3280bis

David Cooper

Changes Since Draft 04

- Name Constraints:
  - Conforming CAs MUST mark this extension as critical and ~~MUST~~ **SHOULD** NOT impose name constraints on the x400Address, ediPartyName, or registeredID name forms.

- Empty sequences in certificates and CRLs:
  - RFC 3280 already included statements about issuer, subject, authorityKeyIdentifier, basicConstraints, policyConstraints, and revokedCertificates.
  - Added statements prohibiting empty sequences in nameConstraints and issuingDistributionPoint.

Changes Since Draft 04

- HTTP URIs in cRLDistributionPoints, authorityInfoAccess, and subjectInfoAccess
  - Modified text so that no constraints are imposed on the URI, only the data that is returned by the server (e.g., use of correct media (MIME) type for the type of data being returned).

- Path Validation Algorithm:
  - initial-permitted-subtrees and initial-excluded-subtrees added as inputs.
  - Initial path length constraint mentioned as possible enhancement to algorithm (section 6.2).

Changes Since Draft 04

- Attributes of type DirectoryString:
  - Added comments to Appendix A (ASN.1) and a paragraph to Appendix B (ASN.1 Notes) to clarify which attribute types use the DirectoryString encoding.