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

IETF 121 (Dublin)

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

What’s new?

- OCSP is now advancing to pubreq
- Minor adjustment in the new shortlived-01
  - Now a MUST for ”x5c”
    - Still a MAY for using a redundant “x5u”
  - Also allowed shortening the certificate chain to exclude the root cert (as a MAY)
    - No text added about shortening it any further (excluding intermediate CA, for example)

Next steps

- Shortlived probably is good for a last call, if we’re good with the “x5u” support