# TLS@IETF101

Chairs: Joe Salowey & Sean Turner

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

# 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 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)

# 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

10min Administrivia

5min Document Status (next)

10min Record Header Extension

2min ¿SRP in TLS?

30min TLS Vizability

- 10min draft
- 10min discussion
- 10min wrap-up

## Wednesday

10min Administrivia

5min TLS 1.3

25min DTLS 1.3

25min Connection ID

25min DNSSEC Chain Extension

15min Exported Authenticators

10min Certificate Compression

10min Encrypted SNI

10min Semi-Static D-H

10min PSK+Certificate Auth

# Document Status

RFC Editor's Queue:

1. TLS 1.3
2. ECC CSs for TLS v1.2 & earlier
3. ECDHE_PSK w/ AES-GCM & AES-CCM CSs

Cycling back to the WG:

4. A DANE Record and DNSSEC Authentication Chain Extension for TLS

On IESG telechat:

5. IANA Registry Updates for TLS and DTLS
6. Record Size Limit Extension for TLS

In-Progress:

7. Example Handshake Traces for TLS 1.3
8. DTLS 1.3
9. DTLS Connection ID
10. Delegated Credentials
11. SNI Encryption in TLS Through Tunneling
12. Applying GREASE to TLS Extensibility (expired)
13. Exported Authenticators for TLS
14. TLS Certificate Compression