# Persistent Symmetric Keys

# Draft Status

- Draft updated to reference RFC 9580 (on Gitlab, not yet in Datatracker)
- Reserved space for future, private and experimental symmetric algorithms
- Added test vectors

# Draft Status

| ID | Algorithm | Public Key Format | Secret Key Format | Signature Format | PKESK Format |
|---|---|---|---|---|---|
| 128 | AEAD | sym. algo, AEAD algo, fingerprint seed [Section 5.1] | key material | N/A | IV, ciphertext [Section 5.3] |
| 129 | HMAC [RFC2104] | hash algo, fingerprint seed [Section 5.2] | key material | authentication tag [Section 5.4] | N/A |
| 130 to 199 | Reserved for Future Persistent Symmetric Key Algorithms | | | | |
| 200 to 210 | Private or Experimental Persistent Symmetric Key Algorithms | | | | |

*Table 1: Persistent Symmetric Key Algorithm registrations*

# Implementation Status

- Implemented changes from last time in OpenPGP.js and GopenPGP
- Added test cases to the interop test suite

## Asymmetric Encryption

### Encrypt-Decrypt roundtrip with a persistent symmetric key

draft

Encrypt-Decrypt roundtrip using the persistent symmetric key from Appendix A.1 of draft-ietf-openpgp-persistent-symmetric-keys.

Additional artifacts:

- Certificate
- Key

| Producer | Artifact | Consumer | GopenPGP 3.0.0-beta.0+pqc | OpenPGP.js 6.0.0+pqc | Expectation | Comment |
|---|---|---|---|---|---|---|
| GopenPGP 3.0.0-beta.0+pqc | | | ✓ | ✓ | ✓ | Interoperability concern. |
| OpenPGP.js 6.0.0+pqc | | | ✓ | ✓ | ✓ | Interoperability concern. |

## Key Generation

### Default key generation, encrypt-decrypt roundtrip

pqc v6

This models key generation, distribution, and encrypted message exchange. Generates a default key with the producer *P*, then extracts the certificate from the key and uses it to encrypt a message using the consumer *C*, and finally *P* to decrypt the message.

| Producer | Artifact | Consumer | GopenPGP 3.0.0-beta.0+pqc | OpenPGP.js 6.0.0+pqc | Expectation | Comment |
|---|---|---|---|---|---|---|
| GopenPGP 3.0.0-beta.0+pqc | | | ✓ | ✓ | ✓ | Interoperability concern. |
| ↳ profile: draft-ietf-openpgp-persistent-symmetric-keys-00 | | | ✓ | ✓ | ✓ | Interoperability concern. |
| OpenPGP.js 6.0.0+pqc | | | ✓ | ✓ | ✓ | Interoperability concern. |
| ↳ profile: draft-ietf-openpgp-persistent-symmetric-keys-00 | | | ✓ | ✓ | ✓ | Interoperability concern. |

# Open Questions

- Separable IV and ciphertext?
- Any other feedback?

# Relation to PQC

- Consider implementing this together with PQC
- Encourage generating both?
- Relation to replacement key draft

# SOP / API considerations

- Allow encrypting & verifying using TSKs? (#110)
- Indicate whether data is for communication and/or storage?
- Allow generating multiple keys in `sop generate-key`? (#114)
- Encrypt with one key per “transferable keyring”?

# Thoughts? Questions?