PQUIP WG

Paul Hoffman and Sofia Celi

IETF 119, Brisbane
2024-03-19, 1730-1830

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)

Agenda

- Post-Quantum Cryptography for Engineers, 10 minutes
- Terminology for Post-Quantum Traditional Hybrid Schemes, 10 minutes
- Hybrid signature spectrums, 2 minutes
- Post-quantum cryptography migration use cases, 5 mins
- Hash-based Signatures: State and Backup Management, 5 minutes
- Composite vs. Parallel Signatures, remainder

Post-Quantum Cryptography for Engineers

- https://datatracker.ietf.org/doc/draft-ietf-pquip-pqc-engineers/
- Aritra Banerjee, 10 minutes

Terminology for Post-Quantum Traditional Hybrid Schemes

- https://datatracker.ietf.org/doc/draft-ietf-pquip-pqt-hybrid-terminology/
- Flo Driscoll, 10 minutes
- WG Last Call ended March 6
- More changes needed before it moves forward

Hybrid Signature Spectrums

- https://datatracker.ietf.org/doc/draft-hale-pquip-hybrid-signature-spectrums/
- WG call for adoption ended March 11
- Authors will make changes to the document before it is adopted

Post-quantum cryptography migration use cases

- https://datatracker.ietf.org/doc/draft-vaira-pquip-pqc-use-cases/
- Alexander Railean, 5 mins
- Call for adoption?

Hash-based Signatures: State and Backup Management

- https://datatracker.ietf.org/doc/draft-wiggers-hbs-state/
- Thom Wiggers, 5 minutes
- Call for adoption?

Composite vs. Parallel Signatures

- Mike Ounsworth and Orie Steele