

IETF 98: TLS WG

Chairs: Joe Salowey & Sean Turner

Info: <https://datatracker.ietf.org/wg/tls/charter/>



NOTE WELL



The brief summary:

- This summary is only meant to point you in the right direction, and doesn't have all the nuances; see below for the details.
- By participating with the IETF, you agree to the follow IETF processes.
- If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.

You understand that meetings might be recorded and broadcast.

The details:

- For further information, talk to a chair, ask an Area Director, or review BCP 9 (on the Internet Standards Process), BCP 25 (on the Working Group processes), BCP 78 (on the IETF Trust), and BCP 79 (on Intellectual Property Rights in the IETF).

Requests

Minute Taker(s)

Jabber Scribe(s)

Sign Blue Sheets

Reminders:

- State your name @ mic for the scribes/minutes
- Keep it professional @ the mic



Photo courtesy of <http://burgerbeast.com>

Agenda

Administrivia (5 min)

Note Well

Blue Sheets

Scribes

30min

TLS1.3

30min

DTLS1.3

15min

A DANE Record and DNSSEC

Document Status (5 min)

Authentication Chain Extension for TLS

15min

Certificate Compression

15min

Delegated Credentials

15min

Disposition of additional drafts

Document Status

Adopted Since Last Meeting:

- [Example Handshake Traces for TLS 1.3](#)
- [Applying GREASE to TLS Extensibility](#)

With/Through IESG:

- [ECC CSs for TLS v1.2 & earlier](#)
- [RFC 5289 to PS](#)

Completed 2nd WGLC:

- [TLS 1.3](#)

Completed WGLC:

- [ECDHE_PSK w/ AES-GCM & AES-CCM CSs](#)

In-Progress:

- [A DANE Record and DNSSEC Authentication Chain Extension for TLS](#)
- [D/TLS IANA Registry Updates](#)

WG Adoption Call ongoing:

- [DTLS 1.3](#)

Patiently waiting:

- [Exported Authenticators in TLS](#)
- [Delegated Credentials](#)
- [TLS 1.2 Update for Long-term Support](#)
- [TLS Server Identity Pinning with Tickets](#)