

16 & 20 March 2026

IETF 125 TLS WG

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 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

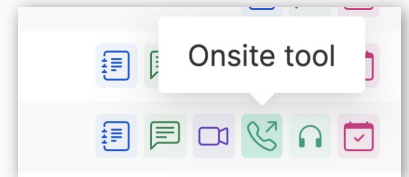
- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the "Meetecho lite") client to join the queue, show hands
- *Keep audio and video off if not using the onsite version.*

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



Monday Agenda

Administrivia: Chairs

- Agenda | NOTE WELL | Scribes (5min)
- Status (5min)

WG I-Ds:

- [draft-ietf-tls-mldsa](#): Tim (5min)
- [draft-ietf-tls-pake](#): Laura (15min)
- [draft-ietf-tls-mlkem](#): Deirdre (10min)

Non-WG I-D:

- [draft-sheffer-tls-pqc-continuity](#): Yaron (15min)

Requested but Withdrawn:

- [draft-yusef-tls-pqt-dual-certs](#)

Requested but Denied:

- [draft-wang-tls-hybrid-ecdh-scloud](#)
- [draft-reddy-tls-composite-mldsa](#)
- [RFC 9261 Clarifications](#)

Friday Agenda

WG I-Ds:

- [draft-ietf-tls-extended-key-update](#): (25min)
 [FATT Summary](#) - Thom
 [I-D](#) - Yaroslav

Non-WG I-Ds:

- [Beyond the 64K Limit in TLS 1.3 Handshake](#): Vallery (20min)
- [FATT Extensions](#): Usama (15min)
- ECH Measurements: Vinicius (15min) – no I-D
- [draft-sullivan-tls-signed-ech-updates](#): Nick (15min)
- [draft-rosomakho-tls-wimse-cert-hint](#): Yaroslav (15min)