通信情報保護學會誌
第8卷 第3號, 1998. 9

해외 PKI 구축 동향 및 사례

신 홍 식*, 이 종 일*

요 약

전자상거래 분야에의 PKI의 성공적인 도입은 기술적 문제의 해결 뿐만 아니라 법 제도적인 불확실성을 어떻게 해결하느냐에 크게 좌우된다. 우리나라의 전자 서명 관련 법제화가 전자상거래 활동이나 전자적 방법의 활성화가 안전하게 발전적인 방향으로 나아가고자 하는 취지에서 세계 주요 나라의 PKI 동향을 고찰하여 본다. PKI의 설계는 정부 국가 기관 등의 공공 섹터나 전자상거래 등 산업계 등의 적용 분야에 따라 각기 다른 인증 정책과 인증 책임의 한계 등 적절한 고려 사항을 충족하여야 한다. 이러한 관점에서 미국, 캐나다, 유럽, 호주 등 세계 주요 국가 활동을 소개하고 특히 비교적 잘 구현된 사례로 전자 카드 지불 수단인 SET 아키텍처와 미 연방 정부의 PKI의 최근 사례를 소개하였다. 대규모의 공개키 시스템을 실현하는 데 가장 중요한 두 가지 문제는 어떻게 적절한 인증 경로를 찾느냐 하는 문제와 찾고 난 다음 어떻게 검증하느냐 하는 문제이다. 경로 찾기는 디렉토리 서비스 등 필요한 정보 Retrieval 서비스만 주어진다면 자동화될 수 있다. 경로 확인은 주의 깊게 정확한 알고리듬을 따라야 하며 또한 안전하게 구현되어야 한다..

1. PKI 개요

공개키 인증서와 디지털 서명은 이전에 서로 모르는 당사자들 간에 신뢰 관계를 수립하게 하고 또한 가능하다면 안전하고 암호화된 통신을 하게 한다. 미국의 연방 정부는 이러한 기술로부터 크게 혜택을 받을 수 있는 대규모의 사용자 집단이라 할 수 있다. PKI는 커다란 사용자 집단간에 인증을 광범위하게 사용할 수 있게 하는데 필요하다.

PKI (Public Key Infrastructure)란 안전한 금융 전자 거래와 미지의 거래 당사자 간에도 민감한 정보를 교환할 수 있게 하는 암호 키 및 인증서 배달 시스템이다. 간단히 얘기해서 공개키 암호화 기술에서 사용되는 공개키 값들을 공표 (Publish) 하기 위한 시스템이다. 여기에는 모든 PKI들에 공통적인 두 가지 기본 오퍼레이션이 있다. 인증 (Certification)이란 하나의 공개키 값을 어떤 개인이나 기관 또는 다른 어떤 정보 - 허가 (permission) 또는 신용 (credential) 등-에 결부시키는 프로세스이다. 검증 (Validation)이란 하나의 인증 행위가 아직 유효 (Valid)한지를 확인 (Verify)하는 프로세스이다. 이 두 가지 오퍼레이션을 어떻게 구현하느냐 하는 방법이 여러 가지 다른 PKI를 정의하는 기본적인 특성이

* 신테크

된다. PKI는 공개키와 사용키 쌍 (Public/Private Key Pairs)의 생성 및 배포를 관리하고 X.500 디렉토리 서비스 등과 같은 공개된 불레틴 보드 (Open Bulletin Board)에 공개키를 인증서라는 사용자의 ID와 함께 공표한다.

공개키 인증

표1은 X.509 v3 인증서를 설명한다. 인증서는 발급자명, 대상자 (Subject)의 이름과 대상자의 공개 키를 포함하는데 이 인증서는 발급자의 비밀키로 서명된다. 만일 영희가 재현이의 인증서를 갖고 있고 발급한 인증기관의 공개 키를 알고 있다면, 영희는 재현이의 인증서를 확인할 수 있고 또 재현이의 공개 키를 사용해서 어떤 문서에 대한 재현이의 서명을 알아낼 수 있다.

버전 (V3)
일련 번호
서명 알고리듬 Id
발급자 이름
유효 기간
대상자 이름
대상자 공개키 정보
발급자 고유 Id
대상자 고유 Id
확장란
서명

표 1. X.509 v3 인증서

PKI 구조

공개키 인증을 제공하는 신뢰할 수 있는 엔티티를 인증기관 (certification authority; CA)이라고 부른다. 인증서들은 체인을 이루며 인증 경로를 만들 수 있다. 예를 들어 재현이는 CA3가 인증서를 발급해 주었고, CA3는 CA2가 인증서를 주었고, CA2는 다시 CA1이 인증서를 주었다고 하자. 만약 영희가 CA1을 신뢰하고 이의 공개 키를 알고있다면 영희는 재현이의 인증서에 이르러 확인하기 까지 인증 경로 위의 모든 인증서를 확인할 수 있다. 이 시점에서 영희는 재현이의 공개 키를 알게 되면서 재현이의 서명을 확인할 수 있게 된다.

인증 기관들은 체계적으로 PKI를 만들면서 상호 인증할 수 있다. 하나의 인증기관은 다른 기관에서 인증서를 받을 수 있다. 두 인증 기관은 인증서를 서로 발급할 수 있다. 이는 교차 인증으로 알려져 있고 이 쌍을 일컬어 교차 인증서라 부른다.

인증서 규정 (Certificate Policy)은 인증서가 인증서 사용자에게 특정 목적의 용도로 적합한지를 규정한 방법을 말한다. X.509 V3 인증서는 적용될 규정을 명시한 부분과 인증 경로가 관할 영역의 한계를 벗어 날 때 당해 규정에서 다른 규정으로의 매핑을 위한 방법을 포함하고 있다. 규정 자격 (Policy Qualifier) 란에는 적용될 인증 시행 지침 (Certification Practice Statement)을 위한 포인터 등의 추가 정보를 포함할 수 있다.

이미 앞에서 보인 바와 같이 PKI의 구조는 크게 두 가지의 다른 PKI 구성을 보일 수 있다. 즉, 계층적 수직 (Hierarchical) 구조와 네트웍 (Network) 구조이다. 계층적 PKI 아키텍처는 몇 가지 장점이 있다. 계층적 PKI는 수직적 트리 (Tree) 구조로 정의되므로 인증 경로를 찾는 것이 수직 경로를 따라 간단히 이루어 진다. 즉, 모든 사용자는 루트에 이르는 인증 경로를 갖고 루트의 공개 키를 가짐으로 그 인증 경로를 다른 어떤 사용자에게나 제공할 수 있고 그 사용자는 인증 경로를 확인할 수 있다. 이러한 장점은 정부 기관과 같이 계층 구조를 갖는 조직에 적합하다.

그러나 세계에 인증 기관이 하나만 존재할 수는 없다. 그러므로 여러 인증 기관 간에 엄격한 수직적 관계가 성립될 수 없음으로 어떤

방식이든지 간에 상호 인증이 불가피해진다. 따라서 계층적 수직 구조만으로는 이 문제를 적절히 해결할 수가 없다. 이렇게 해서 자연히 교차 인증 관계를 해결하기 위한 네트웍 구조의 PKI가 필요하게 된다. 두 인증 기관의 사용자 간에 빈번한 접촉이 있는 경우 인증 경로를 짧게 하기 위해 상호 인증이 직접적으로 되게 하는 것이 요구된다. 아마도 네트웍 PKI의 존재 가치는 인증서 소지자가 자기 신뢰(Trust)를 원거리에 있는 루트 CA에 위치하는 것보다는 근접 지역 CA에 위치하는 것이 보다 더 편리하고 자연스러울 것이라는 점이다.

네트웍 PKI 또한 크게 두 가지 단점이 있다. 첫째, 효율적인 인증 경로를 찾는 수단이 매우 복잡하고, 둘째, 한 사용자가 다른 모든 사용자들에게 자기의 서명 확인을 보증할 수 있는 단일 인증 경로를 제공할 수 없다는 것이다. 다행이 두 가지의 PKI 아키텍처가 상호 배치되지는 않아서 이 두 가지를 적절히 혼합하면 보다 더 효율적인 시스템을 만들 수 있다.

2. 미국의 PKI 구축 현황

X.509 공개키 인증 표준에 의거한 초기의 PKI 시스템으로는 Privacy Enhanced Mail (PEM) [RFC 1422] 과 미 국방성의 Multi-level Information System Security Initiative (MISSI) [9] 등이 있는 데 이들은 계층적 수직(Hierarchical) 구조로 PKI를 정의하였다.

계층적 구조는 정부나 다른 여러 기관의 구조에 비교적 부합하기는 하지만 계층 구조의 주요 이점은 이것이 신뢰와 보안 정책을 관리하는 데 편리한 방법을 제공하였다는 것이었다. 즉, 계층적 구조 내에서는 어느 두 곳의 관계이든지 항상 엄격한 수직적 계층 관계로 정의되므로, 계층적 구조의 여러 브랜치(branch)들은 거기에 해당되는 일관된 보안 정책들을 갖고 그리고 어떤 인증서의 소지자에 할당된 신뢰 수준은 해당되는 브랜치에 따라 일관되게 결정할 수 있다.

그러나 공개키 인증을 위한 표준이 발전함에 따라 엄격한 계층적 수직 구조는 융통성이 없어 받아들일 수 없게 되면서 계층적인 PKI들은 광범위하게 구현되지 못하였다.

CCITT X.509 인증 표준 버전 3 수정본은 인증 스킴에 인증서, 인증 경로, 암호 정책, 신뢰의 이전 등을 양성화 (Explicit)해서 관리하게 하는 기능을 추가하면서 비수직적 구조를 실용적이면서 용이하도록 하였다.

2.1. 미 국방성의 MISSI Infrastructure

미국의 NSA(National Security Agency)가 MISSI (Multilevel Information Systems Security Initiative)라 불리는 이니셔티브 하에서 공개키 기반구조의 개발을 주도하고 있다. 이 기반구조의 주요 응용 분야는 국방성의 DMS (Defense Messaging System)였다. DMS는 SBU (Sensitive-but-unclassified) 수준과 낮은 기밀등급 (SECRET수준) 까지의 군사 통신을 지원한다. 그러나 MISSI 구조는 DMS만 지원하도록 제한되어 있지는 않으며 훨씬 광범위한 응용이 가능하다.

1993년 인터넷 커뮤니티에 의해 PKI를 위한 인터넷 표준으로 개발되었던 PEM (Privacy Enhanced Mail) 디자인과 밀접하게 연관된 MISSI 기반구조는 그림1에 설명되어 있다.

이 PKI는 하향식 계층 구조 (Top-down Hierarchy)를 가지는 데 여기에서의 주요 구성 요소는 다음과 같다.

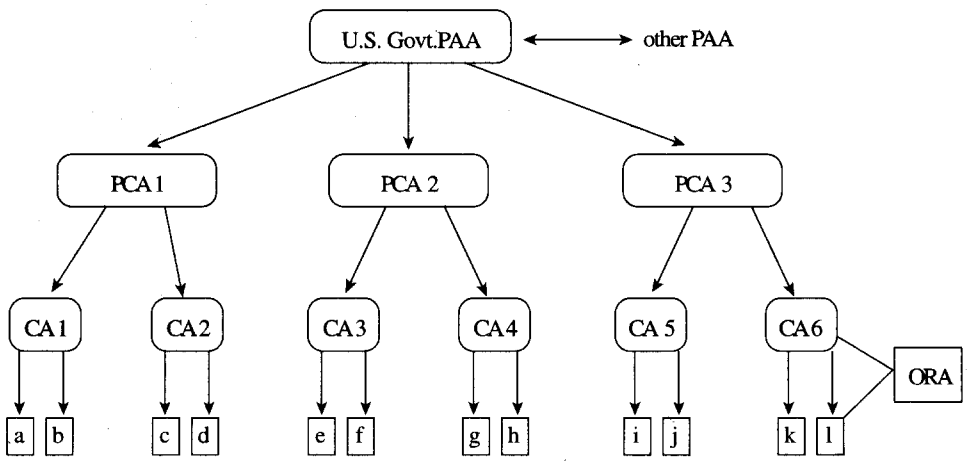

그림 1. MISSI Public Key Infrastructure

- PAA (Policy Approving Authority) - 모든 인증 과정이 시작하는 루트 인증 기관이다. 직접적으로는 아래의 PCA들을 인증해 주고, 완전히 다른 기반 구조의 PAA과 교차 인증을 허가해 주는 역할도 맡고 있다.
- PCA (Policy Creation Authority) - 각 PCA는 서로 다른 보안 정책을 가진 더메인의 루트이다.
- CA (Certification Authority) - CA는 최종 사용자들을 등록해고 인증서를 발급해 주는 역할을 한다.
- ORA (Organizational Registration Authority) - ORA는 LRA (local registration authority)의 MISSI 버전이다. ORA는 인증서를 발급하지 않고, 단지 CA를 도와 사용자를 등록하는것을 도와준다.

MISSI 기반구조는 하향식으로 조직화된 구조가 잘 동작하는 것을 보여주는 또 다른 예다. 이는 정부 자체가 계층적으로 조직화되어 있기 때문이기도 하다. MISSI 기반 구조의 개발은 공개키 기반구조의 다양한 분야에 대한 엄청난 양의 연구를 이끌어 내었고, 정부 영역에서 그러한 기반구조가 어떻게 발전해 가는지를 보여준 좋은 본보기가 되고 있다 [3].

2.2. X.509 V3 인증을 사용한 미 연방 PKI (Federal Public Key Infrastructure)

미국 연방정부의 PKI는 Federal PKI Concept of Operations[4]에 기술되었는데 수직 구조에다 좀 더 일반적인 네트웍 형태의 교차 인증 구조를 추가하였다. 이러한 혼합 구조는 양쪽 시스템의 장점을 대부분 갖는다. 미국 연방 정부의 PKI 개발은 NIST (National Institute of Standards and Technology)의 주도로 이루어지고 있다. NIST 가 디지털 서명 기술의 표준으로 DSS(Digital Signature Standard)를 채택하고 ANSI (American National Standards Institute) 역시 DSS를 전자 금융업무에 채택하면서 이를 베이스로 PKI 네트워크 구축 계획을 세웠다. 연방 PKI는 전자서명은 물론 다른 공개키 기반의 보안 서비스를 제공해 주기 위한 목적으로 개발되고 있다. 또한 NIST에서는 프로젝트와 PKI기반 제품들간의 상호 연동성을 위해 산

업체와 PKI기술 개발팀간에 긴밀한 협력관계를 유지하고 있다.

연방 PKI는 연방 정부와 정보화 자원의 안전한 사용과 국가정보 인프라(National Information Infrastructure)를 지원하는데 그 목적이 있다. FPKI는 정보시스템 보안, 전자상거래, 전자메일을 포함하는 안전한 통신등의 응용 분야에 공개키 기반의 인증서를 사용할 연방부서에서 필요로 하는 설비, 명세 그리고 정책을 수립해야 한다.

PKI 중심의 인증서 기반 보안 서비스는 그림2에 잘 나타나 있다. 그림의 중심은 PKI를 나타내고, PKI에 의해 가능해지는 보안 서비스들은 주위의 원들로 나타내고 있다. 가장 한가운데 중심은 PKI의 핵심으로 인증서를 발급하고 관리하는 일을 하고, 첫번째 원은 이 인증서를 사용하는 클라이언트들을 나타낸다. 그리고 그 다음 원은 다양한 보안 서비스를 제공하는 서버나 에이전트들을 가리킨다 [5].

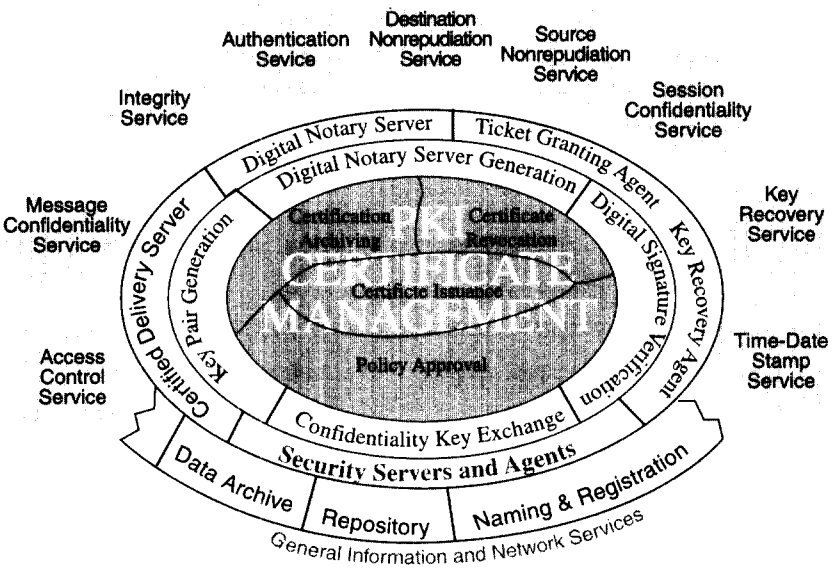

그림 2. PKI 중심의 인증서 기반 보안 서비스

그림 3은 제안된 FPKI 인증 경로의 아키텍처를 보여준다. 정부 쪽에 있는 CA들과 정부 바깥의 CA들은 Bridge CA를 통해 교차인증을 한다. 이런 방법으로 이미 개발되었거나 앞으로 개발될 Non-Federal PKI와의 상호 연동을 한다.

2.3. SET Public-Key Infrastructure

Visa와 MasterCard 사 등은 안전한 전자 지불 수단의 구현을 위하여 공동으로 SET (Secure Electronic Transaction)을 개발하였다. SET는 인터넷 기반의 전자 쇼핑에서 신용카드 지불 수단을 지원하기 위한 복잡한 프로토콜과 기반구조에 대해 명시하고 있다.

SET환경의 구성원은 카드 발급자, 카드 소유자, 상점, 거래 처리자, Payment Gateway, CA등이 있다.

(a)카드 발급자 (Issuer) : Visa나 MasterCard 같이 카드(신용 카드나 직불 카드)를 발급해주는 금융기관

(b)카드 소유자 (Cardholder) : 신용 카드를

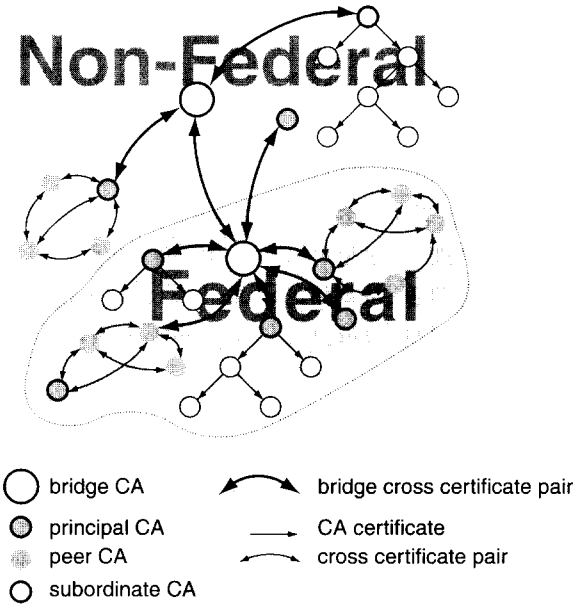

그림 3. 제안된 FPKI 인증 경로 Architecture

가지고 있는 인증된 사용자. 전자 상거래를 할 수 있도록 등록되어 있어야 한다.

(c)상점(Merchant) : 상품이나 서비스 혹은 정보를 판매하는 기관. 전자 지불 수단을 허용한다.

(d)카드거래 처리자(Acquirer) : 카드 거래를 처리하는 서비스를 상점에 제공해 주는 금융기관

(e)지불 게이트웨이(Payment gateway): 상점에 온라인 전자 상거래 서비스를 제공해주는 시스템. 거래 처리자나 그를 지원해주는 다른 기관에서 운영한다. 다른 기관에서 운영할 경우는 거래 내역을 알기 위해서 거래 처리자와 밀접하게 연결되어 있어야 한다.

(f)인증 기관(Certification Authorities): 기반 구조의 구성원이며, 카드 소유자나 상점 등의 공개 키를 인증해 준다.

SET기반구조에 적용되는 공개키 기술들은 다음과 같다.

- 지불 지시의 암호화 - 인터넷을 통해 전송되는 사용자의 카드 번호가 노출되지 않도록 보장해야 한다. 상점의 시스템에 노출되어서도 안된다.
- 카드 소유자의 인증(authentication) (상점과 acquirer에 대해) - 인증되지 않은 사용자가 도난 당한 카드를 사용하여 전자 거래를 시도하는 것을 막아야 한다.
- 상점의 인증 (카드 소유자와 acquirer에 대해) - 개인이 인터넷 사이트를 개설하고 합법적인 상점인 것처럼 위장하여, 사기 거래를 시도하는 것을 막아야 한다.
- acquirer의 인증(카드소유자와 상점에 대해)-acquirer행세를 하는 누군가가 쉽게 지불 지시 정보를 해독하는 것을 막아야 한다.
- 거래 정보의 Integrity-protection-공개된 인터넷 상에서 무단 변조되는 것을 막아야 한다.

SET에서 사용된 PKI 아키텍처는 그림에서와 같이 하향식 계층 구조 (Top-Down Hierarchy)로 되어 있는데 아래와 같은 종류의 인증기관들 (Certification Authorities)로 구성된다.

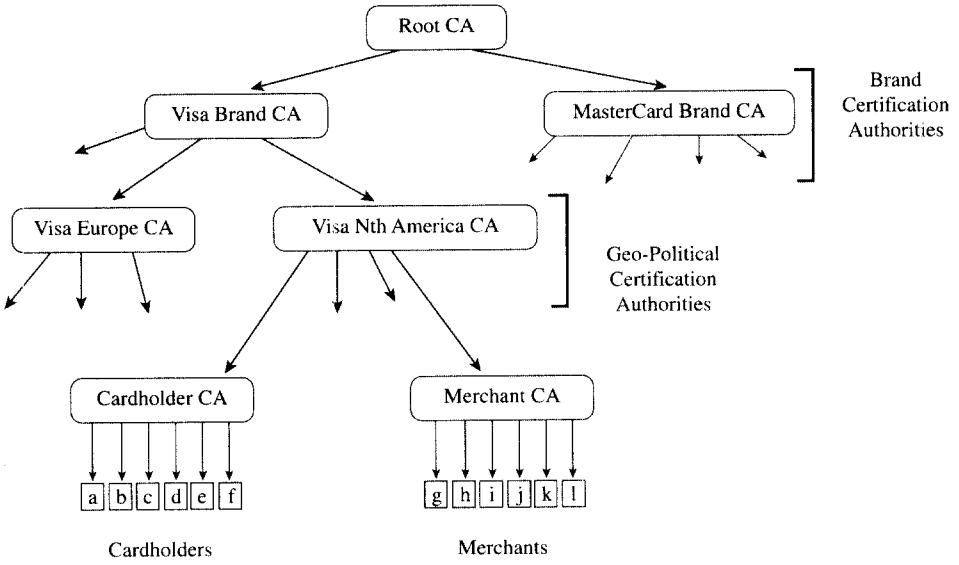

그림 4. SET Public-Key Infrastructure

- 루트 인증 기관 (Root CA): 모든 인증 경로는 루트 인증 기관의 공개 키로부터 시작된다. 이 인증 기관은 오프 라인으로 유지되며 브랜드 인증 기관에게 인증서를 발급하기 위해 사용될 뿐 매우 드물게 사용된다.
- 브랜드 인증 기관 (Brand CA): 이들은 Visa, MasterCard 등의 각기 다른 브랜드 소유자에 의해 운영된다. 각각의 브랜드는 이 시점부터는 어떻게 인증서를 관리하는가 하는 문제에 대해 상당히 자율권을 가지게 된다.
- 지정학적 인증기관 (Geo-political CA): 각각의 브랜드는 지정학적인 고려에 따라 선택적으로 하위 인증서를 어떻게 관리할 것인가를 결정한다. 지역 마다 금융 시스템이 어떻게 운영되느냐에 따라 인증 정책이 달라질 수 있다.
- 카드 소유자 인증 기관 (Card holder CA): 카드 소유자에게 인증서를 발급 배포하는 기관이다. 카드 소유자는 전자 메일이나 웹 상에서 인증서를 신청한다. 인증 기관은 카드 발급회사가 직접하거나 또는 제3의 기관이 될 수 있다. 후자인 경우 인증 기관이 인증서를 발급하기 전에 카드 소유자에 대한 상세 내역을 카드 발급회사와 통신하여 결정하는 것이 필요하다.
- 상점 인증 기관 (Merchant CA): 이 인증 기관은 보통 카드거래 구입자 (Acquirer)의 허가를 토대로 하여 상점에게 인증서를 발부한다. 이 인증 기관은 브랜드 사의 결정에 따라 카드거래 구입자 (Acquirer)나 또는 제3자가 운영할 수 있다.

SET 공개키 기반구조에 사용된 하향식 계층구조는 이런 종류의 응용에서는 적절하다고 판단된다. 왜냐하면 전체 인프라가 하나의 응용 목적에 국한되어 있고, 금융기관의 환경은 필요한 신뢰 관계를 구축하는데 별로 큰 문제가 없기 때문이다. 이 기반구조는 은행카드 지불 외의 다른 어떤 응용 분야를 지원할 의도가 없고 또한 다른 기반구조와 연동할 계획도

없어 인증서를 다른 목적으로 사용하지 않음으로 예기치 않은 위험을 감수할 필요가 없다.

3. 유럽의ICE-TEL Project

ICE-TEL(Internetworking Public Key Certification Infrastructure for Europe) Project는 EU가 유럽전역에 인터넷 X.509 기반의 인증 기반구조를 구축하여 그것을 이용하는 S/MIME, WWW와 같은 안전한 응용분야를 수립하고자 하는 범유럽적인 프로젝트이다. ICE-TEL PKI는 유럽 PKI를 위한 최상위 인증 기관으로 유럽 공동체의 인증 기관들의 네트웍으로 통합되어 있으며 현재 덴마크, 독일, 이탈리아, 노르웨이, 슬로베니아, 스페인, 영국 등이 참가하고 있다. 이들 각국은 각각 인증기관을 갖고 있어 여기서 각국의 인증서 발급과 지원을 하고 있다.

ICE-TEL 프로젝트는 2단계로 나뉘어 진행된다. 1단계는 X.509v1 인증서와 CRL 형식을 따르며 RFC 1422 (PEM)에 제시된 신뢰 모델을 제공한다. 프로젝트에 참여하는 각 국가에는 CA가 있고 이 CA들을 ICE-TEL 루트 CA가 인증해 준다. 국가내의 다른 CA들은 국가 CA에서 인증을 받아야 한다. ICE-TEL 프로젝트의 2단계는 X.509v3인증서와 X.509v2 CRL 형식을 따르며 PEM, PGP의 신뢰모델을 합친 새로운 모델을 제공한다.

4. 캐나다 정부의 PKI (Government of Canada Public Key Infrastructure)

캐나다의 정보화 고속도로 자문 위원회 (Information Highway Advisory Council)는 1995년 9월의 보고서에서 정보화 고속도로 상의 거래 비밀보장과 보안은 캐나다 정보화 고속도로 전략의 기본적인 원칙임을 명시했다. 이 위원회는 캐나다 정부에 제안된 PKI에 투자하여 보안 분야에서 캐나다의 수준을 향상시킬 것을 요구했다. 또한 자국과 타국간의 상호 호환성을 유지하기 위해 호환성 있는 PKI 정책과 교차인증에 대한 연구도 지속적으로 수행할 것을 요구했다. 이에 따라 1995년 12월에 캐나다 정부는 6개의 부문으로 구성되는 PKI 프로젝트에 착수했다[7]. GOC PKI는 연방정부가 캐나다 인들에게 보다 더 효율적인 서비스를 제공하고, 안전한 전자 상거래를 보장해 주며, 연방 정부 내에서 사용되는 정보의 기밀을 보다 잘 보호해주는 것을 목적으로 한다. GOC PKI의 완전한 구현은 1998년으로 예정되어 있다. 이를 위해 Nortel사의 제품인 Entrust를 채택했다.

GOC PKI는 PMA (Policy Management Authority), CCF (Canadian Central Facility), CAs (Certificate Authorities) 그리고 LRAs (Local Registration Authorities)로 구성되어 있다. GOC PKI의 개념은 그림5에서 처럼 정의된다.

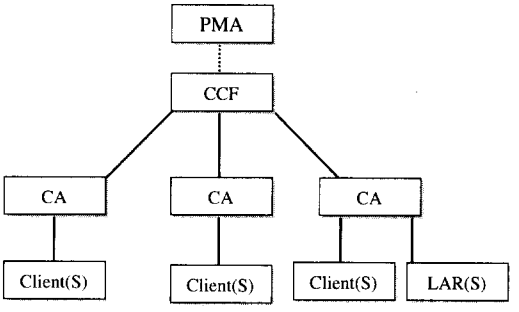

그림 5. GOC PKI 개념도

- PMA (Policy Management Authority)는 정부 부처간 합동 위원회로 현재 재무부 장관이 의장을 맡고 있다.
- CCF는 GoC PKI 를 구현하는 중앙 CA로서 여타의 정부 기관이나 민간 섹터 등의 외부 기관과 교차 인증을 하는 공통점을 제공한다. 이것은 유일한 GoC PKI 레벨 0의 CA로서 Ottawa에 위치한다.

- CA들은 정부 내의 각 부처에서 운영한다. 각각의 CA는 해당 부처의 암호 엔티티들, 전자서명 엔티티들, LRA들, 그리고 휘하에 GoC PKI CA들이 있는 경우 이들을 관장할 책임을 진다.
- 각 부처에 의해 운영될 LRA의 주요 기능은 사용자들의 공개키 인증서를 등록 확인하는 업무를 한다. 또한 LRA는 관할 CA에 종속되어 이것이 사용자들과 지역적으로 떨어져 있는 경우 사용자와 CA간의 연결을 도운다.

5. 호주의Public Key Infrastructure 활동

호주 정부는 1997년 10월 OGIT (Office of Government Information Technology) 를 중심으로 GATEKEEPER 프로젝트를 시작하였다[6]. 이 프로젝트의 개념은 정부의 공개키 기술을 관리하는 정부 기관으로 GPKA (Government Public Key Authority)를 1998년 출범시키고 GPKI (Government PKI) 기술을 발전시키는 것이다. GPKA 이사회는 현재 9명으로 정부 대표와 산업계 2명 및 학계 1명 등을 포함하여 구성되었다. 의장은 단순 과반수로 선출하나 초대 의장은 OGIT가 맡았다. GPKA는 정부의 공식 정책 기구는 아니지만 OGIT의 의장인 CGIO (Chief Government Information Officer)를 통하여 정부와 함께 일하기로 되어있다. GPKI는 상호 인증을 위해서는 NPKI (National PKI) 하에 설치된 루트 CA 관할 하에 두기로 하였다.

이와 더불어 호주의 Standards Australia는 PKAF (Public Key Authentication Framework) Task Group을 구성하여 안전한 전자상거래를 위한 공개키 프레임웍 구현을 위한 표준화에 나서고있다. 이 그룹은 다른 나라의 시스템과 호환성을 가지면서 전자 서명의 생성과 관리를 위한 시스템의 가능한 모든 경우를 검토하는 일을 맡았다. 이 그룹에는 산업체와 정부로부터의 대표들이 참가하여 표준화를 하고 있다. 그리고 DSTC(Distributed System Technology Center)에서 PKI의 모델과 구현상의 문제점들을 연구하고 있기도 하다. DSTC는 X.509 v3를 기준으로 구성되었으며 전송문 전체를 암호화하기 위하여 RSA, DSA, MD5, SHA-1 등의 알고리즘을 이용한다. 인증기관이 관리하는 디렉토리는 인증서와 사용자가 관련된 여러 정보를 저장하고 있는 곳으로 LDAP (Lightweight Directory Access Protocol)를 이용하여 X.500 디렉토리 서비스를 제공한다.

6. 세계의 PKI 솔류션

현재 세계적으로 PKI 솔류션은 미국, 캐나다, 유럽 등의 인증 기술 개발 회사나 인증 서비스를 제공하는 회사 들이 앞서서 개발하고 있다. 미국에서1995년 설립되어 잘 알려져 있는VeriSign은 기업용과 일반 고객 용의 PKI와 디지털 인증 솔류션을 공급한다. 현재 BOA 등 8개 은행 등이 참여하여 기업간 전자상거래를 위한 글로벌 베이스의 신뢰 프레임웍(Global Trusted Framework)을 구축하고 있다. 여기에는 VeriSign의 PKI 솔류션인 OnSite 4.0를 적용하고 있고 현재 BOA 및 Morgan Stanley Dean Witter사를 비롯한 120여 개의 기업이 디지털 인증 기술을 활용한 광범위한 네트웍 시스템의 보안에 이 솔류션을 사용하고 있다. 또한 VeriSign이외에도 미국의 GTE CyberTrust 등이 나름대로의 경험을 바탕으로 잘 알려져 있다.

7. 결 론

앞에서 지적한대로 대규모의 PKI 시스템을 실현하는 데 가장 중요한 두 가지 기술 문제는 어떻게 적절한 인증 경로를 찾느냐 하는 문제와 찾고 난 다음 어떻게 검증하느냐 하는 문제이다. 경로 찾기는 디렉토리 서비스 등 정보 Retrieval 서비스만 주어진다면 자동화될 수 있다. 경로 확인은 주의 깊게 정확한 알고리듬을 따라야 하며 또한 안전하게 구현되어야 한다.

계층 구조의 장점은 수직적인 신뢰 관계의 관리가 용이하다는 점이며 여기에서 인증 경로의 확인은 루트 CA의 공개 키에 의거한다. 그러나 세계의 각기 독립된 인증 기관들을 수직적 관계로 연결하는 것은 루트 CA를 누가 관장하느냐는 문제가 있어 가능하지 않다.

최근의 X.509 인증 표준 V3 버전에서는 교차 인증 기관 간의 PKI 아키텍처 상에서 신뢰 관계를 관리하기 위해 고객의 인증 경로를 확인할 때 그 고객에게 자기의 인증서를 직접 발급했던 인증 기관의 공개 키에 의존하게 하였다. 이것이 개별 인증 기관에 융통성을 주면서 반면 여러 인증 기관 간의 교차 승인 문제를 용이하게 해결하는 수단이 된다. 그러나 이것이 커다란 조직에서 전체적으로 반드시 일관된 신뢰 관계를 관리하는 프레임웍을 제공하지는 못한다. 그래서 앞으로 보다 발전된 혼합적 모델의 연구가 요구된다.

전자상거래 분야에의 PKI의 성공적인 도입은 기술적 문제의 해결 뿐만 아니라 법 제도적인 불확실성을 어떻게 해결하느냐에 크게 좌우된다. 미국에서는 디지털 서명의 사용에 관련한 다양한 법제화가 진행되었다. 각각의 주정부에서는 각기 다른 방법을 추구하였다. Utah 주는 법에 따라 주정부내의 PKI를 제도화하였다. 반면 California주의 디지털 서명법은 공적인 엔티티와 통신하는데 사용되는 디지털 서명의 법적 충족 요건을 단순히 명시하는데 그치면서 디지털 서명을 어떻게 만들며 또한 PKI를 통하여 어떻게 검증되어야 하는지 하는 이슈들을 규정하지 않으면서 자유롭게 하였다. 우리도 세계 주요 국가의 동향을 세심하게 관찰하여 전자 서명법의 제정이 전자상거래 활동이나 전자적 방법의 활성화가 안전하게 발전적인 방향으로 나아가도록 해야 하겠다.

참 고 문 헌

[1] 공개키 기반구조 기술 관련 표준화 동향, '97 정보보호기술 표준화 현황, 한국정보보호센터, 1997.12.

[2] 전자상거래를 위한 공개키 기반 인증 기술, 임신영 외, 통신정보보호학회지, 제7권 제3호, 1997.9.

[3] 공개키 기반구조에 관한 고찰, 김지연, 박성준, 통신정보보호학회지, 제7권 제2호, 1997.6.

[4] A Proposed Federal PKI Using X.509 V3 Certificates, W. E. Burr et al, NIST.

[5] Public Key Infrastructure (PKI) Version 1 Technical Specifications - Part C: Concept of Operations, Federal PKI Technical Working Group, Nov. 16, 1995.

[6] Secure Electronic Commerce, Warwick Ford, Michael S. Baum, Prentice Hall, 1998

[7] Government of Canada Public Key Infrastructure White Paper (MG-15a), Feb. 1998, GoC CSE.

[8] The GATEKEEPER Report, The strategy for public key technology use in the Government, 1998.

[9] MISSI Phase 1 Program Overview ,
VERSION: 3.3, 17 Oct. 1995.

□ 著者紹介

신 홍 식

1974년 서울대학교 응용수학과 졸업
1983년 Pennsylvania 주립대학원 컴퓨터과학 석사
1989년 Georgia Institute of Technology 컴퓨터과학 박사
1989년 ~ 1991년 GTE Labs Senior Member of Technical Staff
1993년 ~ 1996 동양 SHL 상무이사
1996년 ~ 1997 동부정보시스템 대표이사
1997년 ~ 현재 (주) 신테크 대표이사

※ 주관심분야: 전자상거래 인증보안, 지능형 에이전트, 분산객체 웹 기술

이 종 일

1999년 2월 KAIST 학사과정 전산학과 졸업예정
(주) 신테크 재직
안전한 전자지불 수단을 사용한 가상 쇼핑몰 구축(기술개발)
국산전자서명 알고리즘을 이용한 Cryptographic System Toolkit 개발중

※ 주관심분야: