Advancing RFC 5280 to Draft Standard

David Cooper

74th IETF, March 2009

Normative Down References

- 3454 – Preparation of Internationalized Strings ("stringprep")
- 3490 – Internationalizing Domain Names in Applications (IDNA)
- 3987 – Internationalized Resource Identifiers (IRIs)
- 4518 – Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation

Normative Down References

- 2585 – Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP.
- 4516 – Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator
- 4523 – Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates
- 5273 – Certificate Management over CMS (CMC): Transport Protocols [replaces reference to RFC 2797]

authorityInfoAccess

- Requirement (for id-ad-caIssuers):
  - HTTP server implementations accessed via the URI SHOULD specify the media type application/pkix-cert [RFC2585] in the content-type header field of the response for a single DER encoded certificate and SHOULD specify the media type application/pkcs7-mime [RFC2797] in the content-type header field of the response for "certs-only" CMS messages.
- Most certificates point to a file with a ".crt" extension. The HTTP servers specify the media type application/x-x509-ca-cert.
- Some web servers, by default, specify application/pkix-cert for ".cer" and application/x-x509-ca-cert for ".crt" and ".der".

User Notice policy Qualifier

- Requirement:
  - An explicitText field includes the textual statement directly in the certificate.... Conforming CAs SHOULD use the UTF8String encoding for explicitText, but MAY use IA5String. Conforming CAs MUST NOT encode explicitText as VisibleString or BMPString.
- Every certificate located encodes explicitText as VisibleString.
- Recommend changing requirement to permit use of VisibleString encoding.

No Implementations Located*

- Indirect CRLs
- Delta-CRLs and FreshestCRL extension
- SIA extension with id-ad-timeStamping.
- SIA extension with id-ad-caRepository pointing to a single DER encoded certificate
- AIA extension in a CRL.
- AIA, SIA, or CDP extension with an FTP URI.

* This list represents an inability to locate operational CAs that are issuing certificates or CRLs with these features, and thus is not an indication that CA software is incapable of issuing certificates or CRLs with these features.

No Implementations Located

- Certificates with notAfter=99991231235959Z
- Clients that display contents of userNotice (other than certificate viewers)
- Name constraints on X.400 names or IP addresses
- InhibitAnyPolicy extension marked critical
- CRLs with an issuerAltName extension
- issuingDistributionPoint extension with onlySomeReasons present.

Not Yet Tested

- Processing of internationalized names (per Section 7)
- Processing of name constraints on X.400 addresses
- Use of SIA extension for path discovery
- Use of AIA extension in a CRL for path discovery