stir-certs

STIR Interim

5/27/2016

Jon

Added “Cert Usage” Section

- Answers the requirements in RFC4474bis 6.4
  - Mostly boilerplate-ish
- Clarifies that we need have MUSTs for EC256 and RS256 for certificate signing
  - For the time being; hazard tape on RS256
  - Requires certs be capable of generating EC256 sigs for PASSporT

CID or a header?

- Right now, specifies a cert can be carried in SIP via CID
  - That means as a multipart/MIME body, pretty much
- With smaller EC certs especially, do we want to specify a SIP header for this instead?
  - multipart/MIME is ugly
  - Then again, use case might not be crucial

The TBDs

- Out-of-band related items
  - LoA – do we need them?
    - For Proof-of-possession
- Partial delegation
  - This would extend TN Auth List further
    - Probably not worth doing until we have more experience
- Number encoding, IA5?
- OCSP details
  - What to do with the unknown case
  - Moving to SHA-256 (we're doing that)
- We need the ASN.1 module

Not a lot left to do here

- I don't think we want to restrict it more
  - Leave this to implementation and deployment