情 報 保 護 學 會 誌
第17卷 第6號, 2007. 12

국외 PKI 구축 현황 분석

이성진*, 최동현**, 원동호***, 김승주****

요 약

인터넷이 발달되고 널리 보급됨에 따라 안전한 통신과 인증 수단이 필요하게 되었다. 이러한 수단으로 PKI가 등장하였으며, 현재 전자상거래 및 여러 인증과 관련한 분야에 널리 사용되고 있다. 하지만, 더 향상된 통신 기술과 온라인 서비스의 확대로 인해 인증 대상이 확대되고, 서비스 환경이 변화되어 PKI를 이용한 인증체계는 한계에 이르렀다. 따라서 앞으로 계속 변화될 인터넷 환경에 대비하여 현재의 인증체계를 고도화하기 위한 방안이 필요하다. PKI를 기반으로 한 인증 시스템의 고도화 기능을 연구하기 위해서는 현재 국내외 PKI 구축 현황 분석이 선행되어야 한다. 본 논문에서는 국외 PKI 구축 현황을 분석하여 차세대 인증체계의 요구사항을 도출하기 위한 기반 정보를 제시한다.

Ⅰ. 서 론

통신과 컴퓨팅의 발전에 따라 은행 업무, 쇼핑 등의 오프라인의 서비스들이 온라인으로 확대되면서 안전한 통신과 인증 수단이 필요하게 되었다. 안전한 인증 수단으로 PKI 구조가 등장하였으며, 인터넷을 통한 안전한 전자상거래를 위해 현재 널리 사용되고 있다. 전자인증이란 가상공간상에서 신분확인, 전자 업무 내용의 정보보호 및 무결성, 전자행위에 대한 부인봉쇄 등 전자 업무의 중요 인증과 관련하여 신뢰할만한 제 3자(인증기관)가 확인 및 증명하는 것이다. 전자인증에서 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 핵심기술인 전자서명기술이 안전하게 운영되어야 한다. 전자서명기술에 사용되는 공개키 암호 알고리즘에서 비밀키의 기밀성과 공개키의 무결성이 보장되어야 하며, 이를 위해 공개키 기반 구조를 사용한다. 국내에는 1999년부터 PKI가 구축되고 인증 서비스를 제공하기 시작하였으며, 인터넷뱅킹, 온라인 증권거래 시스템, 전자상거래 등에 안전한 통신과 인증을 제공하고 있다.

지속되는 통신의 발달과 온라인 서비스의 확대로 인해 인증대상이 점점 확대되고, 서비스 환경이 다양하게 변화함에 따라 기존의 인증체계는 효과적인 대처가 한계에 다다르게 되었다. 인터넷 환경은 앞으로도 계속 변화할 것이다. 이러한 변화에 효과적으로 대체할 수 있는 인증체계의 고도화 방안에 대한 연구가 필요하다. 인증체계의 고도화 방안을 연구하기 위해서는 국내외 PKI 구축 현황의 분석과 인증 서비스의 성과 분석을 통해 차세대 인증체계의 요구사항을 도출해야 한다.

본 논문에서는 인증체계의 고도화 방안을 위한 국외 PKI 구축 현황을 분석하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 아시아 지역의 PKI 구축 현황을 분석하고, 3장에서는 북미 지역의 PKI 구축 현황을 분석하고, 4장에서는 유럽 지역의 PKI 구축 현황을 분석하고, 마지막으로 5장에서는 결론을 맺는다.

Ⅱ. 아시아 지역 PKI 구축 현황 분석

2.1. 대만

대만의 경우, 정부에서 약 10년 전부터 PKI 개선을 위해 여러 가지 노력을 하고 있다. 1997년 정부 PKI 프

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음.
[IITA-2007-S-601-01, 자기통제 강화형 전자ID지갑 시스템 개발]
* 성균관대학교 정보통신공학부 정보보호연구소 sjlee@security.re.kr
** 성균관대학교 정보통신공학부 정보보호연구소 dhchoi@security.re.kr
*** 성균관대학교 정보통신공학부 정보보호연구소 dhwon@security.re.kr
**** 성균관대학교 정보통신공학부 정보보호연구소 skim@security.re.kr

레임워크가 설계되었고 이듬해 정부 인증기관(GCA)이 설립되었다. 2001년에는 전자서명법이 제정되었고, 정부 루트 인증기관을 포함하는 정부 PKI 프레임워크, 내무부(MOI) 인증기관, 경제부(MOEA) 인증기관이 운영되고 있다[1].

2.1.1. 대만의 E-Tax Filing Service

전자 세금 신고 서비스(e-Tax Filing)는 대만의 납세자 및 정부 모두에게 커다란 이익을 가져다주기 위한 중요한 정부 혁신적 서비스 중 하나이다. 1998년 이후, 재정경제원(Ministry of Finance)은 Individual Income Tax, Tax Withholding/Exemption Certificate, Business Tax, Profit-Seeking Enterprise Income Tax, 그리고 Provisional Income Tax 을 전자적으로 신고할 수 있는 e-Tax Filing 서비스 계획을 시작하였다. 이 중 첫 번째(Individual Income Tax)는 개인과 정부 간의 거래(C2G)이고 나머지 네 가지는 기업과 정부 간의 거래(B2G)이다. 그 후 1년 뒤인 1999년, 대만에서는 개인 소득세의 전자 신고를 시작하였고 이듬해 나머지 네 가지의 서비스를 시작하였다[2].

Trade-van Information Services 사는 2004년에 재정경제원의 금융 데이터 센터(the Financial Data Center)를 대신하는 e-Tax Filing 서비스를 위한 시스템을 개발했다. 이 시스템의 성공적인 개발로 Trade-van Information Services 사는 국가 세금 관리 기관을 위한 어플리케이션 서비스를 제공하는 시스템을 운영하는데 중요한 역할을 했다. 이 시스템은 클라이언트 어플리케이션, 암호 인증 처리, e-Tax Filing 처리 어플리케이션, payment bridge, e-Filing consolidator, 금융 데이터 센터에 데이터를 전송하는 모듈, 인증서 인증 센터와 상호 연결하는 모듈과 같은 주요 컴포넌트를 포함한다.

e-Tax Filing Service를 제공으로 적어도 4시간에서 많게는 며칠 동안을 허비하던 시간을 세금 신고의 모든 절차를 5분 정도로 단축하였다. 더욱이 모든 절차는 전자적으로 가능하여 데이터의 무결성을 보장하고, 기한이 지나 세금을 납부하는 경우를 최소화할 수 있다. 정부 측면에서도 전자적인 작업으로 세금 신고에 필요했던 인력의 낭비를 감소시켜 정부 예산을 상당히 절약할 수 있다. 납세자에게는 세금 신고 절차를 진행하는데 있어 더 빠르고 효율적인 방법을 제공해준다. 이는 정부 효율성을 총체적으로 증가시킬 수 있다.

2.1.2. Land Administration e-Service for Government Agencies

토지 관리는 국가 관리에 있어서 기본적인 토대를 구성하며, 국가재건 및 경제개발, 사회 안전, 일반 대중의 권리와 자산의 보장에 대해 중요한 기능을 한다. 지난 몇 년 동안, 대만의 토지 관리 기관은 그들의 내부 처리 과정을 리엔지니어링하고 전산화를 통해 서비스 효율성을 증가 시켜오고 있다. 또한 인터넷의 급속한 발전으로 인해 온라인을 통한 서비스가 증가하고, 많은 사람들이 토지 정보를 쉽게 접근할 수 있게 되었다. 이는 토지 관리 기관 변화의 계기를 가져왔다[3].

전자서명법 개정 및 중앙 정부 토지 e-gateway 계획에 맞춰 "Cadastral copies issuing DIY on internet" 이라는 서비스가 개발됐다. 이 서비스로 인해 대중은 지역 토지 관리 기관의 웹사이트를 방문해 그 기관에 의해 전자 서명된 토지대장을 다운로드, 입출력 등을 할 수 있게 되었다. 더욱이 정부기관이 내무부의 토지 관리부서에서 제공하는 “e-Cadastral” 시스템에 온라인으로 접속할 수 있게 됨에 따라 대중은 각각의 정부 기관에 토지대장 문서를 신고해야하는 번거로움을 피할 수 있게 되었다[3].

토지 정보 단일 창구 서비스 인프라 구조(The land information single window service infrastructure)는 다음과 같은 컴포넌트들로 구성된다.

- 정부 서비스 네트워크(Government Service Network, GSN) : 상호 연계하는 정부 기관을 위한 국가전역 네트워크 플랫폼
- GCA & MOICA : 네트워크 보안을 제공
- 국가 기관 사용자 : 토지 정보 서비스를 요청하는 공무원
- eService Portal, 내무부 토지 관리부서의 단일창구 (Single window of Department of Land Administration, Ministry of the Interior (MOI)) : 다른 정부 관리기관의 토지 정보 요청을 승낙
- 전송 시스템 : 내무부 토지 관리부서의 단일 창구로부터의 메시지를 받아서 받은 메시지를 데이터 생산 시스템에 전송한 다음, 형식화된 데이터를 단일 창구로 되돌려줌
- 문서 처리 시스템 : 토지 정보를 PDF 형식으로 재변환하고, 전자봉투를 암호화함

“e-Cadastral” 시스템 서비스는 2005년 12월 이후 시

작되어, 급격하게 성장 하였다. 이러한 눈부신 성장은 work flow의 리엔지니어링과 서비스 중심의 e-Cadastral system service가 공무원의 요구, 일반 대중의 이득과 명확히 맞아 떨어졌기 때문에 가능했다. 또한, 이 서비스를 통해 인력 낭비나 사회 비용을 감소시킬 수 있었다. 꾸준한 사용자 성장률은 정부 관리 기관이 PKI를 이용한 e-Cadastral service를 신뢰할 수 있게 하였고, PKI 기술의 적용이 전자정부의 진보에 도움을 줄 수 있다는 것을 보여 주었다.

2.2. 일본

e-japan Strategy가 2001년 1월에 공식화된 이후로 일본은 네트워크의 개선과 e-commerce/ e-government 조성을 위해 필요한 IT 기반을 개발하는데 몰두 하여, 그 결과 일본 내의 인터넷 보급률이 증가하였다. 일본의 두 번째 국가 전략인 e-Japan Strategy II는 2004년 6월에 공식화 되었다. 이는 기존 IT기반 기술을 사회・경제 시스템에 적용시켜 혁신을 불러일으킬 수 있도록 하는데 초점을 맞췄다. 이러한 두 전략은 의료 및 식품, 생활, 중소기업 자금, 정보, 취업, 정부 서비스 등 7 가지 분야에 초점을 맞추고 있다. 이는 민간 부문이나 공공 부문 어느 한 부문에만 이익을 가져다주는 것이 아니라 국가 전체적인 발전을 도모하려는 것이다[1].

2.2.1. Medical and healthcare network 구축사례

Healthcare 산업에서는 환자에게 장기적인 의료 제공을 더 보장하기 위한 개정이 이루어지고 있다. 이러한 개정에는 여러 의료 시설 및 보건소 등에서 함께 접근 가능한 의료 정보 데이터베이스를 구축하는 것이 포함된다. 이러한 의료 정보 데이터베이스는 현재 고려되고 있는 많은 보안 대책 등으로 보호되어야 한다. 이와 같은 네트워크의 구축은 distance 의료에 용이할 것이다[1].

2001년 12월 일본 후생노동성(the Ministry of Health, Labor and Welfare)은 “grand design for the digitization of the medical field”를 공개 발표했다. 이를 통해 국가 전략이 정보기술을 이용하여 의료 산업을 강화하는데 목적을 두고 있다는 것을 알 수 있다. “grand design”의 주요 요소는 의료 기록을 위한 전자 시스템과 건강 보험 청구(claim)를 위한 것의 설립 및 보급이다. PKI 사용에 관한 “grand design”은 개인과 그들의 자격을 확인하기 위한 인증 시스템을 포함할 것이다. PKI를 사용하면 시스템은 의료 서비스 제공자와 서비스 사용자 모두의 자격을 확인하고 자동적으로 사용자 의료 정보를 기록할 것이다.

위와 같은 증명 기술(HPKI)을 위한 인프라 구축의 문제점 중 하나는 의료 서비스 종사자의 자격 증명에 대한 논쟁이다. HPKI 프레임워크에서 시스템은 일반적인 증명 서비스를 통해 사람을 확인하는데 그치지 않고 healthcare 분야에서 일하는 사람의 국가 자격 정보를 담은 증명서를 국제 규격(ISO/TS 17090)에 따라 기록할 수 있을 것이다. 그러므로 HPKI가 개발된다면, 의사의 확인이 요구되는 문서, 새로운 병원에 제공되는 환자에 대한 정보를 담고 있는 소개장과 같은 문서, 급여와 같은 다양한 어플리케이션이 덧붙여질 필요가 있는 examination report 등이 전산화되어 즉시 온라인을 통해 이용 가능할 것으로 보인다.

2004년 산업계에서는 모든 healthcare 분야를 위한 공통의 인증 정책(Certification Policy, CP)을 입안하기 시작했다. 앞서 말한 계획은 HPKI 시스템의 4가지 세부사항 및 CP에 기반하여 구축될 HPKI 시스템을 위한 신뢰할 수 있는 구조를 설정하고, 그 후 증명을 시도하는 것을 고려한다.

이전에는 서비스 사용자(보험 가입한 환자)의 자격을 확인하는 일이나 자동적으로 개인 정보를 전송하는 서비스에 PKI를 사용한 경우가 없었다. 여기에서 제안하는 것은 IC 카드 같은 건강 보험 증명서에 대한 대안이다. 이 서비스의 운영은 reception desk system과 medical history display system, 두 개의 주요 시스템으로 구성되어 있다. Reception desk system은 보험에 가입한 사람의 정보를 참조하여 설정된다. 이 시스템에서는 만약 카드를 분실하거나 도둑맞았을 경우에 카드내의 내용이 서면에 의한 성명을 제출함으로써 무용지물이 된다. Medical history display system에서는 개인의 건강 검사 기록이 의료 검진 정보나 다른 터미널을 통한 건강관련 정보를 참조하여 IC 카드에 저장되어 있다. 의료 서비스 종사자에 분배되는 접근 카드는 관련 없는 환자의 개인 정보에 대한 접근을 제한함으로써 관리할 수 있다.

2.2.2. 중소기업을 위한 전자 외상매출채권

중소기업과 관련된 자금 조달에 있어서 두 가지 포괄

적인 개정이 필요하다. 먼저 중소기업의 원활한 자금 조달을 위한 자금 조달 절차의 간소화, 효율화이다. 두 번째는 신용 보장 절차의 효율성 향상과 금융 기관의 재정적 위험성 감소를 통해 신용 정보를 강화할 수 있어야 한다. 이러한 절차를 좀 더 효율적으로 만들기 위해 필요한 것은 안전하고 빠른 금융 정보의 흐름(유통)이다. 전자 외상매출채권의 대표 비즈니스 모델에 이러한 문제점들을 안고 있다[1].

전자 결제 서비스를 제공하는 Shinkin Central Bank는 인증 부서를 설립하고 공개키 인증서를 발행하였다. 이 은행과 거래하는 기업은 예전에는 문서 교환을 통해 수행하던 결제 작업을 온라인 전자 결제 플랫폼을 이용하여 전자적으로 실행할 수 있게 되었다. 전자 결제 서비스를 통해 수행되는 금융 활동은 실제 비즈니스 작업과 비교해서도 무시하지 못할 정도의 활동성을 가진다. 전자 상거래에서 대출 과정을 완료해주는 전자 대출 시스템이 발달한다면 시스템이 매우 효율적일 수 있다. 즉, 자금 조달의 간소화·효율화를 통한 상거래 촉진과 대출 관리 비용 감소는 효율적인 측면에서 많은 진보를 가져 올 것이다.

2.3. 싱가포르

싱가포르는 지난 1998년 7월 전자거래법을, 1999년 2월 전자거래 시행규칙을 공포해 PKI를 전자거래상의 보안을 위한 주된 기술로 명시했다. 싱가포르의 공인인증기관으로 '넷트러스트'가 2001년 6월 지정되었다. 싱가포르의 인증서비스는 민간 및 정부를 구분하지 않고 전자거래법을 따른다. 넷트러스트는 인증서를 정부 공무원에게 PS카드(스마트카드의 일종)에 넣어 발급했으며, 공무원은 이를 이용하여 급여 등의 개인정보 접근 및 정부 내의 보안 e메일 교환용으로만 사용할 수 있도록 하였다. 현재 싱가포르 일반 국민에게는 인증서가 거의 발급되지 않았지만, 은행과 SME(Small and Medium Enterprise)간 B2B 거래용으로는 일부 사용되고 있다[4].

싱가포르의 PKI에 대한 구체적인 기술 개발이나 연구에 대한 결과는 발표되지 않았지만, 아시아권에서는 최초로 PKI 기반 전자서명 서비스를 도입하였다. 현재 싱가포르 전자서명 인증 체계는 NCB(National Computer Board)에서 중점적으로 추진, 관리하고 있다[4].

2.3.1. CORENET e-Submission

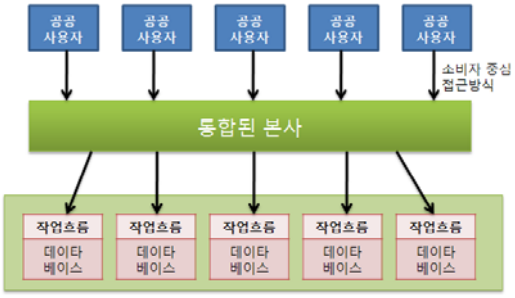
건설 산업에서 있어, 다양한 정부 기관에 의한 승인은 작업 시작 전에 반드시 필요하며, 건설 계획은 전형적으로 하드카피해서 제출되고 이들은 승인을 위해 관련 정부 기관에 전달된다. 이와 같이 제출된 계획에 대한 승인에는 상당한 시간이 요구되기 때문에, 운용 효율성 증가와 비용 절감, 계획에 대한 빠른 승인을 위해 단일 창구 제출 시스템이 필요하게 되었다. 다음 [그림 1]은 이와 같은 단일 창구 제출 시스템의 개념을 보여주고 있다[1].

PKI는 인프라의 절대적인 부분이다. 자격이 있는 전문가(기술자, 건축가, 전기 기사, 배관공 등)는 그들이 공식문서를 온라인을 통해 제출하기 전에 해야 하는 전자서명을 위해 디지털 인증서를 갖추고 있다.

관리 기관의 직원들은 제출된 계획에 대한 승인을 위해 디지털 인증서를 발행 받는다. 모든 제출된 문서는 전자서명을 통해 안전하게 보관되고 서명은 요구가 있을 때면 언제든지 검증할 수 있다.

CORNET e-Submission system(eSS)은 다음과 같은 특징을 갖는다.

- 민간 부문 및 공공 부문에 대해 one-stop 편의 제공
- 자격이 있는 전문가가 언제 어디서든지 계획안에 대해 다수의 승인기관에 제출이 필요할 때 one-stop 포인트 제공
- 제출한 계획안에 대한 결과를 온라인으로 확인하고자 할 때 one-stop 접근 제공



[그림 1] E-Submission 과정

- 승인 기관에서 제출된 계획안의 결과 게시를 위한 one-stop 게시판 제공

2.4. 중국

2005년 4월부터 중국에서 전자서명법이 시행되고 있다. 현재 중국에서 국가 PKI 구조는 루트 CA 운영방식을 따르며, 루트 CA에 지역 또는 업무에 따른 13개의 CA가 연결되어 있다. 민간 부문은 상하이 CA, 광둥(홍콩텔레콤) CA 등 5대 주요 CA가 루트 CA로 연결돼 있는데, 이를 연합(United) CA라고 부르며 상하이 CA가 관리한다. 이 가운데 대표적 CA인 상하이 CA는 30만장의 인증서를 발급했으며 인증서 종류는 신분확인용, e메일용, 웹서버용, 코드사인용, VPN용 등이 있다. 이밖에 전국적으로 자치 정부별로 구축된 80여개의 CA가 운영되고 있다[4].

2.4.1. Shanghai Pudong Development Bank

1993년 1월 9일 People's Bank of China의 승인을 통해 합병된 Shanghai Pudong Development Bank (SPDB)는 홍콩 내에서 대리자로써 26개의 제휴은행과 350 개의 비즈니스 네트워크를 설립했다. SPDB에서는 2003년까지는 은행 카운터를 통해서 은행 업무를 수행해 왔다. 그러나 2003년, 그들이 가진 채널과 소비자 자원을 기반으로 인터넷을 통한 온라인 은행 및 온라인 지불 방안을 개발하기로 결정하였다[5]. 그러나 소비자들은 온라인 뱅킹을 통해 중요한 정보가 외부로 노출되는 것을 염려하였다. 모든 은행의 온라인 업무는 두 가지 상황으로 분류할 수 있다. 즉, 업무 수행에 있어 증명을 하는 경우와 안하는 경우이다. 증명 없이 진행되는 온라인 업무는 계좌 잔고 확인과 같은 간단한 기능만을 수행한다. 그러나 증명을 하는 경우는 온라인 쇼핑, 투자, 금융거래, 비밀번호 변경 등과 같은 외부로의 노출을 막아야하는 정보를 다룰 때이다. 이와 같은 곳에 PKI 기술을 기반으로 한 전자 증명 인증 방법을 사용하여 사용자의 안전성에 대한 불안감을 효율적으로 감소시킬 수 있다[5].

이 방식을 이용함으로써 사용자는 은행을 직접 방문하는 시간을 줄일 수 있고, 더 편리하고 빠른 서비스를 받을 수 있다. PKI 기술에 기반을 둔 전자 증명 메커니즘은 딜러의 신원, 보안, 무결성, 정보의 불가역성을 보호함으로써 안전성을 증가시킬 수 있다. 그러므로 이 방식은 안전하지 않은 영향력 있는 온라인 비즈니스에 적용할 수 있다[5].

Ⅲ. 북미 지역 PKI 구축 현황 분석

3.1. 미국

3.1.1. 국방부(DoD) PKI

미국 국방부 PKI는 국방 정보 인프라를 안전하게 보호하기 위해 중요한 기반을 제공하며, PKI 증명 정보를 저장한 CAC(Common Access Card)를 약 350만 명의 사용자에게 발행할 만큼 세계 최대 규모를 가진다. 국방부 임무와 사업의 넓은 범위를 충족시키기 위해 NSA(National Security Agency)와 DISA(Defense Information Systems Agency)가 미 국방부 PKI PMO (Program Management Office)를 설립하였다. PKI PMO는 미국 국방부의 임무와 넓은 범위의 운영을 지원하고 그 수행에 관련된 모든 개체와 프로그램, 시스템을 지원할 수 있도록 광범위한 PKI를 배치하는 의무를 가진다. 미국 국방부 PKI 전략은 미국 국방부 PKI를 정보기술(IT) 환경에서 개발되고 발전하는 기술과 표준에 보조를 맞출 수 있는 상업적인 제품과 서비스 및 공개 표준에 기반을 두어야 한다고 방침을 세웠다. PKI PMO는 적절한 수준의 보안도 제공하고 미국 국방부 내부뿐만 아니라 외부적으로는 연방정부 그리고 국제기관과 비즈니스 파트너와의 상호 운용성도 제공하는 솔루션을 원했다. 9개 업체가 제공한 디지털 인증서 검증 솔루션을 광범위하게 독립적으로 평가한 후, PKI PMO는 Tumbleweed사의 Valicert VA(Validation Authority)[6]를 선택했다.

미국 국방부 PMO(Program Management Office)에서 130만 명 이상의 사용자에게 디지털 인증서 검증 서비스를 제공하기 위해 도입된 VA는 디지털 인증서의 실시간 검증을 위한 포괄적이고, 유연성 있고 신뢰할 수 있는 프레임워크와 폐기 또는 만료 기한이 지난 증명 정보를 이용한 접근으로 야기될 수 있는 국방 정보 인프라(Defense Information Infrastructure) 손상에 대한 보호도 제공한다. 또한, 다양한 운영체제 플랫폼의 수많은 응용프로그램에서 디지털 인증서 검증을 가능하게 하기 때문에 미국 국방부의 심층 방어(Defense In Depth)

전략과 일관성을 가진다.

미국 국방부 PKI는 실시간으로 디지털 인증서의 상태를 검증해 주는 OCSP(Online Certificate Status Protocol, RFC2560)[7]를 포함하여 다양한 공개 표준을 지원한다. 디지털 인증서의 상태를 확인하기 위해 OCSP를 이용하기 전에 국방부 사용자들은 안전한 위치에 있는 하나의 중앙 서버로부터 1MB가 넘는 큰 용량의 CRL(Certificate Revocation List)를 다운로드 해야 한다. CRL 다운로드는 많은 시간을 필요로 하고 그 시간 동안 생산성이 많이 떨어지게 된다. 심지어 많은 사용자들이 디지털 인증서 검증을 건너뛰게 할 수도 있고 이는 국방 정보 인프라를 폐기 또는 기한이 만료된 증명 정보에 의한 잠재적인 위험에 빠뜨릴 수 있다. Tumbleweed사의 Valicert VA와 OCSP 공개 표준을 이용함으로써 디지털 인증서의 상태를 몇 ms(milli-second) 시간 내에 확인할 수 있고 디지털 인증서 검증 과정을 사용자에게 숨길 수 있다. 또한 정교한 캐싱(caching)과 복사를 지원하는 혁신적인 Repeater-Responder 구조를 특징으로 하고 있기 때문에, PKI PMO가 디지털 인증서 검증 인프라 규모의 향상과 개발을 비용상 가장 효율적인 방법으로 할 수 있게 하여 보안성과 생산성을 향상 시켰다.

VA를 이용함으로써, PKI PMO는 전술적인 작전과 공동 작전 그리고 연합 작전에 대한 부서의 능력을 향상시킬 수 있고, 연합국과 동맹군, 민간 기관, 사업 파트너와의 상호 운용성도 향상시킬 수 있다. 또한 VA는 CA에 중립적이고 국제 보안 표준과 공개 기술을 완벽히 지원한다.

VA는 연방 정보 처리 표준(Federal Information Protection Standard)인 FIPS 140-l(DOD Joint Interoperability Testing Command, and Identrus standards, and is part of the Identrus, SWIFT Trust Act, BACS and Global Trust Authority financial trust infrastructures)[8]을 따르며, 또한 NIST(National Institute of Standards and Technology)와 NSA의 NIAP (National Information Assurance Partnership)에 의한 공통평가기준(Common Criteria) 평가 보증 등급인 EAL-3을 위한 요구사항도 만족한다.

3.1.2. Microsoft사의 PKI

2000년 2월 Microsoft 회사 네트워크를 보호하기 위해 Microsoft의 내부 IT 그룹인 OTG(Operations and Technology Group)는 전 세계 400여 개 지사에 배치된 Microsoft 직원들에게 가용성, 개인 정보 보호 및 보안을 제공하는 서비스, 응용 프로그램 및 인프라로 구성되어 있는 IT 환경을 유지하기 위해 엔터프라이즈 PKI를 구현함으로써 내부와 외부 네트워크 통신 보안을 향상시킬 수 있었다[9].

OTG는 오프라인 PKI 루트, 오프라인 중간(또는 하위) CA 그리고, 온라인 발급 CA에 대한 기능 레이어를 구분하는 3계층으로 구성되어 있다. 이러한 구조는 루트 CA가 네트워크 트래픽에 절대 노출되지 않고, 오프라인 중간 CA가 발급된 후에는 직원들이 거의 관여할 수 없으므로 손상 가능성이 최소화된다. 또한 상위 부분에 영향을 미치지 않고 하위 부분에서 추가 변경이 가능하므로 CA 구조에 유연성을 제공한다. 모든 CA는 OTG가 제어하는 안전한 저장소에 보관되어 있으며, 오프라인 루프 CA와 두 개의 중간 CA는 다음과 같은 기능을 수행하도록 구성되어 있다.

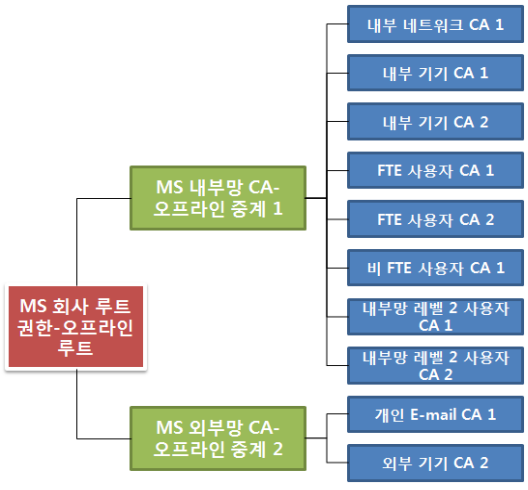
- Microsoft 회사 루트 CA : 2개 오프라인 중간 CA의 인증서를 발급 또는 해지하는 용도로만 사용
- Microsoft 중간 인터넷 CA : Microsoft 회사 네트워크 환경의 경계 내에서만 사용하는 인증서를 발급하는데 사용되는 다른 모든 CA를 인증
- Microsoft 중간 익스트라넷 CA : 인터넷과 Microsoft의 Extranet 환경을 포함한 Microsoft 회사 네트워크 경계 외부에서 사용하는 인증서를 발급하는데 사용되는 다른 모든 CA를 인증

최초의 Windows 기반 엔터프라이즈 품질 PKI는 Microsoft Windows 2000 Server에 포함되었다. PKI의 내부사용을 확대하기 위해 OTG는 Windows 2000 Server가 구축된 Microsoft 회사 네트워크에 PKI를 핵심 서비스로 구현했다. 최초로 Microsoft에 PKI를 배포할 당시, 여러 타사 PKI 공급자가 외부에 기반을 둔 PKI 서비스 솔루션을 제공했지만 OTG는 내부사용에는 타사 기반 PKI를 구축하지 않기로 하고, 비용 최소화, 시스템 제어 극대화 및 관리 간소화 등의 이유로 기존 Windows 기반 서버 인프라를 사용하여 자체 PKI를 운영하기로 결정했다. OTG는 PKI 설계 시, 독립 실행형, 엔터프라이즈 또는 두 종류가 혼합된 CA를 구축했다. 독립 실행형과 엔터프라이즈 CA 종류에는 루트 및 하위 등 2가지 종류의 계층 구성이 있고 루트 CA는 자체 서명되는 반면, 하위 CA는 인증서를 다른 CA가 서

명할 것을 요구한다. 체인에서 하위 CA가 루트 CA 아래에 있지만, 발급 CA 위에 있을 경우, 하위 CA를 중간 CA라고 한다. 신뢰된 루트 인증기관 저장소 내에 루트 CA 인증서를 저장함으로써 클라이언트가 루트 CA를 신뢰하면 기본적으로 계층에서 하위에 있는 모든 CA도 신뢰하게 되는 구조를 따른다. 따라서 조직에서 루트 CA는 가장 중요한 신뢰 위치이며, 그에 따른 보안 유지 및 관리를 위해 CA 계층을 결정할 때, OTG는 보안을 이유로 Microsoft 루트 CA를 오프라인 상태로 두고 네트워크에 연결하지 않았다. 또한, 루트 CA는 도메인에 참가하지 않기 때문에 엔터프라이즈 CA로서 설치할 수 없다.

PKI 서비스는 Microsoft Windows Server 2003 출시와 함께 크게 개선되어 OTG는 핵심 서버 인프라를 통합하고 인증서 발급 사례와 정책을 보다 효과적으로 관리할 수 있게 되었을 뿐만 아니라, 공개 루트 CA가 서명한 내부 하위 CA로부터 자체 인증서를 발급하기 위해 개별 타사 인증서를 구입하지 않게 되었다.

Windows 2000 Server에서 제공하는 PKI는 인증서 서비스를 통해 v.3, X.509 인증서[10]를 발급 및 관리하고, 자체 PKI를 구현할 수 있으며, IIS(Internet Information Services), Internet Explorer, Microsoft Outlook 메시징 및 공동 작업 클라이언트, Microsoft Outlook Express, EFS(Encrypting File System), IPSec 및 스마트카드 로그온 등의 공개키 사용 가능한 응용프로그램 및 서비스를 제공할 수 있다. 또한, Windows



[그림 2] Windows 2000 Server를 이용하는 Microsoft사의 PKI 설계 계층

2000 Server에서 제공하는 Active Directory 디렉터리 서비스를 이용하면 Active Directory와 계정 인증 메커니즘을 통해 계정 자격 증명에 따라 누가 어떤 종류의 인증서를 등록할 수 있는지를 제어하는 등록 기관의 역할을 효과적으로 수행할 수 있을 뿐만 아니라, Active Directory 컴퓨터 계정 개체에 대해 자동 인증서 등록을 구성하는 데 그룹 정책을 사용할 수 있고 PKI 그룹 정책을 사용하면 관리자는 루트 트러스트, EFS 데이터 복구 및 컴퓨터 계정의 자동 등록 등 도메인 내 PKI의 다양한 용도를 정의하고 제어할 수도 있다.

Windows 2000 Server 인증서 서비스는 FIPS (Federal Information Processing Standard) 140-1[8]의 Level-1 요구 사항을 준수하는 소프트웨어 암호화 서비스 공급자(CSP)를 제공하며, OTG는 CA의 개인키에 대해 보다 강력한 보호를 제공하기 위해 하드웨어 보안 모듈(HSM)을 각 CA 서버에 배포했고, 사용된 모듈은 FIPS 140-1, Level-2 및 3에 인증되었다.

3.2. 캐나다

3.2.1. 캐나다 국방부(DND, Department of National Defense) PKI

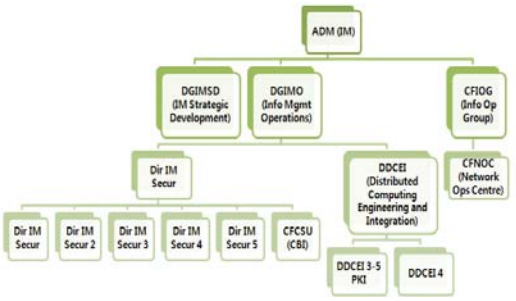
캐나다 국방부 DND와 캐나다군 CF(Canadian Forces)는 2002년부터 엔터프라이즈 PKI를 운영하고 있다[11]. 또한 이러한 PKI상에서 신뢰하고 사용할 수 있는 수많은 새로운 응용프로그램들이 계획되고 개발되고 있다. 국방부 PKI는 DND에서 1995년에 DITSec (Directorate of IT Security)의 추천에 따라 PKI Entrust사의 제품[12]을 도입했다. 이 PKI는 2000년에 SCEM(Secure Common Email) 프로젝트가 시작될 때까지 DND 연구소 환경에서 운영되었고, 그 후 DWAN(Defense Wide Area Network)나 기타 관련 도메인에 연결된 모든 데스크탑뿐만 아니라, 모든 DND 인력과 DND 메일 주소를 가진 CF 구성원이 사용할 수 있도록 배포되었다. 2002년 말에는 약 1,600만 달러의 비용으로 대략 60,000개의 PKI 스마트카드가 발행되었고, 2003년 초에는 SCEM 프로젝트의 운영이 DND/CF 생명 주기 관리 팀에게 인계되었다. DND PKI를 지원할 중요한 책임이 있는 DND/CF 생명 주기 관리 팀은 Dir IM Secur(Directorate of IM Security)와 DDCEI (Directorate of Distributed Common Engineering and

Integration)이다. Dir IM Secur는 PKI 정책과 PKI 운영에 대한 전체적인 책임을 가지고, DDCEI는 PKI 엔지니어링과 설계에 대한 책임을 가진다. 특히, Dir IM Secur 3은 지정된 도메인에 대한 책임을 가지며, Dir IM Secur 4는 분류된 도메인에 대한 책임을 가진다. 또한, DDCEI 3-5는 CA(Certificate Authority)에 대해서, DDCEI 4는 디렉터리 서비스에 대한 책임을 가진다. 그 구조는 다음 [그림 3]과 같다.

DND/CF 내에서 몇몇 비밀정보는 지정된 도메인 상에서 평문으로 전송된다. 이로 인해 많은 보안 사건들이 보고되었고, 지정된 도메인 내에서 신뢰하고 사용할 수 있는 PKI를 위해 새로운 많은 DND/CF 응용프로그램들이 설계 및 계획되고 있다. 이러한 응용프로그램들은 안전한 원격 접속을 가능하게 해주는 DVPNI(Defense Virtual Private Network Infrastructure)와 CFHIS (Canadian Forces Health Information System)를 포함한다. 또한 추가적인 주요 응용프로그램으로 MMHS (Military Message Handling System)와 함께 분류된 도메인을 위한 PKI가 계획되고 있다. 이는 최소 2가지의 DND PKI 시스템이 존재함을 의미한다. 하나는 SCEM과 운영되는 지정 도메인 PKI, 또 다른 하나는 분류 도메인에서 운영되는 MMHS PKI이다.

DND는 현재 PKI에 대해 엔터프라이즈 관리 방법을 적용하지 않고 있다. 그로 인해, 안전한 데이터 교환과 통신에 대한 인프라 지원에 있어 효율적이지 못하며, CRS(Chief Review Service)에 의해 여러 문제점들이 보고되었으며 이를 개선 중이다.

3.2.2. 캐나다 CIBC(Canadian Imperial Bank of Commerce) PKI



[그림 3] 캐나다 국방부 PKI 구조

북미 금융 산업의 리더인 CIBC는 전 세계 8백만 명 이상의 개인 뱅킹과 사업 고객에게 모든 범위의 제품과 서비스를 제공하고 있으며, 전화와 PC를 이용하는 전자 뱅킹 서비스를 제공하고 있다. 전통적으로 모든 CIBC 고객들은 VISA 카드, 은행 계좌, 지사 방문에 의한 과도 인출 방지, 메일에 의한 지원 요청, 또는 고객 지원 센터 연락과 같은 제품과 서비스를 신청한다. 모든 신청은 신청자에 의해 서명되어야 하기 때문에, 여러 절차를 거쳐야 한다. CIBC는 온라인에서 이런 절차들을 제공하여 편리성과 비용 절감을 위해, 빠르고 간편하게 처리하기 위한 방안을 수행하였다. 제품이나 서비스 신청에서 고객 인증과 부인 방지를 확인할 수 있도록 디지털 서명을 설계하고 구현하기 위해 CIBC는 VeriSign사의 인터넷 보안 솔루션을 선택했고[13], 2001년 2월에 CIBC는 온라인상에서 완벽하게 소액 거래 고객들에게 디지털 서명 응용프로그램 기능과 제품을 얻을 수 있는 기능을 제공하는 캐나다의 첫 번째 은행이 되었다.

디지털 인증서는 디지털 인증서의 등록과 발행을 위한 통합 솔루션인 VeriSign사의 MPKI(Managed Public Key Infrastructure) 서비스[14]에 의해 관리되고 있다. 이 솔루션은 웹 응용프로그램과 손쉽게 통합할 수 있고, CIBC가 자신의 웹 인터페이스에 디지털 인증서 기능을 이용할 수 있도록 해준다. 즉, 여러 제품과 통합이 쉽고 이용가능성과 확장성이 우수하다.

다음은 VeriSign사의 Managed PKI(Public Key Infrastructure) 서비스가 기반이 되는 VeriSign Trust Network 구조는 다음과 같은 모듈들로 구성된다.

- End-User Enrollment Pages : 최종 사용자 등록과 인증서 갱신과 같은 최종 사용자 서비스를 위한 지역화와 상표화 가능한 등록 페이지 제공
- Managed PKI Control Center : 완전한 자동화로 인증서 보증 승인, 폐기 승인, 일반 관리 기능과 같은 조직 내 인증서 관리 기능 제공
- CA Control Center : 기업이 인증서 콘텐츠 규칙과 관리 권한 부여와 같은 로컬 CA 정책을 수립
- Certificate Processing : 인증서 보증, 인증서 생명주기 수락, 프로토콜 지원, 온라인 인증서 상태 프로토콜인 OCSP(Online Certificate Status Protocol), 암호키 관리, 레코드 저장, 기타 핵심 기능과 같은 프리미엄 검증 서비스 포함
- Certificate Manager : 기업이 발행될 인증서의 형태(예: SSL, S/MIME, IPSec, 또는 VeriSign Trust

Gateway 인증서)를 선택하도록 해줌

- Key Management Services : 사용자 키 쌍의 생성, 백업과 복구에 최대의 보안을 제공. 하나의 응용프로그램 내에 키 쌍들을 구분하여 dual-key도 지원
- Enterprise Integration : 자동화된 인증서 보증과 기타 다른 관리 기능, 기업의 디렉터리와 데이터베이스에 대해 자동화된 인증서 포스팅(posting), 기업 웹 서버가 제공하는 인증서 폐기 정보에 대한 접근을 지원하기 위해 기업 데이터베이스에 대한 인터페이스를 제공
- Application Integration Toolkits : 상용 응용프로그램 사업자와 기업들이 PKI를 이용할 수 있는 응용 프로그램을 개발할 수 있도록 해줌

이 새로운 서비스는 대부분의 신청서가 24시간 내에 승인될 수 있도록 해주고 고객에 대해 알려진 정보에 따라 사전에 양식을 채움으로써 편리성과 처리속도를 향상시켜 준다. 또한 고객이 웹에서 자신의 신청서 상태를 확인할 수 있는 기능을 제공한다.

이 서비스는 부인 방지 서비스 제공한다. 모든 금융 시설처럼 CIBC도 증거로 사용할 수 있는 서명을 필요로 했다. 예를 들어, 고객이 콜 센터를 통해 제품을 요청했을 때, CIBC는 약관과 조건에 대한 구두 동의를 기록하는데, 온라인 거래를 위해 VeriSign사의 디지털 서명 서비스는 은행에 중요한 부인 방지 기능을 제공한다. 많은 거래가 온라인으로 옮겨짐에 따라, CIBC는 지사 근처에 살지 않는 고객에게도 서비스를 제공할 수 있고 추가로 신청서 처리에 대한 비용도 낮출 수 있다.

Ⅳ. 유럽 지역 PKI 구축 현황 분석

유럽에서는 공개키 기반 구조가 수년간 연구 되어 왔으며 그 결과로 효용성 및 안전성에 대한 신뢰가 검증되었고, eID, eGovernment, eHealth, ePassport 등 다양한 분야에 응용 되고 있다. 현재 유럽에서는 ETS (European Trusted Services)와 ICE(Internet- working public key Certification infrastructure for Europe) 프로젝트 중심으로 공개키 기반의 구조 및 서비스, 보안 기술에 대한 연구가 수행되고 있다.

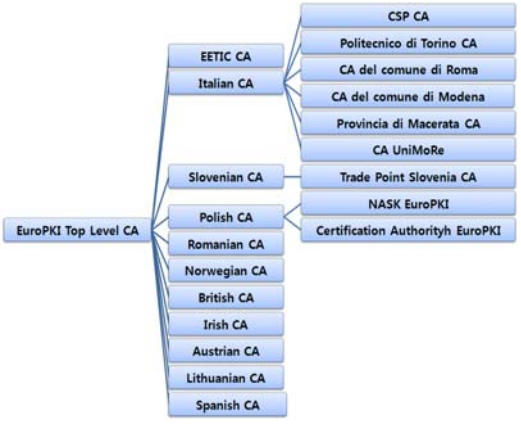
ETS는 1992년 정보시스템 보안 분야 관련 위원회의 주관으로 신뢰 할 수 있는 서비스(Trusted service)를 연구하면서 시작되었다. 프로젝트의 결과로 범 유럽적인 제3신뢰 기관 기반 구조를 확립 하였다.

ICE는 유럽의 13개국 17개 기관(Uninet, COST, Uni-C, SSE, UCL, FCCN, FCR, DFN, Polito, IJS, IAIK, Intrasoft, IOC)이 참여하여 유럽 국가 간 보안 서비스를 제공하기 위한 PKI 구축과 통합 보안 기술을 제공함으로써 다양한 응용 프로그램 개발을 위한 기술의 공유를 목적으로 시작되었다[15]. 첫 번째 프로젝트로 ICE-TEL이 시작되었으며, 산업체와 학술 연구에서 이용되는 인터넷상의 보안 문제를 해결하기 위한 솔루션 제공을 목적으로 하였다. 이 프로젝트의 결과로 유럽의 기본 인증 구조가 구축 되었으며, 덴마크의 UNI-C 인증기관이 최상위 인증기관이 되었다[15].

후속 프로젝트로 ICE-CAR(Interworking public key Certification infrastructure for Commerce, Administration and Research)은 ICE-TEL 프로젝트에서 개발된 인증기관 프로토타입 기관에서 다양한 보안 응용 기술의 데모를 위한 개발 목적을 갖는다. 이 프로젝트는 유럽에서 사용되는 상업적, 관리적 응용을 위한 안전한 인터넷 환경을 지원하기 위한 모든 기술적인 구성 요소를 제공하고, 개발 되는 보안 툴 셋의 가용성 확장, 상호 연동성 확보를 위한 것이다. 즉, 인터넷 환경에서 다양한 응용 서비스에서 동일한 보안 기능을 제공하기 위한 기술 개발을 주목적으로 한다.

이러한 ICE 사업을 통해 EuroPKI 인증 구조가 [그림 4]와 같이 구성 되었다[16].

이처럼, 현재 유럽 각국의 산업체, 학계, 정부가 협력하여 의료, 유통, 정보 조달, 우편 등 국가 기반 통신망을 포함하는 프로젝트를 수행하고 있으며 실질적이고 활용성 높은 공개키 기반의 보안 구조를 만들고 있다.



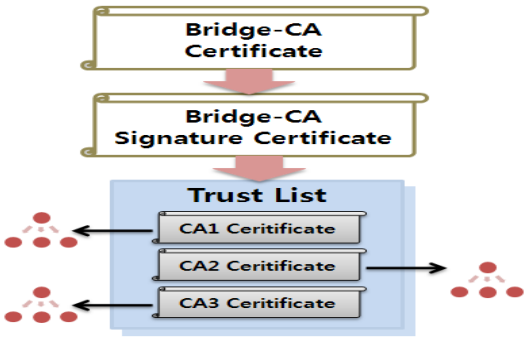
[그림 4] EuroPKI 계층 구조

90년대에 공개키 기반 구조의 주요핵심 기술 및 기반 기술 확보를 위한 연구가 수행, 완료되어 있는 상태이다. 현재 수행되고 있는 주요 프로젝트 내용은 이 전에 완료된 기술을 기반으로 유통분야, 의료분야, 조달분야 등 다양한 응용 서비스와의 연계성을 원활히 추진하기 위한 내용으로 추진하고 있다. 또한 IPv6 환경에 맞춰 자바를 기반으로 한 UMU-PKI 시스템 구축을 계획하고 있다[17].

유럽의 전자서명의 경우 PKI 운영이 나라마다 다르게 구현 되었다. 예로, 오스트리아와 벨기에에서는 등록과 인증이 공공 행정 기관에 의해 이루어지지만, 독일과 스웨덴에서는 사설 산업기관에 의해 등록과 인증이 이루어진다. 또한 현재 European Root-CA가 존재 하지 않아 Europe 국가 간 기술적 단계에서의 전자서명은 상호운영이 이루어지지 않고 있다. 따라서 현재 유럽 전자서명의 표준 설립하기 위해 여러 프로젝트가 진행 중이며, 여러 시스템이 개발되어 운영 중이다. 예로, 비공리 기관인 ETSI(European Telecommunications Standards Institute)에서는 전자 서명과 기반 구조에 대한 표준을 정하고 있다[18].

한편, 독일과 오스트리아에서는 European Bridge-CA를 설립하여 멤버간 PKI와 전자서명의 상호운영성을 제공하고 있다[18]. Bridge-CA의 기능은 중앙에서 기관들을 연결하여 확대된 서비스를 제공하는 것이다. 따라서 각각의 기관들은 서로 개별적인 협약 없이 같은 참여기관들과 통신이 가능하다.

위와 같이 범 유럽을 통합 운영하기 위한 유럽의 많은 국가에서 공동 참여 및 노력은 곧 한 국가에 국한되어 운영되어지는 지역 시스템에서 글로벌 유럽 시스템으로 그 영역이 확대 운영되어지고 있으며, 향후 전 세계로의 확대 서비스까지 구상하고 있다.



[그림 5] Bridge CA 인증 구조[19]

4.1. 벨기에

벨기에의 PKI 구조는 세 개의 Root CA를 갖는다. 하나는 Self-Singed CA 로 2048bits 의 인증서를 사용한다. 이 CA는 범국가적으로 실시되는 eID의 신뢰 체인의 시작점이 되며, 모든 eID Card에 내제 되어 있다. 다른 Root CA는 Root-Signed CA로 'GlobalSign'의 신뢰되는 상업적 CA와 연결 되어 있다. 이 CA의 인증서는 대부분의 웹브라우저에 내제 되어 정부의 행정관련 사이트를 인증해주는 역할을 한다. 다른 하나는 IDA-BC Gateway CA로 IDABC 프로젝트에 참여하는 국가의 행정 기관 간에 신뢰되는 인증서를 주고받기 위해 사용되는 CA이다. 이 CA의 인증서는 eID와 관련된 모든 응용 프로그램에 내제 되어 있다[20].

4.1.1. 벨기에의 eGovernment 구축

벨기에 정부는 벨기에의 국민과 산업, 행정을 관리하기 위해 eGovernment를 구축 하였다. eGovernment의 구축을 위해 범국가적인 PKI를 필요로 하였고, 그 PKI 구축을 위해 FedPKI 기관을 설립하여 연합된 PKI를 위한 프레임워크를 관리하게 되었다.

벨기에는 유럽에서 처음으로 범국가적으로 전자서명 기술을 이용한 eID (Electronic IDentity)를 모든 국민을 대상으로 시행하였다. eID 카드의 신뢰성을 위해 전체적인 시스템과 정보 관리는 정부에서 담당하며 실제 PKI와 eID 시스템 구현은 사설 산업 기관에서 담당하였다. eID의 기능으로는 온라인 tax return, 인증된 e-mail, 온라인 공문 요청, 인터넷 뱅킹, 전자 도서관 서비스 등을 제공하고 있다.

[그림 6] 벨기에 PKI 신뢰 구조[20]

전자서명과 관련한 PKI의 등록 및 인증 기능은 공공 행정 기관에서 담당하고 있으며, 사설 산업기관에서 인증서 발급 서비스 및 CA 기능을 제공하고 있다. 벨기에 PKI 시스템은 각 eID 카드가 벨기에 Root CA 인증서의 복사본과 함께 초기화 되어 “trusted source"로 사용된다. 즉, 각 사용자는 카드의 벨기에 Root CA 인증서를 통해서 ‘trusted chain’ 을 구성한다. 따라서 벨기에의 eID는 국가 전역의 PKI를 구성한다[18].

벨기에의 CA 계층 구조는 세 가지 단계로 이루어진다. 첫 번째 단계는 벨기에의 Root CA 이고, 두 번째 단계에 eID 운영에 관계된 CA가 포함되며, 세 번째 단계에 인증서 사용자(시민, eID 사용 서비스, eGovernment 개체)가 포함된다. CA는 다시 세 가지로 구분 될 수 있는데, Card Administration CA, Citizen CA, eGovernment CA로 구분된다. 이 세 개의 CA는 두 개의 Root CA(Self-Sign Belgium Root CA, RootSign Belgium Root CA)로부터 보호되며, 각각 CRL를 생성한다. Card Administration CA의 역할은 eID 카드 관리(인증서 및 정보 갱신, 키 생성/삭제, 디렉터리 관리, 인증서 생성/삭제)에 포함된 모든 인증 역할을 수행하는 것이다. eGovernment CA는 정부의 웹서버의 인증을 위한 것으로, 주로 전자서명과 관계된 역할을 수행한다. Citizen CA는 Citiizen 인증서의 삭제, 운영, 발급 등에 관한 모든 작업을 수행한다.

eID 카드 안에는 개인 정보가 내제 되어 있으며, 그 정보들은 전자서명을 통해 보호 되고 있다. eID 카드는 세 개의 각각 다른 RSA 개인키(private key)를 포함하며, 이 세 개의 키는 카드의 초기화 과정에서 생성되어 변경, 삭제되지 않는다. 두 개의 키 쌍은 개인 인증을 위한 것으로 벨기에 시민임을 인증하는 X.509v3 Authentication 인증서 키와 상위 전자서명을 위한 X.509v3 qualified 인증서 키 이다. 다른 하나의 키는 eID 카드를 인증 하는 키로 인증서를 위한 키가 아닌, RRN(National Register)와의 연결을 증명하기 위한 키로 사용된다. eID는 벨기에의 PKI 시스템을 바탕으로 eTax, eJustice, eAccess, eMove, eLogin, eCommerce, eBanking, eMail, eWork, eAdministration, eHealth 등의 서비스를 제공하고 있다[20].

4.2. 독일

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 수행한다. 또 전자서명 인증정책 결정이나 인증기관 허가 및 최상위인증기관(루트CA)의 역할을 수행하고 있다. 독일 정보보호원(BSI)은 인증기관에 대한 평가를 수행, 인증기관을 허가하고 전자서명 인증체계를 구축한다. 독일의 첫 번째 공인인증기관인 도이치텔레콤은 인증서 신청자에게 우편으로 전자서명 생성키와 수령증을 발송하고 신청자가 자필 서명하여 반송한 수령증의 서명과 인증서 신청서의 서명을 비교, 동일인임을 확인하는 신원 확인절차를 이용하고 있으며 전화국을 등록기관으로 이용하고 있다.

4.2.1. 독일의 전자서명 구축

독일의 전자서명법은 지난 1997년 6월에 제정돼 1997년 8월부터 시행에 들어갔다. 독일은 PKI 구조를 이용하여 전자서명, 은행, eID, 외국인 card, ePassport, eHealth 등의 서비스를 제공하고 있다.

독일의 전자서명은 독일 내에서 뿐만 아니라 유럽 전역에서 사용가능한 상호운영성을 목적으로 하고 있다. PKI를 기반으로 하는 솔루션을 필요로 하는 모든 IT 보안과 전자서명 응용서비스를 위한 trustcenter working group인 T7 e.V.가 있다. T7 e.V.에서는 PKI 응용서비스 제공자간의 상호운영성을 위한 표준(e.g., ISIS-MTT, Bridge-CA 등)을 설립하는 역할을 한다. 독일에 설립된 기관이지만, 독일 뿐만 아니라 오스트리아, 스웨덴, 유럽 외 국가들 간의 상호운영성을 추구한다. The European Bridge-CA는 독일 내에서 뿐만 아니라 유럽 내에서 상호운영성을 위한 표준이며, 전자서명과 인증서와 관련하여 안전한 eCommerce 솔루션을 향상시키는데 목적을 둔다. 구조는 참여국가간 TrustHub 구조를 갖으며, 실제 구현은 Trust List 방식으로 CA 와 Root CA의 인증서를 하나의 압축 파일로 만들어 압축 파일에 서명을 하고, 압축파일과 서명으로부터 PKCS#7 구조를 구성한다[18].

ISIS-MTT는 40개의 산업체와 기관의 참여로 전자서명, 암호화, 인증과 관련하여 CA 서비스와 클라이언트 응용프로그램 간의 확장된 상호운영성을 향상시키기 위

한 표준을 설립하기 위한 프로젝트이다. 독일의 전자서명이 ISIS-MTT 표준을 이용하여 구현되었으며, 실제 구현에서 현재 사용되고 있는 표준을 이용하므로 국제적인 호환성을 제공한다. ISIT-MTT의 인증 구조는 상이한 인증서간의 인증이 가능한 상호운영성이 가능한 구조를 가지고 있다. 이러한 ISIS-MTT의 상호운영성의 장점은 사용자에게 서비스와 제품의 선택권을 제공하고 비용을 절감이 가능하다는 것이다[21].

4.3. 에스토니아

유럽에서 ICT 와 e-government와 관련하여 가장 진보된 국가로 eIdentity 기반 인증과 전자서명 분야가 유럽 국가 중에서 가장 잘 설립되었다. 또한 공적인 전자서명이 사설 온라인 서비스와 연계되어 여러 서비스를 제공하고 있다[18].

4.3.1. 에스토니아의 eGovernment 구축[22]

에스토니아의 전자정부는 X-Road라는 안전한 데이터 전송 백본과 PKI, 정부의 데이터베이스와 정보 시스템의 기능적 계층 구조의 발전과 함께 시작되었다. X-Road 환경은 모든 종류의 XML형식 전자 문서들을 인터넷을 통해 안전하게 전송하도록 확장되어 있다. 이러한 기반 시설을 바탕으로 eGovernment 뿐만 아니라 여러 서비스들이 개발되었다.

X-Road는 에스토니아 정부의 정보들을 상호연결을 통해 접근을 하기 위해 설립된 프로젝트이다. X-Road 네트워크는 이러한 중요 정보들을 전송하기 위한 통신 백본 이다. 전체 네트워크의 모든 중앙 서버들(중앙 모니터링 서버, 인증 서버 등)이 X-Road center에 연결되어 위치하고 있어 X-Road center는 eGovernment 환경의 핵심 역할을 수행한다. 모든 정보 시스템은 X-Road adapter server(AS)를 통해 Security Server(SS)와 연결되어 있고, 각 정보 시스템들은 특별한 방화벽을 갖춘 Security Server(SS)을 통해 통신을 한다. 이러한 시스템의 장점은 개인 정보들을 실시간 관리가 가능하고, 사용자가 직접 자신의 정보를 점검 할 수 있으며, 다른 행정 기능과 상호 작용하여 여러 서비스 창출이 가능하며, 인터넷 트래픽을 통한 정보의 보안관리가 향상 되었다. 하지만, 이러한 정보관리 시스템이 항상 모든 상황에서 잘 운영되지 않으며, 기술의 발전과 법률 개정의 속도가 맞지 않고, 국민들이 항상 새로운 사양의 컴퓨터와 소프트웨어를 갖춰야 하는 것이 단점으로 드러났다.

4.3.2. 에스토니아의 eID 구축[18]

에스토니아의 eID 구축 프로젝트는 eGovernment 구축 프로젝트와 함께 이루어졌다. eID 프로젝트는 PKI와 전자서명에 초점이 맞춰져 있다. 에스토니아의 eID 시스템은 기업과 사용자를 위한 광범위한 상업적, 공공 서비스를 합리적으로 제공하기 위해 설립되었다. 또한, 물리적, 전자적 인증을 목적으로 한 신분증과 상거래의 목적을 갖는 신분증을 제공하기 위해 구축되었다.

eID 카드는 두 가지 PKI 기반의 전자 인증서를 내재하고 있다. 하나는 인증을 위한 것이고, 다른 하나는 전자 서명을 위한 것이다. 인증서는 X.509 v3 인증서를 기준으로 하고 있으며, 인증서와 관련한 두 쌍의 개인키를 카드 내에 저장하고 있다. 이 인증서는 사용에 있어서 어떠한 제약도 갖지 않는다. 따라서 eID 카드를 이용하여 다양한 서비스를 제공 받을 수 있다. 각 eID 카드에는 정부에서 할당한 이메일 주소가 인증서에 포함되어 있다. 그 이메일을 통하여 사용자와 정부의 행정기관과 통신을 할 수 있게 된다.

4.4. 핀란드

핀란드 정부는 몇몇 국가에서 WPKI를 기반으로 한 은행 서비스의 제공과 금융기관과 정부가 함께 모바일을 이용한 운영 서비스가 시작됨으로써 모바일을 통한 개인 정보관리와 인증 솔루션의 필요성을 느꼈다. 따라서 금융 서비스가 모바일 폰을 이용한 거래로 증가 하게 되고, 모바일 사용자가 늘어남에 따라 기존의 온라인 인증 솔루션의 비이동성을 해결하기 위해 eGovernment에 wireless PKI 기술을 기반으로 모바일환경에서 강력한 인증과 전자 서명을 제공하는 시스템을 구축하였다.

특히 eID Card를 이용하여 모바일 eBanking 서비스를 이용할 수 있도록 WPKI를 구축하였다.

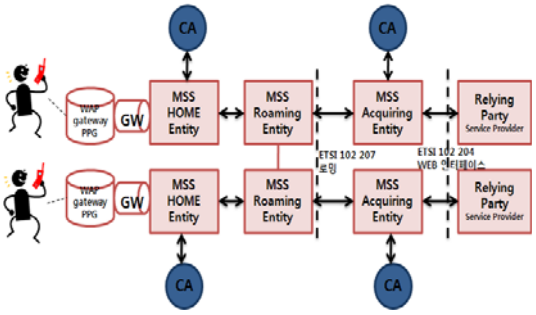
4.4.1. Mobile PKI를 적용한 eBanking 구축[23]

신용카드의 해킹이 늘어나고, e-Commerce이 차세대 서비스로 등장 하면서 모바일을 이용한 banking 서비스의 요구가 생겨났다. 또한 모바일 폰이 장소와 시간에

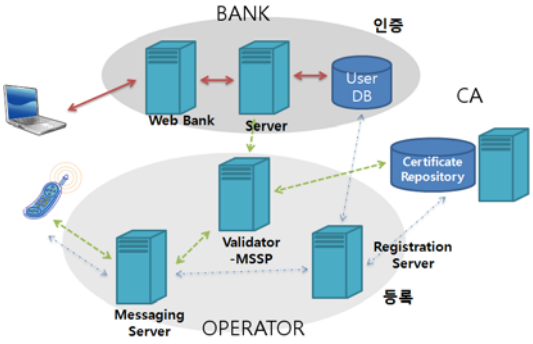
제약 없이 중요한 개인정보를 제공할 수 있고, 전자거래에서 무결성과 부인방지를 보장한다는 신뢰가 보장된 기기라는 인식이 기반이 되었다. 이러한 요구를 바탕으로 MPKI를 기반으로 하는 eBanking 서비스의 구축이 시작되었다. WPKI를 위한 eBanking의 요구사항은 강력한 보안의 제공과 보안의 비용이 적절하고, 기반 작업이 취소화 수준이며 사용자에게 이용이 쉬워야 한다는 점이었다.

Valimo사에서는 eID의 PIN 번호를 이용하여 모바일 폰과 연결하여 공공기관이나 사설기관에서의 식별을 통해 부인방지를 제공하였다. 또한 여러 CA로 얽힌 복잡한 PKI 시스템으로부터 투명성을 제공하여 사용하기 쉽게 구현되었으며, ETSI MSS 표준을 사용하여 상호 운영이 가능하도록 구현되었다. 이 시스템은 모바일 서명을 이용하는 사용자가 MSSP(mobile signature service provider)로부터 언제든지 장소에 제약 없이 모바일 전자서명 서비스를 사용 할 수 있도록 구축 되었다. 사용자는 WAP gateway를 통하여 MSS HOME 개체에 접속한 뒤 인증을 거쳐 MSS Roaming 개체를 통해 MSS Acquiring 개체를 거쳐 서비스를 제공받게 된다.

이 MPKI 솔루션의 기반 구조는 Valimo사의 validator로 모바일이나 wired 인터넷 환경 모두에서 전자서명 서비스를 제공하고, Registration server에서 WPKI 사용자 정보를 관리하며, Messaging server에서는 다양한 모바일 서명 생성 기기간의 통신을 가능하게 한다. ID server는 validator와 registration server와 통신하면서 사용자 인증 및 네트워크 접근과 온라인 어플리케이션과 관련하여 여러 인증 서비스를 제공한다. MSS-SDK는 ETSI 표준을 따르는 MSS 인터페이스를 제공하고 있다.



[그림 7] 모바일 PKI의 이동에 따른 전자서명 인증 구조[23]



[그림 8] 은행의 MPKI를 이용한 등록 및 인증[23]

사용자 식별은 CA에서 발급된 인증서를 바탕으로 하며 인증서는 네트워크상의 CA의 디렉터리 내에 저장되어 있다.

V. 결 론

인터넷 기술의 급속한 발전 및 진보와 인터넷의 높은 보급률에 따라 회사나 소비자들은 온라인상에서 정보를 교환하고 비즈니스 업무를 수행하고 있다. 개방형 환경을 가진 인터넷에서는 데이터에 대한 비인가 된 접근 등의 문제가 발생 가능하기 때문에 보안이 커다란 이슈가 되고 있다. 인증, 무결성, 비밀성, 부인방지의 중요한 정보 보안 기능을 가진 PKI는 일반적으로 이와 같은 상황에서 데이터 보호 목적을 성취하기 위한 가장 효율적인 방안으로 다양한 서비스에 사용되고 있다. 하지만, 인터넷 환경이 점점 진보하고, 서비스가 확대되면서 현재 PKI 인증 시스템의 효율성에 문제가 제기되고 있다. 이러한 변화에 대응하기 위해 인증체계를 발전시키고 고도화 할 수 있는 방안에 대한 연구가 필요하다. 본 논문에서 분석한 국외 PKI 구축 현황을 통해 인터넷 전자거래 환경의 진화를 분석할 수 있으며, 차세대 인증체계를 위한 요구사항을 수립할 수 있다. 즉, 인증 시스템의 고도화 연구에 본 논문의 국외 PKI 구축 현황 분석이 기반 연구로 활용될 수 있다.

참고문헌

[1] “Asia PKI Application Case Book 1st Edition”, http://www.japanpkiforum.jp/shiryou/APKI-F/PKI_App_CaseBook_1st.pdf, Nov, 2005

[2] “E-Tax Filling Service”, http://www.asia-pkiforum.org/WebSite/PKI/UpFile/File401.zip

[3] “Land Administration e-Service for Government Agencies”, http://www.asia-pkiforum.org/WebSite/PKI/UpFile/File401.zip

[4] “암호 및 전자서명 기술 : 1.3-3 주요국가의 PKI 구축 및 산업 동향”, http://www.patentmap.or.kr/pm/report/pop_pm_contents.asp?article_no=3979, Dec, 2002

[5] “The case of the CFCA digital certification applied in Shanghai Pudong Development Bank”, http://www.asia-pkiforum.org/WebSite/PKI/UpFile/File400.zip, Dec, 2006

[6] Tumbleweed, “US Department of Defense PKI Case Study”, http://www.tumbleweed.com/pdfs/Tumbleweed_DISA_Case_Study_0505.pdf, May, 2005.

[7] IETF(Internet Engineering Task Force), “RFC 2560”, http://www.ietf.org/rfc/rfc2560.txt, June, 1999.

[8] NIST(National Institute of Standards and Technology), “FIPS PUB 140-1”, http://csrc.nist.gov/publications/fips/fips1401.htm, January, 1994.

[9] Mcrosoft, “Deploying PKI Inside Microsoft”, http://www.microsoft.com/technet/itshowcase/content/deppkiin.mspx, February, 2005.

[10] IETF(Internet Engineering Task Force), “Public-Key Infrastructure (X.509) (pkix)”, http://www.ietf.org/html.charters/pkix-charter.html, April, 2007.

[11] Canada DND(Department of National Defence), “Review of the DND Public Key Infrastructure”, http://www.dnd.ca/crs/pdfs/pki_e.pdf, March, 2005.

[12] Entrust, http://www.entrust.com/pki/, 1994.

[13] Verisign, “Canadian Imperial Bank of Commerce (CIBC)”, http://www.verisign.com/static/005400.pdf, February, 2001.

[14] Verisign, “Managed Public Key Infrastructure”, http://www.verisign.com/static/005303.pdf, June, 2005.

[15] 특허청, 한국발명진흥회, ‘암호 및 전자서명기술’ 보고서, 2002

[16] EuroPKI, http://www.europki.org

[17] A.F. Gómez Skarmeta, G. Martinez Pérez, O. Cánovas Reverte and G. López Millán, PKI services for IPv6, IEEE Internet Comput. 7 (2003)

[18] Petra Hoepner, ‘Study PKI and Certificate Usage in Europe 2006’, Fraunhofer Institute FOKUS, October 31. 2006.

[10] Arno Fiedler, TeleTrusT Deutschland e.V. Projectmanager ISIS-MTT, ‘ISIS-MTT and Bridge CA : The Framework for the joint use of PKI- Applications’ http://www.japanpkiforum.jp/symposium/presentation/session_ 3/Ses3_Fiedler.pdf

[20] Danny De Cock, ‘Belgian eID Card Technicalies’, http://www.esat.kuleuven.ac.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf, 9 October 2006.

[21] ‘Common ISIS-MTT specifications for interoperable PKI applications’ http://www.teletrust.de/fileadmin/files/ISIS-MTT_Introduction_v1.1.pdf, 16 March 2004.

[22] Kalja, A., Reitsakas, A. and Saard, N., ‘eGovernment in Estonia: best practices’, Technology Management: A Unifying Discipline for Melting the Boundaries, pp. 500- 506, 31 July-4 Aug. 2005

[23] Valimo value in mobile , http://www.oasis-open.org/events/adoptionforum2006/slides/saharanta.ppt

<著者紹介>

이 성 진 (Junghyun Cho)
정회원
2007년 2월 : 성균관대학교 정보통신공학부 졸업
2007년 3월~현재 : 성균관대학교 휴대폰학과 석사과정
<관심분야> 정보보호, 모바일 통신 보안, 정보보호표준/평가

최 동 현 (Donghyun Choi)
정회원
2005년 8월 : 성균관대학교 정보통신공학부 공학사
2007년 2월 : 성균관대학교 컴퓨터공학과 석사
2007년 3월~현재 : 성균관대학교 일반대학원 휴대폰학과 박사과정 재학 중
<관심분야> 암호이론, 네트워크 보안, DRM, 모바일 보안

김 승 주 (Seungjoo Kim)
종신회원
1994년 2월-1999년 2월 : 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년 12월-2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2004년 3월-현재 : 성균관대학교 정보통신공학부 교수
2001년 1월-현재 : 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년 4월-현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년 7월-현재 : 디지털콘텐츠 유통협의체 보호기술워킹그룹 그룹장
<관심분야> 암호이론, 정보보호 표준, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won)
종신회원
1976년-1988년 : 성균관대학교 전자공학과(학사, 석사, 박사)
1978년-1980년 : 한국전자통신연구원 전임연구원
1985년-1986년 : 일본 동경공업대 객원연구원
1988년-2003년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장.
1996년-1998년 : 국무총리실 정보화추진위원회 자문위원
2002년-2003년 : 한국정보보호학회장
현재 : 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호 인증기술연구센터 센터장, IT보안성평가연구회 위원장
<관심분야> 암호이론, 정보이론, 정보보호