STIR Certificate delegation

IETF **106**

STIR WG

Jon - Singapore - Nov 2019

draft-ietf-stir-cert-delegation-01

- 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

Changes since last time

- Added some language on TNAuthList permissions
  - They are additive
    - If there's a list of OCNs, then that cert can sign for any of those OCNs
    - If both OCNs and TN ranges are present, it can sign for the superset of all TNs under those OCNs and the TN ranges
- More on collapsing the cert chain
  - If the same CA issues a delegate cert that issued the parent, the trade-off of just not issuing the cert as a delegate
- More on subcerts
  - Basically to leave the door open to specifying them, if we need them – hopefully we won't

Changes (2)

- Left over from our last meeting
  - Sticking with x5u rather than x5c
    - If people want to start using x5c, fine, though
- No need for the “good bit”
  - Assumed that the CAs issuing these certs are performing any necessary validation
    - Largely to make sure that at TN delegation fits within an OCN range
    - If you want to also check it at the VS, feel free
- For now, nothing about ACME STAR
  - Will be in the short-lived certs draft, if we turn out to need it

Next Steps

- The marketplace is definitely kicking the tires on this
- ATIS still figuring out what it wants to say
- Maybe hold this for another cycle
  - Might we worth getting some more eyes on it
- Basically, this should be ready to advance

BACK UP

Why are we talking about this?

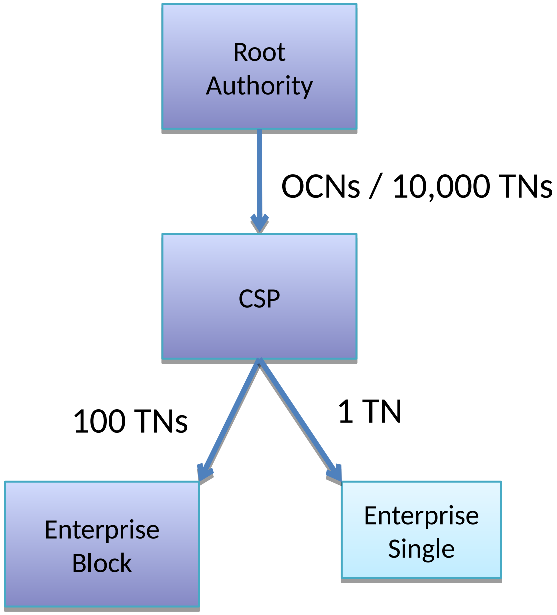
- Sometimes, outbound calls will not transit the AS of the carrier who owns the calling party number
  - Common case is enterprises who use LCR for outbound calls across multiple providers
  - Some “legitimate spoofing” cases do this too
- Motivation: push credentials from TN owners to an AS able to 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?

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