AD Review Comments on rfc5750-bis and rfc5751-bis

Jim Schaad

August Cellars

5751 bis – SMIMECapabilities attribute

- Simplify the requirement language
- If present, the SMIMECapabilities attribute MUST be a SignedAttribute; it MUST NOT be an UnsignedAttribute. CMS defines SignedAttributes as a SET OF Attribute. The SignedAttributes in a signerInfo MUST NOT include multiple instances of the SMIMECapabilities attribute. CMS defines the ASN.1 syntax for Attribute to include attrValues SET OF AttributeValue. A SMIMECapabilities attribute MUST only include a single instance of AttributeValue. There MUST NOT be zero or multiple instances of AttributeValue present in the "attrValues SET OF AttributeValue".

5751 bis – SMIMECapabilities attribute

- Current Text is
  - MUST be signed
  - MUST NOT be unsigned
  - MUST be one occurence
  - MUST be single value
- No statement on what should be done if this is not true
  - Ignore
  - Use ‘first’ for some value of first

5751 bis – weak cryptography

- Using weak cryptography in S/MIME offers little actual security over sending plaintext.

- Written for RC2 and DES – now that 3DES is included, should this statement be “weakened”

5750 bis -

- Convert to absolute MUST NOT on PKCS#6 certificates
- When determining the time for a certificate validity check, agents have to be careful to use a reliable time. Unless it is from a trusted agent, this time MUST NOT be the SigningTime attribute found in an S/MIME message.