Certificate Format from STI-CR

Chris Wendt/David Hancock

COMCAST

Certificate Format - concatenated PEM

- Turns out we haven’t formally specified the specific format of the x5u pointed certificates, hosted by the STI-CR
- This might be sort of implied based on ACME specs but not explicit.
- We thing the easiest, most conventional way of doing this is concatenated PEM certificates
- Conveniently, ACME has defined a MIME type and format for the certificate response when getting the newly created certificate.

COMCAST

Certificate Format - concatenated PEM

- From Section 9.1 of draft-ietf-acme-acme-13
  - File contains one or more certificates encoded with the PEM textual encoding, according to RFC 7468 [RFC7468]. In order to provide easy interoperation with TLS, the first certificate MUST be an end-entity certificate. Each following certificate SHOULD directly certify the one preceding it. Because certificate validation requires that trust anchors be distributed independently, a certificate that specifies a trust anchor MAY be omitted from the chain, provided that supported peers are known to possess any omitted certificates.

COMCAST

Certificate Format - concatenated PEM

- From draft-ietf-acme-acme-13

```
GET /acme/cert/asdf HTTP/1.1
   Host: example.com
   Accept: application/pkix-cert

   HTTP/1.1 200 OK
   Content-Type: application/pem-certificate-chain
   Link: <https://example.com/acme/some-directory>;rel="index"

   -----BEGIN CERTIFICATE-----
   [End-entity certificate contents]
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   [Issuer certificate contents]
   -----END CERTIFICATE-----
   -----BEGIN CERTIFICATE-----
   [Other certificate contents]
   -----END CERTIFICATE-----
```

- Follow same format for STI-CR response

COMCAST

Plan

- If agreed, integrate new text in an errata to ATIS-1000080

COMCAST