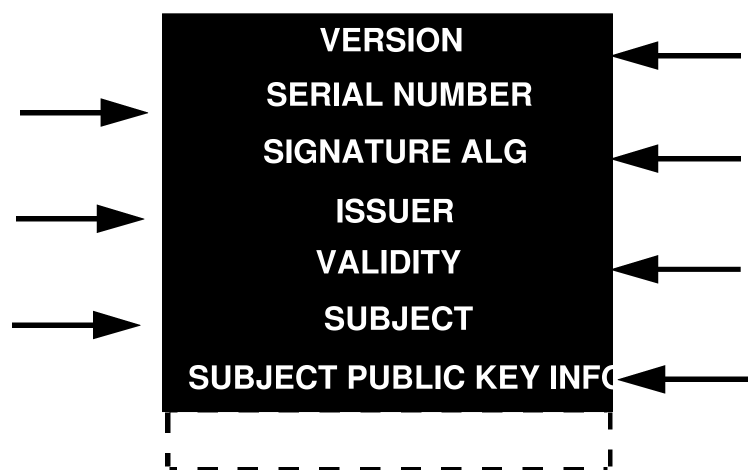
PKIX Certificate Profile

David Solo
solo@bbn.com

X.509 (v1) Certificate Figure



X.509 (v1) Certificate

- **VERSION**
- **SERIAL NUMBER**
- **SIGNATURE ALG**
- **ISSUER**

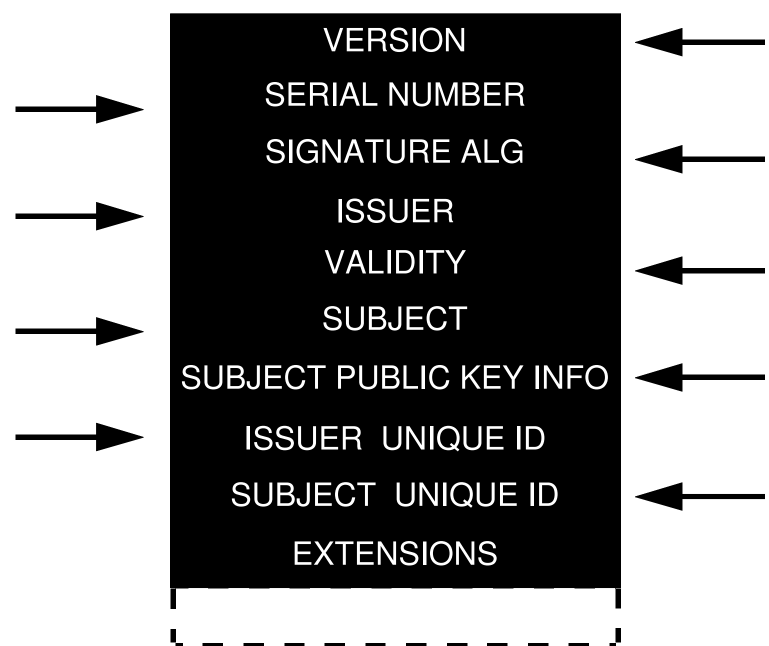
X.509 (v1) Certificate continued

- **<u>VALIDITY</u>**
- **<u>SUBJECT</u>**
- **<u>SUBJECT PUBLIC KEY INFO</u>**
- **<u>SIGNATURE</u>**

X.509 v3 Certificate Extension Features

- **Critical**
-

X.509 (v2 & v3) Certificate Figure



X.509 (v2 & v3) Certificate Description

- **ISSUER UID**
- **SUBJECT UID**
- **EXTENSIONS**

Subject and Issuer UIDs

n

n

n

Alternative Name Syntax

- **subjectAltName**   **issuerAltname**
-

Alternative Name Attributes

n

n

n

Management of Subject Name

n

n

Certificate Policy Syntax

- **CertificatePolicies** **PolicyMappings**
-
-

Certificate Policy

- **CertificatePolicies**

- **PolicyInformation**

- **PolicyElementID**

- **qualifier**

Certificate Policy Mapping

- **PolicyMappings**
- **issuerDomainPolicy**
- **subjectDomainPolicy**

Policy Constraints Syntax

- **policyConstraints**

Policy Constraints

- **policySet**
- **requireExplicitPolicy**
- **inhibitPolicyMapping**

Key Attributes Syntax

n **KeyAttributes**

n

n

Key Usage Attributes

- **KeyAttributes**
- **KeyUsage**
- **PrivateKeyValidity**

Key Usage Restriction Syntax

- **KeyUsageRestrictio**
-

Attributes for KeyUsageRestrictions

- **KeyUsageRestrictions**
- **CertPolicySet**

Conflict between key usage fields

n

n

n

n

n

Basic Constraints Extension Syntax

- **BasicConstraints**
-

CAs and End Entities

- **subjectType**
- **pathLenConstraint**
- **permittedSubtrees** **excludedSubtrees**

Constraints for General Name types

n

n

n

n

CRL Distribution Point Syntax

n **CRLDistributionPoints**

n

CRL Distribution Points

n **DistributionPoint**

n **distributionPointName**

n **reasons**

n

Authority Key ID Syntax

n **AuthorityKeyID**

n

Authority Key ID Attributes

- **keyIdentifier**
- **certIssuer**
- **certSerialNumber**

Subject Directory Attributes Syntax

n **SubjectDirectoryAttributes**

n

NameConstraints Syntax

n **NameConstraints**

n

Certification Path Name Constraints

- **policySet**
- **nameSpaceConstraints**
- **nameSubordConstraints**
- **skipCerts**

InformationAccess Syntax

n **InformationAccess**

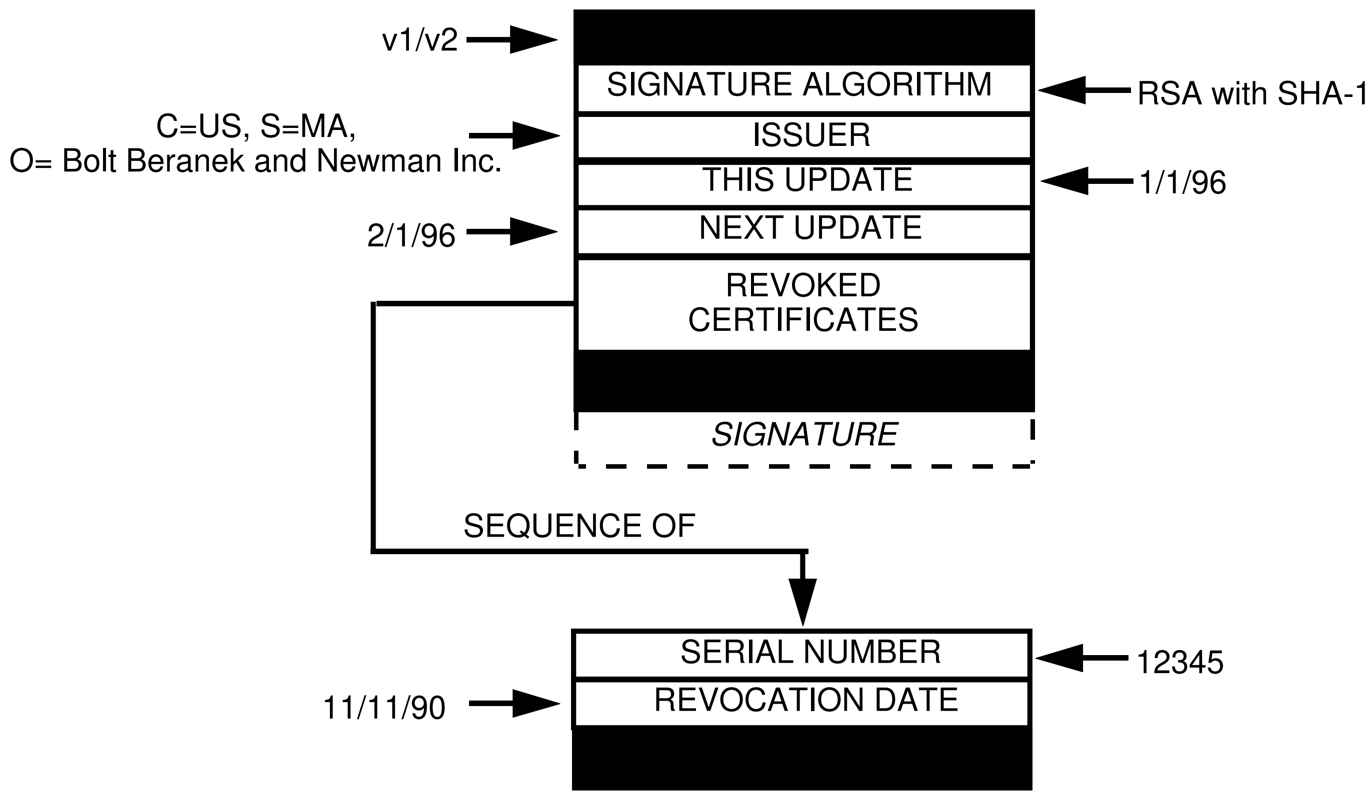
n

Information Access

- **certRetrieval**
- **certValidation**
- **caInfo**
- **userInfo**

Internet PKI: CRL Profile

X.509 Version 2 CRL Format



X.509 Version 2 CRL Syntax

```
CertificateList  ::=  SIGNED  {  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

n ______________________________

n ________

n ________________

n _________________

n _____________________________

n

X.509 Version 1 CRL Entry Description

n

n

n

X.509 Version 2 CRL Description

n ____________________

n ____________________________

Authority Key Identifier CRL Extension

```
AuthorityKeyId  ::=  SEQUENCE  {
     keyIdentifier    [0] KeyIdentifier OPTIONAL,
     certIssuer       [1] Name OPTIONAL,
     certSerialNumber [2] CertificateSerialNumber OPTIONAL  }
        -- certIssuer and certSerialNumber constitute a logical pair,
        -- and if either is present both must be present.  Either this
        -- pair or the keyIdentifier field or all shall be present

KeyIdentifier  ::=  OCTET STRING
```

n

n

n

Issuer Alternative Name CRL Extensio

```
AltNames  ::=  SEQUENCE OF GeneralName

GeneralName  ::=  CHOICE  {
     otherName        [0] INSTANCE OF OTHER-NAME,
     rfc822Name       [1] IA5String,
     dNSName          [2] IA5String,
     x400Address      [3] ORAddress,
     directoryName    [4] Name,
     ediPartyName     [5] IA5String,
     url              [6] IA5String,
     ipAddress        [7] OCTET STRING  }
```

n

n

n

CRL Number CRL Extension

```
CRLNumber  ::=  INTEGER
```

n

n

n

Issuing Distribution Point CRL Extensi

```
DistributionPoint  ::=  SEQUENCE  {
     distributionPoint    DistributionPointName,
     reasons              ReasonFlags OPTIONAL  }

DistributionPointName  ::=  CHOICE  {
     fullName               [0] Name,
     nameRelativeToCA       [1] RelativeDistinguishedName,
     generalName            [2] GeneralName  }

ReasonFlags  ::=  BIT STRING  {
     unused                 (0),
     keyCompromise          (1),
     caCompromise           (2),
     affiliationChanged     (3),
     superseded             (4),
     cessationOfOperation   (5),
     certificateHold        (6)  }
```

n

Issuing Distribution Point (continued)

n

n

n

n

Delta CRL Indicator CRL Extension

```
BaseCRLNumber  ::=  INTEGER
```

n

n

n

n

Reason Code CRL Entry Extension

```
CRLReason  ::=  ENUMERATED  {
     unspecified              (0),
     keyCompromise            (1),
     caCompromise             (2),
     affiliationChanged       (3),
     superseded               (4),
     cessationOfOperation     (5),
     certificateHold          (6),
     certHoldRelease          (7),
     removeFromCRL            (8)  }
```

n

n

n

Expiration Date CRL Entry Extension

n

n

n

Instruction Code CRL Entry Extension

Invalidity Date CRL Entry Extension

```
InvalidityDate  ::=  GeneralizedTime
```

n

n

n

Trust Models

Warwick Ford

March, 1996

X.509 Figure 4

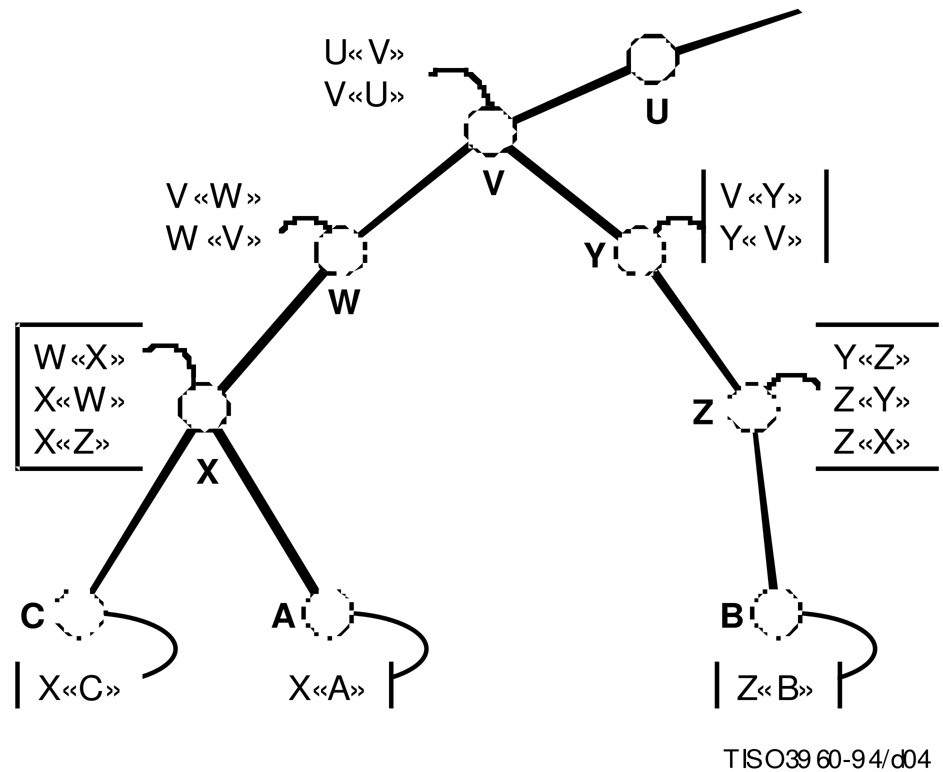


Figure 4 – CA hierarchy – A hypothetical example

X.509 Figure 5

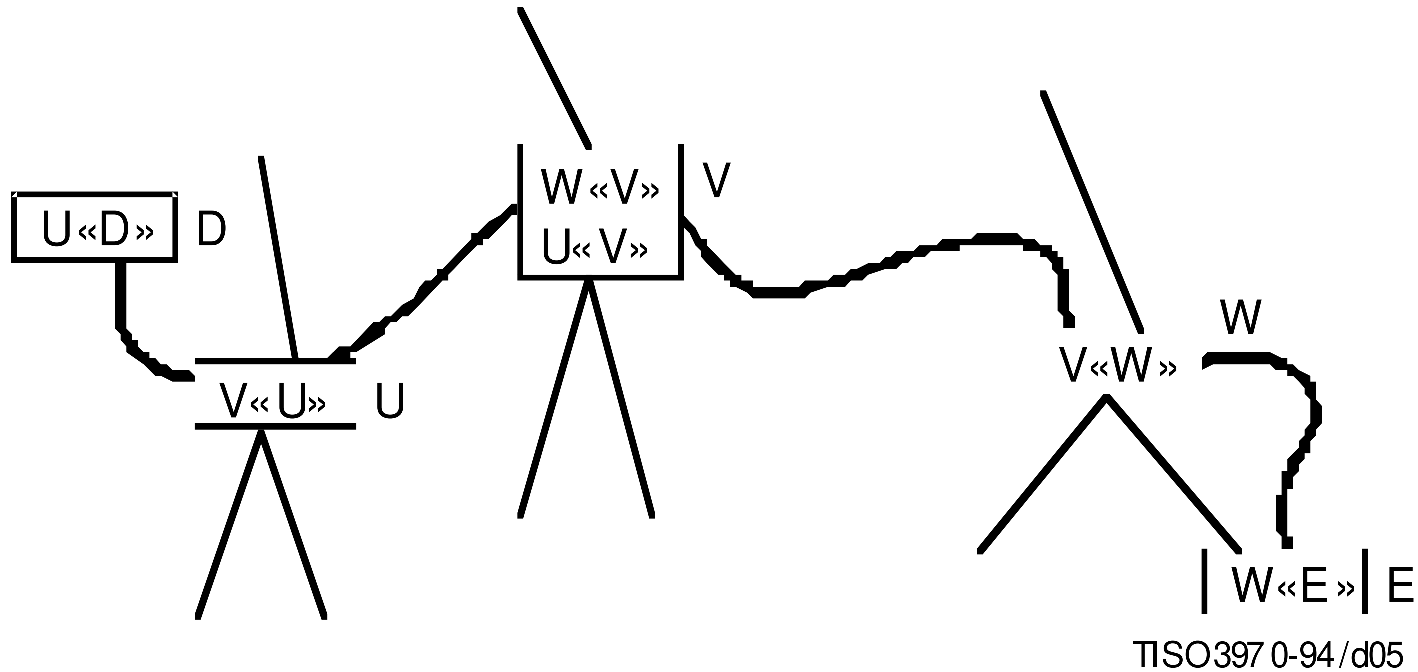
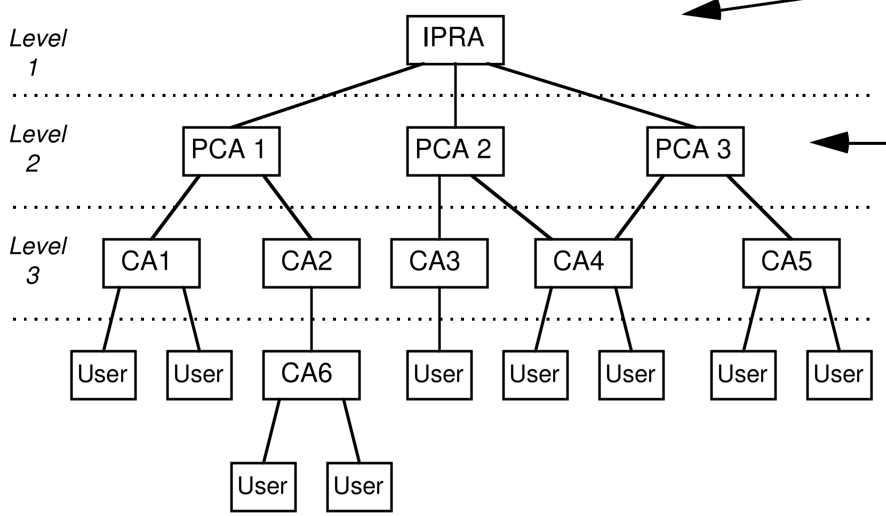


Figure 5 – Non-hierarchical certification path – An example

Privacy Enhanced Mail (PEM)



IPRA = Internet Policy Registration Authority

PCA = Policy Certification Authority

CA = Certification Authority

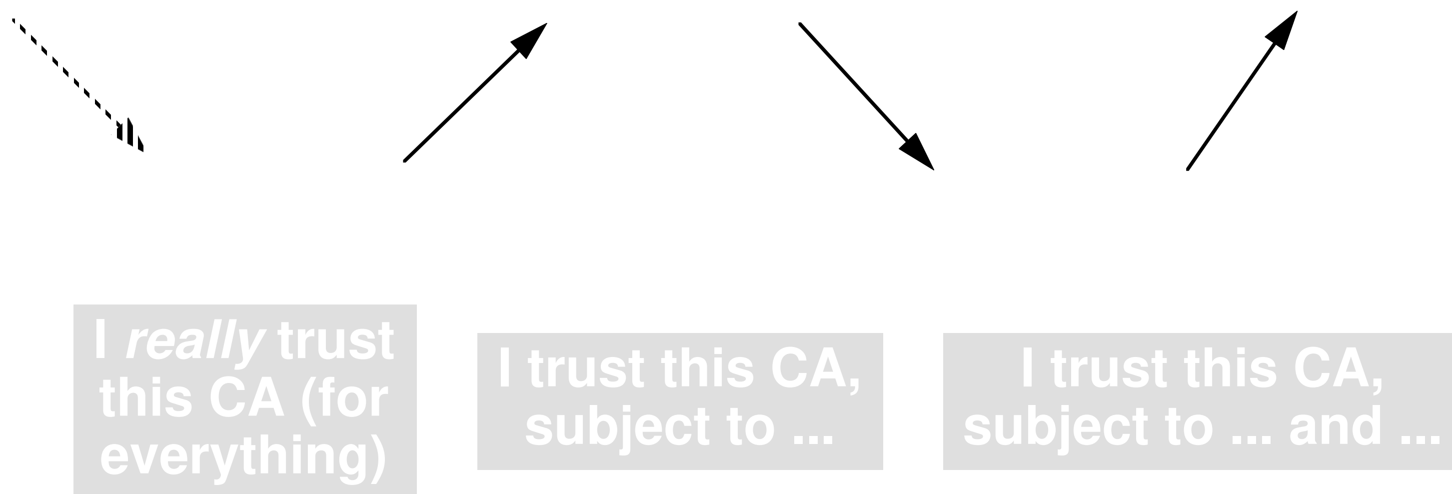
Reasons Behind the PEM Hierarchy

n

n

n

The Trust Model



PKIX Management Protocols