TLS@IETF109

Virtual Meeting Tips

https://www.ietf.org/how/meetings/109

This session is being recorded

- **Make sure your video is off.**
- **Mute your microphone unless you are speaking.**
- **Join the session:**
  - **Meetecho (a/v and chat): tls session**
  - **Audio (only): audio**
  - **Jabber (chat): tls@jabber.ietf.org**

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 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)

TLS@IETF109

November 17, 2020
Chairs: Joe Salowey, Chris Wood, Sean Turner

Agenda

Administrivia (10 min)

- Virtual Meeting Tips
- Note Well
- Virtual Bluesheet (automatic)
- Note Taker
- Jabber Scribe
- Status

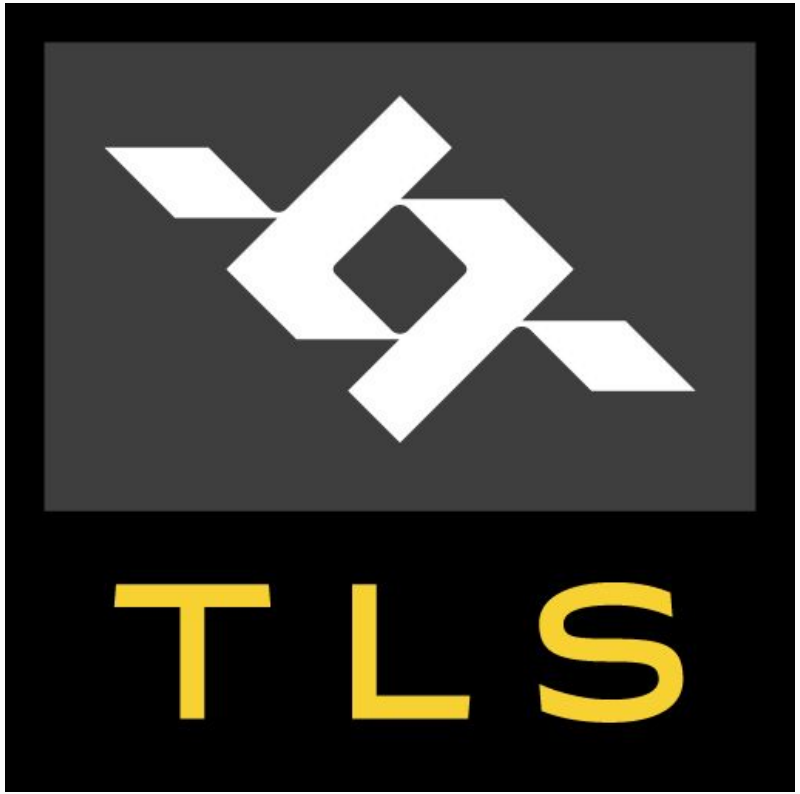
DTLS CID resolution (10 min)

- **Issue:** https://github.com/tlswg/dtls-conn-id/issues/76

ECH (30 min)

- **Draft:** https://datatracker.ietf.org/doc/draft-ietf-tls-esni/

Implementation Targets (10 min)



Status

Published:
- RFC 8744: Issues and Requirements for SNI Encryption in TLS

RFC Editor
- TLS Certificate Compression

Submitted to IESG: Revised I-D Needed
- Deprecating MD5 and SHA-1 signature hashes in TLS 1.2
- Importing External PSKs for TLS
- Exported Authenticators in TLS

IETF LC
- Deprecating TLSv1.0 and TLSv1.1

AD Evaluation: Revised I-D Needed
- The DTLS Protocol Version 1.3
- Connection Identifiers for DTLS 1.2
- TLS Ticket Requests

Active Drafts
- Batch Signing for TLS (expired)
- Compact TLS 1.3
- TLS Encrypted Client Hello
- Guidance for External PSK Usage in TLS
- Hybrid key exchange in TLS 1.3
- Semi-Static Diffie-Hellman Key Establishment for TLS 1.3 (expired)
- Delegated Credentials for TLS
- A Flags Extension for TLS

ECH (Encrypted Client Hello)

Implementation Targets

What is an Implementation Target?

An Internet-Draft that the WG feels is suitable for implementers to write code to, for the purposes of interoperability testing and gathering feedback.

An implementation target could also add or subtract some well-defined feature (likely based on a particular GitHub issue/pull request), e.g., draft-XX + PR#2.

When do we need one?

When there are multiple active implementations.

Before the Hackathon or other interop event.

Additional Points

Declaring an implementation version is not meant to freeze progress on the Internet-Draft.

A GitHub wiki (e.g., QUIC's) would be established to track what's in the implementation target.

Discussion

TLS@IETF109

November 17, 2020
Chairs: Joe Salowey, Chris Wood, Sean Turner