STIR for Messaging

IETF **109**

STIR WG

One Night (not) in Bangkok – Nov 2020

J Peterson

draft-peterson-stir-messaging

- A new draft about leveraging STIR for text and multimedia instant messaging services
  - Helpful for those that use telephone numbers as identifiers, specifically for the originator of messages
- Why?
  - Message spam is a problem, and while email-style content analysis helps, it doesn't help for encrypted messaging
  - STIR certificates bestow authority for communication from a TN
    - Would make little sense to develop a separate PKI for messaging from telephone numbers
- The big question: who would use this?

What we basically get for free

- Session-based messaging negotiated with SIP
  - MSRP, text-over-RTP (RFC4103), similar things
  - Should work through straight-up RFC8224
    - Some questions there about how "mkey" interacts with these
- Is it restricted to just messaging from phone numbers?
  - RFC8224 allows for alternate identifiers (like SIP URIs)
  - Do we want to restrict this to just cases where RFC8226 certs (with TNAuthList) are in play?

Low-hanging fruit

- Identity headers for MESSAGE requests
  - We probably need to be thinking about Identity headers for most SIP requests at this point
- Adds a new claim for message body integrity
  - Proposal: "msgi" claim, for new PASSporT type "msg"
    - Modeled after "rcdi", which provides a hash of "rcd" claim content
  - PASSporTs with this claim should be applicable to any OOB use of STIR messaging as well

What would take work

- Integration with non-SIP messaging systems
  - We could look at direct PASSporT integration with things like XMPP, for example
    - How much XMPP uses TNs, though…
  - Vast number of proprietary messaging systems out there
    - Maybe iMessage does well enough without STIR certs
    - Others might not
- Can we create a framework that is easy for non-SIP systems to leverage?
  - Any interaction with MLS worth exploring?

Next Steps

- Review
  - Do we need work in this space?
    - If so, where do we set the scope?
  - Seriously, would anyone use it (not just a question about people in this virtual room)?
- Adoption?