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

draft-ietf-lamps-cms-kemri-02

Russ Housley, John Gray, and Tomofumi Okubo
LAMPS WG at IETF 117
July 2023
KEMRecipientInfo

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

KEMRecipientInfo ::= SEQUENCE {
  version CMSVersion,  -- always set to 0
  rid RecipientIdentifier,
  kem KEMAChallenge AlgorithmIdentifier,
  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 (1 of 2)

• WG Last Call ended on 14 July 2023
• All issues were resolved on the mail list, except possibly one
• Current document contains compromise between two positions:
  – Mike Jenkins pointed out that if a recipient only supports KEM algorithms that do not need a ukm, then their implementation need not support the presence of a ukm
  – David von Oheimb points out that greater interoperability will be achieved if the recipient is able to handle the ukm in the info structure in all cases
KEM Recipient Info Status (2 of 2)

• Current text about the optional ukm:

ukm is optional user keying material. When the ukm value is provided, it is used as part of the info structure described in Section 5 to provide a context input to the key-derivation function. For example, the ukm value could include a nonce, application-specific context information, or an identifier for the originator. A KEM algorithm may place requirements on the ukm value. Implementations that do not support the ukm field SHOULD gracefully discontinue processing when the ukm field is present. Note that this requirement expands the original purpose of the ukm described in Section 10.2.6 of [RFC5652]; it is not limited to being used with key agreement algorithms.
Is it ready for the IESG?

• Does the compromise text represent consensus of the LAMPS WG?
• If not, what needs to change to reach consensus?

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