

IETF 115 COSE Working Group

8 November 2022

This session is being recorded

IETF 115 London
hosted by



Internet Engineering Task Force
© 2022 IETF Trust
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)



This session is being recorded

IETF 115 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 115 London

- Agenda
<https://datatracker.ietf.org/meeting/agenda>
- Meetecho and other information:
<https://www.ietf.org/how/meetings/115/preparation>
- If you need technical assistance, see the Reporting Issues page:
<http://www.ietf.org/how/meetings/issues/>

Volunteers Needed

- Note taker(s)
 - <https://notes.ietf.org/notes-ietf-115-cose>

IETF 115 COSE Meeting Agenda

- 15:00-15:04 Opening remarks by the chairs - the chairs
- 15:04-15:05 Status of Documents Past WGLC - the chairs
- 15:05-15:10 draft-ietf-cose-aes-ctr-and-cbc - Russ Housley
- 15:10-15:20 draft-ietf-cose-hpke - Hannes Tschofenig
- 15:20-15:30 draft-ietf-cose-cbor-encoded-cert - Joel Höglund
- 15:30-15:35 draft-looker-cose-bls-key-representations - Tobias Looker/Mike Jones
- 15:35-15:40 draft-looker-cose-cwt-claims-in-headers - Mike Jones/Tobias Looker
- 15:40-15:50 draft-prorock-cose-post-quantum-signatures - Michael Prorock
- 15:50-15:55 draft-birkholz-scitt-receipts and draft-birkholz-cose-tsa-tst-header-parameter - Henk Birkholz
- 15:55-16:00 AOB

Status of Documents Past WGLC

- RFC 9052: CBOR Object Signing and Encryption (COSE): Structures and Process, *Internet Standard*
- RFC 9053: CBOR Object Signing and Encryption (COSE): Initial Algorithms, *Informational RFC*
- RFC 9054: CBOR Object Signing and Encryption (COSE): Hash Algorithms, *Informational RFC*
- draft-ietf-cose-countersign: CBOR Object Signing and Encryption (COSE): Countersignatures, *RFC Editor Queue*
- draft-ietf-cose-x509: CBOR Object Signing and Encryption (COSE): Header parameters for carrying and referencing X.509 certificates, *RFC Editor Queue*