BCA(Bridge CA)개념을 이용한 전자정부 PKI(Public Key Infrastructure) 모델

김기수, 이민구, 이병만, 선우종성

한국전산원

Public Key Infrastructure Model for Electronic Government using Bridge Certificate Authority

Ki-Su Kim, Min-Gu Lee, Byung-Man Lee, Jong-Sung Sunwoo

National Computerization Agency

요약

전자문서, 전자결재, 행정 EDI 등과 같은 전자적 매체를 이용한 행정정보화를 실현하기 위한 전자정부 구축 노력이 추진됨에 따라 전자정부 환경에서 발생할 수 있는 각종 정보보호 요소들을 원천적으로 해결하기 위해 전자서명 등과 같은 공개키 기반의 암호 기술 적용이 필수적 요소로 여겨지고 있으나, 공개키 암호 기술에 사용되는 암호화 키의 체계적인 관리를 위한 공개키 인증 체계(PKI) 구축에 대한 방안마련이 미흡한 실정이다. 이에 본 논문에서는 전자정부 환경에서 공개키 기반 암호 기술의 효과적인 적용을 위한 공개키 인증 체계 모델과 관련 조직 체계 구성 방안에 대해 제안하고자 한다.

1. 서론

정보기술과 통신 기술의 급속한 발전으로 인해 기존의 산업화 사회의 모습으로 형성되어 오던 삶의 유형 또한 새로운 패러다임인 정보화 사회의 모습으로 급진전하고 있다. 즉, 지금까지의 사람과 사람 또는 사람과 단체 등간에 행해지던 각종 일상 관행들이 컴퓨터, 정보망(인터넷) 등과 같은 전자매체에 의해 수행되는 환경의 조성이 이루어지고 있는 것이다. 이러한 기술의 발달은 1990년대에 이르러 더욱 가속화되고 있고 이에 따라 미국, 일본, 유럽 등 선진 외국들은 첨단 정보, 통신 기술을 활용한 새로운 삶의 기반 창출을 도모하여 21세기 국가경쟁력

을 확보하고자 많은 노력을 기울이고 있으며 그중 가장 대표적인 개념으로 1990년대 초반부터 미국에 의해 주창되어 오고있는 "전자정부(Electronic Government)"를 들 수 있다.

전자정부의 핵심은 정보기술과 통신기술을 활용한 대 국민 서비스의 향상과 행정의 효율성 확대라 할 수 있다. 즉, 첨단 정보 및 통신 기술을 활용하여 정부 기관 내 각종 업무를 재 설계하고 관련된 다양한 정보를 전자화 하여 정부 업무의 자동화, 정보화를 위한 새로운 업무 관행을 창출하고 이를 이용하여 국민들에게 필요한 정보와 서비스를 즉각적이고 효율적으로 제공할 수 있는 기반을 구축하고자 하는 것이다.

이와 같은 개념에서 볼 때 전자정부에서 반드시 고려해야할 사항 중 하나는 정부 기관간 또는 정부 기관과 공무원, 정부기관과 국민, 공무원과 국민 등간에 전자적으로 이루어지는 업무 및 민원처리에 있어서의 보안성 확보이다. 전자화 및 정보화된 환경 속에서 흔히 간과되기 쉬운 일반 국민의 프라이버시 보호뿐만 아니라 각종 정부 관련 정보의 정부기관간 그리고 대 국민 공유에서 발생할 수 있는 많은 문제점들에 대한 근본적인 해결책 마련이 필요하다. 특히 정보화 환경에서는 정보의 변조, 복조, 차단 등과 같은 지금까지의 일반적인 환경에서 발생하지 않았던 새로운 정보보호 문제가 발생되고 있으므로 이의 해결을 통한 안전한 전자정부 구축이 무엇보다 우선적으로 선결되어야할 과제이다.

현재 정보망과 컴퓨터 등의 정보시스템을 통한 전자정보의 전송과 시스템의 원격 접속, 정보 조회 및 획득, 가공 등에서 발생할 수 있는 보안상의 각종 문제점들을 원천적으로 해결하기 위한 노력이 전세계적으로 이루어지고 있는 가운데 공개키 암호 (Public Key Cryptography)기술을 이용해 정보를 암호화하여 전송함으로써 해당 정보 및 사용자들에 대한 인증성(authenticity), 비밀성(confidentiality), 무결성(integrity) 등을 확보하는 방법이 다양한 형태로 개발되고 있다. 이와 함께 공개키 암호 기술의 효과적인 활용을 위한 기반 체계 구축을 위해 PKI(Public Key Infrastructure)라는 개념이 미국, 캐나다, 유럽연합 등을 중심으로 꾸준히 연구되고 있고 이에 따라 각기 자국 고유의 PKI 체계 구축을 위해 노력하고있으며 IETF, ITU, ISO/IEC 등 국제표준화 기관을 통한 각종 세부 기술의 표준화가 추진 중에 있다.

본 논문에서는 최근 정부에 의해 추진되고 있는 전자정부의 개념과 전자정부에서의 보안성 확보를 위한 PKI 구축 방안 및 고려사항에 대해 논하고자한다. 2장에서는 PKI에 대한 기본적인 개념에 대해 살펴보고 3장에서는 현재 정부에서 추진중인 전자정부 구축 방안에 대한 파악을 통하여 전자정부에서의 PKI 구축 필요성과 그에 따른 구축 모델과 조직 구성 체계를 제시하고 4장에서 결론을 맺는다.

2. PKI 기본 개념

PKI는 일반적으로 공개키 암호 어플리케이션에 사용되는 공개키 값의 효율적이고 안전한 유통을 위해 사용되는 전자 인증서(digital certificate)의 발행과 획득, 조회, 검증 등을 수행할 수 있도록 하는 인증서 관리 기반 구조 즉, 전자 인증서를 이용한 공개키 관리 구조를 말한다. 또한 이러한 전자 인증서의 발행, 배포 등의 관리를 수행하는 믿을 수 있는 인증기관(CA : Certificate Authority) 들간의 신뢰 구조를 말하기도 한다. 특히 PKI는 공개키 암호를 기반으로 하고 있는 전자서명 어플리케이션에서의 무결성(integrity), 송신 부인봉쇄(source non-repudiation), 인증(authentication) 등의 보안 서비스가 효율적이고 안정적으로 제공될 수 있도록 함을 주요 목적으로 하고 있으며 PKI가 제공해야할 가장 기본적인 기능으로 다음의 두 가지를 들 수 있다.

- 인증(certification) : 각 개인 또는 기관 등과 같은 개체들과 그들이 소유하고 있는 공개키 값(public key value)을 공식적으로 연결(binding)하는 행위
- 검증(validation) : 인증(certification) 내용이 여전히 유효한지를 확인하는 행위

PKI에서는 일반적으로 위의 두 기능의 효율적인 수행을 위하여 전자 인증서(digital certificate)와 인증기관(CA)의 개념을 사용한다. 즉, 공개키를 이용하는 각 개체가 소유하고 있는 공개키 값과 해당 개체의 신원 정보를 공식적으로 연결하는 매체로서 전자 인증서를 사용하며 전자 인증서를 발행하고 발행된 전자 인증서의 내용을 보증하고 관리하는 기능은 인증기관이 수행하도록 하는 것이다. 이와 같은 전자 인증서 및 인증기관 등의 활용에 대한 기본 개념은 일반적으로 X.509를 기반으로 하고 있다. X.509는 ISO와 ITU에 의해 국제 표준으로 제안되어 있는 공개키 기반의 인증 프레임워크로서 공개키 기반 인증의 가장 대표적인 기술로 폭넓게 적용되고 있다.

이와 같이 PKI는 공개키 전자 인증서의 발행, 취소, 배포 등과 같은 전자 인증서 관리에 관련된 구성 요소 및 기능의 정의, 인증 구조의 확립 등에 관련된 관리적, 기술적 제반 사항을 체계적으로 수립하여 공개키 관리의 효율성을 고취하고 더 나아가 공개키 암호 기술이 제공하는 보안 서비스가 안정적으로 이루어질 수 있도록 하기 위한 기술이다. PKI는 다음과 같은 기본 구성 요소들로 이루어져 있으며 이들 구성 요소간의 관계와 트랜잭션 유형 등에 따라 각기 고유한 PKI를 구성할 수 있다.

PAA(Policy Approving Authority) : 정책승인 기관

PAA는 PKI내의 CA 또는 ORA 등과 같은 관리 기관들에 대한 종합적인 운영 감독 및 조정의 역할을 수행하며 이를 위해 PKI 내에서 통용될 수 있는 인증 정책(certificate policy) 또는 인증실무준칙(certificate practice)등을 수립하고 시행한다. 따라서 PKI 내의 모든 CA들은 PAA가 수립한 인증 정책 또는 규칙에 따라 인증서를 발행하고 관리하도록 한다. 이밖에 PAA는 PKI내의 관리 기관들의 시스템 보안 정책과 CA들간의 상호 교차 인증 수행 등에 대한 정책도 수립하고 시행 감독한다.

CA(Certificate Authority) : 인증 기관

CA는 공개키 인증서의 발행, 취소, 배포 및 보관 등과 같은 기본적인 인증서 배포 관리 역할과 서로 다른 CA들간의 상호 교차 인증 수행을 위한 교차 인증서의 발행과 취소의 기능 수행, 발행 및 취소 인증서 등 인증서 정보의 효과적인 관리 및 배포를 위한 디렉토리 서버의 운영 등의 역할을 수행한다. 각 CA들은 PAA의 인증 정책 및 규칙을 기반으로 한, 각기 고유의 인증 정책 및 규칙에 의해 인증서 관리 기능을 수행하며 이를 위해 PAA의 검증을 받아야 한다.

ORA(Organizational Registration Authority) : 조직등록 기관

ORA는 인증서를 요청하는 사용자의 신분과 인증 요청 대상 공개키와 한 쌍을 이루는 비밀키의 보유 여부 등을 확인하고 CA에게 인증서를 요청해주는 하나의 기능 요소이다. 일반적으로 ORA는 CA와 분리된 기관으로 구성하지 않고 CA 내에서 수행하지만 해당 CA가 전담하는 사용자들의 유형이 다양하거나 각 사용자 유형에 따른 소속 위치가 광범위할 경우 각 유형에 해당하는 ORA를 두어 CA의 업무를 보조한다.

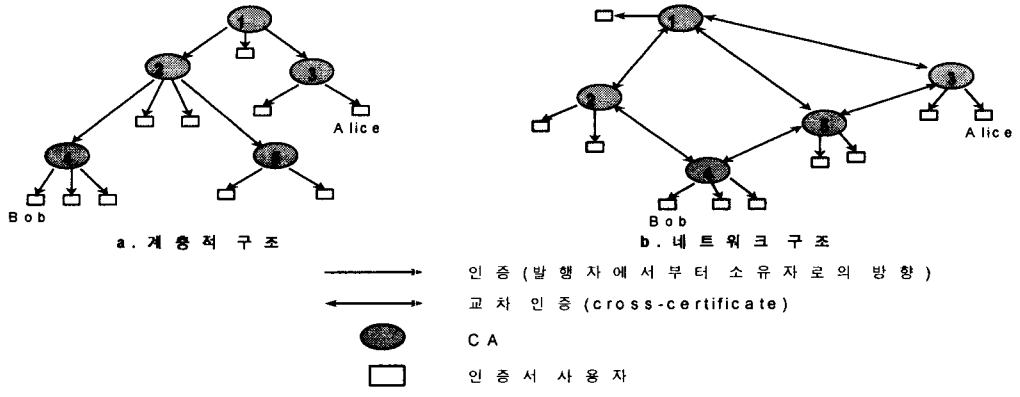
Clients : 클라이언트

클라이언트는 공개키 기반의 어플리케이션을 이용하는 사용자 및 관련 응용시스템을 통칭하며 클라이언트는 자신의 공개키에 대한 인증서의 요청 및 획득과 자신 및 다른 클라이언트의 공개키 인증서의 검증 기능을 수행할 수 있어야 한다. 그밖에 CA가 발행한 취소 인증서 리스트(CRLs)의 검증 및 해석 기능과 공개키 인증서에 의한 전자서명의 생성 및 검증의 기능도 수행하며 인증서 정보의 획득을 위해 CA가 운영하는 디렉토리서버와의 통신이 가능해야 한다.

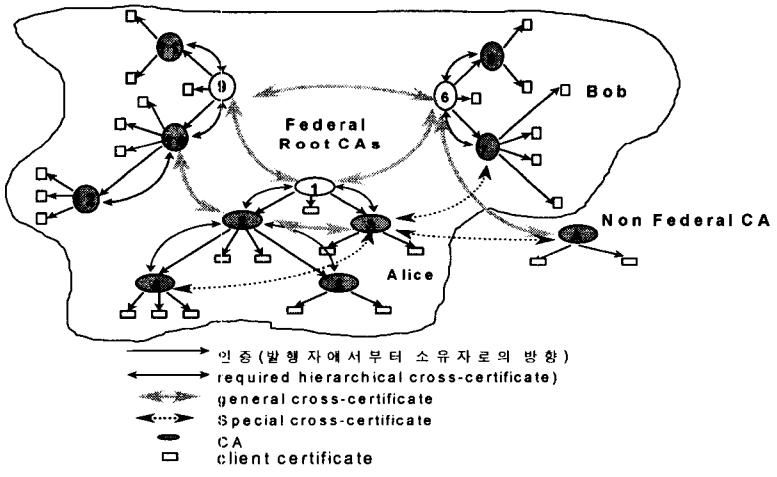
Directory Server : 디렉토리서버

디렉토리서버는 각 CA에 의해 발행된 인증서와 취소된 인증서 리스트(CRLs)에 대한 보관 및 정보제공을 위한 일종의 정보 저장소로서 CA가 담당 관리한다. 일반적으로 PKI에서의 디렉토리서비스는 X.500 디렉토리서비스를 준수하며 디렉토리서버의 접근을 위한 프로토콜로는 DAP(Directory Access protocol)와 LDAP(Lightweight DAP, RFC 1777)가 가장 많이 활용되고 있으며 이밖에 FTP, HTTP 등을 이용할 수도 있다.

PKI에서는 이와 같은 PKI 구성 요소 중 가장 핵심이라 할 수 있는 CA들에 대한 구성 체계를 통하여 인증서와 CRL 등에 대한 관리의 최적화를 도모할 수 있다. 즉, CA간의 신뢰 고리를 어떻게 형성하는가에 따라 해당 PKI의 특성을 결정지을 수 있는 것이다. X.509가 X.500의 디렉토리서비스 개념을 근간으로 하기 때문에 PKI에서의 가장 기본적인 인증체계로는 체계성과 정렬성에 초점을 두고 있는 계층적 구조(hierarchical structure)를 들 수 있고(<그림 2-1>.a 참조), 이와는 대조적으로 체계의 자율성에 초점을 두고 있는 네트워크 구조(network structure)가 있다(<그림 2-1>.b 참조). 또한 이 두 구조의 장·단점을 수용할 수 있는 혼합형 구조(hybrid structure)가 제시되고 있다.(<그림 2-2> 참조)



<그림 2-1> PKI 기본 인증 구조



<그림 2-2> 혼합형 FPKI 인증 구조

3. 전자정부 PKI 구축 방안

3.1 전자정부 구축 개념과 PKI의 필요성

국내에서 전자정부에 대한 개념은 1987년부터 시작된 1차 행정전산망 사업과 1992년~1996년까지 추진된 2차 행정전산망 사업의 추진과 그 성과에 대한 평가와 함께 국가 정보화에 대한 구체적인 비전 제시를 위한 초고속정보통신기반 구축에

대한 논의가 시작된 1994년 말부터 등장하기 시작했다. 전자정부의 개념에는 작게는 정부의 일반 행정 업무에 대한 행정정보화에서부터 크게는 행정, 물류, 국방, 교육 등 국가 전반의 업무에 대한 정보화까지 포괄적으로 포함하고 있으나, 사실 국내의 전자정부에 대한 구체적인 개념 정립은 아직 부족한 실정이며 1998년 초부터 국정 100대 과제에 "전자정부 구현" 사업이 채택됨에 따라 본격적인 논의가 시작되었다고 할 수 있다.

1998년 3월 전자정부 구축을 위해 행정자치부에서는 전자정부 구축 비전 제시를 위해 다음과 같이 전자정부 구현을 위한 6대 분야의 18대 과제를 추진하고자 하는 계획을 마련하고 있다.

1. 국민 지향적 행정서비스 실현
   1) ONE-STOP, NON-STOP 서비스 실시 2) 행정서비스 전달 수단의 다양화
   3) 인터넷을 통한 행정정보 공개 확대
2. 행정업무의 효율적 재설계
   4) 행정업무의 재설계 추진 5) 보고·결재 과정의 전자화
   6) 정책의사결정 흐름의 자동화
3. 행정정보 공동이용의 활성화
   7) 행정정보의 축적 및 공동이용 촉진 8) 행정정보공동이용센터 구축
   9) 정보 보호관리 강화
4. 공무원 개인 사무의 생산성 제고
   10) 개인 사무 자동화 촉진 11) 원격근무제 도입
   12) 정보화 자격증 우대 및 교육 강화
5. 행정정보기반 정비
   13) 정부 인트라넷의 구축 14) 정보시스템의 표준 정립
   15) 시스템의 안정성·신뢰성 확보대책 강화
6. 법·제도 개선
   16) 전자정부 구현을 위한 법·제도의 정비
   17) 고위정보관리자 제도의 도입 및 정보화추진조직 강화
   18) 범정부적 정보자원관리체제 확립

또한 정보통신부를 중심으로 위와 같은 전자정부의 구현을 위해 다음과 같은 3가지의 대표적인 시책을 강구하고 있다. 첫째, 2000년까지 대 국민 민원 서비스를 획기적으로 개선하고자 일회 민원 처리 서비스를 확대하고 PC 통신을 통한 안

방 민원 서비스를 확대할 방침이다. 또한 현재 각 부처별로 나뉘어져 있는 자동차 등록, 검사, 세금 등 자동차 관련 민원업무를 관련 기관의 정보망을 연계하여 일괄처리(One-Stop)할 수 있도록 1998년까지 자동차종합민원정보망 구축을 추진할 예정이다. 또한 주민등록 정보를 필요로 하는 행정기관을 정보망으로 연계하여 국민이 주민등록 등·초본을 발급 받아 타 국가기관에 제출하는 불편을 대폭 감소시킬 수 있도록 의료보험, 고용보험, 국민연금, 국세, 지방세, 자동차 등 6개 업무를 대상으로 하는 시범사업을 실시할 예정이다.

둘째, 정부정보의 공동활용 및 공개를 촉진하기 위하여 정보를 공동 활용해야 할 필요성이 높은 부문부터 정보공동활용체제를 구축할 예정이다. 2000년까지 국회와 법원을 중심으로 각각 입법 및 사법과 관련된 종합정보시스템을 구축하는 한편 정보공조체제가 절실히 요구되는 법원이나 검찰, 경찰 등 사법기관 간 범죄수사정보 공동활용체제를 구축할 것이다. 나아가 정부와 국민 사이에 원활한 정보교류 및 정보공유를 촉진하기 위해 열린 정부 서비스 및 인터넷을 통해 행정정보를 적극적으로 제공할 예정이다.

셋째, 행정정보의 활용 확대를 위한 기반조성을 위하여 2000년까지 공무원 1인당 1 PC 보급을 추진하며 정부청사 및 입법부, 사법부를 연결하는 고속통신망을 구축하여 정보공동활용과 전자적 업무처리의 기반을 확보할 예정이다.

지금까지 살펴본 전자정부의 기본 개념과 정부의 전자정부 구축을 위한 추진방향에서 알 수 있듯이 전자정부의 핵심은 정보기술 매체를 통한 전자 정보의 원활한 유통 체계 확립이라 할 수 있다. 이를 위해서는 현재 개발되고 있는 전자우편, EDI(Electronic Data Interchange), 전자결재 등과 같은 각종 메시징 관련 시스템들을 이용한 메시지 교환 서비스의 활용과, X.500 디렉토리 서비스와 LDAP 프로토콜을 통한 정보의 검색, 획득 서비스 등과 같은 인터넷 관련 기술의 적용이 필수적이라 하겠다. 그러나 서론에서 설명한 바와 같이 TCP/IP 프로토콜이 적용되는 인터넷 기반의 이러한 대부분의 응용기술들은 정보보호 측면에 많은 문제점들을 가지고 있는 것이 사실이다. 특히, 전자정부에서는 정부의 민감한 정보들을 정부 관련 기관간 정보망을 통한 교환이 빈번히 이루어질 것이며 기본적으로 대 국민 정보서비스를 위해 정부 기관의 정보망이 인터넷 등의 민간 정보망과 연결되어 있어야 하므로 근본적인 정보보호 대책의 마련이 필요하다. 전자정부 개념에서 구현되는 각종 정보기술 서비스 상에서 발생 가능한 보안 요소들을 나열

해보면 다음과 같다.

1. 국가적으로 민감한 정보에 대한 불법 노출, 변조, 복조
2. 국민의 프라이버시를 저해하는 개인 정보에 대한 불법 노출, 변조, 복조
3. 전자적으로 처리되는 정부 기관의 업무 처리 수행 및 결과에 대한 권한과 책임의 오·남용
4. 정부기관간 또는 정부와 국민간의 행정 업무 처리에 있어서의 신원 사칭
5. 공공 정보시스템에 대한 정보망을 이용한 불법적 접근을 통한 해킹

위와 같은 보안 요소들은 정보기술 및 정보통신 환경에 있어서의 일반적인 보안 요소들과 동일하며 특히 최근 들어 활발히 전개되고 있는 전자상거래에서의 보안 요소와 거의 유사하다. 이것은 전자정부와 전자상거래는 기본적으로 세부 업무 내용만 다를 뿐이지 그러한 업무를 수행하기 위해 적용되는 정보기술 및 통신기술은 동일하기 때문이다. 즉, 전자상거래에서의 카드 번호 및 개인 정보 등과 같은 거래 정보의 안전한 정보망 유통, 거래 상대방에 대한 효과적인 신원 확인, 거래 수행 후 거래 사실에 대한 부인 방지 등과 같은 정보보호 요구사항이 전자정부 환경에서도 필요한 보안 요소로 적용된다. 따라서 전자정부에서의 정보보호 대책 방안도 전자상거래 등과 같은 일반 정보기술 환경에서의 정보보호 대책 방안을 근간으로 해야만 하며 다만, 전자정부 내에서 수행되는 고유한 업무 특성에 의해 요구되는 보안의 강도에 대한 구체적인 방안이 추가로 정립되어야 할 것이다.

전자정부에서 정보보호 요소의 핵심은 전자적으로 전송, 처리되는 전자 문서 및 보고 자료 등과 같은 각종 문서 정보, 주민등록 및 부동산 정보 등과 같은 민원 처리 정보, 예산 및 회계 등과 같은 행정 정보 등에 대한 비밀성과 무결성의 보장 그리고 전자적 업무 수행 사실에 대한 부인 방지 및 수행자의 신원확인 등과 같은 인증성 보장 등이라 하겠다. 이러한 정보보호 요소에 대한 해결을 위해 전자상거래 등에서 가장 폭넓게 적용되는 기술은 공개키 암호 및 전자서명 등과 같은 기술로서 국제적으로 그 기술의 완성도 및 활용도 측면에 있어 이미 상당한 수준까지 도달해 있으며 다양한 형태의 제품이 개발되어 실제 환경에 적용되고 있기도 하다. 이에 따라 공개키 암호 어플리케이션의 기반이 되는 공개키 인증체계(PKI) 구축에 대한 필요성 및 중요성에 대한 인식이 확산되고 있어 현재 미국, 캐나다, 유럽을 중심으로 활발히 연구되고 있다. 특히, PKI 개념에서는 공개키 인증서만을 가지고 통신 개체들에 대한 신원을 확인하는 사용자 인증과, 송·

수신되는 메시지의 변경 여부 등을 확인하는 메시지 인증 모두를 수행할 수 있으므로 지금까지 시스템 접근통제 기술, 전자서명 기술 등과 같이 각각 분산되어 적용되고 있는 정보보호 기술을 통합된 환경에서 이용할 수 있다는 장점이 있다. 따라서 지금까지 선진 주요 국가들을 중심으로 활발히 연구되었고 일부 구현 제품의 활용이 이루어지고 있는 PKI 개념을 전자정부에 적용하여 전자정부에서 요구되는 각종 정보보호 요소를 해결할 수 있을 것이다.

3.2 전자정부 PKI 구축 모델

3.1절에서 살펴본 바와 같이 현재까지 추진되고 있는 국내 전자정부의 개념은 정부 및 대국민간 행정 업무의 전자화를 주 대상으로 하는 행정정보화를 핵심 과제로 우선적으로 추진하고 있으며 이를 통한 전자정부의 기반 확보를 통하여 추후 외교, 국방, 교육, 과학, 농·수산 등 국가 전 분야의 제반 업무와 대 국민 서비스를 위한 정보서비스로 확장하고자 계획하고 있음을 알 수 있다. 따라서 본 논문에서는 최근까지 추진되고 있는 전자정부의 영역인 행정정보화를 주 대상으로 하고 추후, 외교, 국방 등의 국가 전 분야로의 확장이 가능하도록 하는 전자정부 PKI 구축 기본 모델과 이를 위한 국가적 차원의 조직 구성 체계를 제시하고자 한다.

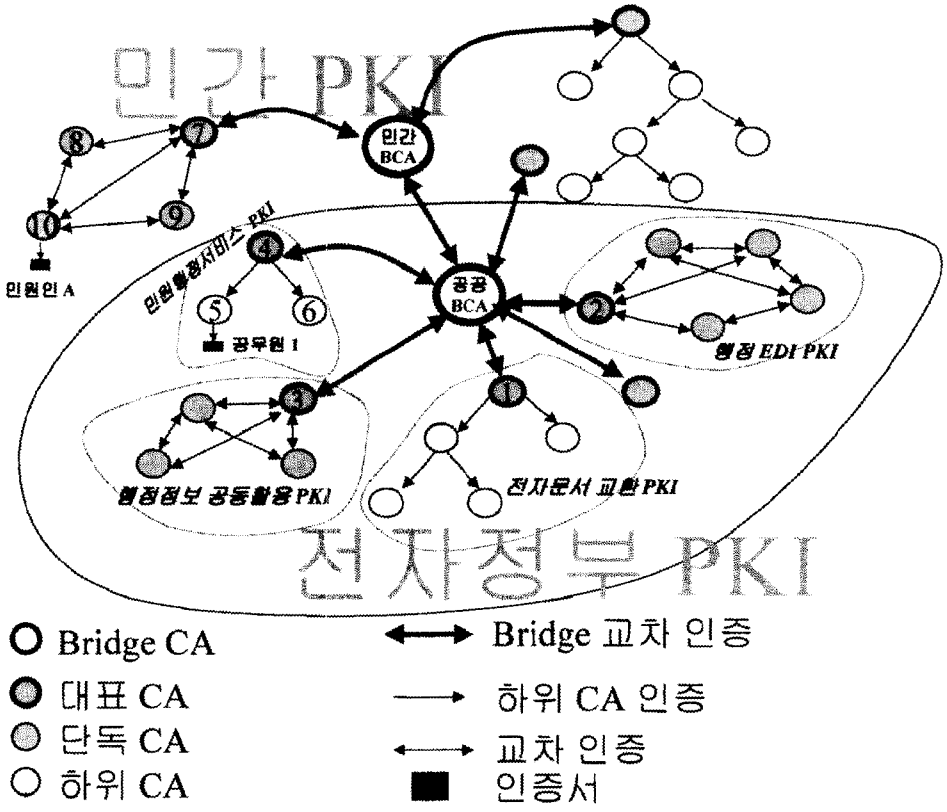
전자정부 PKI 구축을 위해 무엇보다 우선적으로 고려해야할 사항은 바로 어떠한 PKI 유형을 기반으로 할 것인지에 대한 결정이다. 즉, 정부의 조직 구성에 따라 단일화된 체계성을 장점으로 하는 계층적 구조를 기반으로 할 것인지, 세부 기능 서비스별로 자율적인 신뢰 관계를 형성하는 네트워크 구조를 선택할 것인지 또는 그밖의 다른 구조를 기반으로 할 것인지에 대한 결정이 이루어져야 한다. 이러한 전자정부의 기본 PKI 유형을 결정하기 위해 본 논문에서는 전자정부에서 PKI 개념의 적용이 필요한 서비스들에 대한 유형별 분류를 3.1절에서 제시된 행정정보화를 기반으로 하는 전자정부의 기본 추진 과제를 토대로 다음 [표 1]과 같이 4개의 서브 PKI 도메인으로 나누어 보았다.

[표 1] 전자정부내 서비스 유형별 PKI 분류

유형별 PKI 도메인	주요 서비스 내용	예상 인증구조
정부기관간 전자문서 교환을 위한 PKI	• 정부 기관내 및 기관간 지시 및 보고 자료의 전자결재/전자공문서 교환 • 범 정부용 전자우편 시스템 운영 • 통신망을 통한 문서 검색, 열람 서비스 제공	계층적 구조
조달, 관세, 특허 등 행정 EDI를 위한 PKI	• 조달 요청, 계약 요청, 시설공사 입찰 등의 조달 EDI 업무 • 통관 관리 및 여행자 정보 관리 등의 관세 EDI 업무 • 특허 출원, 심사, 등록, 심판 등의 특허 EDI 업무	네트워크 구조
정부기관간 행정정보의 공동활용을 위한 PKI	• 행정종합정보시스템을 통한 각 기관별 정책정보의 적시 검색 체제 구현 • 자동차, 국세, 의료보험, 국민연금 등 정보의 온라인망을 통한 실시간 검색	네트워크 구조
일반 민원 정보 조회, 확인, 처리 등의 민원행정서비스를 위한 PKI	• ONE-STOP/NON-STOP 안방 민원 서비스 • 각종 제 증명 서류 신청 및 발급 확인 서비스 등	계층적 구조

이들 각각의 도메인을 형성하는 응용서비스들은 대부분 상호간 독립적으로 운영되며 서비스 운영의 주체도 각기 다르고 필요한 보안 요구사항의 수준과 각 응용서비스 운영에 대한 기본 보안 정책 등의 특성도 다를 것이다. 이밖에 계속적인 국가정보화의 추진을 통하여 전자정부의 범위로 포함될 것으로 판단되는 외교, 국방, 교육 등의 업무에 관련된 세부 PKI 또한 다른 도메인과는 여러 면에서 차별적으로 운영될 것으로 예상된다. 따라서, 전자정부에서의 PKI는 기본적으로 위에서 제시된 4개의 도메인 등과 같이 독립된 여러 개의 서브 PKI 도메인이 자율적으로 서비스의 특성에 맞도록 계층적 또는 네트워크 구조 등으로 형성되도록 하고, 이들 각각의 서브 PKI 도메인을 연결하는 특정 CA를 두어 서로 다른 세부 PKI 도메인을 통합적으로 관리하고, 필요시 신뢰 고리를 형성해 줄 수 있는 구조로 구성하여 전체 PKI의 확장성과 융통성을 확보할 수 있도록 해야한다.

이와 같은 PKI 구조에 대한 개념으로서 최근 미국의 연방 PKI 구축을 위한 연구에 의해 혼합형 구조를 개선시킨 새로운 개념인 BCA(Bride CA)가 등장했다. BCA는 각기 독립적으로 운영되는 PKI 도메인들과 교차 인증(Cross Certification)만을 수행해 서로 다른 PKI 도메인간에 신뢰 고리를 형성하도록 하는 CA로서 이의 개념을 전자정부 PKI에 <그림 3.1>과 같이 적용할 수 있다.



<그림 3-1> BCA를 이용한 전자정부 PKI 모델

BCA 개념은 각기 고유의 PKI 인증 체계(계층적 또는 네트워크)를 가진 각각의 서브 PKI 도메인들과의 교차 인증만을 수행하는 CA(BCA)를 두어 단일 계층 구조 각 혼합형 구조에서 보여주었던 인증 경로의 획일화에 의한 비 현실성을 해결하 ! 복잡성을 간편화하여 관리의 편리성을 도모한 구조로서 이때, BCA와 교차 인 을 직접 수행하는 각 PKI 도메인내의 CA를 대표 CA(principal CA)(<그림 3-1> ①, ②, ③, ④)라하며 계층적 구조의 PKI 도메인에서는 루트 CA가 대표 CA이 혼합형 구조에서는 가장 대표성을 가지고 있는 한 CA를 선정해 대표 CA로 지 다.

전자정부 PKI에서는 <그림 3-1>과 같이 서로 독립적인 응용서비스별 서브 PKI 도메인은 그 응용서비스 및 주체 기관의 특성에 따라 계층형, 네트워크형 등으로 자유롭게 구성할 수 있으며 각 도메인별로 대표 CA를 지정하여 전자정부 BCA와 교차 인증만을 수행하도록 하면 된다. 따라서 위의 4개의 서브 PKI 도메인 외에도 계속적으로 추가되는 외교, 국방, 교육 등의 응용서비스에 대한 세부 PKI 도메인 형성시 해당 도메인의 대표 CA를 선정하여 공공부문의 BCA와 교차 인증을 함으로써 전체 전자정부 PKI의 기본 구조 및 정책 등을 변경하지 않고 손쉽게 전자정부 PKI의 확장 등의 관리 업무가 수행될 수 있을 것이다. 또한 일반 국민들의 경우 전자정부 BCA에 의해 공인된 민간부문 BCA와 교차 인증되는 특정 CA에 가입하여 인증서를 발급 받아 사용함으로써 전자정부 내에서 수행되는 각종 민원 서비스 및 공공 정보 활용이 가능하도록 하였다.

이와 같은 개념 하에서 공공 BCA는 각 일반 CA들과 사용자들에게 단지 특정 CA와 사용자들에 대한 신원의 정당성만을 제공하는 것이며 각 CA들이 적용하고 있는 기본적인 인증 정책의 수용 여부는 각 CA들이 판단하여 결정해야 한다. <그림 3-1>의 전자정부 PKI 모델에서 실제 인증 경로 검증 절차를 예를 들어 살펴보면, 특정 CA(⑩)가 발행한 인증서를 가진 민원인 A가 민원을 신청하는데 사용한 인증서를 검증하기 위해 담당 공무원 1이 수행하는 인증서 검증 절차는 일차적으로 공무원 1에서부터 민원인 A까지의 최적의 인증 경로인 공무원 1 -> CA5 -> CA4 -> 공공 BCA -> 민간 BCA -> CA7 -> CA10 -> 민원인 A를 파악하고 파악된 인증 경로의 역 방향인 민원인 A -> CA10 -> CA7 -> 민간 BCA -> 공공 BCA -> CA4 -> CA5 순으로 인증서 검증이 이루어진다. 즉, 민원인 A에게 실제 인증서를 발행해준 CA10의 인증서를 확보해 민원인 A의 인증서를 검증하고 다시 CA10을 보증하고 있는 CA7의 인증서를 확보하여 CA10의 인증서를 검증, CA7의 인증서를 보증하는 민간 BCA의 인증서 확보를 통한 CA7 검증, 민간 BCA를 보증하는 공공 BCA의 인증서 확보를 통한 민간 BCA 검증, 공공 BCA를 신뢰하는 CA4의 인증서 확보를 통한 공공 BCA 검증, 그리고 마지막으로 CA4를 신뢰하고 공무원 1이 이미 알고 있는 CA5의 인증서에 의한 CA4의 검증으로 모든 검증 절차가 이루어진다. 그러나 이러한 절차는 민원인 A와 공무원 1간의 인증 경로상 존재하는 민원 당사자 및 CA들의 정당성 확인을 위한 검증의 과정이며 이러한 절차와 함께 공무원 1은 민원인 A가 속하고 있는 PKI 도메인에서 적용하고 있는 인증 정책을 파악하여 이를 수용할 것인지를 결정해 민원인 A의 인증서를 최종적으로 검증한다. 또한, 민원 행정서비스 PKI 도메인의 특정 공무원이 민원 업무를 처리하기 위해 의료보험 또

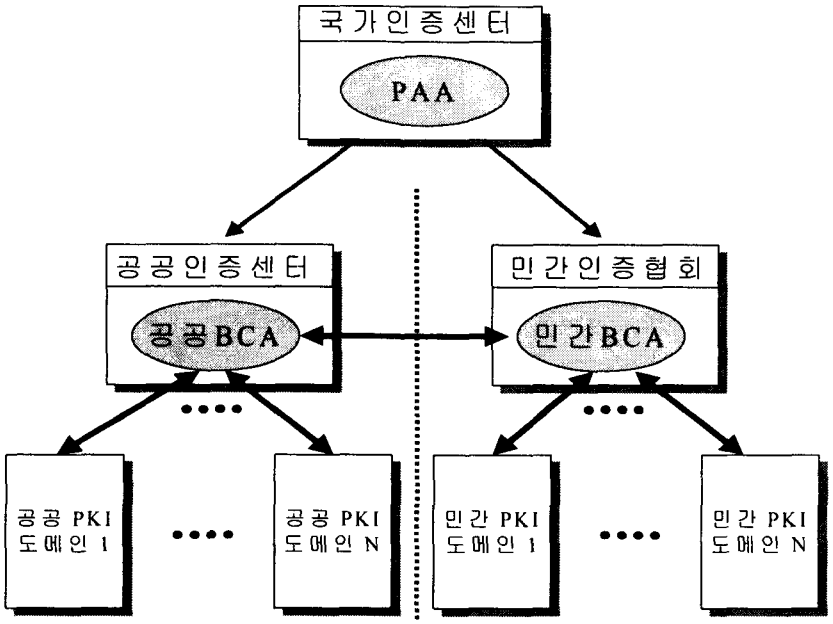
는 국민연금 등과 같은 민원 신청인의 정보 내용을 파악하고자 행정정보 공동활용 PKI 도메인에 접속할 경우 위와 같은 인증 경로 탐색 절차와 인증 정책의 파악을 통하여 해당 공무원에게 특정 정보에 대한 접근을 허락하도록 할 수 있다. 이러한 일련의 인증서 검증 과정은 실제 PKI가 구축된 환경에서는 각각의 인증서가 보유하고 있는 인증 경로 정보에 의해 자동적으로 이루어진다.

이와 같은 전자정부 PKI 모델을 이용하여 다음 <그림 3-2>에서와 같은 형태의 조직 체계 구성 방식으로 국가적 PKI의 체계 구축을 모색할 수 있으며 각 구성 조직들은 다음과 같은 역할 분담이 필요하다.

- 국가인증센터
  인증 정책승인 기관(Policy Approving Authority)으로서 국가적 PKI 차원의 기본 인증 정책 수립 방안 마련과 함께 공공인증센터와 민간인증협회 조직에 대한 승인 및 운영상의 감독 관리 등의 총괄 관리·조정 업무를 수행하며 실제 인증 트랙잭션에는 관여하지 않는다.

- 공공인증센터
  공공부문에 있어 하위 PKI 도메인의 구성 및 대표 CA 선정 등에 대한 승인 업무를 수행하고 승인된 각 하위 PKI 도메인의 대표 CA와 교차 인증을 수행해 실제 인증 트랜잭션 발생시 인증 경로를 제공하며 민간인증협회와의 교차 인증도 수행한다.

- 민간인증협회
  민간부문에 있어 PKI 도메인 구성 또는 CA의 승인, 등록 등의 업무를 수행하고 이들과의 교차 인증 업무를 담당한다. 또한 공공인증센터와의 교차 인증도 수행한다.



<그림 3-2> 국가 PKI 조직 구성 체계

4. 결론

지금까지 전자정부 PKI를 위한 기본 구조로서 BCA 개념을 소개하고 그에 따른 기본적인 전자정부 PKI 구축 모델과 국가 PKI 조직 구성 체계 구축 방안에 대해 설명하였다. 전자정부 PKI 구축을 위해선 본 논문에서 다루고 있는 것과 같이 전자정부 PKI의 기본 틀에 대한 개념 정립이 우선적으로 이루어져야 하며 전자정부 PKI 기본 틀을 결정하기 위해 무엇보다 중요하게 고려되어야 할 것은 확장성과 연동성의 확보라 하겠다. 즉, 추후 전자정부 개념의 확대시 전자정부 PKI도 그에 맞게 쉽게 확대 적용될 수 있도록 전자정부 PKI 기본 틀에 이를 충분히 고려해야 하며, 민간 및 타 국가의 PKI 등과의 안전하고 자유로운 연동이 가능하도록 전자서명 알고리즘 등 관련 기술에 대한 연동성 확보가 무엇보다 필요한 것이다.

전자정부 PKI가 필요한 궁극적인 이유는 전자정부에서 유통되는 각종 정보와 사용자들에 대한 인증성 확보로서 전자정부 PKI가 적용되는 대표적인 예는 바로 전자서명 어플리케이션이다. 따라서 전자정부 PKI 구축도 현재 추진되고 있는 전자서명기본법의 기본 개념과 논리를 만족시킬 수 있는 형태로 진행되어야 한다. 그밖에 전자정부 구축을 위해 CA간 교차인증 수행, 인증 정책 및 실무준칙 등에

대한 등록과 검토에 의한 사용승인 등을 위한 절차와 X.509 v3 certificate extension 적용 방안 등과 같은 기술적 요소들에 대한 충분한 고려도 필요하다.

지금까지 설명된바와 같이 정부가 주도하는 체계적인 전자정부 PKI의 구축 노력에 따라 결국 국가적 PKI 구축이 완성될 수 있으므로, 전자정부 PKI에 관련된 제도적, 기술적 요구사항 등을 해결하기 위해 산·학·연 관련 전문가들에 의한 종합적이고 체계적인 연구 및 실제 구현 환경이 마련될 수 있도록 정부의 적극적인 노력이 절실하다.

참고문헌

[1] Federal Public Key Infrastructure(PKI) Technical Specification(Version 1) Part A : Requirements, Federal PKI Technical Working Group, January 31, 1996

[2] Federal Public Key Infrastructure(PKI) Technical Specification(Version 1) Part B : Technical Security Policy, Federal PKI Technical Working Group, January 24, 1996

[3] Federal Public Key Infrastructure(PKI) Technical Specification(Version 2.3) Part C : Concept of Operation, Federal PKI Technical Working Group, November 25, 1996

[4] Minimum Interoperability Specification for PKI Components, Version 1, NIST, September 3, 1997

[5] Federal Public Key Infrastructure(PKI) Version 1 Technical Specifications : Part E X.509 Certificate and CRL Extensions Profile, Federal PKI Technical Working Group, January 8, 1998

[6] Federal Public Key Infrastructure(PKI) Technical Specification Part D : Interoperability Profiles, Federal PKI Technical Working Group, September 27, 1995

[7] Public Key Infrastructure(PKI) Technical Specifications Part A : Technical Concepts of Operations, Federal PKI Technical Working Group, June 3, 1998

[8] 전자정부의 비전과 전략(안) - 21세기 전자정부로 가는 길, 행정자치

부 행정관리국, 1998. 3

[9] 전자정부 개념 정립 및 구현 방안에 관한 연구, 한국전산원, 1996. 12