



TLS

TLS @ IETF112

WG Info: <https://tswg.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)

State your name

Keep it professional, respectful, and constructive



Agenda

Tuesday Session III

05 min Administrivia

40 min Working Group Drafts

- [Exported Authenticators](#)
- [TLS Flags](#)
- [DTLS 1.3](#)
- [RFC8446bis](#)
- [ECH Implementation Status Update](#)

75 min New Work

- [RFC8447bis](#)
- [PEM-ECH](#) and [well-known ECH URI](#)
- [The Pseudorandom Extension for cTLS](#)
- [Zero-Knowledge Proofs meet TLS](#)



Document Status

RFC Editor Queue

- [Ticket Requests \(!\)](#)
- [DTLS 1.3 \(!\)](#)
- [DTLS CID \(!\)](#)
- [Deprecate MD5+SHA-1](#)

Approved (revised I-D needed)

- [Exported Authenticators \(!\)](#)
- [Importing External PSKs \(!\)](#)

IETF Last Call

- [External PSK Guidance](#)

Publication Request (with AD):

- [Delegated Credentials](#)

Waiting for Write-Up / Revised I-D:

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

In WGLC:

- None

In Progress:

- [Encrypted Client Hello](#)
- [Compact TLS](#)
- [RFC8446bis](#)
- [Hybrid KE in TLS 1.3](#)
- [RRC for TLS 1.2 and 1.3](#)
- [SNIP](#)

(!) In current state for > 100 days