Internet X.509 Public Key Infrastructure: Algorithm Identifiers for Kyber

draft-ietf-lamps-kyber-certificates

Sean Turner, Panos Kampanakis, Jake Massimo, Bas Westerbaan

LAMPS@IETF115 — 20221109

Status: Needs an update

To Do:

1. Complete Kyber only swap
2. Insert ASN.1 (no OIDs yet)
3. Maintain alignment with draft-perret-prat-lamps-cms-pq-kem WRT RecipientInfo

Issues:

1. Private Key Format