draft-ietf-stir-certificates-ocsp

IETF 114 (Philadelphia)

STIR WG

Jon
Why OCSP?

• 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

• OCSP can be bolted on to the existing infrastructure
  – Useful for certificate delegation, and the use of TN’s by-reference in delegate certs especially
    • Need a way to verify that a particular number is valid for a cert that does not involve downloading an entire TNAuthList
  – Not intended to compete with any CRLs for SPC use of TNAuthList, be they centralized or federated
Real-time Credential Validation

- Logical Authority
  - Enterprise (delegate)

- AS
  - Unsigned Requests
  - Credential Provisioning (infrequent)
  - User Endpoint

- VS
  - Signed Requests (rfc4474bis + PASSporT)

- PBX Endpoint
- User Endpoint

- User Endpoint
The OCSP Paths

• Two ways: either terminating side query or stapled
• Proposal: let’s look at stapling later
  – Requirement for AS to get staples from CA would be a heavy lift
  – Best to build it incrementally
    • Trades the RTT at the terminating side for pre-call at the originating side
• (Also, the properties of stapling and short-lived certs start to look real, real similar)
  – Continue to explore the short-lived path separately
So what to do?

• If we punt on stapling, I think we’re probably pretty close on this one
  – Core work was baked a long time ago

• Could use some eyeballs
  – Because this was all done a long time ago

• Not neglecting short-lived, but more work needed there
  – ACME integration, etc.