Decentralized MLS

IETF 124
MLS WG Meeting
Konrad Kohbrok

Quick recap

- Based on the Fork Resilient CGKA paper by Joël Alwen, Marta Mularczyk and Yiannis Tselekounis
- Significantly improves forward secrecy in MLS deployments that allow clients to retain old group states
- Useful when commits may arrive out-of-order and may thus be conflicting
- Relatively simple modification of vanilla MLS, some storage overhead

Use cases

- Large groups (retains MLS's efficiency)
- Environments with relatively low fork probability or DS-assisted ways to know when or when not to retain old group states
- Example: Federated environments where forks occur due to disconnects between individual servers

Changelog

- Simplified draft