rfc2560bis

IETF 85

Stefan Santesson (sts@aaa-sec.com)

Status since last IETF

- WG decided to go with the current draft
  - Minimalistic approach
  - Retain document structure of RFC 2560
  - Retain previous editors
  - Require motivation for each additional update of the original RFC.
- Denis Pinkas submitted a new alternative draft providing a complete re-write
- Draft-06 submitted
- WG discussions on additional changes

New draft from Denis

- Complete re-write
- Changes listed but not motivated
- Hard to tell exactly what changed from current draft
- Did not provide input in a way that could be incorporated in the current draft.
- Some editorial changes from Denis draft made it into draft 06 anyway.

Updates incorporated in draft 06

- Original editors included
- Clarification that the ResponderID field corresponds to the OCSP Responder signer certificate (4.2.2.3)
- First attempt to expand “revoked” to possibly include certificates never issued by the CA.
- Updated text on Authorized responders (clarifications only)
- The value of id-pkix-ocsp-nocheck SHALL be NULL

Non-issued Certificates

- Straw poll on how to deal with status requests for certificates never issued by the CA.
  - Allow “revoked” response
  - Require “good” response
  - Allow “unknown” response
- Clear majority favored “revoked” response, some ONLY if combined with an indication that the server has implemented this behavior.

The “unknown” alternative

- Pro:
  - Cleaner (no need for constructed reason or date)
- Con:
  - Clients are likely to fall back on other sources of status checking (e.g. CRL) and are likely to accept the certificate as valid.

Proposed resolution

- Allow “revoked” response for certificates never issued by the CA.
  - Only IF the OCSP responder knows that the requested certificate has never been issued by the CA.
  - Use certificateHold reason
  - Revocation date: Jan 1st, 1970
  - The CRL Reference extension (id-pkix-ocsp-crl) MUT NOT be included for a response to a certificate that has never been issued.
  - MUST include a new extension (tbd OID, no extension data) that indicates this behavior:
    - In All responses, or
    - In “revoked” responses for non-issued certificates

Other issues ?

Way forward

- Resolve last issues
- Submit draft 07
- WG LC