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

IETF LAMPS 119

draft-ietf-lamps-cms-kyber-03

Daniel Van Geest (CryptoNext Security)
Julien Prat (CryptoNext Security)
Mike Ounsworth (Entrust)

March 2024
• Significant restructuring/rewrite to mirror rfc5990bis
• Fully aligned with draft-ietf-lamps-cms-kemri
• Replace Kyber with ML-KEM
• Made KMAC the MTI KDF because ML-KEM uses SHA3-* and SHAKE* under the covers
• Security Considerations
• Hackathon Artifacts
• AES256-WRAP is strictly stronger than necessary for ML-KEM-768 (AES-192 not as widely deployed)
• MUST support KMAC.
  • **NO** customization label. KEM shared secret is not reused
  • Every security level of ML-KEM uses SHA3-* and SHAKE* under the covers.
  • “What about implementations that don’t support Keccak at the CMS level?”
  • “Keccak is required at the crypto level, what about implementations that want minimal complexity?”
Section 1.4 CMS KEMRecipientInfo Processing Summary

- Basically a clone of section 1.3 of rfc5990bis
- During author’s review it was pointed out this could be confusing. It’s just a rehashing of Section 2 of draft-ietf-lamps-cms-kemri
- Should this section be removed from draft-ietf-lamps-cms-kyber (and draft-ietf-lamps-rfc5990bis)?
• NIST ML-KEM OIDs
• Encoding Examples
• Remove section 1.4?
• Harmonize Security Considerations with *draft-ietf-lamps-kyber-certificates*. Feel free to steal some of our text and we’ll remove it and reference yours.
• ASN.1 Module:
  • SmimeCaps
  • KEM-ALGORITHM (*draft-ietf-lamps-kyber-certificates* please)
Thank you!

Daniel VAN GEEST
daniel.vangeest@cryptonext-security.com

contact@cryptonext-security.com
www.cryptonext-security.com
https://www.linkedin.com/company/cryptonext-security

THE NEW GENERATION OF QUANTUM RESISTANT AND SOVEREIGN CRYPTOGRAPHY