STIR Certificate delegation

IETF 104
STIR WG
Jon - Praha - Mar 2019
New document, sets out to explain:
- how delegation of RFC8226 certificates works
- how AS/VS deal with certificate chains
- interaction with ACME

It’s short, hopefully doesn’t need to be much longer

Supports a number of enterprise use cases
- Also meaningful for some OTT providers
- End users? Maybe someday, not current focus
Delegation & Authority

• Delegation built-in to certificates
  – RFC5280 describes path construction and path validation
    • STIR uses SKID/AKID delegation
• A root authority assigns certificates to number assignees
  – Could contain OCNs or TNs/blocks
• Assignees then delegate individual TNs or blocks to enterprises
  – Authentication Service signs with delegate certificate
  – Verification Service does path validation
How does STIR use it?

• Based (loosely) on RPKI semantics
  – Each certificate in a chain must be “encompassed” by its parent
    • No name constraints used: TNAuthList *is* the constraint
    • Verification services do the necessary path validation
  – Also means these are CA certs, not EE
    • Allowing CA certs to sign PASSporTs to reduce chain length

• In the x5u of PASSporT, specify an application/pem-certificate-chain
  – Stolen shamelessly from ACME

• In our ACME ”atc” work, we’ve added hooks for it
  – ACME knows how to give you a CA cert and a cert chain
  – Delegation is not required to use ACME, however
ACME (through a STIR lens)

- Token Authority
- ACME CA
- ACME CA (Cert)
- ACME CA (Cert Repo)
- ACME CA (Cert Validation)
- ACME Client
- AS
- VS
- Relying Party
- STIR signed calls

Proofing ("atc")

Same entity (or not)

Certificate Provisioning (TNAuthList)

No different for delegation
Future Work

• Maybe define “partial” delegation cases
  – I want to just delegate part of my authority
    • i.e., this entity can only sign MMS messages for me

• Alignment with ATIS

• Flesh out other tools enterprises want
  – Return to work on connected identity
  – Return to short-lived certs work
    • Both have their own drafts, dusty ones now
  – Certificate conveyance in SIP? Maybe time
Next Steps

• Adoption?
  – Prefer to keep this simple, do "future work" in separate drafts

• Review, advance, etc.