PQC Draft Update

Stavros Kousidis
Falko Strenzke
Johannes Roth
Aron Wussler

IETF 121
2024-11-07

Changes to the Draft (04 to 06)

- Replaced initial public drafts with FIPS 203, 204, 205
- Chose SK seed format for ML-KEM and ML-DSA
- Mandated v6 keys for ML-KEM + ECDH algorithms
- Reworked KEM combiner

FIPS 203, 204, and 205

- Released in August from NIST
- Almost all upstream libraries implemented the final standard
- We managed to update in the past weeks
- Test vectors are ready (ML-KEM and ML-DSA)

Seed key format

The standard offers seed or explicit private key format.

We chose seed because:

- Significantly smaller keys
- Libraries prefer or offer only seed format
- They always produce a valid key
- LAMPS also decided for the seed format

Key derivation and combination

- Updated the provisional Key Combiner
- We adapted to NIST SP 800-108
- NIST confirmed informally that the construction is most likely conforming to the new standard [1]
- We place ML-KEM first in the construction so that we already have FIPS compliance

Key derivation and combination

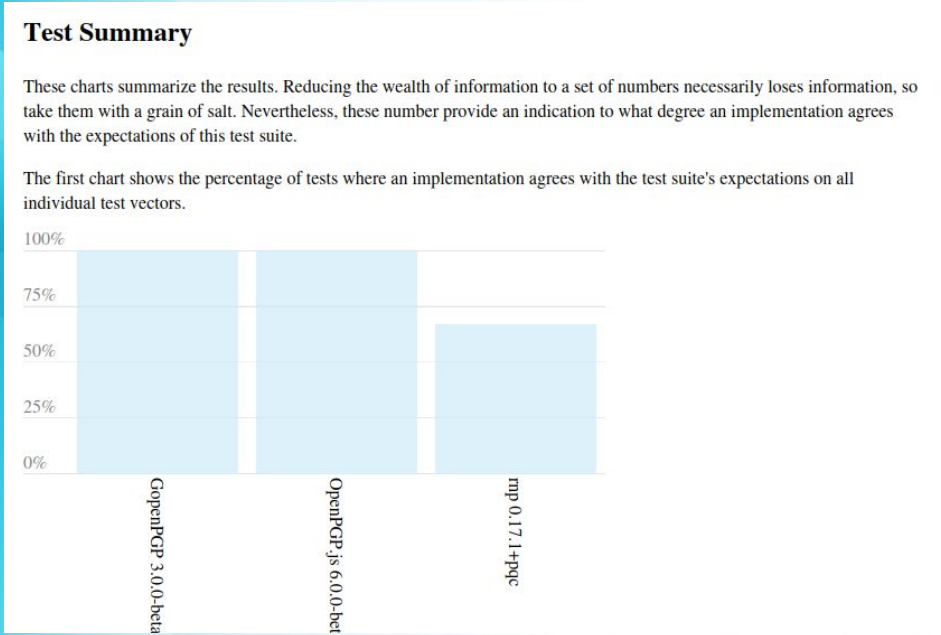
```
KEK = KMAC256(
   mlkemKeyShare || ecdhKeyShare,
   mlkemCipherText || ecdhCipherText ||
     mlkemPublicKey || ecdhPublicKey || algId,
  256, domSep)
```

Implementation Status

Implementation	ML-KEM	ML-DSA	SLH-DSA
go-crypto	✅	✅	❌ (Round 3)
openpgp.js	✅	✅	❌ (Coming soon)
RNP *	✅	✅	✅

* Implementation not upstreamed

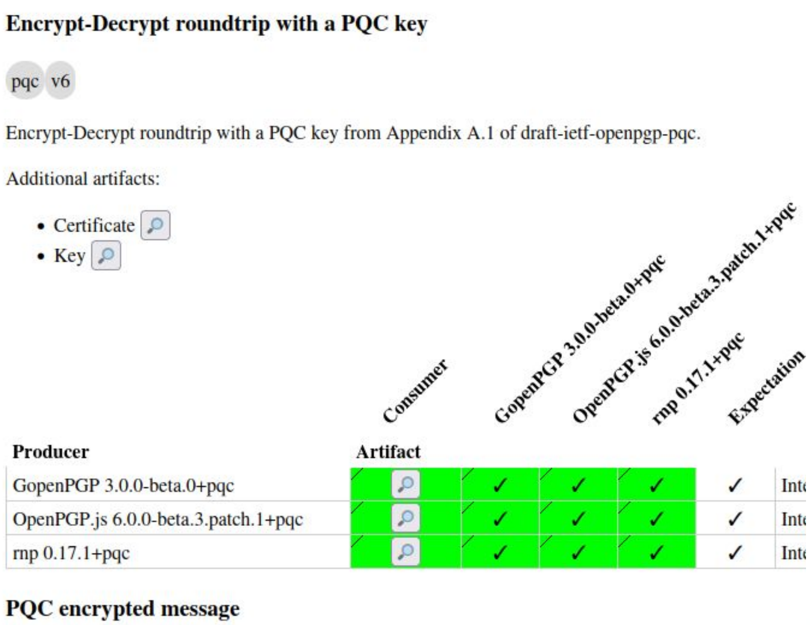
Interoperability Testing



Test Summary

These charts summarize the results. Reducing the wealth of information to a set of numbers necessarily loses information, so take them with a grain of salt. Nevertheless, these number provide an indication to what degree an implementation agrees with the expectations of this test suite.

The first chart shows the percentage of tests where an implementation agrees with the test suite's expectations on all individual test vectors.



Encrypt-Decrypt roundtrip with a PQC key

pqc v6

Encrypt-Decrypt roundtrip with a PQC key from Appendix A.1 of draft-ietf-openpgp-pqc.

Additional artifacts:

- Certificate 🔎
- Key 🔎

	Consumer	GopenPGP 3.0.0-beta.0+pqc	OpenPGP.js 6.0.0-beta.3.patch.1+pqc	rnp 0.17.1+pqc	Expectation	
Producer	**Artifact**					
GopenPGP 3.0.0-beta.0+pqc	🔎	✓	✓	✓	✓	Inte
OpenPGP.js 6.0.0-beta.3.patch.1+pqc	🔎	✓	✓	✓	✓	Inte
rnp 0.17.1+pqc	🔎	✓	✓	✓	✓	Inte

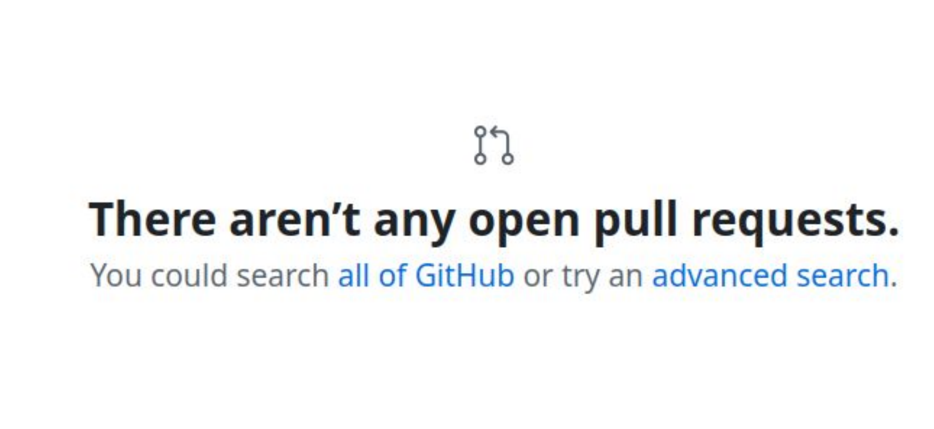
PQC encrypted message

Interoperability Testing

- Asymmetric Encryption
- Detached Signatures
- Inline Signatures
- Key Generation

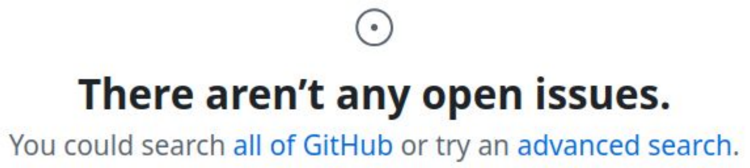
Daniel Huigens has opened a PR to the interop testsuite

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.

Next steps

- SLH-DSA interoperability coming soon
- Assigning actual code points?
- What’s missing for last call?

Useful links

Current version:

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

Open issues:

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

References

[1] https://mailarchive.ietf.org/arch/msg/cfrg/lMjb-LxUS5n1o93-kqvwRIIZ_44/