



TLS

TLS @ IETF114

WG Info: <https://tlsWG.org>

Chairs: [Joe Salowey](#), [Sean Turner](#), [Chris Wood](#)



NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (<https://www.ietf.org/contact/ombudsteam/>) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- <https://www.ietf.org/privacy-policy/> (Privacy Policy)



IETF Code Of Conduct Guidelines

1. Treat colleagues with respect
2. Speak slowly and limit the use of slang
3. Dispute ideas by using reasoned argument
4. Use best engineering judgment
5. Find the best solution for the whole Internet
6. Contribute to the ongoing work of the group and the IETF

Please keep these in mind both at the mic and on Jabber/Meetecho IM



Requests

Minute Taker(s)

Jabber Scribe(s)

Log into [Onsite Tool](#) (queue)

State your name

Keep it professional, respectful, and
constructive



Agenda

Wednesday Session I

05 min Administrivia

85 min Working Group Drafts

- [cTLS](#)
- [A well-known URI for publishing ECHConfigList values](#)
- [IANA Registry Updates for TLS and DTLS](#)
- [Deprecating Obsolete Key Exchange Methods in TLS](#)
- [A Flags Extension for TLS 1.3 - last outstanding PR](#)

30 min Individual Drafts & Presentations

- [Transport Layer Security \(TLS\) Extension: Validation Request](#)
- [Using Attestation in Transport Layer Security \(TLS\) and Datagram Transport Layer Security \(DTLS\)](#)
- [NIST PQC Announcement](#)



Document Status

Published

- RFC 9147: [DTLS 1.3](#)
- RFC 9149: [Ticket Requests](#)
- RFC 9261: [Exported Authenticators](#)

RFC Editor Queue (AUTH48-DONE)

- [External PSK Guidance](#)
- [Importing External PSKs](#)

Approved (AD Followup)

- [Delegated Credentials](#)

IETF Last Call

- None

Paused (Waiting on Implementation):

- [Cross SNI Resumption](#)
- [TLS Flags Extension](#)

In WGLC:

- [RRC for TLS 1.2 and 1.3](#)

In Progress:

- [Compact TLS](#)
- [RFC8446bis](#)
- [RFC8447bis](#)
- [Encrypted Client Hello](#)
- [Well-Known for ECHConfigList](#)
- [Hybrid KE in TLS 1.3](#)
- [SNIP](#)

Stalled/Expired WG I-Ds

[Batch Signing for TLS](#)

[Semi-Static Diffie-Hellman Key Establishment for TLS 1.3](#)