IETF-72

Other Certificates Extension
draft-farrell-pkix-other-certs-03

stephen.farrell@cs.tcd.ie

Use Cases

- If an application associated state with an end-entity certificate then when the certificate changes things don't work
  - Browser form-filler (putative example from W3C)
  - Load balancing(?)
  - Change of CA provider

Idea

- Allow a new certificate for the same end entity to link back to the old certificate via a hash of the old certificate

Extension Syntax

```
OtherCertificates ::=
   SEQUENCE OF SCVPCertID
```

SCVPCertID (from RFC 5055):

```
SCVPCertID ::= SEQUENCE {
   certHash  OCTET STRING,
   issuerSerial   SCVPIssuerSerial,
   hashAlgorithm AlgorithmIdentifier DEFAULT
      { algorithm sha-1 } }
```

To-Do's

- Tighten up use cases
- Tighten up processing rules
- Figure out constraints issue
- ASN.1 module
  - Get OIDs for the extension/module
- Handle stuff

PI

- Use PI instead? (RFC 4043)
  - I-D calls this out as an option
  - Are PI registries available?
  - PI requires 1st issuer to plan ahead; OC doesn't

Constraints

- If 1st issuer placed constraints on the EE cert (e.g. name constraints) those might not be honoured by the 2nd issuer
- If 2nd issuer is constrained (e.g. by a superior CA) can it “escape” those constraints by linking back to an old certificate whose issuer is not constrained
- Real problems or not?

Status

- Accepted as WG draft
  - Aiming for experimental track RFC
  - draft-ietf-pkix-other-certs-00 this/next week
- Plan
  - WGLC next time (tee-hee:-)