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

IETF 113i (virtual)
STIR WG
Jon
Who Cares about Freshness?

• This is a rerun from IETF 98 (!)
• Freshness is different for STIR certs than regular PKI certs
  – This is due to TNAuthList
    • Not for SPCs, really, just 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
• So why are these back on the menu?
  – Because of 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
Two paths

• Refreshed some ancient drafts: OCSP and short-lived certs
  – They have very different privacy properties, potentially
• Basically, I propose we explore both paths a bit and see what the experience yields
  – Still (!) – because the drafts have been updated to be about the TN use of TNAuthList for certificate delegation in particular
  – Not intended to compete with any CRLs for SPC use of TNAuthList, be they centralized or federated
Real-time Credential Validation

Same architecture with either approach
The OCSP Path

• Two ways: either terminating side or stapled
  – Terminating side is where much of the privacy leak occurs

• Probably, we would recommend stapling
  – We would define a SIP header for carrying a staple
    • Probably a general SIP feature, actually, not just for STIR
  – Staple basically says “the cert is valid for this number right now”

• The properties of stapling and short-lived certs start to look real, real similar
Stapled Validation

Credential Stapling (shortlived)

Same architecture with either approach

Unsigned Requests

Signed Requests (rfc4474bis + PASSporT)
Short-lived Credentials

Credential Provisioning (shortlived)

Same architecture with either approach
Short-lived

• Issuing certs that expire soon
  – Could be for individual numbers even (or ranges)
  – Basically says, “this cert is valid for this number right now”
    • Also obviates the need for relying parties to talk to the CA
• What does short-lived mean?
  – Hours? Days? Not months or years anyway.
  – Part of our job is to decide what is appropriate
• The hard part is getting the new cert... but...
ACME makes short-lived easy

Diagram:
- **Proof**
- **Certificate Authority**
- **Proofing**
- **Certificate Provisioning**
- **Validate**
- **ACME Client**
- **Relying Party**
- **Communication**
Individual TN certs: not just for end users

• ACME allows CSPs that control large number blocks to use disposable, single-number certs
  – A CSP basically uses an ACME “account” to get certs issued for numbers under its control as needed
  – Relying parties only know that the cert attests a number – doesn’t reveal the SPC unless you want to
  – Might be useful for some SHAKEN-like environments

• Similar mechanisms could work for enterprises

• Solves privacy concerns without requiring new protocol work for OCSP, new staple header, etc.
So what to do?

• I (still) say let’s explore both a bit, see which story is better
• Not much harm in kicking the tires on both approaches out there in implementation
  – In fact, they aren’t really incompatible, both could coexist in the marketplace
• Should we advance either/both?