STIR for Messaging

IETF 112
STIR WG
Virtual – Nov 2021
J Peterson
• A 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
    • For the moment, that’s a scope restriction of the draft
• 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
Integrity over messaging

• Two paths for STIR:
  1. SDP-negotiated message stream security
     • Aiming for RCS-like (or RTT-like) deployments
  2. Individual message (MESSAGE) security
     • Protects individual messages at the MIME level
       – Avoid worrying about SMPP or whatever
       – Useful for some emergency services applications
       – Still some doubts about whether this is too pat an answer
         » At this point, I think it’s worth putting out there and seeing how things are used
What Else is New

• Added some more security/privacy considerations
  – Fortunately a lot we can borrow from other specs

• Added some text on messaging conferencing
  – Basically says multiparty should work for MESSAGE, but MSRP would require connected-identity
    • Propose kicking any related stuff to there

• Added some text on CPIM
  – Ben on the list: CPIM for metadata still an area we need input from implementers

• Cut out some TBDs, did some general wordsmithing
Open Issues

• Freshness
  – Ben on list: do we need a longer freshness window?
    • Question about store-and-forward, and what counts as a message “delivered” within the PASSporT freshness window (as opposed to read)

• Conferencing
  – People cool with basically punting it?
  – Seems like having some basic tools out there for implementers to play with is better than waiting on solving that
Next Steps

• Had some review, more welcome

• Close to WGLC here? Need more eyeballs