COSE HPKE

draft-ietf-cose-hpke
Status

• At the last IETF meeting we agreed to use the COSE_Key representation.
• The confirmation call on the list was inconclusive, see https://mailarchive.ietf.org/arch/msg/cose/xvKh6WMF1PrRIhG1et5ebIEJCT8/
• Alternative proposal discussed on the mailing list but no conclusion has been reached.
• Next slides show what the new proposals are.
PR#9: Proposal by Daisuke Ajitomi
https://github.com/cose-wg/HPKE/pull/9/files

```
16([
  h'a10120', // alg = HPKE (-1)
  {
    4: h'3031', // kid
    -4: {
      1: 16, // kem = DHKEM(P-256, HKDF-SHA256)
      5: 1, // kdf = HKDF-SHA256
      2: 1, // aead = AES-128-GCM
      3: h'048c...0e7', // enc
    },
  },
]/ ciphertext /
  h'ee22...',
])
```
PR#10: Proposal by Ilari Liusvaara
https://github.com/cose-wg/HPKE/pull/10/files

• Builds on top of Daisuke’s proposal
• Uses an array instead of a map for the HPKE sender information.
  • Prevent extensibility and thereby omit label registry
• Change the name from “HPKE sender info” to “encapsulated_key”
• Proposes to omit the KEM ID and replace it with processing rules for how to “guess” the KEM
Proposal by Ilari Liusvaara, cont.

16([ 
    h'a10120', // alg = HPKE (-1) 
    { 
        4: h'3031', // kid 
        -4: [ // encapsulated_key 
            1, // kdf = HKDF-SHA256 
            1, // aead = AES-128-GCM 
            h'048c...0e7', // enc 
        ], 
    }, 
    /* ciphertext */ 
    h'ee22...', 
])
Next Steps

• Work out the proposal/proposals to have group evaluate