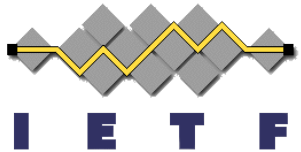
Use of HPKE with JOSE

draft-ietf-jose-hpke-encrypt

Tirumaleswar Reddy, Hannes Tschofenig, Orie Steele,
Aritra Banerjee, Michael B. Jones

IETF 124, Montreal



Updates Since IETF 123

- -14
  - Add HPKE-7
  - Update to Recipient_structure
  - Removed text related to apu and apv.
  - Updated description of mutually known private information.
- -13
  - Switched reference from RFC 9180 to draft-ietf-hpke-hpke
  - Editorial improvements to abstract and introduction.
  - Removed Section 8.2 "Static Asymmetric Authentication in HPKE"
- -12
  - Added the recipient_structure

Use of HPKE info & AAD Parameters

- Changed how HPKE info and AAD parameters are populated
- Incorporates feedback from IETF 123
- Info is now populated with Recipient_structure
- AAD is now empty unless externally provided information is used

Recipient_structure

Recipient_structure = ASCII("JOSE-HPKE rcpt") ||
BYTE(255) ||
ASCII(content_encryption_alg) ||
BYTE(255) ||
recipient_extra_info

- Binds the content encryption algorithm into the HPKE computation
- Enable application to bind additional information into the computation
- Aligned with parallel changes to COSE HPKE

HPKE-7 Algorithm Added

- Algorithm Name: HPKE-7
- Algorithm Description: Cipher suite for JOSE-HPKE using the DHKEM(P-256, HKDF-SHA256) KEM, the HKDF-SHA256 KDF, and the A256GCM AEAD

- Requested by Chanda

Integration with JWE Instructions

- Late breaking development…
- PR #83 defines the JWE Key Management Modes
  - HPKE Integrated Encryption
  - HPKE Key Encryption
- Integrates them into complete set of JWE encryption & decryption instructions
  - This was an ask from IETF 123
  - Was surprisingly straightforward to do
  - JOSE HPKE modes now uses same set of instructions as all other modes
  - Simplified draft by removing HPKE-specific encryption & decryption instructions
- Thanks to Richard Barnes for suggesting this unified approach

Next Steps

- Confer with WG members during IETF 124 about solutions applied
  - Solutions applied in response to feedback received during IETF 123
- Review PR #83 integrating instructions with JWE
  - Filip Skokan, Brian Campbell, and Jospeh Heenan already explicitly invited to review
  - Apply review suggestions and merge
- Then I believe it will be time for second WGLC
  - *Note that COSE HPKE appears to be ready for second WGLC*