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...
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)
What’s new?

• New -07 version of OCSP (as of, well, today)
  – Stapling is built in
  – Now have examples of the OCSP request and response with the extension
    • Just the PEM, not the long-ish decoding – do we need that too?
  – Quick question: do we need to specify anything about algorithms in the PASSporT, or is that built in to OCSP?

• No new version of shortlived (at -05)
  – 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
Next steps

- OCSP draft good to go?
- Adopt/advance shortlived draft
  - Call for adoption is ongoing now