Hybrid Public Key Encryption (HPKE) for COSE

draft-tschofenig-cose-hpke-00

(Russ, Brendan, Hannes)
Background

- The SUIT WG worked on firmware encryption scheme, (which is also used in TEEP).

- Functionality was recently moved into a dedicated document, see https://datatracker.ietf.org/doc/html/draft-ietf-suit-firmware-encryption-02

- We wanted two features:
  - A pre-shared secret-based key encryption □ AES Key Wrap (offered by COSE)
  - Public key encryption scheme □ Also offered by COSE (in form of the ECDH Ephemeral-Static key agreement)

- Everything great but HPKE (Hybrid Public Key Encryption) emerged in the IETF/IRTF as the prominent public key encryption scheme.
  - Already used in several specifications, such as TLS ESNI and MLS.
  - Code for HPKE available!

- Group decided to re-use HPKE.
COSE-HPKE

Layer 3 contains parameters needed to generate a shared secret.
Layer 2 contains the encrypted CEK
Layer 1 contains the encrypted plaintext (unless it is detached)
Ask to the group

We would like the COSE WG to adopt this document.

We believe it is of generic use beyond firmware encryption.
Background Material
HPKE Implementation

• [https://github.com/ARMmbed/mbedtls/pull/5078](https://github.com/ARMmbed/mbedtls/pull/5078)
• Based on Stephen Farrells “HappyKey” code, see [https://github.com/sftcd/happykey](https://github.com/sftcd/happykey).
• HappyKey relies on OpenSSL. Above linked implementation uses the PSA Crypto API and is tailored to constrained devices.
• Code with integration into COSE will be released soon.