Javascript Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 24 October 2026

F. Skokan
Okta
B. Campbell
Ping Identity
H. Tschofenig
UniBw M.
T. Reddy
Nokia

22 April 2026

# JOSE HPKE PQ & PQ/T Algorithm Registrations
draft-skokan-jose-hpke-pq-pqt-04

## Abstract

This document registers Post-Quantum (PQ) and Post-Quantum/Traditional (PQ/T) hybrid algorithm identifiers for use with JSON Object Signing and Encryption (JOSE), building on the Hybrid Public Key Encryption (HPKE) framework.

## About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://panva.github.io/draft-jose-hpke-pq-pqt/draft-skokan-jose-hpke-pq-pqt.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-skokan-jose-hpke-pq-pqt/.

Discussion of this document takes place on the Javascript Object Signing and Encryption Working Group mailing list (mailto:jose@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/jose/. Subscribe at https://www.ietf.org/mailman/listinfo/jose/.

Source for this draft and an issue tracker can be found at https://github.com/panva/draft-jose-hpke-pq-pqt.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

## Copyright Notice



## Table of Contents

## 1. Introduction

[I-D.ietf-jose-hpke-encrypt] defines how to use Hybrid Public Key Encryption (HPKE) with JSON Web Encryption (JWE) using traditional Key Encapsulation Mechanisms (KEM) based on Elliptic-curve Diffie-Hellman (ECDH).

This document extends the set of registered HPKE algorithms to include Post-Quantum (PQ) and Post-Quantum/Traditional (PQ/T) hybrid KEMs, as defined in [I-D.ietf-hpke-pq]. These algorithms provide protection against attacks by cryptographically relevant quantum computers.

The term "PQ/T hybrid" is used here consistent with [I-D.ietf-hpke-pq] to denote a combination of post-quantum and traditional algorithms, and should not be confused with HPKE's use of "hybrid" to describe the combination of asymmetric and symmetric encryption.

## 2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

This document uses the terms "Traditional Algorithm", "Post-Quantum Algorithm", "PQ/T Hybrid Scheme", and "PQ/T Hybrid KEM" as defined in [RFC9794]. The term "pure post-quantum" is used in this document to refer to a single-algorithm scheme using only a post-quantum algorithm, with no traditional component.

## 3. Algorithm Identifiers

This section defines the algorithm identifiers for PQ and PQ/T HPKE-based encryption in JOSE. Each algorithm is defined by a combination of an HPKE KEM, a Key Derivation Function (KDF), and an Authenticated Encryption with Associated Data (AEAD) algorithm.

All algorithms defined in this section follow the same operational model as those in [I-D.ietf-jose-hpke-encrypt], supporting both integrated encryption as defined in Section 5 of [I-D.ietf-jose-hpke-encrypt] and key encryption as defined in Section 6 of [I-D.ietf-jose-hpke-encrypt].

Test vectors for all algorithms defined in this section are provided in Appendix A.

### 3.1. PQ/T Hybrid Integrated Encryption Algorithms

The following table lists the algorithm identifiers for PQ/T hybrid integrated encryption, where HPKE directly encrypts the plaintext without a separate Content Encryption Key:

| "alg" value | HPKE KEM | HPKE KDF | HPKE AEAD |
|---|---|---|---|
| HPKE-8 | MLKEM768-P256 (0x0050) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-9 | MLKEM768-X25519 (0x647a) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-10 | MLKEM1024-P384 (0x0051) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |

Table 1: PQ/T Hybrid Integrated Encryption Algorithms

These algorithms combine ML-KEM with a traditional elliptic curve algorithm in a PQ/T hybrid KEM, with the goal that compromise of either the post-quantum or the traditional component alone does not undermine the security of the resulting encryption.

### 3.2. Pure PQ Integrated Encryption Algorithms

The following table lists the algorithm identifiers for pure post-quantum integrated encryption:

| "alg" value | HPKE KEM | HPKE KDF | HPKE AEAD |
|---|---|---|---|
| HPKE-12 | ML-KEM-768 (0x0041) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-13 | ML-KEM-1024 (0x0042) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |

Table 2: Pure PQ Integrated Encryption Algorithms

These algorithms provide pure post-quantum security using ML-KEM without a traditional algorithm component.

### 3.3. PQ/T Hybrid Key Encryption Algorithms

The following table lists the algorithm identifiers for PQ/T hybrid key encryption, where HPKE encrypts the Content Encryption Key:

| "alg" value | HPKE KEM | HPKE KDF | HPKE AEAD |
|---|---|---|---|
| HPKE-8-KE | MLKEM768-P256 (0x0050) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-9-KE | MLKEM768-X25519 (0x647a) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-10-KE | MLKEM1024-P384 (0x0051) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |

Table 3: PQ/T Hybrid Key Encryption Algorithms

These are the key encryption counterparts of the PQ/T hybrid integrated encryption algorithms defined in Table 1.

### 3.4. Pure PQ Key Encryption Algorithms

The following table lists the algorithm identifiers for pure post-quantum key encryption:

| "alg" value | HPKE KEM | HPKE KDF | HPKE AEAD |
|---|---|---|---|
| HPKE-12-KE | ML-KEM-768 (0x0041) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |
| HPKE-13-KE | ML-KEM-1024 (0x0042) | SHAKE256 (0x0011) | AES-256-GCM (0x0002) |

Table 4: Pure PQ Key Encryption Algorithms

These are the key encryption counterparts of the pure PQ integrated encryption algorithms defined in Table 2.

## 4. JSON Web Key Representation

Keys for the algorithms defined in this document use the "AKP" (Algorithm Key Pair) key type defined in Section 3 of [I-D.ietf-cose-dilithium]. The required "alg" parameter identifies the HPKE ciphersuite as well as whether the key is used for Integrated Encryption or Key Encryption.

The required "pub" parameter contains the SerializePublicKey() output for the corresponding KEM, and for private keys the "priv" parameter contains the SerializePrivateKey() output, both as defined in Section 4 of [I-D.ietf-hpke-hpke]. Both values are base64url-encoded (Section 5 of [RFC4648]) without padding.

Examples of JWKs for each algorithm are provided in Appendix A.

## 5. Security Considerations

The security considerations of [I-D.ietf-jose-hpke-encrypt] and [I-D.ietf-hpke-pq] apply to this document. [I-D.ietf-pquip-pqc-engineers] provides general background on the threat posed by cryptographically relevant quantum computers (CRQCs), the properties of KEMs, and considerations for PQ/T hybrid schemes.

This document does not register algorithms using ML-KEM-512. As noted in Section 3 of [I-D.ietf-hpke-pq], given the relative novelty of ML-KEM, there is concern that new cryptanalysis might reduce the security level of ML-KEM-512. Use of ML-KEM-768 or ML-KEM-1024 acts as a hedge against such cryptanalysis at a modest performance penalty.

The PQ/T hybrid ciphersuites registered by this document are motivated by the PQ/T Hybrid Confidentiality property (Section 5 of [RFC9794], Section 13.1 of [I-D.ietf-pquip-pqc-engineers]): confidentiality is preserved as long as at least one of the component algorithms remains secure. The traditional component protects against unforeseen cryptanalysis of ML-KEM, while the post-quantum component protects against Harvest Now, Decrypt Later (HNDL) attacks (Section 7 of [I-D.ietf-pquip-pqc-engineers]) by a future CRQC. PQ/T hybrid ciphersuites are generally preferred for this reason during the transition to post-quantum cryptography.

The pure PQ ciphersuites are registered to accommodate deployments with regulatory or compliance mandates that require the exclusive use of post-quantum algorithms, such as those governed by the Commercial National Security Algorithm Suite 2.0 [CNSA2.0], as well as deployments where the size or performance overhead of a traditional component is undesirable.

When the Key Encryption algorithms defined in Table 3 or Table 4 are used in a General JWE JSON Serialization with multiple recipients, all recipients MUST use a quantum-resistant Key Management algorithm. Including a recipient that uses an algorithm that is not quantum-resistant would allow an adversary performing an HNDL attack to recover the Content Encryption Key once a CRQC becomes available; see Section 15.4 of [I-D.ietf-pquip-pqc-engineers].

### 5.1. Security Strength

Ciphersuites based on ML-KEM-768 target NIST post-quantum security level 3; those based on ML-KEM-1024 target security level 5 (see Section 11 of [I-D.ietf-pquip-pqc-engineers]). In the PQ/T hybrid ciphersuites, the traditional component provides an additional classical security floor: P-256 and X25519 offer approximately 128-bit classical security, while P-384 offers approximately 192-bit classical security. The -KE variants share the same cryptographic properties as their integrated encryption counterparts.

All ciphersuites use SHAKE256 as the KDF, aligning with the hash family used internally by ML-KEM. They also use AES-256-GCM as the AEAD. As discussed in Section 3.1 of [I-D.ietf-pquip-pqc-engineers], symmetric primitives are only modestly affected by quantum attacks and doubling key sizes is not strictly required; AES-256-GCM is nonetheless selected to provide a comfortable margin consistent with security level 5 parameter sets and with contemporary guidance such as [CNSA2.0]. AES-256-GCM is used as the sole AEAD to minimize the number of ciphersuites and reduce implementation complexity; its widespread hardware acceleration and broad deployment make it a reasonable single choice for all ciphersuites defined in this document.

## 6. IANA Considerations

### 6.1. JSON Web Signature and Encryption Algorithms Registry

This document requests registration of the following values in the IANA "JSON Web Signature and Encryption Algorithms" registry established by [RFC7518]:

Note: The Algorithm Name numbering has intentional gaps so that a given identifier always denotes the same HPKE KEM, KDF, and AEAD combination regardless of whether it is used in JOSE or COSE. The gaps correspond to algorithms registered only in COSE for COSE-specific needs that do not apply to JOSE.

#### 6.1.1. HPKE-8

* Algorithm Name: HPKE-8
* Algorithm Description: Integrated Encryption with HPKE using MLKEM768-P256 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): Table 1 of this document
* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.2. HPKE-8-KE

* Algorithm Name: HPKE-8-KE
* Algorithm Description: Key Encryption with HPKE using MLKEM768-P256 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): Table 3 of this document
* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.3. HPKE-9

* Algorithm Name: HPKE-9
* Algorithm Description: Integrated Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): Table 1 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.4. HPKE-9-KE

* Algorithm Name: HPKE-9-KE
* Algorithm Description: Key Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): Table 3 of this document
* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.5. HPKE-10

* Algorithm Name: HPKE-10
* Algorithm Description: Integrated Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF
* Specification Document(s): Table 1 of this document
* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.6. HPKE-10-KE

* Algorithm Name: HPKE-10-KE
* Algorithm Description: Key Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and AES-256-GCM AEAD
* Algorithm Usage Location(s): "alg"
* JOSE Implementation Requirements: Optional
* Change Controller: IETF

* Specification Document(s): Table 3 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.7. HPKE-12

* Algorithm Name: HPKE-12

* Algorithm Description: Integrated Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): Table 2 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.8. HPKE-12-KE

* Algorithm Name: HPKE-12-KE

* Algorithm Description: Key Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): Table 4 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.9. HPKE-13

* Algorithm Name: HPKE-13

* Algorithm Description: Integrated Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): Table 2 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

#### 6.1.10. HPKE-13-KE

* Algorithm Name: HPKE-13-KE

* Algorithm Description: Key Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and AES-256-GCM AEAD

* Algorithm Usage Location(s): "alg"

* JOSE Implementation Requirements: Optional

* Change Controller: IETF

* Specification Document(s): Table 4 of this document

* Algorithm Analysis Document(s): [I-D.ietf-hpke-pq]

## 7. References

### 7.1. Normative References

[I-D.ietf-cose-dilithium]
Prorock, M. and O. Steele, "ML-DSA for JOSE and COSE", Work in Progress, Internet-Draft, draft-ietf-cose-dilithium-11, 15 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-dilithium-11>.

[I-D.ietf-hpke-hpke]
Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-03, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-03>.

[I-D.ietf-hpke-pq]
Barnes, R. and D. Connolly, "Post-Quantum and Post-Quantum/Traditional Hybrid Algorithms for HPKE", Work in Progress, Internet-Draft, draft-ietf-hpke-pq-04, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-04>.

[I-D.ietf-jose-hpke-encrypt]
Reddy.K, T., Tschofenig, H., Banerjee, A., Steele, O., and M. B. Jones, "Use of Hybrid Public Key Encryption (HPKE) with JSON Web Encryption (JWE)", Work in Progress, Internet-Draft, draft-ietf-jose-hpke-encrypt-16, 16 February 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-jose-hpke-encrypt-16>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/rfc/rfc4648>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

## 7.2. Informative References

[CNSA2.0] National Security Agency, "Announcing the Commercial National Security Algorithm Suite 2.0", May 2025, <https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF>.

[I-D.ietf-pquip-pqc-engineers]
Banerjee, A., Reddy.K, T., Schoinianakis, D., Hollebeek, T., and M. Ounsworth, "Post-Quantum Cryptography for Engineers", Work in Progress, Internet-Draft, draft-ietf-pquip-pqc-engineers-14, 25 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-pquip-pqc-engineers-14>.

[RFC7518] Jones, M., "JSON Web Algorithms (JWA)", RFC 7518, DOI 10.17487/RFC7518, May 2015, <https://www.rfc-editor.org/rfc/rfc7518>.

[RFC9794] Driscoll, F., Parsons, M., and B. Hale, "Terminology for Post-Quantum Traditional Hybrid Schemes", RFC 9794, DOI 10.17487/RFC9794, June 2025, <https://www.rfc-editor.org/rfc/rfc9794>.

## Appendix A. Test Vectors

This appendix provides test vectors for each algorithm defined in this document. For each algorithm, a private JWK, a Flattened JWE JSON Serialization example with Additional Authenticated Data, and a JWE Compact Serialization example are provided.

### A.1. HPKE-8


```
{
  "kty": "AKP",
  "alg": "HPKE-8",
  "kid": "DmOWQi-VwrjZWjO6mQQWdv3CJ_v9k_PH3vS7S0xoah8",
  "pub": "6XRnIatC1KtI7DZlj8ISDxZvtsFeBOPKQETMRRYb45dR0kw6TDSb8UMXHHWhUBdbEBof5gvIJacZ
G4exGku4JsysQcc9AVR6Ydih7kaPNQgCiiKw9QACNCMWx2p171RVCpGSFoOwaejNGZeNJKS4jqulOWFQHGtbWhl64
HZzlkZMxhqdA-EecEOLhzCkbCMMtXxb-cxUVkOxQpKkO5ofmEaKH7tjyNZyVsxqgUZFn6K8jOq9g6GCOEG4awGB6A
ZC72yNXLDBnVCy_7OMn2bAeos8AvhHkbsL0hsFFjsnWcG_IYvNPzUAcyGZlpsqjXJIh4AUxTi6iFeJFOE08nNM3KQ
EYlxkMAulVas2E4KU_TGeoEJeZjA5TPWVAQiPFFQ4nNRh1kotf4OHtHQVpaMzAypItIXAU8LI_gl4rdFKTfYu18MK
nygjEnO9Z7e2cYwj_hqx-AQdA6ulQBcNR4DFSCOTLnMB22GMXGVOMDCmiaxZvchp9iEKNJG4TkZQmoKwR9pbEbahm
sm1WvUbR6kEqNYOE0MMsRWNM3RBNltm0Iqo8RKMlpRq5RceWRRdjRkKdChyhuJ2ebBI05iRsuE6AwWEbCV6dQqNZ0
gqdeU5imECjFWLNqYvs0BaxDgmoSdg4rFlq3UrZ3gLD4UTT4kM97HO5iedxoox__octTEEImMTf8uJI2M0nKTIpbW
BHlofTfulcqVXjFYpr9GvuKM_mElaoJwn3MQYrFNLcwY-fzy9fqvGFtF-62fHcpcL7SVUu9KW7igiAHQfwXmCnMQz
sxwLowVk8mFjDYgV2iIoNIeuwZdc8-I0A1CLiqOQNwCLObgSMVeo-WUvzmocsFOUtSUS1chNNwpjMCGKuHxOYOcvK
LxH7mvPp6czIovPsqQUZdloA5Wqt8U1sDRZfrhRlUi4IVoTmevBpaEYK_Jze3cIMOkRKdO5Y1tB4TIcAHE8oNUarU
EYx1YDUinIolRBBDyBAmR7rbV4iGenGHwgeTIZ0cpppFEDbkAX4AaG4YKGdGWrgWhhiDoPX2mda_BLOSilnlhmM2B
hqGZBkKK2E1B5fgER-_AMYeVl9HEoKCFHm6KApgnLVnYMQjEv7kC6tsqxs-pOcnSs2EpGKMMk4gdIlcFNxsVU6sXI
NHADvNmtNyQgjRFKhmNPtYchXHWz_tgccWNkm1DD6qMATOoZcscAu8BBpKUwUIkIUICwKpay5KUsFjKpC9HPqSONV
MVu7GYysVC8UDTMetWoXlSiDetoiolwFGGpIscf1ic_rUhbD3pyxVI8DqCsdFg2NcSvIJRoJBO12KHKRIYnc8ObgC
zJBULNZ1Rmc5tCbmcW_mmhg0OiA7EJjwi_eoY82_g0eiyAr0K4DmBy8yqWDZV45KfAnYQBQZvK8zlj0npGqVWusxz
P1mw_Dbhnp-Z6SyIrHNI9unG7DbeDhcnBD2QBp2t6cNgvUoCLzPReQPYy_bwVEwcrPSO4SjUG8mhuybiU5NWdgIRD
95gD1ApNRoZeJIhfP7yM1vt1ZCxfV0xEvUSb25DOebimyplEvv7nxam2hbnlRQme00B5wPt9pETxPSQE4ZUd6u60U
9e6F3C-Fqjwfg_xYMk3oOcZQ-P5NrsNxK3ho7xmtpSKVahpf_2P_o2Vz8YFc7t2S7jAx9bRLQQpbA",
  "priv": "c1il1CJwUdajeAm8PMZMq4mw2PH9Z2vThLkHU2MQ10A"
}
```


Figure 1: HPKE-8 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82bVFRV2R2M0NKX3Y5a1
9QSDN2UzdTMHhvYWg4In0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "zRayDf-tglGK_UsfOjbbVDf_GPQKpRLNx-pusFTw6REZlhoXc8INMxK5ETEdsx-0MT
Va_8AIou9zUiaHPw-Iv1nk7X0rdIFYjKOTnjRUy_DuRIRab_o1qSZ5-x6sBn8McfjuKMvcJbwU2uqW9NJyQtK_2yN
mVvrYiPEhnuO73O_BSv_GSBSoHgFWEpbb5FeH7ujs7Pq0bV_pdI3XnabhvIPVTmnrkzP2J4vcYt00B-wxAxiLUc9z
aitKnkn_ofTtOp1lUUeuUzKDPYuo4x-GRZsG_gf2Ez8FFE0RIJq6AmYr3DKtSziHFqeim8uVI8_mtE0wIj6BM6eYY
L7c79MNoDlop5P3QI3-PrZ7HrqULs1U6W7UDScowuP80jJQjawMUd1itDjlB1BkwVH2u0BwoHWzA4NxdgsusIbDDm
H1f-k8Y5t47tb3B1FeBYK0G5MbXQmc-h53dACqTqd8nJq7jQNfzmELY7aWmT_Z72KGyfwUY731JCeODbDIW37g0md
OR7ZcFgHm_Usj02Pj2J_Fsw2N3vkb_IEWi8abtP7NTaB6mYmI-aNGqDEfXRVI5K7ReLaHOqWxtPkkfysYbeUDZncw
kt16rFa0FzeL40sfv7yr0J8Ks-HXPItnfmha_FDB4MuSlxmH8fADldjXNozWwB8HWSCEp111sdh_cP44rRNxPZbsS
7UWyTldMixcjKNncA1dNhafJ5qXjq32NUiN8R2BPkWCBzKMfaKN7bujZphGIRZekETFSx2Cp9mO6hG-CqV2dsu9I_
MDHgiWEV8GwFC4HyILVJRc9qysutXw0b2UupEos9BzuUaoYTvGHwpNWzB77-vON3w_FV94KrwQbiki9_vbVtct5OD
B9Kf8KCHv5DPwYGi7e41zKoS1Rm2Nczt56SC_RqKn9nFR8yfH7bEhvnsQHi_qXHWOFWN7f72H9Cb1ascZo6XTYaVU
Ci_RiRS8wgLG0LvOyCfpzgVNpbFhPGBbTZceZW6eSGNGK-RQ0zb5sJFZSuM9P2cK23dnogEGTPRLp9DWs3NUBW0Z1
yVQw1v9gukwcM0xYlo-zfQbwWzHIdzJboQR-DqeOllx_Jjh1tZPC_nRBdu4DPX5KP6JDsIrv7hw6YQ5ocQwQMdcoG
cFWsrKEOk2ei5HBjbfJQngzKT89TpNaBH_wXpZqUL25bltMM48JG6rTiG96eSF24BDONDAUDgrzPBoT_ipdN3Tie0
hQHxTsT4cZP9o0PeEYgu0CGPUG0wcirNh1hnhf-PTEAgfCoTyqOJ_iVj_HZO748slRlMJ4P-Ij4qah8aYhAWJYSdz
fBCkMPXX-bzw4ovKuCbFlOwT3I_tj0lggb-vVqSzv5nkHyqjvzGTmEK1Tq_Wy6uxyD4gUBPKkNoPMvA6SeghLYy3c
8XF80XxStZX5OAQV36AavxZrGyX3gMS024KX-wbNytokZbocP4EOLumsml35g9ePuXmJjEweCm-D5fqMe_uaLaRP9
RveNyNsCd3arMLkn5PSpRTuTsMOhLm45olI85aNT9TrL1oMw",
  "ciphertext": "Kqt2-MjNX9R4OmghbRcEPdzNJvCyvAUbezJcRvKnbzWqu3JsfGkO54gurgSvQcQhAnTWL
fJbDJvFJWzqCkXoqgYtgsvrnxFNqJ_j7194RxeH39eXb0MoVkTgPRQO1gmbtr9VPTrkPXlGCWZjrdVGEUZ5qJZvZf
HIYyo2_egOP5CuMzbZuNQtjxeTdagfBqAymYpk5O8VqubF160UrVDZnDfm3ndEGH4oFZwPVtPH2IaYcubiTm100ox
```

```
PdTTKZX1PeieRG5RodWY6rMsrA0_dMbXrTDg3spqXloEySB5i9w9ChHZ4s1UHzihtusJvw4qI1kQSZZc6RxELIzED
3s5OHhpuzKTrl-3vVwlf9Ily74215pZwdJW7CVWTL-Xe9fhxEA"
   }
```


Figure 2: HPKE-8 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82bVFRV2R2M0NKX3Y5a19QSDN2UzdTMHhvYWg4I
n0.Uo7Qjidw_FqP-aE7NqWF7tvz_EHaMj2ebRvHtpRFqXZ_cXQG6dZVXDuzdONeZpgvmjox7zdKBUDG81XxTHkWbt
EfHKwA4ByheUzpBiGde_MAyCVaLS0C7tYU1tHSbDIOR3RkWHrsq2O62R4saXt12mUUyvdZnd97cm3wEb7PbC06_b3
OCl0Q2MRC2UPVcGU-yXfldWZKZmotQDQbzoys6Zs2R_TDr7WtilKpN9F6SXt2DMnM6n9zw8ggtUUtg37grjY_Qfo8
NPlBTPcWntQuysl8xt2uls4pe5KUfc3mciSIPLxGQA9AfqHGTrIBeXE51n6WQc0gp8RpAgyeGpHUSx6-e2TQscn1_
TgLBrWSSOUcR6SOd3i9rcWSo3FOmJc6GcCGCvB-tYqSu2ULUIgBXLlM2O8OZXIMHx28m_f--dNZH7YVdxZbIe69RL
kYCxoZlolh2iTfJYvPkBJT9hSbAw0jPh49jDaGJsBGCORk8DBi2Ah1_zJgx3otXr5t3sHgmo-diltyQ_IESRR3Fzw
B3HdLeO_HnAmnKnpABKWzvauVEYoNHKMWG7uSZMLYaoheuW_Gw6wzqETRR-hgYR2K9YVlKmRGewZ-juYE1zpxKk-X
7iAPS0q-DTXIyqsr_4gXulomCy1pzHCdwkc4Ys_jvCUC5MweojTzQTdIomo_JcCVQ6eOIPqopIsonKWKT4lSJ6kes
wboCStOElVdqGtig_WXx-N4AjeZLvnTKPaC0c3zjlVf5Dos-hx_-EjBfvtXDEQUlI28dxr5CnL21MZ_QXcJy8-sbC
4aZjczt8LV_mBJJwm8Y5qfjA45_s_oE7IHcGn47YTb92JfjUv2GD9RnFKLYZyoyULp5ypgxZ0LpgHENksobFjrsQe
tZ9D9UV8Irq_dJ0igW_a5AOkCx4oUT2XMCjhM3Tkt6jUJCU86whvk3Ux6zA86UEiPuU6aee2A7tRU9EdRT4TGv5Ao
fe5XhFtngXP0QV-7xZ35Uk6sOxNsgagaNw_wqKUoIazXxOb5BEHdb5VFTqoBAXAvyi4Kga-caLuWAkCHDViDDKImP
8Orm57_BaxGEjwmlsggLAxXrsx7Seg5qRe_YjKCQcHjtjOtgXsp485CemZjz08CzEloO29eGMVAlUVUlOLi0YnqY_
gfyhF0r8SI04_hC3U9nSGsjz4IPfGjlTgR0hcm3BH-72yangLnEYHFgrPQMosxDzkbp8xEWFntXwAdbbmNkNPvSpT
69zZ1Af_7rrmdXXvVAghL5QlA8u8G3ceurO9NNwfHdr6T2FdclLq_tmGlo_Q5_5hzX_f4kMmt9-xLfmJduoK44-sZ
4YC8jq_OdJNgs2FE7fR2h0fqQI6PpVyYBU8Sg2LkkPYa6sTg57oekqLgUS6ZPNFmV0PcBt1i2JEGwpxC78EQYNKU9
ZdggpnHgpE6aSgBtB-P4Tr5p8gMhF8E53UVNHRPXWOjfChtA-CVpi8p6qE5_a4MPedjf0GkcutKIQ9WNL2zhrYo7D
vlylBcX0YQUcqltcKSS6jaS9FeNQ..k8no633YrPgoESVevhyqn8Q0lihzU9hyVR-uzYzPDXwxLcxEK0pt-if1bKq
8IoJyZWB84Iry5efVn6mSFlz9CpbOKNwX6mZAFjM2gsEa6GXXHFt1JF-tMmQK1T44WRpH7HwZ29d4nrQgTiQ5sjDg
c_Is9ZhZ4NOYpVo5sEcbbx-uJu-0u9cXgoEAXk68BlBQ6YCDQwoRgJzCLz8q2jyrc5RIzJbVZb57MJfAW5_CJoaWq
cqgSj893NXN6-Qgr7KZQ2U2Rm9gx8kyD2A6PrgS_jDvArJHRtFhC7c9ax8btYkcrbmRfWG5UxVOjue_BOh-xvkpWQ
nJXjHOJbPMAgCaZCQ3kVbG_zfhtID1nlQWnFZQA3jG16jAtIGMLb8Qgjn-cw.
```


Figure 3: HPKE-8 JWE Compact Serialization

## A.2. HPKE-8-KE


```
   {
     "kty": "AKP",
     "alg": "HPKE-8-KE",
     "kid": "clBPky-tElQGRa8AQ1MYfMPvfqmhOs_5lIejOuqAdps",
     "pub": "pxQRXrRJLke8BMBXa1FT74gM9fq71fEwRPRndVsmsYAMU6llEnJaeKAagjxk44yl9Psn7YBn3tVX
XLVrqIxyWhGsP2pmH4Y2eogBaRMGBfQy-TM_RzdFE-hKLHqHPmqP_PZES2s6O9tBkvk7D6fKZKiBDSKrvWgrKCIo1
DccgfHEayxCtex1w1ZjVweIZWtVA3V_JdijzobGiSU0dzqyjVBBCQVcWiSFLLuX6rFtiPpsa3SlavpKHaRTIZx_5o
cCO1LBAKq4jwew4jxnhRujX4VcaOE2MQQ3FUmT6UgMpWSfymJNBOqwN3uU3EO_ktgMPwdfrRVihSgirkiV7BhSW9u
N95OTigiJIiedxPV6asK27cCcPhN0lJQOynlah8BjySYKwdMRHyxVVhGDmnJ36veTEDoboBhq5iAkcqwed7O-KwC0
9XcVciegq-tYI2NWMOkBdXE_W2qvvPIkJpOYtKAztpUcxhBBPitRGQcdz-wD4nik2DFk82sfDNpC_lV_XWYR3KVwi
Bix2tCB3tw-j9loE3AaxGefsyl0PPQsFGu2i5qutBlUclRUhMUkiGcyEnx5S0xNYzyuM-lAa3WpNzlEc_SoqmKvob
Zp0pi-ExYnpIQJ7nPJFNXJ9ig3kvpNCxnKlEwsP5w91SbOcLOBQ5dIq-moh4kK9ZCry_JkAmmAxhu9kGCughacCPa
UqgZrigO9bQHHw0giX2EB5hA-r6VxzMwYJcox9SxD0tJVsAMhCUGhGuS5wodrPhay-ss78AMZiXm3D3mDe-sA0VVR
LaN3HgmZw-kud8su7bKh9zYec4iHaygQq2ySGoeOKoGesVK77fiLlWaYLNtqEmywBblQlkZbOIUmcVmsTwd1yZG-r
PIka_eJ9gAE4Te4XgExooaJI4LAdaif1stG-lEZF8RmNlmvm4wdAMZQAqPPLiOwkVAhshMUfavMeViGedgk57y3JN
pgqQuX-sEI5NmNMFW47wR3AesCpuuq_Skqj8EdeWWaIwh-L8iDYCc7N-tLhNwgJOpnI2pH-CpgVShigKi6brIjB4Q
EV-JtRzKFZ_ZF0wM9GYTNsBM7dXlxPUUVjLCyWFWYScRdwHypH_deyvaEjny-0DgpOuR5pxBWtFGEsoAQJBmPZFum
wYB5dZkyBRJrQPUENMNw0eZ_1yql1oFIdTQCQgEln9BFfCPB6MCX8kZknPovhJmq74BALPWaINeZhniI48FGf8tz8
VdJ11Mu7qxrNiUHNApTMcke3Aw2qKl-NtFeR8Ou6fqQH0d2ShV-GvCcuxjKfUdNU1y5zYhlu6ZZwvkZ39jKl-t7Ey
w6rAEnUfWA2hEXXMaDqBVRYvqwhiM0nboODhWUJUW8OEpBp9eI3eel7tRFViiZQ7KsZmUBVyVfGJQvh7DM51VAvUU
Si_xPQzsz--yWJ3DFmYWF6eMQk7FdUXu7HmFxMfuNNGHMypx8S9RqfCiI9OfOeqwVSaa2MAd-b2cgDAo8qVeCGcMV
U9FRwrUscVeltcJI42sZiaoXFPUlyAKncyajZ6gZhFNexIDWiSCp4L54nM948L-KcoFnZwHsueAjiJwE9dcy6kUty
Q6v0_OxWb8OuM04u96GtOld8wVIcB7QE2fd7g9XTCdShgpdmMgNnGKrJM0A2Rbtmnn-gdxGbyArJA",
     "priv": "biUK5NqJzXzWEAN0F2zzkrEr9Rp_QX55is_j7VYuHCQ"
   }
```


Figure 4: HPKE-8-KE Private JWK

```
   {
     "protected": "eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdSYThBUTFNWWZNUHZmcW
1oT3NfNWxJZWpPdXFBZHBzIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiOUdINDFMenpHYXBiUGFPeV92T0RZVEh1c0R
OVjFLdl9xVnlZVDU3b1RZSlRqS3cwOVhUa25BZFJSa0VSTHdQdWZIZ1pKU1FpVzNHVGZXMVNiRVpmNFhDWjhic1oz
Y1c1U2V1SlVDNmlvXzU4enM5SGR6bEE5bnQ3MVp1eE5XbzFvbUxkYkZZTzRnYkE4SXNBaDY3QnB6RS16eVVkWGlVR
ndvWTBTMDRpUE5RMmlmc0VlWEVFdW43ZXJXQ3QzbnVYdEdXeTRxMTBSSWlRcDRWdUdGdWpRNk02UUptby1NVVRJdD
dzOGtGWWN0Ujk3U0ZDU0FFMEZVYnJqRnlOMExsRG9JS01VT1JUWHVpdUctWDNyOFdEdEFMM2NpTGs4T0RNX1NRa19
veTlCSmJJYmRJT0VFZk9QWU5udXl6VHhuNHpUZDFqd29zOTVpUmRxSWFBR0JGaTJaajZOcWxfWWQtWU1aeFB3NFQ4
UGkwb2R5cGRZYjVZdVJZbDdHWlItamRTUEFCSjV0dEt1X1JSSnlZODB3ekNUa014WnI1bVUxZXZpWU9WQm1DY2RTc
FpfY1p0Y2ZxNzNKMHYzV2ctd3U0QmdwWFR4VFZYMjB5aldTaFY1TlhHTjE3Z0pwcVpiTmFMTFVpMU9YRk9EaDcwR0
lhZmNqbmFiVFVsRDJWR3RMZnBySGMyVlA4VHR5Y0FLc05LbDNSeVExNDB3d2pONnZMRFljRUlyUUt3UzlUZURqcXV
pTVJxeXlKcHpYMXFCTTRSVENnMUdEWVNKSTJKQWVXZDNWbTBwOUcwRV9DS29DOTMyelB5c21zWnFoTFBpNEhjNE9v
OUZLb3haQm9JLVI1NUM3NXg2TFJrUHNvRFRJaE5BbW9yRURiOURRcTJPQnZnZllwRnB2ZzE2TXZVNTFVRURyUHBBb
FRabWVWcHpxay1qR1huc2NjaU5relMtLU05SHVUb2ltY0RDbTNUdUo4bGxfcjV0T2JIVXZxYklBSGl4MGJvX3ltel
R1WjRVSDdyckNmMk9sSzhGbG5xVkxwa3JmeE9uY0tadWVWUGs0NEE4VkEzX3luQmVzdV9ORGtJcEFUaHhoYmEwd0Z
mYmlERVQ5OFdYNHhBNjlfU2RaTm1KMUM3SklMWHVzSnItd2d0c3MtZlNqZ3VKdHVpR1pUVzR3UWxKNW1jbnhFcXVK
VEc4Zm5UcnExRVZ4d1R2Rkg5akZlXy1uUWtfMEEwaVFaT0dBLUFfRUZvWHEyeWM1QnM1N1NON2FzQ2k5YnR5Z1BvT
nR6cy1VaUtMb1lJaXF0YzlHRlUtbXhtQ3BSaHh0WXpaZ1o2MTRPZU5temVFUFV0SWVYT2Q2ZDdhX0l3dWdkQ1lfaU
9HOVVZNnV1QjlXclpuc085LW1fYUdKQzZES09VWXVpUVhVRTVaVS00MnNicHYwdDFKUXVVZF9od01HUUpuMVNtN3N
BeUppMTlYcTdyYTNtcnJVY2FGUmk4d2J0dk5Ea2JRZ2RLYmduaDFGMVZRU2lDWk5JRk1oTTdBVDNaUmdhVjhVZndY
a2hmdHhoUTdIYmNzM2ZuNnZMUjNkLXJiQ285QVFULUFlUW94LThDbm5DVXBoSHczemQ3MGJBRFQtYTFRQ19MM0p3a
mpDNEdFSTR6NmtKMno0UGNOa2FxN0hlcC1RVENiUzZ0NE52NVZLU1FLNXc2Y0ZNclVsTktWNHpFTnBpU0RiTWk0OD
ZTWEdlZE51R0ZPUUVYTGtYYmJPV2gzNm5adVVEcTh4d3B4al9hemN0OTdRVE1OWEpBVFpXRWZ4ZjBBQlo2dnlyMkh
hN0tGUWtacWpwMGR1bWVmTzRtcGVnNm5yOU1uaGFyQUMyYndrWVBVSV9EQXlZT3hPOUlGdmsyNDdUMnF5Y3VWSVBW
NzV0UDdmSk96Sk1wWktUeHZjdTRJQnNFOW5hbEdXOTMweld2QW9Hb1dsdkxRZ0ZQSm9fMjI5TnIyN25IcWZfMzRzY
UpidVQ5RjBzX0F0THpENjdjWnYzWXJjQ29XX3NHcXUyam9pZ2xRN0kybUEifQ",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "GRZLhvvj7vBw-FZm",
     "ciphertext": "D5bqaQekeFnn_YlzsERq8jp5w6Y0t2gulaz_ql9AIqozptDIHEAaYwGJzfgv2W_woeFLX
UnnZlnG_aed4vvmFi1r7CLamiwk8Xie_bPEt7Icffle4mjj8DJr5KZUNNfStrKH5_DJRl53dOEeuAhYdXU08OgBh4
ezaTx5I_2fDqVXSGfO5sAWHINXWEPsrf1k275iMApQthhD4aAO2hYLAuAGwFGsySvXoj85BsNH3vLALi-H-RSoXWN
t64OxLyMXY6L5TVBBaSnn19-h6hZIZU7bVQfckoSKftZphRR99hWxZ2JQabTYQMk_UdW7SUBJUJe0s47uFrKC1T46
8hp0WFenqHZjS2oaAodaCZdIayGt",
     "tag": "8A439opYUyFbYJdDno_Bfw",
     "encrypted_key": "K4m6zdOhTuo7VRZuZOmmypBM_WxLAI16vZklK3EnnrPLTyXKrUqySJOIn6TPhnn_"
   }
```


Figure 5: HPKE-8-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdSYThBUTFNWWZNUHZmcW1oT3NfNWxJZWpPdXFBZ
HBzIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiUEd0ajNSUEZVSTZwc3FlRFNQbFNMcG5MTXp4dTc3RmNSSl9kOVBQZ0
gtdEVYT2RSVTJNQjBicXhXekYzM1FTMnVnSkdYZVZJQ0VqamtNMkZNVGc5aHY5NE9GdU01MWwzUWtxNnYwbzdXT1p
sM05tdEdCN0lYMzJNMHBfUVFaZHBtVUFUU3REYWtLQWV2cGZzV0hRR1dqamx1Sm5JTTlqUUxKX3kwbUhUZG5yUnph
ZDEzSW1Zc2gyWHpmak0xRUtQTFlGUXV2Z1c0QTJLSGs2UXQ1dVdlSV9SSFhVUG96QUZCd1JjbFlKNlV3T2g2b1JMV
EE5OHN4eU9zZUx5bmZqcHctTGF3WjhFelZRY1NoY25naG51dWV1RmpHeUk0MUZfUUJyTkZhVGNBbGhUcTBPbDFLaH
NFaGlrZE1mdkNreVNXSHQ5YUJiSWw2VjQycjZVa3hPdlRnWS1jRDdHcFJJZ2RqTHhtM0JVZkhsdnVmTHpyLTU1Yjl
PNXoyYW9XVDBCMkYwM2ZYdHVadmhjNDVWS1JONFFqZEl3REhnMzI2ZHR1bGdFQ0ZMd1ZKZGFWc1JvRUdyTUxaamdG
YVdOWkNKTmJyWE16N3FZZ3h2NV9JcFEtUWtZRXVmb3RUZG16YnFpVHl0WlBtSWFZMzFJbmpTV1p5MGxyTXlGWWRHa
nJ6WVNZSm05SEtkbF9nODlLek1jempTaUV3VzFhMm03aVB4NEZ3Wktlc29BeTJRZXR0Q1VXa1JLS2VIWlgzQkdhUV
gzUjh2NFd0R25pX25uOGgtOEcyMnEwZEpyczRjVlE3MEEtWmdFWUtDQzVWWUpocThXR01meTNIMDVlRmJQeHJxOTl
hOU55VXFDbWwxQ0RvdS1UVTljOVYyWjQ4QUgtSW96Zlk1NEUxdlQ2cFlvTnBVWFJGUEZENVJmR2tOOGFVak9nMHFx
Y1NOR25ydjJQZl85MlQ3cDZFX0J6Qnpwa2FkNTJ3LVFTTzJvQkZiTWhoWEttRkZ5YVlWYS1DMHB5NmVOdDVhQzBQR
mJBVTA5eUg2MmlLYmxNZGRJQVRsY200V29Ddkcwb UtURzRkdTJER1o4RjVyNUtSdm1rUERvMDJIaTJoZlZ2VjdOZE
owWFBNY0N0alhkMnJKdFJIekk3b0o4ZjU2bTA2bllQR2h5SHJqdm1Zd0pZTWxVZnVGeFZEWGl1LS1nbTZfNlM5c0Y
2WVpsQ1dHMmVoeVVRMzlQUEs4djlKNE9OeWx4NEhPOGIxaHJGQ25Bdi1aaFhCbUZ3b1FQckl1X3Rpdko1dkZMU1la
NHAxTTVrV0JvcXZMS0JBRGR0NGhqNUVmdThDU043OUpKZjdYbzIyczFEczJTQnQwN3cyRUxudWhYd2w2N2JscUZ6Z
2Zkd2ZURlc1cUFxbXU3ZlJ3VFpFODA3a0RfWl91Wjd1NUNmS1NlN1pKcGdfQkdiUHYtQW9yMVFzMFJBVmVzVzlOZF
JhcjgzNUZDOW5MZmcxcDVnXzhkczJZZ2FxSzN5dDJiYjNieXV4QUo5RGt5Snl6a0NCaHBfZm4wSDhpejRGUVVydFF
RM2ZzclF2ZG1qbndJeTlsdkpwU0dxMlJKQzVGMTE0bVh5R0Jwa2ItX24zYk9kSzczRTBKdllQSHU2S2JjbUlvdEpf
TFAyVGwyYjVHWjBUWENxMWhsLXlDcXF4blpBaTV1NjJ5bjVNc3JmckhudFJpWnZmZkp3UG5lb1Z2S05lMHB0VDhvT
0p4U2dwYURzR2dQbjdiOFkyaDdUTHMwd2pLNmoxRjRrWVVTVkV2UHpldkU5SnZ6ZUprdnMyM3g1b25fRFEtSlpnbC
1RZDJJTUF5MWZQRnhLRDAwLVE3cnVBenprSlUwMUNjOUtkbkFCRmhDS1ExM1FQYnFLZ2tSYkFOZWZBU2JZcFBJaWR
```

GcEQwdDdhRTBFeTJSUFFMM1ZGQWFaRFEtb29xclRxbEZLZkNTdGlDRG5IdUQ5MnliMVRzbDlpX1hxemt6STNLYkVN
d3BTOTVMWm10aGJFNkhDOTUzUGlNT2p4UjQ0NFEifQ._f1otx5mIKqbhyDDfzk4XHogaC-Gpqra3fJ8bsYN5_D1r0
YATx1vQiLkq5aphuwd.HRUgU3e5dEtTx7EH.6Vtnu3GlZWv4OCdwA-vc0pjJStf-A8jr6fgTAydJWpCxYyz0WYhu0
eoiRk5RjTZEiHH0KKE1RtjrnGF6EX9NuONxrZwGbw2Z3RVqc34MtLJQvkdQ_JLkqg8QL25RGPNCk7IvZW5obfAlkJ
lxfy_Cf0h76G-W2cCBmz3vawWPqH9IslL7-osvMjTcED0XAQpD96q0DIrjRGzls7kEHrLp311VB7ir8xORrzEtH-C
n4M00WJbcLCYDyKmThEZ61Q8pQDTTlHbyOqrp-UU2wIxbIKAwHcPaKna2ehNtOzzkD8uy8iqU9X7fhGlIKIUQIBJZ
PGQKxqGMUyhx2zGW20K0ocJQ4wYB-mNquVzJt05wWlDn.I8b81u8JDAfDrZLQrLpe1w

Figure 6: HPKE-8-KE JWE Compact Serialization

## A.3. HPKE-9


```
{
  "kty": "AKP",
  "alg": "HPKE-9",
  "kid": "BeWp7Y5tolX2sSYMKIaG6WUVE-arTKcS2Ok8EgqFqrE",
  "pub": "ZEbKruTLTRJZf-UygOWQwuBNzChq8yuhGTVITLeU7emGD9tF9oFEy1BP9hmBRWo84Zyjr8xlvkad
CNyu5iOfuoIC7pA5JCc3A7BNp2ZK8TnNPTsYJ9BTicjChlIMMYKVSnk9WjCj3EqM90RaRiSHYxMUJ0VV8fY_06Bqr
ODCwNO_6BYGaaxHszSAVparmkEiSQOZwyB6xsc0dsU2MGVGANQDBCu3NSs2gZmN1fslWpxzqyN4YtZhwkozcmsGzt
ObngYHXEtgqpo44mKqXHfMBIxjvsqgZ-vNzGyp04OErotG5QOeu5gQZquZ4TlS7JqxjjN0ktJ9Wqofvlq1i0JG97V
L7aJ0IHJpnFl8-4cbqwq7-Wan_9U0fJux18PBDBq3jkQiwLiXZOk9Klgin6BGwpx-JPedIOOEEEnKLpQwg3lOZGuH
fXGCT5BkGfk4sVVR3dg7uMvC4yFS5ftvggIWfMPI4LV-3DECG-pDe1vEpQFE5EwSBHUhpyjAWuMEHbpTKau5oGmVA
IYXRKZfZ3CIFQV3gHoBZdZQoRhEXzKmdkPB2jJI16FnFGUK_GSZYsXK68IUk_lEnihTadnBEhM78-wh9ZtAXQsKgQ
tUdWR7nFt6yWAkSQIegmJzzkEw4_FBrNYUIXC930h1dYi1sZw5ZHo3dmY3Viq4pLiiixN9LrdzV6RGIwR8fmpqbqN
Ac_cVsFePATiHnwBQ5kej1BLMAkUfYhJpX1lV-9tloZLA6JdkRoAeXnEvIxyY1TUYpugYuZUeERwlWygVnOidsIi_
Apo1KAUm-TocR6m0zGtG2YQ07mUeI2yqbctcg6EvYVVBLDu_RJeLFyAw-Xd_WXgWNoIzoOM5CXLOtDCcJwMoLJknW
1dgNxdFZHG1mQg9T5wBMbEBpjK8a9oOnfxVblik3eUHYkS7TVhKSqCOuyOBzDQuVtHAt9Q6OCoOguqUmJeBV4GSd5
IPSnpCendqBjEKZ2JTkNwFkuqqbmilEnYMHEOtMUyveWZi6_qm2kPG7aVcjFV9U4pXZEuRIJcugvJUH3qw9UQ7smg
qsaJMFzrDVsAGQWItDJxcEOgBdBTAiit99igYmAeEyNoK-GQ46OYsNzq5-CuCiCGJZKNObWhddnROkmY6jFG7K_k_
RgvAj_aW0oPIEzGz0jBtZqVDMTFHF6d4q9erpHOaO8h9e7k2nnrGyHgkJYOPQImVrLNc93OEJ1qLzUSwJaho8KqwN
lOHqDuJgmKoSfEhqXQRfIh68qNqZ6SC9JYJ_-lwpKk_TQUYxJUdRkHB9fgkBwyoGsi0nLpOhMinsIc32CMyHMqvBs
c9DlSgmZOBgiovynEtj_gqdVZ3ZYwDAaSaXTG7wLMyNwBfVycm5TdMQeZs8dwu6pifo_UYzBhj1EY8u3IdS3OVajD
KZqkw9zeTacE2kwVsCkDOK_y-wQXEvyFCbAYW3IANbpAuIwpirGJfFTWHIFEm1CqL4FXPt8a9DusGHQCuq3bEkCtp
nRiOTGOqgVSZSWkuoxbGnluihrRc5NYY87PCvMSRVxthHPS6-Af2yP_HWMkcfu3DwNyCFxBJgfvtXGLFSm8Zq6EG4
zipdIVLeDl-Mg6s_8jDce27ki2xqXVQWA",
  "priv": "tQDSUt-Mgd0LNFiUK9VEluJnrtg057pCq97A54EdbiM"
}
```


Figure 7: HPKE-9 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTkiLCJraWQiOiJCZVdwN1k1dG9sWDJzU1lNS0lhRzZXVVZFLWFyVE
tjUzJPazhFZ3FGcXJFIn0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "FNPUnD-x_KD2ZlRpfS1i5otH3zXS0p5YqAX1IQXDg7KkVDfPrigLJiUX2olBxmMcer
7yXyH1L1VMt3AnbWWHAH68JXG4maBWMtpy-ahh6X7k16JrzCzzQCuRWS2qDMNw_jjb7L_LiR6N9VigfKC63i8D5fL
9P3y84jab77h5BFeH_px4XNXdj4IZpoQbrF496F3TMCpj0F7VIOPOH9Vjt6gH4sOAvkeuX5riGG9F0dhN67GmRHAe
CZyW8ywvfzjADZnRG0_SX-bfcmICTJziIVy4KaEMH0YvmIrYmQe9jI-XKCIoeSQpXbvXQtniw6vWhPV5pDldRF89f
shN1VIhTT2zsP9of5loHM9DJp7ac8SvhRIPm2GHocU9JtRN0MIkeUEqLMnJlp1dBJl3D3qwcOTvAO0A3ZA876Xu8G
sgcn5VsJj-O1AN2eB08BR3NNGDuuUsgxPVXQWyAFSQ_UlG7IVRp_8__NxfW4cbpCjcE9hvvlQD-xFS0a6rQOKImWK
zwKmY8GiU2SUEAwN6rSPHr8JyGfh0YrA0--FgPuab6PPGrZ1qz427SQIxlJBCipWPLlhJzvbWUGCw0g8Tk2DQGnCB
MZNc4lBNVhnKedQ57g6erNBh0MOZSXj-SLul57DSBXguw9jMUtsJZoF8PjIc-eSrQrZude3S9illlCRM1dfSaxPk8
25PQjBFlMnEb9qe-Uc65ALr093ikk5eYF1mUJ31EAJYBVl4gU6RmD7Dp0Iu1X1zwxB7JZYZCqUOmhyB1lf8oA994C
hY_VkprCF_A0NcLpee8iW7d077OVODp14M4w7D6hPLJDa4T0GDjMH-o21b2n6YqoxbUuPPGAPCypb7e9zGliZWkpI
yBXzvw8pwQ708iFc4AMZswlS8cYiS-6n3VrGosvT5UplUHdpPONfN_UYHOFwIWwErmxABUZbKNHWM0t1opDlysAIX
m5lSOf7NFAVA05UQGofBty1N1rnSey6ElXk9lf3gdxKDfkgZVqKlTiuh54bm9L3Kgu6ZLKqTyxOWYiYW2T2G79tXy
LAQDrl6FxRwlGpUWGhqsmN_MSImcSR3R7Y7uwsQshS6hg7zXJo4IQ3ok7-RvP1-bn9d9goAHPSYASnrWAG8IsIFRK
2yJyAEIiUNL_tFQ3TulU3uEgJIECrqKn6jFcLQ_er4AnCEJy3Old1rXxZsMSLhHuucqhkByUT2iP5jsupSeTaCgRU
KUMQwJ9iUeLAp4aAIZAertDuVVZli5fRrFByO6h7wZ6ewNkNen3vwFgDU3V1_xXIZCo_GFghO-oGMysxETIB-IvqR
H0qLWNn0z771zagoT4Ri2HmQNRcKmA9uBpSpJ2nYIkMJ98CYm5kHvlgZgZp_YEffITAXZ9drxobjxrm4o73l9nhtD
dPpY3D1ztv3l3kFX0K2OdpG5whWZ4kuEYmPuugT49EVQXS4Xdpo_aS6RNKwc7ffpbhl-ztL-H54o9-NIoveutL8V9
57RA",
  "ciphertext": "V4iZyqGIdT83y_Eb6dE2c5l0-LMzKAXVnJwmXt9337d9haaaHlGYFUKvF3zvTZGBJ2PXL
QEFWmqZ59lseWeSGA1TklJIWjQbb-1oCdE8607piGyFiGyjlsd5CEzfJuVZXmYQz3J4g6NIHlMGIoKTx6aa_A-qYk
szxoKdlvnmwHLhm95vr9k9GNxWIblWK-rJkntpPTWecV7Y1nI2yb3nzJUBDfqDzfKb9YW2x--8KFs8n4RcSZr3d07
RCB7QyxQKl9AFd5n5thTO4_UcRChvfc1aawFV4lnTHCGLRAwPo9P0JMNf3v51mfSstGwvRotRG2t9S3IWG4C_94VO
```

```
eEVZPlclmt5uYJXPvQ4Fip4RHtwG1mRFRtTTzTblfqELzPe0VA"
   }
```

Figure 8: HPKE-9 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTkiLCJraWQiOiJCZVdwN1k1dG9sWDJzU1lNS0lhRzZXVVZFLWFyVEtjUzJPazhFZ3FGcXJFI
n0.ZMY3Ynj6V0Tflad99MujhmvSUTEYP-PETVMxSGfdKWjz1n2dvNmUCMfDS-pAzsh3lny2RyTHLFsUoX_Hl_hG4Q
Yd1nZm4X9bgWpPx8e5Mhbx9T8hGRbf8S1q3mkyLyIQNBtPW2KJMAzy6d5MQiJy98V4cL_-GFFUde8gvY1pIqfXSLC
_BBmvnA2DddcGPvi3eKco8PDY2HVNMQlCusFnnYVcRXiRc3tLJ2sAYIdavSJDqUV8QxiOqR6J0g_G0ngqPoP__bwN
bF_UDU4_9flpBy8pQS2P9nBJLdYBi5o_zwdUXTKCSgzUEvxrmr1YrGE7oPczjviXzBK-fbMWS7ShXFQ-ILzAccf2y
b7hef76AduEi9mnS4D6SEsPTEpFUNIrljED4J2QNuYOMlYCTb6Gen2h63FHZmTVMyXqhnKQUjelpg_qoD0L3ASUxR
UC10YR8zidpA4MKIRGXwfN1eeqQc_M4hyurMXLBOSjrZqCsKtk0KlgtFx7AmgZHULmYUcKZupfjCjPpMOAn3zmO_M
F3NrsKtYofQyF3USoVfItSsu-KXDTU_b55EFZfD7ur_4X_Wg_7h0GX_2SNzsRCyqNhmucBPej7Sm6spDjPfYXuyFg
qrEOVVQU6wMcONJLxTktTxciYcXI6gaCOgXgr7zWAQmP2E9UqiAq80yaaM5-WMwUUB1_VlruaqHy7s1cNBq3U0hC3
a0C8_QVgxTYYIZa-IEsHjx2DoLAOgiDrfQYQPer1YVXg6A-q1lPPO-jcahyfUXvPDsNfYJTRe1HvUXEW_IOZOJhod
TyreSPLjvRXhw7MQ4ghScbKusuPOwP3GXB1mcRiG1V1dQumJ5PPD0-b4dO_9ygcZf46A1excJrE5HeJ0SY6Ukue9u
ib4VEXeQi8HbS8hycC38qejW04FIZLukqhSXHST-pCoD1ztFd235WCIFQCsqOUOR6ZxHyO_MnlujxuYGoU_J7QBuu
XRZMWVLo6rwKrUqOkJVqy9UpYFwTOOG1g795uCkprW78W-kTRfiWkVjPReO8skg3u_FpvUXdSIbJ-M40xUq19DsRN
_RlFaMXX8b3m5NjDcBPJpPrVlN910izuecSJOalsPsrp0NWSXkQI42FFK9Wy0xIC7Fm8AZM-_5FnUkGyuqWSNLCkW
PjWWdK9NAnIkkHArv7BHvpQSm-FCeTgFCQIvVSlsjXU2-Nu55w-D0ToW6MPIVQHWtQKgUwJw97eQQ4Ni0Mgl61Iee
jrCaJBTfxJzsM6X7evU-9IY61WJJAFI5BcmUlcpaHm0aLRuLMGLLmrKsvOfEj48AqTHdI13jL4KVME-bRYz87twX7
GXpGmNLa0X3PGLusZ9gH91xZhKu8rK29oSAJM3T4XRP5qO4_8ETE9qZ6-QAa-b5dmXgkcswHwbS09WzBAx1ePVVU_
q-a8U-6HFaGswk9bheV0aoYSPXK_J4PKVM-R7YbxTO1NiOviY3E0XGJJHMp8M4ONbAYO6laXw..W8wioV5NhSNz-r
qzlPSWOPkjX-bVNx_vCiw9rguyL4dgG-rOVJqyBOvnukWT9V1v_ZmtXYdi_oAhOmCSaF5_D1DYNWbpajOSX8m-j3n
CjRaJdAf5N1r4XOw00o2BTdU9b1j6ZeJNB4I_71HFoGTVCY11NJbbgQBzoxWpMDQkn8cCk9QkCOqukakoK7qRB_e2
dJnujcGMTIr3s5n0gTZMkEaEAWdP3TNoQf-0YmCQS-4i-6qo0nkcUUYCH64vASVh5zrPNgCODOoFd2HF65gGKEJrC
EcVefLkYVCM3Zk2PPvOaUSI9eJqbKB9y9ieGxFcgnlLcw8bY-4l6fKjg8mI1H2ZNVRXsRmO0ycR6_7zzBfHUNklpp
1LiQ9wGiCTh3VOGA.
```


Figure 9: HPKE-9 JWE Compact Serialization

## A.4. HPKE-9-KE

```
   {
     "kty": "AKP",
     "alg": "HPKE-9-KE",
     "kid": "I8THo1KoAq9OG96cJTyk2WF8abZqb3kKKHgdfajHUb8",
     "pub": "8rGsDcYDVYgHXJdoG_y4snlf_zZ2J7IJ_dyGafoU-8PBqdSb4dKAAggLvULOi_kwqxCdLXqh7sin
PlUPEQAXeaITnOkYJhCJN_tpWBBbZclC4sAXNHItUAV4KfAmEgyll0KiqKRohYQjhwSlSAQhA9NwAPJhYMgZPWkDf
1zFJexT_prKclLGRzU-AkuACumcboErJqGYIRdXVfN7JqfIXfcNI_QCSpcpuAk_wMOWxOIj2WxdCMMfd1QBFKoAi1
cM-_cuL1JWwOK5SsC7FKg5YJZdZPJ53RkFUusZPrhcWsZMsOFXJmgOjeV9bUWA1npKEJt7nDeU9EGbICVel-RChri
He1tcx4OFgUCrCBvEpJl9d0am5jqwYQB-WmwVZ3IFVHM2c5NCb_MHhknJsaCqrSMmEUJ7XBpTWbdUlMNMMiq9Pcd2
WwvMyoZmNac_xKmk5VxkBqorWUZ3ieVwcGYt7cZO2mvJwilCccsz6TTIZnuymJU57-J510EbVfGXSBN3_BCpfwHAA
qV-rZab5oWPFeYQikjAHieblCgN7bSKl6U-NCpoaPA-n1Q3jMY-vzFy4iaM8ThfoXdzXQo0oLCvyOZ4aqlv4EqYQR
Fh51RN6Jkyk5eqUUaHmaAV_yyj7wBEkZNIDWNOy7ZAunaDl5tXFpUaPmHLQ4RQV1fCA8Y27gQ_4nOY2zdHhnq12WO
rvNN-DrdGI0ShpNWzARMtM6yiDXUV2yR_b6KTDyq0YyMzQCHBQhscrXCN2QxXd4hHj-gjZzoJlim6XybGlrG6EaMk
vIKfwuhZ7oxRTuC3hGJBSkMptQNg3Th4luol-Fl7WepM0vOYOVyYdRANeszJ6WTKZJCtzUhPcSBzeImXaDqNeCAt9
jIBXpoJX6m8RViM4bW8YgtR6vK2ceNW5yWCAfOA9NmiBDAhFaMNTnueistr2eEJhzFZ2wJsT1MG-vG2EIyuUNBqwl
NjVvR4vfEAWOmeBuA5v7By3ycsOMFv2hk2eGssIzmE86ZOj5Oj11QWFPRrSMx5zLdDu0ep_pPCYNUicStcDtIvy-p
fJ2uEdBoJ5hdE9duIGZOlTeozIWdeEcBrv-sEJmKk7hNeOSBpVpAlYDTDTVpvOik-mJAR_hbNnfCY55sFD7C-zxOf
rjQdYwWLDSSH5mV4IQKzseJ8x1w5cbWWzbUqF2pNZBDEAjSpiqqVxgOAikaOwzMaWAERNOeX6NFYkmga2nREl5t46
woTvbqBTSxBMOxcS3KCbzmTcqrLVfS9Cci5DaAdUjad8NzMQBoHywWIAFTA8Bl4p8cb7GqR9FcJYVsM6QlcjcGCZ5
KhahgYOlBH5lw6bRMi48JzHrRWa1otXxmXprcLF4QiBKEZfKpHrSsszlCAKOKytlG7_xtNPRZ_UeZmeTRiyHWVDCc
QSzM2W9U_7hfGa-BErmW20CNBitqWZmEkmGRci2KxP7cJceuTXjpYAcVWm1x4ZVN1_JtCisCU5egDoXIi8uFHwZig
KhcBUBIS-AepvSKNdCA3HqeWzydKaRzM6Hd1iEyiOQZdz4pcGDrkcsbOgiUpCHGM_OPeIAPlZ8DqRjh6Wxa8O8Ywy
rfJZs6vLUcAjW-Jn5AaNpQFWU_VdbhTDQ",
     "priv": "q_aDEMZpRAjbiqHwO23vKcgImYieSqUsCK7wWZEsq8Y"
   }
```


Figure 10: HPKE-9-KE Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiJJOFRIbzFLb0FxOU9HOTZjSlR5azJXRjhhYl
pxYjNrS0tIZ2RmYWpIVWI4IiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiVHd6VWlPTlprbjNvSEl3RU1BX3FXbUtRU1U
zNndNOEl6NUItMzFzdEp1dV9BV3lfTDFSU0xxQkZtQmNlOEotY25hUVhSczk0eVRIT1d2Z1hDMlVuektZdUQyay0w
OERaU2xUb05nZldPaWl6UEV3a2FRQ2dEcFZlZkh2NklTWkctbzRoS3ZrZ2ZmVkxiQTNjdUhNOW14d1VKdTJGUWdLV
jU2TUhQZzJIbDBLQm9ydXlQMGU4SUg3SW45RDV5V2R1WjR6SDJjM1lac3hnSXZMSzY1SU9nSVNvbDFEOHZ2M1k2Yn
ptS0tUQlI1MHZrZ3oyZ3JESVNTMjE5Yl9qM01FRWFXeWdZNFNxQ2x1S2lzN2lkWll1SzM0d0FiYm1MT0tUWGhVNmx
GajV1Nml3eTJLX1MweFJVS29kZmlzU24zOC1hRlREcEtSVEN4Wk55WFNSYWNHOXBMNnE2Q3h6UGZ4U2hHSXpjT2JT
Ym9oREdTdklnRHAybW1POFV1RGNfU18tR1lDN2tyaEpZNk9YRDBsNzR1OE5KQ2lOVGU3LXhPWlNnZVoyNVBiWm9FZ
Xc5b0VINVhFZy0tV3MyZE5uTEpvdEFQaXN2NkNDZVVXQjFESENVUXpqSnNZTThfaFpKZ0R3RmZydzExOEZwaWJVOF
lDd1lNUEF4THpzcTJjLTN0MG00ZnJEcFN0RWNnVHRSM2FnaFlyYW5zTHJmcmxKUkIzTmZpcmpnMFRYdjBEV1ZzM18
wRUdqNDNDOWdGMWRiSXFyTmVpYlBVTGRCRVdZNjR2Uk1IOWJBSGlzTDE0NlQ1RlBuWTRiTzFhTldCNU9tZXJ6OXBG
b2Fhcm9McDl0a1k1Z0NqREhvdmNORUFqNnBNVHhFa2tJMDhSRHlJSkdqRHc2Yi1ObGZsQldpSEZTQjdtZzJ0RUVuZ
GhjNmFRcmJkU2dUQ3liSnVfV0xBUDlQcEVoeDlqUG9vWm5tVGdXVWtVNHdtUXd0WHk4RzhVc3pMbXduWHpwck5mZF
9JRVg5b1ZQQml5VDFZejFoQnJhMnVpWFZQWXM4ZGdlUWdKYnJIaWVzVnRzNlpuMGxIOVl3c2J3QjZTNGlkd2J0UWZ
EVTliVU4tUzNrRWZnWkJZVEFBS1Z0eS1Eam1tMEZrTTktTW9zUVNyNjVOM1NueEtoYVVNbHU0U3VPUG53bVMzVXRa
MDZFQXZXSWQtNEozRkY0Z3B0RXR4czMxY3JEOF90eG9ydGpnR2FUV0o5dmdrZTMxeC1VUmlGb2hobUlMSmtHYjJ2U
C04dmYxOHhOWGZmR20xeHZDR2dESXJya0V4YXJRSlBDLVdRbzdhaVcxNkRpc1JfZHQzRGVGeEdZTUt6S0ZGLUJmYW
J6bGFNRE5aMjhTeTdzUkRPbllpQklkODNRS2FGSXNKZjMxOEZvV0JqSVRqUmtjbnRPNXBsM0FpRUNFTVhfUU9tRXV
OamdLaXNlNmZIYW1XYkZoOUhRdEZUZFJmRE5QMWxxUTFpSnpTSmhIMlVkMC1VMGFoZ2drMFdOLTZpWnhDSy1oOHQ5
WlY2UFMtV0oxU3ZDeTkzaHBqWEV6LVA0RTV5VHhlSFd6ZVB5eUxWQzhqazFxOGZhc3FqRC1HZC1tMW9peDdIOHpOX
19GblB0UTNrNFdWeEs2N1hsX0NpRTJnZjRsZ2FFclZCMDI0czI0SUtZRjVwNEZZdTluaGEwVDJuMkVTMU11RmR4Zk
9pajdMN3dORGxLSjdXWTBUNnUzdGtMdnBKWTBxNS12NldQYk55dVBlbHdrcGxlZlJocFkxNk5UY2RacGozSlVSU0V
WN3pjNzlLTTNkNmR6QzNEb3FZMWNlUlhSVUluRDZmY1lDVHRXUVRqd1dXRjVib25uVWIzcktzeTRxcDBqRHZuR2NP
RG9NVVhkcm81Uzd4WWJ6di1aSTIyTzBWS1NDbGE1N3VzV0VqQzNxM2JvUHNobm90emE1X042clFuOVQxOWJSWVF3I
n0",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "d8CFuwBEVbiI_nK7",
     "ciphertext": "kmsiEt2hnihtuOyfGiFAs26cHoVya0vXhz62N6vmF4NnZP879ES3YkengaFdFYG3l16-N
7GVar6OR0h-atBeDoMeGNv7QHLE9Pky5arS4kaL4y7j9BcffzA1Lq-Hx0cQzgvWu7c9xkOXDb6zS0liTxV6-ZMFHH
dHdAd5ErMvQNtUwh8rvG1APw6QMrzb3SGUsmlTWE4-IMgq4KRKKNHHsdztLynzDcskM0yyASkO0giKYcp85uzZ3WY
wnm5LOOen06Fi1Kj-U9Hd0JmIVsy58mNnCZSeEfLdIGyP3HvLqj4ngp_OvNuBKEp12OBbouXpJ4xuPla9FdgLoF3F
oiw2GRhoqtYWSYuu4oRgmlXYOuSB",
     "tag": "l7BtLt_8bQpsUK0NS-G5Gg",
```

```
    "encrypted_key": "hEaoX4fNiWQ-xb_y31sERZsttys1fGKexhdYll0PkJDtNclb-M9rmeB7xQypVLaM"
  }
```

Figure 11: HPKE-9-KE Flattened JWE JSON Serialization

```
eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiJJOFRIbzFLb0FxOU9HOTZjSlR5azJXRjhhYlpxYjNrS0tIZ2RmYWpIV
WI4IiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiQkxWb1lHUWROenpXUV9zTjVfeVZWOGpWajVqb0ZVSWdRVDBwV3h0Zl
RwLWgxUk91azZZYVN1OXlaR3gtaTg4TW1sY0EwTlVMUHZEVEZCX3otZUJ5dHlubnVfZnB0d0ptaW5JVlcydWdxQ1h
VOTBUQXJ5Z3RWLVJkY1ZJNnhkRGFLRTJjTmx5WVRIVHF4Z1VHb0ZSNVEyMEVJM0dSazVSdGh5REx5cTZRdUdVMHk4
RlM4NFB6OHVCY0VPTnRtZWJ4cW4wUHIyWmFJNld0VW1IdzY2SXJWLW9ZXzRBWk5tazZmOUxld19iVWtFU25oRHBzb
WVYbUpvcy1DbmlQZ1I4SDZYZWlfRHFTcFpqX1BGRTBmVVBDNW91QW1zZ2hRQ2pNNm4tUnhtbDVJd2xaakgweW9qby
0zYkQ0SkxEazZUV3Z3UUF2Qkp0Z2dUMFh0dTZJcTVTaDY0TGprZHZTeXZscHZHckctbzNCNXdHYWh3X0JpVDg1aHV
WOFRadkU1N3FSdy1FOEJqbWpoNHY1eDZVNG1KdnNpQW1KS3NCNUxRdno0QkRkU0o1d3Jqcm9EWlNYV0stVGI5UjJ6
MERKTjZDTThvX3dMRnQwcGMzajZCWjZKOVFIcE5UM0ZUV2NEVFQ5b0lKSHBUQjgyUXpraDN0LVowSW01ckc5OUR0O
GZVY1hXWHVkOWFTV3JUekw2S0RVakU2bENmTnVTRHJNd3JNSE9Nakp2QU5sS0phYzRkbUgtMXR4RTdOZUpBWkFnNE
1ldVlQQ1NFeVNKMUpvcHZtRF9HOGdINUlKc0RIU0ZYVWUybGhCUkF1djNlQmtsY25sSUpRQ3VKc1BGSmVRVkNYU0x
MWFBjcDlRakVXemFGSmc0VDlzak5BLXZNZ0dQZVpYcUpuQzRMcnhPZkVaSHpSTXJoaGw1WFdWeFJ6a2dZLU1aOVhy
clV5dHVnRGptay1UUVZzNjdyWjBTY3lNUXpaVWpmWU04Q3ZJWHUxUW9zc1ozNlHNN3ZlYTh2Tkt1Rmw4WFhPd1RFc
W10Qlh3Y3puYnZLcHBqaWU3NE9RUndJSW4yUVBIRWlEbzU1azJpOWh3aHY1UzYxcHhQMk9Ga0NpTG9TUFU5N1NLck
ZZNDRPNEtSbXdkalp2WkJ6VllkUXBWWjdNY05nTGZoOHZpR2l5SzhObnJBQVItU1RXdTc3UGJNa3JMclZzTHE1bVJ
qT0o1S2NwbjV1aFdCR09EdkwyWkZ5akdFa09ERVpWcUVFLUpwYkc4d2d4Y0JBcTg3TUZfTVQtN1dqZ3RwRWR6NGxZ
U05QbTFaQklZUlVOaGdYaTRrUmNhVkhyb2lvdmFTZVl1OUNDNnZNeXhJWTk2Yk5pMHRxTVdmQkR5dEJfWXI0TXpOR
HN4TmJmMzgtYVpBUnRodkZtT3F3Z2xGZVNjSTZpMkI1OEJua011WUJjbXhzaWFXeHc3N3R3Q2M5Vk5CeHlRRk43aU
FUcjkzbmFHNmNUTWlsQXp0aGpqZ3hhVkQ3Z3BUb0Y5WFFMck5EdVdTWnNuOFZDV2J0dHU1dkhxb1ZaMkhTNDllVTE
yLS1vS0xWWjY5eTRwOHo2cjU4S1BUSmo5dlpodXoyMWNubzFteW41azN5N210NDRTb2MydHRlZjdwQXBRLWZLMkxi
bGNBMlFNMTZXMllKdWhXTkdOMEprbURKb3VpQXEzS2xQNGZyVS1mNU8zdk5fLTdCS2ZYVGlpTGt6MzZMb19Jcllvd
0FpdHBpSHJKSl9NcVFzX0xrRzJHZ1RFTWpNeEc4RG5MSlZPYXFzdGttZWpFUWN3cTNOek11S2FkSmJqVlVLNlRncl
83S1BTMmRXeFREZDFlelVPb0hxZVlrY2lRNEQ5N0RrZWZBRTNVQTM0QVUzNVZNSEtpak9NM1ZaeURHd1gtUzA4VlV
hbTJmMThrclQxNTMzQWVSZlkyXzVnWVktYVNhTVM2dGZXRkU4MGRNVUNybXdfeTlTOE1nIn0.m33rDckJMAweQB0e
1C7cc17C52_oNyzEtnoz5VZ1cLxEAMdx5YD-AP7wLeg6b4aQ.l3pLYmere0K8G8AF.k6oT3m_ISW8okLHfAjFYBlT
tMpB2rO7mRgkjHRSz-uGHo1naLCfzcQlgDKm4n5XmvUnxJ09Z5Xq877G2omHaAnJXWjA5r1zv7_rB7RgrkkU4EMPP
fRYlRqlfReYGEv5rH2V0SUHMmVABgH1NbmMtWm2ccwyKtbZEgxMru79aDKbZ8MV_Zkt3hGJWVcQRYljGL-MM2gqWp
Kn8Q73FT5CX4HsiLI0zn_b5j4qDXqsZGz_A66wndg5vcSRyt6F08bfvQ5hptrfdftUeMKn1z7PxI2T3Ye7AI34EIQ
dIJalrmGMUdzNU9xvLdwWD3N6Cy0HFEoWvFNpXVxxcDV2ybCRGsNzP-RlNhOeD56l-6Pf_mG7v.77mxN7ZlNwLuUi
o3mcxoxA
```

Figure 12: HPKE-9-KE JWE Compact Serialization

## A.5. HPKE-10

```
  {
    "kty": "AKP",
    "alg": "HPKE-10",
    "kid": "EkIcXLM8dkXQX6mzrxYWNBY8lndA5H3H-v8TfiSDLfI",
    "pub": "1KUYqsq90ghiwoFuSJjL1qKhZhRQujGf6cXJtSRSJoShpMyQGMdsu-eTJTE6FnZeUQNtWyNfsRAj
zQqYgCvKB9MWZddwzkYlCqRSXlcSHmgQCLkj9_TIJZipHIXL1km4_2nGOIQ80PCbxscLN-iyKKt9ikJt1Ks95aa_P
SwRnum14MVuHIyZu5wAQxPNTjw9S3EnI0ODyDaPaVG5zHqIB-mW83I6WfJUFQRErfRHjTwWhztsYLNkdjHMZYKxA
iwouemzdymoIoBxaebXIyLnHsAycKP3NByWaxMXrEpdJMGQveDwbW1sXOffAulTzw7boeHBdQcGINzg7xiIXcgYeq
95KmqbNqKMkZNFiA5wFpOjoy1kUE9snCwVsV-I_dUrWckargyJNUONoRMOCox4cuziEUU3WkBK9pOBKV1WjrL0kBq
BZUy2DhsmJLG6QjJLng4M6S4AxAmCwp_2zNjFGaMbLZCoKqPt-FGe_uXyAVqoYeZ2jAfWgQubrRAl3NVd4RzAnQh4
hp4gPU_t9mwS7sD1kd3-zm0sCiqRedvNGag59JDFAIxuUaw-XrMyVx6dZG5xfOnaUE8ivuZ64iPQ9asASugUFVJtu
QgD7pONlw0cUQq2-qVV-QTS3SG_Agdn-SDhqe8ixVrqQI0TYmFVAquRniDgEx68NM4jmyPvwuEQeN10piAj9w7jOd
F98dutkd6UsQGpPcgXcsCRXrN9uSLpVQCJUUzFoG3SBcuUEhh7DOr6mAcG0Zae0c9E5e2qTZ6bUU3E2KZZXub-xcZ
j7oGSspwgrG2ITd-xzi6aexu7guYMMaP4ek3PEhjUFwV5HgtzNSgp9SOQEAPlYJs8mCpE5tNsYquJ0Q3CXYa6uqe5
SKYY8MOpmkpuajOmIQEbvUjmJQxjSQxPXcDP0a0ucdbG0k0kshqrPAUWvSoLSjAVxAdgyxe5pdXICkrSjs0LuG7fa
c0gctlw9RIurq36EF4EitsM0WhAeubkmEd7ghIB_FImfQKx7JaJscx0taYAehRD3lN3dA8m-NNd2JkX2DBXmQyKqh
1JslcaCHNYaco5rlRqvpwR0t94_nNbklO5oAy25ZcJ2iaAiwAkPSWptfMRAM1P_TMoTFTv6R-qKAexgqtKYBK5_aJ
KpGjCri4GSkwv1RPeXC3mrOJNAJ_8_jNl1yVjVVVh9lDSTQGOrtYWlmHA9jGATRK3eso_DO5ONWRytaY_awbxLJ3Z
eSttLZEl3Jj79kd1LigAXFmLiS5fNxiqElcjugb3Wx2dNPEhVlc2dI06Nm4nnfIEUZDwzkfDcU1-dJV0PcUCbAbPy
oraEqVSGJwMVFkt5a9QqqUXKY03hJsTaqEukgM0rYoPlEJ_UuqRptoGFZBWdSct2pEI7muOZA0licZpuYqx4jGCAk
jS_xuaFKjieExA1IGySoEX5ETuREZTtNdp9hDKyJQ76wVcoVqlniEHeUTSdxgTIEGM3NLacqxHFVAmgURfAojo2UC
x4sXXdK47RtBuQiBf5Z-0hx2DDqvgkTOKzy5trEJ9MhvKctYsYRWQsWz5ly0WTAgUeLPWYWkLXxi5BYAF2KqF2yCa
tyQ_FQZO7mwCZUB5ZutKQcxAOAcm3JGQRsDL3cG2MBlH4UkOihSUNsbsrJ3p9i6HEFc8IVmiViuBtEZbdFZ4wKD1J
qah3ghkjtHbhwLdME4ZQKs5jJZvjGFBsGZG0KCYGKbf9QQ8Ooc-PNjyOqzo2k2y-ETtMCos6KdcnGbyrEBVKk2rKL
JuaDF_CQ9q0YQdsQ70VaBjeckNGLL22OvhiVN7jbL1kJ8bubIYeymm1KyLRcT0xmpDDgYtvAsygUdQykKbtSmOxhH
ZrcIFeKazWWe6qcSZCOML0hszyw16MGUiLtVfEAvp8gzrGWQFCA6aDhrnSs8YDMAz5Yoflp2wai8H7gC27ltycEpV
```

```
sWz9oBhQPcmq9C6h_kX7RqfrtusXPBai1pGXBIz_tu9V6ETzgszMUFOFdoKxscc5JcNWgWRaayYDBy08VenbQggLs
Od_BsJ8kVV2fwnIp4dGUmthqqjVkrGtl1OKCYX5_wb8D6mCByPQ_BsXIMEJqvQYJp8bSZ0Bp3NUvY7EBwNvM1gfMi
Ow_pwcXoglaZNgzWLi_VBzXIY9lcM4qjigOlj9JyfbYRGPkTJ5Gj4Taj57OC-wIVoeofByZ5tLATYBKFPwjA6SlRh
I8j4EiKN",
     "priv": "Ru9DwxiJ7BdWBh82FsXaAPPR4s5MZoadKL9y2wGmino"
   }
```


Figure 13: HPKE-10 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiRWtJY1hMTThka1hRWDZtenJ4WVdOQlk4bG5kQT
VIM0gtdjhUZmlTRExmSSJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "PqSkdKSW75FL3sRXdax8xJP8rcRgzVg3pvPe5diLa2U7Zq5rklP-pVqcS_4YmoS132
XKT-AFp3Ft2qcWu10h2vvFSoCLH1-6IKIIE8xYHe8zFg09mgOcLhevHKPnQ2d6KsghZLUJjeN3KmFRS8Px2Qmntt
XHl_aCkcWC8ztu70fHA0fR9miNtjeP92J69aXXBjzqYvPn7ZIapiYUXTQaLvMQNiMOwMv7g5DYY7mFTBh9nWyPmxv
-WrOKGsd9-Bo_farLI64EIgkAogMKA7Xda6v1gCu6ne6nQoP3Q9YLENSDkfgBbj0FBbAehOLOEGkkhCB9qX0FvicV
98CBXwI_42bYar3v-My_g5-elG5v6OqdMB4foD8cwo1QG4YB7jHwqrRBHp8Je5lWIHhIUjmwrKNM7_kwp9phQ4Ix7
SUX8nEIhXAwwaNmlEzcxm5VdGlts1SPtqtOfRmmRSpwJVArA50tURKaMsrpx8rLJKkJEpyUWm_4O_1U-7fQXCfURH
0LVPPePi7wg-AYizp5zAGJPTZSBqM89imBiC-a0jeyPJBgm-ZDD-kD2_Q5JnTUMWTm3v0oPp0gYW3eO-rCjLebcHq
9XQInKq_wgm3ccCkjuWvsHUyWsw6gQDEqljNSCyWIHS4RJospOwuJ1ruw1sY0mVzvpK9q7AMFJ7_8WRAgKe6pokSQ
-3J-stoVjNaT8T9cW8zbm1_2y5epgDzPlI1UFVXWG3U6VB7fQAiL5w7HUgTB-2GQMxRURz951l0jLvi7SkZGFag8F
3BBrH_H_x9kt9aVj6QFuQHK-gCK5OAbgeGNLlEuG4aVGz6EHvc58gXr7AsXr_aSscewPPSNy06kQnh8Q1xJIuxvyb
QANSKUk79ueUzoOPBL0Inkyoym-nAI25gpM1cDFUzbmOjrWOaSLHz8CojJckAzuh25IROCzHhMNSa-y6_mFt2htSF
UQAMrZ6Rx3kq4KK2MlK61VLVYKUHmvMA8SuiYCgQVdKzoG2sYvPjQLFE4eNKaPXA6wmrOheu_-0pLB4ysflgpCkEH
3hW7xuNbMGgkkg95ljQ5xJCSl3YtGyCKYAyU4wgLX5t8ojnke8eCyaS0Pz70dr5j5viS3s0CzNh37gAEq-ez9_TeW
43aUBHp4raYtb-oedm7lGl0FuhgCU0DkzC9pH30gL7SRXM17eLGO9PBG2hwMjtb2oKYScDiObG_16sFSOI2_jhWjv
7qfz7IFX3Jr91MfIB8foQPBgfy0TFPGjoOb41uquC5f2qJYIDkne66XA0cvxrSfQ3070a4DeNrT0l7q6BIR-CbX18
6OxuCB5r790vyQAT5WyXf9OXkC9woysfEf0WkHvEme9-LQTeZJp_ZRXaJSbOJZslF80NaTY4t4IPfHDDchntXHyvt
tJMJSlaJMKjXYOyQOr2JqIDJ-95aoDQdg7Up8jR4MpAL9pbmbh_7AmNVGjN9S0u2aszJfUDNqg1LL1CD9WqDg6DqH
UWkVv0XZ20tf1fcOkDuc9EHPjyyjNZ7kTsrRHqp49vsRayY6jkKJPndLtZQTGiiKsdZEavlGo5XiBeNrr0OWY-Yhe
DQMHxK2aQH0GxQbigqriclmQiaaKn3LTv7MtkdSo-8QaZBgO6tF60i0gKtrPNkHcyYQicvZj_RIZGh0-VfA_GutRs
9ozqSzajcbmjoZl50rsLK5MUOXHGztEi2hd-z9rF62YpYLlpnF7dSlsc11LlSuxEjiorshM5F3EqolNsnjHCEA2Xy
wYfgYE7cDHD07cvjCC_Fj7mlWSFhE4pyX-jOEtSAD9c-iEUSVXcScjeApwg9_c7hYC3njVQtvkI7qh7bA8w_fgMiw
rqq25EJEw3pw1z59uoEhB5txVzzyfZiv9xvm3S1sYMC_UL55nCad2KwjaEavl2NGua6WBbHlIUQ2EhwmwzCUWvvbk
53c6WoJtsEWP2h6CNN5y1mi9_7HSrIU6KVQXC32jUsQ542Xv_eVzGz6uaxRsBK-QE7CovOhUpFHR9lf4gmJaox5Gw
hImq6besAmBy6g-3PwpwxpYAXP3qRefX9jngLfJXc25eQvpwmNjKQMnoHrs9C1pZGFsE1r99wKUcahH7bIvQDk4GK
FcL4eoUqlij1RlP16c2G1LImEWOBXWoqubqVqfU6OvH8NjqYKc7deIHGfrpu9fQCy0l9En-bLXwCAFklKXjeVmmvE
ilbaucHuvznrgZYexz",
     "ciphertext": "9kfFny-tTRwymjXj75P84eWObnYaSy3BpPcM4Duh-TMYi2ZjKUDogtdcCwN92Whe-O8RC
BcEy31EMcair8LuViyVmB1MTe2EmjZAf-jAxy4VY5nKU41dP3KB3TRNeN-6Yb8XmGa2jW7pFHab8lTz4_LiepU19M
VN-J4L4aKrd0fHt87VQLHH6swyz-NdheA9cvVQWcV-cOaoh0gfED9mekWhF3iLKVfTeJjs7R_ZbcmKnfx-rwcPcp0
bfQlOwqpjygmjyC27i_WKX6VAzwf0onjH1mgWUU8VuND53DzSgjnMvc8QNhD3VoJyAM55LF-sb83nH_ShtyiQCVl5
r66uZCXkbMMVgySw1EBsfmLJUZzuiZtr9U8ipA94iU9xM9zIPw"
   }
```


Figure 14: HPKE-10 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiRWtJY1hMTThka1hRWDZtenJ4WVdOQlk4bG5kQTVIM0gtdjhUZmlTRExmS
SJ9.TgRvKwbOBAKJZtbM4JyaUwIJsGbiSlIK6uOFlP3FBnmxJJ935SRazR62b4t7lxQiZwJZYrpPM6ebcgZ8n0lch
Z07bKdCrEJwJMuogXnK96hBl92IriI0PzlPB5Hzz12dNmSFqX8nhOWTZ5aurXMaGoU56MUDxzRMM9G_k6ryqYGsoG
bJ-KI5e2rG9UImwehwG8ObmgUy60-Z5Hv9DJNbs14SWtDybh5eUey3yNpSAjj0JuTd2Hh4EmWwsGYby9vpTz3BJ3r
vAmBhnZgfUibotSzdweb5DWFPcw7jQNNd2sg1HBLQq-A1R5ReZA6hfimNE96y5g35_4ZiADPHqoRJ7VM_stA4IOEi
rNixdJ46dhyaQ31s693cQ1TF_tUbrPaU-WNv9PRAWnXeXF5-T73scRKCOTR2qFz8lrrmm2Q4xyxy58xKfJcFJbo_g
xgFLm9TJa9vWsRN6lyzCHwL35bVjKCgMyBEiKAGAin3_GkIy_hBlKoAVBOfcTKEdR8nodzO6JYOfT5GbP_C67IsR_
r8H4jDv4QTP7rgbh0BVgpnSBnORR8ns1l5oQA9erEcAWSs47SYEc6NPDIWU714SpH40LuJxTYNqOqXpk6-Mz_apPG
tN5GDObTzAbLnwXRatv53gPtFORWWT5mXu6zMut_QgB5GElvQwWyaWG_MciQ6mDpLlnA3Uq-3Y5d-pkDvzmx1fD0-
1VUk0W0qRyGojH8fPgXXBzljzP45J_g-ZVZkvB4LDQIP-uiww0O1TpoZQQMfJcKg2rfKzpiT_AxZ8eP8H09Vh7Cvd
TGKKpeizHWxIW-DhJFHLzjfgfT5Sf-BFb0P7SrIrJBqnlMNawy-41y-c0JIp3xp-ag_c3zrsZbN3pp2dfsWEjlF7r
MbBBHBJ7vZR9Uz2c4Nt-Mv62itoNBOW1foIZhut1ie-p-41ZI3F2WSNzZePj_gZnA_4xAQpAx4PPYut_QQ_cO27BY
1X0UQ6TUSUysQcCPw4D4-uza3roA0smzm8Gmw2Ejy5NQd8K4GPY3pXIs6qp_yVZpIBz7gM0YJx4rtTu_lrMBjDWgu
kq96PJA-dbuP3uzTktl2kf2qEHaXaEvUqYX3Vaigh4yVwpFeBQEbXJc7RZ14pqkQuJXRI89PpJsxsr-yOVucir9Tu
ubv91UJuRPFFI5GWP7qv5ZONTt9SeWvq6AyeS521VQVCxvQReRHGt7vj_UU7a9BEEhcQBL-nxD9uHq1u5p7ksGLV4
uiMeSzn0SgthUTFSosqpWi1J-vTrMrESINuwq89vZAHTID6VJ_Vgk0Ahx-3mrGOscjm_8slQJtlibPTrpAw3K7eEe
vFUERor2ItJmprKDJQBVDIDhXCbTnACf7UsGr-va7Km3miy_iekhebmB3es8LSG48JG5nsyPdOOKfMRhVybgEqyRu
nfzmW2nC4-drZS3_m3uUKIVAZVbiDYQjtM_vRFa8reO7H6_lOQMZS5ikE63KzPS9QwjcmsBuksXr1RhlMXO8tHGRZ
```

ILAEVvxqo86pLWVZWPcrzsVmm5tMMGezykUKjRwh7En9Wy4L6DeYnlrN36DGNgsEHGdi1yry__pH3NkT_lRkyeane
NvKdDb5mtyig049XYxhxmPMKwu5hHB5PGKGAhSGeyyoAjSik8djxq1kkDKIlnXNMsMGGfHsZPcaqAGwbuD5mg1IsE
E-r3jRKTOlmjwUkTOQcdwlq4X2NibI4Ul_1tI7ycZJlY6C7Cw6qOQTRdDfYOd1fEd1LsHRp_D3uThgBmB9OjDlImw
ER6S4_sQR7cF94twgO2OpPRlk_5SIXDCoFQ25HPHZHm7PFcKFTf0wt186arqwiTrq0Tcm9IGunkYcNm6uTYzUqm-U
94__IDUoN5FQcHyr_m4zpZRWSC1z17B3gSIC3kBqanfFjzM4zPN7IM2HZpcom7Ib4wIc82yiHuD4rof5M1DvUHNf2
QJm3ec6Ma7b1aVcxmwJW_EHk9DvjZmLy2RRC2xt6UA_uM3H1DdBpg1kHyv2oZnV0UiMvQdbisu4DO_qBgR-IWYxXl
cQ5LQFlDA6WjzJjcjKD7Ngod-W1so5J_64i8KbGpoR_P4MfIEGjRe8Y1KihkjLppWehZwoyD2UVzv2wi-sUTDcaRC
M2tJn28asl8EyRW34FvCZNrRtTabcZbH2xrz0EWxT9RQ8drbiFJqOHus7qMDitXKqXY8MuICyR5lu46zPw0UjvLe.
.XNUZgrnJGf8pQMiH49mqGqzfA5MjcMUzpWBpFpLm7tF0qULkHgj6IkG8MLwnwSuRXXIxo0wvJdEozwKeVsXwokRa
_V2kmUdKFeg3ger-9qw4fsz8AeASDxWDOsEzLX2MiJq6WXpVdJwQum76o8vLSE624ATEAz3aS-VXauyx1Fsn1wKhw
5Yz9nIp9EHtpR6gE3-osNLIai6fPzyoT9V05CDFaIuOvLXWRrggM3vYWicbdInOMCnCdTCj04WVt2yzwnm-ZJw3Nk
Meq9uV8XCyXrbPyGWgLdAgUW7v9TcFQWUAEh6dGs2JbgUJgC0qFopRJBtwwJJ2fGOnwyZ84gpQK-zBqnKp_kn-6jy
jl9fPRfh2jPoK61Sy7gTDXV5Ceq55Nw.

Figure 15: HPKE-10 JWE Compact Serialization

## A.6. HPKE-10-KE


```
{
  "kty": "AKP",
  "alg": "HPKE-10-KE",
  "kid": "UVzPOxx3jthVCg56hBO353HIP_hObFaFrI-pf3maRr4",
  "pub": "9ALOt9bAhXcL6nyuwPy-cqzMgPbADhIWe-g3IFA6fFUeidZ_SDun5zbISBE1i5YKT9STKCBYVlCU
ZlAo8lnMtbc73bNy3DNkQvii6TptYNmPTXmwauN5qsUFM5ouqjFtwBhQTFkVR1i5YuOynqhC4fp5Z3lcEesDFRQxh
wGJlNgxiNGWkNKkeWBVELxU4yUPHUt366Z5_8eFxGxpRALKxrfNamuU5zeokAxmLAsVKZkwfIISxQV6EgQ0JCgApf
RXp1gaHWk_5hBrD6WKlwagDFWO9npfrhFtHHNCm5U_FdTNheampphf0LJpdOLL2BGZWtqYn7xDuegxEJCBiWoBoEl
4wpMcz4kqIDchWzTAvaCLtXvB0FOYlKqGY_MosDMIfYRpfkxlTdKDxMxWC_YZdTQCW9aGZqu-gqw5RCmwkzUUxKrM
W8lVWbRXHsGa1WQmMTJlTLGGRnBP54YwisvJp3tRvzy3y-JXDadAxeK5u9UJIMZLvgmAs9cC3xt79YahZbo8FzIRC
QIpUJsh7uC7VaG7f4KzgDZSEIaIqMRKY7uTUvasmiZbtoBMU_GPrwZ0XmFNi3R5bua0ieBu0RWducQaqrlQAPYVfR
kuFHkPsMmcFToVmQtq4YlhE3hsSpdVIVs-PEGeKcciBDtJEIkJzxt2tsDPfagb7DlQQmqMsTg5d9K-2FYFUny6n3s
XL3wdffoM2kG_XLwmpPERyxOi2uq_rYYazOHBWPxCdPg-bBkWy4uLOqp81vSHx0R-JpavAMEfs0dzLAFYo7a8BEpU
cmNo4cciVsoOV7lUkqNskhXCtSeoSKw8zDxCo0ye1cMGNuogZnKNCPhGUSo9igeAcGqkHofMS3B4SJcnHYMMD0QJ7
eDE_Hh0cMsT54aueuuJ8PauLHuT4mokG1s2exZP3uaXG1BmPMtpARyCJTNax2Qd1OVqqxukummV33Ja8pdC2zULU_
XATzZjBdiQZ6e3R3vLQgtH5vpvnzBHvbRHAbKJdQS_szVihbeUxgEdGSwtcgHNQMMamedO3qmHYsRqc9lPo-W34_C
UhyDHq6K8n0kgcxFBI-RmM_iE8RIyfrulMyNPXdnJ1dJociljcSUyjpZIRgE5BCeS7sGp1ZJ6c8w7JhiSDEWTl2OU
b9GsbXNLo6PMrIBWkgl_A5EpMipqwgLQPHTCTmIJF0usHcYnMtECT7U1dPQVKgSvNusaXldU5miARrvOn0osBnk_u
zPBayCi8DU7chRXMnoMSQlhOmeNIwS6d9RM64HI0oAcwAAFkYyV-pMvqRuz4Ax-EWlHubrGDvbMWTwMNpZOhzNhwD
IslaggOoqHqZMegozO4qkjcueLDPBBZTamjdeShbkQfvcSRix_fdphv6sdnXyN7Umr9kxA_3dLS4m0AFuPBACn_So
hc-gLwRSHLueo3vut9VUbltNXTyQSHBzC_TgYVtCBPLKWlSvGhNw5eXiARYI659l2ObeD-8JQFjwN1fEcesBjfXWJ
KOhJoYbC2dUO6fLKolxt72UU5ZWcdwYjq9W1WEO8z6C1s_QqaDOrKCtuLRCO03lcXLIkKHkwAaspTVw3nhB8_6kn1
heCfjafA1lds2dx-4zBechsq2E7l6GnobhnhUp0-HQXuGeTSiO4aamm0tou3-inXpNzuXsR6CYPG2q1RYAlgWoLJA
MijgTMRNxtvGSPg1d52qxDXBQIpJOTScQf3fONnHBb5GZHTmiQ-BW9zyhPM5KUEoZ07nx_beEhzrtMX8VZOJe5swc
dalMC8MejzOYvLhh7jdFYkeIbbgkxMBMZEkHHtfijFgC0T7qCLTkQAtXA6wKZLgjHwxsWDjsTDuuXglDFxxhv_dJN
UXLD6XQe4vkDxnEI3xFBzVmoZ6VsRmwKdZVo3WylBShYO1h8YBaT8iARj8x6NekIPsaFFbs_KOhLR_ttA7ETiGCrn
_U_E4UFjCqyGcZPEFvPc7YNcyMi60ujwIh1pWQEIDG8I5qsZwMPRXY1MXY_ipyOVmE2sxUbhWGDrHgxl7Rm0swGBm
Y8JdBH_dZ7IqQUmpfcFmsztkfIoV36-la8UmqjSN56xacvlWK6Wwj7RTcE5jkstUY_rBwX1kBU8IITnA8irT2vsR0
28wS2lsVFIVcmlGloIbCU6Oazzm3MujqBobbHMKqXnv9Op437pCNlilyNtAXS_6ZEcLdUIe3wTTxAd5idwaPiZKy9
o3KyjiWZ",
  "priv": "uSDPZnwwnLpJ18lwAGHj75e-fGohW7zOWhAG-7DGLis"
}
```


Figure 16: HPKE-10-KE Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiVVZ6UE94eDNqdGhWQ2c1NmhCTzM1M0hJUF
9oT2JGYUZySS1wZjNtYVJyNCIsImVuYyI6IkEyNTZHQ00iLCJlayI6Inp3aHhKWTNHNmlqSW82TDJCMk55b3lpT0J
VY1FlVVE0bTYtZlFVTHR2eGFHVDh5T0k2SWFsNUlaa2pxSnZIVlZ4NEgzY0cydXhxRFZ4dXVOQlotTjBuWW9PSnot
QnJjTnh0dnRUMHlldXo0dE44QmlIVm05R2dFNGtGR2JGTk1FeUNfbm1vbDZvY0xmY2NWMXJCUGxvQV8yZE1BVFpJN
WJlWlFpTjlKTmw2UWktSmdZbHlHTHlFX0NtZnhXWXhVRjBTVzlhS3NmaEpVUlJRVDVlb1FiMURNTm9sZi1EQlBlMk
h2cWZxS25JalU2T1JBb2ZSbThEdEJFOEFaTmZwRUJWTUZYTU9JcWFYVnV3OHdCWkhXVkRKQk5VOU1NSUtlUFBqRW1
UT3F3QVFCZmp1eC1ES1dYc0J4S2xmREFyYUV4UUtVUWI1LWVHSjk5RTRJLVFGd1dRSDdWYVFRRWgwQ1lXNkU4b3JF
eXpzQXc0ZlIza2wzbGJyVmc0Z1R1NnNpX2lnaXZYV05EOUNXU3BXNy1FSzE2amlQQUtlaEQ1c2w2eUt5RnZLc3R3c
UZVcWVidlBPb3EyTDRaWGxnX2VGcTdnYjluSkV5eUFvT0NPSEVJRmViQlVFOHg0ODJLWXJuMTlsQlEwWGtEdmhXRj
BIV1BYdFpWN05fZVBFX0J5dk5zMlpqY21uaHNJSm5ESUZHbHkxeGlZcVVvX1RPbkhzdjhXQzc1QmhZbmRGYkZsa2l
KOGVZU21QU2hkNkR5aGhzdnc0amR6MzN0TWUxdmlVUnI2VVB3TjFueUQ2OE9hWkl0OW5NQ2dERVJXaUZENmN2eWRZ
U0tUdVBqaXR0ODFWX1JsYnItXzB6M0h4Z2F4dUNxWWhwR05GOEtoRENPUUdVc01OcURUQzdqeGZYejRiWUZxS2Zld
GxrTWdsUVRtaEpmaGdSUHpUNC15dzMxR3RWb3ZaRENGQmZ1N0dkRVVsM01zcVdCckI5aG9GdEpfdkI3V0liZ3lVbl
BhS1JqZ09SeFhkLTNmQzF1bC1fS3RaWS04aDJRYmtsMlBibWc2NEtjNktQN0FRcVo4UHA4U1BTY1AyR1dWVUJjY2N
ZUHJ3ejJWVzhLSXRBRFhhb0ltSkZJN05OX2xzM3V1RnA5SnhkcjBpQmJhV1RrbjNUa2lLanNxVmVBd3ViMktqZWRh
cGNYT1BkNzhCeGVXdFJxcHVPVUJHU1hyVEVjYkJLdUxaS0ROOWtPV3RZRVJ4VThlZzU4QWJqWkN3UE82aDJNN1VDN
lRhMTlWQXdLcXZNQ3ZFNXhyNTl6bmlzY3I5cmhfUzRFU0RtZVlSd0U3ODVUNmRnVTdWSV8wdGg0NjJETDhxVVQtNW
s0dlloVW9xbDZRUkg2SWdLNGtKb2FKLUFoTEpkclFiRnczaU1KcUF3b0ZRbzF5MHduelVOUk9nU3hrSVJsd2ZaZnM
5aDg3aTVWRzhkQW1Yam50ZnZMbXU2WWd0Q3FsdlpQOWFpQ09jbHlPMnp0MlpZdmhqdVJuT24wb0ZTVF9YNEdfZFlQ
Sl9nbURLWFJlLXhDb19peV82eERVYmhfVExHc3EwNkpIOHFBU3p6UWZRX1VONEVLN3FreEQ0S0lqaGQxQXZlX0NDN
GtUWTF2UE9MR1NMX3NsYU9EdVBGbjM1d3pwU1Q3LUF1blRBdGZwbFBTNl84bXpjUGtudmZ1VUg5b1BMTVp0RVk5UF
lSNVBDdmh4ejF2WlVPaHAzdjFIX3B6N1gxTFQ3UWw4OHU2OEhOOF9VYUdiMHpna2ViNGVOSW9ZZFdDdEFncDl4SUV
```

```
wemJDSTU5UzZzTnN6UkZWQnVOOENLZm9jeDM3dE83Z2Rzd25fMkFyQUpsTTN1TTZXM2hVTHFKSFl1TmRCa0cxTXph
VjktZThuMUduUk5rVGFycEIzeUIyd24zdi1ScDdmSzBBczJfSmFWdDFReFkwTTlDWWZsbV9BYVlyRnBXMzcxb2pGT
FlhZ2pLdXR5YzhyWENReElfWDBnVUgzSVBFc016ZGcwSm5zY08zN2dQLUVWc1kwYlU3bnVSanZWdE43Z0NtN2JYNT
lnQ2FzZ0pRaTdBNU9DaDA1N2gtSnZMVjllaGJnX1Fxb3h5VFJIQURGaGpXQ3o3aGt2Nk9tTE9TWVRjUFFwRUJBcE1
0NkpLSVpYNktFRkhCTEI4RTZsSjRyYU9VQTlLRDU3akxpQmdZNGlXall5clg5QkZhNFFteXJsZV9uaFh4aG9qZ3Ew
bVVGb0VKVURFQlZYSGFUTnhBQ3c1T2lJUmpuMVItdThqakppVm9rYnhEa3pxdTBqVzFsX29xUW9WdVVRN2QzNWU4T
ndfcWppQzdMNDBfUUdDTGJUMlRxdWJzR1VMNF84bDYxeUVHdFFVWEpzTnpNUVpwblI1V0xmMGhXUjhjeXdiM1poZE
xQeHVjVEZXYzhZWG9zRHp0MEM3UUs1MjcyX2l6djdwb2pkWWdSY3k2MlNTS0RqYXBwTG9NbFlMWjVqS0g1bXlETlI
5a1hiTktIWDcyajlYQURGTVhiRV8wZko1bkljbTJ0VHlLT3FxSmdvR1ZqUnZlTE1YNUZQdVRST19iQVUybFlWdXhB
ZXUtM0tuVzJ3dTROUHRIbjNPWHUtM0NMbFZQSjczR0s3aXRmXzlhTjVzdmduVnFOd20yX2lXc1NndlJldThiY1JHR
ms4NU0zRGJHVXdlN0ozYXFYQ3Q3aV9KdVdRU0JiWE1ieTRSSFFTbVpxSFBqV1ZERWQxaTBHWjJZV0EzaWlYY0U2a3
FTUGRmWE5BVF9SUEpocFRjUTJrbWFrOTV4NVMtMVdvSjJXQ0NWdWEyODVnNFZaQ0x2Wmd1QjNESzJRUGVQRGRkdHo
xOVVaVGdvWmpZdjA0V0hwTXhLN0lyZ3llS1IwV01FbjdjWDBiQ0Q4OTJjeE5FZXRhYmJNZFlYQ2tEcyJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "QhIHZiO-gUr7ZkJU",
     "ciphertext": "9ct3eSqXU0voatHvMht3bpOxfTEsFNcxgPHqJykMbQYsRzdgD5wN4KpdUZ8OzxwI65OB6
ifP3ekDEwqOybu8W8jlPlW-5O_Rpn7anpoYDKDw_Na6_gEIsdJi89L_9N_3gh8v4dM8n4feY_jVmuWf2JLNrLuIag
htginwHzVeSctFF_anTP6toPOAql9Nm2v4UYJlNoi56oN4jZKYSZoQq8l4Bhiw2I7IlU33_bhUOu7U8AcaEJ3bemH
gGY9grjv9E7zVk6VSsWx2kdmCMHc7uPHoT0akt-pzUBmbmJXq86z5BrWdfwPi-Z1IZ_h86rShfB3hF8FKjCQrpQCC
iAO3gWO6UBa_Uyse4ma0K5uqBQol",
     "tag": "H9VOy57gURPVe2hxW6pq0Q",
     "encrypted_key": "FF9SOzjoJxyoocqLxl7zsPeX7982LMT7kDpWdliwzPAQh4sWKE_8VGvncRwTGS41"
   }
```


Figure 17: HPKE-10-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiVVZ6UE94eDNqdGhWQ2c1NmhCTzM1M0hJUF9oT2JGYUZySS1wZjNtY
VJyNCIsImVuYyI6IkEyNTZHQ00iLCJlayI6IlJwUUVpeUtraTdNOThVaVlGZlNQNG4yZEJ2WEdISUhGSXhXWXZ0U3
JIcjA3V3c3SG1lWnJ3T2k3a1FJVi1PcDFtRzhqVHpmRTV2UEVzeDFfVmlhZVp6a2ZlVENzbkUwbXlBSlBEZkZkLVl
jRjhBamF2YktvWktiTEJrYUNrRjc0bkF0TlNyWVNuWWdlQXBuWFVRVF9ObTJ1QVZhaUE4al9sYV9SS1ZNUm81ak1v
cUpxUW5RQ3BIRTlQcVEybEV3MjR6b3pBQ3l4dEtwZWwtSWROckZYaTQ1NnRldC0wa2R0TElUMFc0aTFjNUl0MnRvM
ElUbVBxdHYxSnpPRDV5ZFdDVU9Jb1puSXlKVndFVzl1cVZvSF85LUo0SUJnY25VZ0J2SHdJMFFJX3Q3aS03TnJBOG
xsamd3UVZ0VUZNVUs5RHV6aFZ4OExmTnJLenRFTHlyRHM2Z3c5ZkpZeVVneEVJRHYwc0JPQnBxM2wybmtCUzZhN2E
4eEU2TEx0MEhJTDl6eWJGaFBzcVFVdmt5U2hCZ2EtNnJvY3k0NE1uMnpDcGx1MVFjSjFWOG9raXhLYk1sRGVZR3gw
d1U2akVuaWtfWnBJYWE5aHdoZW1qbzR2MnBieE41MGFPNmk0VklWVDhCckxlSXNKM2F5NVZSUE55UmZlOTRGUUN2c
G9hdmZKNTdheXhrRlVaZFNrX0h1RG9MaDItMHBsbzJrMkpzbVdsLTJseXVET0hueC05R1BPMC12NVVhNUNMT2pFSz
VYN3N3SEQwa0tUbkc1VjZOSG5NYkNmRVc0RWZ0S2dPYWJ3UGJnelJiRS1tc2t4Nmk4RnZnYVZidXBKU2VkdDF3Zkx
1dEt2ZzMtSTRrVDhuSERMZ3JpYjNyeERMSGYxM05CR0hJTThzVldNTjVYaXhUcVdQSVA3VFdnY01jY3RPMXNTbjJL
UFJuTFFFS1BnNVNEMExIS0otTVdOTEJZSWY4RV96eWNLTjlUbXQxRWwxR1dsREJueE1aNTF5ckwwaDZxUmlmLXZBW
FowNGs2a2NQbUNULWRsUGp1YVhCRjNCeU5WME5hWjdqRmRJaE1TNnBhUVJlVlZCVWlUYXltTlhDZk5GN081VmZiM2
JUWjhKLWVUTkp2YS1MUjd6eFBYd1ZLNW9YLUpMRFNTaWd6VTJFRU1jLWpPNmFCYm9CME11QldHMGt0UEc2WDdWVEY
3NWN5eFNEQTFCUkhWbm00R25Sb0hvYWd6Yl9FX3RhZWdiTkJUR0w3cUFvMWFEY0NiYlhKbDV2TDJnZzJDWmoxSWZV
aTE5S21SNm1yd3lPSXVwblVTMFlKVTZTX0NxTTQ4azQyN3JMV2FDTjBWOUFfV2ItOHFidVR0Nm1kaVliN3dDblA2S
HVJTE5rUDJyZGZ4NVNtb0VjX3FiZ2NYa0FuY0JEVkNhV2ZnNnZsdnVFZWlqdFlEdm10MU5SOEF3d25Ed2pNOHM2Tn
BWdnptakx3Z05GSVdOZmFFQU9zZlphN2dXaW45OS1sZ2xOZ1R0ZnJJc3lEUDR5TlU1MUNxX2RSQmVwNENCZU1VRXZ
kandMcWNBS2lkaDc1bnlJdEtqYmpkUF9XT2x0RjZ1aUJ3VzJNOFBCc3Uxb2t5SVNrYXMtN1pLUTlkRDlwM2ZYaGZw
Uko5cFRfUHQtMndKb2E2cjAxVFpIajFwcTFqR3JWTGVXRmV0N19QM0lnVUFNaUdBOHV6bE9DSzgyZktIOXV3ajVCM
0RzMmJyNWI1S1FWaHRQRTFJN2duV05CNURjdVFqS04tNnlyMDZKTzJzSGcwemRZal9fT1RHS1NBN0RhdXRqaWREMH
pkUmdpWUpITDNaNGNMLWo2b2IyS2l5TjFJRDd5T3JkdUZONGRpNjVjMTZTQV9kOFZlVE9jdmp4RnVjck4yNVlmUC1
zNzhhYXZ4OXk3WVRkSFRkd0kwUkhMZUN3R1M2S0tva0taOFVaZnh2dEZyei1wY19YSWM0cTctU0U3OUR6eDlwdlQt
UFBEbnFQTDlrU3hJTE01cGRJM0V4WlU1ckNfZEtjY0VQS2xVcFF3cW9RcllHbUw1TXluX1Q1TkFUTTZiR29PYXJZS
2d6TEZ5MHRnSjh4MWRTRkZXUl96WjduNThET3ZBeDZzbko4ZmtQc19SUFU4Q1diQVZ6VkFraGNBUk5lazA3ZzBQX0
Rxa2Z1WTdfaXNJX3VzQl9UdHpWR1I1OFZWSlp3Rm94Qmwwb3JVR1lYaUl4aE9SMV80OUphWnNaUEVrT2d4d0ZwVzN
HdWtfM0tWWWFtQ1lLcy1HTEdfcjNLSWV3RHZkYWZEcDhhNVZFOFZEaGZTVFRPdTRTMTR5aFNYLWczU2ZTbnpsTzFp
aGJpcHJBZVZSdGNKTDR5WFZpdk54YTRRTmtJRTRUTFhjVHhhakhxbnRvalU4cW9kMjZzVXdxcERldXRoM0F1N0xje
k1ybkx2NEM3V19UcDc1MDNaaXJDRDRIRlZLMl9BWmppek1PcVJnOWtMSUdyenI5VVR4bE1kNkQxQTlBeGdFT01aUF
RuenRFelhZbGdwWGtXZHNITHJ1ZWxvdXlXV0ZKMXg0dWkzdGNFcjZVeU9XZkVrZmYydXk5QnpHd0ZBVURnQUYtVG9
KV1ltZlF3NnRBVExLNkpyV0FiTUVFNm1mT2g3MWIyUUYzTnc2RzlnVWw0X0RNeTJ2RnVEMTR5am1aclpZelZzdXhT
blYzd1pVODBZRm1qemhvMk1OT2x6bk9Jc0xWUFV5QzdhR1JaSXJTLVUyY0t5b1NjSUVET2lqMkwwQnZVTS1BZTU0T
DRpWVBWUk5DNm1qdEVsc25SejdISXVsMlZaa0pQbTlYcnd6akkxUlBnMmRrbDY4ckN3OE1LNUZ2VXh3cF9sZHhXZ2
VmR3ltZUhDTGtha25HMWVqWUg5OEFMQWFHaFlYZFlzNFBPNmpqQkltMlBiTCJ9.jkEPj7ylMwa9yBW_p-Cjjn_Mjd
je7sTgrAajsy-VSxV8Ruploiqxqx D-V12m3Jwr.6S0_LInPwcyTMCYE.4fSopMO3uXyReYk7XqATTKmzi7mRBR_GV
qKPVMWJ1ScMOzcsjnvpX1pgWKuERYY457AoQbzxBmHYYvuTmXR5LZQ3GT2uYKC-NcsnNRx0q25fCR_R7N1ttksFWZ
7fIrdFVnItd2AiQKk8yoddSRh35hVj3g2BNygdA2DI55I9A0mJsx4ofxX03rPbK1MB-X8Vz75ktqAWLzLVwgzT6wF
SbFH3e1B9BLB4WFlsEdO_MIycd76LKoaUS63DFZnJJW-cAwtYueAohxwXDj2PNYVIpEYR0zDdNlkN07SALNwsZr8C
dBS5ow3nUiTrtcHcFtFgPvN-nHVPjijsFlhXYRmwjHeg58Qg8oOKF_0oJHnQqhi7.ZXV1oGmydREjiXVQtEpUFg
```

Figure 18: HPKE-10-KE JWE Compact Serialization

## A.7. HPKE-12


```
   {
     "kty": "AKP",
     "alg": "HPKE-12",
     "kid": "jw8GWrYDUzjH0aZRXlCtcokQwI4elPLJKKulziQwsB4",
     "pub": "2dmLwuO_9-eptid4KThePBhKHFBdOwVPc8lNjbeSGLOmFdmzR3yD_-ZucZgrSHqacNVD_oES2ZCS
9CEeFQyNgYQxrBRb1gQ8JYC9PmiNFWdbN-eixSaWsYaLTwekCiucwOhsSwSusRgMt0Ii2DyKl6m2J1fDgDCCevVhe
8II0Axm2JaJZaNgftU9pLE8QwAKY9tfotx3wzQRXdE61rmcEQOfIQiJr6TG-YSl_cERxbsJFryH1gmugWkjcFOje9
NSiZfLa2mi_0s6MHpkAQhxm2EVaCfHM8fMsCpkBqKOgPTKkCGTG0A6RnKgA7SclXi8P8kJupx46Km3ueR6KEGF2Rt
Bt6SmFkceujZ3oWt7Toqtc1SBjFONk0GRuZABZisiUhqXM9I_T7yagLhdQqOvsrIVllCfFOFHiJhPFEPLOAMyQUrC
j7d1V8h-crAhypiQYQFFqSq309oeRqYGVHyPLEe5m_lvfxfFMSitRcFrmchO2ORCbZQTm-tioyslu6UNDwYWarR0U
mgJIPlfNLJ98XNO5LO3fjiz84hHC0nLnOqmD_O4kWEDXkBCPWs_mzomlZKncZdiQDGXsucMUUhs-ySo_aqslswumf
k45GsP_pUj51ROcVqgjzCSydtkaKN2nkolubGv4mvNAacz99oLKLzDbqAIqoRTAbGAJVywNpBuzFw_2gGiqSidtrU
mCJcuaihnoAB-dlpCLgcNUTATJ1RtClSbXpGW9XJQ9cQ003UwfVIp8owxEsFqgkHEjRsDjJJ9sikq9AaSzoJ6q-mQ
SRcycAaM-OdwaohFsrEEtVRZ07C8UahelEMmZ2qtEMEHpkEBiNAQ95l6mBjLFdXGKoOvBIu9oshYa3G_raBO4rg6F
4kKkhO0h0u7usKC8mWQedfJ3WtAmpiNwNJxCdRRjtdigjoVbRMkImVvJhaaI2KRQ3AYneWcAbRra3aY3SkKjkMhPZ
p2NVqyd3XDUNAiFgHDOfvJMFOkz-VgWTlfMze2z8w3wPUtZpjH4bQUtXslmVxUGwi1_Du6qHyin9xPO8Sv6eNKqth
W9YwYiBjE79AHNJYx7nQ63IM9G9RtF3GbWQtP9kye16Who5sZi9k-9BhOxwwXLeiqHOwPRFMGyQE5ySd9hOUSaNGa
jVWZytWOmpt8RSrLnXY4moxAKZEGfhIFYIOVRImjtLGeEBZfRyVSYwfPLJnH5SDBBimoltw1Uhx3HQBOd6FmuGsRV
iYu_UfKDxKscAgJB0FYS6FyoKxIeknPHpowlJdJdbpMF9QIF2mNynddFEfGJHYldfBxyHQCIJaWxHwFTfYxeiKrtu
cnrCmm2wBWI3wntUUrC5d1vGmLI_q6Vcd5sXiVm5ZvENddrPeInGaLYUgj6Nl5HiMhXjp7t2lLMRNNtkoomRx0Ugw
sgQJx6LEC6_s0G6E4nXe52UVdkfsQzKpB7dmaxSkWWGupmgdBcXpyX9yqYDqZiFyu3pbHo7VEAC0Lp1Oya1pCP6kO
NJZuDGRscQrObIuBmZwzj4B_CwSeu6ZnJ4QYCR374LlG4VHMX9hIw7S-tp1j0QZb3ojmna67QydOt-M",
     "priv": "oNrZa1bdAQtxbp26w5mcZgzw7fKR0WxEbpRhVH5tcPRQxzIk3Iiqt6p9Fn88pjYoaUmmlaNymuT
k_ws1WgWd2g"
   }
```


Figure 19: HPKE-12 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTEyIiwia2lkIjoianc4R1dyWURVempIMGFaUlhsQ3Rjb2tRd0k0ZW
xQTEpLS3VsemlRd3NCNCJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "sq1TmK2Oa6_P7yp6eYYDAzYv1biKXQ9fO2zORNkdFAFOnTZTKN4MvaESlHx-Bx75d9
enCHMhkYtrGgvfpjTCH-XmrRp-UexBp2mKVo1C3LFOBZInoESOf33-1BhbM2X3M2j-mhm7i4VGIO60UrHeSaZgH2m
AqSZgkHHP6y5WiPutwnAAdP_SlpswWEZDPvwzvCNI-pvSaqW1rzUe8iDGHycTkpv6V1mKUaXIhaETVmNQFRXZIvkQ
Df6cVatOtkiBCsHLFUNpaSUjXJdwJBdDsqjbfa_TFJaqgy3vtOiRYOBtKDlaUWcI1osJXSCpkOfXB8halKlq42khb
Ff7nbDon4H0EJSGoKHvUw0LG8zVlPzw8_DYs9XiYTpWAYeAX-mkJmX1FH8H8IgYR6APRsAzwagCGIUlCIbY6TKSRA
ENxAS1fy19XVpne8ouZQ8lWVKIm9bqgRcin7T5lYQiG3lkGdqlN54LndxCWQWfC6fX66UDH1rGtF09PC7i30Ncyut
eFBaVXPoSluaKYKOwFiQIxtL9MEVGEWazgJEdxvgoiZnCQCF5RqinqYbFrKtgej-4Adck_uz6H4G2l35EGc8BfUhY
Oc_ddqs2nJcF6JPjj29ASvYZl4MjWpR11YEQPEXlSIK9aLIXgujxai7FJL_nhqSFm5AiAp3Bdszp_146vMoPaV3P7
d1C_WgLS8i5i_2qmzXn5KorN00g6Cd36VdRGQHftpr1X6vvQit7eLKf4jqQ2DITcXGJPqi4oZn0FHlQoTfBegmDno
sVyaoYyrSPglCMBM7XtvjefhVTSsz7oQHclYUtfGnCsPUh06nVJ51PdZA2SX20md97TH6RPq4dnn2GIebn3Hzc1Jj
uDkrkfRf_2NNdTHyv03IXGXjygigb6w2BRDYu_oPSLyDJ9MBvJAJv_f9JFOlqEiYD9LFwR_3rEJAvQkEL6xA9DOF_
3urdOrYwMAZ-Up1AqBxUzMJ8WVkbElwQKMe7o4gZ_AHV27NSWf78kjGVNsCQoNMSGtrvx3eojYcfK3mFJUUBjnogn
rn23Dq5_mR2s64XdLcL5nJY0D5pulB90x094S04rb_6wO9OpfmdRlRbuh0O5LpNlmLYPpa_BZtwNwtmCNKsxRW-Br
pOy_kfOxpl2UaewqWjEIBvoIKqThfkqx9GiMEhCQTUKZR8cejvbWRWtVgJxJLTA0IW3QyMU8_Gi9MXMG7NOrE0Osp
kRe_gAexc8sGO9O58qYbfSuqlTR7GHkLaUczi7yejtYYGzjastPKFMYHOHsBYau2FgF6eNrFWVeE-bkNWrgs4sZyc
pIJEYktDvvODRZHG-7TpFbLRyAOCcqBoQXnWcCMzjMmmecRi7yZepjAaslZuF7hGRGCMivDUVNQIEytC-nigKVoi6
Ya0pZ3yC4aVBFPPitRFKK15ktdh8T-g8Lk04_faM3LoZMCnLgU",
     "ciphertext": "opqe-7Y8RSKoR6OAbqm0n0GuRQa0oLttHqH6RXRDR2dqgnn1P9a5tpqnUAalwkyT9UUkv
i5CPpZkFk-2rw9THiUMRNhP9TWcqmLF4iC9pzFJZWflW0AsjTDU9SKe8JFFUgcLejw2v_pyRDcPB2zvMQxxlLfsXX
ggtntqT4DCPBI3rBMfTt_V6RDEWKLFSseOF54zdIw6z-aBnhEOB5OW4seXHvCSVmdrH5B_vimGVciBZW86e2xwix0
PAIqg0CnFHMqarOLADeWfj2bBwUI1FtXi0YxwXOQEy-5hRch76wuQ01gQWUdqLd-PPxfUWkGJukZ4XWifc0p6ho0S
SLgkFERvpugQTqyi7G8fHlQMSjSIkRcVFXyDBwXQUG7BhMTnrA"
   }
```

Figure 20: HPKE-12 Flattened JWE JSON Serialization

eyJhbGciOiJIUEtFLTEyIiwia2lkIjoianc4R1dyWURVempIMGFaUlhsQ3Rjb2tRd0k0ZWxQTEpLS3VsemlRd3NCN
CJ9.e69-F0C9xtPkza2EzcpZJD7ogDwzuZmdPqg9L0J5M_vuPm9F-3FFfLPpiqKINn2bozlj80Tfia3tBHpC7PUyV
JiXsyh417ZdMgim_DG8Na_wG7A_j-H8vpXrW7EEsW0wqYohkGJwi6eSq0Vbd4tDPeWCL7rRDeMmseRPUkzhmTKmhx
9T_jSgI0M4D0UHeXPud1eUAavFZS8xiAdADoiJFxtnS67s8tNobg63099O2ZAciOvfTZucqwSWPwqL8GBh5ieHizV
nk8YvPSqByJ-rjdezRU_GghZ6F8Mk2PqzuMARVUR-QknbFqQO9rHYRMxTdEPBmGHfhpRJDgHxADLTgHuNNnrnAzTZ
gnsQC9lljfnvqcwdDb5SYqcqEz4F3t9m5d_QiiFtrXUdZi6u581uuXLU4vrgiLC3aRvCNrcU-qY7NaBA2vO2nOCsd
jRAotWlYbFwYkX5tPXkqzj7_ZXiM0GR55koR_mnTV-_i574qJfry7w8J2yru-0DVCYtSAaXTNEwlwXSsyCQtRN19L
rTixKpP0U928m6DMrl6TJ5IJ56sn9BVrQI6Q1aoogWZDfH-KQT1sI6oRisMQNdV14SKawZbMjhbCn1mQFpGH8SCdC
ofOV1LQhCKHwJ9jYZTKjLPjRX1bPauzHSDhFR70yr2xazK2Hx-tqwwllKyKkBvJIDRmg7r8IyjZ6sAKDR5J2zf6hI
VLpEu3_j2XQvo1KX4lxD0f5qXvBLE0R1n57dF45NE1Ij_nvVO-l-rQzE3SAQylQ6bRlRyXRrtGkdw6GLOuPyoQJZg
R3PWNdxTSlFSKzAOIzIVlgxo6Fot1EAYJsxttbrZ2sINh6Qkdh5Q-MUUPTdixdiwOLaCJIs9_dsF54uPbUPq3n6aT
Qve2xJ6Dkj4wC5hOsaOejH705y7TLgiHaIBwOyfJd06LkVf8tgZea6q-3cQ9Jji0qDPr2bq3uXzTubHxn1a-FrsKv
KHwW2ljifnyzTYozxDUVDf51euk5Fn-mR-Ns0dalVNwVqlK-YYo3kIbhmLKHvSgXVB76T903qLVRqrQQWHO_w46g_
lnT10Ta3SfZw3u_2oBQ_dC--68_b1xDKOqLGvApXFRCl4-u4rOTMuVfZ6RT2_fNR67mOk71vG9fc-ZWn69myX4yfj
co1ZcbsW0qb9otY1auNDefmoXGK-j7oFknOpyjEQ5qXy5B17l5pYS_nqHKkgUznQm5UMUWydtF8W-Pb1rvfdHGSav
TkdaZKUd4Uyq70ylIzFFx1cK7Bi4KjJH7Q8Uhzpt4miATD6hEe-kc8iybdoSMJqe_QhIKJtngRrjkuDYNEGwcb-rZ
kn3KLh0juFkoOlmbTPcHcLBKv_a4-PcB2CUAp8pJTf-uiJg6eZzsgyIvY_JQKgCnGfDqk9QXO2NlFyG_R6y9kaVw6
5YXAJSSni7bMBQbymhExMgfBDqs9xTQ..OVegzSMbIG9TxaH4xHXD_8GemaeruyQ-pPV5jvUHwkUmcgV04TQkJ33o
ooQJApX4rh1B89AR8Vd3Fqtlb8gMfunbnSHE-iejZNRc9qVXzfyueskK8zMKFEydGRUI63BFZJLRXZIuZv_dmYqwc
9nbJJOpqo9mU5jkdyHVK3Hbbs4qzA7jbqx0wXFaifakYMprOptUKrTXtTBUAVvxyf6JldJLmKR6FjrElMxA0BPWKu
Pduhkz9JhOkwurJ_LfZqx4c5tsjYYXbFTAM9PkGkkMPQuON3OP_WutBZEItOb5xtF2s6o6bwZ9URknWRL22oI0n8I
6QlrjWNab_f8GIuBlxFiFuUQH2NfzWFE_eiwjUHzCg9q5kz4MuDWizCy3NE-UCw.

Figure 21: HPKE-12 JWE Compact Serialization

## A.8. HPKE-12-KE

{
"kty": "AKP",
"alg": "HPKE-12-KE",
"kid": "ogbSkvF4f3pRb1dWsBe1HpdXtfiRwZsYrhaxzxlWv_Q",
"pub": "HzogrJREUPAOuEVqa-DP_tVzOjIvQ3PBDwozMZK-LnQht_mjYEphugmVjFq2IsGfF9fK2TevQDQv
nQKHoERnSFzP47aBxXBjCZAokdV_w6lI_jlrZLNmEncW7KyQpZVkrrdQArYLiRQxlkozD7FaXlUE6_yUCYFwOFinC
0Vbf7tDqZwGordZoCwhXwdGzUqU5HPHlEdzVTl-NtGQdoY0N7E2ziYKq9C0E9QSstyYCBKqd_qWSDwmTBiJRqjNhX
eTt4e6DEI2OxK25KKxrfYd6kpHYFpZYCwtfGYF6jWWNjpSWVcXuDx0xLco8MgVk5cN72lvvVlg2fDBOLexGAwHlqe
nB5WiA8qxHYcJr9xJi8cFjCdpVoqmVbGxOUR_lAM1s_eoR6ME8-IAGZRluTxQk4bHOISjiCZZu7Se_dNFN4hNCOxc
UnBdv3Rb5Eg7CNgYFBZAh_QXVMGLiMGgaQV6Ifk4wCoxl4chmLVnqQsEjlsybTwzqziOLNkCgaJoorRvbpw-jAaUX
bCtqwcBU8shpNhQ7liSzXFOdwQaBVsKYwfQCTpskbVLLqOZKSjFu0PNv3TPYWDP6JUgFdh5T4SKYGILClVa0DpARe
sKomPG_XxyKWFFqUOhgvxDZxmResssUORAt_hDsmN0GmRpcfrB8SQvXjmbmEdOVxsDl2PNw5zIovOZQJVtvsC4H_P
I_kJ2hQydxYB28PkYuiMiibpLfux6tZlPB-NWv7ck-GpZnZxrEZYbMeEbSLBmvAVLYVVVvYx6RcYRBnSRR0AfgJG8
IJPKXEmcM8y72TsFF6zDiQGsmfq1aEwUURJ7Pnl_kgBcZYWgw6Mn1VsC7sAjlvSnSfowW1yZSrCkwkcFzfkq2LGt5
PY5xPPKBdwVaGC9HpOlbzegPdnB4FcQaRPEHlevSsLE8thjHmiRdJsVFzYsoJSCMyBCnkMaLlJ7v8YyYskgJ7l6oW
qCwycFjUN3RWG0btuwnyIbaHJQTcak0IBNABKZKEJTSXURTeGaYVk8HqdxXWIy0uE4nkoVZ0s1gBd9sGHKPOhEOtd
sERxJZPsMhDaiLjGuuFMUEhPE0DQeKrEomTcSwbWxPXwUJApUKsvEKBNoFcRGV-Y0OGEzJPSM4JtlQ7FBVPi55iZd
9bd34qrCbkpFD-yixzCnnrBRd3gsK0tyXidvjTtSNka48aBnI8lFKcvJzOWLxWNlugRN-erP-yOTwGoL5uKByHh2R
3zKNHbPvRyvTVkDApMxmPOrayeSMphL5-G3P2FSs4qLCXy5rMsN8KKA91AqMdYwAXqsc3AbGlKE6Ik3M3NYK5BI_C
sFSkZgUkw7XKugCoRtBtN9dVlu0XaLmuIH6oIc__wXyBFMX6E9bNdESTwN6jGBGpyFVHt03QQxCxmWT1A7bxBeeAd
1oHR6gxoqD1geCCAh_RqLBJyuk1YoIsy55EifLwyPLCQwkwSRh3t8qTWMIAYXL9N3ALuCCKhxfZJsmzW5kmeZcTJr
TENiePs3ZBKalINDrKitOBfGolzOwfluANQurHpgR7OYJfNVNxKrKqtkeiY0kJBpHnMssTekX2TQuKQ",
"priv": "r5W6TvhlPnuzH-g2OggdYADlRWW7ccGhUd2MADCdAFxZ1oCX1YANTcjXvEVSjYQ6cLYhHgkYPmC
qLJkv9JuGlQ"
}

Figure 22: HPKE-12-KE Private JWK

{
"protected": "eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoib2diU2t2RjRmM3BSYjFkV3NCZTFIcGRYdG
ZpUndac1lyaGF4enhsV3ZfUSIsImVuYyI6IkEyNTZHQ00iLCJlayI6InNqSzNodU9uV0ZUN1hDeXJSSFk2MFM2X2d
1MU40SW92QjdnUmZ3TkhBZlh0R2VwOW01Zy1fOHAtXzV5bV9RSUdvX05LNl9HVGxGbWpTSGdWdHhiUm42RC1xQkVM
amxkdjR1ZkZNWHlpbnhIUElvM2FWdlF0UVplNnotWHd0TGR5TlRuSE5KWldyY0FXLUVESjRMbHRlMEJSODJ1TlhhV

```
jZSOTdhQklGZVM4TkdzOFNhMTFSVWJzb045ZDJwdVpQQ0lybzQ3d3lRTUxJSDBkUDZWd3NXOWd3OFprYmJIb2lFWX
NYc1hleWhOVUp0ZV9WM3c3U1liU2puNVZHOC1OM0JOODYwR1o1Y2phZWwzT0wycmhER2Vac3M2VWNpXzRhQi1tU29
aUDN2ZGFBUjBOeUZZNHJRT2FPVkRHWjg0c3lEQnpsdkVJdWpncnllUmpaSTV2b3psRTMxZmdFZFhjRnFQZzU3a2M5
cElDaHFqSEI0UTgzV3pwUGFRUWRQd3pBTmY3ak5XMUNOYjZhRHVkOHlWQjk1UGhNU2pmbHlTNzJMZG53VWdTYkdEe
U1PRXNlOU0xOTJtTkxqajJJblVIUWxUdXFpR01hVEQwVjBzenRtTXU1UXRlNEEzTFYyQ2VHcV9zZkVZNTluZDV1VG
hSUGIzeW94WGpQVWRnRVYwZDJqYXpLQlZNU3EtQ0YzVnZ2UTItNjVpckI3Qldqd2ZzQVQ2dG85RmYwZG5vbld2ZFQ
5cnJPdmh0dlFHT3M4cWtrUE1OX1BCUjJFb1E3WTVsbGxheUh3ajRZRGRZdW92czVDSUhXRHJYbEs3UE9kZU0wZkEy
Z1RONm9uNjVPQWRzcHZwZWhsakRwTDdHdWs2dVhVUG1HXzUwSjRlWHdxbkR4ZEFRa1EyaElXUVktUl9wSFpueXNJc
jFoeGNJaUVWcExaTVFLRHVycXFOODd6RmZPMFhWbzlsVmp2eGx0ZkV2T0tHU0xvc2VvOGxwbjZuTmxrMXRfM3p0MW
plUzR3YnlaemN6VEtpeHd4Zkl3WGNzLVpUeGF4T19MWFZWY2VURUEzeGV3eVV4b1l4MnA4aDNvczJTRjB1ZDVwWHd
KeXIyODVDQ0FicGNDc25Ma1JlbXFuSkYtV3dNdFFWdXctNmMzZFZHV1Y0a21saFVVMTloVUduSkl6aWNnVDB4MFhX
SGkyeEdBa2tlalU4bjZDMmtnblBKSWQyb0JMY2ltYzF6dzcxVFdMRXdGTl9ydU1vazFNUkFQc1BFZ2JCVG4yVW04Y
292VzAyTWFGYW9kbUMwR1VLUDE2c0ZKUUQwVi1USWVtR2VPS2p0bWJTR1c0bTZHeW0zdVltVVlNeHJYby1qTUJMYk
xxTTVINUJLdjgxVmhaYXBDU1p0OGktWkNTMU1xdk5VdXRlZlgxYWxSdDZ1QlYwdkVtM1Z3b2NYVkplaFVObWVDd1I
5UEtVSTBkMFA2cG5YWjFYSzRhS2ZMR1VfSzFhaURZOEZKZC1kQkZFRXVjc2ZMUnFzWTBzT0VHdmdkNkIwbDZTVVI0
SlpzNFRfMTZwM0dsWVZnRWtBLWw1WEszYU93TFZLM1ZPLW5NWi00WUMyaXZQOGNuZDJNYVRGcFlrcVgxZVRUMFFpT
jBFc05CUm1RNDNtZHNqd0pwLWRuR0dIWWo4ZExCWG9zYUpiTkNiQUwyTTdlbGM4cmIzdkV6alY3QVRCVlBzRmZJVE
NhVXZac2lOWjFoeWJIRGJIaGs2bzBEc2ZZOUNKamZlVDlRRWlLamlFTTB2NTJpTkJBNzZzXzc0MktkNVlUZ3dtSU1
Ud2sxOEdybUV3WGwtOF9Zalp3d21KSk5XdzNZY09kYURsbXFlbVpVMVZjNmx6Y1FacEpJWUM2Wk1iSmx2bGVocDhv
STNUdkpNLUdwLVdIVk96WTZxczBFWlVvIn0",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "0nl1mu3QLNZhTMZ2",
     "ciphertext": "GMIQ0AeAXSYshWUO2mK14kgZpaEVNX9iR4-khwuZIdjvZuHLIaV6LuuVC_m2dqCLUL2Us
bbVCH-Xsyroy0_eEnENDY-b8j1lVIWK065z3ONMwlQI-Q_Agy3YKOZQdttsTnoH3eKLy_tTkl9SrdLJ4RYhFm_h8I
vGIMVqn0jfoJxjUWS8jr8FFGltHYrfJBqNtydJHF2vvXMUSXubdoow-_FkG8DWDClLkKIs_1GDHIkMnXQ3ROzRI4w
NH5zdqYOXvnxbVZ9eeQFhpdWZN_O-C0mK_pXsJm-vQSswpoU8fql55YbI8ljSy3TcmtyIPoLAV63uWVkQmIiIIbFM
UQWJsqv4k5jw7EfCgm4QPiYMDtL6",
     "tag": "6eK5vdz8D1Klac80UZ61Dg",
     "encrypted_key": "BvAkmT0cnwAim8X6efNitQN2OKhZ4UWlAzI8rpQfglu6Tvc0XEdVHJQFAy4mEbHo"
   }
```


Figure 23: HPKE-12-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoib2diU2t2RjRmM3BSYjFkV3NCZTFIcGRYdGZpUndac1lyaGF4enhsV
3ZfUSIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjFpWWpQelVGQlBIdUQ4UWktMlZsMTYxbml3MjdKX1hvYUpaRVZ5U0
5zWTZSTVd0a2FsTEFGa0pCWWZtRWFVMFVEQjB3bEJYN3owOHZjcWg0ckJJNTh5TFVDVF95WFdpQVN4Y2psR1BIbUh
Qa3h6VEswaXgyd292cjVHWGY5VFIxaVQ5blY2WVB3NFV0V0pvY1FYQVJxZnJVaG1saXR0VDlrX0ZIZ1Q5OERBbTh6
YnlSMkdoajVGa1FZUWRUSHBQUUVNa0V1N2dhS211a192VHl3d1U3VTR3d1YyOFZubi1zelNkVk1mb090SkFXemtrY
kp4azlKOUFXNGtuTkVSaTYtX1ZyTjlUMFlWZjY5VGFKV2JhcXBMWjRHOXZJOUZTRHhzZ1VnVXBFNW5GZXp3RWZ4OE
lhTGpHWk8ybmFjZzNnMkpmek9MeUhCa3VKNmd2V1cwMk1QemROX1oyU2trOUZQQXh4bGF6X1pFRzhzdHVYMENGYmR
OYzY5VExtaTlXME95SkV4MUNUdDZiTEpDNGVJOTQ1WFl2em9wLTdLVnBjYmUyazNWcDQ3NHJEWndwckJmdUk2WXlD
dDZqZW90UzVBRkdPbUc4RTVsb3RXWm9adGJLZVl0ZGhtckxFQjFlOGJXTG5YbzhpY0duREhJVkZJdWpERHhOMjJ1d
XA3bWZzcllOVGRyTjN0YjNNajFkcGtJMkZLN3FVaXBaN3dmejcyFU1UEU1YXZUQUt0NTBtb0FUekdrVm93dkh3dm
c0d2tMXzVqUVJVZHg1MVRnMFlWUUdfNXlvZ1AzLXpfNXR0LVI0bEpNa3B5dHl6Y2hOb1Y5MHFLRThQVk1ZVi1nc1c
0dGtudTV3VnlFRlRFeWo4d1FabklmdFFOeUF5d3pjR2pWT1g0M0k0Q1dRSkNjclFCbTRJMTYwYnVpcUxIaGpUdUVE
S1F3WVFkOGotdWhwRmF1ODZfT3A2cWNkaml0QnRnakFpRm91UjlLWDlpaERialJhRDJDOFdsdldObzNIM3hfbENOQ
2ltN2lUNkdwaDFXYUFNb1FKU3Zaa0lyUlJpSXM5dTkyMXdieW9KYnNPejJNN1p0U2luS1RXZHduN0FNdEgyQm1rS2
xCUGYwbmRjcXJVd2ZtS1ZYV2t5ZjhpU2ZEdXpRb2FQZTZjd1lZWmtQb2xRQlZRVlZOUNVUW1CM2xIbzBoTlBHX1g
yV0pFc2prQmUyb29YREVsM0ZjaXFOSnh6Q0EteHRHWTd6d3dTUjNiZUFmMVh1cXFrWDc3bWxrUVRYMjVjTUdyQVJ2
LXJTWE5kTWNVb2lEVUk3WE4zd09kSG5SQlRoZFN1M2dkSmlSSXVaZlZ5eWtkbVBIUmxqSXZ3V25kdjdhY0RGWE1yR
XNhaWx5S1lFMU0wcXRfNmZqN0J4dEFZMDA2OE9iVzBRd0t5cm5ucU5hTGdKLUVJWW1YRVEwbmVySWM3ZVBNa1F6Z3
laamYxVnRmaFNnNkZtSW4xYVJjN25tYzB1U0pya0x3Z09NNjRtZ21vMFMxSXExaVNQOGx4c0NxS2VLUDZtQ0paMUJ
5dkJJZ2hkb0QzRE5nMlcyb0ZHZ29XMk5lWGFMM3pESmFyRXVnMWFPRkNvX3N6dzE1bTJHNVUtYzdQS091TExvbWVl
bmlJcm5BT0ZCRzhzSHVsNXU2ZVdDajlsb2VzblpNZmVCY2JJSVpCc1ZDOERSZExmWUVEZlpUX29tVFZHZGF5UkVvR
3M2Zm1hQnJLc0NSTU9Yai1fQTVzXzJlUjVyLUQ3YzJnZDdzVmRSN0JsUlVhZVc3bDBzMWhsLURQZjdNR095RFJWam
VoM2didG13YXUwcmZzWVowbEhLU3dXYU9xcG1IUVU1SkdaLW9kZi1sTGszcllrelcxdzRMeXBCYjdZSGRYdXdiOWc
0RHYxd08wZ01NIn0.XPv9zhwB4MGyuID1hRH0vXNXQtsAPywTHM8E38oe1NOpxCIGFXz87bMtHXvZzRZ.MeWwu89
Msj_Ctumk.H3WmRv2jqrVpWES82_3bkkgFdBoJgJ3rQSObhCHbHSW3Ie_-UBQ-Op3PNxfdUBIYnwQvnYYgBL0AJAH
naNtVA73_2_QLO7ukcXeyVpNjN234VF7vTKzZYBajd1R2yGLG4IH-ZJqbuPgZmGS2sTV3K2rNot8UBGftVTkYD31E
A_ZJ1ay7iBvL4-xxCAPasc8Di-CNAF3ZxLFYDuzi2cU8FJQxnN3WHnx6nggVnBYhlZfZG0j9irI-EiQmhmtWCQ0KO
TNgbicP_F6WBUEjG7cyG-3fvV0I6GUt2IHSYUYp-HwMSDmaDeWE1cN5o34OGcuRreGP_xOYp7rdCMJAf54hMTBSTE
xcYxMEw8pIR2qcYIFN.ekNZLiJkAkjMsXYOMlcrsA
```


Figure 24: HPKE-12-KE JWE Compact Serialization

## A.9. HPKE-13

```
   {
     "kty": "AKP",
     "alg": "HPKE-13",
     "kid": "wIKmf5ISyZZlOkqqjwW707KCxkqEc4cJg7fYFLBkr5o",
     "pub": "59oD4empWTtMhOR7pGVyBEKEb5lttgUhITCq85eyJGpyZXa56wd-HfoHj9MxM4pg4Se_iwmjBEZZ
v5UHbYpoUGKW-QFh5CGjCCuvtjIAofAShNEaBpQ2dBGnkXeBGZhx_EPA3Fxv33tY9WAoUNVhEEa1sRuAwLI5dFe8Z
RLDDCUoz9h1Axpa2pxP1Plmj6gRtDayfAU9mvWZhhpwZ3ydbnIEjPFLgwwPYGUCYtNj87i4K4aHa2QcWlyJlSOO0u
mCHFJbsEsNL0VNaQsieSWP_2FB90mYBuQsY5UCN1g8p-DFicWAAEtUE0uukYe9X5u3z6y7A6Bb9HyAFhKH4TelarS
7xSfBK6xxK6MpbGzP5YSBoZF8MBBeMNbLwNSJ9dlMKYZmPIO7Z_Y4bjlnUzCsK-aC_sERbElaSzFiLImIwQp1IMxu
C-igzqljtxepYXCinRi8yhyiHNMuAlDJAcLL11uW7faXb2J3OdrFLrdKjwNYrOdMw8uZaexXkWdCUlKV8CdJrBKKx
3a6oJApUhM3lAolyquTeXeGx1AryyhGualBEPrFI3ROcgRHWIFaCYFF7YZjkVB7CYKOVOpXWOdnHCSNOPMWWtGvVE
RXRbe0K6eeX0iXB_YxddByq3IwCIczXwYA1luZjKjMXORjv_qVTzI7HPBFeVGdXIc5TxTARJR15lEEoLRIOPuzcek
2q-KlyyIzSqZqrHeereRhJHBPliMsJYGOAsR_NSLLxwDHWggO5mqxnxoNyVMXYPgxerB763eZZtwjBuobvGpwtNwg
jlqmZLfLP1wqdcpINlheQZcQsjIO3YdWIQu01VsvmgPAlkSAYnqkhmJbnDk3RcqGdHZzFekkcas2_sSrBsEdqhsQX
BWoYkOqrbLP5MqaIaKjQuOwutCgsUOoLImGwcwpNYW-gJyj4dckDfhrqcN2zreQW-gqmMgnXUZa5iEx8-xa5sRQmV
mKEwls3_GpMrtUV2yG2elPFtTAlHxZsgUjm-Exxgxmmyagstz JFFCrmJAqNCKnU9Ee2paKzQBw7qihMvNBNCQ5vtm
Qq-BWwDQDeMwRaiJYJVqGnNPOUKoT23hTU3rPosAGctpODVOyFPLHY7ZoQlqKkwZ7F_dbSWLJROyFVrahcPMtt4Af
yiozSqlJAgpfS-mBxieo4WHD_7GxHeSzW9Wk-pmmlDiytqaw9lyCDDZnLxUT2qF55SQuvPYr-JFgyVma4LsB2kARI
SdQ02eQwZvBlYTHK4EN9fhFMvS2MZYfbOKJocaKOap-djcCMWp8yoyUP9OKuaabs9o51bqKCgcoRqFjqWQZCWXBgb
DOyBAhAwlJRyciojeH6NtUBDxSM0t_I1q8lQli9nNGKHklGEd86spm1nRMTARzy-qmGTlUb8g9HUvF3ly516YoKeV
BcuUppUp0v4u2Tme_llhNa5EF-6IHybjP_VUBg4NOGmGE59kKXURxiAUz8vidSWLO9RkG1IQoNtJ9r3Uyx-woFTUp
3IC_eHCfA4Gb5FlIqDUcCRZIkHgOodAofbtWyQRZkAFs_8iQS1UGT-O25ajAD2jMnAgXbWOqdrIvRaMkOnl0QOOZw
KkMfok53vOqRJumO8dGIuCK5IUARRdJspF8dkMsrky2M5BA_QqfGIZ7vYfG_LcifNpQAxCj73qrNZZCEgWH3KVq0Q
aaR3QIMXGS-Ag7LMYC3lNPB8VOUvgC6wEZIdmct4NR48IPNDjOEihG8qzFgtkZ8rdJ51UA3lFFMZhRsucj-GGkhCh
GRkib4rxL-Rkoi5VbdwxZkOYIMDhTXYN3pUOG-2p0Z4y4_TezT3BvbtmzEDOiSUiSOvMVSphsEeAkv4woy8he85DP
xxMwsACgpelKX-hjqYMaott-8WChtrrENzPHlxd6H7ipoyo9nACk8Mke51QCBxM1Y2dL-fLEKjMDblS59wsk1yHI_
BF6u6kdDAhvfyNQ_4g-uFxqSkgbC1FYs7jNguciJEUFSfNta4ZDUcyWrrmHmymm7dwGzHBWoaBc_cI7ghNGM2yGhW
u3XSdLp1aLnaCiRXeYb5UNiRXUL6CNAqp0K6GVHkxowUsEBIV9qA-BiLg",
     "priv": "JKfunEpR_O-GX8PenAcjHl37FB3kSP3X6v8Bg8HIcIR1snymjQjiWomcAq17HbYyeeOm2yIEgzj
uncXDElfXbA"
   }
```


Figure 25: HPKE-13 Private JWK

```
   {
     "protected": "eyJhbGciOiJIUEtFLTEzIiwia2lkIjoid0lLbWY1SVN5WlpsT2txcWp3VzcwN0tDeGtxRW
M0Y0pnN2ZZRkxCa3I1byJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "A7QASMGmBzxW6c03sNy4wWpCV2IpNMWZpGMzU6potmBO-VehOaVw8vteHXEL_ARRxH
UswAAQKBND01MeyByhBUjQ6Z_3IqDseFE54QQiPGdI44Cz-XDpbux06YP1z6cyGDxcX25UOU-CID_g8wG_TIhmOIE
x4PUSuCz_ZVZniLKDlIDbWF_v6NR-BhYC6y__2mxfejVIk-ONgGPOKzY2CnmLRzb4f2lWLzD3tcAXDeGCYnomeVS_
bea2cygy2lsuGnfAvqfGztHiY6dbIuePMLEFuPYbIk6jlbMewAmfqH9hqxdmDJNLesqlQIwCyrYJAEfPOjsXgWeUh
nkWrMN8r0IoCCPtpzvIehuYYCkjVQS8GDAfwg5CKxRRZ7Ji1B-SDAZ4_rTwgua_cxWLMeXFokqw2MS3x6Ssl-Hw9I
elaqnt1crd6gYHBnaPL57txOyX5J5pRBhENsfQq9YTUWAnzQvOaGyo9KHg04I-RI--hjQFGvtdQEg9UrwEEsVYAk-
AUU-lqAGw5b6yVqvbZKkhnxHAsOYpmXrmAd_6ABT1Imovxggj09foCoS8d2foO8ddQh7Vu0w0unJNY22bR6o29L5A
c1tNq4Co0TMztnmOUnR9o_Tlp_7Zox87UwClvJj8PO-b81yBaZduQ311WK50d0fwH2PruOTvWiPS1UFs3EmhplkSc
hKAbkCHSASvcBlbE-dzvF-FoKBDpocQc10C7h7ap2fl3-2amAlcGqIvb8LuzCM8vxqCRxewZtgbfKPPTQvEzYPx4U
b-Unh72MnHjH-oPylXY5p2cCdqi6xhJwEE-dqXtzn0z50JsisNuNvIM-nmALE8JFknNWqTCMskSTt98b9OktDA0QM
NuNdZkAiOgLYf6UFGWrt0RJyKRVLlKB4myD-YbKLw9nbtk0a4I6Dk2rSSpGJ_KZEbq9G-OQFIcved1l8FRGCM8hA8
88k25jxRxrfSjndnSs_o3nhDdaZBQOBqzm1mYQm4Vc5eq6bo5F9JbdvdXVwWS2sZsz-ef4qOoY0HS0FsgwmE4vnML
csQCQuBgRONd6PL185D-PryaVCig98n0r9MPSKSQrvtam6vVqbrKdubBniUkMndhnGg1cPoU8ndo4yS9gwqvtqeWh
VNeOCu-cHtvgHO1F0-5-CHt4y3wK5RyhCZTt1JirBZivjDzZNM23c51qNmLjUWlGzeupK5HJMe3qScz1KRxVxJXle
DL2XF8X8_5PZm7Xc-1eE50AaP-4PgCGDvSzEdxkle6Epb5LwzGPD8w8frzil7xZr5cd7rQg8_Il-MZUupS_YM4CTB
L6SgIlsa5DeMoKTbHn1EXI-e32RammLK79-8exaeaCBFscqqnWXbH4ZW_mGHsgmYPy86U6RXARFgNtsOe7atKQNRk
_Xsy7-EGV1kfEckX4VlhbyGl5l5Wd5PhMAFlUiMvJ37uBFAVEPyzptrIxzQk4dMJdkeHKjDFScThbWOxwJlf3es9B
iG_jr3cV1jeIpqdF78ZmG0nfGbbPidzweVR9QlCvjYgFU9ZhakNLDoErV_euHoEOdWSuvV0u890cth5InzQzqxtEQ
b7hrHrgrCUQpclMRw0LoHQligiZnl1quJaWBljyBVxjLHAVkwNwmzmOgcnzrgNJw2iKmbJ0V819rmHaoXl5Qf5HMR
eaBLds3qIFjkVapofh2UMgJbsPdGRshFnpZLQZZ-tN9SKVQhZSqeIW7n3bjphf1spLCc78FycqyqRr--ZZBcZ01S0
6Jo_hfbHLUomm0v35JVc2K81LZNHq62gDJYJhH0cww4oE8_M0wKkjn_TQ1JZFxGWkAqnG_MVLxhrIyYosG3ufWoC-
lVu9Qj8L6C21flexkjs54kz197UoDqEOgUIBA6dY0f_hy-QZjtJie0zNWZc-uEoia4UKYJOwpnLE4grZdN3rA6Ske
aY_l8zewMuMgO6pNlQiyZyFDmyywzfEB3eEMc6KcimnMSuZGG-J_UmEnysYAve5AbnpgdSuqRQj8kzb2yfNUwV6fc
l7v_njYR9uh0m4Nqc7PB8OgYS8rNv9guGy30cjj-UtrhqksXCyr2rweMW6md7rLgbY8",
     "ciphertext": "09RTEoHUgifJuBgWnroH3CcK_8dPA10jT6NxNV9hN8TDF0007BvHRzKCj0uKVqXka9e_4
dN36g9mrdDTvaIkZKaWdFbLTz2xNjdYgEAM1FsJ-XBx3KfEl1mvm4vSjOG6MIKtGTWIqpx_tGFSMSqbO7H7ctVJW7
b70p_NPvMKM759vzodxbUjlNc8AtM6YM8H4MNTI32z8uKzdxESNksyMiLEYGn2fftQaq5O9gqrUe9ojW4Q22kmTu5
2rhIQ5TIOcLKX4QQuv7c0PZbEr0lPGbyb2N0iuALwOVy8xeIl4b_vRRQYJf9MGSEgVOjcDF9Pfjh8BEfv_1GpDQyM
3HLNWDQgJY19CmibuAL9F-Dz_OxETiHm8ebrZwSKBudmd0vlEg"
   }
```


Figure 26: HPKE-13 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEzIiwia2lkIjoid0lLbWY1SVN5WlpsT2txcWp3VzcwN0tDeGtxRWM0Y0pnN2ZZRkxCa3I1b
yJ9.VoqDQcN9sElKe9DRwlCgccR1tOK3VhqjsjXxdN3ypaKYrIlkFRuBGk9b2581ucMkchAI2x3K8DUlqJ3ORu-SU
0Ebgscz5IeP6lwmxtvl6-12Q7n2Tt5h4pnQrZemixE71b0TCC2c3vALCKt5ivRUB9jfbRC3-dheXYZjt_KZW2uqhl
jbLJxraITtrBfFtw7vbOGvV7n_cLBaYrTNjcU8QnsGWQX1FRi0yL0CpJvA6Vzy6VrBRGiR4z9t7rRCcIZPwBAhQFY
DUiFsmhHwHDo3FN_epfFRHPClgREtA67CY5kBO8aKkPrvRijTRKqHQM0FVZCb16DaUuhRvqUXYUe5xNcsOsjpjRTt
ZWNNAmVy7gHqDIr2DDZw6SDzhN5_z8XV_DzfD0ziUEKkYzyQI7R3GiiJ85Bl4vPIeSR0cgxquN5ZWWofWsQO0OPgZ
PEfLO5kZ5VUgsMIReanC_b0gezZsPCoTrijKE6pS1lFqtgxujsc1LHFApuHip4WMrxYj7vIoyO1OZpkcGuz-5rv4K
qVxDhM5-2Kb6qcAFLKpb2sAerp0Pewdyatj4LwtKmoC360BqEhkn21NyCsfl1cqpFu2DmZ72S-DKgYoq68wCD-mOn
dFc4hgxVyADLuOMwFsbwTbDJ5GlKuPTUfblWwNn6pIwbzMC-clxhglUkIG5VbkQ5kVxPhVNlwZCrlsUMUbTrblXNz
PqCrxB0bpeI2w_1dng-812-wh4ncv5Ky61MShFkQ5uOz3qTJ4zkOx7pZQS42-_nMicMPV0lwAWi_IBjBsvcocwstc
uXxbD_yL8-Tzf357Chtms-XMe1JuNGVH4AhDdDOV57o7noByIbRX9ner2PSyd3TYCfeS4TocF2zmZX_bO0A-sAqyP
I5ObqiDK5gkY3vccuzCP6rohuRluaBlTw1RcXXHQPtf8XJJ0u4yAornBt334E20TLAgepXgtDgwBx6bgD7x9E5hNd
RVdpLj_EaAnJJ2lLEqY-0mFEnDJdRK1yC7XzvWE3ohNOQBE8jiUSUEy6b15l0El_BagVCNXHK9QAwhVjeUhy9W5u3
1kzw7-OHp4JR00icG8APd5uLfZqdmXntFea5ow3NDurTtH8HBo7foX4TlX9zmsgramo5ZLjz3hRvovQWLSNSQG5Zq
pT8xqfC8_RKvq-Ak5TMnLQd2zhXBZlM9ESJqfSeUm59FbKjPdx18sj7S9Etxqqb-RgoREMKJamJ-dqx7fHgiNNR0t
lJk9XQKUN-jgSRxrnZvCN_WljUdoiBnlrJpXIx4g7oRXm05WfgDrmV6-fYE-8ddCnA3RgG_Hxh1WaQ-thyS8ZIWIo
3ETVTZydrMorERQ_ExGuckbvsBRQm40iFshOtTyOKq3MXGjWxQIuje7HuBnioJxNfHV_CLP2hNdMJRXRDe-gy15K6
L5mWGe1jGt3q68FqgKOC9abNy9AKjZFcp3p3gj3QNNfuca8Eepf0DVCWsD6n7b54mRmsHDQ2BX_kouMJXU8TD0N8w
BaAIbM1zsW6N_j0ZyPU2m_OO7KZ60Ak0NXKMDt4sk8c0qVXPc5yM_DeDF_6jXBU9PqaNyq9eqCX4WYblv5HfoRLoW
lhYqGuMUyj-3jVW6_mOXEtrLgbESadyvV21l1qy3B4PwQWj56Ee1QpJf3e2-jmkh5BXxocGtIi0YhIlaz4q5ZFD0H
kkYTQ3FQP9W5G8COK66JlP93l1S-5d5ikg-ZhUyvM7cN6WpgBUeOm458oaaeJtRG6YeaBr7l_qNpmqS6BXU197KR5
0hmVwnCV_v2JEsKOqflKkafhn3vibE--ItHXUiXu-axlVAodXBKcOF_pYTHZe_26Q1CECQxHtg8MZG5NMcZ_ZNUoh
izSvNj_x5wtAR4gaiP-eiU5vNMK8p0ch_NQ4BNw5iNIdRaJnLsQ7zsRgiCQvK0F_Zk9OXKKJdAtbKrmw2PALBijJE
2IdIAgJyafqu9U4jFCL25aNXmV_SgHkFhDYB6Y8e7lPcWMOzbfmAMwAqETBqgifVHYdtRRroREhIWZRdfFk1BLSbo
PBi32JYjUwBa8oGoMPaWKgqRlIuoYRFy06Kgxq2pqiLYMZdU..yvdUQEJ6vubOBf7_3ZTn-_jn-11RxwmNp3mGRlo
```

lntghI5Sh1EJjnhRBsOKhP5AoRdCesJhI--Cpj16sCWdF6_wBTFl9HLRJ5OrIK7u7ew63eGBF6e3RMvYya15pffCg
L0LNDMr4wRJW85_ys-k-xSgCI75IiEMdUd1VubrN-xmbGvoSoENhHdmHvdV-Geq4leqPnlx_9yPe4tOZM-QR8zRFr
JPXhXDY-pPHVk0ZUk38J7UZ_1WSsyGEL3Y8lsFM9RyjByMRG5NOBPy5-yfecIHidLgoUH57JqSQRMu1Us_cyvriYF
Mg9L6gAVpScrJsLrvlyLcqEGt4GQhPuYJ-1ObQRA1sZO7kDZSL-jOtaYVtkx9WXGyM0Qp5JprkIY_hhw.

Figure 27: HPKE-13 JWE Compact Serialization

## A.10. HPKE-13-KE


```
{
  "kty": "AKP",
  "alg": "HPKE-13-KE",
  "kid": "OJo7M3Ej3shaFw4VdozYxtqoGXsMA9TDkwy4Pvn0BCo",
  "pub": "h3uSp1uJz_gkIKvKFSE-v6IM7SQ3hRZpDpxr-3Wym8lDvzRM6yUrOOzPQKFtUcU8FwxhUmVlMneN
i7MenyAW_AyZtkaCAhaZhWRUGnUWcCNZkFO8K7yNU5qX0KzDE5IlybiUH5GpXWrLx5fNqFU7BpzCe3K6X5JHdLG-S
cfOVfgs4Eaoaym4W8oGLxpSrBqZ_wYhsSiGCdguTIWfu4otmFMyaKIY46uzRTR2dvrEH1eZDhUc_lsULUSGS-IuwE
yBI5VNHgJj0YRuxEgU92WtFLlaRigckszNR6qrn3QgQZdC_Pk74qWPJlpbMIhs-ytHTqZhi7RluIUeDMljOSNMNMw
7nhe6lco61sSDirK4feYFqCcjMioL3yipPJkWWlV31MM9izaXGSUhroNdAkwMCDaUgPWN_8de7ZpNTIcnc3k5IcUg
1qe0P2mYbwwJkPDK5iKVscqdJhMA5wUK6bO6VbslDJIhfIp3a4tes1FFiDQtrTBtz7vJAMM8JKBEy8nISMfKM9ZRu
3F__UvDFmskvdl-YMdZ5SxCt4B4HnZbd6t_MzWGXZoFqOuaPEILzhcenNGkUxldIwfIM9UKVeGuYBNrONyef_BuCp
jGLCU0RwVrAJExLjogO_ukK2ipHMuA_eAB_YNEaQgarKQb-ZpojrUZt8XMSFM2dATITGHOIrkkBQFmIwHQfCR92fw
mz1YzRGUhHXRfjQGF23g5u_IEI_wPComPAQE3h-hajAA9bVxikYcmgQyUb_EXXzRdJeVYC1jFWaMiR6RwX6SsP-fB
iIIxk7dUhAY0XXlJgZok2PUxLuIqroV0X4A2VZMZQmoaFAu35CigSeo3kXKW1UkU6KGKYQOA05CnsVJ7JmJ2hiJhX
fFP4Zi77xSQF7SoxQsi5PqzuglA2kg2MRkq0fC2HxGWoVOe7yWBTEAvlvEHvbgo3lup8MUCsppEjaQgJbJFOilbpi
V7bKJH_SCkDfE9LqUULeOykXV8tpaRteewTdZQzJiVLVkLpvQlVJQqGoKbC8cXD9UkPAJBD7ASEvvBYSqlSMIycHu
nJZdkzduGvJO-O9iVlmtgisS5wpx82re6IzgT1bsniBECY4l-AFs37tuDhJZQp8kOulR4icCcemyEzMciILI0MiEB
_4skaXmFY_m6ify1PLs_ECRZXbWmYRZO6TpiBlUDgLSiwgVSVUIbyAxL7LOiVZQ8_5q_xIeIsyUqYkcecGSdUsec7
MJInYQlPJKT7WslMAAX3zl9o4ubt3aBXTe8pSV5uzdNVFSL8rKed1lWw5BkT5qiJSYy0EvDemY7MUeRgpwntyDFHR
SD9-Es1OfB84tq2YpeHBR2g1GnbaEmflKb-3u20eB9SQhrHok7kwl_OSCEm6ELjfsI1rmxXbxl_ak-AEMZ_hu75My
rc-ADNfYWexmRJZFWtCY1VJHBGjKVb8eY9upzw2PI1bNx1CAIkTQtYOCbi3nK3EFSgdVudZMARbIgPRcX1CCunFgE
fTgRm_lxEcq6Qkca59JcfWTAF4SOdBoi8jQn-yoTX8uZrLqqH2gCHUuTZ8A4nBULgSB8Z7sbdNB_lOdyn_yrFpACA
EAl7aJ6MWhb-tPCJ8BSh7Qw1ypCWzVXhVScReg9ttkL0sMGYyyRI5B2dgepYJhVMLwsQAIgdpfCGSEiTWSs2TpLpV
i0znww9QPISQIa2pWN8Ht5PSW-iyefVdMYDosDzbOoQrYNwVdhB_k6MhifKpKOrzAoQZYKdwg0krKV7ftkq7pQ-9M
c5HowjMmDfLhltEAJHtVtbzy3nnYI0-J4gAa5iHs26UC9IQEALFk2Gxx88kO3CPu3SvxGK8zD-jlrgvMffVNExgpi
mqghNzyQhPMSw2AeA8U5_fpF9cbN0UQJx7t6gmE1c7kkepNATRecEeesdrvKklyxuRazI4GL7qlKHUykktTBwQQfh
No_VMVArGSU_gjM-VaWIEJxefMJnQFsgqQ0ALvBAsx0HCK1OcUkIuWaafccK2yKv6Vvf9wytulxiXknDkhMV7gTWY
KcuHWDYAJqezqBlWV6yvGGWkGqWquq7HwyPY-uATVbu8mdKz_H2sgmYdQ",
  "priv": "TK5a5VLDLOMcxsYNS49vGjawNMMl0Bbm846PPVwPAKMvawmQFwwVBD-OthN-LrGWW6f-d2jz_Rl
IcnSPhckg5A"
}
```


Figure 28: HPKE-13-KE Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiT0pvN00zRWozc2hhRnc0VmRvell4dHFvR1
hzTUE5VERrd3k0UHZuMEJDbyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjA2dmlReUFxSHZ0WE14R2lFMmw4NzByOEk
tYXRLOU42ZUVhcG8xajBMX2dGNEp3MUF2Mjk4SkpVY2VHemh0RHMtSHhia01LS0Nsb1JHUU1rWEN3N3VYMGR4emR2
U3A3U3VYU3dDcmdYUEFXSWdKMVUwbVhTMFAtNG5XVjMyT29xRDlMOEFvdUc0ZV90bzYwNV9RcEtiSjc5NkhSekhQe
TBTODRjVmk4WVNWMWpCbGtlbnZSUXNEWHEwUUxYRG9xd0ZNN1lmRjJZLThqQUJRQ0UzQ2J0T0JYdi1SZ3dSN1l1Zj
B1VjFzZHpvS2luM0VQTmoyMXZPcm1iUS1RSDc2YzVwR3NRaUlpQWRCUkpud1JhRFJJOE5kYW0zMEFNMWVQemZ6UkV
JR2dvdjhBSldaNUFWb0RpcTFSYmR5OE9PQm1fRm9ZNjJzTmZacWNIWmlnS3czcS1EeExLTmFpaEV1MEYwbDJrQ01B
ckJ1WDFycjF3dHA5dC1DQW5mZHhlazZlWWNoazFWOFM2RjlEMWFpUEJXeGhoTzZxRWxjMnZNYnk5eXRyTGl4d0t3N
VBVaWYxU1dqZEh1dlhnZy1MZDlyWDIxckhWc2NJSWRMMWI5anJxSEpjeENaN29WamFiV0JpeDZDRVEzZkU5RzJTRG
FTNG1uemxHQUphM0tmY01iQnU5Sm1QOWJDTjFQUUd5b21iWUNLWDZqSWstXy1lOVF1YnFicVNYVVVkNlMxU3ZrZDd
WUmNZdHVmb1MxaWdINm5ET2UzZHlvYnNYLTJNTHVndlhYYThxT091UzR6eGFaMVA2LWMyalg4aG1kM3FXSGpOc2Yt
TDk2eVFvd2gtY201ZFZ6MHhhLXpBQy16cUYxOXRGOGQ5dmdVQlpNUC0tUzU4OUhpQVlLNG5MZk1CemxvSTRCR3pDN
01hUElkSmp6dWJZWG1MQWhFYm0ydzdtNTQ2dXNtaUQ2NTFPUUcyVkFMM3pjQ0hBQW1RLWpYalAxZUJKZGhCMnFFZj
dFbkhCRzMxY01fNHF1Rmt3TXNILTVnXy1rQzJuWmdOSW5HNlBHdXlTMVp4X2VyaUJXVUlNOXV0TURtWG9UOGN1RUx
iMnVBODhCM1RGN1BCeDVick9ZQWlIUnI5LWI0dHFmUXJ1UTlvcnNHaWFDNDdOazBid2F0Q292YXl3UXhDR1hieVU3
QUE4RUJhSm5UNVNTV01PV1JBMDRLWU1PTFluX0MzazRUUm1ib0dpR2tjX3lfN1pKdGxjTnUxVG1xblJySVRjQWtQU
DZNZlJxa1pOTGlUMWVQSElaSlp2VWV6ZkdMb1cteUFKQmptUkhvRGEzSktqQmFSSVQ2V3dFSW9LbDBTZC1Gd3VBNl
BnV2lsaV9yRWwwbHRVdWlmOF9heDJ4RG0zRnpCc19sZFh0d0c5MTZsMHVwWFYxUkdwMlZmTlc2ak82WjRRM3VVbU8
2eGtnUy1VVklwbnFMdFlpek1lNWdCb2Zhb2tMV203bVotaG5VdXpwNGhndy02RWp3TlRHWXp2dExseXBRVmZBM1pn
ZnRsVFVRYVhISDRsOFVHWFYyMTYwdUs0Vnk2bUc2WEIzbTJLekYzczI3cHY4Mll5dF9qdFZxdmNfcDYxd2RpUkd2a
0Y0RV8td2w3eUZaNXpqZk1BRjgta1FhZ1pTLUhWbGtTLW0xUjY3THFkRjlRcnNmSXVudThFSC12YW5zUlhxUmhUTj
ByXzRGWGZoLTE5Y1ZjNHFnem1IVzMyNHNfZUxWa2dRSHVleUczeUlyUU9LTkdwbFBjWWJFVmpuS3pvMUc0WGRlQVl
```

```
WWjc3YzUyTGdBbTBlZnkycFZMRVBTd042TnpXYTktY0R3bHJDZEd1dndzN2t0dnpUejk1czZDRTAtNEg5MHY5bERi
NGFDREhvVTJiNGVoVGl1QmpSNXB5V3JGMGRicUYyTVFMaXFqWHhmOWNzWnduU0U4Nl9TdXNhX09TUlZpRXc2VzVOd
2RoeWV4UnhKN1lMazVoalNLanVyNzVVUm5XQ0VpUjFiNERhSXJ2ejFHd0xES3Flc0lWR19ZUEtLY0NtdGQ5VEJPNV
hFWFg4TEFwNFh3aU9aT3RZUElXQW9iTHNVVDhZUDdUOHZ3MlJCYjlyeFhkZzg4U1pGYTlKaHN5b0pmRllXT24zc1B
EWFRCbnJsbFZhQ2tGVDhScW9hb2lDS09VUWM3czhfS1ppcmxGZkNyZlNLTVhhVFk1c056RmxXT0hyWmlMMjlYZHJr
ZHl0WVc3ZExLWHZKUnNtMnJfMFB6OEZpc09kbXZ3LUhOalFKM0dRZUY5QkNIaUY0UVdpa3hsSjMyU1BjQVZRRFp3N
UEyQlE5SzU1M1p5Yi1xeUNlUUlqZVNMcWlXQnFhNXRyNU82cGlwQWlZWU5GMHRIaVlCVHNkbDlvdmJtdnZSRTd2S0
VkMU9XUkstV2VvNFhHOVpJN0w3bml3TUk1eG5CYlJzM1NSUXlZVGNwbUdjS2dqa1pmNERhMzltRkxISy1DbmwwYzR
pZjFwRm5IT05CZEE0NHJzR0RpN0UyRUZSSVcyOUJvZDJnRDJWeDJrTDhjQWh0UF9ObnFNWHhTeVZkSERwaHRiXy1Y
ZEsxSkY4LWJ2eUJsTkxVMDNENktZNHRtVVBmT2U5QkF0bWx6STVPZndRRjNUWC16MjNfZ2pzcjI3WWRKeE1lUWFlQ
ThNVEZadW80Nnd0ZFhVelJ2ME0yV25yaUN2bTlBOFM0UG0walZyalV1cVJ0SjRLNHhMbk1GUTNkSWdIbEFqdyJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "4kbBObrz8_rXvess",
     "ciphertext": "rp61DElcDQKgF_QsxMP2YsdsXLUdFiBVV-FcfEg7rf5Dgny1s5YnTDs7d9Y_TPwWXEIhI
UmPrsSlSd2VJPEmzW76oY663xchZ4VfXyQGHV3wmBWAIpNm1rm0cIUgFJMUIkGsgGiFCs2mLhzQKpASFzzA7Iwu9j
xnryhw01dMc9xbOYJ_fNrMWQI5aepqyQKQcfCkSU8f_FSvp9NQypbd1jOf773NFk-vurwu9mg-I0P0UnIWcRWgQpE
6aXzdxZ3f8VzxxTBjpPw_HertfqyW0F-YfR3nHXwqnrItH1oY3NZWT8rPLujEqG4U5RBUY6fbNUiPc5FQCNNseTRU
CWZNLFoLKQdHL4rd1IVK3MXMXuD0",
     "tag": "857uXyIeZ-VhuBmOFb6Y3g",
     "encrypted_key": "P0RlHe_TVfzgUj-hqTTlUXJgMpX8IJ6VY9sM_IWoAj9D7mEVC6Hrha2xnIeUOp71"
   }
```


Figure 29: HPKE-13-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiT0pvN00zRWozc2hhRnc0VmRvell4dHFvR1hzTUE5VERrd3k0UHZuM
EJDbyIsImVuYyI6IkEyNTZHQ00iLCJlayI6InZjaFdSM2RwVTFjNUVnYklEVWxtNWVUVnE1TVhJWXp1NkE5LThCVG
NGZ2RWR2JOMndOWERsejhNVmVuMWFjMklPMU1KX3Znd0ZmNjJlNE5NSVZsQ1dCbUdCTmtYWlByaVVoWGhxUW03UjA
5Q1VjVm1CX2Nud1YtYnpHQVIxcHBfS1cwX0xsVll2YzZpSnhCRGtyWFdOMjJLcXc4YWo4aGVVaXVPWXltbmQ1ZmxY
ZjRzWjdhOFc1bk5vVzJqOXRJNnR1ZXlDSnJsNXZDQXRHMjVDb2lqT1UzcnczaGZQdFdlX1hyRENHa1ZUbUpBQ00zR
09SdC1NV0xHaDlxeklEM1UzMGhaQ0NSMXZndWxETGhGWXF0cWFyckVZSkFPYTNEaENUdWN4ZXc3ZkNuelhmQTFxRV
MwcWJoTEs2VHA5S29zYnp1TmE2TDlPQVRTQmhFbDNjOEZydnhwUU8wY0NDUEljWmstcllhNV9HUU53cmpDTkdfMGF
iVFdzc1c3amlrUUU0ckVwcHNDYk0zamNINjBjVzZtZk1WZW4xNE5VY3pFMU1EeldlejRiOXdCSWxEQlNoVU5RWmlt
WFdRWXduZklHSlFiOE1YT1BlWVhYQVVPcEtLbFFocjVSZEFyTXE4NGZOY0x5RzdjMUwydENSaUNjLTBWZnhaUmlEd
0dNZms4UG5kY0pSQzhrUldHSTJzTTNGdmJpaTloV0JYeWYtRnh4Z21EdWY2UFI2elI5QzhBZC1YRHdJcTJpT0dNSk
5NWHZtNXk3dDV0elpDNFJ2cTBQWjh4QmlmWHotWWhVY1Z0WnM0Qi11aERuQTJwZ2VWMks4Rk4tVGtubXlFd0VVSnN
rNDVhZTktMndLaVlha0J5QTNsdzdOZkJuN2diaGI0WjhHb1FIV2RYSGJtLUtIbGZiS1psczBEUC1IeVlWVWVDdGdf
cWVPX1BweW5Fa2tzOWdXTmpYZnNXSFFxcUVNVmZyMGRKcHJKeU9SSGtzQWFSdEUta0VvWTYzOUEtanpMTjBSdUZKS
nBkQXpKY3BkWHRGMm5KQ1JYZExNanlHV002WmZsM3hXa0ttV0VUNmZITDdQZlJKRWFUM2RRR3BBTWlCRm1DTTQwME
8tRmo0MXNndUJabEF2RUF5VjZaNjRpalg2dHA5cTI2LWJxd25RdUZBMU1OYUg2YVNRSXJVM0Z0ZWI4Wm9MR2trWjJ
COEZNRFUyT0sySDNmWC0xd25zVWpya0RIZDdrMU5XdDdzdEtKMUJ4MzVFUzEzZUc5NndRcTZYb0FQVXRLUktuTkow
R3VqOTdjcTRkUDZjaV9RWFVKYld5ME9jdWFtNU1KV2hCdktkdTZDUzhrSU5WbDdndFJQOHZKRDg0d1VBNFlKYWpwX
zd3YzU5UkdIV1FRSmNXS3duS090TzlPUDVTQTgyLTBucHY4Tm5xLW1PU21DYi1hZVh3SFBGSkNIZU11MUtoZmY1U1
B5ejdaY0EzUDVzVGZISC1DOWg3aTRVUG1qWl9lek5JNW55dTZqYXNIVkZtODZyd3pUWmZGVS1lbk5iMmZUcE5DOC1
TUFl4R0xVdDZZOEtJV1JmRFpsQ1VSUy0tZkItZEMyYTVSSUtFSHg0VFBfclRwc2h0aVFPcGhWX1VmMFhfX0l5U0py
eVNxRjNfSTJMUm1wZ201ZjRDWVJXRTJmRnd6QXJWVW1fMTd1ODdGVHVUc3k4ZThPOG9Fc1lKQzNhSzBhQm8tVjJHM
1hpS2J4dk9fTE9WOGk2M21ETkJUM2Frem9tM09lTFFvR2dhbWI1d3R1cXJyTTExQVhPdERZOGI3OHlMU3Z5dlA5Zj
hRdWhBQlhCYlEzSUVVNEI2LU1WVlpKNEdDZ3FPdlc0NHhOS3Rnak13SVRpYy1mMkhaakdUaVBkMmlnNzd0SGVlZjM
2UDk5SlFHV2ozX1lmMXRVVmpTVDJ3SWNGSnhrYWVIQ1pqUHY0aUoyRTJ4ZjZOZW45Nk0wVDlkMGszRWhDdWtuX05u
WDhqX0ctemVtTm94ZVVORHRpT00zYzBiTmNMVldaM2UwTFVHNFhOeEpqSnVUdkc5ek9fVkVsOGdUV3llbTExOTg5Z
khINHotQWxlYl9ZV2hfUm9DT21GOUtMUWtnQ3hwR04wZkpJS1RfSVJNMERieFRKLUxVbFlDX2RGTjEydjBDellNRl
ROOU5FQUFmdTQtaV82c2lyajdNdjZRUkg1X2xMVjFRSjAxTldCcjdhejQxcnBBRVFsOVA1cXBIS3VhU2dNM25nMHB
Ic0tmLUhSTFIxV2J4VFVVSTFCbHpaY2U1aTJORWtZV3l6ZFhlQnFIWC1fVUdUcXZQTHRNb29MSHd2dm9vYmpXa3Nq
ckVaQjBPZXZGXzJrXzlIQWM0VzJyOXdLclBNMVFSeVYxM3lhRkxXS2NXblRlUHNRQXJBMk5RNGtsTGNxR0VQRnpGN
UxMNnV3dFdCZU5pOU44c1R3XzQyYmNIVEc2LUlCXzFMMGZqTEg5X0ctOTFxeWtYenpjYjBkeWI5RVNuOVROMHlhQV
I1dTQwTXlkVGJ5MlMwd1RQTExNMGt4VGRTMUxpdG54SXRFQVRhdEFfbl9TMzlIYlFMMmJFZ0NEUXBuUU9VaEFEU2Z
VdGdJQ2lYTEZuVzZLX0Z5ZnhtdExhNy1pblpLdGtLa2J0NHp4LXJlUnBjWWI0TWxuNDYwYXNzMGVuYzFSMVpOVUFP
alNZbjdYb1Y5WW1qZGhhb1BLUTJEWm90UnFqeXE2R1l4SHh0R05LbnVNOUNKbVFBMCJ9.NblHYeR4VJuwv8x-oDPk
CG93nKNQBwla3QWw5eb_HEhPRn_wTVPfolDTuFk4LXOC.pmOmnDiJrW0Wzr1D.cNEPZGEgnCttzsihzRc14vw6ZMW
DSU0VK3AJqGHhCyffGoR3ZigtJVy7wG68VBtEBdbe1BtTbXtP6E662zYJXybH48g23gJ-SlElmunc5aYGLYwPwctI
QZHW1LUiLOcrsR1XDzCIXN7T3TqCFYmPEDDeaseU4y1jL-Ho_dHvkyQrc7oOpE9-y_vbl60oT1mRBH6YKroErIcil
FoxxDpBWraAIBL2herQij9GCkVTg5tUwkpnaedDhFwZTHMvf2mmfn6v5rC5EOqKFZEtQFgpPJfzDCG7_wNwLw9QI5
RYtfTm5SlgFTkY-YnvDQjNgMmrV8Tfzqt_8VtgXbQ7FdrcrTUXeRj1SCFWDr5g2ZbBW240.JQvmVqR8rT6QqANUI0
6G8g
```


Figure 30: HPKE-13-KE JWE Compact Serialization

## Acknowledgments

TODO acknowledge.

## Document History

draft-skokan-jose-hpke-pq-pqt-04

* Removed ChaCha20Poly1305 AEAD ciphersuites

* Renumbered algorithms with intentional gaps to align identifiers with COSE; added an explanatory note in IANA Considerations

* Added a Security Strength subsection and HNDL/multi-recipient guidance to Security Considerations

* Added rationale for selecting AES-256-GCM as the sole AEAD

* Refactored the JSON Web Key Representation section

* Added informative references to I-D.ietf-pquip-pqc-engineers, RFC 9794, and CNSA 2.0

* Adopted RFC 9794 terminology in Conventions and Definitions

* Added rationale for registering both PQ/T hybrid and pure PQ ciphersuites in Security Considerations

* Added Hannes Tschofenig and Tirumaleswar Reddy as authors

draft-skokan-jose-hpke-pq-pqt-03

* Clarified "hybrid" terminology disambiguation in the Introduction

* Added descriptive text to Key Encryption algorithm sections

* Expanded Security Considerations with ML-KEM-512 omission rationale

draft-skokan-jose-hpke-pq-pqt-02

* Added Test Vectors appendix

draft-skokan-jose-hpke-pq-pqt-01

* Added example JWK representations

draft-skokan-jose-hpke-pq-pqt-00

* Initial draft

## Authors' Addresses

Filip Skokan
Okta
Email: panva.ip@gmail.com

Brian Campbell
Ping Identity
Email: bcampbell@pingidentity.com

Hannes Tschofenig
University of the Bundeswehr Munich
Email: hannes.tschofenig@gmx.net

Tirumaleswar Reddy
Nokia
Email: k.tirumaleswar_reddy@nokia.com