JOSE HPKE

draft-ietf-jose-hpke-encrypt

Tirumaleswar Reddy, **Hannes Tschofenig**, Aritra Banerjee, Orie Steele, Michael Jones

IETF 120 Vancouver
Nov 2024

What does it do ?

- Adds new JSON Web Encryption Algorithms based on the popular HPKE algorithm
  - HPKE is a variant of a public key encryption algorithm offering a Key Encapsulation Construction (KEM)
  - HPKE has been designed for use with traditional crytographic primitives. Extensions being made for hybrid and for PQC support.
- Specifies JSON and Compact serializations
- Supports single and multiple recipients with
  - Integrated Encryption
  - Key Encryption

Call topic number 1 (Yes / No)
HPKE JWE Integrated Encryption Mode

- The "alg" algorithm name will be fully-specified of the form "HPKE-P256-SHA256-A128GCM".
- The "enc" value will be "dir".
- This algorithm operates on the plaintext in this mode.
- The draft will explain what "enc:dir" means, and how it related to "alg", including updating RFC7516 Section 4.1.2 as needed.

Call topic number 2 (Yes / No)
HPKE JWE Key Encryption Mode

- It is similar to Key Agreement with ECDH-ES
- The "alg" algorithm name SHALL be of the form "HPKE-P256-SHA256-A128GCM".
- This algorithm operates on the Content Encryption Key (CEK) in this mode.
- The "enc" value SHALL be any registered AEAD here - https://www.iana.org/assignments/jose/jose.xhtml, per section of RFC 7518.

For both modes call topic number 3 (Yes / No):

- The hpke-aad will be from JWE Section 5.1 step 14.
- By default, HPKE setup info is empty.
- When apu / apv are present, the HPKE setup info will carry the JOSE context-specific data defined in Section 4.6.2 of [RFC7518].

Comments and suggestions are welcome