STIR certificates

IETF 95 (Buenos Aires)

STIR WG

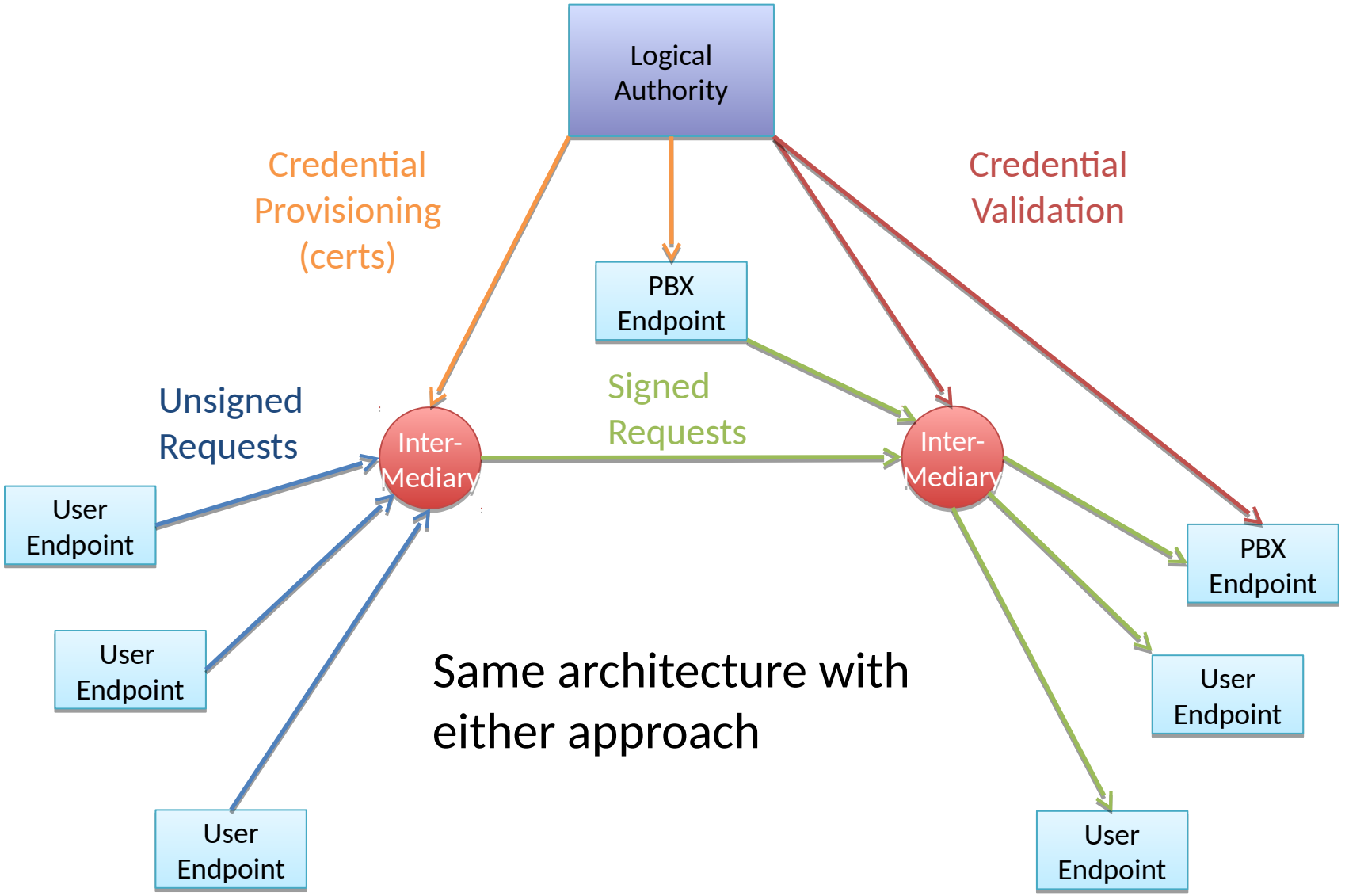
New version -03

- This revision clarifies the two existing approaches to the cert architecture
  - Both are valid, neither recommended over the other
  - In fact, they aren't even incompatible
  - A potential migration path can be mapped
- Otherwise, little different in -03, same core mechanisms
  - Hopefully, we are close to done now

The Two Approaches

1. Certificate's **subject** identifies the number holder
   - Maybe that's a domain name identifying an administrative entity: e.g., comcast.net
   - Maybe it's a SPID, or an OCN
     - Could be encoded as a domain name, or as a cert field
2. Certificate exists to identify the held **numbers**
   - Cert doesn't need a clear subject
   - Could carry numbers by value, or require a lookup

In-band STIR Logical Architecture



The First Approach

- How verifiers validate calls when the cert only identifies the carrier (or surrogate ID)
  - If carrier A trusts carrier B, and carrier B has signed the call, maybe that's sufficient
    - Advantage: deployable!
    - Disadvantage: not very inclusive
  - If carrier A receives a call from carrier C, and doesn't know them, maybe some service could help
    - Query to determine if the calling number is in carrier C's authority
    - This could be a local database detailing all carriers' authorities
    - Or a network service of some kind – no "golden root", could be several service providing identical information

The Second Approach

- How verifiers validate calls when authority over numbers is built in to the cert
  - If numbers appear by-value, one comparison and you are done
    - Advantage: dead simple, no RTTs
    - Disadvantage: new CA needed for such certs, and dealing with large, hetergenous blocks of numbers is tough
  - If the numbers don't appear by-value, you need a network dip
    - This could look a lot like the network dip on the previous slide
    - We've proposed OCSP for this, could be a simple web service too

Either way

- STIR certs are still certs
- Need CAs, need some CRL/freshness mechanism
  - Web is not our primary use case, not essential to use existing CAs
- Makes a lot of sense to me to use OCSP to kill two birds with one stone
  - Check cert freshness
  - Check if number is in scope of cert
- But IETF isn't going to mandate which to use
  - We're just specifying the protocol machinery

A Migration Path

- If we start with certs identifying the carriers
  - Let some big players get some deployment experience
  - Similar to how a few large email services seeded DKIM
- Then stand up some support services
  - Answer queries like “does this number fall under this cert’s authority”?
    - Could be OCSP, could define a simple web service too
  - Allows smaller players and more experimental approaches to play as well
- But the on-the-wire format (4474bis/passport) stays the same as we migrate

The IETF and the Industry

- The IETF isn't going to tell a verifier who it should and shouldn't trust in an authorization decision
- We are on the hook to document one or more ways to find out if a number is assigned to a carrier
  - We aren't forcing anyone to use any one in particular
- The industry can decide this
  - May well be different in different parts of the world
  - Or for different numbering spaces in one country

Moving forward

- If we think this migration path makes sense, let's get out the thumbscrews
  - Not aware of any new protocol work
    - Well, gotta fix the algorithms we talked about this week
  - Could use more eyes and reviews here on -04
- Do we want to specify a non-OCSP we service for determining carrier scope of authority?
  - If so, that's new work, propose that be a new deliverable

One Last Plug…

- Come to MODERN (next)
- Some of the questions about provisioning credentials spill over to there
- However, it's been tough to get agreement on the problem statement
  - Could use some eyeballs and energy