Use of FrodoKEM in the Cryptographic Message Syntax (CMS)

draft-chen-lamps-cms-frodokem-00

Presented by: Meiling Chen, Guilin Wang

Session: IETF 125, LAMPS WG

Background & Motivation

The Problem:

- Existing key transport algorithms in CMS (e.g., RSA-KEM) are not resistant to attacks from large-scale quantum computers.
- There is an urgent need to integrate Post-Quantum Cryptography (PQC) into CMS to ensure long-term data confidentiality.

Why FrodoKEM?

- Conservative & Robust Choice: Based on the standard Learning With Errors (LWE) problem, a well-studied basis for security.
- Standardization Momentum: One of three KEMs undergoing ISO standardization, indicating maturity and industry consensus.
- Platform Flexibility:
  - AES variants: Optimized for devices with AES hardware acceleration (e.g., Intel AES-NI).
  - SHAKE variants: Offer competitive performance on platforms without hardware acceleration (e.g., embedded systems, general-purpose CPUs).

Goal of this Draft:

- To define clear specifications for using 8 variants of FrodoKEM (Security Levels 3 & 5).
- To leverage the KEMRecipientInfo structure from RFC 9629 for seamless integration into the existing CMS framework.

Technical Solution: FrodoKEM in CMS

Core Mechanism: Leverages the KEMRecipientInfo structure from RFC 9629.

```
KEMRecipientInfo ::= SEQUENCE {
    version             CMSVersion,  -- MUST be 0
    rid                 RecipientIdentifier,
    kem                 KEMAlgorithmIdentifier,
    kemct               KEMCiphertext,
    kdf                 KeyDerivationAlgorithmIdentifier,
    kekLength           KeyLength,
    ukm                 UserKeyingMaterial OPTIONAL,
    wrap                KeyEncryptionAlgorithmIdentifier,
    encryptedKey        EncryptedKey
}
```

Conventions for FrodoKEM:

- kem (KEM Algorithm):
  - One of the 8 FrodoKEM OIDs defined in this document.
- kdf (Key Derivation Function):
  - MUST support: id-alg-hkdf-with-sha256 (HKDF [RFC5869]).
- wrap (Key Wrap Algorithm):
  - MUST support:
    - For FrodoKEM-976 (192-bit security): id-aes192-wrap ([RFC3394]).
    - For FrodoKEM-1344 (256-bit security): id-aes256-wrap ([RFC3394]).

Security Strength Alignment:

Security Strength	FrodoKEM Algorithm	KDF Preimage Strength	Symmetric Key Strength
192-bit	(e)FrodoKEM-976	192-bit	192-bit
256-bit	(e)FrodoKEM-1344	256-bit	256-bit

Algorithm Variants & Identifiers (OIDs)

8 FrodoKEM Variants Covered:

- Aligns with ISO standardization progress (NIST Security Levels 3 & 5 only).
- Includes both standard (long-term key) and ephemeral (short-term key) modes.

Algorithm Name	Security Level	OID Suffix
id-kem-frodokem976-shake	3	{ frodokem 1 }
id-kem-efrodokem976-shake	3	{ frodokem 3 }
id-kem-frodokem976-aes	3	{ frodokem 5 }
id-kem-efrodokem976-aes	3	{ frodokem 7 }
id-kem-frodokem1344-shake	5	{ frodokem 2 }
id-kem-efrodokem1344-shake	5	{ frodokem 4 }
id-kem-frodokem1344-aes	5	{ frodokem 6 }
id-kem-efrodokem1344-aes	5	{ frodokem 8 }

Related Specifications:

•Public Keys in Certificates: Follows conventions in draft-smyslov-lamps-frodokem-certificates [I-D.S26].

•S/MIME Capabilities: Implementations MAY include these OIDs in the SMIMECapabilities attribute to advertise support.

Summary & Next Steps

Summary:

① **Provides a Solution**: This draft offers a clear specification for using the quantum-resistant FrodoKEM in CMS.

② **Reuses Existing Framework**: Builds upon RFC 9629 KEMRecipientInfo, ensuring an easy adoption path.

③ **Defines Clear Parameters**: Mandates specific KDF (HKDF-SHA256) and key wrap (AES-192/256 Wrap) algorithms for interoperability.

④ **Establishes Identifiers**: Provides the necessary OIDs for all 8 specified FrodoKEM variants.

⑤ **Aligns with Standards**: Follows ongoing ISO standardization efforts, making it a stable and reliable choice for deployment.

Next Steps:

① Solicit feedback and comments from the working group.

② Address any open issues or concerns.

Thank You!

Questions & Discussion?