17 March 2026

LAMPS WG @ IETF 125

This session is being recorded

Internet Engineering Task Force
© 2026 IETF Trust
Production by Meetecho

Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit **www.ietf.org/note-well** or use the QR code below

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see **RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy**). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in **RFC 7776: IETF Anti-Harassment Procedures**.
- If you are aware that any IETF contribution (as defined in **RFC 5378: Rights Contributors Provide to the IETF Trust**) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see **RFC 8179: Intellectual Property Rights in IETF Technology**).
- For detailed process information consult **RFC 2026: Internet Standards Process** and *RFC 2418:* **IETF Working Group Guidelines and Procedures** and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the **IETF Privacy Statement**.

For advice, please talk to Working Group chairs or Area Directors.

I E T F

This session is being recorded

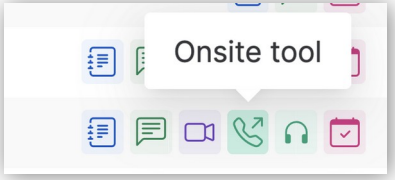
IETF 125 Meeting Tips

In-person participants

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to join the queue, show hands
- *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.



All participants

- State your name each time you begin speaking in the queue

Resources for IETF 125

- Agenda & Slides:
  - https://datatracker.ietf.org/meeting/125/session/lamps/

- Notepad:
  - https://notes.ietf.org/notes-ietf-125-lamps

- Zulip Room:
  - https://zulip.ietf.org/#narrow/stream/lamps

- Meetecho
  - Full Client: https://meetings.conf.meetecho.com/ietf125/?session=35082
  - Onsite Client: https://meetings.conf.meetecho.com/onsite125/?session=35082

Agenda (1 of 3)

0) Minute Taker, Jabber Scribe, Bluesheets

1) Agenda Bash

2) Recently Published RFCs
   a) draft-ietf-lamps-dilithium-certificates (RFC 9881)
   b) draft-ietf-lamps-cms-ml-dsa (RFC 9882)
   c) draft-ietf-lamps-x509-slhdsa (RFC 9909)

3) RFC Editor
   a) draft-ietf-lamps-rfc5019bis
   b) draft-ietf-lamps-rfc7030-csrattrs
   c) draft-ietf-lamps-kyber-certificates
   d) draft-ietf-lamps-x509-alg-none
   e) draft-ietf-lamps-cms-kyber
   f) draft-ietf-lamps-pkcs8-prikeyinfo-contenttypes
   g) draft-ietf-lamps-rfc{5272,5273,5274}bis

IETF

Agenda (2 of 3)

4) With IESG
   a) draft-ietf-lamps-pq-composite-sigs
   b) draft-ietf-lamps-cms-composite-sigs
   c) draft-ietf-lamps-keyusage-crl-validation
   d) draft-ietf-lamps-macaddress-on

5) Active Documents
   a) draft-ietf-lamps-csr-attestation (Mike)
   b) draft-ietf-lamps-attestation-freshness (Hannes, Hendrik)
   c) draft-ietf-lamps-certdiscovery (Corey)
   d) draft-ietf-lamps-caa-security (Henry)
   e) draft-ietf-lamps-pq-composite-kem (Mike, John)
   f) draft-ietf-lamps-cms-composite-kem (Daniel)
   g) draft-ietf-lamps-cms-euf-cma-signeddata (Daniel, Falko)

IETF

Agenda (3 of 3)

6) Under consideration for adoption
   a) draft-jpfiset-lamps-attestationkey-eku (J.-P., Mike, Hannes)
   b) draft-santesson-one-signature-certs (Stefan) [ADOPTION CALL]
   c) draft-smyslov-lamps-frodokem-certificates (Valery)
   d) draft-chen-lamps-cms-frodokem (Meiling)

7) Wrap up

IETF