通信情報保護學會誌
第7卷 第2號, 1997. 6

공개키 기반구조에 관한 고찰

A Study on the Public Key Infrastructure

김 지 연*, 박 성 준*

요 약

현재 정보통신기술과 인터넷의 확산으로 가상공간상에서의 상거래인 전자상거래가 활발히 전개되고 있다. 이미 선진국에서는 전자상거래를 국가경쟁력 강화의 일환으로 국가전략차원에서 추진중에 있으며 우리나라에서도 정보통신부가 전자상거래 활성화를 위해 한국정보보호센터를 중심으로 전자상거래 정보보호기술 개발 및 관련 법·제도 개선을 추진중에 있다. 이러한 법·제도의 핵심은 바로 전자인증제도의 확립이다. 전자인증제도는 전자상거래 정보보호기술의 핵심기술인 전자서명기술의 안전한 운영을 의미한다. 이러한 전자서명기술의 안전한 운영을 위해 필요한 기반기술이 공개키 기반구조이다. 즉, 공개키 기반구조는 전자인증제도의 실체화된 정보보호망이다. 전자상거래를 통해 국가경쟁력을 확보하기 위해서는 무엇보다도 전자인증제도가 확립되어야 하며 이것의 실체화인 공개키 기반구조가 구축되어야 할 것이다.

1. 서 론

통신과 컴퓨터 기술이 비약적으로 발전하면서 현재 우리가 일상적으로 행하던 은행업무, 쇼핑 등의 거래를 전자적으로 행하는 전자거래가 이미 일부에서 시행되고 있고, 이러한 추세는 전자 공간에서 전자적 방식에 따라 이루어지는 상거래인 전자상거래의 자연스러운 출현이라고 생각된다. 특히 인터넷의 급속한 확산에 의한 인터넷상의 전자상거래가 활발히 전개되고 있는 실정이다.

특히 미 행정부는 인터넷을 21세기 미국 무역의 주요 통로로 삼는 등 인터넷을 통한 전자상거래를 활성화하기 위해 전자상거래 육성을 위한 방안을 모색중에 있으며 우리 나라도 이에 발맞추어 현재 정보통신부, 재정경제원, 통상산업부 등 정부 부처는 물론 민간부문에서도 전자상거래의 실현을 추진하고 있다. 미국의 시장조사업체인 주피터 커뮤니케이션스가 조사한 바에 따르면 전자상거래 시장은 지난해 10억달러에서 오는 2000년에는 70억달러로 성장할 것이라 한다. 그러므로 전자상거래는 국가경쟁력 강화의 중요한 요소로 고려되어야 한다.

국가경쟁력 강화의 일환으로 전자상거래를 활성화하기 위해서는 먼저 전자상거래의 안전

* 한국정보보호센터

성·신뢰성을 확보해야 한다. 현재 국내에서는 전자상거래의 정보보호 문제로 인하여 전자상거래를 활성화하는 데 많은 한계점을 노출하고 있으며 이를 해결하기 위하여 관련 부처에서 현행 법/제도 정비 필요성을 인식하여 많은 논의가 이루어지고 있는 실정이다.

전자상거래의 안전성·신뢰성을 확보하는 시작은 전자인증제도의 정립이라고 말할 수 있다. 전자인증제도란 가상공간상의 전자문서, 전자거래 등 관련 전자업무에서의 당사자의 신분확인 기능, 전자업무 내용의 정보보호 및 무결성 기능, 전자행위에 대한 부인봉쇄 기능 등 전자업무의 중요 인증과 관련하여 신뢰할 만한 제 3자(인증기관)가 확인 및 증명해 주는 제도이다. 전자인증제도의 핵심은 전자상거래의 안전성과 신뢰성을 확보하기 위한 핵심기술인 전자서명기술의 안전한 운영을 의미한다.

전자서명기술은 공개키 암호알고리즘으로 비밀키와 공개키가 사용된다. 공개키 암호알고리즘에서 사용되는 비밀키가 전자서명을 생성하는 생성키가 되고 공개키가 전자서명을 검증하는 검증키 역할을 한다. 그러므로 전자서명기술의 안전한 운영은 서명키(공개키암호알고리즘의 비밀키)와 검증키(공개키암호알고리즘의 공개키)의 안전한 운영에 달려있으며 서명키의 안전한 운영은 비밀키의 안전한 보관을 말하며 검증키의 안전한 운영은 공개키의 안전한 관리를 의미한다. 공개키는 공개키암호알고리즘을 사용하는 사람 누구에게나 공개되는 정보이므로 비밀키의 보관보다 얼핏 보기에는 매우 단순한 것 같지만 실제 구현시 공개키를 공개하는 데에 사용되는 메커니즘(공개키 디렉토리, 게시판 등)이 그 자체적으로 안전하지 않아 누구나 쉽게 접근하여 정보를 변경할 수 있으므로 공개키의 무결성을 보장해야 하는 문제가 발생한다. 즉, 공개키는 공개된 정보이므로 어떻게 공개키 위·변조 문제를 해결하는가 하는 공개키 인증문제로 귀착된다.

이러한 공개키의 인증문제를 해결하기 위해 나온 것이 바로 공개키 기반구조(PKI: Public Key Infrastructure)이다.

다시 말해, 전자상거래의 안전성과 신뢰성을 확보하기 위해서는 전자인증제도가 요구되며 전자인증제도는 바로 전자서명기술의 안전한 운영을 의미하고 다시 전자서명기술에 사용되는 공개키암호알고리즘의 비밀키의 기밀성과 공개키의 무결성을 보장해야 하며 이를 해결하고자 하는 것이 바로 공개키 기반구조이다. 즉, 공개키 기반구조 구축는 전자인증제도를 실체화하는 것이다.

본 고에서는 전자인증제도의 실체화인 공개키 기반구조에 대해 알아보고 각 국의 그 구축현황을 살펴보도록 하겠다.

2. 용어 설명

본 장에서는 우선 PKI에 관련되는 용어를 정리하도록 한다.

◇ 인증기관(CA: Certification Authority)
인증 정책에 따라 인증서를 생성하거나 취소하는 객체(entity)로 모든 인증기관들은 자신의 키쌍을 생성하고 선택적으로 사용자의 키를 생성할 수 있다.

◇ 인증서(certificate)
인증 기관의 비밀키로 암호화되어 위조할 수 없는 사용자의 유일한 이름, 사용자의 공개키 및 기타 정보로 이루어진 문서로 인증서를 발행한 CA의 인증 정책도 포함한다. X⟨⟨Y⟩⟩는 인증 기관 X가 사용자 또는 하위 인증 기관 Y에게 발행한 인증서를 의미한다.

◇ 인증정책(certification policy)
인증정책은 CA가 작동하는 메커니즘과

사용되는 암호 알고리즘과 서명 알고리즘, 최소 키 크기, 인증서 유효의 최대 길이, 인증서 취소 목록 갱신의 최대 기간, 인증서를 발행하기 위해 사용자의 신분을 확인하는 메커니즘 등을 기술한다. 정책은 객체 식별자(OID : Object Identifier)로 명명되고 정책의 OID는 그 정책하에 발행된 모든 인증서내(extension 영역)에 포함된다.

◇ 보안 정책(security policy)
보안 서비스 및 기능의 제공을 관리하는 보안 기관에 의한 규칙들이다.

◇ 도메인(domain)
공통적인 보안 정책을 구현하거나 밀접하게 관련있는 명명공간(namespace)내에 사용자들에 대해 인증서를 발행해주는 CA들이 논리적으로 그룹화되어 있는 것을 도메인이라 한다.

◇ 고유 이름(Distinguished Name)
PKI내의 객체들을 유일하게 구별하는 이름으로 보통 X.500 명명 방식[1]을 따른다.

◇ 상호인증서(cross-certificate)
한 CA가 다른 CA를 신뢰하여 그 CA에 인증서를 발행할 때 그 인증서를 상호인증서라 한다. 한 CA를 신뢰하는 모든 객체는 그 CA가 상호 인증한 CA에 의해서 발행된 모든 인증서를 신뢰한다.

◇ 인증 경로(certification path)
경로상의 최종 객체에 대한 공개키를 얻기 위한 인증서들의 정렬된 순서로 A→B는 A로부터 B로의 인증 경로를 나타낸다. A→B는 A의 인증서로 시작되어 B의 인증서로 끝나는 고리의 형태인 CAA〈〈A〉〉 · · · CAB〈〈B〉〉로 구성된다.

◇ 디렉토리(directory)
객체에 대한 정보 저장소로 사용자들로 하여금 그 정보에 접근할 수 있는 서비스를 제공한다.

◇ 신뢰(trust)
일반적으로 한 실체는 다른 실체가 자신이 기대한 바와 같이 행동을 하리라고 가정할 수 있을 때 실체는 다른 실체를 신뢰한다고 말할 수 있다. 이러한 신뢰는 일부 특정 기능에만 적용될 수 있다. 인증 프레임워크에서 이 신뢰의 주요 역할은 인증하려는 실체와 인증 기관간의 관계를 기술하는 것으로 인증하려는 실체는 인증 기관이 유효하고 신뢰할만한 인증서를 생성한다고 확신할 수 있어야 한다.

3. 공개키 기반구조(PKI: Public Key Infrastructure)

공개키 암호기술은 보안이 필요한 응용 분야에 널리 사용된다. 공개키 암호 기술에서는 비밀키와 공개키를 이용한다. 비밀키는 그 소유자만이 알고 있고 공개키는 공개된다. 공개키를 공개하는 문제는 비밀키를 소유자만이 알도록 하는 것보다 얼핏 보기에 매우 단순한 것 같지만 실제 구현시 공개키를 공개하는 데에 사용되는 메커니즘(공개키 디렉토리, 게시판 등)이 자체적으로 안전하지 않아 누구나 쉽게 접근하여 정보를 변경할 수 있으므로 공개키의 위·변조 문제를 야기시킨다. 다음과 같은 경우를 생각해 보자. A가 B에게 문서를 비밀리 보내고자 하는 경우 A는 B의 공개키로 그 문서를 암호화할 것이다. 그런데 제 3자인 C가 공개키 디렉토리에 접근하여 B의 공개키를 자신의 공개키로 바꾸어 버리고 전송되는 암호문을 중간에 가로채 버린다면 A가

원래 문서를 보내려고 했던 B가 아닌 C가 그 문서를 읽게 될 것이다.

이렇게 공개된 공개키가 위·변조되지 않았음을 보장하는 문제 즉, 공개키의 무결성을 보장하기 위해 등장한 것이 공개키 기반구조(PKI:Public Key Infrastructure)이다. 공개키 기반구조에서는 공개키를 공개하는 대신 공개키와 그 공개키의 소유자를 연결하여 주는 인증서(certificate)를 공개한다. 인증서는 신뢰할 수 있는 제 3자(인증기관)의 서명문이므로 신뢰 객체가 아닌 사람은 그 문서의 내용을 변경할 수 없도록 한다.

3.1 PKI의 정의

공개키 기반구조에 대한 정의는 다음과 같이 여러 가지로 생각할 수 있다.

◇ 사용자의 공개키를 인증해주는 인증 기관들의 네트워크
◇ 모르는 사람과의 비밀 통신을 가능하게 하는 암호학적 키와 인증서의 배달 시스템
◇ 공개키의 인증서를 이용해 공개키들을 자동적으로 관리해주는 기반구조
◇ 공개키 인증서를 발행하고 그에 대한 접근을 제공하는 인증서 관리 기반구조

이를 통합하여 정리하면 공개키 기반 구조란 정보시스템 보안, 전자 상거래, 안전한 통신 등의 여러 응용분야에서 인증서(certificate)의 사용을 용이하도록 하는 정책, 수단, 도구등을 수립하고 제공하는 객체들의 네트워크이다.

3.2 PKI가 제공하는 서비스

PKI는 다음의 5가지 기본 보안 서비스를 제공한다.

◇ 프라이버시 : 정보의 기밀성을 유지한다.
◇ 접근 제어 : 선택된 수신자만이 정보에 접근하도록 허락한다.
◇ 무결성 : 정보가 전송중에 변경되지 않았음을 보장한다.
◇ 인증 : 정보의 원천지를 보장한다.
◇ 부인 봉쇄 : 정보가 송신자에 의해 전송되었음을 보장한다.

3.3 PKI 응용 분야

PKI는 공개키 암호기술이 사용되는 모든 분야의 하나의 기반기술로서 반드시 필요한 기반구조이다. 그러므로 그 응용분야도 무궁무진하다. [표 1]은 인증 기관과 서비스 받을 객체들에 따른 PKI의 다양한 응용분야들이다.[2]

[표 1] PKI의 응용 분야

인증 기관	서비스 받을(인증될) 객체들	응용 분야
재정 협회들, 은행들	상인들, 카드 소지자들	안전한 지불 거래들
은 행	계좌 소지자들	홈뱅킹, 대불/저당 절차들 등
연방 정부	국민들	납세를 위한 소득신고 제출, 사회보장제도에 대한 문의와 그에 대한 응답 등
연방 정부	기업들	재무상태 보고서 제출

우체국	우체국의 고객들	전자적 소인, 전자적 등기 메일 등
의료 보험 회사, 건강 관리 조직들, 의료 연합회	의사들, 병원들	환자 기록에의 접근, 치료 계획의 제출, 안전한 치료 인가와 수행된 서비스에 대한 상환
법 기관들과 법원	판사들, 변호사들, 법률가들	법원 선서와 다른 법 문서의 제출
인터넷 서비스 제공자들	ISP 서비스들을 이용하는 기업들	dial-up 계정 접근
소프트웨어 사업들	소프트웨어 모듈들	다운로드할 소프트웨어가 바이러스등에 안전함을 보장
	고객들	전자적 소프트웨어 전송과 제공

※ ISP(Internet Service Provider) : 인터넷 서비스 제공자

3.4 PKI 모델

3.4.1 PKI 구성 요소

PKI를 구성하는 최소 객체들은 등록기관(RA:Registration Authority), 인증기관, 디렉토리, 사용자이다.

1) 인증기관

공개키기반구조를 구성하는 가장 핵심 객체로 그 역할 및 기능에 따라 계층적으로 구성되며 여러 명칭으로 불리운다. 아래 세기관 모두를 통틀어 인증기관이라 한다.

◇ 정책승인기관(PAA: Policy Approving Authority)
PKI 전반에 사용되는 정책을 생성하고 PKI구축의 루트 CA로의 역할을 하며 다음을 수행한다.
- PKI 전반에 사용되는 정책과 절차를 생성하여 수립한다.
- 하위 기관들의 정책 준수 상태 및 적정성을 감사한다.
- PKI내·외에서의 상호 인증을 위한 정책을 수립하고 그를 승인한다.
- 하위 기관의 공개키를 인증하고 인증서, 인증서취소목록 등을 관리한다.

◇ 정책인증기관(PCA: Policy Certification Authority)
PAA 아래 계층으로 자신의 도메인내의 사용자와 인증기관(CA)이 따라야 할 정책을 수립하고 인증기관의 공개키를 인증하고 인증서, 인증서취소목록 등을 관리한다.

◇ 인증기관(CA: Certification Authority)
PCA 아래 계층으로 다음과 같은 기능을 수행한다.
- 사용자의 공개키 인증서를 발행하고 또 필요에 따라 취소한다.
- 사용자에게 자신의 공개키와 상위 기관의 공개키를 전달한다.
- 등록기관의 요청에 의해 인증서를 발

행하고 되돌린다.
- 상호 인증서를 발행한다.
- 최소한의 정책 책임을 진다.
- 인증서와 그 소유자 정보를 관리하는 데이터베이스를 관리한다.
- 인증서, 인증서취소목록, 감사 파일을 보관한다.

2) 등록기관(RA)

인증기관과 멀리 떨어져 있는 사용자들을 위해 인증기관과 사용자사이에 등록기관을 두어 인증기관대신 사용자들의 인증서 신청시 그들의 신분과 소속을 확인하는 기능을 수행한다. 사용자들의 신분을 확인한 후, 등록기관은 인증서 요청에 서명을 한 후 인증기관에게 제출한다. 인증기관은 등록기관의 서명을 확인한 후 사용자의 인증서를 발행한 후 등록기관에게 되돌리거나 사용자에게 직접 전달한다. RA는 조직 등록기관(ORA: Organizational Registration Authority)라고도 불리운다.

3) 디렉토리

인증서와 사용자 관련 정보, 상호 인증서쌍 및 인증서취소목록등을 저장 및 검색하는 장소로 응용에 따라 이를 위한 서버를 설치하거나 인증기관에서 관리한다. 디렉토리를 관리하는 서버(인증기관)는 DAP(Directory Access Protocol)나 LDAP(Lightweight DAP)[3]를 이용하여 X.500 디렉토리 서비스를 제공한다. 인증서와 상호 인증서 쌍은 유효기간이 경과된 후에도 서명 검증의 응용을 위해 일정기간동안 디렉토리에 저장된다.

4) 사용자

PKI내의 사용자는 사람뿐만 아니라 사람이 이용하는 시스템 모두를 의미한다. 다음의 기능을 수행한다.
- 자신의 비밀키/공개키 쌍을 생성할 수 있어야 한다.
- 공개키 인증서를 요청하고 획득할 수 있어야 한다.
- 전자 서명을 생성 및 검증할 수 있어야 한다.
- 특정 사용자에 대한 인증서를 획득하고 그 상태를 결정할 수 있어야 한다.
- 인증 경로를 해석할 수 있어야 한다.
- 디렉토리를 이용하여 자신의 인증서를 다른 사용자에게 제공할 수 있어야 한다.
- 인증서 취소 목록을 해석할 수 있어야 한다.
- 비밀키가 분실 또는 손상되거나 자신의 정보가 변했을 때(예: 조직의 탈퇴) 인증서 취소를 요청할 수 있어야 한다.

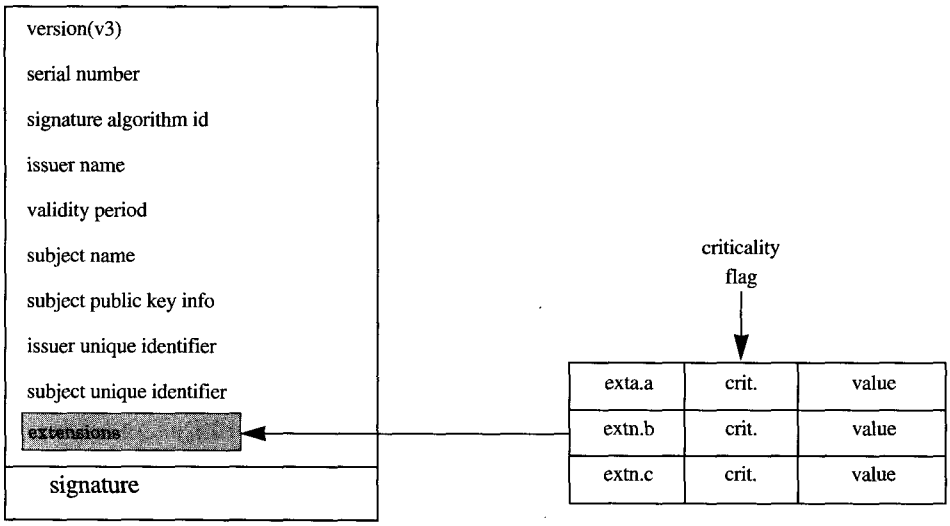
3.4.2 PKI의 관리 대상

PKI에서 관리해야 할 대상은 크게 인증서와 인증서 취소목록, 상호 인증서쌍이 있다.

1) 인증서

인증서는 사용자의 신분과 공개키를 연결해주는 문서로 인증기관의 비밀키로 전자서명하여 생성된다. 다시 말해 이것은 사용자의 공개키가 실제로 사용자의 것임을 증명한다. PKI에서 인증서의 발행대상은 인증기관과 사용자, 서버등으로 인증기관에게는 상위 인증기관이 인증기관의 적법성을 증명하기 위해 발행하고 사용자와 서버에게는 사용자의 신원, 서버 등의 적법성을 증명하기 위해 인증기관에서 발행한다. 인증서의 형식은 1988년에 ITU-T가 X.509 초기 버전을 공표하고 1993년에 버전 2를 공표했으며 1995년 이후로는 ISO/IEC 9594-8의 문서와 동일시되어 공동 개발되어왔다. 현재에는 X.509 버전 3까

지 공표되었고 인증서의 extensions 영역에 대한 개정이 진행되고 있다. X.509v3의 형식은 [그림 1]과 같다.



version	X.509의 버전으로 0은 버전1, 1은 버전2, 2는 버전3를 의미함
serial number	발행자가 생성한 각각의 확인서에 대한 유일 식별자
signature algorithm id	발행자가 확인서를 서명하는 데에 사용한 알고리즘을 기입
issuer name	확인서를 서명하고 생성한 발행자의 id로 X.500 명명 방식을 따름
validity period	확인서가 사용될 수 있는 시작 시간과 끝 시간을 기입하는 것으로 시간과 날짜(UTCT 형식)로 표현됨
subject name	확인서를 받는 공개키의 소유주의 id로 X.500 명명 방식을 따름
subject public key info	사용자의 공개키와 공개키에 대한 정보(알고리즘과 파라미터)를 기입
issuer unique identifier	(선택) 버전2이상에서 사용되는 것으로 발행자의 부가적인 정보를 포함함
subject unique identifier	(선택) 버전2이상에서 사용되는 것으로 객체의 부가적인 정보를 포함함
extensions	(선택) 인증 정책등 여러 가지 사항을 포함함
signature	앞의 목록들에 대한 서명값

[그림 1] X.509v3 인증서 형식

2) 상호인증서쌍(cross-certification pair)

한 도메인이나 서로 다른 도메인의 인증기관들사이에 발행하는 인증서로 두가지 형태가 있다. 이것은 쌍을 이뤄 각 인증기관(X)의 엔트리로 디렉토리에서 관리된다.

◇ 순방(forward) 인증서 : 인증기관 X에 대해 다른 인증기관에서 생성한 인증서

◇ 역방(reverse) 인증서 : 인증기관 X가 다른 인증기관에게 생성한 인증서

상호 인증서를 사용함으로써 같은 도메인내에서는 인증 경로를 단축할 수 있고 서로 다른 도메인내의 사용자들에게는 그들간의 안전한 통신 수단을 제공할 수 있다.

3) 인증서 취소 목록 (CRL: Certificate Revocation List)

인증서는 인증된 공개키에 해당하는 비밀키가 노출된다든가 그 공개키의 소유자가 다른 도메인으로 옮기는 경우 등 여러 가지 이유로 유효기간이 만기되기 전에 그 효력이 상실될 수 있다. 인증기관은 이렇게 효력이 상실된 인증서들에 대한 목록을 생성해 PKI내에서 관리한다. 인증서 취소목록은 X.509v2 형식을 따르는 추세로 [그림 2]와 같다. CRL은 형식에서 볼 수 있듯이 주기적으로 생성된다. 이 주기는 인증 정책에 명시된다.

signature	algorithm identifier	CRL을 서명할 알고리즘
	parameters	필요한 파라미터들
issuer	CRL 발행자 이름으로 X.500 명명방식을 따름	
this update	UTCTime	갱신일에 대한 타임스탬프
next update	UTCTime	다음 갱신일
revoked certificates	취소된 인증서들의 목록	
CRL extention(선택)	위 영역외에 부가적인 정보를 선택적으로 기술함	
issuer' s signature		

serial number	취소된 인증서의 일련번호로 발행자에 대해 유일함
revocation date	인증서 취소일로 UTCTime으로 표현됨
CRL entry extension(선택)	취소 이유등 부가적인 정보를 기술함

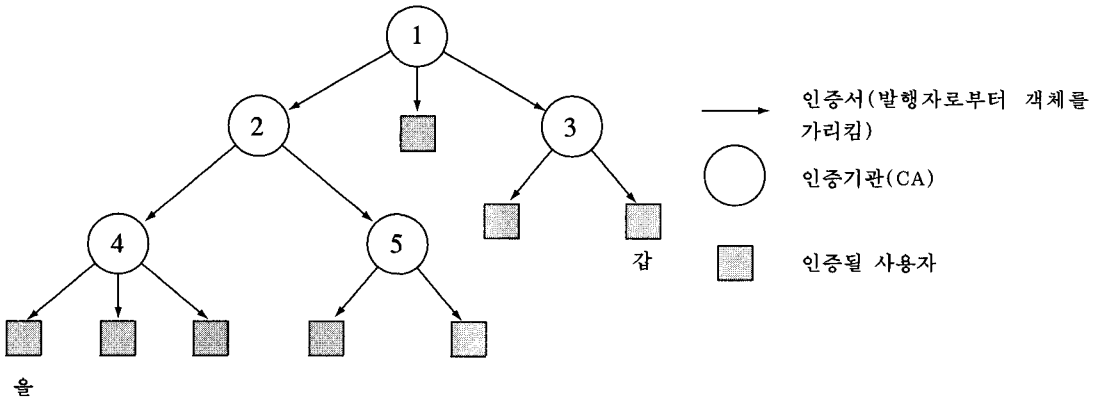
[그림 2] X.509v2 CRL 형식

3.4.3 PKI 구성

PKI에서 신뢰는 인증 경로를 통해 전달된다. 전자 서명을 검증할 때를 생각해 보자. 전자서명의 검증자는 자신이 신뢰하는 인증 기관의 공개키만을 알고 있으므로 그 인증 기관의 공개키를 이용하여 인증 경로를 검증함으로써 서명자의 공개키를 획득한다. 이렇게 획득한 공개키는 무결성이 보장된다. 검증자는 무결성이 보장된 공개키를 이용하여 서명을 검증할 수 있는 것이다. 이러한 신뢰가 인증 경로를 통해 어떻게 전달되는 지에 따라 PKI는 다음 두가지 형태로 구성될 수 있다.

1) 계층적 구성

인증기관들이 하위 CA에게 인증서를 발행하는 "루트" CA(PAA)아래에 계층적으로 배열되어 있는 구성으로 인증기관들은 자신의 아래 CA들에게 인증서들을 발행한다. 계층적으로 구성된 PKI에서 루트 CA의 공개키는 모든 사람에게 알려져 있어 사용자들의 인증서는 루트 CA로에서 자신이 신뢰하는 인증기관까지의 인증 경로를 검증함으로써 검증된다. [그림 3]에서 갑이 을의 전자서명을 검증한다고 하자. 우선 갑은 을의 공개키를 획득해야 한다. 갑은 CA1과 CA3를 신뢰하고 을은 CA1과 CA4를 신뢰한다. 을은 갑에서 서명문과 함께 인증기관 CA1에서 CA4까지의 인증경로를 전송한다. 갑은 을이 자신과 같은 도메인에 있음을 확인한 후 자신이 알고있는 CA1의 공개키를 이용해 CA1에서 CA4까지의 인증경로를 검증하여 을의 공개키를 획득한 후 서명문을 검증한다.

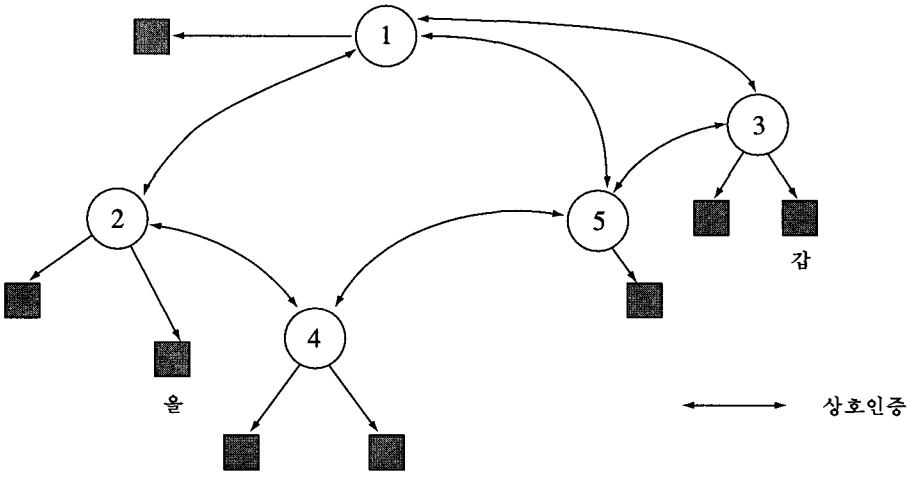


[그림 3] 계층적 구성

2) 네트워크 구성

인증기관이 각각의 도메인을 형성하여 독립적으로 존재하는 구성으로 CA들이 서로를 상호 인증하여 서로에게 인증서를 발행한다. 네트워크로 구성된 PKI의 사용자는 자신의 인증서를 발행한(즉, 자신이 신뢰하는) 인증 기관의 공개키만를 알고 있다. [그림 4]와 같은 구성에서 갑이 을의 서명문을 검증하고자 한다고 생각하자. 갑은 CA3를 신뢰하고 을은 CA2만을 신뢰한다. 을에서 갑으로의 인증 경로는 여

러개가 존재하므로 이중에서 가장 짧은 인증 경로를 찾는 탐색과정이 필요하다. 가장 짧은 인증 경로는 CA3〈〈CA1〉〉CA1〈〈CA2〉〉CA2〈〈을〉〉이다. 갑은 이 인증경로를 이용해 을의 공개키를 획득하고 그를 이용해 전자서명을 검증한다. 네트워크로 구성되었을 경우에는 인증 경로가 여러개 존재할 수 있으므로 이중 짧은 경로를 찾는 것이 중요 관건이다.



[그림 4] 네트워크 구성

PKI의 두가지 구성은 서로 장·단점을 가지고 있다. [표 2]은 그 장·단점을 비교한 것이다.

실제 PKI 구축시에는 기본적으로는 계층적 구조를 구성하면서 효율성과 다른 PKI와의 통신을 위해 한 도메인내 또는 다른 도메인내의 인증기관들사이에 네트워크 구조를 허락한다.

[표 2] 계층적 구성과 네트워크 구성의 장·단점

PKI 구성	장 점	단 점
계층적	• 많은 조직의 관리 구조가 계층적이므로 자연스럽게 부합된다. • 계층적 디렉토리 이름과 잘 부합된다. • 인증 경로 탐색 전략이 간단하다. • 도메인내의 모든 사용자는 루트의 공개키를 알고 있고 인증하고자 하는 사용자는 루트로부터 자신이 신뢰하	• 각 국가별 PKI가 구축될 경우 이것을 모두 통합하는 하나의 루트 CA가 존재한다는 것은 현실과 맞지 않다. • PKI가 상업적인 분야에 이용될 때는 관계는 계층적일 필요가 없다. • 루트 비밀키의 노출은 끔찍한 상황을 야기하고 복구하기 위해서는 PKI내의 모든 사용자에게 새로운 공개키의 안전한 분배가 필요하다.

	는 인증기관까지의 인증 경로를 제공할 수 있으므로 인증서를 검증하고자 하는 다른 사용자는 루트의 공개키를 알고있으므로 그 경로를 검증할 수 있다.	
네트워크	• 유연성을 가지며 사업 기관의 상호 신뢰 관계를 잘 반영한다. • 사용자는 자신의 인증서를 발행한 CA를 신뢰해야 하고 이것이 모든 신뢰 관계의 기본이 되는 것이 자연스럽다. • 조직적으로는 멀리 떨어져 있지만 그 속의 사용자들이 높은 신뢰감으로 함께 일할 경우 CA들이 서로 직접적으로 상호 인증될 수 있다. • 자신의 사용자들이 빈번히 통신하는 CA들의 직접적 상호인증을 허락함으로써 인증 경로 처리 부담을 감소한다. • 만약 CA의 비밀키가 손상되어 복구할 경우에 CA는 새로운 공개키를 자신의 사용자들에게만 안전하게 분배하면 된다.	• 인증 경로 탐색 전략이 계층적 구성에 비해 훨씬 복잡하다. • 사용자는 PKI의 다른 사용자에게 단일 인증 경로를 제공할 수 없다. 왜냐하면 네트워크형에서의 두 사용자 간의 인증경로는 여러개가 존재하기 때문이다.

3.4.4 PKI 관리

PKI의 관리는 PAA에서 수립하는 인증 정책에 의해 관리된다. 본 절에서는 운영의 효율성을 위해 관리해야 할 도메인의 분류방법과 인증 정책에 관해 살펴보도록 한다.

1) 도메인의 분류

사용자들을 PKI내의 PCA와 CA들과 어떻게 연결할 것인가의 문제로 다음과 같은 방법이 있다.

◇ COI(Communities of Interest)

사용자들이 빈번히 수행하는 작업에 따라 사용자 그룹을 조직하여 그 사용자들과 자주 통신하는 사용자들은 물리적으로 떨어져 있더라도 기반구조내에 가깝에 위치되어야 한다. 사용자들은 자신과 자주 통신하는 사용자의 인증서를 미리 저장함으로써 효율성을 증대시킨다.

◇ 조직적 분류

기존의 조직 계층과 유사하게 조직화함으로써 기존의 관리 구조를 따른다.

◇ 신뢰 수준(assurance level)에 따른 분류

신뢰수준에 따른 분류는 3개 또는 4개의 보안 정책이 기관들의 요구조건들을 만

족하는 데에 충분하다는 생각에 기반을 두고 사용자들이 필요로 하는 인증 신뢰 수준에 따라 사용자들을 분류한다.

◇ 혼합 분류

위의 세가지 방법을 혼합한 것으로 위 세가지 방법은 단일 그룹이나 형태가 일정한 그룹에는 적합할 지 모르나 활동이 다양한 사람들의 그룹에는 적합하지 않다. 위 세가지 방법을 혼합하여 도메인을 분류하는 것이 실제적이다.

2) 인증 정책

인증 정책은 인증시행성명서(CPS: Certificate Practice Statement)로 공개되며 인증서를 발행할 때 인증기관이 사용하는 시스템과 작동 절차들을 자세히 설명하고 있다. PKI내의 각 CA들은 인증시행성명서에 의해 작동하고 CA의 CPS는 PAA에의해 승인받아야 한다. 그리고 인증시행성명서는 CSOR(Computer Security Objects Register)와 같은 적당한 저장소에 공개되어야 한다. CPS는 다음을 포함하는 CA 작동을 설명한다. 그리고 또한 CPS에는 PKI내의 객체들을 유일하게 식별할 수 있는 고유 이름을 명명하는 방식도 기술된다.

◇ 백업(backyp) 절차들
◇ 기록 보관 절차들
◇ 작동 임원의 제한과 자질들
◇ CA 작동자의 기능적 역할들
◇ CA에 제공될 물리적 보호
◇ CA 암호학적 모듈에 대한 140-1 수준의 요구조건들
◇ CA 비밀키에 대한 접근 제어
◇ RA 작동 절차들
◇ 사용자나 다른 CA들을 인증하기 위한 개인식별 조건들
◇ 키를 생성, 안전한 관리, 취소, 보관하기 위해 인증서 소유자에게 요구되는 절차들

4. 공개키 기반구조 구축 현황

현재 PKI는 미국, 캐나다, 유럽을 중심으로 여러 가지 응용분야에 이용되고 있으나 그 외의 국가나 인터넷에서는 전자상거래를 위한 인증기관구축중에 있다. 본 장에서는 그 현황을 살펴보도록 하겠다.

4.1 미국

◇ 공적부문

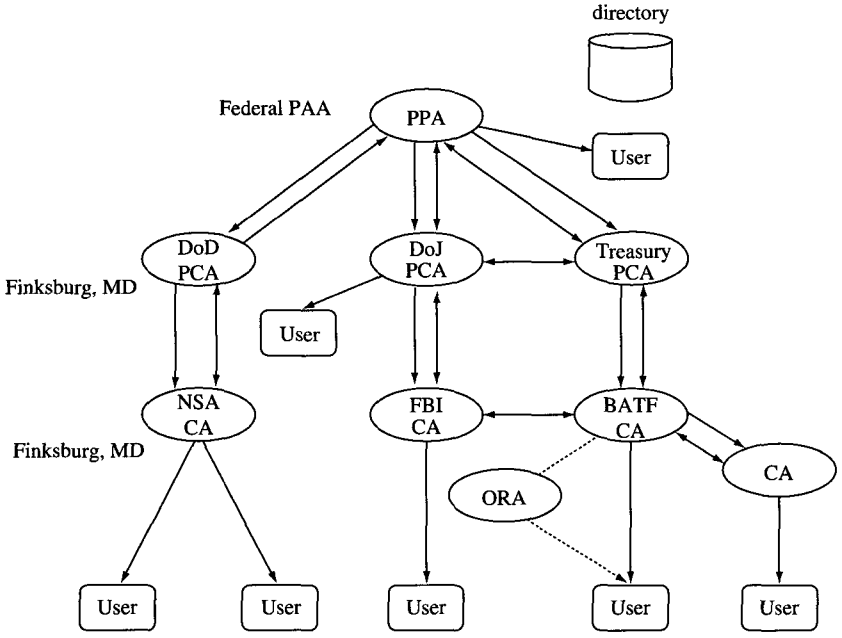
- 연방 부문

DSS(Digital Signature Standard)가 표준으로 채택되면서 미국 정부내의 연방기관들은 전자서명기술의 역할을 개발하고자 NIST(National Institute of Standards and Technology)에 그 연구를 요청해서 NIST를 중심으로 연구가 이루어지고 있다. NIST의 PKI 작업그룹(working group)에서는 기술적 명세서와 CA 작동 개념 및 다른 PKI와의 상호연동성(interoperability)에 대한 연구가 꾸준히 이루어지고 있다.[5][6][7][8]

미국의 연방 PKI(FPKI: Federal PKI)는 국방성의 Multiple Information System Security Initiative(MISSI) type2로 구현된 것을 모체로 구현될 것이다. FPKI의 PAA는 총무처(GSA: General Service Administration)가 관리하고 연방 기관들에 의해 구성된 Security Infrastructure Program Management Office(SI-PMO)가 관리할 것이다. 또한 SI-PMO는 다른 PKI와의 상호연동에도 책임을 질 것이며 PAA의 위치도 결정할 것이다. 제안된 FPKI는 구성은 [그

림 5]와 같다.

X.509v3 인증서와 X.509v2의 인증서 취소목록 형식을 지원하고 X.500 디렉토리 서비스를 제공한다. 사용되는 전자서명 알고리즘은 DSA(Digital Standard Algorithm)이다.



[그림 5] 제안된 FPKI

- 비연방부문

연방외의 기관이지만 연방기관과 유사한 정부기관인 미국 우정공사(USPS: United States Postal Service)는 전자상거래(ECS: Electronic Commerce Service)를 위한 CA 구축중에 있다. 이를 통해 고객에게 인증서 등록, 검색, 취소 서비스를 제공하고자 한다. 그러나 이 서비스가 유료이고 USPS가 정부기관이 아니므로 FPKI에서는 ECS CA가 배제된다. NIST에서는 연방PKI와 비연방PKI와의 상호연동성을 연구중에 있다.

◇ 민간부문

'95년 RSA 데이터 시큐리티사가 인증서의 발행에 관한 서비스와 시스템을 판매하는 자회사로 설립된 Verisign사와 '96년초에 [사이버트러스트(cybertrust)]라는 서비스 명칭으로 이 분야 진입을 발표한 GTE사를 중심으로 전자상거래분야의 인증기관시스템 개발·서비스 중에 있다.

4.2 유럽

◇ ICE-TEL(Interworking Public Key Certification Infrastructure for Europe) 프

로젝트

유럽의 13개국의 17개 산·학·연 단체가 참여한 프로젝트로 1995년 12월부터 1997년 11월까지 2년동안 수행되며 2단계로 나누어 수립된다.[9]

첫 번째 단계는 1996년 6월 18일에 작동되는 것으로 X.509v1 인증서와 인증서 취소목록 형식을 따르며 기본 모델은 PEM을 따른다. 두 번째 단계는 X.509v3 인증서와 X.509v2 인증서 취소목록 형식을 따르며 PEM과 PGP 모델을 통합한 신뢰모델을 따른다. 이 두 번째 단계는 1996년 10월부터 작동된다.

최상위 루트인 ICE-TEL-CA는 유럽 전역의 산·학·연 단체에 인증서비스를 제공한다. ICE-TEL-CA는 다음을 인증한다.

- ICE-TEL 프로젝트의 각 국가 PCA들
- TERENA 조직의 각 국가 PCA들
- 유럽 연구 프로젝트를 위한 PCA들
- WWW 서버를 위한 서버 인증서들

ICE-TEL-CA는 미국의 FPKI의 PAA와는 달리 최종 사용자를 인증하지 않는다. FPKI와 마찬가지고 ICE-TEL-CA를 중심으로 계층적으로 구성되며 상호 인증을 허락한다. 사용되는 서명 알고리즘은 RSA이다.

4.3 영국

◇ 공적부문

영국의 우체국공사에서는 [PATHWAY]라는 프로젝트를 통해 영국전국에 있는 2만의 우체국을 연결하는 네트워크의 전자화, 신서비스의 도입등으로 우편사업의 활성화를 지향하고 있다. 1997년에는 200국에서 운용을 개시하며 '99년에는 전 우체국에 적용할 예정이다. IC카드를 2천만매 발행하여 암호키 관리 등 인증업무도 행하고 있으며 흥미로운 것은 사회보험청이 이 시스템에 함께 타는 형태로 업무 합리화를 도모하고 있다는 것이다.

4.4 캐나다

◇ 공공부문

- CSE(Communications Security Establishment)의 GOC PKI(Government of Canada PKI)

CSE 주도의 GOC PKI 프로젝트라 불리는 캐나다의 PKI는 모르는 사람들끼리의 안전한 전자 거래와 비밀 정보의 교환을 가능하도록 하는 암호학적 키와 인증서를 운반하는 시스템으로 정의된다. 이 프로젝트를 통해 캐나다 정부는 모든 국민들이 안심하고 정부 각부서에 공개키 네트워크를 통해 중요한 정보를 비밀리 전송하도록 하며 전자서명의 사용를 용이하도록 한다. 이 프로젝트에는 캐나다정부의 많은 부서가 관련되어 있으며 인증기관들은 계층구조를 이룬다. GOC PKI의 정책관리기구(PMA: Policy Management Aurthority)는 국가재정위원회사무국(Treasury Board Secretariat)가 의장인 각부처 위원회이며 여기에서 CA가 인증서를 발행하는데 따르는 정책과 시행등을 승인할 것이다. 이 GOC PKI 프로젝트는 1998년 후반에 작동할 계획이며 이를 위해서 Nortel에서 개발한 보안 기구인 Entrust를 채택했다. 1996년 9월에 이미 캐나다의 국방부, 외무부등 많은 부처에 Entrust가 보급되었다.

◇ 민간부문

- Certicom사
캐나다의 정보보안회사의 하나인 Certicom 주식회사는 PKI의 요소를 개발할 미국 통상부의 NIST에 의한 initiative에 참여해 PKI의 기술적 구성요소를 위한 최소한의 상호연동적 명세서를 개발하고 있고 이 결과는 PKI 개발 측면에서 활동하고 있는 그 외의 회사들(AT&T, Verisign, Nortel 등)과 적당한 표준단체와 연방 정부 기관들 그리고 산업 조직들과 공유될 것이다. Certicom은 큰 규모의 PKI를 제공하기 위해 ECC(Elliptic Curve Cryptosystem)가 유용하리라 기대하여 개발중에 있다.

4.5 일본

◇ 공적부문
일본의 통산성에서는 전자상거래실증 실험에서 실제 이용자를 포함한 실험이 행해지고 있으며 그 가운데서 인증기관도 가동하고 있다. 그리고 우정성, 법무성, 대장성 등 관련 기관에서 인증 비즈니스의 방향, 프레임 짜기 등을 검토하기 시작하고 있다.

◇ 민간부문
Verisign사와 일본 지부인 일본Verisign사가 1996년 2월에 설립되었고 1997년 4월에 GTE, BUG, NRI, NTT 이동통신망의 4사를 중심으로 금융관계를 포함한 다수의 기업이 참가하여 설립된 사이버트러스트사를 중심으로 인증기관에 대한 연구가 진행중이다. 일본의 219개 회사로 구성된 일본 전자상거래 진흥 협회(ECOM:Electronic Commerce Promotion Council of Japan)에서는 인증기관에 대한 가이드라인을 공개했다.

4.6 호주

호주에서는 Standard Australia에서 "Strategies for the implementation of a Public Key Authentication Framework(PKAF) in Australia"라는 이름으로 표준화 추진중에 있으며 호주 정부와 기관들사이의 연합 기업인 Distributed System Technology Center(DSTC)에서 PKI 모델과 구현상의 문제점을 연구중에 있다. 그리고 DSTC는 인터넷 표준기구인 Internet Engineering Task Force(IETF)에도 참여하여 활동하고 있다.

5. 결 론

현재 국내에서는 전자상거래를 국가경쟁력 강화의 일환으로 관계 부처 및 민간 부문에서 독립적으로 추진하고 있다. 그러나 전자상거래가 활성화되기 위해서는 전자상거래의 안전성·신뢰성 확보를 위한 정보보호기술이 뒷받침되어야 한다. 이러한 정보보호기술 중 핵심기술이 바로 전자서명기술이다. 전자서명된 문서가 전자상거래에 이용되기 위해서는 그 법적 효력이 인정되어야 한다. 전자인증제도는 전자문서, 전자서명, 전자인증 등의 법적 효력을 정의하고 전자상거래의 안전성 및 신뢰성을 보증해 준다. 그리고 공개키 기반구조는 이러한 전자인증제도의 실체화된 정보보호망인 것이다.

본 고에서는 공개키 기반구조와 그 구축현황에 대해 살펴보았다. 공개키 기반구조 구축은 주로 국가차원으로 이루어지고 있으며 민간부문에서는 전자상거래 분야에 관심이 있는 민간단체가 인터넷상에 공개키 기반구조의 핵심 구성요소인 인증기관을 설립하는 것으로

진행되고 있다.

국내에서도 데이콤과 한국통신 그리고 금융계에서 독자적인 인증기관을 구축하려는 움직임이 있다. 그리고 한국정보보호센터는 전자인증체계 정립 및 공개키 기반구조 구축을 위한 기술개발을 담당하고 있으며 가장 기반이 되는 전자서명기술을 '96년도에 개발 완료하였고 '97년 7월 중에 한국전자통신연구원과 공동으로 한국 표준 전자서명방식을 제안할 예정이다. 특히 전자상거래 활성화를 위하여 개발된 전자서명기술을 올 하반기에 국내 관련 산업체에 기술 전수할 예정이며 이와 병행하여 인증기관에 필요한 관련 정보보호기술도 올해 안에 실용화할 예정이다.

21세기 국가경쟁력의 가장 핵심요소가 될 전자상거래의 활성화를 위해서는 전자인증제도의 수립과 그 실체화 기술인 공개키 기반구조를 구축하고 공개키 기반구조의 핵심 구성요소이며 국내에 설립될 인증기관들을 통합할 수 있는 국가차원의 인증기관의 설립이 시급하다고 사료된다.

참 고 문 헌

[1] CCITT X.500, The Directory:Overview of concepts, Models and Services, CCITT, 1992

[2] Mark Greene, Role of Certificate Authority in Internet Commerce, 1997.5

[3] RFC 1487, X.500 Lightweight Directory Access Protocol, http://ds.internic.net/rfc/rfc1487.txt

[4] The 1994 Mitre PKI Study Final Report, NIST, http://csrc.ncsl.nist.gov/pki/mitre.ps

[5] Federal Public Key Infrastructure Technical specification Part A : Requirements, NIST, 1996.1.31, http://csrc.ncsl.nist.gov/pki/require5.ps

[6] Federal Public Key Infrastructure Technical specification Part B : Technical Security Policy, NIST, 1996.1.24, http://csrc.ncsl.nist.gov/pki/tspolicy.ps

[7] Federal Public Key Infrastructure Technical specification Part C : Concept of Operations, NIST, 1996.2.12, http://csrc.ncsl.nist.gov/pki/conops.ps

[8] Federal Public Key Infrastructure Technical specification Part D : Interoperablity Profile, NIST, 1995.9.27, http://csrc.ncsl.nist.gov/pki/cross.ps

[9] ICE-TEL, Architecture and General Specifications of the Public Key Infrastructure, 1996.9, http://www.darmstadt.gmd.de/ice-tel/deliverables/download/D1-Architecture.rtf

[10] Standards Australia, Strategies for the implementation of a Public Key Authentication Framework(PKAF) in Australia, SAA MP75-1996

[11] Robin Whittle, Public Key Authentication Framework: Tutorial, 1996.6, http://www.ozemail.com.au/~firstpr/crypto/pkaftute.htm

[12] GOC Public Key Infrastructure, http://www.cse.dnd.ca/cse/english/gov.html

[13] Petra Gloeckner, Basic Security Policy to be employed in the ICE-TEL project, 1996.6.18

[14] The DSTC Public Key Infrastructure, http://www.dstc.qut.edu.au/MSU/projects/pki

[15] IOS/IEC 9594-8:1995| ITU-T Recommendation X.509(1993E), Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1993.11

[16] W.E.Burr, N.A.Nazario, W.T.Polk, A PROPOSED FEDERAL PKI USING X.509 V3 CERTIFICATES

[17] S.Kent, Privacy Enhancement for InternetElectronic Mail, Part II: Certificate-Based key Management, IETF FCC 1422, Feb. 1993.

□ 著者紹介

김 지 연

1995년 2월 성균관대 정보공학과 졸업(공학사)
1997년 2월 성균관대 대학원 정보공학과 졸업(공학석사)
1997년 ~ 현재 한국정보보호센터 연구개발부 연구원

※ 주관심분야 : 암호 프로토콜, 정보이론, 전자자본 시스템

박 성 준

1983년 2월 한양대학교 수학과 졸업(이학사)
1985년 2월 한양대학교 대학원 수학과 졸업(이학석사)
1996년 2월 성균관대 대학원 정보공학과 졸업(공학박사)
1985년 1월 ~ 1994년 3월 한국전통신연구소 부호기술부 선임연구원
1996년 4월 ~ 현재 한국정보보호센터 연구개발부 책임연구원

※ 주관심분야 : 암호이론, 계산이론, 정보이론