Encryption Key Derivation in the COSE using HKDF with SHA-256

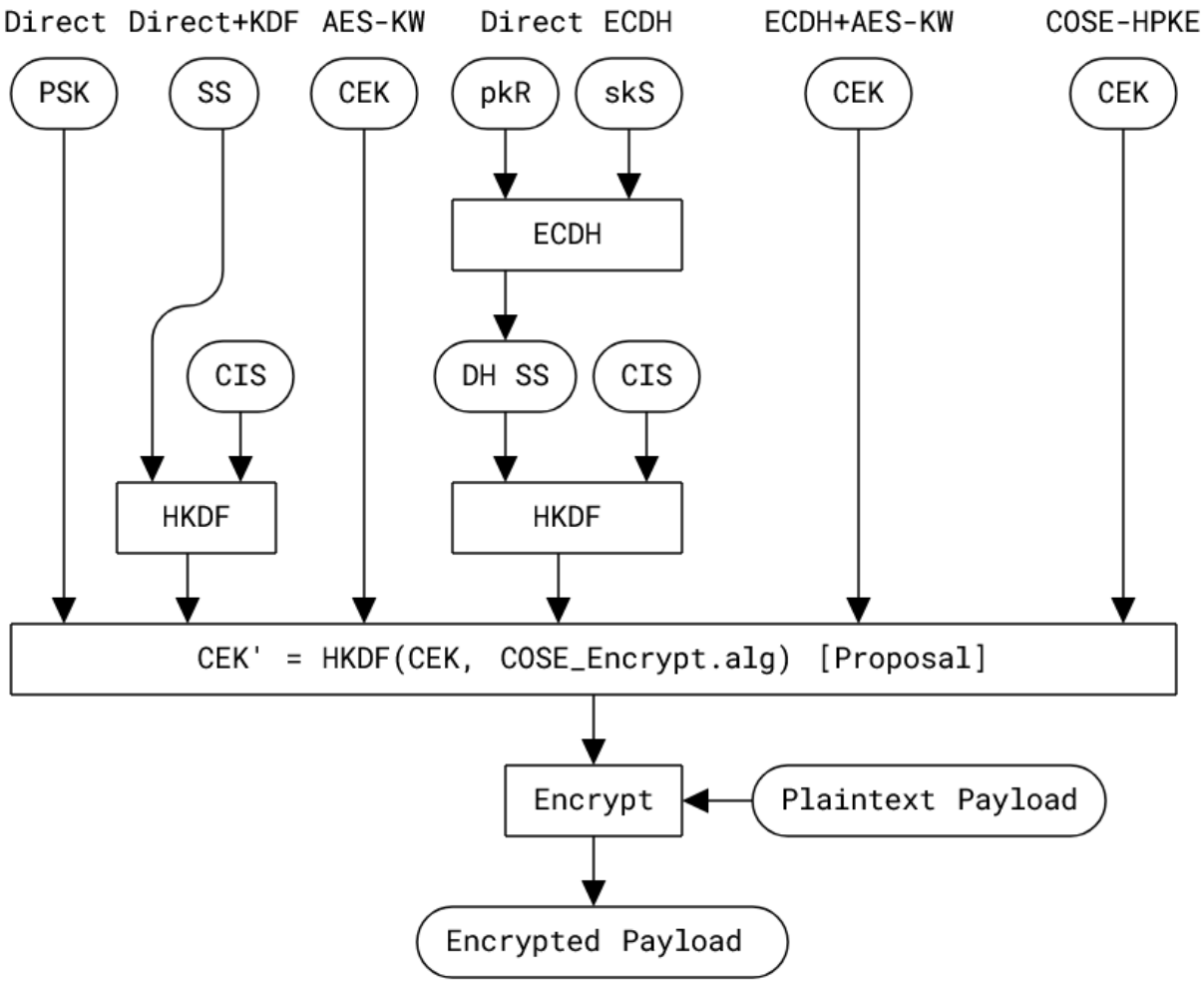
draft-tschofenig-cose-cek-hkdf-sha256

Hannes Tschofenig, Russ Housley, Ken Takayama

COSE, IETF 121

Staus

- Risk of an AEAD to non-AEAD downgrading attack, where an adversary manipulates the content-encryption algorithm identifier.
- To prevent adversary from making the modification, the algorithm identifier has to be included in the key derivation function.
  - Modification of the algorithm then lead to a different CEK be derived.
- Mirrors what is done in LAMPs with I-D.ietf-lamps-cms-cek-hkdf-sha256
  - Additional key derivation step with HKDF on the CEK to produce a new CEK’


Direct
Direct+KDF
AES-KW
Direct ECDH
ECDH+AES-KW
COSE-HPKE
PSK
SS
CEK
pkR
skS
CEK
CEK
ECDH
CIS
DH SS
CIS
HKDF
HKDF
CEK' = HKDF(CEK, COSE_Encrypt.alg) [Proposal]
Encrypt
Plaintext Payload
Encrypted Payload

Asking group for adoption!