IETF PQUIP
draft-ietf-pquip-pqc-engineers
“PQC For Engineers”

Tim Hollebeek

Aritra Banerjee, Tirumaleswar Reddy, Dimitrios Schoinianakis

2024-07-22

IETF 120 Vancouver

PQC For Engineers

Quick recap of the draft

The draft explains why engineers need to be aware of and understand post-quantum cryptography.

It emphasizes the potential impact of Cryptographically Relevant Quantum Computers (CRQCs) on current cryptographic systems and the need to transition to post-quantum algorithms to ensure long-term security.

Adopted by the WG following IETF 117.

Since IETF 119

- Draft now uses official NIST names (ML-KEM, etc)
- … and that’s about it

Ship it?

Hopefully CRQCs are not that scary any more after reading this draft.

Are we ready for WGLC?