

Hackathon Special Report on PQC Interop

Justus Winter <justus@sequoia-pgp.org>

IETF 118, 2023-11-09

Hackathon project: Send an v6 OpenPGP PQC Email

- development versions of OpenPGP.js, GopenPGP, and RNP
- created keys using GopenPGP and RNP:
 - v6
 - Dilithium/Ed25519 as primary
 - Kyber/X25519 as encryption subkey
- successfully encrypted and decrypted an signed-then-encrypted message
 - sent over SMTP, for extra fun
- team
 - Daniel Huigens
 - Aron Wussler
 - Justus Winter

```
-----BEGIN PGP MESSAGE-----
Version: OpenPGP.js v0.10.0 (https://github.com/terryknight/openpgp.js)
Comment: v6 OpenPGP.js, GopenPGP, and RNP
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: OpenPGP.js v0.10.0 (https://github.com/terryknight/openpgp.js)
Comment: v6 OpenPGP.js, GopenPGP, and RNP
-----BEGIN PGP MESSAGE-----
-----END PGP MESSAGE-----
```