Certificate and CRL Profile

Russ Housley Dave Solo
SPYRUS BBN

4 December 1995

X.509 Certificates and CRLs

Foster interoperability and a reusable public key infrastructure

Common locations within a certificate along with common representations

Support a wide range of environments and internet applications:

electronic mail, IPSEC, WWW, and more

X.509 v3 Certificate

version
serialNumber
signature
issuer
validity

- subject
- subjectPublicKeyInfo
- issuerUniqueID
- subjectUniqueID
- extensions

X.509 v3 Cert Extensions

Subject Alternative Name

Issuer Alternative Name

Certificate Policies

Key Attributes

Key Usage Restriction

Basic Constraints

CRL Distribution Points

Information Access

X.509 v2 CRL

version

signature

issuer

lastUpdate

nextUpdate

- revokedCertificates
  - signature
  - issuer
  - userCertificate
  - revocationDate
  - crlEntryExtensions
- crlExtensions

X.509 v2 CRL Extensions

Encourage Use:

- Authority Key Identifier
- Issuer Alternative Name
- CRL Number
- Issuing Distribution Point

Discourage Use:

- Delta CRL Indicator

X.509 v2 CRL Entry Extensions

Encourage Use:

- Invalidity Date

Discourage Use:

- Reason Code
- Expiration Date
- Instruction Code