draft-ietf-stir-certificates-ocsp
draft-peterson-stir-certificates-shortlived

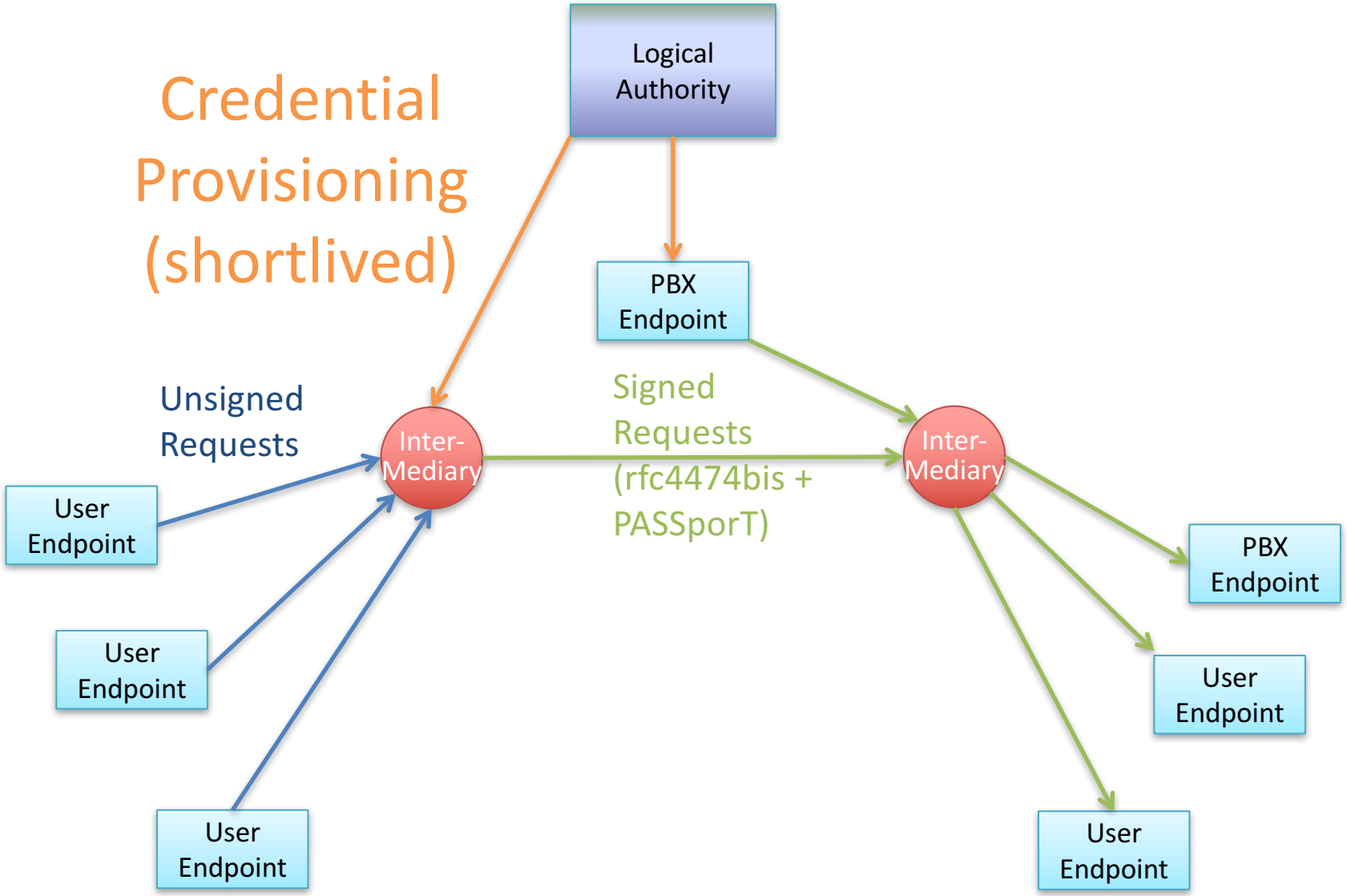
IETF 99 (Prague)

STIR WG

Two real paths

- We need a cert freshness mechanism
  - Specifically, one that allows delegations to be revoked
- We likely aren't going to propose using CRLs or SCVP for this
  - If you feel differently, write a draft
- That leaves OCSP and short-lived certs
  - They have very different privacy properties, potentially
- We've been exploring both paths a bit
- Today talking mainly about short-lived

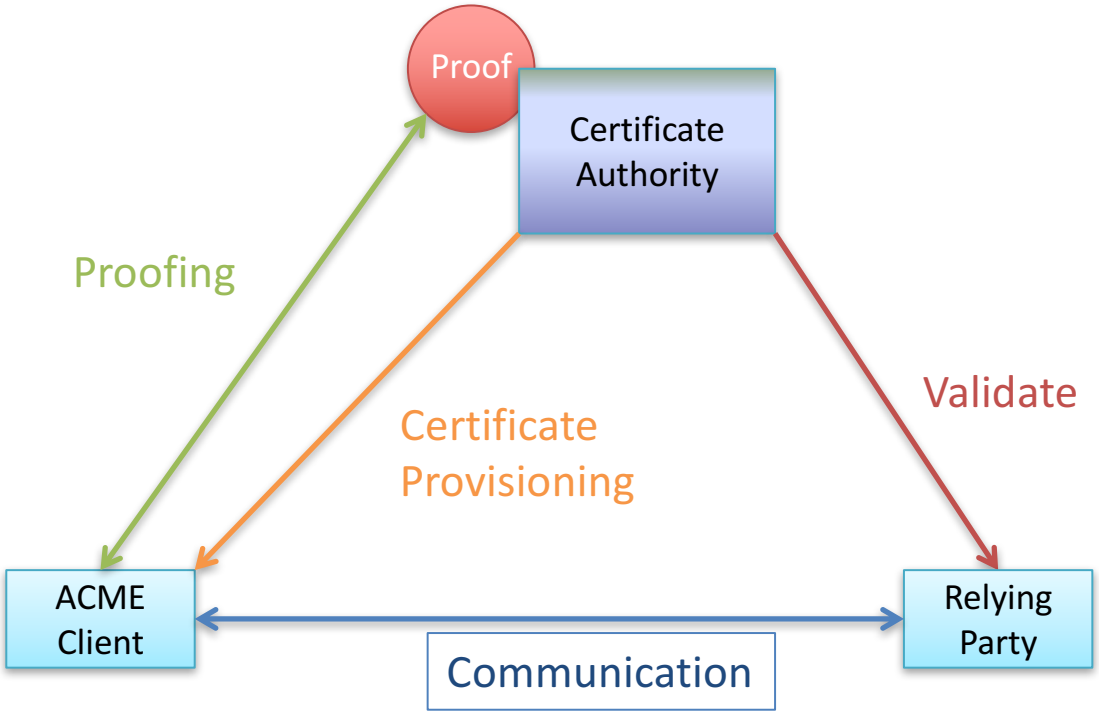
Short-lived Credentials



Short-lived

- Issuing certs for individual TNs that expire soon
  - Though not necessarily certs to individual people!
  - Basically attests, “this cert is valid for this number right now”
    - Also obviates the need for relying parties to talk to the CA
- What does short-lived mean?
  - Hours? Days? Not months or years anyway.
  - Part of our job to decide what is appropriate
- The hard part is getting the new cert… but...

ACME makes short-lived easy



ACME interactions

- Two STIR-related drafts in ACME now
  - draft-ietf-acme-telephone (TN)
  - draft-ietf-acme-service-provider (SPC)
- Both show ways that ACME can be used to get certificates of the two types shown stir-certs
- acme-telephone now also shows a way to “delegate” a TN cert from an SPC cert
  - If a carrier has an SPC that contains a TN, it could tell ACME to let an enterprise owning that TN to get a certificate for it, say.
  - In some cases a carrier might want to get its own cert for a single TN to sign calls, to conceal allocation data

ACME STAR

- ACME has a short-lived mechanism in the works now
  - Based on the LURK problem space
  - Specifically allows a name owner to delegate a name and quickly revoke it
- It could be adapted to STIR, with a little work
  - When a carrier delegates a single TN under and SPC, say, easy to revoke it when needed

So what to do?

- As we get some better alignment with ACME on STAR, might be something to consider adopting here