Document History

- Earlier attempt to update 2560:
  - draft-ietf-pkix-rfc2560bis-00 February 2002
  - draft-ietf-pkix-rfc2560bis-01 February 2002

- Current attempt to update 2560:
  - draft-cooper-pkix-rfc2560bis-00 June 2010
  - draft-ietf-pkix-rfc2560bis-02 October 2010

Changes from draft-cooper-pkix-rfc2560bis-00

- Nonce extension:
  - Specified OCTET STRING as ASN.1 syntax for nonce extension.
  - Added appendix on implementation notes that
    - Explains that RFC 2560 did not specify a syntax for the nonce extension.
    - Explains why an OCSP responder may choose to include a nonce in response to a request that did not include a nonce.
- Modified the IMPORTS section of 1998 version of ASN.1 module as described on mail list.

Changes from draft-cooper-pkix-rfc2560bis-00 (continued)

- Determining whether an OCSP Responder is integrated or designated:
  - Added security consideration about the risk of name collisions that is modeled after similar security consideration in RFC 5280.
  - Clarified that if two certificates or a certificate and an OCSP response are signed by the same CA then the DNs will match rather than stating that if the DNs match then the signers are the same CA.

Changes from draft-cooper-pkix-rfc2560bis-00 (continued)

- Incorporated some minor editorial changes from February 2002 drafts of 2560bis
  - Calculation of issuer key hash
  - Definition of the “good” status response

Unresolved Issues

- Handling of unrecognized critical extensions
- Preferred Signature Algorithms extension
  - draft-ietf-pkix-ocspagility needs to be finalized and any changes need to be incorporated into 2560bis.

Questions