OCSP Algorithm Agility

Phillip Hallam-Baker

Status

- WG Draft submitted
  - Specifies default client algorithm selection
  - Optional mechanism to permit client to specify supported algorithms
    - Handles case where certificate does not exist

Outstanding Issues

- Use of algorithms other than SHA1 for identifying certificate by digest
  - SHA1 is hardwired in OCSP spec
  - Will require fix before OCSP goes to STANDARD
- Security remains dependent on certificate signature algorithm
  - May be an issue for archival applications
    - 'What is the status of this RSA-SHA1 cert used to sign a mortgage 20 years ago'

Proposed fix

- Extension to allow digest of certificate to be specified