X.509 PKI 인증서 프로파일 분석

이윤경* · 한종욱*

*한국전자통신연구원

Analysis of Various PKI Certificates Profile

Yun-kyung Lee* · Jong-wook Han**

*Electronics and Telecommunications Research Institute

E-mail : neohappy@etri.re.kr

요 약

본 논문에서는 PKI에서 가장 기본이 되고 중요한 요소인 X.509 인증서의 구조를 기술하였다. X.509 인증서는 기본 필드들과 버전 2 인증서에서 추가된 unique identifiers field, 그리고 버전 3 인증서에서 추가된 확장필드들로 구성되어 있다. 버전 3의 확장필드들은 기본 필드들로 부족한 부분을 채우기 위한 필드로써, 현재 인터넷에서 사용되는 인증서용으로 정의된 확장필드값들과 그 의미에 대해 기술하였다.

ABSTRACT

This paper describes X.509 certificate profile, which is basic and important element in the PKI. X.509 certificate consists of basic fields, unique identifiers fields(added in version 2 certificate), and extension fields(added in version 3 certificate). extension fields of version 3 certificate supplement basic fields. We describes extension fields value and its meaning in current internet certificate.

키워드

PKI, certificate, X.509, certificate profile, certificate extensions

I. 서 론

인터넷뱅킹이 널리 사용되면서 인증서는 생필품의 하나로 자리잡게 되었다. 그리고 전자상거래에서도 고액결재시 인증서를 이용한 인증을 필수로 하고 있다. 이들 모두 공개키 기반구조의 안전성에 근거한 것으로, 인증서는 공개키 기반구조의 기본요소라 할 수 있다.

X.509 인증서는 1988년 X.500 디렉토리 억세스를 제어하기 위해서 사용될 목적으로 나왔으나, 곧 범용으로 인증하는데 사용할 수 있도록 개정되었고, 이것이 발전하여 오늘날의 X.509 인증서가 되었다. 인증서의 기본 개념은 명함과 신용카드의 특성을 갖는 디지털 물건이라 할 수 있다. 즉, 인증서를 가진 사람, 즉, private key를 가진 사용자의 이름, 사용자의 회사명, 사용자와 접촉할 수 있는 정보등을 포함하고 있다. 또한 인증서의 내용을 함부로 변경할 수 없으며, 인증서 내용의 유효성을 즉시 결정할 수 있다. 또한 인증서로부터 그 인증서가 적용될 수 있는 어플리케이션을 결정할 수 있다.

본 논문에서는 이러한 X.509 인증서의 구조와 구성요소에 관하여 기술하고자 한다.

II. X.509 Certificate Profile

X.509 인증서는 공개키 기반구조에서 사용하는 인증서들 중 가장 기본이 되는 인증서 이다. X.509인증서라는 이름은 이 인증서가 처음 정의

된 문서인 CCITT Recommendation X.509를 따서 지어졌다. 이 문서는 X.500 Directory에 대한 인증구조를 기술한 문서로써, directory를 지원하는 차원에서 인증서의 개념이 기술되어 있었다. 그후 일반적인 목적의 PKI개발로 전환되어 현재의 X.509인증서(버전 2와 버전 3)가 나오게 되었고, 현재 사용하는 대부분의 인증서는 X.509버전 3 형태를 따른다. X.509 인증서의 기본요소만으로 이루어진 인증서가 버전1 이고, 버전2에서는 "reuse of names"를 외치면서 'IssuerUniqueID' 필드와 'SubjectUniqueID'필드가 추가되었다. 또한 버전3에서는 인증서의 확장필드가 추가되었다.

X.509는 1988년 처음 나왔고, 그 후 IETF에서 인터넷용 X.509인증서의 개요를 작성하여 1999년 3월 RFC2459[1]를 통해 발표하였다. 그리고 RFC2459를 업그레이드하여 2002년 RFC3280[2]을 발표하였다.

X.509 인증서는 그림1에서 볼 수 있듯이, tbsCertificate(to-be-signed certificate)와 서명알고리듬, 서명값 필드로 구성되어 있다. 그림 1에서 짙은색으로 표현된 부분은 필수필드이고, 다른 부분은 옵션필드이다. 각 필드의 의미를 살펴보자.

1) version: 옵션이다. version필드가 생략되면 버전1 인증서를 의미한다. 버전1 인증서는 그림1에서 unique identifiers 와 extensions를 생략한 형태이고, 버전2 인증서는 unique identifiers 부분은 포함, extensions는 생략된 형태이다. 버전3 인증서는 unique identifiers와 extensions를 포함한 형태인데, unique identifiers 부분은 주로 생략된다.

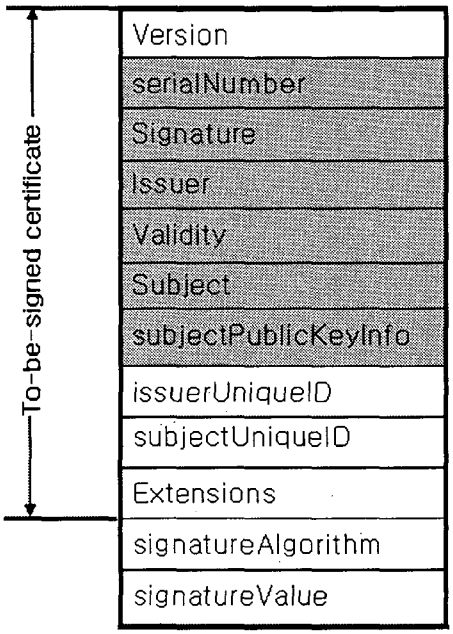

그림 4 X.509 인증서 구조

2) serialNumber: 인증서 발급시 인증서에 할당된 상수값으로, 특정 issuer가 발행한 인증서들에 대해서는 유일한 값이된다. 인증서를 구분하는데 참조정보로 활용된다.

3) signature: signature algorithm 필드의 복사본으로, 인증서 서명에 사용된 알고리듬이 적혀있다. 이 필드는 tbsCertificate에 포함되므로, 디지털서명에 의해 보호된다.

4) Issuer: 인증서를 발급한 인증기관을 기술하는 필드로써 distinguished name[1] 형태로 표시된다. 이 필드는 반드시 값을 가져야 한다.

5) Validity: 인증서 유효기간을 나타낸다. notBefore, notAfter로 구성되어 있고, 2049년 이전의 기간에 대해서는 YY로 표현되는 UTC time 표현방법을 사용하고, 2050년 이후의 기간에 대해서는 YYYY로 표현되는 generalized time 표현방법을 사용한다.

6) Subject: 인증서 소유자(인증서에 적힌 공개키에 대한 비밀키를 소유한 사람)를 distinguished name 형태로 표현한 값이다.

7) SubjectKeyInfo: 인증서 소유자(subject)의 공개키 정보와 공개키 알고리듬의 OID[2](Object Identifier) 및 파라미터 정보를 포함한다.

8) issuerUniqueID and subjectUniqueID: issuer와 subject의 이름이 중복되는것을 막기위해 만든 필드인데, RFC3280에서는 이 필드의 생략을 권고한다.

9) extensions: 버전3 인증서에만 있는 옵션필드이다. 버전1 인증서의 항목 만으로는 인증이 힘들기 때문에 extensions 필드가 추가되었다. 각 extension은 extension identifier, criticality flag, extension value로 구성되어 있다. extension identifier는 각 extension을 구분하는 OID 이고, criticality flag는 extension의 중요도를 나타내는 것으로 criticality flag가 'critical'인 extension이 검증에 실패하면 반드시 '인증실패'가 되고, 'non-critical'인 extension은 검증에 실패하더라도 이 결과가 무시된 채 인증과정이 계속 진행될 수 있다. extension value에는 해당 extension의 내용이 적혀있다.

1. Certificate Extensions

1) distinguished name(DN)은 country(c=), organization(o=), organizational unit(ou=), locality(l=), common name(cn=)으로 구성된다. domain component(dc=)가 추가되기도 한다. 예: c=US, o=Fox, ou=R&D, cn=alice

2) 공개키 알고리듬들과 파라미터에 할당된 값으로 RSA의 경우 NULL 파라미터 값과 함께 OID 1.2.840.113549.1.1.1로 정의되어 있다.

X.509 인증서에서 확장필드는 CA에서 정의해서 사용할 수도 있지만, 표준으로 나와있는것을 사용할 것을 권고한다. 이는 다른 CA가 발급한 인증서와의 상호 호환성을 위함이다. X.509 인증서 표준에 정의된 확장필드는 다음과 같다.

(1) Basic constraints extensions

해당 인증서가 CA용 인증서인지, end-entity용 인증서인지를 명시하기 위한 확장필드이다. 또한 유효한 CA의 수를 명시함으로써 인증서 검증을 명확하게 할 수 있다. 예를들어, end-entity 인증서를 발행하는 CA의 경우 path length는 '0'이 된다. critical 혹은 non-critical이 될 수 있고, CA의 인증서에는 이 확장필드의 사용을 추천하고, end-entity 인증서에서는 이 확장필드의 사용을 권고하지 않는다.

(2) Issuer alternative name extensions

인증서를 발행한 CA의 general name을 나타내는 확장필드이다. 그러나 end-entity의 입장에서 CA의 general name은 별로 중요한 요소가 아니므로 non-critical이다.

(3) Subject alternative name extensions

end-entity의 인증서에는 아주 유용한 값이 되는데, 사용자의 인증서의 경우에는 e-mail 주소와 DNS name이 되고, 컴퓨터(서버)용 인증서의 경우에는 URLs와 DNS names가 된다. 또한 Ipsec 라우터의 인증서의 경우에는 IP address와 DNS names가 된다. 기본 인증서 필드들 중 subject 필드의 값이 zero일 경우, subject name extension이 반드시 포함되어야 하고, critical이 되지만, subject 필드값이 zero가 아니면, subject name extension은 non-critical이 된다.

(4) Name constraints extensions

메쉬구조의 PKI에서 subject와 issuer 이름이 겹치는것을 막기위한 확장필드이다. 두 가지 타입이 있는데, 하나는 허용되는 이름들을 적어두는 것이고, 다른 하나는 허용하지 않는 이름들을 적어두는 것이다. 우리나라처럼 hierarchical PKI구조에서는 거의 사용되지 않는다.

(5) Key usage extensions

인증서에 기술된 공개키의 사용 용도를 기술하는 확장필드이다. 9가지 시큐리티 서비스들중 해당하는 서비스에 대한 bit를 '1'로 표시한다. 9가지 KeyUsage bit string은 다음과 같다.

```
KeyUsage ::= BIT STRING{
    digitalSignature    {0},
    nonRepudiation      {1},
    keyEncipherment     {2},
    dataEncipherment    {3},
    keyAgreement        {4},
    keyCertSign         {5},
    cRLSign             {6},
    encipherOnly        {7},
    decipherOnly        {8}   }
```

위 9가지 항목들 중 digitalSignature는 인증서의 공개키가 서명확인에 사용될 수 있음을 나타내고, keyCertSign, cRLSign, nonRepudiation을 제외한 시큐리티 서비스에서 사용된다. 또한 nonRepudiation은 공개키가 부인방지 서비스를 제공하기 위한 서명검증에 사용될 수 있음을 나타낸다. keyEncipherment는 공개키가 키 전송에 사용될 수 있음을 나타내고, RSA 키가 key management에 사용될 때 적용한다. dataEncipherment는 공개키가 데이터를 암호화하는데 사용될 수 있음을 나타내고, keyAgreement는 공개키가 key agreement에 사용될 수 있음을 나타내는데, Diffie-Hellman key가 key management를 위해 사용될 때 적용된다. keyCertSign은 공개키가 인증서에있는 서명을 확인하기 위해서 사용될 수 있음을 나타내고, cRLSign은 공개키가 CRLs에 있는 서명확인에 사용될 수 있음을 나타낸다. encipherOnly는 key agreement와 함께 사용되는 것으로, key agreement의 결과 형성된 대칭키가 데이터 암호화에만 사용될 수 있음을 나타낸다. decipherOnly 역시 key agreement와 함께 사용하고, key agreement의 결과 형성된 대칭키가 데이터 복호화에만 사용할 수 있음을 나타낸다.

(6) Extended key usage extension

인증서에 기술된 공개키가 사용될 수 있는 어플리케이션들을 나타내기 위한 확장필드이다. 주로 end-entity용 인증서에서 볼 수 있다. 이 확장필드의 사용예를 들자면 다음과 같다; 공개키가 TLS 웹서버 인증에 사용(id-kp-serverAuth), 공개키가 TLS 웹 클라이언트 인증에 사용(id-kp-clientAuth), 공개키가 다운로드하여 실행할 수 있는 소프트웨어 코드의 서명에 사용(id-kp-codeSigning).

(7) Private key validity extensions

인증서에 있는 공개키에대한 비밀키의 유효기간을 나타내는 확장필드이다. 이 필드는 실제 서명이 생성된 timpstamp가 필요한데, timestamp의 사용이 어렵기때문에 거의 사용되지 않고, [1],[2]에서는 이 확장필드를 사용하지 않을것을 권장한다.

(8) Subject key identifier extensions

인증서 공개키의 해쉬값으로, 짧은 key identifier를 위해서 해쉬값을 자르거나, 섞을 수 있다. 이는 subject가 여러개의 인증서를 가졌을 때, 특히 이들 인증서가 여러개의 CA들이 발행한 것일 경우, 관심있는 공개키를 포함하는 인증서를 빨리 찾는데 도움이 된다. 즉, 인증서 경로를 구성할 때 참고정보가 된다.

(9) Authority key identifier extensions

CA가 여러개의 인증서 signing key를 가지고 있을 때, 특정 인증서 서명에 적절한 한 개의 키를 확인하는데 이용한다. Subject key identifier extensions과 함께 인증서 경로 구성에 도움이 된다. Authority key identifier는 issuer의 이름과 인증서의 serial number로 구성될 수도 있고, 스트링으로 표현될 수도 있다.

(10) Certificate policies extensions

해당 인증서가 어떤 정책하에 발행되었는지를 나타낸다. 이 확장필드는 CA인증서의 경우에는 하위 인증서들에 포함될 수 있는 정책들의 집합을 정의하고, end-entity 인증서의 경우에는 그 인증서가 사용되는 어플리케이션에 대한 정책들을 기술한다. 이 확장필드는 policyIdentifier와 policyQualifiers들로 구성된 정책들의 집합이라 할 수 있는데, poliyIdentifier는 각 정책들에대한 OID 값이고, policyQualifiers는 옵션인데, CA인증서의 경우 CPS[3](certificate practices statement)의 위치를 URL로 표현하고, 사용자 인증서의 경우에는 user notice qualifier(인증서가 사용될 때 display되는 텍스트)가 기술되어 있다.

(11) Policy mapping extensions

CA인증서에만 나타나는 것으로, 두개의 정책 도메인들 간 정책정보를 변환하기 위해서 사용한다. 즉, A라는 CA가 인증서를 발급할 때 사용했던 정책들과 B라는 CA가 인증서를 발급할 때 사용했던 정책들이 서로 다를 때, A라는 CA가 자신의 정책 a'은 B라는 CA의 정책 b'에 해당하는 것이라고 인증서에 기술해 두는것을 말한다.

(12) CRL distribution points extensions

인증서 사용자에게 CRLs를 어디서, 어떻게 얻을 수 있는지를 알려준다. 인증서 발행자(issuer)와 CRL 발행자가 다를경우 CRL issuer는 반드시 포함되어야 한다.

(13) Freshest CRL extensions

Delta CRL 정보를 어떻게 얻을 수 있는지를 나타낸다.

(14) Authority information access extensions

CA의 정책 데이터들과 온라인 인증서 상태를 알아보기 위해서 어떻게 접근할 수 있는지를 나타내는 확장필드이다. access descriptor들의 리스트로 구성되어 있는데, access descriptor는 access method field와 access location field로 구성되어 있다. access descriptor에는 두 가지가 있다: 해당 인증서를 발행한 CA의 인증서를 발행한 상위 CA들의 리스트를 얻는데 사용하는 CA issuers descriptor와 인증서 폐기여부를 알고자할 때 사용하는 OCSP[4] descriptor가 있다.

(15) Subject information access extensions

Authority information access extensions과 동일한데, 단지 CA가 아니라 subject의 추가적인 정보를 제공한다는 점이 다르다.

3) CPS는 CA가 동작하는 방법에 대해 기술한 문서로, 인증서 사용자들은 자신이 이용하고자하는 어플리케이션에 그 인증서가 적합한지를 결정하기위해서 CPS를 읽을 수 있다.

III. 결 론

본 논문에서는 X.509 인증서의 역사에 관하여 간략하게 기술하였고, X.509 인증서의 기본 구조 및 확장 필드에 관하여 상세히 기술하였다. X.509 인증서의 확장필드는 버전 3 인증서에만 있는 것으로 옵션이다. 이 확장필드는 인증서 기본구조에 포함된 내용만으로 사용자를 인증하는데 한계를 느끼고 추가된 필드들이다. 확장필드를 이용하여 인증서 검증을 더 명확하고, 빠르게 할 수 있으며, 인증서의 사용용도 등을 알 수 있다. 현재 사용되는 인증서는 X.509 버전 3 형태의 인증서로써 본 논문에 기술된 내용을 통해서 우리가 사용하는 인증서에 대한 이해를 높일 수 있으리라 본다.

참고문헌

[1] R. Housley, W. Ford, W. Polk, D. Solo, "RFC2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile," January, 1999.

[2] R. Housley, W. Ford, W. Polk, D. Solo, "RFC3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile," April, 2002.

[3] Russ Housley, Tim Polk, "Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure," Wiley Computer Publishing, 2001.

[4] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "RFC 2560: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol-OCSP," June, 1999.