COSE HPKE
draft-ietf-cose-hpke-04

Hannes Tschofenig, Brendan Moran

IETF #116 – Yokohama, March 2023
Progress

• Since IETF#115 (London) two new draft versions have been published.

• draft-ietf-cose-hpke-03
  • Big change based on months of mailing list discussion.
  • Introduction of encapsulated_key array containing the kem id, kdf id, aead id and the encapsulated key
  • Delegated algorithm registration to the HPKE IANA registry.
  • Only need to register HPKE-v1-BASE and encapsulated_key header alg parameter

• draft-ietf-cose-hpke-04
  • Terminology change with "encapsulated_key" to "sender_info"
  • Improved description regarding additional authenticated data.
  • Served as foundation for the hackathon.
Hackathon Report

• Participants:
  • Laurence Lundblade
  • Daisuke Ajitomi
  • Hannes Tschofenig

• Implemented and tested functionality:
  • T_cose can create and verify a two-layer COSE_Encrypt as in draft -04.
  • python_cwt can verify what was created by t_cose.
  • python-cwt has complied with draft-04 except for handling the info parameter (Section 4.4).

• Code available at:
  • https://github.com/laurencelundblade/t_cose/tree/dev
  • https://github.com/dajiaji/python-cwt/pull/368/files
Open Issues

https://github.com/cose-wg/HPKE/issues

- Support for more than HPKE base mode
- Confidentiality without integrity
- Externally Supplied AAD only processed at layer 0
- Use of HPKE for COSE_Mac
- Empty String for Info Value
- Terminology Updates
Additional Authenticated Data (AAD)

Two Layer Structure

One Layer Structure