PQC Draft Update

Stavros Kousidis
Falko Strenzke
Johannes Roth
Aron Wussler

Interim meeting
2025-02-10

Changes to the Draft (06 to 07)

- Assigned code points 30 - 34 for ML-DSA+EdDSA and SLH-DSA algorithms
- Aligned KEM combiner with LAMPS
- Dropped CCA-conversion of X25519/X448
- Switched to hedged variant also for SLH-DSA

Seed key format

- At IETF 121, we chose seed format
- … but PKCS#11 technical committee plans to allow both seed and expanded format!
- LAMPS apparently decided to allow both seed and expanded format
- Some HSMs allow key exporting: not all exported private keys might allow conversion to OpenPGP wire format

Seed key format (Revised)

We kept the seed format because:

- We consider the HSM private key export for further use in software an edge case for OpenPGP
- We want to reduce complexity and allow only one format
- Significantly smaller keys
- Libraries prefer or offer only seed format
- They always produce a valid key

Key derivation and combination

- Updated (again) the Key Combiner
- Aligned to LAMPS (no CCA-conversion for ECC)
- FIPS compliance from NIST SP800-56C and SP800-227
- Key Combiner corresponds to “Kitchen sink” construction in draft-irtf-cfrg-hybrid-kems-01

Key derivation and combination

```
KEK = SHA3-256( mlkemKeyShare || ecdhKeyShare
    || ecdhCipherText || ecdhPublicKey
    || mlkemCipherText || mlkemPublicKey
    || algId || domSep )
```

Implementation Status

Implementation	ML-KEM + X25519/448	ML-DSA + EdDSA	SLH-DSA
go-crypto	✅	✅	✅
openpgp.js	✅	✅	✅
RNP *	✅	✅	✅

* Implementation not upstreamed

Open issues

There aren’t any open pull requests.

You could search all of GitHub or try an advanced search.

There aren’t any open issues.

You could search all of GitHub or try an advanced search.

Last call?

Useful links

Current version:

https://datatracker.ietf.org/doc/draft-ietf-openpgp-pqc

Issue tracker:

https://github.com/openpgp-pqc/draft-openpgp-pqc/issues