

IETF 99: TLS WG

Chairs: Joe Salowey & Sean Turner

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



NOTE WELL



Photo courtesy of prague.eu

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 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



Agenda

Monday:

5min [Administrivia](#)

5min [Document Status](#)

15min [Exported Authenticators](#)

15min [Record Size Limit
Extension for TLS](#)

25min [SNI Encryption](#)

Wednesday:

5min [Administrivia](#)

20min [TLS1.3](#)

15min [A DANE Record and DNSSEC
Authentication Chain Extension for TLS](#)

45min [DTLS1.3](#)

25min [Impact on TLS1.3 on Network Ops](#)

25min [TLS Is Not For Obligatory
Interception, Luckily](#)

Document Status

RFC Editor's Queue:

- [ECC CSs for TLS v1.2 & earlier](#)

With/Through IESG:

- [ECDHE_PSK w/ AES-GCM & AES-CCM CSs](#)
- [RFC 5289 to PS](#)

Adopted Since Last Meeting:

- [DTLS 1.3](#)
- [Exported Authenticators for TLS](#)
- [TLS Certificate Compression](#)

Completing 2nd WGLC:

- [TLS 1.3](#)

Completed WGLC:

- [A DANE Record and DNSSEC Authentication Chain Extension for TLS](#)

In-Progress:

- [D/TLS IANA Registry Updates](#)
- [Example Handshake Traces for TLS 1.3](#)
- [Applying GREASE to TLS Extensibility](#)

Needs more work:

- [Delegated Credentials](#)

Patiently waiting:

- [TLS 1.2 Update for Long-term Support](#)