Security Analysis of Proof-of-Possession for KEM-Based Certificate Enrollment

Stavros Kousidis

Master thesis · Published: 2026-10-15

Research question

Which security guarantees do KEM-based proof-of-possession mechanisms establish in certificate enrollment, and under what assumptions are they resistant to challenge relaying, identity misbinding, and premature certificate issuance?

Description

Certificate enrollment protocols need to establish that an applicant can use the private key associated with a public key to be certified. Traditional proof-of-possession (PoP) often relies on signing a certificate request, but a key encapsulation mechanism (KEM), such as ML-KEM, cannot generate signatures. Alternatives include a challenge encapsulated to the applicant's KEM public key or delivery of an encrypted certificate followed by confirmation.

These mechanisms raise subtle security questions. A successful challenge response may have been relayed from a different key holder rather than computed by the authenticated applicant. In the encrypted-certificate approach, the certification authority may generate a certificate before PoP succeeds. Whether these behaviors create a vulnerability depends on authorization, protocol binding, certificate publication, and the assumed attacker capabilities.

You will analyze KEM-based PoP in existing and proposed enrollment mechanisms, focusing on Certificate Management Protocol (CMP, RFC 9810) and Enrollment over Secure Transport (EST, RFC 7030). The aim is to establish precisely which properties these protocols guarantee, not to presume that any particular mechanism is insecure.

Scope and evaluation

Define a threat model that includes unauthorized certificate requests, challenge relaying, concurrent sessions, and access to a legitimate key holder as a restricted decapsulation service. Distinguish private-key usability from applicant authorization, session binding, and exclusive key control. Compare direct challenge-response with encrypted-certificate confirmation; examine when certificate generation, confirmation, release, and publication occur.

Implement a small, isolated ML-KEM proof-of-concept to demonstrate selected attack or defense scenarios. A full production implementation of EST or CMP is not expected. Evaluate whether observed behavior violates a clearly stated security objective and identify the assumptions on which the conclusion depends.

Expected outcome

A documented security model, a comparative protocol analysis, a reproducible experiment, and concrete recommendations for KEM-based enrollment. Results may motivate further work on formal PoP definitions or IETF standardization.

Starting points

- RFC 7030, *Enrollment over Secure Transport (EST)*: EST enrollment and TLS-related PoP binding.
- RFC 9810, *Certificate Management Protocol (CMP)*: KEM PoP, direct challenges, encrypted certificates, and security considerations (Sections 4.3.4, 5.2.8, 8.1, and 8.11).
- RFC 9629, *Using KEM Algorithms in CMS*: encapsulation-based certificate encryption primitives.

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