MLS-DSA / ML-KEM Certificates I-Ds

IETF 121 - 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


FIVE
2012
LAMPS
DUBLIN BREWERY
THE BEER
OF DUBLIN

ML-KEM Certificates

tl;dr: basically done.

New version; see diff.

Added NIST OIDs.

Aligned more closely with SLH-DSA I-D.

Refactored! Moved ASN.1 modules and examples to appendices.

Updated examples for ML-KEM-512, -768, & -1024 private & public keys based on FIPS 203; private key is 64-bit seed.

*SHOULD*ed publicKey not be in PKCS#8; no need for PKCS#8 v2.

Added security considerations; see PR 69; refers to -ml-kem-security-consideration.

Need:

- ML-KEM certificate example; personally hoping for a ML-KEM-768 signed with ML-DSA-65 private key from ML-DSA I-D.
- Acknowledgements!

ML-DSA Certificates

New version; diff.

Converter to md.

Added NIST OIDs.

Aligned more closely with SLH-DSA I-D; still needs work.

Refactored! Moved ASN.1 module and examples to appendices.

Examples for ML-DSA-44, -65, & -87 private & public keys based on FIPS 204; private key is 32-bit seed.

*SHOULD*ed publicKey not be in PKCS#8; no need for PKCS#8 v2.

To do:

- Security Considerations; queue Bas/Deirdre on use of 32-bit seed.
- SLH-DSA alignments.
- Need ML-DSA certificate example; self-signed ML-DSA-65.
- Add Pre-Hash!!!!?!?!?
- Add Acknowledgements!