Key Encapsulation Mechanisms (KEM) in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-cms-kemri-00

Russ Housley, John Gray, and Tomofumi Okubo

LAMPS WG at IETF 116

March 2023

Key Encapsulation Mechanisms (KEM)

Every KEM has these three functions:

- KeyGen() -> (pk, sk)

  Generate the public key (pk) and a private key (sk)

- Encapsulate(pk) -> (ct, ss)

  Given the recipient's public key (pk), produce a ciphertext (ct) to be passed to the recipient and shared secret (ss) for the originator.

- Decapsulate(sk, ct) -> ss

  Given the private key (sk) and the ciphertext (ct), produce the shared secret (ss) for the recipient.

KEM Overview – The Originator

1. The content-encryption key (CEK) is generated at random.
2. The key-encryption key (KEK) is established for each recipient:
    a) The recipient's public key is used with the Encapsulate() function to obtain a pairwise shared secret and the ciphertext for the recipient.
    b) The key-derivation function is used to derive a pairwise KEK from the pairwise shared secret and other data that is send in the clear.
    c) The KEK is used to encrypt the CEK for this recipient.
3. The CEK is used to encrypt the content for all recipients.

KEM Overview – The Recipient

1. The recipient's private key and the ciphertext are used with the Decapsulate() function to obtain a pairwise shared secret.
2. The key-derivation function is used to derive a pairwise KEK from the pairwise shared secret and other data that is send in the clear.
3. The KEK is used to decrypt the CEK.
4. The CEK is used to decrypt the content.

KEM Recipient Information

```
KEMRecipientInfo ::= SEQUENCE {
   version CMSVersion,  -- always set to 0
   rid RecipientIdentifier,
   kem KEMAlgorithmIdentifier,
   kemct OCTET STRING,
   kdf KeyDerivationAlgorithmIdentifier,
   kekLength INTEGER (1..MAX),
   ukm [0] EXPLICIT UserKeyingMaterial OPTIONAL,
   wrap KeyEncryptionAlgorithmIdentifier,
   encryptedKey EncryptedKey }
```

Note that rfc5990bis shows that the structure works for RSA-KEM.
We believe it works for all KEMs.

Please Review

The I-D was recently adopted by the LAMPS WG

- Please review the draft
- rfc5990bis shows that the structure works
- rfc4210bis is making use of this structure
- Composite KEM is making use of this structure
- Please send comments to the mail list

- Tim will make all LAMPS WG consensus calls related to this document