# STIR for MLS

IETF 119 (Brisbane)

STIR WG

Jon

# STIR for (Secure) Messaging

- -01 draft by myself and Richard Barnes
  - Sort of a sequel to a recently-advanced draft about the application of STIR to messaging (now RFC9475), especially messaging sessions (including RCS )
- 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
  - Be nice if MLS had a story for telephone number identifiers
- Our -01 draft specifies two (and a half) approaches

# Approach 1: Certs

- Define an MLS Credential Type for RFC8226 certificates
  - MLS already has a credential type for X.509, so this new Type is specific to X.509 certs with the TNAuthList extension
- Note that this could work for either TNAuthLists with SPCs or TNs – including individual TNs
  - Note however that with SPC certs, they don't communicate any specific TN
    - Basically, it would be up to the application using MLS to communicate the identifier of a group member
      - The assurance to groups would be "carrier A asserts the user's TN"
  - With individual TNs, say via delegate certs, this would have similar properties to SIPBRANDY
    - This is probably the most secure mode overall for integration
- Properties of SPC vs. TNs certs are fairly different – but not so different that we propose them as different MLS Credential Types

# Approach 2: PASSporTs

- Define an MLS Credential Type for PASSporTs (RFC8225)
  - PASSporTs makes it explicit which identifier to use for a group member – the “orig” value of the PASSporT
    - Also, we can RCD etc to provide additional information about the group member for the application using MLS
  - The “mky” PASSporT claim can carry a hash over a public key used for MLS
    - Note however that if the PASSporT is signed by an SPC cert, the security association is with the SPC-cert holder (e.g. carrier), not the end user device as such
- PASSporT expiry would need to be handled carefully – message sessions can be long-lived

# Relationship to mimi-identity

- Some preliminary work has been done in the MIMI group on how identity should be asserted
  - Currently description is good for Service Specific Identifiers, but the present doc may help with how TNs might be asserted as identities in MIMI
- More coordination and integration to be done in all this
- Also relates to the discovery problem in MIMI
  - Broadly, why we should trust that a given messaging provider is an appropriate route for messages to a telephone number
  - Interested people could look at my draft-peterson-mimi-idprover
    - Does some ACME integration for proof-of-possession of telephone numbers

# Next steps

- Obviously there’s plenty to flesh out here
  - Probably much will hinge on what MLS integration for RCS ends up looking like
  - More work to be done in MIMI
- Perhaps too early for adoption still