06 November 2025

IETF 124 PQUIP WG
Post-Quantum Use In Protocols

This session is being recorded

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.

I E T F

Note Well

You already agreed to follow the IETF guidelines when you registered.

IETF participants are expected to behave in a professional manner and extend respect and courtesy to their colleagues at all times.

See https://www.ietf.org/note-well

IETF®

This session is being recorded

IETF 124 Meeting Tips

In-person participants

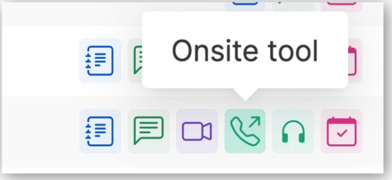
- Make sure to sign into the session via Datatracker or the QR Code in this session.
- Use Meetecho (usually the "Meetecho lite") client to join the queue, show hands
- ***Keep audio and video off if not using the onsite version.***

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



Agenda overview

- Documents completed
- Brief notes on outside projects
- Two current WG drafts
- ETSI and Quantum Safe Cryptography
- Possible future WG work: guidance for adopting PQC

Full agenda: https://datatracker.ietf.org/doc/agenda-124-pquip/

WG documents completed

- RFC 9794, “Terminology for Post-Quantum Traditional Hybrid Schemes”
- “Hybrid signature spectrums” and “Post-Quantum Cryptography for Engineers” are in the RFC Editor queue

Brief notes on outside projects

- PQC in certificates interop testing
  - Active at the IETF Hackathon and between meetings
  - https://github.com/IETF-Hackathon/pqc-certificates
- PQ DNSSEC
  - Did not meet this time
  - pq-dnssec@ietf.org
- CFRG
  - Met earlier this week, and is meeting later today (17:00-19:00, Laurier) has many PQC topics

Hash-based Signatures: State and Backup Management

- draft-ietf-pquip-hbs-state
- https://datatracker.ietf.org/doc/draft-ietf-pquip-hbs-state/

Adapting Constrained Devices for Post-Quantum Cryptography

- draft-ietf-pquip-pqc-hsm-constrained
- https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-hsm-constrained/

ETSI and Quantum Safe Cryptography

- It's not all about NIST ☺

Post-Quantum Algorithms guidance

- draft-prabel-pquip-pqc-guidance
- https://datatracker.ietf.org/doc/draft-prabel-pquip-pqc-guidance/

Drafts on how to migrate to PQC

- Is this work relevant to the IETF WGs, or just to outside organizations who use IETF protocols?
- There are already many drafts on the subject
  - draft-reddy-pquip-pqc-signature-migration
  - draft-kwiatkowski-pquip-pqc-migration
  - draft-bonnell-lamps-chameleon-certs
  - draft-wang-lamps-root-ca-cert-rekeying
  - draft-li-pquip-teleco-pqc-migration
  - draft-li-pquip-escape-message
  - ... and possibly others

What can PQUIP contribute?

- A skeptical view
  - Is there value in saying "you should think about this and that in your environment" if we cannot tell them how to make a decision?
  - What can we contribute to the discussion that is not already covered by existing articles and consultancies?
  - We can't predict the future
- A less skeptical view
  - There are lots of experts here
  - Maybe a catalog of all the considerations would help some readers