

# TLS WG Status



TLS @ IETF 123  
Deirdre Connolly, Joe Salowey, & **Sean Turner**

**20 (active) WG I-Ds**

# **5 (expired) WG I-Ds**

**DTLS 1.3 (bis)**

**Abridged Compression for WebPKI Certificates**

**Compact TLS 1.3**

**Secure Negotiation of Incompatible Protocols in TLS**

**TLS Resumption across Server Names**

# 6 with RFC Editor

TLS is in Feature Freeze

The SSLKEYLOGFILE Format for TLS

TLS Encrypted Client Hello

Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings

IANA Registry Updates for TLS and DTLS

Return Routability Check for DTLS 1.2 & 1.3

## **2 Approved by IESG**

TLS 1.3 (bis)

Deprecating Obsolete Key Exchange Methods for (D)TLS 1.2

# 1 through IETF LC (with AD)

Hybrid Key Exchange in TLS 1.3

# 1 in IETF LC

TLS 1.3 Extension for Using Certificates with an External Pre-Shared Key

## 2 ready for WGLC

Legacy RSASSA-PKCS1-v1\_5 codepoints for TLS 1.3

A well-known URI for publishing service parameters

**We will start these ASAP.**

# EATT Review

Skipped (see messages to list: [here](#) and [here](#)):

- Legacy RSASSA-PKCS1-v1\_5 codepoints for TLS 1.3
- Large Record Sizes for TLS and DTLS with Reduced Overhead

In process:

- Extended Key Update for Transport Layer Security (TLS) 1.3

Queued:

- DTLS 1.3 (bis)

# WG Adoption Calls

Active:

- SLH-DSA in TLS 1.3\*

Queued:

- Use of Composite ML-DSA in TLS 1.3\*
  - A PAKE Extension for TLS 1.3
  - mTLS Flag\*
-

# PQ Algorithms

Plan was to do 5 adoption calls!

Things change ̄\\_(\ツ)\\_/

Adopted:

- Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3
- ML-KEM PQ Key Agreement for TLSv1.3\*
- Use of ML-DSA in TLS 1.3

Ongoing:

- SLH-DSA in TLS 1.3\*

To Do — BUT taking a pause:

- Composite/Dual Signatures\*
  - New Key Share Extension for Classic McEliece Algorithms\*
-

# PQ Algorithms

Need consensus on these for each I-D

**\*NOT PICKING MTI\***

Timing:

Now (Hybrid + Pure ML-KEM)

Later (sigs)

Much later (dual certs/comp sigs)

Intended Status:

Informational or Standards

Recommended Column Value:

Y or N

Applicability Statement

Security Considerations

---