Internet PKI: Part 1 Certificate and CRL Profile

Russ Housley
SPYRUS Chief Scientist

housley@spyrus.com

X.509 Version 3 Certificate Syntax

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version must be v2 or v3
     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version must be v2 or v3
     extensions      [3]  Extensions OPTIONAL
                          -- If present, version must be v3
     }
```

X.509 Version 3 Certificate Syntax *(continued)*

```
Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity  ::=  SEQUENCE  {
     notBefore            UTCTime,
     notAfter             UTCTime  }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
     algorithm            AlgorithmIdentifier,
     subjectPublicKey     BIT STRING  }

Extensions  ::=  SEQUENCE OF Extension

Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING  }
```

X.509 Version 1 Certificate Description

- SERIAL NUMBER identififies the certificate. A unique integer is assigned by the Certification Authority (CA).
- SIGNATURE specifies the the signature algorithm and associated hash function used to sign the certificate.
- ISSUER is the distinguished name of the CA that issued the certificate.
- VALIDITY is the time period that the certificate is valid.
- SUBJECT is the distinguished name of the certificate user.
- SUBJECT PUBLIC KEY INFO contains the user’s public key. For DSA, it may also conatin

X.509 Version 2 & 3 Certificate Description

- ISSUER UNIQUE IDENTIFIER is not used in the PKIX profile.
- SUBJECT UNIQUE IDENTIFIER is not used in the PKIX profile.

- EXTENSIONS is an optional sequence of fields.

Standard Certificate Extensions

- The X.509 Ammendment defines thirteen extenstions:

Authority Key Identifier	recommended, non-critical
Subject Key Identifier	recommended, non-critical
Key Usage	recommended, ***critical***
Private Key Usage Period	***not recommended***
Certificate Policies	recommended, non-critical ***(?)***
Policy Mappings	recommended, non-critical
Subject Alternative Names	recommended, ***non-critical and critical***
Issuer Alternative Names	recommended, ***non-critical and critical***
Subject Directory Attributes	***not recommended***
Basic Constraints	recommended, ***critical***
Name Constraints	recommended, ***critical***

Internet Certificate Extensions

- Three extensions are specified in the PKIX profile:
  - Subject Information Access recommended, non-critical
  - Authority Information Access recommended, ***non-critical and critical***
  - CA Information Access recommended, ***non-critical and critical***

Internet Certificate Extension Syntax

```
SubjectInfoAccessSyntax ::= SEQUENCE OF AccessDescription

AuthorityInfoAccessSyntax  ::=  SEQUENCE  {
     certStatus        [0] SEQUENCE OF AccessDescription,
     certRetrieval     [1] SEQUENCE OF AccessDescription,
     caPolicy          [2] SEQUENCE OF AccessDescription,
     caCerts           [3] SEQUENCE OF AccessDescription  }

CAInfoAccessSyntax  ::=  SEQUENCE  {
     certStatus        [0] SEQUENCE OF AccessDescription,
     certRetrieval     [1] SEQUENCE OF AccessDescription,
     caPolicy          [2] SEQUENCE OF AccessDescription,
     caCerts           [3] SEQUENCE OF AccessDescription  }

AccessDescription  ::=  SEQUENCE  {
     accessMethod          OBJECT IDENTIFIER,
     accessLocation        GeneralName  }
```

X.509 Version 2 CRL Syntax

```
CertificateList  ::=  SEQUENCE  {
     tbsCertList          TBSCertList,
     signatureAlgorithm   AlgorithmIdentifier,
     signature            BIT STRING  }

TBSCertList  ::=  SEQUENCE  {
     version                 Version OPTIONAL,
                                  -- if present, must be v2
     signature               AlgorithmIdentifier,
     issuer                  Name,
     thisUpdate              UTCTime,
     nextUpdate              UTCTime,
     revokedCertificates     SEQUENCE OF SEQUENCE  {
          userCertificate         CertificateSerialNumber,
          revocationDate          UTCTime,
          crlEntryExtensions      Extensions OPTIONAL  }  OPTIONAL,
     crlExtensions           [0]  Extensions OPTIONAL  }

Version  ::= INTEGER  {  v1(0), v2(1) }
```

X.509 Version 2 CRL Syntax *(continued)*

```
AlgorithmIdentifier  ::=  SEQUENCE  {
     algorithm              OBJECT IDENTIFIER,
     parameters             ANY DEFINED BY algorithm OPTIONAL  }
                                 -- contains a value of the type
                                 -- registered for use with the
                                 -- algorithm object identifier value

CertificateSerialNumber  ::=  INTEGER

Extensions  ::=  SEQUENCE OF Extension

Extension  ::=  SEQUENCE  {
     extnId                 OBJECT IDENTIFIER,
     critical               BOOLEAN DEFAULT FALSE,
     extnValue              OCTET STRING  }
                                 -- contains a DER encoding of a value
                                 -- of the type registered for use with
                                 -- the extnId object identifier value
```

X.509 Version 1 CRL Description

- SIGNATURE specifies the the signature algorithm and associated hash function used to sign the CRL.
- ISSUER is the distinguished name of the CA responsible for this CRL.
- THIS UPDATE is the date and time when this CRL was issued.
- NEXT UPDATE is the date and time by which the ISSUER will issue the next edition of the CRL.
- REVOKED CERTIFICATES is a sequence entries consisting of :
  - the SERIAL NUMBER of the revoked certificate.
  - the REVOCATION DATE when the certificate was

X.509 Version 2 CRL Description

- CRL EXTENSIONS is an optional sequence of fields pertaining to the whole CRL.

- CRL ENTRY EXTENSIONS is an optional sequence of fields pertaining to a specific CRL entry.

Standard CRL Extensions

- Five CRL extensions are defined:

Authority Key Identifier	recommended, non-critical
Issuer Alternative Name	recommended, ***non-critical and critical***
CRL Number	recommended, non-critical
Issuing Distribution Point	recommended, ***critical***
Delta CRL Indicator	recommended, ***critical***

- Three CRL entry extensions are defined:

Reason Code	recommended, non-critical
Hold Instruction Code	recommended, non-critical
Invalidity Date	recommended, non-critical

ISO/IEC and ITU-T X.509 Amendment on Certificate Extensions: Changes Since the DAM

Warwick Ford
June, 1996

Areas of Change

- Criticality-related changes
- Key usage bits
- Name forms
- Constraints
- Indirect CRLs
- Hold mechanism
- Delta CRL mechanism
- Matching rules

Note: Every extension syntax change will mean a new OID. Old OIDs to be phased out over time.

Criticality-Related Changes (General)

- Criticality of all extensions reviewed
- Still 3 alternatives:
  - always critical
  - always non-critical
  - critical/non-critical as CA choice
- More extensions are now at CA choice
- Rationale given for each standard rule; more explanation overall
- Any extension that can be critical now has clearly stated mandatory semantics

Criticality-Related Changes (Specific)

- keyAttributes split into 3 extensions:
  - subjectKeyId (always non-critical)
  - keyUsage (CA choice)
  - privateKeyUsagePeriod (always non-critical)
- certificatePolicies changed to “CA choice”
- keyUsageRestriction dropped
- subjectAltNames and issuerAltNames changed to “CA choice”
- nameConstraints and policyConstraints changed to “CA choice”

Key Usage Bits

- Definitions clarified
- No change in the set of bits

Name Forms

- New options added to GeneralName:
  - URI
  - IP-address
  - object identifier
- General Name now usable for any of:
  - end entity
  - CA
  - CRL issuer
  - CRL distribution point
- Clear rules as to non-requirement for implementing all name forms

Constraints

- New name constraints extension
  - takes permitted subtrees and excluded subtrees constraints from X9.55
  - adds the ability to chop the subtrees at numbered levels (min and max)
  - the policy-linking and the complex name subordination options from the old name constraints have been dropped
  - chain validation algorithm is now significantly simplified
- Basic constraints
  - no name constraints
  - simplified to a single Boolean plus a length constraint

Indirect CRLs

- Can have a CRL Issuer whose CRL contains revocation notifications from multiple CAs
- Extensions relating to CRL distribution points enhanced to support this
- New CRL entry extension “certificateIssuer”

Hold Mechanism

- Mechanism retained but simplified
- Expiry date dropped
- A “hold” reason code means that you should currently consider certificate revoked but it may be reinstated later
- If reinstated, entry just disappears from CRL
- If revoked rather than reinstated, reason code changes on entry

Delta CRL mechanism

- Mechanism clarified
- Problems with links to CRL number corrected
- Deltas can now be cumulative from any desired base CRL

Matching rules

- New “exact” matching rules added for all attributes (for admin. purposes)
- Extra fields added to the “certificate match” rule