Use of ML-KEM in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-cms-kyber-05

Julien Prat, Mike Ounsworth, Daniel Van Geest

IETF 121 – LAMPS

-05

- Aligns with FIPS 203
- Examples (private keys need to be updated to use seed)
- KEMRecipientInfo.kdf = HKDF with SHA-256 (next page)

KDF

Only HKDF with SHA-256

- People want HKDF with SHA2 and it seems to be FIPS compatible.
- FIPS 203: “If further key derivation is needed, the final symmetric keys shall be derived from this 256-bit shared secret key in an approved manner, as specified in SP 800-108 and SP 800-56C”
- SP 800-56C (§5.1): “[RFC 5869] specifies a version of the above extraction-then-expansion key-derivation procedure using HMAC for both the extraction and expansion steps.”
- pqc-forum (2024/10/11): “NIST intends to allow all key-derivation methods in NIST SP 800-56C to apply to the outputs of the ML-KEM key establishment scheme specified in FIPS 203.”
- Why SHA-256? SP 800-57pt1r5 (Table 3): SHA-256 is sufficient for 256 bits of security in a KDF

Next

- Fix private key examples
- Depends on draft-ietf-lamps-kyber-certificates
- ~~WGLC~~