Certificate Credentials

STIR WG

IETF 91 (Honolulu)

~~Sean~~ Jon

draft-ietf-stir-certificates-00

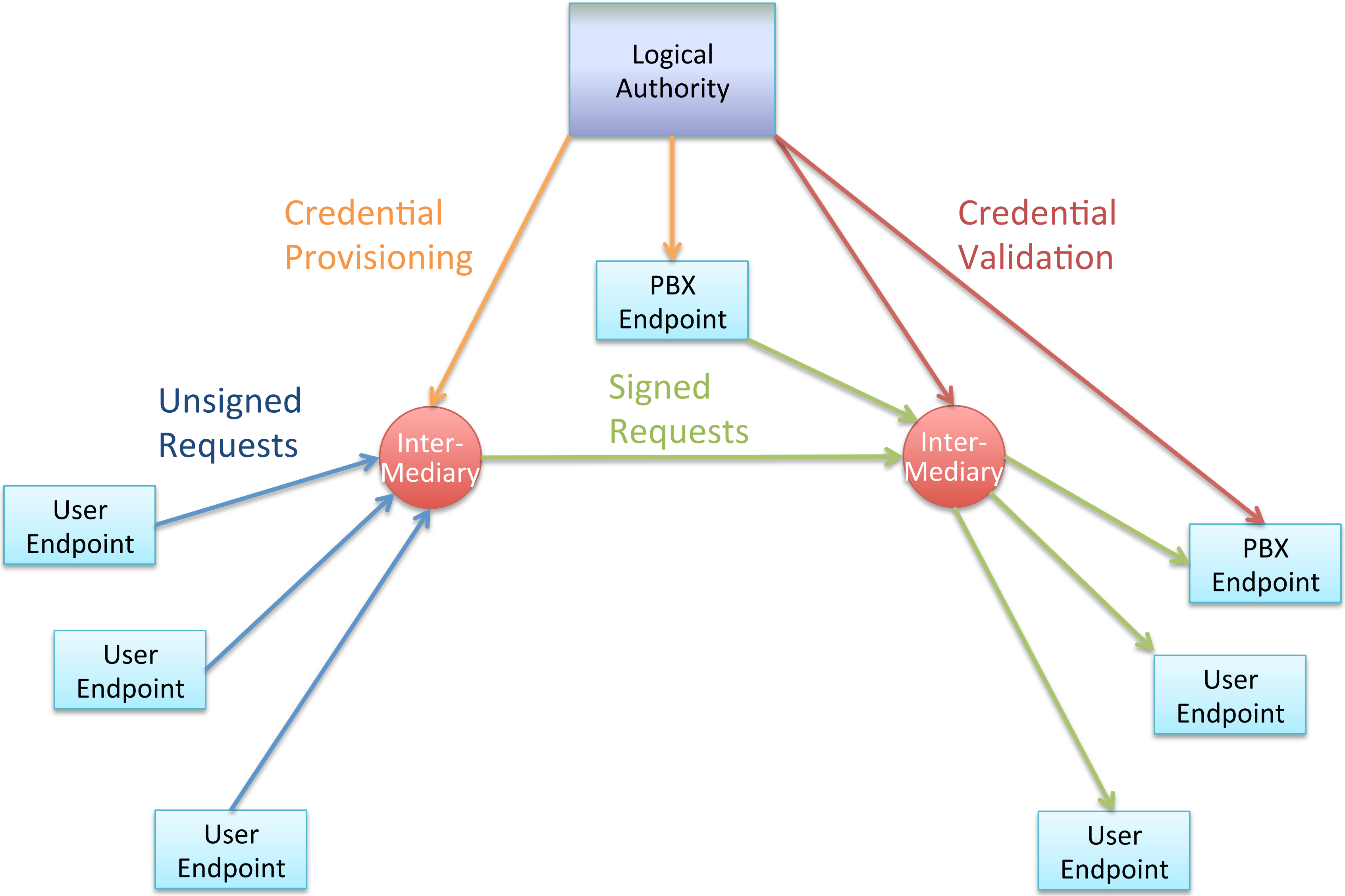
- Now a WG item!
- Provides a certificate-based STIR credential system
- Defines attributes for telephones numbers and number ranges
- Defines ways of acquiring the certs
  - Largely follows the RFC4474 Identity-Info paradigm
- Sketches techniques for real-time cert validation

Enrollment

- Document assumes a threefold method
  - Direct assignment
    - From numbering authorities, regulators, etc.
  - Delegation from above
    - From other number holders
  - Proof of possession
    - Last time we talk about this here, we had “no opposition” to going forward with that
    - Cullen will talk more about this next…

- Do we need a credential strength, LoA?

In-band STIR Logical Architecture



How do verifiers find credentials?

- Can we uniquely identify the needed credential based on TN alone?
  - Depends on how many authorities there are
  - If a user, enterprise and carrier all have certs that cover a particular number, due to delegation
    - Or proof-of-possession
  - Some kind of hint needed to disambiguate
    - Identity-Info URI can contain this
      - For out-of-band, this is tough, we'll talk about that next
    - Remember the CIDER "public key index value"

And then, credential caching

- Deferred to this document from RFC4474bis
- Should Identity-Info contain a credential hash
  - Let verifiers know that they already hold the credential
    - As multiple credentials might sign for the same number
      - So verifiers can't just tell from the From canonicalization
    - Some other form of UID for the credential also possible
  - Potentially complex interaction with caching
    - Verifiers can't assume the credential is still valid, so a lookup of some kind is still necessary
- But is there some value as an optimization?

Acquisition Protocols

- Different methods of acquiring certs
  - Push (e.g., credential arrives with a SIP request)
    - MIME multipart body
  - Pull (e.g., verifier acquires credential on receipt of request)
    - Either dereferencing Identity-Info URI
    - DNS: or creating a fetch based on the originating number
      - For certs, current recommendation is to use EST (RFC7030)
  - Prefetch (verifier gets top 500 keys) with pull
    - SIP SUBSCRIBE/NOTIFY mentioned in the text
  - Others? Probably – no need to choose one (but MTI?)
    - DANE? If you there's a DNS tree…

Open Issue: Handling Ranges

- But some entities will have authority over multiple numbers
  - Administrative domains could control millions of numbers
    - In non-continuous ranges
  - Includes service providers, enterprises, resellers, etc.
- Ideally, a service provider should not have to have one credential per number
  - The draft contains syntax for number ranges
  - But past a certain point, certs get too big
- Do we want to have by-reference approach?
  - Cert contains URL, URL contains the list
    - Reduces cert size
  - Or, cert contains a URL of a service where you can ask about a particular number

Expiry, Revocation and Rollover

- All credentials will have a lifetime
  - Ordinary rollover
    - Sometimes keys will be compromised before their expiry
  - But telephone numbers change owners, get ported, transfer normally
- Some sort of real-time checking required
  - DNS gets this for free (presuming no caching)
  - For certs, pull method could encompass this check
    - As could the prefetch
  - OCSP checks, but adds some overhead
    - More investigation to be done here
- Related to by-reference number ranges?
  - URLs for that give fresh responses – same problem?

Open Issue: Public or Confidential Credentials?

- How much information are we willing to make public?
  - Should credentials advertise a subject (e.g., “AT&T”)
    - Okay when a call is received to know the originating carrier?
      - Receiving user vs. receiving carrier may be different
    - More seriously, can an attacker mine a public database to reveal who owns *all* numbers?
  - Will we introduce VIPR-like privacy leaks?
- Can we restrict access to the credentials?
  - Identity-Info, say, could carry short lived, unguessable URLs
  - How important is endpoint verification?
    - Does trust become transitive if endpoints rely on intermediary verifiers?

Open Issue: Partial Delegation

- Authority over numbers conflates many powers
  - Power to claim identity for VoIP vs. SMS, power to port the number, etc.
- Should it be possible to delegate authority for specific services rather than the whole number?
  - e.g., my SMS provider can sign my texts (MESSAGE), but my voice provider signs my INVITEs
    - Yes, example is kind of contrived
    - Can I give my SMS provider a text-specific cert that would not enable to them to sign voice calls?
- Too complex? Do we need this?

Open Issue: Private Key Provisioning

- How do signers acquire and manage private keys for delegated certs?
  - Self-generated and provisioned at the authority?
  - Generated by the authority and downloaded to devices?
- Intermediaries and enterprises
  - Provision keys for number blocks, sign on behalf of calls/texts passing by
  - May possess many keys
- What’s the right tool to accomplish this?

END