 등에 대한 개발이 필요하다. 이에 따라 정부는 한국정보보호진흥원, 관련 업체 등과 2000년 12월 무선인터넷 PKI 기술기준협의회를 구성하여 무선 인터넷 PKI 모델과 무선 인터넷 PKI 기술기준 4종을 개발한바 있으며, 2001년 8월 무선 CA 시스템 구현에 필요한 무선 PKI 기술규격 11종을 개발한바 있다.

현재 공인인증기관은 2001년부터 이동통신사와 협력하여 무선인증시스템을 구축 중에 있으며 휴대폰 가입자를 대상으로 무선 공인인증서비스를 준비중에 있다. 한국증권전산은 SKT 무선인증시스템에 대하여 2002년 8월 한국정보보호진흥원의 실질심사를 통과하였으며 증권분야 고객을 대상으로 2002년 12월부터 상용서비스를 제공 중에 있다. 한국정보인증 역시 2002년도에 LG텔레콤 무선인증시스템 및 KTF 인증시스템에 대해 한국정보보호진흥원의 실질심사를 통과하였으며 현재 시험운영을 준비중에 있다. 이외에도 한국전자인증 및 금융결제원이 무선인증서비스를 제공하기 위해 시스템을 구축 중에 있다.

현재 국내에서는 한국정보보호진흥원이 공인인증기관, 이동통신업체 등과 협력하여 전자서명인증관리체계에 적합한 무선 인터넷 PKI 운용기술을 지속적으로 개발 중에 있다.

4.4 상호연동

가. 공인인증기관간 상호연동

초기에 각 공인인증기관들이 독자적인 인증시스템을 구축한 관계로 사용자가 다른 공인인증서비스를 이용하려면 각 기관에서 별도로 공인인증서를 발급받아 사용하여야만 했다. 따라서, 사용자가 하나의 공인인증기관에만 등록하면 모든 거래에 전자서명을 이용할 수 있도록 공인인증기관간 상호연동의 필요성이 제기되었고, 2000년부터 정보통신부와 한국정보보호진흥원은 공인인증기관간 상호연동을 위하여 법·제도적, 기술적 조치를 취하여 왔다.

법·제도적 측면에서는 전자서명법을 개정(2002. 4. 1 시행)하여 정당한 이유없이 특정 공인인증기관의 공인인증서만을 요구하지 못하도록 상호연동을 의무화하였고, 사고발생 시 공인인증기관이 그 손해를 우선 배상하도록 하여 면책을 위해서는 자신이 과실 없음을 입증하도록 규정하였다. 또한, 가입자 신원확인의 신뢰성 확보를 위해 신원확인 절차 및 방법을 시행규칙에 구체적으로 규정함으로써 상호연동을 위

한 법·제도적 환경을 마련하였다.

기술적 측면에서는 2000년 8월 "PKI 상호연동 기술규격"을 마련하고 이를 공인인증기관에 배포하여 구현하도록 함으로써 상호연동을 위한 기반을 마련하였다. 그러나, 금융권에서는 추가적으로 사용자의 편의성 제고 및 인증서 소유자의 주민등록번호 확인, 실시간 인증서 상태확인 서비스의 단일화를 요구하였고, 이에 따라 정보통신부는 한국정보보호진흥원과 2002년 3월 관련 기술규격 마련하였으며 각 공인인증기관은 2002년 10월 이의 구현을 완료하였다.

2003년부터는 공인인증기관간 상호연동성이 확보되어 각종 전자거래에 전자서명을 적용하기 위한 응용프로그램 개발이 용이해져 전자서명 이용분야의 확산이 기대되며 국민들이 공인인증기관에 관계없이 하나의 공인인증서로 다양한 전자거래에서 전자서명을 이용할 수 있을 것으로 기대된다.

나. 정부 전자서명인증체계(GPKI)와의 상호연동

현재, 국내에는 민간분야의 NPKI(National PKI)와 별도로 전자정부구현을 위한 민원서비스혁신(G4C) 사업의 일환으로 정부 전자관인 분야의 GPKI(Government PKI)가 운영되고 있다. 전자정부의 전자민원행정서비스는 인터넷으로 모든 민원이 처리됨에 따라 서비스의 신뢰성을 위해 전자서명의 이용이 꼭 필수적이며, 이에 따라 2001년 3월에 시행된 전자정부구현을위한행정업무등의전자화촉진에관한법률에 기반해 행정자치부 산하의 정부전산정보관리소(GCC : Government Computer Center)에서 GPKI 인증서를 발급하고 있다.

국내 민간분야의 공인인증체계와는 별도로 전자민원서비스를 위한 공공분야의 인증체계가 구축됨에 따라 두 인증체계간의 상호연동의 필요성이 대두되게 되었다. NPKI의 가입자가 공인인증서를 이용해 행정기관에 민원을 요청하는 경우, 민원을 처리하는 행정기관은 먼저 민원인의 전자서명을 검증해야 한다. 하지만, 민원인과 행정기관이 신뢰하는 최상위인증기관이 상이하기 때문에 전자서명의 검증은 실패하게 된다. NPKI의 가입자가 행정기관의 전자서명을 검증할 경우에도 같은 이유로 검증은 실패하게 된다.

이러한 문제점을 해결하기 위해 정보통신부, 행정자치부, 한국정보보호진흥원은 인증서신뢰목록(CTL : Certificate Trust Lists) 방안을 NPKI와 GPKI간 상호연동 방안으로 결정하고 "인증기관간 상호연동을 위한 CTL 기술규격"을 제정하였다. 그리고, 한국정보보호진흥원은 2002년 4월 인증서신뢰목록의 생성 및 검증 모듈을 구현하고 관련 기술을 공인인증기관들에게 이전하였다.

이러한 NPKI와 GPKI간 상호연동 추진의 결과, 2002년 4월부터 두 인증체계간 상호연동이 수행되고 있으며, 현재, 약 400 여종의 전자민원 서비스가 국민들에게 제공되고 있다.

다. 국가간 전자서명 상호인증

인터넷을 이용한 글로벌 전자상거래가 확대되면서 국가간에도 전자서명을 이용할 수 있는 환경에 대한 요구가 제기되고 있다. 즉 글로벌 전자상거래를 활성화하기 위하여 국가간 트랜잭션에 대한 안전성과 신뢰성이 요구되고 있으며 이를 위한 수단으로써 전자서명의 활용이 대두되고 있는 것이다.

한국정보보호진흥원은 국가간 전자서명 상호인증 기반을 조성하기 위한 활동의 하나로 2001년 6월부터 한국, 일본, 싱가포르, 대만 등 4개국과 국가간 전자서명 상호인증 추진을 위한 양해각서를 체결하고 국가간 실증프로젝트를 추진해오고 있다. 상호연동 실증 프로젝트에서는 정기적인 회의를 통하여 국가간 전자서명 상호인증을 위한 기술규격을 개발하고 이에 기반하여 상호연동 실험을 수행해 오고 있다. 국제적으로 이와 유사한 전자서명 상호인증을 위한 프로젝트들이 있었으나 대부분 한 국가내에 있는 인증기관간의 상호연동을 목적으로 하거나 전자서명인증 관련

제품 개발 업체들을 중심으로 제품간의 상호연동성을 검증하는 것을 주된 내용으로 하고 있다. 그러나 현재 4개국간 진행되고 있는 실증프로젝트는 아시아권의 여러 국가들이 참여한 가운데 각 국에서 법적으로 공인된 인증기관을 대상으로 하였다는 점에서 그 차별성을 찾을 수 있을 것이다.

지금까지의 실증프로젝트 실험결과는 국가간 전자서명 상호인증의 실질적인 적용 가능성을 성공적으로 보여주고 있다. 전자서명 상호인증 실험을 통하여 아시아 국가간 전자서명인증 구성요소간 상호연동은 완료 단계에 이르렀으며 현재 응용서비스 상호연동을 위한 단계적 실현방안이 순조롭게 추진되어 가고 있다. 아울러 실증프로젝트를 통한 아시아권 국가간의 긴밀한 협력관계는 향후 국가간 전자서명 상호인증을 추진함에 있어서 든든한 밑거름이 될 것이다.

5. 전자서명인증체계 발전 추세

현재 기반이 조성된 국내 전자서명인증관리체계를 안정적으로 발전시키기 위해서는 관련 제도의 지속적 정비, 유·무선 PKI의 통합 등 사용자의 편의성 제고뿐만 아니라 새로운 응용분야를 추가 발굴함으로써 이용분야를 확산하고자 하는 노력이 지속되어야만 할 것이다. 본 절에서는 향후 전자서명인증체계가 발전해 나갈 것으로 예상되는 여러 가지 분야에 대해 이야기 하고자 한다.

5.1 차세대 인터넷을 위한 전자서명인증 기술 개발

무선 통신의 진화 및 발달에 따라 Mobile IP, All-IP 등 다양한 방식의 무선 인터넷 기술이 등장하고 있고, 이에 따라 가까운 미래에 사용자에게 글로벌 로밍과 Mobile IP 기반의 이동서비스가 제공될 것으로 예측된다. 무선 통신을 이용한 인터넷 제공기술은 특성상 유선에 비하여 보안이 취약한 실정이나 Mobile-IPv6 기반의 4세대(Beyond IMT 2000)인터넷에서의 보안 기술은 아직 그 연구가 미진한 것이 현실이다. 특히 글로벌 로밍 등 무선 단말기의 도메인간 이동이 이루어질 경우 사용자 인증, 기밀성, 무결성 기능 등은 핵심적인 보안이슈로 떠오를 것이다. 그러나 단말기의 핸드오프 및 글로벌 로밍시 사용자 및 네트워크 간 인증은 기존 보안방식이 확장성에 한계를 갖는 반면, 다양한 분산망 환경에서의 구축을 전제로 설계된 전자서명 인증 기술은 확장성이 용이하여 기존의 문제점을 쉽게 해결할 수 있을 것으로 보인다.

IMT-2000 등 3세대 이동 통신 시장을 주도한 우리나라가 Beyond IMT 2000인 4세대 이동 통신 시장에서도 선도적인 역할을 할 수 있는 기반을 제공하고 4세대 이동통신 서비스를 준비 중인 이동 통신 사업자가 다양한 무선 인터넷 서비스를 안전하게 제공할 수 있는 기반을 마련할 수 있도록 지금부터 글로벌 전자서명인증에 대한 기술적인 준비가 이루어져야 할 것이다.

5.2 유·무선 전자서명인증체계 통합을 통한 단일 전자서명인증 인프라 구축

국내 전자서명인증체계는 유선 전자서명인증체계가 구축된 상태에서 무선 전자서명인증체계가 구축됨으로써 그 체계가 이원화되어 있다. 따라서 유선 전자서명인증체계와 무선 전자서명인증체계간에 상호연동이 어려운 문제점이 있고 사용자는 유·무선별로 별도의 인증서를 사용하여야 하며, 공인인증기관에서는 시스템 구축을 이원화해야 하고 응용서비스도 별도로 제공해야 하는 상황이 발생하게 된다. 그러나 유·무선 전자서명인증체계를 단일체계로 통합하게 되면 사용자의 편의성을 제고하고 공인인증서비스 제공에 필요한 시스템 및 응용서비스를 단일화할 수 있을 것이다.

유무선 통합 전자서명인증체계의 기본적인 형태는 이러한 분리된 인증서의 통합뿐 아니라, 유선과 무선

네트워크의 구별 없이 인증서를 관리할 수 있는 프로토콜의 통합을 의미한다. 향후 무선의 환경을 고려하면서 유선환경과 호환성을 유지할 수 있는 통합 기술규격을 개발함으로써 단일 전자서명인증체계 인프라를 구축하고자 노력이 지속적으로 있어야 할 것이다. 이러한 노력으로 추후 통합된 하나의 전자서명인증체계 환경이 구축된다면 사용자의 편의성 제공에 크게 기여할 것으로 생각된다.

5.3 생체인증 등 Non-PKI 기반의 차세대 전자서명인증기술 연구

암호학 및 생체인증기술 등의 발전으로 공개키 알고리즘을 좀더 보완하거나 대체할 수 있는 다양한 비공개키 기반의 전자서명기술이 개발 중에 있다. 지문 등의 생체인증 기술을 PKI기반 전자서명기술에 접목시킬 경우 스마트카드 등과 같이 인증서 및 개인키와 연계된 물리적인 장비에서 보안성 및 사용자 편의성을 획기적으로 개선할 수 있다. 또한 생체인증기술은 단순히 전자서명에 대한 보조수단이 아니라 제한된 응용분야에서는 PKI기반의 전자서명을 대체할 수 있는 기술로서의 가능성이 보이고 있다.

따라서 비공개키 기반의 기술분야와 PKI를 접목하는 연구의 일환으로 생체인증을 이용한 비공개키기반 전자서명 기술 등에 대한 연구가 향후 지속적으로 추진되어야 할 것이다.

6. 맺음말

21세기 정보사회를 주도하는 정보기술은 컴퓨터와 정보통신기술의 발전에 힘입어 인류 생활터전을 지식정보기반 사회로 정착시켜나가고 있다. 21세기의 경제·사회적 측면에서 가장 두드러진 특징은 유·무선 인터넷의 비약적인 확산과 전자상거래의 활성화라고 할 수 있다. 이는 장차 인터넷 기술발전과 확산을 바탕으로 전자상거래의 활성화가 국가경제력과 국제경쟁력을 좌우하는 주요요인으로 평가될 것임을 의미한다고 볼 수 있다.

우리나라에서도 매년 인터넷 이용자가 급속하게 증가하고 있으며 이는 그대로 전자상거래의 활성화로 연결되고 있다. 유·무선 인터넷에 기반한 전자상거래에서의 신뢰성은 궁극적으로 사용자간 인증, 기밀성, 부인방지 등의 전자서명 기술에 의해서 보장된다. 그러나 이러한 전자서명 인증기술이 널리 보급되고 확산되기 위해서는, 유무선 전자서명인증체계의 통합, 차세대 인터넷을 위한 인증기술 개발 등 기술적인 준비가 지속적으로 이루어져야만 하고, 다양한 응용 분야의 발굴을 통해 서비스를 다양화하고자 하는 노력도 있어야만 할 것이다.

정부의 적극적인 지원 및 육성책에 힘입어, 인터넷 뱅킹, 사이버 증권거래, 전자민원 서비스 등 이제 전자서명을 이용한 전자거래는 점차 일상 생활화되어 가고 있다. 이러한 여세를 몰아 전자서명 인증제도가 사회에 안정적으로 정착할 수 있도록 우리 모두는 최선을 다하여야 할 것이며, 전자상거래 정보보호의 필요성과 중요성을 국민 모두가 인식하고 안전한 전자거래에 대한 의식개혁이 이루어 질 수 있도록 대국민 홍보 및 인식 제고 등 전자서명 이용활성화를 위한 노력을 아끼지 말아야 할 것이다.

이 홍 섭

1979년 : 한양대학교(공학사) 1985년:한양대학교(공학석사) 1999년 : 대전대학교(공학박사) 1980년~1996년 : 한국전자통신연구원 실장 1996~현재 한국정보보호진흥원 단장

주관심분야: 전자서명인증 활용, 정보보호시스템 보안성 평가, 정보보호 정책 및 관리