MIMI Content Format

draft-ietf-mimi-content-04

Rohan Mahy — rohan.ietf@gmail.com
IETF120, 19-June–2024
What’s new in -04? (and -03)

• Now using concrete CBOR syntax (complete with CDDL schema)

• All examples are CBOR instance documents which validate to the CDDL schema.
  • All examples are in the GitHub repo:
    • https://github.com/ietf-wg-mimi/draft-ietf-mimi-content

• Added a hash of the content to the ExternalContent array (in -03)
Summary of open issues

• Some CBOR encoding options - largely looking for CBOR community input
  • NestedPart has a double-wrapped array which could be replaced with an embedded CBOR sequence #18
  • The implied Timestamp could use CBOR time tags - maybe we move this to the MIMI protocol
  • To tag URIs or not. Currently we do
• Subject field (#7) - propose we close this (can be handled in the extensions map)
• Matrix extensible events (#5) - propose we close. Not longer seems relevant.
• Also need to confirm some changes from -01 version
Concern about an implicit message ID

• Content format currently uses a message ID calculated from the hash of the cipher text and timestamp chosen by the encrypting client

• For abuse prevention and (consensual) history sharing the party looking at a decrypted message may not have the ciphertext

• Old solution
  • client chooses a UUID
  • expose a (possibly encrypted for the hub) copy of the message ID in the MLS Additional Authenticated Data field (AAD)
  • clients are primarily responsible for detecting duplicate messages IDs among messages they have received
  • hub provider can reject a message with a duplicate message ID, but is not required to.
    • owning provider can check if user part duplicates prior messages it has a record for; 100% elimination of duplicate messages is not possible in high availability architecture.
  • Would allow the message ID to also be franked when franking messages