Updates to OCSP Agility

Stefan Santesson

3xA Security

sts@aaa-sec.com

Changes summary

- General nits in response to IESG comments (no protocol changes)
- Change to ASN.1 syntax (slide)

Change to Security Considerations

From:

```
In archival applications it is quite possible that an OCSP responder
might be asked to report the validity of a certificate on a date in
the distant past.  Such a certificate might employ a signing method
that is no longer considered acceptably secure.  In such
circumstances the responder MUST NOT generate a signature for a
signing mechanism that is considered unacceptably insecure.
```

To:

```
In archival applications it is quite possible that an OCSP responder
might be asked to report the validity of a certificate on a date in
the distant past.  Such a certificate might employ a signing method
that is no longer considered acceptably secure.  In such
circumstances the responder MUST NOT generate a signature using a
signing mechanism that is not considered acceptably secure.
```

Changes during IESG process

```
id-pkix-ocsp-pref-sig-algs OBJECT IDENTIFIER ::=
{ id-pkix-ocsp 8 }

PreferredSignatureAlgorithms ::= SEQUENCE OF

PreferredSignatureAlgorithm

PreferredSignatureAlgorithm ::= SEQUENCE {
    sigIdentifier          AlgorithmIdentifier,
    pubKeyAlgIdentifier    SMIMECapability OPTIONAL
    }
```