OCSP Digest

Phillip Hallam-Baker
Rob Stradling

What

- Extension specifies the certificate whose status is being reported

Why?

- Algorithm Agility
  - SHA-2 Certificates break legay browsers
  - SHA-2 Digest extension does not
- Transparency
  - Allows any party to audit OCSP responder
    - May become a CA requirement.
  - Does responder know if the certificate exists?
    - Have they been compromised like DigiNotar?

How?

- Lack of digest = 'I do not know'

Against?

- Means that the responder must have more information than CRLs provide.
  - This is not a concern for a public CA.
  - Transparency is not a concern for non-CA responders
  - Can obtain the necessary data from other sources
    - LDAP
    - New scheme

Possible extension

- Range response
  - No certs exist in the range X through Y
  - Enables static signed response for 'not valid'
    - Tree walking might be an issue
    - But Public Cas likely to be forced to be public