OCSP Agility

Stefan Santesson
AAA-sec.com

Scope

- A mechanism that allows a client to indicate the set of preferred signature algorithms.
- An algorithm for signature algorithm selection that maximizes the probability of successful operation in the case that no supported prefered algorithm(s) are specified.

The added extension

```
id-pkix-ocsp-preferred-signature-algorithms OBJECT IDENTIFIER ::= {
        id-pkix-ocsp x }

  PreferredSignatureAlgorithms   ::=     SEQUENCE {
        Algorithms      SEQUENCE OF AlgorithmIdentifier
        }
```

The algorithm

1. Using an algorithm specified in the client extension.
2. Using the signing algorithm used to sign the CertID
3. Using the signing algorithm used to sign a CRL for the target certificate
4. Using out of band source
5. Using a mandatory signing algorithm specified for the version of the OCSP protocol in use

Way forward

- Are we ready for WG LC?

Time-Stamp Protocol 3161 update

Stefan Satesson

AAA-sec.com

Current Proposal

- draft-ietf-pkix-rfc3161bis-01
  - Allows ESSCertIDv2 from RFC 5035 (Enhanced Security Services Update)
  - Changes the model from RFC 3628 used to describe the entity providing time-stamping services as well as its subordinate functions
  - Defines minimum DN attribute set for a TSU Certificate
  - Updates references

Result of WG discussion

- Consensus to update RFC 3161 to allow ESSCertIDv2
- Strong opposition against alignment of terminology with RFC 3628

- Conclusion
  - Scope limited to small update document to add support for optional use of ESSCertIDv2
  - New draft is needed (draft-ietf-pkix-rfc3161bis is rejected by the WG)

Certimage

Stefan Santesson
AAA-sec.com

Mission

- Defining a new image type to be used with RFC 3709 to store a complete certificate image
- Defined image formats:
  - PDF/A
  - SVG Tiny
  - PNG (for raster images)

Outstanding Issues

- Enable embedded images
  - Not to be handled within this draft but may be solved by separate effort (extension) if needed
- Need for other image formats
  - VML (Problem: not based on any stable standard)
- No other issues recorded
- Several discussions held outside of PKIX