IKEv2-bis Certificate Issues

Yaron Sheffer

IETF-76, Hiroshima

#116: The AUTH Payload Signature

- The definition of the payload (sec. 3.8) should mention explicitly that the payload hash algorithm is unrelated to the one used in the certificate, or the algorithm used to sign the IKE Encrypted Payload.
  - Tero: in some cases they are related
- Moreover, the words "by default" are confusing and should be deleted.
  - To promote interoperability, implementations that support this type SHOULD support signatures that use SHA-1 as the hash function and SHOULD use SHA-1 as the default hash function when generating signatures.

#117: Hash-and-URL Interop

- To improve interoperability, allow only the "http" URL method. The current text (end of sec. 3.6) implies that any method is allowed, although HTTP MUST be supported.

#118: Reference for PKCS #7

- PKCS #7 should reference RFC 2315.
  - Russ: there are quite a few RFCs to choose from (2630, 3369, 3852, and 5652)

#119: Which certificate types can be mixed in one exchange?

- Should be added to Sec. 3.6, probably as a new subsection.

1. One H&U bundle only. Or...
2. One Raw RSA key, or...
3. One or more cert payloads of either type 4 or H&U (type 12)

- 1 and 3 can also have one or more CRLs and/or OCSP content (RFC 4806) added

#120: CA indication with cert req - allowed types

- Sec. 3.7 has:

  > The contents of the "Certification Authority" field are defined only for X.509 certificates, which are types 4, 10, 12, and 13. Other values SHOULD NOT be used until standards-track specifications that specify their use are published.

- This excludes certificate requests of type 7, i.e. for CRLs. For requesting a specific CRL, Type 7 would make sense, in particular in chain situations. Should we add it to the list of allowed types here?
- OTOH, this allows type 10, which is unspecified and should be removed.