OCSP update
rfc2560bis-04

Stefan Santesson
3xA Security
stefan@aaa-sec.com
What happened to it?

• Process stalled about a year ago since authors could not agree on clarification text concerning designated responders.
Updates of OCSP

• Defines the nonce extension that was missing in RFC 2560
• Aligns with RFC 5019 (Lightweight OCSP)
  – definition of the ”unauthorized” error response
  – May include status for certs not in the request
• Includes the updates from RFC 6277 (OCSP Algorithm Agility)
  – Preferred Signature Algorithms extension
  – Updated mandatory algorithms
Clarifications

• Clarifications in 2560bis do not change the bits on the wire.

• Most important clarification is text concerning Authorized responders
Authorized responders

• Original text

OCSP signing delegation SHALL be designated by the inclusion of id-kp-OCSPSigning in an extendedKeyUsage certificate extension included in the OCSP response signer's certificate. This certificate MUST be issued directly by the CA that issued the certificate in question.
And

They MUST reject the response if the certificate required to validate the signature on the response fails to meet at least one of the following criteria:

1. Matches a local configuration of OCSP signing authority for the certificate in question; or

2. Is the certificate of the CA that issued the certificate in question; or

3. Includes a value of id-ad-ocspSigning in an ExtendedKeyUsage extension and is issued by the CA that issued the certificate in question."
Big question

• The CA that issued the certificate in question
  – What about if the CA was rekeyed?
  – What is the MUST support requirement for clients?
    • MUST Accept if OCSP certificate is chained to a new CA certificate with new key, different from the CA certificate used to validate the certificate in question?
    • **Presenting author thinks this is a really bad idea**
Why not?

• This is simply NOT how OCSP is implemented in the vast majority of cases.
• Creates false expectations on what OCSP responders can expect in terms of client behavior
• Introduce the need for name matching and/or discovery of key rollover certs
• What if the new CA subject name is identical to old CA subject name but expressed using different character encoding?
  – Many chaining libraries do byte array match
Proposed resolution
By the presenting Author

• Clients MAY accept an OCSP certificate issued with another key than the CA key issuing the certificate in question. **IF**;
  – they can determine that this is a key of the same CA that issued the certificate in question.
  – Responders should not expect clients to handle CA key rollover.
  – Designated responders MUST/SHOULD present an OCSP responder certificate that was issued through the same key that was used to issue the certificate in question.
  • This author suggest ”MUST”
Way forward

• Resolve the designated responder clarification
• Final review?
• WG-LC

• Let’s get this over with.