TLS@IETF106

WG Info: https://tlswg.org

Chairs: Joe Salowey, Sean Turner, Chris Wood

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

Agenda

Thursday Morning Session I

05 min	Administrivia
15 min	Importing External PSKs for TLS
05 min	Exported Authenticators
05 min	Delegated Credentials
25 min	Compact TLS 1.3
15 min	Semi-Static Diffie Hellman
15 min	Batch Signing in TLS
15 min	TLS 1.3 Extended Key Schedule
---------	Re-charter discussion

Agenda

Thursday Afternoon Session III

05 min	Administrivia
05 min	Well-known URIs for ESNI
10 min	Deprecating MD5+SHA1
40 min	Encrypted SNI

Document Status

RFC Editor Queue

- GREASE
- Issues and Requirements for SNI Encryption in TLS

IETF LC

- Cert+PSK for TLS 1.3

Publication Requested (waiting on AD):

- DTLS 1.3
- TLS Certificate Compression

AD Evaluation (waiting on AD):

- Deprecating TLS 1.0 and 1.1

Waiting for Write-Up (chairs):

- Exported Authenticators for TLS

WGLC: (just completed)

- Ticket Requests

In WGLC Soon:

- Delegated Credentials
- DTLS Connection ID

In Progress:

- ESNI for TLS
- External PSK Importers
- Deprecating MD5+SHA1
- TLS Flags Extension

Discussion Needed

Hybrid key exchange

RSASSA-PKCS1-v1_5 codepoints for TLS 1.3