Targeted messages

draft-mls-ietf-targeted-messages

IETF 125 – Shenzhen / Remote
MLS WG Meeting
Raphael Robert

Progress update

- Separate draft (was part mls-extensions before)
- A few inconsistencies between this draft and RFC9420 have been ironed out
- No changes in functionality
- Implementation with test vectors underway

Scope

- One shot mechanism to encrypt an authenticated message from one member of a group to another, using HPKE
- Authenticated by the sending member’s signature key
- Also authenticated by PSK injection of an exported secret from the MLS exporter

Open questions 1/3

Do we want to allow external senders?

Since external senders are already defined in RFC9420, and all we need from the sender is a signature key, this should be straightforward.

Open questions 2/3

How do we compose this with APQMLS?

Two options:

- We ignore it and only use the classic group. We get weak PQ confidentiality guarantees through the PSK injection.
- We define a combined cipher suite for HPKE from the two individual group cipher suites and use that.
- Secret third option: We wrap one targeted message inside another one.

Open questions 3/3

Do we want a simple ratchet for efficiency?

We could add a simple one-way hash ratchet that follows a targeted message and encrypts subsequent messages.

Caveat:

- We only get FS when the receiver has updated its leaf node.
- Let’s not reinvent the double ratchet here and now.