MIMI Content Format

draft-ietf-mimi-content-04

Rohan Mahy — rohan.ietf@gmail.com

IETF121, 7-Nov–2024

Summary of open issues

- Get rid of lastSeen if Hub timestamp reaches fanned-out clients? (#27)
- More guidance on message delivery statuses (#26)
- Can the topicId be updated in an Edit? (#25)
- Can non-sender edit/delete a message? (#24)
- Add more specific guidance on GitHub Flavored Markdown (#23)
- Support relative expiration times (#22)
- 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 - propose to make optional (#13)
  - To tag URIs or not. Currently we do. Suggest we remove (#12)

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

What’s next?

- Let’s get some more implementation feedback!
  - Thanks Marvin and Timo!

- I plan to make another version before the next MIMI interim