Lots of Proposed MLS Extensions

draft-mahy-mls-x25519kyber768draft00-00
draft-mahy-mls-selfremove-00
draft-mahy-mls-room-policy-ext-00
…

Rohan Mahy — rohan@wire.com

IETF 117, 27-July-2023

draft-mahy-mls-x25519kyber768draft00

- A ciphersuite using an already defined, *already IANA registered* HPKE KEM (0x0031).
  It's a Hybrid post-quantum/traditional (PQ/T) KEM: X25519 + Kyber768
- Protects from "**Harvest Now, Encrypt Later**" attack.
- Its fast, but its big (1216 bytes vs 32 bytes per public key). KEM performance roughly 2.5x slower than X25519 alone.
- Super straightforward to plug into MLS
- Implemented now.
- Next steps?

- Not the last PQ ciphersuite approach. Also coming:
  - Kyber is not yet standardized
  - PQ-only vs. Hybrid KEMs
  - Hybrid mixing vs. concatenation
  - PQ Signatures and PQ/T Signatures
  - More efficient PQ approaches which require MLS extensions

draft-mahy-mls-selfremove

- Adds SelfRemove proposal type.
- What problem does this solve? In groups with lots of joins and removes, it is hard to leave. External commits invalidate Remove proposals, so client might have to wait an undefined amount of time (often several epochs) to leave. Has access to the group keying material for this entire time.
- How is this different from the Remove proposal?
  - External Committers are required to include pending SelfRemove proposals. Remove proposals are not valid inside External Commit
  - Because it is only sent by client removing itself, SelfRemove omits the leaf index. (Uses the `Sender.leaf_index`)
  - Client sending an external commit skips validating the `membership_tag`.
- Status: all issues raised on the list addressed in editor's copy: https://github.com/rohan-wire/ietf-drafts/blob/main/mahy-mls-selfremove/draft-mahy-mls-selfremove.md
- Next steps? Add to extensions draft? Standalone draft?

Extensions for MIMI?

- FYI: MIMI is likely to define some policy document that should go into a GroupContext extension
- Allows the MIMI room policy to benefit from **MLS group agreement**.
- Example: draft-mahy-mls-room-policy-ext-00
  describes how you would do this.
- Probably need to define a room policy extension container. The actual policy will likely be defined in MIMI.
- Next steps? Wait for MIMI or Define generic policy container.

draft-mahy-mls-group-anchors

- 75% of comments in Japan were complaining that you could use this extension to do something (download new trust roots) the draft explicitly says not to do.
- other comments suggested using
- just says that if you have identity domain foo, use root certificate bar (of the certificates you already have) for that domain
- please actually read the draft (it is very short) and comment.
- interest in solving this problem?