STIR TNs for ACME

Jon

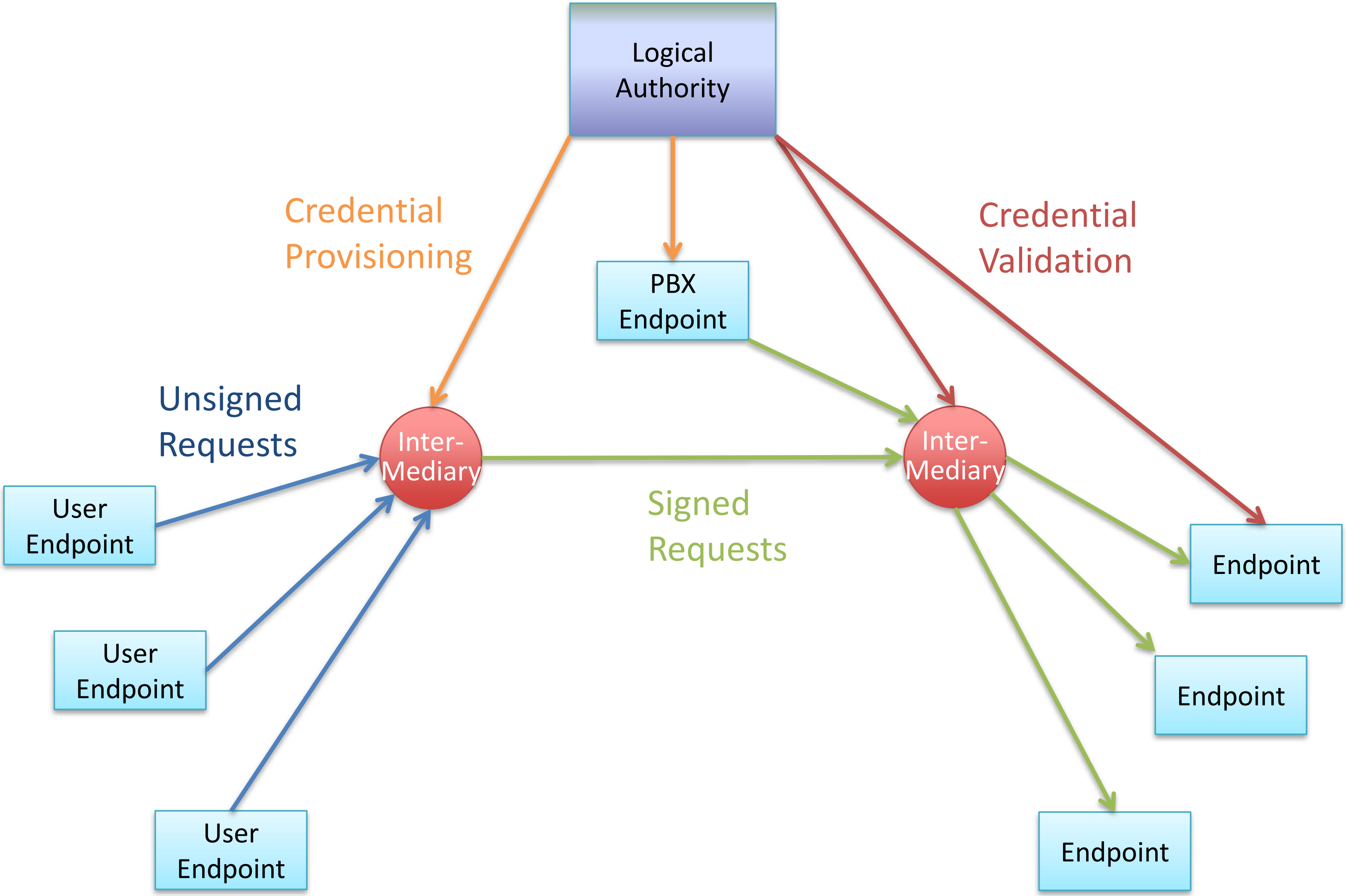
ACME WG

Prague - Jul 2017

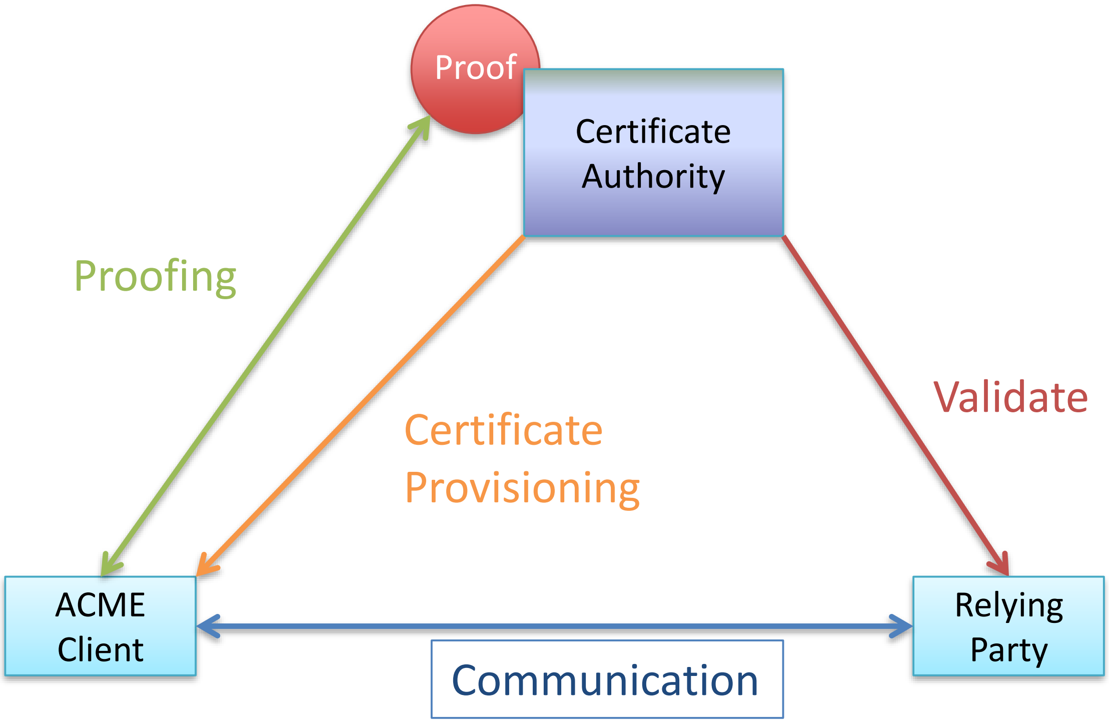
STIR and ACME

- What is STIR? Secure Telephone Identity (Revisited)
  - Providing cryptographic authentication for telephone calls
  - Detecting impersonation is crucial to blocking illegal robocalling and other attacks on the telephone network
- STIR uses certs to attest authority over telephone network resources
  - draft-ietf-stir-certificates
  - Supports certs with extensions for TNs and SPCs
    - I’ll be talking about TNs, Mary will talk about SPCs in a minute
  - We need ways to issue and provision these certs

In-band STIR Logical Architecture



ACME (through a STIR lens)



What are interesting proofs?

- For TNs, a few approaches:
  - Either “effective control” via return routability or similar tests
    - Ability to receive an SMS at a TN is a common security check today
      - However, not rock solid by any means; best combined with another factor
  - Or a top-down attestation of assignment
    - Probably some kind of token-based approach
      - Carrier gives a token to an enterprise, who can redeem the token via ACME to get a cert for a TN
  - Maybe others – still mulling

Things we want to do with ACME

- Issue short-term certificates
  - Telephone number assignments can be dynamic
    - Blocks of numbers allocated for long periods; individual TNs can move around due to porting etc.
  - STAR is great; but reads specific to DNOs today
  - Also, specific to the more “delegative” approach to proofs
    - Be great to have something like it for “effective control” sorts of tests if we can do automatic re-proofing as well as re-issuing
    - That also suggests approaches to automatic renewal for cases where the DNO would not have to initially bootstrap

Things we want to do with ACME (2)

- Generic tokens for proofs?
  - Tokens that allow authorities trusted by the CA to attest ownership for names
    - CA then issues certs with ACME for particular names
  - Example: A carrier has a cert for an SPC
    - That SPC covers a range of numbers (1.212.555.1XXX)
    - Enterprise comes to carrier to request a cert for 1.212.555.1001
    - Carrier signs a token (JWT?) authorizing enterprise to get a cert for that number
    - Enterprise goes to ACME with a CSR for that number
    - ACME challenge is for this token
  - Surely there are many potential uses of such a generic token?

Next Steps

- Read the draft
  - This is still pretty preliminary, not looking for nit review at this point
- Happy to work with folks on adapting short-term certs for this
- Same for generic tokens