Clarifying Certificate Handling: Fun with Sec. 3.6-3.8

Yoav Nir and Yaron Sheffer

A Quick Review

- Hash and URL: should only allow the HTTP URL method
- Hash and URL: replace “allow” with “allows”
- Replace PKCS#7 by RFC 2315 – why is it left unspecified? Should we deprecate it?
- Define rules on which cert types can be mixed in the same exchange
- Allow one bundle at the most, with no additional certs?

A Quick Review

- For the cert request, “If multiple CAs are trusted and the certificate encoding does not allow a list, then multiple Certificate Request payloads would need to be transmitted.” But what if I get back a bundle? Why can’t I specify both CAs in the same request?
- Cert req does not allow to request a CRL explicitly. Should it?
- Cert req OTOH is defined for attribute certs, which are not specified themselves. Why?
- Auth payload: “SHOULD use SHA-1 as the default hash function”. Sec. 2.15 should simply say that the MAC is SHA-1. And yes, we have a crypto agility issue