06 November 2023

IETF 118 Transport Layer Security

This session is being recorded

Internet Engineering Task Force

Production by Meetecho

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)

Note Really Well

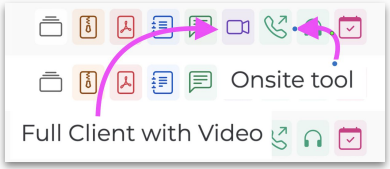
- IETF meetings, virtual meetings, and mailing lists are intended for professional collaboration and networking, as defined in the IETF Guidelines for Conduct (RFC 7154), the IETF Anti-Harassment Policy, and the IETF Anti-Harassment Procedures (RFC 7776). If you have any concerns about observed behavior, please talk to the Ombudsteam, who are available if you need confidentiality to raise concerns confident about harassment or other conduct in the IETF.
- The IETF strives to create and maintain an environment in which people of many different backgrounds and identities are treated with dignity, decency, and respect. Those who participate in the IETF are expected to behave according to professional standards and demonstrate appropriate workplace behavior.
- IETF participants must not engage in harassment while at IETF meetings, virtual meetings, social events, or on mailing lists. Harassment is unwelcome hostile or intimidating behavior—in particular, speech or behavior that is aggressive or intimidates.
- If you believe you have been harassed, notice that someone else is being harassed, or have any other concerns, you are encouraged to raise your concern in confidence with one of the Ombudspersons.

This session is being recorded

IETF 118 Meeting Tips

In-person participants

- Make sure to sign into the session using the Meetecho (usually the “Meetecho lite” client) from the Datatracker agenda
- Use Meetecho to join the mic queue
- *Keep audio and video off if not using the onsite version*



Remote participants

- Make sure your audio and video are off unless you are chairing or presenting during a session
- Use of a headset is strongly recommended

Resources for IETF 118 Prague

- Agenda
  https://datatracker.ietf.org/meeting/agenda
- Meetecho and other information:
  https://www.ietf.org/how/meetings/preparation
- If you need technical assistance, see the Reporting Issues page:
  http://www.ietf.org/how/meetings/issues/

Agenda

Administrativia (5min)

- Blue sheets / scribe selection / NOTE WELL
- Agenda revision
- WG Status

Working Group Drafts (20min)

- TLS Encrypted Client Hello (ECH) - Chris Wood - 15 min
- Compact TLS 1.3 - Hannes/Joe - 2 min
- IANA Registry Updates for TLS and DTLS - Joe Salowey - 2 min

Adoption

- SSLKeyLog

Agenda Continued

Individual Drafts (Remaining Time)

- AuthKEM - Thom Wiggers - 15 min
  - KEM-based Authentication for TLS 1.3
  - KEM-based pre-shared-key handshakes for TLS 1.3
- TLS 1.2 is frozen - Rich Salz - 10 min
- Legacy RSASSA-PKCS1-v1_5 codepoints for TLS 1.3 - Andre Popov - 15 min
- TLS Trust Expressions - David Benjamin - 30 min
- TLS Key Share Prediction - David Benjamin - 15 min
- TLS Flag - Request mTLS - Jonathan Hoyland - 5 min
- TurboTls - Deirdre Connolly - Time Permitting

cTLS Update

- New draft version available: draft-ietf-tls-ctls-09
- Formal analysis now available (thanks to Karthik & friends):

  "Comparse: Provably Secure Formats for Cryptographic Protocols"
- The further reduce the size of public keys draft-mattsson-tls-compact-ecc has been written. Thanks to John Mattsson.
  - Will ask for adoption in the mailing list.
- Next steps:
  - Gather more implementation feedback
  - Formal analysis of optimization to remove the randoms with the key share public keys ongoing.