Other Certs Extension draft-farrell-pkix-other-certs

stephen.farrell@cs.tcd.ie

Use Cases

- If an application associated state with an end-entity cert then when the cert changes things don't work
  - Fictional example: browser form-filler
- Can happen when:
  - Load balancing
  - Change of CA provider
- Motivated by discussion in W3C WSC group

Other Certs Extension

- This CA says that the subject of these other certificates is really the same end entity.
  - MUST NOT be marked criticial

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

```
RFC5055:

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

Issues

- Level of interest (if any) in this?
- Rules for RPs to apply to this extension?
  - In addition to normal 3280 processing
  - Its like SDA, i.e. not part of path-processing so maybe nothing to say?
    - Other than all other certificates referenced SHOULD (have been) valid when previously seen by the application?
  - OTOH, maybe we'd need more rules for CA operators wrt what "same E-E" means
    - e.g. "don't point at VPN g/w certs from an SSL server cert"

Options

1. Wither-and-die
2. Progress an experimental
3. Progress on standards track

- 2 or 3 could be either as draft-ietf-pkix or draft-farrell-pkix