TLS

TLS @ IETF115

WG Info: https://tlswg.org
Chairs: Joe Salowey, Sean Turner, Chris Wood

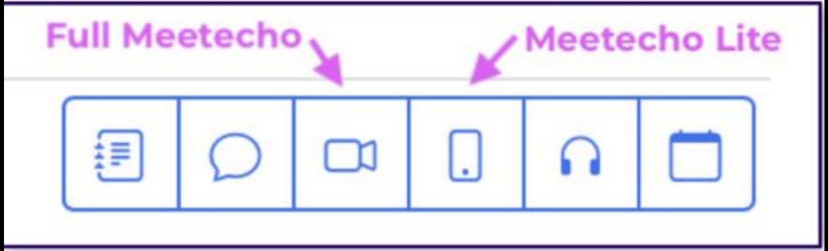
IETF 115 Meeting Tips

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.**



IETF Mask Policy

- Masks must be worn in meeting rooms and are recommended for common areas but not required.
- In meeting rooms, masks may briefly be removed for eating and drinking, but that cannot be an excuse to leave them off for long periods.
- In meeting rooms, active speakers, defined as those who are at the front of the room presenting or speaking in the mic queue, can remove their mask while speaking.
- No exemptions for mask wearing, medical or otherwise, will be allowed.
- Masks must be equivalent to N95/FFP2 or better, and free masks will be provided.

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 reminder:

- 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 Code Of Conduct Guidelines

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

Please keep these in mind both at the mic and on Jabber/Meetecho IM

Requests

Minute Taker(s)

Jabber Scribe(s)

Log into Onsite Tool (queue)

State your name

Keep it professional, respectful, and constructive

Agenda

10 min	Administrivia
100 min	Working Group Drafts

- 8446bis
- 8447bis
- Deprecating Obsolete Key Exchange Methods
- URI for publishing ECHConfigList

10 min	Individual Drafts

- SSLKEYLOGFILE

Document Status

Published

- **RFC 9257:** Guidance for External Pre-Shared Key (PSK) Usage in TLS
- **RFC 9258:** Importing External Pre-Shared Keys (PSKs) for TLS 1.3

RFC Editor Queue (AUTH48-DONE)

- Delegated Credentials

Paused (Waiting on Implementation):

- Cross SNI Resumption
- TLS Flags Extension

Waiting on Chairs:

- RRC for TLS 1.2 and 1.3

In Progress:

- Compact TLS (expired)
- RFC8446bis
- RFC8447bis
- Encrypted Client Hello
- Well-Known for ECHConfigList
- Hybrid KE in TLS 1.3
- SNIP

Stalled/Expired WG I-Ds

Batch Signing for TLS

Semi-Static Diffie-Hellman Key Establishment for TLS 1.3