STIR certificates

IETF 96 (Berlin)

STIR WG

A Few Quick Revisions

- Now at -07, and in WGL
  - Shifted to ECDSA P-256 and SHA-256
    - Aligned with PASSporT
    - Still allowing RSA for certificate signature verification
  - Furnished the ASN.1 module (Appendix A)
  - Added a Level of Assurance (LoA) for certs
  - Tightened the (optional) OCSP profile
  - Eliminated TBDs, put in some organization
  - IANA and references clean-up
- Speak now or etc.

Levels of Assurance

- Want to distinguish different methods of enrollment
  - Some interest in the SHAKEN model as well
- Decided to reuse an existing registry
- Level of Assurance Profiles (RFC 6711)
  - Created a STIR sub-registry
  - Requires CP to add a new LoA value to the registry
    - Better than defining the CP/CPS ourselves here

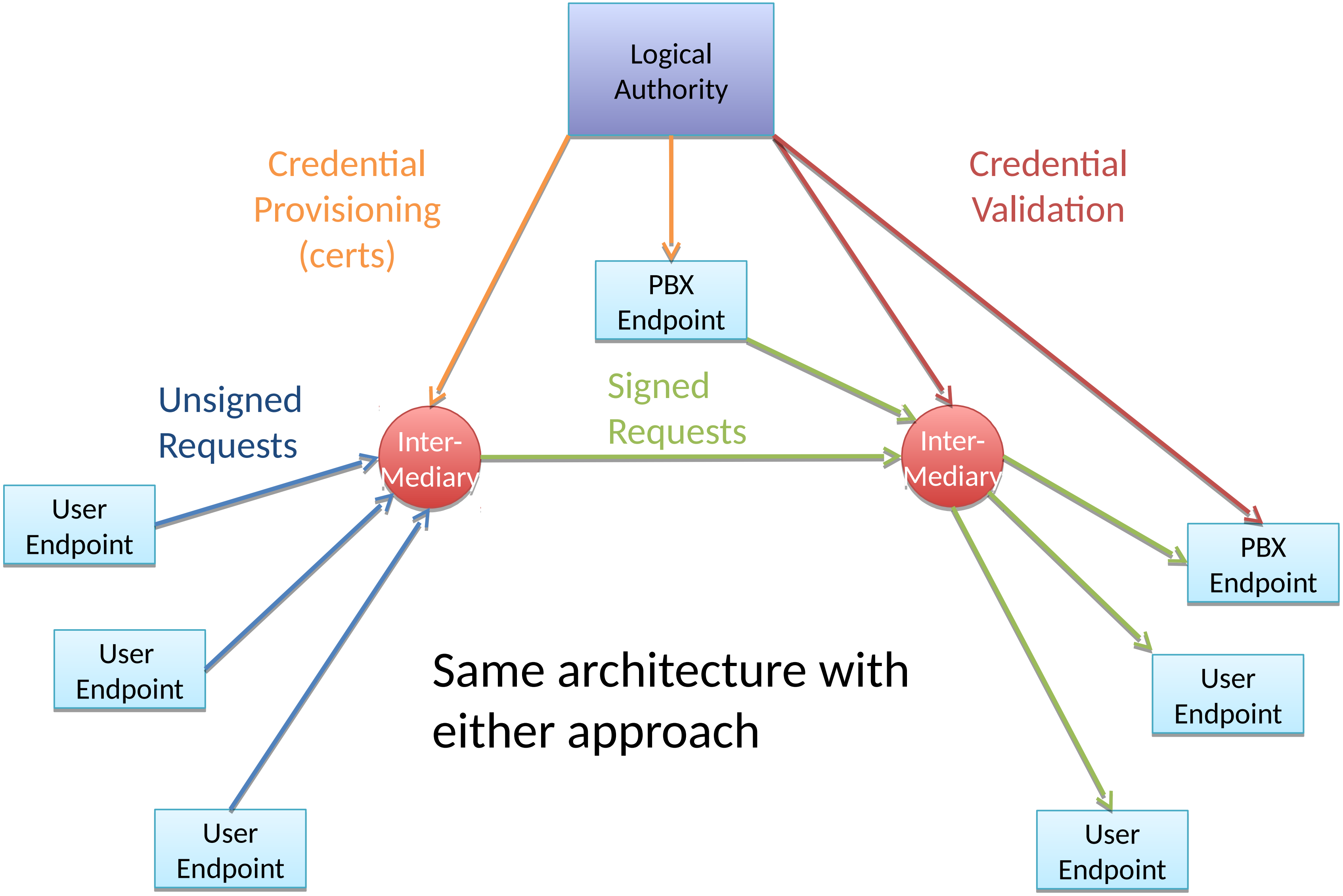
OCSP Profile

- Profiling away the “unknown” response
  - Servers SHOULD send “not good” instead of “unknown”
  - “clients MUST treat returned “unknown” responses as “not good”
- Also note that OCSP responses MUST be signed with the same alg as the cert itself
  - Which could be ECDSA or RSA

That’s it

- Read it, send comments, let’s finish this

In-band STIR Logical Architecture



Same architecture with either approach