ML-KEM (née Kyber) Certificates

IETF 118 - LAMPS WG

Sean Turner, Panos Kampanakis, Jake Massimo, Bas Westerbaan

Datatracker: draft-ietf-lamps-kyber-certificates
GitHub: kyber-certificates

Status

-02: current

- keep-alive draft, i.e., no substantive changes

-03:

- Kyber ⇒ Module-Lattice-Based Key Encapsulation Mechanism
- Example?

-04:

- Private key format