OCSP Algorithm Agility

PHB
Problem

- OCSP does not specify how signing algorithm is selected
  - E.g. CERT is RSA 2048 SHA256,
    - Valid response is ElGamal 512 with MD2
  - That’s not sensible
    - What is?
- Ambiguity impedes deployment of new signature algorithms
  - E.g. upgrade to ECC
  - E.g. upgrade to SHA-256
First cut

• OCSP clients should be capable of verifying the signature algorithm used in the certificate
  – Caveat: OCSP Server may not support this
  – Caveat: Certificate validation and signature verification may not take place in same device
  – Caveat: Downgrade attack (albeit in very limited circumstances)
Relay Example

- CA
- OCSP
- Key Manager
- PC
Proposal

1. Specify OPTIONAL mechanism for choosing signature algorithm
   • Address ambiguity

2. Means to allow client to tell server which algorithms are preferred
   • Deals with corner cases
Options

• Separate Draft
  • See draft-hallambaker-ocspagility-00
  • A one pager (i.e. 8)
• Update main OCSP draft
• Do nothing