Voucher Profile for Bootstrapping Protocols

draft-ietf-anima-voucher-04

ANIMA WG
IETF 99 (Prague)

Recap

- At IETF 98 we presented the Voucher document as having just a few open issues remaining, with an expectation to be ready for a Last Call in a few weeks

- Bootstrapping Design team has met weekly since, about 50% discussion on BRWSKI and 50% discussion on Voucher.

Updates Since IETF 98

(Sorted by Importance)

1. Introduces the use of the Voucher structure for signing requests
   – signing request may embed other voucher structures
   – enables traceability
2. Opens the possibility that alternative voucher artifact signing structures MAY be signaled by external mechanisms
   – enables transition to JWS ⊐ CWS
3. Introduces flag for Voucher to signal to Pledge that it MUST fail-close
   – 'domain-cert-revocation-checks'
4. Added the 'proximity' assertion type
   – to support voucher-requests
5. Removed the 'domain-certificate-identifier' field
   – now the 'pinned-domain-cert' is used exclusively
6. Clarified that the Voucher SHOULD staple intermediate CA certificates
7. Clarified that the Voucher MAY staple revocation objects for the intermediate certificates stapled to the Voucher
   – needed to support private networks

Open Issue (Just One!)

Mandatory or optional fields?

- when voucher structure used for requests, some fields that are normally mandatory no longer are...

Options:

- fill in dummy values for mandatory fields
- change YANG to say they're not mandatory
- define a separate request structure

Thoughts?