Downgrade Resistance and Certificate Selection in Post-Quantum OpenPGP E-Mail

Stavros Kousidis

Master thesis · Published: 2026-10-18

Research question

Under which certificate, capability and migration conditions can OpenPGP mail clients silently lose post-quantum protection, and which selection policies prevent such downgrades?

Description

RFC 9980 defines composite post-quantum/traditional OpenPGP algorithms in which both components contribute to the cryptographic operation. These guarantees apply once a particular key and algorithm have been selected. During migration, however, a mail application may know several certificates for the same identity, including classical and post-quantum certificates with different authentication, validity or capability states.

This thesis investigates whether certificate discovery, authentication and application key-selection policy can cause a message to receive weaker protection than the sender intended. The existing Fedora test environment with KMail, Claws Mail and Evolution provides three independently observable client paths for the experiments.

Scope and evaluation

Develop an explicit attacker and migration model. Distinguish, for example, an attacker who can publish or introduce a competing certificate, interfere with certificate availability, or exploit stale local state from one who can forge certifications or break the underlying cryptography.

Construct controlled identities with combinations of classical and RFC 9980 certificates. Vary relevant properties such as authentication state, expiration or revocation, encryption-capable subkeys, algorithm support and locally cached certificate versions. For each mail client, determine whether it selects post-quantum protection, falls back to a classical alternative, warns the user, or refuses the operation. Inspect the generated OpenPGP packets rather than relying only on user-interface indicators.

Compare the observed decisions with explicit policies such as "post-quantum required", "prefer post-quantum with visible fallback" and "legacy allowed". The objective is not to assume that every fallback is a vulnerability, but to identify the conditions under which a downgrade violates a clearly stated security objective.

Expected outcome

A threat model and reproducible downgrade test matrix for KMail, Claws Mail and Evolution, together with an analysis of certificate-selection behavior and concrete recommendations for migration-safe OpenPGP policy.

Starting points

- RFC 9980: Post-Quantum Cryptography in OpenPGP.
- Post-quantum OpenPGP on Fedora 45: shared setup.
- Sequoia PGP: Authenticating certificates.
- RFC 9580: OpenPGP.

Contact: stavros.kousidis@th-koeln.de
Code publication: open source by default; exceptions require prior agreement (policy).