STIR Certificate delegation

IETF **105**

STIR WG

Jon - Montreal - Jul 2019

draft-ietf-stir-cert-delegation-00

- Specification 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/CPaaS providers
  - End users? Maybe someday, not current focus

Why are we talking about this?

- Sometimes, outbound calls will not transit the AS of the carrier who owns the calling party number
  - Common case is enterprises who use LCR for outbound calls across multiple providers
  - Some “legitimate spoofing” cases do this too
- Motivation: push credentials from TN owners to an AS able to sign for the call
- Alternative: let outbound carriers sign even though they don’t own the number
  - If we just allow carriers to sign for any number, what’s the point of STIR?
    - Enables traceback, which is a good start, but real-time authorization/blocking is the direction of the industry

SPCs and TNs

- Early deployment is based on SPCs
  - Specifically, OCN-level certs
- Some non-carrier entities probably should have SPCs
  - Assigned complex, non-contiguous and large set of TNs
  - Carriers in all but name (and regulation)
- But many enterprises have simple, stable TN blocks
  - Or even just want to sign calls from a single dial-out number
- Delegation from SPCs to TNs requires understanding when a TN range is “encompassed” by an SPC
  - But that’s something verifiers need to understand about SPCs anyway when a call from a TN arrives
  - The real question is when is “encompassing” checked: when certs are issued, or during call processing at the VS?

To CA or not CA?

- Setting the CA bit to “true” enables X.509 delegation
  - We’ve added this to the ACME “atc” mechanism for STIR
- This means we’re dealing with certificate chains
  - Though, if the same CA is issuing a carrier’s SPC cert and the delegated enterprise cert, possible to collapse
  - We may also have cross-certification to consolidate credentials and permissions
- There are alternatives if we can’t set the CA bit
  - A STIR variant of draft-ietf-tls-subcerts
    - Workaround for PKI environments where you can only get EE certs
    - Basically, a pseudo-cert with a narrower scope

Smaller questions

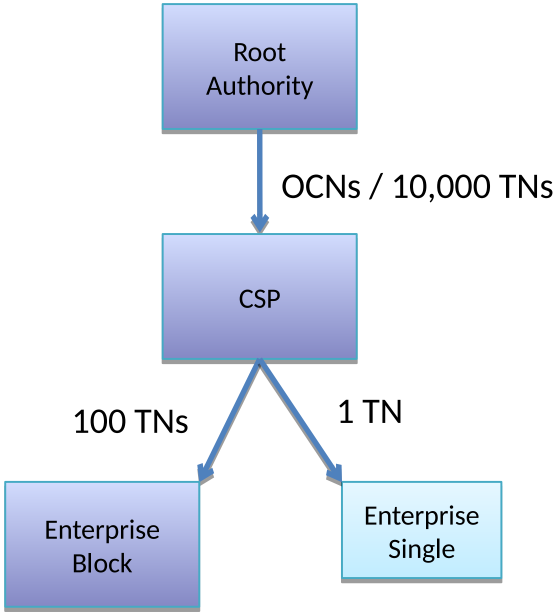
- x5u vs. x5c
  - There is a JWT way to do certificate chains
  - Are we too locked-in to x5u?
- Setting a flag for “encompassed” validation in certs?
  - Yes, it is a sort of “good bit”
    - But CAs are kind of in the business of validating names when CP/CPS includes some formal requirement
  - Note that this is auditable offline, which is handy
- Interaction with ACME STAR
  - Lots of work on short-term delegation around that, some may be reusable for our ACME interfaces

Next Steps

- Resolve issues, advance
  - Pressing need for solutions in the marketplace

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


Root Authority
OCNs / 10,000 TNs
CSP
100 TNs
1 TN
Enterprise Block
Enterprise Single