

draft-ietf-stir-certificates-ocsp  
draft-peterson-stir-ocsp-staple  
draft-peterson-stir-certs-shortlived  
(etc)

IETF 117 (Bay Area)

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
  - But there are a lot of subvariants here...

# Jack Richard's Summary

- Options in play
  - **Existing by-ref using the AIA extension**
    - Already documented in RFC8226
  - **OCSP without stapling**
    - draft-ietf-stir-certificates-ocsp
  - **OCSP with stapling**
    - draft-peterson-stir-ocsp-staple
  - **Short-lived without stapling**
    - draft-peterson-stir-certs-shortlived (expired)
  - **Short-lived certs with “stapling”**
    - More on that in a moment

# Why so many?

- All of these have very similar properties, with fairly minor trade-offs between them
  - Mostly about how cacheable certs are, and whether you pay the cost for freshness on the originating or terminating side
- Some work more “out of the box” than others
  - RFC8226 AIA works for some use cases
  - We’re extending OCSP (for single TN queries)
    - And then extending PASSporT to carry the staple
  - Short lived works with no extension provided you don’t mind the latency/caching problem
    - “Stapling” would entail pushing the cert and its chain, making PASSporTs bigger, but making caching largely irrelevant
- Narrowing down to a single solution still seems premature (to me)

# Stapling – for more than OCSP?

- Current draft defines a way to carry an OCSP 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?
- For short-lived, proposal is to carry the certificate chain in x5c in the PASSporT header
  - Effectively a “staple”

# Discussion

- (we need more)

# Next steps

- Proposal:
  - Advance OCSP baseline (it's close to done)
    - I understand some other SDOs are incorporating it
  - Adopt/advance shortlived draft
    - Probably downplay ACME
  - Flesh out OCSP stapling and advance