draft-ietf-stir-certificates-ocsp
draft-peterson-stir-ocsp-staple

IETF 115 (London)

STIR WG

Jon

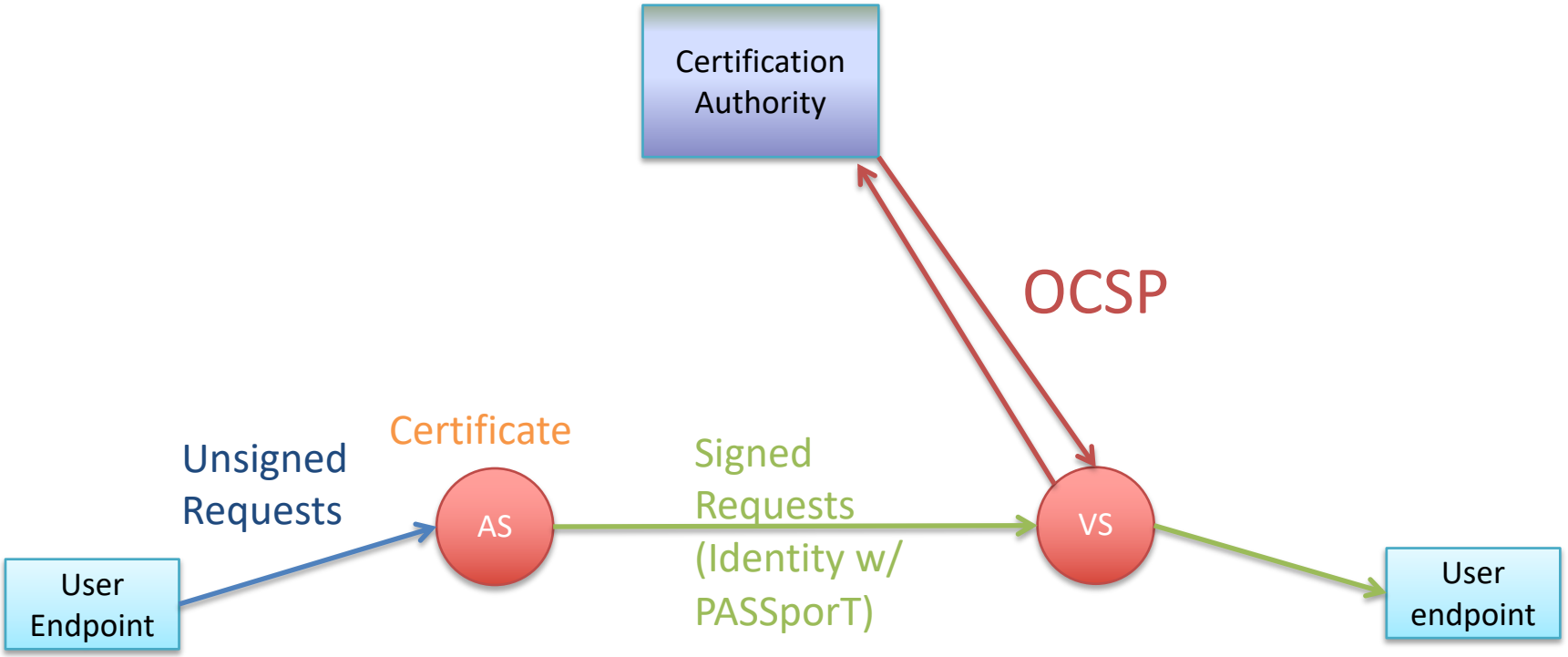
Freshness for STIR certs

- Freshness is different for STIR certs than regular PKI certs
  - This is due to TNAuthList
    - Not so much for SPCs, really, but 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
- We're looking at a couple of approaches
  - OCSP and short-lived certs seem to be favored
  - Today, we're just focusing on OCSP

The OCSP Path

- Two OCSP approaches: either terminating side query or stapled
  - Terminating side is where the potential privacy leak occurs
- As of draft-ietf-stir-certificates-ocsp-03, we have split out stapling to a separate draft
  - draft-peterson-stir-ocsp-staple-00
- The properties of stapling and short-lived certs start to look real, real similar

Real-time OCSP Validation

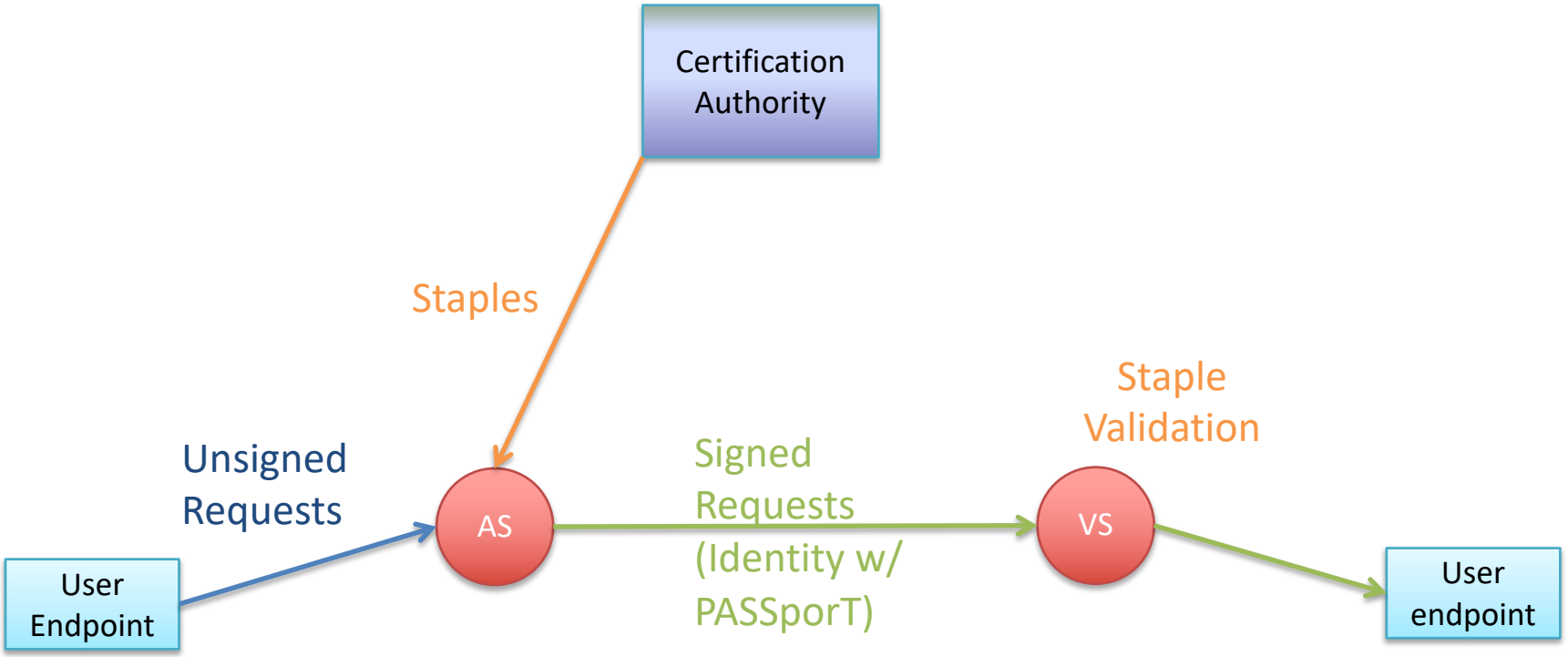


Cost: One RTT on the VS side per call

Stapling

- New draft about this
- Proposal is to carry the staple in the PASSporT
  - New “stpl” element in PASSporT payload
  - Alternative would be a separate SIP header, but:
    - Then you need a correlation function for multiple PASSporTs
    - And what about out of band?
- Basically, need to have the staple in hand when the PASSporT is created
  - Either you’ve already pre-cached it
    - Remember: that means caching a staple for each number you could *potentially* sign for
  - Or you fetch a staple for this TN during call setup time

Stapling



Cost is either:

- Push all staples (per TN) to AS in advance
- One RTT on the AS side per call

Open issues

- Diversion?
  - Like, one staple per “div” PASSporT?
- Interaction/coexistence with CRLs
  - If we want to say anything about that
- Should including with the TN singleExtensions in responses be a MUST?
  - Otherwise, how does this work for pre-gens in stapling?
    - i.e. The staple will just say “yes” and not “yes for this number”
    - Maybe only a MUST for stapled?

Next steps

- If we're okay breaking out the OCSP stapling draft, then the OCSP draft is probably close enough for LC
- Adoption for stapling draft?