LAKE @ IETF 114

27 July 2022



This session is being recorded

IETF 114 Philadelphia
hosted by

COMCAST
NBCUniversal

Internet Engineering Task Force
© 2022 IETF Trust
Production by Meetecho

IETF

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)

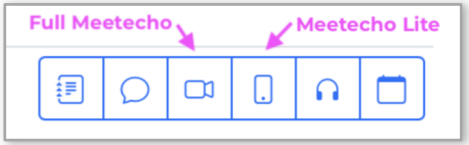
IETF

This session is being recorded

IETF 114 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*
- Wear masks unless actively speaking at the microphone.



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

LAKE Resources for IETF 114



- Agenda
  https://datatracker.ietf.org/doc/agenda-114-lake/
- Remote participation (Meetecho)
  https://meetings.conf.meetecho.com/ietf114/?group=lake&short=&item=1
- Notes
  https://notes.ietf.org/notes-ietf-114-lake
- Zulip
  https://zulip.ietf.org/#narrow/stream/lake



Agenda:

- Administrivia and agenda bash
  - chairs, 5 mins
- Computational analysis of EDHOC Sig-Sig
  - Marc Ilunga, 15 mins
- Computational analysis of EDHOC Stat-Stat
  - Baptiste Cottier, 15 mins
- draft-ietf-lake-edhoc-15 & draft-ietf-lake-traces-01
  - John Preuß Mattsson & Göran Selander, 15 mins
- Hackathon report
  - Marco Tiloca, 5 mins
- What else is needed before WGLC?
  - chairs, 5 mins
- AOB

Status:

- Formal analysis of the protocol is now done
  - Symbolic analysis of *all methods*
    - presented at IETF 113 by Charlie Jacomme
  - Computational analysis of *Method 0 (Signature-Signature)*
    - presentation today by Marc Ilunga
  - Computational analysis of *Method 3 (Static-Static)*
    - presentation today by Baptiste Cottier
- Implementation security
  - Completed hacspec implementation of edhoc-rs
  - Update planned for IETF 115
- Goal of the meeting: What else is needed before WGLC?

Keeping track of the different activities at: lakewg.org