

Standardization of PQC in OpenPGP

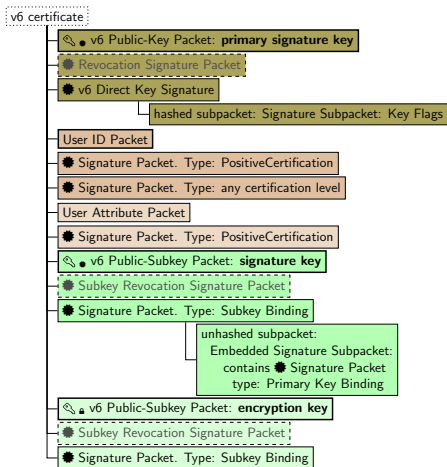
Joint work with Stavros Kousidis (BSI), Johannes Roth (MTG AG), and Aron Wussler (Proton AG)

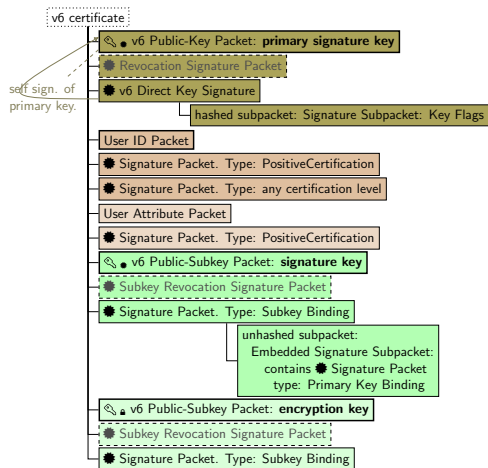
Dr. Falko Strenzke, MTG AG | [SPIQE Workshop June 24, Munich](#)

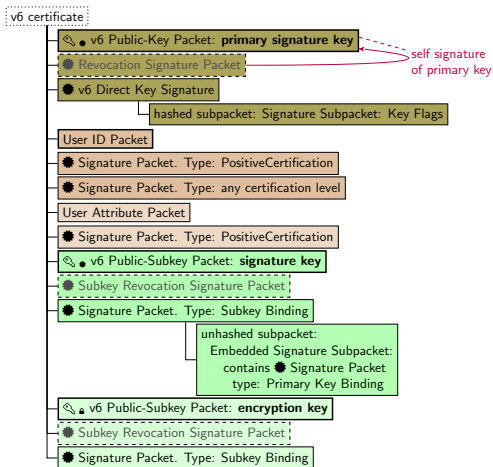
The work of MTG AG was carried out in the scope of Project 480 commissioned by the German Federal Office For Information Security (BSI).

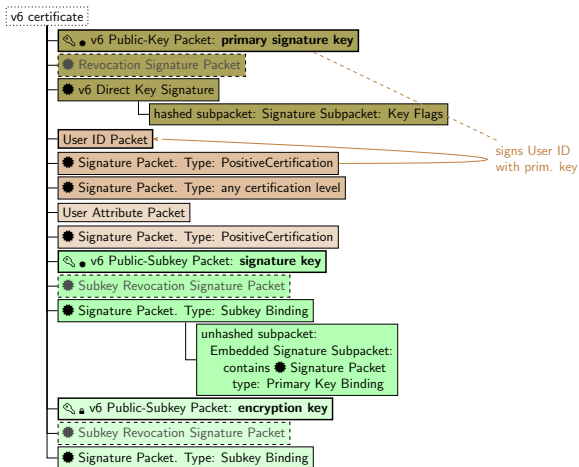
OpenPGP

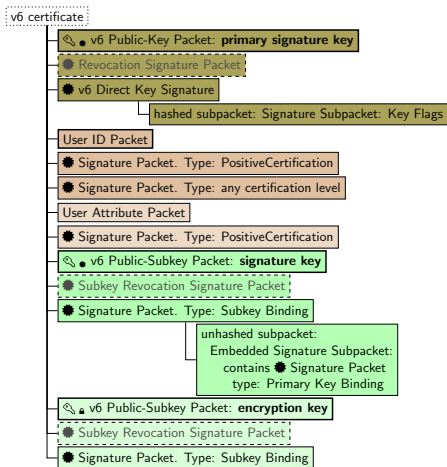
- ▶ OpenPGP Protocol
 - ▶ Public key signature and encryption
- ▶ Applications
 - ▶ E-Mail security
 - ▶ Code signing
 - ▶ File encryption
 - ▶ Backup encryption

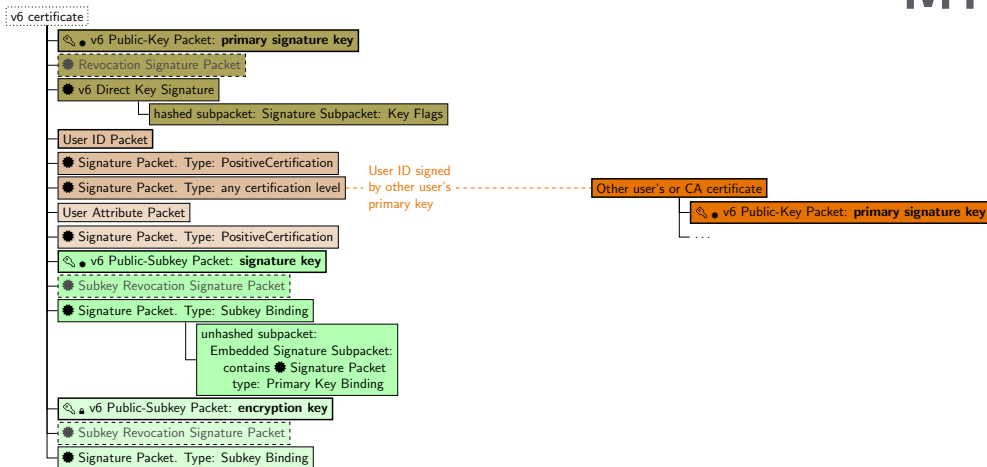


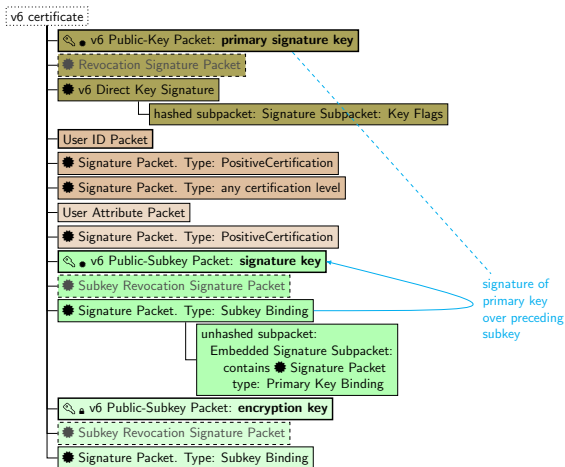


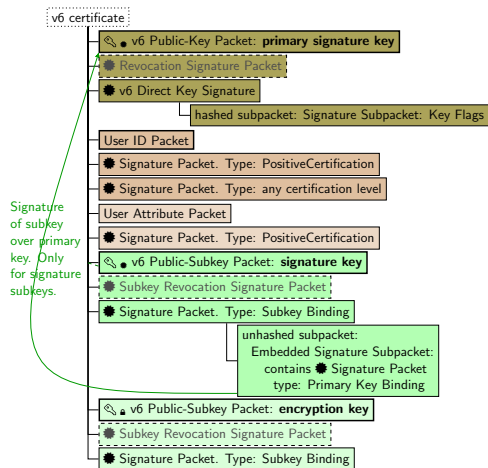


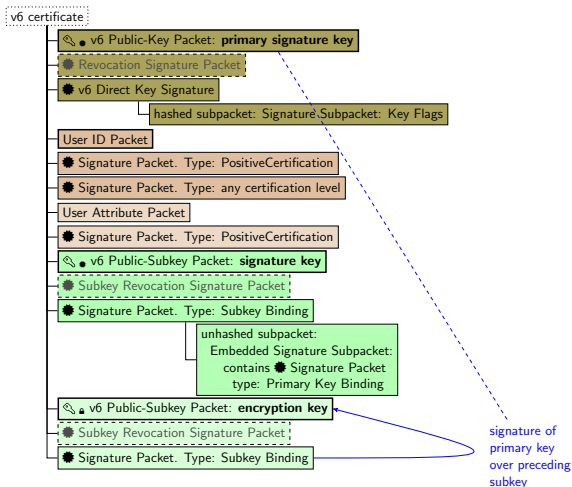


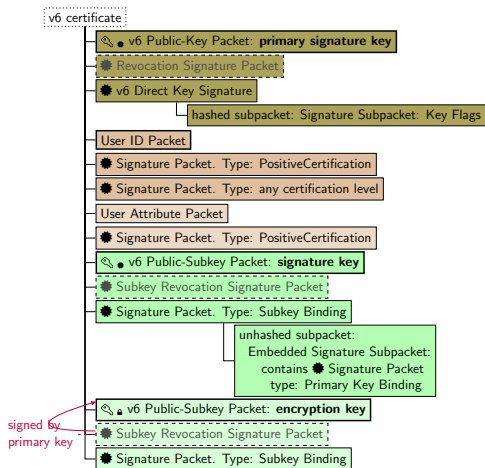


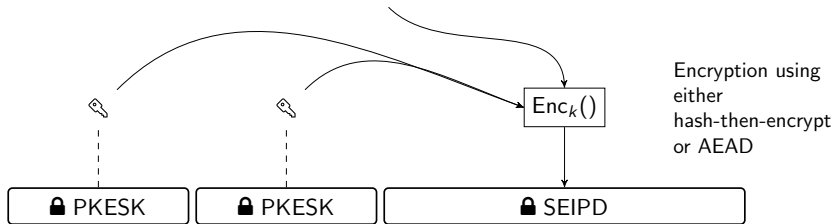
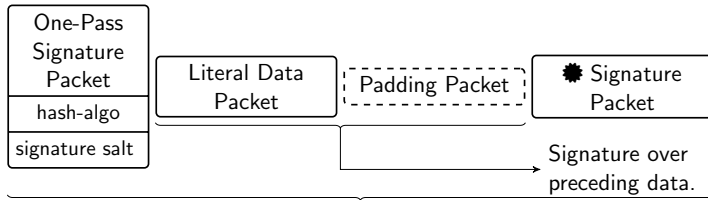












Public Key Encrypted

Session Key.

session key
encrypted to
public key
of user A

session key
encrypted to
public key
of user B

Symmetrically Encrypted Integrity

Protected Data Packet.

(message encrypted
with session key)

Two PQC Drafts

draft-ietf-openpgp-pqc
(adopted, passed WGLC)
BSI, MTG, Proton

| algorithms | requ. | security |
|--------------------|-------------|-----------|
| ML-KEM-768+X25519 | MUST | 192 / 128 |
| ML-KEM-1024+X448 | SHOULD | 256 / 224 |
| ML-DSA-65+Ed25519 | MUST | 192 / 128 |
| ML-DSA-87+Ed448 | SHOULD | 256 / 224 |
| SLH-DSA-SHAKE-128s | MAY | 128 |
| SLH-DSA-SHAKE-128f | MAY | 128 |
| SLH-DSA-SHAKE-256s | MAY | 256 |

draft-ehlen-openpgp-nist-bp-comp
(**not** adopted)
BSI, MTG, NIST

| algorithms | security |
|-------------------------------------|-----------|
| ML-KEM-512+ECDH- NIST-P-256 | 128 / 128 |
| ML-KEM-768+ECDH- NIST-P-384 | 192 / 192 |
| ML-KEM-1024+ECDH- NIST-P-384 | 256 / 192 |
| ML-KEM-768+ECDH- brpP256r1 | 192 / 128 |
| ML-KEM-1024+ECDH- brpP384r1 | 256 / 192 |
| ML-DSA-44+ECDSA- NIST-P-256 | 128 / 128 |
| ML-DSA-65+ECDSA- NIST-P-384 | 192 / 192 |
| ML-DSA-87+ECDSA- NIST-P-384 | 256 / 192 |
| ML-DSA-65+ECDSA- brpP256r1 | 192 / 128 |
| ML-DSA-87+ECDSA- brpP384r1 | 256 / 192 |
| all "MAY" | |

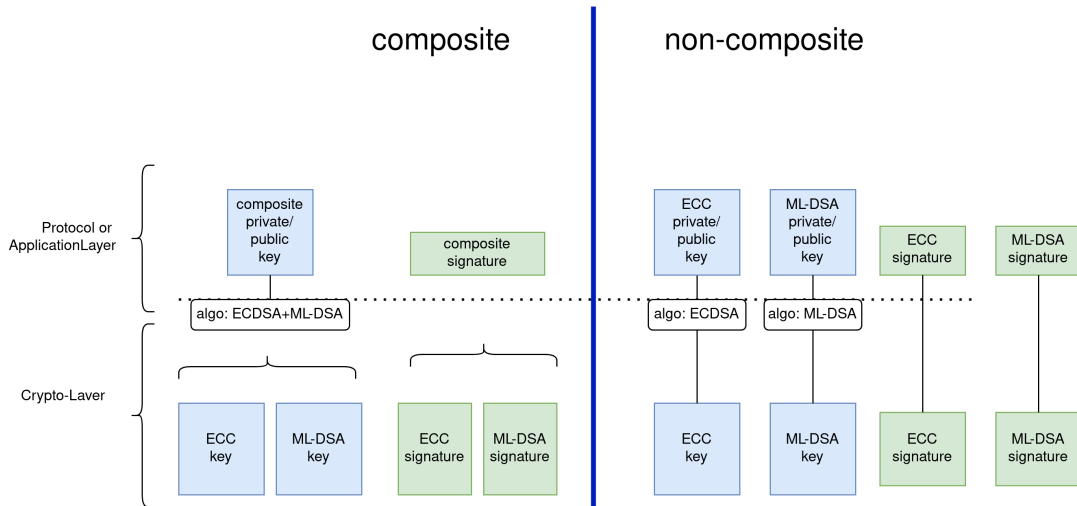
PQ/T hybrid schemes

- ▶ European Governments recommend/require pairing PQC schemes with traditional algorithms¹
 - ▶ exception: hash-based schemes
- ▶ NIST: "new stuff sometimes gets broken"²

¹See Appendix A for references

²<https://csrc.nist.gov/csrc/media/Presentations/2025/draft-sp-800-227-overview/images-media/sp-800-227-galagic.pdf#page=11>, NIST's workshop for Guidance on KEMs Feb 25, 2025

PQ/T hybrid signatures



PQC integration: original idea from the project

- ▶ in any case: hybrid = “multi-algorithm” (except SLH-DSA)
- ▶ first approach: completely generic
 - ▶ New algorithm ID for ML-KEM, ML-DSA, SLH-DSA
 - ▶ Non-composite for generic combinations of algorithms
 - ▶ Multiple signatures already provided in OpenPGP
 - ▶ e.g. ECDH + ML-DSA specifying the respective algorithm IDs
 - ▶ and specifying the parameters:
 - ▶ ECDH with 256-bit curve **128 bit**
 - ▶ ML-DSA **192 bit**

Decisions for PQC integration

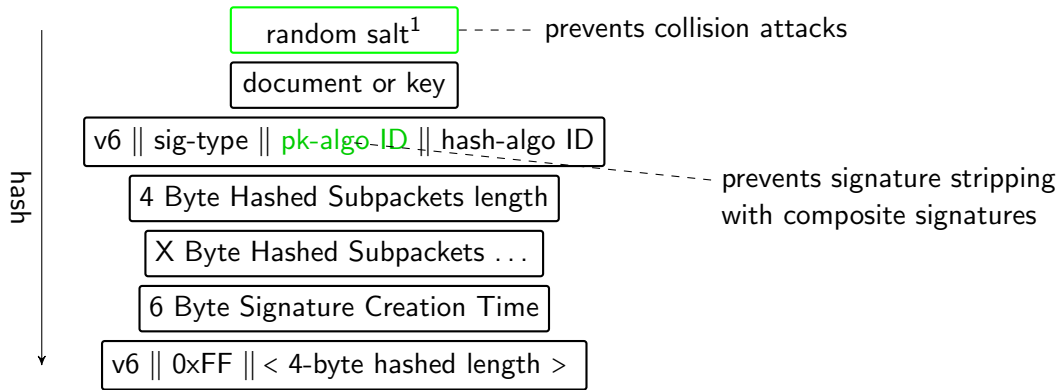
- ▶ Change decision 1
 - ▶ Composite
 - ▶ Algorithm ID: Fixed combinations of PQ / T
- ▶ Change decision 2
 - ▶ Set security parameters also with Algorithm ID
 - ▶ Algorithm ID = 30 → “ML-DSA-65+Ed25519”

PQC signatures in OpenPGP







- ▶ NIST specifies pure and pre-hash (=hash-then-sign) variants
 - ▶ pure variant = internal hashing with prefix
 - ▶ hash-based: prefix = random value (randomizer)
 - ▶ ML-DSA: prefix = public-key
- ▶ OpenPGP committed to hash-then-sign
 - ▶ → use pure variant to sign the hash
 - ▶ (theoretical drawback: hash-substitution attacks)
- ▶ No use of context parameter

RFC 9580 – signatures

v6 signatures — hashed data



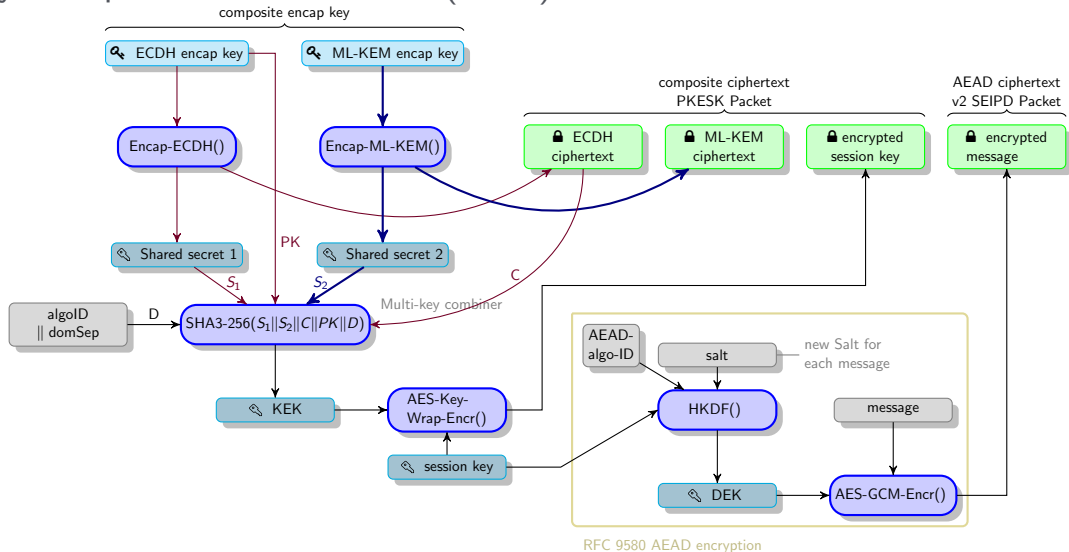
CMS – signatures⁴

- ▶ Cryptographic Message Syntax
 - ▶  X.509 certificates
 - ▶  signatures,  public-key encryption
- ▶ CMS legacy problem
 - ▶  EUF-CMA problem with Signed Attributes
 - ▶ Alternative views of what was exactly signed ([eprint 2023/1801](#)³)
 - ▶ Was not solved with context parameter of new PQC algorithms
- ▶ No meta-data is hashed
 - ▶  public-key algorithm not fixed by signature
 - ▶ → in case of hybrid: signature stripping attacks require extra countermeasure
 - ▶ not fully sound if PQ-signature is stripped off and legacy signature remains
- ▶ No random salt
 - ▶  signatures potentially vulnerable to hash-collision attacks
 - ▶ even with pure variants! (due to SignedAttributes → pre-hashing)

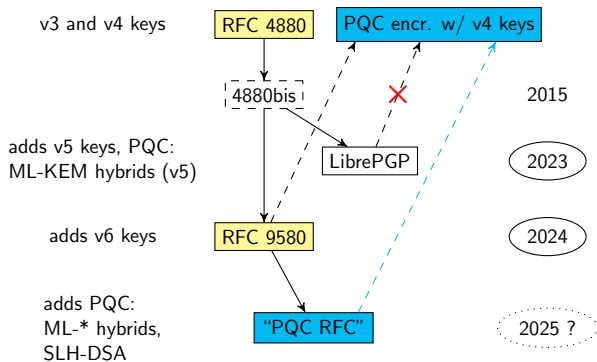
³ slides with 2nd attack variant: <https://cryptosource.de/slides/bsi-kry-sem-sig.pdf#page=30>

⁴ disclaimer: none of the CMS PQC standards are final RFCs yet

Key Encapsulation Mechanism (KEM)



v6/v5/v4 PQC



- ▶ Main goal: fast adoption of PQC encryption
- ▶ GnuPG LibrePGP standard features incompatible ML-KEM hybrids
 - ▶ LibrePGP (outside IETF) is a recent fork of OpenPGP due to WG-internal unresolved technical "issues"

Private keys in seed format

- ▶ ML-DSA and ML-KEM allow expanded and seed format
- ▶ heavily discussed in LAMPS
 - ▶ decision: support for both formats due to PKCS#11/hardware compatibility issues
- ▶ OpenPGP specifies seed-only private keys
 - ▶ achieves MAL-BIND-K-PK with given KEM combiner

Performance Aspects

- ▶ Typically, OpenPGP is not performance critical (time, memory)
- ▶ SLH-DSA-256
 - ▶ small: 29KB
 - ▶ ~~fast: 49KB~~
 - ▶ OpenPGP certificates carry multiple signatures
- ▶ SLH-DSA-256s signing: 1.5s @ 2GHz
 - ▶ Problem for Proton's in-browser signature generation

LAMPS WG: X.509, CMS, etc.

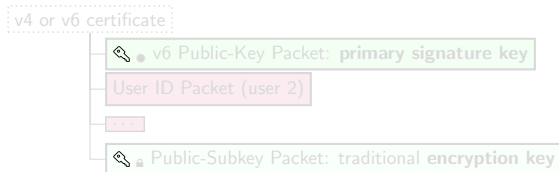
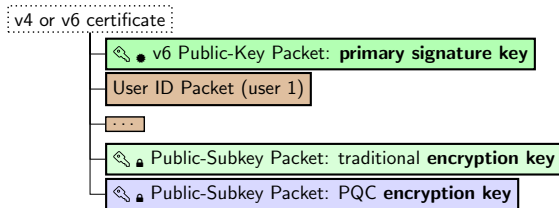
- ▶ Similarities:
 - ▶ Also only fixed algorithm combinations
 - ▶ Also definition of security parameters by algorithm ID
- ▶ Differences:
 - ▶ XMSS for X.509
 - ▶ LMS for X.509 & CMS
 - ▶ All 12 SLH-DSA parameters⁵
 - ▶ ML-DSA and ML-KEM as standalone
 - ▶ Composite
 - ▶ Combinations with RSA and ECDSA (NIST, Brainpool)
 - ▶ Inclusion of the Falcon signature scheme (not yet finalized by NIST)

⁵SLH-DSA in LAMPS has both pure & pre-hash → 24 OIDs altogether

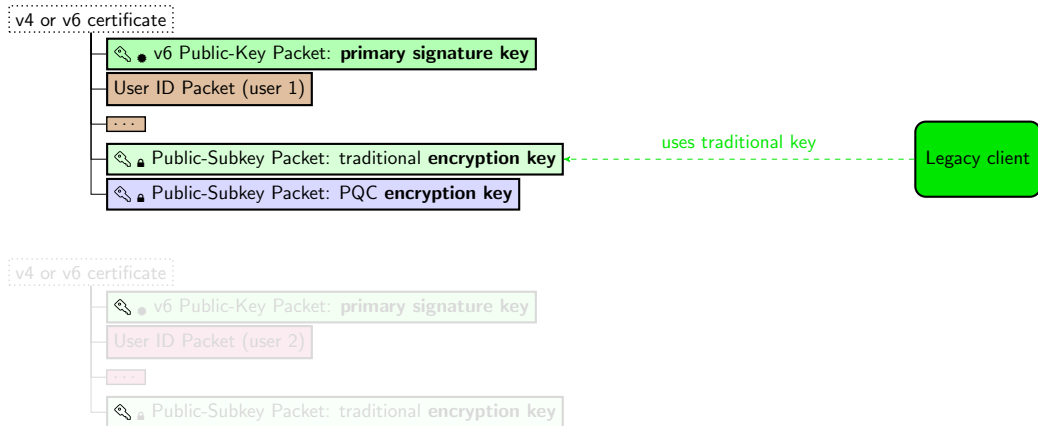
PQC transition

- ▶ PQC transition ...
 - ▶ Depends (largely) on transition to v6 keys (RFC 9580)
 - ▶ No general v6 roll-out so far
 - ▶ No supporting mail client
- ▶ Typical migration: first passive support, later generate new formats

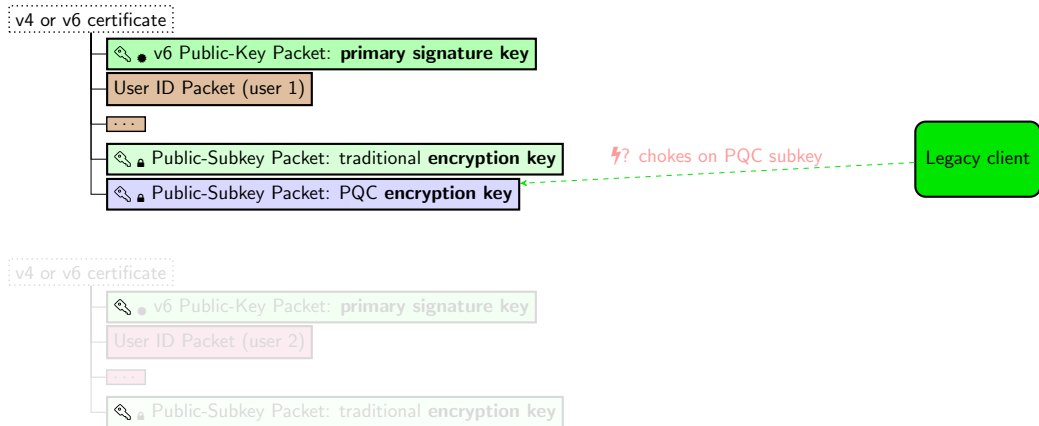
PQC transition for encryption keys



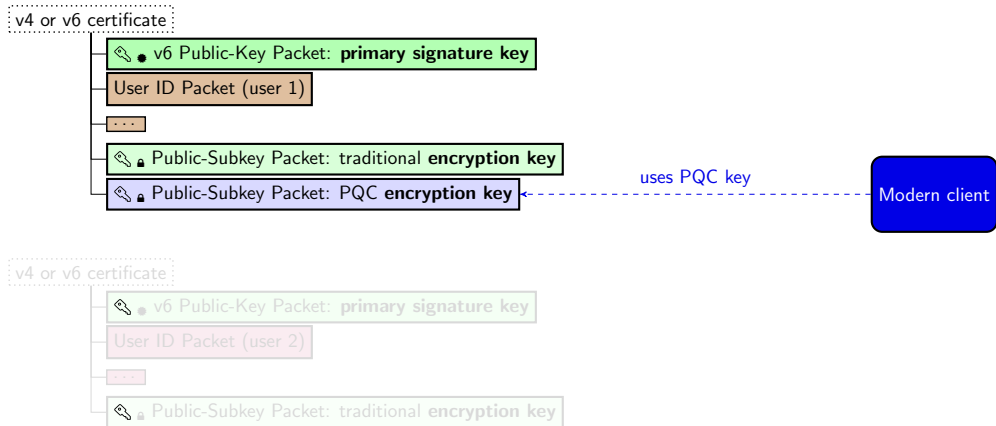
PQC transition for encryption keys



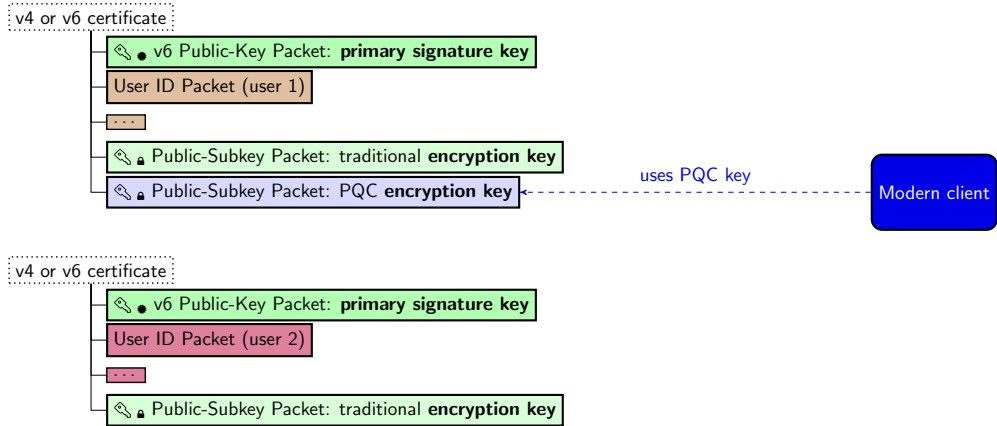
PQC transition for encryption keys



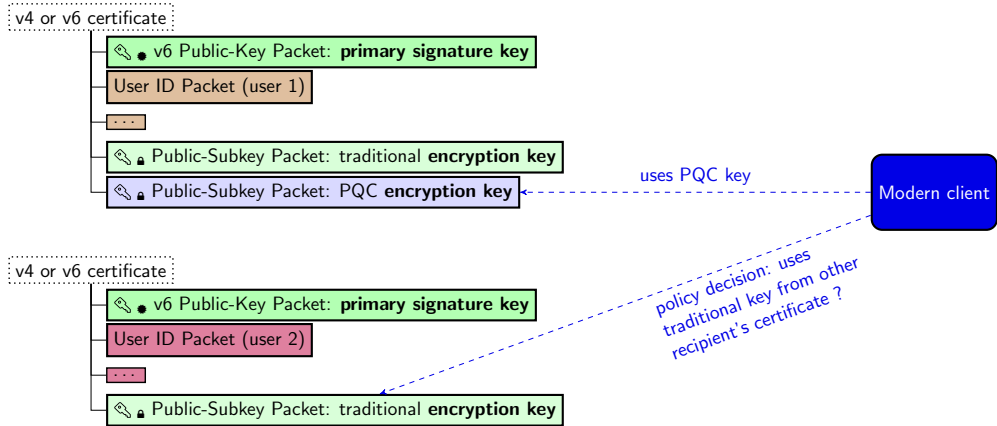
PQC transition for encryption keys



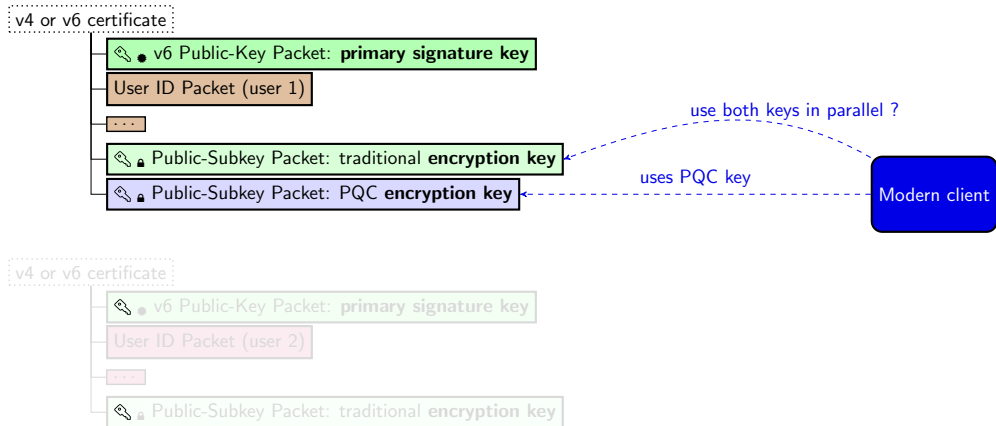
PQC transition for encryption keys



PQC transition for encryption keys

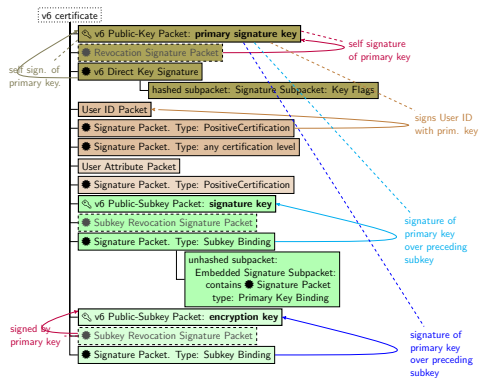


PQC transition for encryption keys



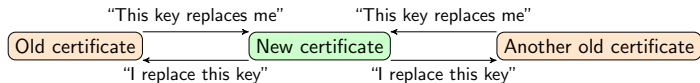
PQC transition for signature keys

- ▶ Signature:
 - ▶ Sender needs to assess whether recipient can verify PQC signatures
 - ▶ do so by checking recipient's certificate for PQC signature keys
- ▶ Potential problem:
 - ▶ PQC primary key requires recipient to understand PQC signatures
 - ▶ Only PQC signature subkey: no long-term trust in certificate



PQC transition mechanisms

- ▶ Enable key servers to serve two certificates:
 - ▶ v4 with traditional algorithms
 - ▶ v6 with PQC
- ▶ Replacement keys signalling mechanism draft⁶



- ▶ Symmetric reencryption draft⁷
- ▶ Proton:
 - ▶ Single-step v6 + PQC transition soon for Proton users
 - ▶ Semi-open user group
 - ▶ No uncontrolled exposure of v6 or PQC keys to outsiders

⁶<https://datatracker.ietf.org/doc/draft-gallagher-openpgp-replacementkey/>

⁷<https://datatracker.ietf.org/doc/draft-huigens-openpgp-persistent-symmetric-keys/02/>

Conclusion and Outlook

- ▶ Draft PQC for OpenPGP with current NIST spec on the way
- ▶ Unclear when large scale deployment of
 - ▶ PQC signatures and encryption with v6
 - ▶ PQC encryption-only with v4
- ▶ v6 signature features help PQC integration
- ▶ A look into the future ...
 - ▶ ... HQC as alternative to ML-KEM
 - ▶ ... NIST's new signature call

Thank you for your attention

Dr. Falko Strenzke
falko.strenzke@mtg.de
+49 6151 8000-24

MTG AG
www.mtg.de

Appendix A – Authorities on multi-algorithm

- ▶ ANSSI, <https://cyber.gouv.fr/en/publications/follow-position-paper-post-quantum-cryptography>
- ▶ BSI, <https://www.bsi.bund.de/TR-02102>
- ▶ NLNCSA, <https://english.aivd.nl/binaries/aivd-en/documenten/publications/2022/01/18/prepare-for-the-threat-of-quantumcomputers/Prepare+for+the+threat+of+quantumcomputers.pdf>
- ▶ EUCC, ECCG Agreed Cryptographic Mechanisms - version 2, https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en
- ▶ EU Joint Statement “Securing Tomorrow, Today” (18 member states): <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf>

Appendix B – RFC 9580 signature salt

- ▶ RFC 9580 signature salt sizes
 - ▶ 128 to 256 bits of random salt
 - ▶ salt size meets at least the collision resistance security level of the algorithm