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

draft-ietf-lamps-cms-kemri-06

Russ Housley, John Gray, and Tomofumi Okubo

LAMPS WG at IETF 118

November 2023

KEMRecipientInfo

```
id-ori-kem OBJECT IDENTIFIER ::= { id-ori 3 }

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.

KEM Recipient Info Status

- IESG State is Waiting for AD Go-Ahead::External Party
- All issues were resolved on the mail list, except possibly one
- Falko Strenzke and Johannes Roth posted a message about a new attack: *Inverse CBC Decryption Oracle Attack on Low Entropy AEAD Blocks in CMS*
  - One solution is to add the content-encryption algorithm identifier to the CMSORIforKEMOtherInfo structure
  - This only mitigates this attach for KEM recipients
  - Prefer to explore solutions that mitigate this attack for all RecipientInfo flavors

Is it ready for the RFC Editor?

- Does the desire to seek solutions for all RecipientInfo flavors text represent consensus of the LAMPS WG?

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