



16 March 2026

# LAKE @ IETF 125

This session is being recorded

# 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](http://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.

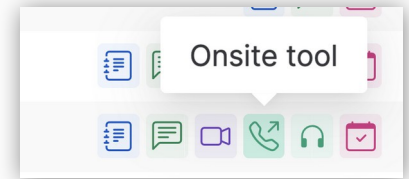


This session is being recorded

# 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 mic queue
  - participate in shows of 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.

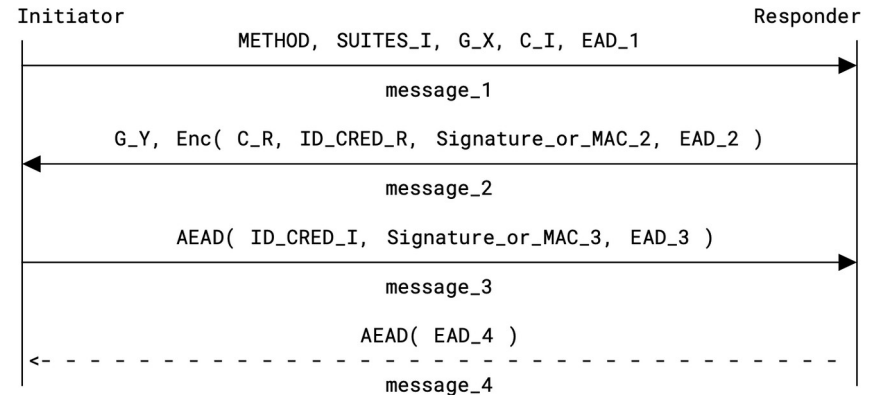


# Resources for IETF 125

- Agenda  
<https://datatracker.ietf.org/doc/agenda-125-lake/>
- Meetecho for remote participation:  
<https://meetings.conf.meetecho.com/ietf125/?session=35188>
- Minutes:  
<https://notes.ietf.org/notes-ietf-125-lake>

# Recap: EDHOC ([RFC 9528](https://www.ietf.org/rfc/rfc9528.html))

- Lightweight Authenticated Key Exchange protocol over COSE
  - RFC 9528 and RFC 9529
- Targets constrained IoT use-cases
  - BLE, 6TiSCH, IEEE 802.15.4, LoRaWAN
- Developed in sync with the formal methods community
- Deployed, see e.g. [1]
- More info, implementations, formal analysis pointers, etc. available at [lakeswg.org](https://lakeswg.org)
- Current work: rekeying, remote attestation, 3<sup>rd</sup> party authorization, implementation considerations, extensions, ...



[1] <https://www.ietf.org/blog/edhoc/>



# Status

- 6/6 active adopted documents got recent updates for this IETF
  - Today: 5 Presented, Formal analysis presentations for 2 of them
- 4 individual drafts will be discussed at this meeting
- Re-chartering : Done (thanks Paul!)
  - <https://datatracker.ietf.org/doc/charter-ietf-lake/>
  - Allow new EDHOC methods including quantum-resistant ones
  - Maintenance, new cipher suites, including work on reducing transport overhead
- GREASE document not in the agenda
  - Hackathon report: <https://github.com/lake-wg/grease/issues/5>
  - Start WGLC?



# LAKE Agenda

- Administrivia -- chairs, 5 mins
- Formal analysis of [draft-ietf-lake-edhoc-psk-06](#)
  - Dhekra Mahmoud, 20 minutes
- [draft-ietf-lake-edhoc-psk-07](#)
  - Elsa Lopez Perez, 5 minutes
- Formal analysis of [draft-ietf-lake-ra-03](#)
  - Elsa Lopez Perez, 15 minutes
- From formal analysis of attested TLS to attested EDHOC
  - Muhammad Usama Sardar, 5 minutes
- [draft-ietf-lake-ra-04](#) -- Yuxuan Song, 10 minutes
- [draft-ietf-lake-authz-07](#)
  - Geovane Fedrecheski, 15 minutes
- [draft-ietf-lake-edhoc-impl-cons-06](#)
  - Marco Tiloca, 10 minutes
- [draft-ietf-lake-app-profiles-04](#)
  - Marco Tiloca, 15 minutes
- [draft-pocero-authkem-edhoc-02](#)
  - Lidia Pocero, 5 minutes
- [draft-pocero-authkem-ikr-edhoc-02](#)
  - Lidia Pocero, 5 minutes
- [draft-papon-lake-pq-edhoc-00](#)
  - Clement Papon, 10 minutes
- draft-chen-lake-edhoc-aka-?
  - Meiling Chen, 5 minutes (if time allows)
- AOB



# AOB?

Making the Internet work better

