

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

draft-ietf-cose-hpke-09

Hannes Tschofenig, Orie Steele, Daisuke Ajitom, Laurence Lundblade

COSE, IETF 120

Status: -09 Version Published

- Significant change in the way context information is being dealt with.
 - Previous versions of the draft used the COSE_KDF_Context as input to the HPKE info parameter, which was used to impact the key generation.
 - -09 now uses a new structure, recipient_structure, which is included in the authenticated data.
- New terminology being used to refer to single layer / multi layer approach, namely HPKE Direct Encryption Mode and HPKE Key Encryption Mode
 - Not aligned with the JOSE version (yet).
- Other items:
 - Reduced list of initially registered ciphersuites
 - Shortened ciphersuite label
 - Rename encapsulated_key to ek
 - Added text for COSE_Key representation
 - Editorial improvements

Example

```
Recipient_structure = [  
    context: "Recipient",  
    next_layer_alg: int/tstr,  
    recipient_protected_header: empty_or_serialize_map,  
    recipient_aad: bstr  
]
```

```
96_0([  
    / alg = AES-128-GCM (1) /  
    h'a10101',  
    {  
        / iv /  
        5: h'b3fb95dde18c6f90a9f0ae55',  
    },  
    / detached ciphertext /  
    null,  
    [  
        [  
            / alg = HPKE-Base-P256-SHA256-A128GCM /  
            h'a1011823',  
            {  
                / kid /  
                4: h'3031',  
                / ek /  
                -4: h'04d97b79486fe2e7b98fb1bd43  
                    c4faee316ff38d28609a1cf568  
                    40a809298a91e601f1cc0c2ba4  
                    6cb67b41f4651b769cafd9df78  
                    e58aa7f5771291bd4f0f420ba6',  
            },  
            / ciphertext containing encrypted CEK /  
            h'24450f54ae93375351467d17aa7a795cfede2  
            c03eced1ad21fcb7e7c2fe64397',  
        ]  
    ],  
])
```

Next Steps

- Getting closer to finalization
- Recompute examples with new version
- Include example parameters in the protected headers