Javascript Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 14 November 2026

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

13 May 2026

JOSE HPKE PQ & PQ/T Algorithm Registrations
draft-skokan-jose-hpke-pq-pqt-05

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

Copyright Notice

Table of Contents

1. Introduction 3
2. Conventions and Definitions 3
3. Algorithm Identifiers 3
  3.1. PQ/T Hybrid Integrated Encryption Algorithms 4
  3.2. Pure PQ Integrated Encryption Algorithms 4
  3.3. PQ/T Hybrid Key Encryption Algorithms 5
  3.4. Pure PQ Key Encryption Algorithms 5
4. JSON Web Key Representation 6
5. Security Considerations 6
  5.1. Security Strength 7
6. IANA Considerations 7
  6.1. JSON Web Signature and Encryption Algorithms Registry . . 7
7. References 11
  7.1. Normative References 11
  7.2. Informative References 12
Appendix A. Test Vectors 13
Acknowledgments 45
Document History 45
Authors' Addresses 46

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-17, 11 May 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-jose-hpke-encrypt-17>.

[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>.

[RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/rfc/rfc8792>.

[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. Long lines in the examples are folded using the single backslash strategy from [RFC8792]. Before using a folded example as a test vector, remove the RFC 8792 header and unfold the lines according to that strategy. The complete unfolded vector set is available as examples/jose-vectors.json in the repository (https://github.com/panva/draft-jose-hpke-pq-pqt) for this document.

A.1. HPKE-8

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-8",
  "kid": "DmOWQi-VwrjZWjO6mQQWdv3CJ_v9k_PH3vS7S0xoah8",
  "pub": "6XRnIatC1KtI7DZlj8ISDxZvtsFeBOPKQETMRRYb45dR0kw6TDSb8UMXHH\
    WhUBdbEBof5gvIJacZG4exGku4JsysQcc9AVR6Ydih7kaPNQgCiiKw9QACNCMWx2\
    p171RVCpGSFoOwaejNGZeNJKS4jqulOWFQHGtbWhl64HZzlkZMxhqdA-EecEOLhz\
    CkbCMMtXxb-cxUVkOxQpKkO5ofmEaKH7tjyNZyVsxqgUZFn6K8jOq9g6GCOEG4aw\
    GB6AZC72yNXLDBnVCy_7OMn2bAeos8AvhHkbsL0hsFFjsnWcG_IYvNPzUAcyGZlp\
    sqjXJIh4AUxTi6iFeJFOE08nNM3KQEYlxkMAulVas2E4KU_TGeoEJeZjA5TPWVAQ\
    iPFFQ4nNRh1kotf4OHtHQVpaMzAypItIXAU8LI_gl4rdFKTfYu18MKnygjEnO9Z7\
    e2cYwj_hqx-AQdA6ulQBcNR4DFSCOTLnMB22GMXGVOMDCmiaxZvchp9iEKNJG4Tk\
    ZQmoKwR9pbEbahmsm1WvUbR6kEqNYOE0MMsRWNM3RBNltm0Iqo8RKMlpRq5RceWR\
    RdjRkKdChyhuJ2ebBI05iRsuE6AwWEbCV6dQqNZ0gqdeU5imECjFWLNqYvs0BaxD\
    gmoSdg4rFlq3UrZ3gLD4UTT4kM97HO5iedxoox__octTEEImMTf8uJI2M0nKTIpb\
    WBHlofTfulcqVXjFYpr9GvuKM_mElaoJwn3MQYrFNLcwY-fzy9fqvGFtF-62fHcp\
    cL7SVUu9KW7igiAHQfwXmCnMQzsxwLowVk8mFjDYgV2iIoNIeuwZdc8-I0A1CLiq\
    OQNwCLObgSMVeo-WUvzmocsFOUtSUS1chNNwpjMCGKuHxOYOcvKLxH7mvPp6czIo\
    vPsqQUZdloA5Wqt8U1sDRZfrhRlUi4IVoTmevBpaEYK_Jze3cIMOkRKdO5Y1tB4T\
    IcAHE8oNUarUEYx1YDUinIolRBBDyBAmR7rbV4iGenGHwgeTIZ0cpppFEDbkAX4A\
    aG4YKGdGWrgWhhiDoPX2mda_BLOSilnlhmM2BhqGZBkKK2E1B5fgER-_AMYeVl9H\
    EoKCFHm6KApgnLVnYMQjEv7kC6tsqxs-pOcnSs2EpGKMMk4gdIlcFNxsVU6sXINH\
    ADvNmtNyQgjRFKhmNPtYchXHWz_tgccWNkm1DD6qMATOoZcscAu8BBpKUwUIkIUI\
    CwKpay5KUsFjKpC9HPqSONVMVu7GYysVC8UDTMetWoXlSiDetoiolwFGGpIscf1i\
    c_rUhbD3pyxVI8DqCsdFg2NcSvIJRoJBO12KHKRIYnc8ObgCzJBULNZ1Rmc5tCbm\
    cW_mmhg0OiA7EJjwi_eoY82_g0eiyAr0K4DmBy8yqWDZV45KfAnYQBQZvK8zlj0n\
    pGqVWusxzP1mw_Dbhnp-Z6SyIrHNI9unG7DbeDhcnBD2QBp2t6cNgvUoCLzPReQP\
    Yy_bwVEwcrPSO4SjUG8mhuybiU5NWdgIRD95gD1ApNRoZeJIhfP7yM1vt1ZCxfV0\
    xEvUSb25DOebimyplEvv7nxam2hbnlRQme00B5wPt9pETxPSQE4ZUd6u60U9e6F3\
    C-Fqjwfg_xYMk3oOcZQ-P5NrsNxK3ho7xmtpSKVahpf_2P_o2Vz8YFc7t2S7jAx9\
    bRLQQpbA",
  "priv": "c1il1CJwUdajeAm8PMZMq4mw2PH9Z2vThLkHU2MQ10A"
}
```


Figure 1: HPKE-8 Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82\
    bVFRV2R2M0NKX3Y5a19QSDN2UzdTMHhvYWg4In0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "zRayDf-tglGK_UsfOjbbVDf_GPQKpRLNx-pusFTw6REZlhoX\
    c8INMxK5ETEdsx-0MTVa_8AIou9zUiaHPw-Iv1nk7X0rdIFYjKOTnjRUy_DuRIRa\
    b_o1qSZ5-x6sBn8McfjuKMvcJbwU2uqW9NJyQtK_2yNmVvrYiPEhnuO73O_BSv_G\
    SBSoHgFWEpbb5FeH7ujs7Pq0bV_pdI3XnabhvIPVTmnrkzP2J4vcYt00B-wxAxiL\
    Uc9zaitKnkn_ofTtOp1lUUeuUzKDPYuo4x-GRZsG_gf2Ez8FFE0RIJq6AmYr3DKt\
    SziHFqeim8uVI8_mtE0wIj6BM6eYYL7c79MNoDlop5P3QI3-PrZ7HrqULs1U6W7U\
    DScowuP80jJQjawMUd1itDjlB1BkwVH2u0BwoHWzA4NxdgsusIbDDmH1f-k8Y5t4\
    7tb3B1FeBYK0G5MbXQmc-h53dACqTqd8nJq7jQNfzmELY7aWmT_Z72KGyfwUY731\
    JCeODbDIW37g0mdOR7ZcFgHm_Usj02Pj2J_Fsw2N3vkb_IEWi8abtP7NTaB6mYmI\
    -aNGqDEfXRVI5K7ReLaHOqWxtPkkfysYbeUDZncwkt16rFa0FzeL40sfv7yr0J8K\
    s-HXPItnfmha_FDB4MuSlxmH8fADldjXNozWwB8HWSCEp111sdh_cP44rRNxPZbs\
    S7UWyTldMixcjKNncA1dNhafJ5qXjq32NUiN8R2BPkWCBzKMfaKN7bujZphGIRZe\
    kETFSx2Cp9mO6hG-CqV2dsu9I_MDHgiWEV8GwFC4HyILVJRc9qysutXw0b2UupEo\
    s9BzuUaoYTvGHwpNWzB77-vON3w_FV94KrwQbiki9_vbVtct5ODB9Kf8KCHv5DPw\
    YGi7e41zKoS1Rm2Nczt56SC_RqKn9nFR8yfH7bEhvnsQHi_qXHWOFWN7f72H9Cb1\
    ascZo6XTYaVUCi_RiRS8wgLG0LvOyCfpzgVNpbFhPGBbTZceZW6eSGNGK-RQ0zb5\
    sJFZSuM9P2cK23dnogEGTPRLp9DWs3NUBW0Z1yVQw1v9gukwcM0xYlo-zfQbwWzH\
    IdzJboQR-DqeOllx_Jjh1tZPC_nRBdu4DPX5KP6JDsIrv7hw6YQ5ocQwQMdcoGcF\
    WsrKEOk2ei5HBjbfJQngzKT89TpNaBH_wXpZqUL25bltMM48JG6rTiG96eSF24BD\
    ONDAUDgrzPBoT_ipdN3Tie0hQHxTsT4cZP9o0PeEYgu0CGPUG0wcirNh1hnhf-PT\
    EAgfCoTyqOJ_iVj_HZO748slRlMJ4P-Ij4qah8aYhAWJYSdzfBCkMPXX-bzw4ovK\
    uCbFlOwT3I_tj0lggb-vVqSzv5nkHyqjvzGTmEK1Tq_Wy6uxyD4gUBPKkNoPMvA6\
    SeghLYy3c8XF80XxStZX5OAQV36AavxZrGyX3gMS024KX-wbNytokZbocP4EOLum\
    sml35g9ePuXmJjEweCm-D5fqMe_uaLaRP9RveNyNsCd3arMLkn5PSpRTuTsMOhLm\
    45olI85aNT9TrL1oMw",
  "ciphertext": "Kqt2-MjNX9R4OmghbRcEPdzNJvCyvAUbezJcRvKnbzWqu3JsfGk\
    O54gurgSvQcQhAnTWLfJbDJvFJWzqCkXoqgYtgsvrnxFNqJ_j7194RxeH39eXb0M\
    oVkTgPRQO1gmbtr9VPTrkPXlGCWZjrdVGEUZ5qJZvZfHIYyo2_egOP5CuMzbZuNQ\
    tjxeTdagfBqAymYpk5O8VqubF160UrVDZnDfm3ndEGH4oFZwPVtPH2IaYcubiTm1\
    00oxPdTTKZX1PeieRG5RodWY6rMsrA0_dMbXrTDg3spqXloEySB5i9w9ChHZ4s1U\
    HzihtusJvw4qI1kQSZZc6RxELIzED3s5OHhpuzKTrl-3vVwlf9Ily74215pZwdJW\
    7CVWTL-Xe9fhxEA"
}
```


Figure 2: HPKE-8 Flattened JWE JSON Serialization

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82bVFRV2R2M0NKX3Y5\
a19QSDN2UzdTMHhvYWg4In0.Uo7Qjidw_FqP-aE7NqWF7tvz_EHaMj2ebRvHtpRFqXZ_\
cXQG6dZVXDuzdONeZpgvmjox7zdKBUDG81XxTHkWbtEfHKwA4ByheUzpBiGde_MAyCVa\
LS0C7tYU1tHSbDIOR3RkWHrsq2O62R4saXt12mUUyvdZnd97cm3wEb7PbC06_b3OCl0Q\
2MRC2UPVcGU-yXfldWZKZmotQDQbzoys6Zs2R_TDr7WtilKpN9F6SXt2DMnM6n9zw8gg\
tUUtg37grjY_Qfo8NPlBTPcWntQuysl8xt2uls4pe5KUfc3mciSIPLxGQA9AfqHGTrIB\
eXE51n6WQc0gp8RpAgyeGpHUSx6-e2TQscn1_TgLBrWSSOUcR6SOd3i9rcWSo3FOmJc6\
GcCGCvB-tYqSu2ULUIgBXLlM2O8OZXIMHx28m_f--dNZH7YVdxZbIe69RLkYCxoZlolh\
2iTfJYvPkBJT9hSbAw0jPh49jDaGJsBGCORk8DBi2Ah1_zJgx3otXr5t3sHgmo-dilty\
Q_IESRR3FzwB3HdLeO_HnAmnKnpABKWzvauVEYoNHKMWG7uSZMLYaoheuW_Gw6wzqETR\
R-hgYR2K9YVlKmRGewZ-juYE1zpxKk-X7iAPS0q-DTXIyqsr_4gXulomCy1pzHCdwkc4\
Ys_jvCUC5MweojTzQTdIomo_JcCVQ6eOIPqopIsonKWKT4lSJ6keswboCStOElVdqGti\
g_WXx-N4AjeZLvnTKPaC0c3zjlVf5Dos-hx_-EjBfvtXDEQUlI28dxr5CnL21MZ_QXcJ\
y8-sbC4aZjczt8LV_mBJJwm8Y5qfjA45_s_oE7IHcGn47YTb92JfjUv2GD9RnFKLYZyo\
yULp5ypgxZ0LpgHENksobFjrsQetZ9D9UV8Irq_dJ0igW_a5AOkCx4oUT2XMCjhM3Tkt\
6jUJCU86whvk3Ux6zA86UEiPuU6aee2A7tRU9EdRT4TGv5Aofe5XhFtngXP0QV-7xZ35\
Uk6sOxNsgagaNw_wqKUoIazXxOb5BEHdb5VFTqoBAXAvyi4Kga-caLuWAkCHDViDDKIm\
P8Orm57_BaxGEjwmlsggLAxXrsx7Seg5qRe_YjKCQcHjtjOtgXsp485CemZjz08CzElo\
O29eGMVAlUVUlOLi0YnqY_gfyhF0r8SI04_hC3U9nSGsjz4IPfGjlTgR0hcm3BH-72ya\
ngLnEYHFgrPQMosxDzkbp8xEWFntXwAdbbmNkNPvSpT69zZ1Af_7rrmdXXvVAghL5QlA\
8u8G3ceurO9NNwfHdr6T2FdclLq_tmGlo_Q5_5hzX_f4kMmt9-xLfmJduoK44-sZ4YC8\
jq_OdJNgs2FE7fR2h0fqQI6PpVyYBU8Sg2LkkPYa6sTg57oekqLgUS6ZPNFmV0PcBt1i\
2JEGwpxC78EQYNKU9ZdggpnHgpE6aSgBtB-P4Tr5p8gMhF8E53UVNHRPXWOjfChtA-CV\
pi8p6qE5_a4MPedjf0GkcutKIQ9WNL2zhrYo7DvlylBcX0YQUcqltcKSS6jaS9FeNQ..\
k8no633YrPgoESVevhyqn8Q0lihzU9hyVR-uzYzPDXwxLcxEK0pt-if1bKq8IoJyZWB8\
4Iry5efVn6mSFlz9CpbOKNwX6mZAFjM2gsEa6GXXHFt1JF-tMmQK1T44WRpH7HwZ29d4\
nrQgTiQ5sjDgc_Is9ZhZ4NOYpVo5sEcbbx-uJu-0u9cXgoEAXk68BlBQ6YCDQwoRgJzC\
Lz8q2jyrc5RIzJbVZb57MJfAW5_CJoaWqcqgSj893NXN6-Qgr7KZQ2U2Rm9gx8kyD2A6\
PrgS_jDvArJHRtFhC7c9ax8btYkcrbmRfWG5UxVOjue_BOh-xvkpWQnJXjHOJbPMAgCa\
ZCQ3kVbG_zfhtID1nlQWnFZQA3jG16jAtIGMLb8Qgjn-cw.
```

Figure 3: HPKE-8 JWE Compact Serialization

A.2. HPKE-8-KE

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-8-KE",
  "kid": "clBPky-tElQGRa8AQ1MYfMPvfqmhOs_5lIejOuqAdps",
  "pub": "pxQRXrRJLke8BMBXa1FT74gM9fq71fEwRPRndVsmsYAMU6llEnJaeKAagj\
    xk44yl9Psn7YBn3tVXXLVrqIxyWhGsP2pmH4Y2eogBaRMGBfQy-TM_RzdFE-hKLH\
    qHPmqP_PZES2s6O9tBkvk7D6fKZKiBDSKrvWgrKCIo1DccgfHEayxCtex1w1ZjVw\
    eIZWtVA3V_JdijzobGiSU0dzqyjVBBCQVcWiSFLLuX6rFtiPpsa3SlavpKHaRTIZ\
    x_5ocCO1LBAKq4jwew4jxnhRujX4VcaOE2MQQ3FUmT6UgMpWSfymJNBOqwN3uU3E\
    O_ktgMPwdfrRVihSgirkiV7BhSW9uN95OTigiJIiedxPV6asK27cCcPhN0lJQOyn\
    lah8BjySYKwdMRHyxVVhGDmnJ36veTEDoboBhq5iAkcqwed7O-KwC09XcVciegq-\
    tYI2NWMOkBdXE_W2qvvPIkJpOYtKAztpUcxhBBPitRGQcdz-wD4nik2DFk82sfDN\
    pC_lV_XWYR3KVwiBix2tCB3tw-j9loE3AaxGefsyl0PPQsFGu2i5qutBlUclRUhM\
    UkiGcyEnx5S0xNYzyuM-lAa3WpNzlEc_SoqmKvobZp0pi-ExYnpIQJ7nPJFNXJ9i\
    g3kvpNCxnKlEwsP5w91SbOcLOBQ5dIq-moh4kK9ZCry_JkAmmAxhu9kGCughacCP\
    aUqgZrigO9bQHHw0giX2EB5hA-r6VxzMwYJcox9SxD0tJVsAMhCUGhGuS5wodrPh\
    ay-ss78AMZiXm3D3mDe-sA0VVRLaN3HgmZw-kud8su7bKh9zYec4iHaygQq2ySGo\
    eOKoGesVK77fiLlWaYLNtqEmywBblQlkZbOIUmcVmsTwd1yZG-rPIka_eJ9gAE4T\
    e4XgExooaJI4LAdaif1stG-lEZF8RmNlmvm4wdAMZQAqPPLiOwkVAhshMUfavMeV\
    iGedgk57y3JNpgqQuX-sEI5NmNMFW47wR3AesCpuuq_Skqj8EdeWWaIwh-L8iDYC\
    c7N-tLhNwgJOpnI2pH-CpgVShigKi6brIjB4QEV-JtRzKFZ_ZF0wM9GYTNsBM7dX\
    lxPUUVjLCyWFWYScRdwHypH_deyvaEjny-0DgpOuR5pxBWtFGEsoAQJBmPZFumwY\
    B5dZkyBRJrQPUENMNw0eZ_1yql1oFIdTQCQgEln9BFfCPB6MCX8kZknPovhJmq74\
    BALPWaINeZhniI48FGf8tz8VdJ11Mu7qxrNiUHNApTMcke3Aw2qKl-NtFeR8Ou6f\
    qQH0d2ShV-GvCcuxjKfUdNU1y5zYhlu6ZZwvkZ39jKl-t7Eyw6rAEnUfWA2hEXXM\
    aDqBVRYvqwhiM0nboODhWUJUW8OEpBp9eI3eel7tRFViiZQ7KsZmUBVyVfGJQvh7\
    DM51VAvUUSi_xPQzsz--yWJ3DFmYWF6eMQk7FdUXu7HmFxMfuNNGHMypx8S9RqfC\
    iI9OfOeqwVSaa2MAd-b2cgDAo8qVeCGcMVU9FRwrUscVeltcJI42sZiaoXFPUlyA\
    KncyajZ6gZhFNexIDWiSCp4L54nM948L-KcoFnZwHsueAjiJwE9dcy6kUtyQ6v0_\
    OxWb8OuM04u96GtOld8wVIcB7QE2fd7g9XTCdShgpdmMgNnGKrJM0A2Rbtmnn-gd\
    xGbyArJA",
  "priv": "biUK5NqJzXzWEAN0F2zzkrEr9Rp_QX55is_j7VYuHCQ"
}
```


Figure 4: HPKE-8-KE Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdS\
    YThBUTFNWWZNUHZmcW1oT3NfNWxJZWpPdXFBZHBzIiwiZW5jIjoiQTI1NkdDTSIs\
    ImVrIjoiOUdINDFMenpHYXBiUGFPeV92T0RZVEh1c0ROVjFLdl9xVnlZVDU3b1RZ\
    SlRqS3cwOVhUa25BZFJSa0VSTHdQdWZIZ1pKU1FpVzNHVGZXMVNiRVpmNFhDWjhi\
    c1ozY1c1U2V1SlVDNmlvXzU4enM5SGR6bEE5bnQ3MVp1eE5XbzFvbUxkYkZZTzRn\
    YkE4SXNBaDY3QnB6RS16eVVkWGlVRndvWTBTMDRpUE5RMmlmc0VlWEVFdW43ZXJX\
    Q3QzbnVYdEdXeTRxMTBSSWlRcDRWdUdGdWpRNk02UUptby1NVVRJdDdzOGtGWWN0\
```

```
      Ujk3U0ZDU0FFMEZVYnJqRnlOMExsRG9JS01VT1JUWHVpdUctWDNyOFdEdEFMM2Np\
      TGs4T0RNX1NRa19veTlCSmJJYmRJT0VFZk9QWU5udXl6VHhuNHpUZDFqd29zOTVp\
      UmRxSWFBR0JGaTJaajZOcWxfWWQtWU1aeFB3NFQ4UGkwb2R5cGRZYjVZdVJZbDdH\
      WlItamRTUEFCSjV0dEt1X1JSSnlZODB3ekNUa014WnI1bVUxZXZpWU9WQm1DY2RT\
      cFpfY1p0Y2ZxNzNKMHYzV2ctd3U0QmdwWFR4VFZYMjB5aldTaFY1TlhHTjE3Z0pw\
      cVpiTmFMTFVpMU9YRk9EaDcwR0lhZmNqbmFiVFVsRDJWR3RMZnBySGMyVlA4VHR5\
      Y0FLc05LbDNSeVExNDB3d2pONnZMRFljRUlyUUt3UzlUZURqcXVpTVJxeXlKcHpY\
      MXFCTTRSVENnMUdEWVNKSTJKQWVXZDNWbTBwOUcwRV9DS29DOTMyelB5c21zWnFo\
      TFBpNEhjNE9vOUZLb3haQm9JLVI1NUM3NXg2TFJrUHNvRFRJaE5BbW9yRURiOURR\
      cTJPQnZnZllwRnB2ZzE2TXZVNTFVRURyUHBBbFRabWVWcHpxay1qR1huc2NjaU5r\
      elMtLU05SHVUb2ltY0RDbTNUdUo4bGxfcjV0T2JIVXZxYklBSGl4MGJvX3ltelR1\
      WjRVSDdyckNmMk9sSzhGbG5xVkxwa3JmeE9uY0tadWVWUGs0NEE4VkEzX3luQmVz\
      dV9ORGtJcEFUaHhoYmEwd0ZmYmlERVQ5OFdYNHhBNjlfU2RaTm1KMUM3SklMWHVz\
      SnItd2d0c3MtZlNqZ3VKdHVpR1pUVzR3UWxKNW1jbnhFcXVKVEc4Zm5UcnExRVZ4\
      d1R2Rkg5akZlXy1uUWtfMEEwaVFaT0dBLUFfRUZvWHEyeWM1QnM1N1NON2FzQ2k5\
      YnR5Z1BvTnR6cy1VaUtMb1lJaXF0YzlHRlUtbXhtQ3BSaHh0WXpaZ1o2MTRPZU5t\
      emVFUFV0SWVYT2Q2ZDdhX0l3dWdkQ1lfaU9HOVVZNnV1QjlXclpuc085LW1fYUdK\
      QzZES09VWXVpUVhVRTVaVS00MnNicHYwdDFKUXVVZF9od01HUUpuMVNtN3NBeUpp\
      MTlYcTdyYTNtcnJVY2FGUmk4d2J0dk5Ea2JRZ2RLYmduaDFGMVZRU2lDWk5JRk1o\
      TTdBVDNaUmdhVjhVZndYa2hmdHhoUTdIYmNzM2ZuNnZMUjNkLXJiQ285QVFULUFl\
      UW94LThDbm5DVXBoSHczemQ3MGJBRFQtYTFRQ19MM0p3ampDNEdFSTR6NmtKMno0\
      UGNOa2FxN0hlcC1RVENiUzZ0NE52NVZLU1FLNXc2Y0ZNclVsTktWNHpFTnBpU0Ri\
      TWk0ODZTWEdlZE51R0ZPUUVYTGtYYmJPV2gzNm5adVVEcTh4d3B4al9hemN0OTdR\
      VE1OWEpBVFpXRWZ4ZjBBQlo2dnlyMkhhN0tGUWtacWpwMGR1bWVmTzRtcGVnNm5y\
      OU1UaGFyQUMyYndrWVBVSV9EQXlZT3hPOUlGdmsyNDdUMnF5Y3VWSVBWNzV0UDdm\
      Sk96Sk1wWktUeHZjdTRJQnNFOW5hbEdXOTMweld2QW9Hb1dsdkxRZ0ZQSm9fMjI5\
      TnIyN25IcWZfMzRzYUpidVQ5RjBzX0F0THpENjdjWnYzWXJjQ29XX3NHcXUyam9p\
      Z2xRN0kybUEifQ",
    "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
    "iv": "GRZLhvvj7vBw-FZm",
    "ciphertext": "D5bqaQekeFnn_YlzsERq8jp5w6Y0t2gulaz_ql9AIqozptDIHEA\
      aYwGJzfgv2W_woeFLXUnnZlnG_aed4vvmFi1r7CLamiwk8Xie_bPEt7Icffle4mj\
      j8DJr5KZUNNfStrKH5_DJRl53dOEeuAhYdXU08OgBh4ezaTx5I_2fDqVXSGfO5sA\
      WHINXWEPsrf1k275iMApQthhD4aAO2hYLAuAGwFGsySvXoj85BsNH3vLALi-H-RS\
      oXWNt64OxLyMXY6L5TVBBaSnn19-h6hZIZU7bVQfckoSKftZphRR99hWxZ2JQabT\
      YQMk_UdW7SUBJUJe0s47uFrKC1T468hp0WFenqHZjS2oaAodaCZdIayGt",
    "tag": "8A439opYUyFbYJdDno_Bfw",
    "encrypted_key": "K4m6zdOhTuo7VRZuZOmmypBM_WxLAI16vZklK3EnnrPLTyXK\
      rUqySJOIn6TPhnn_"
  }
```


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

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdSYThBUTFNWWZNUHZm\
cW1oT3NfNWxJZWpPdXFBZHBzIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiUEd0ajNSUEZV\
STZwc3FlRFNQbFNMcG5MTXp4dTc3RmNSSl9kOVBQZ0gtdEVYT2RSVTJNQjBicXhXekYz\
M1FTMnVnSkdYZVZJQ0VqamtNMkZNVGc5aHY5NE9GdU01MWwzUWtxNnYwbzdXT1psM05t\
dEdCN0lYMzJNMHBfUVFaZHBtVUFUU3REYWtLQWV2cGZzV0hRR1dqamx1Sm5JTTlqUUxK\
X3kwbUhUZG5yUnphZDEzSW1Zc2gyWHpmak0xRUtQTFlGUXV2Z1c0QTJLSGs2UXQ1dVdl\
SV9SSFhVUG96QUZCd1JjbFlKNlV3T2g2b1JMVEE5OHN4eU9zZUx5bmZqcHctTGF3WjhF\
elZRY1NoY25naG51dWV1RmpHeUk0MUZfUUJyTkZhVGNBbGhUcTBPbDFLaHNFaGlrZE1m\
dkNreVNXSHQ5YUJiSWw2VjQycjZVa3hPdlRnWS1jRDdHcFJJZ2RqTHhtM0JVZkhsdnVm\
THpyLTU1YjlPNXoyYW9XVDBCMkYwM2ZYdHVadmhjNDVWS1JONFFqZEl3REhnMzI2ZHR1\
bGdFQ0ZMd1ZKZGFWc1JvRUdyTUxaamdGYVdOWkNKTmJyWE16N3FZZ3h2NV9JcFEtUWtZ\
RXVmb3RUZG16YnFpVHl0WlBtSWFZMzFJbmpTV1p5MGxyTXlGWWRHanJ6WVNZSm05SEtk\
bF9nODlLek1jempTaUV3VzFhMm03aVB4NEZ3Wktlc29BeTJRZXR0Q1VXa1JLS2VIWlgz\
QkdhUVgzUjh2NFd0R25pX25uOGgtOEcyMnEwZEpyczRjVlE3MEEtWmdFWUtDQzVWWUpo\
cThXR01meTNIMDVlRmJQeHJxOTlhOU55VXFDbWwxQ0RvdS1UVTljOVYyWjQ4QUgtSW96\
Zlk1NEUxdlQ2cFlvTnBVWFJGUEZENVJmR2tOOGFVak9nMHFxY1NOR25ydjJQZl85MlQ3\
cDZFX0J6Qnpwa2FkNTJ3LVFTTzJvQkZiTWhoWEttRkZ5YVlWYS1DMHB5NmVOdDVhQzBQ\
RmJBVTA5eUg2MmlLYmxNZGRJQVRsY200V29DdkcwbUtURzRkdTJER1o4RjVyNUtSdm1r\
UERvMDJIaTJoZlZ2VjdOZEowWFBNY0N0alhkMnJKdFJIekk3b0o4ZjU2bTA2bllQR2h5\
SHJqdm1Zd0pZTWxVZnVGeFZEWGl1LS1nbTZfNlM5c0Y2WVpsQ1dHMmVoeVVRMzlQUEs4\
djlKNE9OeWx4NEhPOGIxaHJGQ25Bdi1aaFhCbUZ3b1FQckl1X3Rpdko1dkZMU1laNHAx\
TTVrV0JvcXZMS0JBRGR0NGhqNUVmdThDU043OUpKZjdYbzIyczFEczJTQnQwN3cyRUxu\
dWhYd2w2N2JscUZ6Z2Zkd2ZURlc1cUFxbXU3ZlJ3VFpFODA3a0RfWl91Wjd1NUNmS1Nl\
N1pKcGdfQkdiUHYtQW9yMVFzMFJBVmVzVzlOZFJhcjgzNUZDOW5MZmcxcDVnXzhkczJZ\
Z2FxSzN5dDJiYjNieXV4QUo5RGt5Snl6a0NCaHBfZm4wSDhpejRGUVVydFFRM2ZzclF2\
ZG1qbndJeTlsdkpwU0dxMlJKQzVGMTE0bVh5R0Jwa2ItX24zYk9kSzczRTBKdllQSHU2\
S2JjbUlvdEpfTFAyVGwyYjVHWjBUWENxMWhsLXlDcXF4blpBaTV1NjJ5bjVNc3Jmckhu\
dFJpWnZmZkp3UG5lb1Z2S05lMHB0VDhvT0p4U2dwYURzR2dQbjdiOFkyaDdUTHMwd2pL\
NmoxRjRrWVVTVkV2UHpldkU5SnZ6ZUprdnMyM3g1b25fRFEtSlpnbC1RZDJJTUF5MWZQ\
RnhLRDAwLVE3cnVBenprSlUwMUNjOUtkbkFCRmhDS1ExM1FQYnFLZ2tSYkFOZWZBU2JZ\
cFBJaWRGcEQwdDdhRTBFeTJSUFFMM1ZGQWFaRFEtb29xclRxbEZLZkNTdGlDRG5IdUQ5\
MnliMVRzbDlpX1hxemt6STNLYkVNd3BTOTVMWm10aGJFNkhDOTUzUGlNT2p4UjQ0NFEi\
fQ._f1otx5mIKqbhyDDfzk4XHogaC-Gpqra3fJ8bsYN5_D1r0YATx1vQiLkq5aphuwd.\
HRUgU3e5dEtTx7EH.6Vtnu3GlZWv4OCdwA-vc0pjJStf-A8jr6fgTAydJWpCxYyz0WYh\
u0eoiRk5RjTZEiHH0KKE1RtjrnGF6EX9NuONxrZwGbw2Z3RVqc34MtLJQvkdQ_JLkqg8\
QL25RGPNCk7IvZW5obfAlkJlxfy_Cf0h76G-W2cCBmz3vawWPqH9IslL7-osvMjTcED0\
XAQpD96q0DIrjRGzls7kEHrLp311VB7ir8xORrzEtH-Cn4M00WJbcLCYDyKmThEZ61Q8\
pQDTTlHbyOqrp-UU2wIxbIKAwHcPaKna2ehNtOzzkD8uy8iqU9X7fhGlIKIUQIBJZPGQ\
KxqGMUyhx2zGW20K0ocJQ4wYB-mNquVzJt05wWlDn.I8b81u8JDAfDrZLQrLpe1w
```

Figure 6: HPKE-8-KE JWE Compact Serialization

A.3. HPKE-9

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-9",
  "kid": "BeWp7Y5tolX2sSYMKIaG6WUVE-arTKcS2Ok8EgqFqrE",
  "pub": "ZEbKruTLTRJZf-UygOWQwuBNzChq8yuhGTVITLeU7emGD9tF9oFEy1BP9h\
    mBRWo84Zyjr8xlvkadCNyu5iOfuoIC7pA5JCc3A7BNp2ZK8TnNPTsYJ9BTicjChl\
    IMMYKVSnk9WjCj3EqM90RaRiSHYxMUJ0VV8fY_06BqrODCwNO_6BYGaaxHszSAVp\
    armkEiSQOZwyB6xsc0dsU2MGVGANQDBCu3NSs2gZmN1fslWpxzqyN4YtZhwkozcm\
    sGztObngYHXEtgqpo44mKqXHfMBIxjvsqgZ-vNzGyp04OErotG5QOeu5gQZquZ4T\
    lS7JqxjjN0ktJ9Wqofvlq1i0JG97VL7aJ0IHJpnFl8-4cbqwq7-Wan_9U0fJux18\
    PBDBq3jkQiwLiXZOk9Klgin6BGwpx-JPedIOOEEEnKLpQwg3lOZGuHfXGCT5BkGf\
    k4sVVR3dg7uMvC4yFS5ftvggIWfMPI4LV-3DECG-pDe1vEpQFE5EwSBHUhpyjAWu\
    MEHbpTKau5oGmVAIYXRKZfZ3CIFQV3gHoBZdZQoRhEXzKmdkPB2jJI16FnFGUK_G\
    SZYsXK68IUk_lEnihTadnBEhM78-wh9ZtAXQsKgQtUdWR7nFt6yWAkSQIegmJzzk\
    Ew4_FBrNYUIXC930h1dYi1sZw5ZHo3dmY3Viq4pLiiixN9LrdzV6RGIwR8fmpqbq\
    NAc_cVsFePATiHnwBQ5kej1BLMAkUfYhJpX1lV-9tloZLA6JdkRoAeXnEvIxyY1T\
    UYpugYuZUeERwlWygVnOidsIi_Apo1KAUm-TocR6m0zGtG2YQ07mUeI2yqbctcg6\
    EvYVVBLDu_RJeLFyAw-Xd_WXgWNoIzoOM5CXLOtDCcJwMoLJknW1dgNxdFZHG1mQ\
    g9T5wBMbEBpjK8a9oOnfxVblik3eUHYkS7TVhKSqCOuyOBzDQuVtHAt9Q6OCoOgu\
    qUmJeBV4GSd5IPSnpCendqBjEKZ2JTkNwFkuqqbmilEnYMHEOtMUyveWZi6_qm2k\
    PG7aVcjFV9U4pXZEuRIJcugvJUH3qw9UQ7smgqsaJMFzrDVsAGQWItDJxcEOgBdB\
    TAiit99igYmAeEyNoK-GQ46OYsNzq5-CuCiCGJZKNObWhddnROkmY6jFG7K_k_Rg\
    vAj_aW0oPIEzGz0jBtZqVDMTFHF6d4q9erpHOaO8h9e7k2nnrGyHgkJYOPQImVrL\
    Nc93OEJ1qLzUSwJaho8KqwNlOHqDuJgmKoSfEhqXQRfIh68qNqZ6SC9JYJ_-lwpK\
    k_TQUYxJUdRkHB9fgkBwyoGsi0nLpOhMinsIc32CMyHMqvBsc9DlSgmZOBgiovyn\
    Etj_gqdVZ3ZYwDAaSaXTG7wLMyNwBfVycm5TdMQeZs8dwu6pifo_UYzBhj1EY8u3\
    IdS3OVajDKZqkw9zeTacE2kwVsCkDOK_y-wQXEvyFCbAYW3IANbpAuIwpirGJfFT\
    WHIFEm1CqL4FXPt8a9DusGHQCuq3bEkCtpnRiOTGOqgVSZSWkuoxbGnluihrRc5N\
    YY87PCvMSRVxthHPS6-Af2yP_HWMkcfu3DwNyCFxBJgfvtXGLFSm8Zq6EG4zipdI\
    VLeDl-Mg6s_8jDce27ki2xqXVQWA",
  "priv": "tQDSUt-Mgd0LNFiUK9VEluJnrtg057pCq97A54EdbiM"
}
```


Figure 7: HPKE-9 Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTkiLCJraWQiOiJCZVdwN1k1dG9sWDJzU1lN\
    S0lhRzZXVVZFLWFyVEtjUzJPazhFZ3FGcXJFIn0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "FNPUnD-x_KD2ZlRpfS1i5otH3zXS0p5YqAX1IQXDg7KkVDfP\
    rigLJiUX2olBxmMcer7yXyH1L1VMt3AnbWWHAH68JXG4maBWMtpy-ahh6X7k16Jr\
    zCzzQCuRWS2qDMNw_jjb7L_LiR6N9VigfKC63i8D5fL9P3y84jab77h5BFeH_px4\
    XNXdj4IZpoQbrF496F3TMCpj0F7VIOPOH9Vjt6gH4sOAvkeuX5riGG9F0dhN67Gm\
    RHAeCZyW8ywvfzjADZnRG0_SX-bfcmICTJziIVy4KaEMH0YvmIrYmQe9jI-XKCIo\
    eSQpXbvXQtniw6vWhPV5pDldRF89fshN1VIhTT2zsP9of5loHM9DJp7ac8SvhRIP\
    m2GHocU9JtRN0MIkeUEqLMnJlp1dBJl3D3qwcOTvAO0A3ZA876Xu8Gsgcn5VsJj-\
    O1AN2eB08BR3NNGDuuUsgxPVXQWyAFSQ_UlG7IVRp_8__NxfW4cbpCjcE9hvvlQD\
    -xFS0a6rQOKImWKzwKmY8GiU2SUEAwN6rSPHr8JyGfh0YrA0--FgPuab6PPGrZ1q\
    z427SQIxlJBCipWPLlhJzvbWUGCw0g8Tk2DQGnCBMZNc4lBNVhnKedQ57g6erNBh\
    0MOZSXj-SLul57DSBXguw9jMUtsJZoF8PjIc-eSrQrZude3S9illlCRM1dfSaxPk\
    825PQjBFlMnEb9qe-Uc65ALr093ikk5eYF1mUJ31EAJYBVl4gU6RmD7Dp0Iu1X1z\
    wxB7JZYZCqUOmhyB1lf8oA994ChY_VkprCF_A0NcLpee8iW7d077OVODp14M4w7D\
    6hPLJDa4T0GDjMH-o21b2n6YqoxbUuPPGAPCypb7e9zGliZWkpIyBXzvw8pwQ708\
    iFc4AMZswlS8cYiS-6n3VrGosvT5UplUHdpPONfN_UYHOFwIWwErmxABUZbKNHWM\
    0t1opDlysAIXm5lSOf7NFAVA05UQGofBty1N1rnSey6ElXk9lf3gdxKDfkgZVqKl\
    Tiuh54bm9L3Kgu6ZLKqTyxOWYiYW2T2G79tXyLAQDrl6FxRwlGpUWGhqsmN_MSIm\
    cSR3R7Y7uwsQshS6hg7zXJo4IQ3ok7-RvP1-bn9d9goAHPSYASnrWAG8IsIFRK2y\
    JyAEIiUNL_tFQ3TulU3uEgJIECrqKn6jFcLQ_er4AnCEJy3Old1rXxZsMSLhHuuc\
    qhkByUT2iP5jsupSeTaCgRUKUMQwJ9iUeLAp4aAIZAertDuVVZli5fRrFByO6h7w\
    Z6ewNkNen3vwFgDU3V1_xXIZCo_GFghO-oGMysxETIB-IvqRH0qLWNn0z771zago\
    T4Ri2HmQNRcKmA9uBpSpJ2nYIkMJ98CYm5kHvlgZgZp_YEffITAXZ9drxobjxrm4\
    o73l9nhtDdPpY3D1ztv3l3kFX0K2OdpG5whWZ4kuEYmPuugT49EVQXS4Xdpo_aS6\
    RNKwc7ffpbhl-ztL-H54o9-NIoveutL8V957RA",
  "ciphertext": "V4iZyqGIdT83y_Eb6dE2c5l0-LMzKAXVnJwmXt9337d9haaaHlG\
    YFUKvF3zvTZGBJ2PXLQEFWmqZ59lseWeSGA1TklJIWjQbb-1oCdE8607piGyFiGy\
    jlsd5CEzfJuVZXmYQz3J4g6NIHlMGIoKTx6aa_A-qYkszxoKdlvnmwHLhm95vr9k\
    9GNxWIblWK-rJkntpPTWecV7Y1nI2yb3nzJUBDfqDzfKb9YW2x--8KFs8n4RcSZr\
    3d07RCB7QyxQKl9AFd5n5thTO4_UcRChvfc1aawFV4lnTHCGLRAwPo9P0JMNf3v5\
    1mfSstGwvRotRG2t9S3IWG4C_94VOeEVZPlclmt5uYJXPvQ4Fip4RHtwG1mRFRtT\
    TzTblfqELzPe0VA"
}
```


Figure 8: HPKE-9 Flattened JWE JSON Serialization

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTkiLCJraWQiOiJCZVdwN1k1dG9sWDJzU1lNS0lhRzZXVVZFLWFy\
VEtjUzJPazhFZ3FGcXJFIn0.ZMY3Ynj6V0Tflad99MujhmvSUTEYP-PETVMxSGfdKWjz\
1n2dvNmUCMfDS-pAzsh3lny2RyTHLFsUoX_Hl_hG4QYd1nZm4X9bgWpPx8e5Mhbx9T8h\
GRbf8S1q3mkyLyIQNBtPW2KJMAzy6d5MQiJy98V4cL_-GFFUde8gvY1pIqfXSLC_BBmv\
nA2DddcGPvi3eKco8PDY2HVNMQlCusFnnYVcRXiRc3tLJ2sAYIdavSJDqUV8QxiOqR6J\
0g_G0ngqPoP__bwNbF_UDU4_9flpBy8pQS2P9nBJLdYBi5o_zwdUXTKCSgzUEvxrmr1Y\
rGE7oPczjviXzBK-fbMWS7ShXFQ-ILzAccf2yb7hef76AduEi9mnS4D6SEsPTEpFUNIr\
ljED4J2QNuYOMlYCTb6Gen2h63FHZmTVMyXqhnKQUjelpg_qoD0L3ASUxRUC10YR8zid\
pA4MKIRGXwfN1eeqQc_M4hyurMXLBOSjrZqCsKtk0KlgtFx7AmgZHULmYUcKZupfjCjP\
pMOAn3zmO_MF3NrsKtYofQyF3USoVfItSsu-KXDTU_b55EFZfD7ur_4X_Wg_7h0GX_2S\
NzsRCyqNhmucBPej7Sm6spDjPfYXuyFgqrEOVVQU6wMcONJLxTktTxciYcXI6gaCOgXg\
r7zWAQmP2E9UqiAq80yaaM5-WMwUUB1_VlruaqHy7s1cNBq3U0hC3a0C8_QVgxTYYIZa\
-IEsHjx2DoLAOgiDrfQYQPer1YVXg6A-q1lPPO-jcahyfUXvPDsNfYJTRe1HvUXEW_IO\
ZOJhodTyreSPLjvRXhw7MQ4ghScbKusuPOwP3GXB1mcRiG1V1dQumJ5PPD0-b4dO_9yg\
cZf46A1excJrE5HeJ0SY6Ukue9uib4VEXeQi8HbS8hycC38qejW04FIZLukqhSXHST-p\
CoD1ztFd235WCIFQCsqOUOR6ZxHyO_MnlujxuYGoU_J7QBuuXRZMWVLo6rwKrUqOkJVq\
y9UpYFwTOOG1g795uCkprW78W-kTRfiWkVjPReO8skg3u_FpvUXdSIbJ-M40xUq19DsR\
N_RlFaMXX8b3m5NjDcBPJpPrVlN910izuecSJOalsPsrp0NWSXkQI42FFK9Wy0xIC7Fm\
8AZM-_5FnUkGyuqWSNLCkWPjWWdK9NAnIkkHArv7BHvpQSm-FCeTgFCQIvVSlsjXU2-N\
u55w-D0ToW6MPIVQHWtQKgUwJw97eQQ4Ni0Mgl61IeejrCaJBTfxJzsM6X7evU-9IY61\
WJJAFI5BcmUlcpaHm0aLRuLMGLLmrKsvOfEj48AqTHdI13jL4KVME-bRYz87twX7GXpG\
mNLa0X3PGLusZ9gH91xZhKu8rK29oSAJM3T4XRP5qO4_8ETE9qZ6-QAa-b5dmXgkcswH\
wbS09WzBAx1ePVVU_q-a8U-6HFaGswk9bheV0aoYSPXK_J4PKVM-R7YbxTO1NiOviY3E\
0XGJJHMp8M4ONbAYO6laXw..W8wioV5NhSNz-rqzlPSWOPkjX-bVNx_vCiw9rguyL4dg\
G-rOVJqyBOvnukWT9V1v_ZmtXYdi_oAhOmCSaF5_D1DYNWbpajOSX8m-j3nCjRaJdAf5\
N1r4XOw00o2BTdU9b1j6ZeJNB4I_71HFoGTVCY11NJbbgQBzoxWpMDQkn8cCk9QkCOqu\
kakoK7qRB_e2dJnujcGMTIr3s5n0gTZMkEaEAWdP3TNoQf-0YmCQS-4i-6qo0nkcUUYC\
H64vASVh5zrPNgCODOoFd2HF65gGKEJrCEcVefLkYVCM3Zk2PPvOaUSI9eJqbKB9y9ie\
GxFcgnlLcw8bY-4l6fKjg8mI1H2ZNVRXsRmO0ycR6_7zzBfHUNklpp1LiQ9wGiCTh3VO\
GA.
```

Figure 9: HPKE-9 JWE Compact Serialization

A.4. HPKE-9-KE

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-9-KE",
  "kid": "I8THo1KoAq9OG96cJTyk2WF8abZqb3kKKHgdfajHUb8",
  "pub": "8rGsDcYDVYgHXJdoG_y4snlf_zZ2J7IJ_dyGafoU-8PBqdSb4dKAAggLvU\
    LOi_kwqxCdLXqh7sinPlUPEQAXeaITnOkYJhCJN_tpWBBbZclC4sAXNHItUAV4Kf\
    AmEgyll0KiqKRohYQjhwSlSAQhA9NwAPJhYMgZPWkDf1zFJexT_prKclLGRzU-Ak\
    uACumcboErJqGYIRdXVfN7JqfIXfcNI_QCSpcpuAk_wMOWxOIj2WxdCMMfd1QBFK\
    oAi1cM-_cuL1JWwOK5SsC7FKg5YJZdZPJ53RkFUusZPrhcWsZMsOFXJmgOjeV9bU\
    WA1npKEJt7nDeU9EGbICVel-RChriHe1tcx4OFgUCrCBvEpJl9d0am5jqwYQB-Wm\
    wVZ3IFVHM2c5NCb_MHhknJsaCqrSMmEUJ7XBpTWbdUlMNMMiq9Pcd2WwvMyoZmNa\
    c_xKmk5VxkBqorWUZ3ieVwcGYt7cZO2mvJwilCccsz6TTIZnuymJU57-J510EbVf\
    GXSBN3_BCpfwHAAqV-rZab5oWPFeYQikjAHieblCgN7bSKl6U-NCpoaPA-n1Q3jM\
    Y-vzFy4iaM8ThfoXdzXQo0oLCvyOZ4aqlv4EqYQRFh51RN6Jkyk5eqUUaHmaAV_y\
    yj7wBEkZNIDWNOy7ZAunaDl5tXFpUaPmHLQ4RQV1fCA8Y27gQ_4nOY2zdHhnq12W\
    OrvNN-DrdGI0ShpNWzARMtM6yiDXUV2yR_b6KTDyq0YyMzQCHBQhscrXCN2QxXd4\
    hHj-gjZzoJlim6XybGlrG6EaMkvIKfwuhZ7oxRTuC3hGJBSkMptQNg3Th4luol-F\
    l7WepM0vOYOVyYdRANeszJ6WTKZJCtzUhPcSBzeImXaDqNeCAt9jIBXpoJX6m8RV\
    iM4bW8YgtR6vK2ceNW5yWCAfOA9NmiBDAhFaMNTnueistr2eEJhzFZ2wJsT1MG-v\
    G2EIyuUNBqwlNjVvR4vfEAWOmeBuA5v7By3ycsOMFv2hk2eGssIzmE86ZOj5Oj11\
    QWFPRrSMx5zLdDu0ep_pPCYNUicStcDtIvy-pfJ2uEdBoJ5hdE9duIGZOlTeozIW\
    deEcBrv-sEJmKk7hNeOSBpVpAlYDTDTVpvOik-mJAR_hbNnfCY55sFD7C-zxOfrj\
    QdYwWLDSSH5mV4IQKzseJ8x1w5cbWWzbUqF2pNZBDEAjSpiqqVxgOAikaOwzMaWA\
    ERNOeX6NFYkmga2nREl5t46woTvbqBTSxBMOxcS3KCbzmTcqrLVfS9Cci5DaAdUj\
    ad8NzMQBoHywWIAFTA8Bl4p8cb7GqR9FcJYVsM6QlcjcGCZ5KhahgYOlBH5lw6bR\
    Mi48JzHrRWa1otXxmXprcLF4QiBKEZfKpHrSsszlCAKOKytlG7_xtNPRZ_UeZmeT\
    RiyHWVDCcQSzM2W9U_7hfGa-BErmW20CNBitqWZmEkmGRci2KxP7cJceuTXjpYAc\
    VWm1x4ZVN1_JtCisCU5egDoXIi8uFHwZigKhcBUBIS-AepvSKNdCA3HqeWzydKaR\
    zM6Hd1iEyiOQZdz4pcGDrkcsbOgiUpCHGM_OPeIAPlZ8DqRjh6Wxa8O8YwyrfJZs\
    6vLUcAjW-Jn5AaNpQFWU_VdbhTDQ",
  "priv": "q_aDEMZpRAjbiqHwO23vKcgImYieSqUsCK7wWZEsq8Y"
}
```


Figure 10: HPKE-9-KE Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiJJOFRIbzFLb0FxOU9H\
    OTZjSlR5azJXRjhhYlpxYjNrS0tIZ2RmYWpIVWI4IiwiZW5jIjoiQTI1NkdDTSIs\
    ImVrIjoiVHd6VWlPTlprbjNvSEl3RU1BX3FXbUtRU1UzNndNOEl6NUItMzFzdEp1\
    dV9BV3lfTDFSU0xxQkZtQmNlOEotY25hUVhSczk0eVRIT1d2Z1hDMlVuektZdUQy\
    ay0wOERaU2xUb05nZldPaWl6UEV3a2FRQ2dEcFZlZkh2NklTWkctbzRoS3ZrZ2Zm\
    VkxiQTNjdUhNOW14d1VKdTJGUWdLVjU2TUhQZzJIbDBLQm9ydXlQMGU4SUg3SW45\
    RDV5V2R1WjR6SDJjM1lac3hnSXZMSzY1SU9nSVNvbDFEOHZ2M1k2YnptS0tUQlI1\
    MHZrZ3oyZ3JESVNTMjE5Yl9qM01FRWFXeWdZNFNxQ2x1S2lzN2lkWll1SzM0d0Fi\
```

```
      Ym1MT0tUWGhVNmxGajV1Nml3eTJLX1MweFJVS29kZmlzU24zOC1hRlREcEtSVEN4\
      Wk55WFNSYWNHOXBMNnE2Q3h6UGZ4U2hHSXpjT2JTYm9oREdTdklnRHAybW1POFV1\
      RGNfU18tR1lDN2tyaEpZNk9YRDBsNzR1OE5KQ2lOVGU3LXhPWlNnZVoyNVBiWm9F\
      ZXc5b0VINVhFZy0tV3MyZE5uTEpvdEFQaXN2NkNDZVVXQjFESENVUXpqSnNZTThf\
      aFpKZ0R3RmZydzExOEZwaWJVOFlDd1lNUEF4THpzcTJjLTN0MG00ZnJEcFN0RWNn\
      VHRSM2FnaFlyYW5zTHJmcmxKUkIzTmZpcmpnMFRYdjBEV1ZzM18wRUdqNDNDOWdG\
      MWRiSXFyTmVpYlBVTGRCRVdZNjR2Uk1IOWJBSGlzTDE0NlQ1RlBuWTRiTzFhTldC\
      NU9tZXJ6OXBGb2Fhcm9McDl0a1k1Z0NqREhvdmNORUFqNnBNVHhFa2tJMDhSRHlJ\
      SkdqRHc2Yi1ObGZsQldpSEZTQjdtZzJ0RUVuZGhjNmFRcmJkU2dUQ3liSnVfV0xB\
      UDlQcEVoeDlqUG9vWm5tVGdXVWtVNHdtUXd0WHk4RzhVc3pMbXduWHpwck5mZF9J\
      RVg5b1ZQQml5VDFZejFoQnJhMnVpWFZQWXM4ZGdlUWdKYnJIaWVzVnRzNlpuMGxI\
      OVl3c2J3QjZTNGlkd2J0UWZEVTliVU4tUzNrRWZnWkJZVEFBS1Z0eS1Eam1tMEZr\
      TTktTW9zUVNyNjVOM1NueEtoYVVNbHU0U3VPUG53bVMzVXRaMDZFQXZXSWQtNEoz\
      RkY0Z3B0RXR4czMxY3JEOF90eG9ydGpnR2FUV0o5dmdrZTMxeC1VUmlGb2hobUlM\
      SmtHYjJ2UC04dmYxOHhOWGZmR20xeHZDR2dESXJya0V4YXJRSlBDLVdRbzdhaVcx\
      NkRpc1JfZHQzRGVGeEdZTUt6S0ZGLUJmYWJ6bGFNRE5aMjhTeTdzUkRPbllpQklk\
      ODNRS2FGSXNKZjMxOEZvV0JqSVRqUmtjbnRPNXBsM0FpRUNFTVhfUU9tRXVOamdL\
      aXNlNmZIYW1XYkZoOUhRdEZUZFJmRE5QMWxxUTFpSnpTSmhIMlVkMC1VMGFoZ2dr\
      MFdOLTZpWnhDSy1oOHQ5WlY2UFMtV0oxU3ZDeTkzaHBqWEV6LVA0RTV5VHhlSFd6\
      ZVB5eUxWQzhqazFxOGZhc3FqRC1HZC1tMW9peDdIOHpOX19GblB0UTNrNFdWeEs2\
      N1hsX0NpRTJnZjRsZ2FFclZCMDI0czI0SUtZRjVwNEZZdTluaGEwVDJuMkVTMU11\
      RmR4Zk9pajdMN3dORGxLSjdXWTBUNnUzdGtMdnBKWTBxNS12NldQYk55dVBlbHdr\
      cGxlZlJocFkxNk5UY2RacGozSlVSU0VWN3pjNzlLTTNkNmR6QzNEb3FZMWNlUlhS\
      VUluRDZmY1lDVHRXUVRqd1dXRjVib25uVWIzcktzeTRxcDBqRHZuR2NPRG9NVVhk\
      cm81Uzd4WWJ6di1aSTIyTzBWS1NDbGE1N3VzV0VqQzNxM2JvUHNobm90emE1X042\
      clFuOVQxOWJSWVF3In0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "iv": "d8CFuwBEVbiI_nK7",
  "ciphertext": "kmsiEt2hnihtuOyfGiFAs26cHoVya0vXhz62N6vmF4NnZP879ES\
    3YkengaFdFYG3l16-N7GVar6OR0h-atBeDoMeGNv7QHLE9Pky5arS4kaL4y7j9Bc\
    ffzA1Lq-Hx0cQzgvWu7c9xkOXDb6zS0liTxV6-ZMFHHdHdAd5ErMvQNtUwh8rvG1\
    APw6QMrzb3SGUsmlTWE4-IMgq4KRKKNHHsdztLynzDcskM0yyASkO0giKYcp85uz\
    Z3WYwnm5LOOen06Fi1Kj-U9Hd0JmIVsy58mNnCZSeEfLdIGyP3HvLqj4ngp_OvNu\
    BKEp12OBbouXpJ4xuPla9FdgLoF3Foiw2GRhoqtYWSYuu4oRgmlXYOuSB",
  "tag": "l7BtLt_8bQpsUK0NS-G5Gg",
  "encrypted_key": "hEaoX4fNiWQ-xb_y31sERZsttys1fGKexhdYll0PkJDtNclb\
    -M9rmeB7xQypVLaM"
}
```


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

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiJJOFRIbzFLb0FxOU9HOTZjSlR5azJXRjhh\
YlpxYjNrS0tIZ2RmYWpIVWI4IiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiQkxWb1lHUWRO\
enpXUV9zTjVfeVZWOGpWajVqb0ZVSWdRVDBwV3h0ZlRwLWgxUk91azZZYVN1OXlaR3gt\
aTg4TW1sY0EwTlVMUHZEVEZCX3otZUJ5dHlubnVfZnB0d0ptaW5JVlcydWdxQ1hVOTBU\
QXJ5Z3RWLVJkY1ZJNnhkRGFLRTJjTmx5WVRIVHF4Z1VHb0ZSNVEyMEVJM0dSazVSdGh5\
REx5cTZRdUdVMHk4RlM4NFB6OHVCY0VPTnRtZWJ4cW4wUHIyWmFJNld0VW1IdzY2SXJW\
LW9ZXzRBWk5tazZmOUxld19iVWtFU25oRHBzbWVYbUpvcy1DbmlQZ1I4SDZYZWlfRHFT\
cFpqX1BGRTBmVVBDNW91QW1zZ2hRQ2pNNm4tUnhtbDVJd2xaakgweW9qby0zYkQ0SkxE\
azZUV3Z3UUF2Qkp0Z2dUMFh0dTZJcTVTaDY0TGprZHZTeXZscHZHckctbzNCNXdHYWh3\
X0JpVDg1aHVWOFRadkU1N3FSdy1FOEJqbWpoNHY1eDZVNG1KdnNpQW1KS3NCNUxRdno0\
QkRkU0o1d3Jqcm9EWlNYV0stVGI5UjJ6MERKTjZDTThvX3dMRnQwcGMzajZCWjZKOVFI\
cE5UM0ZUV2NEVFQ5b0lKSHBUQjgyUXpraDN0LVowSW01ckc5OUR0OGZVY1hXWHVkOWFT\
V3JUekw2S0RVakU2bENmTnVTRHJNd3JNSE9Nakp2QU5sS0phYzRkbUgtMXR4RTdOZUpB\
WkFnNE1ldVlQQ1NFeVNKMUpvcHZtRF9HOGdINUlKc0RIU0ZYVWUybGhCUkF1djNlQmts\
Y25sSUpRQ3VKc1BGSmVRVkNYU0xMWFBjcDlRakVXemFGSmc0VDlzak5BLXZNZ0dQZVpY\
cUpuQzRMcnhPZkVaSHpSTXJoaGw1WFdWeFJ6a2dZLU1aOVhyclV5dHVnRGptay1UUVZz\
NjdyWjBTY3lNUXpaVWpmWU04Q3ZJWHUxUW9zc1ozNlNHN3ZlYTh2Tkt1Rmw4WFhPd1RF\
cW10Qlh3Y3puYnZLcHBqaWU3NE9RUndJSW4yUVBIRWlEbzU1azJpOWh3aHY1UzYxcHhQ\
Mk9Ga0NpTG9TUFU5N1NLckZZNDRPNEtSbXdkalp2WkJ6VllkUXBWWjdNY05nTGZoOHZp\
R2l5SzhObnJBQVItU1RXdTc3UGJNa3JMclZzTHE1bVJqT0o1S2NwbjV1aFdCR09Edkwy\
WkZ5akdFa09ERVpWcUVFLUpwYkc4d2d4Y0JBcTg3TUZfTVQtN1dqZ3RwRWR6NGxZU05Q\
bTFaQklZUlVOaGdYaTRrUmNhVkhyb2lvdmFTZVl1OUNDNnZNeXhJWTk2Yk5pMHRxTVdm\
QkR5dEJfWXI0TXpORHN4TmJmMzgtYVpBUnRodkZtT3F3Z2xGZVNjSTZpMkI1OEJua011\
WUJjbXhzaWFXeHc3N3R3Q2M5Vk5CeHlRRk43aUFUcjkzbmFHNmNUTWlsQXp0aGpqZ3hh\
VkQ3Z3BUb0Y5WFFMck5EdVdTWnNuOFZDV2J0dHU1dkhxb1ZaMkhTNDllVTEyLS1vS0xW\
WjY5eTRwOHo2cjU4S1BUSmo5dlpodXoyMWNubzFteW41azN5N210NDRTb2MydHRlZjdw\
QXBRLWZLMkxibGNBMlFNMTZXMllKdWhXTkdOMEprbURKb3VpQXEzS2xQNGZyVS1mNU8z\
dk5fLTdCS2ZYVGlpTGt6MzZMb19Jcllvd0FpdHBpSHJKSl9NcVFzX0xrRzJHZ1RFTWpN\
eEc4RG5MSlZPYXFzdGttZWpFUWN3cTNOek11S2FkSmJqVlVLNlRncl83S1BTMmRXeFRE\
ZDFlelVPb0hxZVlrY2lRNEQ5N0RrZWZBRTNVQTM0QVUzNVZNSEtpak9NM1ZaeURHd1gt\
UzA4VlVhbTJmMThrclQxNTMzQWVSZlkyXzVnWVktYVNhTVM2dGZXRkU4MGRNVUNybXdf\
eTlTOE1nIn0.m33rDckJMAweQB0e1C7cc17C52_oNyzEtnoz5VZ1cLxEAMdx5YD-AP7w\
Leg6b4aQ.l3pLYmere0K8G8AF.k6oT3m_ISW8okLHfAjFYBlTtMpB2rO7mRgkjHRSz-u\
GHo1naLCfzcQlgDKm4n5XmvUnxJ09Z5Xq877G2omHaAnJXWjA5r1zv7_rB7RgrkkU4EM\
PPfRYlRqlfReYGEv5rH2V0SUHMmVABgH1NbmMtWm2ccwyKtbZEgxMru79aDKbZ8MV_Zk\
t3hGJWVcQRYljGL-MM2gqWpKn8Q73FT5CX4HsiLI0zn_b5j4qDXqsZGz_A66wndg5vcS\
Ryt6F08bfvQ5hptrfdftUeMKn1z7PxI2T3Ye7AI34EIQdIJalrmGMUdzNU9xvLdwWD3N\
6Cy0HFEoWvFNpXVxxcDV2ybCRGsNzP-RlNhOeD56l-6Pf_mG7v.77mxN7ZlNwLuUio3m\
cxoxA
```

Figure 12: HPKE-9-KE JWE Compact Serialization

A.5. HPKE-10

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-10",
  "kid": "EkIcXLM8dkXQX6mzrxYWNBY8lndA5H3H-v8TfiSDLfI",
  "pub": "1KUYqsq90ghiwoFuSJjL1qKhZhRQujGf6cXJtSRSJoShpMyQGMdsu-eTJT\
    E6FnZeUQNtWyNfsRAjzQqYgCvKB9MWZddwzkYlCqRSXlcSHmgQCLkj9_TIJZipHI\
    XL1km4_2nGOIQ80PCbxscLN-iyKKt9ikJt1Ks95aa_PSwRnum14MVuHIyZu5wAQx\
    PNTjw9S3EnI0ODyDaPaVG5zHqIB-mW83I6WfJUFQRErfRHjTwWhztsYLNkldjHMZ\
    YKxAiwouemzdymoIoBxaebXIyLnHsAycKP3NByWaxMXrEpdJMGQveDwbW1sXOffA\
    ulTzw7boeHBdQcGINzg7xiIXcgYeq95KmqbNqKMkZNFiA5wFpOjoy1kUE9snCwVs\
    V-I_dUrWckargyJNUONoRMOCox4cuziEUU3WkBK9pOBKV1WjrL0kBqBZUy2DhsmJ\
    LG6QjJLng4M6S4AxAmCwp_2zNjFGaMbLZCoKqPt-FGe_uXyAVqoYeZ2jAfWgQubr\
    RAl3NVd4RzAnQh4hp4gPU_t9mwS7sD1kd3-zm0sCiqRedvNGag59JDFAIxuUaw-X\
    rMyVx6dZG5xfOnaUE8ivuZ64iPQ9asASugUFVJtuQgD7pONlw0cUQq2-qVV-QTS3\
    SG_Agdn-SDhqe8ixVrqQI0TYmFVAquRniDgEx68NM4jmyPvwuEQeN10piAj9w7jO\
    dF98dutkd6UsQGpPcgXcsCRXrN9uSLpVQCJUUzFoG3SBcuUEhh7DOr6mAcG0Zae0\
    c9E5e2qTZ6bUU3E2KZZXub-xcZj7oGSspwgrG2ITd-xzi6aexu7guYMMaP4ek3PE\
    hjUFwV5HgtzNSgp9SOQEAPlYJs8mCpE5tNsYquJ0Q3CXYa6uqe5SKYY8MOpmkpua\
    jOmIQEbvUjmJQxjSQxPXcDP0a0ucdbG0k0kshqrPAUWvSoLSjAVxAdgyxe5pdXIC\
    krSjs0LuG7fac0gctlw9RIurq36EF4EitsM0WhAeubkmEd7ghIB_FImfQKx7JaJs\
    cx0taYAehRD3lN3dA8m-NNd2JkX2DBXmQyKqh1JslcaCHNYaco5rlRqvpwR0t94_\
    nNbklO5oAy25ZcJ2iaAiwAkPSWptfMRAM1P_TMoTFTv6R-qKAexgqtKYBK5_aJKp\
    GjCri4GSkwv1RPeXC3mrOJNAJ_8_jNl1yVjVVVh9lDSTQGOrtYWlmHA9jGATRK3e\
    so_DO5ONWRytaY_awbxLJ3ZeSttLZEl3Jj79kd1LigAXFmLiS5fNxiqElcjugb3W\
    x2dNPEhVlc2dI06Nm4nnfIEUZDwzkfDcU1-dJV0PcUCbAbPyoraEqVSGJwMVFkt5\
    a9QqqUXKY03hJsTaqEukgM0rYoPlEJ_UuqRptoGFZBWdSct2pEI7muOZA0licZpu\
    Yqx4jGCAkjS_xuaFKjieExA1IGySoEX5ETuREZTtNdp9hDKyJQ76wVcoVqlniEHe\
    UTSdxgTIEGM3NLacqxHFVAmgURfAojo2UCx4sXXdK47RtBuQiBf5Z-0hx2DDqvgk\
    TOKzy5trEJ9MhvKctYsYRWQsWz5ly0WTAgUeLPWYWkLXxi5BYAF2KqF2yCatyQ_F\
    QZO7mwCZUB5ZutKQcxAOAcm3JGQRsDL3cG2MBlH4UkOihSUNsbsrJ3p9i6HEFc8I\
    VmiViuBtEZbdFZ4wKD1Jqah3ghkjtHbhwLdME4ZQKs5jJZvjGFBsGZG0KCYGKbf9\
    QQ8Ooc-PNjyOqzo2k2y-ETtMCos6KdcnGbyrEBVKk2rKLJuaDF_CQ9q0YQdsQ70V\
    aBjeckNGLL22OvhiVN7jbL1kJ8bubIYeymm1KyLRcT0xmpDDgYtvAsygUdQykKbt\
    SmOxhHZrcIFeKazWWe6qcSZCOML0hszyw16MGUiLtVfEAvp8gzrGWQFCA6aDhrnS\
    s8YDMAz5Yoflp2wai8H7gC27ltycEpVsWz9oBhQPcmq9C6h_kX7RqfrtusXPBai1\
    pGXBIz_tu9V6ETzgszMUFOFdoKxscc5JcNWgWRaayYDBy08VenbQggLsOd_BsJ8k\
    VV2fwnIp4dGUmthqqjVkrGtl1OKCYX5_wb8D6mCByPQ_BsXIMEJqvQYJp8bSZ0Bp\
    3NUvY7EBwNvM1gfMiOw_pwcXoglaZNgzWLi_VBzXIY9lcM4qjigOlj9JyfbYRGPk\
    TJ5Gj4Taj57OC-wIVoeofByZ5tLATYBKFPwjA6SlRhI8j4EiKN",
  "priv": "Ru9DwxiJ7BdWBh82FsXaAPPR4s5MZoadKL9y2wGmino"
}
```


Figure 13: HPKE-10 Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiRWtJY1hMTThka1hRWDZt\
    enJ4WVdOQlk4bG5kQTVIM0gtdjhUZmlTRExmSSJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "PqSkdKSW75FL3sRXdax8xJP8rcRgzVg3pvPe5diLa2U7Zq5r\
    klP-pVqcS_4YmoS132XKT-AFp3Ft2qcWu10h2vvFSoCLH1-6IKIIE8xYHe8zFg09\
    mgOcLhevHKPnQ2d6KscghZLUJjeN3KmFRS8Px2QmnttXHl_aCkcWC8ztu70fHA0f\
    R9miNtjeP92J69aXXBjzqYvPn7ZIapiYUXTQaLvMQNiMOwMv7g5DYY7mFTBh9nWy\
    Pmxv-WrOKGsd9-Bo_farLI64EIgkAogMKA7Xda6v1gCu6ne6nQoP3Q9YLENSDkfg\
    Bbj0FBbAehOLOEGkkhCB9qX0FvicV98CBXwI_42bYar3v-My_g5-elG5v6OqdMB4\
    foD8cwo1QG4YB7jHwqrRBHp8Je5lWIHhIUjmwrKNM7_kwp9phQ4Ix7SUX8nEIhXA\
    wwaNmlEzcxm5VdGlts1SPtqtOfRmmRSpwJVArA50tURKaMsrpx8rLJKkJEpyUWm_\
    4O_1U-7fQXCfURH0LVPPePi7wg-AYizp5zAGJPTZSBqM89imBiC-a0jeyPJBgm-Z\
    DD-kD2_Q5JnTUMWTm3v0oPp0gYW3eO-rCjLebcHq9XQInKq_wgm3ccCkjuWvsHUy\
    Wsw6gQDEqljNSCyWIHS4RJospOwuJ1ruw1sY0mVzvpK9q7AMFJ7_8WRAgKe6pokS\
    Q-3J-stoVjNaT8T9cW8zbm1_2y5epgDzPlI1UFVXWG3U6VB7fQAiL5w7HUgTB-2G\
    QMxRURz951l0jLvi7SkZGFag8F3BBrH_H_x9kt9aVj6QFuQHK-gCK5OAbgeGNLlE\
    uG4aVGz6EHvc58gXr7AsXr_aSscewPPSNy06kQnh8Q1xJIuxvybQANSKUk79ueUz\
    oOPBL0Inkyoym-nAI25gpM1cDFUzbmOjrWOaSLHz8CojJckAzuh25IROCzHhMNSa\
    -y6_mFt2htSFUQAMrZ6Rx3kq4KK2MlK61VLVYKUHmvMA8SuiYCgQVdKzoG2sYvPj\
    QLFE4eNKaPXA6wmrOheu_-0pLB4ysflgpCkEH3hW7xuNbMGgkkg95ljQ5xJCSl3Y\
    tGyCKYAyU4wgLX5t8ojnke8eCyaS0Pz70dr5j5viS3s0CzNh37gAEq-ez9_TeW43\
    aUBHp4raYtb-oedm7lGl0FuhgCU0DkzC9pH30gL7SRXM17eLGO9PBG2hwMjtb2oK\
    YScDiObG_16sFSOI2_jhWjv7qfz7IFX3Jr91MfIB8foQPBgfy0TFPGjoOb41uquC\
    5f2qJYIDkne66XA0cvxrSfQ3070a4DeNrT0l7q6BIR-CbX186OxuCB5r790vyQAT\
    5WyXf9OXkC9woysfEf0WkHvEme9-LQTeZJp_ZRXaJSbOJZslF80NaTY4t4IPfHDD\
    chntXHyvttJMJSlaJMKjXYOyQOr2JqIDJ-95aoDQdg7Up8jR4MpAL9pbmbh_7AmN\
    VGjN9S0u2aszJfUDNqg1LL1CD9WqDg6DqHUWkVv0XZ20tf1fcOkDuc9EHPjyyjNZ\
    7kTsrRHqp49vsRayY6jkKJPndLtZQTGiiKsdZEavlGo5XiBeNrr0OWY-YheDQMHx\
    K2aQH0GxQbigqriclmQiaaKn3LTv7MtkdSo-8QaZBgO6tF60i0gKtrPNkHcyYQic\
    vZj_RIZGh0-VfA_GutRs9ozqSzajcbmjoZl50rsLK5MUOXHGztEi2hd-z9rF62Yp\
    YLlpnF7dSlsc11LlSuxEjiorshM5F3EqolNsnjHCEA2XywYfgYE7cDHD07cvjCC_\
    Fj7mlWSFhE4pyX-jOEtSAD9c-iEUSVXcScjeApwg9_c7hYC3njVQtvkI7qh7bA8w\
    _fgMiwrqq25EJEw3pw1z59uoEhB5txVzzyfZiv9xvm3S1sYMC_UL55nCad2KwjaE\
    avl2NGua6WBbHlIUQ2EhwmwzCUWvvbk53c6WoJtsEWP2h6CNN5y1mi9_7HSrIU6K\
    VQXC32jUsQ542Xv_eVzGz6uaxRsBK-QE7CovOhUpFHR9lf4gmJaox5GwhImq6bes\
    AmBy6g-3PwpwxpYAXP3qRefX9jngLfJXc25eQvpwmNjKQMnoHrs9C1pZGFsE1r99\
    wKUcahH7bIvQDk4GKFcL4eoUqlij1RlP16c2G1LImEWOBXWoqubqVqfU6OvH8Njq\
    YKc7deIHGfrpu9fQCy0l9En-bLXwCAFklKXjeVmmvEilbaucHuvznrgZYexz",
  "ciphertext": "9kfFny-tTRwymjXj75P84eWObnYaSy3BpPcM4Duh-TMYi2ZjKUD\
    ogtdcCwN92Whe-O8RCBcEy31EMcair8LuViyVmB1MTe2EmjZAf-jAxy4VY5nKU41\
    dP3KB3TRNeN-6Yb8XmGa2jW7pFHab8lTz4_LiepU19MVN-J4L4aKrd0fHt87VQLH\
    H6swyz-NdheA9cvVQWcV-cOaoh0gfED9mekWhF3iLKVfTeJjs7R_ZbcmKnfx-rwc\
    Pcp0bfQlOwqpjygmjyC27i_WKX6VAzwf0onjH1mgWUU8VuND53DzSgjnMvc8QNhD\
    3VoJyAM55LF-sb83nH_ShtyiQCVl5r66uZCXkbMMVgySw1EBsfmLJUZzuiZtr9U8\
    ipA94iU9xM9zIPw"
}
```

```
}
```

Figure 14: HPKE-10 Flattened JWE JSON Serialization

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiRWtJY1hMTThka1hRWDZtenJ4WVdOQlk4bG5k\
QTVIM0gtdjhUZmlTRExmSSJ9.TgRvKwbOBAKJZtbM4JyaUwIJsGbiSlIK6uOFlP3FBnm\
xJJ935SRazR62b4t7lxQiZwJZYrpPM6ebcgZ8n0lchZ07bKdCrEJwJMuogXnK96hBl92\
IriI0PzlPB5Hzz12dNmSFqX8nhOWTZ5aurXMaGoU56MUDxzRMM9G_k6ryqYGsoGbJ-KI\
5e2rG9UImwehwG8ObmgUy60-Z5Hv9DJNbs14SWtDybh5eUey3yNpSAjj0JuTd2Hh4EmW\
wsGYby9vpTz3BJ3rvAmBhnZgfUibotSzdweb5DWFPcw7jQNNd2sg1HBLQq-A1R5ReZA6\
hfimNE96y5g35_4ZiADPHqoRJ7VM_stA4IOEirNixdJ46dhyaQ31s693cQ1TF_tUbrPa\
U-WNv9PRAWnXeXF5-T73scRKCOTR2qFz8lrrmm2Q4xyxy58xKfJcFJbo_gxgFLm9TJa9\
vWsRN6lyzCHwL35bVjKCgMyBEiKAGAin3_GkIy_hBlKoAVBOfcTKEdR8nodzO6JYOfT5\
GbP_C67IsR_r8H4jDv4QTP7rgbh0BVgpnSBnORR8ns1l5oQA9erEcAWSs47SYEc6NPDI\
WU714SpH40LuJxTYNqOqXpk6-Mz_apPGtN5GDObTzAbLnwXRatv53gPtFORWWT5mXu6z\
Mut_QgB5GElvQwWyaWG_MciQ6mDpLlnA3Uq-3Y5d-pkDvzmx1fD0-1VUk0W0qRyGojH8\
fPgXXBzljzP45J_g-ZVZkvB4LDQIP-uiww0O1TpoZQQMfJcKg2rfKzpiT_AxZ8eP8H09\
Vh7CvdTGKKpeizHWxIW-DhJFHLzjfgfT5Sf-BFb0P7SrIrJBqnlMNawy-41y-c0JIp3x\
p-ag_c3zrsZbN3pp2dfsWEjlF7rMbBBHBJ7vZR9Uz2c4Nt-Mv62itoNBOW1foIZhut1i\
e-p-41ZI3F2WSNzZePj_gZnA_4xAQpAx4PPYut_QQ_cO27BY1X0UQ6TUSUysQcCPw4D4\
-uza3roA0smzm8Gmw2Ejy5NQd8K4GPY3pXIs6qp_yVZpIBz7gM0YJx4rtTu_lrMBjDWg\
ukq96PJA-dbuP3uzTktl2kf2qEHaXaEvUqYX3Vaigh4yVwpFeBQEbXJc7RZ14pqkQuJX\
RI89PpJsxsr-yOVucir9Tuubv91UJuRPFFI5GWP7qv5ZONTt9SeWvq6AyeS521VQVCxv\
QReRHGt7vj_UU7a9BEEhcQBL-nxD9uHq1u5p7ksGLV4uiMeSzn0SgthUTFSosqpWi1J-\
vTrMrESINuwq89vZAHTID6VJ_Vgk0Ahx-3mrGOscjm_8slQJtlibPTrpAw3K7eEevFUE\
Ror2ItJmprKDJQBVDIDhXCbTnACf7UsGr-va7Km3miy_iekhebmB3es8LSG48JG5nsyP\
dOOKfMRhVybgEqyRunfzmW2nC4-drZS3_m3uUKIVAZVbiDYQjtM_vRFa8reO7H6_lOQM\
ZS5ikE63KzPS9QwjcmsBuksXr1RhlMXO8tHGRZILAEVvxqo86pLWVZWPcrzsVmm5tMMG\
ezykUKjRwh7En9Wy4L6DeYnlrN36DGNgsEHGdi1yry__pH3NkT_lRkyeaneNvKdDb5mt\
yig049XYxhxmPMKwu5hHB5PGKGAhSGeyyoAjSik8djxq1kkDKIlnXNMsMGGfHsZPcaqA\
GwbuD5mg1IsEE-r3jRKTOlmjwUkTOQcdwlq4X2NibI4Ul_1tI7ycZJlY6C7Cw6qOQTRd\
DfYOd1fEd1LsHRp_D3uThgBmB9OjDlImwER6S4_sQR7cF94twgO2OpPRlk_5SIXDCoFQ\
25HPHZHm7PFcKFTf0wt186arqwiTrq0Tcm9IGunkYcNm6uTYzUqm-U94__IDUoN5FQcH\
yr_m4zpZRWSC1z17B3gSIC3kBqanfFjzM4zPN7IM2HZpcom7Ib4wIc82yiHuD4rof5M1\
DvUHNf2QJm3ec6Ma7b1aVcxmwJW_EHk9DvjZmLy2RRC2xt6UA_uM3H1DdBpg1kHyv2oZ\
nV0UiMvQdbisu4DO_qBgR-IWYxXlcQ5LQFlDA6WjzJjcjKD7Ngod-W1so5J_64i8KbGp\
oR_P4MfIEGjRe8Y1KihkjLppWehZwoyD2UVzv2wi-sUTDcaRCM2tJn28asl8EyRW34Fv\
CZNrRtTabcZbH2xrz0EWxT9RQ8drbiFJqOHus7qMDitXKqXY8MuICyR5lu46zPw0UjvL\
e..XNUZgrnJGf8pQMiH49mqGqzfA5MjcMUzpWBpFpLm7tF0qULkHgj6IkG8MLwnwSuRX\
XIxo0wvJdEozwKeVsXwokRa_V2kmUdKFeg3ger-9qw4fsz8AeASDxWDOsEzLX2MiJq6W\
XpVdJwQum76o8vLSE624ATEAz3aS-VXauyx1Fsn1wKhw5Yz9nIp9EHtpR6gE3-osNLIa\
i6fPzyoT9V05CDFaIuOvLXWRrggM3vYWicbdInOMCnCdTCj04WVt2yzwnm-ZJw3NkMeq\
9uV8XCyXrbPyGWgLdAgUW7v9TcFQWUAEh6dGs2JbgUJgC0qFopRJBtwwJJ2fGOnwyZ84\
gpQK-zBqnKp_kn-6jyjl9fPRfh2jPoK61Sy7gTDXV5Ceq55Nw.
```

Figure 15: HPKE-10 JWE Compact Serialization

A.6. HPKE-10-KE

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-10-KE",
  "kid": "UVzPOxx3jthVCg56hBO353HIP_hObFaFrI-pf3maRr4",
  "pub": "9ALOt9bAhXcL6nyuwPy-cqzMgPbADhIWe-g3IFA6fFUeidZ_SDun5zbISB\
    E1i5YKT9STKCBYVlCUZlAo8lnMtbc73bNy3DNkQvii6TptYNmPTXmwauN5qsUFM5\
    ouqjFtwBhQTFkVR1i5YuOynqhC4fp5Z3lcEesDFRQxhwGJlNgxiNGWkNKkeWBVEL\
    xU4yUPHUt366Z5_8eFxGxpRALKxrfNamuU5zeokAxmLAsVKZkwfIISxQV6EgQ0JC\
    gApfRXp1gaHWk_5hBrD6WKlwagDFWO9npfrhFtHHNCm5U_FdTNheampphf0LJpdO\
    LL2BGZWtqYn7xDuegxEJCBiWoBoEl4wpMcz4kqIDchWzTAvaCLtXvB0FOYlKqGY_\
    MosDMIfYRpfkxlTdKDxMxWC_YZdTQCW9aGZqu-gqw5RCmwkzUUxKrMW8lVWbRXHs\
    Ga1WQmMTJlTLGGRnBP54YwisvJp3tRvzy3y-JXDadAxeK5u9UJIMZLvgmAs9cC3x\
    t79YahZbo8FzIRCQIpUJsh7uC7VaG7f4KzgDZSEIaIqMRKY7uTUvasmiZbtoBMU_\
    GPrwZ0XmFNi3R5bua0ieBu0RWducQaqrlQAPYVfRkuFHkPsMmcFToVmQtq4YlhE3\
    hsSpdVIVs-PEGeKcciBDtJEIkJzxt2tsDPfagb7DlQQmqMsTg5d9K-2FYFUny6n3\
    sXL3wdffoM2kG_XLwmpPERyxOi2uq_rYYazOHBWPxCdPg-bBkWy4uLOqp81vSHx0\
    R-JpavAMEfs0dzLAFYo7a8BEpUcmNo4cciVsoOV7lUkqNskhXCtSeoSKw8zDxCo0\
    ye1cMGNuogZnKNCPhGUSo9igeAcGqkHofMS3B4SJcnHYMMD0QJ7eDE_Hh0cMsT54\
    aueuuJ8PauLHuT4mokG1s2exZP3uaXG1BmPMtpARyCJTNax2Qd1OVqqxukummV33\
    Ja8pdC2zULU_XATzZjBdiQZ6e3R3vLQgtH5vpvnzBHvbRHAbKJdQS_szVihbeUxg\
    EdGSwtcgHNQMMamedO3qmHYsRqc9lPo-W34_CUhyDHq6K8n0kgcxFBI-RmM_iE8R\
    IyfrulMyNPXdnJ1dJociljcSUyjpZIRgE5BCeS7sGp1ZJ6c8w7JhiSDEWTl2OUb9\
    GsbXNLo6PMrIBWkgl_A5EpMipqwgLQPHTCTmIJF0usHcYnMtECT7U1dPQVKgSvNu\
    saXldU5miARrvOn0osBnk_uzPBayCi8DU7chRXMnoMSQlhOmeNIwS6d9RM64HI0o\
    AcwAAFkYyV-pMvqRuz4Ax-EWlHubrGDvbMWTwMNpZOhzNhwDIslaggOoqHqZMego\
    zO4qkjcueLDPBBZTamjdeShbkQfvcSRix_fdphv6sdnXyN7Umr9kxA_3dLS4m0AF\
    uPBACn_Sohc-gLwRSHLueo3vut9VUbltNXTyQSHBzC_TgYVtCBPLKWlSvGhNw5eX\
    iARYI659l2ObeD-8JQFjwN1fEcesBjfXWJKOhJoYbC2dUO6fLKolxt72UU5Zwcdw\
    Yjq9W1WEO8z6C1s_QqaDOrKCtuLRCO03lcXLIkKHkwAaspTVw3nhB8_6kn1heCfj\
    afA1lds2dx-4zBechsq2E7l6GnobhnhUp0-HQXuGeTSiO4aamm0tou3-inXpNzuX\
    sR6CYPG2q1RYAlgWoLJAMijgTMRNxtvGSPg1d52qxDXBQIpJOTScQf3fONnHBb5G\
    ZHTmiQ-BW9zyhPM5KUEoZ07nx_beEhzrtMX8VZOJe5swcdalMC8MejzOYvLhh7jd\
    FYkeIbbgkxMBMZEkHHtfijFgC0T7qCLTkQAtXA6wKZLgjHwxsWDjsTDuuXglDFxx\
    hv_dJNUXLD6XQe4vkDxnEI3xFBzVmoZ6VsRmwKdZVo3WylBShYO1h8YBaT8iARj8\
    x6NekIPsaFFbs_KOhLR_ttA7ETiGCrn_U_E4UFjCqyGcZPEFvPc7YNcyMi60ujwI\
    h1pWQEIDG8I5qsZwMPRXY1MXY_ipyOVmE2sxUbhWGDrHgxl7Rm0swGBmY8JdBH_d\
    Z7IqQUmpfcFmsztkfIoV36-la8UmqjSN56xacvlWK6Wwj7RTcE5jkstUY_rBwX1k\
    BU8IITnA8irT2vsR028wS2lsVFIVcmlGloIbCU6Oazzm3MujqBobbHMKqXnv9Op4\
    37pCNlilyNtAXS_6ZEcLdUIe3wTTxAd5idwaPiZKy9o3KyjiWZ",
  "priv": "uSDPZnwwnLpJ18lwAGHj75e-fGohW7zOWhAG-7DGLis"
}
```


Figure 16: HPKE-10-KE Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiVVZ6UE94eDNqdGhW\
    Q2c1NmhCTzM1M0hJUF9oT2JGYUZySS1wZjNtYVJyNCIsImVuYyI6IkEyNTZHQ00i\
    LCJlayI6Inp3aHhKWTNHNmlqSW82TDJCMk55b3lpT0JVY1FlVVE0bTYtZlFVTHR2\
    eGFHVDh5T0k2SWFsNUlaa2pxSnZIVlZ4NEgzY0cydXhxRFZ4dXVOQlotTjBuWW9P\
    SnotQnJjTnh0dnRUMHlldXo0dE44QmlIVm05R2dFNGtGR2JGTk1FeUNfbm1vbDZv\
    Y0xmY2NWMXJCUGxvQV8yZE1BVFpJNWJlWlFpTjlKTmw2UWktSmdZbHlHTHlFX0Nt\
    ZnhXWXhVRjBTVzlhS3NmaEpVUlJRVDVlb1FiMURNTm9sZi1EQlBlMkh2cWZxS25J\
    alU2T1JBb2ZSbThEdEJFOEFaTmZwRUJWTUZYTU9JcWFYVnV3OHdCWkhXVkRKQk5V\
    OU1NSUtlUFBqRW1UT3F3QVFCZmp1eC1ES1dYc0J4S2xmREFyYUV4UUtVUWI1LWVH\
    Sjk5RTRJLVFGd1dRSDdWYVFRRWgwQ1lXNkU4b3JFeXpzQXc0ZlIza2wzbGJyVmc0\
    Z1R1NnNpX2lnaXZYV05EOUNXU3BXNy1FSzE2amlQQUtlaEQ1c2w2eUt5RnZLc3R3\
    cUZVcWVidlBPb3EyTDRaWGxnX2VGcTdnYjluSkV5eUFvT0NPSEVJRmViQlVFOHg0\
    ODJLWXJuMTlsQlEwWGtEdmhXRjBIV1BYdFpWN05fZVBFX0J5dk5zMlpqY21uaHNJ\
    Sm5ESUZHbHkxeGlZcVVvX1RPbkhzdjhXQzc1QmhZbmRGYkZsa2lKOGVZU21QU2hk\
    NkR5aGhzdnc0amR6MzN0TWUxdmlVUnI2VVB3TjFueUQ2OE9hWkl0OW5NQ2dERVJX\
    aUZENmN2eWRZU0tUdVBqaXR0ODFWX1JsYnItXzB6M0h4Z2F4dUNxWWhwR05GOEto\
    RENPUUdVc01OcURUQzdqeGZYejRiWUZxS2ZldGxrTWdsUVRtaEpmaGdSUHpUNC15\
    dzMxR3RWb3ZaRENGQmZ1N0dkRVVsM01zcVdCckI5aG9GdEpfdkI3V0liZ3lVblBh\
    S1JqZ09SeFhkLTNmQzF1bC1fS3RaWS04aDJRYmtsMlBibWc2NEtjNktQN0FRcVo4\
    UHA4U1BTY1AyR1dWVUJjY2NZUHJ3ejJWVzhLSXRBRFhhb0ltSkZJN05OX2xzM3V1\
    RnA5SnhkcjBpQmJhV1RrbjNUa2lLanNxVmVBd3ViMktqZWRhcGNYT1BkNzhCeGVX\
    dFJxcHVPVUJHU1hyVEVjYkJLdUxaS0ROOWtPV3RZRVJ4VThlZzU4QWJqWkN3UE82\
    aDJNN1VDNlRhMTlWQXdLcXZNQ3ZFNXhyNTl6bmlzY3I5cmhfUzRFU0RtZVlSd0U3\
    ODVUNmRnVTdWSV8wdGg0NjJETDhxVVQtNWs0dlloVW9xbDZRUkg2SWdLNGtKb2FK\
    LUFoTEpkclFiRnczaU1KcUF3b0ZRbzF5MHduelVOUk9nU3hrSVJsd2ZaZnM5aDg3\
    aTVWRzhkQW1Yam50ZnZMbXU2WWd0Q3FsdlpQOWFpQ09jbHlPMnp0MlpZdmhqdVJu\
    T24wb0ZTVF9YNEdfZFlQSl9nbURLWFJlLXhDb19peV82eERVYmhfVExHc3EwNkpI\
    OHFBU3p6UWZRX1VONEVLN3FreEQ0S0lqaGQxQXZlX0NDNGtUWTF2UE9MR1NMX3Ns\
    YU9EdVBGbjM1d3pwU1Q3LUF1blRBdGZwbFBTNl84bXpjUGtudmZ1VUg5b1BMTVp0\
    RVk5UFlSNVBDdmh4ejF2WlVPaHAzdjFIX3B6N1gxTFQ3UWw4OHU2OEhOOF9VYUdi\
    MHpna2ViNGVOSW9ZZFdDdEFncDl4SUVwemJDSTU5UzZzTnN6UkZWQnVOOENLZm9j\
    eDM3dE83Z2Rzd25fMkFyQUpsTTN1TTZXM2hVTHFKSFl1TmRCa0cxTXphVjktZThu\
    MUduUk5rVGFycEIzeUIyd24zdi1ScDdmSzBBczJfSmFWdDFReFkwTTlDWWZsbV9B\
    YVlyRnBXMzcxb2pGTFlhZ2pLdXR5YzhyWENReElfWDBnVUgzSVBFc016ZGcwSm5z\
    Y08zN2dQLUVWc1kwYlU3bnVSanZWdE43Z0NtN2JYNTlnQ2FzZ0pRaTdBNU9DaDA1\
    N2gtSnZMVjllaGJnX1Fxb3h5VFJIQURGaGpXQ3o3aGt2Nk9tTE9TWVRjUFFwRUJB\
    cE10NkpLSVpYNktFRkhCTEI4RTZsSjRyYU9VQTlLRDU3akxpQmdZNGlXall5clg5\
    QkZhNFFteXJsZV9uaFh4aG9qZ3EwbVVGb0VKVURFQlZYSGFUTnhBQ3c1T2lJUmpu\
    MVItdThqakppVm9rYnhEa3pxdTBqVzFsX29xUW9WdVVRN2QzNWU4TndfcWppQzdM\
    NDBfUUdDTGJUMlRxdWJzR1VMNF84bDYxeUVHdFFVWEpzTnpNUVpwblI1V0xmMGhX\
    UjhjeXdiM1poZExQeHVjVEZXYzhZWG9zRHp0MEM3UUs1MjcyX2l6djdwb2pkWWdS\
    Y3k2MlNTS0RqYXBwTG9NbFlMWjVqS0g1bXlETlI5a1hiTktIWDcyajlYQURGTVhi\
    RV8wZko1bkljbTJ0VHlLT3FxSmdvR1ZqUnZlTE1YNUZQdVRST19iQVUybFlWdXhB\
    ZXUtM0tuVzJ3dTROUHRIbjNPWHUtM0NMbFZQSjczR0s3aXRmXzlhTjVzdmduVnFO\
    d20yX2lXc1NndlJldThiY1JHRms4NU0zRGJHVXdlN0ozYXFYQ3Q3aV9KdVdRU0Ji\
```

```
      WE1ieTRSSFFTbVpxSFBqV1ZERWQxaTBHWjJZV0EzaWlYY0U2a3FTUGRmWE5BVF9S\
      UEpocFRjUTJrbWFrOTV4NVMtMVdvSjJXQ0NWdWEyODVnNFZaQ0x2Wmd1QjNESzJR\
      UGVQRGRkdHoxOVVaVGdvWmpZdjA0V0hwTXhLN0lyZ3llS1IwV01FbjdjWDBiQ0Q4\
      OTJjeE5FZXRhYmJNZFlYQ2tEcyJ9",
    "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
    "iv": "QhIHZiO-gUr7ZkJU",
    "ciphertext": "9ct3eSqXU0voatHvMht3bpOxfTEsFNcxgPHqJykMbQYsRzdgD5w\
      N4KpdUZ8OzxwI65OB6ifP3ekDEwqOybu8W8jlPlW-5O_Rpn7anpoYDKDw_Na6_gE\
      IsdJi89L_9N_3gh8v4dM8n4feY_jVmuWf2JLNrLuIaghtginwHzVeSctFF_anTP6\
      toPOAql9Nm2v4UYJlNoi56oN4jZKYSZoQq8l4Bhiw2I7IlU33_bhUOu7U8AcaEJ3\
      bemHgGY9grjv9E7zVk6VSsWx2kdmCMHc7uPHoT0akt-pzUBmbmJXq86z5BrWdfwP\
      i-Z1IZ_h86rShfB3hF8FKjCQrpQCCiAO3gWO6UBa_Uyse4ma0K5uqBQol",
    "tag": "H9VOy57gURPVe2hxW6pq0Q",
    "encrypted_key": "FF9SOzjoJxyoocqLxl7zsPeX7982LMT7kDpWdliwzPAQh4sW\
      KE_8VGvncRwTGS41"
  }
```

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

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiVVZ6UE94eDNqdGhWQ2c1NmhCTzM1M0hJ\
UF9oT2JGYUZySS1wZjNtYVJyNCIsImVuYyI6IkEyNTZHQ00iLCJlayI6IlJwUUVpeUtr\
aTdNOThVaVlGZlNQNG4yZEJ2WEdISUhGSXhXWXZ0U3JIcjA3V3c3SG1lWnJ3T2k3a1FJ\
Vi1PcDFtRzhqVHpmRTV2UEVzeDFfVmlhZVp6a2ZlVENzbkUwbXlBSlBEZkZkLVljRjhB\
amF2YktvWktiTEJrYUNrRjc0bkF0TlNyWVNuWWdlQXBuWFVRVF9ObTJ1QVZhaUE4al9s\
YV9SS1ZNUm81ak1vcUpxUW5RQ3BIRTlQcVEybEV3MjR6b3pBQ3l4dEtwZWwtSWROckZY\
aTQ1NnRldC0wa2R0TElUMFc0aTFjNUl0MnRvMElUbVBxdHYxSnpPRDV5ZFdDVU9Jb1pu\
SXlKVndFVzl1cVZvSF85LUo0SUJnY25VZ0J2SHdJMFFJX3Q3aS03TnJBOGxsamd3UVZ0\
VUZNVUs5RHV6aFZ4OExmTnJLenRFTHlyRHM2Z3c5ZkpZeVVneEVJRHYwc0JPQnBxM2wy\
bmtCUzZhN2E4eEU2TEx0MEhJTDl6eWJGaFBzcVFVdmt5U2hCZ2EtNnJvY3k0NE1uMnpD\
cGx1MVFjSjFWOG9raXhLYk1sRGVZR3gwd1U2akVuaWtfWnBJYWE5aHdoZW1qbzR2MnBi\
eE41MGFPNmk0VklWVDhCckxlSXNKM2F5NVZSUE55UmZlOTRGUUN2cG9hdmZKNTdheXhr\
RlVaZFNrX0h1RG9MaDItMHBsbzJrMkpzbVdsLTJseXVET0hueC05R1BPMC12NVVhNUNM\
T2pFSzVYN3N3SEQwa0tUbkc1VjZOSG5NYkNmRVc0RWZ0S2dPYWJ3UGJnelJiRS1tc2t4\
Nmk4RnZnYVZidXBKU2VkdDF3Zkx1dEt2ZzMtSTRrVDhuSERMZ3JpYjNyeERMSGYxM05C\
R0hJTThzVldNTjVYaXhUcVdQSVA3VFdnY01jY3RPMXNTbjJLUFJuTFFFS1BnNVNEMExI\
S0otTVdOTEJZSWY4RV96eWNLTjlUbXQxRWwxR1dsREJueE1aNTF5ckwwaDZxUmlmLXZB\
WFowNGs2a2NQbUNULWRsUGp1YVhCRjNCeU5WME5hWjdqRmRJaE1TNnBhUVJlVlZCVWlU\
YXltTlhDZk5GN081VmZiM2JUWjhKLWVUTkp2YS1MUjd6eFBYd1ZLNW9YLUpMRFNTaWd6\
VTJFRU1jLWpPNmFCYm9CME11QldHMGt0UEc2WDdWVEY3NWN5eFNEQTFCUkhWbm00R25S\
b0hvYWd6Yl9FX3RhZWdiTkJUR0w3cUFvMWFEY0NiYlhKbDV2TDJnZzJDWmoxSWZVaTE5\
S21SNm1yd3lPSXVwblVTMFlKVTZTX0NxTTQ4azQyN3JMV2FDTjBWOUFfV2ItOHFidVR0\
Nm1kaVliN3dDblA2SHVJTE5rUDJyZGZ4NVNtb0VjX3FiZ2NYa0FuY0JEVkNhV2ZnNnZs\
dnVFZWlqdFlEdm10MU5SOEF3d25Ed2pNOHM2TnBWdnptakx3Z05GSVdOZmFFQU9zZlph\
N2dXaW45OS1sZ2xOZ1R0ZnJJc3lEUDR5TlU1MUNxX2RSQmVwNENCZU1VRXZkandMcWNB\
S2lkaDc1bnlJdEtqYmpkUF9XT2x0RjZ1aUJ3VzJNOFBCc3Uxb2t5SVNrYXMtN1pLUTlk\
RDlwM2ZYaGZwUko5cFRfUHQtMndKb2E2cjAxVFpIajFwcTFqR3JWTGVXRmV0N19QM0ln\
```

```
   VUFNaUdBOHV6bE9DSzgyZktIOXV3ajVCM0RzMmJyNWI1S1FWaHRQRTFJN2duV05CNURj\
   dVFqS04tNnlyMDZKTzJzSGcwemRZal9fT1RHS1NBN0RhdXRqaWREMHpkUmdpWUpITDNa\
   NGNMLWo2b2IyS2l5TjFJRDd5T3JkdUZONGRpNjVjMTZTQV9kOFZlVE9jdmp4RnVjck4y\
   NVlmUC1zNzhhYXZ4OXk3WVRkSFRkd0kwUkhMZUN3R1M2S0tva0taOFVaZnh2dEZyei1w\
   Y19YSWM0cTctU0U3OUR6eDlwdlQtUFBEbnFQTDlrU3hJTE01cGRJM0V4WlU1ckNfZEtj\
   Y0VQS2xVcFF3cW9RcllHbUw1TXluX1Q1TkFUTTZiR29PYXJZS2d6TEZ5MHRnSjh4MWRT\
   RkZXUl96WjduNThET3ZBeDZzbko4ZmtQc19SUFU4Q1diQVZ6VkFraGNBUk5lazA3ZzBQ\
   X0Rxa2Z1WTdfaXNJX3VzQl9UdHpWR1I1OFZWSlp3Rm94Qmwwb3JVR1lYaUl4aE9SMV80\
   OUphWnNaUEVrT2d4d0ZwVzNHdWtfM0tWWWFtQ1lLcy1HTEdfcjNLSWV3RHZkYWZEcDhh\
   NVZFOFZEaGZTVFRPdTRTMTR5aFNYLWczU2ZTbnpsTzFpaGJpcHJBZVZSdGNKTDR5WFZp\
   dk54YTRRTmtJRTRUTFhjVHhhakhxbnRvalU4cW9kMjZzVXdxcERldXRoM0F1N0xjek1y\
   bkx2NEM3V19UcDc1MDNaaXJDRDRIRlZLMl9BWmppek1PcVJnOWtMSUdyenI5VVR4bE1k\
   NkQxQTlBeGdFT01aUFRuenRFelhZbGdwWGtXZHNITHJ1ZWxvdXlXV0ZKMXg0dWkzdGNF\
   cjZVeU9XZkVrZmYydXk5QnpHd0ZBVURnQUYtVG9KV1ltZlF3NnRBVExLNkpyV0FiTUVF\
   Nm1mT2g3MWIyUUYzTnc2RzlnVWw0X0RNeTJ2RnVEMTR5am1aclpZelZzdXhTblYzd1pV\
   ODBZRm1qemhvMk1OT2x6bk9Jc0xWUFV5QzdhR1JaSXJTLVUyY0t5b1NjSUVET2lqMkww\
   QnZVTS1BZTU0TDRpWVBWUk5DNm1qdEVsc25SejdISXVsMlZaa0pQbTlYcnd6akkxUlBn\
   MmRrbDY4ckN3OE1LNUZ2VXh3cF9sZHhXZ2VmR3ltZUhDTGtha25HMWVqWUg5OEFMQWFH\
   aFlYZFlzNFBPNmpqQkltMlBiTCJ9.jkEPj7ylMwa9yBW_p-Cjjn_Mjdje7sTgrAajsy-\
   VSxV8RuploiqxqxD-V12m3Jwr.6S0_LInPwcyTMCYE.4fSopMO3uXyReYk7XqATTKmzi\
   7mRBR_GVqKPVMWJ1ScMOzcsjnvpX1pgWKuERYY457AoQbzxBmHYYvuTmXR5LZQ3GT2uY\
   KC-NcsnNRx0q25fCR_R7N1ttksFWZ7fIrdFVnItd2AiQKk8yoddSRh35hVj3g2BNygdA\
   2DI55I9A0mJsx4ofxX03rPbK1MB-X8Vz75ktqAWLzLVwgzT6wFSbFH3e1B9BLB4WFlsE\
   dO_MIycd76LKoaUS63DFZnJJW-cAwtYueAohxwXDj2PNYVIpEYR0zDdNlkN07SALNwsZ\
   r8CdBS5ow3nUiTrtcHcFtFgPvN-nHVPjijsFlhXYRmwjHeg58Qg8oOKF_0oJHnQqhi7.\
   ZXV1oGmydREjiXVQtEpUFg
```

Figure 18: HPKE-10-KE JWE Compact Serialization

A.7. HPKE-12

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-12",
  "kid": "jw8GWrYDUzjH0aZRXlCtcokQwI4elPLJKKulziQwsB4",
  "pub": "2dmLwuO_9-eptid4KThePBhKHFBdOwVPc8lNjbeSGLOmFdmzR3yD_-ZucZ\
    grSHqacNVD_oES2ZCS9CEeFQyNgYQxrBRb1gQ8JYC9PmiNFWdbN-eixSaWsYaLTw\
    ekCiucwOhsSwSusRgMt0Ii2DyKl6m2J1fDgDCCevVhe8II0Axm2JaJZaNgftU9pL\
    E8QwAKY9tfotx3wzQRXdE61rmcEQOfIQiJr6TG-YSl_cERxbsJFryH1gmugWkjcF\
    Oje9NSiZfLa2mi_0s6MHpkAQhxm2EVaCfHM8fMsCpkBqKOgPTKkCGTG0A6RnKgA7\
    SclXi8P8kJupx46Km3ueR6KEGF2RtBt6SmFkceujZ3oWt7Toqtc1SBjFONk0GRuZ\
    ABZisiUhqXM9I_T7yagLhdQqOvsrIVllCfFOFHiJhPFEPLOAMyQUrCj7d1V8h-cr\
    AhypiQYQFFqSq309oeRqYGVHyPLEe5m_lvfxfFMSitRcFrmchO2ORCbZQTm-tioy\
    slu6UNDwYWarR0UmgJIPlfNLJ98XNO5LO3fjiz84hHC0nLnOqmD_O4kWEDXkBCPW\
    s_mzomlZKncZdiQDGXsucMUUhs-ySo_aqslswumfk45GsP_pUj51ROcVqgjzCSyd\
    tkaKN2nkolubGv4mvNAacz99oLKLzDbqAIqoRTAbGAJVywNpBuzFw_2gGiqSidtr\
    UmCJcuaihnoAB-dlpCLgcNUTATJ1RtClSbXpGW9XJQ9cQ003UwfVIp8owxEsFqgk\
    HEjRsDjJJ9sikq9AaSzoJ6q-mQSRcycAaM-OdwaohFsrEEtVRZ07C8UahelEMmZ2\
    qtEMEHpkEBiNAQ95l6mBjLFdXGKoOvBIu9oshYa3G_raBO4rg6F4kKkhO0h0u7us\
    KC8mWQedfJ3WtAmpiNwNJxCdRRjtdigjoVbRMkImVvJhaaI2KRQ3AYneWcAbRra3\
    aY3SkKjkMhPZp2NVqyd3XDUNAiFgHDOfvJMFOkz-VgWTlfMze2z8w3wPUtZpjH4b\
    QUtXslmVxUGwi1_Du6qHyin9xPO8Sv6eNKqthW9YwYiBjE79AHNJYx7nQ63IM9G9\
    RtF3GbWQtP9kye16Who5sZi9k-9BhOxwwXLeiqHOwPRFMGyQE5ySd9hOUSaNGajV\
    WZytWOmpt8RSrLnXY4moxAKZEGfhIFYIOVRImjtLGeEBZfRyVSYwfPLJnH5SDBBi\
    moltw1Uhx3HQBOd6FmuGsRViYu_UfKDxKscAgJB0FYS6FyoKxIeknPHpowlJdJdb\
    pMF9QIF2mNynddFEfGJHYldfBxyHQCIJaWxHwFTfYxeiKrtucnrCmm2wBWI3wntU\
    UrC5d1vGmLI_q6Vcd5sXiVm5ZvENddrPeInGaLYUgj6Nl5HiMhXjp7t2lLMRNNtk\
    oomRx0UgwsgQJx6LEC6_s0G6E4nXe52UVdkfsQzKpB7dmaxSkWWGupmgdBcXpyX9\
    yqYDqZiFyu3pbHo7VEAC0Lp1Oya1pCP6kONJZuDGRscQrObIuBmZwzj4B_CwSeu6\
    ZnJ4QYCR374LlG4VHMX9hIw7S-tp1j0QZb3ojmna67QydOt-M",
  "priv": "oNrZa1bdAQtxbp26w5mcZgzw7fKR0WxEbpRhVH5tcPRQxzIk3Iiqt6p9F\
    n88pjYoaUmmlaNymuTk_ws1WgWd2g"
}
```


Figure 19: HPKE-12 Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTEyIiwia2lkIjoianc4R1dyWURVempIMGFa\
    UlhsQ3Rjb2tRd0k0ZWxQTEpLS3VsemlRd3NCNCJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "sq1TmK2Oa6_P7yp6eYYDAzYv1biKXQ9fO2zORNkdFAFOnTZT\
    KN4MvaESlHx-Bx75d9enCHMhkYtrGgvfpjTCH-XmrRp-UexBp2mKVo1C3LFOBZIn\
    oESOf33-1BhbM2X3M2j-mhm7i4VGIO60UrHeSaZgH2mAqSZgkHHP6y5WiPutwnAA\
    dP_SlpswWEZDPvwzvCNI-pvSaqW1rzUe8iDGHycTkpv6V1mKUaXIhaETVmNQFRXZ\
    IvkQDf6cVatOtkiBCsHLFUNpaSUjXJdwJBdDsqjbfa_TFJaqgy3vtOiRYOBtKDla\
    UWcI1osJXSCpkOfXB8halKlq42khbFf7nbDon4H0EJSGoKHvUw0LG8zVlPzw8_DY\
    s9XiYTpWAYeAX-mkJmX1FH8H8IgYR6APRsAzwagCGIUlCIbY6TKSRAENxAS1fy19\
    XVpne8ouZQ8lWVKIm9bqgRcin7T5lYQiG3lkGdqlN54LndxCWQWfC6fX66UDH1rG\
    tF09PC7i30NcyuteFBaVXPoSluaKYKOwFiQIxtL9MEVGEWazgJEdxvgoiZnCQCF5\
    RqinqYbFrKtgej-4Adck_uz6H4G2l35EGc8BfUhYOc_ddqs2nJcF6JPjj29ASvYZ\
    l4MjWpR11YEQPEXlSIK9aLIXgujxai7FJL_nhqSFm5AiAp3Bdszp_146vMoPaV3P\
    7d1C_WgLS8i5i_2qmzXn5KorN00g6Cd36VdRGQHftpr1X6vvQit7eLKf4jqQ2DIT\
    cXGJPqi4oZn0FHlQoTfBegmDnosVyaoYyrSPglCMBM7XtvjefhVTSsz7oQHclYUt\
    fGnCsPUh06nVJ51PdZA2SX20md97TH6RPq4dnn2GIebn3Hzc1JjuDkrkfRf_2NNd\
    THyv03IXGXjygigb6w2BRDYu_oPSLyDJ9MBvJAJv_f9JFOlqEiYD9LFwR_3rEJAv\
    QkEL6xA9DOF_3urdOrYwMAZ-Up1AqBxUzMJ8WVkbElwQKMe7o4gZ_AHV27NSWf78\
    kjGVNsCQoNMSGtrvx3eojYcfK3mFJUUBjnognrn23Dq5_mR2s64XdLcL5nJY0D5p\
    ulB90x094S04rb_6wO9OpfmdRlRbuh0O5LpNlmLYPpa_BZtwNwtmCNKsxRW-BrpO\
    y_kfOxpl2UaewqWjEIBvoIKqThfkqx9GiMEhCQTUKZR8cejvbWRWtVgJxJLTA0IW\
    3QyMU8_Gi9MXMG7NOrE0OspkRe_gAexc8sGO9O58qYbfSuqlTR7GHkLaUczi7yej\
    tYYGzjastPKFMYHOHsBYau2FgF6eNrFWVeE-bkNWrgs4sZycpIJEYktDvvODRZHG\
    -7TpFbLRyAOCcqBoQXnWcCMzjMmmecRi7yZepjAaslZuF7hGRGCMivDUVNQIEytC\
    -nigKVoi6Ya0pZ3yC4aVBFPPitRFKK15ktdh8T-g8Lk04_faM3LoZMCnLgU",
  "ciphertext": "opqe-7Y8RSKoR6OAbqm0n0GuRQa0oLttHqH6RXRDR2dqgnn1P9a\
    5tpqnUAalwkyT9UUkvi5CPpZkFk-2rw9THiUMRNhP9TWcqmLF4iC9pzFJZWflW0A\
    sjTDU9SKe8JFFUgcLejw2v_pyRDcPB2zvMQxxlLfsXXggtntqT4DCPBI3rBMfTt_\
    V6RDEWKLFSseOF54zdIw6z-aBnhEOB5OW4seXHvCSVmdrH5B_vimGVciBZW86e2x\
    wix0PAIqg0CnFHMqarOLADeWfj2bBwUI1FtXi0YxwXOQEy-5hRch76wuQ01gQWUd\
    qLd-PPxfUWkGJukZ4XWifc0p6ho0SSLgkFERvpugQTqyi7G8fHlQMSjSIkRcVFXy\
    DBwXQUG7BhMTnrA"
}
```


Figure 20: HPKE-12 Flattened JWE JSON Serialization

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTEyIiwia2lkIjoianc4R1dyWURVempIMGFaUlhsQ3Rjb2tRd0k0\
ZWxQTEpLS3VsemlRd3NCNCJ9.e69-F0C9xtPkza2EzcpZJD7ogDwzuZmdPqg9L0J5M_v\
uPm9F-3FFfLPpiqKINn2bozlj80Tfia3tBHpC7PUyVJiXsyh417ZdMgim_DG8Na_wG7A\
_j-H8vpXrW7EEsW0wqYohkGJwi6eSq0Vbd4tDPeWCL7rRDeMmseRPUkzhmTKmhx9T_jS\
gI0M4D0UHeXPud1eUAavFZS8xiAdADoiJFxtnS67s8tNobg63099O2ZAciOvfTZucqwS\
WPwqL8GBh5ieHizVnk8YvPSqByJ-rjdezRU_GghZ6F8Mk2PqzuMARVUR-QknbFqQO9rH\
YRMxTdEPBmGHfhpRJDgHxADLTgHuNNnrnAzTZgnsQC9lljfnvqcwdDb5SYqcqEz4F3t9\
m5d_QiiFtrXUdZi6u581uuXLU4vrgiLC3aRvCNrcU-qY7NaBA2vO2nOCsdjRAotWlYbF\
wYkX5tPXkqzj7_ZXiM0GR55koR_mnTV-_i574qJfry7w8J2yru-0DVCYtSAaXTNEwlwX\
SsyCQtRN19LrTixKpP0U928m6DMrl6TJ5IJ56sn9BVrQI6Q1aoogWZDfH-KQT1sI6oRi\
sMQNdV14SKawZbMjhbCn1mQFpGH8SCdCofOV1LQhCKHwJ9jYZTKjLPjRX1bPauzHSDhF\
R70yr2xazK2Hx-tqwwllKyKkBvJIDRmg7r8IyjZ6sAKDR5J2zf6hIVLpEu3_j2XQvo1K\
X4lxD0f5qXvBLE0R1n57dF45NE1Ij_nvVO-l-rQzE3SAQylQ6bRlRyXRrtGkdw6GLOuP\
yoQJZgR3PWNdxTSlFSKzAOIzIVlgxo6Fot1EAYJsxttbrZ2sINh6Qkdh5Q-MUUPTdixd\
iwOLaCJIs9_dsF54uPbUPq3n6aTQve2xJ6Dkj4wC5hOsaOejH705y7TLgiHaIBwOyfJd\
06LkVf8tgZea6q-3cQ9Jji0qDPr2bq3uXzTubHxn1a-FrsKvKHwW2ljifnyzTYozxDUV\
Df51euk5Fn-mR-Ns0dalVNwVqlK-YYo3kIbhmLKHvSgXVB76T903qLVRqrQQWHO_w46g\
_lnT10Ta3SfZw3u_2oBQ_dC--68_b1xDKOqLGvApXFRCl4-u4rOTMuVfZ6RT2_fNR67m\
Ok71vG9fc-ZWn69myX4yfjco1ZcbsW0qb9otY1auNDefmoXGK-j7oFknOpyjEQ5qXy5B\
17l5pYS_nqHKkgUznQm5UMUWydtF8W-Pb1rvfdHGSavTkdaZKUd4Uyq70ylIzFFx1cK7\
Bi4KjJH7Q8Uhzpt4miATD6hEe-kc8iybdoSMJqe_QhIKJtngRrjkuDYNEGwcb-rZkn3K\
Lh0juFkoOlmbTPcHcLBKv_a4-PcB2CUAp8pJTf-uiJg6eZzsgyIvY_JQKgCnGfDqk9QX\
O2NlFyG_R6y9kaVw65YXAJSSni7bMBQbymhExMgfBDqs9xTQ..OVegzSMbIG9TxaH4xH\
XD_8GemaeruyQ-pPV5jvUHwkUmcgV04TQkJ33oooQJApX4rh1B89AR8Vd3Fqtlb8gMfu\
nbnSHE-iejZNRc9qVXzfyueskK8zMKFEydGRUI63BFZJLRXZIuZv_dmYqwc9nbJJOpqo\
9mU5jkdyHVK3Hbbs4qzA7jbqx0wXFaifakYMprOptUKrTXtTBUAVvxyf6JldJLmKR6Fj\
rElMxA0BPWKuPduhkz9JhOkwurJ_LfZqx4c5tsjYYXbFTAM9PkGkkMPQuON3OP_WutBZ\
EItOb5xtF2s6o6bwZ9URknWRL22oI0n8I6QlrjWNab_f8GIuBlxFiFuUQH2NfzWFE_ei\
wjUHzCg9q5kz4MuDWizCy3NE-UCw.
```

Figure 21: HPKE-12 JWE Compact Serialization

A.8. HPKE-12-KE

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-12-KE",
  "kid": "ogbSkvF4f3pRb1dWsBe1HpdXtfiRwZsYrhaxzxlWv_Q",
  "pub": "HzogrJREUPAOuEVqa-DP_tVzOjIvQ3PBDwozMZK-LnQht_mjYEphugmVjF\
    q2IsGfF9fK2TevQDQvnQKHoERnSFzP47aBxXBjCZAokdV_w6lI_jlrZLNmEncW7K\
    yQpZVkrrdQArYLiRQxlkozD7FaXlUE6_yUCYFwOFinC0Vbf7tDqZwGordZoCwhXw\
    dGzUqU5HPHlEdzVTl-NtGQdoY0N7E2ziYKq9C0E9QSstyYCBKqd_qWSDwmTBiJRq\
    jNhXeTt4e6DEI2OxK25KKxrfYd6kpHYFpZYCwtfGYF6jWWNjpSWVcXuDx0xLco8M\
    gVk5cN72lvvVlg2fDBOLexGAwHlqenB5WiA8qxHYcJr9xJi8cFjCdpVoqmVbGxOU\
    R_lAM1s_eoR6ME8-IAGZRluTxQk4bHOISjiCZZu7Se_dNFN4hNCOxcUnBdv3Rb5E\
    g7CNgYFBZAh_QXVMGLiMGgaQV6Ifk4wCoxl4chmLVnqQsEjlsybTwzqziOLNkCga\
    JoorRvbpw-jAaUXbCtqwcBU8shpNhQ7liSzXFOdwQaBVsKYwfQCTpskbVLLqOZKS\
    jFu0PNv3TPYWDP6JUgFdh5T4SKYGILClVa0DpAResKomPG_XxyKWFFqUOhgvxDZx\
    mResssUORAt_hDsmN0GmRpcfrB8SQvXjmbmEdOVxsDl2PNw5zIovOZQJVtvsC4H_\
    PI_kJ2hQydxYB28PkYuiMiibpLfux6tZlPB-NWv7ck-GpZnZxrEZYbMeEbSLBmvA\
    VLYVVVvYx6RcYRBnSRR0AfgJG8IJPKXEmcM8y72TsFF6zDiQGsmfq1aEwUURJ7Pn\
    l_kgBcZYWgw6Mn1VsC7sAjlvSnSfowW1yZSrCkwkcFzfkq2LGt5PY5xPPKBdwVaG\
    C9HpOlbzegPdnB4FcQaRPEHlevSsLE8thjHmiRdJsVFzYsoJSCMyBCnkMaLlJ7v8\
    YyYskgJ7l6oWqCwycFjUN3RWG0btuwnyIbaHJQTcak0IBNABKZKEJTSXURTeGaYV\
    k8HqdxXWIy0uE4nkoVZ0s1gBd9sGHKPOhEOtdsERxJZPsMhDaiLjGuuFMUEhPE0D\
    QeKrEomTcSwbWxPXwUJApUKsvEKBNoFcRGV-Y0OGEzJPSM4JtlQ7FBVPi55iZd9b\
    d34qrCbkpFD-yixzCnnrBRd3gsK0tyXidvjTtSNka48aBnI8lFKcvJzOWLxWNlug\
    RN-erP-yOTwGoL5uKByHh2R3zKNHbPvRyvTVkDApMxmPOrayeSMphL5-G3P2FSs4\
    qLCXy5rMsN8KKA91AqMdYwAXqsc3AbGlKE6Ik3M3NYK5BI_CsFSkZgUkw7XKugCo\
    RtBtN9dVlu0XaLmuIH6oIc__wXyBFMX6E9bNdESTwN6jGBGpyFVHt03QQxCxmWT1\
    A7bxBeeAd1oHR6gxoqD1geCCAh_RqLBJyuk1YoIsy55EifLwyPLCQwkwSRh3t8qT\
    WMIAYXL9N3ALuCCKhxfZJsmzW5kmeZcTJrTENiePs3ZBKalINDrKitOBfGolzOwf\
    luANQurHpgR7OYJfNVNxKrKqtkeiY0kJBpHnMssTekX2TQuKQ",
  "priv": "r5W6TvhlPnuzH-g2OggdYADlRWW7ccGhUd2MADCdAFxZ1oCX1YANTcjXv\
    EVSjYQ6cLYhHgkYPmCqLJkv9JuGlQ"
}
```


Figure 22: HPKE-12-KE Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoib2diU2t2RjRmM3BS\
    YjFkV3NCZTFIcGRYdGZpUndac1lyaGF4enhsV3ZfUSIsImVuYyI6IkEyNTZHQ00i\
    LCJlayI6InNqSzNodU9uV0ZUN1hDeXJSSFk2MFM2X2d1MU40SW92QjdnUmZ3TkhB\
    Zlh0R2VwOW01Zy1fOHAtXzV5bV9RSUdvX05LNl9HVGxGbWpTSGdWdHhiUm42RC1x\
    QkVMamxkdjR1ZkZNWHlpbnhIUElvM2FWdlF0UVplNnotWHd0TGR5TlRuSE5KWldy\
    Y0FXLUVESjRMbHRlMEJSODJ1TlhhVjZSOTdhQklGZVM4TkdzOFNhMTFSVWJzb045\
    ZDJwdVpQQ0lybzQ3d3lRTUxJSDBkUDZWd3NXOWd3OFprYmJIb2lFWXNYc1hleWhO\
    VUp0ZV9WM3c3U1liU2puNVZHOC1OM0JOODYwR1o1Y2phZWwzT0wycmhER2Vac3M2\
```

```
      VWNpXzRhQi1tU29aUDN2ZGFBUjBOeUZZNHJRT2FPVkRHWjg0c3lEQnpsdkVJdWpn\
      cnllUmpaSTV2b3psRTMxZmdFZFhjRnFQZzU3a2M5cElDaHFqSEI0UTgzV3pwUGFR\
      UWRQd3pBTmY3ak5XMUNOYjZhRHVkOHlWQjk1UGhNU2pmbHlTNzJMZG53VWdTYkdE\
      eU1PRXNlOU0xOTJtTkxqajJJblVIUWxUdXFpR01hVEQwVjBzenRtTXU1UXRlNEEz\
      TFYyQ2VHcV9zZkVZNTluZDV1VGhSUGIzeW94WGpQVWRnRVYwZDJqYXpLQlZNU3Et\
      Q0YzVnZ2UTItNjVpckI3Qldqd2ZzQVQ2dG85RmYwZG5vbld2ZFQ5cnJPdmh0dlFH\
      T3M4cWtrUE1OX1BCUjJFb1E3WTVsbGxheUh3ajRZRGRZdW92czVDSUhXRHJYbEs3\
      UE9kZU0wZkEyZ1RONm9uNjVPQWRzcHZwZWhsakRwTDdHdWs2dVhVUG1HXzUwSjRl\
      WHdxbkR4ZEFRa1EyaElXUVktUl9wSFpueXNJcjFoeGNJaUVWcExaTVFLRHVycXFO\
      ODd6RmZPMFhWbzlsVmp2eGx0ZkV2T0tHU0xvc2VvOGxwbjZuTmxrMXRfM3p0MWpl\
      UzR3YnlaemN6VEtpeHd4Zkl3WGNzLVpUeGF4T19MWFZWY2VURUEzeGV3eVV4b1l4\
      MnA4aDNvczJTRjB1ZDVwWHdKeXIyODVDQ0FicGNDc25Ma1JlbXFuSkYtV3dNdFFW\
      dXctNmMzZFZHV1Y0a21saFVVMTloVUduSkl6aWNnVDB4MFhXSGkyeEdBa2tlalU4\
      bjZDMmtnblBKSWQyb0JMY2ltYzF6dzcxVFdMRXdGTl9ydU1vazFNUkFQc1BFZ2JC\
      VG4yVW04Y292VzAyTWFGYW9kbUMwR1VLUDE2c0ZKUUQwVi1USWVtR2VPS2p0bWJT\
      R1c0bTZHeW0zdVltVVlNeHJYby1qTUJMYkxxTTVINUJLdjgxVmhaYXBDU1p0OGkt\
      WkNTMU1xdk5VdXRlZlgxYWxSdDZ1QlYwdkVtM1Z3b2NYVkplaFVObWVDd1I5UEtV\
      STBkMFA2cG5YWjFYSzRhS2ZMR1VfSzFhaURZOEZKZC1kQkZFRXVjc2ZMUnFzWTBz\
      T0VHdmdkNkIwbDZTVVI0SlpzNFRfMTZwM0dsWVZnRWtBLWw1WEszYU93TFZLM1ZP\
      LW5NWi00WUMyaXZQOGNuZDJNYVRGcFlrcVgxZVRUMFFpTjBFc05CUm1RNDNtZHNq\
      d0pwLWRuR0dIWWo4ZExCWG9zYUpiTkNiQUwyTTdlbGM4cmIzdkV6alY3QVRCVlBz\
      RmZJVENhVXZac2lOWjFoeWJIRGJIaGs2bzBEc2ZZOUNKamZlVDlRRWlLamlFTTB2\
      NTJpTkJBNzZzXzc0MktkNVlUZ3dtSU1Ud2sxOEdybUV3WGwtOF9Zalp3d21KSk5X\
      dzNZY09kYURsbXFlbVpVMVZjNmx6Y1FacEpJWUM2Wk1iSmx2bGVocDhvSTNUdkpN\
      LUdwLVdIVk96WTZxczBFWlVvIn0",
    "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
    "iv": "0nl1mu3QLNZhTMZ2",
    "ciphertext": "GMIQ0AeAXSYshWUO2mK14kgZpaEVNX9iR4-khwuZIdjvZuHLIaV\
      6LuuVC_m2dqCLUL2UsbbVCH-Xsyroy0_eEnENDY-b8j1lVIWK065z3ONMwlQI-Q_\
      Agy3YKOZQdttsTnoH3eKLy_tTkl9SrdLJ4RYhFm_h8IvGIMVqn0jfoJxjUWS8jr8\
      FFGltHYrfJBqNtydJHF2vvXMUSXubdoow-_FkG8DWDClLkKIs_1GDHIkMnXQ3ROz\
      RI4wNH5zdqYOXvnxbVZ9eeQFhpdWZN_O-C0mK_pXsJm-vQSswpoU8fql55YbI8lj\
      Sy3TcmtyIPoLAV63uWVkQmIiIIbFMUQWJsqv4k5jw7EfCgm4QPiYMDtL6",
    "tag": "6eK5vdz8D1Klac80UZ61Dg",
    "encrypted_key": "BvAkmT0cnwAim8X6efNitQN2OKhZ4UWlAzI8rpQfglu6Tvc0\
      XEdVHJQFAy4mEbHo"
  }
```

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

NOTE: '\' line wrapping per RFC 8792

```
eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoib2diU2t2RjRmM3BSYjFkV3NCZTFIcGRY\
dGZpUndac1lyaGF4enhsV3ZfUSIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjFpWWpQelVG\
QlBIdUQ4UWktMlZsMTYxbml3MjdKX1hvYUpaRVZ5U05zWTZSTVd0a2FsTEFGa0pCWWZt\
RWFVMFVEQjB3bEJYN3owOHZjcWg0ckJJNTh5TFVDVF95WFdpQVN4Y2psR1BIbUhQa3h6\
VEswaXgyd292cjVHWGY5VFIxaVQ5blY2WVB3NFV0V0pvY1FYQVJxZnJVaG1saXR0VDlr\
X0ZIZ1Q5OERBbTh6YnlSMkdoajVGa1FZUWRUSHBQUUVNa0V1N2dhS211a192VHl3d1U3\
VTR3d1YyOFZubi1zelNkVk1mb090SkFXemtrYkp4azlKOUFXNGtuTkVSaTYtX1ZyTjlU\
MFlWZjY5VGFKV2JhcXBMWjRHOXZJOUZTRHhxZ1VnVXBFNW5GZXp3RWZ4OElhTGpHWk8y\
bmFjZzNnMkpmek9MeUhCa3VKNmd2V1cwMk1QemROX1oyU2trOUZQQXh4bGF6X1pFRzhz\
dHVYMENGYmROYzY5VExtaTlXME95SkV4MUNUdDZiTEpDNGVJOTQ1WFl2em9wLTdLVnBj\
YmUyazNWcDQ3NHJEWndwckJmdUk2WXlDdDZqZW90UzVBRkdPbUc4RTVsb3RXWm9adGJL\
ZVl0ZGhtckxFQjFlOGJXTG5YbzhpY0duREhJVkZJdWpERHhOMjJ1dXA3bWZzcllOVGRy\
TjN0YjNNajFkcGtJMkZLN3FVaXBaN3dmejcycFU1UEU1YXZUQUt0NTBtb0FUekdrVm93\
dkh3dmc0d2tMXzVqUVJVZHg1MVRnMFlWUUdfNXlvZ1AzLXpfNXR0LVI0bEpNa3B5dHl6\
Y2hOb1Y5MHFLRThQVk1ZVi1nc1c0dGtudTV3VnlFRlRFeWo4d1FabklmdFFOeUF5d3pj\
R2pWT1g0M0k0Q1dRSkNjclFCbTRJMTYwYnVpcUxIaGpUdUVES1F3WVFkOGotdWhwRmF1\
ODZfT3A2cWNkaml0QnRnakFpRm91UjlLWDlpaERialJhRDJDOFdsdldObzNIM3hfbENO\
Q2ltN2lUNkdwaDFXYUFNb1FKU3Zaa0lyUlJpSXM5dTkyMXdieW9KYnNPejJNN1p0U2lu\
S1RXZHduN0FNdEgyQm1rS2xCUGYwbmRjcXJVd2ZtS1ZYV2t5ZjhpU2ZEdXpRb2FQZTZj\
d1lZWmtQb2xRQlZVRVlZOUNVUW1CM2xIbzBoTlBHX1gyV0pFc2prQmUyb29YREVsM0Zj\
aXFOSnh6Q0EteHRHWTd6d3dTUjNiZUFmMVh1cXFrWDc3bWxrUVRYMjVjTUdyQVJ2LXJT\
WE5kTWNVb2lEVUk3WE4zd09kSG5SQlRoZFN1M2dkSmlSSXVaZlZ5eWtkbVBIUmxqSXZ3\
V25kdjdhY0RGWE1yRXNhaWx5S1lFMU0wcXRfNmZqN0J4dEFZMDA2OE9iVzBRd0t5cm5u\
cU5hTGdKLUVJWW1YRVEwbmVySWM3ZVBNa1F6Z3laamYxVnRmaFNnNkZtSW4xYVJjN25t\
YzB1U0pya0x3Z09NNjRtZ21vMFMxSXExaVNQOGx4c0NxS2VLUDZtQ0paMUJ5dkJJZ2hk\
b0QzRE5nMlcyb0ZHZ29XMk5lWGFMM3pESmFyRXVnMWFPRkNvX3N6dzE1bTJHNVUtYzdQ\
S091TExvbWVlbmlJcm5BT0ZCRzhzSHVsNXU2ZVdDajlsb2VzblpNZmVCY2JJSVpCc1ZD\
OERSZExmWUVEZlpUX29tVFZHZGF5UkVvR3M2Zm1hQnJLc0NSTU9Yai1fQTVzXzJlUjVy\
LUQ3YzJnZDdzVmRSN0JsUlVhZVc3bDBzMWhsLURQZjdNR095RFJWamVoM2didG13YXUw\
cmZzWVowbEhLU3dXYU9xcG1IUVU1SkdaLW9kZi1sTGszcllrelcxdzRMeXBCYjdZSGRY\
dXdiOWc0RHYxd08wZ01NIn0.XPv9zhwB4MGyuID1hRH0vXNXXQtsAPywTHM8E38oe1NO\
pxCIGFXz87bMtHXvZzRZ.MeWwu89Msj_Ctumk.H3WmRv2jqrVpWES82_3bkkgFdBoJgJ\
3rQSObhCHbHSW3Ie_-UBQ-Op3PNxfdUBIYnwQvnYYgBL0AJAHnaNtVA73_2_QLO7ukcX\
eyVpNjN234VF7vTKzZYBajd1R2yGLG4IH-ZJqbuPgZmGS2sTV3K2rNot8UBGftVTkYD3\
1EA_ZJ1ay7iBvL4-xxCAPasc8Di-CNAF3ZxLFYDuzi2cU8FJQxnN3WHnx6nggVnBYhlZ\
fZG0j9irI-EiQmhmtWCQ0KOTNgbicP_F6WBUEjG7cyG-3fvV0I6GUt2IHSYUYp-HwMSD\
maDeWE1cN5o34OGcuRreGP_xOYp7rdCMJAf54hMTBSTExcYxMEw8pIR2qcYIFN.ekNZL\
iJkAkjMsXYOMlcrsA
```

Figure 24: HPKE-12-KE JWE Compact Serialization

A.9. HPKE-13

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-13",
  "kid": "wIKmf5ISyZZlOkqqjwW707KCxkqEc4cJg7fYFLBkr5o",
  "pub": "59oD4empWTtMhOR7pGVyBEKEb5lttgUhITCq85eyJGpyZXa56wd-HfoHj9\
    MxM4pg4Se_iwmjBEZZv5UHbYpoUGKW-QFh5CGjCCuvtjIAofAShNEaBpQ2dBGnkX\
    eBGZhx_EPA3Fxv33tY9WAoUNVhEEa1sRuAwLI5dFe8ZRLDDCUoz9h1Axpa2pxP1P\
    lmj6gRtDayfAU9mvWZhhpwZ3ydbnIEjPFLgwwPYGUCYtNj87i4K4aHa2QcWlyJlS\
    OO0umCHFJbsEsNL0VNaQsieSWP_2FB90mYBuQsY5UCN1g8p-DFicWAAEtUE0uukY\
    e9X5u3z6y7A6Bb9HyAFhKH4TelarS7xSfBK6xxK6MpbGzP5YSBoZF8MBBeMNbLwN\
    SJ9dlMKYZmPIO7Z_Y4bjlnUzCsK-aC_sERbElaSzFiLImIwQp1IMxuC-igzqljtx\
    epYXCinRi8yhyiHNMuAlDJAcLL11uW7faXb2J3OdrFLrdKjwNYrOdMw8uZaexXkW\
    dCUlKV8CdJrBKKx3a6oJApUhM3lAolyquTeXeGx1AryyhGualBEPrFI3ROcgRHWI\
    FaCYFF7YZjkVB7CYKOVOpXWOdnHCSNOPMWWtGvVERXRbe0K6eeX0iXB_YxddByq3\
    IwCIczXwYA1luZjKjMXORjv_qVTzI7HPBFeVGdXIc5TxTARJR15lEEoLRIOPuzce\
    k2q-KlyyIzSqZqrHeereRhJHBPliMsJYGOAsR_NSLLxwDHWggO5mqxnxoNyVMXYP\
    gxerB763eZZtwjBuobvGpwtNwgjlqmZLfLP1wqdcpINlheQZcQsjIO3YdWIQu01V\
    svmgPAlkSAYnqkhmJbnDk3RcqGdHZzFekkcas2_sSrBsEdqhsQXBWoYkOqrbLP5M\
    qaIaKjQuOwutCgsUOoLImGwcwpNYW-gJyj4dckDfhrqcN2zreQW-gqmMgnXUZa5i\
    Ex8-xa5sRQmVmKEwls3_GpMrtUV2yG2elPFtTAlHxZsgUjm-Exxgxmmyagstz JFF\
    CrmJAqNCKnU9Ee2paKzQBw7qihMvNBNCQ5vtmQq-BWwDQDeMwRaiJYJVqGnNPOUK\
    oT23hTU3rPosAGctpODVOyFPLHY7ZoQlqKkwZ7F_dbSWLJROyFVrahcPMtt4Afyi\
    ozSqlJAgpfS-mBxieo4WHD_7GxHeSzW9Wk-pmmlDiytqaw9lyCDDZnLxUT2qF55S\
    QuvPYr-JFgyVma4LsB2kARISdQ02eQwZvBlYTHK4EN9fhFMvS2MZYfbOKJocaKOa\
    p-djcCMWp8yoyUP9OKuaabs9o51bqKCgcoRqFjqWQZCWXBgbDOyBAhAwlJRycioj\
    eH6NtUBDxSM0t_I1q8lQli9nNGKHklGEd86spm1nRMTARzy-qmGTlUb8g9HUvF3l\
    y516YoKeVBcuUppUp0v4u2Tme_llhNa5EF-6IHybjP_VUBg4NOGmGE59kKXURxiA\
    Uz8vidSWLO9RkG1IQoNtJ9r3Uyx-woFTUp3IC_eHCfA4Gb5FlIqDUcCRZIkHgOod\
    AofbtWyQRZkAFs_8iQS1UGT-O25ajAD2jMnAgXbWOqdrIvRaMkOnl0QOOZwKkMfo\
    k53vOqRJumO8dGIuCK5IUARRdJspF8dkMsrky2M5BA_QqfGIZ7vYfG_LcifNpQAx\
    Cj73qrNZZCEgWH3KVq0QaaR3QIMXGS-Ag7LMYC3lNPB8VOUvgC6wEZIdmct4NR48\
    IPNDjOEihG8qzFgtkZ8rdJ51UA3lFFMZhRsucj-GGkhChGRkib4rxL-Rkoi5Vbdw\
    xZkOYIMDhTXYN3pUOG-2p0Z4y4_TezT3BvbtmzEDOiSUiSOvMVSphsEeAkv4woy8\
    he85DPxxMwsACgpelKX-hjqYMaott-8WChtrrENzPHlxd6H7ipoyo9nACk8Mke51\
    QCBxM1Y2dL-fLEKjMDblS59wsk1yHI_BF6u6kdDAhvfyNQ_4g-uFxqSkgbC1FYs7\
    jNguciJEUFSfNta4ZDUcyWrrmHmymm7dwGzHBWoaBc_cI7ghNGM2yGhWu3XSdLp1\
    aLnaCiRXeYb5UNiRXUL6CNAqp0K6GVHkxowUsEBIV9qA-BiLg",
  "priv": "JKfunEpR_O-GX8PenAcjHl37FB3kSP3X6v8Bg8HIcIR1snymjQjiWomcA\
    q17HbYyeeOm2yIEgzjuncXDElfXbA"
}
```


Figure 25: HPKE-13 Private JWK

NOTE: '\' line wrapping per RFC 8792


```
{
  "protected": "eyJhbGciOiJIUEtFLTEzIiwia2lkIjoid0lLbWY1SVN5WlpsT2tx\
    cWp3VzcwN0tDeGtxRWM0Y0pnN2ZZRkxCa3I1byJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "A7QASMGmBzxW6c03sNy4wWpCV2IpNMWZpGMzU6potmBO-Veh\
    OaVw8vteHXEL_ARRxHUswAAQKBND01MeyByhBUjQ6Z_3IqDseFE54QQiPGdI44Cz\
    -XDpbux06YP1z6cyGDxcX25UOU-CID_g8wG_TIhmOIEx4PUSuCz_ZVZniLKDlIDb\
    WF_v6NR-BhYC6y__2mxfejVIk-ONgGPOKzY2CnmLRzb4f2lWLzD3tcAXDeGCYnom\
    eVS_bea2cygy2lsuGnfAvqfGztHiY6dbIuePMLEFuPYbIk6jlbMewAmfqH9hqxdm\
    DJNLesqlQIwCyrYJAEfPOjsXgWeUhnkWrMN8r0IoCCPtpzvIehuYYCkjVQS8GDAf\
    wg5CKxRRZ7Ji1B-SDAZ4_rTwgua_cxWLMeXFokqw2MS3x6Ssl-Hw9Ielaqnt1crd\
    6gYHBnaPL57txOyX5J5pRBhENsfQq9YTUWAnzQvOaGyo9KHg04I-RI--hjQFGvtd\
    QEg9UrwEEsVYAk-AUU-lqAGw5b6yVqvbZKkhnxHAsOYpmXrmAd_6ABT1Imovxggj\
    09foCoS8d2foO8ddQh7Vu0w0unJNY22bR6o29L5Ac1tNq4Co0TMztnmOUnR9o_Tl\
    p_7Zox87UwClvJj8PO-b81yBaZduQ311WK50d0fwH2PruOTvWiPS1UFs3EmhplkS\
    chKAbkCHSASvcBlbE-dzvF-FoKBDpocQc10C7h7ap2fl3-2amAlcGqIvb8LuzCM8\
    vxqCRxewZtgbfKPPTQvEzYPx4Ub-Unh72MnHjH-oPylXY5p2cCdqi6xhJwEE-dqX\
    tzn0z50JsisNuNvIM-nmALE8JFknNWqTCMskSTt98b9OktDA0QMNuNdZkAiOgLYf\
    6UFGWrt0RJyKRVLlKB4myD-YbKLw9nbtk0a4I6Dk2rSSpGJ_KZEbq9G-OQFIcved\
    1l8FRGCM8hA888k25jxRxrfSjndnSs_o3nhDdaZBQOBqzm1mYQm4Vc5eq6bo5F9J\
    bdvdXVwWS2sZsz-ef4qOoY0HS0FsgwmE4vnMLcsQCQuBgRONd6PL185D-PryaVCi\
    g98n0r9MPSKSQrvtam6vVqbrKdubBniUkMndhnGg1cPoU8ndo4yS9gwqvtqeWhVN\
    eOCu-cHtvgHO1F0-5-CHt4y3wK5RyhCZTt1JirBZivjDzZNM23c51qNmLjUWlGze\
    upK5HJMe3qScz1KRxVxJXleDL2XF8X8_5PZm7Xc-1eE50AaP-4PgCGDvSzEdxkle\
    6Epb5LwzGPD8w8frzil7xZr5cd7rQg8_Il-MZUupS_YM4CTBL6SgIlsa5DeMoKTb\
    Hn1EXI-e32RammLK79-8exaeaCBFscqqnWXbH4ZW_mGHsgmYPy86U6RXARFgNtsO\
    e7atKQNRk_Xsy7-EGV1kfEckX4VlhbyGl5l5Wd5PhMAFlUiMvJ37uBFAVEPyzptr\
    IxzQk4dMJdkeHKjDFScThbWOxwJlf3es9BiG_jr3cV1jeIpqdF78ZmG0nfGbbPid\
    zweVR9QlCvjYgFU9ZhakNLDoErV_euHoEOdWSuvV0u890cth5InzQzqxtEQb7hrH\
    rgrCUQpclMRw0LoHQligiZnl1quJaWBljyBVxjLHAVkwNwmzmOgcnzrgNJw2iKmb\
    J0V819rmHaoXl5Qf5HMReaBLds3qIFjkVapofh2UMgJbsPdGRshFnpZLQZZ-tN9S\
    KVQhZSqeIW7n3bjphf1spLCc78FycqyqRr--ZZBcZ01S06Jo_hfbHLUomm0v35JV\
    c2K81LZNHq62gDJYJhH0cww4oE8_M0wKkjn_TQ1JZFxGWkAqnG_MVLxhrIyYosG3\
    ufWoC-lVu9Qj8L6C21flexkjs54kz197UoDqEOgUIBA6dY0f_hy-QZjtJie0zNWZ\
    c-uEoia4UKYJOwpnLE4grZdN3rA6SkeaY_l8zewMuMgO6pNlQiyZyFDmyywzfEB3\
    eEMc6KcimnMSuZGG-J_UmEnysYAve5AbnpgdSuqRQj8kzb2yfNUwV6fcl7v_njYR\
    9uh0m4Nqc7PB8OgYS8rNv9guGy30cjj-UtrhqksXCyr2rweMW6md7rLgbY8",
  "ciphertext": "09RTEoHUgifJuBgWnroH3CcK_8dPA10jT6NxNV9hN8TDF0007Bv\
    HRzKCj0uKVqXka9e_4dN36g9mrdDTvaIkZKaWdFbLTz2xNjdYgEAM1FsJ-XBx3Kf\
    El1mvm4vSjOG6MIKtGTWIqpx_tGFSMSqbO7H7ctVJW7b70p_NPvMKM759vzodxbU\
    jlNc8AtM6YM8H4MNTI32z8uKzdxESNksyMiLEYGn2fftQaq5O9gqrUe9ojW4Q22k\
    mTu52rhIQ5TIOcLKX4QQuv7c0PZbEr0lPGbyb2N0iuALwOVy8xeIl4b_vRRQYJf9\
    MGSEgVOjcDF9Pfjh8BEfv_1GpDQyM3HLNWDQgJY19CmibuAL9F-Dz_OxETiHm8eb\
    rZwSKBudmd0vlEg"
}
```

Figure 26: HPKE-13 Flattened JWE JSON Serialization

NOTE: '\' line wrapping per RFC 8792


```
eyJhbGciOiJIUEtFLTEzIiwia2lkIjoid0lLbWY1SVN5WlpsT2txcWp3VzcwN0tDeGtx\
RWM0Y0pnN2ZZRkxCa3I1byJ9.VoqDQcN9sElKe9DRwlCgccR1tOK3VhqjsjXxdN3ypaK\
YrIlkFRuBGk9b2581ucMkchAI2x3K8DUlqJ3ORu-SU0Ebgscz5IeP6lwmxtvl6-12Q7n\
2Tt5h4pnQrZemixE71b0TCC2c3vALCKt5ivRUB9jfbRC3-dheXYZjt_KZW2uqhljbLJx\
raITtrBfFtw7vbOGvV7n_cLBaYrTNjcU8QnsGWQX1FRi0yL0CpJvA6Vzy6VrBRGiR4z9\
t7rRCcIZPwBAhQFYDUiFsmhHwHDo3FN_epfFRHPClgREtA67CY5kBO8aKkPrvRijTRKq\
HQM0FVZCb16DaUuhRvqUXYUe5xNcsOsjpjRTtZWNNAmVy7gHqDIr2DDZw6SDzhN5_z8X\
V_DzfD0ziUEKkYzyQI7R3GiiJ85Bl4vPIeSR0cgxquN5ZWWofWsQO0OPgZPEfLO5kZ5V\
UgsMIReanC_b0gezZsPCoTrijKE6pS1lFqtgxujsc1LHFApuHip4WMrxYj7vIoyO1OZp\
kcGuz-5rv4KqVxDhM5-2Kb6qcAFLKpb2sAerp0Pewdyatj4LwtKmoC360BqEhkn21NyC\
sfl1cqpFu2DmZ72S-DKgYoq68wCD-mOndFc4hgxVyADLuOMwFsbwTbDJ5GlKuPTUfblW\
wNn6pIwbzMC-clxhglUkIG5VbkQ5kVxPhVNlwZCrlsUMUbTrblXNzPqCrxB0bpeI2w_1\
dng-812-wh4ncv5Ky61MShFkQ5uOz3qTJ4zkOx7pZQS42-_nMicMPV0lwAWi_IBjBsvc\
ocwstcuXxbD_yL8-Tzf357Chtms-XMe1JuNGVH4AhDdDOV57o7noByIbRX9ner2PSyd3\
TYCfeS4TocF2zmZX_bO0A-sAqyPI5ObqiDK5gkY3vccuzCP6rohuRluaBlTw1RcXXHQP\
tf8XJJ0u4yAornBt334E20TLAgepXgtDgwBx6bgD7x9E5hNdRVdpLj_EaAnJJ2lLEqY-\
0mFEnDJdRK1yC7XzvWE3ohNOQBE8jiUSUEy6b15l0El_BagVCNXHK9QAwhVjeUhy9W5u\
31kzw7-OHp4JR00icG8APd5uLfZqdmXntFea5ow3NDurTtH8HBo7foX4TlX9zmsgramo\
5ZLjz3hRvovQWLSNSQG5ZqpT8xqfC8_RKvq-Ak5TMnLQd2zhXBZlM9ESJqfSeUm59FbK\
jPdx18sj7S9Etxqqb-RgoREMKJamJ-dqx7fHgiNNR0tlJk9XQKUN-jgSRxrnZvCN_Wlj\
UdoiBnlrJpXIx4g7oRXm05WfgDrmV6-fYE-8ddCnA3RgG_Hxh1WaQ-thyS8ZIWIo3ETV\
TZydrMorERQ_ExGuckbvsBRQm40iFshOtTyOKq3MXGjWxQIuje7HuBnioJxNfHV_CLP2\
hNdMJRXRDe-gy15K6L5mWGe1jGt3q68FqgKOC9abNy9AKjZFcp3p3gj3QNNfuca8Eepf\
0DVCWsD6n7b54mRmsHDQ2BX_kouMJXU8TD0N8wBaAIbM1zsW6N_j0ZyPU2m_OO7KZ60A\
k0NXKMDt4sk8c0qVXPc5yM_DeDF_6jXBU9PqaNyq9eqCX4WYblv5HfoRLoWlhYqGuMUy\
j-3jVW6_mOXEtrLgbESadyvV21l1qy3B4PwQWj56Ee1QpJf3e2-jmkh5BXxocGtIi0Yh\
Ilaz4q5ZFD0HkkYTQ3FQP9W5G8COK66JlP93l1S-5d5ikg-ZhUyvM7cN6WpgBUeOm458\
oaaeJtRG6YeaBr7l_qNpmqS6BXU197KR50hmVwnCV_v2JEsKOqflKkafhn3vibE--ItH\
XUiXu-axlVAodXBKcOF_pYTHZe_26Q1CECQxHtg8MZG5NMcZ_ZNUohizSvNj_x5wtAR4\
gaiP-eiU5vNMK8p0ch_NQ4BNw5iNIdRaJnLsQ7zsRgiCQvK0F_Zk9OXKKJdAtbKrmw2P\
ALBijJE2IdIAgJyafqu9U4jFCL25aNXmV_SgHkFhDYB6Y8e7lPcWMOzbfmAMwAqETBqg\
ifVHYdtRRroREhIWZRdfFk1BLSboPBi32JYjUwBa8oGoMPaWKgqRlIuoYRFy06Kgxq2p\
qiLYMZdU..yvdUQEJ6vubOBf7_3ZTn-_jn-11RxwmNp3mGRlolntghI5Sh1EJjnhRBsO\
KhP5AoRdCesJhI--Cpj16sCWdF6_wBTFl9HLRJ5OrIK7u7ew63eGBF6e3RMvYya15pff\
CgL0LNDMr4wRJW85_ys-k-xSgCI75IiEMdUd1VubrN-xmbGvoSoENhHdmHvdV-Geq4le\
qPnlx_9yPe4tOZM-QR8zRFrJPXhXDY-pPHVk0ZUk38J7UZ_1WSsyGEL3Y8lsFM9RyjBy\
MRG5NOBPy5-yfecIHidLgoUH57JqSQRMu1Us_cyvriYFMg9L6gAVpScrJsLrvlyLcqEG\
t4GQhPuYJ-1ObQRA1sZO7kDZSL-jOtaYVtkx9WXGyM0Qp5JprkIY_hhw.
```


Figure 27: HPKE-13 JWE Compact Serialization

A.10. HPKE-13-KE

NOTE: '\' line wrapping per RFC 8792


```
{
  "kty": "AKP",
  "alg": "HPKE-13-KE",
  "kid": "OJo7M3Ej3shaFw4VdozYxtqoGXsMA9TDkwy4Pvn0BCo",
  "pub": "h3uSp1uJz_gkIKvKFSE-v6IM7SQ3hRZpDpxr-3Wym8lDvzRM6yUrOOzPQK\
    FtUcU8FwxhUmVlMneNi7MenyAW_AyZtkaCAhaZhWRUGnUWcCNZkFO8K7yNU5qX0K\
    zDE5IlybiUH5GpXWrLx5fNqFU7BpzCe3K6X5JHdLG-ScfOVfgs4Eaoaym4W8oGLx\
    pSrBqZ_wYhsSiGCdguTIWfu4otmFMyaKIY46uzRTR2dvrEH1eZDhUc_lsULUSGS-\
    IuwEyBI5VNHgJj0YRuxEgU92WtFLlaRigckszNR6qrn3QgQZdC_Pk74qWPJlpbMI\
    hs-ytHTqZhi7RluIUeDMljOSNMNMw7nhe6lco61sSDirK4feYFqCcjMioL3yipPJ\
    kWWlV31MM9izaXGSUhroNdAkwMCDaUgPWN_8de7ZpNTIcnc3k5IcUg1qe0P2mYbw\
    wJkPDK5iKVscqdJhMA5wUK6bO6VbslDJIhfIp3a4tes1FFiDQtrTBtz7vJAMM8JK\
    BEy8nISMfKM9ZRu3F__UvDFmskvdl-YMdZ5SxCt4B4HnZbd6t_MzWGXZoFqOuaPE\
    ILzhcenNGkUxldIwfIM9UKVeGuYBNrONyef_BuCpjGLCU0RwVrAJExLjogO_ukK2\
    ipHMuA_eAB_YNEaQgarKQb-ZpojrUZt8XMSFM2dATITGHOIrkkBQFmIwHQfCR92f\
    wmz1YzRGUhHXRfjQGF23g5u_IEI_wPComPAQE3h-hajAA9bVxikYcmgQyUb_EXXz\
    RdJeVYC1jFWaMiR6RwX6SsP-fBiIIxk7dUhAY0XXlJgZok2PUxLuIqroV0X4A2VZ\
    MZQmoaFAu35CigSeo3kXKW1UkU6KGKYQOA05CnsVJ7JmJ2hiJhXfFP4Zi77xSQF7\
    SoxQsi5PqzuglA2kg2MRkq0fC2HxGWoVOe7yWBTEAvlvEHvbgo3lup8MUCsppEja\
    QgJbJFOilbpiV7bKJH_SCkDfE9LqUULeOykXV8tpaRteewTdZQzJiVLVkLpvQlVJ\
    QqGoKbC8cXD9UkPAJBD7ASEvvBYSqlSMIycHunJZdkzduGvJO-O9iVlmtgisS5wp\
    x82re6IzgT1bsniBECY4l-AFs37tuDhJZQp8kOulR4icCcemyEzMciILI0MiEB_4\
    skaXmFY_m6ify1PLs_ECRZXbWmYRZO6TpiBlUDgLSiwgVSVUIbyAxL7LOiVZQ8_5\
    q_xIeIsyUqYkcecGSdUsec7MJInYQlPJKT7WslMAAX3zl9o4ubt3aBXTe8pSV5uz\
    dNVFSL8rKed1lWw5BkT5qiJSYy0EvDemY7MUeRgpwntyDFHRSD9-Es1OfB84tq2Y\
    peHBR2g1GnbaEmflKb-3u20eB9SQhrHok7kwl_OSCEm6ELjfsI1rmxXbxl_ak-AE\
    MZ_hu75Myrc-ADNfYWexmRJZFWtCY1VJHBGjKVb8eY9upzw2PI1bNx1CAIkTQtYO\
    Cbi3nK3EFSgdVudZMARbIgPRcX1CCunFgEfTgRm_lxEcq6Qkca59JcfWTAF4SOdB\
    oi8jQn-yoTX8uZrLqqH2gCHUuTZ8A4nBULgSB8Z7sbdNB_lOdyn_yrFpACAEAl7a\
    J6MWhb-tPCJ8BSh7Qw1ypCWzVXhVScReg9ttkL0sMGYyyRI5B2dgepYJhVMLwsQA\
    IgdpfCGSEiTWSs2TpLpVi0znww9QPISQIa2pWN8Ht5PSW-iyefVdMYDosDzbOoQr\
    YNwVdhB_k6MhifKpKOrzAoQZYKdwg0krKV7ftkq7pQ-9Mc5HowjMmDfLhltEAJHt\
    Vtbzy3nnYI0-J4gAa5iHs26UC9IQEALFk2Gxx88kO3CPu3SvxGK8zD-jlrgvMffV\
    NExgpimqghNzyQhPMSw2AeA8U5_fpF9cbN0UQJx7t6gmE1c7kkepNATRecEeesdr\
    vKklyxuRazI4GL7qlKHUykktTBwQQfhNo_VMVArGSU_gjM-VaWIEJxefMJnQFsgq\
    Q0ALvBAsx0HCK1OcUkIuWaafccK2yKv6Vvf9wytulxiXknDkhMV7gTWYKcuHWDYA\
    JqezqBlWV6yvGGWkGqWquq7HwyPY-uATVbu8mdKz_H2sgmYdQ",
  "priv": "TK5a5VLDLOMcxsYNS49vGjawNMMl0Bbm846PPVwPAKMvawmQFwwVBD-Ot\
    hN-LrGWW6f-d2jz_RlIcnSPhckg5A"
}
```


Figure 28: HPKE-13-KE Private JWK

NOTE: '\' line wrapping per RFC 8792

{
"protected": "eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiT0pvN00zRWozc2hh\
Rnc0VmRvell4dHFvR1hzTUE5VERrd3k0UHZuMEJDbyIsImVuYyI6IkEyNTZHQ00i\
LCJlayI6IjA2dmlReUFxSHZ0WE14R2lFMmw4NzByOEktYXRLOU42ZUVhcG8xajBM\
X2dGNEp3MUF2Mjk4SkpVY2VHemh0RHMtSHhia01LS0Nsb1JHUU1rWEN3N3VYMGR4\
emR2U3A3U3VYU3dDcmdYUEFXSWdKMVUwbVhTMFAtNG5XVjMyT29xRDlMOEFvdUc0\
ZV90bzYwNV9RcEtiSjc5NkhSekhQeTBTODRjVmk4WVNWMWpCbGtlbnZSUXNEWHEw\
UUxYRG9xd0ZNN1lmRjJZLThqQUJRQ0UzQ2J0T0JYdi1SZ3dSN1l1ZjB1VjFzZHpv\
S2luM0VQTmoyMXZPcm1iUS1RSDc2YzVwR3NRaUlpQWRCUkpud1JhRFJJOE5kYW0z\
MEFNMWVQemZ6UkVJR2dvdjhBSldaNUFWb0RpcTFSYmR5OE9PQm1fRm9ZNjJzTmZa\
cWNIWmlnS3czcS1EeExLTmFpaEV1MEYwbDJrQ01BckJ1WDFycjF3dHA5dC1DQW5m\
ZHhlazZlWWNoazFWOFM2RjlEMWFpUEJXeGhoTzZxRWxjMnZNYnk5eXRyTGl4d0t3\
NVBVaWYxU1dqZEh1dlhnZy1MZDlyWDIxckhWc2NJSWRMMWI5anJxSEpjeENaN29W\
amFiV0JpeDZDRVEzZkU5RzJTRGFTNG1uemxHQUphM0tmY01iQnU5Sm1QOWJDTjFQ\
UUd5b21iWUNLWDZqSWstXy1lOVF1YnFicVNYVVVkNlMxU3ZrZDdWUmNZdHVmb1Mx\
aWdINm5ET2UzZHlvYnNYLTJNTHVndlhYYThxT091UzR6eGFaMVA2LWMyalg4aG1k\
M3FXSGpOc2YtTDk2eVFvd2gtY201ZFZ6MHhhLXpBQy16cUYxOXRGOGQ5dmdVQlpN\
UC0tUzU4OUhpQVlLNG5MZk1CemxvSTRCR3pDN01hUElKSmp6dWJZWG1MQWhFYm0y\
dzdtNTQ2dXNtaUQ2NTFPUUcyVkFMM3pjQ0hBQW1RLWpYalAxZUJKZGhCMnFFZjdF\
bkhCRzMxY01fNHF1Rmt3TXNILTVnXy1rQzJuWmdOSW5HNlBHdXlTMVp4X2VyaUJX\
VUlNOXV0TURtWG9UOGN1RUxiMnVBODhCM1RGN1BCeDVick9ZQWlIUnI5LWI0dHFm\
UXJ1UTlvcnNHaWFDNDdOazBid2F0Q292YXl3UXhDR1hieVU3QUE4RUJhSm5UNVNT\
V01PV1JBMDRLWU1PTFluX0MzazRUUm1ib0dpR2tjX3lfN1pKdGxjTnUxVG1xblJy\
SVRjQWtQUDZNZlJxa1pOTGlUMWVQSElaSlp2VWV6ZkdMb1cteUFKQmptUkhvRGEz\
SktqQmFSSVQ2V3dFSW9LbDBTZC1Gd3VBNlBnV2lsaV9yRWwwbHRVdWlmOF9heDJ4\
RG0zRnpCc19sZFh0d0c5MTZsMHVwWFYxUkdwMlZmTlc2ak82WjRRM3VVbU82eGtn\
Uy1VVklwbnFMdFlpek1lNWdCb2Zhb2tMV203bVotaG5VdXpwNGhndy02RWp3TlRH\
WXp2dExseXBRVmZBM1pnZnRsVFVRYVhISDRsOFVHWFYyMTYwdUs0Vnk2bUc2WEIz\
bTJLekYzczI3cHY4Mll5dF9qdFZxdmNfcDYxd2RpUkd2a0Y0RV8td2w3eUZaNXpq\
Zk1BRjgta1FhZ1pTLUhWbGtTLW0xUjY3THFkRjlRcnNmSXVudThFSC12YW5zUlhx\
UmhUTjByXzRGWGZoLTE5Y1ZjNHFnem1IVzMyNHNfZUxWa2dRSHVleUczeUlyUU9L\
TkdwbFBjWWJFVmpuS3pvMUc0WGRlQVlWWjc3YzUyTGdBbTBlZnkycFZMRVBTd042\
TnpXYTktY0R3bHJDZEd1dndzN2t0dnpUejk1czZDRTAtNEg5MHY5bERiNGFDREhv\
VTJiNGVoVGl1QmpSNXB5V3JGMGRicUYyTVFMaXFqWHhmOWNzWnduU0U4Nl9TdXNh\
X09TUlZpRXc2VzVOd2RoeWV4UnhKN1lMazVoalNLanVyNzVVUm5XQ0VpUjFiNERh\
SXJ2ejFHd0xES3Flc0lWR19ZUEtLY0NtdGQ5VEJPNVhFWFg4TEFwNFh3aU9aT3RZ\
UElXQW9iTHNVVDhZUDdUOHZ3MlJCYjlyeFhkZzg4U1pGYTlKaHN5b0pmRllXT24z\
c1BEWFRCbnJsbFZhQ2tGVDhScW9hb2lDS09VUWM3czhfS1ppcmxGZkNyZlNLTVhh\
VFk1c056RmxXT0hyWmlMMjlYZHJrZHl0WVc3ZExLWHZKUnNtMnJfMFB6OEZpc09k\
bXZ3LUhOalFKM0dRZUY5QkNIaUY0UVdpa3hsSjMyU1BjQVZRRFp3NUEyQlE5SzU1\
M1p5Yi1xeUNlUUlqZVNMcWlXQnFhNXRyNU82cGlwQWlZWU5GMHRIaVlCVHNkbDlv\
dmJtdnZSRTd2S0VkMU9XUkstV2VvNFhHOVpJN0w3bml3TUk1eG5CYlJzM1NSUXlZ\
VGNwbUdjS2dqa1pmNERhMzltRkxISy1DbmwwYzRpZjFwRm5IT05CZEE0NHJzR0Rp\
N0UyRUZSSVcyOUJvZDJnRDJWeDJrTDhjQWh0UF9ObnFNWHhTeVZkSERwaHRiXy1Y\
ZEsxSkY4LWJ2eUJsTkxVMDNENktZNHRtVVBmT2U5QkF0bWx6STVPZndRRjNUWC16\
MjNfZ2pzcjI3WWRKeE1lUWFlQThNVEZadW80Nnd0ZFhVelJ2ME0yV25yaUN2bTlB\

```
      OFM0UG0walZyalV1cVJ0SjRLNHhMbk1GUTNkSWdIbEFqdyJ9",
    "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
    "iv": "4kbBObrz8_rXvess",
    "ciphertext": "rp61DElcDQKgF_QsxMP2YsdsXLUdFiBVV-FcfEg7rf5Dgny1s5Y\
      nTDs7d9Y_TPwWXEIhIUmPrsSlSd2VJPEmzW76oY663xchZ4VfXyQGHV3wmBWAIpN\
      m1rm0cIUgFJMUIkGsgGiFCs2mLhzQKpASFzzA7Iwu9jxnryhw01dMc9xbOYJ_fNr\
      MWQI5aepqyQKQcfCkSU8f_FSvp9NQypbd1jOf773NFk-vurwu9mg-I0P0UnIWcRW\
      gQpE6aXzdxZ3f8VzxxTBjpPw_HertfqyW0F-YfR3nHXwqnrItH1oY3NZWT8rPLuj\
      EqG4U5RBUY6fbNUiPc5FQCNNseTRUCWZNLFoLKQdHL4rd1IVK3MXMXuD0",
    "tag": "857uXyIeZ-VhuBmOFb6Y3g",
    "encrypted_key": "P0RlHe_TVfzgUj-hqTTlUXJgMpX8IJ6VY9sM_IWoAj9D7mEV\
      C6Hrha2xnIeUOp71"
  }
```


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

NOTE: '\' line wrapping per RFC 8792


```
eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiT0pvN00zRWozc2hhRnc0VmRvell4dHFv\
R1hzTUE5VERrd3k0UHZuMEJDbyIsImVuYyI6IkEyNTZHQ00iLCJlayI6InZjaFdSM2Rw\
VTFjNUVnYklEVWxtNWVUVnE1TVhJWXp1NkE5LThCVGNGZ2RWR2JOMndOWERsejhNVmVu\
MWFjMklPMU1KX3Znd0ZmNjJlNE5NSVZsQ1dCbUdCTmtYWlByaVVoWGhxUW03UjA5Q1Vj\
Vm1CX2Nud1YtYnpHQVIxcHBfS1cwX0xsVll2YzZpSnhCRGtyWFdOMjJLcXc4YWo4aGVV\
aXVPWXltbmQ1ZmxYZjRzWjdhOFc1bk5vVzJqOXRJNnR1ZXlDSnJsNXZDQXRHMjVDb2lq\
T1UzcnczaGZQdFdlX1hyRENHa1ZUbUpBQ00zR09SdC1NV0xHaDlxeklEM1UzMGhaQ0NS\
MXZndWxETGhGWXF0cWFyckVZSkFPYTNEaENUdWN4ZXc3ZkNuelhmQTFxRVMwcWJoTEs2\
VHA5S29zYnp1TmE2TDlPQVRTQmhFbDNjOEZydnhwUU8wY0NDUEljWmstcllhNV9HUU53\
cmpDTkdfMGFiVFdzc1c3amlrUUU0ckVwcHNDYk0zamNINjBjVzZtZk1WZW4xNE5VY3pF\
MU1EeldlejRiOXdCSWxEQlNoVU5RWmltWFdRWXduZklHSlFiOE1YT1BlWVhYQVVPcEtL\
bFFocjVSZEFyTXE4NGZOY0x5RzdjMUwydENSaUNjLTBWZnhaUmlEd0dNZms4UG5kY0pS\
QzhrUldHSTJzTTNGdmJpaTloV0JYeWYtRnh4Z21EdWY2UFI2elI5QzhBZC1YRHdJcTJp\
T0dNSk5NWHZtNXk3dDV0elpDNFJ2cTBQWjh4QmlmWHotWWhVY1Z0WnM0Qi11aERuQTJw\
Z2VWMks4Rk4tVGtubXlFd0VVSnNrNDVhZTktMndLaVlha0J5QTNsdzdOZkJuN2diaGI0\
WjhHb1FIV2RYSGJtLUtIbGZiS1psczBEUC1IeVlWVWVDdGdfcWVPX1BweW5Fa2tzOWdX\
TmpYZnNXSFFxcUVNVmZyMGRKcHJKeU9SSGtzQWFSdEUta0VvWTYzOUEtanpMTjBSdUZK\
SnBkQXpKY3BkWHRGMm5KQ1JYZExNanlHV002WmZsM3hXa0ttV0VUNmZITDdQZlJKRWFU\
M2RRR3BBTWlCRm1DTTQwME8tRmo0MXNndUJabEF2RUF5VjZaNjRpalg2dHA5cTI2LWJx\
d25RdUZBMU1OYUg2YVNRSXJVM0Z0ZWI4Wm9MR2trWjJCOEZNRFUyT0sySDNmWC0xd25z\
VWpya0RIZDdrMU5XdDdzdEtKMUJ4MzVFUzEzZUc5NndRcTZYb0FQVXRLUktuTkowR3Vq\
OTdjcTRkUDZjaV9RWFVKYld5ME9jdWFtNU1KV2hCdktkdTZDUzhrSU5WbDdndFJQOHZK\
RDg0d1VBNFlKYWpwXzd3YzU5UkdIV1FRSmNXS3duS090TzlPUDVTQTgyLTBucHY4Tm5x\
LW1PU21DYi1hZVh3SFBGSkNIZU11MUtoZmY1U1B5ejdaY0EzUDVzVGZISC1DOWg3aTRV\
UG1qWl9lek5JNW55dTZqYXNIVkZtODZyd3pUWmZGVS1lbk5iMmZUcE5DOC1TUFl4R0xV\
dDZZOEtJV1JmRFpsQ1VSUy0tZkItZEMyYTVSSUtFSHg0VFBfclRwc2h0aVFPcGhWX1Vm\
MFhfX0l5U0pyeVNxRjNfSTJMUm1wZ201ZjRDWVJXRTJmRnd6QXJWVW1fMTd1ODdGVHVU\
c3k4ZThPOG9Fc1lKQzNhSzBhQm8tVjJHM1hpS2J4dk9fTE9WOGk2M21ETkJUM2Frem9t\
M09lTFFvR2dhbWI1d3R1cXJyTTExQVhPdERZOGI3OHlMU3Z5dlA5ZjhRdWhBQlhCYlEz\
SUVVNEI2LU1WVlpKNEdDZ3FPdlc0NHhOS3Rnak13SVRpYy1mMkhaakdUaVBkMmlnNzd0\
```

```
   SGVlZjM2UDk5SlFHV2ozX1lmMXRVVmpTVDJ3SWNGSnhrYWVIQ1pqUHY0aUoyRTJ4ZjZO\
   ZW45Nk0wVDlkMGszRWhDdWtuX05uWDhqX0ctemVtTm94ZVVORHRpT00zYzBiTmNMVlda\
   M2UwTFVHNFhOeEpqSnVUdkc5ek9fVkVsOGdUV3llbTExOTg5ZkhINHotQWxlYl9ZV2hf\
   Um9DT21GOUtMUWtnQ3hwR04wZkpJS1RfSVJNMERieFRKLUxVbFlDX2RGTjEydjBDellN\
   RlROOU5FQUFmdTQtaV82c2lyajdNdjZRUkg1X2xMVjFRSjAxTldCcjdhejQxcnBBRVFs\
   OVA1cXBIS3VhU2dNM25nMHBIc0tmLUhSTFIxV2J4VFVVSTFCbHpaY2U1aTJORWtZV3l6\
   ZFhlQnFIWC1fVUdUcXZQTHRNb29MSHd2dm9vYmpXa3NqckVaQjBPZXZGXzJrXzlIQWM0\
   VzJyOXdLclBNMVFSeVYxM3lhRkxXS2NXblRlUHNRQXJBMk5RNGtsTGNxR0VQRnpGNUxM\
   NnV3dFdCZU5pOU44c1R3XzQyYmNIVEc2LUlCXzFMMGZqTEg5X0ctOTFxeWtYenpjYjBk\
   eWI5RVNuOVROMHlhQVI1dTQwTXlkVGJ5MlMwd1RQTExNMGt4VGRTMUxpdG54SXRFQVRh\
   dEFfbl9TMzlIYlFMMmJFZ0NEUXBuUU9VaEFEU2ZVdGdJQ2lYTEZuVzZLX0Z5ZnhtdExh\
   Ny1pblpLdGtLa2J0NHp4LXJlUnBjWWI0TWxuNDYwYXNzMGVuYzFSMVpOVUFPalNZbjdY\
   b1Y5WW1qZGhhb1BLUTJEWm90UnFqeXE2R1l4SHh0R05LbnVNOUNKbVFBMCJ9.NblHYeR\
   4VJuwv8x-oDPkCG93nKNQBwla3QWw5eb_HEhPRn_wTVPfolDTuFk4LXOC.pmOmnDiJrW\
   0Wzr1D.cNEPZGEgnCttzsihzRc14vw6ZMWDSU0VK3AJqGHhCyffGoR3ZigtJVy7wG68V\
   BtEBdbe1BtTbXtP6E662zYJXybH48g23gJ-SlElmunc5aYGLYwPwctIQZHW1LUiLOcrs\
   R1XDzCIXN7T3TqCFYmPEDDeaseU4y1jL-Ho_dHvkyQrc7oOpE9-y_vbl60oT1mRBH6YK\
   roErIcilFoxxDpBWraAIBL2herQij9GCkVTg5tUwkpnaedDhFwZTHMvf2mmfn6v5rC5E\
   OqKFZEtQFgpPJfzDCG7_wNwLw9QI5RYtfTm5SlgFTkY-YnvDQjNgMmrV8Tfzqt_8VtgX\
   bQ7FdrcrTUXeRj1SCFWDr5g2ZbBW240.JQvmVqR8rT6QqANUI06G8g
```

Figure 30: HPKE-13-KE JWE Compact Serialization

Acknowledgments

TODO acknowledge.

Document History

draft-skokan-jose-hpke-pq-pqt-05

* Folded long test-vector lines using the RFC 8792 single backslash strategy and added a pointer to the unfolded vector set in the repository

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