Use of HPKE with JOSE

draft-ietf-jose-hpke-encrypt

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

IETF 123, Madrid

Developments Since IETF 122

- Published drafts -07 through -11. Substantive changes were:
  - Use "enc": "int" for integrated encryption
  - Described reasons for excluding authenticated HPKE
  - Mutually known private information MAY be used as the HPKE info value
  - Clarified relationships between steps in spec and those in JWE spec [RFC 7516]
  - Corrected examples
  - Updates RFC 7516 to allow "enc": "int" for signaling use of integrated encryption
- Working Group Last Call for -08 – June 4-20, 2025
  - Active participation by working group members
  - Much of the WGLC feedback addressed in -09 and -10

Use of "enc" updated per feedback at IETF 122

- When "alg" is a JOSE HPKE algorithm
  - If "enc" is “int", HPKE Integrated Encryption is used
  - If "enc" is an AEAD algorithm, the recipient Key Management mode is key encryption
- RFC 7516 updated to allow "enc": "int"

Decisions Needed to Finish

- WGLC feedback contained requests to change representation
- WGLC feedback contained requests to change structure of draft

- These questions should be resolved before second WGLC
  - Next slides ask for decisions on these questions individually

- Also, COSE HPKE received requests for changes on Monday
  - We should thoughtfully coordinate with pertinent COSE HPKE changes

Decision 1:
Update or Obsolete RFC 7516?

- JOSE HPKE currently updates RFC 7516
  - All existing JWE functionality remains in RFC 7516
  - JOSE HPKE specifies deltas to it
- Some reviewers suggested JOSE HPKE obsoleting RFC 7516
  - This would copy all JWE functionality into the JOSE HPKE spec
  - The HPKE functionality would be sprinkled throughout it as needed
- In comparison, OAuth WG decided at IETF 122 to update rather than obsolete RFC 7523
  - So that deltas to it would be easier to understand
- Unless there's clear consensus to obsolete, I would continue to update

Decision 2:
How to signal integrated encryption?

- Drafts have used three different syntaxes over time:
  1. "alg": "dir"
  2. "enc": "dir"
  3. "enc": "int" - current syntax resulting from feedback at IETF 122
- One WGLC reviewer suggested a variant of (1)
  - "alg": "int"

- Unless there’s clear consensus for another option, I would propose leaving syntax as-is

Decision 3:
Define new JWE Key Management Mode?

- One reviewer suggested defining new key management mode
  - Direct Public Key Encryption
    - HPKE Integrated Encryption would be first instance of this new mode
- For context, existing modes are
  - Key Encryption
  - Key Wrapping
  - Direct Key Agreement
  - Key Agreement with Key Wrapping
  - Direct Encryption
- Do people favor generalizing HPKE integrated encryption to define and use this new JWE Key Management Mode?

Next Steps

- I believe once we make those 3 decisions, the path to finish is clear
- Also note we'll need to coordinate with COSE to keep the drafts semantically aligned if COSE HPKE makes semantic changes
    - Please participate in COSE WG as well to help with this coordination

- Apply results of 3 decisions
- Apply results of continued coordination with COSE HPKE
- Second WGLC