28 March 2023

# TLS @ IETF 116

This session is being recorded

IETF 116 Yokohama
hosted by
WIDE
PROJECT

Internet Engineering Task Force

Production by Meetecho

I E T F®

# WG I-Ds Status

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:

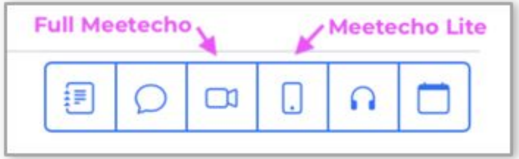
- BCP 9 (Internet Standards Process)
- BCP 25 (Working Group processes)
- BCP 25 (Anti-Harassment Procedures)
- BCP 54 (Code of Conduct)
- BCP 78 (Copyright)
- BCP 79 (Patents, Participation)
- https://www.ietf.org/privacy-policy/(Privacy Policy)c

This session is being recorded

# IETF 116 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*
- **Wear masks unless actively speaking at the microphone.**



**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 116 Yokohama

- 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

Administrivia - Chairs - 10min

- Blue sheets / Scribe selection
- Agenda Revisions

Working Group I-Ds - 30min

- RFC8447bis, Joe Salowey, 10min
- CTLS, Ben Schwartz, 5min
- Hybrid KeyX, Scott Fluhrer, 15min

Individual I-Ds - 65min

- Bootstrapping TLS Encrypted ClientHello with DNS Service Bindings,
  Benjamin Schwartz, 10min
- Merkle Tree Certificates,
  David Benjamin, 20min

Individual I-Ds (continued)

- Compact ECDHE and ECDSA Encodings for TLS 1.3,
  John Mattsson, 10min
- NULL Encryption and Key Exchange Without Forward Secrecy are Discouraged,
  John Mattsson, 10min
- Plaintext Sequence Numbers for Datagram Transport Security Layer 1.3,
  Boris Pismenny, 15min

TLS 1.2 Deprecation - Chairs/All - 15min

# WG I-Ds Status

AUTH48

- Delegated Credentials for (D)TLS

In WGLC very shortly

1. The Transport Layer Security (TLS) Protocol Version 1.3
   IANA Registry Updates for TLS and DTLS
2. Deprecating Obsolete Key Exchange Methods in TLS 1.2
3. Return Routability Check for DTLS 1.2 and DTLS 1.3

Awaiting implementation

- A Flags Extension for TLS 1.3

Awaiting experimental results

- TLS Encrypted Client Hello
- A well-known URI for publishing ECHConfigList values

Expired

- Secure Negotiation of Incompatible Protocols in TLS