

TLS WG Update



IETF 125 - 16 March 2026
TLS Chairs

WG Complaint/Appeals

-ML-KEM

- Complaint was unsuccessful and I-D is still an adopted WG draft

Moderating Issue

- IESG upheld the moderation action as conformant with RFC 3934.
- Chairs kept DJB's moderation settings longer than 30 days. A message was moderated that should not have been.
 - Our Apologies - moderation extended for a few days because we did not click all the right mailman buttons initially

WG Doc Status

PUBLISHED RFCs!

RFC 9847: IANA Registry Updates for TLS and DTLS

RFC 9849: TLS Encrypted Client Hello

RFC 9848: Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings

RFC 9853: Return Routability Check for DTLS 1.2 and 1.3

WG Doc Status

RFC Editor:

- `-rfc8446bis`
- `-rfc8773bis`
- `-hybrid-design`
- `-tls12-frozen`
- `-keylog-file`
- `-tls13-pkcs1`
- `-deprecate-obsolete-kex`

WGLCs:

- `-super-jumbo-record-limit`
 - Completed - 2 implementations by the same person.
- `-ml-kem`
 - More on this later.

Implementation Experience Needed:

- `-key-share-prediction`
- `-tlsflags`
- `-wkech`

Breaking News...

(3rd Time) Prohibiting Key Reuse

RFC 8446 and RFC 8446bis do not forbid the reuse of ephemeral keys.

In RFC 8446bis, we added a SHOULD NOT in Appendix C.4.

We have a renewed push to Prohibit Key Reuse; see [thread](#) and [PR#1410](#).

Concern has been expressed about whether the change has any practical value - is a “feel-good change” - implementation do and will continue to do this.

We will begin another consensus call to address this point for RFC 8446bis.

NOTE: If you already responded to the thread no need repeat yourself.

Liaison Statement from IEEE 802.11

[IEEE Liaison Statement Page](#) (will be posted): GIST of it:

The IEEE 802.11 Working Group would like to express support for publication of draft-ietf-tls-mlkem as an RFC with its definition of key establishment options that use pure ML-KEM.

We would further request that the IETF look at updating EAP-TLS once draft-ietf-tls-mlkem is published as this is one of the mechanisms that IEEE P802.11bt will use.

ML-KEM I-D WGLC Summary

We are working through issues brought up during the working group last call. We do not believe we have consensus without resolving the following points:

- Key Reuse
- Text for preferring Hybrids
- Whether to include motivations (see Liaison Statement)

We expect resolving these issues will take a few weeks after which we will run a targeted consensus call to see if text changes are acceptable to the working group.

Stay tuned ...