OCSP Agility

Stefan Santesson

3xA Security

sts@aaa-sec.com

Updating Preferred Signature Algorithm declaration

Change from:

```
 PreferredSignatureAlgorithm ::= SEQUENCE {
        sigIdentifier   AlgorithmIdentifier,
        certIdentifier  AlgorithmIdentifier OPTIONAL
        }
```

To:

```
 PreferredSignatureAlgorithm ::= SEQUENCE {
        sigIdentifier   AlgorithmIdentifier,
        pubKeyAlgoritm  SMIMECapabilities OPTIONAL
        }
```

Or other?

Rationale

- sigIdentifier provide a simple identifier for specifying a supported signature algorithm (unchanged from current ASN.1) which maps to current PKIX documents
- pubKeyAlgorithm is an OPTIONAL field for giving more specific information (parameters) about the supported public key algorithm
  - SMIMECapabilities has been suggested as a better vehicle for carrying parameter information
  - Name is changed from certIdentifier to pubKeyAlgorithm to avoid confusion (This is not an identifier of a certificate)

Other issues

- P H Baker has suggested a solution if the hash for certID is unknown by the responder.
- Proposed solution by PHB:
  - The responder my include a list of supported hash algorithms in a new response extension

- Questions to PKIX
  - Is this mechanism motivated?
  - Should discussion be deferred to the rfc2560bis process since OCSP agility is in IESG processing stage?

Way Forward

- Publish as separate RFC
  - Conclude update
  - New WGLC
  - Publish
  - Integrate with rfc2560bis and obsolete this RFC when 2560bis is published.
- Or kill draft and merge with rfc2560bis process