STIR for MLS

IETF 118 (Czechia)

STIR WG

Jon

STIR for (Secure) Messaging

- New -00 draft by myself and Richard Barnes
  - Sort of a sequel to a recently-advanced draft about the application of STIR to messaging, 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 -00 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, this 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

Next steps

- Current thinking: advance both approaches
  - They may be valid in different applications/situations
  - Anyone think differently?
- If people think this is a good direction, then, adoption?
  - (Any coordination with MLS WG?)
- Obviously there’s plenty to flesh out here
  - Probably much will hinge on what MLS integration for RCS ends up looking like