RFC 2560bis
OCSP update

Stefan Santesson
stefan@aaa-sec.com
Status

• Last IETF meeting discussed the current direction of the draft and the problem associated with the material changes compared to RFC 2560

• A new draft 05 has been posted, providing the same material changes as 04, but doing minimalistic changes to RFC 2560.
Why minimalistic changes to 2560?

• Serious oppositions to draft 04 (presented and discussed at IETF 83)
  – Authorized responders relative to re-keyed CA, a major issue.
• Hard to ensure that the new document don’t do material changes to RFC 2560
• Hard to process a materially new document of a widely deployed protocol through the IETF process.
The updates to OCSP

• Specify ASN.1 syntax for the nonce extension
• Include OCSP algorithm agility RFC 6277
• Extend the unauthorized response (RFC 5019)
• Responses MAY include status for certs not included in the request (RFC 5019)
• Clarifications on Authorized responders.
• Updated ASN.1 section
WG Straw-poll
(Ending August 12)

a) Go ahead with the draft 05
b) Revert to draft 04
c) Kill the effort (no update)
d) Start a completely new document

• Currently a majority has voted for option a)
• Voice your opinion
If draft 05 approach is accepted

- Finalize text regarding authorized responders
- What else need to go into the draft?
- WG Last Call before Atlanta
If WG decides to revert to 04

• Figure out how to proceed
  – Editor?
  – What need to be fixed?
Questions
Comments