rfc4474bis-01

IETF 89 (London)

STIR WG

Jon & Cullen

First principles (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

- Last time, we agreed to accept this point of modularity
- rfc4474bis is now about (1)
  - But contains guidance for future specifications of (2)

Recap

- Identity Signature over To, From, Method, and Date
- The mechanism works for TNs, could also work for SIP URIs
  - Would need to specify credential systems for greenfield IDs
- Optional Identity-Reliance header
  - Optional for signer to add, optional for verifier to check if present
  - This too follows agreement from last meeting, and STRINT
- Identity-Info now much broader
  - Acts as a selector if multiple parties can sign for the name
  - Not just for certificates per RFC4474, more on this later
- Canonicalization (just a stub now)
- Keep much of the original RFC4474 apparatus
  - All the response codes, etc.

Credential Systems (5.4)

- All credential systems must specify:
  - What URI schemes are permitted in Identity-Info
    - Any special procedures required to dereference those URIs
  - How the verifier learns the scope of credentials
  - Procedures required to extract keying material from the resource specified in Identity-Info
  - Any algorithms other than baseline required by those credentials
    - With the caveat that new algorithms require "Standards Action"
- Is this the right list?
- This creates a point of modularity
  - We let multiple flowers bloom, or pick one, or something in between

Credentials

- Certificates
  - Would follow the original RFC4474 model
    - X.509 certs have always contained telephone number**s**
  - Assume a new CA (or set of CAs) issuing certs for this purpose
  - Ex: draft-peterson-stir-certificates
- DNS
  - Make keys (or pointers to keys) available through the DNS
  - Ex: draft-kaplan-stir-cider
  - If we were going down this route, more likely we'd use DANE?
    - Also, more likely we'd use post-ENUM label syntax?

- Do we really need to choose between these?
  - DANE and certs are both options for the web, now – problem?
  - All credential systems need to meet base requirements, that's it

Canonicalization

- So how do we do it? (still just a stub in the draft)
  - Strip special characters, append a country code if missing (crib from ENUM procedures?)
  - End up with a format like:
    - +17004561000 (should we include the +?)
  - What if country code can't be inferred (at either side)?
    - Two possible options:
      - Guess that it's from this nation and append a cc, if the call is international, it fails
      - Leave it without a country code and don't include a +?
  - What about special numbers?
    - Especially if we're canonicalizing To as well
    - Short codes, emergency codes, many corner cases

Open Issues

- Plenty
  - Do we want something like a hash in Identity-Info to recognize that credentials have been seen before?
  - Do we want explicit, always-on integrity protection for keying material in SDP?
  - Is the signing algorithm right?
    - Do we want to consider EC for smaller keys?
  - Biggest TBD: canonicalization
- This was a Frankenstein pass, editing needed

Way Forward

- Technical knobs and buttons now in place
  - Details may change, but there's a framework here

- Is roughly this how we want to go forward?

Back UP

Canonicalization

- Proposal: **Identity is in the From**, always
  - Some discussion about alternate headers (PAI)
    - More to talk about there?
  - Some services have a reply-to semantic
  - But, the From header field value is what UAs render
- Intermediaries may tweak numbers in transit
  - No bounds on intermediary behavior
  - Some behaviors might make canonicalization impossible
    - In that case, it just doesn't work
    - If this takes off, hopefully policies will make this easy
- Both the signer and verifier must canonicalize
  - Must arrive at the same result, or the verifier will fail it

Replacing RFC4474

- Use Identity as the name of the header (or not)?
- We do want people to use the results of STIR rather than RFC4474
  - But, we want to keep all the response codes and related apparatus
    - 428 “Use Identity” – verifier requires signed Identity
    - 436 “Bad Identity” – verifier couldn’t verify it

- Punt on Identity-Info as part of the credential piece

Just TNs, or other URIs?

- Signers and verifiers must be able to recognize a TN in the From
  - Potentially non-trivial, we can't depend on user=phone or a +
    - **sip:67463@shortcode.com**
  - So, STIR implementations will necessarily be aware of non-TN URIs
- The proposals so far favor doing both
  - For the **signaling module**, what would we do differently, really?
- How much new work is there for non-TNs?
  - RFC4474 has a good story about this
    - Once you fix the signature fields, as above
  - DANE support is the only new wrinkle
    - But the dns: URI could go in Identity-Info…