STIR certificates

IETF 94 – Yokohama
STIR WG
No New Version

• But not because there has not been much talk about it...

• Clear that we need to reaffirm some first principles
What is the STIR certs draft?

• Specifies a way to associate authority for TNs in a certificate.

• Why? Our threat model (RFC7375) reads:

  The design of the credential system envisioned as a solution to these threats must, for example, limit the scope of the credentials issued to carriers or national authorities to those numbers that fall under their purview.

• So, we made this a WG item, etc.
In-band STIR Logical Architecture

- Logical Authority
  - Credential Provisioning (certs)
  - Unsigned Requests
  - Inter-Mediary
    - User Endpoint
    - Inter-Mediary
      - Signed Requests
        - Inter-Mediary
          - Signed Requests
            - PBX Endpoint
  - Inter-Mediary
    - User Endpoint
    - Inter-Mediary
      - Signed Requests
        - Inter-Mediary
          - Signed Requests
            - PBX Endpoint
  - Inter-Mediary
    - User Endpoint
    - Inter-Mediary
      - Signed Requests
        - Inter-Mediary
          - Signed Requests
            - PBX Endpoint
  - Inter-Mediary
    - User Endpoint
    - Inter-Mediary
      - Signed Requests
        - Inter-Mediary
          - Signed Requests
            - PBX Endpoint
Is There Another Way?

• Sure!
• We aren’t going to design or select a CA
• We aren’t going to tell a verifier who it should and shouldn’t trust in an authorization decision
• We are on the hook to document a way to find out if a number is assigned to a carrier
  – We aren’t forcing anyone to use it, though
Ultimate Requirement Questions

• Should these calls be publicly verifiable on the Internet?
• Should you be able to trust a call signed by an entity with whom you have had no previous association?
• Should you need to know the entity signing a call in order to trust it?
• Should non-traditional entities (not LECs, in the US) be able to sign for numbers?
Transitive Trust vs. Intransitive Trust

• If carrier A trusts carrier B
  – And A and B each have certs identifying themselves in the subject

• Can A sign (rfc4474bis) a call with that cert, and can B trust that call
  – Yes, of course – deployable today, with web certs!

• But are the semantics any different from sending the call over a TLS connection pinned up with A’s cert?
  – Or any other transitive trust closed network today?
  – All B really knows is that A is willing to vouch for the call
  – Signing here has limited value compared to baseline PAI
    • Could persist through transit networks, say
Public or Confidential Credentials?

• How much information are we willing to make public?
  – Should credentials advertise a subject (e.g., “AT&T”)
    • Okay when a call is received to know the originating carrier?
      – Receiving user vs. receiving carrier may be different
    • More seriously, can an attacker mine a public database to reveal who owns all numbers?
  – Will we introduce VIPR-like privacy leaks?

• Can we restrict access to the credentials?
  – Identity “info”, say, could carry short lived, un-guessable URLs
  – How important is endpoint verification?
    • Does trust become transitive if endpoints rely on intermediary verifiers?
Certs for OCN

• Or SPIDs, or some other surrogate for identifying a carrier
  – Might alleviate “leakage” concerns
• Verifiers could query a back-end database that tells you whether or not a number falls under that OCN
  – Really, very much what the OCSP check in stir-certs is about
• Assumes a new CA for those OCNs or whatever, though
  – And if you’re doing that, why not stir-certs?
Other Transitive Approaches

• Imagine defining a “spec” (rfc4474bis) that means “third-party signature”
  – Like, carrier A got this from carrier C or enterprise D, and carrier A is vouching for them
  – Maybe carrier C or enterprise D also has an Identity sig in the message
So what now?

• If someone wants to propose new work on certs for OCNs, or with carriers as subjects, feel free
  – Doesn’t have to be done here, even

• This is a time for trying out approaches
  – No one has a monopoly on answers here

• We should continue with the stir-certs work