인증기반을 활용한 e-행정서비스 도입을 위한 정책방안

A Policy Study on the Government Electronic Service Delivery through Digital Certification Infrastructure

정 충 식 (Choong-sik Chung) 경성대학교 행정학과

목 차

Keywords: *Electronic Government, E-Public Service, Digital Signature, Public Key Infrastructure, Certificate Authorities.*

Ⅰ. 서 론

앞으로 전자상거래에서는 기존 종이문서에 의한 계약이 전자문서로 이루어지고 인증기반에 기초하여 계약당사자가 확인될 경우에는 인증기관을 통한 문서의 작성자, 문서의 내용, 문서의 작성 시점 등에 대한 인증이 필요하게 된다. 따라서 인증기관의 지정 및 이러한 인증기관이라는 신뢰받는 제3자로 하여금 거래당사자의 신원을 입증하도록 하는 사회적인 인프라가 필요한 상황이다. 이처럼 인증기관을 통한 사회적 인프라에 신뢰성을 부가하기 위해서는 정부부문 특히 대국민 민원행정 처리의 분야에서 인증업무를 도입하여 선도적인 전자정부의 인증기반을 구축하여야 한다(김경섭, 2000; 정보보호센터, 1999a).

이처럼 전자정부를 구현하기 위해서는 이제 비대면의 행정처리, 즉 원스톱내지는 진정한 논스톱 서비스가 제공되어야 한다. 이를 지원하는 방안으로는 현재 널리 활용되고 있는 인터넷 기반기술을 민원행정처리에 도입하여 웹기반의 민원행정시스템을 구축하는 것이 필요하다. 이러한 웹기반의 민원행정시스템은 시간과 공간의 제약을 넘어서서 민원인들에게 언제 어디에서나 정부의 서비스에 접근하여 행정업무처리를 수행할 수 있게 하는 혁신적인 방안으로 인식되고 있다(류석상, 1998; 정명선, 1998).

이러한 인증기반은 오늘날 전자상거래 등의 유통분야와 금융분야를 중심으로 하여 구매자와 판매자의 신원확인 및 전자지불 등에서 활성화되고 있다. 그러나 이러한 분야들보다 훨씬 중요하게 국가정보화의 관점에서 인증기반 정책이 추진되어야 하는 부문이 행정분야이다(한국전산원, 2000). 왜냐하면 민간부문의 모든 거래행위는 단순히 정보기술의 도입에 의해 수행될 수 있는 것이 아니라 정부의 정보정책에 의한 사회적 기반의 확립에 의해 좌우될 수 있기 때문이다.

따라서 이러한 행정서비스 제공의 입증기반 즉 인증기반의 구축이 전자정부 구현에 있어서 핵심 성공요인으로 부각되고 있다(김용훈, 1998). 결국 전자정부는 전자적인 행정서비스에 대한 인증이 원활하게 이루어질 때, 그 구현이 앞당겨질 수 있을 것이다. 그

러나 아직까지 국내의 학계나 정보화정책 담당자들에게 전자서명에 기초한 인증기반의 구축은 생소한 분야로 남아있다. 더 나아가 이러한 인증기반을 정보정책에 통합하여 추진하는 것에 대해서는 아직까지 부처이기주의에 의해 도입방안이 확정되지 못하고 있다. 그러므로 이 글에서는 국내외 e-행정서비스의 현황 및 공개키기반구축(Public Key Infrastructure: PKI)을 개관하고, 이어서 인증기반에 기초한 e-행정서비스 도입을 위한 정책방안을 모색해 보고자 한다.

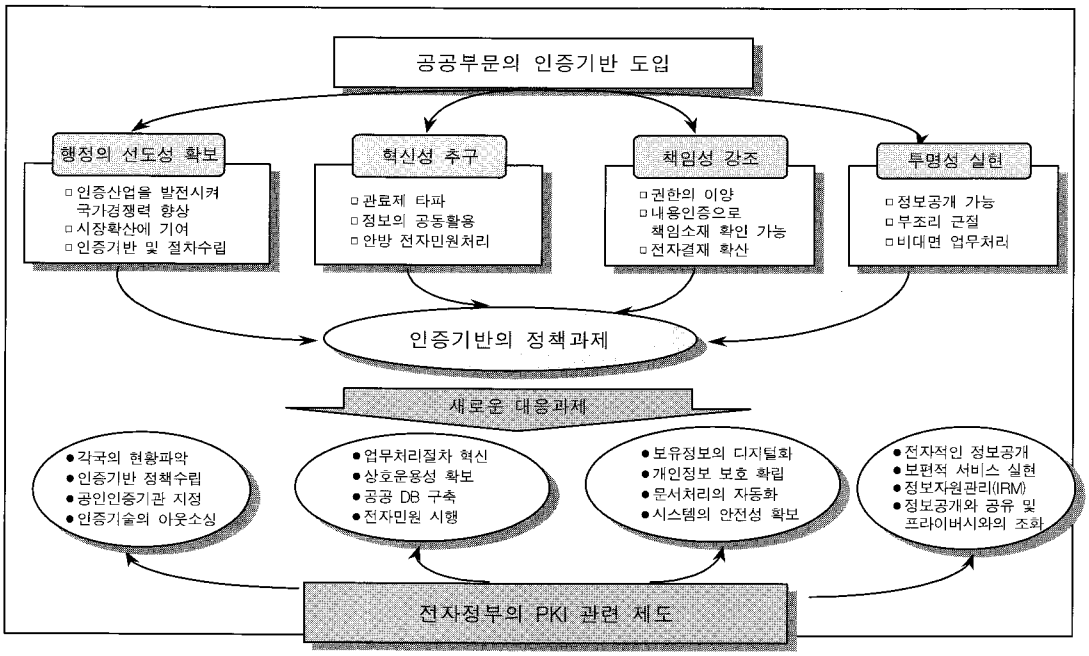
Ⅱ. 공공부문의 전자서명 도입 현황

2.1 공공부문에 인증기반 도입의 중요성

이제부터 우리나라도 전자적인 민원처리를 위한 구체적인 방안으로 24시간 민원서비스 개방과 민원정보 종합처리시스템에 의한 원스톱 행정서비스를 실시하고, 인터넷과 무인민원발급기(KIOSK) 등 행정서비스 전달수단을 다양화 해서 시간과 장소에 구애받지 않도록 민원서비스를 개선할 예정으로 있다. 그러므로 정부의 전자정부 구현을 위한 과제가 완료되는 2002년부터는 행정업무에 사용되는 각종 서류는 물론 국민들이 정부에 제출되는 모든 증명서 등이 전자적으로 처리될 전망이다(전자정부특별위원회, 2001).

이 경우에 전자적인 행정서비스 시스템을 구축하는데는 여러 가지의 어려운 문제들 - 즉 정보의 누출과 변경 가능성, 사생활 침해, 메시지 발생이나 수령에 대한 부인 가능성 등 - 이 먼저 해결되어야 한다. 이러한 문제점들을 해결하기 위해 시급히 도입하여야 하는 것이 행정부문에서 전자서명에 기초한 인증기반의 구축이다(정원섭, 1999). 이처럼 전자서명 및 인증제도는 전자상거래 뿐만 아니라 공공기관이 발행하고 있는 등기, 호적, 주민등록 등본 등의 문서들을 시민들이 전자적으로 통신망을 통하여 신청하고 발급받기 위해서도 필수적으로 도입되어야 하는 제도이다.

이러한 행정부문에의 전자적인 민원행정서비스 기반의 도입은 단순히 전자서명이라고 하는 정보기술을 행정업무에 활용하는 것에 그치지 않고, 다음 <그림 1>과 같이 행정의 선도성, 혁신성, 책임성 및 투명성을 제고하여 행정혁신을 이루어낼



〈그림 1〉 공공부문 인증기반 구축의 중요성

수 있는 중요한 요인으로 작용할 것이다. 이러한 내용을 구체적으로 살펴보면 다음과 같다.

첫째는 행정의 선도성의 측면이다. 현재 정부내의 행정업무뿐만 아니라 민간부문의 업무처리 등도 정부의 사무관리규정에 근거하여 처리되고 있는 부문이 많다. 따라서 정부가 행정내부의 업무처리와 대국민 민원행정처리에 있어 인증에 기반한 전자문서를 활용할 경우에 이것은 바로 민간부문에 적용되어 확산될 것이다.

둘째는 행정의 혁신성 측면이다. 이제 공공부문에 전자서명의 도입이 확산되면 기존의 업무처리절차가 변화되면서 행정정보의 공동이용이 활성화되어 사회 전반의 네트워크화를 촉진시킬 것이다.

셋째는 행정의 책임성의 측면이다. 인증기반의 활용은 단순히 이제까지의 종이문서를 전자문서로 바꾸거나 사용자의 신원확인에만 국한되지 않는다. 앞으로 행정부문의 내부 업무처리에서 인증이 도입되어 모든 정부부처들 사이에 활용될 경우에는 문서 전달에 있어서 시각증명과 배달증명 등의 내용인증에 기초하여 책임행정을 구현할 수 있는 기반이 마련될 것이다. 따라서 이러한 인증기반의 도입은 행정내부의 정보를 공동활용하여 고객지향적 행정서비스를 제공할 수 있는 유력한 수단이다.

넷째는 행정의 투명성에 대한 측면이다. 기존의 민원처리 방식은 민원인 본인이 필요한 구비서류를 준비하여 직접 관공서에 와서 이른바 담당공무원과 얼굴을 마주 대한 상태에서만 일이 진행되었다. 따라서 이 과정에서 민원인의 시간적, 금전적 낭비와 손실 및 민원인과 담당공무원 사이에 이른바 부조리가 생길 수 있는 여지가 존재한 것이 사실이다. 그러나 인증기반을 활용한 전자적인 민원행정의 경우에는 민원인과 담당공무원 사이의 대면 접촉에 의하지 않고 모든 행정처리가 투명하게 이루어질 수 있는 환경이 조성될 것이다.

2.2 공공부문의 인증기반 도입현황

현재 정부는 공공기관간에 처리되는 전자문서의 유통, 인사, 급여 등 행정기관의 공통업무 분야, 각 기관이 보유한 행정정보의 공동이용 분야에 우선적으로 인증기반을 도입하려고 준비하고 있다(행정자치부, 2001). 이처럼 각 기관이 보유한 행정정보의 공동이용이 촉진되면 시스템의 중복구축에 따른 예산낭비를 줄일 수 있고, 민원인이 제출하던 증명서류를 정보통신망을 통한 조회로 대체하여 문서감축과 함께 민원인의 불편을 크게 줄일 수 있을 것이다.

이에 정부의 각종 정보들을 효율적으로 연결·활용할 수 있는 정부차원의 공동이용기반을 구축하여 행정의 생산성 제고 및 국민 편익을 증진하고자 행정정보공동이용규정을 1998년 8월에 제정하고 이 정보들이 공공분야 전자서명 인증기반(GPKI) 위에서 안정적으로 공유될 수 있도록 추진하였다(박인재, 2001).

대표적인 사례로는 행자부에서 추진한 「생산적 복지정보 공동이용시스템」 구축사업이다. 이 사업은 2000년 10월의 국민기초생활보장제도 시행에 맞추어 시군구의 복지담당공무원이 GPKI를 통해 시군구 보유정보, 행자부 국토정보센터, 국세청의 국세통합전산망, 노동부의 고용정보시스템, 국민연금, 의료보험, 근로복지공단의 DB 등을 공동이용하여, 관련정보를 신속·정확히 수집하고 생활보호대상자를 효율적으로 선정·관리할수 있도록 지원하는데 그 목적이 있다. 2000년 현재 추진 중인 GPKI 관련 사업추진 현황은 <표 1>과 같으며, 향후 그 범위는 급격히 확산될 것으로 예상되고 있다.

그러나 이처럼 공공부문에서의 인증기반 구축이 행정정보의 공동활용에 초점을 두게됨에 따라서 전자적인 대민행정서비스 부문은 상대적으로 인증기반의 도입이 지연되고 있다. 정부는 현재 정부단일 서비스 창구의 구축을 통해 민원의 신청에서 처리까지를 공개하고 이를 행정정보공동이용 시스템과 연계시켜 정부대표전자민원실로 확대 발전시킬 계획을 가지고 있다. 또한 정부대표전자민원실에 GPKI 기반을 적용하여 가상 행정공간에서 민원인의 신원확인 수단을 확보할 예정이다. 하지만 아직까지 구체적으로 민원인

〈표 1〉 공공분야의 PKI 사업 추진 현황

주 관 부 처	업 무 명	인 증 기 관
행정자치부	정부전자문서유통	행정자치부
	인사, 급여, 지방채 EDI	행정자치부
	생산적 실업복지	행정자치부
병 무 청	병무종합행정	병무청, 공인 CA
국 세 청	국세 EDI	행정자치부, 공인 CA
특 허 청	특허넷시스템	행정자치부, 공인 CA
조 달 청	조달관련 문서유통(정부내)	행정자치부
국 방 부	국방조달 EDI	한국전산원
조 달 청	조달EDI(민관간)	
재정경제부	재정정보시스템	

들에게 어떠한 민원행정서비스를 전자서명을 통하여 가능하게 할지 결정을 내리고 있지 못한 상황이다.

Ⅲ. 세계 각국의 PKI 구축동향

현재 선진 각국은 전자인증체계의 구축 및 확산을 통하여 전자상거래의 주도권을 장악하고자 관련 법과 제도의 정비에 심혈을 기울이고 있다. 이를 위해 미국의 유타주에서 1995년에 세계 최초로 디지털서명법을 제정한 이래 많은 국가들이 전자서명법을 제정하거나 또는 추진중에 있다(신일순 외, 1998).[1] 미국의 경우, 최근에 총무청(GSA)을 중심으로 하여 정부내에 전자서명의 도입을 활성화하고자 하는 사업을 추진하고 있으며, 연방공무원들에게 전자서명이 내장된 스마트카드를 신분증으로 교부하고 있다(GSA, 2001).

최근에 이러한 전자적 행정서비스에서 인증기반을 범정부적으로 활용하고 있는 국가로는 호주, 영국, 대만 및 홍콩 등이 선도적이다. 특히 영국정부는 1999년 정부의 현대화 계획을 발표하면서 정부서비스의 전자적 전달을 구현하는 새로운 서비스 채널의 가능성을 보여 주었다. 영국 정부의 정보화 비전은 정부업무를 2002년에 25%, 2005년에는 50% 그리고 2008년에는 100% 전자적으로 처리하는 것이었으며, 최근에는 목표년도를 2005년으로 단축하였다(http://www.citu.gov.uk/moderngov.htm).

호주 정부 역시도 지난 1998년 5월에 공공기관들이 업무를 전자적으로 처리하는데 많은 영향을 미치는 정부의 인증활용전략인 GATEKEEPER를 발표하였으며, 인증기반을 활용하여 정부기관이 국민과 기업들에게 행정서비스를 온라인으로 제공하고 있다(http:/www.ogit.gov.au/gatekeeper/aboutgatekeeper.html). 이들 국가들의 공개키 기반구조의 구축현황 사례를 구체적으로 살펴보면 다음과 같다.

3.1 미국의 PKI 구축전략

현재 미국의 상무부 산하 국가표준업무 담당기관인 국립표준기술원(NIST: National Institute of Standard and Technology)은 정부기관의 안전한 통신을 위한 연방공개키기반구조(FPKI)를 구축하고 있으며 전자서명 인증업무를 시범운영하고 있다. 이것은 전자

1) 미국의 유타주에서 1995년 전자서명법이 제정된 이래, 1997년 독일과 말레이시아 및 1998년에 이탈리아, 싱가포르 등 많은 나라들이 전자서명법을 제정하였다. 또한 일본도 올해 이를 제정하여 2001년 4월부터 시행하고 있다. 우리나라도 이러한 세계 여러나라들의 입법동향에 따라 전자서명법을 제정하였다. 전자서명법안은 1998년 7월 입법예고를 거쳐 11월 국회에 제출되었다. 이 법안은 1998년 12월 24일 국회 본회의를 통과하였으며, 1999년 2월 5일 법률 제5792호로 공포되어, 1999년 7월 1일부터 시행되고 있다(신용섭, 1999).

〈표 2〉 FPKI 추진체계

NPR		
GITS Board		
FPKI Committee		
Project Working Group	Technical Working Group	Legal/Policy Working Group

서명키에 대한 관리 및 인증서 분배를 자동으로 수행하는 시스템으로, 인증서 취소목록 지원, 디렉토리 서비스 제공, 공개키에 대한 인증서 생성 및 열람, 확인 기능 지원 등이 포함된다.

현재 미국의 FPKI 추진체계의 최상위에는 다음 <표 2>와 같이 정부혁신위원회(NPR: National Partnership for Reinventing Government)가 위치하고 있다. 이 NPR 산하에서 정부서비스의 정보기반과 관련한 구체적인 작업을 정부정보기술위원회(GITS: Government Information Technology Service)가 수행하면서 정보기반의 신뢰성을 위한 사항은 FPKI의 운영위원회가 담당하고 있다.

이러한 FPKI운영위원회 산하에는 사업, 기술 및 법/정책 등 3개 영역의 작업그룹이 있으며, FPKI운영위원회는 GITS에 의해 주도되며 이것의 실제적인 임무를 NIST가 담당한다.

FPKI의 특징적인 측면은 FPKI의 역할이 연방기관과 관련되는 공개키기반구조의 구축에 국한되며, 국가사회를 포괄하는 공개키기반구조을 구축하고자 하는 것이 아니다라는 사실이다. 미국의 경우에는 연방기관이 민간부문이나 지방정부와 관련이 되는 범위에 있어서는 FPKI의 고려사항이 되지만, 민간부문이나 지방정부의 PKI 구축은 자율적으로 이루어져야 한다는 원칙에 따르고 있다. 이것은 이른바 FPKI의 구축을 개별 주체의 자율적 활동을 보장하는 미국의 전통에 기반을 두고 있는 것으로 해석할 수 있다.

이러한 미국의 PKI전략은 1998년에 제정된 문서작업삭제법(Paperwork Elimination Act)에 의해 행정부내의 업무처리에 보다 구체화되어 활용되게 되었다. 이러한 문서작업삭제법은 이전의 문서감축법에서 진일보하여 전자서명을 활용하여 정부내에서의 종이문서의 생산을 금지시키고 있다.

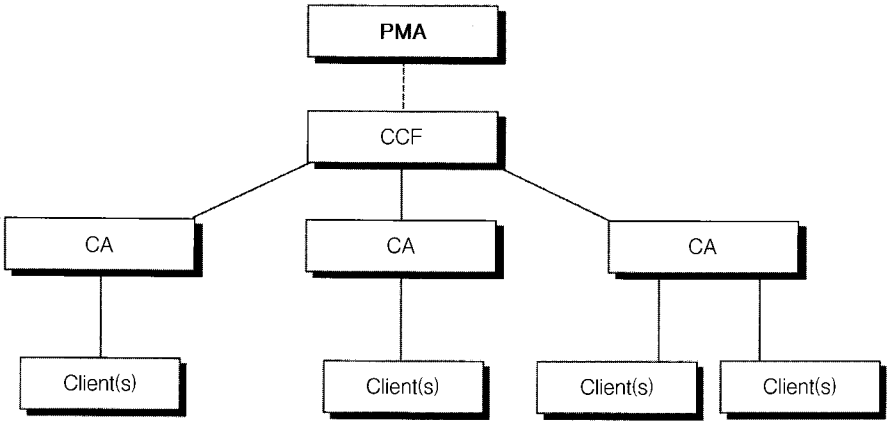
3.2 캐나다의 PKI 구축전략

1995년부터 캐나다 정부는 자료의 안전한 전송이 정부의 혁신에 있어서 중요한 주제로 부각되고 있음을 인식하고 정부혁신위원회 주도로 정부의 공개키기반구조의 구축을 시작하였다. 이것은 자료의 암호화와 복호화 및 확인 기술을 필요로 하며, 이외에도 공개키의 서비스와 관련하여 정부부처들간의 관리기반을 필요로 하는 것이었다. 이어서 캐나다 하원에서는 1998년 10월 "개인정보보호 및 전자문서에 관한 법률(Personal Information Protection and Electronic Document Act, Bill C-54)"를 입법 심의하여 제정하였다. 본 법률에서는 연방 정부가 전자문서 및 전자서명을 공문서로서 접수할 수 있으며, EU "프라이버시 지시각서" 수준의 개인정보보호 제도를 마련하여, 전자문서를 법적 증거로 채택할 수 있음을 규정하고 있다.

보다 구체적인 추진사항으로는, 1995년 9월 정보고속도로 자문위원회(Information Highway Advisory Council)에서 정보고속도로에서의 안전과 보안을 강조하기 위한 보고서에서 정부가 PKI구축에 민간부문과 협조하여 주도적인 역할을 수행할 것을 권고하였다. 따라서 1995년 12월에 6개 정부부처에서 PKI프로젝트가 시작되어 1998년 이행을 목표로 준비되었다.

현재 캐나다 정부의 PKI추진기구는 다음 <그림 2>와 같이 구성되어 있다.

- Policy Management Authority(PMA)
- Canadian Central Facility(CCF)
- Certificate Authorities(CAs); and
- Local Registration Authorities(LRAs)



<그림 2> 캐나다 정부의 PKI추진 구조

PMA는 재무장관에 의해 주도되는 범정부적인 위원회이다. PMA는 정부의 PKI추진과 관련되는 정책, 기반요구사항 및 관리에 대한 것을 결정하며, PKI운영에 있어서 정부부처 및 외부와의 연계를 위한 정책개발을 감독한다. 특히 캐나다는 이러한 PMA를 중심으로 PKI구축에 있어서 미국정부와의 협력을 강조하고 있다.

3.3 호주의 PKI 구축전략

호주 정부는 고객지향적인 대국민 전자적 행정서비스 및 정부내부 부처들과 민간기관들간의 전자적인 거래를 지원하면서 거래의 안전성을 확보할 수 있는 수단으로서 인증기술에 주목하여 왔다.

1997년 후반기에 호주 정부는 온라인 전자거래의 사용자 신원확인을 위한 국가기반의 발전을 선도해야 한다는 결정을 내렸다. 이어 정부정보기술처(OGIT: Office of Government Information Technology, 현재는 OGO로 전환됨)가 이러한 전자거래를 위한 공개키 기술(PKT: Public Key Technologies)의 사용 가능성을 위한 전략개발의 책임을 지게되었다.

OGIT는 공식적으로 1997년 10월에 GATEKEEPER 추진계획을 수립하였다. 이어서 OGIT내의 정보관리, 접근 및 정책부서(IMAP: The Information Management, Access and Policy Branch)에서 추진계획의 조정 책임을 맡게 되었다. 또한 범정부적인 협조을 얻어내기 위하여 OGIT의 주도로 자문위원회를 결성하였다. 이러한 자문위원회에는 국방부, 보건보험위원회, 국가정보경제국, 조세국 등과 OGIT가 참여하고 있다.

호주 정부는 1998년 5월 정부의 인증활용전략 GATEKEEPER를 발표하였다. GATEKEEPER는 공공기관들이 업무를 전자적으로 처리하는 데 많은 영향을 미칠 것으로 기대되고 있다. GATEKEEPER는 인증서비스의 활용자로서의 공공기관들이 상호연동성을 유지하면서도 다양한 인증기관을 평가하여 스스로에게 적합한 상대방을 선택하고 정부전체에 통일된 수준의 공신력을 달성할 수 있도록 지원하는 메커니즘을 구축하게 될 것이다.

이러한 맥락에서 OGIT는 정부부처의 온라인 트렌잭션을 최적화 할 수 있는 적절한 전략을 세우는 역할을 해왔다. 호주정부의 GATEKEEPER 추진구조는 다음 <표 3>과 같다.

GATEKEEPER의 추진은 국가정보화책임관(CGIO: Chief Government Information Officer)가 의장을 맡는 운영위원회(steering committee)가 최상위 감독기관이 되는데, 이 운영위원회는 국방부, 국세청 등 다양한 국가기관의 대표들로 구성된다. OGIT는 프로젝트의 조정 책임을 맡으며, OGIT에서 임명하는 프로젝트 관리자 아래 사용자요구, 보안, 기술 문제를 다루는 3개의 실무그룹이 구성된다. 이러한 세 그룹들 뿐만

〈표 3〉 호주 GATEKEEPER의 추진구조

Steering Committee		
OGIT Information Management, Access & Policy Branch		
OGIT Project Manager		
Business & User Requirement Working Group	Security Working Group	Technical Working Group

아니라 개인이나 민간부문들로 부터의 요청사항들도 광범위한 수준에서 수집되어 정부의 GATEKEEPER 전략에 활용되고 있다. 이러한 정책의 방향을 지원하기 위하여 호주는 지난해 3월에 전자거래법(Electronic Transaction Bill)을 제정하여 운영해 오고 있다.

3.4 대만의 PKI 구축전략

1997년 말, 대만의 연구개발평가위원회(RDEC: Research, Development, and Evaluation Committee)가 전자적 행정기관 애플리케이션이 GSN(대만 행정부가 제공하는 서비스 네트워크) 및 인터넷 프로토콜 상에서 구현되어야 함을 지적하였다.

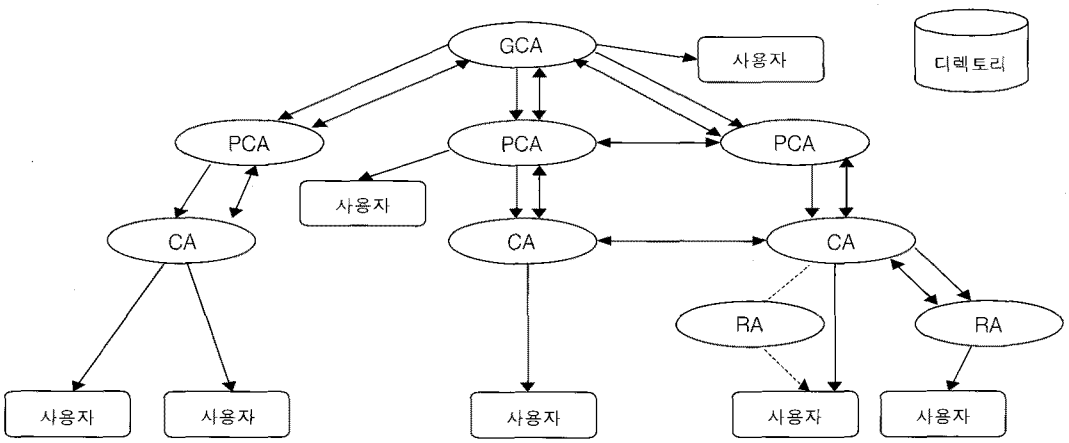
이러한 방향하에 1998년부터 대만의 PKI구축 계획이 시작되었다. RDEC는 GSN 기간망, 공개키기반구조(PKI), 안전한 메시지를 위한 메커니즘, 공무원 및 국민이 인터넷 상 행정서비스의 편익을 취할 수 있도록 하는 애플리케이션 등을 요구하였다. 이에 따라서 중화텔레콤(CHT)은 대만의 공무원 및 국민이 행정부가 제공하는 인터넷 서비스에 참여하여 향유할 수 있도록 하기 위하여, 물리적인 기간망 시스템 및 GSN이라 불리는 네트워크 서비스를 설립하였다.

중화텔레콤(CHT)은 자사의 직원 및 고객을 위한 자사 서비스 목적의 사업차원 보안 기반구조를 제공하려는 의도을 가지고 있으며, 이 서비스는 이동통신 고객을 위한 통계조사, 통신 정책 및 차세대 안전한 메시지 시스템을 위한 이동통신 기록 감시 등이 포함된다. 이처럼 중화텔레콤은 현재 대만 인증기관(Certification Authority in Chinese Taipei. GCA)을 운영하고 있다.

CHT는 인터넷 상의 전자상거래를 촉진하고 행정부 PKI 구성요소 간의 상호운용성을 유지하는 <그림 3>과 같은 혼합형 CA 모델을 제안하였다. 이 모델은 미국 NIST의 PKI 모델을 답습하고 있으며, 수직적계층구조(hierarchical)와 수평적망구조(network)을 혼합한 것이다. 이처럼 수직적계층모델을 활용함으로써 조직적 관계가 유지될 수 있으며, 수평적망 형식(network mode)을 통해 인증기관 간의 상호인증을 가능케하고 침해의 위험을 감소시킬 수 있을 것이다.

또한 CHT는 전자적 행정부 구현을 목표로 행정부 PKI의 최상위 인증기관으로 root CA 혹은 GCA를 설립할 것을 행정부에게 제안하였다. 대만의 GCA는 인터넷 상에서 신원확인이라는 근본적인 목적 하에 대만 국민에게 인증서를 발행하는 유일한 법적 인증기관이며, PKI 사용자, 고객 또는 서버 상호 간의 진정성 확인을 촉진하기 위하여 조직 및 애플리케이션 서버에게도 인증서를 발급하고 있다.

대만 정부는 1998년부터 전자적인 행정기관의 적용업무가 인터넷상에서 구현되는 프로젝트를 추진하였으며, 이의 추진기관으로 중화텔레콤을 신설하였다. 중화텔레콤이 개발한 기술 및 툴을 통해 최근 5개의 적용업무가 운용 중이거나 곧 운용될 예정이다. 이 모든 적용업무들은 인터넷 상의 국민 또는 기업의 신원을 확인하기 위해 인증서를 활용하며, 고객의 프라이버시 보호를 위해 전자봉투(Digital Envelope)을 활용하고 있다. 구체적으로는 전자적인 세금신고의 납부시스템(Tax Reporting and Payment System)이 서



〈그림 3〉 대만의 혼합형 행정부 PKI 모델

비스 되고 있다(한국정보보호센터, 1999b).

3.5 선진 각국의 시사점

이처럼 현재 여러 나라들이 전자적 민원행정서비스를 대상으로 국가적인 인증기반을 활용하여 정부서비스를 제공하고 있다. 이를 위해 각국 정부들은 공공부문에서 선도적으로 전자거래를 통한 민원행정서비스 실시와 이를 위한 전자서명을 통한 인증기반의 활용으로 인하여 국민들에게 공인인증기관을 통하여 인증서비스 보급의 기반을 마련하고 있음을 알 수 있다.

따라서 우리의 인증기반 정책은 앞에서 살펴본 선진 외국의 사례를 참조하여 추진할 필요가 있다. 즉 <표 4>에서 알 수 있는 바와 같이 미국과 호주 등은 전자정부의 주도적 정책 추진기관들과 인증기반의 구축기관이 밀접한 관련을 맺고 있다.

미국은 NPR의 정보기술을 활용한 정부혁신 정책이 IITF를 통하여 추진되면서 GITS를 연결점으로 하여 NIST가 정보보호의 역할을 수행하였다. 특히 정보기술을 활용한 정부혁신의 구체적인 실행계획에 일련번호를 부여한 후에 모든 실행계획의 책임부서와 지

〈표 4〉 각국의 PKI구축 전략 시사점

국가 / 내용	미 국	캐 나 다	호 주	대 만
추진 시기	1995년부터 시작 2000년부터 실용화	1995년부터 시작 1998년 시범사업완료	1997년부터 시작 1998년 GATEKEEPER	1998년부터 시작 1999년에 실용화
관 련 법	1995년 전자서명법 1996년문서업무삭제법	1999년 개인정보보호 및 전자문서에 관한 법률 제정	2000년 3월에 전자서명 관련 법인 Electronic Transaction Bill 제정	1996년 통신법제정
추진 기관	NPR과 연계하여 NIST가 추진함	통신보안기구 및 정책관리기구가 수행	OGO(당시는 OGIT) 전자정부와 연계	1996년 중화텔레콤을 설립하여 추진
추진 업무	총무청(GSA)에서 주관하여 연방정부 사업에 전자서명 활용	정부내부업무 활용 전자적 민원행정서비스는 아직 제공안함	MAXI프로젝트 빅토리아주 시범사업	전자적 세금납부 시스템이 활성화
특 징	정부혁신 작업과 연계하여 수행	보안을 강조 미국 사례를 따라감	암호정책과 연계 외주전략 활용	정부주도로 강력한 PKI정책 추진함

원기관 및 완료일을 지정하여 범정부적인 추진체계를 갖추고 진행하고 있다.

호주의 경우에는 OGIT가 중심적인 역할을 하고 있으며, 캐나다에서는 IHAC가 초기에 주도적인 역할을 수행하여 효율적인 정책의 수립과 집행이 가능하였다. 특히 캐나다는 미국과의 인접국가로서 국가PKI 구축에 있어서 미국과 연계그룹을 결성하여 협력하고 있다.

현재 국가PKI기반을 구축하는데 있어서 가장 중요한 측면은 민간부문과의 협력일 것이다. 캐나다 정부의 PKI는 기본적으로 민간기업인 Entrust Technologies Inc의 제품을 바탕으로 진행되고 있다. 호주의 경우에는 빅토리아주 정보화를 NEC에 외주(Outsourcing)하고 있는 실정이다. 따라서 국가적 인증기반의 구축과 같이 기술진보가 급격한 분야에서는 민간기업과의 효율적인 유대전략이 우선적으로 고려되어야 한다.

Ⅳ. 우리나라의 공공부문 PKI 구축동향

4.1 관련법규의 동향

공공부문에 인증기반의 도입과 관련하여 법과 제도적인 측면에 최근에 많은 변화가 있어왔다. 그 가운데서 현재 가장 중요하다고 여겨지는 것이 전자서명법의 제정과 "전자정부구현을위한행정업무등의전자화촉진에관한법률"(이하 전자정부법)의 제정일 것이다. 이들의 핵심 내용을 요약하여 살펴보면 다음과 같다.

4.1.1 전자서명법의 제정

우리나라도 전자상거래에 대응하고자 세계 여러나라들의 입법동향에 따라 전자서명법을 제정하였다. 전자서명법의 주요 내용은 다음과 같다.

우선 전자거래의 활성화를 위하여 공인인증기관이 인증한 전자서명에 대하여 법적 효력을 부여하였다(법 제3조). 이것은 공인인증기관이 인증한 전자서명을 법령이 정하는 서명 또는 기명날인으로 간주하는 것을 의미한다. 따라서 공인인증기관의 인증을 받은 전자서명으로 서명한 전자문서의 경우 당해 전자서명이 당해 전자문서의 명의자의 서명 또는 기명날인이고, 당해 전자문서가 전자서명된 후 그 내용이 변경되지 아니하였다고 추정할 수 있게 되었다.

정보통신부 장관이 공인인증기관을 지정하도록 하였다(법 제4조, 제5조). 전자서명 인증업무에 대한 공신력을 제고하기 위하여 정부가 지정하는 공인인증기관 제도를 도입하였다. 구체적으로는 기술적, 재정적 능력 등 일정한 요건을 갖춘 국가기관, 지방자치단체 또는 법인을 공인인증기관으로 정보통신부장관이 지정할 수 있도록 하며 인증기관의 임·직원에 대한 결격사유 등을 규정하였다.

인증업무의 지속성 및 적정성 보장을 위한 공인인증기관 관리제도를 도입하였다(법 제6조 내지 제10조). 인증업무 수행에 필요한 인증실무준칙의 신고, 인증기관의 업무 휴·폐지 등 인증기관 운영에 관한 사항을 규정하였다. 또한 공인인증기관의 적정한 업무수행을 보장하기 위하여 지정취소, 업무조사 등에 관한 사항을 규정하였다.

인증업무의 신뢰성 확보를 위한 인증서 발급을 규정하였다(법 제15조 내지 제18조). 인증업무에 대한 신뢰성 확보를 위하여 인증서에 포함할 사항을 명확히 하고 인증서의 발급·효력정지·폐지 등에 관한 사항을 규정하였다.

인증업무의 수행과 관련한 개인정보의 보호에 대한 규정을 제시하였다(법 제24조 및 제32조). 인증업무에 필요한 개인정보의 수집 및 사용의 제한, 누설금지 등 개인정보 보호에 관한 사항을 규정하고 이를 위반한 자를 처벌하도록 하였다.

인증기관의 책임과 의무 등을 명시하였다(법 제19조, 제21조, 제22조 및 제26조). 이 법은 인증기관으로 하여금 인증서의 변조방지대책 강구, 안전성·신뢰성 있는 인증관리체계 운영, 전자서명키의 안전한 관리, 인증관련 기록의 안전한 관리 등의 의무 등을 규정하였다. 나아가 인증기관이 법적 의무 불이행 등

으로 인하여 이용자에게 손해를 주었을 때에는 배상하도록 하였다.

전자서명 및 전자문서의 보호에 대하여 규정하였다(법 제23조 및 31조). 전자서명 및 전자문서의 안전·신뢰성 확보를 위하여 타인의 명의를 도용하여 허위로 인증서를 발급받는 행위, 타인의 전자서명키 도용행위 등을 금지하고 이를 위반한 자를 처벌하도록 하였다.

전자서명 인증관리센터의 설립과 운영에 대하여 규정하였다(법 제25조). 전자서명의 안전한 이용환경 조성과 인증기관의 효율적인 관리를 위하여 한국정보보호센터로 하여금 인증기관의 전자서명키에 대한 인증업무 등을 수행하는 인증관리센터를 운영하도록 하였다.

4.1.2 전자정부법안에서의 전자관인의 내용

행정자치부는 2000년 10월 3일 정부업무의 전자적 처리에 관한 원칙과 절차 등을 규정한 '전자정부 구현을 위한 법률안'을 마련하여 입법예고하고, 11월 20일에 정기국회에 상정하였다. 이러한 법률(안)은 국회에서 의원입법(안)과 절충과정을 거쳐서, 2001년 2월 28일 "전자정부구현을위한행정업무등의전자화촉진에 관한법률"(이하 전자정부법) 제6439호로 공포되어 2001년 7월 1일부터 법 시행에 들어가게 되었다.

이 법안은 지금까지 종이문서로만 제출하도록 규정된 각종 법령조문을 보완해 컴퓨터를 통한 전자결재의 법적 근거를 마련하고, 부처간에 행정정보를 공동이용 하도록 하는 등의 내용을 담고 있다. 그러나 공공부문에서는 전자서명이 아닌 전자관인에 의하여 인증을 하도록 하고 있다. 전자정부법에 의하면 제2조 용어의 정의에서 다음과 같이 전자관인을 명기하였다.

"전자관인"이라 함은 전자문서를 작성한 행정기관, 보조기관 또는 보좌기관의 신원과 전자문서의 변경여부를 확인할 수 있는 정보로서 당해 문서에 고유한 것을 말한다.

이어서 제20조에서 전자공문서에는 전자관인을 사용하도록 하였다. 그러므로 행정자치부는 본인확인을 위한 전자서명과는 별도로 공문서의 전자관인을 계속해서 사용할 의도를 갖고 있는 것으로 파악할 수 있다.

4.2 PKI 구축 관련 부처의 입장

현재 PKI의 구축과 관련하여 쟁점이 되는 사항은 여러 가지가 있을 수 있으나 가장 중요한 문제는 정부와 민간 영역을 분리할 것인가하는 점이다. 이 문제에 있어서 정보통신부와 행정자치부는 다음과 같이 다른 견해를 나타내고 있다.

4.2.1 정보통신부의 입장

정보통신부의 기본 시각은 별도의 정부 PKI를 구축할 필요가 없으며 국가 단일의 PKI체계가 구축되어야 한다는 것이다. 즉 전자서명법에서 규정하는 인증관리체계내로 정부의 PKI도 포함되어야 한다고

〈표 5〉 공개키 기반구조에 관한 정보통신부의 입장

<table>
<tr><td colspan="5">최상위인증기관
(한국정보보호진흥원)</td></tr>
<tr><td>공인인증기관
(행정분야: GCC)</td><td>공인인증기관
(전자상거래)</td><td>공인인증기관
(금융분야)</td><td>공인인증기관
(증권분야)</td><td>공인인증기관
(기타분야)</td></tr>
<tr><td>등록기관
(구청 등)</td><td>등록기관
(기타)</td><td>등록기관
(은행 등)</td><td>등록기관
(증권사 등)</td><td>등록기관
(기타)</td></tr>
<tr><td colspan="5">기업 또는 국민인 사용자들
(공인인증기관 또는 등록기관으로부터 인증서 발급)</td></tr>
</table>

보는 것이다. 이러한 구도에 따른다면 정부전산정보관리소(GCC)는 별도 정부 PKI의 최상위 인증기관이 아니라 정보보호진흥원을 최상위 인증기관으로 하는 국가 PKI에 포함되는 정부 영역의 공인인증기관이 된다.

<표 5>는 정보통신부가 구상하는 국가 PKI의 구성을 나타내고 있으며 실제로 행정분야를 제외한 나머지 분야가 먼저 공인인증기관으로 지정되어 업무를 수행하여 왔다.

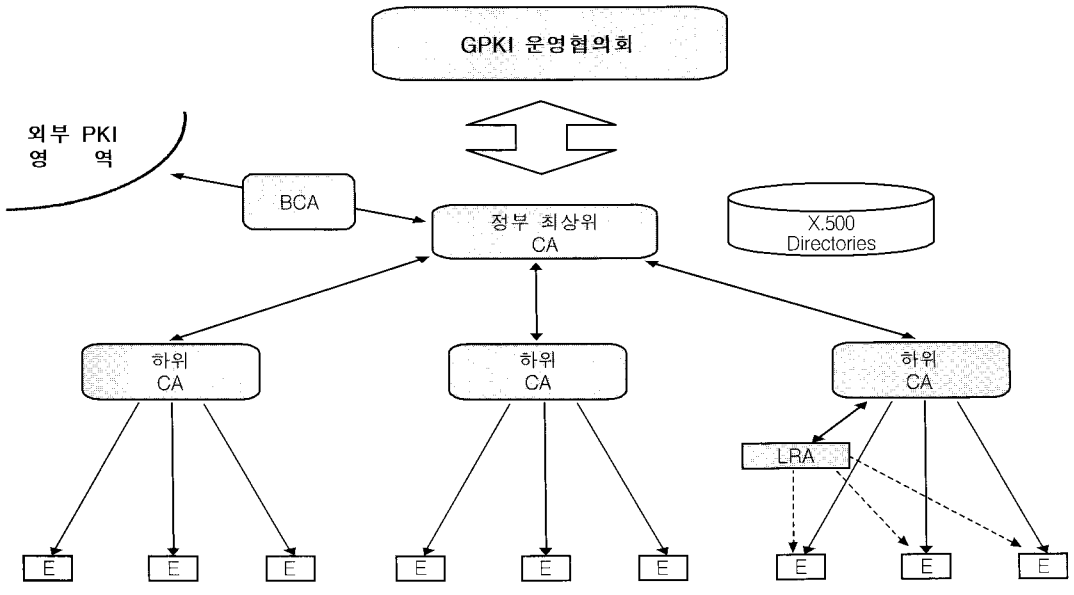
4.2.2 행정자치부의 입장

행정자치부는 정보통신부가 추진한 전자서명법은 민간부문 위주로 되어있기 때문에 행정부문의 인증은 전자정부법을 통해 하여야 한다는 입장이다. 이러한 관점에서 기존의 행정부 고유기능 등을 고려할 때 국가 PKI(NPKI)의 구성으로 <그림 4>를 제시하고 있다.

즉 민간부문의 PKI 구축은 정보통신부, 한국정보보호진흥원(KISA)을 중심으로 추진함과 동시에, 정부공개키기반구조(GPKI)의 암호체계와 적용분야 및 범위가 민간분야와는 대별되는 부분이 있으므로 GPKI 운영협의회를 중심으로 관계 부처간의 공동 연구와 노력이 필요하다는 것이다.

구체적으로 인증서 발급정책에 있어 정부주도의 GPKI의 관리범위는 민간의 시장에 대한 부정적 파급효과(시장규모 축소 등)를 최소화하는 범위 내에서 정부기관의 인증만을 관리하고, 민원인 및 민간기업에 대한 인증관리는 공인인증기관이 전담할 수 있도록 하는 정책 조정자의 역할을 수행해야만 한다는 것이다.

또한 민·관 인증관리체계의 상호연계는 정부전자서명인증관리센터(GCC)를 GPKI의 대민관련 정부기관의 인증을 전담·관리하는 Bridge CA로 지정·운영하여 국가 최상위 인증기관(KISA)과의 신뢰경로를 제공하도록 하는 것이 현 행정기능상 효율적인 방안이라고 주장한다. 행정자치부는 이러한 국가 PKI 관리체계의 구현을 통해 모든 정부 내·외부기관과 국민들이 공유할 수 있는 범 국가적 차원의 정보보호체계가 완성될 수 있을 것으로 보고 있다. 그러나 이것은 국민들에게 여러 개의 전자서명을 요구하는 결과가 초래될 수도 있다. 물론 행정자치부는 모든 상용화된 전자서명을 받아주는 호환성을 갖추겠다고 하나 구체적인 추진실적은 없는 실정이다.



○ E(End-Entity) : 최종 GPKI 사용자

<그림 4> 행정자치부의 국가 전자서명 인증기반 구성방안

V. 정책제안

5.1 인증기반에 기초한 e-행정서비스의 시행

현재 전자정부의 추진정책에서 가장 중요한 사항은 전자정부의 구현에 따르는 파급효과를 국민들에게 널리 알려서 전자정부 추진정책에 대한 국민적인 공감대를 얻어내는 일이다. 이를 위해서는 내부의 행정혁신도 중요하지만 그 보다는 e-행정서비스를 확대하여 국민들에게 전자정부의 구현을 체감할 수 있게 하는 것이 그 무엇보다 시급한 과제이다. 따라서 전자서명의 활성화를 통해 인증기반에 기초한 전자적인 대민서비스의 관점에서 전자정부의 구현정책이 추진되어야 한다. 이를 위해서는 다음과 같은 문제점들이 우선적으로 해결되어야 한다.

첫째, 민원인이 최소한의 서류제출로 한 번에 민원을 처리할 수 있는 서비스체계를 구축하여야 한다. 이러한 서비스는 발상을 전환하여 정부의 측면이 아니라 국민들의 민원행정서비스 불편사항에서 출발하여 방법을 모색하여야 한다. 이를 위해서 주민망과 부동산망과의 연계를 통하여 주민등록 등·초본 등 단순확인을 위한 첨부서류와 토지대장, 도시계획확인원, 재산세완납증명 등 부동산종합정보시스템을 통하여 확인할 수 있는 첨부서류들은 폐지되어야 한다. 이를 위하여 전산망의 연계에서 우선적으로 인증기반이 구축되어야 한다.

둘째, 앞으로는 정보화정책의 입안과 시행에 이르는 전 과정에 전자서명에 기초한 인증기반 정책이 포함되어야 한다. 현재 정부에서는 시군구 행정종합정보화 및 부서별 정보화추진 등 수 많은 정책이 추진되고 있다. 그러나 이러한 정부부처 내의 정보화 정책에서 조차도 인증기반을 통한 민원인 확인이나 내용인증 등이 활용되지 못하고 있는 것이 현실이다. 현재 행정자치부에 의해서 도입되고 있는 무인민원발급기(KIOSK)에서 인증을 통한 신원확인이 이루어지지 못하고 있는 것이 대표적인 사례가 될 것이다. 현재 행정자치부는 시범운영중인 KIOSK에서 신원확인의 수단으로 전자서명보다는 주민카드의 지문을 활용할 예정이다. 따라서 이 경우에는 모든 국민들이 가상공간에서의 신원확인 수단인 전자서명을 전자적인 민원행정서비스에서 활용할 수 없는 결과가 초래되는 것이다.

셋째, 이제 정보화정책의 궁극적인 목적이 국가 개혁의 수단이라는 점이 강조되어야 한다. 이러한 맥락에서 전자정부의 구현과 정보공동활용 및 인증기반 구축을 연계시키고, 정부내 정보공동활용 추진 조직을 구성할 때, 전자서명의 활용이 시작단계에서부터 이루어져야 한다.

이를 위해서는 전자서명의 도입이 단순한 기술의 도입이나 정부부처간의 전산망 연결이나 자료의 공동이용이 아니라, 위로부터의 제도 개혁과 함께 아래로부터의 내부 조직문화의 변화를 일으킬 수 있는 방법으로 양면적인 정부개혁 전략으로 추진되어야 한다. 보다 구체적으로는 전자서명의 활용을 통한 정부정보서비스 혁신방안 또는 정부업무처리 혁신방안 등이 제정되고 이러한 혁신 방안에 따르는 정부업무에서의 전자서명활용 기본계획이 수립되어야 한다.

5.2 통합된 범정부적 추진체제의 구축

정부는 현재의 부처이기주의를 극복하고 국가적인 인증기반의 구축을 단순히 전자상거래의 안전성을 지원하기 위한 기술개발의 시각에서 탈피하여 전자정부의 구현전략의 일환으로서 거시적인 국가정보화의 관점에서 정책을 수립하여야 한다.

현재 국가적인 인증기반의 구축에 있어 국가사회정보화의 주무부처인 정보통신부와 전자정부 구현을 추진하는 행정자치부간에는 서로 추진정책의 차이를 나타내고 있다. 정부통신부는 별도의 정부 공개키기반구조(PKI)를 구축할 필요가 없으며 전자서명법에서 규정하는 인증관리체계내로 정부PKI가 포함되어야 한다고 주장하고 있다. 이에 행정자치부는 전자서명법은 민간위주로 되어 있으므로 행정부문의 인증은 사무관리규정을 통하여 별도의 정부PKI에 의해 추진

되어야 한다는 입장이다.

그러나 여기에서 중요한 것은 어느 부처가 인증기반과 관련하여 어떠한 대상 범위내에서 얼마만큼의 권한을 갖느냐하는 것이 아닐 것이다. 보다 중요한 것은 정부의 행정서비스를 제공받는 국민의 시각에서 정책을 수립하여야 한다는 사실이다. 따라서 국민의 입장에서 볼 때, 현재 정보통신부가 추진한 영역별 공인인증기관의 지정이나 행정자치부가 추진하고 있는 민간과 정부부문의 구분 등은 모두 시민들에게 불편만을 초래할 뿐이다.

그러므로 이제부터 정부내에서 전자정부의 구현전략으로 전자적인 행정서비스를 인증기반에 기초하여 제공할 필요성이 있으며, 영역과 대상의 구분이 없는 통합된 서비스를 제공하여야 한다.

참 고 문 헌

김경섭, "전자서명을 이용한 e-행정서비스 발전방향," 행정과전산, 22(3), 행정자치부 전산정보관리소, 2000.

김용훈, "전자정부구현을 위한 호주의 인증기반 구축 전략과 시사점," 정보화동향, 5(14): 13-21, 한국전산원, 1998.

류석상. "인터넷 웹을 통한 대국민 서비스 해외동향," 정보화동향, 5(13): 1-9, 한국전산원, 1998.

박인재, "정부전자관인인증기반(GPKI) 구축정책 및 추진방향," 디지털행정, 정부전산정보관리소, 2001년 9월.

신용섭, "전자서명법에 따른 인증제도체계 정책방향," 제4회 정보보호심포지움논문집, 서울: 한국정보보호센터, 1999.

신일순 외, 전자서명 및 인증제도, 서울: 정보통신정책연구원, 1998.

전자정부특별위원회, "전자정부추진 구현동향 및 향후 추진계획," 2001년 5월.

정명선, "인터넷을 통한 민원처리 현황과 선결과제," 정보화동향, 5(17): 1-10, 한국전산원, 1998.

정원섭, "전자서명법 제정 이후의 정책과제," 정보화동향분석, 6(2): 11-28. 한국전산원, 1999.

한국전산원, 21세기 전자정부 비전과 실천전략에 관한 연구, 1999.

한국전산원, 공공부문 e비즈니스 도입분야 발굴 및 도입방안 연구, 2000.

한국정보보호센터, 전자정부에서의 정보보호 대책연구, 1999년 12월.

한국정보보호센터, "대만의 PKI 구축현황 및 전략," 1999년 6월.

행정자치부, "증명민원제도 개혁방안," 1999년 7월 2일.

행정자치부, "전자민원시스템구축 기본계획," 2000. 5

행정자치부, "민원서비스 혁신(G4C)시스템 구축 과제 제안서," 2001년 8월.

GITS, Access America, Government Information Technology Services, 1997(http://www.gits.fed.gov/htm/access.htm).

U.S General Service Administration, "ACES-Access Certificate for Electronic Services," http://www.gsa.gov. 2001.

Office of Government Information Technology, Management of Government Information as a National Strategic Resource. August, 1997.

http://www.citu.gov.uk/moderngov.htm

http://www.gsa.gov/aces/aces.html

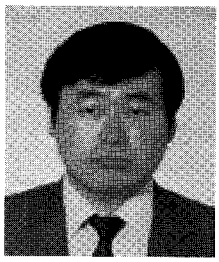
http://www.homeminwon.go.kr

http://www.info.gov.hk/itbb/content/index.htm

http://www.ogit.gov.au/gatekeeper/aboutgatekeeper.html

http://www.samsungfire.com/

◐ 저 자 소 개 ◑



정 충 식 (cschung@star.ks.ac.kr)

고려대학교 사회학과를 졸업하고, 고려대학교 경영대학원에서 경영정보전공으로 석사학위를, 성균관대학교 행정대학원에서 컴퓨터감사전공으로 석사학위를 취득하고, 성균관대학교 대학원에서 행정학박사학위를 취득하였다. NCR Korea, 안권회계법인 경영자문부, 씨티은행 전산부, 감사부, 법규부 등에서 근무하였다. 씨티은행에서는 4년간 EDP Auditor로 정보시스템 감사의 실무를 경험하였다. 용인전문대학 사무자동화과 조교수를 거쳐서 현재 경성대학교 행정학과 교수로 근무하고 있다. 주요 관심분야는 전자정부론, 정보시스템 감사론 및 정보통신정책 등이다.