Use of HPKE with JOSE

draft-rha-jose-hpke-encrypt-01
IETF 118, Nov 2023

Tiru Reddy (Nokia)
Hannes Tschofenig
Aritra Banerjee (Nokia)
Orie Steele (Transmute)
Michael B. Jones
Problem

• HPKE (Hybrid Public Key Encryption) emerged in the IETF as the prominent public key encryption scheme
  ➢ [https://datatracker.ietf.org/doc/rfc9180/](https://datatracker.ietf.org/doc/rfc9180/) (CFRG at IRTF)
  ➢ Used by several protocols Oblivious HTTP, Encrypted Client Hello in TLS, MLS

*JOSE based version of HPKE aligns with the work done in COSE*
Overview

• The HPKE specification provides a variant of public key encryption of arbitrary-sized plaintexts for a recipient public key.

• This specification utilizes HPKE as a foundational building block.

• Use of HPKE with JOSE
Ciphersuite Registration

• The Ciphersuite approach was finalised for the COSE HPKE draft rather than the A-la-carte approach

• HPKE-<Mode>-<KEM>-<KDF>-<AEAD>
  ➢ Three authenticated variants including PSK, Auth, and Auth_psk are defined in HPKE

• The "KEM", "KDF", and "AEAD" values are taken from the HPKE IANA registry (Hybrid Public Key Encryption (HPKE) (iana.org))
Example HPKE Computation

- HPKE-Base-P256-SHA256-AES128GCM
  - KEM: DHKEM(P-256, HKDF-SHA256)
- KDF: HKDF-SHA256
- AEAD: AES-128-GCM
- Mode: Base
- payload: "This is the content"
- aad: ""
Example HPKE Computation (Cont.)

- Protected JWE header for direct key agreement

```json
{
  "alg": "HPKE-Base-P256-SHA256-AES128GCM",
  "kid": "7",
  "encapsulated_key": "BIxvdeRjp3MILzyw06cBNIpXjGeAq6ZYZGaCqa9ykd_Cd-yTw9WHB4GChsEJeCVFczjcPcr_Nn4pUTQunbMNNwOc",
}
```
HPKE Encryption with SealBase

- Direct and Key Wrapping mode for key agreement are supported

- HPKE SealBase(pkR, info, aad, pt) encrypts a plaintext pt using a recipient's public key (pkR)

- In Direct Key Agreement mode, the plaintext "pt" passed into SealBase is the content to be encrypted

- In Key Agreement with Key Wrapping mode, the plaintext "pt" passed into SealBase is the CEK
HPKE Decryption with OpenBase

- The recipient will use HPKE OpenBase(enc, skR, info, aad, ct) function with the enc: "encapsulated_key" and the ct: "ciphertext" received from the sender.

- The "aad" and the "info" parameters are constructed from JWE AAD and JOSE context, respectively.
• Comments and suggestions are welcome

• Consider for WG adoption