TLS @ IETF111

WG Info: https://tlswg.org
Chairs: Joe Salowey, Sean Turner, Chris Wood

TLS

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)

Requests

Minute Taker(s)

Jabber Scribe(s)

Sign Blue Sheets (now automatic)

State your name

Keep it professional

Agenda

Wednesday Session I

05 min	Administrivia
15 min	cTLS
10 min	Hybrid Key Exchange
30 min	Encrypted Client Hello
15 min	Deprecating Obsolete Key Exchange Mechanisms in TLS
15 min	AUTH-KEM
15 min	Bootstrapped TLS Authentication
15 min	Secure Negotiation of Incompatible Protocols in TLS

Document Status

RFC 8996 - Deprecate TLS 1.0/1.1

RFC Editor Queue

- Ticket Requests
- DTLS 1.3
- DTLS CID

Approved (revised I-D needed)

- Exported Authenticators
- Importing External PSKs

Publication Request (with AD):

- External PSK Guidance

Waiting for Write-Up / Revised I-D (Sean):

- Delegated Credentials
- Deprecate MD5+SHA-1

In WGLC (end July 30th):

- TLS Flags Extension
- Cross SNI Resumption

In Progress:

- Encrypted Client Hello
- Compact TLS
- RFC8446bis
- Hybrid KE in TLS 1.3
- RRC for TLS 1.2 and 1.3