draft-ietf-stir-certificates-ocsp
draft-peterson-stir-certs-shortlived

IETF 118 (Prague)

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 baseline RFC8226
  - **OCSP without stapling**
    - draft-ietf-stir-certificates-ocsp
  - **OCSP with stapling**
    - (Now also in draft-ietf-stir-certificates-ocsp)
  - **Short-lived without stapling**
    - draft-peterson-stir-certs-shortlived (revised)
  - **Short-lived certs with "stapling"**
    - Now also in draft-peterson-stir-certs-shortlived

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” here entails pushing the cert and its chain, making PASSporTs (much) bigger, but making caching largely irrelevant
- Narrowing down to a single solution still seems premature (to me)

Stapling – for more than OCSP?

- Current OCSP draft defines a way to carry an staple in the PASSporT
  - New “stpl” element in PASSporT payload
- For short-lived, proposal is to carry the certificate chain in x5c in the PASSporT header
  - Effectively a “staple”
    - Bear in mind it’s a big staple…

What's new?

- New -06 version of OCSP
  - Per our previous discussion, folded stapling back into the document
  - Need some help getting a plausible example of a stapled OCSP response
    - SPT is on it
- New -05 version of shortlived (just submitted)
  - Expands on the prior mention of "x5c" to convey shortlived certs within a PASSporT
  - MUST be supported by compliant VS implementations, SHOULD be used by AS's when certs are shorter-lived than a week
    - Is that the right threshold?

Next steps

- Fix stapling example in OCSP draft, then advance
- Adopt/advance shortlived draft