Algorithm Identifiers for NIST's PQC KEM Algorithms for Use in the Internet X.509 Public Key Infrastructure

draft-turner-lamps-nist-pqc-kem-certificates

Sean Turner

LAMPS@IETF112 - 20211108

I-D’s Content

OIDs for NIST PQC KEM Algorithms winners that go in certificates

- `AlgorithmIdentifier`is an OID with **no** parameters
- Multiple algorithm identifiers per algorithm to account for parameters

Key Usage Bits

- MUST `keyAgreement`
- MAY `encipherOnly`and `decipherOnly`(?)

Subject Public Key Fields

Private Key Format

ASN.1 module

The ask:

Obviously still a WIP, but is this a good starting point for a WG I-D?

Help with examples!