PQC Draft Update

Falko Strenzke
Johannes Roth
Stavros Kousidis
Aron Wussler

IETF 120
2024-07-22

Changes to the Draft (03 to 04)

- Fixed the ML-DSA signature size
- Re-sorted parameter order in PKESK description
- Added the missing parameters for KEM combiner
- Changed parallel encryption guidance (issue #2 / #67)
- Added ML-DSA test vectors

Implementation Status

Implementation	ML-KEM-ipd	ML-DSA-ipd	SLH-DSA
go-crypto	✅	✅	✱ (Round 3)
openpgp.js	✅	✅	❌
RNP	✅	✱ (Round 3)	✱ (Round 3)
Libgcrypt *	✅	✅	✅

* Implementation not upstreamed

Upcoming planned changes before IETF 121

Key derivation and combination

- We are still using a provisional version of the KEM Combiner
- There is an open discussion for NIST SP 800-56C compliance (issue #132)
- Depending on the outcome of the discussion with NIST and the CFRG it will be updated

Binding encryption keys to V6 (1)

Mixed opinions on the list:

- No: Not all implementations ready for v6
- No: Quicker deploy for encryption
- Yes: It is difficult to ensure backwards compatibility
- Yes: It may hinder adoption of v6
- Yes: Limits the combinations, simpler implementations

Binding encryption keys to V6 (2)

Discussion at the interim:

- No: LibrePGP allows v5 PQC subkeys to v4 primary keys
- Yes: Reducing complexity
- Yes: Avoid holding back v6 migration

Binding encryption keys to V6 (3)

Discussion at the OpenPGP mail summit:

- No: Less work (faster) to get a working implementation
- No: Not all implementations have v6 ready
- Yes: Only implementation without v6 is RNP, that is considering v6
- Yes: Only one migration necessary
- Yes: v4 PQC is more fragile

Binding encryption keys to V6 (4)

- The current draft allows encryption with v4
- There is clear consensus on allowing PQC with SEIPDv1
- There are slightly more opinions preferring a binding to v6
- Those opposing the binding could accept it, if there is wide support for v6 and a migration strategy
- Considering the increasing support for v6, we plan on binding to v6 in the next draft (~2 months from now)
- Raise a concern if you disagree!

Useful links

Current version:

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

Open issues:

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