Some more MLS Extensions

Rohan Mahy — rohan@wire.com

IETF 118, 08-Nov-2023

SelfRemove proposal in MLS Extensions

- Open Issue: User still cannot ensure that removing oneself is atomic
  - Option 1: User's client sends a commit with Remove proposals for other clients, then sends a SelfRemove Proposal. Takes 2 epochs to remove, with one client present
  - Option 2: User's client sends Remove proposals for other clients and SelfRemove proposal at the same time. External Commit still is obliged to ignore the Remove proposals.
- Solutions:
  - Option A: Add list of other client indexes to delete (must be clients of the same user) to the SelfRemove
  - Option B: Change the behavior of External Commit in presence of SelfRemove to commit valid Remove proposals. Makes the extension no longer a safe extension?

draft-mahy-mls-kp-context

- KeyPackage extension which restricts the use of the KeyPackage to a specific context
  - Only use this KeyPackage to join a specific MLS group
  - This KeyPackage is only meant to be used if the Adder has the following “user” identity
  - This KeyPackage is only meant to be used if the Adder is in the following domain
  - This KeyPackage is only meant to be used if the Adder has the following public key
- Might add
  - Only use this KeyPackage to join a specific “room”
- Any other contexts we might be missing?
- Next steps? Add to extensions draft?

Extensions for MIMI

- MIMI is currently planning to have room state shared as GroupContextExtension to get **group agreement**.
- This consists of a **room policy document**
  - Ex: This room is a members-only room. You have to have the “admin” role to add and remove users
- And a **participation list** which is maintained by each client
  - Ex: Alice is an admin, Bob is a regular participant
- The participation list is updated (patched?) via a new proposal type which does not require an *UpdatePath*

- What do we need in MLS?
  - Safe extension for this ParticipationList proposal (or possibly a hash)
- The actual policy will likely be defined in MIMI.

draft-mahy-mls-x25519kyber768draft00

- NIST announced the ML-KEM standard based on Kyber.
- Need to update to reference ML-KEM.
- Will ask to adopt as WG item after recharter

draft-mahy-mls-group-anchors

- FYI: I am abandoning this draft / idea
- We are using a combination of existing tools to get similar functionality
  - X.509 NameConstraints extension (domain in the URI must match)
  - RFC 5914 Trust Anchor Format
- Did anyone else care about this?