Use of Post-Quantum KEM in the Cryptographic Message Syntax (CMS)

IETF LAMPS 113

draft-perret-prat-lamps-cms-pq-kem

Julien Prat, Ludovic Perret (CryptoNext Security)
Mike Ounsworth (Entrust)

MARCH 2022
TABLE OF CONTENTS

1. Design Rationales
2. KEM-TRANS mechanism - Definition
3. KEM-TRANS mechanism – Use in CMS
4. Open Points
RFC Purpose:
Define how to use a Key Encapsulation Mechanism algorithm (KEM) within the Cryptographic Message Syntax (CMS)

CMS Context:
One of the typical use case of the CMS Enveloped-Data Content is to:
1. randomly generate a CEK,
2. encrypt the data with a symmetric algorithm using this CEK
3. individually send the CEK to one or more recipients protected by asymmetric cryptography in a RecipientInfo object.

Requirements:
Need to define a new Key Transport mechanism fulfilling the following requirements:
• the Key Transport Mechanism SHALL be secure against quantum computers.
• the Key Transport Mechanism SHALL be able to take the Content-Encryption Key (CEK) as input.

=> Definition of the KEM-TRANS mechanism
A key encapsulation mechanism (KEM) is an asymmetric cryptographic algorithm allowing secret sharing between two entities.

KEM consisting of 3 functions:
• Key generation **KeyGen()**:  
  • Returns a public key and a private key (PK, SK)
• Encapsulation **Encaps(PK)**:
  • Takes as input the public key
  • Returns a ciphertext CT and a shared secret SS
• Decapsulation **Decaps(SK, CT)**:
  • Takes as input the private key and the ciphertext
  • Returns the shared secret SS

=> Impossible to encrypt a fixed CEK with KEM
A key derivation function (KDF) is a cryptographic algorithm that derives one or more secret keys from a
secret value using a pseudorandom function.

KDF consists of 1 function:
• Key Derivation Derive(SS, KEK_LEN):
  • Takes as input a shared secret SS and the length of the output secret key KEK_LEN
  • Returns a secret key KEK
A wrapping algorithm (WRAP) is a symmetric cryptographic algorithm protecting data in confidentiality and in integrity.

WRAP consists of 2 functions:

• Wrapping $\text{Wrap}(\text{KEK}, \text{K})$:
  • Takes as input a wrapping key KEK and a plaintext key K
  • Returns a wrapped key WK

• Unwrapping $\text{Unwrap}(\text{KEK}, \text{WK})$:
  • Takes as input a wrapping key KEK and a wrapped key WK
  • Returns the plaintext key K
KEM-TRANS mechanism - Description

Assumptions:
Sender has been provided with:
• \textit{recipPubKey}: the recipient's public key for KEM.
• \textit{K}: the keying data to be transported, length is compatible with the chosen WRAP algorithm.

Sender's operations:
1. \((SS, CT) = \text{KEM.encaps}(\text{recipPubKey})\)
2. \(\text{KEK} = \text{KDF.derive}(SS, \text{kekLen})\)
3. \(\text{WK} = \text{WRAP.wrap}(\text{KEK}, K)\)
4. \(\text{EK} = (\text{WK} \mid \mid CT)\)

Recipient's operations:
1. \((\text{WK} \mid \mid CT) = EK\)
2. \(SS = \text{KEM.decaps}(\text{recipPrivKey}, CT)\)
3. \(\text{KEK} = \text{KDF.derive}(SS, \text{kekLen})\)
4. \(K = \text{WRAP.Unwrap}(\text{KEK}, \text{WK})\)

\(\Rightarrow\) KEM-TRANS mechanism allows the transport of any keying data, including CMS CEK
\(\Rightarrow\) KEM-TRANS mechanism can be instantiated with any KEM algorithm, including a Quantum-Safe KEM, making the KEM-TRANS mechanism Quantum-Safe
RecipientInfo Conventions:
• RecipientInfo Type MUST be KeyTransRecipientInfo
• KeyTransRecipientInfo value MUST have the following values:
  • keyEncryptionAlgorithm.algorithm MUST be id-kem-trans OID (KEM-TRANS mechanism)
  • keyEncryptionAlgorithm.parameters MUST be a value of type GenericHybridParameters
  • encryptedKey MUST be the encrypted keying data (EK) output by the KEM-TRANS Mechanism

Certificate Conventions:
• Key Usage Extension MUST contain only the value *keyEncipherment*
• Subject Public Key Info MUST be set to *id-alg-xxx-kem* OID (KEM algorithm)
RecipientInfo Conventions:
3 possibilities to communicate info:
• Use KeyTransRecipientInfo (as it is done in RSA-KEM and in here)
• Define in this RFC a KemRecipientInfo as instance of OtherRecipientInfo
• Define in this RFC a new top-level KemRecipientInfo

Certificate Conventions:
Depend on the work item PQC-PKIX

New OIDs to be defined:
• id-kem-trans (KEM-TRANS mechanism)
• Several id-alg-xxx-kem (all the KEM algorithms)

Algorithm limitations:
• Choice of KEM
• Choice of KDF
• Choice of WRAP
Thank you!

Ludovic PERRET
ludovic.perret@cryptonext-security.com

Julien PRAT
julien.prat@cryptonext-security.com

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