MLS Extensions & Federation

IETF116, Yokohama
Raphael Robert

Federation

- Stable: new version uploaded, still waiting for MIMI to better position it

Extensions

- More IANA registries in -protocol (wire formats, labels: signatures, public key encryption, exporter)
- Content Advertisement extension (Rohan)
- Group anchors draft (Rohan)
- Safe Extensions (Joël)

Safe Extensions

- Clarify terminology: what is a “Safe Extension”?
- What is the purpose of the Safe Extensions API?
  - Safe Extensions cannot harm core security properties of MLS
  - Safe Extensions cannot interfere with each other

Examples of Safe Extensions

- RBAC for MLS session
- Cryptographic agreement on application data
- Safely exposing some keys (e.g. signatures, leaf HPKE) for use by external applications. e.g. Targeted messages.
- PQ with flexible classic/PQ overhead trade-off
- Application triggered custom event injection into MLS session
- Alternative (e.g. more deniable/anonymous) application message formats