IETF 117

Messaging Security Layer

27 July 2023

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

Note Well

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

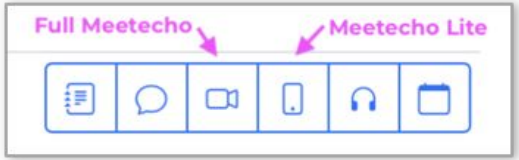
Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

IETF 117 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Session Details

Agenda:
https://datatracker.ietf.org/doc/agenda-117-mls/

Notes:
https://notes.ietf.org/notes-ietf-117-mls

WG Chairs: Nick Sullivan & Sean Turner

Agenda

Administrivia - 5min

Additional MLS Credentials: Richard Barnes - 10min
https://datatracker.ietf.org/doc/draft-barnes-mls-addl-creds/

MLS Ciphersuite using X25519Kyber768Draft00 KEM: Rohan Mahy - 10min
https://datatracker.ietf.org/doc/draft-mahy-mls-x25519kyber768draft00/

The SelfRemove Proposal for MLS: Rohan Mahy - 10min
https://datatracker.ietf.org/doc/draft-mahy-mls-selfremove/

Research results on security tradeoffs: Britta Hale - 10min

Safe Extensions / Deniability / Last Resort Extension: Raphael Robert - 10min

MIMI Interactions: Chairs / All - 5min