21st July 2026

# JOSE WG @ IETF 126

This session is being recorded

Internet Engineering Task Force
© 2026 IETF Trust
Production by Meetecho

# Note Well

By participating in the IETF you agree to follow IETF processes and policies. This Note Well is a reminder of some of those policies. For a linked version of this text, please visit **www.ietf.org/note-well** or use the QR code below

- IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times (see **RFC 7154: IETF Guidelines for Conduct and IETF Anti-Harassment Policy**). If you have any concerns about behavior, please contact the *Ombudsteam* who have a duty of confidentiality and extensive powers to act, as set out in **RFC 7776: IETF Anti-Harassment Procedures**.
- If you are aware that any IETF contribution (as defined in **RFC 5378: Rights Contributors Provide to the IETF Trust**) is covered by patents or patent applications that are owned or controlled by you, your employer or your sponsor, you must disclose that fact, or not participate in the discussion (see **RFC 8179: Intellectual Property Rights in IETF Technology**).
- For detailed process information consult **RFC 2026: Internet Standards Process** and *RFC 2418:* **IETF Working Group Guidelines and Procedures** and updates to those.
- The IETF routinely makes public written, audio, video, and photographic records of IETF activities, including your personal information as set out in the **IETF Privacy Statement**.

For advice, please talk to Working Group chairs or Area Directors.

This session is being recorded

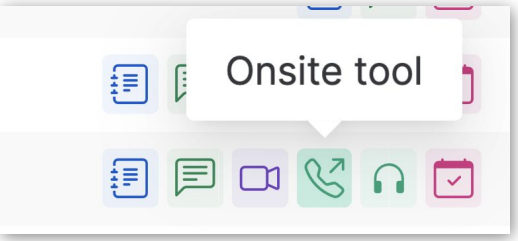
# IETF 126 Meeting Tips

**In-person participants**

- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the “Meetecho lite”) client to join the queue, show hands
- *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.




**All participants**

- State your name each time you begin speaking in the queue

# Resources for IETF 126 Vienna

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

# Today’s Agenda

Admin, Agenda Bash, document status (Chairs)

Working Group Documents

- Use of Hybrid Public Key Encryption (HPKE) with JSON Web Encryption (JWE)
- JOSE: Deprecate 'none' and 'RSA1_5’
- JOSE HPKE PQ & PQ/T Algorithm Registrations
- Post-Quantum Key Encapsulation Mechanisms (PQ KEMs) COSE
- PQ/T Hybrid Composite Signatures for JOSE and COSE
- JSON Web Proof Document set

Individual Drafts

- BBS and Modular Sub-proofs with JSON Web Proofs
- Long-Term Validation for JSON Web Signature (LTV-JWS)

Any Other Business (AOB)