情報保護學會論文誌
第14券 第2號, 2004. 4

정부의 행정전자서명인증체계(GPKI) 활성화 및 발전방안

추 경 균[a)†], 김 종 배[b)], 류 성 열[c)‡]
행정자치부[a)], (주)이엔터프라이즈[b)], 숭실대학교[c)]

A Study on activation and improvement of the Government PKI

Kyung-Kyun Choo[a)†], Jong-Bae Kim[b)],Sung-Yul Rhew[c)‡]
Ministry of Government Administration and Home Affairs[a)],
E-Enterprise Co.,Ltd[b)], Soongsil Univ.[c)]

요 약

본 연구에서는 국내·외 인증체계 현황에 대한 검토·분석과 현재 운영되고 있는 정부의 행정전자서명에 대한 인식·이용실태 설문조사를 통하여 행정전자서명인증체계의 문제점을 도출하고, 이에 대한 활성화 및 발전방안을 제시하였다. 본 연구에서 제시한 행정전자서명인증체계(GPKI)와 민간전자서명인증체계(NPKI)간의 상호연동, 표준보안 API의 활용, 인증서의 발급·재발급·갱신·폐지 등의 관리, 보안성·안전성 측면의 기술적 발전방안과 홍보·교육 등의 정책적 발전방안, 그리고 인증업무세부지침 등의 법·제도적 발전방안은 정부가 행정전자서명의 이용을 활성화하고 발전시키는데 활용될 수 있을 것이다. 앞으로 행정전자서명의 이용이 활성화된 이후에도 본 연구에서 분석한 설문조사 결과를 참고하여 행정전자서명의 수요 및 만족도 조사를 주기적으로 실시하고, 이를 통한 지속적인 유지·발전과 사용자의 확대가 이루어져야 할 것이다.

ABSTRACT

Study and analysis on the digital certification of the world today, and census on how digital signature is being used or considered for the government will be used to sum up what can be the difficulties and problems in operating digital signature certifications for the government administrations at this research, and of course the answers to these problems will be provided too. This research suggests practical ideas on how to interoperate between Government PKI (GPKI: Administrational Digital Certification for the Government) and National PKI (NPKI: Digital Certification for General Public & Business), how to make use of Standard Security APIs, how to manage (e.g. issue, reissue, update, revoke) digital certificate, how to improve technical side of security and reliability, and how to improve political issues on public education for information security. Digital certification will become more popular and widely used in government administrations in the future. Therefore, census and research on demands and satisfactions of digital certification for public and government will be regularly performed. Of course, continuous maintenances and improvement in this field will be necessary to obtain firmer way of information security.

Keywords: *digital certification, Information Security, GPKI, NPKI, APIs*

접수일: 2004년 1월 19일; 채택일: 2004년 3월 15일
† 주저자, kkchu@mogaha.go.kr
‡ 교신저자, syrhew@soongsil.or.kr

Ⅰ. 서 론

정보통신기술의 비약적인 발전으로 정보화 사회로의 진입이 가속화되고, 이로 인하여 사회 전반에 많은 변화가 일어나고 있다. 이러한 변화에 대응하여 세계 각 국 정부는 전자정부로의 발전을 경쟁적으로 추진하고 있다.

우리나라도 초고속 인터넷 사용인구의 폭발적인 증가와 함께 인터넷 사용인구가 2,600만 명을 넘어서고, 사이버 증권거래, 인터넷 뱅킹이 활성화 되는 등 실세계의 많은 부분이 가상공간으로 넘어가고 있다. 특히, 행정분야에 있어서는 정부의 다양한 노력에 힘입어 기존 민원창구 중심의 업무처리가 인터넷 기반의 비대면 온라인 처리체계로 급속히 전환되고 있다.

그러나 이러한 전자정부의 도래와 함께 인터넷의 특성으로 인한 역기능 또한 심화되고 있어 이에 대한 정부 차원에서의 대응은 전자정부의 성패를 좌우할 수도 있다. 이러한 인식에 따라 정부에서는 전자정부의 성공적인 완성을 위하여 국민이 정보유출과 위·변조에 대한 불안 없이 자유롭게 정보교환을 할 수 있는 범 정부차원의 정보보호기반 구현을 목표로 2000년부터 '정부의 행정전자서명인증기반(GPKI : Government Public Key Infrastructure)구축사업'을 지속적으로 추진해 오고 있다.

본 논문은 국내외 각종 문헌, 논문, 설문자료, 간행물 및 보고서, 인터넷 검색 등을 참고로 이를 분석하는 문헌적 연구방법과 현재 운영되고 있는 행정전자서명인증체계의 사용자 인지도 및 이용실태에 대한 설문조사 방법을 동시에 적용하여 문제점을 도출하고, 이에 대한 개선사항 등 해결책을 기술적 방안, 정책적 방안, 법·제도적 방안 등 3가지 측면에서 제시하여, 정부에서 행정전자서명의 이용 활성화 및 발전 업무를 추진하는데 참고자료로 활용할 수 있도록 하였다.

Ⅱ. 국내·외 인증체계 현황

2.1 정부의 행정전자서명인증체계(GPKI)

정부(행정자치부 정부전산정보관리소)에서는 3단계에 걸쳐 'GPKI 구축사업'을 추진하고 있다.

1단계 기반조성 단계(2000.4~2001.5)에서는 사무관리규정 및 동 시행규칙 개정(2001.2), 전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률 제정(2001.3) 등 전자관인 인증제도 도입을 위한 법·제도적 기반을 마련하고, 정부전자관인인증시스템 구축(2000.4) 및 이중화(2000.12)를 추진하였다. 이를 기반으로 생산적 복지정보 공동이용, 급여·인사·지방채, 여권만료 통지 등 행정EDI에 전자관인 인증서비스 제공을 시작하고, 정부용 전자서명 표준 보안 API를 개발·보급 하였으며, 행정기관 전자서명 인증기반 상호연동 기술표준을 제정(2001.3), 보급하였다.

2단계 민·관 상호연동 환경 구축단계(2001.6~2002.4)에서는 안전한 전자민원 행정서비스 제공기반을 구축하기 위하여 NPKI(National Public Key Infrastructure)와 상호연동을 위해 정보통신부 등과의 협의 (2001.6~8)를 시작으로 민·관 전자인증 합동작업반을 구성·운영(2001.9)하고, 전자관인 저장매체 표준화 (2001.8~2001.12)의 진행, 정부 전자관인 인증관리시스템 확대 구축 (2001.11~2002.4)을 추진하였다.

표 1. 정부의 인증관리체계 지정현황

구분	주관기관	비고
정부인증관리센터	행정자치부 정부전산정보관리소	2002. 3 지정
정부인증기관	국가정보원, 국방부, 대통령비서실, 교육인적자원부, 대검찰청, 병무청	2002. 8 지정
등록기관	정보통신부 등 10개 중앙행정기관 및 16개 시·도	2002. 9 지정
원격등록기관	42개 중앙행정기관, RA의 소속기관, 각 지방청 및 16개 시·도내 시·군·구 등 등록기관장이 지정·운영	2002. 9 지정

3단계 보급 확산 단계(2002.5~2002.12)에서는 전자정부의 정보보호기반을 조기에 구현할 목적으로 본인확인이 필요한 전자민원(70여종) 서비스에 전자관인을 적용하고, 행정자치부 공무원에게 행정전자서명 보급을 완료 (2002.5)하였다. 또한 전자정부 단계별 행정전자서명 보급계획 수립 및 수요조사 실시(2002.6)를 토대로 인증기관, 등록기관, 원격등록기관을 지정하여 정부인증관리체계를 구축하였고, 25개 등록기관에 행정전자서명 등록시스템 설치를 지원(2002.10~12)하여 효율적인 확산보급 추진체계를

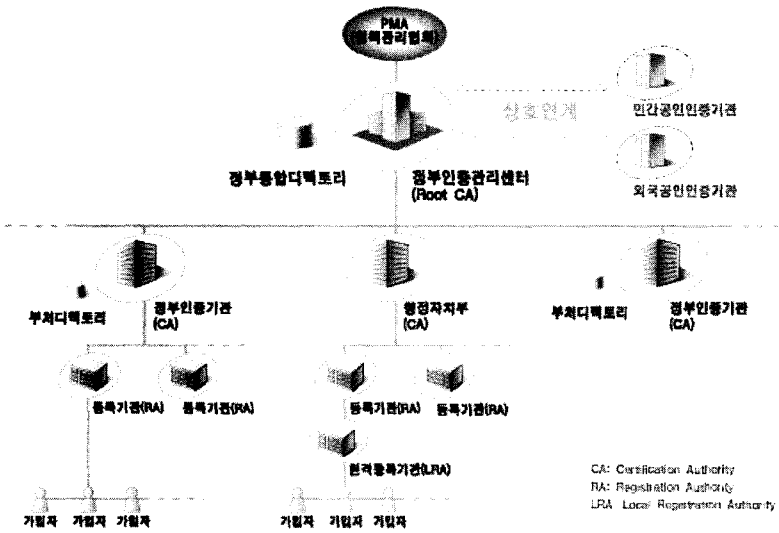

그림 1. 정부인증관리체계(GPKI) 구성도

정립하는 한편, 행정전자서명 사용자인 각 기관의 인증담당자와 인사, 서무 담당자 등에 대한 전국 순회교육을 실시하는 등 행정전자서명의 홍보 및 보급 확산에 노력하고 있다.

그림 1에서와 같이 GPKI Root CA(Certificate Authority)는 NPKI와 상호연동될 수 있도록 추진하고 있으며, 하부에 CA를 두고 있고, 하부 CA는 등록기관과 원격등록기관을 통하여 가입자에게 인증서를 발급하는 계층 구조를 이루고 있다. 이는 NPKI 인증체계의 구성과 동일한 계층적 PKI 구조이다.

또 정부에서는 국가 차원의 정보보호 인프라 확산을 선도하고, 전자행정의 안전성 보장을 목표로 '공무원 1인 1행정전자서명 갖기 운동'을 전개하고 있다. 그 결과 초기의 260여 기관에 불과하던 행정전자서명의 보급이 2003년 6월말에는 71만명이 넘어서는 성과를 거두었다. 이는 인증서를 발급받을 수 있는 거의 모든 공무원이 발급받은 것으로 NPKI에서 인터넷 뱅킹 이용자나 사이버트레이딩 이용자에게 90%이상 편중 발급된 것과 비교하면 거의 모든 행정업무에서 인증서를 사용할 수 있는 기반이 이루어진 것으로 커다란 성과라 하겠다[1].

한편, 행정전자서명 적용업무 현황을 보면 232개 시·군·구에서 담당하고 있는 생활보호대상자 선정·관리업무를 신속하게 처리하기 위한 "생산적복지정보공동이용업무" 등 3개 업무를 전국단위의 시범사업으로 실시(2000.10) 한 바 있고, 2003년 말까지 20여개의 전 부처단위 업무에 적용하는 등 월 700만건 이상의 전자문서가 전자서명을 통해 유통되는 등 비약적인 발전을 이루어 왔다[2].

표 2. 행정전자서명 인증서 보급현황(누적)

연도		2000	2001	2002	2003.6
인증서 종류	개인	0	0	517,210	716,210
	기관	268	1,039	2,983	3,183
총 계		268	1,039	520,193	719,393

2.2 민간의 전자서명인증체계(NPKI)

1999년 '전자서명법'에 근거를 두고 한국정보보호진흥원(KISA)이 최상위인증기관(RootCA)으로 설립되었다. 여기에 6개의 공인인증기관이 하위 인증기관으로 지정(2000.2~2002.3)되어 개인과 법인에게 인증서를 발급하고 있다[3].

GPKI와 마찬가지로 NPKI 인증체계도 계층적 인증체계로 구성되어 있다. 한국정보보호진흥원에서 운영하고 있는 RootCA, RootCA 하부에 6개의 공인인증기관, 공인인증기관의 등록을 대행하는 등록대행기관, 등록대행기관이나 공인인증기관으로부터 인증서를 발급받아 사용하는 가입자로 구성되어 있다.

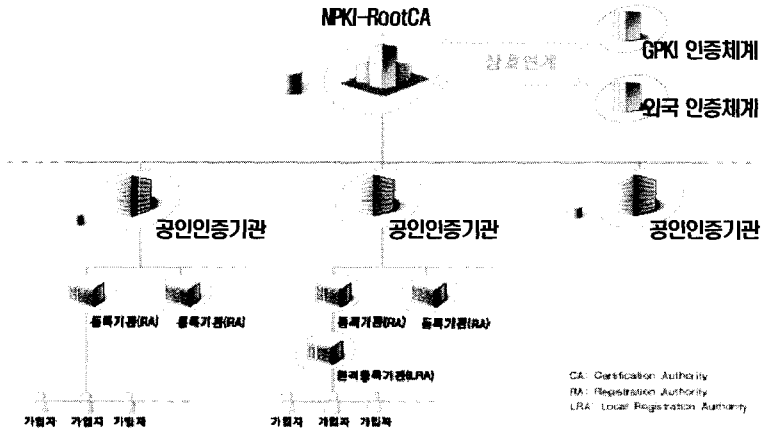

그림 2. 민간 인증관리체계(NPKI) 구성도

표 3. 민간공인인증기관 지정현황

회사명	지정일	영문명
한국정보인증(주)	2000년 2월 10일	signgate
한국증권전산(주)	2000년 2월 10일	signkorea
금융결제원	2000년 4월 12일	yessign
한국전산원	2001년 3월 12일	NCASign
한국전자인증(주)	2001년 11월 25일	CrossCert
(주)한국무역정보통신	2002년 3월 11일	TRADESIGN

표 4. 민간분야의 공인인증서 발급현황(누적)

연 도		2000	2001	2002.11
인증서 종류	개인(명)	18,470	1,293,850	3,579,205
	서버(EA)	38	228	335
	법인(명)	8,337	207,457	503,226
총 계		26,845	1,501,535	4,082,766

NPKI의 인증체계의 경우 시장의 상황에 따라 확산이 이루어지고 있으며, 현재 무선인터넷의 급격한 확산에 힘입어 무선 인증서비스로의 확대가 이루어지고 있다.

NPKI 인증서 발급현황을 보면 2000년 조달분야를 시작으로 하여 첫 공인인증 서비스가 도입된 이후 인터넷뱅킹, 사이버증권, 전자민원 서비스 등 전자서명 인증서 이용분야는 꾸준히 늘어나고 있는 추세이다. NPKI 공인인증 서비스의 경우 초기에 금융결제원(은행), 증권전산(증권)을 중심으로 확산 보급되었고, 현재는 정부분야와 민간 의료 분야 등으로 확산되고 있다.

2.3 외국의 공인인증체계

공개키기반구조(PKI) 기술은 세계 각국에서도 활발히 이용되고 있다. 특히 아시아의 경우는 우리나라와 국가간 상호연동을 추진하고 있을 정도로 PKI에 대한 열기가 높다. 나라별로 보면 우리나라처럼 공인인증체계를 두고 있는 곳도 있고, 미국과 같이 지역별로 인증체계를 갖추고 있는 곳도 있다. 국가별 PKI 활용현황을 살펴보면 다음과 같다[4,5].

미국은 지난 2000년 전자서명법을 제정하고 시행하면서 연방정부 차원에서 PKI 구축을 꾸준히 추진하고 있으며, 대표적인 PKI 기업인 베리사인이 전세계적으로 민간 차원의 인증서비스를 제공하고 있다. 지난 1996년부터 유타주를 필두로 주정부 단위의 전자서명법 제정이 활발히 이루어져 왔으나 연방정부 단위의 법 제정은 비교적 늦은 편인 2000년 6월에야 이루어졌다. 연방정부에서 전자서명의 효력을 인정한 법은 'The Electronic Signatures in Global and National Commerce Act(E-Sign)'로 2000년 6월 30일 제정되었고, 같은 해 10월 1일부터 시행되었다. 전자정부를 구축하기 위해 '정부문서 감축법(Government Paperwork Elimination Act)'을 공포하고 이를 뒷받침하기 위한 PKI 구축에 힘쓰고 있으며, 또한 일반 민원서

비스에 PKI를 응용, 범위를 확산시켜 나가고 있다. 미국은 서로 다른 도메인간 상호연동을 위해 브리지 인증(Bridge CA) 체제를 도입했는데, 이는 연방정부 차원에서 다양한 CA를 계층적 또는 수평적으로 구축하고 각각의 CA를 PCA(Principal Certificate Authority)가 연계해 주는 방식이다. 2000년 6월 연방 브리지CA 운영을 맡게 될 FPKIPA가 설립되었는데, 여기에는 미 GSA(General Service Administration)와 OMB(Office of Management and Budget), 국방부, 재무부, 상무부, 법무부 등이 참여하고 있으며, 연방 브리지CA 운영을 감독한다. 또 인증서에 대한 발급 권한을 갖고 있으며 상호인증의 참여자 및 등급을 결정하고 인증서 정책을 관리하는 역할을 담당한다. 그리고 GSA는 국민을 상대로 한 정부의 정보서비스를 안전하게 하기 위해 '전자서비스를 위한 접근인증(ACES)' 서비스를 제공하고 있다.

일본은 전자서명법을 2000년 5월에 제정·시행하고 있다. 민간 및 정부 부문에 PKI를 구축·운영하고 있으며, 정부PKI(GPKI)는 브리지CA(BCA)방식으로 연계되어 있다. BCA는 경제산업성에 의해 통제되고 총무성이 관리 및 운영하고 있다. 정부부처로는 현재 총무성 및 경제산업성·법무성 등이 CA구축을 마치고 운영중이며, 2004년말까지는 모든 부처가 CA구축을 마칠 예정이다. 중앙부처의 CA는 법인에게 인증서를 발급할 수 있고 지방자치단체는 LGPKI(Local GPKI)를 구축해 국민들에게 인증서를 발급할 수 있다. 모든 법인은 법무성의 등록사무소 CA에 법인등록을 해야만 인증서를 받을 수 있으며, 일본의 공인인증기관인 'JCSI(Japan Certification Service Inc.)'는 히타치·후지쯔·NEC 등 3개 회사에 의해 설립됐다. 현재 일본의 공인인증기관으로는 TDB(Teikoku Databank, Inc.), SECOM 트러스트넷 등 6개의 인증기관이 있고 7개의 인증서비스가 있다.

싱가포르는 지난 1998년 7월 전자거래법을, 1999년 2월 전자거래 시행규칙을 공포해 PKI를 전자거래상의 보안을 위한 주된 기술로 명시했다. 싱가포르의 공인인증기관인 '넷트러스트'는 2001년 6월 공인인증기관으로 지정됐다. 싱가포르의 인증서비스는 민간 및 정부를 구분하지 않고 전자거래법을 따른다. 넷트러스트는 6만5000개의 인증서를 정부 공무원에게 PS카드(Public Sector Card : 스마트카드의 일종)에 넣어 발급했으며 공무원은 이를 이용, 급여 등의 개인정보 접근 및 정부 내의 보안 e메일 교환용으로만 사용할 수 있도록 했다. 그러나 우리나라와 마찬가지로 일반 전자상거래 용도로는 사용할 수 없다. 현재 싱가포르 일반 국민에게는 인증서가 거의 발급되지 않았지만 은행과 SME(Small and Medium Enterprise)간 B2B 거래용으로 일부 사용 되고 있다

중국은 전자서명법을 아직 제정하지 못하고 있으나 향후 2~3년 안에 법적 체제가 마련될 것으로 보인다. 현재 중국에서는 기본적인 국가 PKI 구조로 우리나라와 같은 Root CA 운영방안과 미국 방식의 브리지CA 운영방안이 거론되고 있다. 민간 부문은 상하이CA·광둥(홍콩텔레콤)CA 등 5대 주요CA가 Root CA로 연결되어 있는데, 이를 연합(United) CA라고 부르며 상하이CA가 관리한다. 이 가운데 대표적 CA인 상하이CA는 30만장의 인증서를 발급했으며, 인증서 종류는 신분확인용·e메일용·웹서버용·코드사인용·VP N용 등이 있다. 이밖에 전국적으로 자치 정부별로 구축된 80여개의 CA가 운영되고 있다.

유럽의 경우 독일은 전자서명법을 지난 1997년 6월에 제정하고, 1997년 8월부터 시행에 들어갔으며, 독일의 PKI는 법무부와 연방경제기술부가 관여하는 2계층의 구조를 지닌다. 법무부는 독일의 전자서명법 및 하위법령을 제정·적용하고 있으며, 독일 연방경제기술부(Federal Ministry of Economics & Technology)는 산하에 통신우편국(RegTP: Regulation of Telecommunication & Post)을 두고 통신·우편·전파 및 전자서명과 관련된 규제업무를 수행하고 있다. 또 전자서명 인증정책 결정이나 인증기관 허가 및 최상위인증기관(루트CA)의 역할을 수행하고 있다. 독일 정보보호원(BSI)은 인증기관에 대한 평가를 수행하면서 인증기관을 허가하는 전자서명 인증체계를 구축·운영하고 있다. 독일의 첫번째 공인인증기관인 도이치텔레콤은 인증서 신청자에게 우편으로 전자서명 생성키와 수령증을 발송하고 신청자가 자필서명해 반송한 수령증의 서명과 인증서 신청서의 서명을 비교, 동일인임을 확인하는 신원 확인절차를 따르고 있으며 전화국을 등록기관으로 활용하고 있다.

영국은 PKI구축을 위한 여러 가지 계획을 진행중이며, 이미 디지털서명을 법적 효력이 있는 서명방식으로 인정하고 이를 골자로 한 법안을 제정하였다. 영국의 't스킴(tScheme)'은 산업체가 주도하는 자

발적 승인체계로 업체들이 참여하고 있으며 정부 대표자들도 위원회 위원직을 맡고 있다. 영국에서는 PKI가 비용이 많이 들고 복잡함에도 불구하고 필수적인 기반구조로 인식되고 있다. 정부와의 거래에서 인증서를 사용하게 될 경우 t스킴의 승인을 받도록 하고 있으며 민간부문에서도 t스킴의 인증서 사용을 장려하고 있다. 정부 내에서는 클라우드 커버라는 방안이 내부용 PKI를 제공하기 위해 채택되었다. 클라우드 커버의 목적은 정부기관이 안전하고 상호연동이 가능하며 비용효과적인 가장 광범위한 PKI 솔루션을 사용할 수 있도록 보장하는 것이다.

Ⅲ. 행정전자서명에 대한 인식·이용 실태조사

행정전자서명에 대한 공무원들의 인식부족과 온라인 기반으로 전환되었으나 아직 정착되지 않은 업무 등으로 인해 아직은 행정전자서명의 이용이 저조한 실정이다. 설문 조사를 통하여 행정전자서명에 관한 인식과 이용 실태를 조사하고, 이를 통하여 사용자의 행정전자서명 이용활성화 방안을 수립하기 위한 기초자료를 획득하고자 하는 것이 본 조사의 목적이다.

3.1 조사의 기본설계(Research Design)

모집단은 전산직 및 비 전산직 공무원 10,000명(유효표본)을 대상으로 하였고, 자료수집 도구로 구조화된 설문지를 사용하였으며, 2003년 11월 18일부터 11월 30일까지 13일간 홈페이지를 통해 설문조사를 실시하였다. 그리고 설문 항목은 다음과 같이 구성하였다.

표 5. 행정전자서명 인식·이용실태 조사 내용

구 분	내 용
본 문 항	1. 인터넷 이용실태 - 우려되는 역기능 2. 전자서명에 대한 인식 - 전자서명에 대한 인지도 - 전자서명 인지 경로 3. 전자서명의 필요성 4. 행정전자서명과 공인인증서에 대한 인식 - 행정전자서명과 공인인증서에 대한 인식 - 사용 인증서의 종류 5. 행정전자서명 이용 저해요인 - 행정전자서명인증서를 발급받지 않은 이유 - 이용 빈도 - 이용 용도 - 이용 만족도 - 이용시 애로사항 6. 행정전자서명 보안 실태 - 인증서 수령 형태 - 인증서 신청정보 수령 형태 - 인증서 보관 장소 - 인증서 백업사항 - 인증서 재발급 사유 7. 행정전자서명 이용활성화 요구사항 - 행정전자서명 이용활성화 요구사항 - 행정전자서명 이용 확대를 원하는 분야
배경 변수	1. 나이, 유형 2. 인터넷 이용기간, 인터넷 이용시간

3.2. 조사 결과

설문 참가자들을 분석한 결과 남자가 62.1%, 여자가 37.9%의 비율을 보였다. 연령별로는 20대가 9.7%, 30대 60.7%, 40대 24.5%, 50대 이상 5.0%를 보여 30대가 가장 많은 비율을 차지하였다. 부문별로는 전산직공무원 20.0%, 비전산직공무원 58.0%를 보였다.

3.2.1 인터넷 이용실태

대부분의 설문참가자들이 인터넷 서비스를 이용하면서 가장 우려하는 점으로는 '신용카드정보 등 전송되는 정보의 유출 우려'(74.5%)', '개인ID의 도용'(8.1%), '전자문서의 위·변조'(6.7%)', '전자거래시 상대방의 신원을 확인하기가 어려움'(6.7%)' 등으로 나타나 많은 사용자들이 보안에 대한 우려를 하고 있음을 알 수 있었다.

3.2.2 행정전자서명에 대한 인식

설문참가자들 중 95.0%가 전자서명에 대해 '알고 있다'고 응답하여 설문에 응한 대부분의 사용자가 전자서명에 대하여 인식하고 있는 것으로 나타났다.

전자서명에 대해 알고 있다고 응답한 283명을 대상으로 인지경로를 질문한 결과, '직무교육'(33.6%), '행정자치부, 정보통신부, 전자서명인증기관, 관련업계 등의 홍보물'(39.6%), '인터넷'(15.8%)을 통해 알았다는 응답자가 가장 많았고, 그 다음이 '신문, TV, 라디오 등 언론매체(4.7%)의 순으로 나타나 전자서명을 홍보하는 가장 효과적인 방법은 '직무교육'과 '관련기관의 홍보활동'이라는 것을 알 수 있었다.

전체 응답자의 96.0%가 '모든 전자거래'와 '보안성이 요구되는 일부 업무처리'에 전자서명의 필요성

을 인식하고 있었으며, 필요하지 않다는 응답은 전체의 3.3%에 불과한 것으로 나타나 '전자서명에 대한 필요성'이 확산되고 있음을 알 수 있었다.

응답자중 전체의 74.5%가 행정자치부 인증기관(GPKI)에서 행정업무용으로 발급한 '행정전자서명 인증서'와 민간 인증기관(NPKI)에서 전자상거래용으로 발급한 '민간전자서명인증서'의 차이를 알고 있었다. 그러나 설문자의 대부분이 행정전자서명인증서를 사용 중인 공무원임을 감안할 때 25%에 가까운 사용자가 양 인증서의 차이를 모르고 있다는 것은 낮지 않은 비율이라 할 수 있다.

'행정전자서명인증서'는 59.4%가 이용하고 있었고, 27.9%는 '행정전자서명인증서'와 '민간공인인증서' 두 가지 모두를 이용하고 있었으며, 두 가지 모두 이용하지 않은 응답자는 7.4%로 나타났다. 특히 '행정전자서명인증서'는 응답자 대부분이(87.3%) 발급받아 이용하고 있는 것으로 나타나 행정전자서명인증체계의 기반이 완성 수준에 이르렀다는 결과를 보여주었다.

3.2.3 행정전자서명 이용 저해요인

행정전자서명 비이용자들이 행정전자서명 인증서를 발급받지 않는 가장 큰 이유는 '행정전자서명 인증서 사용의 필요성을 못 느끼기 때문'(27.3%)이었으며, '행정전자서명을 이용할 수 있는 응용프로그램이나 서비스가 부족해서'(16.9%)라는 응답이 그 다음으로 많이 나타나 행정전자서명 활용 업무나 서비스의 확대가 필요함을 나타내고 있다. 그리고 '신청절차를 모르거나 복잡해서'(31.2%)라는 응답도 적지 않아 '행정전자서명 인증서 신청절차의 간소화'와 '행정전자서명 인증서 신청절차에 대한 홍보의 강화'가 필요한 것으로 나타났다.

행정전자서명 인증서를 발급받은 응답자들의 행정전자서명 인증서 이용 빈도는 하루에 3회 이상(23.83%)이 가장 많았고, 다음으로 하루에 1~2회(19.46%)로 나타나 행정전자서명인증서의 보급에 비해 행정전자서명인증서의 사용은 조금 저조한 편이며, 사용하지 않는다는 응답도 17.79%로 나타나 행정전자서명인증서 이용 활성화대책이 필요함을 알 수 있었다.

행정전자서명 인증서를 이용하는 용도를 두개만 선택하도록 설문한 결과, '전자정부 민원서비스(G4C) 업무용'(65.8%), '전자문서유통'(25.4%), 'G4C를 통한 민원신청'(23.1%) 순 이었으며, '활용분야 없음'도 23.8%로 나타났다. 이처럼 행정전자서명인증서는 주로 관련업무에 이용되고 있어 행정전자서명인증서의 활성화를 위해서는 우선 업무중심의 활용방안을 마련하는 것이 가장 필요한 것으로 나타났다.

행정전자서명에 대한 만족도를 살펴보면 68%가 행정전자서명 이용에 만족하고 있고 18%가 불만족한 것으로 나타났다. 대부분의 사용자가 행정전자서명에 대하여 만족하고 있다는 것을 알 수 있다. 그러나 18%의 사용자 불만족 부분에 대한 해결방안도 고려되어야 할 것으로 보인다.

행정전자서명 인증서 사용자들이 가장 불편해 하는 사항은 '행정전자서명 인증서를 발급받고 이용하는 절차가 복잡하다'(59.2%)는 것과 '인증서를 활용할 수 있는 응용프로그램이나 서비스의 부족'(46.5%)

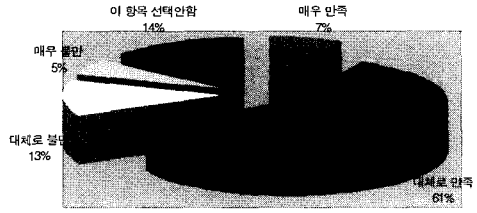

그림 4. 행정전자서명인증서 이용만족도

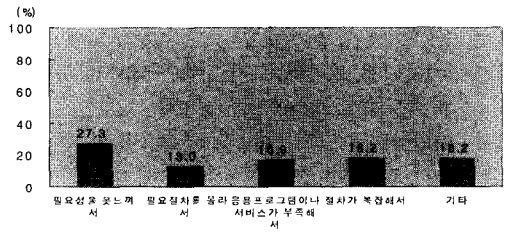

그림 3. 행정전자서명 인증서를 발급받지 않은 이유

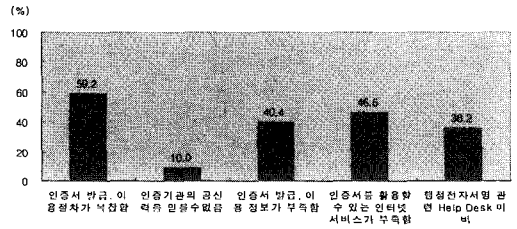

그림 5. 행정전자서명 인증서 이용 시 불편 사항

이라고 응답해 응용프로그램 및 서비스의 확대와 이용 절차 간편화에 대한 대책이 필요한 것으로 나타났다.

3.2.4 행정전자서명 보안 실태

행정전자서명 인증서 발급형태를 보면 '인증서 직접발급'이 73.7%이나 '동료의 도움'을 받은 경우가 11.1%이고 '동료직원으로부터 인증서 및 비밀번호를 전달받은 경우'가 15.3%로 나타나 인증서 발급 시 인증비밀번호 노출의 위험과 사고가능성이 큰 것으로 나타났으며, 또한 '행정전자서명 인증서'에 대한 보안 인식이 매우 낮은 것을 알 수 있었다. 따라서 '행정전자서명 인증서'에 대한 직무교육이나 홍보활동시 '행정전자서명 인증서 보안'에 대한 대책이 필요하다 하겠다.

행정전자서명 인증서 신청정보 수령형태를 보면 '정부 E-Mail(시군구 포함)'이 68.1%이고, '사설 E-Mail'이 16.3%, '공문서(수기결재 또는 전자결재된 문서포함)로 수령'이 11.8% 로 나타나 비 대면에 의한 '행정전자서명 인증서 신청정보' 수령에 따른 보안체계의 마련이 시급한 것으로 나타났다.

행정전자서명 인증서 보관 장소를 보면 응답자의 74.6%가 '하드디스크'에 보관중이고 14.6%는 '기타 플로피디스크, 스마트카드와 CD-KEY'에 보관 중으로 행정전자서명 인증서는 대부분 하드디스크에 보관하는 것으로 나타났다. 재발급 사유와 관련하여 컴퓨터로 인한 문제 발생이 대부분의 재발급 사유를 차지하는 것으로 나타나 행정전자서명인증서의 불필요한 재발급에 대한 대안으로 스마트카드 또는 플래시메모리 등 별도의 장소에 보관을 유도하는 것과 인증서의 백업을 의무화 하는 것이 바람직한 것으로 나타났다.

응답자의 14%가 행정전자서명 인증서를 본인이 아닌 인증관리 담당 동료직원이 별도관리 하는 것으로 나타났는데 이는 인증서의 비밀번호를 다른 직원

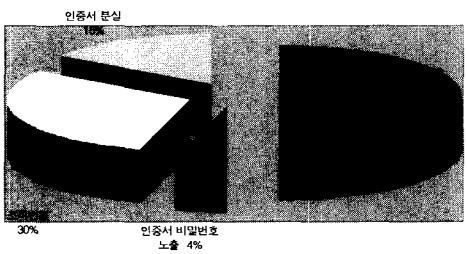

그림 6. 행정전자서명인증서 재발급사유

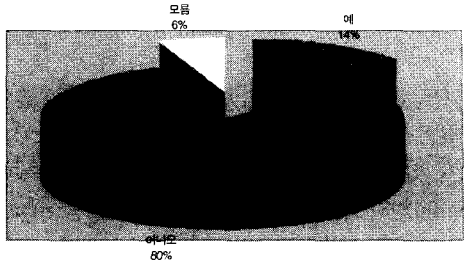

그림 7. 행정전자서명인증서의 다른 직원 별도관리여부

이 안다는 것을 나타내므로 이에 대한 대책마련이 시급히 이루어져야 하며, 또한 사용자 교육프로그램에 인증서의 중요성과 보안성에 대한 인식을 강화해야 할 것으로 나타났다.

또 응답자중 32.9%만이 행정전자서명 인증서 백업용을 보관하고 있는 것으로 나타나 백업을 통하여 재발급을 줄일 수 있고, 이로 인한 인력의 낭비를 최소화할 수 있는 것을 감안하면 이에 대한 홍보 및 교육 강화가 필요한 것으로 보여지며, 행정전자서명 인증서 백업용 매체로는 '플로피디스크'(64.9%)의 보관비율이 가장 높은 것으로 조사되었다.

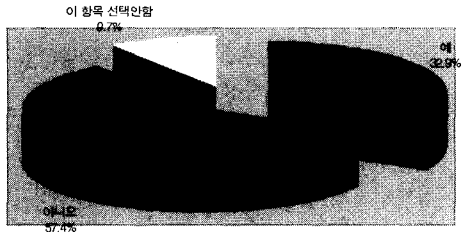

그림 8. 행정전자서명인증서 백업용 보관여부

'행정전자서명인증서' 재발급사유를 보면 '인증서 비밀번호 분실'(48%)과 '조직변경'(30%), '인증서분실'(15%), '인증서 비밀번호 노출'(4%) 순으로 나타나 행정전자서명 인증서의 중요성에 대한 인식개선과 체계적인 관리방안의 마련이 필요한 것으로 나타났다. 조직변경의 경우도 비교적 높은 비율을 나타내 이에 대한 대책도 필요한 것으로 나타났다.

3.2.5 행정전자서명 이용활성화 요구사항

행정전자서명 이용을 활성화하기 위해 우선적으로

해결해야 할 문제로는 '전자서명인증서 발급 및 이용의 간편화'(22.9%)와 '행정전자서명 활용분야 확대 및 온라인업무로의 전환'(21.7%)이라고 응답해 '이용절차의 간편화와 활용분야 확대'가 필요한 것으로 나타났다. 또한 '교육강화'(14.9%), '홍보강화'(13.0%)라는 응답도 상당수에 달해 지속적인 교육과 홍보의 강화도 필요한 것으로 나타났다.

행정전자서명 이용활성화를 위한 요구사항 설문의 경우에는 전체적으로 설문문항에 대해 고른 분포를 나타내고 있어 전반적인 부분에서 사용자들이 행정전자서명 이용활성화가 이루어져야 한다는 인식을 가진 것을 알 수 있었다. 특히 '안전성에 대한 보장과 책임소재의 확립'이 15.5% 이상을 차지한 것을 보면 행정전자서명에 대한 안전성 보장과 책임소재의 확보도 시급한 사항으로 나타났다.

복수응답을 통해 설문한 행정전자서명 이용이 확대되길 바라는 분야는 '전자금융거래'(56.5%), '전자민원'(43.5%), '인터넷교육'(20.0%), '전자우편(20.6%)의 순으로 나타나 사용자 대부분이 행정전자서명의 이용이 업무 및 실생활과 관련된 부분으로 확대되기를 원하는 것으로 나타났다.

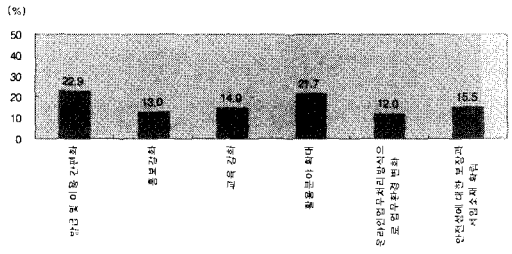

그림 9. 행정전자서명인증서 활성화를 위한 선결과제

Ⅳ. 행정전자서명인증체계 활성화 및 발전방안

4.1 기술적 발전방안

기술적인 부분은 GPKI와 NPKI 인증체계간의 상호연동, 표준보안 API의 활용, 인증서의 발급·재발급·갱신·폐지 및 관리, GPKI 인증체계의 보안성·안정성 등 네가지 측면에서 여러 가지의 문제점과 해결방안을 생각해 볼 수 있다.

4.1.1 행정전자서명인증체계(GPKI)와 민간전자서명인증체계(NPKI) 간의 상호연동 분야

GPKI와 NPKI간의 상호연동을 통해 본인확인 서비스가 필요한 경우 NPKI 응용프로그램에서 GPKI 인증서를 사용하면 본인확인에 실패하게 되는 문제가 발생한다. 현재 GPKI 인증서에는 사용자 본인확인을 위한 식별번호가 인증서의 확장영역인 '주체 객체 이름' 필드에 들어있지 않기 때문이며, 다음 그림은 인증서 확장 필드에 본인확인을 위한 식별번호가 없는 GPKI 개인용 인증서를 보여주고 있다.

이의 해결을 위해서는 GPKI 인증서에 식별번호를 넣는 방법을 고려할 수 있다. 식별번호를 GPKI 인증서에 포함하게 되면 NPKI와 GPKI간의 본인확인 서비스에 필요한 호환성을 쉽게 확보할 수 있기 때문에 이 문제는 해결할 수 있다. 지금까지 발급된 사용자 인증서를 재발급해야 하는 부담이 있지만 현재 GPKI 인증체계에서 사용하고 있는 본인확인 방법을 적용하면서 동시에 유효기간이 지나 다시 발급해야 하는 인증서에 대해 점차적으로 식별번호를 포함하여 재발급하는 방법으로 해결해 나가야 할 것이다.

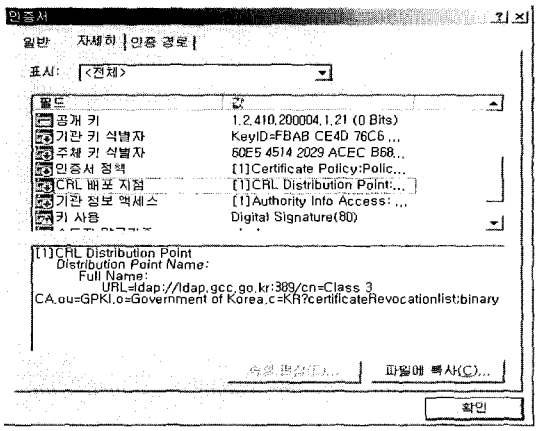

그림 10. GPKI 인증서의 확장 필드 영역

그리고 GPKI 인증체계에서는 DeltaCRL (Certificate Revocation List) 방식이 인증서의 검증에 이용되고 있으나 NPKI 인증체계의 경우 인증서 검증에 DeltaCRL 방식을 지원하지 않고 있고, DeltaCRL 갱신이 2시간 간격으로 이루어지고 있어 NPKI 인증체계에서 검증하는 시점에 CRL만을 검증하는 경우 2시간 사이에 발생한 문제를 확인할 수 없는 어려움이 발생한다. 이를 해결하기 위해서는 NPKI 응용프로그램의 GPKI DeltaCRL 기능을 추가로 지원하도록 하는 방법을 생각할 수 있다. 그러나 이는 NPKI에서 사용중인 응용프로그램

을 업그레이드 해야하고, 이를 NPKI 인증체계에서 시행하는데 필요한 시간적인 문제도 발생한다. 다른 방법으로는 DeltaCRL 부분을 수행하지 않는 방법이다. 이 경우 2시간 사이에 발생한 문제에 대한 대응이 필요 하지만 중요한 응용 프로세스의 경우 반드시 실시간 인증서 검증을 실시 하도록 함으로써 이를 보완할 수 있다. 그리고 현재 NPKI와 GPKI의 상호연동을 위한 방식으로 CTL(Certificate Trust List) 방식이 사용되고 있는데, CTL 방식의 경우 다른 도메인의 인증체계 상태를 실시간으로 반영하는데 어려움이 있다. 즉 NPKI나 GPKI의 최상위 인증기관의 서명키가 노출되는 등의 문제가 발생할 경우 이를 반영해야하는 어려움이 생긴다. 다음표에서는 표준보안 API에서 CTL 검증시 암호학적 연산이 증가하고 있음을 비교하여 보여주고 있다.

표 6. CTL 검증시 암호학적 연산 비교

	CRL 검증 시	CTL 검증 시
암호학적 연산	KCDSA 서명검증 1번 RSA 서명검증 5번 (CRL, ARL 검증 포함) RSA 서명(OCSP 검증)	KCDSA 서명검증 1번 RSA 서명검증 6번 (CRL, ARL, CTL 검증) RSA 서명 (OCSP 검증)

표에서 보는바와 같이 RSA 서명검증이 추가적으로 발생하고 있는데, RSA 서명검증에 따른 처리시간이 빨라 이로 인한 문제는 적다. 그러나 CTL 획득을 위한 디렉토리 서버 접근으로 인하여 처리시간의 증가를 가져오게 된다. 현재 NPKI와 GPKI의 상호연동을 위한 방식으로 사용되고 있는 CTL 방식의 경우 인증서 체인의 검증 뿐 아니라 CTL의 유효성을 검증해야 하는 문제, CTL 유효기간이나 변경에 대한 정보를 획득하는 방법의 문제, 외부 PKI 도메인으로부터 신뢰경로에 대한 정보를 획득 해야하는 문제 등 몇 가지 문제점이 있다. 이러한 문제점에 대해서는 다음과 같은 해결방안을 생각해 볼 수 있다. 우선 CTL의 유효성을 검증해야 하는 문제의 경우 사용자 입장에서 볼때 추가적인 암호프로세스를 수행하는데 걸리는 시간이 필요하지만 이는 사용자가 느끼지 못할 정도의 시간에 불과하므로 표준보안 API 등에서 기능을 지원하게 함으로서 해결할 수 있다. CTL 유효기간이나 변경에 대한 정보를 획득하는 방법상의 문제는 인증기관간 상호연동을 위한 CTL 기술규격에서 유효기간이 만료될 경우 이를 지원하도록 규정함으로써 해결이 가능하다. 또 변경에 대한 정보를 획득하는 문제는 Off-line으로 변경된 사실을 서로에게 통보하도록 하고 있는데, 사안이 매우 중요하기 때문에 이 경우에는 사전에 협의된 절차에 따라 Out-of-band 방법으로 전달하도록 기술규격에 정의하면 된다. 외부 PKI 도메인으로부터 신뢰경로에 대한 정보를 획득해야하는 문제는 외부 PKI 도메인을 신뢰해야 한다는 문제가 있지만 이미 NPKI와 GPKI 인증체계의 주체인 한국정보보호진흥원과 행정자치부간에 상호 신뢰구조를 가져가기로 협의하고 있다.

상호연동성 분야에서 또 하나의 문제는 다른 나라들과의 상호연동 문제인데 우리나라와 마찬가지로 세계의 각 국가들은 전자서명법 등의 제정을 통하여 인증체계를 구성하고 있으며, 국가간의 인증체계 상호연동을 위해 독립적으로 구성된 각 나라의 인증체계와 상호 연동하는 작업을 활발하게 진행하고 있다. 그러나 정부의 행정처리를 전자화 하기 위한 인증체계의 국가간 상호연동은 아직까지 이루어지지 못하고 있다. 따라서 현재 우리나라에서 사용되고 있는 CTL방식과 상호연동 방식이 각기 다른 나라와의 상호 인증체계에 대한 고려가 이루어져야 한다. 다음은 주요 국가별 상호연동 방식을 나타낸 표이다.

표 7. 주요국가별 상호연동 추진방식

	상호 인증 추진 방식	상호연동의 형태
일본	BridgeCA 방식	응용레벨의 상호 연동
대만	계층구조 방식 + 상호인증 방식	응용레벨의 상호 연동
싱가포르	계층구조 방식	응용레벨의 상호 연동
독일	BridgeCA 방식	응용레벨의 상호 연동
영국	미 추진	인증서 프로파일 등의 협의의 상호 연동
미국	BridgeCA 방식	응용레벨의 상호 연동

상호연동 추진방식으로는 상호인증 방식, 상호인정 방식, 인증서 신뢰목록 방식, Bridge CA 방식, 인가 인증서 방식, 계층구조 방식, 인증서 경로검증 위임 등이 있다. 이 중 계층구조 방식과 인증서 경로검증 위임 방식의 경우에는 하나의 PKI 도메인에서는 가능한 방식이지만 국가간의 이해관계와 정책적인

차이로 인하여 실현이 불가능한 방식이다. 국가간 인증체계의 연동에 관한 연구는 최근 활발히 진행되고 있으며 그 중요성이 매우 큰 분야이다. 향후 각 국가별 고려사항과 상호연동을 위한 해외진출 방향에 관한 더욱 더 심층적인 정책이 제시되어야 할 것이며, 운영적인 측면에서도 GPKI와 국가 상호간의 요구사항에 적합한 연동방식의 모색이 요구된다. 따라서 이를 진행하기 위해 국가간에 지속적인 상호 정책 및 법적 보완과 기술적 교류가 요구되며, 아시아 지역의 운영과 관련한 표준화된 인증업무준칙의 마련에 관한 논의가 필요하고, 다양한 응용 분야에 대처하는 유연성을 갖추어 나가야 할 것으로 생각된다. 그리고 2001년부터 진행되고 있는 한·일·싱가포르 3국의 PKI 포럼으로 구성된 상호연동 실무작업반 활동에 GPKI의 주체인 행정자치부의 참여도 바람직 할 것이다. 실무작업반 활동 등의 참여는 초기 수행에 따른 운영상의 문제점들을 조기에 발견하여 해결할 수 있도록 해줄 것이며, 또한 국제 환경과 국내 환경이 상이하여 나타나는 여러 문제점들에 대해서도 잘 대응할 수 있도록 인증정책의 유연성 확보노력도 필요한 것으로 보인다.

다음으로 마이크로소프트사의 SSL인증서 상호연동 문제인데 현재 정부인증관리센터(GCMA) 홈페이지에서 사용하고 있는 SSL 인증서의 경우 마이크로소프트 익스플로러의 루트 인증서에 등록되어 있지 않다. 사용자가 GCMA 홈페이지에 방문할 경우 안전하지 않다는 경고 창을 보게 되고, 이는 사용자의 신뢰를 약화시키는 문제가 있다. 다음 그림은 마이크로소프트 익스플로러를 사용하여 GCMA의 서비스를 이용할 때 나오는 경고 창이다.

마이크로소프트사 익스플로러의 사용에 따른 경고창이 발생하는 문제와 관련하여 NPKI 인증체계에서는 NPKI SSL인증서를 마이크로소프트 익스플로러의 "신뢰된 최상위 인증기관" 인증서에 등록 하도록 하고 있다. GPKI의 경우 이미 인증서의 프로파일 형식 등은 X.509v3 표준을 준수하고 있으므로 호환성의 문제는 발생하지 않는다. 따라서 GCMA 홈페이지에서 사용하고 있는 SSL 인증서를 마이크로소프트 익스플로러의 "신뢰된 최상위 인증기관" 인증서에 사용자가 등록하도록 하면 경고창이 발생하는 문제를 쉽게 해결할 수 있다. 또한 프로그램의 배포에 사용되는 코드사인 인증서의 경우에도 "신뢰된 최상위 인증기관" 인증서의 개인키를 사용하여 서명할 경우 마찬가지로 문제는 발생하지 않게 될 것이다.

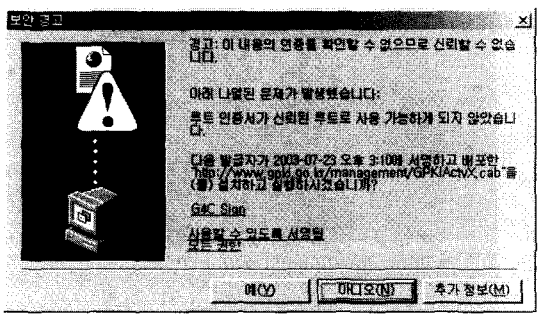

그림 11. GCMA 홈페이지 경고 화면

4.1.2 표준보안 API의 활용 분야

현재 GPKI 인증체계에서 사용 중인 표준보안 API는 3 종류가 있다. 기존의 표준보안 API가 변경되는 경우 사용자 측면에서는 기존 시스템의 교체가 어렵고, 관리자 측면에서는 기존 표준보안 API의 이중적인 관리문제가 발생한다. 기존 시스템 교체의 어려움은 표준보안 API 설계상의 문제에 기인하며, 기존 표준보안 API는 개발당시에 변경이 용이하도록 설계되지 못했기 때문에 내부적인 모듈의 변경이 필요할 경우 이를 수용하는 것은 사실상 불가능하다. 이러한 문제를 최소화하기 위해서는 추후 기능의 수정이나 추가가 발생할 경우 유연하게 적용될 수 있도록 설계되어야 한다. 표준보안 API가 유연성을 가지도록 설계되어 개발될 경우 이러한 문제는 하부 표준보안 API의 간단한 교체만으로 해결될 수 있을 것이다. 물론 현재 적용중인 표준보안 API는 일정기간의 유예기간을 두어 단계적으로 새로이 개발되는 표준보안 API로 교체하여야 할 것이다.

또 하나는 현재 사용 중인 표준보안 API가 사용자에게 지나치게 높은 수준의 암호학적 지식을 요구하고 있어 두가지의 문제점이 제기되고 있다. 첫째는 암호학적 지식이 부족한 응용프로그래머가 API를 사용할 때 개발이 어려워 개발기간이 매우 길어지게 되며, 둘째는 잘못된 사용으로 인하여 보안상의 문제를 야기할 수 있다. 이 두 가지 문제점은 새로운 응용시스템을 개발할 때마다 장애로 작용하여 GPKI 인증서 이용 확산에 걸림돌이 된다. 이 문제를 해결하기 위해서는 표준보안 API의 설계시점에서 암호학적 지식이 낮은 사용자를 고려하여 설계해야만 해결이 가능할 것이다.

4.1.3 인증서의 발급·재발급·갱신·폐지 및 관리

분야

GPKI 인증서를 사용하려는 이용자는 발급·재발급·갱신의 절차를 Off-line으로 진행하여 인증서를 신청할 수 있도록 되어 있는데, Off-line 신청시 인증서와 비밀번호가 인증담당자에게 노출되는 절차상의 문제가 발생한다. 또한, 단체 인증서를 신청하는 이용자의 경우 인증담당자에게 인증서의 발급과정을 일임하게 되므로 모든 단체 인증서 신청자의 개인키가 노출되는 문제점이 있다. 따라서 인증서를 발급받는 부분을 인증서 신청자가 직접 수행할 수 있도록 해야 한다.

또, 인증서의 갱신주기 문제가 있는데 등록기관, 시점확인(TSA : Time Stamping Authority), 기관용, 개인용 인증서의 경우 인증서의 유효기간이 2년 3개월로 되어 있다. 일반적으로 NPKI의 공인인증서는 보안상의 이유 등으로 유효기간이 1년으로 되어 있는데, 이는 보안상의 문제라는 표면적인 이유보다는 기업의 이익차원에서 설정된 것이다. 현재 행정전자서명 인증업무준칙과 세부지침에서 이미 인증서의 유효기간에 대한 사항을 정의하고 있다. 우선 GPKI 개인용 인증서의 경우 무료로 인증서를 발급하고 있으므로 특수한 보안상의 이유가 없다면 인증서의 유효기간을 연장하여 인증서의 유효기간이 짧아서 생길수 있는 인증담당자의 업무 부담과 인증서 이용자의 신청서 작성 등의 불편을 줄일 수 있을 것이다. 이와는 별도로 현재 단체로 신청한 인증서의 경우에는 인증서의 유효기간을 단축할 필요가 있다. 단체 인증서의 경우 업무의 편의성을 위하여 보안 부분을 많이 약화시킨 경향이 있다. 불가피하게 단체 인증서를 처리해야 하는 경우에는 단체 발급자에 한하여 단기간만 유효한 인증서를 발급하고, 이의 갱신을 유도하여 단체 인증서 처리로 인해 발생할 수 있는 문제를 줄일 수 있을 것이다.

다음으로는 인증서 검증시간의 문제인데, 현재 GPKI 인증서의 경우 인증서 검증시점에서 OCSP (Online Certificate Status Protocol) 서버에 매번 인증서의 유효성을 확인하고, RootCA, CA 인증서를 매번 접속하여 다운 받도록 되어 있다. 이는 사용자 측면에서 서비스 시간이 길어지는 문제와 디렉토리 서버에 부하를 주어 통신 대역폭의 낭비를 가져오게 되는데, 이러한 문제를 해결하기 위해서는 다음과 같은 절차를 생각할 수 있다. 우선 RootCA와 CA의 인증서를 미리 다운받아 로컬 시스템에 저장하는 방법이다. 그러나 이 경우에도 관리자가 변경되고 인증서가 갱신되면 서버 관리자가 인증서를 다운받아 저장해야 하는 문제가 발생할 수 있는데, 이 문제는 로컬 디렉토리에 인증서가 있는지 확인을 하고 없을 경우 자동으로 다운받는 구조를 응용프로그램이 가진다면 쉽게 해결할 수 있다.

그리고 현행 GPKI 홈페이지에서는 인증서 폐지를 할 수 없게 되어 있어 매우 불편한 문제가 있다. 즉 서면으로 인증서 폐지를 요청하고 폐지를 진행하도록 되어 있어 도난·유출이 발생할 경우 신속한 대응이 필요한데도 이를 온라인상에서 즉시 처리할 수 없는 문제점이 발생한다. 이러한 문제를 해결하기 위해서는 도난이나 인증서 비밀번호등이 유출된 것으로 판단될 경우 신속하게 사용자가 폐지 요청을 온라인으로 할 수 있는 절차가 요구된다. 인증서의 폐지 절차가 온라인으로 쉽게 이루어게 되면 인증서의 중요성을 사용자들이 인식하지 못하는 문제가 발생할 수 있는데 이러한 문제는 인증서에 대한 교육의 강화 등을 통해 해결하도록 노력해야 할 것이다.

4.1.4 행정전자서명인증체계의 보안성·안정성 분야

범용적으로 사용되고 있는 IBM호환 PC의 경우 안전한 전자서명을 생성하는데 여러 가지의 위협요소를 가지고 있다. 예를 들면 사용자의 키 입력을 도청하여 전자서명 비밀키의 비밀번호를 공격자가 알아낸다거나, 전자서명이 진행되는 과정에서 메모리 덤프 등을 통하여 전자서명키를 알아내는 공격이 발생할 수 있다. 이러한 문제를 해결하기 위해서는 안전한 서명의 생성을 지원하는 HSM(Hardware Security Module) 장비의 사용이나 스마트카드를 사용하는 방법을 생각해 볼 수 있다.

그리고 현재 행정전자서명인증관리체계에서 사용하고 있는 표준 보안 API의 경우 X9.17 ANSI 표준을 사용하고 있는데, X9.17난수 생성 알고리즘이 입력에 사용되는 의사 난수값인 현재의 날짜와 시간 및 임의의 Seed값 추측가능성과 난수생성에 사용되는 56비트의 키에 대한 Attack부분이 알려지면서 안전하지 않은 알고리즘으로 분류되고 있다. 이를 해결하기 위해 NPKI 인증체계에서는 공인인증기관의 실질심사 과정에서 안전한 난수생성시에 ANSI X9.31의 기준에 준하여야 한다는 기준을 마련하였다. 또한 FIPS PUB 140-1에 의해 생성된 난수의 안정성 테스트에 대한 기준을 마련 하였고 한국정보보호진흥원에서도 권고하고 있는데 이의 활용 방안이 필요하다.

표 8. 행정전자서명인증체계의 기술적인 문제점과 해결방안

구분	문제점	내 용	해 결 방 안
GPKI와 NPKI 인증체계 간의 상호연동	GPKI 인증서를 이용한 본인확인 불가	본인확인을 위한 식별번호가 인증서의 확장영역인 '주체 객체 이름' 필드에 포함되어 있지 않아 NPKI 응용프로그램에서 GPKI 인증서를 사용시 본인확인에 실패	-GPKI 인증서에 식별번호를 포함
	응용프로그램의 Delta CRL 처리지원 미비	DeltaCRL 갱신은 2시간 간격으로 이루어지고 있는데, NPKI 인증체계에서 검증하는 시점에 CRL만을 검증하는 경우 2시간 사이에 발생한 문제를 확인할 수 없음	-NPKI 응용 프로그램의 GPKI DeltaCRL 기능을 추가로 지원 -DeltaCRL 부분을 수행하지 않는 방법
	인증서 검증시 CTL방식의 문제점	CTL 방식의 경우 NPKI나 GPKI의 최상위 인증기관의 서명키가 노출되는 등의 문제 발생시 CTL의 유효성을 검증해야 하는 문제, CTL 유효기간이나 변경에 대한 정보를 획득하는 방법상의 문제, 변경에 대한 정보를 획득하는 문제 등이 있음	-표준보안 API 등에서 기능 지원 -인증기관간 상호연동을 위한 CTL 기술규격에서 지원 -변경된 사실을 협의된 절차에 따라 Out-of-band 방법으로 전달
	해외 PKI와 상호연동 고려 미비	전자행정의 국가간 상호연계를 위해 필요한 전자서명 인증체계의 상호연동 고려 미비	-GPKI와 국가 상호간의 요구사항에 적합한 연동방식의 모색이 요구됨 -국가간에 지속적인 상호 정책 및 법적 보완과 기술적 교류가 필요
	마이크로소프트사의 SSL 인증서 상호연동 문제	현재 GCMA 홈페이지에서 사용하고 있는 SSL 인증서의 경우 MS IE의 루트 인증서에 등록되어 있지 않아 안전하지 않다는 경고 창을 보게 되고, 이는 사용자의 신뢰를 약화시킴	-SSL 인증서를 MS IE의 "신뢰된 최상위 인증기관" 인증서에 등록 -프로그램의 배포에 사용되는 코드사인 인증서의 경우 "신뢰된 최상위 인증기관" 인증서의 개인키를 사용하여 서명
행정전자서명 인증서의 표준보안 API 활용	표준 보안 API의 변경에 따른 적용의 어려움	기존의 표준보안 API가 변경되는 경우 사용자가 변경된 표준보안 API와 데이터의 호환성을 확인하기 어렵고, 변경된 표준보안 API의 적용을 위하여 기존 응용 시스템의 수정이 어려움	-기능의 수정이나 추가가 발생할 경우 유연하게 적용될 수 있도록 설계 -현재의 표준보안 API는 단계적으로 새로이 개발되는 표준보안 API로 교체
	표준보안 API의 적용 편의성 향상	현재의 표준보안 API는 사용자에게 높은 수준의 암호학적 지식을 요구, 암호학적 지식이 부족한 응용프로그래머가 사용할 경우 개발기간이 증가하고, 잘못된 사용으로 인하여 보안상의 문제가 야기될 수 있음	-표준보안 API의 설계시점에서 암호학적 지식이 낮은 사용자를 고려하여 설계
인증서의 발급·재발급·갱신·폐지 및 관리	Off-Line 인증서 신청의 문제점	Off-Line으로 인증서 신청시 인증서와 비밀번호가 인증담당자에게 노출되는 문제와 단체 인증서를 신청하는 이용자의 경우 인증담당자에게 인증서의 발급과정을 일임하게 되므로 모든 신청자의 개인키가 노출되는 문제	-인증서를 발급받는 부분을 인증서 신청자가 직접 수행할 수 있도록 하여야 함
	인증서 갱신 주기의 문제	인증서의 유효기간이 짧아 인증담당자의 업무 부담과 인증서 이용자의 신청서 작성 등의 불편이 발생	-인증서의 유효기간 연장
	인증서 검증시간의 문제	인증서 검증시점에 RootCA, CA 인증서를 매번 접속하여 다운 받도록 되어 있어, 디렉토리 서버에 부하, 통신 대역폭의 낭비, 인증서 검증시간이 증가	-RootCA와 CA의 인증서를 미리 다운받아 로컬 시스템에 저장, 로컬 디렉토리에 인증서가 없을 경우 자동으로 다운받는 구조
	인증서 폐지 시 불편함	현재 운영되고 있는 GPKI 홈페이지에서는 인증서 폐지를 할 수 없고 서면으로 요청하게 되어 있어 도난·유출이 발생할 경우 온라인상에서 즉시 처리할 수 없는 문제 발생	-도난이나 인증서 비밀번호등이 유출된 것으로 판단될 경우 신속하게 사용자가 폐지 요청을 온라인으로 할 수 있는 절차가 요구됨
현행 행정전자서명 인증체계 보안성 및 안정성	범용 IBM PC의 문제	IBM호환 PC의 경우 사용자의 키 입력을 도청 또는 전자서명이 진행되는 과정에서의 메모리 덤프 등을 통하여 전자서명키를 알아내는 공격에 대한 피해 우려	-안전한 서명의 생성을 지원하는 HSM장비의 사용이나 스마트 카드를 사용
	X9.17 난수 생성 알고리즘 사용문제	현재 사용하고 있는 표준 보안 API의 경우 X9.17 ANSI 표준을 사용하고 있는데, X9.17 난수 생성 알고리즘의 경우 안전성의 문제가 있음	-NPKI 인증체계의 경우 공인인증 기관 실질 심사 과정에서 안전한 난수 생성 알고리즘을 사용하도록 권고하고 있음
	RootCA인증서의 검증문제	현재 사용 중인 RootCA 인증서의 경우 인증서에 CRL 분배점이 존재하지 않아 폐지 여부를 확인할 수 없음	-CRL 분배점 추가, 키와 비밀키 쌍은 유지하고, 필드만 갱신

보안성·안정성 측면에서의 다른 하나는 Root CA 인증서의 검증 문제이다. 현재 행정전자서명인증관리체계에서 사용 중인 RootCA 인증서는 인증서에 CRL 분배점이 존재하지 않는 문제점이 있다. 이로 인하여 RootCA의 인증서가 폐지되었는지 여부를 확인할 수 없다. 루트 인증서가 폐지되거나 갱신된 경우 신문이나 TV 등의 대중 매체를 통하여 신속히 사용자에게 알려야 하고, 현재의 표준보안 API에서는 루트 인증서의 경우 매번 다운받아 검증하는 방식으로 구성되어 있기 때문에 사용시점에서 인증서 경로 검증에 실패하게 되며, 다른 방식으로 인증서의 경로검증이 수행되면 문제가 발생하게 된다. 이 문제는 인증서에 CRL 분배점을 추가하여 해결 할 수 있다. 그러나 루트 인증서의 갱신으로 인해 하위에 모든 인증서를 교환해야 하는 문제가 남는다. 따라서 인증서의 키와 비밀키 쌍은 유지하고, 인증서의 필드만 갱신하는 방법을 사용할 수 있다. 이 경우 앞에 나온 모든 인증서를 교환해야 하는 문제점은 발생하지 않으며, NPKI의 CTL이 갱신되도록 하여야 한다.

4.2 정책적 발전방안

현재 행정전자서명인증체계의 경우 세부지침이 규정되어 있고, GCMA 운영자에 대한 교육은 1차와 2차에 걸쳐 이루어졌다. 그러나 실제 인증서 사용자에 대한 교육은 필요성이 증대되고 있음에도 불구하고 이루어지지 않고 있다. NPKI의 경우 공인인증기관의 수익 확대를 위하여 지속적인 이벤트와 홍보 활동 등을 수행하고 있다. 그러나 GPKI의 경우에는 상대적으로 적은 인력과 예산등의 문제로 활발한 활동이 이루어지지 못하고 있다. 이러한 문제점은 GPKI 인증체계의 인식에 대한 저하를 가져올 뿐 아니라 인증서의 이용률을 떨어뜨릴 수도 있다. 또한 사용자가 인증서에 대한 중요성을 인식하지 못함으로 인해 인증서를 함부로 취급하고 이로 인한 인증 담당자의 업무 부담과 보안사고 발생 위험이 높아질 수 있다. 따라서, 행정전자서명 인증서를 실질적으로 사용하는 일선 공무원에 대한 지속적인 교육을 실시하여야 한다. 이를 통하여 설문 조사에서 나타난 대리인을 통한 인증서의 사용이나 비밀번호 노출 등과 같은 문제의 심각성을 알려 보안사고의 예방과 이용 활성화를 도모할 수 있을 것이다. 또한, 1차, 2차에 걸쳐 인증 담당자에게 실시된 교육을 정례화 하여 운영자에 대한 교육이 정기적으로 이루어지도록 해야 한다. 공무원에게 실시되고 있는 컴퓨터 교육과 마찬가지로 인증체계에 대한 교육을 사용자가 수시로 받을 수 있도록 교육과목의 개설도 이루어져야 한다.

GPKI의 홍보활동은 한정된 인력과 조직 등의 문제로 인해 활발한 활동이 이루어지지는 못하고 있으나, 이러한 문제점은 다양한 홍보 방법을 사용하여 보완할 수 있을 것이다. 행정전자서명을 홍보할 수 있는 홈페이지로는 일반적으로 많은 사용자들이 이용하는 전자정부 홈페이지나 행정자치부의 홈페이지를 활용할 수 있을 것이다. 예를 들면 지속적인 사용자 설문 조사 등을 통하여 사용자의 인식을 제고 한다거나, 어린이들이 친숙하게 접근할 수 있는 홍보용 게임의 제작 등을 통하여 GPKI 인증체계의 인식을 제고할 수 있을 것이다. 또한 이러한 활동을 통하여 사용자가 인증서에 대한 중요성을 인식하고, 인증서를 함부로 취급하지 않게 된다면 인증 담당자의 업무 부담과 보안사고 발생 위험도 줄어들 뿐 아니라 대국민 서비스 측면에서도 질적 향상을 도모할 수 있을 것이다.

4.3 법·제도적 발전방안

현재의 GPKI인증체계에서는 인증서 신청을 받아 대행 업무를 처리하는 인증 업무 담당자에 대한 정의가 없다. 따라서, 인증서 발급과정에서 발생한 문제에 대하여 책임 소재를 명확히 할 수가 없다. 일반적으로 책임 소재를 알 수 없는 문제가 발생할 경우 NPKI 인증체계에서는 인증기관이 책임을 지도록 하고 있다. 그러나 GPKI 인증체계에서는 이에 대한 사항이 명확하지 않다. 그러므로 인증 업무 담당자에 대한 정의가 이루어져야 하며, 이를 통하여 인증서 발급과정에서 발생할 수 있는 문제에 대해 책임 소재를 명확히 할 수 있고, 문제 발생에 대한 명확한 책임소재에 따라 책임 있는 행정이 이루어질 수 있을 것이다.

인증업무 세부지침에서는 신청자가 직접 인증서를 발급받지 못할 경우 즉, "인증기관에서 신청자 행정전자서명키를 안전한 방법으로 생성하고 신청자에게 전달하며, 전달되기 이전에 이용되지 못하도록 한다."고 규정되어 있다. 그러나 이미 발급된 인증서가 이용되고 있어 인증업무 세부지침을 위반하는 경우도 발생하고 있다. 기술적으로 이러한 문제를 해결하기 위한 노력은 많은 비용과 시간을 요구한다. 따라서

기술적인 해결 이전에 제도적 개선을 통해 인증기관에서 신청자가 직접 인증서를 받도록 하여 보안문제가 발생하지 않도록 해야 할 것이다.

V. 결 언

본 논문에서 설문조사를 통해 행정전자서명 인증서에 대한 인식과 이용실태에 관한 부분을 확인할 수 있었고, 행정전자서명 이용 활성화의 걸림돌이 될 수 있는 여러 가지 요인들을 살펴보았다. 또 이러한 검토를 통하여 도출된 문제점에 대해 개선해야 할 사항과 발전방안을 모색해 보았다.

행정전자서명의 활성화 및 발전방안이 본격적으로 추진되어 행정전자서명의 이용이 활성화된 이후에도 본 연구에서 분석한 설문조사 결과 및 발전방안을 참고하여 행정전자서명의 수요 및 만족도 조사를 주기적으로 실시하고, 이를 통한 지속적인 유지발전과 사용자의 확대가 이루어져야 할 것이다.

참 고 문 헌

[1] 박인재, "전자정부의 행정전자서명기반 구축현황 및 향후 발전방향", 정보보호학회지, 2003.8

[2] "전자문서 활성화 방안", 행정자치부, 1998.9

[3] 이동훈, 제8회 정보보호심포지움 "전자서명기술", 2003.7.15

[4] 박영하, "PKI포럼, 각국 법·제도 연구 활발", 전자신문, 2002.9.5

[5] 박영하, "PKI 해외 활용현황", 전자신문, 2002.9.19

[6] 국가정보화백서(2002, 2003), 국가정보원

[7] 전자정부백서(2003.1.), 전자정부특별위원회

[8] "전자서명법", 정보통신부, 1999. 7.

[9] "전자정부구현을위한행정업무등의전자화촉진에관한법률", 행정자치부, 2001. 3.

[10] 서동규, "공인인증시장 활성화 왜 안되나", 전자신문, 2003.5.20

[11] 염흥렬, "PKI 도메인간 상호연동 방안", 전자서명인증워크샵, 2001. 9.

[12] 이재일, "Certificate Trust Lists의 개념 및 모델에 관한 연구", WISC 2002, 2002. 8.

[13] 강원영, "미국 FBCA 구축동향 분석", 전자서명인증관리센터, 2000.12.

[14] 이석래, "일본의 전자서명추진동향", 정보보호뉴스, 한국정보보호진흥원, 2001.5.

[15] 정진명, "인터넷 관련 독일의 법제 동향과 전망", 한국법제연구원, 2001.

[16] "공인인증기관 평가지침", 한국정보보호진흥원, 1999.11.

[17] Chris Sundt, "PKI - Panacea or silver bullet?", Information Security Technical Report, Vol 5, No. 4, 2000, pp. 53-65

[18] Satoru Tezka, "Achieving PKI interoperability - An experiment between Japan, Korea and Singapore and Future plans", Asia PKI Forum, September 2002.

[19] http://www.gpki.go.kr

[20] http://www.gcc.go.kr

〈著者紹介〉

추 경 균 (Kyung-Kyun Choo) 정회원

1983년 2월: 숭실대학교 전자계산학과 졸업
1988년 8월: 숭실대학교 산업대학원 전자계산학과 석사
1998년 9월~현재: 숭실대학교 대학원 컴퓨터학과 박사과정(수료)
1982년 11월~1997년 1월: 총무처 정부전산정보관리소
1997년 2월~현재: 행정자치부 행정정보화담당관실
1992년 12월: 정보처리기술사(전자계산조직응용 분야)
1993년 2월: 정보처리기술지도사
1998년 12월: 한국 정보시스템감리인
1996년 2월~2001년 8월: 한국정보통신기술사협회 이사 역임
〈관심분야〉 전자정부, 정보시스템보호, 전자서명, PKI, PMI, 프로젝트 관리

김 종 배(Jong-Bae Kim) 정회원

1996년 2월: 서울시립대학교 경영학과 졸업
2002년 8월: 숭실대학교 정보과학대학원 정보산업학과 석사
2002년 8월~현재: 숭실대학교 대학원 컴퓨터학과 박사과정
2001년 3월~현재: (주)이엔터프라이즈 대표이사
〈관심분야〉 정보보호, 소프트웨어 개발 방법론, 에이전트 시스템 등

류 성 열(Sung-Yul Rhew) 정회원

1997년 2월: 아주대학교 컴퓨터학부(공학박사)
1997년 3월~1998년 3월: George Mason University 교환교수
1981년 3월~현재: 숭실대학교 정보과학대학 컴퓨터학부 교수
1998년 3월~2001년 2월: 숭실대학교 정보과학대학원 원장
1998년 3월~현재: 숭실대학교 전자계산원 원장
〈관심분야〉 소프트웨어 유지보수/재사용, 소프트웨어 재공학/역공학, 정보보호 등