通信情報保護學會誌
第 10 券 第 1 號, 2000. 3

선진국의 PKI 관련 정부 지원 프로젝트 현황 분석

염 흥 열*

요 약

공개키 기반구조를 이용한 정보보호 서비스 개발이 활발히 추진되고 있다. 우리나라에서도 1999년 7월 전자서명법이 발효된 이후 민간부문 공개키 기반 구조를 이용한 다양한 인증기관이 구축되고 있고, 이는 전자상거래 시스템의 안전성을 크게 향상시킬 수 있을 것이다. 그러나 현재 정부 공개키 기반 구조 구축은 완료되지 않고 있다. 본 논문에서는 미국, 호주, 유럽, 그리고 캐나다에서 수행해왔던 공개키 기반 구조와 관련된 과제의 내용을 파악하고, 각 나라에서 구성된 PKI의 특성을 분석하며, 이를 바탕으로 국내 공개키 기반 구조를 위한 기술 표준안을 제시한다.

Ⅰ. 서 론

인터넷을 통한 전자상거래가 일반화되면서 거래 데이터의 신뢰성과 안전성을 확보하기 위한 암호 기술 특히 공개키 암호 기술의 중요성이 매우 증가하고 있다. 전자상거래 시스템은 공개키 암호를 이용한 공개키 기반 구조를 활용하여야 인증 및 기밀성 서비스를 제공받을 수 있다. 선진국에서는 전자상거래 시대에 대비하여 자국의 정보보호 산업의 경쟁우위를 확보하기 위하여 암호 기술의 발전과 공개키 기반 구조의 구축에 총력을 기울이고 있다. 본 연구에서는 선진국의 노력을 살펴보고 이를 바탕으로 우리의 대응 방안을 마련하기 위한 기초 자료를 제시하려 함에 있다.

IETF(Internet Engineering Task Force)에서는 인터넷을 위한 공개키 기반 구조에 대한 표준안을 마련하고 있고, 각 나라들마다 독자적인 형태의 공개키 기반 구조를 구축하고 있으며, 자국의 실정에 맞는 효율적인 공개키 기반구조를 구축하기 위하여 다양한 프로젝트가 진행 중에 있다[1][2]. 특히 미국과 캐나다 등의 선진국에서는 정부 차원의 PKI(Public Key Infrastructure)를 구축하고 있거나 완료하였고, 민간 분야의 PKI와의 상호 연동 방안을 활발히 연구하고 있다. 이를 위하여 정부, 민간 부문, 기타 기관들과 협력하여 얻어진 PKI 표준들이 자국내 뿐만 아니라 국제적으로 인정받을 수 있도록 정책 및 프레임워크를 개발하고 구현하기 위한 노력을 경주하고 있다. 공개키 기반구조(PKI)는 다음과 같은 하부 구조에 바탕을 두고 있다[3].

- 사용자에게 공개키 인증서를 발급하고 이를 관리하는 인증서 관리 기반 구조
- 인증서를 누구에게나 신뢰성 있게 공표하기 위한 디렉토리 기반 구조
- 사용자의 공개키를 인증해주는 인증기관간의 상호 인증 구조

본 논문에서는 선진국에서 추진하고 있는 공개키 기반 구조와 관련된 과제를 분석하고, 이를 바탕으로 각 국에서 고려 중인 공개키 기반 구조 관련 표준안을 살펴보며, 국내 공개키 기반 구조 관련 표준안을 제안한다. 이를 위하여 미국, 유럽, 호주 등의 주요 선진국에서 수행한 중요 정보보호 프로젝트를 분석하고, 각 선진국에서 구축된 PKI 구축 현황과 채택하고 있는 표준화 동향을 분석한다. 이를 바탕으로 국내 PKI 표준안을 도출한다[4].

* 순천향대학교 정보기술공학부

II. 선진국의 정부 지원 PKI 프로젝트와 PKI 구축 현황

1. 호주 정부 PKI 추진 프로젝트

호주 정부는 정부 서비스를 개선하고 부처간 거래를 효율적이고 안전하게 수행하기 위하여 정부 부처간, 기업과 공공 기관간에 거래를 안전하게 수행하기 위한 공개키 기반 구조를 개발하였다. 그리고 현재는 호주 정부 PKI를 고도화하기 위한 2차 프로젝트를 시작하였다.

Standards Australia는 "호주에서 공개키 인증 프레임워크(PKAF : Public Key Authentication Framework)를 실현하기 위한 전략" 이라는 보고서를 1996년 발표했다. 보고서에는 다음 사항을 권고하고 있다.

- PKAF를 위한 최상위 기관(PARRA: Policy and Root Registration Authority) 설립
- PKAF 체재 하에서 생성되고 이용되는 전자서명에 대해 법적인 상태를 부여하기 위한 법제정
- 사용자 책임성 정의

현재 호주 표준화 기관인 Standards Australia 서브위원회 IT/12/4/1에서는 PKAF를 위한 기술 표준을 준비하고 있다[5]. 연방정부는 정부기관인 OGIT(The office of government infortion technology)가 정부PKI(GPKI: Govern- ment Public Key Infrastructure) 구축을 위한 보고서를 준비토록 하였다. 정부 PKI 프로젝트를 GATEKEEPER라 한다[6].

GATEKEEPER 프로젝트는 NPKI 작업 그룹의 활동을 고려하고 있다. 호주 PKI는 그림 1에서 알 수 있듯이 크게 3부분으로 나누어 져서 추진된다. OGIT 주관하의 GATEKEEPER 프로젝트는 정부를 위한 PKI이며, NOIE의 NPKI 작업 그룹에서는 PKAF의 최상위 기관인 PARRA 구축에 관련된 문제들을 분석하며, Standard Australia는 호주 표준 기관으로 PKAF에 관련된 기술 표준을 추진 중에 있다[7].

Gatekeeper 프로젝트에서는 정부 기관이 공개키 기술을 이용하는데 필요한 다양한 메커니즘을 제공하고, 호환성 있는 동작을 가능케 하며, 사용자가 다양한 서비스 제공자를 선택할 수 있게 하며, 정부의 활동을 관리하기 위한 운영 메커니즘을 제공하는데 그 목적이 있다. Gatekeeper 프로젝트를 요약하면 표 1과 같다. GATEKEEPER에서 수행된 주요 연구 결과는 표 2와 같다.

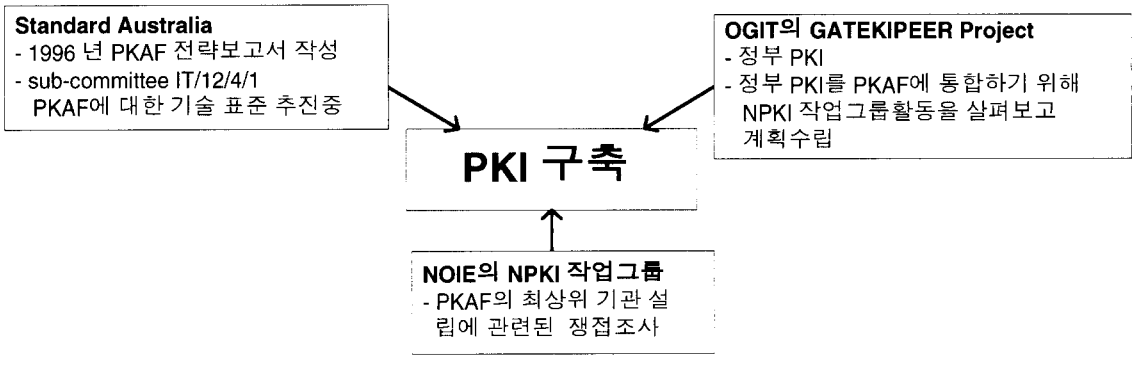

그림 1. 호주의 PKAF 추진 체계

표 1. GATEKEEPER 과제 요약

항 목	내 용			비 고
프로젝트 이름	GATEKEEPER			
연구기간	1997.10. ~ 1998.5.			
연구지원기관	호주정부			
예산	-			
과제 수행 주관 부서	OGIT(The office of government information technology)			정부부처중 한 부처
프로젝트 형태	한 개의 자문위원회와 3개의 작업 그룹으로 구성됨	자문위원회	- 위원장: OGIT의 Chief Government Information Officer - 위원: 국방부를 포함한 정부부처 대표	
		사업 및 사용자 요구사항 WG	- WG 의장: Health Insurance Committee의 Mark Mynott	
		보안 WG	- WG 의장: Attorney General's Department의 Steve Orlowski	
		기술 WG	- WG 의장: Department of Primary Industry and Energy의 Peter Justice	
GPKA 구성 일시	1998.5.6.			
GPKA 이사회 구성	The Officer for Government Online, The attorney-General's department, the australian tax office, The health insurance commission, the defence signals directorate, the national office for the information economy, the australian electrical and electronic manufacturers association, the australian information industry association and a privacy advocate			8개 부처의 대표들로 구성됨
GPKA 구성 일시	1998.5.6.			
프로젝트 총괄 책임자	OGIT의 The Information Management, Access and Policy 부서			
프로젝트 홈페이지	http://www.ogit.go.au/			

표 2. GATEKEEPER 연구 결과

주요 연구 항목	수행된 주요 결과	세부 내용	
최종 목적	정부 PKI 구성	정부 공개 키 기관(Government Public Key Authority) 구축	
WG의 역할	비즈니스 및 사용자 요구사항 WG	목적	공개키 기술을 사용하기 위한 일반 요구사항 제공
			- 범위 및 목적 - 비즈니스 시나리오 개발 - 비즈니스 요구 분석 - 프라이버시, 감사 - 기능 요구사항
	보안 WG	목적	- 보안 표준 제공 - 인가를 위하여 보안 표준이 평가되는 방법 제공 - 보안 조치와 위험 관리 조치를 확인
		주요 업무	- 보안 표준 권고 - 표준 평가 방법 권고 - 개인 인증 절차 권고 - 이용되어야 하는 표준 확인 - 보안 타켓 확인 - PKT 실현을 위한 기술적 측면 확인 - 보안 인가를 요구하는 PKT 실현 측면에서 권고안 조사 - 관련 표준안 확인 및 이용 가능성 조사 - 인증서의 다양한 등급 확인
	기술 WG	목적	- PKT 실현을 위한 기술 표준 확인 - 가술 표준 평가 방법 - 각 WG 지원
		주요 업무	- PKT 실현을 위한 기술적 측면 검토 - 기술 표준 확인 - 고려중인 기술의 비용, 유용 가능성, 복잡도 검토 - 디렉토리 서비스로의 접근 방법 제시 - 인가를 위한 표준 평가 방법 제시

표 2. GATEKEEPER 연구 결과(계속)

보고서 주요 내용	프로젝트 개요	- OGIT 역할, GATEKEEPER 프로젝트 구성, 작업반 역할 및 임무 - 주요 문제
	프라이버시 및 공정한 정보처리	- 프라이버시 관점, 법 및 정책 선언
	동작 개요	- GPKI 조직 및 구조 - 구성 개체들(CA, 사용자, RA), 키복구, 데이터 복구, 인증기관
	기본 PKT 과정의 설명	- 공개키를 얻는 사용자 과정 - 인증서를 발행하기 위한 인증기관 과정 - 인증서를 취소하는 과정, 인증과정 - 키교환 과정, PKT로 응용을 실현하는 기관들
	기관 요구사항	- 13가지 기관 요구사항: 즉시성
	정부 공개키 기관	- GPKA구성 . 의장: 위원회에서 선출되는 정부 기관 대표(초대: OGIT) . 정부기관 대표들 . 2명의 민간기관 대표
	ICA 기능	- 정부 운영 ICA(Intermediate Certification Authority) - 상용 ICA, 루트 인증기관 - ICA 기능 . 정책, 서비스, 인가
	OCA 기능	- ICA 소속 OCA(Organization Certification Authority) - 기관 소속 OCA, 산업체 소속 OCA - OCA 동작 . 정책, 서비스, 인가
	ORA 기능	- ORA(Organization Registration Authorities) 기능
	보안	- 암호 알고리듬, 키 생성, 관리, 전달, 사용자, 인증기관 - 카쌍의 생성 장소, 신원확인, 물리적, 개인적, 관리적 보안 - 인가
	기술	- 복지부 요구사항, PKT(Public Key Technology) 기술 표준 - 개인키 저장을 위한 토큰의 유형 - 인증서, 디렉토리 서비스, 다양한 서비스: 공증, 타임스탬프
	인가	- 인가를 요구하는 개체: ICA, CA, RA - 구성 요소 - 표준 - 동작 정책과 절차
	법적 문제	- 전자 인증의 법적 효과
	비즈니스 모델	- 정부 서비스 제공자 - 민간 서비스 제공자
	위험 관리	- 위험 관리 접근 방법 - 확인된 위험들 - 위협 - 관리 방법
	산업체 육성	- 목적 - 서비스 및 기술 제공 - 기술, 서비스
	다른 프로그램으로의 효과	- 법적 프레임워크 - 정책 프레임워크 . ORCD, APEC PKA 작업반

호주정부는 1999년 11월 30일 정부 PKI를 고도화하기 위한 Gatekeeper 2 프로젝트의 제안서를 공모했다. Gatekeeper 2에서는 정부 공개키 기반 구조의 도입 및 개발을 위한 정부의 전략을 전면 수정하려 하고 있다. 이는 1998년 5월의 Gatekeeper 문서를 전면적으로 변경하고 새로운 정책과 기술 개발 사항을 포함하려 한다.

2. 공개키 기반 구조 프로젝트(ETS)

본 절에서는 유럽 평의회에서 지원하는 공개키 기반 구조인 ETS에 대하여 살펴보고 프로젝트의상세 내역을 제시한다.

2.1 ETS(European Trusted Service)

ETS(European Trusted Services)는 3개의 과정으로 수행된 20개의 소 과제들로 수행되었다. 이 프로젝트는 1998년 말에 완료되었다. 이 프로젝트는 3개의 과정으로 구성되며, 1년 이하의 연구 기간을 가지며, 연구비도 3백만 ECU 이하이다[8].

이 과제에 대한 평가는 1998년 4월 독일, 프랑스, 스웨덴의 평가자에 의하여 수행되었다. 평가결과 추후에 수행되어야 할 과제는 표 4와 같다.

표 3. ETS 프로젝트 요약

항 목		내 용			비고
프로젝트 이름		ETS(European Trusted Service)			3단계 20과제로 구성
연구기간		1996. - 1998.(3년)	초기 준비 단계	1996.(6개월)	
			ETS 1	1997.1-1997.12.(1년)	
			ETS 2	1998.1.-1998.12.(1년)	
연구 과제 평가		1998.4.6.			
연구 과제 평가자		Franz Peter Heider(독일), Hans Nilsson(스웨덴), Denis Pinkas(프랑스)			
연구지원기관		European Commission(DG XIII)			
예산		-			
프로젝트 형태		20개의 개별 과제로 수행됨			
준비단계 과제		1과제	유럽 신뢰 서비스		5개 소과제
		2과제	TTP와 디지털 서명과 관련된 법적 제도적 문제		
		3과제	TTP에서 이름과 키를 사용하기 위한 가이드라인		
		4과제	ETS를 위한 표준화 문제		
		5과제	생물학적 기술의 검토와 평가		
ETS 1	1과제	유럽 TTP의 운영적 구조적 측면 (OPARATE: Operatioanal and architectural aspects of TTPs Europe)			
	2과제	EUROTRUST			
	3과제	개방형 디지털 서명 인증 구조 (OSCAR:Open digital certification architecture)			
	4과제	안전한 정보시스템의 키 복구 (KRISIS:key recovery in secure information system)			
	5과제	MANDATE II (Managing and Administrating Negotiable Documents and Testing them Electronically)			
	6과제	디지털 서명된 전자문서의 법적 효력 (AEQUITAS: The admission of evidence in trials of penal character of elecronic document signed digitally)			
	7과제	유럽 보건 서비스를 위한 TTP 서비스 (EUROMED: TTP service for health care in Europe)			
	8과제	TTP를 사용한 키관리 시스템 (EAGLE(Key management system for european users using TTPs)			

표 3. ETS 프로젝트 요약(계속)

ETS 2	1과제	유럽 상호 영역 PKI 구조 (KEYSTONE: European cross domain PJI architecture)
	2과제	사용자 신뢰와 ETS 인정을 위한 서비스 평가 정의 (SEDUCER: Service evaluation definition for user confidence and ETS recognition)
	3과제	신뢰 서비스 제공을 위한 책임과 증거의 법적 문제 (LEGAL: Legal issues of evidence and liability in the provision of trusted services)
	4과제	유럽 신뢰 서비스의 비용 모델 (COMETS: Cost model for the european trust model)
	5과제	신뢰 서비스의 비즈니스 환경 정의 (BESTS: Bisiness environment study for the trusted services)
	6과제	타임스템핑을 갖는 공개키 기반 구조 (PKITS: Public Key Infrastructure with time stamping)
	7과제	새 기술의 평가 및 ETS와 WWW간의 상호 효과 (TRUSTWEB: Assessment of new technologies and mutual impact of ETS and WWW)

표 4. 추후 수행 과제

추후 연구 항목	주요 내용	비고
부인봉쇄	- 속성 인증서의 지원: 인증서에 속성을 넣는 방안	
	- 다중 서명 지원: 지원 방법 강구	
	- 전자서명 정책: 정책의 일관전적이고 유일한 참조의 필요성 대두	
	- 전자서명문 포맷 표준화	
	- 전자서명문의 추후 타당성 확인 방법	
등록, 취소, 명명	- 초기 등록 방법: ITEF 초기 등록 방법의 보완책 요구	
	- 대규모/규모가 변경가능한 인증서 취소 방법	
	- 명명법 및 신분확인법: 조직의 이름, 개인의 이름	
상호 인증 및 경로 검증	- 인증기관의 상호 인증서와 명명법	
	- 인증 경로 검증	
	- 믿음 근원점 관리	
개인키와 인증서를 저장하기 위한 스마트카드의 활용	- 개인키와 인증서를 스마트 카드에 보관하는 방법: PKCS #15가 대안일 수 있음	
법적 및 규제적 문제	- 인증 서비스 제공자나 타임스탬프서비스 제공자를 위한 통일된 인가 및 인증 기법	
	- 전자문서: 법적인 관점에서 전자문서의 정의 필요	
	- 유럽 회원국 간의 강한 암호의 사용시 문제점 분석 . 암호 통신에 대한 각 나라의 입장 분석 . 제재하고 있는 나라와 비 제재 국가간의 암호 통신의 필요성	

3. 공개키 기반 구조 프로젝트(ICE)

본 절에서는 유럽 평의회 지원 공개키 기반 구조인 ICE 프로젝트의 상세 내용을 기술한다.

개선이 요구되는 분야로 인증서 자체 분야, 인증 관련 초기 등록 문제, 상호 인증 문제, 그리고 법/제도적 문제 등을 제시하고 있다.

3.1 ICE(Internetworking Public Key Certification Infrastructure for Europe)

ICE-TEL의 목적은 산업체와 학술 연구에서 이용되는 인터넷상의 보안 문제에 대한 해답을 구하기 위한 연구 개발 과제(계약번호:RE1005)이다[9]. 이 과제는 1996년 12월 1일에 시작되어, 1998년 2월 28일에 완료되었다.

이 과제는 유럽 평의회(Telematics Applications Programme의 Telematics Research Sector)의 재정 지원으로 수행됐다.

이 과제는 독일 GMD에 의하여 총괄되었다. 이 프로젝트는 다음과 같은 연구 배경을 갖는다.

- 보안 구조를 제공하고 다양한 플랫폼에서 공개키 기반 구조로의 사용자의 이용을 가능케 하기 위해 요구되는 툴을 개발하고 설치한다.
- 공개키 기반 보안 서비스를 실제 응용 서비스에 통합시키는 보안 툴킷을 개발하고 설치한다.
- 인증 서비스의 사용을 가능케 하는 보안 능력을 갖는 사용자 서비스를 개발하고 설치한다.
- 보안 서비스에 대한 다양한 응용으로의 통합을 지원한다.

표 5. ICE-TEL 과제 요약

항목	내용	비고
프로젝트 이름	ICE-TEL(Internetworking Public Key Infrastructure for Europe)	
연구기간	1996.12.1. - 1998.2.28.(27개월)	
연구지원기관	European Commission(Telematics for Research)	
예산	총괄예산액: 3,261,500 ECU(European Currency Unit)	
	European Commission 지원액: 1,699,500 ECU	
프로젝트 형태	독일 GMD를 중심으로한 12개국 17개 기관	
주요 프로젝트 참여 기관 및 책임자	GMD(독일 담스타트)	12 개국 17 기관
	University College London(영국 런던)	
	Isode Ltd.(영국 리딩몬드)	
	COST AB(스웨덴 스톡홀롬)	
	SSE(Soft and System Engineering) Ltd.(아일랜드 더블린)	
	Intrasoft(그리스 아테네)	
	Technical Univ. Graz(오스트리아 그라츠)	
	Politecnico di Torino(이태리 토리노)	
	University Salford(영국 맨체스타)	
	Uni-C(덴마크 코펜하겐)	
	Uninett SA(노르웨이 트로드하임)	
	INSEC(포르투칼 리스본)	
	FCCN(포르투칼 바르셀로나)	
	FCR(스페인)	
	University politecnica de catalunya(스페인)	
	Institute Josef Stefan(슬로베니아)	
	Institute of Cybernetics(에스토니아)	
프로젝트 총괄 책임자	이름: Wolfgang Schnider	
	회사: GMD	
	주소: Dolivo Street 15, 64293, Darmstadt, Germany	
	나라: 독일	
	schneider@gmd.de	
프로젝트 홈페이지	http://www.darmstadt.gmd.de/ice-tel/	

- 안전한 테스트베드를 제공한다.

툴의 사용 가능성과 적용 가능성을 위한 타당성 확인이 세 가지 응용 분야에서 시험되었다. 이 선택된 세 가지 영역은 다음과 같다.

- EU 지원 정보통신망 내에서 조정된 토리노 지역에서 문서의 전자적 요구와 전달간의 안전한 통신을 위한 응용
- 컴퓨터 비상 대응팀(Computer Emergency Response Teams: CERTs)과 다른 분산 망 지원 그룹간의 안전한 통신
- 영국 연구 기관간의 보안 기능 탑재형 디렉토리 서비스의 제공

프로젝트의 초기에 인증 구조를 설정하고 난 후, 프로젝트 II 인증 구조가 현재 구축되었다. 최상위 레벨 인증기관은 덴마크에 있는 UNI-C 인증기관이다.

표 6. ICE-TEL 연구 결과

주요 연구 항목	수행된 주요 결과	세부 내용
일반 규격	공개키 기반 구조 및 규격	- 믿음의 ICE-TEL 모델 - 보안 정책 - 인증기관 동작 모드 및 가이드라인 . 온라인 인증기관/오프라인 인증기관 - 인증서 관리 프로토콜
	안전한 WWW 규격	- WWW 컨소시엄에 디지털 서명 이니셔티브 참여 - Basic Coperation Protocol(WWW 보안)
	국가 보안 규제	- 사용되는 보안 기술과 관련된 각국의 규제
	안전한 회의를 위한 ICE-TEL PKI 사용	- 공개키 인증 및 암호를 부가하는 방법 - SAP 패킷의 규격
	방화벽 기술	- 인터넷 보안의 소개 - TCP/IP 5 계층 모델을 이용 - 망보안 정책의 특징과 역할 분석 - 방화벽의 기능 - VPN 의 실현 방안
보안 기술의 개발	보안 툴킷	- 범용 보안 툴킷(SECUDE 5.1), 자바 보안 확장 및 SSL 3.0 - COST(일반화된 보안 툴킷) 보안 기술 - Isode 디렉토리 및 보안 기술, UCL로부터 OSISEC 툴킷
	인증기관 툴	- SSE 제공 CA 툴 . 웹서버로의 역할-기반 액세스 제어 . 128-비트 기밀성 서비스, 벤더 독립 툴 . 웹 인터페이스를 위한 관리, 고객과 서버간의 상호 인증 . 2048-비트 RSA 알고리듬, 내용 무결성, 보안 감사 . 웹서버상의 CGI 지원 - 사용자 투명 인증 . 패스워드 기반 인증, 공개키 기반 인증 - GMD 제공 CA 툴(SECUDE-5.1) . X.509v3 인증서, X.509v2 CRL - COST가 개발한 http 기반 인증 프로토콜
	안전한 문서 툴	- MS Exchange/Outlook를 위한 S/MIME와 PEM 프러그인 - Eudora를 위한 PEM, Eudora를 위한 S/MIME - Exmh를 위한 PEM 통합, UNIX를 위한 PEM GUI - 안전한 회의를 위한 사용자 에이전트
	X.500 Guardian DSA	-인증서와 CRL 보관
	안전한 DSA	- Isoda의 액세스 제어 관리 툴 . 직접 그래픽 관리 - LDAP v3

ICE-TEL 과제를 요약하면 위의 표 5와 같다.

ICE-TEL에서 수행된 주요 연구 내용은 표 6과 같다.

4. 미국 정부 공개키 기반 구조 프로젝트

FPKI(Federal Public Key Infrastructure)는 미국 연방 정부를 위한 공개키 기반 구조이다. 이는 3개의 작업반과 여러 산업체를 중심으로 추진되고 있다. 클린턴 대통령은 「1993년 3월 3일 효율적인 정부와 저비용의 정부를 창설(to create government that works better and cost less)」을 목적으로 부통령 앨 고어를 의장으로 하는 NPR(National Performance Review) 이라는 TFT(Task Force Team)을 결성하였다[3][10]. 이것은 연방 정부의 경영 방법을 개혁하기 위한 클린턴-고어 행정부의 이니셔티브(Initiative)이다. "정보 기술을 통한 리엔지니어링(Re-engineering Through Information Technology)"이라는 NPR의 보고서에서는 정부의 개혁을 위하여 정보기술을 이용해야 함을 강조했다. 이 보고서에서는 정보 기술을 획득하기 위해 정부가 수행해야 할 3 가지의 협의사항(agenda)이 요구되고, 총 13개의 이니셔티브들을 제안했다. 이의 내용을 살펴보면

- 정보 기술력 지도 강화
  - 정부사업에 정보기술을 통합하기 위하여 강한 지도력 제공
- 전자 정부 구축
  - 국가 규모의 통합적인 전자적 연금이체 구현
  - 정부정보와 서비스의 통합적 전자접근 개발
  - 국가적 법시행/공공 안전 네트워크 구축
  - 정부부처간의 세금보고, 지불처리를 제공
  - 국제간 무역 데이터 시스템 구축
  - National Environmental Data Index 생성
  - 정부규모의 전자메일을 계획하고 실증실험을 통하여 제공
- 전자정부확립에 필요한 메커니즘의 설정
  - 정부의 정보기반구조를 개선
  - 프라이버시와 보안을 보장하기 위한 시스템과 메커니즘을 개발
  - 정보기술획득의 방법을 개선
  - 혁신을 위한 동기 제공
  - 연방 피고용인에게 정보기술분야에 대한 훈련과 기술적 도움 제공

NPR은 이를 지원하기 위해 GITS(Government Information Technology Services)라는 작업 그룹을 구성했다. FPKI 개발을 총괄하고 있는 FPKI 운용위원회(FPKI Steering Committee)는 그림 2와 같이 미국 정부 조직 내에 존재한다. FPKI 운영위원회는 1993년 9월 클린턴 대통령에 의하여 주창된 NII(National Information Infrastructure)을 추진하기 위하여 부통령 산하에 IITF(Information Infrastructure Task Force) 팀을 결성했다[11]. NPR은 IITF와 협력하여 정보 기술과 관련된 NPR의 13개 이니셔티브를 구현할 수 있는 권한을 GITS 작업그룹에게 주었다. GITS 작업 그룹과 IITF와의 관계는 그림 2와 같다. GITS 작업 그룹은 IITF 내에서 응용과 기술(CAT: Application and Technology) 산하에 소속되어 있다.

GITS 작업 그룹에는 연방 정부의 여러 정부 기관들과 관련이 있는 정부 기관들로 구성되어 있다. GITS의 활동은 다음과 같다[12].

- 미국내의 전자정부 형성에 필수 조건인 전자거래, 전자문서교환, 보안기능 등과 같은 기술 요소 개발을 촉진하고 유도.
- 미정부의 디지털 문서 보관센터 운영과 민간용 네트워크의 운용정책 수립.
- 미정부가 정보자원을 활용하고 전자정부의 구현에 필요한 소프트웨어를 이용하여 효율적인 IT 기반구조를 개발 구축하도록 활동

FPKI 운영위원회는 그림 3과 같이 산하에 3개의 작업 그룹을 두고 있다. 각 작업 그룹은 기술적, 사업적, 그리고 법/정책적 문제를 다루고 있다.

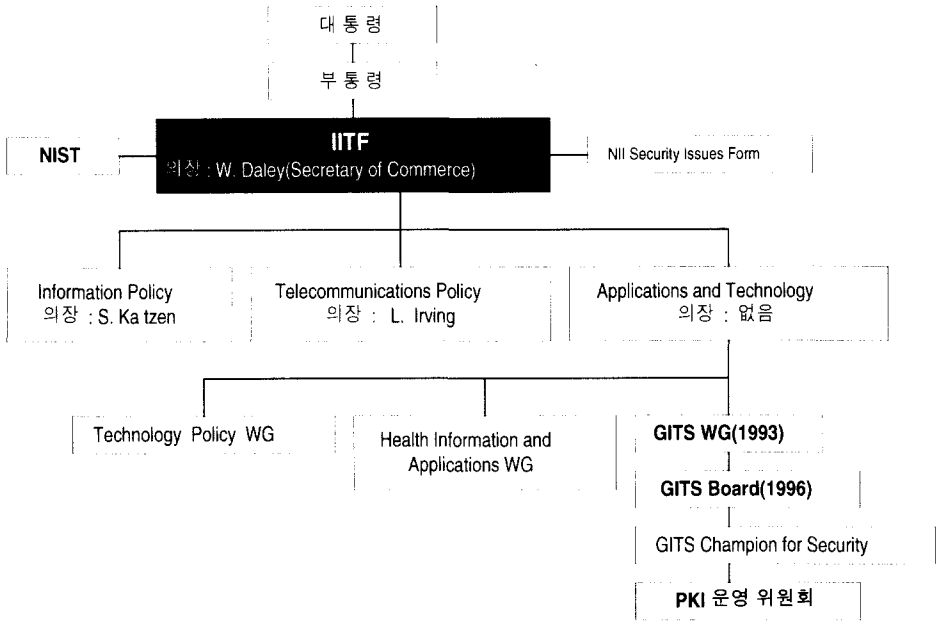

그림 2. IITF와 GITS와 FPKI 운영위원회의 관계도

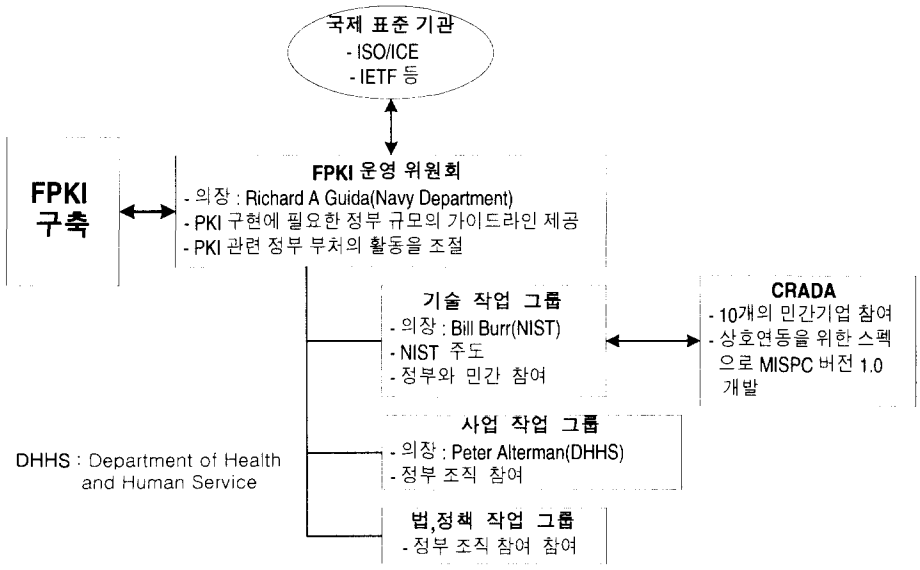

그림 3. FPKI 구축 체계

5. 캐나다 정부의 공개키 기반 구조(GoC PKI)

본 절은 캐나다 정부 PKI 구축을 위한 프로젝트의 상세 내용을 제시한다[13][14]. GoCPKI의 주요 특징은 다음과 같이 요약될 수 있다.

5.1 배 경

캐나다는 자국의 정보 고속도로(information highway)를 구축하려 했고, 정보 고속도로를 통한 트랜잭션의 프라이버시와 보안의 중요성을 인식하게 되었다. 이를 위하여 정보 고속도로 자문 위원회(Information Highway Advisory Council)는 프라이버시와 보안 문제를 연구했고, 1995년 9월에 다음과 같은 권고안을 마련했다.

- o 연방 정부와 주 정부는 정부, 민간 부문, 그리고 국제 무역에서 전자상거래를 저해하는 법적 규제와 보안 관련 문제들을 협력하여 수행한다.
- o 캐나다 정부(GoC: Government of Canada)는 상호 수용할 수 있는 보안 표준을 개발하기 위하여 주 정부, 민간 부문, 기타 기관들과 협력하고 이러한 표준들이 캐나다뿐만 아니라 국제적으로도 인정받도록 한다.
- o 정부, 민간 부문의 서비스 제공자, 사용자들, 프라이버시 옹호자, 정보 고속도로에 관련된 사람들은 캐나다 정보 고속도로를 지원하는 보안 기반 구조의 정책 및 프래임워크를 개발하고 구현하는 데 협력해야 한다.

정보 고속도로 자문 위원회는 다음과 같은 사항들을 캐나다 정부에 요청했다.

- o 캐나다 정부는 GoCPKI를 구축하기 위하여 민간 부문의 능력을 활용한다.
- o 캐나다 정부는 국가적·국제적 기관들과 상호 연동성을 보장하기 위하여 호환성 있는 PKI 정책들과 상호 인증실행준칙을 개발하기 위해 계속해서 민간 부문과 협력한다.

캐나다 정부(GoC)는 6개 부처가 참여하는 PKI 프로젝트를 1995년 12월 착수하였다. 이 프로젝트는 캐나다 국민을 대상으로 하며 1998년까지 수행되었다.

정부는 GocPKI를 통해 국민들에게 보다 효율적인 서비스를 제공하며, 안전한 전자상거래를 가능하게 하고, 연방 정부 비즈니스를 위한 정보의 기밀성과 프라이버시를 보호받게 될 것이다.

5.2 GoC PKI 추진 체계

GoC PKI 구축은 그림 3과 같은 체계로 추진된다. Task force는 연방 정부의 각 부처들로 구성된 특별한 팀으로 Treasury Board의 Chief Information Officer 산하에 있다. 임무는 GoC PKI 구축을 전반적으로 지원하고 조정한다. 이 팀은 1998년 4월 1일에서 2000년 3월 31일까지 2년간 운영된다. PKI Task Force는 다음과 같은 업무를 수행한다.

- PKI에 대한 공통적인 관리 구조와 정책 프레임워크 개발
- PKI에 관련된 법·정책·운영적인 문제 해결
- PKI에 대한 표준 개발 지원
- 구현상의 문제를 해결하고 PKI 기능을 테스트하고 데모하기 위해 선택된 테스트 프로젝트를 분석 및 지원
- 정부 사업 응용에 PKI 수용에 대한 인식 제고 및 증진
- PKI 구현시 각 부처 지원
- 정부 또는 다른 조직과의 상호 연동성에 대한 상호 인증 협정 개발

SILC(Senior Interdepartmental Lead Committee)는 PKI(Policy Management Authority) 구현을 감독하고 증진하며, PMA로 가이드라인을 제공한다. PMA는 GoC PKI 정책을 총괄하는 범 부처 위원회이다. CSE(Communications Security Establishment)는 캐나다 정부 기관들에게 정보기술 보안 솔루션을 제공하는 연방 정부 기관으로 PKI 전반의 기술적인 부분을 담당한다. 또는 CSE는 루트 CA를 운영, 관리, 유지할 것이다. 또한 정보기술 보안 관점에서 연방 정부 부처를 지원하고 가이드라인을 제공한다. GoC PKI에서 지원될 IT 응용에 대한 요구조건들을 자문할 것이다. 각 WG(Working Gorups)는 각 부처의 전문가들로 구성되며 GoC PKI에 대한 표준과 권고안을 개발한다.

표 7. GoCPKI 구축 요약

항목	내용	비고
프로젝트 이름	GoCPKI(Government of Canada Public Key Infrastructure)	
기간	1993. - 현재	
프로젝트 지원기관	캐나다 정부	
프로젝트 형태	주정부와 연방 정부가 협력하여 구축	
Task force	연방 정부의 각 부처들로 구성된 특별한 팀으로 Treasury Board의 Chief Information Officer 산하에 위치	
PMA	Treasury Board Secretariat가 의장, 범부처 위원회 - GoC PKI 운영에 대한 정책 개발을 감독 - GoC PKI와 외부 PKI간의 상호 인증 협약과 정책 매핑(policy mapping)을 승인정부 기관의 대표가 주도하고 민간 산업체들(10개)이 참여	
PMA 참여 부처	○ 국가재정위원회사무국(Treasury Board Secretariat) ○ 부처 및 기관 - Citizenship and Immigration Canada(CIC) - Communications Security Establishment(CSE) - Foreign Affairs and International Trade(DFAIT) - Government Telecommunications and Information Services(GTIS) - Health Canada(HC) - National Defence(DND) - Revenue Canada(RC) - Royal Canadian Mounted Police(RCMP)	9개 정부 기관
홈페이지	http://www.cse.dnd.ca/cse/english/gov.html	

6. 각 나라별 PKI 특징 및 표준안 비교

표 8은 현재 각 국에서 구축 중인 PKI 특징들을 비교한 것이다.

표 8. 각국의 PKI 특징 비교

	미국(FPKI)	캐나다 (GoCPKI)	유럽(ICE-TEL)	호주(GPKAF)
PKI 구조	수직 계층 구조와 네트워크형을 혼합시킨 하이브리드 구조	계층 구조	PEM과 PGP의 혼합형 신뢰 구조	계층 구조
최상위 인증 기관	PAA	PMA	ICE-TEL	AUS PARRA
주관 기관	NIST	CSE	EU	OGIT
제품	각 부처에 맞는 제품 선택 가능	Entrust사의 제품군	COST, ICR, OSISEC, SECUDE, SESAME 등	-

캐나다의 CSE는 정부 기관들에게 정보기술 보안 솔루션을 제공하는 연방 정부 기관으로 PKI 전반적인 기술부분을 담당하는 부서로 캐나다 PKI 추진체계의 핵심적인 역할을 수행한다. 미국, 캐나다, 호주의 PKI는 국민들과 정부 기관들간에 보다 안전하고 빠른 서비스를 제공하고자 하는 목적에서 진행되고 있다. 유럽의 경우는 유럽의 공동체 국가들간의 보안 서비스를 제공한다는 취지로 진행되고 있다. 또한, 각 나라들은 정부와 비정부 선진국의 PKI의 계층 구조의 비교는 표 10과 같다.

PKI, 자국과 외국의 PKI를 위해 상호 연동 모델을 제시하고 있다. 미국의 경우는 Bridge CA를 두어 정부와 정부외 PKI와의 상호 연동 모델을 제시하고 있으며, 상업적인 목적을 위해 최소 상호 연동모델(MISPC)을 개발하고 있다.

표 9는 각 나라에서 채택하고 있는 핵심 보안 알고리듬을 비교한 것이다. 대부분의 나라들은 자국에 맞는 암호 알고리듬을 사용하고 있다. 한국 PKI는 한국형 표준 서명 알고리듬인 KCDSA를 사용하는 것을 우선한다.

표 9. 각 나라별 핵심 보안 알고리듬

분류	알고리듬	암호키 크기	국가
대칭키 암호	CAST	128 비트	캐나다
	DES	64 비트	캐나다, 미국(NIST), 호주, 유럽(ICE-TEL)
	IDEA	64 비트	유럽(ICE-TEL)
	Triple DES	112 비트	캐나다
	RC2	가변	캐나다
	RC4	가변	캐나다
	AES	128 비트	미국(NIST)
전자 서명/해쉬 알고리듬	RSA/MD5	512/1024 비트	캐나다, 미국, 호주, 유럽(ICE-TEL)
	RSA/SHA-1	512/1024 비트	캐나다, 미국(NIST), 유럽(ICE-TEL)
	DSA/SHA	512/1024 비트	캐나다, 미국
	EDDSA	512/1024 비트	미국(NIST)
	KCDSA	512/1024 비트	한국

표 10. PKI 계층 구조 비교

구분		FPKI(미국)	GoC PKI(캐나다)	PKAF(호주)	ICE-TEL(유럽)
인증기관	PAA	PAA	CCF	GPKA	ICE-TEL CA
	PCA	PCA	PCA	ICA	PCA
	CA	CA	CA	OCA	CA
	RA	ORA	LRA	ORA	RA

7. 국내 PKI 기술 규격

위의 선진 외국의 PKI 구축 분석 결과를 바탕으로 국내 PKI를 위한 관련 표준(안)을 인증서 규격, 암호 API 분야, 저장소 규격, 그리고 데이터 인코딩 부분으로 구분하여 제시한다.

표 11. 국내 PKI 표준(안)

규격 이름		규격 내용	관련 표준
인증서 및 CRL 규격		- 인증서 기본 및 확장 필드 - CRL 기본 및 확장 필드	- IETF RFC 2459(1999.1.) . X.509 Certificate and CRL Profile - ITU X.509: Certificate Profile - USA FPKI MISPC
인증서 관리		- 인증기관 초기화 - 최종 개체 초기화 - 인증서 발급 요청 - 키쌍 갱신 - 인증서 갱신 - 인증기관 키쌍 갱신 - 상호인증 요구 - 상호 인증서 갱신 - 인증서/CRL 공표 - 키쌍 복구	- IETF RFC 2459(1999.1.) . X.509 Certificate and CRL Profile - IETF RFC 2511(1999.3.) . Certificate Request Message Format . 인증서 발급 요청시 공개키를 전달하는 양식 . 템플릿 기반의 인증 요청 . PKCS#10 단점 보완 - PKCS#10: 인증서 발급 요청을 위한 양식 - USA FPKI MISPC
암호 API	암호 API	- 암호/서명/해쉬 - 암호키 생성	- GSS API(RFC 2510) - GCS API - Crypto API
	인증서 관리 API	- 인증서 생성 - 인증서 검증 . 기본 필드 검증 . 확장 필드 검증 - 인증 경로 검증	- RFC 2549: X.509 Certificate and CRL Profile - ITU X.509 - GSS API(RFC 2510) - GCS API - Crypto API
저장소 규격		- 인증서/CRL 공표 - 인증서CRL 검색	- RFC 2559(LDAPv2, 99.4.) . 인증서 조회 및 공표를 위한 프로토콜
데이터 인코딩		- 인증서/CRL 인코딩	- ITU X.680 . ASN.1-Specification of Basic Notation - ITU X.690 . ASN.1 Encoding Rules-Disinguished Encoding Rule)
타임스탬프 프로토콜		- 전자서명 발생 시점 확인	- IETF Draft 표준(1999.6.) . 데이터가 특정 시점에서 존재했다는 것을 증명 . TSA로의 요구의 형식 . 응답의 형식
온라인 인증서 상태 프로토콜		- 인증서 상태의 온라인 조회 기능	- IETF 2560(1999.6.) . CRL의 도움없이 인증서의 상태를 조회

Ⅲ. 결 론

본 논문에서는 미국, 유럽, 호주 등의 주요 선진국에서 추진하고 있는 프로젝트의 세부 내용을 살펴보고, 그 프로젝트 추진 결과로 얻어진 선진국의 공개키 기반 구조의 구축 현황과 PKI 표준화 동향을 제시하였다. 또한 이를 바탕으로 국내 PKI에서 채택해야할 관련 표준(안)을 제시하였다.

미국, 유럽, 호주, 캐나다 등의 선진국에서 지원되고 있는 정부 지원 프로젝트의 내용을 분석하기 위하여 호주의 공개키 기반 구조 구축을 위한 프로젝트, 유럽 평의회의 두 가지 PKI 관련 프로젝트, 그리고 미국과 캐나다의 PKI 관련 프로젝트 내용을 자세히 제시했다. 또한 프로젝트 수행 결과 구축된 각 국의 주요 PKI 구축 결과와 표준안 채택 현황을 제시하고, 이를 바탕으로 국내 PKI를 위한 표준(안)을 제시하였다. 본 논문의 결과는 정부 및 민간 부문 PKI 구축시 기초 자료로 활용될 수 있을 것이다.

참 고 문 헌

[1] IETF homepage, http://www.ietf.org/, 1999.

[2] 이만영, 김지홍, 송유진, 염흥열, 이임영, 류재철, 전자상거래 보안기술, 1999.8.

[3] 정보보호센터 홈페이지 연구자료들, http://www.kisa.or.kr/, 1999.

[4] Public-Key Infrastructure(X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html, 1998. 4

[5] Standards Australia, Strategies for the implementation of a public key authentication framework (PKAF) in Australia, 1996

[6] OGIT, GATEKEEPER: A strategy for public key technology use in the Government, http://www.ogit.gov.au/gatekeeper/index.html, 1998. 5.

[7] OGIT, http://www.ogit.gov.au/aboutOGIT/mission.html

[8] http://www.cordis.lu/infosec/src/ets.htm ETS 연구자료, 1998

[9] ICE-TEL, "Interworking Public Key Certification Infrastructure for Europe", http://www.dramstadt.de, 1996.

[10] 염흥열, 윤호선, 이강석, 김락현, 류영규, 류종호 '공개키 키관리 체계 표준화 연구', 한국정보보호센터 1998.12

[11] IETF, Security Area, "X.509 (pkix) Document", http://www.ietf.org, 1999.7.

[12] GITS Security, http://gits-sec.treas.gov/index.html, 1999.

[13] GoC PKI, http://www.cio-dpi.gc.ca/pki/home_e.html, 1999.

[14] Government Public Key Authority(GPKA), http://www.gpka.gov.au/.

〈著者紹介〉

염 흥 열 (廉 興 熱)

77. 3 ~ 81. 2 한양대학교 전자공학 학사
81. 3 ~ 83. 2 한양대학교 전자공학 석사
83. 3 ~ 90. 2 한양대학교 전자공학 박사
82. 12 ~ 90 .9 한국전자통신 연구소 선임연구원
90.9 ~ 현재 순천향대학교 공과대학 정보기술공학부 부교수
90. 12 ~ 현재 한국통신정보보호학회 논문지 편집위원 및 정보보호응용연구회 위원장
97. 3 ~ 현재 한국통신정보보호학회 총무이사
97. 3 ~ 2000.2. 순천향대학교 산학연 컨소시설 사업단장
〈관심분야〉 암호이론(서명, 비밀분산기법), 부호이론, 전자상거래보안(전자화폐), PKI 기술