通信情報保護學會誌
第8卷 第3號, 1998. 9

공개키인증 기반구조로서의 X.509에 대한 연구

Study of X.509 as an infrastructure of a public key certification

김 상 균*, 백 종 현*, 이 강 석*, 이 석 준*

요 약

인터넷을 통한 거대한 새로운 가상 세계가 구축되고 있으며, 우리는 이러한 가상세계의 새로운 이주민으로서 살아갈 준비를 하고 있다. 대부분의 사람들이 예측하고 있듯이 앞으로 펼쳐질 가상 세계는 거래되는 대부분의 데이터가 디지털화되어 전송되고, 또한 디지털화되어 저장될 것이다. 이러한 세계에서 기본적으로 요구되는 것이 각 데이터의 신뢰성과 서로 모르는 상대방간에 신뢰이며, 이러한 신뢰성을 위한 새로운 기구나 도구 또는 제도적 정책들이 요구되고 있다.

이러한 현안들 속에서 본고에서는 상호 인증과 접근제한을 위한 기본 요소로서 공개키 기반구조의 핵심을 이루는 X.509의 구조에 대해서 살펴보고자 한다. 또한 모든 버전의 X.509의 일반적 장점과 단점에 대해서 논하고자 한다. 그리고, 실패한 PEM과 계획중인 X.509기반의 PKI 표준에 대해 살펴보고자 한다

서 론

앞으로의 암호화는 비밀키 방식 보다 공개키 암호방식을 이용하는 쪽으로 나아가고 있으며, 공개키 방식의 암호화는 사용자들의 공개키를 관리하는 시스템을 필요로 한다. 폭발적으로 증가하는 인터넷 사용자들을 고려해 볼 때 공개키를 어느 한 단체 또는 조직이 관리한다는 것은 제도적이나 시스템적으로 많은 문제점이 있다. 따라서 어떤 계층 구조를 이루면서 공개키를 관리하여야하는데, 역시 여러 가지 문제들이 발생한다. 강력한 인증을 위해서는 인증서에 많은 속성들을 기록해야하나 이것은 개인의 비밀을 공개하는 것과 다름없게 된다. 이러한 맞물린 문제점들을 어떻게 해결해야하는지, 계층구조에서 상대방을 모르는 상황에서 어떻게 공개키들을 주고받을 수 있는지, 서로에게 어떻게 믿음을 가질 수 있는지, 계층구조에서의 각자의 역할 분담은 어떻게 되는지, 책임관계는 어떻게 되는지 등 여러 가지 문제점들이 존재함에 따라, 이에 대한 여러 가지 해결책들이 제안되어 왔고 설계 중에 있다.

X.509는 X.500 디렉토리 서비스를 보충하기

* 사이버게이트

위해 고안된 인증 구조이다. X.509와 X.500은 모두 ISO/ITU에 의한 국제표준 X 시리즈의 부분이다. X.500 표준은 거대한 컴퓨터네트웍에 디렉토리 서비스를 제공하기 위해 고안되었다. X.509는 X.500서비스를 인증하기 위한 PKI 구조를 제공한다.

X.509의 첫 번째 버전은 PKI에 대한 가장 오래된 제안으로서 1988년에 만들어졌으며, 이것은 가장 광범위하게 PKI를 채용한 X.509를 만들었다. 적어도 열 개정도의 회사들이 X.509에 기반한 제품을 만들어냈고 그 수는 늘어나고 있다. 일 예로, Visa 와 MasterCard 가 안전한 SET표준으로 X.509를 채용했고[1], 넷스케이프사의 WWW 소프트웨어도 X.509를 사용한다. Entrust나 TimeStep처럼 인트라넷을 지원하는 회사들도 X.509기반의 많은 제품을 선보이고 있다. 또한, 인터넷처럼 국제적 네트웍을 지원하는 X.509기반의 PKI를 디자인하려는 노력이 진행중이다. PGP와 함께 X.509는 현재 상용중인 PKI 시스템이다.

X.509는 현재 최종본으로 버전 3까지 나와 있으며, 버전 3은 현재 ISO/ITU에 마지막 채택 단계에 있다. X.509v3은 X.509표준의 기능을 확장하고 있으며, 오늘날 대부분의 제품들은 X.509의 버전 1, 버전 2를 사용하고 그 외 일부만 버전 3을 사용한다. SET 프로토콜은 대부분의 국제적 X.509 PKI 제안들처럼 버전 3에 기초한다.

2. X.509 표준의 개요

2.1 X.500

X.509 PKI의 완전한 이해를 위해 원래 X.509가 디자인 된 목적인 X.500 디렉토리에 대하여 파악할 필요가 있다. X.500 디렉토리는 사람의 이름, 사람에 대한 추가 정보들이 있는 전화 번호 목록과 비슷하다. 그러나 X.500은 이름, 주소, 전화번호 이상의 것들을 제공한다. X.500 디렉토리 내에 있는 엔트리는 어떤 사람의 전자메일 주소, 직업명, 직장명처럼 속성들의 모임이다. X.500 디렉토리 엔트리는 사람뿐만 아니라 컴퓨터들, 프린터들, 회사들, 정부들, 나라들과 같은 실세계의 모든 항목들을 나타낼 수 있다. 엔트리는 개체의 공개키를 인증하는 인증서를 포함 할 수 있다.

디렉토리 내에서 원하는 엔트리를 찾기 위해 각 엔트리는 국제적으로 유일한 이름(DN: Distinguished Name)을 가진다. 그들의 유일성을 확신하게 하기 위해 이름들은 특별한 방식으로 할당이 된다. X.500디렉토리는 〈그림2-1〉과 같이 DIT(Directory Information Tree)로 불리는 계층적 방법으로 구성되어 진다.

트리안에 각 노드 혹은 정점은 루트를 제외한 하나의 부모를 갖고 다수의 자식을 갖는다. 각 정점은 루트를 제외하고 정점의 누이(동일한 부모를 가진 형제 자매)들을 구분하기 위해 유일한 RDN(Relative Distinguished Name)이 할당된다. 각 정점의 조상들의 RDN들은 엔트리의 DN을 구성하기 위해 정점자신의 RDN과 결합된다. 루트정점 하부의 각 엔트리에는 각 나라들이 존재한다. 이 엔트리들은 ISO에 의해 각 나라마다 유일하게 두 문자로 코드된다. 각 나라 정점의 하부에는 각 나라의 조직들인 각 부서들, 주들, 지방들, 그리고 회사들이 존재한다. 이 하부 엔트리들 또한 각 조직마다 유일한 RDN을 부여받는다.

마지막으로 각 조직들은 그에 속한 모든 엔트리를 구성한다. 이들 역시 각각 유일한 RDN이 할당된다. 〈그림2-1〉의 예에서 Louis Riel 씨는 캐나다 회사, Bombardier에서 일한다. Bombardier회사는 Riel 씨에게 그의 이름을 RDN으로 할당한다. Bombardier는 그것 자체가 RDN으로 "Organization = Bombardier"라는 것을 캐나다에 의해 할당받는다. 캐나다의 RDN은 두 글자 나라 코드(Country = CA)를

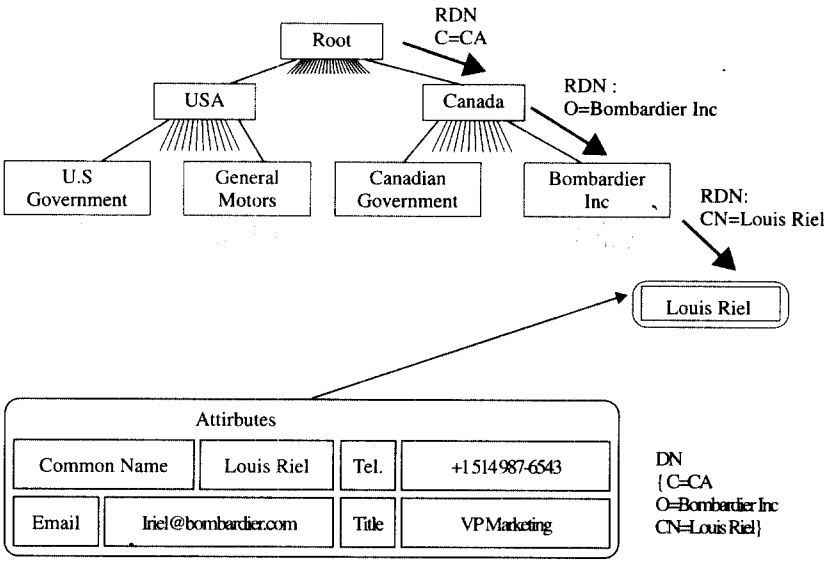


그림2-1 X.500 Directory Information Tree

갖는다. Riel씨의 DN은 이 RDN들의 결합체로 루트부터 시작해서 Country= CA, Organization= Bombardier, CommonName= Louis Riel 이다.

2.2 X.509 version 1 과 version 2

X.509는 X.500 디렉토리의 엔트리들의 인증을 지원하기 위해 만들어졌다. 마지막 버전은 X.500 루트 이상으로 발전시켰다. 버전 3은 곧 X.509표준으로 공식적으로 채택이 될 것이다. 버전 3에 덧붙여져야 할 확장사항들을 살펴보기 전에 먼저 X.509v2를 살펴보도록 한다.

X.509v2 증명서는 〈그림2-2〉에 묘사되어 있으며, 그 구성요소들은 다음과 같다.

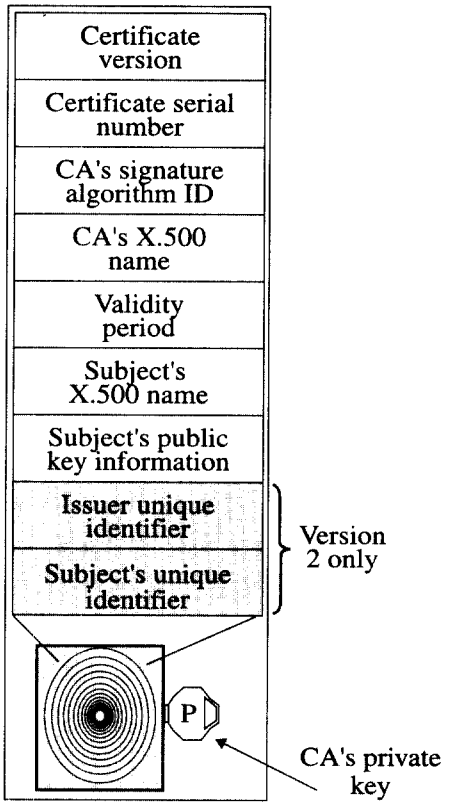


그림2-2 X.509 version 2 certificate

- **Version**
  증명서가 확인하는 X.509버전
- **Serial number**
  CA인증에 의해 부여된 증명서에 유일한 번호
- **CA signature algorithm**
  증명서를 서명하기 위해 CA에 의해 사용된 알고리즘 표시
- **Issuer name**
  인증하는CA의 X.500이름
- **Validity period**
  증명서의 유효 기간으로 Not Before와 Not After 필드로 구성
- **Subject name**
  증명이 되는 공개키에 대응되는 개인키를 가진 개체의 X.500 이름
- **Subject public key information**
  키가 쓰이는데 연관된 알고리즘의 확인자와 함께 대상(subject)의 공개키 값
- **Issuer unique identifier**
  옵션으로 버전 2에서만 나타나며, 비트 스트링이 인증하는 CA의 X.500이름을 명확하게 해준다. X.500이름이 특별한 개체에 할당이 되고, 할당이 해제되어 또 다시 새롭게 할당되는 것이 가능하다. 특정한 확인자(identifier) 필드가 이 관계를 알려준다. 이 필드는 다루는데 곤란하므로 잘 쓰이지 않고 대개의 구현된 품들에서도 생략되어 있다. 이 문제를 알릴 바람직한 방법으로, 결코 재 사용되지 않았다는 것을 확인하기 위한 수단으로 RDN들을 디자인하는 것이다. 가령 CommonName 속성을 사용하는 것보다, RDN을 CommonName과 Employee Number 모두 사용하는 것이다.
- **Subject unique identifier**
  옵션으로 버전 2에만 존재하는 것으로, 비트 스트링이 대상(subject)의 X.500이름을 확실하게 하는데 쓰인다.

X.509는 X.500과 밀접한 관계가 있기 때문에 X.509의 CA 들은 흔히 X.500 DIT와 유사한 계층구조로 이루어진다. X.509자체는 특별한 CA구조를 나타내지 않는다. 그러나 그것은 교차 증명서(cross certificate)와 함께 일반적 계층모델을 묘사하고 X.509와 사용되도록 권장된다.

X.509 버전 3은 하나의 계층구조 이상의 수단을 제공한다. 그러나 현재의 X.509 제품들은 대개 버전1과 버전2에 기반을 두고 있고 주로 한 조직 내에서 사용하기에 알맞게 디자인되어있으며, 대개 계층구조 형태에 의존하고 있다. 큰 규모의 회사와 같은 조직들은 계층적 모델에 잘 맞는다. 회사는 일반적으로 고용자들에 증명서를 인증하고, 그 회사 PKI는 내부적 통신을 위해 사용된다. 원래 그 회사의 계층구조를 따르는 PKI는 신뢰 관계를 정의하고 관리하데 유용하다.

X.509 와 X.500은 현재의 폭발적인 인터넷 사용증가 이전인 1980년대 중반에 디자인되었기 때문에, 컴퓨터들이 일시적으로 접속하는 off-line 환경에서 동작하도록 디자인되어있다.

X.509는 인증서 취소목록인 CRL(Certificate Revocation List)을 채택하고 있다. X.509의 버전 1과 2는 크기 문제나 time-granularity 문제를 언급하지 않는 매우 단순한 CRL을 사용한다. time-granularity 문제는 철회 인증서가 갱신되기 전에 사용될 때 발생하는 문제이다. 버전 3은 이러한 문제들을 해결하려는 여러 시도들의 결과로서 만들어졌다.

〈그림2-3〉은 X.509의 버전 1과 2에서 쓰이는 CRL 형식을 나타낸다.

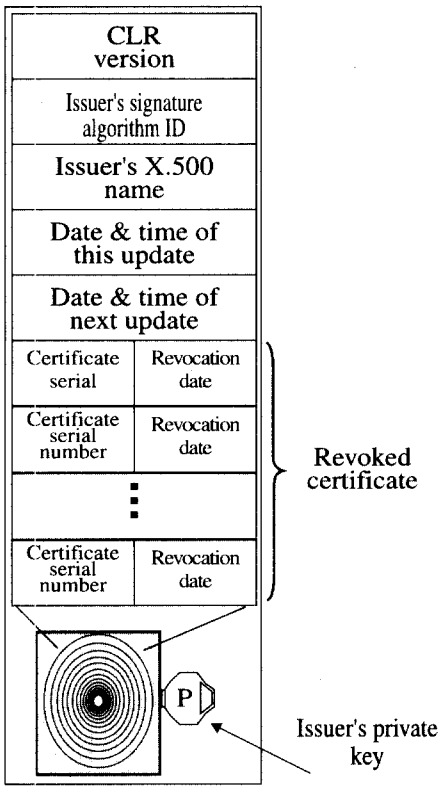


그림2-3 X.509v1 CRL format

2.3 X.509 version 3

버전 3은 X.509표준의 중요한 변화를 나타낸다. 근본적 변화는 증명서와 CRL 형식에 확장성을 준 것이다. X.509를 구현하는 사람들은 그들에 맞게 증명서의 내용을 정의할 수 있다. 또한 여러 표준 확장(standard extension)들은 공개키, 정책 정보, 대상(subject), 인증자 속성, 인증경로 제한점들, 확장된 CRL 기능들을 제공토록 정의되었다. 여기서는 X.509의 PKI 특성들에 영향을 주는 확장성들에 대해 분석한다.

2.3.1 Version 3 Certificate Extensions

Certificate policies and policy mapping

X.509v3는 CA에게 증명서를 만들 때 수반되는 정책(policy)들의 리스트를 증명서와 함께 포함할 수 있게 한다. 이런 정책들은 사용자에게 증명서가 특정한 목적에 적합한지를 결정하는데 도움을 주기 위해 사용된다. 예를 들면, 어떤 정책(policy)은 증명된 키가 보통 전자메일 메시지를 위해 사용될 수는 있지만 재정적 거래를 위해서는 사용될 수 없음을 나타낸다. 일반적으로 증명서 정책은 CA의 보안 절차, 대상의 확인 수단, 법적 권리포기나 수단들 같은 것에 대해 나타낸다. Policy mapping이란 CA에게 다른 CA의 정책과 동일한 정책이 있는지를 나타내도록 하는 것이다.

Alternative names

X.509v3증명서는 대상(subject)이나 식별자에 대해 하나 혹은 여러 선택적 이름들을 가질 수 있다. 이것은 X.509가 기초를 이루는 X.500 디렉토리 없이 동작할 수 있도록 한다. 선택적 명칭의 예들은 전자메일 주소들이나 WWW(World Wide Web) 공용 자료 저장소와 같은 것들이다. 구현자들은 그들 자신의 선택적 명칭 형식을 정의할 수 있다. 선택적 명칭들은 CRL의 식별자를 나타내는데 사용될 수도 있다.

Subject directory attributes

이 확장은 어떤 대상(subject)의 X.500디렉토리 엔트리 속성값들이 증명서에 포함될 수 있도록 한다. 이것은 증명서가 대상의 명칭 외에도 추가적 확인을 위한 정보들을 가질 수 있도록 하는 것이다.

Certification path constraints

이 확장은 CA들이 그들의 기반 조직을 의미 있는 형태로 연결할 수 있게 한다. CA는 다른 CA에 대한 인증을 하는 증명서로부터 확장되는 증명 경로의 종류를 제한 할 수 있다. CA는 증명서의 대상이 실제 CA인지 아닌지를 구분할 수 있다. 이것은 종단 사용자가

CA인 것처럼 속이지 못하도록 한다. CA는 또한 가령 주어진 인터넷 도메인 내에서만 쓰이도록 할당된 특정한 이름 공간에서만 혹은 인증 정책들을 따르는 증명서에 대해서만 인증된 증명서로부터 증명서로 갈 수 있게 길을 제한할 수 있다. 이것은 CA에게 무한정 증명 경로가 늘어나는 것을 막는 progressive-constraint 신용 모델을 채용할 수 있게 한다. 이 개념은 〈그림2-4〉에 묘사되어있다. 사용자 a는 그녀의 증명 기관으로써 D를 사용하고 그녀는 D를 완전히 신뢰한다. D는 다른 CA인 E를 인증한다. 예를 들면 다른 CA에 대한 증명서들만 인증하는 E를 신뢰하는 것이다. 조건 X하에서 D는 단지 다른 CA를 인증하는 E를 신뢰한다고 할 수 있다.

E는 F가 도메인 foo.com안의 종단 사용자에 대한 증명서를 인증할 때만 믿는다고 말하면서 CA F에 대한 증명서를 인증했다. 그래서

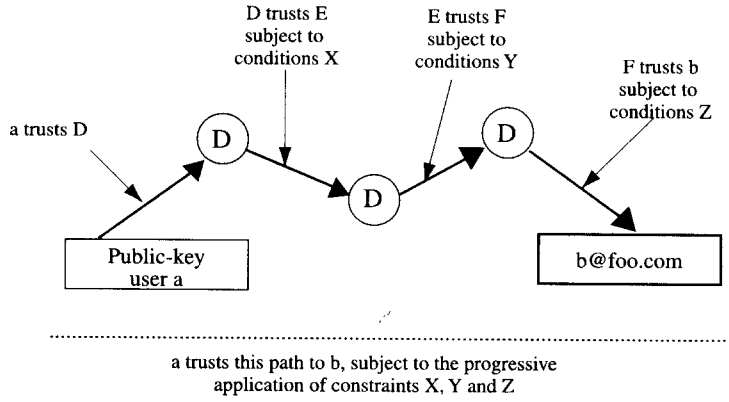


그림2-4 A progressive-constrained trust chain

조건 Y하에서 E는 F에 의해 인증된 증명서가 단지 종단 사용자이고 사용자 이름이 foo.com 도메인에 있다는 것을 증명할 때 만 믿는다고 할 수 있다. 마지막으로 F는 사용자 b에 대한 증명서를 인증하지만 단지 보통 전자메일에 대해서만 b를 믿는다. 그래서 조건 Z하에서 F에 의해 인증된 b의 증명서는 보통 전자메일에 대해서만 쓰일 수 있다고 말할 수 있다.

이런 식으로 증명 경로가 커지면서 D에 있는 한계 없던 신용은 점점 제약이 가해진다. A가 B에 대한 증명서를 가졌을 때 그녀는 그녀가 단지 그것을 보통 전자메일에 대해서만 사용해야 한다는 것을 알고 있고 그녀는 증명 경로를 따라 어떻게 신뢰가 제약이 되었는지를 알 수 있기 때문에 PGP의 신뢰망보다 인증력에 확신을 둘 수 있다. 이런 제약점들이 주어졌을 때 그녀는 B를 위해 E에 의해 인증된 증명서를 받아들일 수도 없고, F에 의해 인증된 CA로부터의 증명서를 받아들일 수도 없다. 만약 CA들이 다른 CA들을 증명할 때 엄격한 조건들을 정의한다면 증명 경로가 길어질수록 더 이상 길어 질 수 없을 때까지 점점 제약이 부과된다.

2.3.2 Version 3 CRL Extensions

CRL number and reason code

주어진 증명서 수에 대해 각 인증된 CRL은 점차 증가하는 수열로부터 수를 할당받는다. 이것은 CRL이 손실되었는지를 가려줄 수 있게 해주며, CRL내에 있는 각 증명서는 CRL 엔트리에 덧붙여진 철회이유를 가진다. 이런

두 가지 확장성은 보다 섬세한 CRL 확장을 허락한다.

CRL distribution points

이 확장은 CA의 사용자에 의해 처리된 CRL의 크기를 감소시켜준다. 사용자가 전체 CRL을 가지게 하는 것 보다, CA는 여러 방법으로 CRL를 나눌 수 있고 다른 분배 지점(distribution point)으로부터 각 부분을 인증할 수 있게 한다. 예를 들어 CA는 회사의 각 부서에 대해 다른 CRL을 인증할 것이다. 사용자가 특정 부서로부터 어떤 사람에 대한 증명서를 확인하고 싶을 때, 그녀는 단지 전체 CRL보다 각부서의 CRL을 확인하기만 하면 된다. CRL을 나누는 다른 방법은 철회 사유에 의한 것이다. 이름변경에 의한 철회는 보안 협약에 의한 철회와 다른 CRL에 위치할 수 있다. 그 타협리스트는 갱신될 수 있고, 모든 철회들이 발생할 때마다 처리해야 할 필요 없이 자주 확인 될 수 있다.

Delta-CRLs

이 확장은 CRL의 크기를 줄이는 다른 방법을 제공한다. 전체 CRL을 인증하는 것 보다, CA는 단지 마지막으로 전체 CRL이 인증된 후로 발생한 변화들의 리스트를 인증하기 만 하면 된다. 자기 자신의 CRL 데이터베이스를 유지하는 사용자들은 계산시간 과 대역폭을 아끼기 위해 전체 CRL의 모든 엔트리들을 처리하고 다운로드 해야 할 필요 없이 그들의 사본들을 갱신할 수 있다.

Indirect CRLs

이 확장은 CRL가 CA가 아닌 개체로부터 인증될 수 있게 한다. 이것은 CRL들을 다수의 CA들로부터 모으고 그들로부터 한 분배 기점을 제공한다.

이런 CRL 확장들은 여전히 time-granularity 문제를 극복하지 못한다. 조각으로 분리된 CRL들이나 잦은 delta-CRL 인증이 있을지라도 여전히 더 이상 유효하지 않은 증명서가 쓰일 가능성이 존재한다. X.509v3 구조는 온라인 구조에서 사용되므로 CRL들이 모두 모일 필요가 없다. 그러나 그런 형태로 정의 된 시스템은 아직 없다.

2.4 대상 등록

X.509v3의 확장성은 많은 유연성을 제공해 준다. 그러나 확장성이 제공되는 방법은 국제적 PKI로 사용자 정의된 광범위하게 쓰일 수 있는 응용들을 어렵게 한다.

X.509가 어떤 대상(subject)을 확인할 때마다(가령, 서명 알고리즘, 인증 정책, 사용자정의에 의한 선택적 명칭 혹은 사용자정의에 의한 확장), 국제적으로 정의된 object identifier 구조를 사용한다. OID(Object IDentifier)는 숫자이다. 이것은 다른 OID들과 다른, 유일한 정수들의 수열로 만들어지며, 다음과 같은 수치할당 구조에 의해 만들어진다[2].

본질적으로 어떤 회사나 단체나 값을 할당하는 기관이 될 수 있다. 그 회사는 그것이 정의하는 대상들의 모든 값들에 대해 앞에 값을 붙이는 형태인 prefix 값을 가진다.

〈그림2-5〉에서의 OID에서, 미국 내에서 동작하는 CA가 있다고 가정할 때, CA는 2-16-840-1-45356 같은 OID값이 할당될 것이다. 이 OID값은 그 CA가 관리하는 대상의 OID의 앞에 붙는 값이 된다. CA가 특별한 증명정책을 기록하고 싶다면 특별히 할당된 가령 15라는 숫자가 CA조직의 정책 가지 밑으로 할당이 될 것이다. 가지번호 3번이라는 정책 번호 아래로 할당 될 때, 그 CA의 증명 정책은 2-16-840-1-45356-3-15 이라는 개체 숫자를 부여받게 된다. 이 시스템은 개체들에 숫자 부여하는 일을 잘 수행한다. 그리고 X.509에서 사용된다.

가령 〈그림2-5〉에서, CA는 증명서에 대한

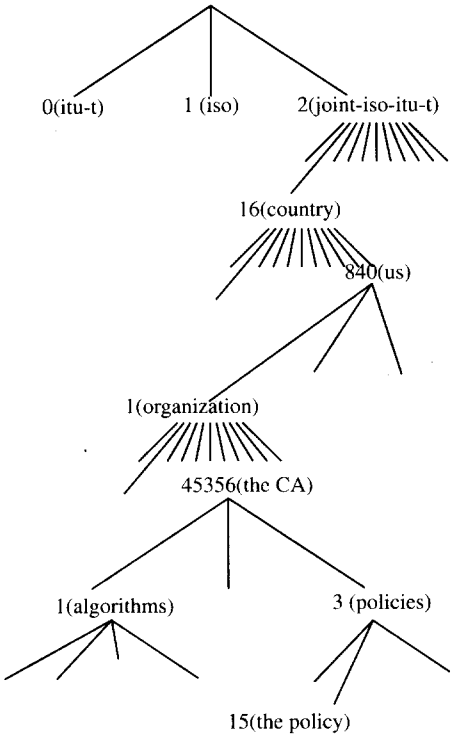


그림2-5 대상등록(Object registration)의 예

어떤 정책을 사용한다고 하자. 그 정책은 단지 그 CA에 OID로써 증명될 수 있을 것이다. 그 OID값들의 의미에 대한 우선적 동의 없이 OID가 사용된다면 문제가 발생한다. 만약 우리의 예제에서 그 CA가 그들의 증명서에 그들의 정책을 사용하길 원한다면 그들은 증명서를 사용하고자 하는 개체(사용자 혹은 대상 혹은 CA)에게 그들의 정책을 나타내는 OID의 의미를 미리 알려 주어야만 한다. 그렇지 않으면 개체가 2-16-840-1-45356-3-15 라는 값을 볼 때 그 정책을 이해할 방법, 즉 그 값이 무엇을 의미하는지 알지 못하게 된다.

또한 같은 객체가 다수의 OID값을 가질 때에 혼란이 발생할 수 있다. 예를 들어 SHA-with-RSA같은 서명 알고리즘에 두 CA가 각각 하나씩의 OID를 부여한다고 가정해보자. 그들의 사용자가 사용하지 않는 한 문제는 없지만, 하나의 CA에 속한 사용자가 그 다른 쪽의 CA에 의한 증명서를 사용하고자 할 때, 그는 SHA-with-RSA에 부여된 두 번째 CA에 의한 OID값을 인식 할 수 없게 된다. 실제로는 그 증명서를 가지고 충분히 원하는 작업을 할 수 있지만, 그 증명서의 대상의 서명을 확인 할 수 없다. 이 문제는 두 CA가 그들의 조직을 연결하고자 할 때 만들어진다. 그럴 때에 CA들은 그들의 사용자에게 같은 OID에 대한 정보를 주어야 하거나 혹은 한쪽 OID를 바꾸고 그 쪽 사용자에게 알려야 한다.

OID문제는 X.509의 확장성에 대해 거대한 규모에서 자유로이 사용되는 것을 방해한다. 누구든 새로운 확장을 해나가는 사람은 관계된 OID에 대한 일들을 해야하기 때문이다.

현재로써는 하나의 OID의 의미를 결정할 시스템적 도구가 없다. 정기적으로 알려지는 것도 아니

고, 중앙 저장소에 저장되는 것도 아니다. 단지 OID의 의미를 알 방법은 OID를 만든 사람에 의해서만 알 수 있는 방법밖에 없다.

3. X.509의 PKI 기본 특성들

본 장에서는 어떻게 X.509가 PKI의 특성을 만족시키는지 살펴보고자 한다. 〈표3-1〉을 통해 이러한 사항을 쉽게 파악할 수 있다.

표3-1 X.509 PKI의 전체적 특성

	Versions 1.2	Version 3
Certificate information	X.500 names. CA & subject 명칭들, subject 공개키, 유효기간을 포함한다.	어느 정보든지 포함할 수 있다.
CA arrangement	정해진 CA 배열이 없지만 교차증명을 포함하는 일반적 계층구조가 권장된다. 신용을 제한하는 구조를 가지지 않는다.	신용을 제한하는 구조가 제공된다. 교차증명을 포함하는 일반적 계층구조가 권장된다.
CA 〈-〉 Subject 〈-〉 User relationship	CA들 대상(subject) 그리고 사용자들이 다르다.	
CA 〈-〉 Subject 〈-〉 User trust relationships	각 사용자는 적어도 한 CA를 완전히 믿도록 요구된다. CA들은 대상(subject)과 다른 CA들과의 신용관계를 다루는 메커니즘을 가지지 않는다.	각 사용자는 적어도 한 CA를 완전히 믿도록 요구된다. CA들은 어떻게 그들의 신용을 대상과 다른 CA들에게 줄 것인지 에 대해 제한할 수 있다.
Certificate validation method	Offline. 모든 메시지와 증명서 체인이 저장되고 전송된다. 비준은 각 증명서의 비준 기간을 확인하거나 그 증명서가 가장 최근의 CRL에 등록되지 않음을 확인하는 것에 의해 이루어진다.	Offline, 그러나 아직 정의되지 않은 확장을 통해 online으로도 이루어질 수 있다.
Certificate revocation method	CRL(certificate Revocation List)	복잡한 CRL 메커니즘으로 Online 방법이 확장을 통해 정의될수 있다.
Identity vs. credential certificates	Identity 증명서만 지원. Credential(속성) 증명서는 X.500디렉토리 엔트리에 덧붙여질 수 있다	주로 identity 증명서들을 가짐. 어떤 표준들은 credential적 기능을 제공하기도 한다. 완전한 credential증명서를 제공하도록 확장될 수 있다.
Irrefutability and strong authentication	X.500엔트리의 정확성에 기반한 인증 강도. CA는 증명서가 오류로 발급되지 않도록 해야한다.	CA는 여전히 증명서의 정확성에 책임이 있다. 하지만 비X.500명칭의 사용은 이것을 어렵게 한다.
In-band vs. out-of-band authentication	사용자들은 적어도 하나의 CA키를 out-of-band로 얻어야 한다. 또한 OID들의 확장적 사용은 새로운 확장이 정의 될 때마다 out-of-band 통신을 필요로 한다.	
Anonymity	X.500엔트리가 익명적일 수 있는 정도로만 익명적이다.(X.500엔트리에 영향을 받는다.)	확장에서 완전한 익명 서버를 제공할 수 있다.

4. Privacy Enhanced Mail

본 장에서는 X.509v1에 기반한 Privacy Enhanced Mail PKI를 살펴보고자 한다.

4.1 PEM의 개관

Privacy Enhanced Mail(PEM)은 1993년 초 암호화가 증가된 전자메일에 대한 인터넷 표준으로써 제안되었다[3],[4],[5],[6]. 이것은 공개키 암호화를 사용하여 인터넷 전자메일에 확실성, 인증, 메시지 무결성보장, 그리고 부인방지(non-repudiation of origin)를 제공해준다. 끝으로 PEM을 지원하는 인터넷 PKI가 제안되었다. 다양한 이유에 의해 그 표준은 인터넷사회에서 수용되지 않았다. 제안된 PKI가 인터넷의 평등한 형태의 구조에 적당하지 않은 것으로 판명이 되었기 때문이다.

PEM PKI는 〈그림4-1〉와 같이 하향식 CA 계층구조를 사용한다. 그것의 루트는 인터넷 정책 기록기관(internet policy registration authority, IPRA)이다. IPRA는 전체 인터넷에 대한 국제적 증명 정책을 수립한다. IPRA는 단지 정책 증명 기관들(policy certification authorities, PCAs)을 증명해준다. 각 PCA는 보다 특별한 증명 정책을 수립하고 PCA의 정책들을 따르는 CA 조직들을 증명해준다. PCA의 정책들을 수월하게 이용하기 위해 독립적으로 다른 정책을 가진 적은 수의 PCA들이 존재하도록 기대되었다. PCA들 아래에 있는 CA는 다른 CA들이나 PEM 사용자들을 증명해 줄 수 있다.

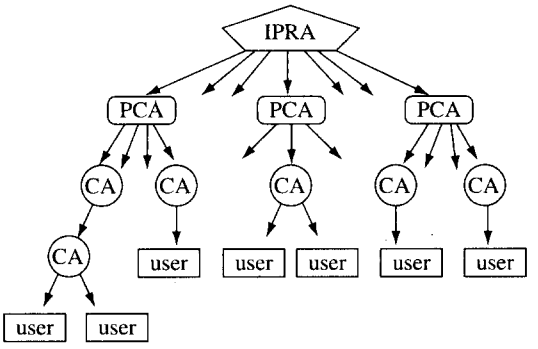


그림4-1 The PEM CA hierarchy

이런 종류의 CA 배열은 각 개체들 사이에 계층구조가 존재하면 잘 돌아간다. 예를 들어 미국방성은 성공적으로 공개키 기반조직에 하향식 계층구조를 사용하였다. 국방성은 원래 이런 구조로 이루어져있다. 그래서 그 계층 구조는 일을 잘 수행할 수 있다. 그러나 인터넷은 계층 구조적 측면을 거의 가지지 않는다. 또한 X.509v1은 증명 정책을 공표할 메커니즘을 기본적으로 가지고 있지 않기 때문에 PCA들의 정책들은 인터넷 RFC들을 통해 배포되었다. 그리고 사용자들은 그들과 접촉하는 CA들뿐만 아니라 여러 PCA들의 정책들을 항상 가까이 하고 있도록 요구된다.

본질적으로 PEM은 인터넷에 직접 X.509v1을 채용하려는 시도였다. 각 개체들(사용자, CA들, PCA들, IPRA)에는 X.500에서 분배된 고유이름(DN)이 할당된다. CA를 증명하기 전에 PCA는 CA의 DN이 유일한지를 결정하기 위해서 IPRA에 의해 유지되는 데이터베이스에 질의를 한다. 또한 CA들은 그들의 DN들을 따라야 하며, CA들은 대상의 DN이 인증자의 (CA's) DN을 따랐는지 증명서에 서명한다.

DN 데이터베이스는 도처에 존재해야 하는 X.500 디렉토리의 부족 때문에 요구되었다. 어떤 두 PCA도, 같은 PCA아래 어떤 두 CA도 같은 DN을 가지지 않지만, PCA들은 디렉토리 이름 공간의 연결되지 않은 부분들에서 조

직적인 CA들을 증명하도록 요구되기 때문에, 그리고 X.500 디렉토리들이 여러 곳에 존재하지 않기 때문에, PCA들 사이의 협력으로 CA DN들의 유일함을 증명하는 데에는 좀더 수월함이 요구된다. 또 여러 다른 CA들은 같은 DN을 공유할 수 있는 특별한 조건이 있다. 그래서 데이터베이스는 그들을 추적해야 할 필요가 있다. 보다 상세한 것은 [RFC1422]의 3.4.2.2 섹션을 통해 파악할 수 있다.

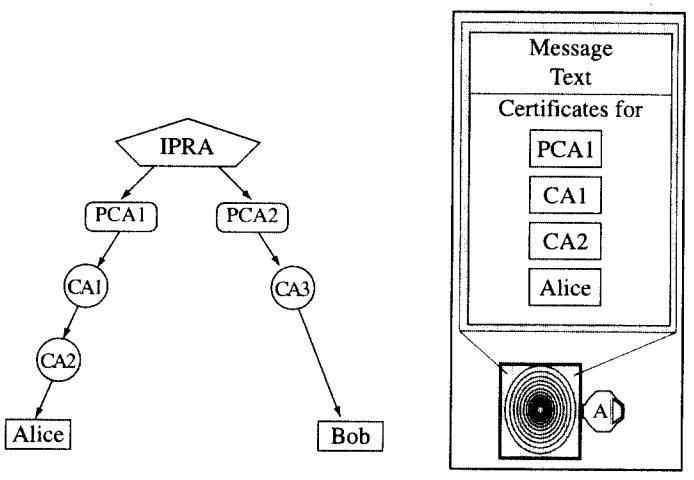
4.2 PEM의 운영

PEM 동작의 여러 면을 보여주기 위해 Alice가 Bob에게 메시지를 보내길 원하는 상황을 가정하자. 그녀는 그와 한번도 통신을 해본 적이 없고 둘 다 〈그림4-2〉에서 보여주는 증명 구조 내에서 움직인다고 가정한다.

Alice가 메시지를 작성하고 그녀는 그녀와 IPRA사이의 인증 경로를 덧붙인다. 예를 들어 그녀 자신, CA2, CA1, 그리고 PCA1에 대한 인증경로 순으로 경로를 덧붙일 수 있을 것이다.

그녀는 이들 증명서를 인증하지 않는다는 것을 주목하라. 그녀는 단지 그녀의 메시지에 그것들을 포함하기만 할뿐이다. 그녀는 그녀가 CA2에 의해 그녀 자신의 증명서가 인증이 될 때 그것들을 포함시켰다. 그리고 나서 그녀는 증명경로를 포함하는 완전한 메시지에 서명을 한다.

Bob이 그 메시지를 받고 그것을 비준하고자 할 때, 그는 IPRA 키를 가지고 인증서가 만료가 된 것인지 철회가 된 것인지 Distinguished Name



(a) certification structure (a) Alice's message

〈그림4-2〉 PEM 의 예

의 종속관계가 관찰되는지를 확인하면서, Alice의 공개키를 얻기 위해 메시지에 포함된 인증경로를 인증하기 시작한다.

만약 Bob이 계층구조의 PCA1의 가지를 따라 인증경로를 추적하는 첫 번째 경우라면 그의 PEM 프로그램은 Bob에게 확실히 PCA1의 인증서를 받아들일 것인지를 묻게 된다. 이것은 Bob에게 그의 새로운 인증정책 영역을 시작하는 것에 대해, PCA1의 정책을 다시 확인하게 경고를 해주는 것이다. PCA1의 하위에 CA들 정책뿐만 아니라 얼마나 PCA1이 그것에 속한 CA들에 CA들 자신의 정책을 제한하게 할 것인지 결정하게 한다. 이 정책에 대한 사전지식 요구는 Bob이 메시지의 원천이 내용과 일치하는지를 결정하게 도와준다.

4.3 Privacy Enhanced Mail PKI

성가신 PEM PKI환경이 인터넷 표준으로써의 PEM의 몰락을 초래했다. 주된 교훈 중 하나는 PEM처럼 경직되고 계층적인 모델은 국제적 인터넷에서 잘 움직여지지 않는다는 것이다. PEM PKI의 특징을 다음과 같이 파악할 수 있다.

- **Certificate information**
  PEM certificates 는 X.509v1 certificates
- **CA arrangement**
  PEM 는 경직되고 하향식의 CA 계층구조
- **CA 〈-〉 Subject 〈-〉 User relationship**
  사용자(Users), 대상(subjects)은 CA와 다르며, PEM 사용자는 CA가 될 수 없음
- **CA 〈-〉 Subject 〈-〉 User trust relationships**
  모든 증명 경로는 IPRA의 키를 가지고 시작하기 때문에 모든 PEM 사용자는 전적으로 IPRA를 믿어야 한다. 사용자는 또 증명경로에 나타나는 PCA들과 CA들을 믿어야 한다. 사용자는 PCA의 정책들에 민감해야 하고 PCA와 CA가 그런 정책들로부터 벗어나지 않았음을 믿어야 한다.
- **Certificate validation method**
  증명서들은 "online" 상으로 전자메일을 써서 비준이 된다. IPRA의 키를 사용해서 수신자가 비준할 수 있게, 메시지 제작자들은 모든 증명 경로(certification path)를 메시지안내에 있는 그의 키에 포함시켜야한다. 비준이 이루어지는 동안 사용자는 어떤 증명서도 철회되지 않았고 만기가 되지 않았음을 그리고 DN 종속관계가 만족되었음을 확인 해야한다.
- **Certificate revocation method**
  PEM은 전자메일을 통해 사용자간에 배포된 X.509v1 CRL을 사용한다.
- **Identity vs. credential certificates**
  PEM certificates 는 순수한 X.509v1 identity certificates 이다.
- **Irrefutability and strong authentication**
  PEM 구조는 강한 인증을 줄 수 있다.
- **In-band vs. out-of-band authentication**
  각 사용자는 어떤 out-of-band수단을 통해 IPRA의 키를 구해야한다. 그 키가 주어지면 다른 모든 인증은 in-band로 이루어진다
- **Anonymity**
  PEM은 "PERSONA" CA들을 호출함으로서 익명성 메커니즘을 제공한다. PERSONA CA는 그것의 대상(subject)의 정체성을 확실한 방법으로 인증하지 않는다는 면에서 PEM CA와 다르다.

5. 결 론

인터넷에서 X.509v3 기반의 PKI를 정의하려는 노력이 수행중이며, PKIX라 불리는 제안이 초기 설계 단계에 있다. 그것은 몇몇 다른 확장성을 가지고 X.509v3 표준을 따르고 있으며 가능한 한 양쪽 표준을 가지도록 하려는 노력이 있다. 사실, X.509v3를 만들려는 많은 사람들이 PKIX에 연관되어 있다. 최종 PKIX에 대해 언급하는 것은 이르지만 우리는 PKIX가 X.509v3 PKI와 비슷할 것이라고 예상할 수 있다.

X.509v3를 사용시 주된 결점은 object ID number에 대한 의존성이다. OID들의 의미를 알려낼 방법 없이는 X.509v3 PKI 사용시 모든 개체들이 모든 OID들을 이해 할 수 있다고 생각하기 힘들기 때문이다. PKIX는 이 문제를 해결해야 한다. PKI 기능을 만드는데 있어 상대적으로 작은 OID들의 집합이 정의될 수 있기를 바란다. X.509가 기본적으로 거의 혹은 전혀 속성 증명서를 포함하지 않고 identity PKI가 되려한다고 하면 그런 집합을 만드는

것이 가능할지도 모른다. 그러나 그러한 일은 가능할 지라도 실제로 생기는 것은 어렵다.

공개키방식에서 제일 중요한 부분은 공개키를 누가 관리하는가, 관리하는 조직들간의 관계, 온라인 상만으로도 이루어 질 수 있기 위해 서로를 어떻게 식별할 것인가 하는 문제들이다. 앞으로 국내에서도 전자상거래가 이루어지기 위해서는 분명 이런 문제들이 해결되어야 할 것이다. 공개키 관리 조직들이 어떻게 통신상에서 자리 잡아야 하는지, 사용자와 인증 대상간을 어떻게 연결해야 하는지 하는 문제들에 대한 완전한 해답이 아직 만들어지지 못한 상태이다. 급속도로 발전하는 인터넷에서 사용자들이 쉽게 자신의 정보에 대한 보안을 기할 수 있는 인간 중심의 공개키 기반 구조의 구축을 위한 연구와 노력이 지속되어야 할 것으로 생각된다.

참 고 문 헌

[1] Secure Electronic Transaction (SET) Specifications. MasterCard and Visa. May 1997.

[2] Ford, W. and Baum, M. Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption. Prentice Hall, 1997.

[3] Linn, J. Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. February 1993.

[4] Kent, S. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management. February 1993.

[5] Balenson, D. Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers. February 1993.

[6] Kaliski, B., Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services. February 1993.

□ 著者紹介

김 상 균

1993년 10월 ~ 1994년 7월 터보정보통신 개발팀장
1996년 2월 중앙대학교 제어계측공학과 졸업(학사)
1995년 3월 ~ 1996년 6월 정화기술(주) 과장
1998년 8월 연세대학교 산업공학 졸업(석사)
1996년 10월 ~ 현재 사이버게이트 인터내셔널 기술이사/기술기획실장
1998년 8월 ~ 현재 연세대학교 인지과학과 박사과정

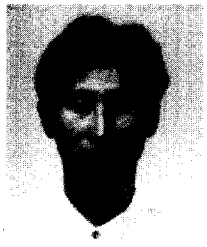
※ 주관심분야: 정보보안 및 정보전쟁, 산업정보 시스템, 전자상거래

□ 著者紹介

백 종 현

1996년 2월 순천향대학교 전자공학과 졸업(학사)
1998년 2월 순천향대학교 대학원 전자공학과 졸업(석사)
1998년 3월 ~ 현재 사이버게이트 인터내셔널 주임연구원

※ 주관심분야: 공개키 기반구조, 전자현금 프로토콜, 네트워크 보안



이 강 석

1997년 2월 순천향대학교 전자공학과 졸업(학사)
1997년 3월 ~ 현재순천향대학교 전자공학과 석사과정

※ 주관심분야: 공개키 기반구조, 네트워크 보안, 전자상거래

이 석 준

1997년 2월 고려대학교 물리학과 졸업(학사)
1997년 3월 현재 사이버게이트 인터내셔널 주임연구원

※ 주관심분야: 정보보안 및 정보전쟁, 네트워크 보안, 전자상거래