

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`