Post-Quantum Cryptography in OpenPGP

draft-wussler-openpgp-pqc

Stephan Ehlen[BSI], Andreas Hülsing[TU/e], Evangelos Karatsiolis[MTG], **Stavros Kousidis**[BSI], Johannes Roth[MTG], **Falko Strenzke**[MTG], **Aron Wussler**[Proton]

BSI: German Federal Office for Information Security
MTG: MTG AG, Germany
Proton: Proton AG, Switzerland
TU/e: Eindhoven University of Technology

Request for adoption of draft-wussler-openpgp-pqc

Current Algorithm and Parameter Choices

Protocol additions

PQC KEM and signatures

draft-wussler-openpgp-pqc

We propose adoption of `draft-wussler-openpgp-pqc`

- `https://datatracker.ietf.org/doc/draft-wussler-openpgp-pqc/`
- public repository
  - `https://github.com/openpgp-pqc/draft-openpgp-pqc`

Algorithm Choices

Kyber768 + X25519	**MUST**	192/128 [1]
Kyber1024 + X448	SHOULD	256/224
Kyber768 + ECDH-NIST-P-256	MAY	192/128
Kyber1024 + ECDH-NIST-P-384	MAY	256/192
Kyber768 + ECDH-brainpoolP256r1	MAY	192/128
Kyber1024 + ECDH-brainpoolP384r1	MAY	256/192
Dilithium3 + Ed25519	**MUST**	192/128
Dilithium5 + Ed448	SHOULD	256/224
Dilithium3 + ECDSA-NIST-P-256	MAY	192/128
Dilithium5 + ECDSA-NIST-P-384	MAY	256/192
Dilithium3 + ECDSA-brainpoolP256r1	MAY	192/128
Dilithium5 + ECDSA-brainpoolP384r1	MAY	256/192
SPHINCS$^+$-simple-SHA2	SHOULD	
SPHINCS$^+$-simple-SHAKE	MAY	

[1] classical security levels PQC/EC

Current SPHINCS+ Parameters

SPHINCS+-simple-**SHA2**-128s	SHOULD
SPHINCS+-simple-**SHA2**-128f	SHOULD
SPHINCS+-simple-**SHA2**-192s	SHOULD
SPHINCS+-simple-**SHA2**-192f	SHOULD
SPHINCS+-simple-**SHA2**-256s	SHOULD
SPHINCS+-simple-**SHA2**-256f	SHOULD
SPHINCS+-simple-**SHAKE**-128s	MAY
SPHINCS+-simple-**SHAKE**-128f	MAY
SPHINCS+-simple-**SHAKE**-192s	MAY
SPHINCS+-simple-**SHAKE**-192f	MAY
SPHINCS+-simple-**SHAKE**-256s	MAY
SPHINCS+-simple-**SHAKE**-256f	MAY

Request for adoption of draft-wussler-openpgp-pqc

Current Algorithm and Parameter Choices

Protocol additions

PQC KEM and signatures

Protocol additions

- PQC signatures
  - v6 keys only
  - v6 signature packets only
- PQC encryption
  - v4 or v6 keys
  - v3 or v6 PKESK packets
    - → v1 or v2 SEIPD packets

Request for adoption of draft-wussler-openpgp-pqc

Current Algorithm and Parameter Choices

Protocol additions

PQC KEM and signatures

PQC KEM and signatures

- Arguments for quick standardisation of KEM
  - KEM / encryption is highly pressing / too late already
  - using KEM combiner proposed to CFRG [2]
- Arguments for simultaneous standardisation of signatures
  - SLH-DSA with well understood security
  - ML-DSA PQ/T composite is a default for migration period
    - various European countries (France[3], Germany, Netherlands)
  - long term secure signatures (document archive, secure firmware update)
  - assessment of PQ-readiness requires both encryption and signatures
  - industry and public sector won't like two-step migration
    - long migration / field deployment and life-cycle times

[2] draft-ounsworth-cfrg-kem-combiners

[3] ANSSI views on the Post-Quantum Cryptography transition (08/2023)