IETF 100: TLS WG

Chairs: Joe Salowey & Sean Turner

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

NOTE WELL

©Bule Sky Studio/shutterstock

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

Agenda

10min	Administrivia
5min	Document Status (next)
40min	TLS1.3
30min	DTLS1.3
25min	Connection ID
10min	IANA Registry Updates for TLS and DTLS
10min	Exported Authenticators
10min	Extension for protecting (D)TLS handshakes against Denial of Service
10min	Application-Layer TLS

Document Status

RFC Editor's Queue (misref):

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

Addressing WGLC comments:

- A DANE Record and DNSSEC Authentication Chain Extension for TLS

Adopted since last meeting:

- Delegated Credentials
- SNI Encryption in TLS Through Tunneling
- Record Size Limit Extension for TLS

Awaiting Test Results but through 2 WGLCs:

- TLS 1.3

About to be in WGLC:

- (D)TLS IANA Registry Updates

In-Progress:

- DTLS 1.3
- Example Handshake Traces for TLS 1.3
- Applying GREASE to TLS Extensibility
- Exported Authenticators for TLS
- TLS Certificate Compression