draft-ietf-stir-certificates-ocsp
draft-ietf-stir-certificates-shortlived

IETF 120 (Vancouver)

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…

What's new?

- New -08 version of OCSP
  - Now have examples of the OCSP request and response with the extension
    - Thanks to Russ for the assist
  - For now, keeping .cer in examples
    - Just because it's in absolutely everything else (e.g. RFC8225)
- At long last shortlived is a WG item! (at -00)
  - We think we've got "x5c" basically correct now
    - Even a good (RFC8226) example of "x5c" in there
    - Allows both "x5c" and "x5u" to appear simultaneously
    - Still not a MUST for "x5c" however… should there be?

Next steps

- OCSP draft good to go?
- Shortlived probably is good for a last call as well?