Use of the RSA-KEM Algorithm in the Cryptographic Message Syntax (CMS)

draft-ietf-lamps-rfc5990bis-08

Russ Housley & Sean Turner

LAMPS WG

24 July 2024

It is in the RFC Editor Queue, but

- IANA noticed that RFC 5990 is the reference for the id-alg-rsa-kem object identifier, and rfc5990bis needs become the reference
- A developer noticed that the document did not explicitly say that the output of the KDF MUST be the side of the KEK
- Expect an update to resolve these in the next day or two