PQ/T Hybrid KEM: HPKE with JOSE/COSE

Tirumaleswar Reddy.K , Hannes Tschofenig

draft-reddy-cose-jose-pqc-hybrid-hpke-03

Content

Name	Description
HPKE-Base-X25519MLKEM768-SHA256-AES256GCM	Cipher suite for COSE-HPKE in Base Mode that uses the X25519MLKEM768 Hybrid KEM, the HKDF-SHA256 KDF, and the AES-256-GCM AEAD.
HPKE-Base-X25519MLKEM768-SHA256-ChaCha20Poly1305	Cipher suite for COSE-HPKE in Base Mode that uses the X25519MLKEM768 Hybrid KEM, the HKDF-SHA256 KDF, and the ChaCha20Poly1305 AEA

Adopt?