Use of the ML-DSA Signature Algorithm in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-cms-ml-dsa

IETF 122 – LAMPS

What’s new?

- SHA-512 now a MUST
- Removed text recommending SHAKE

- Key formats/ASN.1 moved over to dilithium-certs draft

- Test vectors (please verify!)
  - Haven’t included for “no signed attributes” case

To SHAKE or not to SHAKE?

- Panos asks: Should we add SHAKE256 as a SHOULD for people who want code economy?
  - If SHA-512 is a MUST, you still need to implement SHA-512 so you don’t get code economy
- Could make SHAKE a SHOULD anyway?