MLS Extensions

Raphael Robert
IETF117 San Franscisco

Agenda for the document

- Include general guidance on the use and design of new extensions
- Include a concrete API that extensions can use to interface with MLS proper without breaking security guarantees
- Include examples that show how the API can be used

Extensions in the Document

- AppAck
- Targeted Messages
- Content advertisement

Safe API for Extensions

- Secure re-use of key material, e.g., signing leaf signature public key using a new label and the extension type
- Injection of key material
  - New PSK type specific for use by extensions, where the PreSharedKeyID includes the extension_type
- Exporting extension-specific secrets
  - From the epoch_secret (at the beginning of an Epoch for FS)
  - From a newly defined extension_secret (during the Epoch)

Guidance for Extension Design

- Guidance on how to use the AAD in regular MLS messages
- Inclusion of proposals: Validation logic designers have to define (inclusion of path, use with an external commit)

Planned Extensions

- Deniable mode for MLS groups
- MIMI-related extensions
- RBAC extension
- Application messages from external senders
- Encrypted group context extensions
- Post-Quantum optimized mode
- Unsigned application messages
- Last resort KeyPackage extension
- … and more