

TLS WG Update



IETF 126 - 23 July 2026
TLS Chairs

Complaint/Appeals

-ML-KEM/-ML-DNA related

- 6/27 complaints from DJB to chairs
 - “jeopardy claim” - Denied
 - “charter complaint” - Denied
- There are others but they are handled by IESG, IAB, and ISOC Board.

WG Document Status

PUBLISHED RFCs!

<u>RFC 9846</u>	TLS 1.3
<u>RFC 9850</u>	SSLKEYLOG File
<u>RFC 9851</u>	TLS 1.2 is Frozen
<u>RFC 9954</u>	TLS Hybrid Design
<u>RFC 9963</u>	Legacy RSASSA-PKCS1-v1.5
<u>RFC 9973</u>	Certificates + PSK
<u>RFC 10015</u>	Deprecate Obsolete KEX

RFC Editor:

- [-ecdhe-mlkem](#)
- [-mldsa](#)*

WG Document Status

Ready for WGLC & FATT Review:

- -extended-key-update

Send/Sent to FATT:

- -pake

Implementation Experience Needed:

- -super-jumbo-record-limit
- -key-share-prediction
- -trust-anchor-ids
- -tlsflags
- -wkech

**Chairs and IETF determined
there was rough consensus to
change the values in the
Standards track
draft-ietf-tls-ecdhe-mlkem for
X25519MLKEM768 to
Recommended=Y.**

**Chairs determined there was
rough consensus to progress
draft-ietf-tls-mlkem -
Informational track all values
Recommended=N.**

List Behavior

Monologue

It's been bad, really bad; srsly, really bad.

The monthly reminders do not seem to have an effect.

Not doubt some of this is because the chairs.

Reminder: Moderator team is formed and is working on policies.

List Behavior

Show of Hands

1. Do you want the list to get more functional?
2. Should the chairs be more draconian in their dolling out of moderation actions?

What's off topic -> see Monthly Reminder

- Unsolicited bulk e-mail (from RFC 3683)
- Discussion of subjects unrelated to IETF policy, meetings, activities, or technical concerns (from RFC 3683)
- Unprofessional commentary, regardless of the general subject (from RFC 3683)
- Repetition of arguments without providing substantive new information
- Requesting an unreasonable amount of work to provide information
- Including derivative work notices (see [IESGStatement])

What's off topic -> Also ...

Excessive process deliberations

FATT

Monologue

It has been a bumpy road.

There is now more transparency;
see GH pages.

Some believe FATT discussions,
especially around the little “p”
process, are a distraction.

Chairs still believe the FATT review
is valuable.

Chairs want to smooth out some of
the bumps; see PR#24.

EATT

Show of Hands

1. Do you think FATT procedural discussions are a distraction?
 2. Do you think chairs should be the ones that determine whether a draft goes for the initial sniff test?
 3. Do you think authors and those performing the formal analysis should collaborate?
-