MLS goals & roadmap

Timeline through IETF 109

- Two more interims (Oct 6 & Oct 20)
  - Option to schedule more (Oct 27, Nov 3, Nov 10)
- By end of October:
  - Complete current outstanding issues / PRs
  - Issue draft-10
- Early November: Issue Last Call #1
- IETF 109 (Nov 16-20)
  - Discuss any feedback received during LC #1
  - Issue draft-11 if required to address feedback

Post-IETF109

- Issue draft-11 if needed to address feedback from LC#1
- “Feature freeze” for implementation and analysis
  - Length TBD
  - Higher bar for breaking changes (see next slide)
- Goals for implementation & analysis period:
  - Multiple implementations with verified interop
  - Multiple security analyses
- Issue Last Call #2 after this phase

Rules for implementation & analysis phase

- Non-breaking changes can still be done
  - Editorial changes
  - Functional changes that clients do locally and that don’t affect the protocol, e.g. improve entropy locally
  - Define new extensions that don’t affect the core protocol
- Breaking changes are only accepted under the following conditions
  - Academic research reveals security flaws, especially when current security guarantees cannot be kept
  - Implementation issues: when the current draft cannot be implemented at all or incurs unreasonable engineering costs