rfc4474bis-03

IETF 92 (Texas)

STIR WG

Jon

First principles (yet again)

Separating the work into two buckets:

1) **Signaling**
   - What fields are signed, signer/verifier behavior, canonicalization
2) **Credentials**
   - How signers enroll, how verifiers acquire credentials, how to determine a credential's authority for identity

- rfc4474bis is our signaling solution
  - But contains guidance for specifications of (2)

What we did since -02

- Deleted a good deal of legacy text
  - Also, tried to eliminate some cross-referencing
  - Probably more optimization to be done here
- Lowered Date threshold to one minute
  - Consistently, we hope
- Fixed the mandatory signature over a=fingerprint
  - Now should support multiple fingerprints, when needed
    - Fingerprints are concatenated in alphanumeric order
      - Is that our best idea?
- Improved “canon” text
  - Still some to discuss here

Open issues: On “canon”

- Last time we talked about canonizing To
  - Without it, if To: changes, verifiers could fail
  - Plan: canon=t:<TN1>;f:<TN2>
- What about mixed cases?
  - From is a greenfield URI, To is a TN
    - Or vice versa
- Proposal: either t: or f: or both may be present in “canon:
    - Written up in my -04

Open Issues: Signing PAI

- Sometimes, a TN lives in PAI (RFC3325)
  - This is regrettable
- Easy out:
  - Allow “canon” to reflect the PAI
  - In PAI-using networks, the recipient could know what to do
  - Of course, if PAI is chopped off, and “canon” remains…
- Good idea? Hidden problems?
- Also, is this a slippery slope?
  - Lots of numbers in different places in 3GPP specs

Signing anything else

- CNIT and extensibility in general
- Typically in security mechanisms, the less the better
- If we want STIR's signature to cover CNIT, what's the best way to leave that door open?
  - Not clear which header we'd be signing yet, or what parsing needed
- Could have another field with an extensibility mechanism defined
  - Similar in style to Identity-Reliance
  - Best idea: we would create a blank CNIT will fill in

Anything else?

- Some more organizational work could be done
- Last call this, or wait?