Use of HPKE with COSE

draft-ietf-cose-hpke-07

IETF118, 2023-11-07

H. Tschofenig, O. Steele, D. Ajitomi, L. Lundblade

Status Update

- -06 (2023-10-06)
  - Switched from a-la-carte approach to ciphersuite approach based on the result of the Consensus Call.
    - Introduced *encapsulated_key* parameter instead of *hsi (HPKE Sender Info)* parameter.
    - Defined a ciphersuite naming convention, such as *HPKE-Base-P256-SHA256-AES128GCM*
    - Introduced 16 ciphersuites an as a rough draft. (discuss the details later)
  - Changed authors: +O. Steele, +D. Ajitomi, +L. Laurence, -B. Moran
- -07 (2023-10-22)
  - Re-generated the examples using a draft-06 compliant implementation.
  - Added an example for the COSE_Mac structure.

Status Update

a-la-carte approach (- draft-05)

```
16([
    h'a10120',  // alg = HPKE-v1-BASE
    {
        4: h'3031', // kid
        -4: [       // HPKE_sender_info
            16,     // kem = DHKEM(P-256, HKDF-SHA256)
            1,      // kdf = HKDF-SHA256
            1,      // aead = AES-128-GCM
            h'048c6f75e463a773082f3cb0d3a701348a578c67
              80aba658646682a9af7291dfc277ec93c3d58707
              818286c1097825457338dc3dcaff367e2951342e
              9db30dc0e7',  // enc
        ],
    },
    / encrypted plaintext /
    h'ee22206308e478c279b94bb071f3a5fbbac412a6effe34195f7
      c4169d7d8e81666d8be13',
])
```

merged into the alg value

ciphersuite approach (draft-06 -)

```
16([
    / alg = HPKE-Base-P256-SHA256-AES128GCM (Assumed: 35) /
    h'a1011823',
    {
        / kid /
        4: h'3031',
        / encapsulated_key /
        -4: h'045df24272faf43849530db6be01f42708b3c3a9
              df8e268513f0a996ed09ba7840894a3fb946cb28
              23f609c59463093d8815a7400233b75ca8ecb177
              54d241973e',
    },
    / encrypted plaintext /
    h'35aa3d98739289b83751125abe44e3b977e4b9abbf2c8cfaade
      b15f7681eef76df88f096',
])
```

Remaining Issues: Summary

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

- **Ciphersuite selection**.
  - (#36) Reduce the number of ciphersuites.
- **Context Information Structure**
  - (#24) Externally Supplied AAD only processed at layer 0.
  - (#25) Empty String for Info Value.
  - (#44) COSE_Recpient header protection
- **Key representation**
  - (#35) COSE Elliptic Curve needs to be added for the x25519/Kyber hybrid.
  - (#46) Key reprentation
- **Editorial issues** (improve readability, remove redundancies)
  - (#41) Could reduce restatement of COSE requirements.
  - (#44) Specify in terms of Seal() and Open APIs.

Ciphersuite Selection: Current Draft Status

COSE-HPKE Cipher Suite Label	HPKE KEM	HPKE KDF	HPKE AEAD
HPKE-Base-P256-SHA256-AES128GCM	0x10	0x1	0x1
HPKE-Base-P256-SHA256-ChaCha20Poly1305	0x10	0x1	0x3
HPKE-Base-P384-SHA384-AES256GCM	0x11	0x2	0x2
HPKE-Base-P384-SHA384-ChaCha20Poly1305	0x11	0x2	0x3
HPKE-Base-P521-SHA512-AES256GCM	0x12	0x3	0x2
HPKE-Base-P521-SHA512-ChaCha20Poly1305	0x12	0x3	0x3
HPKE-Base-X25519-SHA256-AES128GCM	0x20	0x1	0x1
HPKE-Base-X25519-SHA256-ChaCha20Poly1305	0x20	0x1	0x3
HPKE-Base-X448-SHA512-AES256GCM	0x21	0x3	0x2
HPKE-Base-X448-SHA512-ChaCha20Poly1305	0x21	0x3	0x3
HPKE-Base-X25519Kyber768-SHA256-AES256GCM	0x30	0x1	0x2
HPKE-Base-X25519Kyber768-SHA256-ChaCha20Poly1305	0x30	0x1	0x3
HPKE-Base-CP256-SHA256-ChaCha20Poly1305	0x13	0x1	0x3
HPKE-Base-CP256-SHA256-AES128GCM	0x13	0x1	0x1
HPKE-Base-CP521-SHA512-ChaCha20Poly1305	0x15	0x3	0x3
HPKE-Base-CP521-SHA512-AES256GCM	0x15	0x3	0x2

Shape the initial ciphersuite list

How should the list be constructed?

A) Adopt the same set of the ciphersuites defined in MLS (Messaging Layer Security).

B) Add some combinations of the DHKEMs with NIST curves and ChaCha20Poly1305 to A).

C) Add some combinations using the DHKEMs with compact NIST curves to B).

D) Add some combinations using a post-quantum hybrid KEM (X25519Kyber768) to C).

- Plan is to go for A + B, i.e.
  - remove the compact NIST curve based DHKEMs, and
  - remove the post-quantum hybrid KEMs.
- Comments?
  - Can always be extended later!

Proposed Ciphersuite List
(green + orange marked list)

- A) **7** ciphersuites from RFC9180 (same as the MLS choices).
  - HPKE-Base-P256-SHA256-AES128GCM (MLS-0x0002)
  - HPKE-Base-P384-SHA384-AES256GCM (MLS-0x0007)
  - HPKE-Base-P521-SHA512-AES256GCM (MLS-0x0005)
  - HPKE-Base-X25519-SHA256-AES128GCM (MLS-0x0001)
  - HPKE-Base-X25519-SHA256-ChaCha20Poly1305 (MLS-0x0003)
  - HPKE-Base-X448-SHA512-AES256GCM (MLS-0x0004)
  - HPKE-Base-X448-SHA512-ChaCha20Poly1305 (MLS-0x0006)
- B) **+3** for adding some combinations with ChaCha20Poly1305.
  - HPKE-Base-{P256-SHA256, P384-SHA384, P521-SHA512}-ChaCha20Poly1305
- C) **+6** for compact NIST curve-based DHKEMs.
  - HPKE-Base-C256-SHA256-AES128GCM
  - HPKE-Base-{C384-SHA384, C521-SHA512}-AES256GCM
  - HPKE-Base-{C256-SHA256, C384-SHA384, C521-SHA512}-ChaCha20Poly1305
- D) **+2** for post-quantum hybrid KEMs
  - HPKE-Base-X25519Kyber768-SHA256-{AES256GCM, ChaCha20Poly1305}

Key Representation


```
{
  "kty": "EC",
  "crv": "P-256",
  "alg": "HPKE-Base-P256-SHA256-AES128GCM",
  "kid": "test-key-42",
  "x": "xXCWZk-jG9Tjd7M361sAEUi8JvKBxFIQgqhqkZa5cgs",
  "y": "y-9jpXy5gNhxl9BV4smqO36MXRlbkrC3PvvjDOrpOgU",
  "use": "enc",
  "key_ops": [
                "deriveBits"
  ]
}
```


Considering to add brief text about how to represent public and private keys for use with HPKE.

Should be non-controversial.

Our Plan

- Handle remaining issues towards draft-08.
- Add more examples / test vectors.
- Get draft-08 ready for WGLC.