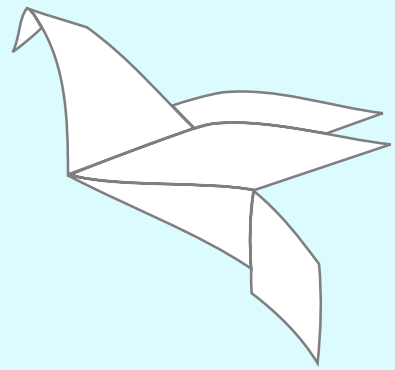
Migration paths to PQC

IETF 119

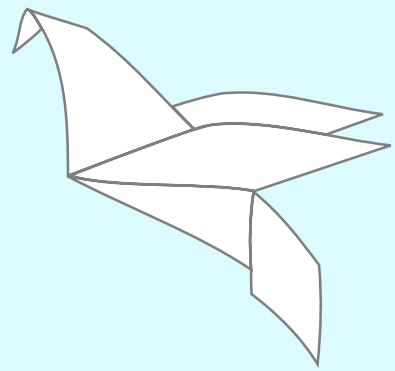
Justus Winter <justus@sequoia-pgp.org>

2024-03-19



Binding to v6 or not

- draft-ietf-openpgp-pqc-02 binds PQ signatures to v6
- draft-ietf-openpgp-pqc-02 does not bind PQ encryption to v6
  - as to not impede the adoption of PQ encryption
  - should it?

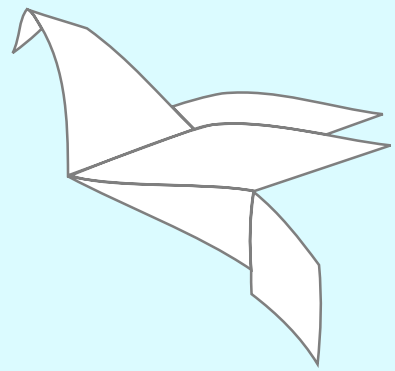


I think it should bind to v6

- clear and concise messaging
- let PQ be a reason to switch to v6!
- binding PQ encryption subkeys to v4 certificates isn't viable

Figure: https://tests.sequoia-pgp.org/#Mock_PQ_subkey

Producer	Artifact	Consumer	Sequoia 1.17.0	LibTMCG 1.4.0	GopenPGP 2.7.4	GopenPGP 3.0.0-alpha	OpenPGP.js 5.5.0	PGPainless 1.6.6	rnp 0.17.0	PGPy 0.6.0+dkg-crypto-refresh	PGPy 0.6.0	rpgpie 0.0.1	Sq's GnuPG Chameleon 0.6.0	GnuPG 2.4.4	GnuPG 2.2.40	GnuPG 1.4.23
Bob's cert		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unknown algo, MPI encoding		✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓
Unknown algo, opaque encoding, small		✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓
Unknown algo, opaque encoding, big		✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	
ECDSA, unknown curve, MPI encoding		✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓	
ECDSA, unknown curve, opaque encoding, small		✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	
ECDSA, unknown curve, opaque encoding, big		✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	
EdDSA, unknown curve, MPI encoding		✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓	
EdDSA, unknown curve, opaque encoding, small		✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	
EdDSA, unknown curve, opaque encoding, big		✓	✓	✗	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✗	
ECDH, unknown curve, MPI encoding		✓	✓	✗	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓	
ECDH, unknown curve, opaque encoding, small		✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✓	
ECDH, unknown curve, opaque encoding, big		✓	✓	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✗	✗	



Encrypting to classical and PQ

- encrypt a message for an ECC recipient and PQ recipient
  - obviously losing the PQ safety
  - but maybe better than plaintext
- should that work?
- should that fail?
- who decides?
  - the spec?
  - the sender?