TLS@IETF103

WG Info: https://datatracker.ietf.org/wg/tls/about/
Chairs: Chris Wood, Joe Salowey, and Sean Turner

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

State your name @ the mic

Keep it professional @ the mic

Be succinct @ the mic

Agenda

Monday - 1330-1550

TLS

10min	Administrivia
20min	DTLS 1.3
05min	Deprecating TLS 1.0 & 1.1
25min	ESNI in TLS
20min	Proposed charter text
10min	PSK + Certificates
10min	TLS Certificate Types: ETSI and IEEE certificates for V2V
10min	Universal PSK/PSK Importer
10min	Ticket Requests

Agenda

Wednesday - 1120-1220

05min	Administrivia
55min	DNSSEC Chain Extension

Document Status

Published:

- RFC 8422 - ECC CSs for TLS v1.2 & Earlier
- RFC 8442 - ECDHE_PSK with GCM/CCM CSs for (D)TLS v1.2
- RFC 8446 - TLS 1.3
- RFC 8447 - IANA Registry Updates for TLS and DTLS
- RFC 8449 - Record Size Limit Extension for TLS

RFC Editor Queue:

- Example Handshake Traces for TLS 1.3

Cycled back to the WG:

- A DANE Record and DNSSEC Authentication Chain Extension for TLS

Adopted:

- Deprecating TLS 1.0 and 1.1
- ESNI for TLS

WGLCed:

- Issues and Requirements for SNI Encryption in TLS

Soon in WGLC:

- Exported Authenticators for TLS
- DTLS Connection ID
- Applying GREASE to TLS Extensibility

In Progress:

- DTLS 1.3
- TLS Certificate Compression
- Delegated Credentials

TLS Designated Expert Assignments

Designated Experts:

1. Rich Salz
2. Nick Sullivan
3. Yoav Nir

tls-reg-review@ietf.org archives now public.

TLS Designated Expert Assignments

ExtensionType:	value: 26, extension: tls-lts,		recommended: N
	value: 29, extension: pwd_protect,		recommended: N
	value: 30, extension: pwd_clear,		recommended: N
	value: 31, extension: password_salt,		recommended: N
SupportedGroups:	value: 31, group: brainpoolP256r1,	DTLS: Y,	recommended: N
	value: 32, group: brainpoolP384r1,	DTLS: Y,	recommended: N
	value: 33, group: brainpoolP512r1,	DTLS: Y,	recommended: N
Exporter Labels:	value: EXPORTER-oneM2M-Bootstrap,	DTLS: Y,	recommended: N
	value: EXPORTER-oneM2M-Connection,	DTLS: Y,	recommended: N
	value: EXPORTER-oneM2M-ESCertKE,	DTLS: Y,	recommended: N
	value: EXPORTER-Token-Binding,	DTLS: Y,	recommended: Y