OCSP Agility

Stefan Santesson
3xA Security
sts@aaa-sec.com
Nits

re-preferred-signature-algorithms EXTENSION ::= {
    SYNTAX PreferredSignatureAlgorithm
    IDENTIFIED BY id-pkix-ocsp-pref-sig-algs  }

Changed to:

re-preferred-signature-algorithms EXTENSION ::= {
    SYNTAX PreferredSignatureAlgorithms
    IDENTIFIED BY id-pkix-ocsp-pref-sig-algs  }

PreferredSignatureAlgorithm ::= SEQUENCE {
    sigIdentifier  AlgorithmIdentifier{SIGNATURE-ALGORITHM, {...}},
    certIdentifier AlgorithmIdentifier{SIGNATURE-ALGORITHM, {...}}
        OPTIONAL  }

Changed to:

PreferredSignatureAlgorithm ::= SEQUENCE {
    sigIdentifier  AlgorithmIdentifier{SIGNATURE-ALGORITHM, {...}},
    certIdentifier AlgorithmIdentifier{PUBLIC-KEY, {...}}
        OPTIONAL  }
Other issues

• Open issue from David Cooper on specifying parameters for signature algorithms
• Potential ASN.1 updates to resolve this.