Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)

draft-ietf-cose-hpke

Hannes Tschofenig, Orie Steele, Daisuke Ajitomi, Laurence Lundblade

IETF 124
Montréal, November 2025

Changes since Madrid IETF Meeting

- Reflected discussion at the last IETF meeting regarding the "info" parameter for the Recipient_structure (in case of Key Encryption Mode)
  - This is a normative change
- Updated examples based on two implementations (Daisuke & Hannes)
  - https://github.com/hannestschofenig/t_cose/tree/new_hpke
  - https://github.com/dajiaji/python-cwt/pull/638
- Clarified that only one-shot APIs are supported.
- References RFC 9180 and not draft-ietf-hpke-hpke
- Improved the description of the Recipient_structure
- Removed COSE_Mac support

Next Steps

- One (trivial) open issue:
  - Define the HPKE-7 algorithm, corresponding to https://www.ietf.org/archive/id/draft-ietf-jose-hpke-encrypt-14.html#name-hpke-7

    in the JOSE HPKE specification.
- Request to issue WGLC next week