MLS-DSA / ML-KEM Certificates I-Ds

IETF 120 - LAMPS WG

Jake Massimo, Panos Kampanakis, **Sean Turner**, & Bas Westerbaan

Datatracker: draft-ietf-lamps-dilithium-certificates & draft-ietf-lamps-kyber-certificates
GitHub: ML-DSA Certificates & ML-KEM Certificates

ML-DSA Certificates

Some alignment with ML-KEM certificates I-D:

- New ASN.1 Module paragraph (just an intro to get refs in I-D)
- Algorithm Identifier ASN.1 is now ‘21

Address John’s comments; didn’t include refs to ML-DSA+CMS, OCSP, etc to avoid dependency

To Do:

- Make sure private key text is aligned with SLH-DSA / ML-KEM I-Ds
- Add OIDs

ML-KEM Certificates

Some alignment with ML-DSA certificates I-D:

- Added a para in intro to repeat what's in the document
- Merged two sections
- Moved DRAFTFIP203 to normative

To Do:

- Make sure private key text is aligned with SLH-DSA / ML-DSA I-Ds
- Add OIDs