TLS@IETF105

WG Info: https://tlswg.org

Chairs: Chris Wood, Joe Salowey, 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

Tuesday 17:10-18:10 EDT
Afternoon Session III

05 min	Administrivia
10 min	Delegated Signing Keys (née Delegated Credentials)
10 min	Deprecating MD5 and SHA-1 signature hashes in TLS 1.2
10 min	A Flags Extension for TLS 1.3
10 min	Suppressing Intermediate Certificates in TLS
05 min	TLS 1.3 Impact on Network-Based Security

Agenda

Thursday 10:00-12:00 EDT
Morning Session I

05 min	Administrivia
10 min	DTLS 1.3
15 min	ESNI
10 min	Compact TLS
10 min	Hybrid Key Exchange
10 min	TLS Metadata for Load Balancers
10 min	HTTPSSVC service location and parameter specification via the DNS
05 min	Return Routability Check for DTLS 1.2 & 1.3

Document Status

AD Evaluation:

- Applying GREASE to TLS Extensibility

Waiting for Write-Up:

- Exported Authenticators for TLS

Publication Requested:

- Issues and Requirements for SNI Encryption in TLS
- TLS Certificate Compression
- Cert+PSK for TLS 1.3
- Deprecating TLS 1.0 and 1.1

Soon in WGLC:

- DTLS 1.3
- Delegated Credentials
- DTLS Connection ID
- Ticket Requests

In Progress:

- ESNI for TLS
- External PSK Importers

DE Assigned Values

draft-ietf-trans-rfc6962-bis extension type: transparency_info

draft-ietf-tls-dtls-connection-id extension type: connection_id

draft-ietf-tls-certificate-compression handshake type: compressed_certificate

draft-ietf-tls-dtls-connection-id content type: tls12_cid

draft-camwinget-tls-ts13-macciphersuites: TLS_SHA256_SHA256, TLS_SHA384_SHA384

draft-wang-tls-raw-public-key-with-ibc signature schemes: eccsi_sha256, iso_ibs1, iso_ibs2, iso_chinese_ibs

draft-bruckert-brainpool-for-tls13 cipher suites: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1

draft-smyshlyaev-tls12-gost-suites supported groups: GC256A, GC256B, GC256C, GC256D, GC512A, GC512B, GC512C

draft-smyshlyaev-tls12-gost-suites cipher suites: TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC, TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC, TLS_GOSTR341112_256_WITH_28147_CNT_IMIT
client certificate types: gost_sign256, gost_sign512