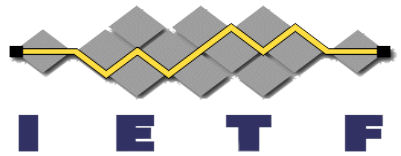
COSE HPKE

draft-ietf-cose-hpke

Hannes Tschofenig, Orie Steele, Ajitomi, Daisuke,
Laurence Lundblade

IETF 119, Brisbane
March 19, 2024



What Does It Do?

- A kind of “Direct Encryption” to a single recipient.
- A kind of “Key Encryption” for symmetric encryption to multiple recipients.

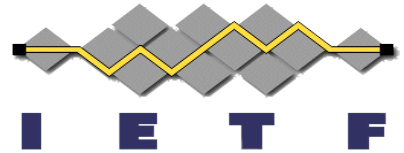
Why Do It?

- HPKE security baseline is better than status quo in COSE.
- HPKE interfaces are friendly to post quantum and hybrid encryption.
- Consistent post quantum encrypted JWT and CWT support.

Status

- Useful discussion – approaching consensus on the following
- Agree to defend against cross-mode attack (described in LAMPS WG in Prague)
- Eliminate use of COSE_KDF_CONTEXT
  - Very confusing, much of it very unnecessary with HPKE
  - Alternate mechanism for useful parts of it
- Define new Enc_Structure for COSE_Recpients that
  - Protects COSE_Recipient headers
  - Addresses cross-mode attack
  - Has useful parts of COSE_KDF_CONTEXT
- Next step is a PR
- Should we align with JOSE HPKE?... Decision Yes (please)

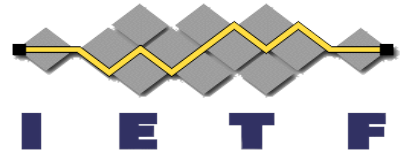
Example: Single Recipient (HPKE Direct Encryption)




```
16([ / Single Recipient Encryption /

   / Protected Headers alg: 35 / h'a1011823',

   { / Unprotected Header /
     / kid / 4: "urn:ietf:params:oauth:ckt:sha-256:KV_398FhP…XBNQM",
     / ek / -4: h'048024424acb…71a9117db7abf19a'
   },

   / Ciphertext / h'693181d2479…64745eceb97f3bbf'
])
```

example from draft-steele-jose-cose-hpke-cookbook

Example: Multiple Recipients (HPKE Key Encryption)




```
96([ / Multiple Recipient Encrypted Message /
   / Protected Headers alg: 1 / h'a10101',
   {
     / IV / 5: h'335552a987fd47dc85016ccc760bb541'
   },
   / Ciphertext / h'a0d7678a14400…1a39c311554970c7bdaa40d4c1',
   [ / Recipients /
     [ / Recipient 0 /
       / Recipient Protected Headers (alg: 35) / h'a1011823',
       { / Recipient Unprotected Header /
         / kid /  4: "urn:ietf:params:oauth:ckt:sha-256:KV_398FhP…0XBNQM",
         / ek  / -4: h'044e73351…45d9dfea583ef14e0f'
       },
     ]
   ]
])
```

example from draft-steele-jose-cose-hpke-cookbook

Next Steps

- Lots of discussions, little progress.
- Should we protect against cross mode attacks caused by AES-CBC? … Decision Yes.
  - Should we define a new Enc_Structure?
    - Use in HPKE AAD? … Decision Yes.
  - Should we define mandatory COSE_KDF_CONTEXT?
    - Use in HPKE Info? … Decision No.
- Should we align with JOSE HPKE?... Decision Yes.