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 preferred algorithm(s) are specified.
Major issues since last IETF

• Minor updates of the preference guidance for choosing signature algorithm
• Signature algorithm inadequate to express requirements for algorithm parameters. E.g. to specify preference for a particular ECC curve.
The updated extension

\[
\text{id-pkix-ocsp-preferred-signature-algorithms \hspace{1em} OBJECT IDENTIFIER ::= \\
\hspace{2em} \{ \hspace{1em} \text{id-pkix-ocsp} \hspace{0.5em} x \hspace{0.5em} \}}
\]

PreferredSignatureAlgorithms ::= SEQUENCE OF
PreferredSignatureAlgorithm

PreferredSignatureAlgorithm ::= SEQUENCE {
  sigIdentifier AlgorithmIdentifier,
  certIdentifier AlgorithmIdentifier OPTIONAL
}
Currently in WG LC DONE?
Time-Stamp Protocol
3161 update

Stefan Satesson
AAA-sec.com
Since last IETF

- draft-ietf-pkix-rfc3161bis-01 rejected by WG
- Replaced by draft-ietf-pkix-rfc3161-update-09
- Past WG Last Call – Currently in IETF Last Call
WG process

• Added support of ESSCertIDv2
  – No hard problems
• Security Considerations
  – Draft does not address any real security threats
  – Address scenario involving a “Bad trusted CA”
  – However: “Bad Trusted CA” is generally out of scope for PKI protocols to solve.
  – Real motive of draft: To allow accommodate hash migration from SHA-1
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)
Resolved Issues

• Enable embedded images
  – Enabled by the data: URL scheme
  – Example to be added

• Need for other image formats
  – VML excluded
  – Current set sufficient

• No other issues recorded
Way forward

- New draft with data: URL scheme example to be issued after Hiroshima IETF
- Ready for WG last call