rfc4474bis + PASSporT + certs

IETF 98 (Chicago)

STIR WG

The good news

- We’re done with the core drafts, pretty much
- Past IESG review, ballot cleared (!)
  - Still a little cleanup to do, mostly on certs

Last minute fixes

- Synchronization across drafts
  - Twiddling whether TNs can include “#” or “*”
  - Getting the right syntax for PASSporT claims
    - ASCII or UTF*? We’ll do ASCII
- Honed the text about how we handle Date in PASSporT vs. the SIP header
- Relaxed some of the reason phrase text in rfc4474bis

JWT Claim Constraints

- Kind of a last minute thing to begin with
  - Subsumed “Levels of Assurance” into this
- Idea that a CA can limit which PASSporT claims a cert is authorized to sign for
  - i.e. this cert cannot sign claims with“cnam”
  - If no Claim Constraints are present, anything is allowed
- A blacklist or a whitelist?
  - Originally allowed both
  - Ultimately a blacklist doesn’t make much sense, so we dropped the “exclude” semantics
- Is it right yet? Let’s talk about it…

Crossover to SIPBRANDY

- On the SIPBRANDY mailing list, Adam raised an issue
  - Regarding connected identity (RFC4916) and any problems we've created with the Identity changes
- This led to some fixes to the text about retransmissions
  - Retries already kind of a hack
  - Now rfc4474bis is clearer about where UAS behavior might trip on this
    - Basically, we advise to override a SHOULD in RFC3261 intended to compensate for certain spiraly things in sequential forking

But that’s all done

- rfc4474bis and PASSporT are hopefully stable with those tweaks
  - Some spanned all three drafts

- For stir-certs, more than just tweaks

STIR certificates

IETF 98 (Chicago)

STIR WG

Final Hurdles

- This document got some attention in IESG review
  - Blocking points now resolved
- Yes, we still need to fix EKR's thing about TN range arithmetic boundaries
  - Have text, will either put in a -14 or AUTH48
- Other major changes

Service Provider Codes

- OCNs? SPIDs? AltSPIDs? LastAltSPIDs?
  - All very national-specific, definitions slippery
- Replaced now with the concept of an SPC
  - A simple ASCII string, identifies a service provider
  - Profiles of STIR (like SHAKEN) can further specify what these mean
    - For current North America deployments, it's an OCN
- Coordinating this with ATIS, hopefully we're in sync

The Cost of Freshness

- Stephen's DISCUSS on stir-certs focused on privacy
  - Doing OCSP potentially reveals to eavesdroppers metadata about calls in progress
    - Worse, the way we defined the OCSP extension passes around the TNs over the interface
  - There's some text on OCSP about confidentiality, but not much
- We can (and should) do better

So…

- Freshness is now **punted** from stir-certs
- We kept in some general discussion about approaches to freshness
  - Stephen had asked why nothing was MTI
- I don’t think we’re ready to bless any One True Way to approach this
  - Need some further elaboration and implementation experience
- Leaving in the approach of providing a TN Auth List by reference
  - URL in the AIA

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

IETF 98 (Chicago)

STIR WG

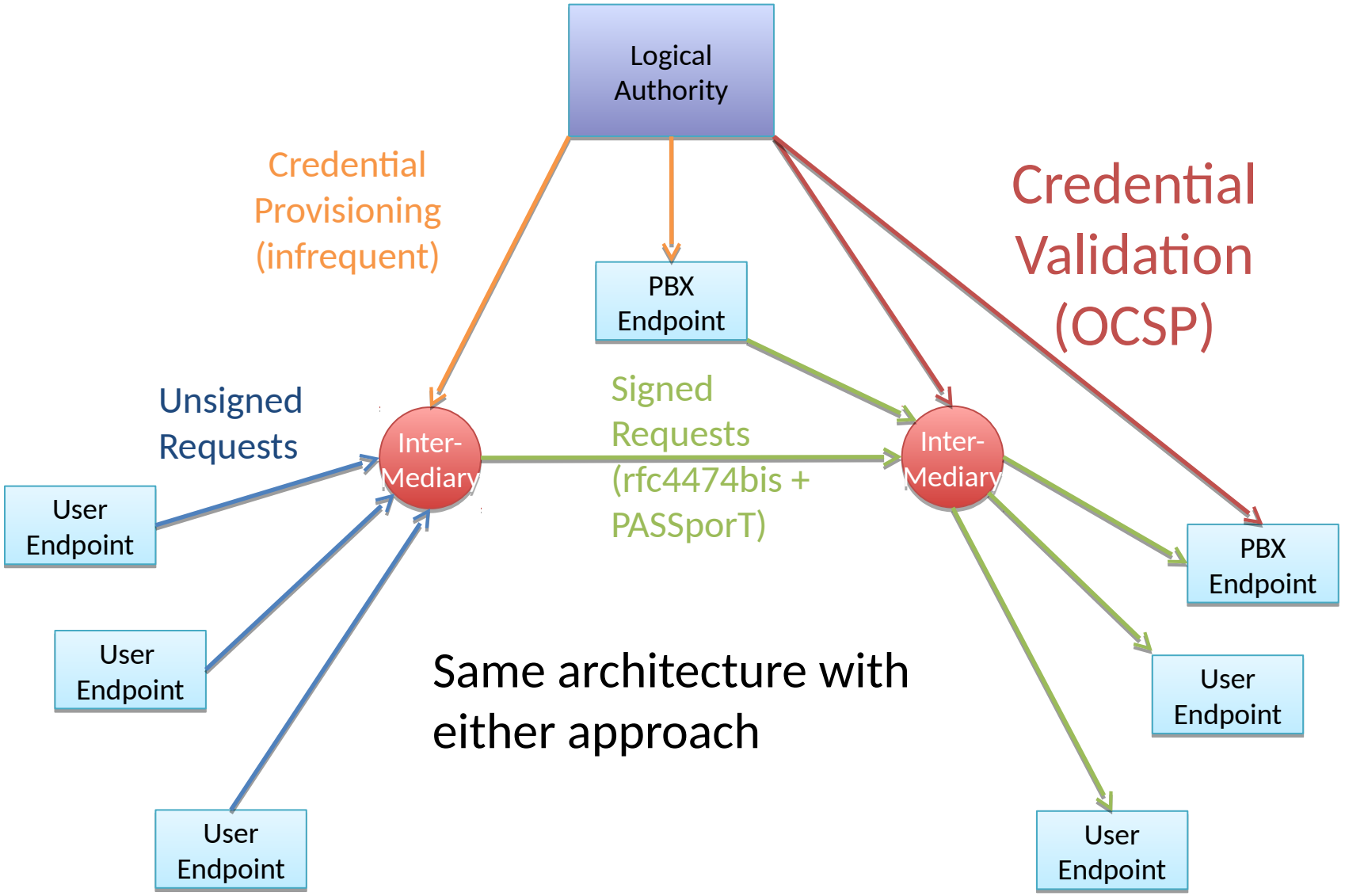
Who Cares about Freshness?

- Freshness is different for STIR certs than regular PKI certs
  - This is due to TN Auth List
    - Not for SPCs, really, just for TNs
  - The problem is the inherent dynamism of number assignment
    - Relying parties want to know if a cert is still valid for a number right now
- So if I don't care about TN Auth List for TNs in certs, can I not care about freshness?
  - Let me try to convince you that you should

Two paths

- 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
- Basically, I propose we explore both paths a bit and see what the experience yields

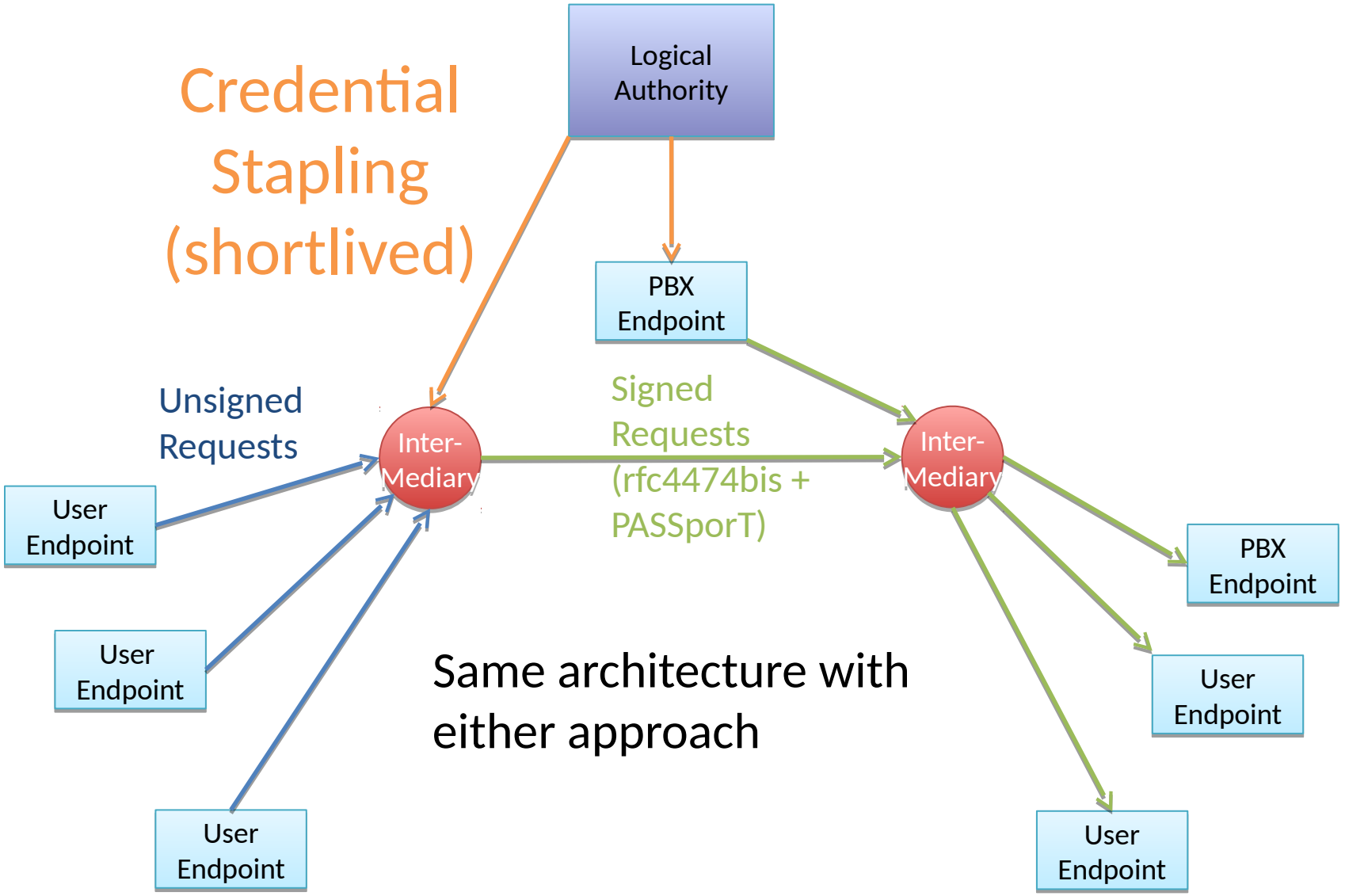
Real-time Credential Validation



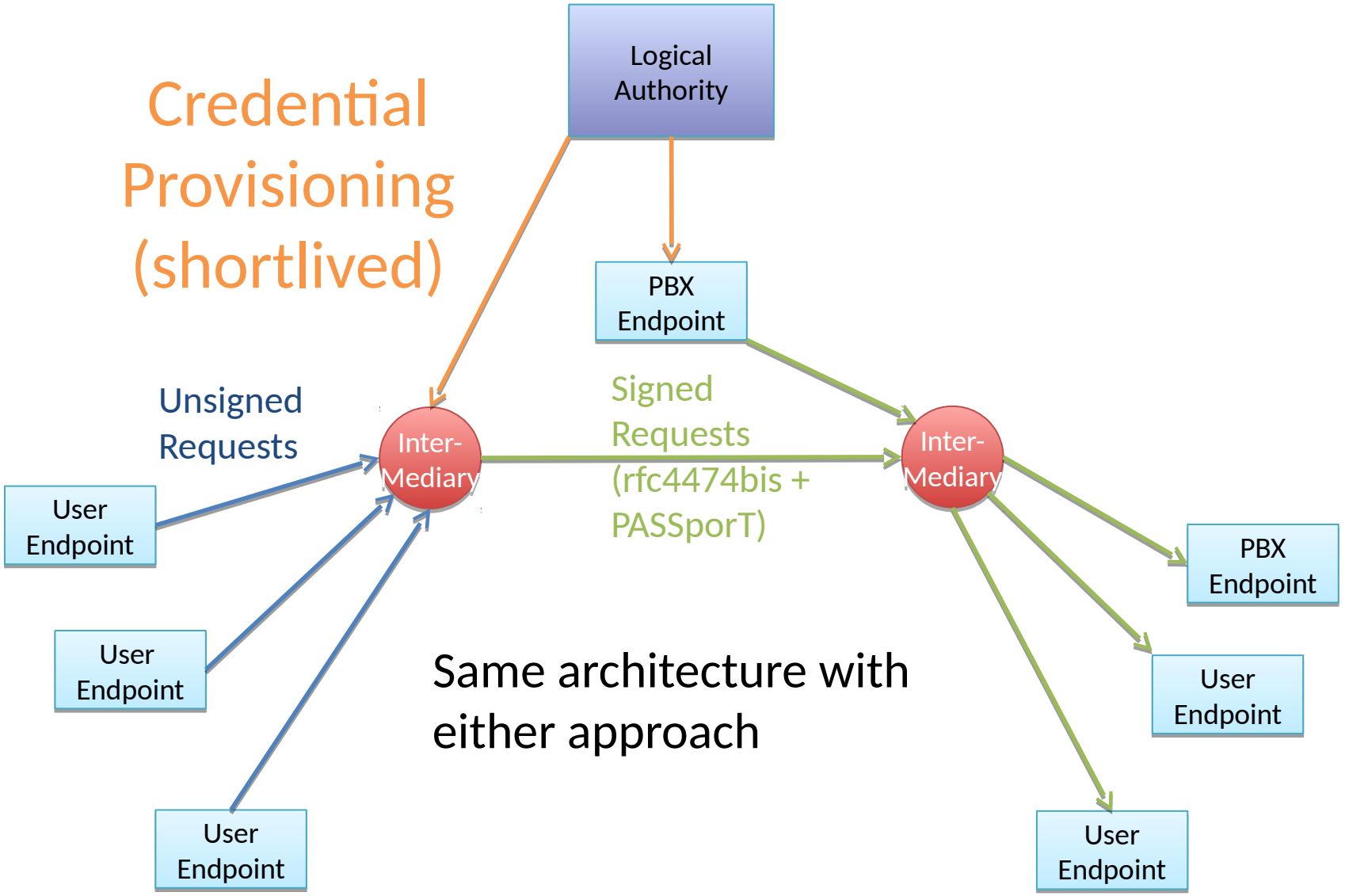
The OCSP Path

- Two ways: either terminating side or stapled
  - Terminating side is where much of the privacy leak occurs
- Probably, we would recommend stapling
  - We would define a SIP header for carrying a staple
    - Probably a general SIP feature, actually, not just for STIR
  - Staple basically says “the cert is valid for this number right now”
- The properties of stapling and short-lived certs start to look real, real similar

Stapled Validation



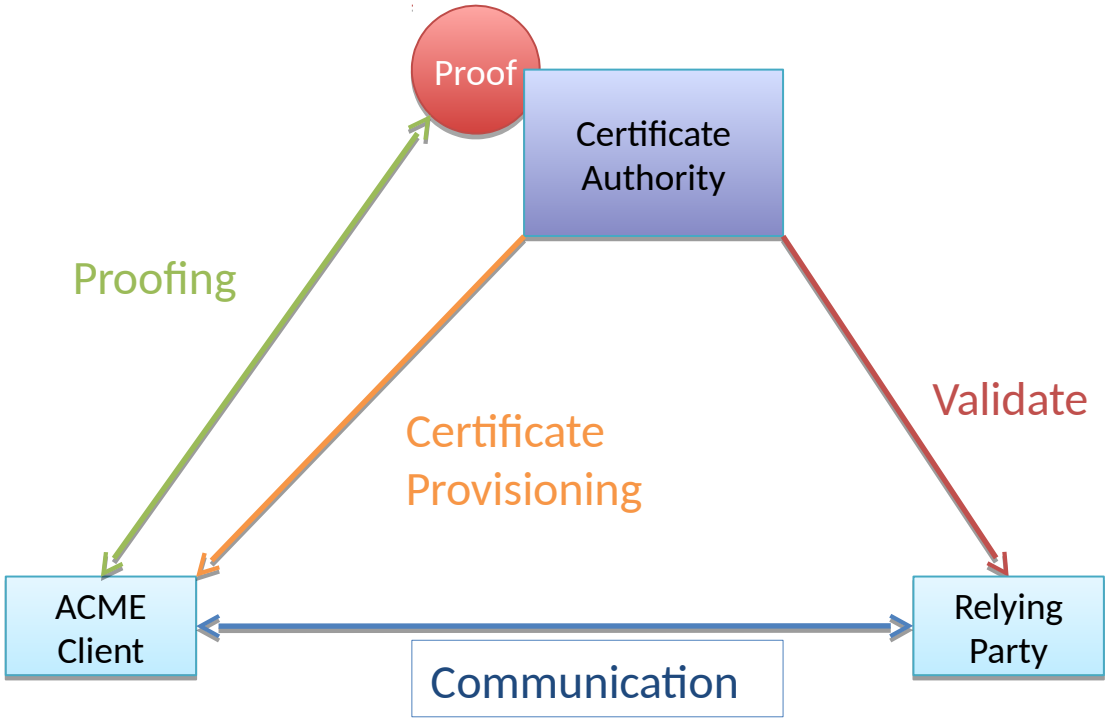
Short-lived Credentials



Short-lived

- Issuing certs for individual TNs that expire soon
  - Though not necessarily to individual people!
  - Basically says, “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



Individual TN certs: not just for end users

- ACME allows CSPs that control large number blocks to use disposable, single-number certs
  - A CSP basically uses an ACME “account” to get certs issued for numbers under its control as needed
  - Relying parties only know that the cert attests a number – doesn’t reveal the SPC unless you want to
  - Might be useful for some SHAKEN-like environments
- Similar mechanisms could work for enterprises
- Solves privacy concerns without requiring new protocol work for OCSP, new staple header, etc.

So what to do?

- I say let’s explore both a bit, see which story is better
- Not much harm in kicking the tires on both approaches out there in implementation
- Thoughts?

draft-peterson-passport-diversion
draft-peterson-stir-cercnam

IETF 98 (Chicago)

STIR WG

Don’t Forget

- I keep hearing that people need these things
  - CNAM draft just defines a PASSporT claim to carry a caller name
    - Works in a first or third-party mode
  - Divert draft leverages multiple Identity headers to allow chaining of Identities when call forwarding occurs
- If we need these things, let’s adopt/finish them