MLS Extensions

IETF 118 Prague

Raphael Robert, Konrad Kohbrok, Joël Alwen, Marta Mularczyk

Recent additions to the document

- Last resort KeyPackage extension
- SelfRemove proposal
- Safe Extensions API
- New IANA registry entries for use by extensions

Last Resort KeyPackage Extension

- KeyPackage extension without any data
- Marks KeyPackages for use in cases of last resort
- Visible to DS, as well as group members
- Authenticated through signature on the KeyPackage

SelfRemove Proposal

- GroupContext Extension that allows use of the SelfRemove proposal
- SelfRemove proposal proposes the removal of the sender
- Can be committed as part of an External Commit

Safe Extension threat model

- Assumption: Folks start writing MLS extensions
- 3 actors: MLS protocol spec authors, MLS extension authors, application developers
- Scenario: application developer wants to use MLS with extensions A & B
- Questions:
  - Do extensions A & B break security guarantees of the vanilla MLS protocol?
  - Does extensions A & B break each others' security guarantees?

Safe Extension API

- Interface through which extensions can interact with the main MLS protocol
- Extensions interacting with MLS only via the safe extensions API are called safe extensions
- Safe extensions don’t break MLS security guarantees
- Safe extensions don’t break security guarantees of one-another
- Targeted messages changed to use safe extensions

Safe Extension API (cont'd)

- Safe extensions can use
  - public key material from the main protocol (HPKE/signatures)
  - export secrets
  - inject PSKs
- Safety enforced through domain separation by extension ID
- Next step: access control on group context extensions
  - GroupContext Extensions (i.e. their proposals) can modify only their own extension data
  - Might remove the need for a GroupContextExtension proposal

New IANA registry entries for extensions

- There are now IANA entries for extension specific
  - Credentials
  - Proposals (multiple variants)
  - WireFormats
- Each entry contains an extension ID field and a data field
- Extension authors only have to register an extension code point and can then use any of the above structs

Next steps

- Continue the work on Safe Extensions: better separation, address feedback
- More extensions:
    - User Trees
    - New stab at deniability (depends on User Trees)
    - MIMI related extensions
    - Encrypted group context extensions
    - Post-Quantum optimized mode
    - Application messages from external senders