stir-certs-02

IETF 93 (Prague)

STIR WG

Jon

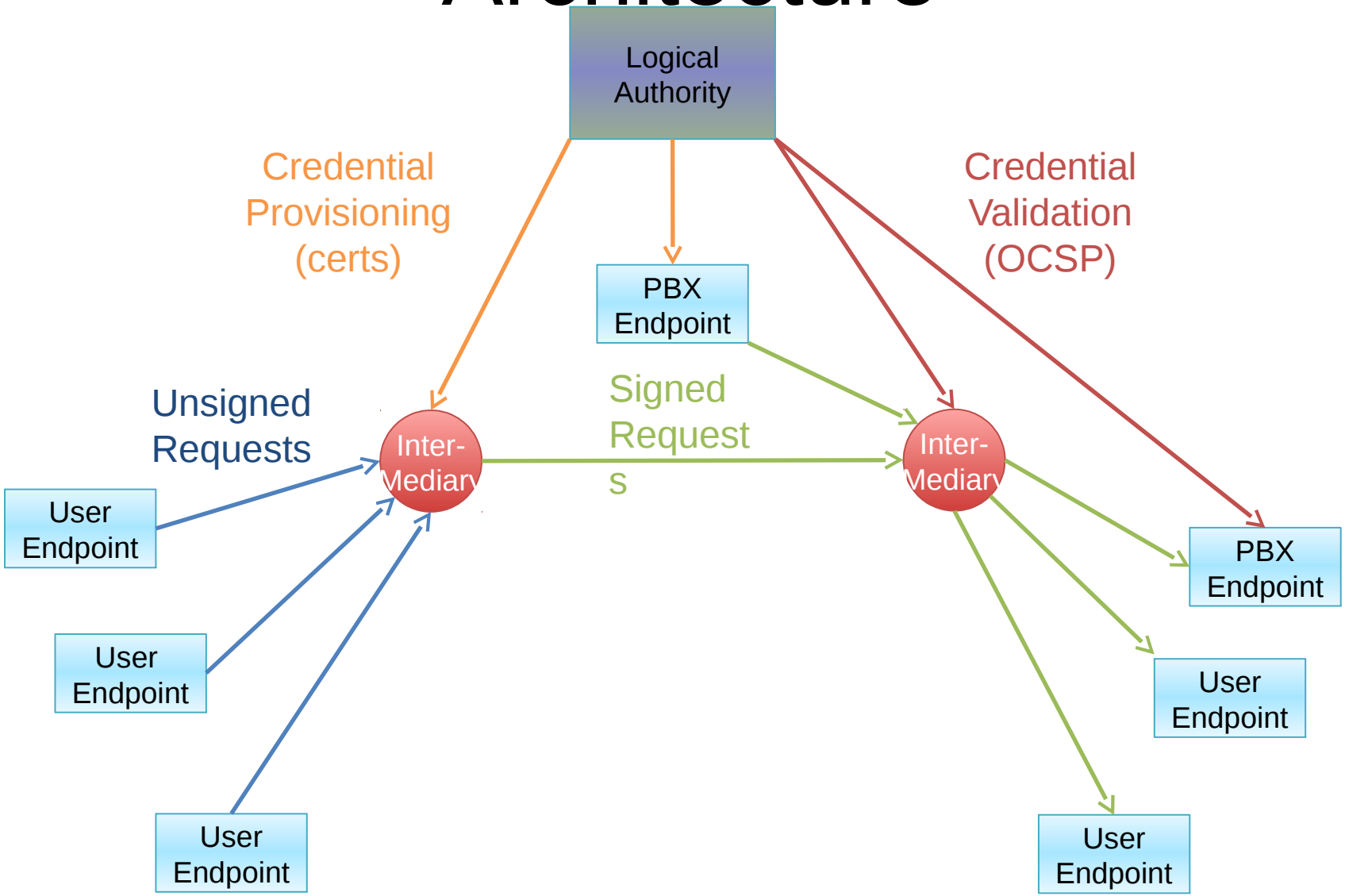
What we did since -01

- Basic specification of the cert extension (TNAuthList) didn’t change much here
  - Cert scope may include one or more or many TNs
- Fleshed out the OCSP mechanism
  - Defined extension for TNQuery
- Also specified a means of acquiring TNAuthList by reference

Why OCSP? (Refresher)

- Certs expire and sometimes are compromised
  - Relying parties check validity with mechanisms like CRLs or real-time checks such as OCSP
- Our case is special because of TNs
  - We extend X.509 with a TNAuthList
    - Says which TNs are under the scope of a cert
  - When a STIR verifier receives a call, it wants to know if the signing cert is valid *for that calling TN*
- OCSP can provide this functionality
  - Some extensions required

In-band STIR Logical Architecture



RFC5019 vs RFC6960

- Baseline OCSP (RFC2560) can be heavyweight
- Therefore, RFC5019 created an HVE profile
  - High-volume environments
- Unfortunately, it also reduces extensibility
  - We need some extensions to get our job done
- So currently, we’re approaching this as a profile of baseline RFC6960 (current OCSP)
  - TN-HVE, as it were
  - Allow our own extension, while keeping it light
- Assumes that STIR OCSP clients will not just use existing OCSP code libraries

Our Extension: TNQuery

- Basic syntax and semantics
  - Include TNQuery in OCSP requestExtensions
    - May contain one E164Number
  - If the TN is valid, server repeats the number in responseExtensions
    - If not, responseExtensions is absent
- Criticality is optional
  - If the OSCP server doesn’t understand the extension, it simply validates the cert itself
  - But remember: CAs issue the certs, and know if they support OCSP or not

TNQuery (2): Open Questions

- Is the extension syntax right?
  - Could have a binary yes/no response, defined in a separate TNAnswer in responseExtensions, say
    - Could make responses smaller, good for HVE
    - But will we ever want to query/respond for multiple TNs as an optimization?
- OCSP “unknown” response
  - Our thinking is to disallow unknown in our profile
- In HVE, does it make sense to ask about more than one number at a time?

TNQuery (3): Why do you ask?

- Any OCSP service the CA identifies in certs could be used by verifiers to ask about arbitrary numbers
  - When a verifier receives a call, necessarily it should be able to ask if the signing cert is valid for any number
    - An impersonator might try to use it for any number
- But a verifier could then use that service to ask about numbers it never received calls from
- Would we prefer to prevent this?
  - How badly would we want to prevent this?

Fancy Measures

- Could have the CA grant a secret to certificate holders
  - When signing a call, cert holder could somehow hash that secret with the calling number
    - Inserts result into the call itself
  - OCSP clients must include that hash into OCSP requests
  - OCSP servers could then detect whether or not a client had received a call for the number in the TNQuery
    - Policy could dictate when they make they check
- Makes OCSP messages larger, but, seems to put the burden of work in the right places
  - Would require a tweak to RFC4474bis – or maybe it could use Identity-Extension…

Acquiring TNAuthList By Reference

- How many TNs are in the scope of one cert?
  - Maybe it’s just one TN, maybe a thousand block, perhaps millions of numbers
  - We want some flexibility
- We propose using the AIA extension
  - Defines new accessMethod, “id-ad-stir-tn”
  - Currently, this is defined as HTTPS only
    - Should we be looking at other protocols? SIP?
    - If so, how do we want to organize those?
  - The object returned is the complete TNAuthList for the cert

Future Work: Subscriptions

- Once a STIR verifier pulls TN data from a certification authority, could the CA push it?
  - Some sort of SUB/NOT mechanism
  - Real-time notifications of changes in cert scope
- Imagine a HVE intermediary verifier
  - Effectively caching certs of carriers
  - Receives real-time notifications from the CA
    - Potentially more efficient than OCSP
- In STIR v1, or save it for later?
  - Try at least to future proof to allow for it

Other Open Issues

- Definition of range today
  - Starting telephone number, followed by an integer of the count
  - Do we need something more complex? Or prefixes?
- Level of assurance indication
  - Meaningful for some proof-of-possession mechanisms
  - We haven’t defined them yet – where to provide for that?
- Partial delegation
  - Beyond TNAuthList, do we want to indicate what services or applications a cert grants authority for?
    - E.g., one service authorized to sign for texting, another for calls

Eric’s Comments

- Eric Burger sent some comments last night
- Eric is concerned that there is a MUST for using OCSP (100,000+ tps!)
  - There isn’t
- Eric is concerned that the draft says we don’t want to use MIME in SIP
  - It doesn’t

Next Steps

- Resolve open issues
- Decide what to punt to later versions

- Be done

- (Do out of band!)