STIR for MLS (and MIMI?)

IETF 117 (Bay Area)

STIR WG

Jon
STIR for (Secure) Messaging

• We recently did a draft about the application of STIR to messaging, especially messaging sessions including RCS – now with IESG

• Recent talk about integrating Message Layer Security (MLS, RFC9420) into RCS has made for a potentially interesting interaction here
  • MLS is also in play in the work in MIMI
  • Lots of messaging still uses telephone numbers as identifiers

• What would MLS integration look like for STIR?
  • Short answer: the same “mky” PASSporT element could carry a hash over the public key of the MLS credential
    • MLS also has a hook to point to a certificate (potentially an RFC8226 cert)
    • Maybe some more glue (SIPBRANDY style) is required here
    • Some potential work on certificate expiry and synchronization will need to be done as well

• Draft forthcoming, unless anyone thinks this is a terrible idea