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

draft-ietf-lamps-cms-kemri-08

Russ Housley, John Gray, and Tomofumi Okubo

LAMPS WG at IETF 119

March 2024

KEM Recipient Info Status

- Since last IETF, the document was temporarily bounced back into the working group due to discussions on whether to including the cipherText as input to the KDF.
  - Ultimately no changes were made to the document other than to highlight the required security properties of the KEM algorithm in the introduction section. A more detailed discussion of these properties was already contained in the security considerations section.

- The document has now progressed in the RFC Editors Queue