Javascript Object Signing and Encryption
Internet-Draft
Intended status: Standards Track
Expires: 12 August 2026

F. Skokan
Okta
B. Campbell
Ping Identity

8 February 2026

JOSE HPKE PQ & PQ/T Algorithm Registrations
draft-skokan-jose-hpke-pq-pqt-03

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/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/jose-hpke-pq-pqt.

Status of This Memo

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

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

Copyright Notice

Table of Contents

1. Introduction

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

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

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

2. Conventions and Definitions

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

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-P256 (0x0050)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-10	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-11	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-12	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-13	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)

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 construction, 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-14	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-15	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-16	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-17	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)

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-P256 (0x0050)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-10-KE	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-11-KE	MLKEM768-X25519 (0x647a)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-12-KE	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-13-KE	MLKEM1024-P384 (0x0051)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)

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-14-KE	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-15-KE	ML-KEM-768 (0x0041)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)
HPKE-16-KE	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	AES-256-GCM (0x0002)
HPKE-17-KE	ML-KEM-1024 (0x0042)	SHAKE256 (0x0011)	ChaCha20Poly1305 (0x0003)

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 [I-D.ietf-cose-dilithium].

For the algorithms in this document, the "pub" parameter contains the base64url encoding of HPKE's SerializePublicKey() output for the corresponding KEM, and the "priv" parameter contains the base64url encoding of HPKE's SerializePrivateKey() output.

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.

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.

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]:

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-P256 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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-P256 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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 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]

6.1.6. HPKE-10-KE

* Algorithm Name: HPKE-10-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]

6.1.7. HPKE-11

* Algorithm Name: HPKE-11

* Algorithm Description: Integrated Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.8. HPKE-11-KE

* Algorithm Name: HPKE-11-KE

* Algorithm Description: Key Encryption with HPKE using MLKEM768-X25519 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.9. HPKE-12

* Algorithm Name: HPKE-12
* 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]

6.1.10. HPKE-12-KE

* Algorithm Name: HPKE-12-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]

6.1.11. HPKE-13

* Algorithm Name: HPKE-13
* Algorithm Description: Integrated Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.12. HPKE-13-KE

* Algorithm Name: HPKE-13-KE
* Algorithm Description: Key Encryption with HPKE using MLKEM1024-P384 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.13. HPKE-14

* Algorithm Name: HPKE-14
* 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]

6.1.14. HPKE-14-KE

* Algorithm Name: HPKE-14-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]

6.1.15. HPKE-15

* Algorithm Name: HPKE-15

* Algorithm Description: Integrated Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.16. HPKE-15-KE

* Algorithm Name: HPKE-15-KE

* Algorithm Description: Key Encryption with HPKE using ML-KEM-768 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.17. HPKE-16

* Algorithm Name: HPKE-16

* 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]

6.1.18. HPKE-16-KE

* Algorithm Name: HPKE-16-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]

6.1.19. HPKE-17

* Algorithm Name: HPKE-17

* Algorithm Description: Integrated Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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]

6.1.20. HPKE-17-KE

* Algorithm Name: HPKE-17-KE

* Algorithm Description: Key Encryption with HPKE using ML-KEM-1024 KEM, SHAKE256 KDF, and ChaCha20Poly1305 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-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-03, 6 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-pq-03>.

[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-15, 30 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-jose-hpke-encrypt-15>.

[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>.

[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

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

Appendix A. Test Vectors

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

A.1. HPKE-8


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


Figure 1: HPKE-8 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82bVFRV2R2M0NKX3Y5a1
9QSDN2UzdTMHhvYWg4In0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "zn5k3HEI3RkdpXGGdYM2Jh-dKMjpaOIOdV0ktJYiT_4ZF7hoHGIxdvtRi1qFccO0Sy
y0nGCqquwQXTiGvVXV8-xM51oP5ihdfMezPX_vBMpaiG-9e9uWKnH9iS1YeXXKNwTXqRTlT4Y0gVmcQ3PC0-JiG3t
FfxWUd_njQMJz9RBLS6XxFxh2huK_z8DdEgBJiE00XOwfmtzradLowkaOrHDMjLmkDfj4izxI1NplLAGl6k2-iw1G
VBP3GOZH5oDxwdo9pzGccHxifsnF3mT5Rpsr7hOVn-JQuWRVB7ym-DeIJhHdtttknxfh_n6C1oKRgC9wD6kXu3N1y
I7Xrya-ZTt-iL8qyDFvj-s84V6qPWTVWzX1hhq71isintPZjvp1wB3UQRhqQLd1Wmg8S41-FYcogbR2GUdzH6utB2
bZK-wz3k0jL5pBsk_waA08h6wyzfRoU5BQRhWb9umI61mF4FOhW6UoNX6NsNzdi8Giqwskb_uv_yNG1Tvdv1Ima0f
8A9uw2RIjLs1L0mVa7JHhawhT6vgLixkNqfQ-n7QeADWygm9M7Yw3wKV4GSeNy4daLK8k-DWwoxkURfKrcbU5azN3
8bcDuDlLXpwn6faiVzMNmyu6No3b_jp4tdfOd5VZKzRyNWWHSD84Z58GQEnS1UaBgaIP1_VSgY1__Bf7PWCv0qVgY
KgLaDv_TiOhC4n-wRj6tKgbWnzcjx6R9pSHYvtP-9lE1cc7__Rceuw07HZzeUs2vsTVmwFThVJ7jJDo4ixW5Ceh-W
evI0CYO3KcPGS91maeQmJglwIRbzjZ7GdBLklxAEMVDM5fDUqPssInVScOSTueAXaieOwhIelszsCsYK1bst-hgdH
dNmJyYPjRFkXnagb8oftbOaePibhV2zi7o6f4XMn_4UHnS1rvo8xVUoN9s0vbPBkFxzgifn_cf-kQlXzj-iZZ56IJ
Rcs5v8qZyDFjjOzzjX86ST22Mn4ZcDeySRMOPIglvNrCIxDNj4YCoGvU-FzrzsHhm3euR0b7-fwvM7A0xD3i-Gvlf
DlZtolHRMSit2XSdtsBZeVN4P4KIeeZ58OdliTwKjSp8cXC2OUe-_q6K9hccfwcg4xYY9nEw2iPVp6rqDF0EgWlGi
mVIhPlvKsV7evROs9aVmTeLni-u6fgt0KOjaGeHmGS8beEPUwHCclUk2SisJZvCyOPswoT00HJGqc6EVYNGt9_gK5
qKHuM32MEmEls2ZHMg7kvruTEuHkSahtqrMykrV_77q0xgbJbMHemc4u0rpK8Qgg3TloxHWnBHxZAKhQwb7TYg2_c
rEj3rY2ninenA4iO6Yv0Rhu_UmI9NANvRWPzJREhVFS7RMwscG2Ep46ezHWO2b2QtzyBIaUF6rvdeTSzPwmrUX_qN
r-ZQMkuwhBoAqt_nK4KY6du6yPBF1mbP3RhZoOoB1R-yHLoLxIEM0b5aSInfikgqDpAg7YC9bXGbO49jdXjFoovtN
tHUciDHufC_oNizbAFSM67xrDKwHdp0VK0zPiptJrz39bC8Q",
  "ciphertext": "F1VkyLk154-wLPTIPKKZWBlbhot9YyF-_kHyXnRTsr53qgJwE4SqSmz0GdhFOTch0budM
wlZuLCoqjBa2FEnjGdPCbCsKC5MVlRUvFUBxDS3FI8NBF_R3Cj87Xia-luFwrSV8brW3p6IDobEmJVGKhHWax7gKZ
Mc-nvUkfG88qcUwGH2ltGQUfrjoNP2tMYdtxdwhyvtx7qCoDJnv176Vp-ySAgjnzSZhGSe9_SPooqtSX86fuauADV
```

```
auOVVTHYJlzUv8Pb0bBgrA2PKhuEd9YvCTHTkCTrczJFmQJit_KQ2k50e4qo88KuIMVdYHeAPzyLwyRCYyq_2o5F5
SjxlvCqsJ-XixQog5EumMz8zVSnUmvAQzCgGiolNOKro8_Dypg"
   }
```


Figure 2: HPKE-8 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTgiLCJraWQiOiJEbU9XUWktVndyalpXak82bVFRV2R2M0NKX3Y5a19QSDN2UzdTMHhvYWg4I
n0.dfD8NhCXNZzcHEudD-fYyOnARkPpCU85i9xWYK8FCQlxF38Cvzxi7vf5lv2zicOhiJPBtapFfajU4QSVQ-xpN4
7BG8IKdroWUVGg964RgmxYHjetCi-DlbmeFCVaPlLieycvxuEdWmmUaL2g6lWmc8bqSo27tatK8ZLxqZKBrGGAXGV
pdtP1MgjxKYpd12o-e7Lu_tjmYA6z-ws8LvR6StoNZD5oOmuAUwJvlISQ_LIz5y0A1uETSaKRyvyHORFRr7PiNRA_
kSv8zGsUQFKdKCVXiVawylU20YSbBmw5tUeiOEfOp7McsHByWlVos75k2oQzd_HB6ymPaCp2Yo8CpaWyklb7YBup1
5Csy1bEgawr2pGdohxPMTsa3SmHOF8a4hYVqUjxK-8V-2Tshm9ZdibmhYqtqDuYW2EnRVTWKTrIXr7YBF5WTaxAXh
Mg-8txtcMEYA7kJwBSSU39uMvBZE1wS1N-rYwCUaVecjWeXRWNmpO-HsxIliUy5cRbpWCKUhTymGHxJOX5jUsCPzD
WQvDXRBLDT_-JsgSgO8UZXic8HajfhBTxj-zdi6vT6v-uYi9wAvHlp7yL-rBlKLGvI8jdGj0Y4krfYtaeaKa2ZI3l
OLk6IUZGKqn5x1NrZxZzTKbTI47_AZyQcTnuKgcHk7Oku_Nf26nBumWqqz4y4gRVZRPRi0Z0eNsld19sYonzlHWJM
2oYu6vmThmW8uyzXjZr0ABjAL1X9pLxU2IMsgjhID3pauc8J4MazDd1uLuzygBAb1ztDDX3J2YtBGmONxzieP1G4I
AZVAtQcPCuMxk_RWhGK1j9l-nQMgjP0DKSBxVGLutrf9zOA-Myvf8lAGZQGv2QQKymc-R1Gq4uobZGHA92u-8hm3h
AVbFunA8pnQWWJVkRiGckO7ssS-d6mfmgNKoyp8khnprai8g30vFRIoVgijxWCXdkkSDsM-aEEkDfhde1vZxNQpbB
9qld6VjJfVVlpfEkjbjE_RN9sjMGqInAlsxBVFcJQBMTNb1N_3YVuB7l_TKBt9fSdURg13jH8wP0jKybWqyUNIQYb
av9JVT_o-GfJJKw-CtnXNyqDz0INKFfJHT8psTn6CZhsjGVtdR7sLM-ZYblnc6QQwey-mAf5Et7-DDlrRPTPv7yoB
6o6J6cJwtuyhhu-HFxCmRZIpSYMRe8lIRrPUXk3MRmcQWmZf5emPEbEPsEAL0UeT9XFrHFqeIZvGgzpmbJgJn5BSU
arqCcXWX6uAcAdat1nabT7nAHYPXNnxG6-CCwSjwvrvVSdNmSJq2fkwOjo6F1kz3smAUcUhjW7W7iC443oDgY3X_u
YbhYSZUXB0XtqCuWSo8ImoeMxfddgxvdwmfFaHiNlqvSVCkewAcL9Mje1lyagnGtLCqO9lJ2uivnJCyNlPB9A7aDq
pGt9DG1UnmHNHkaj7bqKFD265HJufoEmNG2eP9YnzRTEVkbYSzmvGH_pKXqmTv8HhSSTvWvrpKNSxLwbp-IAKtyex
Cuyjcg4AnQRIqvyh6sMM2qU8ERhA..I440XaEekuepH9Bw77viw84dJoqNozKkTAXuWGcuc0MeTfHXuEnixKkMljP
X8DqM0hLIx7fq_bsM_A-HA3i3erkcMHPL7GKo7Tvgaa3GvHr6Iq6mb0iED4k4_TudWz8dW9762L2jinjdK-aTy19T
2bDUr8Em2Wl8evBRtWaRbZi-LZrM0cuocqHep2A_ghhUVSv-sWrLuYmwvW3tXLGGtqpHnUleG0rYOJozw8Z0Ovs4t
f9wPvr-sOg5g99XuoUKtlADhJEy2GtX7BYFC5XHICt6zcKipt1X9xEDsRh-EgSIcYg1oaXpFzsO-CSfzfSPVhwU5b
ZIKdAF3rpAjNr4gMPsAPY2IKviVQoioDCf_1xyWHoGw7P3EbX8_LmzufHUoA.
```


Figure 3: HPKE-8 JWE Compact Serialization

A.2. HPKE-8-KE


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


Figure 4: HPKE-8-KE Private JWK

```
   {
     "protected": "eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdSYThBUTFNWWZNUHZmcW
1oT3NfNWxJZWpPdXFBZHBzIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiX2lGVGNibnN4cEdoNkZMalBzbFN3aGF6a0d
6RzhJamQ4TEl2TEJFRE9tczUxbEZFY2RkTDh5ZzlrMFNSSmotRjRQQ0tVN1llZ1EwZGYxa1dvSWtaVVRVbzZscUVp
OU04TzFPYllUUmE3NVNzR0xFQ1ZtbmFjQXlXUzFLT0p2NFFUWmdxbDRCZzVlcFJDZWVrNnpxWWpzVWQzbEloZk1mS
jdCdWE0QlNqS0F3amlPT0ZQbGZ3TTRuSkF4c05RV2dFRlhQbmFLblkxbFl5eTEtRE82YUZYanNXQ3RQbGxzbXlONW
N3VXRlc3VOVlJHWWlhTGlheWtheWtiY3prR3lMZS02MjhONmRqeDhSdUVkbUtsUDU1TmpMY1JnWGpJc0hFR1FxUFp
xTkp1cHRSNjRMdFh5VzRkME1nYUNXOU9IUmY2dlFPZHkxbVR1NkdDaFRtTmVzVUZvdHlvWGVXV3RGVjZkYmtoNEtW
M1lINHRBOVRWd1FvWFIzWFduYnBMUFlRTEJ0a18tTm82T3JMMXlIQXNzdnZTTWFORE1xbTlZR1E2ZEdxa2MweG1tT
ExjSDJ2UUNLRXp4MmFuS1RUdEowVXJyZkVCSFdnUnRsNW5zNWJuMUh0bFlMQUFCOFoyclFnY0JwWUFpUVdITnB0RV
B5dVR0Zk5HSUxHcmhwMGNzYUR5aG5OQWNNT1VPOHFtV2JnM1I1WGhQaFF1WXB6VEJORjlYazNqbHdkR1RHZHBLeDA
wT1hxS29nUGFvR1dsVkFOWWF6MVFzamF0dzBvNmJYaUpPTFhSOXFmY3k5WDRwbXJwejYzU2pNSDc0UDUwUlJ5T1Ux
bDhlZHVKN0hNR0kwZEtUMU8wRThYRy02Q0N1V0huN0ZHVVF6bHJzYzhlbmtHZ2JFekI5MzRXbktFeGtpUE5BREl0R
0ZFN0MyUU92UVBZUWlNcFhNenZiMjVrMFJ5SGZ5MEs0eE1VbUNpUVBzS2lWbGlja3NtcXNOTXB1ZXVnRjE0cEd2MH
JZb3VaYzFaUmdRWXNKWV9qV0hDN3IxSkt4MWtyYThfN1FSbFRoMkg4c19FUW1URVpUakNSc1NSbmNkazVnOHFQSUR
vS2ktdF9nSmFMQ3hUbFZiRXFrbU9tLVRqSGU4dGowb3RYSTVWRjVrcGQ3VEN4eVNVeTZNU2dxYlNSNGpFSzQtVXNU
Y2N5NzJpZThQNV9ZRFQ0eTZob0dVMmpKWEEzNEkxcDRpeWhycVI0WlBpTjNvZTBueGR0N0c3YjFJMUhrRFBkNWRXe
lF1WkNCWWZoMzk5aU9SeDVxcDhBenBVRmRHWVEtM0JYUU5tOG5CRWUycWhRYjdCeW91c0lwd01qVEFPQjVCSU9VSU
03NVhGNzBVb3k5cURLM0tVSllNTzljV0Jld0hBVG9kVHpvdGVNR3BuV1NiSEhadkFDQ1JNcXJIMlY2RWswZnRST1J
0RFVEZGM0VlNqUWZsQjNEZkNKUzFjeUkzd1pKb3prdWdMQ1NiQVJsVEFLWHd3aGFqTlVWQndsZGFVR3ZvQ0ZnQ2xF
RXlWN1czb1Zhb0swaE02blk5MGVMYW1BULNtNkV3Rl9jMFR4SnExRUV6dmdkYjVhZEI2aWE3Zm5neklhWGIwbl9Yb
kNNZmFmMmxzWkd6UGQzdlpMRDF2TXVBenNUcm1TU19FOTdKWVF6VExKU2JGVVo0SExuYWpvQkU4MUVuVzhfMFprOW
9lWnZwZUxXeE1IeGpkMkFaTGNicnZiZWszcTNZMWFoSnlfalBBNzBPUVZXR0pET0RmTXctbDFvN0JCQW5zTlNqVGd
NQ09YY2w5RjVKY2hFQ3NXSGFuZE1iS2ZnNzVaMjJDWUo4Sl8zWk11dWtKVFVWSFBQOFFIeWNvRHI5R1VWSE5Ncl9L
Y05ObHl1Q3RoRWdVMzZTUGF6ajliNGtFZTJkVHAxdDBSTTk3eDBTYWZNbzBDblRuYm5hQ2Z6eUZ2ZE5qaU9xS0xha
VgtUGE0ZmNUTGlLTUw3MGs0WDR2LVFNdFNybjFBS1RoRXZxVjlnRG95X1EifQ",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "0aukXUnpQczTtS5n",
     "ciphertext": "lbv67n97TIcLw6LArd7QspB-pE5HLGM42rk89Lsp5G8t8CS57V9StRYiRAJekaf4wOSNo
Yk8AYGsazhkQtyXIqDk3tmrOjffkR06NB8rD1L-i3XFnlP1oiF31qCiKeChvLuQE_KXUTAI84MHxQj4082y-l3y0B
rE4J9lkz6LrxbUs-i9q6mfqU4Gp3pmr08OI5eOtXZgGUSZWaKbpL9hd6G8s1TOrCG_HN_I41Z24m-r_O4KvH3DOEX
dPOQqTHHAwistJM6acBhwkq3GA2thKpIRxVcB9LJCglEiNPud_pxG4dbIYFHSLJkeDsAeuUsFFhWuVFvttbQinngU
nW4yIjSVmxCXEvLiQX3wcWBgSMQe",
     "tag": "a0gDQpq6LklNWWPGgpXHmA",
     "encrypted_key": "RoY6etXCUcUlPSVvM56k3dkyqgKVsyu808d0z8R0fnyXM0PpegK-JIjZLub_8NK6"
   }
```


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


```
eyJhbGciOiJIUEtFLTgtS0UiLCJraWQiOiJjbEJQa3ktdEVsUUdSYThBUTFNWWZNUHZmcW1oT3NfNWxJZWpPdXFBZ
HBzIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiOEl6LUtILVQzZ3g5Tjdqc05aY0RBV0FXN0RHSTdNcGhPeFhMZkhQZ1
ZkblBueXd0MWNJcXlZM1FVbTl1SkxybjZwOTZ6RmUwV3RpZGYtRW5wS0w4ODFGYnlFeGZRWjJlS192MHVQT0IyRVk
4RVRJYUhJNnpadjJNMjBRUktJZ3RoQVFvOG9JSmJSZFJ0Wi1PSDBDREcycXUxOENudllSeWo0S3JSWmZ5UmdlZHJ6
a1k2Ni02bW5xY0luRlVlcy00SVd6cm12MHhzR0pOVGR0YVFWalJ0R0w0UVVyLUowbXNHc0owSW5RSlphOGZYaXA0W
TdESEEzOVpEYWtIMVF2TExtTlFvLW9EUDhRVXBlbnluMDVrOFdBMkZRMkFZd2ZYNnlsSHpheFpsUDNKS3RtdzlpTE
FnSkVWcExZU3JZem9lTGFEOXF2T0F4bm5vcnRvUC1rekl4akx4aml5RlVPUlBfZGxsakItMDFKY3R1YW1uMTRCYmN
DQ3ZKd1YwaXZyejg5aGd2cUZSaFpRX01Ya2c2VXE2WFhlT3NSTTR3SzNRUFNrRmxGWkUtdHZMellvbmRVeVg4ZDEt
R0k4YmpLaHhBLWN4bWNfYWREQWVnZWZtYkRvRGJNaW41UXRxem9KcHB2RHprVk45RVRhaWpUeENRemxyOXFlb0MyV
FNxUDc1VDl4VHFZdkxOaGkyT3d4MFJoMlV3VXIzOW9IcEtVNExnZ0hQc243YTJNMVlPcXJ4alI0TG9yVlZWUjFIan
JCSXN0aTB2Mnlzbmd6YWNKbHFkcXN5SmZxci1EbTNqdGNMQnZuaHF4VHZqNjQyY1VVMGhuMTNMbzE3NjY0Z2t2Xzg
1V3oyeGRZMGllTXl0Wk10TkZrY3NjMWcwaU9JRVpVUmJLcnE1aGNnZC15eGZQRUhfcF94Yjl6U2dVb0lxd24xeGlf
UWxnWkllOTgxQl9yeXlWcVRSS29CQWFnaV9lMmxxaFVsbVdFMERNdUx2MzZHeHFVOGtFZXJfRlVJUGhJai1EREJTL
UV5UFIwZjZMM1A3WmdWVlBsWDdZMWFaeWkxaDNyam01VE55UUc2REVGWHBYOU9lRXhJekdLMnZtZkhRTjY1NFBxQU
U1N3lpbnRJV0hVeGZfbF9peUcwSEpKZUxueVhlRGh2SWxtSDhiU0ZUdFkyWERhd3RhYWJXTFJYNGZzbWtFSzQ4Um5
BMWg0TDNfRWZBYjI1WHF4NnludTY5OV8yUGY3MjVqc1h0ZVdGdzRVdlFRQWdHT2tvN1ZPeGd0MlNfYTRUVV9oQ0d6
aTU5SW95WEw1dkNHakk5aFNzQlpzUEd0bk5qN1VCV0E5WEFaMTJTR3kyaGNWTWYtRktNNHB1UDc5anRGaHlZeEU0S
WJaaTY1SGlKaVk5MTBhSVFCWlU3Y3FXeXF0NXlianhKWmhhN1Y0bW1LR1BpOEM2azlIbWxJSlhzZkFRakgzaTh5Wn
VXU3FJVkV0Q3J5VVNGZGtmcHk4OWhFVjdPY3pEbzNwWkNUSENnaW5heU91Sjc5dGdyTE9xTDNBMWhPbXJNQ09zSWF
CVzlsdGZ6NGJPeTZjNXR4ZFlyMzBXa3pfSzFGX0kyc1NuZ1dobWpkR0RrcWdfcmN5bVB3dlhPNG5PWG5zLXNEcEtf
d0xlaWZGdHVmcUQwQXZlNmRZdzR2dVl2REJLb19ub2tiNV9FeEZ2UWpVMU9hY3ZpYURSSkk5N0hpZkhIb3pZc3Y4b
213dmZQQjkyXzdmeWZlODNpNDNuVlZWc3NHYkJfSHo3Wk5JSElfRERVS1BRTjFhMjFpemFGZjJ5R1ByRFUzTkExMU
wzNzBIVEl5QXJlMWtPbFkxZ2d2cUo1MEtXQ2VHeHVyOUk4NVhLc3JqNW5aQjF2MXJ0Y1dQMHRqMGgtVjVNTm9ldTB
```

nS20zS3pQQThFMFZUeE5TR29KODdKMFpvdDcxLTZCczR1NW5VZE9WZDJVM3VYcDI3WlpUck9FallldExqUWNyazdH
WHNfTmo5dkNTeWstWk1fYWZUbVNvWE9qaHFKX3cifQ.wrUWvWJcDAucAZmzM9DFJ0nnzpqbg1RbkXH2YdRH71s18R
tgNsAI8HoEL5Tl4FZC.5Pe6qU0dQKkv_-vH.cHWwkbsSVMRMfugjYotDWfkQ5cweOEtqkCGSBqVirv43YyNkw07MX
u42at2g1O16L_Dk-8jiekCV1fH2Iqj1FvI_x8b63nw5UGH0baXMFngzdTHH1xWleIZJa68oXeSZSBPMNREqvpG3qU
uHEPa7PP7JLBGK7HqVu8B7-uFo-NOzHqxzLWrjy_XDEPicYcbrrKKHuYkntKJqU_iLHUGQgHzXMRLX2hZEawHAdOi
7O--19jFkuYBktgs-cggvSkFgtOesIs4C90pLiQ31bVx91PbsyWSc3Xb7M4DYQayWqL5Qaw-gZtGSJaOIBCQXexvK
14sPSkccue2Czi1BDMDPv47GyuBSBSubSJxPGoPHvbd1.XSzi1NNTvTIEN5fkULexvg

Figure 6: HPKE-8-KE JWE Compact Serialization

A.3. HPKE-9


```
{
  "kty": "AKP",
  "alg": "HPKE-9",
  "kid": "eb7WHB9a-KjAiddCtfLZx0_Y0LmShdR_ogy2FPlsd9E",
  "pub": "dovE-nonYvV3JQQ9Q3eSbtIvjjBAY2ivhZlHdEoNxIsawjsrJWG-v6VW4uGeZVcmB4EHe_ePHctf
r3xDrlt4VOgYjYyOCGVgm6syKQLF4qwVzoJCBkCI3LJxK4hYVzHJ6oekQ-uijuEeJ6un6iEKSzWJ6tMyltG5h8WlW
WmQnPgkt8FHz5ohoKpfhEKsLgRrNpjBcMhPNbOF60K5wPRL-VhQjbxlQQtomeQCAAGLQwKL8lEF1umjwLe7MdlSws
Z9ixOcHwxuNRKwJ2a7zwWG68C4V4TLVSiKC7I5gRC6mZY1gjFUcoCFAdg1sdkZUviLMlwizIoTpzIITZSo5upD9QB
rMsTDIEo19GWSACIsZhK2rgEoekZ-4UZcd3qazsZgMSY57CZqqfhXgEBqv6a9mntvLRVXM0Ro12B_wtdJvNZl-fFS
BTMkLoRPQeXKB_Vo6mYul1CRKEm37hpMJagk-aZFEMlYSSVoYMmPyEMExyY9xkMCvcESntxljcAHqtyO94w-Wjq33
vOgvDFkv6yu-cKlg-m4NeSNcaQAQpQE78DGTdUovEhNOJdB9TCghNUfBtUMVLiwlKaoEBE2aGovjua1sjcPR5G7AD
Vo6POcwlKujUZBBBpqJiefHgg2BEe9z0E0CTyWprsAnUeMrAihblMK2UJ2xxKIQgF1sXNEPRUJu7Nh4roZ6zxSaDM
71fJfyTNSL9lEZAOxMpcv64iWwmXDzuwHy-C6P7IlhZRRhQaa4htsOjpQ9mymL4UAsii21MHI6kOD0imFqWeceNcd
RPhnTJcdW4NUnOuPTRi6yZB5RdFqBosTTGZrP6sMs0ANCUdimtWo5sayTEMJdXSPLmYrV8q2NuZmk2WAxBszxGUfC
XxWGTRME7laBNkyY4yyWcAOnCavJIObfYC35zSIDRgYxjoZIoyUiEYDj1jBXqVRXBkbtPyU1FZMsxiynQFi0RoA9M
ZoFDRUqdNaJLOabYqKzCsjRicCsSoz8qSLNaeIeNRrslhGEaEOhvOzygBUbvcwtbyB8XUlZcYJnbUvrYZPwgbLbVq
CnPgjfemvxOGXmIHKabB-fla82QAXSPDE4Siw-_UFfrMQPcNl49ethPC_WDS4BkrMZfsBFBGHVYURIyNKa-dwcpgT
XnBSxXq0-vFk2qg1rsQRIOpk5URLySdDtcgpZckNuXMB4QZi3EM2I4UpKJVFJ-VmbridVuUyoIIaDhs1PGOCZxFX3
bdCgXW7DrGg89HI4xW1e6oG6ETMDWJ79UGZFsDIY3NpKdOzPxZB25KC62ysoUQAAeW04hJoh1ufxiss4civNlQhXz
Ox5aOm6kVRjBsBF0YvEwioa3QND8pqQaGuPJmPSyk1_BHI7ScPBNfCiWlWjgO2zYh5rSEKO2sRJ3kkaCcle9FbpyM
U-OdjccQ8g4KFYXdH4ZdDP3g8LBLP0YRnOwBz_PgcIPQbesiH6PuHK3XJcryso1U41OZVPtyyokFBiOt_wky9gxWb
kqxvnvJz3xlbCrqbfKQqWbtROViI6DIksDa0raQbC9sIuc5ihVwkzjQci_PmQLrnryrezp0cRcCuXGQEhC58adU99
n3Ix3tXYRIQ9MH_IuXXZaWhtzCtm4yDSFZ7r39u2q4DsVnMXRDFRPeumDvQIiKi_OVWXPZXiwnPVA",
  "priv": "LNSniTzUEi-OzELspR9-P9T9Bs9wSUEEO8Xv8keGJ5g"
}
```


Figure 7: HPKE-9 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTkiLCJraWQiOiJlYjdXSEI5YS1LakFpZGRDdGZMWngwX1kwTG1TaG
RSX29neTJGUGxzZDlFIn0",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "4DHXgJP8raAFh9EiAZ6Hdd7sfGTjuRGq_bcY0ET5N7BGalXDbqUP0rPVFX3deVdrVU
C6JqZ-Q9vZc_KAxaxI2t2mlmwKWwUZHX-9sd83VgnGg7exhgLUSSwp5O-FyEKgBAfrYD-DtknEnCO8IREPJj9JqIY
REieUKzjHdyergncqHcb3zngZvJW3QsPpTriFelzL_9peB_PhPQonqzaBxCSE2pNq-VPjL-vsVzdBccEUezHiJ1PI
0hGmAdrBh6YChO_VpHVyhytz_5oDeHwD1KJqiuVLXgLQaXHv4E4kJX-lr_GnoWLwGWSjvMftraxYTWnZ0OtH7IaD5
9UQmVRoI2zpNEl0v3y9BAtwVE8PdoUhr5dhJSSc3lxGXekvuU3LT0r6J_KCvqooP5Yr3TBbIRFB0cTH80zR9ASYtb
_PVoEILt2dZu4jiPEi-YVJQJ9KH_zL4THFbm0IUnhwiEOjq3RfsSXdkNER0DaoT11WoxvB8s631EhpiBwjobmtxb3
a5JQRKog-hpBHFQnhcS6bgvl8D5arJxRiHPdowVEW3PFWSGTWvExfegh43h1tlmosFc3U8vHRBMQ4zjQ2xnL8QGpF
Q55b6aUqSD2KU4WEDf2oLqXJwbA_JEGAW9y0Dbwm7jvN-0BVhk-ngvK5c59kmkGRWzMIlS5YXIPCxQ_uo8Q0wavp6
R4C7NNJH6qow-JMFlJ4eW4JA1eL_rkEIZAFhn4z9ll7y69gIS5c-uwvzI14aYdXhDOvhhozsMMNnywTpmG99CIcci
uVP4uSsceYoIhjfbH5RVJHvtsLcWj39Ht1MyM_ORHftcHqCPN4ukGOk0s1o1t4MmQrfUt0mS8exA8WjKKVJ9zsnMs
8kqmtA6p0TBydh5QKDZ0CQdcxAS1JlLwWfcYa8VNJ7vtQZxOuUUJFeQ_Tw_qlj8rnwmVF0eVVgBLGuNqRT191FWcZ
T6POYkyWa7gZ5oLpEv2xFmZvi3KDfOQDLMSWizFJUnCyNsZmnemTjQ0CbQsf5piwVcHDrWnPyjTuw6S2mpQA2NgMo
JqzYjt3opMpYVDDKYD47HEq5Wt82LTcZ3FXuqxL-kfzUH_XnH10sNnTIfWtexdqySDwvvp6n9lEN4p_uzlwoibuLn
55zyrAxXirhRHHFb7vByaGzX2BFtdjXIxI-NE8XJCZFBy9KysXhoAInk46LCJ1H6WUzJjeq9a2rKsHYPiu15FfX_E
ADQTS6y-ewKQo-cJE8xGbZpi152oRKUvIUMgoaWCDHnTNfVOcARHkMoPoBwSWMoJ6DVUknIITLYP4bZXN8sFS1CBG
q3M40FWAVwTkPMbRa8rZKJEWKcfuV2g04tp180yaXK6EJO1RWTwfnSlB1DCEWEJecO3IHUBIy5i8G0Fsr2XLQFLHB
VgjX0gpdi6suA0vU17m64lic-Rijn0Bd8h1Gpf3GeQzCFoUZgwEeA6m-NJO8sGYqgtJx1B2OwBn1odRBAdXa3-f4v
P-96rtM9TsRVU0qj6YDoVQ6SmXV3TCqbKGRerxOc-hujo66w",
  "ciphertext": "SM5aJqXd-wXt8OwqJtfBHxhKj1zbZQ4X8RGFv6LOuqxXrETo1hEAuOSDmYuv_QzSXN6YU
fQj6rQ9C9Q2o2-9-QfWTU0g--EV9fZ-RhUlEWkHeOOWEBQXiPHQ-qBbwyuMRs_wKma-NYYfnEmby7mnpEKb1QTjmQ
_sEJZ4fVDyP1AlJrH9VcVgMvkcQI5Dj9HHNAUjQCXc6K9KK86eWo62FRC8J62_c9IP9MDf5dvpbHf_RHZmHusV8cq
gwgKCU84lVpacruiiBdvAS1YDpR6fVrcXY55E--zSL0Yg0wCLIQVSFBESrdFdpBO9Gn7mCVLgu1biJmMNcX2tpFdk
```

```
b3jOAqpIMoVZrBrHsb3Xam2TNqV9EW04s9pCortCBKfQEeFtLw"
   }
```

Figure 8: HPKE-9 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTkiLCJraWQiOiJlYjdXSEI5YS1LakFpZGRDdGZMWngwX1kwTG1TaGRSX29neTJGUGxzZDlFI
n0.YixiKg5xesnjE6mnMa3ijN9qVtFF0edAZUpJjibK6VGD7pmsmqsHPrAtvdyVCP6qx5nmk7WC4RT1RcHvHZ25wf
qkLFSaK8y1zp4n0mLBnd71rv5X1064_8kzoLFgcQr9uJHkV4PHbI8hBp8hxydgAf2uDw4BCj8M16PzW2pTPg9KQkm
RUDfyB_PopArYr0DtXgecstqypcfC-UuIRWK-17bVUCvMRME4kzcc_u3EO_MrT3uCZDYdPzQsvXDCnT9GP4ReX-BF
_wzSH_oxSC2lvcB7ykCXO64i0jROIsKMIT5qa-D8BUCXBeEdZ9KUf1sQnKPyrzooLmwKblwt7MU4_KGPWug_tETJU
lNze6NRqSsAPTv8ySUQfhWmQxrwupI1vuI8ZK2kO35g9lfCxQ5XREmvlKQHBWpB82cCb5HQvGlKHi9LVnQEiuP9-3
1bZrr7EKwSu9LC7BiVeXMGkyVtPhad_q1VS6N3NF8gjsvyl56U34ze4dpqDQdb-rWMev9AQZAF4gTEBh_kx0rnqxG
5otBlH_7zJpqUpeBNKVdZLpnfE9Yqo44qKcQxqgMxAYCCKET3Lb_rr_gJZeQ5Uef2qggTQmGv2zDvyxjJVK1g2joT
xnlIbXW6pev2jVCvg3S0HrPdbdtL5vK2oL5_18_PxKF-39jAJdrX0AC130lj1dInHB76WQuCWHbt8gAcF4CzELWe4
lTRlV0Ft3afXnntUSr_JLJn67QzDTwnfEI3Kj1q05ttGETSiaOkOiQ4TujC9koDebM9y1jrnr-pvrLjmX75zC79Kr
bLvigg0AzihmbnFdR58IQSZ3Uxja7lxjVOUe1QOOs0xk8_Mn1rgu9w8SJHfcbncl6uufEb0odf2emPyRoZZ5ONpIq
td2pLeDiOFvFeieM7qeA23yDFOmomJ77teVmuKG-tY4QCi15P9bHEVIbICryTRIKofklOS97CgzoWGqSbvzeVb4Sd
Y0qs-Gtk591YmqZsHlpz0ITF7yi0taLI47Mrfe1hNz2-lEZ9iQWOsCi1xixOnkQaAexP8HLbJkC_dnxKI057unWoF
gJ6poMtBem0663VgEafx7E741e7aiWz73B4585256pthNoUD1NatoIJS93pgsGodHFDgTMuGLbmF2FRjvx2jNnywS
xxTr4XMxkaAJyJiUFYPTXh9sSRBYfn5QfqKzKqjBjjFqdmVrqAzBzUAkGbjAKYL2ao_zUbVI3sKoeB2uGc8Svf4TU
qJqGcyLSA0gS7UTFMicOqkO0Sour7SiOkYb9s6i-2S99AFN7JwpI2UWe9Xy96_sBC9YdIhOS3RhIOPQ-lw6ULUFMC
wjLNyk4dV0-9YvaE3DCoh3PQC8xqG6-JKNgLaQXaaw5YBCV3F_La2IXrDAbw1kIsHz-7D68YO-Cxl8r4Vg58imG0i
WC7hB63cDuML3HtmXsJWev-W1UfYZIEMzXf4aaKpP24OV_XM_eFj4nqG9GUr563HNATC_xpIR5yAAyLPXBoWhqIDu
k4k8CHlEk_qMwLE8KwLur6e9KxdA..qJ18Vn7_NeIcXfUx8ghZFY9cTCOR04Fr0JfY4-tQym0Jyc62ywkQDwu8Hea
Lowk_1WChzVQmO_BR75cHZVW-wooVYVDwdZykKw6f10yK-ubk_G541JinHeXx2yDEYW__TnXMpLH4a9PMFJWgrwGM
oK_z6LSNW2ZTlaQf2sYVnBYPX4ygdhUsGiLgJfvPP48ZuH-QR3vk-dQY35uFgKIyXJgxUE9KQJjOcWjqZM0-1sup3
OKBQMl7jBPRhmp_Xljcg50lr_Y7VXcttlduMh2h9HLfZlzFmFoBPzwJqaDgKusd4SBT2kCfp3kMS67C7FS_SxIVBt
EMvCQunsR7f8ci7dV5l92lwwKArKZ1aPMgnTbieHg45De4DvF5P6OfJXuW7w.
```


Figure 9: HPKE-9 JWE Compact Serialization

A.4. HPKE-9-KE

```
   {
     "kty": "AKP",
     "alg": "HPKE-9-KE",
     "kid": "-V9VDorHU5_DOFXFxSSNoQvhWMat3LtsFnzd3BSObnk",
     "pub": "_VGNHTKXEdAnfXdDRfOCcEQtrdphLmbIcKp2oBZbVvCU6ptwNgJVBiodmypvByrDHShkqYkng6CD
2YUHdBMdYGvFKNwNS7V5fnI3fYpVvemlaanFmAN_7eEbhzSuf_B-J_k7ahilfdMBO2BUEcpkmhRWr5gVkveyv3uks
oJIAbMy4CkEgEFuEBsLOlHLMyxxmCau4GBa6uWqPBkCVygnoBCBNChquUymfDQoA5MEBwuMiruyl8Jp2QmsUHgqMS
d34Pm0I2dhEYsXwUihaqUhPqbPRSfA8oNNpwc0p7MwRmx2M0iOXZU9ClU2iqNSYHEHXkZ6iAm3R8R68BlXL4BHJng
lpSiHi4YQovuUGeOBCotesMU_ALXKP_NZ5Vm88dhSLfernRjD53UPSUvL8hvLgcKM7KJmhmUrlUQOcDjBlSpsYpNw
aJVCunSW_aI47Dlyr9CPGWCX2nsHkyag38dq1nQuFolJIkogDHmQakZ5E8BYA-liO6kYyyi62llUa7sAN7osTIA_s
vhkW7LH_tyOqKbFsDGB3XmHY0VxzsNo3bQeKFQ7DwVxBXk2KSJq-EMzKgsVLgq7cDdlneQQt8LCzYk8J0VD0FlMZm
u6J2UnZaCk4naY8YS0DcLK3wcgThGW-rZIwwpKXJrMkdGAn0cQyEi5JDJX5UOI_to4dgdWXWeA0pudbrVZzXZeuBm
IPPgiDbVsUONdcDS8wijNjSQ5tIPJtPp9nHl4erY5feh7J_imp7a1HVFyLwyyeDUwoyN6RXZowlMWVFCvmaUNF_tc
4rg2eJaugOhuVxEiWRygJjoow5ynQIcrHJrPVEdJvNkRumpJYIZ-oCSGRtBwbRE38ylM6vckFHtbLNW8nbmWDsyhe
7KznhoTE4V1znlvs1pzWNWut0ElsOuoACnDg7OvcoMxp7pMK7KxLNpn-HOKMvswUMXJ03fJDUc34jtoIVfGt7yALY
AW_gNg-MypzDtEJ0C6ezdPvdEcbEdyfFksVjAjL5MJorYLSvx1uAFlMSors0Zi-oWSn2as3iAP7QclUAJBoGsVU1l
yGFsHxiKQnSw0VhhMy5pM4dVBKuunLBpe77mAW0AEgomO-BCJWIaZmByeiRaU-WQ8rDO21Zh15jksGPVMI3CGl0IJ
BWZjnNJJwzPA4Dhk8yXLZORlG8nGxCxaDVWTBtFlRMsB0aMwC6LJ66lkevZCPise0Ld4CtDEhKkWPRipHckb1bg7z
UZnQDwO4wx3kRNzPbqbG5DGjwCl55ZC_7EECKOIqzWNqBmcS0tMHxJ2TXl_NPybc1AxQYeixyd8NOsQtwCwcKjPAb
w5FMK86PwprFEzpqwi83taWhV1u3puLTdPW1BuhpN_XHQEg-KeOzuu1URVngllB1ge9otW3JNupUCjBXWislV8gfq
zBUcPJ4SSfgy7goJF0tRUSEcdNhNagSRbo-sxtmU9oRwka_LB6nh9o1WldYwM4UWs4fIl64GDw3l4WXdAM7A7-rC6
TIfKM7BmC6OH6Sp_SiBSTftRYtIUQboSl9eFnIjpJ-y3Ki0cd1O--A5qjebaWE2MKc0q7oNaaLuWsowEMugnHM1bm
6KEdXJJeWa7TAC3a78t488s5-VCvW09vWbER_SfjU2Ch_nxrtt6nnHlNmIZoJMeZQzbIQnO-glZzw",
     "priv": "65u2v_r9I_dK7QCtjTBmMhQjytdcc6kAqNRSbyCGj5Y"
   }
```


Figure 10: HPKE-9-KE Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiItVjlWRG9ySFU1X0RPRlhGeFNTTm9RdmhXTW
F0M0x0c0ZuemQzQlNPYm5rIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiZ1h0Q1FxNUE3cy1pR1h3ZGp1VlpZRC03WWt
iRHBaZFdSZDZEMjdVLWZEQUpXTUdEZjlRVnlYN2IzNEhsUm1ZSXlJdWh3LURuOUZoSndpNUFfZXZOalZPNExIWm95
RFJjY1dBSWdBXzhLNGRHbXZtc2drMWFQV1E4MjJqd1k5X0Y4N1A2MlVfSEgtbERCREU1LWU3X1I4cGVVbXBESVhqZ
lhpRVAyc080UEY3aDY4ZkJpclF6SzliTG5YRFZKSEZiOE9zRk9UcDVQTlJtYnpEeWpFYjlkcTVGOGVZaDRPelZyVm
5fVzg4cFBROUJXZWhEVUs2Wk2amUtVERBRzZMQk9jclAwU3g0V2gyQk5IQXZaOE9rbzNRRm5vdGU0U3VVdG5Ed3o
2a2NVQ0RER1hTU1NqNUs2NHFwVE5SVk1pRUN4Nl82WGQ5bVFYa2FNQWtibzM3S3lVbTJSeGZnODNUT3IwbGpLMDN4
Nno0NWN1Y0t6NVZLU0ZMNGlFZXYtMFZZWFVBR1U3b2w5enROdy00NjNKbGZHWDhWeFRGVFJpWm9rLUJnaWRoZlVJc
lBORFhwTXBfRzRJM1hrWHpRZ21STEdFaWQ4bU9XdGVVbDlDR1h4TUJBc2xpMzc5X0luUjUxSFEzSE82RzhiNG1yZ0
c5VDJMVTAwbVd2V3FOMjRIZFJkcmQtdnZVX0ltY3lwTm4zcDQtS1B6eWRsQnFacm10dmVQSkxDU0FtTkxOc2ZoRVN
hR3F3ZHdxMnN2WW1TQ25CYnpvVmxqMk5KaEhsQ21HNmhYYkxOTW45Vkl2Z1Z3eEdwV1dpa1dyaktDdm82bW5XS3JW
SllBTnZyRFNJOWg0TXlieXVFXy02VXhveE00RlZGUDlOVkRZSS1IcTROZFV3a0M3RjZ1Y2d4djV4TmRITy1ockJQY
XBxOGJRQ3ZyV0ZLSHE1c3lobklFN2ZZZklLcm9NQVNIeHNlMjY2RGNzUmRLSWMydzJYQlo2NHVmaWE4bjVvUDlYRF
IzNVN5VTh2M0Q1eXpDN3Nyc2NuSkhVemo4UmNGNmc1c1JqeWhRc2o2cVppYVVCVm9ObVd6T09nS1Y0TjNMQ1hxdVN
FeDlzUC1La2p4eGQzanVZX2t6WnZhWEM0VnNqYlQtR2c1WGRtZW4zZjJ0VVBuSy1tWGtNUXlBdUJOTTVwSndESl9K
azQ5SUx2cF94d0RzNzEweUJiSFVKaEhza2lYeE1aMDh3UmkySGoyUFdjU2VkT2YxVTFwaG5MclRJMXhQdVRPQWhpL
U1EQjBjU0YxUTl3UmFJaGc3ckhOM0stYWt1Q0hwQmdKMV9QazB2SGpaeHNlMDVIUUNLc1VHcVN1elF1cFliM2N5ZH
lMYXE1dWM5V0JiWHhneFk5U05najdMdXRhM0pWbThqWVZEMjZ6eDdPdWpHVzQxaTVfZTFmN0hNYkZ6SnFIOUJSUVV
RcV9qNXI2c1ZMWDJRUjlSWmIzOV8xWk1fZjFmOFVEbWZ2eVFITXlwYVpmNmg0aDdDM29FV2k4LW9FY1BZbnhfbEFl
a0xVaFRsUXVDTlZkNS13b29uT1VuakYwN2NTUWtRYnB2a29GSkdCb0RUd0tFbnQtcWNQdjBzZS1iSXBQYjUzeTdiM
3hxUmVXNmNUZy1hZDM4RjlWcnlYWU1iREd4RlVyQ1BPbGVKRGktcmY4MWplVS1HMDh0S083Xy1GbjlqYkZNUkRNN0
1XQ2hoNzllRGIxaTVZM0diZU8zUXNXU3BvMFE3Uy1KazNGMFhEMHg4SjhiNlNQQnF0ejdvZnprYzRRYWRlbFRLdVl
SdUNUaEV2RGxIZ2V4OXFidUgzZ0Zza3NoekZSX1JIVm1ablhtRWJwbFkyQ3gwU09GWXRpOVJnRU0tQUFmWW82NklS
U1Njb1FlUFQ4Y0g3dUxuSHAtVUQwYVVFQm1NMThIeTZQbFJXNEFGWFR3bXhVQnFrcXFJR2N1SklWMHc2ODhwTm5xT
3EwZkd4aUpVOTZpV0FQdnlUM21XT28zQ2l2MGlUVUI4MVZLMk1zTmJFS0EifQ",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "XYg8K00xhq2EnFx2",
     "ciphertext": "vvQX6OAD5uuiyTmzu2ZXoPBRF86Se4Yw4hDVp9lDfIO_rFxce_tR2UHc2yeLFxHgg0JQs
7DbB2ahWrmqFQa4Faowvd4vy1FbDQophz8WDHaHq7h43hjv8h3yZJDQtVIbRQvqMPsUivoJ6J6W02r3bBtEjMflMv
xwBuZNs1uMbomx3YN9D6y6Ze8VigP78Uv1Xy4K6R_wd6PVW8AJaPfTBV1sMWbCS2enqNtQms8qfDk_7sUhQyZvawP
RxmlQE8FbSDoXfh7bA9UfBcoKKB-ni02MlTRs1DVWT0JttYEreqpx3cccIBTJ2gOSy-k9ZepJipmW2-tPPok759Sc
6LqrxJgqJ9rRhNIWIKRnPkLElSNp",
     "tag": "rZzBJn-V7ZmPUOYBhPR0wQ",
```

```
    "encrypted_key": "8doxqTRQHU33CXcWOtIr2b7xKX_xA0-WYbRbtxlHcVsX6-LlV0InnWJkwjInsymv"
  }
```

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

```
eyJhbGciOiJIUEtFLTktS0UiLCJraWQiOiItVjlWRG9ySFU1X0RPRlhGeFNTTm9RdmhXTWF0M0x0c0ZuemQzQlNPY
m5rIiwiZW5jIjoiQTI1NkdDTSIsImVrIjoiVUhwd1RDdHZES3pyMUNkS1FISEFoY1hUckNFdHAyQi03M3Ixc0RLS1
FubV9VUTlJRDBRSmlrT1RiejB5d09wb1NIbVhPS3U5RUpmVVpuYTB6YUY4MmIzUVd2ckVOdnFudW9maEpXVDhWVUh
mNWFFYkJ5MTdRQmwzNjJvZlA3Ni1EZ1dlX040VUNJYmlxSDJha1lHaTliOVR4MEFTdExuZk9VajNxdENhZ0htMVpI
Ulg4bjduM1NxQlpSTVpEUFlSRW1oS2NCaWx5a1BTRkQzeWFTQzE4UjBTM05YYTNEWjh3UHNhdDFNb0d3a0JtYXZPa
F9QMnpETXh6UjRJeWNmenCRWxfMlZVbk80bXFoMDJmLVk2RUpaT2xBRXBfRmNUWU96SnNUTEV5Y0ZUZlNUYlkwYU
9DZncyU3pzOU5DWk8tSGp2QThxejNVNWRJNkRBQXJLanZaT1dEbjc4YUtxakI3YlRCVFEySkxKbVRfS1JCTXo4YWl
jTmkzUy1LdnRLU01OeU5SRU5renlFd2lqR25OWmtrM09WTk1ZaVJ1SExzbFBIX1JQRUdlVnhMS0xackVJLTlrc2hR
dFlFUDdOMGJ1azZaS2VpWElpN3JoQ1JkejRrdGdDanIxSldiVFJvVEZWZjJPQjBJdXdkUHdSVFFfanFQVEZwbzhtV
WU5RFJwOTVGYlg1M0E0TDk5NkZoMzB4bjBEQjlNV2hVNFZGLUVOX2tjMC1NbGs3VXdJYWtmQ0NvVUUxWmZmcUxEd0
JDODdDaDJRbVFaWUhmZk9xTEwxaHlONGVyQUlRdnVMMWdYaG4xV05Nb1lSeDVEbEs0c1RMa0RLWkVVZ1ViSmtUeS1
XSEMzcWdMUW9HSEJyNGpYRmFzd0drU1NGeFVVOTlFUE05Zmp4TDF1ak5CQUFNdk14VXNFbEdfcFF1OVNKcF9BVF9O
SzMtRzJFc2dHU3ZIOVdxNHVDSktnUjF3RHZwTnlvNHRPLTJHb3FtOGdReG5JTUVuV2tvTW5wblBKYi1vcm5BZDVMZ
npKSndfd3NwS3lMXzI3eHhsOXZCOGlPb09vSTM5WG9yZHN3Y2Z3X2lwRXJWUmtJNnJlN0JnckR6QW1PbDFwSjFpLU
pDZDFHc0ZZSk5XZHVzbDExSVZtQnBiQjVkS3d3VDdGeXVqRVhOZGRsUnpqdzNvM1k5NmhCV1huSVN2cEV3OEo1RGF
BMHBCY1l0V0dsaWtYeVdVXzkyaTA5YTVaMzVWNkxnREdTM2ZSamlIZ2FGNUJCOGNGVVlISFpZbFczRkdvZGNQZERX
VFB1MDY2YXRtTVlNTWZka2h6VHppSTFkM1dWX1RvR2lycXl1eDlETjFvc0dHeEpCdzZkejVzNmhpelUyTHdSbHJ1a
zlfVGR5STRLaDBORUgyMzZibzN6NnFUa0VCQU95eDBCYmdyVHlFU1M2cnpkVTJfODZaSXhOb2l5ZEN1UmVWY1JjaT
BIclhBX29ON1dVVVYyYi1tQWlLUWlDVlk3LURfOHYxYU5mX3RGZkRjLVZTMXczbW9UQ19IVjNpaE1VVnFWN3YyeFQ
yODlCS0NqdXdvenoyUTFTM3BZYzZJVC1abVJVTl95ZjFQa0hqVzJULVBrb0RGRTkzYzBuaTVrSk5fVDRocXM5NzhW
c1A3TUdKRWJkc1dPNllUNTR5ellCTERHUmkwcXBJWENvRzJ0M0VYbGVuZTlWWTg1TE90dlA1SzQ4RjdzME1JcHVnQ
TVQWGliWkNBNkExZ093WExfQmp2RlRFSjBNOU16YVN2UzN1d285cEh5cmhsdENGTXdNaERJblBBVlNubVp0VHd2Zk
daRFpXT1A0SE1VRkRWb0tsLTQ2NlJRR2NXaVA0ODRLazJXcjZ1X29May1odmFBdk1wU0pQTml1cjR0U2plNGcxWnh
NQ3pfRTZJczRFVHNPejlUQ2xRNm9sTzh6QzZMTzJWR1lFaEw5TUdvTG9tMWZLdnVXMmxaZE80Vy1jeXdvbU9TVWQ5
bF9YZjVzMXVxb1hJX2I2T0oyWjFLY18tTUNiRXcifQ.jfm7zFDOXJ4AZ0rXCJqFGZWfrMcZr-MjgiM8b3Domnl-_w
RnCdj06K8QoVBteE1y.Zla_65DmP-jTbGfV.MhIsLHQU9365GD_dX_oIqQpdi6ES14T0FDUEThCrM6hGaa9vjdLHZ
9TqX6Bh9eOaqwlwpqzD4FArTJnA9omKm-qnS74c6--ZThkTbI2eLQ1KM47G_0rU3BY2bebARwDvGEihxoAgzoLaHF
B0RcHDg2b1Q_jSTNzZHSMfcedZ6Tmg45aJnZ8CT5VkRUDIegaLODcC3YlybloLz0jAuwR8lYLG-_HZPIWRsGvUaP1
NMm_UKw_htNajAh4c_nSkcO6oyfuy7a9xphy6AY5lj6LIPNHUolwtVlDuKkXiy4OFn4aNnJrhtLJtjYhrQiOWGl-7
CxwffIr_G1L669V1li27qpuo84wzWdvYmuuxEWZmaIKP.jRIy4Dxq-zZ3w2ooEmPHpQ
```

Figure 12: HPKE-9-KE JWE Compact Serialization

A.5. HPKE-10

```
  {
    "kty": "AKP",
    "alg": "HPKE-10",
    "kid": "a6S3CFflyR--3T_COOiiWl-QogGvjJdBHlYjUvSgY_U",
    "pub": "xklAICae0qgkKfVvsRSeBudZynYNfEZpzrkcuncC-6JezFhrj2sfxxECQKy6DtFIgdEEpKqdWsa1
dTaqdhGfZhoUL4wO8RN5GAJhUUFJcVgmxTaDUWi96ZwOPICAIfgUphuy1hxxWESiw1uSjPkcd3tjeDOdONMC3dAg8
sR1cWxrv4OKRKipQHqAJdxnT3NxF2AYShYT2tmy6SBKoKBkewWyE2R7CughGVG3KjEau8S-EJIWRcxMxsim92AJML
hgYXOPZTrLgrAPrnFrggIgKAnD3HpgJZtUriOcf0p3m6N_g6NdyRKuoTDIKkjDvNQE1_dVf2Qa98Fy41m-E9Zi7Em
7tlIwMuKpKJt8MJbGZ8BhtoQ0UkiLc2FSwdJeNosem2kJfet4LdxXBjpgkNvNtBa_39ACiIq5DHI9E9iaKrwIFAGq
27sOjNKM6mSNTxpzxrs25lOupXV8oDkTP9qOd_ObuvYoWyGqYkWFeQkrDqMnI-YYvrm6gNOdgaA2L8wSeZLLkSG0z
5U__lWHJXW-tttSjyczVQpEsqcHzsgIYIqod3yzpdlekqo-9aanlkCOt8WSH7jBCvcQ1zrJOEss2LzOKUeX0zG7tT
gGf1hrMaweTrlAZYtDoiCtJqAgUPQtm7gFx_uUzRGLyKthvpEnVKUQ6mBYJoa8c6GGRZQTWUMDA6fHhbNmPIEIekq
FqezGJdtXuHHF9-QFaCyi1ddPcZLDmqI-50AcpIV5U9hTWtqegqfGBhvJZsK2YUJABDNm1zmPILibzhCby2DNEkUr
iEOosNeofKKfCrXCJuR8_7ueGbpnpueTp5mUdOkoDkyPAQp2t7qOrNVyBelub8UjqDwpKREi2LuE9hOqNNIFWzpvF
ly81PrPxboi2WSPYOJweAUGR-K1BAJSKbWS6tGx-ehepjYCvbNhJ-N1_dlVlBIoTtmWDttjUNlDz2hxY8TNcnymse
i3tPG74gadWosHKXai0DiexVIGzLMjeGwRI2CkxSe-sskaF9hx9DIiD8lEpjZlyZlgbVxpghdjS0khX5Eb7JF61cd
rqOyJ2ATHSSRnoDPOLozDsNevIuCiXsO_i5wfxfdbSvmveqSD4qViUTEm8XErc4Y_OuU2iiATb2wetOWKR1YUE7A9
wZpfKMQSDtRzXovO34wWUjOm4kZAMKdXr3nE4NMHYdjJ_oAP-SxcibSC2OuqfEliFat-qgsZB8mxOvp7maKy1BlCo
tUneLMclfXPnhJbUUofsSyag-tFvyo-0uiM-JbFhLvOPgkOqauN52aJaksY9ktpbjMF32Ed6BohCaR9qeZ_loE_jI
JCH4RUhjNxx3wlaEmtlwSZPByS2ix9l_pvGKIKBgeWext1dSB-MZYRLFyzIeOOONQVMpSaNMKz4ietseBfNuKk3uO
wDkOlMOUy2dMQ7ruHleOv5gSs6JO70oqMiDEJGfxx84d2ytJ2ASk5GSc820fHwGsaHRA3dUspLWoqVeq7EKcsxKAT
dAdxbXB4Uosl-TWcZ0p36Kg6kql6oYk_tCN4BJhu0O3zQac4MKj5_8wjrW_KbAj9DJgzv3MiafR2X9-FRLC7_0Dss
rAwTlMIxRr-olVTpOIF26zl9mShTY3ZEA",
    "priv": "uCM4b1UrxQIuPvS-wIq9I4-kehldr520pg0W7jE0laU"
  }
```

Figure 13: HPKE-10 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiYTZTM0NGZmx5Ui0tM1RfQ09PaWlXbC1Rb2dHdm
pKZEJIbFlqVXZTZ1lfVSJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "VDzycd93m02BgbO7ChprDh92-r4jtEmi2BwGuu-veTVIYohLOEnuhvAzNcA3hlVVOX
40GX6w4OKJoG7bB1bSUGjDNqsCgZBk6gKP9Ne31YwgQEMkJ57XSDpx38wMpwR_hVIJmcdS9fLsndkSNWTITI1iUL2
gG-XFmfcTz99bJvwzJ0Q7BhAsz65KNxu4OE2zfAYc-HTe2hMdjQE-m1Bofj-JnYb7fU9pwIqjy4bC6t39FloK8fbv
0Vzxucr75Puy8uIoGLgTwBTT9pNJHRKr2szVskmj_q2gA9AXSoSoIw5wnWojGkWy5oKoXU0w9-cMuoMgRzcaGDQhr
oTjC2KWGsamvg-tpL8DhmfbFSRhjl0a7wo6ktHq-uUgnJveNryxvdem_I8-PJqmm6EpPnOdVpDn-YHqeV-GufWtSZ
frvFzkMlkSP0ARaTjpWyvfQ1YafDoFwplawuX8mfkusLbjEpyy5tAr7QcDFzIV9hqg1YcxZeoacHIG9mdixD3wquC
DtvnYZJsOLGdMrOsBv3iI0UoPgpfLHCuVpxLYuKebFwPxLKv-eCcl_B6rxqL3V47XNZ3oODqNW6zza6-SaO9ZvW_q
HRiOurzdKcvfchgbu_ZZfc8bhE6ZORTu3IFcDrrJg2UxI6kNP4vjyVw5bk9iXhgEUXKOUlhcM2Kx_Mi3a-nJ3_xzK
LENWKXL4DTdLgUec9BFW0WBHLx97lst3vbTpSerbf1KAHibY6gzGU5rRpxJ1y-D_RHJBYGfDq-NAYyjrLU4pvJZ7j
sWcCjiVhDZs6hbAdl8Q89TJYH9bmVD9ycRugg3BLf1z4xKihGOtzXx9Zg4d6LK5_0EPr74nCSzMhUeJ_RUZ-2fz18
hxnt1Z7x9D8WZ7mZHNGyp0vgvd09iPoK0zTGbxf-lfvRnlZ2jgzvcfeNr_nwlepgoyGmnEk3cHy8arVPobC9A9Yum
tChq2AL6krrKiW5PYYjUUOwbUILd79Nw5o_JXr24EUkT7usMhRxiFlx3W7A-bxapuC3alm48hIUBoj_vETyginrQ-
JApzEbM5Si-hlRomgTu8xeEI5dRjJtbHds4f3mwHq-TXZ0vMOo7D42DFOO-wcQKKGyAAC0Z2y9_U2khqq91gSjSL_
DuXYzYEI1KeKlHeHNWtsen_UOEDaUBieVbx3W2vVKBFfIxJ8HbSu0gdOsHm4Ffa2Aur6FvvG2M67NFcleE9R-3_-f
BljPKBLI7YHR7ebKMqMUT9AoQtKKNWpck6MuED6xjtcOHqEJvM_Czap_-sMHmmKIt1vsbUWLOyTDw72fl3awQJ4ou
W4vZlJz0zAW1QS4Ht7I4qZ0vQ0_zQt2qvmC8jf3CnbCmQF42TfFC7Jg50aS7KcCKnWxmvjGe14JqZq1RFpkm_o4s-
daTSBo1xP6MPd6d2oojPO-cfMtpssRmvBjw7XqikFXE9pouqG8JMvl1QxxpIrG7Xw474tsjAp4LfKAfa2fcuK12Jl
PdVw",
  "ciphertext": "bEKvmLNeGhm1mkLNQ8lSFdeGNjVGOXsEPPyp29pzjEoTiW_pP6nEEOk2F7u6Iu4Gds2mQ
ZDijV3KSYYJ3A-oY1RA2OOq_71N0WynRiNZoBPiSaxNYTA26ha3iQobCxUb7t7XKwQXnfIBumr_Hsb-NwOVM-zj2U
x5OmHOAAqdCB1QUd8Xh2l_PlBJ1FJmbm3R8CnEFrn5Rf0e7mh-tWP1Z5pQoA1_dKaRCBDas4EtI3Vb9gHXZbBg4Bc
uyu50clHTxP60g2DXiSuL2b5AIwGiEur8IaXCTjRA93QTLHUJiqBQWi5VcjbGZjAC7NRX6PdqX3b7pQEQlDj3G5mm
IyJnYqrwvm-DPIzCdSyefEPo11IrWRfp-1sy18xYVy9GGuCpnw"
}
```


Figure 14: HPKE-10 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEwIiwia2lkIjoiYTZTM0NGZmx5Ui0tM1RfQ09PaWlXbC1Rb2dHdmpKZEJIbFlqVXZTZ1lfV
SJ9.wzAce3W67vBDznwSud70PuFAzU3b0YNkXFvA6XL0x3VZ4CnjiXQudcgot9tVpdFkmVGAHQNg5SSnVsjE46nRl
AjiIqfSiNFUGeDDFcoqIpqbM4nQP7U8bJBRHVwWCkTkklmgxuisYVSR1Z_DDys7xC_3v2MuVFtY3fciZCDuGq5A72
R0ghlg61fOpOyIGRyEfsOoyfBmlUBds6NUKn5rpNqBGlCMCut7wes_Yyl2S06j0JZ5gmzhJKsKXkoAAcPBRquJLea
BKOXOdHNwu4lhAaUcuBnhrM6bBDiulcjQKeSjtyMn_MulAjxFfoiheSf-4mvceV2TZeRZ4elzCRSII7zV2tKrVaXJ
OMepemql2KqyOVSA0R7AmjGPxCOKL_QQAPFzI4HaxXWydcylnUY7k_oDfG9m0S_tQd90MprUSCJw2wA4mgjAVu4Bj
OuZbPPoRDwdfyvmBfsmoIG-HEROY7VMzRBlcD2mYeOgBBrldteOd4TRtr4c4hQDCaI431sFYQ2iqMsD3BOF0R9yiw
pmzumvrNU6da6M4QO0arKFUtlk65MkfnLUzgE6xBFMgOkjkPLwfvnTFVJMmXoEz79LFkdCxu0w0N54mobig2W4Epx
A9czXgYhU80dZhNHaInx82Gu7ULNhFcOS-odtCojY3x5yVFFLtozMPNcMfdG_ThA6S5-l9WWXsDgr9Brz_FldsWZG
Sb5aM66bNDacUdkXeAu72jdhTJElzcWmvH_YWx1O9L4kJj-wrwW2zGfI7Aq-Iek1Trf0lXpayXgq1d-WBsCDzTM_U
Ijf3S0FIqPJouahe8CoATtW3_DGis4cQnY3QzRIiZYx8AjC2B_3WXLxIzNnc8YXwZ5OzHakpZsF3ry0Azkh_NaR5D
O5JCG13F3l9BhrX8dvfEbNunFbfRjHsJKzEcjhQERiKeFzGnO6DPe7WuWRm8Z0R_d_DMa2uAqUmRqg8hsYDkMiilB
XYfkdUkdQJV8uJ07Rpv800aywHI7cBWEPRX7msyKkF4lnqaDCHUYBjXC0ZgWiYSPNXfbGJ3oYTGvU35Fr_-ekj2TO
aW_Q9K9CKjH1hkwfwz48dvVHYdARRmXRp44jouLlXPw_9HI-N3mUjxEhPqnwHaLjUya6nNR9b7u4_gyNFirZH6zak
9Pzl4GPMmAozyffqCE7yG_ksPnJk9gtJoVSwIGKHef2d_1m0Mx5dVvXIUq60C2AFMV5SOJpc8cjkfkKmJq7qRL29G
qnTxRywI-SvshAk07r0g0AisjPEh3crwxh7nhyQga9oDNF447Hch9zoujYC1LkElm7ybofBI8cnXe-cedIXZC3gd8
knQLZWHGdqjM_UFmP8u5eT8R1JKSL2Pp0Jj_7LSMcv_mc66tdJpoLyzzp4w18NS9u23HrzBMSPhSrRl_wqZCwWVWx
1WQfU2bWUq_o5xhJcmVvHuR5Q4RlKxNOoRoRdqLnjRu77zb0AJce6937yBI6vsO0UBgLM7JJSw..mTZq6R_1yLiGA
ihJ5jmjFmE6hqXEWjGLZJ383eMnZsMxYNNj0paBq1YWDtA6cpIJhyJUwqULwb53TxfnDqfbWowCU3HEK-DBy8IM_p
ZyuTptIKGWiPA3Z2L5kAE6MMW394R6e18-Fo_0aYjD0Z4XTEi4mxe7dd43gQ4qqMidZGNnMZ1XkVTS_xW5Xx8O9a5
sA3AzLPG6BPiFPqDQs_8EV0HVwQqFxnzxTiRPjeBYME10hTKn-Ao9vWgDxXenjWtGkpTfT3uwY_QTKN8_9EwjM-2C
n7sVzKZZUGby1Oo-5PQmku0n1C285aR_VNPR8CXcRALArA9wLZ8bBigX7gqJNec_kaunz4CVZNmJOabEih27kMl2V
wU0NUtm2W-dL1pWYg.
```

Figure 15: HPKE-10 JWE Compact Serialization

A.6. HPKE-10-KE


```
{
  "kty": "AKP",
  "alg": "HPKE-10-KE",
  "kid": "Xm6lJa_lUA0szEe-830gP_eXOVMebXlypAKquOzYaI4",
  "pub": "7BGc3VNf0-Qtnkh39mc9TKQQdNZ2CKPOI0kfuMxepdoEhpCMDbiFCFGQAbKlsxY4-9aepuB_3zdr
dFO1NIbOnMy9WTC4tQloATJhdZpsC0gDzhku0fgjH_d7HSgwFVQlTWKJoimHYWCC-0trP7LK3hd0ugpYYcMEaJdit
NQG9LsaSuOAJww4s0LD74cpsfEEYpKjSedpxXprMXBC21SRd9OV3QGbK-TOCxHM_TQ9HCUzZmh8CpFMa0CsmVRgAF
VCaQuEuRMKkJpXT7cKaTqlGKySDDhQYJtxu7GjmxS1kbGl7aG2kmmgxLBDCkobm5ElnSciFIyXPLlpuva6ZgqUedm
JKcpea_RI3JoLTSGFJVOCOUVGQGhF75Vj-qCPNpkxQOoWIuxWNzhMHshB9MxoQgpfNpfGHpMMYNlqiZnGX4ydIax0
xZmuhbGtAKqSD-G6v8OC6IaPv7vA89hJurESDgBnSTWCjXAXUirGG6QKyDANwFwteupljIuACwiFs2NQ-pq8mXOiF
cnIQJaI5pAoMTNJgemcORLHpBY-1Aqgc0gmvKeP1xuI8ThupGoABVNJHFtc-pnMWqq6_HxVLAkSnEO_6mRsnSl3ni
ILCqlLfPPI3DgCw9OLXERwP6udNERGNty6bhi4UjwbfhE1dDZMQ7zMLwnQSVw6sfWQjdC6XzZZKdamMlRlKqpnsDK
UGis2Bzs8VjsxDDOdJCu3n3UxBJZwP0eR1PSkKghSJVmuGmml8JociFAxARgWKdpyDQGdHpNVjSorX8WPZZa1BMy2
RtMiDoykWFiHKrMoTgpWncB4aEBLR8lTXRKckKdCRgFllsoKx4SIjuSGxSKheYl7-7GAC2V4kCVCBUetyiFUVomBe
BHLmkNf8zkDfMa8-iuv0vRw61wkB3hHdaBQx_htHrUuKlIfQkyyBNWkxnCq5eJjS2emO7qvJcSZWQRWJdwrYPMm1D
ok9BCVxvImElsSqTWlHEmAHmVJ1uQ2MvAK2MEktKfKnCdWnJCcVHWtPEQ-svJJn3lOL4GpIDqIznauVZYyOBNVBzn
HpOkIXIUtLFwg4uFMrNrFybKBjfq26OR__-AdIbGASUArIaVVJCCWQQIcZ3wCugiIx0SacAKV3HU3TVqCgGDIJIy_
rce-1mshNHKeSimgZ9UyL_hzMzkGTFmK5TWROddjUWHPFSZ8FtiO5MY54Ty-KfpaSHjJDNLH3iq2MxsipZY4xBSp8
OxEKciXnDgzRLAPscAgXjtutdJKSgga9qKZM0BkzOKI--Ztf5kXsDQoM9KtNts0lMKsEDCqMMZS_7KqsvcC5jmku_
x3y9bKBzBoK5eE6Re5X5kANNoUBKmXTWjDNPPNJpAr8lnFWqm4EemlECwYxGBWmjCFPKa8VPNV6dnEfPdb-QHHFuY
rMqVjStSvOunJNAk5QmQq07M2esrJl9U1EDEXKYiUXjmoM1oj8vEGQeazWcQm8wIC9aTDH6FYasZ1CnWGJkukE9R9
QVRzMLzN8GaZ-aYm-ekbGidpa2GgYfo28bpiYJ7TorXxIzD7dccmDg_zPILaV1-ya9d2JLdz_4rZZQ42f67fHMmE9
3JkGCO5fInubiEUsxGRfENaU7KlDJzQJg",
  "priv": "Qaa29navsF7XGQ2OMq6X9N1eB1WTrW1v-NSiOctY7YM"
}
```


Figure 16: HPKE-10-KE Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiWG02bEphX2xVQTBzekVlLTgzMGdQX2VYT1
ZNZWJYbHlwQUtxdU96WWFJNCIsImVuYyI6IkEyNTZHQ00iLCJlayI6ImtSdXlHTmh5VGpVNkNBRWVVLXdhUzRWV2l
FU2F3SGdqVGIyTUhDWmdlck56NTlGX3ZOTzZ4ZFpSMVFaM29KZWp0c280WkNDcTRsRHlnMGo5Tnk1UHVPaVlKYlEz
cjREWXNIb1kzOEVfaTRYWjdrZXJtRWVSTEpKc3pfazlWU3FocFBrUkkyTGdEVFZITS1kdWE5TENoUDU2dDVENEs3Q
XhOQWZFNzM4ZzRVREFmMUhickpYMS1aR3J6RzZxRnI5OGZESHF5Q3RRb2JjR29ENXZoWm95ZE5haFJxT3lvS0VSSV
92WGZhWHMyczhUZ0ZhVFBnQ2xTTGlxM2U5NWNqZWlFRENZMldMM3FPaUdwejFwLXF1ZnROU3JKRm9WU0pkSWdtejQ
wVXhxWk9SOXktWGN6QWhZODJXQUpQLThXMDItQ3hHZEhGcWNOSi1KSjVLWFFaMWFqdi1MclZ2X2REWHpwRlBON2F5
OVZtMEVtNnNfQnFscVFrY1dudE9fcU1aZVV6OWJCbmZ1WEprWUFGT09jRDBpOVV0bW8tV25taVF3QlEtSTBUU3RkU
XdnWlNOeVRvSFkzcm1RTTRUZ3dqMlpmXzhMaE5TNWZrV0dkT28td095V2ZwZERBenhVaFFRLU9QZzZ6bmU4d3cxa3
VEN2stYnVMMXBLSDY0a19mZURzU2RGV003VV9McGc1OWtaQ0s5QnFwazBBZWVGalA2T0hwMXpKOHUtY2NQOTZKb3p
iajc0OHpSS056YWdlWG9GT3ZUSEM4TERuNF9YSnJBZXd3YXJISmZsejJ3RDZvNnBVMFo5VDl3OV91aF83MnNtNEpT
WWhlWVZQakFIS29obEY2Q1luYTdUVUFJSllvVjhEODRKY3ZTblBpYURHT1REWkI3WEVzU3UtLUloVzdMdHY1Sjhvc
3puRmsyYzE4Q1gzSWxlYTU3NmRNakxzSHNsWjVtRzRqaVJGaFU1alRoVjFhcURVdUlIV2FZSHc1WnNlMERUYlV0Tk
xuZzc1RnVodnc4V1VrZUYtcXNPekplM18zVkxxRkZmS0E2RlBQdzUxaFBLbmZIUVhPQzlFVUhoZjNHNUZDbldNQW9
nbXFkNTBheC1wUHpyeU1HdU5PVVBVT0d4Q1dxVTNaRTRrdFE0WTQ2QV9qMDBEdFNmNGF3cTZIbVFMWlIxWVM5Tmln
TkZpVlRRLXp5WjlrSDJCZklwbm5sWkMzUHRVZHpzVjZYSlJaUWtvOHpWQXRRWlNRUNTU0pXWE5wZHRRcHQyUmFYZ
zBGSW9hZGZCWVdwYmx1YXdVU3U5Ymd3ckhoNXNHM1ZkNExUeXB2dmFTMnlSemtDcm5YM3R6aFk4S2M3c2twRWc4Ul
ZjcUVMU3hXeUs2N1J3dDBJYmNLNW81Z3ZsUGZHOWFnckZBLWpBRXVSZGFKc2ttRExLRnd2b1dhVTRVWHVNSFFwbC1
mZXkwUWtoTDRhQUFuRUhrdVhabUxnMWdMeUd5bDcwZU9VU3pFaW5maHBFYUExdi1HeExQa1NUM3plWWdfdkd6Mkw3
dE8tUVQtanVQTTI0X0dTeFptLUlRZ245SkVkWi05dGYzM0tyT2lQdHZablhpOE1NNFRCNlQtUWhuMlc0Sm9yV2ZRV
V9zbTNfM2hXZFdoQTFMZ3lhUU05LTdDYmpCeUN4Umw2aWt1N2R1ZnQ2eVd0SldIcDIwZ1hyVWFBZFNuVGp5TV9Ga0
RfcVhUcFI0RTlqUkhxQWNDNVBhVFdyTWxWUkdqS0lQaTBQUXlPOGdqS19YaDJqd3V3ZVM3YWZ4Q3lVRjRvd1FkVkx
6QkY0X3RCUGttM0tpcmdrRVZROXBxMV9vSURjaHAzcXhEVXJyN0oxYW9XNVdBdWd0RkpQLWNKSXdtcEwzV01KV1NU
RlhQd1o1bHRhSXZwdjhIbUx5Nkt4WXI0bjZZZ1o3Y1RMZTRPdGsyWFpkc18zZ01KcEU5dk9Lbm12aG5lQ29FejVmZ
yJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "iv": "1-TNketin2DrWVAP",
  "ciphertext": "fzV5uM6AqRNg832UWliKrNMWCnjMEQQO5KBcvHBQsQmGKcNmuwzs7JqJwzYQEwqiL7iGI
pJ2hpKd-432n_E72KzlugqGtOxQUjiTFOT2KdfhdOkSUbYr0AdTmwaE4U1gOSKIPPtufolUjhF26b7W5WHPX1bcQI
```

```
L1MvtJCG889OkZ-5vADUYJc2NJ88BZQ7CxYnpUd9K-cBKTcO96HY9KUCfgUO_5coDOcJKe97hCUYN8tluyeKZBRKC
En8DNElLemTweOGUcW_b1arpvvi9xIx5TJK1x-XKvqMAieDqPEq2uij4VVsnGkkpe_iAdCHAlCbltI3sZDEKDbbWW
H5LrzpXb7kwoNroKTU2LVIp7OM4U",
     "tag": "PYzkgIA22naRoXLWPaLvRw",
     "encrypted_key": "Yl52JxIODY0hQAxV7oQ1BL6gC-ennjuA08vZ1XXPnt94TsgUpFZdT60dq0Di0SgC"
   }
```


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


```
eyJhbGciOiJIUEtFLTEwLUtFIiwia2lkIjoiWG02bEphX2xVQTBzekVlLTgzMGdQX2VYT1ZNZWJYbHlwQUtxdU96W
WFJNCIsImVuYyI6IkEyNTZHQ00iLCJlayI6ImVvanJ3VVN5aTdGSWFIdTE4cjVOcElHNHlaVFN4YVpJTVZCX2JSME
NCekhrR29tbjdiRUdLQWYxdlFYb3J4eWRYSjlFN2hfMmJaM0tWbUpybUhwelIwQ01xNFc4enBKZkpNT3FrMjhleUc
wNXhiREJHNmVWR0VpbnI1VU9XcHhZLXJOMW5nWEJGaVAtRTlfcldwNnpVbndkLVhOZGNQYUloS0hrMmhDSGkzaXlr
ZTJfbndlV1o2d1pLNW1jbEZJZENqTi1uWTFnMlBtSVB6RDNqN2kyY2JsRVBvY1R4dVpyTU5RZUlXM3R3MV84Q3dyb
jZvM25HSjBmUkNBRmY3MjRFSkFmNjhqNE1UM0h2NjlnWVpZRENvQzMzWHZ3MkE4S0tnQVBPQkV5MTJzR2p0LTBHN0
FiOVhGVjJndm04RUFndGlrOXJNbEJYZ1pkLWI5T0NmWlAwdnhMeFhoSFU5Zko1WFYxRThzaUN6WTZ0MVdFWEM4Rml
TMGhMNGQwbUNCa3c0RThWZ21lWEdrcTA5MEpva2l5WkVvcVk2N0pzc201VW9FTGlvajFSX24xamU3cXZWS3BQcmVr
Y3FVT0NwSkVfZTdsY1VxRlJfY1l6b3pqRnhNd290SGtPMHA0QUJleU5jQWdVRENLSjBOVUd2b1lNQUtZXzVLdncza
DYyZzhXUWZWWUhrVVM2UUFoN0JrV0NsY0tOTThLZHRVTEd1STlkU1cwUm8wWnMzak12SWtJdHBXT0sxZkxiMUNZNm
pwd3ZsYTFFam13NmgxdG5rLTFhakxIYU1JbnBTbFBrcVJuWDJxQUdLdkRuRHA5RGRXTlBSZm9KVU9NX0QwdzhTQTV
sckdzVFNnR0ZGZS0zbEdwQWZLN3lYbjJiNGhwYTAzWE4zT1VueDkxaEZMckdJOVBSMFFpQjA3c1dMYWN5WnlDeWxZ
dG1VdmNwVG44aUhCNExSVkliYkJQc2hnTWxCenRjeDVZbi1hdWZEYWItSkh4RnNNTUtrVnZRZlpGejROUndWV3E3L
XZBbTlXSjYwRTJjekt2UnBueXJLVnJzWHZWRTQ2SktDZzRfR01YMzFpZkp2WGtSNjBycmlnOVJxeWp5VnRWNk1xcz
N5WVNsZWQzVTVkVlpyRWdhXzM5eWNVTzdvQk1hcTlIb2loTnNlclZTUklpOTFQV0pFcGYySTJHeUkxMWVfOHRBc1l
6VXNpaFJha0lEdG9oeW82cUZKLWNPYlZzTnJwajc5ZmZyNC1CeXBmU1MzVlN0elJGTDRlbDR4bmVQNU9nN0tkODdR
M2JvZ1laQ2VYY0g0MkNXaHBfSE1RQzFROVIwN3lMWU90UUJLQ3lNY2tSWVhoMGQwVzBJcG5EenpEX2tHbjAwX2RDb
1EwZF9SY0dIaWV6VXhocVVNcXlIcnVUNW9UMHhiVDh5QnE2a2RzLVNKU2txYldGazB6dUFCbk81WmFTQ2NIOFBpSj
J6cFBxeXd2LTNyTkRhY1ZDSm1GU2FkMkUtQ1lTUTdSbTFsQnZrcWtuQ1A2Y3lwemFZQXpRdjctOU04cFBrMmtNdjF
qV3lQR3BRcXl3OFFuSG11TEJUQkY2MVZobFlNZnZ1ZVNaUGpncGRlVUt3RjdQYV9FbDc5Y0NraFJTaUVhUlVDTmtP
eEJnMFhyam4xZUQyLXNLNXh6QnpOZC0welZQS1hocGVBZmlTSjNKTjkwdVpKZW5VVG5DTUhnV1hpeDJoZDNMRFl2Z
l9Bc3h1ZGxEbUtfYnhKdHJTbFlWYkMtNzBuNEtiQzc0YjdwYVdCN0ZMZUFnTWdvN3UxTUkxcWZ2THQ5bUxFUmZCdl
dNamF2QzE2VmZ6Vnd0M3F3NkFCZTRQSVl4ejdhLWdYVUc3enlqS3VOVkpBcVAteGVORUJKb0RQenM0SlY2b01YcEV
ZWWVYWk9fWmJNOXRIWFd0RjZTcTRaU1RBSHg2VTQyUTZ0WDlfRktFUlVqNXFJM2NuRllFZyJ9.CCbUgX0KG6-I_zT
bamEUOZaKxWEaNQa5JhhTmIovBtD2b-8QDy8XuOeEl3Zyb5At.h-w7sa3cWuxCst_u.-dHH2g1WEBE3lOcWjXtQfw
SjSwuk1yEhVju4YQ5NLe82S0-VrgIgTcBtuUhcFv2qg100zWubrmKY4SBeskLi24VKeX-8dOZ8ZeGu4tmVfvSKM9V
7PYEcvuDGn6lz-oWQxjba1r97r0eEgFYiBAc9q141AoZeIXGv7CdTGpvYaTZYfNc62IEmUtKafXS6PhzAspCY0i8_
4MwItTa0VuB2cUCjlgFdPL0BRi5h7dGyo_sf-myRFQ6oCU0ejgp4lGxyZ7mVATz9TpA4Ki9RIsjfL4BiQfW2hWR8r
ujGhoo_ovwAHWLI8zNf5Wz6FvRrgTsaRSb8Lo7pyUCMppW93qujj3oa2oRu6htv9waXiSZpwC9Y.absbwmpYW35HU
m-hSd6HaA
```


Figure 18: HPKE-10-KE JWE Compact Serialization

A.7. HPKE-11


```
   {
     "kty": "AKP",
     "alg": "HPKE-11",
     "kid": "oATA96dt4yMW31bur8UcRzxVBNV0Y0x30-NZ8x6dW3A",
     "pub": "rtOlgemxnEE1spKpxRZjEawan7uQlgA4JPQKxViqjZE_ITiUd_cA3PQJRmVLGefIIODEIZqgoHhX
2qLIRDhY2oIMcQFsDsuzX2G18BcGIYNiUGU9YzoEsEat-KDELTJTirkaA8ODJnlPeJda7oBB08lC4pu6OYDLzQcCt
7iYdTCFPbrHH-wIDYIMzfM0bzlINJUTmKAXk6aNCTNAUggxgkaTRSNU5qUlXzYdjeTGeKoSayMUiXK2Y9ewM3qV3p
vBbmkVPqR_uahgtkk-81QbnOEho1mZVVGDkHdn6bMWiYBYQfQVvmRxhifD17TNMlLKYHROUudxoaZt_aMBBzc-dSV
6KtcE1ykdknmd6hMA1qFGq2kO5dk11ChLHQt0LCGDa7kVodnMy1HCbIMj-IF3d5tEw0Uwh2Y2lUSODKO_S4aJjAGc
olp1RPGftKhh73OqpwpptcYpeeaDPUxbJHYW3yaygfpjjKgpQiog6OzGcfDIyAKkefFRiQQfdBMEercKFqgnjpN03
zePQlYEjtpcNyhtg4mkcDUQfKJ5FqGbenY6DwHF3LyT3kTG-NljCamDcrQPA0ldXJPPTYwLPZlyzPtQRTPBhrhC-7
se90g38tOXP-N9Sbax8fWtP-ykQQbBQQk9Pled82hrRWyg5gXBnSc__OIDSbEUIMMFhqy-UrqnrkMzXxq5vwgp7RQ
BWTQKrwGZjICbOMiPiDlQ4GTD8BUqmRgUW0mXeaiRtMoeIzzHwpQpDLEMsCddfskNIpV4deJqcfi_8CVRY1LBrZyX
vVypmsSx_nSJb8k8S9WrBafG-DAZtAO8UAMmBnvOw6eaf7RuqVypexAkvsYW3bpFcAjLGaqqVuQPChSBRUQot-Wxm
BdET0kkTOUCLMpeK9nEi3Zi_jqG44lR9Hm7ZmfColYHhLguMKduKut03Th6TuhssuotLVmO-si2arOWWzRgB-tcAh
cfRWDIgCcOHEmQfKAYw2RRTcS84zvHoGBdCSA2ILzGAHBESQAcvoc0SWvIons9yLSvaZZrpudSHDoV5XDMbNtCIcx
4OsxIc_vEYSCFDPxLlcK5MNWzaGV4_Opgn5a89LcTyLgSukxsSaFxsvmhLnDI-axYvTezhzatjfmhYwg2VcVNOyQy
mau1GXXAnneS-9uwGEWXEEgA4JLI8zqVESOajMJQNtqhdYAPVfOKn1lJKPpz73abLNlU-JI6NxGSsapQiMfLbpIEH
KhP7Pc1hzg4nnwmZ2xgnYwWUski4lCqeWKRiRSYEqqL1-SMDMHKJRs04kWZ_HVBbPkXLAzOajAXksFbBCt9NLwkhf
RNnbVzQAe5CBAfUNUYyFuxWyw8IGZkvnIHngyKgVGztQVOkHGPnhWA1kgn4QFdyKuHPNNwEnh4EpNQBLXBe1Bmq6M
wPOJ7U9SrwnuDRtGCU0u2WuyIBZq-kPNE6Rpe44ZEKuWflFoMqBIFZspuJRvOKJteINN2NCk3zKKTamYpmNqI8Fxd
XHF3Kix-pNdn4MyWy6CXBStwXUiMKiF2rLBvCh1N2kgtbkZSh1SM3Lf7EwK5vBHKgtzFMncy0jTUHWKLpyYut0fp1
```

```
cyud8VefH6I4YWjqUg-IPY-XTna20PnMQ",
     "priv": "fhCGTZ2DqLNXWjKdD8z7uSd28DZfYszfPpv4ndr44oc"
   }
```


Figure 19: HPKE-11 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTExIiwia2lkIjoib0FUQTk2ZHQ0eU1XMzFidXI4VWNSenhWQk5WMF
kweDMwLU5aOHg2ZFczQSJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "fTSIrdEBYblWybEHWNZ5dVy6o_4iQu89alYtPbkuC-8yS7lzXiRyQhfi3GFKrj3HjC
oExpa0xI8I7YbiGLNDcqnS5Kk-CHSWsvhYM1OqusTwYXicPJuJtWEm8KkPsRlaY8aaosXGxSBfiIOXF4SS4aeDi8q
rVUNhc-8yMTcjxrmtT2NZPCwSiCqnhutmklNSs8liopmgSkAyUBNCbIpLWOpPm5OR3pJ3yFqm3MUCjh1e3qvrh_96
iQNJJTWy93xwEaYFk-MvoouRDy_mzVyd9bBTg6CJ8QyFIzbGBDTdOLbxKh83YrwBG5rvIdNnbx3ugNc94xlQ283py
NT6gERgyiTIQI_ifV9N7LhDRMwaGTjY5Acv2FWG6rIsyedMPcZqQhvUS29YLkkR4A2R4w8Pz_QzUNNJKhePWZ1U-9
HgTmP3zAQ3aTiscDNnwcA4r2l9BaNjNMsgh8bb_B6ZvucN4ZFRQcqvSjWhZTmVdOFuuC4TppvA3fvWpRCu3Pq4NkO
KfRySuIQ3D47ovgSgY6AWvIxssrPs7gf0BP_SzgP6pI1oeGLOXdOMFwwKdP7VVlW-yNd3KZuC-93EXBplVs4_zlmB
rFR7ENxZ0pS_ME4wQYH_muacX8VypPltvSrx7vABkHdNnkZKJmlNku-wxmc4SxRrzbCg-oN9ebSeX3me-1FVQXxEj
M0cq5_ZGeb7aAkDryxxfwS2SxTETd9aazR4ee2MKTIqo_Un7V0JUwjPJwV92FL3OIvv2pDktuYyaXrxGzhHrpzJtw
ZeDds_4qJ_WODXkF_4Kcmd_a-w754LO6fbhp2xTAeqvMJi6RIIaunA-vzJKhl576An5E7-FbOmAb0lZlRdanWr5z4
IZ3KC7x87mB28Wxi_bhiT3grX3PAfdnI9hDz6F7X7Rjjq78LWK0grili4z1VDx2f5aNijlktMZZvzKkQAou8f5OCv
Z1wv0Hi5fRFMQpK6As8XjdBYApQEPcrRFmdHwp3kuSCxt43KIkYJ99zC4tfZ36VZHO2at39PCaMPRAmi8h1Qg8caI
R7kO2Y7INiKDJ6JvY6jJxCtw91Dx2-Mn-KOqIyb_PSBqgexK9myfYkVor05bg1d-dIfAbV5ZTv68g6z6RAj5G2Lm7
vfdmjhhiNjQYeYCreFg0cZaKqcwRpPJokKW8vangv3ldqcj5oBp6eqnSkwj6PuHbNvTcbBiffXQLkgyUBAENPwpjE
zdLdreNs3MLCnv7SVtEmrCnnDfmUGoi15C_MdmCtztZO_YH-o6e_L8MlJChU5YUxWlN19lpr_CSlLbhjH7HO2Jol3
MM21Ro3TtW-fk4EVItP1N1vKJpCksTJpeLZRfTlr76jmZqUZW6qik8ZQiENHlxtG7KKhyfJAMzzOjywNOJDQq6cHI
aWiFI1pjOw-K1NMEDB7NEQNHteZLCZOycDmxnjWpDMB_9p2kfU7JY1gQbQwulLVDoVDEkLVB0PP7pITYEV2pVNu91
GwDg",
     "ciphertext": "Dhkcafzism5hwZHcEOiNQv4CKCbL7zQhHamZ02dGXV1gcik0REe6O-LhHTsrqKvMbkKBo
84Jyw8t3rw7L5m_X5g_yv46FHfV97ym0fnF5s8tND-F55-7J8eOrYkyn9C4Fpojt8L08cHSU-gkFMpDfoOa3wBTCi
TpX0V5hbPwKBJo1waLl-2GMRrPdh-hJiWT3qBYw2yO9nzyOnyEV2Pn8IjjXHzQmJds9VAUC9tOIs39d2BwV0Vyuey
SceDRwnoKUVHzwOkonyUaUpg66OnE_0GjARyogFdqI92Jd6_Hb6ASxFO12cGVqXR77cPE2WKG84Mx9D3UKy0SsWSO
c0jFOANvaOwbzca-XcSri0Pq6ljA-U0j-QQYjHOvo8coPSspbg"
   }
```

Figure 20: HPKE-11 Flattened JWE JSON Serialization

eyJhbGciOiJIUEtFLTExIiwia2lkIjoib0FUQTk2ZHQ0eU1XMzFidXI4VWNSenhWQk5WMFkweDMwLU5aOHg2ZFczQ
SJ9.8xYP0x1f5Vx5Zr-5Ia0t3Hohqo70_ATNEU4-luULrhYaMIrr9iWmumRtgU_2gKkhTgd3Eg9FN9EHMqPHURMne
jjR964pLhOAaWc76n82huEZkrfrBpbgQ88z75ajMoOIdyKrD2fcuSVyk5oLmvLxAfyR46iV3LPWMXpR1AEEmPrcQ2
zgzc2GNjQuwA33Hed_JfDqIRo-rWASIA9uP_JZAKqyDc6X4kygyaUl-W-TIYs8-LiR7SbQbKyN05T3i-6Cx_ym3_-
Cu9Zl_5KJFT2NBWkwKNE07m6yzr28ArOtxnLKpIfZT2LdFKi9x8k_qjdCQgTenjF5xw0Yd1lfj9ykAvKLAElQ8JMm
XaKmF-IRtSxbD9B-zCDNKc1XY3KuVzNuhH3Aj435JXV5oZEik-8lBsuSQq5cKw_GXzfwRei0k_4uzEIGgzruFxR4l
AIuqAWCx35_8VHPxgUqBei6kDr_ZUrEBiVKuSt0H7U_ooVDSg_IRIlC3uCvRQIeu20Lma_k7GMu-klS8GZK_9LIc7
kfbhl7jh0mKaPMTMmr21twEjMTz2kqAXVU6OwMtR2YG4CJhNDjtfD81ZJP2MGYUqVLzvNL4cQ0zZE4eUGxG2NdDjf
mt4ths85oXVpqQ9L7AeK1jeAojC8zi48eCtmDBsO06YEghNSJ86f9rZIRDvzXwuAWuRQvj05x7nDGw4b0GdCtJw7c
iUmetx-HqlYQACSztgGbZ9z5L9NAsj32sA8FIp6MZDTtEpdKEQVjQzSbppwmoVQiDKItu0X9bQbmZu4gtv5eHesCS
CcdAgDivS6czMGol26xNPiYouru6ph3m6Zv8gGjf7clEG5kiYewGefW8cRdLXClfEGGTJJn29BLFId1NQ_7F9wTAp
6fqgnKOzWVMpkF3Z1XkQLyn8ugworwXgMfxcCTcAUMMvHFeLWKkQNXWYYotJxVhZYpMP9usq38v764YCxPeSellIS
GFM-_5uyuo8ghISJxxgP4I0ZJ8QIdX02WFF6R5BFwmv45wysNElHlHGWFQgHr2-hbMx7xcnukEmZFs2QRaUZj0q6i
p9b0TKM0-XtHBEbavR4qwEpe1q06uw7l_imQ9MpwU8GeJihxN8AuddUmTJcj0iA22RAmUPD7XpasPC62VRq-rx9bi
7FaUmZfEmx3Ml8gKMxR-_ou6pRDzHOAl_B77hYeklKgbtqkdS6soJFpXviXUZgwCCEiBAgKxtmJZoDNsX6mB9pOlj
PHn9RzCry6xAMiWgSNblmxsv_BxKCW3bHJmx11hsmnV4ABIl_PIL3-qingouxIp0t3HvCEK0-QxaOdmQ8ERvbFjPk
iVtl17yt0RSdF07s24GsHGGEx5LoaF1_5hnIeOZVh5p0gzhbbCH-M1ZkIgCJ6sEBfUUAg7OILZOavDEkToc3pANfh
WPjobYKPsF_8m2L6iAq7_TVMnXRB4afgUYxWYv4LB4FFase1KpPgSw2g7WJ2Ecnryznc5icSHg..8SpXD2Tg30qLy
pKNXKeGHHEawWe-BLAB1jtRgCFc5WW21V9ZhMWoCZp5Ia2wxwzNisWDvD1NeW7ZhSGfsNj5d76lCLFDqexDfzKT-e
PtlLx-RTgbuQJSUUB7kLdtDn5szRUFaELsJjul0A-IODMaFJoJp5ysROBjb8Xw4eBcvRYtBtnW56gRsF6rK5eqSI3
W-ih0s_725QnHMGQQV2Oxzi2erHVCFZaESg8WxEpEctTuX8-EFoMlUQHUKJP9SzGDrbPtm1Z7EeH0occBB0fdDdu3
0jm7WXBwXDMvHm3_yoHCiO2TqPWyUW5HGxUJBaR6SyPviHL3APMlYZa7aHBnQvCzT77ZgzR4ENH5gkZaOuQzdMM24
Ab3NKM_HV7XCb89eA.

Figure 21: HPKE-11 JWE Compact Serialization

A.8. HPKE-11-KE

```
{
  "kty": "AKP",
  "alg": "HPKE-11-KE",
  "kid": "16yw6KY41e407komeO6qxf7YL28xG0UNh9TkrMAgTsw",
  "pub": "lKq4-lnE13ccmSgduMxLqbPAeVCW49W_HRc0LZN74BpbXtd3vBour6MEzvNTPOxCFUNadTdY-FkE
Dlu5vzZCtEGv5ja9TuyY1MC2D7rGIyQLt1E-jYGlgnHDWRBGh1AKT4y5VDzKp4WGCWHBbrueXJkTy_pAsqLNONceB
THMNZszg3q4Gwd3frc4UEnKi8yexpLDUhyyf3NCQ_ijZaCePMRL2eS8XLhhzDow7Hh0AHFzddQKTFnMCQtb_xJZgd
TOrRqfx4LBJlPKSgVy6IV7VzJU0HQ-pcV7LOhbX-RzzscWFiSnQGpUxTx_jUy7QWxk7BVUlnMFPHRs7jIjSYhNVMy
bE-ul68fEW4mRhZQGEoomLRgAgGhBUrIjXyAJghwTczOyFdvDqOokziKMH9BT1DAYDPsh1bVLVhUypYwVZJkOzvhM
f3gY48Ehg5Z8SigNvetrKIp0S4GKBRJmQgcnqsKEEyNlqESOmTduYzclyvlaK_WbxRlS7cELH2KLNoO3DjeY1aWy3
VgHzDnDAtAMDFlIh6hW57Z_FAJgDsOyw1w3xaonSkBzXeq6EJEK9Lh2yBKlWHKpGxNlLBaWNMUNZyQbYrBPzUQSr3
FAoMzM0cgd6ixYOBax6KQCdEee0vmO36vDr-BjhHIWDsM7FnXHMIVoBimzpxtAoSm7BgGRR7C8L0Sx3QUxNnAy87W
Zm1wzY5BbkMUImIRc-ImI6pAimXS11Ry3QZKfFIoPbgoWP3CSDlWsUvW1zsPHtKFQB6ctZqA9dsxUGIlvz_NU1lRm
xCikX_i5D7ODyGtO20Qc-JRfN0Gz--AZBvUBnuERU0l6T4VfrGnAjloaHXE3-dmH2WGZfFsN5jmuDjF6TftXkGAd4
XSCTeBRK8bJXMMEfgwySWkJ1paBqKgcz_kdxAdq_YgqJnBVXpuySakJpFFZRVdwy4pPFGTEG9efyNA4cytF-dcES8
CdosoQuhZECCgt1DmKwDeIzMQblYdAzLGmUPFm-kh9PIiSj2RbZMRqUWujP1Ih9tqZszsYk0O14PCqg6Q5srZV6Ku
JcIal13mGKmPIoNuY2hagL8Cm8SgPkIwJxspIuPdFAFMVW0skQgKvE5kr54uJqkks6fWNCcwrOsleZQgghAFBPUeC
AaPJs6ahpARdRAAXXGe0wHBZtCCMCisLmgeY96lb2IejO-GxXpIVkKQW5rqnuRYV0bo-TQm3eqZ8Zle9JImoe4gAE
DpKubuBsBYiJdDG0vKV_OCbqVo7RjfOOOII_JVgcPSHIMY_7wK3vMVm_9sVLgwTlgY3aeOf2xc2WuxB8CorF_YEXu
bAUvpmBTGvy_PMjBCOP-ZKmXjH0-QeWkozUHwI9PoIx5cN6CAup8N-UnBETUGo86Y0jvVppHQ_I_HDSsaxPwZG6xp
Ilot_-9ZBFSARk_CXTBaUnFoD9pyhNhorZwwzq1B60uGsATVAawNUnYzLA3BHm8pVqQujN8OccpwNoVA_J3pNHbms
M3ZSr1FOOoiiemIrzHSii1RtFjs5qemnMNyx1W3RehOz9jm3l2iiwsHMvqzWvDkHCLDW-62p7XiswDjQzsndtR18l
IDU-qywIMTYeOB6mS8yrAbnL_Gib3jqSQ",
  "priv": "2VXc3UQXfKmSzSm0X88gL36qs_QJMPYyhQ3jHiIF1UM"
}
```

Figure 22: HPKE-11-KE Private JWK

```
{
  "protected": "eyJhbGciOiJIUEtFLTExLUtFIiwia2lkIjoiMTZ5dzZLWTQxZTQwN2tvbWVPNnF4ZjdZTD
I4eEcwVU5oOVRrck1BZ1RzdyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IllaQTFjZEx6bkt4c0RXd3dvLU1nVlN5dXJ
sYVB0eHI4bFp0djdldmd0QjJPcHhSTTVGc3llb0JoLVdjQm0xWEg1TWphVE8yWThSajBqdHpQb1NvNmdSbnR3ZEtW
```

```
UEJOMzMtVnhmNzhEYlRRSm9DYUJoQWIzbFI4SHdYRzktQkVzNW5Calo5ZVZ0LXYtYkMxbkh6eExuclRkZ2lBZHpTT
TNFTHVMSFhDNDh6bHZHSGN6dnVzSUFsYmVLbUs0ZGNfZ3RzbUlfem5EZEhnZnhnZkRPS2VYNml5X2JEbERCcTU4Rl
9MX0RoVVBib0RvZERzN1hUMGJWdmdycnF5R0o3OFRLdUp3TmVGeGRjX2NvY1Rsb1pUVWlRelludXVpcFc0MVdKYlp
pNGtnM21VYk5vZGFDTTllbUEyUkNJY20zaWJNZEszemhoNjlEdWNORDNOV3h1aEluTGVnNjUyd1NRZE5UdGU5NWNU
UVlkT3dtcllVb241WU5KREJScWJNMUJrMUlxempsNm9fRUFMeDcxaW1LZ1ZzTG5VSlNUZ21QSm9MVFAybXJ2Vmx0Z
mdUTG5ObjNyV1V4LXVHWndjYThXTm9TSTVwQ2hfZEU1Sm5YZGtVaHhnMlBBYWxNWkZNeld0RG1URDE4V2pEaDItb0
8wMC15REZFRDNiVnNfVEpOa1JhU3lNM0RrT1ZSemc0eV9XWDJiMm5lVGVUamVGTHlSd0k0ZmY2b1NvMmFaY3ZDZ1B
aNWlLTWV2Vmcxay1CZXdyc0w0UEpxci1hbkVPVjZrZVBLemktbFlhYWxlUXlLU040RU9PZjIwZlNScXM5d3Q3RTVT
MVZodXdRLW1oLVNzS3pRVm9mN2YxNmJjR3VReV9UZTFPN3A5ck1ycXdPbzNvSUcydWp2TzRLazUxbUFHcnZIZzM3Z
DdINWU2WHVMcVRtelFfX0ZCU0hiSUwyNnY4TGd1VU4wdnJYMWZFbXVBaWI0YnBwZjlZTFo3djgtUEliNEVRcHY3Rz
dMNDVveVVUNWc1QnhSLXFza25OSmswYlpOb3gzOV9ITHMwRVBlMERnUzFPeHo5MVNHckh6NFFBTG1vUGtFOGxaM3o
3dEVXN0JMcUZHMThLelpMdjZYRVNlQ0VTTERNSjhOSU1Ka1IyWnNtZFExU21Xb01iLW5JVHlnQzNrbFdQclVuLUFC
ZGFpTU91dmFqZC1DM3BSbXdDd1l1OWR3eWdfaTBiZjB5akJNZGlWNkRsc1c4ZTg3Ykt1aEhsTGpHNHlOUm9lZHNFd
m5hckRYYVBoZjl1bGVnRmFXNC0tQWh0OG5IUlVJNmlQNk5vXzJ1TTBaR3lMeDFDcDRrTEpBYmliRnZZbGRhcFhqMW
JpeV9fcDc4NERjZC1oSDdFbTd0WU5jdEtyWHNJSXdRUVFtd3ZpYzhRV3lfZU50VEYwZk9kREZmbkM1U1JqdWNRLUR
OeUt2T01oSVB4WmRZb2lWOExTaVFXUTNpRUUxa2N0WFVZUnlPc1VKR2FvcGJ5enJ3S043V2pVZlIxRW1CeC1xQW8y
WVBQeG1OWjFDdGRHampTZzMyMFNTYnJPUFJjWXpMdG9KZENkckRaVlRsa1J5ZXQ0NENGX0poS2RhbGJBLWZyUFRNU
lEwcFVmVTdPdUN3aTRiS1p3VjVWeEZRRkRzUm1DQkYyUTdYYmU0ellFeWZDeTVBRWUtODlpZVBoT0ZMRWF6YmxxcU
9hWFZ6ckdQRmRNQnoxSlFEeTVyXzBHbjkteFFYUjNXRnRPZkJFOTVUeEkzN25iYlNYVmV3NUpDblVmMFlBZkxMQkl
RVHhwbmF6MXJYQkJ1ZnQ2MDdBWnhnMjVYV0U2VmgzalJFU1NtZnFrZllGcjBqQzJmdnpCVTUzR1lDRU9BRVJYODlZ
Z1ZwVWtzYjFhRS1OWFA2MlBzU0JKWHFZVUItcW1xaUg5cnVsMmpmZW9HS1BJVzE5dEpjR1JpZzdRVFJaX2RWRmlTQ
SJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "cg0f-dpji5qHsko5",
     "ciphertext": "0kgNEY2Uu1dYAhc1--H00VfnQFJ_FPoYxPmqRyQdv1U624O-oFv2WXraV2ML4nMmKPpVY
V6CSrlNWMzPgkSL-JFqi7xdaXhwXcdUoFWcCdhSNdywiCidhAMDkTkZ7hBWscslaVtzvpoFyDdqaOHQL7Ybh-UaNg
wv7Mvr9ReHyVP34pdbOibvnLiCLIpfqxMYGYqlYk5xV6jzMr08BZM5sQe_G89SIzbp_kOORWIiHEtX7x92fK1zi-p
U8fAZX0jYCpg2jnH-bg_NFsYeK2GIpf0pvxDs_1Eq4D1ZDsi61r6qS3wFA5yjZy7GBddRfh6OkwFfd5Aj1xH9N0U6
xwj5Zj1QGGY2N7sD7jF94HT1l8lt",
     "tag": "Fwv6YMW9AqPTR7Rb_HF8aw",
     "encrypted_key": "LNSoax9Ga2QpxI9jxzEGQNXnKignO9Su9hhWxKs-o5y7DplfHR-xvzmM9EJH8aV8"
   }
```


Figure 23: HPKE-11-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTExLUtFIiwia2lkIjoiMTZ5dzZLWTQxZTQwN2tvbWVPNnF4ZjdZTDI4eEcwVU5oOVRrck1BZ
1RzdyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjRUTlIwcjdNQUVpMEZQZUlBTW9WNWx3MWNYWEFYSlk0a1VQcGN0U3
BIazR5eUxmSGxuUl9VaGNDZnpwSlg4aDZUbG83XzM1MEZSdy1pd1lNX3RTTXBVWUJ2VjBvdnFWa0tnV3NGY3A2R2x
uRi1ld3ZsNUs1ZUxaMklYN3F6bkpfaXk4TEFvRGV1YmdudjQ0ZmN6aWV6Z1dfOF9Ud2FHUzh0TkRtaHdTcllOZ0VU
cGwyYk9paG9jWUZIOUhnbGs1NjdsUVlLd1k4R3hSN3J4TnAxWDB2T0c4OHlCV19QVGt2U2loS2ZZWDJsV01mY2M3N
VNobEtZdVlzSkxYVG4yNTdtNkRlUjFEdGFRRVAxMkJJa05KR1pNZlNCeF9hR044NU1RRkxrZEY4VkZ0SGhVRC1OVV
J4WnJSMElmTjhQbzF5UjJzVGx4TGwtOTdlZXBJVVNDNEF0Q0JRU1YzUDNCbHRHWkRGTjZyNm5fT2hmNVBDTmk3VkZ
JeG54emZtaEtTRDFGY0s1UVNucHJGQnlfX1IxWVlpVVkzZWtSN2QwUzR2emhvMEZyaVZZY0d6dmx6QTNjUENrNE02
elRCWGw5Y0stQldyRnlkMVJCNnNuSWhXRjNmbWRwMm5EZ3dKb21JdTJqSUhNbm5aclIzVEtUUUllWnkyaV9icVFjZ
jdGdENQTXVXQ3lPdWt2Vzd5YURBOTJVRzdNTnR1NUtJMXVyZVNZR3FCdWMtYTZzcmdnS3pzRDFYeGNUckR4Q2RsRi
14ZHM3RVVpUEZLYlY0RFNCdjhzNUpZTnFhMEhCSHd5eE5KcFAzQm1PeDZPUFA4dzEwcVJ6SVBBbkVkU0ZLWi04cWZ
weHU4aTFVRWM5OW9ENGsxY0UtUERLcXlhOUNuOUtqenJodlU1TUowOVppX3o0eXNPQzhhQ21FQ1RwalN3ZmMyWkZZ
cVJXUE9VSkpNTjRxR0xodGJKNmVxUDJxX1l6Qi1WN0xZOVY1ZXNpZFpYV0RudUFVdkNKSHNDNzkwdm5fMENGX0EyT
nBRbHo1aVZqb0d3XzYzUEJPamFLUTYtazhyY1VNd0NTakJXNlpCNHhkdElGQld5Y1NZb0pTSTczalFyZmtxZXlCOU
dRV0hTQ294R0MtcjdGdlJiZnpPRmdyMVNrdjFvLXM0bkswX3MyMTN0a3NYeXlySTR0dTl5OW1MUjFHRktjRnZvalp
IbjlnejRWZDlJS2Ywb3VLWnl6ZjBqVkpmNFpJTGwzaU1FME5uTlExTkxXMXRFUkxIQmpfa0dJT3FCckRkNGtsdGZN
N2Y3QzFaSGdoTzFkSGRzQkYyZ1ktWkU3Y2FSd0lNYUJNb29RQW90QjJHZkxXNFJhaVlWNVZwMGpxZ0JDRU12WUdyd
nluQVRSOTQzVm5SLXVaWE1YcHlTT0MtbXZOZnVmbWpSVDQwR1c5VHBRRlhrdU00RDRzdWtCalRMMzdSVkl5V0psN0
ZMbUQxYUJ6TXdyd19ZY0xqQkp6YTNwXzhTcFlnNWhJVVR2MTNIbkhWeDcxZFIxQlB3MXlpb1RXb1M4NmFTeEtKbWl
ORmZabzJlUUxaSzJST2pMbUh4N2gzcXNnZGJaWkMwOWtkb2c5a3Z6Q0NtM05xcHN5TU9vQnFURVV0UC1XZHoxTkVh
STBCM0xPTVczNEV4REItbnZDMWp3clNYVjV6Rk00Sk40dFpsR0JlXzFfOUpBM0JmRS1DWWRNOGllTHhzMzFjdW9xU
HNodVU3NkpKbEFVZzhvTnAydWhMb3pPTVRFY3ZucURBeG4ybGFqUHU3dTR6WHJJbmoyUnBKUkFoQjJWbm1sY21FN3
NRWUhIaVV6clpCczNrQWNnaWJnRWtpRFExcG5xWUluQlZXRmdCQlFTUW9XUEh0X0xGazVYbVpnZktRN2FtRXU4eGR
SaWRzdWNGSnN2S3NOZXgyU3NKbk1kTGdVQ0VibU56M0tOakZzVnNHVlBmWWJ6QnlhZmxBUSJ9.dSfMqiYf0VBU0_N
Fc_xhyV8P9QfT9NwL2Prsf_N8bBQEWtVJz8ekaqblI5Y28Dd9.JdlIcfXr_xiVPWp1.Kg09nPOFMWSm-bV6bbZh6k
6qpvZOqVn68IzWf418Ifn8eMLCdq_cbUT79yi9JjZq8pPIXs7stQqYhIWjI4W_cXvVv2sGxEMXoy41A_6mYMi2xP5
bdxqfwsjo_YjtiSgBjpIutKmjrFlYc4hnUVAW8VTDKi-calET2lJ1b7CvRJsiGrGzM1snQxLjCFwdJdeWrUESw1Dm
sqYdOsNdPoP9uW9AOe9GCYO5MPpmbywwxPjUZyQi6iTcu2SAfySC-2cp-wkdcUapAporqOP3cWSmVCabIwF-fq_t
DxyM0t5ybKhxRWdk8n_-MN1ajVgplT_1RoOhaPNYckI8hzNNbR_eX0owVJ98CelfAnds-PUN36T.SfL3UTfQjrwP6
TL-Q2NJbw
```

Figure 24: HPKE-11-KE JWE Compact Serialization

A.9. HPKE-12


```
{
  "kty": "AKP",
  "alg": "HPKE-12",
  "kid": "9hyupt1l9mp8RxMj0gWDx4uZFh-Ltznar1iPyKSOjAI",
  "pub": "T5e9TgLP4Bh4gVFU_cyS4_iimjOLAvFmPGemydw7nRVhhEu3oncfGINoOfi-fTJIQCvGKOzCPbVa
rggmVCJkZuFkchMhCeaFA6G-RWAZriFRc5A0XuuE3pJLXHnNj5WfTrOMiboZpVeDfjx1NvTItrI2NKhEhCiJrFZOz
1xVy-aOtsMx7pJYR_Gp1ReG2byJ9LCgqeyPyTeGXCdgGBQg2gLFguqGlqmRNGCEkGE6uhUpbehBn9k3CmJtMmMZ_Q
klIgMebBy1fjWzjnSRXhu0v9A_G3GJQbGDGxuj_Uoj_Ma5BEWOu9ZIKpewyEyMVTqkDwzHGtoAWRKAfVmcImdrRWs
vJja0H1hN_uiL-PUY_ZyyVOobGfVXdUgkJbFx7_K68xoCIhKmHgAlzSC878o24UUrIXopgrmL7fJppwhH0-URz_wq
tOGlz2tDMUm85CkRzcdTMHqMpmhIYbCSm2dFwNZTZCpfboE0cXRRLHI7C6YFMXFZTGmo-ZpOJ-FT0RMnw2hWnMS7O
buDxvrCSPRdEACseAaCvDN4wRAt1YGN26gVvAo7wIyqT5jDLfiZ05jCmhMQwjNzsYgQGgOwAGHNlIig0lAAaQuFlp
UjpEBzsXEc1skNrXuOPyhn7sysibu75LNvc_hsXRgOF3aIKLl7OQBIe9i7Z0pjT-EHCUGLR4CulIscQCc5UKIDb2d
C1OAfFfHETWAfhsUKXBmsQKECZ8Rr7GasO2oON3pBJONbXHVVS_Ybngle3di_THMO9YOmNtt1ByI75egWLvOjD4Q2
XTdjBnh9o9qa9WQTUqB1YeNzv7yrDtBAFIQecORT89G-pvhnkOcfzWeMrakW80hGfxNCE_UsgcG4f_csFZlophaQ8
UGu1sJ5DgeFFNOQ2-AMgHk52LK1pIdQs-ONrndBGzrEEvEEYokRD3UQbwec_eYn_djLGco4VAYdedodBnUbezqYZI
ugd5xVRsfEB7QRgDcXeByH7tixrxUvckIHIJyngJWKFRUlLCyX8owV-3B6K7VkvkoTFlWbOzqtViGicWw5ApwfNBg
Vu_hlOAY8bURbWsGLc4wtQ2ZI4_GNfKgTMULH01CMPrst5mNfYvgJsNVqlkNIoCIDzvhZjSjGCHtJOQYQzDx2TpV7
eYpiocM943ANKfuz3ICDApETaWYeWFdgn6wS98dDfQFzSwgq6vEGT9mQLhNOGZWdGlJvrVMeExmXsrdim9hsigIrS
otrziU8wyKsx8JMl2DMXAiA1UeGJoMWPDAwM9ocVhHF8-p1AjeuGoI3ieqVPuKBufiEO3cwZtwSwRtCR_ZnGDfMio
VtVMNPcfUGA_FxyyymKDmQBUoYbwqhTId7zDlK0CgyJuNn2oEa4EYxmmRgkbxo7tl-3QVfXvikqtdjdeRWuye_h5t
MgEh9o2O0QmcskTK-R3KTt2HKwRuZe2eBjLudxVx8Dppu2vIodYJ7YIDAoHZQ9haev0du5cCbfpReqjtEbqRYBIho
eRa4lppjcFp4C7N0nFnIAVBGPRnINkCQkWImdiqWMtkPw-w7BmzIXVFAt2FpGWlWkLC--mmk9ctxW-bPU5ctWxgy5
3A3qUAq7iei8kRCujQnCYpNawRgHPhEOExmybupAQwYS8mXLaRT41cgT9zPxHMtJ9MjugQaayObZhDNWGWRM1oT_q
KOb9ChrHNYcsTJShMnPRKEuqrIaHhPflyRzGcMTELK30OqDjzCBue_5GAcNJOd_NkY5Mlb5GkNZFuNvSdNZuWASHC
uFrEdl5EEg4FPkuG1OwCfyDEl36Iqe0s72NGrpzClC_inu3iN7uBiewrA5MuaQgArAmeTKzTJ6xlh0acUIFljdSI6
fjVIPnQxd0ZgpSi4a-eRNNh7XVx6_FCBUpMx_upRo_dbkum5sykUyFp9lBsU-lG2asWmAECCPOF_vYNxjfZdx8qMO
RUAlFejtIA7Y1l59Twj_sUpgRt1MqifqHqC1hl6r-TO4nkEpGNIsMlGoZssYXqF8VKqy2xYtOO7z-ekQ4lXuXbGU0
p0ispKA6g27jiD_i3cOqthr3qfhE9US8S9vX3Se3fFV1vtqXrmzKf3iHcEGzWdhwMZNnPxSXIbXrgVV7IIfgrDUd-
LRuiCU17Y-pOdgA8CRx8uZt9MAuQH-Llt1DZ-Uj9VqTqHXi75vaOmfh9DG19qrZyV2p-IqT_B7fpqd6apRjdO0yN5
aybNY-Zq",
  "priv": "HqetV1Ap1ngNbKSzJfWFZKTK_8QjORJ4iWF6NW0GdV0"
}
```


Figure 25: HPKE-12 Private JWK

```
   {
     "protected": "eyJhbGciOiJIUEtFLTEyIiwia2lkIjoiOWh5dXB0MWw5bXA4UnhNajBnV0R4NHVaRmgtTH
R6bmFyMWlQeUtTT2pBSSJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "mOKslMw24OI5dL4k7tqGQtuAJFYDzv80cC3Jjj1qDIFOwjEHQpXE6cj3sCsX35X-W9
nq8F2sVX5QNAXkeCG3oW-dpOyy9u4lOxLcxDx2L0u4a3kdSNTOFFIRyrQnGjAcRw45RmUZWB2Q0hKRBT-5pkzOnxT
bSMSgVJbsztaYYWw34YzJ5rH-UYLsLVSG-gIkV_ZLDn7jiM6uqh9_IctnIDyJXi21-S5VVUNKzBPTe45ZWuaO-bWZ
VzmfSVbX0V0KeK92I7k3r6Uk5nRBTd5_9tAf4-xZgPR70p0XipvVTtsnfRbBB0AqyCuMqNxOoaUCijogeqA6rrVLf
FwrGtiaNlLkloQWgVOWL9tALDoMcSBE874wQ8_WKQSavGAkibe1LPFveg8ak0xTZkTx2LQrDjwtTD8_FIq2e75lmI
jtnxYcr0N_bccBVeEhDJ9c_XSBzUyavA659SFxt2pK9HLGSsRr5W60ySkT3ROMipIf2SJ1tkbJcHOgFkofKti9II8
0G7C91V8i-gkk0En-UiuE5YAnO87oomCcH20rm86TaVVroMqNevsUmGbFwXzxPXMWHSrTemhN5QGj7iWiIngFjmd6
W_o5QIuEz_6pCcQoYyxp-EVRP7ZJj--FQJKR5LJQHCrrlCqRXj0fSuq-eraWzbP0jfFmiDWO8J0uIflYq3m1TXoR1
P5mx9dPWYF8e9a1p8CldRMwJBbLJe8KW1ylei35Hr7jY1raWMizfR_rCQ2KJtXKoLSmUZ83kx5deEILbg1-VConWa
mEmCPFsdr9mbiqX5ize8W-xs4G9UT0ZZcIfgLKuQctmIUI50A6EuVQN0zbsjbiIJungaNc559wgkr1McxdwDdc-sV
g4X97Csx0_7tDmoqWsKwQbquKfKfArkJmCOcD_LlXIPP9BnKmWIB2GYpUpFiXLqgxvKxAowofMT_KUI1w250GnK6n
L8eNa-HjR5y9lpQizUpHkfVRZhDq05ZnqTxt2hTV4lArzsThYjIiv5o3YuyOOQGlRsFPMvU-Ht_fEhhkEbQs0IrJh
KRbzFr--S--keDsKHG6MlvehrJf0ZOqmNG8m2KAaLH-UZnuJcephbc5hZit5KHEfRlBno7VOWQUFKdNO5xhgn0F3p
ZN34xnGCA4zbfuFNWhiE6O3C-y5Ya-O9oiu2IWc49GeS8CRO7s13V-P2jHJm97qfVzBa1SsG6Ue3UjyaDqIf5wXAV
btxW-oCOdHBFJzOkkv6YRUoZDuLXbt_2ghL9M1sONfn4lhkGh77OloU2S_3DESDRQTC6Cj8i3a-5MfsiPBBfUzLtW
GAwo3p5BzPZckSFnRj-rA2keculv_gZdbNcFAEd-196zTAKK8zCEssHSDIVR1PQXSmsRmy_GztkcEermDBip-AgTz
gP9JbP2GOQB2M7nXVHprAmAr4LJH_x_jdpeKW9TZLIhM7nhNQ6yvWhj0hCEKm1SGb8gTWoJVVM6bSilIzuviKBuLH
zPV_0WZPmKNeO3a6Tib7xFhfcN1GgHWxhxQhWlRj2gHUmgioiwjiVncLgRAqStkkGnBIp8GhdxUsoQfv6ydnmyQeP
Gl785KSuj5FkCSQBupSPvURgDrwB1Uo94iBLceF9jfYCa--6m5syebQ7wAPxhmPqXcTaH9q6gh60cwG0rmI_rM5LO
-V1ErmzoeA85bPLA62tgUJoQP0P6BWrnsjvNjutK3KdxrfQfSPP_5QT1oCkEoqrA67EN3Zn0WBLnZoWVYyum1XMPx
55PMUfd-2ErnKG-4UViW4pNr-TfvQKm4cFG4E6V8KJC0Zg3xRvb3TJTLp6B8tsZL09bkkT46KuliGPuH0EXqG0OyA
MqdBFbkKuNBfO8IrIDnX9Guh2U_5Qv-_UadYifMywB1ndqM_V5Tyi6YPg73abAZySg_vG6lBJfY7ZmwmpL3PR5QEU
I-bjpk2wna5E4yaNa98ZgdAeDls9ZMPT3KWDH0r9J3eua3yuiqdfzS5r5fDnlJZZU-9213CwZEiZ99B9a5h_IKr5U
jLVIM23w6KdPKnA8JAKqkob7HctJR7VQhJQ1SXaV8I-AVMqjcl7Yu-GnZY6TfehVPMYEdC5iKJKvJZVvojyFnZanu
ONjtfHrJr58P3RG2dYQwruwhheOYewNcci99LObrw_AIHJF3VhqpU93kdX8RDauxZJtYl2kDbVaedgN8P05253i1S
CBoUVdBF8w9VUbJalz",
     "ciphertext": "6HfdMud0wbJkF5pQOcdQYbyl4IeJhdfWzlm7oZTlVCz32V1Oc5ls5XQEOpaHEYUQ_DeKi
6rIZbTrPfpkt2OEFLadbL9sJrDhWxxunlAOfrSF-_cbp0gb7qA2OYCC_gfhTD3yVrKIAtNf2E0B4W9RUGg3emqynH
Oa5A54GT4WHSW7P7KCiAbibiuBFwcEH9GBxy_c3UOEcfPeytw8oEUhIGTApMgAT28m6qUaZv_-saa-441Cqz8TIg4
tLnZi6ir_PGALRXB_lv4K7iXIhChVZKzNxb60dN8Ka0BYsfh1pp8Bg9RduA1vaaK89KmnmZSMUB08xhykJnLurS1e
aiLo75yIg7ebaIkmHObjgKMQYR6XWVws5Y8ofN_R49GjCIEXMg"
   }
```


Figure 26: HPKE-12 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEyIiwia2lkIjoiOWh5dXB0MWw5bXA4UnhNajBnV0R4NHVaRmgtTHR6bmFyMWlQeUtTT2pBS
SJ9.BBkqIHG9zOgCdcTtbrFZFzjenqoHnnnpNc3BO9Q26GkwQ7NlKnIzNuHBltZTSclj8qS050mnCThc5IQ0t_ba-
OVprlkUvcUxUVpfblG3znGmZ8gqHOMOajxu4XSs1An4J0n-oa-nApPZMCLf9cUgWHBRK8Bb1_mHBFz2sKrlzeuBNe
791X8CgbmLHpwKgOjM43P5dfp_84X3lPp7usb43itWyACU5m-iiLNnL_6o4uunKheCv-hw0BH5AF08y8xqku_3j29
kqF3Hi2g622bKm_T17JuNq9BRY_OeJLxuExoWNzULuFkk_OVfl46DMU7jTggkcbvWO0Eo67u5UTRZQaJsee2LL_Q2
S45jwOGTx7JSyOANVUH_ypTNtIl8AW5N0iV9p_-UVsS_szMea5tiaJVZMSOJNngbVJJLeyDZ0FdJxDsmfa--6nxsc
YJRSSN821SIT1OMLonFIbaFXCSzkezwYpIVBmYm6wxmkRAhnQbKmjMSQIKMvVGXdmi4s4Sw_8ciniTEVj2DYu9q_9
Evaajc_tBPeZYqKiHawpGYKizs1qVm3Oy66CqVyEKfyu_C3vMpgvVhGDZU0iLpJQCl5rixQ8Ab5TmDoLJFjXVwh6k
fG8k41W_81b4GXfeZxOQ-nWuUWKM-1yZMxYK4lr2UmnJYduaOJNcXcnXE-EO51hyTBSe5R-_lcABIga0bt-lpJoXM
rBiPv5KRml5oIJnmwlCz5kYIhA05x-V7Z2b-1gsDry9ONrjMFb5L7-sqHp2qh6xEzpekILmNOYtBqa6hi2iBuadGK
JRgaqbDOBeCmh6ZqJJrS2leKov2FHJc2TpQ3uVNipXTadDEh9ImdSI6YjFjVCZhkyu90OYzXTKS-oBQQcnFHa9rOp
gMJYmJQ0FWjvwoQwGJ0rCpnWvfeKUco6b9xXBWeR1bhMwsQwyd39Z9Isyo12w8iw4w5oEfxrr6xJcDvwCkP6dyE8-
0YHT7dIcDwyQDYdlhmz5gU8vWJiREPwvjBYEVAM--LuNbH5drUOczp1BaX1WtWt0RmmYNuL6SztEONqyxyvTaArS7
30hmF4kvnuDYY-iGW_wFcvSAMZwTJUBhYG2oEFmldhKMKlsOiOgeZNl4yn6xpbsBuCmBiTPTTqUZoGCYOjgF4HjLF
zW9u2apfrSUNk0P4C6cM5IsbtfkJ8I3cfVWaqpLxTfYog2nW_iM7ptTWe9Uja3qE6FWh8JYBDF9iDiWKi_kx1NVox
8SwjoCgcd1kmpd8z-lM_1GY3G-mU-_j6vpJiL_-t_uUZcGtEL_yjorVvlhtWkZJrzoMebbZ6B3LNMTXdFrf_3O8nA
s2qoztNrYMHoJF8RjXRZ2ofV-CBvmwvDjaoPiV6aILWwlHEKvlUXPlKEKihP9ELlGPfOBkMMyUC0isLTHtXuEMx8Y
36nQw9-vCaaQTj9TfQXk7nz1O-hIO-BKPc-wi1s3T6b5mHQGDQu-0PsTYo5MAwEYoQmyMEKG5G2TKn8qsbU_qb9fe
gHPyqk2oLtUJvNBjQM-dt5u2hRWHX-MsaGvud8EpbsE4KLrxs3XMx3gWsEw7zSACxNGeXjiLn09XCGslbnGma1HYb
M3YbsO_a5FSj8EzgAAYYuznqqlbgLN26VMmar1hfB4HUYvSjOW6sYsSIY7FL8Wk3rKoKKrg1xC7RxqY8H8mKfFRPV
z_d7FdmBYvA-fKua0f4L9XoFnPf91h-L2nBL2-0vhx63rSTRZUlmqHmumNRYOHQN4ofG-QNX7u62EriJ74ZrrC2i8
JKu7gdYK0GRjxhjilNMp3tcDeD_1pCVEvepJD0rSOs1QUfz3RvDxEzDmTjYgZhwYG_QmOdLUTlj58ZiPVTz7uJ4zF
pqKpEcdRy8Lld2oqsNakHpyDBUGCa_szdihyw5joca3g5mblqEporj-FxEC3VSYGO5UHtdxEd22CzgAJOmDe-nstu
```

wyoyG3xSGav3vU8c0CGzSKxRtCfcFuMRSgbDQpOHcLv6XTcW7cIpUgrb8KoRgpvNB76wSQGALKPQk0CM9vLMdTRRt
jvsyxDT55QByPrV5Oq3Tcbw-BoxowPCLrnadERLacGRvoJfgEC3CJHrFT7e3p9FzBHH3lB5qwsn3h3twLZOLZTfGW
LWvh_EgzAyS7WTcIIArPqjxLh__CKHYFlIOBT-JPle3eyYPeOlZTFFDH91wbqH3En64dNDHPH586wYzY5Q86-H7y.
.83T3De69LdZ94fHzNW7dsIZRSHYpx2Nx1w70DR_7nfhidGRetVk5Fdt672fSnTvML6PzfIX7ClQwUUo7wa7u1RSr
pYu3gAbdvGvhz3abVXD289UYVDbPhf0v5zg60S-k8cuyIYxPrP-LvPZX6Pt5Sc8ju9SGh5G9RVvUF40BIoPUxKuSU
-AISsAVsGso33kqob_WgeCl4rt3r58iNAXeWCpH0iMYkkjXm7attTxKJzDb6pVlcGQnHqh4uJlHp6Cj35IT_SDgN1
jaAkEmrJDjoktxx98e77joX6ti1OCWlBThdrJjXyRzeiD_Q7Hv-iP3aJATSgKKDv3jmuWpsByNylMBH3GiHGMXUSA
bNYDEn8v4JBnN6vqhdC1L1lPVS8e2LQ.

Figure 27: HPKE-12 JWE Compact Serialization

A.10. HPKE-12-KE


```
{
  "kty": "AKP",
  "alg": "HPKE-12-KE",
  "kid": "BsXA57jAXzbAJAOhd53PswMI15Hkgk4DZ5Q_FMN_E-M",
  "pub": "8gl3omYa2xs2taMSZ7wKMRm1AZVTxfgNoLQnCoEX83tgYOtAG8hxDHxSXrcjDvYbcciEXIaEFDOe
bVZ22raDEttnFBYYkGHO49Vx1eS2u-HPn_uC0kaVzkiUBKOF13wLr_qtVaIJWGCYO4Kr88pg6_e2JGVCuplK_5s-H
AKYQscucJwJmKg9ImAYNflPhhtXs2NH3QqkAVIPHxBYr5GjVhVFjeazH6wIKhu17btHecdwuXSi8xYM3pKuI2SsSa
Jt74ie_Ic8zHROgSkgUhFdV6B-XwKuMuCUoFMjxVdsKFcdfdvBa1tzbMS4XUec8FSbQ5am0JRvYlR4MbiXv0dO6lu
mQgZBw0yBYBmni7FrNPMoBexobbF9i1MdIVOI6LpK_2QjD7l4HseO-RIhuKPG41mWPcmwEBQxR3FjY1uZLMiH_cVG
VGxcD3Iye3AUlaNDTIU6HjQU-gFVgPVOpPSp7jw26TY-o-BldOVu6cRSgnYLROdZrWE0x-MPwJJ4UDpWu_CvjNs2T
VxbSMoXeGmyWDqq18YCTPcRQjUGGgpahhgjh5d7iTNIoeh4TDAJB3cP38pW6VJerfDKT8d14asQ8mlbgal-kLMVpL
qF5jS_p4pd8Yaas4iNWaGKIImtGfPFpFyuqPJLMDGNHRyGZHJTZ3RdjksC7ONQ6kp-A_JozJTAwdUzVWiLbnTFdhq
SlWKcI_k2HFN_2qWlNHYPM0x5LSVuxrwxBQJ7x7EwfWLKvdAazFM6flc6oWS_wIR_f5oh1RzKSMyZtikHNTvHJUFb
8JVVa7hg8WeCaaCbJpvOd4UwAuXOjrN_fsjGbqbC4GBXmzyy5eUecHRNIMO7JAeDXHExoiSE9RRKzeFUT9YIbAAJM
oUeBfk7ixAgKMWsLsm-63hUlcNsL4qWJalLETYvQoGjj-AnFUIybPgo8WW7C4wDkDhq1pwLFuFCySJniIRXrUR8HY
tcJKRXVgJfxsgzuIcNemWQtcanaUSpq0tYlLS4TcMRcSAPtyZlTvqCqgI5E8CSIcYIKBxA1YSMeCc2htEGt2AQ1hY
GE6RkSqxNQ0Sg5Dc2sVZW2MKvCTc82OcJphiBTEFHUswKCOpWTCaS16CYS9UHn-c5vRJGmlLNyWVWdme0qLgE6Nox
bayMwwtgOICHFkESrDTE0TlpnhEbN9UZhFhQMpIRtmqWddigBtpJFQKKmcXHospN12apeJVLPFdKYBA7YXOZibStu
hVljIwF2aYlAHpTLGuqkBsWuDMMj8FDgSVi6BQr-9fMtkOXvncbR1Vi68NEmoRWt-YKnjs1JEw8QVwC6WCDygqZKl
G_tOSFAgljsLkf-WZZ-JN8nRGDXPmzLcTLmxS8hZaXkqcSHVJij6bCVoK9olcSccac83YZd7E1SexjwWzLR1pTzjV
ZZ_rPK8I4asZxWEGIHAXMtjJlEGWA8UV7tBdK0tc84DDA52kRhUUBmcjAU3uU1csQMTlr3zwccyMfmqsCtNoGESG-
zQRRi1zAuDpnofGnpqjG_piD8WC85ykco_JqzJMK1KFR90dYThmf1HFwEDtfvDNPSyLOiSd4dwRw0hUB0XHHLGNwK
kcocyI7pBIBl0xJO8RjuQuxacYyh3ND1BJP4mQQwnqt9PYomxOhs_OK_HIVwZssf2eKEHvJk5Am10O_N4KbsoebXA
Zg34tK6NSaKWvFAbkSkWmuYWm1fnp1bBM1Qxs94rETZnXMlVRho9IIQbIPvpFTQ1QXvbzPFDs4JCZKY0F32IC7f1O
8oqvBmAgjtNqaLRFs6dHKzOJDsDTLjQMMmOYTUYI4HHBV_vRI3GZY3EcWxAWn8wcLY3hBNPshkGrJBIfIR-ZgvLwq
1kFj3YEKUdIPGoXGm_RoFYO0jWtFe9KM_8Y3IZxA0WU0WRhhv1azGGMnnkqZLxNJFcWZfsMVQcKdiflYXld2Alp97
1bK5zMTyKSJGEanfvLPKmkDWXlyiWnF07TAfks5fBXNnxCb00uT4wKWZ8vBtce0DkE_b8dYLMlbqSCae4Yb3HkE0k
CwnqPMKHNzK2C0QjuaBAWAyxotOTs3bdgV5f8oTOwaRHkaCZqKw2Z8mtME_n9odztcVrqHyDHY26wUSZDVWbrpyma
bfcph3uMuDUWSRPnaNi2FtfPrTdhRfwZ4vSFA40wNAzC_ozZn8x70Negu4AGZSOXcx_1lBDH8tYyzuvwskNfttxTl
G8dZAwzE",
  "priv": "0P1ur4tTdzfRWIfl8Y85Wlv5FC3byzBUzEuqMuXjdh8"
}
```


Figure 28: HPKE-12-KE Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoiQnNYQTU3akFYemJBSkFPaGQ1M1Bzd01JMT
VIa2drNERaNVFfRk1OX0UtTSIsImVuYyI6IkEyNTZHQ00iLCJlayI6InduTGc0U2dyc1gzR3huREpSeFBHQ2RQSS1
3U0xSSU9NR2c0OUc3SVFaeGFOTWRfbTdjVkI1SmU3VnY0T2RYVDlrMzJTNzdqU1BKU1k4T085cVpfWk5fYmtjTngw
WWZTNFZ5LVY4M0pyaWtYVjJVNV9OQ0FsRWE1M29aX2R0MFpLWjFGZWVKNzNsNjZoamhKQzZabTVMZVAzS05JNHFvZ
lVsSER6dHJpOWE0MEV4TmY5V1haRWo1VC1jUnI1WFZ6MWNHTzBGUWJqMDRNUmVwOTNTcC1JWk1kTThXWjNRN2dDeU
pSaG9SUGR2R0hxX0ZhaXdLVVdKaVBMMHhkQmc3VEttblItVmQycFBrS3AwSG9Cb3lvdnhJNXk3TjdkcTYtWllwQXh
DM2Fzd1oyazBGRVhTS29kcmRrbEQxd01kUlN1elpFSFNVaThNTmxMSmlDZ1lBeUhNNm5MdzE2Z2xUTnFQR252VkpY
TWZNT2pSMVo4MEtiVmd2MzhWXzJvV0pIQ2NKQ2NFMUR6WXR5OEZKVC1sbzhVUzZoZEc0bE10R2tnbHBqX3JPUmVIM
Wo3a2Z1NlpCQV9wNjMxN2V0SC1TcUhTOURSZWYya1NLckgzNU5TaXlUYzNKMHF4aU1XbXFyMGVlenRqdVpCVi1RNW
FDUU5xNjA2NUpabW5rMVlrRUlGOGhCa2pmU2FGV2ZzdHRWNG1Ia0huXzVITW5TdGs4c2NvREVJalNQZklXS1NEUGt
5ODk5dHZDTHE1eHBnRmVWSFZ3TVYzb2hUX2RJbVZXd1FtRk9rNXZKaFVDekhucnhsSzFzR0ptZVMwQlVXNWxKdmFl
TXhLZlV2eWs0aE5VYmtxTmtYMzBhZmFzUElFWXluS2xKaGhyMjNKNTlTcmFjcXNrWHYtSFJJNzJORk1NYlBsNmEwY
1BiQktZcjA2S3BzMjg1TEY2V2IwMGI3N2JYR0NEQmhIR3RoMmhvRjBIc24xcTl6RU9xUWloOWxlRmsza2ZmUUVBUW
9QUEpHUGZnalduRE9mRDhJanJzMDMyVkVsME5pRHlJc05Wd2JaR1llMWlTNnE5LTZHcTh5clc0N1c1b1ctS00wTGE
xSnVWb19MQ1ZlVFFRRWNabGo0dG84cEFuNnQtSS13NkpXMkxYUmNnMERBT3JPd0pIaVhjYWJlVkFKeEpTcWJMQUdP
MS1MX0FNQkgyNTlpSWVoWF82MktiTlJwSVhEOUJrSUJlS042RUpNYi14TmJyVkhBazZEbk9aaEM3enBzLWJ1d2EwU
2JqZG80ZWhHVlJPZHFuYjc5SUQ4UVI3LXBuTTM4QmpzdG1WdFY4bXY2RllSaC0xRlhaT0VzanlZN0FCN3RRbGZhU2
```

```
9fY29KSlZlcnVtZDRoRnJzekdKTXpzdFZ0RjFHeXVyRjZMRlhobU4tNDh5d2tVbzNITUZVajJlLWVWNVFPUHZYVk5
sQXZhQjlXanU1VUJxaWtFSVlwLVA4WWo3dnVWTU54bV9HelIzS0VUbmhQRmwxcVE0bV92WGZzN01tUzRtZjExMkNK
clV0c1hlX25RcGJtTVBiMGhtNnpud2Q1Q1Q0cnZUWHQ0UGlFblJiUFFzek53aUZuRlNJQ083NkZVVzBoajJESU5Ec
TAycjZrY095ZGxPdEhMdEt5WThmbG5aMWNZWVBDRV9DcElqcEFqUFVkYlppckZ6Q2VUbmlrc1VYaHA3ZXNOc3l1SW
tVcDZzaUU4TnhXMFJCRXp3Z2trQmVuUnBrVlF2TThmWkJZSzA1MTBMRnkzRF9XNEQ3Mi04WHoxZDJMT0VDakk3S05
nTS1lak4xU3N1bmprb3BoVkV4RXpxME92dHVrY0FOVEc0cGZjTnZZWVVYR1lrOEYwWV9MUTZpOEFZTXNlTEhLS3Ay
cmpxT3Y0VlAzSWJia1JqbGRXZTdSQThBXzhsZk9oeHpvcVE1eS1GVG81N184R2ZTMEEtSzRldkxYT0dQdktJSUxZW
DYyRlByMlJndGRULXlaMFJCNHFwa21VNm9HcTJKSnFMS2hrcm5CR29hdUVvTGhSZ0hseS1WYTFHUUpZdjh2c3B4R2
JpeUt0c05BWFJPMWxCSkFlT2dSTkpNcTEtSU1xUGR6VGhiS1RfaFdFTkRUNnVPMmJLeXRHNXVCS1dVOFVCMVBvcEp
0UmNvMVhHLTJPM1htTk1KdFBmSDF2dzh5ZVRnVXNNSVB0VjFQa2ozUTNaTTFtSE1FcldReUhwNFEtQVRRRW04Mmw3
OU91ckhIcFlqQm1CbTFKYUlZQkw5MmdJUnVRUDJ2bmQtckk3dmJKSmZ6dGxMdnBLbl9FeG1tUGxaYmdlQVRRWXlNa
FdXdDlrOHk1UDRXR3VKYmg5TkExQzFIMmQ2NmhmTWJ1a18zYUtWSHNUb0pMTkVScm56YnBkQkttVW9iODZHaV9SUU
tVVTdkeDQ4Nk41TzFvdHN2bEhUWnV0UFV0X0djOEtCZWw0dkh2RUlZWk9JTGtldElLYnplS3otdTVjTFNQY0RqQ2w
zVVpBY1BBMjY0aUdjbFpubkRRUVM2UnZ4cWZ4SEVDQmJqNnF4TEdlRTFWVm1zb3BWbkVkMG9vbjgzbWJ6ZGtiaGtz
WlNQbF9LazJpNGhfZVlVbC04V1B1TjZYVVZfZWtpZnlfQkNGRnhGaEwtZ3ZCVUhCSFJIb3c0Q2R1OXZQTk1zemF6U
m15Z2J6SV8zWmZXamJiTGN5dlFkb2I2MEdwUkhMQU9zdXhIUGc5SmtYYUFNZFdvVnpQMzVQSzVTMXoya0U5RUUwaU
RsRTdSRGEtRm5xZFRtNU9vVXZkeDA3bmI5WmtFYXd2cWkxVFFKR1d3cnlQSThEWC1wMXo1Nm9sQjRfSzV6VlpQMHN
pWEdwTHlQdjc0Y3dkQTZpZlMzeUdaMXh2WHVIWVFubC1kWVdSM05PS1JoaUZUNnhtVnB0VWZ6aVBkMiJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "3bhqLXggqXRBDCVq",
     "ciphertext": "N7Iautxehldwvl AgWG3RQVZx42vpt34VbBgboBRwXl-v9H4dPha-NbItvkWeaa5H-FbRy
k27Fk8IbZpbYlu58eTS6TmFKA748L4rzdzcdWTR4FO_zWCOJAVDq_sWOh0ns-fTWMci0vcA9vJXyDSWd1XTyD3iVW
W1RuMIJFZ9AAnVtSGEoZPWg5OBroFNKjuWXAMzJ2kwntaKpkE7WamTg-An3BKbJ200rLXvuhsMF6mh1guyvWFnuSz
GaXt3D11PA66mRycuASPiI0m7kBJvIyXaHvkvQyI8kSc5Hli_oCQP8t3hlFUz0s-g8R54qkkMM8CG7y9p129DCvB2
adx85nCmQNLa7YHYQ_QAbffBWu4R",
     "tag": "mHnowjgWKTTTKyc7HgcK4g",
     "encrypted_key": "D32Uhx5SCPOA3TvtLy30PNsium52O4DcgAVFfV6LLkcRxSGJY4p4XlsQgrUpRSj8"
   }
```


Figure 29: HPKE-12-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEyLUtFIiwia2lkIjoiQnNYQTU3akFYemJBSkFPaGQ1M1Bzd01JMTVIa2drNERaNVFfRk1OX
0UtTSIsImVuYyI6IkEyNTZHQ00iLCJlayI6IndSUWJneXYyaEpBS3A1YUxSaENqandsMXA2TUNib1c2bXlUdXBLUn
RFdHlvN2RLSjJobGNsZWFVTWFLWWMxcUpVQXJNY3Jwd2I0OWZNUWJOdUkxXzFpUWdLX2ZlSGE2UjBiVXhhWkoyUG8
3UW44MTQxdnZUd3ludno4dHlLQ2g1aU9BU3VfUmlnb1BmQXlpS0h0cEJucE5PcTBGbVA2bFFRQTBXaFN3NnN6OERw
dG5qenF0ZGVndHRQOTdGY2xYY09iRkJDeHpkOGQxa2hRTXFGRE4xZHZHdjk0TVhSRXBxa3g0MW03ckYzT2laRUhue
HBPelhMWkU3TEVqU24zWXhLU0gyeXdpOHFNS09kMHVDR0o5ckFVSVlwRU9kNHJYVnBYR0NwS1AwN01WVEVzV3d4aD
h5Zk84blRXRExDeW1DVi1rVHY4bnR6aGVfNDd6dDZLYkpVdmlIbUJHWDNYeUJVSGZOZkhHNDY1dTl2MzhxLTlocGR
1d2x4bDJUR05kUkY1blNpcjlWVEpTQkVqdmw4NW1RMlpYeWtkak1vbk5FOENXdzhhMlFBWHBjTFVpZG5mNUJVd25Y
Z1VmTXpvSHJGMENudzRNcGtRckx0TGk0VE1mODl4My1PWnZmMnJ4c1VnNlJpb3IwRGdQYXdmR011cGtPcUMtMm5MM
E0xeE5GN09JU3g5dk9mZzBhOVdSVGRtM0s5VVNnTHpLc0lCaXdvcF9ZMnZKWTRWaHZ1QmJvZTB3TUwwRnMyTGpLU0
U2UkJfY284d0czN083YVRvR0llUDRsdUtZM0xRNDIzSUFXMnpTaWw1SGxIazh4bTFONUVPZUkta08tUFZ1dld4bXV
1QkNUQkcxTXM0ai1yU2lSRlZBTGxxdlBKekxYR0FmVHdWNXI3WURYU3VTNWxhRUtjYVdpemlPc2dCbGEtWm9wNVBh
SmlFNUdIT0tXTXhaVlhKQ3M2Z19wWHNFVHdhOEpjSGNJajFBZnI5QUw2Z0RpY21jTDBuV0I0RVhpY1BXTnFFSVlHe
Ux6NlNaZmFkNHVzN2p0WDdtZVJxMWwwV1lBR3gxSlBObXNnZWtUejlVTk9OdGd6R2hsZ2dzcWhDeHRWWkR5MWxjU2
FCZWRDRFV3Y2trUFFUM0dLQTN2X3gwSGZMUm95TThDX3dxamdEOWgyc0JxRXd3QnhrRjVpQzVEeTkyV3RsZTVDbTJ
NMjhZQ01tQzBVNG5PbktDWC1hNGZGcnQ0YnhHZG5CWXVNX1dFbzlwVHYyMVM5SXhRUkJXSHo1S1RxTDE0djRCVnV2
ekJCSFNQY0owM3Fpc2E4WlA2M0NKTnVST3JKUk1lSzQ0U2tiZGQ5NElMSW9rTVZPSFRCZ0pWczM5TFZvelh0X2RGd
HdwOTlHNi03Wk5fWWRHZ1ZYSmlOTWozZDZEYVVYaFpzZGtLYjRSZWVlNnRHQ3NJVUl3Mm11dVMtZzRaak5LajJWWW
4wMF8zN1I4MjRNTWw5Y1NCWlNmVjBlV1RKWVRMRV93T0NCSTV1aW5DYTVpandQOV9nN2p4d2ppYTdqREs3Qkt1WTB
MNF9wTWUwWlQ4a1h4TkVSSnhJazA3NkhXUEJvQ1FmRlZzQUlkdFlfdlhrLUQxMzF0V211S0pORWNIYUxKYWh0NW83
alNyeWIwZ0pjTlpxMmxjX1pZTk1mb2M2U01tX09LMVk2MmxOZHUwLThEeElwNDlaMlpyZHEwc2tyQV9GUHVpUTNjY
ktkb2oyaFFYZ3Zaem40TVVRcFZSeTlPZmJaVWM2STNxZloyT0ZUZXFIbGEzUmx6RzZEcGo0TGRWakVZUllaTmFrWT
FXTHl3a0dHTWl6c0gwV1E3dGFjSFhiOHVyUlRaRXd0c01TejY0VkdTM0tKREJFQVVzOE1JdC0tVm83MDZLUHU4S0J
6cDdxMzJSMEVteGdFY2U0blFlZU5NeTNyLWNpaWZvWWJTMFZIWWpyMkREa05iUmR3Q1Qtamd3NFFHMXVwbVN5Sk1U
NWJBaThub3BSTWp1NjFXTzJVUG95UVNCdGIxWEMxQnlqb05NVkxPd1FWWk1zalFnTmhlbnBaaDEzdXQ1c2VSVG5iL
WpHUEFqT1htS3VaWDY2eF9rWnBDWkRzQVI0R1AzUWZqNjdVVDVZMFFwSDl5NFNPWVdBZEZYY0NhMEJtY1Nla1hOOT
B2UTltcHMtT0piNmQxa1hKakdKTDZ3NmhJTjhYQ2hyZU92UWltdnU3RWlpVFFSOGRFRWJGV1FoM0Vob18wOHkxdnB
VYVdMbVIweDYzUmZSMmNEVi1yZWpON2ctWmtZbFRHMG1Dc0ZUSkVnMlNYYU5ZaTdoQVhNMEpZOTAyM3MyNGtOckU4
Y3hoaHJ6MzgtMnRKOWVyMWZ3OWw4SFhLdGt1VlZQOUNLcWhqaHZ5S2o1M3AzekdkLTcxRWl6WU1IV2xMNmlYRXN1W
DhzdDVUdW5OanV6NVpkVFlnLURlamNiNWl6ZllEVWtuZDRxbnpheTBBQy1XY3Zhak5xMXdRam5MWGdTWV9YWG9TRj
U5T1F4VTZWQktwVXVoTm53QTR3UEhXNklLVzdEX1VObFQxZFE4Q3ZlbUdwdjRYUUxVcko3R0xfRTExVW1tbEdXeWl
icFA5Zlhfd2hQemp0eHpBbXNQZEx3Q0N4WUNUdnkxOWR2N1FQNWFPR2tzMzJDV3MtOTBid0pFSHJBT2dWMWNDX3hs
Z3BHemRXRExlc1BOLUlWcWdpR2lpVDYtUFo2YklrSmlXZWtnYU1KdUpBMzc4R2ZfOEVEMkRBNmk2ZWNFX1h0RkFxZ
VREaDk0NmVzRjVBbGxaV1Byc3lmd0hZYXNvUjAtZ0tyZnNhWlBOWndJaTZjczVFbW00Y3Yza0kyT1lZOTJYcHFndm
NYWWd1emwwT0pwWlNTa2ZoRUtBZW11MnJPdmRsSlNmYlRISWczOGlMSFM5cSJ9.49MMArVj91AvUzgI9mBNuJWkEx
```

GCRCagTGI0eURyhM0UHWb-30YYdtZPWDr-nc0C.Ptyo1FSG1A4a6Uu5.-MvYteyKVKdbHlG3tKjeiTOl3e3t5wxT8
kq5_tdYcch3RsSl5YJhnTVLeyFGPsj7a2q3LE0bhVZFUkTJznAUmmUecLaeoHRj4FrQ2TPE2ccwzBF01fTNIcfxto
P3mOvgvY423ID1NA2BNEhQwGNwTHfwyPTxA7_eZLdmIx2U4isg48oZxR7PAvl1U9l2t30SDeaazeexVP_ec6qssJ9
D-40SK7ozvr5MfKLF2bHxTjFBnglJZw0HFyHAQJcjmwc4AKsUnPFWATBckTkn_tUSRmFkkBXoTJ5VBbZdvGGTVqc2
7PZronArRGjjTstsfPr14oiKuTh4XntPbPteEg9MKOXkesL1ZUi-rMWv_8BTAn4-.r_411Yemx9Y7KIXxIhVvyw

Figure 30: HPKE-12-KE JWE Compact Serialization

A.11. HPKE-13

```
   {
     "kty": "AKP",
     "alg": "HPKE-13",
     "kid": "4xifOIawsHO0-c6lM_fIgh0hmcKUGV0ohj0aw8BQrA4",
     "pub": "XCYFhAuieqBanCe6DZR7Rbdl2kST_-vGeTIobXcQuFAwaHiqlFuwf_BS2CAbcfe_j2pZO2JMNnaC
pHU618FiPlu6jRsmYUy4m7aIB_xblaShNpuzO4eL16ZSh5KtILqNB9AbAVAuLOtigWGbQ7UeBuG8idyjXROjWpgHX
rplOqmCyqQInfuMHESRsGU7_wN5pFRA8LpA01dPTjJffQGwnvND6VZfN1MuVMc1-cA2c8KYoaSDFtWhitVAestW-C
GIL1G2xBKT1SK0CltxTRRR_UgrpUcvm3c0W6U4Y9QTRIZbncdhD3kdiYXNwwEXEstlvdYuSjcnwlIEhZFsLNCuH_G
-a1aBmfyeUoHCKlYxHxsmf7sJvXYLyQEfzhfLA8lyqZWEXRNOshTNMrC7NimiHNIK-zF9vyqFTsE8Q4a0HKIjTvdM
NXaoKgpqxgUDqTQk3HUS7oIYJOVN0qSeXqeaZnweAfy972CSOfVkTEk2BZQxzBFJRDGabMIuztggAbElcLEZVbMue
_OvdOCj18w3BYI-PHs4zUU3R6NK21jGiJGIWYNyxui36KOqcvceGiG3X9V_zfUIrUtvdEsQ2_JKQvZcw8Rtw2JTnV
QPKhpFsDZkzwhkaHOgdWnJPqSA8CmK0ZJnkXyS2CWYBiy9LQm018sn6hm5rLslIos4SHudeZBnOpdwkteQghFkx2I
c59Zmggw1mvJyYCyDUCMXYRVkXZGPrIe-CcAiUPQV_nmJjLwBwOdfh1rPF2KOsrcid3Zv06IuvJS5R8Oj37QfAKq_
LtUjOTebm6Vr21VRzsJ0B3gN2wwei1MjM8VIS0yKMwtW1qg0vaoswSKpHvtYeqQt80CGK9yYx1R5X7Nih3sGQABMo
_Gd_qu4m6XOI1QZUWmRQ7RcjzMDFvQVx-hxrtfFRRgqg3pyybnJkjlGhjyeChFGtBk15wskdGRu5Aql0WYnEcRhds
JnMcugA5nDGkSOEDQh8hmjCrqWLySwuzjBBlMNrfELTQSg3ZKMMDDBCfkKIBJzKNqOSch9FIoAubQBFqgthzpbLYa
fp9Y4IOvObpS-WkkyaVKy4YW4zuk49aQkkbeW4ZMlwCuhhHOga9VriKs1BWIfk0ukrECDWGWisstZTdW50LlTUlZZ
cvKgjfRTeUmuptsQWBtTDKaP3tFzq2wNjAQJpkuKcamIbLeKfXKCyvNrDgggfQggBNFCUgYXeIjL6KUbDbIIE3qtH
ZB_JwNMCogKzxi7rwsXZ-wQZGG7iNweL1rORhK8UUrFJ5uXKowHZNpwI6prZknPHOmEuJO0lXOnoDs5SKxzJHQ1kP
CExymAClBeO6KPlTK0x8AWXos4wWeL3JoJjvNbhAMuzip9GTofQAfIGQIENfZ7D2WYAOa4tLwFHeAn1mTLRgVcD5Q
RGJdU-epS2gGhvdwcbhc5LjtXXVdWeWR6YuSw7ZGdwdSLHitYGLkJwMhZNCt4muDH94rLfnhYoXPOFzyrYeKRjdFC
IhAj1aZsxTBYEpqTv8jDQcFdNTNGiazOB4c2G4G7IbdK92mYdrtwMGpW3YmPLYJKNhoIVhPKrQN0BYjJUPkDJlVPK
Zo9cWPAhVOCXbu8QkF85LkcR-wIfuClBzlWVWK8MBsB-DaBJkQgaNVQ2UqtQhw31rB41JMMZYQQUsyCl7lhVYu5eS
d_x4qTEjl7TCu6xGkqXlAPZWUO8XeeuThSR4MqwFwqhYuQ35GPSVaI3bhvlfE1U_c7kmANl4ywPdUQVUOmOHt4abi
kK1GOKLurRHoZpRLCzsDJifRt5jJkBUiTpxkX7iY6-HV7J1DB2qCe5buiq1BixnqRFwmOx8ch1XZbmrZZc6iOP3GV
qfW5jAxHCNrC-LYDfGg774uBzsIfyHdv8rUFmpQExcRYiQgnIdxsFAdkbkeucYKo2tgXyppUjYhe7ByjOmDOStyOV
WPL_0cV9dRHSnhLRNJixaefp-AuyKBHzvmEvmNb5DeW39pIFTID6VpwQDBrFPyalvJXkhiQ1xkyfGEHXkNFAdpEbT
NT0GC_K7BpYZWisXF-CPBYUNti0acN-izfVBRxV7TVEOCly9H9rzUWBn0EL_Alcz4-0u16W3ufnpD1NNsYaGu5ZyG
CabEGaoAgPS8izvrwqFC-2kcS05W7Am6Rx4uMxZTjx3j2QG6KLkkw3SSbaOsfVABOlArIplM1Jv7ajoAFSPCKfhOK
tOmSYljF",
     "priv": "P8toumlkmiSZKU6UB6tJC0jx1pEqf2kpiawqW6x4Zsw"
   }
```


Figure 31: HPKE-13 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTEzIiwia2lkIjoiNHhpZk9JYXdzSE8wLWM2bE1fZklnaDBobWNLVU
dWMG9oajBhdzhCUXJBNCJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "25ZgeYG8Yoyk4S7wykXmZYjAqNOxNWdqof4-kvdFo36W-8amyT11xCgBNQUxBFBI1y
mkq5mTRzdeLoX2ONXjpLQngbxelhiccKeKbuAsUlR7zp_MO8fZIwRSDZTjtny0S_yURmLFWnPpdebCb2KJpMN3jn9
ePdmPLzrrtW781kqYZ4CIRlAjT9ilcsuz1tQJLouCN4zjCStAMSWdnhxITe8zKU4iya1OlcniQfcyyHDpnmLf3TLE
eczWeqj5sCihqh_TnxtG537JVQWkjbTCUBNbHXQb2RSC3t2pPO7rPr-a0GNUV4zTLyCc0TdpUXuMEI6zEAeYq8Ccb
GddOxToXSWzgByQLrY754Zm2z4xhvTvQ7UwbGYoMVrmW3LtRO10qX0bLfjXswexIDtaEhKyW0WoT0NYLylwPHoiUc
DrT_AyjieS7eil9kK00kPxL1sOv3NT297iChR3J620JZpU-0pEfaQBASDQ1c_xjAvQwwBU2f7HVvc1Vdw0AXvOFwc
AaZopO2Pullsi31kKuiQH8KaATrZaUlL_Cf2HUq9FHbUrSOkvG6Be66Lwa2bNERWcFiBF2x0S_i754DNW7d09Lf1p
pe4rRSG_CdGmyM356-uc30828eUvrTeNvJNqLPADEzPyXRSP7hC3XTY2vKtMBc-iJmS8pjC0z8_bkL7umzpsU_HFw
P9vBxSlr6ytx3kDdqz2rcxVDzptMg3P99hZ1DdxtNUv34ciLyZv_QCJkht1kfMVSzQgDzag06sYcHsWbBsOK4vTuB
hfWM85cPzYK8edEqMwVuElGyqPmReTNOwzgMCVPPZ_b4jlgQvaTm7Ll6aDxGu_V4D7poFerWnKrxm9TexWen8Leuj
Css1HAZtTny2vHg1koEqEQRKPakWO2zkYjxqzkQOO6XnrYSd-QWKeGAy3be3yu_7OW40aszrD0ekcX6YNL5PVCpSm
O_wTR3QBgBA-RMo3psfJmdZ9pJ0GkAKQrX4BsjRDPC6zbsW4JI3rE9ZXIETy5iI8qBjS2eIfmDeF-12ZjB8m0S0U6
_WrSyO204S7yDCc2J5_TUobuyTZAd2fbxd2idCBFpCLQ32Lg01wbjlZsrP7vlCkXH22T9pDoO3dtDDcj9QiK2LR0-
itQZiNWkFiU47817a_VLBRWhJVhIGVy3kRWdz0Na55eo1qRprNMU4sX-aFYnrCb7np69MikLCJZPxAEkw6yhx__yg
3dXPdD_I_vYTtyQMPKSHNKDLIQhZWh-oBvUySlcpoctA1MzcSZCAUXcyGYC9KWEzjvbO3L4PrkJoN3A7wYHVWMP3T
Ci10u_xtob3_B8IqsxzcoUhTriAl6A7MK5lQdvqK99I49bQCEygOTTw8SIVVMef-5Cy3ERECJ3aV1RLnRi9TqP4_f
i_XsU8EKnHoyD_HBCW5HIpa0hRFsHFpP3_hFFmJ-EWgamgwnyKqN_fIezZUFqcO-lpYxe5559WUr4FSHYlMUVz0gK
yW9bKDzlwCZW3bjzm8RCf2jyWFHKilRlYt_WCCr_iFmiLWXGCYEVaL_qIOMX837FUVBOY6M__8gX2Uq9aAlxr9bjw
TliJ8LTIdd41UQ-m9h1pZ6lOIE5nnDD_Jjj48REbWbGAE_-QryQVlU1oFitYxET2WxszMVivrWWjhQ2hraj1AV7U-
A0bE2XA9yLoGROOeWkjoUqAW7jVhlBp_pViqkuYEwHrxwMME5w43CYOnmH4GIOHfbnsf5xzRVg9HMUQu95kGwSegW
uCnI5jhKy5fIAukFTQjA0sCrJ9esZDH6hQW5MCQeS6TX56waGpNcvMSazrNKMEw8HTWcl8s8tmi82DOga93FxDicA
Mn5C1E4D6wJKr5V9zTk1_qE4FWDvt-fvzP3eJNWwsTya_hGGtJNazyT58NVYlAJauhqDCuI6wqwv4imX7Vo5Jdn57
ibZmd1eGdr189NU9LkkhVanfMeFo_w_adNVumvUnrvYdKlO7IAr5DSDlaWOIisZvkYu3SHDed54OhpsLp8lAqJZVn
```

```
g0w2mFxm_kUZNW0YDkQ5CU1_7WG7FV-1nGf-hsUekkLPwa5pyLZCIkGnZHpw7imSS_oEyvyuaDg3NF2tYvrw6CM5N
QXzOXzzH0ax8mRGPf5ur1Z4YtzyqGT8xooomfUbDlFIawi2sWQYd7mwa9zIbcz30HWNhEsERaM5clYfUT-DAlrqQ4
Tt3vjhBzHfN6TFtOQ9",
     "ciphertext": "evHuU7AbtmLiCvhITweAJmsUr79rAD1ylsnw64hiANTM1qh39GbvzqJepSPXn7pAb2cNe
0wiVwvMlP4Td_Yd_VzRgdpg57Utwt6haKKeKGHU6iBEwpl_JQS_bOyc7thJTUORXdPj1Mny83KE8xmXMJ_M5qyeHl
H_usF-afPKLrj7OWcXQ9p2irz_DNEPBCDqnxnJmb8WsChkWu_ABPGZ79vzQbUJzXvvTxbfZqc5QGkqb59qygphsvz
gKFCfguIsuz29gSyehOXz3poMrB1nffl53MWoGuG8ijYS6XpGqu0ULqaIR1NHXImCbKITVY8fXe-JvwK6nUx1jK44
q9EqTuLmsjHoOpUGRIDwJSgyH4SaXpmjdgsEqZVtZKtVfiUYhQ"
   }
```


Figure 32: HPKE-13 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTEzIiwia2lkIjoiNHhpZk9JYXdzSE8wLWM2bE1fZklnaDBobWNLVUdWMG9oajBhdzhCUXJBN
CJ9.l6iJ90Oc2GkCzuM-p4hYiVeZsiyvOiE-gG8ACFGhre0EUNxvpcKtCbGbO2Wt8U3xy9E75FblWp02_9-W4DnWJ
yAbRimwF2IeVkxaqFZ5TDKM1dSoUhdzaZO81DQLdOn9esI6yLNzx7akNNY3LSdIhB8tD4GNaHB4uUAmRcR5u2ffbW
CeY0yB_Cdoh4UG3hDsHcnbe3TPHMyLJXpkhpZuMTSiMyWvbWV6mzG6sZo-G4Pu59-bSNurhGz3ad-XKZATJUtedj0
YriUNHHdycpxOcgvqQEnTaZJ3CjsNuP4NOKCWRJnXuBiv6b0ZAvPSsJ--gNugEZiBwi8-eA6uNkxuxEjPfutqfw3E
lB66iOmLumoW2XQiN2VgJBisAeDO2sfSCU19LiXMTOpjdARL8qNOWjrjKlOZd1zuuqSB_CJnqwepZ9uCgl9P6uBta
7SsbWfI7JK8gsGPKu-bpZBk-JK6sFSYcTRRViYWXPj_UHuxXmqpSRA8PuXMn9wURV-dC2fes-POFMgYYBaJJV5pV3
yOvUt5aeH13isGHxYJhKhoGxYUx8quxjqxeUCV3CuhSyp2uMP9D90BTffABsyROQeeWEjlKsxvMI82vumeY8kKl7K
oy77-7JwJiAUJNvu4vMnTI2FPVNOCKnoL4I0MsJrcZTkGksY9ELe2fMt0BnQezDjS0YldoMsbcHiJvhwyaAqySkDb
Ae5V5sIx7WLb_Aj9V8XCkyqf0Fqd5v6cK0IVeNXU3Ed1VWicMx6m8yT1oE81mP8ca-hdv9td237QbZR77ZubhipBk
geUh0cVzVUSATGiReXhPRbiP0dSEzsaOFTzCSDirN_l43JZOc6PXLTJoS36-JODptyfUqZIrMuhswbahlu2GVF1Qv
cd_3Xr47GLs3J0-eyqjv6XB2ABrjk7CHBblLAIsz3XxioaSvaEoLrweTE5aQ1NL_PWVWi3rXnh5uai05CfPqHq-Y2
QgHw_ne0xwMNeeH92SLaH8zFH3u46uJVYzBy_YI9Z1vdo7CmTgvA7dGXIdwAQ2GqvjitHno2RhyicPCExpigQctf2
nWpNMuoKUyHNS69qSG4s2wthxJoUHwR5JaWX5oRUPu-rLTIF4GqecWfpPXS00YUZWC9Z4_Q5_P1iTofELSWKk89ym
-_qnQNTMlE3VQFrBvRj1GMDQWK7JCYWoGeN3ECnl8kp4wz_nqgSs30naA-LpyXBAFyXxvC3kLsupG2HenYs-pwZFx
wcSyt38C5pqxJ6ZaZLHZ5GUpt4Qybx1MfkBcHg3dKy1bLafCouFZ75yumyFX9TrNgfcZVGRey3q86Xnyzd_1dTIXL
_l2ZoJA2B14SEm2sTn9m-6Yy-NQjUa_ItCYYMlOQ02fAGPfGIrEWxysWLfqe1k_m-YyvSOvdyk8UNrlknUhOclbvP
sQ2Hznq3ugavzB38z5NsJHNkAjls3Tbwo8x6jSRah4pYb0KXMP9Mbyz6cMJ_zFqj4R7FsHAf5Hh2sYq2fs6xmCKKy
-6N4DebT2R8qPaRzbZjSyFGibSzBjUwT3w4DRryeC5byV0aEbb-AD1hKwpHJtFr5wi_gvr-FOYrpQ5o8i07rFHxob
j505CMCECMdblWCY4sJ1QA67qTQLkqoneibjO-TfVt4_nD2N0Ip1ZHZCmb7D1jkL3Z5GUVVS2HA-MUO07PZ3snPCa
JZnPGnCs5EoV1reuPAaHxiGbJFKoaM1pdEOkI8HjyPLC7hbZcCwaCpgkjYo_M8PTIBER629MMbSOVkLBS2R9DJktE
bilwu2qTOSKH8jTg2teZ7NvVRe5TLIAbuYfgR2KA1pTV5s3ASfYZtxjAzr0gLI1nPJ2e88VatocmoqBxpuRHFsczB
dxcQcv_Fx2AEh-I9jz79uktnRWHNdP9hXcgIYThKcUbxwsTxSCtCwG-3rgedypqdi4dHCZ7UAZPqeVveBu9asXfCq
qmuKbRjfF7dOrguagKUa0gEN7rMuctdcjDIAXB4ryFmj9mfFveMOmxNV72gpOZ1jjaJB3Xbe7xdhVKOKe1vwc2GpL
_sMgE59XjAKfsf5gs0MecOK-IcTwNf6SEYld27kvlR1M6QYsEQUdl_biL7d_OmMOeaaYxCLPTg2IL2XBscw5Bwd76
mNlhPhVf0Bz1tA0ZMjyDBENBwyVC4Y1ihy5GerWHQTslWySwQqC2VM6Y6Z8IRlZbF6-H8Dz7Vnloa2Y6FQ0oifQW.
.P-shvFCzgdVVW5l0keplsRfMfXRY-YmYkpg336M8xK9GtgTo91-uLrLcqrenl85JkkyBOr4jY61LueJGqZeC1fKU
bviUI_rl-X3U9Jv1qbGoVW_5_Qnwlh6kZfrTzYSq1o3TuAgjODrjL1HYLfwzpE7JRt-Tjtg_RCsOpT5z1Byh35Ypu
-plhu95F957aKSWN9DEHUF1bcA1j3VHsa31xqaYLBVr3-d4CQwtHgzQzuwyIbnKGKVgznAQkQ-065xvSkxhdCxY81
AY_D9mDJ7BwPt6guBF8Pngjrla2_wjuKsqcVrfOo_frNRntuC096SbzShXCZe5giiM-vSpi7My3i2odjprl-n10G6
QYEg_jrrWPFWD9-cI8HhF6WL0E6vvIQ.
```


Figure 33: HPKE-13 JWE Compact Serialization

A.12. HPKE-13-KE


```
   {
     "kty": "AKP",
     "alg": "HPKE-13-KE",
     "kid": "0BrDfMl9Ou81OD27zcoCEKWuQVbsviuJAEr-9IJNTTk",
     "pub": "lIeR2RU7WtrK4pOlWdXISQq4tPy37ZkqmoGkTWGlIseElHjFabGZ9KecMDeHTMpSNESRf3Kn5zeq
39NCJWyBnMBWIsGc2eaiN1RAzuml3AIG3_mu_BSwNAWpURZPMwBOCLVaGeerd9UU7Ux6W4UUSNxmFBQlBdB_uplDO
6of9ihkBEOpbDSpXHoEblTCx-dVEEXDN7CkDLcSt6KKZ5BI5bfLHNdR66teXmqvAuaG3iLMAuepAhRQw6XCgiVrG8
MZDmSMzlRKXnSdUomIk9J8Lch5o3M0iQJXnXqYODg7sKFLRzQjU1mtneTIPRujvPlwBbWqxeJP2FqPfoO3egjAVxp
CCnjNYWUgw6EweuKk3YcjGcOTZZaZKdmDONkQLjfBSRZzIvk28SOfBeJWkPo5fJCU_pmjqRkMUJWiKEec0keTq3eM
YeGKnOgqVvkgO9ObWzCsoQtdx9bI4eBBhVIP8vStWQIRkzbG9IOfnZRB3yCeVyKVLDO0gFyACEGncxBREzaCH2qTn
pGAi8OOwaAflXGo9FCcbYOYsLBmNCYrrGw2R8ga8fZeBzdE9DSgHvaFU8m4Whq8WOMhOJiE7hivcjybR0OL0idcwh
pt8wUs7GC-ESNWd0ti3wS0bTk3_WMStDwKQxnCZXxYLdPEXUe4gepUu5cXTxua_tBkXNmestLHWZqm4qsEFCCHjDo
ShQoI8RNoZ9Eaz1o_JegtucAZu-sLNUcPRyVSVatCBXexIBqVExA-oxWCV0ZQYsE7PxyCG3hpzihX69IktQSlcIAl
dnORc9A61CMwLhS17NwTJOHK7IvEtyJQTrlC0iJ0oxghDsS_HLseGdLIaUOh4uNJfKybZsyWquaS6LMXFSI1ASEiZ
QROTMAEx4gfIDCZuitoCRhpl2Rr4pacNExhqzAOU4keQnaYzskTJ3wGGwIcXEivpHCM1yqHDMeI7RRUYHe6-Vp3Nl
xIz-W769Slh6wi8pxF4zS4L-KmMJMz6EmXjAq-hCBVo0iUMma7vqhK39VJDdoxvvGRRUEfudVl96GAiAi8dwm1icq
yXaMPhZE__4WqN3oSBZONeCw5C0K5fnjOeDLFYBxxkBt25vjNPtFxCwewtjG1-VjIRiPJCalWZpS6BnaBqyUD8jgM
YZsHhEVOeNyk0wynv2iNisyNt6E8d7pbF_sxVdzDSbh2w1Fyz-PAjVULffcYIRohQCw1J4mYfXJc03eF3YFT2wMsH
```

```
JgvOAwFUvYzXIZ0-pldQeorn3ioU1t_lLM7P0F32mW_pGpVZMHATklxjqcG6otoRLZENzMKzTHMZhBp8PBTZBo4Ub
toMqscL4SJJ5lNCUQHC-AVP2uNc9elnAsRRYnHp7erXcttvlNlIVYLRNNYa-e_O1i_rAdDQuyQ5mwdxiauMCwM2TY
MqlS42-aHgXQID-EZxGSSgHul_6BBLdN0LKtMQyeITzfNypZb28BbBeZ_0Figr0FMVVhKOktdgeS1-LgTTyaHUiSk
U8PO8Hga1Pt_fSE52vFpX0tPjUKY7nkU4sbFheRjq2JQYCM-TIBQyVwrCCjDpusKY8mY46qRxXVsriGuRVYT5ldZ9
JJ7snePgxLKivqGxSC3Ilw9PmHI1gJ8Fmdu4VEf4wgrOQQuEIVYVQk4UFkZX3wJevrLTUxprpVcamxFazG-gbeBlY
OS24FgLYg5VZCk19iVMnqvZMML7gyc0UYZrlvCZnpCcVzNdYmPx_q3WpZVAycduim_Y4wQztgZVwx1tAxNsnw4h9c
jheAw7pWnsHeh8TSh4JMFVDM4HTWLJJNuAEUq3XJMfjkKWqevzpmT3ut6rWua6Osw1PNdEcB3OjoLDpsmzTuPWxRY
94POXfsSwFO94orDGIAo-px4J7I79qFUk7l0NzFHUtxhr-VvTGAPOxE3uSEOmQKNR9irzleuiLh82xxzp5QDKfQ3B
GqFvcISj7fOZvYtufiKF-hFnZUeJxO3JknHu9cLPqBT8HV_ANUtkdUAjVIjwjkOPbNAViusbPq1fhCApMsF7YRp9d
teJllx2LIKR_ZQ8fJ8z4MhCyPl_S6Bd9SOZz585v9bd6oo-B3bD1NTj9kEEkc2OVuDC3U5PxksCawjJjD3ijBJBc6
EO7zOZ0DnP5PBkNMIVJkT60gJBtH5r-Py6IWmUh2bILE_R7e-rKEbdJzm2c4YsiYYOQsfbhFkniTdp9fOBRlTAlmZ
APnzcq6H",
     "priv": "ab0bJL7Uw-bWrw3usR85Camu8riwNWawtW1XdVREAjA"
   }
```


Figure 34: HPKE-13-KE Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiMEJyRGZNbDlPdTgxT0QyN3pjb0NFS1d1UV
Zic3ZpdUpBRXItOUlKTlRUayIsImVuYyI6IkEyNTZHQ00iLCJlayI6InJ4S0hmRkNxQVpzWGdzVnhGc3dRS09WeUY
5SWo1anJZWGdMUVNSTXRfYjlsWTZKRTF6cGhqdWZpTlFXUmYwalBwcmN3eGZjbW5Mc3dqUG55S01DaWtzNmlBeDU1
UWJaOThvd1Q3bHpzdDhNNnMwVm9kYnctLVBhVW1pRXI1WDhSZU13S3k4aUJrZi1fUHg2dEZ6clF5T1R0R0VOdENaU
mlyRUMwXzlDeHgwWVJJbFpqek41T2h1UGtmNDF3WEQxM2RGN0lpS0VTb2FDTkhPcUFFSG1pVlVanZZZnkxVkpGV1
k2bkllemVISXVHTE9VbGZvNVZBU0M2TWxVU2V5R09meGdycmwzeDNBSWFpMUotaUV0ZENGSFlOVHNKWVBLdEFtN2F
DQ0R3YTZYZkZwSmZNR2JwRndsbEFOYWJaTXBxcjhiVEhQaTZDU3VncDNGNHRyYkxvVXFpeTBDcTBoTThPaGNFMW9C
TjZwdk5zV05ScnRxMzFLSkxHYVM4ZHhrNGVqTkZ0YklYQ1FsN1NrX25TaDhMeFViMTdrM2d5UVQxQ3VWT0lUSW0wN
Xg2emUzdkhqbmVjaWVtX1Z3ZVFzYlB3TXhhcXdJMlNKaExxdUhqbHFyQnZ0QWFwMGdLaGtZUGdOYkR5MzJRV1dyMn
JBcnRESFdiUk9SaWJNRHplMnNraDNTNWFYcUhGbXNIMDhHN0dNWk1EY2VhVW5Ic2RyN2g0OUFUU0R5cEF5Mm5CUVY
3UDJhVDdVTDVONFBJWllJS241Y19TaGRYYTg3Q0FXNGlkYkNHZTNUdGoyY1NDb1ZhaDVFSXM5Q25ULXRab3pMam56
RHN6THNHVlQ0Rjc3X29ib2I2LTg3bWtsbDlTcUpGZkI1elNxR1FqRU8wRm1mYVJVeklPUjdmU3lRLXgxaHpFQkdKd
EtCVUdwbVZLUG9sc3lMeDJNZXpaNVZqVEhWMGRfcXdrdkpXbEVnVGk5UHRuZ2k4ZUk5TjRaakUxYmtud2xocXVkUn
FST2lrejd3VUw3dTllZ1VhQ3JXcDV6RVVlR1ZZaDV6MzdIRi14RFduV3VRLTd3ZHNFdFhqeTZOSTBYdzlQWDA4djA
tN1ItOWFGZE9KNzNZNDk0YlNpWlItVkUyT3g5OXZ5TXlHLXJWOVV6bzI1V211WmxOcmJoZmNjUklpRERkcHlYbE1v
MG40QW13RVN1azdVTTQwMG8wQTZBcHhDMTFGa2J4b09JRUp5WFA4OFg1a3lxNzdtZzc0VDhRbW5aVXZCRGkxczB4d
WRnTFMyeUdmem8wdzJMWnFuM2FVQ0Ezb2RXdGNkVENrWHZ1QjRhUHNZWFRWcERKYjFfRmFPYkFxcWswcXZLaGd0aU
J4aU1IUjZHRHZVcnpsOEZYZWVDRWFLaGd6R2xWdGJQaERUT0ZyMjNoMmZqRTA3RlBTQXJvZXFNRW5YTzBhUmppZkF
uRnRJbHp4OUtZN3lyaXVyTGV0X3Z1VVQ3QlZmS1k4R1M3OGtZY3BWVUtfLVhEWHh4MU81UEhxN2FoRDZydmhENkNq
MzY2dUpJMVRlTGJHMHdSbXZUU0FjNkpwTnFzdnV6bDRmLWR4T2lEZ2JjSE9ER2ktNElpMFFqeThjbjFFR1k0SWhqV
F9vM1I2NGRZTDl6T2JfSm1PTlNfMTQwdEFCbXJNeTQycWxLa2xPdVg0VWZsOGpIWF9SeU0wX2R6ejIwNWZuaEhoWH
FTS0Q5c0phenlrSmVOU1RncFlUTlVSSEdkTlpSS1JfUVpOSzZ4VEVXNGVRYWJHenZueWp1Umt5azRRZjJYcXJNUU5
wOTE5dGV6S2doRlZpOF9zbGtoXzRvd0lHeUI2eThMTmczaktyR0JLaGRZa19fU2ZYT3dvYmpSRGVsNUVVWE9DcjlH
bjNRd3psNDh4MzVtbV9DWER5YWR6WFM1Q0R5Qkp6TVM5dndscWdkNU1PWUhPdjJMZVNqM1JyUWlsbTJIeE9sN0xqa
0NmRnRBeWREVUZPaFRKMzZpWHlqU25VUXpGaGdtQUczOTNRTGg0VG84RW82Szl6XzBDalE4UU5lUE9pRDdHOW5VZG
pOUnNwZWZFdnZGVTROLW5CZnRxa3NmaXRRdjdyWGctZ1hHYXpqUnQxS0FjdUFvc0hIdk9FRFR2b29rbDlzSUFtRFN
zcFRsOHhlREc0N2hsQlkwcjNTZU5lMFNJOWNuekdLdFJYWjhoeEZzSUNrcTdTV0x3NjRYZm8xOHNzTUpfcDBrbVZD
bUJJSHA4a3NFSVZ1VjhraE1fUFhvM2FrSWxCNDFqVms4bXRkTHhyQ2pQMVhja2NpV2NoUHFBQVI5eXlwSmhlU3pwM
nVfTmtweERZXzNmbmJhRGZHZkFaLWh3OEVELUdFREQza1BSeEkzYVNBbDlaTUdjQTZaWHcyZ1FSYUZ1aThPWV8wd0
l4VWdfd2swTmktRE8tcTBCc3FyeHFBeGFaWVRRNlJJQk1hZUlHU3F2MU9QcGlOQmthWjdJZHBkVWl2VWZVNkctczY
yWmx1V2Q1OXRJT1d4eHlNWk1kQlItcG1lamM4M0xYUzhucnZkSG94ZUprLWxvLUhjN3pXZ2daQ1VLdllFcWh1aDdB
Y1NSOVEtenRUbHVVU1RGQlFCMXBsTGJtMlF6Ynkta19IUmxGOGZBVXpkazQ5aDdEcS1oZjBCazhhY2ZsTDU0NGFhZ
XNReWV5dkJMbzgyem9GVW5nVWJIQU9ueDBrdC1MRkRGVEJMSmFJX3NkWXZQZ3p6WVBZSDlpcXA1VGlOS1FIa0Vobj
JHejVHcW9aZVlqYllYNTV5SXM1WWQ0bl8xcDZvSlRTTUZ1Y0NxY3k1U2YzeUtCVmxobHFXbnJIVXNyNUg0RlFyT28
4djFVNHU1VHhRSHd3VDJlaHJDYVpLeFAzS1V2ZGpwYk11R3BxaGZlSEx0NXk0QnY5MHlGdWE0dHd2TCJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "hAt8r15Rv6ygUo9U",
     "ciphertext": "ZhkElOeJIgqcgJTN1QOn2MOSxeYw2b0czFHp0TxD0vj9CWQDk_pisQsQYCXiQfbE8tcZi
2vNdZv82uBOkAkggjVKbwFdWs6W4etH0EaYvI_55pkppZuyhfY_P1igJaCIwfm2LhFGtBhYGCqjD67i7mqMOmq0j_
x0Ofg3XMQtyVi5PqF1_90NxKEom2nUFla5K55WjxxqPCt6d4zMQFCUI-Z-dBnduOyQnKK0FIgSZQASXZhfMi2m5fJ
_zFqvWwE4NEbhM3hnQczDxoCQq-E4nmkOW1Pl2v3iDYPCDnafUfqqama2mx1-8OmPKL8P6UJyYXTW3Ve_5NBykWMI
iJAYis4ACnS3RV5NziUex6cPEeNo",
     "tag": "P4hRMm9qskdV4TT_0D-IGw",
     "encrypted_key": "hCtP_FodNMBRK8sZiCwueCbuPG6jIq8iegt1-Kv3dasloWfJ0lQClNdFVQQ1OeBB"
   }
```


Figure 35: HPKE-13-KE Flattened JWE JSON Serialization

eyJhbGciOiJIUEtFLTEzLUtFIiwia2lkIjoiMEJyRGZNbDlPdTgxT0QyN3pjb0NFS1d1UVZic3ZpdUpBRXItOUlKT
lRUayIsImVuYyI6IkEyNTZHQ00iLCJlayI6ImhHODJsT0p5QnItR21ieFRrZ2hEVWlVTWJiVFBCcTBzYVZZMUptal
Ezc1VjTnF3T2RDTU00SWtUSlJBNzhMY0Q0Y3V4b1ExemNKOFgtRUNtUFZGRnZJU01FT3pTbDQxTkE3S003UlpvUHJ
aNG5CTTl6QVdhN2xneTh3X09ocHlCYXlfcUFDT05fcU1VcG5nbGdvZUk1YzJRd1hwV3V5azE4c3AzOG8xV2ZTRklj
cmx2OWVDSkR1bS1OVDg3ZDdkM01KMzkxV0NJdXIzTHNjOUdGOWxhYnhDMFVYYzRUb3VFeFZIanlxZWx6NWN1bF94V
WN5RzJsU3V4ZElYSmJzOTIzVHZQWS1zRG1ta2JETERYb3pFVWROdlBKV2g3X0lhN01XcE90ZDRFbFJnRmZvVk9FUV
BFVzQ3UWFNbXViQm84VmpRb2E0U3N0X18talBwWVZCNG1MdDhmQnAzRkJDM1ByOWRzZWFiY3dESFJacGc3QlBkS2Z
iZVowendqdEpGZzlKWEJhVll0c0Y4WVRZUG1xRlFWODFpM1cxVlJsVlJOdGVBVVlKTGVBQTJxMmt4X0hNb1BvMjla
bG5jbkY1VDFlYlluR2Z2cWllZWdOam5UeWhCTEx6dkRZaEc5eTdLamUwUktuR3JqWGJTVTVnYTBWaEQ4UkFQU3FIR
05TT01EOEs5Nk8zdlk3MFo2VjRYNkFxRDBaSUZqVm1saEJzei03amtrYlVWOUVPVHdwQ3dtUmdRc3l6d25aWDNYYT
c4V1JSQTBOdUdqeXk5bHlTVTlVSHNXMEdQSXdUYmE4amJWSUl1NGcwWlIzN2lORXNhYkYwRVkzTmx0V3puMWlESzg
5WUtDQ0NwTWhrYXhFMi1CenJqblJLSEFqZTJOdjdzTFhBQk9ZWEJSSlV2dGlOTWVVeEpSeWFLTGJCYTZOQzc4QU81
Szd3Qko4NV9WMTg5TC1ISG1xeEYzeUVsZ2FLQk52U0hILVpmdnV3My16NU9HQVdCSG9PYUdIWU1RTHIwVWhBd0xJR
jFZT1huR0E2ZnVSeFo1TXhyTjExQVIzbW9EUkx2ak9aa0NxSnVFVWRSWU5BS19rYndneUtfRGliTTRGelM5NWZpTU
xYSDJNNEtkSXFLRXdBc2VDaUVYOGFXWklQZG1fbFJLazlqMVlRZGgyRFFDa0h0WHpaOHNmN3FvVFVTSWxhTUVLVXh
lYlJ4b0ltRXZFWnZJd3pFZENzMEhJWDR5Y0VPTExDZUVaOUxRV3VHaGdQNnRyMmJ0UkhOVWQ0TlEtazdmck01dm5X
ak83dGVfR2p1V2JRaHo3bWk0dE9URGxxOWlNNHlQZDliX0xOTDd6X0c1WTNQNmtLcVBoU0p3dlB4Z2Jmc1p6Wms5d
VU0Rmx0QjQ3LWZwWUpvYjVWSHp1QnF4djdHckxxdHJGOWt5bXpiUEZMY2V6WGJsOUFSUnkzS19EanFRSURFc1g1aX
JBNlFjd3Bla0lzNFhQLUhaN19GNW1HR0pSVUpOMnlyc0lONnIxc0dKMi1ONEhuZ2lxNEhrdmtJMkV0Q0VNcno2VTN
iTGRVeU5tY2kwM25YOXlsekl0b1VyZzlDNDNCa0xaZmplQXp5MDZVZF9VUkF6OWJURGtnTzlVTjFOZ2MxdGdxSGQw
cnFOb01lMGNsTGFLN3BtNFF5c2pUbEpTdHlrUzhPQTJHU3BRUjVVd1dhaTFtWGdzcGhjRnpmZk9CTHdjMVBTMU95M
kt0VnczQXdQWXlBRE03V1pjRi0tN1F4d1JJM0J5UjJkTE0yRjNMR0laWUtGekU3STRQWURWclVOZUk1Qy0wQUJDVT
VLQzRKYmZ0NGpUWlJObkluTnRwRWtPekV3ZFd5VGw1V3hkc2prSFN4ZnduMGF0V1JyeXdDLUhLSWIxWnhLYXVpNFZ
5YTR4QWdPcDFyZGZxTTJndlhuU0xVNjFyMW5oeUdFeHhzc1dZcWhWTTNpeS0wOS1BN1A5c2J5bVY1UVFidEZZMmlL
OUJFNTUzM29HWk5OSnFxb2lQYmI0N2FCZy1LX0F4SzYxMV8tRXF0RDFoc3cwdU5RSkxzNHZQY1hNNjVRMk5yUmtsL
XRlQWhKdU1WdEVvcEhnTVRORWN3MlpCZ1g1eFYzcmhXQ3NVODM0V0pic2dOcnVOTFVnc0N1OGsybGNJZ0R2d2lmYl
g4WVcxUDAzYmx0X29UU1h6M3VrNVZoWmlrZ01rV2d0Y2t1aFFhbFp2RDhDU3pnVjhydlJVMHFFdGZDREEtbmN0bmZ
4Q001dURSeDllUjNiZlVlOGl0cjZSdVlKRVFoaDJoTGNabFZHZVdjRzFlZ0JpZmtJWWZwdFRoYXNMX2w1NFh4Z3JK
eHFCT19kYmJkV0FNTzUxZGRKTkFTY29WeF9rbTJlTndjNmxZZWdwY1c4djVGdkpqa3VWTU40RzdQdzlpTnJyenNUd
jFMWkpJc2NrQ2lXc1o2ZWVQdlRVVHF5TXVvR2ZPaFZzTU5UZU52VEtra2RsZUxYNEZBY3lDVUJFaWU4VFdReFk4LT
Z5RmhKVDNsVEoybElBVG15c2NNcmQyWW53enlibG5kMjVSSGNaa2Z0MjNkdzRheElGNDh4eVptM2ZuaWlRaDE3VDl
5U19QNGFMMlR6NHNfcnFPbGRJOU5HTktEaWg2RGk3UUxNcXNkVnJJUFhRMGwwUUthU3paeThGSmN3MkFvb3FSSlNB
VWRIdXdmRXUzWlplNjdhdzhGZEV3Q0wwUGktTDlvSEJOUTVqemJPSWdlbXJEcmRURUV4OHAtRVBOeXFUeGl3YVpxd
WMxN1JtWkdxREVtd2g3akFCS2RXa0ZhbWwwUFpOT1FZR0pxVDhCTkZiWWl6d2ZtRlViYkVlck15OTJyblJfaFFHbW
RJdDkwdzk1am9wdmN2MW9Ndy1kNWhsa2N3ekVoUHV2M1FSSHJNLUtSQk5QQSJ9.9fG45drJG0-KwSFjk94DnvCLWY
yklZDNmWjQRBcA8iFBT4pp2PmI_J5ZX159F4Zj.dcZbRxnnrOtPRzin.wQA74WJBvOwjfSJoN1jqdjlztoZvhyLk6
0OK-kfHKOqsI1lB9QIoQReOHkyUvP8MswThMFtXU2zR6BLq197NBOydYsIhxR1CEbc-tUpJ8pqBdvpUUNL0PKwI9z
tWhHDiCy8sqg0MXVPC-91KZmXvGmQ-DL2AnpnVm_XYfB4lUKm4Et70AaspwXnAF8UbasDOYPymTSmBXLjbYUjpuCl
I6YOfcBNuUU1GuIvl6Hs6uHVlxMKz4wNX7axdnLHWEtCatVuTWOtyPQsXASU_Ib7B1Ioiwkyh3my_iF9tyG5yF5FZ
jzAK0GwTlipJSIjrBikE-98GfW687XT1-6ivK1mqXIYOJ9EbcbA2FvPxk-Gsgz8Z.Xo5BSgUbW2PM37DtM5DGIg

Figure 36: HPKE-13-KE JWE Compact Serialization

A.13. HPKE-14


```
{
  "kty": "AKP",
  "alg": "HPKE-14",
  "kid": "tTd2rviNEWmlDSv55i7bpOBkYgi5nYuGG44ptRhV51A",
  "pub": "NPoE7SUAWwcVJbAWGEAUiZUcIrAIN1UJIoR-ZjZSAvIUxKJcyhMFoeliHppZ1ncZuqqmSTCNmCM7
j5XCvRRUZgqYgHgmHuCJOdMK3raAbPF_g2kkj-iRqtQJ5poXC4bIpYd7ruJcHyyf8rEytrTGOKejA7xw_9IN8VtW2
7ah89F-3fUGm3xidSJTgrgGHcHKPhewgnNkNprFpzqwwpUz1jlnz-mPGwAkMBlM-xiIeUlX6hqKR0xeTDGUbyt53i
MUdbqi0EaRdHC63GSruEwE8NYjr-Wy1-NXPEYSU7qlLjGNeSRSxZInTarM0ulwnFTFzii7kkmygCkGDgIaeufJ7hG
VvwSI_hcE5pyBMcaTDiSyH-ExcCQC3RpXsTGbvEm8uSRqCfkiucLKgKPMbmpkcRR_bqESteo-JoYrNtLDLbtifGDK
nit823vKEDRpbDMpQzlNThOO-vlNh-hHIHNjCUocRqBp6HwLRTQBpkIv0ka4djEU3HVDNkEZfNAkcJK3lDQDgGdWz
ltRb8gBZjBrWLB4zdCxXGSjwaGwRJcHfmVTBZtCx5GAlDjBiYxhmqdS20ZnXDMTRbyh3kPFxcpNa1Ch9uBkAsLORt
Y2rVIdztxsmkOQ2pg6lJBM5ugPRaRCeZmUhfFFQhB9dQVQNno2R1skBHh8InJe7PNBhKu1P5Uom-p5Hll3PgVWsus
4QbfG5fsykOWC1QByTCgcvewJftuc-XUtq3dBcVCNrsaOMACE60Ci55WxFtlHHpJ7qvvJMfeYkeyfGaCweFFMFOc9
BbeRVaKGItC73QLPM-Fsuylr90BcXGKTMHNyIHIuSEFChzOzb4AefYuz1VZeWXwhuETOkFkPlFkVOdueGJZLvUhu9
BC2bDgcETosxYlX77dbxiGjSilEI6TI-NiG5IxznwoctbxIv2kp7pUu-WdMJEiYJSCCO8io4XpqKQI6S5Zh48drHQ
G7NjcGhgAyGuUNWKUS9qauz_iyYihl1AAel4DL-keymseFwPk8NAuwORtPhiR671RWYNoUJvWG5pwhJBczvVCx2mg
rLjZAFhaGgPJcdRY_Ymy-aQmVlWFgpkjOuaZCjKtInfJn79AMUKoLaFwj9LEaf_RYyCtlslnH1Ym2_0aIpqmGeFu4
e3O4M4Yi-HAOK0kQmgUx2BS7xpfPmksEMiZ47CZMBqRqJGHK1vWlVAKbjRE3m4o0qSe2LlAUQPJvPwt3ktjA1VsyG
tpROSw0-CcGUtEiHQMrOXQhIaUFebVWVnOVMnNeISpQj4gtDEkXTbUBdUqJSBZsJ3upmNqxckie-OC2c0GiflFOJj
bD-rw7ORlqyaZPYqKyKUo2uEhlJYc2StwnG9J7FiJq_jLA-ROc-QLIirdxDGNxvKA8FddTCnqtxyR_y1ac9CQXL4m
azTNWFLGjcmiXm1S1BSg9eYzJe_tC3FJlijSV1vpCEEljF6u8pMaRhIhGuCSPC3ifEZMzl8a8E9CkdjOug-hTWkdJ
zjE_vZkkBGce8vJSVelkY_mTVnO4kBqYyRmqo56COq_xTDAOFj12mqzWYsB0FfV1aXwEIThj4GHHhD8",
  "priv": "N_Ad_9j_QIuhusOi_mWxWKvtFWt_Wvw8f5pL7LOW6hepmK0yxo8tk72JwqMJNfKM5-xzI3CjEM_
ZdotrjtKHlw"
}
```


Figure 37: HPKE-14 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTE0Iiwia2lkIjoidFRkMnJ2aU5FV21sRFN2NTVpN2JwT0JrWWdpNW
5ZdUdHNDRwdFJoVjUxQSJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "o_WkCvL36wuLHZLnwGKL7iIxcC4i0RgJbZIHoTaqDEqGdLGngTAfL-RvT36q8Dk97L
jRDrA2jIKLffPbGYBp2B_vUpIY3OiIGu7YydEL5Yn6FLgkcg4R_XXpVzwLQ9z8WlDyoBEUoOCb4CHEcz6SghPybNP
YkNWm3eKD786JPo2WfunxJpFjLHRLfjHkb4bHC34wmPjrbtacAJugpJNz3jHLotOCM1wH4RL6MiGrRzC8_pgTiXHQ
zoPIgJSS6pstFhe18U1MLtZckKFly88AmYus_m5S8MYkOmGLk6mI1fjBO2fpfTee5FVhzcD6geavYNv6Q7Jwge0lX
ehJQ1lvBl4aYdTib95UDlC-TLKl6mSob6dOlQjH7BMPdfA3Se_txyxfcfDSgCxnKLTmocP6zgZxcSdqsfBCbIVfjN
RvQt9Ps64vQQ7c-1zEKGgKj4FMnK6vhHsfdA4QqBgQzyZPz5F8KkwYjjCOUS3N-y1FKtiQAzsGLSXWwZy15gbm1Ct
fVc9NNtw_iJ2u60UbexBJUJIAbQDeeIc1qeeyuzSs73sNvWG4qShb66xP70At9TSABNyCG0Wnv8aAPRXIWyI4c1aW
1cTvhPm18ssMR0Q6vsxrOOdB14EuubwrqNTx4wk3x5hB0NjnZvRhHNLmloSzF3JOeBq_ToASMLQ4YTBjcrVqYQwOC
oYLXwVS2VB_uwqUwgmBjCwlFvghGQAinKEDc3oWadF3yx0GI5ifyTMctVCo5O7FhkZQ88Xa6rJrw6S4herDuwxqWL
bptamRQ-w1Aw0Ro-dMSqFzfD03k2bslWDOotdCH14cqVDZUoa_Ttv_u40NCtrNzm0jkBsfxP3tMN5zkOLpgOn5djs
q0GpHl5_TWDuAbiaTYnl7_4s_bm3evJ8v_1IMKWJh0SV3b4SkW7fsR8TdDW-ininL4c0dT44_I2PcqjxSA7rCv_f8
AyvVNmSFYXzO3D6PgnQ3hpy20LRFut-8LvmVYUxxPE79yopOibXvPRSNqksUi2_WMAaRG43r6almBuKjeab47kOHO
VN_gyX-2BynU8kjUchgqDkn29OPSpFabZmcS3hg-XhrSLM4rqEzzyeTa1b2a6hfqMwt7VMFm3ikUljQjwfqWxAYpC
DKbRSFvTIELpRQt_ruSa6VpPfUrv8I-a9eHnYjD5JcgqEzMcGVKp064A6KNvr1Qo0xgY4EGobxCAS_oK-uKCbHaD_
7sRRQNOIXUJYb6gwl4VyMWmNRmae9wJUZcAKwErVj_1WMWDCUQw_-6_2kBqxR5LBtkDkfBLtXjpOUus4rWD_JOZ8H
aFxjhtJCT9RUa7KUQz8pTWX3TAvHvrBMNVe39HhfdIP_YwaqzPzFFZR03YYssvUMhhV5-o8hxqRuUayDQs-PONCYJ
YW6trtQvz5v-RmJNuXwBIqwnjTGqVKiaz79qwdqQevMMb_WA4s",
  "ciphertext": "6aJMWpn-x_Yc0ltWt50xOGyCyNIJOVB9F5P3ImqDWjFROrlcxzlN-P--Ht3CcFcCbghu7
qPPya3Rl_eEQDi0dqj-YuVB8Iwm8hYD_c7Y3NALHDOURIDIkqG9jLo4vDenlu7gxTKfAKIat4Vj2hG4r5DYOBC665
aj6wHkyI49ZdpOdL2jUj5_uR5Wbtf_TL6VxNYEP0nbQJ25znOqq-fO1IoaZtn0nOdV88g2vaX7ybGCe11jgvr19l6
Ys5TGU7AHrUO_WC2oXak8pfxFgNP6aDJijj-PmwGyCOwAZJ7S9kqC3X0iUZi54phqfOGJM7OZArv_xP6MfGaKqtHb
FeSXdUilu0m1FpRk4zZRMDwkentztQWVpoWUZ-eBD34Kqgmg-w"
}
```


Figure 38: HPKE-14 Flattened JWE JSON Serialization

eyJhbGciOiJIUEtFLTE0Iiwia2lkIjoidFRkMnJ2aU5FV21sRFN2NTVpN2JwT0JrWWdpNW5ZdUdHNDRwdFJoVjUxQ
SJ9.ZP5RugHbTix4Mt_Pu4A05QRcq5CpMyItvXR9eoC10M-t-OYq4nNtNkHrJSLyS8jquuviJ8bxPpY4SnGjt6V4a
l28t_ErevUqxrxwF_vjHcGs5LOyfLU6EA7Gy5Zc13GDrnKegBAYph3TfN3M8TNAgJqfBuV6C6UB94CrWDf4GlRyt5
v3_fBIJAg2RBwH4wxlwX7T88iyhYmNPLDo0d9WTVZ379Xv2Af8K5HHw0wvCWQRn-0pbSDTEbIzu7fyju51pIvhMYR
IWV_mtF5mOqjjBPymu8Nm6UL3-mN8kuKDwfDEnjBMZnpi1frhB51Akj8VgyD2t-5F0YCZDXo2khfRphWdfmYljunM
iq3dEAv1BtPaEPu2BUKcEPJEplo3lfz3HXZowJC3Gpq7GPrEhu-5ra3P6ZE2hlNvbdwTWt-c4qCvYFZiyDaRB-W1Q
wPC5iEyj4AX4zc8sBWhqq-AIyJrZeiH7VXwWOYD_cajZlm3Pb-gdFdX2Xej1SAgQOtCubTyR7OUs2DDNJcalmJswl
8nHLo4rjalAsC41X7g8j7-6w7LoAb9I4rgvoWf0p3w_nja5PvajoqZgvERrYDhUwNqgJUcIWg16ucVhYl1KwJ09yl
HCmSC0Q26nmimQ8-ty_ZWCiuyKwx5LHuk3nqzBzCIJalA5JdtK_PyZ66nCy7yq4oNqpKbAxEUliKflxiT8OexUW8T
1f0vMcN3BCjPQFTxXlDkggalu7-X6cfxz0NqImJ0sAzZ4glqhvWOEJZRCHTDq_uKacUUYx4EhMls7XvfrHUcVtdFZ
pfNbE5SF_O-L9e9bEe3A1Q_XeVLoq4TKycYTSlIYEbxne-thzbCRsbfoU2ZC4O3AN-6YGonVizLJcuAyKGP4LgTRj
gmGKAO7hKs57x398FHGmcSWRPLBcPTsWkgiVfRjv-AZxRh5A5hVwR7H37CjajMey6DLxLe258xEwEp9aUvE47WZdt
1LvJo4LxL0TXddCXl0XLGlOM61ULP8h7EGD9Ju0BNaUHsUgSoUii70UM4TNE5QhGpLi7Jqd9H9ims725IzB0pChrp
IWd1WmRhmo_pbqn6_8RWgiJSc03_y5FBQ9zdhzJ99i67j8pWFiw7yXjEcYCBj36znvgS8HltSxsc6j-ECIbhJJZQd
em_8TTKy_wmmFrTcU27AaiDsBINSZyBTgrdWP83zRfkr4HkOJSuaTkuw3NCzHWgMM8zOEHD19hDT4x-N8jvxaAlp0
cjZVHKZobIvSgyCE3DMSyOacltz1o3OTPbzUeT9FTXUEqUGLT3NTdD3Poe9-pINQgek3uNA3ihL8LBlnlN5NnJ-bK
QLxAdtbCyr0xnpJSGnAFXrANyE6eupaCWeRPinlUTjKfnZuEbGpvtZ7xv_Bnvx-7Pt0ecz8BVWiUOUtaMT4PNMoNZ
xCe3lOXVl5aeH33TeUdWtlNiQ0A7Yns..5zAVwDsdj8PIEMWvwGbW0enbH3dPtmorf-e0mXFuCLF4W46jVikY08Eh
Ygl9MfCpdw6TsGMB01wqIQeKNeEXmSutrKzv7Ptk-c-CnERT03lVXna0tM2sPtfc6yxZdCoYaKLUibR8iRseVFYgz
g5s8dpSqbl9om1wryBrLIjaf-y_W8WWglJ73qVlANslgJgt-TDuLx5Fi1L9NCfB_Sp3O7ZZhoLlH0HwKSBrMNPVti
_1OrmtA_51rQYVEer6WM9Ppy5aqnGrdYC5dEhmFbgVjia3P3BzETAOYxvPI8o48yRKReu6GXPxZs-PnhifmNYEYNd
DjR4Q3rqA-MLra25SEh7W5_BBDzTBZK-Fooa5-Y-5PDU5xgWhae2ErXsNPJuw_w.

Figure 39: HPKE-14 JWE Compact Serialization

A.14. HPKE-14-KE


```
   {
     "kty": "AKP",
     "alg": "HPKE-14-KE",
     "kid": "7BWJHphdDp43WeKHRiCJq8brdH_QZaPcqOdxp8Cx_5w",
     "pub": "RNNzFVw6RPUq_fEOf6KOUuy1ykikeZbCkAo9LCVr5CkPIEgLS6wRNFORcMxlutHJUkLFl2PJqDG-
qqGgeWknYmhqfxZyrDW6mADI5psA4lFdljNeMps7wXyV8hW5_gJ_5xMSnERJUraHGYiIsbYli5qTMfI_VRk0l0yT_
YlRfJQbB0iO0fhO6eu8gnQI0ICLBjBlebwSdpKfQ4MU5TVEZfF5XcY4bvtXtDCHPCKjf4U5HPanLokYXZkRIdMJbx
M0kCcG28i_MpaC38R6QKgxiNhjCZQdfuS6bYlJCocupsC9OCYKnGcpjrCdVHF7u3lAZPRwRjW8aOut1uAmziihwng
PP7y5C1VF-VadDGk6FXIKsKEQzcgG_6o9koPCdZkh4JVzzSShOaZrb8C1HxYTp8ZC6sYpVdmZXvdtOOhMUAofwSpO
AttN3gk6y0cWOnc8Jfs_0wkDhkl8-yB7-oV1xsSRM8c1wioyo1jMTuc2kBKzB_aLr_EVyGEC3vh_7VhkIUJSpZOQH
QxyTylnYIs7H1FzuZSBsodirigqi-OPelINm8ZKMgqxoAdqocMYIuPIaOiTHPjHkWLF2pde9pJI89oqdSWE5RXBfc
CSZFAGZvYf-YdZHGR9NAcjzUaz-pkbnVGTGQWylloCgQTCe8EPUnImW5RVYuA2TpuzOWutmkFeXEoQzXsKb5XGdfQ
Z7fMQitiuIEtCxHNqeFnO1HdM3_sR6yI6mliakWx4qNwf98k7YvmZufQuEHXNaSyXoswFa1inD-iJM4wk_1jPQex9
ugR6fJF0GSLI23QtNkQcOcEvhoowqIO_fMB4RFAn_-KlS7iZeBiIN0qVR4YKgiKAsoWgRctPbAqGX4ecqRnPKvhmw
7g22zcNF7cW9CwWKEEeX0qR2ORUlYRaAys7erNh4NyT3CURykmcuyhaOyGoR7ObO6IpeZN_ofBg3NAeXdKTcoxd5s
dl3dNJtUpy67Qj_GMws3WwAkye7MVD6PnILwJIx3sKS5dp30SlhPODg1IGPTtQDjo88YMyMXkjzig9_TiMO4S4L3x
JwhMAnOBwCOEUHzODC3wgVjskWHavg0WsHKgy-PCzYRGS2Gkr6cQ9yCtop5GbE2XGv1UhjUrOifeuGtAsvPc74LxG
B7h-iRSH6VvEo0QKcGcYI_h3TipOQrS7S3oq-Fx60vm2dBRcxYTDYmWfTiloZFiSY2K112hdbYhFuvskRdMrdwGj0
6oMf5FS2BtnIQlGRsokrcgUq0ITD-urnEgVHdIFd9hPlCG0LESazwuGP_BIsZczC7GsfHHGf6A3wcuJzghdCet-2-
ay3Fm4rPU-d0Bm1dS1FHOIZSUwpnZfcOoc-_xRnetWxQA2l0qZX7iOiEdsgFtvh8EUDERsKnSj4YFx-wR5IKQ7c-a
8RUgemhsJNbFHTpDH4OCGrplKCySkZgYw9fE6jqyJoDqCadMs76IjG5Swp_mUOiUOuZmEWmsMtKUEPmNiNfojEvk1
mdyP3eFZazUnhHGJSKYM7zCv4tgBAWxgW2JUM_qMDb-VNEAqLf-02Htt9uFnw1Iuk-sckMHfcogpKPU",
     "priv": "Hb3zfRRFdGQl0I9cMurrDBR82FDNmkbxfC9aHBfAbOnCOYx-v-uiPuHxc6I4s4tIxmusMpWYHtA
h5PCOekQgqw"
   }
```


Figure 40: HPKE-14-KE Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTE0LUtFIiwia2lkIjoiN0JXSkhwaGREcDQzV2VLSFJpQ0pxOGJyZE
hfUVphUGNxT2R4cDhDeF81dyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IllIUWRlNzdMR3l4eHpFOXFEZG5MZk5fclI
zdlFobWlGTnJEM0RFaVcteTZzRjVDVE9BYndEV09yOGtnOGN1Rmo0VThGakl0bV9KTXh5ZU1Sc0d6TWxHNFVVVmxT
c1N2aHRUYzJUU2VYMEx4Z3g0MUR4WjNOZ3p6Um1aUWRzbS1IZW1DdlYxVHoyUHpsZlpyWm1KRWZJaF9qRXh5bHFJQ
U9VZnVqNHdOczlZOUpVQ1RES0lhOEczUjlxU2lNMVdwNlJBeTZ0UHFOc1d5SGZoX1ozWXZ1dUpJQXgxMkc4RDdRMn
EwRURJUy1pbnpWeE9NOEpKbGtVMXdUSlEwTEFxeWpTNlRxcURtbVN1YTljYzZaQmhkM3cyMVo2V2NoaFBLTXdYTEV
hSk9aV1ExMmdHTTBwRG02bktiQmw5QlhvM2VKQl9zOFY0QWNMV0NXTnR2bThwcE96V1RENFdTREtYVUZsSWsyQjRv
TVdkUXd6OUhMMUZPejY3bHEyMlA0dmZfNFdRZzZSMmtib2pMc1lIUFF5Z2U2bFJsMWlVLWI3Z0xzRGVxMFE1ZnBzS
TFvbHZuaE9zbllxQWVuT0M3NHQwMHJSN1QyQTA4MXJWZGcyZVlIV0dUSzdwUWszckZmMTNJU1lyaHRCQWJ2OGpmTk
5iUE52QWk5RjBycHpYNTBKb1dQYUlvNTRtU1ljOEozWDlRNm96Tk1qbHVFcWItdVdneFZHWnhtS21kWktpcDB3V1R
```

```
5blR6WWlXS0VLQkhhMmVHbjg4ekV5LXRMMWYweVh4UUQ3ZmVVYU1FR21YUWpmdmxnLXNBUmFxeVpVTEVaTm9wc1RC
WDVkbTBSZWpUWEItcVJnTW9kaFJMWm5lNFBsNGpvWm4yM2RWTlF6aFRhZXRNVm5VQklNNTJmQXlSdGFQeGZncGpYQ
1U5MWo0SDQyeXJRQnpLeS1CRUUwbko4M3BvQ3ZqX29vMWh5c3FhdkYwalYzbXo3aTk2WEVtUklSZ2VVSVFyWUZpcm
9hcUYwNnFaOXRGZDJpZ1R5QW9SNk1vZFJIeTFTOWdGZDBLVmRtd0RNZ0VXVkNzSXFpcUwyWTRLb3JnLXhXR25yVmt
tNm03YmhmWG41eG1ZSk41cVhsa0tVaEtNRmR6ZUhuOTIySDQ4UEJPb1FGVVZRVnlQeWxldS1PU2diY2hnUkRaSTFf
S2NYckxVR2IzX1dsVDJ4c1RsZlQwa0hlQ0NKeXI5UGVpUnFNSWJOZUNjVkpFeDlWMm8wendTOFFGRnNhcFJBRDJwQ
UVzeklWcHZCMjdNSTlhOG5PTTNmVHRuOEZ0QnA4ckZzQWpxRWFKa0g4TFdtN2dqcUprTlJXUEdpYnR6ZHBTT1htNV
FhWFp4WTFRdEgzUTgyTExBczRyNTNtM0o1WEI4ZjZMVUw4bEhlaEtOcVRQRTMyNUw1aFZFa2R1aWJTQ2VFUnFPeHZ
IXzhnRW8xU1BiVk13NUVmZHZmT0FCdXZ1QjUxbzZHY1dVUElaOWpONXVQcFlnak1MU19lQUFaUlppY05QbURwLVNw
MUpfdm44eVdFV25HT2ZUOFlpM1dFb0Y0LTdCMjRvZnUyZS1QcUEwZjAwcG9rVkRZd2s2YV9pMEV5NkJMNVczQ01Tb
VVvbmVJbDVsaTVETFJLMThjbHZRRFZKMzZrZ3Roekdha0p0U0JjWllSSHVvYW5ZQ05GVmVSWVRHWWpXeEJaeTBJRE
gzakZEY0NfQXFoRGhoMHlXTURhUWxYWTR4UUhWTElXc0Y5UzloSzE5cnBBM3U4MDJyYTA4R09aMXFSdU1ZVEVkS1A
1RTBYSjVxUFh5UkM4TFlSRGNyTGktMmxwczdaX3lvRlkxUDd6QTB4U25QYmZiMlhleGpkbXhNdFRtVXpEU1FaemdI
aU1Wd0FmQVVKbEsya2FseFM4SGNxbEVvIn0",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "pMkpDTKo8w1fQKf8",
     "ciphertext": "A7KIQ8cBai8seXDfYlswOxAi8OVFsmbd2NZQGdtIvHsBNtGTpRSf3IFM2QNSKJrr5J4rv
waCPEav0dgAPq1vdjGYzVhgApvBu589G81UGJQz11262vqXn0sGnsTozZSKZ-4LfEobLiZwgLLOL63HtaRkHSUtv8
gvti9zsq9oG0hTrJOEsq_vGuzNYOYR2CH-F7_StQlfg122UYFLASE_WxAf0erVHp3nDnJ6dU4oEtCNAd2UXot1DKz
xBPVsR4BCJFmNkoJl4sQ5KzZDUqo9alghazaFobnvJjiLZmMYG8qZ36MyBSTmbQLfjOM5UurtF7fMRWkPlkadbW4M
cu9AiDIcEYK7XsdOLEI9GP4lTHuw",
     "tag": "lo85SGTZM7L0EtxiLUZb0Q",
     "encrypted_key": "MTvV9_ja9VljRM8jFxjnbnQYKi42hsWU-ym50Gh73e7IcBJgpFcdFLREaJs74TO_"
   }
```

Figure 41: HPKE-14-KE Flattened JWE JSON Serialization

eyJhbGciOiJIUEtFLTE0LUtFIiwia2lkIjoiN0JXSkhwaGREcDQzV2VLSFJpQ0pxOGJyZEhfUVphUGNxT2R4cDhDe
F81dyIsImVuYyI6IkEyNTZHQ00iLCJlayI6ImdUNzE2ZFpva2FpVzZ5NEVIbE1NWTZkRDNtRURXZndjT2k2TE9WeU
RoMTZidnpXQjU0R0lCSldpajBsZlFEcF9YLUowSXdleDdyZVB2U2wzbFZWMzdzbE5CZUk1eHNRbnJoUWhlRVA1Yk1
sUm9NMWVxaFh6RktuRV94MzBVTlFqdWM5Z3FHakdTQzZEZU5GcGhta3AxRGcySHZoUm1SUTVYVTA5TFNZajctZkRU
T0lGMzkyYTE1TkRlSUFwNWl1MTdJel9wMTRmWkI5NW5uamdTWUc4U2F3anlCQms5MEltZW5VaXYyTHluODNqT0Q5R
2o4MHNFNlEzVzQzUGkzbU5rTDlBbFVQS1c5aGpiNjlfemVMNU80a1hpcFg3OGFlWHpTUzhwNkJENHk0QjNZVFNkUm
9sUUN1TkI4TnliZ1VkUml6dVFHZ2E5ck9mcTJuQnlIQzNpY3AzajFxWlowb1pLMEtDcDN2UklwbDY0U1JJR3BiUlF
zLXJndUIteVhFMmQ1aFR2T0YxVU5GQ2p3VzJ5NkpfTDd3T1VWdWlWd0doclo2NDJxYUNfclp3OFNSc09Ob1JMS3lx
Zjh6NmhnNHhNdXg1T0dQUnBlcFRVSmZxQkdBVUk0YWhreU9FQUN2aVNjVWVpLUtKcVdTdXdoUlVpV2ZqWThXQ0RLe
lRYMUFlcC1fdXBfaU9xd2pDQ3k4QVA5ZzdBMGllTVVXTFZqckJIWW9VMGI4eEFieXJ1bVFJNml2c2ZTR2FWOTkxUF
gyQnZzdUZoYnV3V2k4VnUtQ1NfMHFCRDRfaVJDUmNWUXVyLVdpN1Z0a0FPRzYwWHZENWZKcEJta3dtR1VIcThmenV
hcDl1dXFzSWozZU8xN0Z5SU1CQWx4MEVIaEV4NzhqUmdtTnk1Wm1mbG42aS1zRXVBYzgzM09lTi1VeTk4TFhJOFI3
UU9IUjZlZVB0a215R3VmeS1GVnVmZ3Z1VVFDR3pnUG53X0ViUy1XR1B2MmRUbFVEN3NIZE1sQWd5VTFKQlduX3RJb
lRjc1B5ZEhWREJaZ2V2WW1nb1NOV3BVSnhpZ3RYanBoaExEOFVSOXhrMG1GaE1PNmR6ejY3Rzc4MHc0WUQyOXpobF
9vTnVlLXl0UHd5SzJNeVJhX1czWk8zWVY4YUZYTnBPbFlEOVhGYkJHejdjNjI2bGNMOWFqTHd1bnhzd0ZhT3pLYW5
waWZfX29icFNSOUJkVFZNSHVuUWFKZ1BxempaOTVubVJRclRVdXVtMkNYeW8tVUtHRlN2cHViUnVqQXlRckZvbGwy
X3VoLTBHMjR4am9BNDU3MldIdUt4aUJnNHItOTJkRFE5RnZZc2lpTHcwTzgyNERqT1dCeElkRXhfTU94UTAxaXF1c
DBUeVFFaUxpRE5sZ3U1MVFETUQ2QWFHWFN1bFIteTZKZF9keTBXOUs2Wm9ybkR0WjlSMnhqbE1fWEk4ekw4R183NG
NhaGJkUW5hWTZpT18yTlBWSFBGbDB0Zy1uQVp3YjYxbTdKZnRscllpNms0WGMxZTRhTGVaenVVenpXZHBsRXdXNjA
5SEwyaHhGb21FcnBPYUJYLUNGWUdDRUl2M2MyYmJrUG5uWlc5YnE1ME5uVm9GTENSYnBXeWdtUGNvM0s2b0xkOVNh
c1B3ZHJxeUFnVUdBdHdzWUU0RmR5T0J5eGU1ZzRsREl6X3NlVHBybjhIWG1sTFNDWHpCcmU3T0NqM2tFM1Y5SHhOb
VlKaGdiS3lGb3hhQ3Zuc2VPY0pmTXg1dTVkSkxUWVhPRE96MXhwRjI2VVRaekVlX2g0YXUtWmp6YnpfSXhydzFiVE
9Fd2IzOTNacEpXNG9Jc3ozQzhFN3RFaFVRbE5pbmNYUk4zNzJkR2FfR0VMOVAwOUxwTU1LOHhPaXVZeVNLbDBwTkp
2aHpwN2w1Q3NFIn0.pUFBSTN1UwoAcUmaAV_Y-BN9JkIIO81rjoY_J3WOCLrmHFCD4pOtqbxz6qXabi7C.m0qOIOM
8WLG6BSlQ.xRhjUVCb4iDeoz35EvoZVPkXHPfEFCqcem_OAsdoEAjGfL_SbjsUCMEa_WLo93oY9FGJ5v4XvqkDssg
RejSk2CHqZNTKsCl7kdpGWpAdVmpspfriScs1W4rAdwS51ezAy8WEbtPeIWsqbZgD06OwiIh6q2RW0XyvDSkHxD4k
Fr6cW9bsKxtsoXYRcMSwrQ4R5InkS7s_OjdKVZ5WBl6_2ebIaUwu7YxQs5R_PTTUHVQjAkAUq9Y4N5EoHbyyLJ5o_
42MHVmef5yEgzxYPuI4BpwChUXAM9kgp2cy0LzjsQx0qCTraLcF4eF73y7NxSLsW3kHFLx_rT33JwmNrOGVdUbYRh
mRm2JXc5EEXAChvvKE.8vrAlP5KTXVBcojU-vO2dA

Figure 42: HPKE-14-KE JWE Compact Serialization

A.15. HPKE-15

{
"kty": "AKP",
"alg": "HPKE-15",
"kid": "ZGM6NvYI58WstMDq7U_u7MEL5ZJf4aswWZBOyEqVIHo",
"pub": "2qrLZycIp1uSVzC0B7Nck2cweEC4OFZmKNCYuUZWymnDYPCP3BNMzfgQnaoIQei1LVNkaEQwDDNE
1Eo_dtAN_jwf1wqN7dt2t1aH0ds-syNm6bsqjugwl3mnhOW4oZOhEut-YGMQQ8wensFWFPhcqOSdwFmWv_S5aZR60
fYt4ggKS6eh6FcKbdOMEcSytDodKhwtSbkuEHuim5ZnNjRTiznIo9vFQzi0C7BZZfNF7-A0t8l-2wexEPpxkCVUvm
xoK9qN9xRT8RRHNAF6__ku_-PJEdMkHoKu9aoj4leu03ZnT3ZdxVkmWrldg9NOzXNXkPe1c0WUPUwfJyIhpAhP-3W
mzIAQhNAaAMIiVLZ2rCirKROl6PFTC6oRwnaYEMhBgIMlUAxADjoEVgpmlldijfSOUahOegTCvDLBz7XEH7SLiXBp
LrIoOYgFSDmFUbcLyNO0mbF2sebD23ezAFpVBxY95pklmMsU0tiyi2qSU3F3Y6OxIOhEDoCiY8tSMSxMWVZ93wwQU
OtgyaUXiFqTXbN5g_dd3BJAgltRa1eqb3SH__Cw-wZDdtsjGElT1lgGiQm2D4tJb8Z86vIIm6STRKzL11YXZNunH1
miqdx3XGiYgbcLXAABspS6rqE_yAaPyNkAnGKh46FilDF7DzVwMFsaLqgX2MFvHgIOYPR0JSMVYDOFINlxziZdh1N
Nn_Neb0og23KfBBlsZEBJA-mG46Mv6Axx0YOsx8QhSbmie_ImEAQw4DkFnVxabqKNWWPKHeA-soQAr7IcjnBxZOud
wIo6qENjC0JNf8K493Ngf9wzCKohE7UJYeVixggF4Ykl2Qp0eRKQdNGygUeSV-SABuuvbQJNVSdjmqGSlJXOTds7w
_KgIzqHPOokdrZLOQyC81hpeVwQJAGbmRy6oxUq3HTJ3IepPCJ1BMxLQkIvsYitbjMlH_sKlyEcYGpS6lwI2qAERi
gUZDdHWTm5swscXbqMzHUoC1J7DJeONUqh6PozHNQJqRAR2WyvjYCm8AkJv-U1l8iQ8UtIjoUI9mlCQGxk_bppX1a
KfutIugM2GHfBdBiwtYvOrTkNibxev8CQfrVrLwswTto4NONqTtkD3hFjZSlao0OhhkakYRZf9KBY8TmE-GOQ0VIl
NmVFH8tbPgw8aHMVq-EcodhWI0bDxCuvcCJnESgAVBq5kbRrohYPcVghF5lqN9OEcGbM__FsxpnDT-oVirsMHWJdL
bkH6gRizTtK2IwijKtxNeI_u8cMtFEbJFM34kgW_kt4YRIipLYWTrC4uQWRN9mK29QPj8lu0mpfnkcMaCYXljLOje
wlPaVoeNmKgRLKi5lzFyRzadiiqvIVbYiJxXaexua5yblKyVLJu-axVye0qWgqOgwA2kG-8BfFRdONyZAnwHs_riA
w4mElIsQyvNeUyBDOjgxL1iNRN-tD4eUrbkdN9CuCI7QddIsqn1I-IclbSPnPapEzfCnGlpJWryiamCICWbyQmpUM
hVpb6dlSBGB7YjN41CgXCnp3QGHKzwFf6yKYgZXI0edmG0UWdB8KXsL4N9BSZ7c9Sylgcgo-YYDGAF4",
"priv": "pdAf_z4ndILPTG3a9oDpluy85vzVupYFvu4GYkJXgOBpm1MXuljgxJNSscynZ75LPSl3hcbGhGE
eerhFmksIeg"
}

Figure 43: HPKE-15 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTE1Iiwia2lkIjoiWkdNNk52WUk1OFdzdE1EcTdVX3U3TUVMNVpKZj
Rhc3dXWkJPeUVxVklIbyJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "dkXwmkS5DhliGgZoKYHpbsA7qfhYz8zPy0ijhJkWD1pBW2rwArljom5CmRZ75DklCA
27MSQlB2I1U5avR7jpMu7Lo2V4sSkf-0GEdMbCmujnKwu-aIJqBglvQK20yyMvQJZ4uVQa4wagxEwOsxcjMFx8waR
Njb_vW8DZqs6xoSoQElBGnh1LKxLh3iQhzEye4aMLZFz3UjBf5560JaT0rnYVNP6IRMo7iZBrsXEfPw4G9K06BHao
zG972FBvPwrMp60pwdmo4_pEsajlothC6rsd9UWLKBHN9cK6UgPmOS6u2nd01d9eW6Gu_LHJ92tdLT-q89TpnteJi
MAaVnVqqTwrJ8IKYfOog2cbYDvg9PZXbF_dQoCYf7t5rKX_aiTgIxtilhElZnlpMyZwg1Y-qGwRtV6zw68sv37kNu
SSW1WfiIX6nBZdI9qRYqRYsZlNhSevEbD6OyL7b6fhmShhlGcswSzaj3ut1nnBnThJnQbzLTzWWcChm7YcAgimECl
C9BZyFP3WO3dYSpCfgrB-7V_3m9hlLqdRYdNE5WZs86kgIApkFT0h3z7pR2HxYkx2t2-Gf_fjN5x2IsZ_cKIrzzTA
46oJtD9sXjQxEFdlHbQxHrtgsTMs8FWK7QGmC1QRlKnLme0dye8z0ri5ckJqg-92OhmWqo0BLB4LN_HPgjdRsznlc
WmDDLsKyZT5x9YBBlMXnn8ouV_NI1gwOkTtWWolyWhdUt25im2p1gqmHLlD8z77rkqwi0RHxC58sfSD2p9oUpX8xd
ESq5KQEKSVyI-U2uU63lNFEDVsZxptInwPv5JM4JmInQmTsqktSUFBI1Pe3ZboeabdpZxwKBCO2IR055AUFDYQykd
EHsiiSe8TKT13wkc_Jn-pImrYtUDhYOk-V1L0Jz5MHyIusUjjKi_5netW_tblgKWR0tKh6Bokcf6sNy9d2nFKayAi
Lw_mvfYLV1W6BErg5sVWRdWkzYYMtDse-ssc57A-PAMj8LuuVZpkpDlqWWeVLp3iNEg8g6t_ZrNvyBnhPtGXTg7x4
uew1OcE52dTCnAEqOk8Bt_ld1Zywtk7XKieseSsbwq2LuBSQqiDJKLbJTWUg5ec2PPqvJFhivSpflamdzBqFKUCrL
aL36PzVZFiQ5SXRaxirTYnOioA7kCUY0LHSkZMcfhD29HN06kF_8o4G69ErhTvdtULzDsVD5SBuo6hDXrP6i-q6u9
iFLe-2gq2ZPBzHCApmfzs2HuK2kQUDqI6bycRb4Id3lSxuE-Pko8_qmukMxGvGlqHDhC_jPpcMo81b7hzRVDVFl58
aqkc2m2p-WC-_lR1ulJAS1WATcDExEOuEWtZEG5LkVLLSdvrz8gbtDtZnMxbZPi8DEsnJyu2BnlAIKMHLD5hbOcW9
5YcKDqhR6pdgws0xn4S999mYi3w7X9QdL2IgbMEwoBi9kHZGLs",
     "ciphertext": "w6dLvmV0guszLYz5Lfd1oJlYHt-6MH2LlZc9kg8zSmAxWAJe34Or9ezbHFhdCNrHEMqse
p5iFWEcqfpgrelZAJDbg9dl5o7y8mdy3iizKTMKRz9G7SSrOooux7K4NIhcCHqQhthPicSHEVbb90as-e5wvySNzb
Op3SKSmf1NJ-dWkQctl_DDPVE1s9NCXLwqKOdMCdH0MBZrhevWHDe5nzD7SmMMEp2ZkyY7DQTU4HrAVZ2d9rgDYrc
CpwYGq1FiklI9sEOJ3mP2JzaGlAWC63JMDeI7DinKWVBTjgBUqOyRE6Q3NAZFKzrNt-F6lxqCmXCIGQEjOcTe_QSq
FtXQr65j-Ehdm_zgQaonvaLx0ZSEwY70fwPIX2VzP2r1WdAiFg"
   }
```


Figure 44: HPKE-15 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE1Iiwia2lkIjoiWkdNNk52WUk1OFdzdE1EcTdVX3U3TUVMNVpKZjRhc3dXWkJPeUVxVklIb
yJ9.F2le5B9l9Ysnrf7DAF5rOIlB2yKNcVJ1e3PMRLRz1w2FcFGBWiivrwmmCBMo90s3WrJq-aHEGSoG4IzUIdTKn
R1nQyy1E8SbQqV69AeyFZE4r3k_Q8khIbSkLnYdDpBV-SWuIxOmlTTXuGjd5TIAoz1yv4stjqmzGeBJB-PCEv0Ufh
g6n2diZeKgLRvEcdeDipQ_o1dowSqTDWEe-LYIu1lCwL4IKrQdHsDYnb-K2chGFAlpGcqw40P-McEPihI1xWbjOdn
b096txeU6Xd0HxV4qOVVVAm73Tzm-_5gWuBDDyue7DI_SLXNiPHG2Bisbx-M5YVrNRWpQSCXjL8yg2h6J1MIzpEGa
9ee7JVkBZcEwfUSK88j-1BNmk-2lkCHcen6cTDI3VbbWheA90XC5TqSZ3WxoLpfPxhGSs76c6rZ9gP_d9CtDTxg-S
DwlvJJx7E1gtMtrHw6CU4DUK2YJzo_9_ITZjuMlNrRv2V_t0TVvNROwYLjkzwPaXyG-EY2XBngtc9yaGYFfd7-Akx
bRf5iokUkG61etVvDsEXb2RK9XZIH3CyEeyDWxCdVKW03vksXKnQgNBQZOz-6Z2O0Ir4LzG5auKW_W4uf95FZ-Ch5
2AR56p6WQmw7d3eofUa1tCYxjm_2ApqoCm_hV-83kFyyZy8YItBgiO7lzdZFq4dDp2kAp5VQuPg2j9noclZgheKAJ
1M1_XblG43st-L56-n44U6ouVDhbDmGD6RB9p_H0cCMlrl1nvzJ2UAfHCP0mDGWqzLxwr3YJP1FBuLqtPBMQmIStb
S5lDFnXz2JhBRQ_tiulR7AXPUVU5lMvjBPfzKTUA-O5NfOXUVmG1M4Pl2gecTJHiw4kvfTsERFkvDq99-ifQoseFV
YJOkmddeIwZYRD76mOfrkAcYzTR0yWjfj3fgy1R1gHSURktDVgdudrlp0hAW4QFK8cgPnsv7d1cDz-NjjvFp4a879
nXKEc1wb8Vd5g8BWOVDBOu4CWqMcXB_Os6jGhfqboZ8aeDOuLvfsLuYro2V6XyJs4PYGURwz67IC8TvcUzmKg3vMS
hGhjU9WiZtHGAZFx9bgADtiTll1vcbgL6zTnLb0rUOP98Zb6FO0dPIaWeEDwX0I_NGN8JEHIP3Djb0mRj9-eZWnPO
mK1BGV6AzmYPm5PX8Xd872UqdxoPspfvipHVg3hVsHcrthYV4HEKujHkacoZA3FkTfpREjV4bly782sRsF7IW7BHV
6KOJ6c2_vT1dpiuSNmjOBInMRqn_66QJbfpoFabtCJ87grjo8hAs7tQ5uq-EIwNiZaU2z-_pP4qVazzYRHW_IHRJv
81li0hidylgd7D4FkMZCEsyi2H-hQqEtA04rJx7gj1aN3iXUJ4LJ0Y9to_sylUM2y2mRCHQZnsLhx3N6fyqtacpj2
G4PjjTmE8UIRbu28vJhVJN9J_xQBlvo..PQ0C50veoY2_cMCxu0aF8aougc8tboxxViqTTtLXeDutkeh2YP0r2I4h
U3Ps-N0FG9t9A6cib7C7Cr1ITU7XQmBWQ75ERgstD4pkmTRK_uZIV7jVDY6h29euM2huhp1-hh61EngbPVdkiIVPv
jYBu0m_LdCuMeqJ9Zmuz6_AURdkA567Jz12_xMXRpHMYliLl7_kMzChtAlfcN-_nhKrOizFqwd9C8Sx1eH07P8Mg8
mmHObS_9sQblgmKrB7-NZZrGXY0QQ_aCH0Gfe56ZB-THZFm3RzgeF7jxlrds0haJTPyTTbu5Wz5buRRgqY2MCBjFT
RlKVigres22kAvxw7R4Iez6PrPMHNdkB4dDZqcr_Q7Gk_0moYoMYbkimOWSHnbg.
```


Figure 45: HPKE-15 JWE Compact Serialization

A.16. HPKE-15-KE


```
   {
     "kty": "AKP",
     "alg": "HPKE-15-KE",
     "kid": "hRKbl6DMKnXFBvYQNMKY7mVem8y7bZyAvrO-iwa1KMs",
     "pub": "rwWNymaOwngk_VwtXcAdmJVpdtSt-8K-nUAeLua8q1GrLoHISveTb4W2lFug9UrIoaNocuZcnhO5
oYcj5yWr41bM_BFGoOgrqkWF9gHAa0DP4lK1ZrlawfyrNvaYrrtLdKxj9PyQFLHCVgtMs-JDjSdFhmR28UMkfFYCZ
RLL9SlTJvcVtPSWMdSnv-R8tjazZcc8jMi-NdfLHSGOFOFnSPcKoFAttYm1nis3glocMySCW7ph3zoKa9jJ8jR-a4
```

```
cfLyBmqeWZIXun6xYzmOixk_G4HUPMcQuZWKEXcjUd2_wJ5jRb7FYoSIgBkJNJaCAx11kmn3JYfAuR6VMKQfRRKyi
oBnIhB0a2hqgnN6OSXqWg9lgvSLx1hRkGWcMCuol93YZGiLuM-juB97NMXBhvK_ERCZu6ROm7LrOMICGR3GkYqDRn
uIxT2DR6v4GP_9ECzooNVKmgEzzFlnd8chpVfTo-vrzIYcahCWwYDRMqB9NnQuVR79kwnbZDv_xu8rIoEKm_xMDF_
DAwHntp-hIf5JiN8oPDq6qzaEoDAEe9QdB8QDmK3qF3mmcV_WCdHbO5PPxKrkDJkcMUHCdqaeW2ePaXO5S9h4S9_i
NeFHNAzZxsOgoelDepfWl7Kcxd2hEak2Ifh_ArjodwH6EAvXfDr9k90yVinUwJPqAboriuKUGxq-ZulVsEGHdAfbe
u43KcqEI4JdCH28Ar_nutKEOsOXltqehFGBRL3dY6F_agYKqxZIiZFbcsTVqkwNvHLda9tig3m0eZuRAdoTC8NDCe
2qO5y6B9EylvoaWpqliUuxVEAwdUzYsgWnzJ-ZacylpU_kOqZvLNvXYpNMlyvGuC12KvEHJ0pAJNZqw0-5dKhdk0d
wKaMNqW7EE1sLNhJFuNUXlkgQsLKQNGlQSzQagJVmdx_mmEn4JZ7vxrfEtwJhF8XGCeBzQwxuJjrMFRUKNWVWpdg_
ivU3B5B_NQgGCfHOrCYwtbn1oP0PB6n3mTYterxyudlYQz-sEMVGsyHCItJMvCs1AqfNiFaAUfPCELZTQOegfDeFA
hbImTRNk-LCQQaKgcobiFCxZoBhVlQ5p7oAV6-yGUr5lZMYS3I9udJOVM_myr5QBAKGosy1VD9Kxzd4vM7AqsHjQa
liWrl6lzzDKWowWrrDg2W9J811IbdAOaHCF-EjrNIxxzGgZCDaaf5NRcLpC-XuMbWGhDDRF6G_fPMxE5wCTEXaMtW
bRHCLmagaeOzPAK9MbNEFGzwvvMa1Ing1d_57NmNNIJ8gcyRSJwVSXDehdHLxehROYZATSPliN9SHEISYyulAJeoz
jMuYFi5XaP5yyGKQeI_jxULnlEEJI0IglXVCEuLgzOqoQnjGSO51N7RNFLkisju2EbEXeUE-EniPe0i4ZOYXSK8dR
9arE3kSV-b0aI2qe146WPYRxJ8DpSmQt2G8VYNCG6NuaJIQVKp6ewdyIYYqGkXCKhLLE1eJfKzMUzBZZCJXejCop0
7LZb29MQj3IJFNMabjc_iialIco8CYGnbfA4YlaSy_djZzkypKPmCaO2HnyDdH4rrNGh65prWA0QdMA",
     "priv": "2nnooF569OslD-_JSWfUpKoHdcTACB5PNmKDOFf_3FD9LcxyNCxS-UFDjG0rwKNU5o9jtd1QxKO
V0qTKO-bepQ"
   }
```


Figure 46: HPKE-15-KE Private JWK

```
   {
     "protected": "eyJhbGciOiJIUEtFLTE1LUtFIiwia2lkIjoiaFJLYmw2RE1LblhGQnZZUU5NS1k3bVZlbT
h5N2JaeUF2ck8taXdhMUtNcyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IlRXVmlQTU1hVWYzT09KRGJOMGRBbzNkT2g
2TUZycTVMV1ZPU0ZKV0dLNnlROTFiczRyZVFQcEV4RkxIV0ZoektaSnhLRGpPeHlObXIyOUlBYkZSYnNfRGx6ZFJZ
N3pwMGxDV2hkX09qX3l6V0swSlNpUzdkVVRHSFFEUXE1aW5sSEswREZxSGl5TmU0U295QTlIUWw1VmpqM2xhSUVrc
3NZdUtsNllhUnppay1FVi1ZV1R5RnFfMFFGV3paUU92eTFCVjV2ZjhlYUVvVXlUTzBhaFZDSXM4RjNkYzF0dE10cU
JvWkgtNW83dzhSakdJTGUtZm1JYWoxOWgtTGJLRTluOXpMVWlybHY1NnFvVUtwdzNsS2FxTzlPRm83dDJJNGpQeHB
BMEZsdE1HbUVPSUxXSjlVcGItNG1BSUZ1dXJsOTRpbmNhWFdyNGMzd2RraHJ4a3dGdGc0c0hNT3JYcnJmRjV5dkVJ
LXM1NHhIZlRCTXVOSC1IUktrVlRlejZqbnVFYjROQ3pfLVpoWFRkMk1Mclo5eG9uU3c1V2FQSUVJVWhzVHZzX2QtY
3ZMaTZPdjE5ZXBCdmQwSGlBVXlEb2YxRnFTVEt4LXRHdW8tUV9YeEtYRXlRNlFHMWhPcWRDTTdIakZ2ajdTQjV4NW
x5NWxKNmw3UFZ1d0FYdHJ6YV90TDdURXJWQk44a0ZUczNsSzZfRTBaX1h6RHR0Q3NlaU93Nm0yNVI1Z1B6dEtIeFd
iNHRURmFybUZvOTBGbGZEajFwUFZkOVY5cXdQMWRJU2FnQUtBSDk2YjM0S292RUtZTDdldGpDdnFndW4tTVZiN3p2
ODV2WXhVT213cWl1RlJaRmR1UDlBX08td2cyRzhwaTBxVzRucFE1Z09ySUVPWUdCV2p2LVM0OW8yYjNxRExyVDRGa
nlzSDdTQmlnVnFrT25qY3MxRU91RDVEZGdUbDBhV2ZNQkZxTmhYY3NFeXpKMVhhWUNOcm04aUtFay03bEtSWFROZX
p6d251V2xKb0d0Ui1lN0JmVTYyaHVPMFlsZC03RXZwbDFjamRUbHlJeGpNbWxZa2xHY3ZtRy10SmxaaHJxY2tlOTF
nc1lTWDlVa2t2UDhwbE9iOG5XLWFQRmwwQ2k5anFQbFJlNG5LV3FDZjMwVWd0TFhwekFjR09ubEwxYXY3ZXlHZTIy
UW5xVVNsOThhd05JenRQNkthNmNCR0NFU3Y0aVI1QkdsY0FKckdiRXpwMy1lMV81NXJ2b3BzbkxuaGF6Z09iZUdzZ
2U1b2F2amNjVEJ2ZlBYVGRHbDhiTXdvX0l3Tlo5YjJxbFlpR0hRek53MzBsMUt6Ykxpd3JBQk9ZM01hUmN2VG5pUV
d4N3NGSXBQbF9TTGxZcDJUa3RhRUQ5Y2s4R3pmckgxU3NTN1VQWEstQlVTaXFFTHQ3Y0V3c1kyUFNlWndxd1BZRTN
kYUx4b2U2TnN3cU42MHRLX3lHSHZSOUlpUndlTFE4MU95UkhFandYc2t1UGx5RzZCT1ktU0FrelBTZy1wMVZXY3Fz
RmZHQzBxZUFkVHR5amhDa0xVdERJNDdRSEszNFA5V1NrczNtUEJSRXU0MTRZbzNVaFV4d1RhS0N4NEl6dHRCaFA2a
nhiLTZvQktrbmx2QVJEU2lJaXVvQmlTRDBRUmswdFdnSWpOSG5CeHFuXzJ4REhSZjFveU1HWndudktSM0VtT09FXz
FZQTJjaU1JU3hyZE8tbWJYMWlqTVZaM1RYa3JDaklQa2Q1b2dGTEU1ZXlvbjJuV21pc2NzQ1dMQ2ZubnFDN3BUU2V
OeEpjbUZWeTFVRzZlSXd6Skk3M1pPUXdJcERnVXdHZERoNktUVEhwdVllWldaY0k2Y1A3U1lxRWwtN3VKNk9fNFdO
RUZPM2Vjci1VcUM2TjJ3VkVJMkt1MnZzIn0",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "u1hQIAYmBXujPWjr",
     "ciphertext": "FC0_4PRrnjaK7MClejTSiOk1TJTLW6hnf81PgSz75p5SY2zlpX_RLohI80Bx58c4Xl7hl
oVn3miVjRJRoXV6o6EISR_nhApngJZthFiGA5waQS4t8A1RhOanAjxvnB5TByYS8RV-KUhfxidbMVn7QWX-o_kcWc
Qys1GNh3JxyvfNnMsIE0Ad1CAqJb4mH0l1nPR3BqMWl1U7D_iPQ4lnRAJZz-BV2IYwXX0pC-qVArv8wyeGfcrFGZw
eFb1TSytN2me2P_WbogdYyyqg99N8QbmKqlv20mDlNXuUDw_t3entF8zdrA-Q06qkYvYA2bIfbaR4AO2jRUNmTP9r
xZ-waNC9opZ89uiqNqR7QqoHLlqd",
     "tag": "7_VEqU4IIQtqp45ky_fXjQ",
     "encrypted_key": "jWyjtLfOpdFbtcZ7nVrTTl5cbpjZnHWmd5jB0DsweDYxauI6mgFsCTr78xmNrpVE"
   }
```


Figure 47: HPKE-15-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE1LUtFIiwia2lkIjoiaFJLYmw2RE1LblhGQnZZUU5NS1k3bVZlbTh5N2JaeUF2ck8taXdhM
UtNcyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjQ3bGM0dHJ5ZXFvQ0FERVJzUlhCLXpPSnJSeGdEb3hPY3pVMTdMXz
BYQ2k5eGFCYmlNX2t0VjFSMXp2U0ZJMHllZ2tBRmxvTEpObGQ5a2c3VTY0LXUzRklLSGE2d2otM2c1RGtvd0VVMlB
uc0tjLUVSbmxyY09OcjU5NWRQY1YtOEhOdHRValR1ckJGcTVqYVJJT2Fxd2dqYVhtVk5JUFhLaVRTTVk3NEdoQzdl
OEQtM3RLRm1TTlk5NmFMOEdPdkFvZlFaVnBjTk9mOHBUR0JZUWVDS202a3ZhdWk3bzNBZnRPSU1LNERVZlZrUlNaa
1k0dFRoeDBXVDRWdW5NR0F6SHptT2hpanpHamdHTkFYYjlUUmtCbU1malhDb2NRbWxaYTM4azZrVUlNYmM5M2Zwcm
ljMnJRQ0ZqV2pySDRrMU5YS1pxa3R6QjBvSUNZV3QzNHdtbWVvaEtlUjBhcmN4cU9Kd01kSHBtQ0pjMkFyeS1JYU8
5ZmVLcGhZcm4xQlFhUWhwNEtDR2pjajZtLXBVX0ZUcm9fR3FpWmN0bDU2V1ZaNUFWREpOdlhKQXdtajN6c1hEaXdk
VXhhcW5wdVkzRVdoRFZXQUZ6eWlmRl9vNVhhaUdQNWdPaWJTOTZ2d2ZjMDI3bXZzVmttN05HMzVBNEhUQ2dTT0k1a
1RiNzdmVzFDR0RBeVNDSmhRZGlaRUJ2OU9nd1NVT19OYmZVeTFtZm94Z2FaUTM2a1hMMzFoUjYwVDAxeENxdkh0cU
16TU50YXdfZlJUXzYwWVBhN0Z3YUxoYXBhdUk4QXJ4R2xYNVBQVHRWbEhfUTBmdWpoZXpYUTBLcUJOdUFTS1NtZkp
JVkZzcFF2d2EzYnFiSUNrSzBRd002RGNlalVybzRtblJZUXVpNl9hREVHYmZWOHBndW1qY2NYb1lHeWdFbW9LbjNV
TEN4dlA4S1hhenE2UXdieHNRVnJid0tmYktWTnI0RHQyUWpKOWVnQWVSRnVmV2xJRzlIeFRmTHBsTVotTkxyS3h4a
lppdUJ2Q2I4elBaTUg2V2FGQ3hsanZDVVNOdmlRWUpfUDQyRWdTRk1mUTFzM09RQjhnZWQ2WV9jUnBZNHJpNmtwMj
BnU2hoQjJlaDM4dUFjbXNlNnJXLXVoUzdSRzBuYW85cW5ENzFqeWVWR2JFemxyLUFrSnh5ZFdPMWp4c3B2azVhLTc
4TjBVRU1tQm56dGxoMTFmQk9XOC1QR0dsSmdDcS1xVzdJZWd1QnYxRTRYcjJHU25XV0dSbkp3Zk5YVmlzTlRCanFM
UXduQ2pwT0tEZVN1d0hGVjFvVzVBd0V4YUlTMDZ6djdRTFdQQktLVy1fNDR6MUVCcXJlbGZ3V1l0YzFTMlZzM1BnY
mg3eWRxVkFocG5SbXBMMHkyeVZ3WGNpdVdSOTVBWXJuTkgyWkg1UUd6S3pTVXJBMHJaX1l2cGtjV1E5SnhPSFd4V1
phMlloaXpncnkyYmpESGdMWl9VTndpc0ltYmdvSERpdWNnb1JuUFVqdzN2czdZc1BvT054a2gwQkJWT0U0V2xIY21
xV1k3am1YbWJzUFhUMURUa0xoQ3NKRXc4VlhManpkRy01dWliR0poSVNXRXduRERwaXd3SXA5Q2VWODJfVWFHeS1X
c1UtaFB4cXo0c2FXSzBid1otdG5lamIyUXQyYlc2MHlyNURzRVU2a3JzTi1oWTBncUNjM3RJQzdTR3hCODVOZmQzT
TM2QXZzcHY1bUdpbW44U0NFNWY1cFV0amVQVnEwVzNSTkJ1UFNIYncteEs3bWw4T0V3R0d1dGZtZG01bUcwSWs0bn
J6clBkZmJfWWFwRWpiY2FQQnZKSkdBemd4YlBGQVBOand4WXVWUHZpTmc5XzNFSzk0dUVKQVFEWmNfWjVENEczT2N
mV2dVOTdSSGlNIn0.2wODp0VWHq3ca2J6Q45EFBqZrfqAOBwCYXFLufm6yrUjChuVYcO4Exbb3gQXz_Mt.F7mBMsN
```

T50wX5uf8.YHC1UnsMFlklwSuExABvsTSwcYYkshn_0ITK6rdRh_i5vyx2d6N2rdt6MT9lM3rlcrv9pSqL4fSUvy5
g6rdQXyfhF5hgrvN-y4rXAIYI8ZgH0glNAXLjQPdvd-6BfGIn_Sxf9mo9otulKtqzgYbjp5Z4s-7PTS13CRRapcOJ
n0-eEvQDgI4G4K-Dcf5ncoePQ-y4SBv2CmwNYm64229rkmmNZ8VMpy8wJVRflmiuwC9jGiwX0Pwx5-23fuK0VkMJh
eihsaYcR_HbjMU1TQohcaO-qoUBoDyQXCkExz-B_QTwPQ1uCDt4kf9ZL0uFDSIfH_wlT-QuEw1lgENIa2ZKI15uye
9v0gccWP2qE5PWl8l5.bDxCOdD8iYXkFeZRlyYArA

Figure 48: HPKE-15-KE JWE Compact Serialization

A.17. HPKE-16


```
{
  "kty": "AKP",
  "alg": "HPKE-16",
  "kid": "I8JfWq07ay30SY_COHidQ2Y62ZTA8jzU5SKaMag8DWs",
  "pub": "3yqOZRgLTWIKtdAVtcfNBKWBGcmi54VqPmqXzDGq0ySjp5FHfHq06up4qug6NuOuqHWPKjaRX6s-
_beW_YTLWIVxzKMzZmCMhtwQ_eUDeppbPrwwF3WGR2rMZrmPKutNv3CppZkWtBwKLboJ6ChVW1ivYOExNrrPp_o5h
ZQ73TNXt3gE99hdbOUbr-cMpIMATfNO1MSIpuqZkft9tllGdgm7lWU3WGwE3oZgn8mAapzFuvQqFgYjhENT30iGgI
BAp7xKHMY5FfFUvcWIiwl0VhgPANa_AclvZOdcWnp7EpoT6tQnQBSOD_zPdPxuXgl-mjx94thauWJL2-QQ0zR-9Mu
-CnkBNaiJzmOt--enuRRGB8uuMboHs7OsGCV3J4WqDBWoswx0NdqUEdVxQwVss_R8fgfDpZWgtxx180ASX1cnr-oJ
R3BCFBAaMbFfRFhBfkxr82h5n0lPGkCHAqdE12MLUVqWIfeURahwXmJlfSC-YGDGoChtM0kDazgFyKsdL9pbmpNJO
agtj0Ug_LAoXLYoJoC7wRdaDNdgdVZ56Yh5d3simaV9tgd7ndU4ndy5HDt6X_JzIpetaMi-zbAV8YtWGjNhWDEMtZ
e3S6xbloqtMctV12PKhBy1EhW9mkgt7RBHVvao6wA3OPWIYLODJrtfitLGsLsqmbyHK6E7eeRp9yUsD0hdjRMcdbc
sbQK79vA2x0l5F3K7Gui_HCkkNzF_1esEGEaYzmpKQidJriN7PzlG-DsoQpU1hYmQEOPIRCN1lIgiqNKdHMwjPOZ6
U7JoMekj4AQFXhgokLKGtZZTrKd_8BdbmiI2rtKIIRagLYhT_MtClix25tItLKYDGhBii3Kf_cUlgFyeA4l5myYnD
HqnnIS_ieEybwye_qcPRFRiuxazx9yV2vFTSAN4TZg5MtFGNwEwygvNwwVKISequKRVmttw_IgvfmQRmDerg8wqRV
y3rxVPDzW8oauiM8QdnFtFTUtwlJOyqKCMQjU7JZhjPikItbtwIPlMLhCcifXNE9OmrNVO1VlSRvwVBIc6NIMuw2A
qVNSTYHQCvFF3uvh9p6uJywmfg1icXsUgABJvlpuqKHAXWVJ6kFYBTzqnHSoChNdA0wa8TLkYxcckG4FCL4iUShsa
-2VJf6lu7pJqjPudaZprdKiwD0Mj7mym2fStHRmE2qoefiwGMNocFgKVe0s_KyfOe8ZmR5iUzpiAfeYL5dE9Gxsut
JiMUYqHmCJ71rkHKZodDcUJlEMoTDhDMMPIBkqTjRxDfvqnm-w4yBUEQdCz9ykLyhYT2fMn06pT27Wc8uEFkHMULH
RTdWFL6ZSVD7WX2QJh16UIq7e2R1bCsvxQTRc004KKV-uSnUEkt0NbqUh6rHUzVLUeDGJf4uyd0-XBXAM87exSY7V
4bCp1uyiq7IQujMym85A9EuBX82e31VBnHlhD0zREy-yx0sIrKIC-SjyLaLt9AgoXVUhW8PwOnrtPcLZ1Btsv5YKN
OtTJWuNXKizORXvIWaielZyeoHBBEpFylyY-GlRodQe0N_gKdLV5MVNuFapg2JTHmcIcrwi3CJaRiptBDtxJnOS1W
PwxtvsJQkWPhWaqzkYqApjGh6m_8DIXV5xTabp0ojwAuBa9RizHAck2QqEoQZu9F0d6cHSJpCV-o9QoskaLyIp2PX
JdUGJ6s5E6R3WncaecF5xkZta_TEUd-TZkiOx1cmsWFilxhQiN73RHehh97zVJYoS3Whh4gbiOWMKoNRiv9euVkrc
Ae_dyEnTO2GBM7uKZR_U3JgbPQdId1-uxHJMr7GgmKUpoi6gRHxKp5JoRwydxcYptjEdF2rJwGBVZqSdPfJgXpmEW
AUxaIqUOAIbENVUgz1BpQJgCoarBVEAc0YEhaoQ5H1wofdB5dygpS3KNY9Uon7p1zHJnZdYUvdEb8neJatgS-Rq0U
giqJvIiLUAK0OEE4TW_TFI88IG37egFunjEncMX15XD7srFd_YdwOACeZBHZnkC8wKuufZuEGW8feaEcIlPWORVEY
ACtylZX7kucwK2_zgUxdgODy8Oql5w0uHct6Y_sCGPSfFfBuczO8rYGuM",
  "priv": "iTLE-qXqN8gkBsHca_rct0437-53kn3BwSBz2VOdDppbXeq5Ru50zy6vQLYUgkdSB8Q7A64dyz5
7967mHyN7cw"
}
```


Figure 49: HPKE-16 Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTE2Iiwia2lkIjoiSThKZldxMDdheTMwU1lfQ09IaWRRMlk2MlpUQT
hqelU1U0thTWFnOERXcyJ9",
  "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
  "encrypted_key": "9SCtl8C5imfrsH0XGTPLe7HyGO4aUlGdcFs4xK17YCiTQ0aC7q0dC_FLTdsKzUO5Ui
Hmc_wJw6DiMNwSuZeA5gn7yGTqidirlBHeDLNnePeq4nS5ER7lYAzP53cobsaWZZ3Cgy5j31xLleK-xypnt2OBAmx
IaGquEsfVYaH2fQNQp8EYLLPdRgQyY6DEnWwksr0PsvkgjHY8CquUGiQ_IcbOVF6mUa445Ax1Jp400fDKeyC77v22
RZyWQ0jqtWH7oIGhkc67IAXi1GhzKaBZG7_K-NeTU0J_r0yfFRuU1MDaTHFWOBFG06qHBpZcuO7o_gY3gthAl8ghm
KlvEDU9W0mymY4PgQxZGBqnUKGq2qpG3j7gtvHRqZ3sExHDVRi2X19XSQYV-0-q5Rt5Xo9i71bDa8R0T179iGEDJg
aStuJJOUbdR0Ww7loZpnhpwlyo-DQE0lx64m1VFpjLzwfpX3BU7iBluEBcxzdlNNPOKaIb82gjvYmv8Qd7GpDq_P4
nEtNJXP08NcMt9DL8LZFQTlH_MripmQ2phdZPWqsNDzqnucTSGwjAq0WNtHREYWZe7rrC4d4pkLvpA5MwKJD42m6U
xPRxIMae6Xw5kMNwQfhI0VyA3aE5WjtA27kQTb64RbGaPyrkTW-n_yMaTZe-qTjwUBsD9zMknO0hiVv8L-MkPBnKj
g2BKRJC2RQFfH3cP1DXywmuHJ3wHbRQxg1EVk_pWTn78H-iSQsO0BXwLtA-AlcNJwHImXwALd6fmkvB-omxtlPJ8z
j0YZD9Hnv4Ekz1Y97lwQ8OVBVycWoz3-kACbeJ2tQEwGkh3KbczltAvz9_O01znIidUNcKHNO9v0E7Ji2EWP7n2Zo
RvR04tb2Cz_dGqdSMawFNccKWDa4h4Pqzj4XsUiJTZPWuUTtP5jkMwSLqCpa8WueQy8fqhyLAWzMcJ0UUNRWS9Hkd
IJbJl0gIQAxjaLC4TWVXxooyxZn0a9JJqpZudrye71zcZ4cC3YlqsuTRwDRpvHKZSkKQCEZLvwWyBdUtSumtfAyiX
FrejFt09aekFgzwYU_B2P0mFwyvzuDambtuedlp9LvqsR9gYnJjff32eXfh_Uqjt6GXJnqEjTDmAm3xfXLilbPPDX
F6hTocTtbV1sadDAoBm8KsRUG_4XDTzum8AB7KbBeqqMPVHPIU5VMIvodw-wRWsA1GM8Ibs0zQkeNrsJnchQ8DcvL
nvREg5sJZ5HgYsGeHxcBPjio9UJsJ-RTTu6km_ZkgR7HBzO0Wnfs_rxFAMFsDuRlRoCZM2b-8XnVpQlj7PaH6dj8L
230BppDeByaQhKUicm1Cum1Lxh2K8KkgGXeiZc0TacAqgpJUyKFxc0x9EM53-jPiDbW0Fx-lb3OMUZKFBlefiOwec
-6bLTD-MngJmAuleupgZ6rnut6iKNildvX1W1qkmIpL2av4aoPsxucINkkoet9Ljh9qWKMdeuHy-0NS9CQQnqbX4a
RxlXL-k3KXiCLOe__ebyEICDtDrft8X4pQBJS3eiya31C7NJdNkkJdUvtxdibr4dkbvgrN7evniHw80QcUoRfK0J1
```

```
h81rPW8aRlwB00LdcroJWdL768JbY-X78kqO0nWsd1dBMHxyNUGHJSGgCl4tRp64fcg-Ke6P_SqSgbUHoxNXG5S4S
d6cRH4KXTa2rwWgz29hZm6QlN3cbfUgApnromN8s5bgMGIV3z0hpQWwvwuM5lKu0gzSRugTSCGeubXek4mBxSt3Ql
JwFYq7i0camhDDWsGCieFrfuoHN5LJUZPSIQfdanrJwYggfPoxxqLeoqsSibQwhT4Fesi-GEEQWwrgTZUJCCJIoxR
F1CVha_nfKFPyRLX5cyy6XwlIB63bN-StKD4Y3fMEozJuxJf77wGSShFyBVKnIF9nXV6N2qzsOOQnq9hLaWj4W2ZD
9DAea3qFEFDMjdaBSHSNgiDTobQiwOmJXKzbU11X7e0FgEGouXWhG2IJpfumciZgUvl5Q5YyD0p06UZPdt-ngD2ZF
RBDT5T44O9sqbtKAYF-APNu8ylDbFSSxvZuSVrNOwtfQFcH_3ZBxjr7o-IDxcP9XZDM",
     "ciphertext": "t0aZYvdQaiE5S_cps8Gy3putNe9CmV11-x8JhkwXs7b6FVBdWW9hJPvDUy7n-o3nQ57Gb
2f9_Pt9Ji_3LAecuTBzGb2TS-xdzvI1RzwxPPtMIULD1ZddshdYFmwX31CJcTrOdYgU47D9pt1uhaYQwn_ILG_gWZ
_XrPYwZFKQE-jDidOUfb9SHZMyk8jeEZ-wFMYIjA2B61iIqhHOCsh5aOYPb-H4M_87ETVQy3G4_FSFaY6UgdP76R1
wPwiZqJ1wraQ8dX-YRy3b-hF0PFbbySlCQN_xvCGrq22xYiFO-aaZlgdGNZF15O6oB5AseNHN2kUizZTYKhNGX6B1
p7fREjYBc1VwP0wHBfZTW4YdKFzQvXwOznEe6o2TY7cGc8u2aQ"
   }
```


Figure 50: HPKE-16 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE2Iiwia2lkIjoiSThKZldxMDdheTMwU1lfQ09IaWRRMlk2MlpUQThqelU1U0thTWFnOERXc
yJ9.vgIJFWxQP5T1it2PGqYOPIk2HUVbPiiaIavXkVv16G-HY8zDIFynWiyae9H1Z0dlKGGUus3JnI5jxL8nzctgx
Wt_YtpwOpuIDaudMocLEcuJJ7Y9oUV1DcXTPQH5z4k2VfD0SIrws2M8qiDiTaL2JoFAEDRPkH2pbA57pLDYLv6uoW
tfdohKJ3coq5_9zz5ZIuzMc2owIOBMuVr-xQSZubrFlGiZ__fbaG-5i3R-HuaNC6yFROPAcMZ7X_wnvA5hpjMct9Q
VSzcTl7gM_xXYs4BWlw0j-1wT7-kBAHUpWZ3ntfHxKmGqqd9ThZZddHKgeVl1E7OpCeF-ZEEGZS-x5_RS_6lS6p-1
Lb43dTc-YzZIVUvECTTBqlUB9MayY8vUhQjedus5BhQmS6xld7N3mlZ3t1ONxsETcj6rG6cDkKCZ-bGD4-ay0jYb_
SaTL3vVtnovxuoEWTR6KKcOSzXqHyaExcxYseKbAhKYOEVnj8IMmh7eIZ6p1oOd9LFI_CS3zo3kjS4NG2kVhF0Kfo
AaYcK4IXsWa67WNNGfRrV3mNFUMtUDXKSBs8qdo8kEjC397saxKFSCfw-I8uaKRhzb85xJNgDtpYbmCBlMKiOQATX
1qutAQw4utpEIHusyySvXhakjbmYUE1HNhMsd7cOJojKr_rFOYSWBCumbosOsPmMrNwJNSfsgvj4ucnkmBHKa3nBA
OY_SjwTOaJlKsMYvKq6JO8kuGBFxX9MuBrBEIpaeOxB_KUsJL24fx6vL4oISr2QA2RxL4r9nc1kqLTKneCq_aq6D1
Mg_mH2_qnRn7UZLLJjGYe4xgo3QPUiCyh4DQEyxG8zUrpLJ3fx7a-4p1rhNC9FKnJwc3RUwL7jaSJIdHtC9Tv3UHg
_S4dzPijiRBFqLzi2Wjt05zjs2ySa8egehsoS8-sYUjZKVWsi4wFFlkAnQcrkMoSNxhgGufZGmLbatQy6oN-sNTzL
r6jfJnD9tsAB4oBpTR1lNMadXth8dvYKk2z702I6BfzAEKl98DDo2f3fL3vv_WPOeswXQyY0KAzTlnIxsGxzDnBle
a6NRAFOMp6o9XpCA95rcvVjf9ODAO_S0q22mOeMaz7Vu9G7KRFui8YXUO-KjmM6128p7RQSf_fX4DggOvSF3FTsaI
cZ-8ggMDjpAT5aRyGOki5rIxAWH_YhVks6SIymUj0MUYh_GfWCS9SJsLDjMKfdHbabTM20HvTQr6JYHifzVzsnzMG
wN7NU5Mx8z9QTJ-8_RBFiOpDEj7X3EcsePiGI5YKCf6KuAmT2JzRiNq_-gXc4igMbv7PR9ezQ1foHOJTsJl0qBS-E
pHu1_Sv9FkBrqXiAVsDMSPZhFQjBN0WafejQ-UBAEMZx_C1dZmeVf76GWZCTBczhGGv6s5hpaKOh_IY_yI-72C3Wu
m7sG0ruXPa_NbSjUizeNUJ_kKhJCmObWaxdXlvWwu6epT070WaHYGCkem0PoV5mH3K9ManF1VWnsrcl2m87Sydlpi
R2Oh-ZA4W6jI7co-3GNsdGbVhtNA5mD_IP8eVgN2zdNKhdzkFb06Vsi8hBWOgAmIFw8KP5UY7DZH4iiWDaXvUnCQC
8yub2iuidbAOJQJodIMq1wKAgGGPhwaj2JA1dw7T4G2by2A5QcwBTvSee4ikgGFXhfsErgREpLg5ojpUwn15CQrz0
VFFua_VW4oqZf4RmcBVu4-xidWf0s08NdCPWnsHMeAbfgovM_4ro_xekFtuMs3eayKEffo2rLLwyCI0WjKk1NQiYc
PUtqX10JeQlRWVlRDnAWKaA2Q2fEN8OMj-XhSkgqwCsh7lUx-TT2doEt-ZJVJ4uja3d5wmRl8mGqCsjtscitqCA04
cxzHEMkLitDXl0xE_2p5n-zyE36GkoCHHxFNq8zDozy3PTpgCyZ2Bl2yuIpw1dYNNmY6Q5pC2ORCFQMonzvEMwRJ2
AGlZVl4fIgpE79xEw6Irb0VBNZyUGkxL0KwejiD9VTDXdqG4ILF7x3_ctfNis4IYfEcm3DCygzJ6kX8-sLdyOQk7-
JXdIOXV_dJnDdcM_Q-I3ouewvn4hd-mWCU44MDmTqPNvr6Tw.._PneAnhrXaXywIX1_ueYhGnmTtLkHnPOjD3Q2-C
xcx3XUtyAEiN4kZunwUVrppRqWq7xd3KkGmjXZCP6SP37fPlnPnHZhBUMdf2G0XnPcnyA3nCfSrjYWmg3klImuQPt
3uWIiFxwRp9gW6bp-VPbyuYbK8atf3aGm-PxgL71RMAiUkW3oLASPEAnzTnv1VLEgoWp6Ujld2EOChzwNZz1OnuCD
T6Eyr7toQ37xLE9Sy625du7V-xUMvIhXSqWVXlxkxMfc0UMc_Nhc2zZ2n6m3VCP-EMQV6bPBN8QKT5_u9lVW0fTaW
xXgAfqv2nbuXitBl8VwWgxrJJdh64kV6R2x9YQBj3VjV-5AUGEBWB44dGMXEfEBW_GwRdaMvysEQ-Vdg.
```


Figure 51: HPKE-16 JWE Compact Serialization

A.18. HPKE-16-KE

```
   {
     "kty": "AKP",
     "alg": "HPKE-16-KE",
     "kid": "fp7xFR02KVoSNoplFuqmztr0Y1SeZdEHrDKyP3-PpMg",
     "pub": "b9qWvEdkGIscWrHN18uSxDXG3wC1XJJJzEodohGvzUErjph_5DmT3Btf1xyixux4M8lImQeCO8V6
IXjELxajS0Zcnxew-SqL6RO_c6NJFVUjGNJgipofRpRmoTm0mAV93rF10AJ3dSfPeORGoSqAYiGujdkdSLqfHnlsu
2yAiFUbhZV2O8xHGSR1XIeIg6miIoOuJwzDF0UGbKsrAQS2JIdEYfF7LVVgsDB8teOOe5p0fMCLhihi3naM_UUKmy
uahiNspuWP9ehQ4EZfrqicGSYfuRLGuLiuipNaSwROZjMw8nUc3jJlKVUukfQeVWQKdJi7ZnXMDadysIFarrBJyhK
zqelv_tsVtICA9nIbjrGGoSlYSYadrLaUW6sU7AqdbxUQeqMiTpFY8_OAoWrKXPR-p9BkVptOBINeCfRZnZvEE8sB
RLIyt8cuOdAig2iWb5F3Y0cxxTdX4gFOzphtQZBRF6yWv3RhQsWwm-m2u4ojRJS2PrYhm4eyGUEH45h-8rMaq-mqq
hnFeYC9bAdn0Ul55Uc7wPUf7jA7L6RLuqLMA3ucRGvOKfEwQLi6pNNdfFDBRPs6XAxgebyfzAMWVLmgePSnALu2cT
B_pViu_CEI3nGKuYMoXayWF5bCtbo8cQvEjsK7mnqTUmctpdtJDMdldPWApCq-SwUl99eshnRr8Dx3zgEAR9jAAVw
tcRFeT6oFoMQqL_MwaECvcSyws6qogbBywFWw6GiqerAQAfBU28COb4u0eSpWBRayMduhziZbyhNF6WOwIohaJFAe
8rt1VIkBQgxeZNKxIwI54-FZn1A6fKVzgzGFR9V-fUpOO4lpUzoHv5kRhjUM_VimWceAb-lzsPHK49QXFTWCQ1ELG
rR5mAi21tFtC7EE4_Yh3tovTggj7AYPQBnObWqHv6k5ssCNqfuWObGATLuaE1tOx3ZP_MW0k5EPAEKiFLINZCoKDf
o8ulAZF2F88eNUSjUTWke627CG_hXCmEAu5uSaSmtHvpjG0RsDmPBojVFWSod90bJQObmgwPvAZ6cxTQRekyxPAsL
PwBetqqc3I8IDZUuTcMdmhtkIfXxZNFiXOPc-twB_NwAHiou4MDqZYatV_0QEqatNIwuoxemKf5QG4FCurEo_H8W0
O3cKe6gNgnpTcGgknmMDmnVq46cHvcGdxIjOh-eX1TQL1QS7XYd7xykxw0Mc_TVJoysn7CR04FKkDWwRFQVSzGGAp
SK1fEN3LaxC4cUBilkLSmWJEIjOE-eJFAA62WE911uSFmQeVIe88mx5C1ONdBrHOQLI6JsoNcFG0Hke1Sk3dvA3yT
EEYlOg0saF3URvpsJUc9gy21EEugOxAScsfbEVf3oqlZmAopGNBCQzn5KrEgKvZyVZj3ZM7CcSTeugWPcp0hI27NY
DHnUSUjdPLolJzOinIHykY0WoQ1Etx6pnBDfAo8FcBXEafIOZFxAg9hFopolShGGz1GBBzjin5BirX1Ielqd7R4FR
tAbBJgAhNsukEAYuWYhI9JUPVymSISm6MZcHuWp8JKU0Q2dS2FImjEeMm9VMIEdQtwlPZ3i3JdAgGQNfa0o1JWEzc
QNcerApY_c4SxnGQ9V6L_gJ6SmA9atK42WRREIURWFTA3xn9zVS0-gY72h-V2W0gGchCHBQLCBf3roWp0W-SDRRZ3
wCKdargnh9hNwQO7MNJvVYYEuQodzKF9d0I_MOKsjCEagi7VkOrGzFL-ypoeeMqRyWEksYTNKLCMfDCtet_JMkp4Z
YECme7aslDyh_V2uQaMUmK5u838Wj6fJHZCZR-ENOrsEKSxFNLpke5OosRwBA01ZZFrclaqmPVVw9fqc49wZQ-3Za
SNlKm5bL09slXlSZnFd_NnFzyRyekNq-CrZ40EJt-TCoqQJmEZKu95MlW0hM7JQUQDGOD1dvQAUrE9TCGSoy6hmaP
cvAgDOTVTY-hRoQt3lY64LIe2PCkGphKkSp4AJvMBa-lZSh-bkx6MPDI7ZqgbOeIBGtskackyhxs8O6ORNd48Noj2
SlzqcnMeNUdVVwSd1GgHF7XsoI9B75mib4ohphIg-NndvckxCNEUtZbgQ",
     "priv": "HtyU6HdQnRWu6bsyxJOsXsKf8VzkEpioQY-G3nOQF4cmGn30-0l8ig7fSTc2ZQqC-lI6Hib4uxX
HHwO8chLdFA"
   }
```


Figure 52: HPKE-16-KE Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTE2LUtFIiwia2lkIjoiZnA3eEZSMDJLVm9TTm9wbEZ1cW16dHIwWT
FTZVpkRUhyREt5UDMtUHBNZyIsImVuYyI6IkEyNTZHQ00iLCJlayI6Imp1bGNwNW5SdzREd21XRVFWYTc1c2hUY2l
Jek0yVHVzekhuUzBaRGNZcTVROVBpeVBodHQ3QkRzV0VzX3NNeHd3OUh4Ql9NSVdBX3IwWUN2emZZRU5KTTd4LUNz
dHZmVkpkQWRUajROQTh5dmNzOTJ6cXBRMmlYYjNBWmVqblVudW5reWRETW5PMHNKSnVXTjBoeDFkZU9xMHpCRDd1T
DRlbV9odDNFNFF3emJZdUFmTUhQRE83UVQwOE1Ud21XeFVQM19LbU9WYXNYcUdQNFZOUXZzWjJBblN3aEFpTEtsam
Y3bEdIWVhkUkVnTkM0QzVnalNvSUJSUUhlaVBFQnVJelM2UUlFQjdSUGJpd3lYazd2MlR1SUpRay0wRzdNSFNnQlQ
4SjlhYVZyd1NKc0RZQXQ5SG1ySjRqb0tYaDRqX1cyLXA4M1lyc0xDVEVkTDlEbjNnZXVvd2pTSVVpMnVremFwWTNZ
cEVGTjdsbFZGV2dGdl9PODVvZ211SF9MaTBiUFYwYXA0ODNmRVY5OHU3NlNnckFNYnpmdEVaMThmajhiM1FmRzNIT
kx5ZzFDb3lHZnVMd1dJcjlBdTVNNXJ2bkc1UFpyRFprRDAtU21pV05xdUo4OFFGeENMV2paampzNEFRZjdTODAzX0
E5Zlh6Smk2eFZWT1h5Nm5QS3VUNkUtbnNvUUlrNUk1LURzeXBJdGxkX2FOSTRGVUFxTGREQk5JME1aQ1ZId2lyMXp
hek03Q1hKZHEybE16cEdsdmtaWlY1elpWYTFSU1k3MldxdVJlSlkyaVNORTdrWDJvWTlPbllJOW9GMWdWX2pEQXN3
d21HYnh1RmZuelVub3BfSkwydXBZZWVwUTlqVHV1eDVNbjZXV0VGdTVFOGtKTk1pWGswN05ZV3QzbW9IdjBoRzFxM
kdVM0NOVFpKblJLS2RCbFlfUnhtcWp0ZW12OERBaGZ3UFBVVHNTM2RNak1MeHIxeEQ0NHMwV3h5emFnQTNmdFZPV2
xZb1NjWEtnNmcwa25vaThhQ3FsczdGN0xlMHYtdWpHMWJkYmg3TTU4NEJrRGZaajJSY205RTYzRmFia1NibVJYVDB
NTjF5WTdSeUZMZWU5S1c2Sm93VzJPdldzaTROSWJIT21ZWDBWRGhzT2tyVmQzQTlmeE1oSmd3UXg0SjYtNmItSEE4
UDA1Zlp0MUpNLWJsdFhRdnZoVzNISk1DQkswb1ZOU3N6YlJITzBFekwyUEpkYS1TU1h6dzBhYlduV1ZIcGw4bG5PS
jMyODhCd0hRSVF0Y0lBYkFfVHVobGNyam5lNW1tVlgxNHhHUk1RRllkRnNwVHNnMUVsSHpXRW12bDlNMTlJUmNtdm
Zib1BhTmNucVdmUTdpQnFJeEJ4ZFoybTNDZkNqZ3B0dEtVdkV4WkpmVnJpTE9mT3ZDQjdqRTR3NDduNWw2dHEyNU1
sMkZYdFo0a1lISG5oc2U1VXZYanBrcjlIWllDbmoyaGtrRkZ3SkVST3gwRnlJa2xuUW1yU2FmZ2hnVWpOVy02U0J5
UVp3aDVnaERfbHJqSkNJME1hYWlwOS0wWU1EQUI1VjRubktUM1plSmJzSFM2V3ZuU251QS1scTg1OFh2M3RBbTdIU
ldnZWt0d2xUYW5TTDBhWmt2N3ZjRmNsd1Q1RktQaUpYR0p6THliZlBDa043eldINGhQbmVlSVlCVDBHemdiYUNIUm
hRWkVpNG1haXlNRGZVeThvVUtCWnZNZ2NIMUFsanZ6elhSU1duNElRbmZEVWxXOVB4NUV3M21VMmVGUS1pTkFOZ2Z
rRVBPR1ZEUlRLandpTm1LSGJxS1lmTUw3a0dVaWpScW92dTJ6TWpTYlFoSFZmRnVMQnZ0dXlmSXFDU3dFMTFvamZV
VXk5UlEyMjRhdGo5LUpUUlJUS1RUYzZDS0dtcFVDb2o2YUg2NW5ra2ZFcndnUDVicTM2RVdza19CR0Y4MFJOd21mU
U9HZEREQ3kyZE5xMlVtc255VVExUzNwSXVUUmN5N1ZMNWdTaHVodXhrRnBvSG5LOFU5bHBSQ3M2NnE0bGxDT2VXUl
JGT0dzcWdlYV9Jck1nckRPZ0xqdmtnbDd6YjMyU3FIaDMyZGEzeHI5VnB0bm56VlJwZ3pES2NXYlMydXJ5Y0hySTE
2S2ZCQ2hnX0pDNWxuR2J6dHVZcXVEay1qcHFiRmtkcEhhdDROVXUwV0tvT3REZUVrSDA2dXR5dGxsZnFXTDVRTzZm
```

```
aUg0ckJVajZSQVc3RnF3RlNiUF90T3VVaEt4OTdFaGNGdU85dXlzUFF0VWJaYjR1TEM3U3RjeGJTQlhCcmxqUVhKa
HI3RkQ2YndQVVhsdlEzZHdqNk95c3FLaktBNmFxT2pNYzM1NXU3NUR0V09RWkFJb0NxaGJfeGE4SXZCdHFuQnpPb0
VBalh2R1dJQTZpT3dwcEZ2T1N4dkFMZVZOczhHelp2S2Yxb3l6VEZLN2ZzSVJtNTdJQTdNb2wwa1UyZ0NpVXAwM2g
1a0laRjBOeGxyVEl0eDJHRFFGQWVJS1MtTG8xNTF3ZEM0OXhyS28yb3h2N19PY1ZXeVcyRlVxa194M3d5Q2pSSjE5
X3VmajBjOE10RHNsTGQydFFLN0ZXeUR4a1ZfdlF4SUZIUnkzblRaTU9aR0NXZGJxVmlwNTJxbzZNbEdoUmNzY1paW
XJWSUJZZjF0WHpFSVB2T1o3WWowMnEzNjljTm5SWGgwcHVnVmdQZGxjX2tNamI5TXlULU5aOExXcm1rQ1dxNCJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "jGzcw7nTSxcmnbtf",
     "ciphertext": "3YHbZCBPMVQRvr39aLYdHQ4xb2EeuV_Ko-d2X5AmIjt9Bi8RhK_RYB63q_D0YCOTTuIfg
bKAWrdh5Fi3UwCpvVk3ZadNVjYEKmqWmu7WU_7hYX__hBHdxMi3BHc10grMgBo7T_BHBFz_RGRBmdtx4-X7uX_WFa
lLK1olr4tuxQUC5j8JAOQIsmHvNbNVQX1QzSii2TSpMB2KO6e9-wKMIcwgtsUUKWGC00BAnkAjpNtQP477uabz3gY
aSwtbMd8-AyvsR9-7yaz-uRODBXDr4_xlHZWDgjbeqwApRurEPvGgaKJIV96bWpNVWIU4WzvDEolRkgcdE4u26N32
8Wp9OnyGRVgoAY14W7uvfk5JaNCu",
     "tag": "mTh7DfqlSHP5sGt4ZnYOgQ",
     "encrypted_key": "TuOhaiJVyK3Pjic_XPNJivjJS42eCyo2pz4HVNUIb-SSPCYEffEAf0F8LEOhpWHP"
   }
```


Figure 53: HPKE-16-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE2LUtFIiwia2lkIjoiZnA3eEZSMDJLVm9TTm9wbEZ1cW16dHIwWTFTZVpkRUhyREt5UDMtU
HBNZyIsImVuYyI6IkEyNTZHQ00iLCJlayI6IllXbGxPbXV2N3dkYVpJbmJEQmV4ZTZwNUVkaFFwYWtGWUtxWENicE
9VeENyRnVuOG1tcW1WZ19JYldHMmpZTE9ET1lYQk5HdC1qNkx0NXMxbzRwTkUxbUJTUXFtNWJRcUxjc195ZGJWV1l
hWW1IWDFCUHlKcHBxLWZpSVFWRi1LSUpicnFMN1lyQXVLUFhkNjJBZno5U05RMTh4aE5BVUNmclNtU2thczJkT3dY
Q21qZF9HQkMxUHQ0Q3FRaHpFemlSNDNBRDNLZGEzMl8tM3paVWJMUHdGUG80b250TGNNSzZsXzdJZnlkT0VFZllQY
UtvTVFFZlRLN045a2hueGtHWHFDNll1Y21POUhJb1BaM0k4aFFmRkNhcnZrcnZlamdvdUNka2xWYVVncmd3U2lXek
wyZkpKQTg1cVVESGFOdFYtaEpWUXloTnZIN0hMMk5Ra3BSUDhNSVpLWlR2MUVrYXFFOFVqWm1icVFGNkhvV21JMjl
4bXFRX0VQRGU2VHI0U0VvY2xfVlcybVdGNmhGNjFwZXZCSGdIdW9YdVZIUm10ZzFHUXhETkVZMGRrNEctNXNiRFpo
ZHAyMWN3T0pZeDB2Ui1TNzNZNW1XS0NKM2RsNEpfX1JlSUdLSF8tYjhBNnBjRW5GXzdZQ21wV0xBUlhKSE80c212R
WFjVGt3VTdNVGw0U0dwWUhPNGZmVEk2RkNwcE41MW1NazQyM1RvZzRFeWROUjF5ZHlXd3Y3aER5bnUwNWFSU3lrZj
g1aF9ERXZQMi1GOHFnSzhtcHlJMFFWSDBBQzQtX1pZTGdOYVc2b1VsSUwzUERpRW9IMkV0cmtteWJfYzY0c3pnTW5
SQjVDTlZKcXBQdXRkNzRHSVpVMldfMDhzSDlpVFB6ZUIxaDJ6WFJpem1ORUdQNmp2U0lnRjhlaFFfbkdON1ZWSnZs
X2syN1BtR1VWd0RqWThqR1hPYU1JNGtmSFVuVWc0dUdBNEZCRnhTUGFFVDFKdG93RE11WEszeXZubE9UV1FxV3N0c
mU5WHp6bEs1WWt2T2pjUHNXa255WWtKM2dwanF1UnZxYmhZOUVJVHJ5TDJpRElsckVrX1kwYTNKRmRIaG9DcE4wSH
hNQTFRM00zS2dZUnZsNFl5b2FiRWJjVk9pRVR3b1R3RERQZzN3QXJOd0tnMFRYYjZCQzk2R2RpVlp5QnhTT0ZJNUh
iRU5xQ3RfLTZzWkNZdjNLS1VUenBrdzUxX1cxcDUxQm00bmllVjQ2NkpKaHNYbnAwZy1PbHZ5djBNRGVsSHQwVFpG
ZG9NSzROZ09MSGFCaWlyUWtnR0paVVZGbVg3R2V5SDJrQ3p2YUxGUWt5S1lhMjdEVDdtWWtuR28yNV9WYzVKdnczc
kRrM2dvR2JtQTRWMnZVZXZfT21UcFpCRXBYOFlyZkNWTGZaT1JGWWVJV1kzZk5reEFiaGVSUEQ4WDZQZmpkZExrR0
9DNV8zZDFqNlIyMV9Ja0x1bzk4TU9teUFWdWNTXzViUUNwNzZkWkxybjctU294cmtwWnFOOFJJSDVGdFVXRElJRDQ
wU0JMeEI1THUtdWhNMHZ6TjJOMXo3S2E2Qk9CNkhadk83ZXlpdWg4aVVkWUlRSlh1dm45OWJMVGNqbE5WdF9rakVv
OEt3bXZoNWl2Z29IVElualdiRXFpYmE2Z0ZibU9PQ1FWaDJvaUVEQ2p4aVQtQ3RCVUhHSThJTmloSlBlN29UWlU3N
m1TYjZGblBZeWtSQV8tRVB3aWhlc3pDQzBQeWRlVEUxZnBFYU55VHAxMXh4dmM5VTRoTC11Ukc2Nmt5RkN4RXpFbk
lsM0xPNlVXbm5lQlZvcjNoUkdMNmYtbUoxTnVybkRZMWpuQVpzUHgxWWdSS2VIQ1NTb1AwTS01UmoybExwLUoxb28
xdXVNR3BUQno2RnZJRTlwLV9KS3dyWXluYUNvVE5hT2YwUjdBWmpaV2NxMzJjZ2lNMGR2XzNTcHF4YzQxNWZxTzJD
aVFYNms1ekc3bXJzSkxOSkU0YzM0cE0wOFdLaERQcjNsMUw4dXRrUDVSNnE5RG94QlMwRW4zcnhTUnJ0Vzkzaks0V
WR6V0JZMzc4VklBVW1EVzM3aVlneldHUmk3SWdJT3lXWFNFQ0hDVVdsVGlfTDRzRzIzTEYxdVdEaG9aSG9rQjV1ak
NhVjd0bnB2d0JnWm9UT0NkMEFXY0xmcmlWbEVQQmJRYkJERE44aF9ldEVkYlc1VFFUU3RzUWowdUI0cU4tS1NHajV
rNnNyaURfZ2htOFVfSWtzTnV6Q3p5TUs2bHcwWE8wbjhxUEZmZE5pd3FlQ3NjREtJOFBnZ1EyOXFnbU1RMzJ1ZkxW
TGVFQ1YwcDNRUVZLSW41ckNDRV82NVZFSU90MTE4YjU1NUZXcUExNVBOdzU4NDRNbzFsWVp4YWZvSUJEWHU5aVV0R
zU0dEdWd2dGMjVGNFByX1BqUkZicWZxRXhkOFJHODd4QmZYdEJVbFE4WWRhRzY5RkRSbDlIZFczUmdrV1RVRjdyNV
NjTGNQS2tPTTE0bk5VdUZjQXAyZ09DTDdNSk9nVWZNSXA1T0RNOTR3THVfdmd2N2pyUnNMNWdsNDRDb1FGU1FmeTB
HbkVpdGJwMkdLc0RkMFRBRTFvQ2Z4SGtjRXgzd1pvRFI4aktMQV9mZWV3YjI3N3B1bTd0M3huZ2llSzU4MFUtWkcz
YVlYSXRuQlZFUUJWQmJEZ3llMi1IQ3M4MDJ5QlppUDJOUVhlRnFZbjVfUTFEa0VHQSJ9.xzRGj4HEx_bxAF7v4Gyw
oj4IoZytz25KNiSkQiNtzDCx1kL6V81cntf0JoPKU6ZA.l9JgcEwO0nPYNM-1.5ZPwol7KmPIJ1ZOR_KtuXm7pH-Q
io1K1fTR0AUrWSeMtCv2LWHZ1FDiq7MnbLC6pxp-JZ_2CNaHvLLCdSMaQi0td9Vg3GLYLwI6stuGzURSBAoIjS8gd
TOrB13aAoVJ9p7OVJ93xPP_Z_Y1VD8yrHrvOkF35cXv9MHWEGs_1b3ziHS2yqtKfOZ5uZnyNBynTpziIIXCIcWAU1
atU4akiDAqFCWEOyzaHAAq7GGSm8gWltegbbXy_LtRaNGbRsbqNY4mlnsYVqHoc84izoEh9Sehb5kmUuoqvCEkkHn
tuk4w6ubHLliNsa4cYFMMBZ-YbSYmqFjHe6Rf7e5E3owTKKC1SRsltykQsK0UmyQcZIu0l.c-OQ2YJ2VYxpFkEebk
IbiQ
```


Figure 54: HPKE-16-KE JWE Compact Serialization

A.19. HPKE-17


```
   {
     "kty": "AKP",
     "alg": "HPKE-17",
```

```
     "kid": "QWZdkjasH-qrIlYW1fIk0iqfSMJQBhY4-FbbeIMVErY",
     "pub": "LTEwJhh9rvh6Qal4SbKkTHws7-RJvpEc8hBzO4BYl2KgEHCEd1LC62EvAAIMhQnJSil24tEh0IMD
-JeyDiZ3ugUZ8dmM7Sc-zDc-StiEEiDBdLwNa3JUPjETBvkMcXk9rTjM-Xanl4QdY4oaHzPMv1c7g5eojHiXmWqj4
MS-N1Sus7dmVkIsS2TIMsxIpiZWMAOzSmULK1FB6IRplXEyrKBKCshj-yBz45Ku7cwkQXnIZ2NHnjdh7jJfNdqhKg
p8GcMej9s0y8MWCWt7phUIZKO3jZh1mvQ1GEqGRgBkQRINISxmlqA2UlyQZkE2w8dxCzzO7Sp3W4dvP5kpCPpDn4V
6GphogiPMwogzfESSAGKjWsEIn7I6ECm39cAlMch1ccFB5-XF1ajFnYGVdOeopeUsW6J1yPhkuycXUZlExadrfcyM
5Dg3xeKgmuy0w1yiuqXIRauaZ0oiSNoxQ7UfeRWY_aK4ujm2dDG1W5ce81qKZfyqD8HB4LqLUTebMQCCMkZyCgRRK
-Mc7FmaRqFx01SIYwg4cvevjzeU2FyvfCqVGHy2lbRzFjdGDet0s-NgAgcsdfI8CUV4XZixA3B-xFaTBHq8OKpaNu
FEsyu6fhQUfXxY7Peu4YxPsxKdQwqTJkVn0vYZGTABGyQ-uyWH3qKIqXkPLhMNBHs9DPESRDAcNcNbNgXK7HIFt7m
vVzIB-1BGhPRiJDKosalBmRVoVUEq7JQ6AsQRmnRbgHouI_WTIyR8cCaqJWdpjvEOZghynYYL37ohT1cZlnFaRop_
GppK-1k0gGqF7vJ_niKy8hhud5WA1LcjzXVE6vCWfunKv8IxjyUWzLsWBqaPmSaeEWUlWvcbJlZTjekMiDwtmqQdg
oI33vwslieT__EhbDeEBERTGfJqO2ZP7luPQDTOVegmTVnAWpwWUOGY8VVdbGqADye-Ubt5oaWse3tThpXPXKeOpD
NEvHzLy7KF0iIlNEQjYQrN_cQb0tKOMdWeVHqkmqsqNah9lfJXonQSqkerSgV2u0B639yew7gJ4-h2ZFg9WDcTO6K
x46GaA9Mr0MtuUawqqOLBiaW724qTKZiuJTUzkBZ7NKcgdbRy_SwEbbFvA6tbg7KNtaJIJUBZnLySnfSbB6R5lAdT
LSlBx_HKUAE6Tcim6_tUJEmGNOyHOfTMFqHCUOoop1Zl7dlbkGVGdLY2eckVqBO6a_k9Scqa3IAQkNBYRlgsBKSKj
WSkitF72FadR2wsnZIpbMqY-OWutZgKg7RrfTaMGioYrEuEcRRiCXEHhUBTpaQsWtISmnWF_sZkMkOkKTK_L9MUSm
Wqnxo5yLt5nWshAQWuVsU7QcIFP6oNnok5ObUL1AithOTFk1mBIKBgMelk58ptXydifTkgTfyeKFl7ffcpf7EpAbg
l7gMVPVKAH6iFZNgs5OyDSyUJ-IUjgQSVPxpNr9S82WOAonh8UlBVGtiNUKca3Zx9SbpvDppsTQVdPhox5CUcv0hj
F9mqr7qV6AUODCJpmGWJ4QpexiOOyZZ8MRetOSOdpVxviDotR7cTC4W8osYHvEbDo1V-axClLFaA8IBJK7N73tVcj
8yoPBCuTGo-6-bAxLgZpRpOhNqDiAeUKoy-8FuCLdd8C8B9Fct-u7A6GbgWw9RwpqFES2BnqQzA-AtYBuF9HChrdO
CHs6EmbwE0F0dGmQHGI4aVv4OPBJNjF3EO5LQ8UbQTj-Rt3fEhZ2MlMRVUxvQ_tDfNIwmtXPzIbhI4Q9QX0JVL46Y
N8pmV7Fw-ChdgEjxFywrB7JpzavacoLEHvtejHlFKLXnGtdLM7yrOBPHECBujbqdvIHfJNauyz2NVvoG7w7nEIZse
KrEdPbanEMsGr7QA3mcPDxlMyORSSpsvP4QgUGWuy-JwrISjjyMHuLJJrXTI42fG-6uIQSAugHWOJmMQaXpNPWZDa
7RtIThcigaWLhnO9NeX-iYEceKTGnlULLO8nLelaGeTnthdbcw6JhtpteLDMfZFEPs_-6p4NKY8BGi7k8ICggtrk9
ywo-qo2jPLSHFtkJdYuqHz5Gdm3331wMfI-spQk4JNFy1der3YZkwP8TU",
     "priv": "I1v-IPJPcDMw2xO4rcknLwMM89dk7Yto68XITmRf7YCQ5R99pM_cm0NLKf_zSzrd55rQEKk5KED
1Mv3NBtxkJw"
   }
```


Figure 55: HPKE-17 Private JWK


```
   {
     "protected": "eyJhbGciOiJIUEtFLTE3Iiwia2lkIjoiUVdaZGtqYXNILXFySWxZVzFmSWswaXFmU01KUU
JoWTQtRmJiZUlNVkVyWSJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "encrypted_key": "jySECvTTwfiXW2mYkfNqqe9IlvNYzSSeiZ5CgXV7Zt5pFDGjdiDFDQ09IeaUnDtfCM
x51sK58dwNv3cFCp9dBi-kdAynCutCnd90LS6aYBtvxqwdWMmsfTFQGheJDnrVYBqdE5K6zN2fxo8BYXeD-np61Kx
QPqhPyoOGEJ7Vt2QCAlFoIzPnBAW5bsUfUX1fmp30Kv61KWfS7Z9oIs48WnGqZbcxzVicwmV9rgFwOQHbEBgVyIMZ
dLKIpjxWDkd08x6lxn_ay2yXvEQ0Qc_jePb9aw6QQ4K8MrzK1IxphPrLvz_xYAi-UwZezAEViOLtNha8BeqvjUcpY
prXsHaIals2SrOvo_H9i2K817hrYTDkuEp0YHMCYDY-dKKvyBeyYbb9XXxCtARYUEqWU7kw0i-6oTesuV8zC4g4Eu
_S3xj39F4jrf0n7W7VWilVJWXp-4ibVyRA8mmwerbLte4wafceKh8KwS05m0oWRnQB4qlIXiHFOQfD3wOGK0qKEPi
BJC9qXyPpFXnabBjLWtBazvWJd2bapZljKYMMk3yiQhFH_DmS2dD8X_Nb9Qta_v2MA392GUUyFBF8P8_8-hUauzc8
HhiTv_vtqLg2nDiMP1icRHqM5NtrJSsmeVhHt-Y1V4BHAolEsu0RSiarFR6Lz_vBAmeJ4bpfJ_8k2c8Aj-yc2Yn9Z
TQuFNXl1tTRIjJjuDcBfdna4doMcJU5qqxpDy2SfByB0DoUiIV1o5LvdnnDpWHxxcn0a2G0B8vz3khwc28-bnzJpP
1oZx-EGYNMYEd99RPj6iJx92S3SjpTdx3Q3JLaMppXHE1PzOOTI_3nQqW9tdmxSLj1zDgwxh4IpsK0N695vODOixn
Ajlg5P7n76G2dDCRGn-ylvwodhhpvrUjs5EwTmkzdDXk4f21E86PCVTVEFz-Oi4ifVrYLLyRcBHm5b-TrOLunQooi
QN9w6OPifNKWm1NIiEJcRJWA5fCopFA7YNQVy-FqXIAMMBfGvVttqAyK_yEpHQlu5w8tsbcBTsgXsY2ve1Ah5aLpA
ylu5lliXbtGK_3b-hxjy-QiF-n3WfnJUdSyTv7icdngBFZ9HkWvzgmISfkPSyIAn2Jl9iGlA0ud8PALoBjRQcO7Q9
rc9ppOAhhzn7hxFmCFuACEu07Wrog-wbZNko_23uf8DymkT5LDaYmmvjTeN_0sPzjzf41iRBL1PdMaVQsBZAR3cXA
Q1hpuGiymt9BgRIr1gQeItRQ64Fhy6OnIk3WDYQiDjKWKNuc6gk36iVQ28upKg2ExMwSM3eSY1bjzhglZaMitRDWG
uXuwROyNW2WZORO6b0bZvDpWaCaQ4d3RFvpq5cdfUf8XiPGfn4RIIZcxkTrrQZIbX8iCGVlflzmXKYMmAFQiRkHll
85Axv0ZieXwj_SX9ZsT-TCqad59iqMR4j6pjME2WWSgaJk6WrMwKR7dQNq_t7Fl9MewHKdYnlPlQx18KbvCP0vNTJ
zRqhyEoERuUkInhgWF0HeTXXy9mkLZ9Yp7td6jLLOwEvKL9r1Bi4Y2ta4_VFOHoE5MpgAoA-z9twNPbh7F53glT1Q
R1vDFBubzF66vipUZW1qDrdqXpvvxNP9w2YdGzOUPUpTO4LxkEz1rxoeqmU-7rDUhmltuMYvxly6ppAIpTTXTbvfP
GxMB2AtHzqRBaBFCoTWMjGfaVVQt98w0vaFUfm1gyGPOcH4Dh2iMgS_98lGUDmmuFWP7m-fFEsjH79k4eWTvto71q
LBjZLemgB4A1lbOu6ut2jcSaVcNv8I1stNJCEX5zwGKrPDiE6LGRWvG2PT27OL8VpBk7n1vhp1TJPbM7OhDoP5lSE
LpGiiIXN6ox4n0lHPP88_SBupev-fmLEe1e5-o1X94nd4jRz1o_f4pjN0iIHOcF1MhOrYPlFfdOMBD7bPtVTU7M2Y
rXc1_Gq98CTsJpdmh9ELUvf-V71dZodiMmj9H8CrbRfH7pBDgsZ3J65hgvlTSJYKhpVnT8yh2qgqfyd25YIwo1xRT
DITK_Wd99jnkFrdepJoSsGfsMcl8HdJ0RLh3GxUsaHeIVb-a_7evRkOA6FTju0aCHU4",
     "ciphertext": "NpGyuCe7oy8GbDqnKCHFJ7iN8ABTE9BEILnTKt9jVVomuxSGq-VVuym7sso_bL_KPbLln
m6YcrfBr087oNAX47zvooXJHjt6Gafwpj8qcTHOxXv0iisMYqFL0CbnWmCp92KYu76J_4EUbpcnNhW-RxllZrycMm
bNM6Cjjirn3nbwDFE50hV_Xho4N7GBuUxl_cOL_PJYebtQz4cz6j4FeZkaeeZXkqQs3v1LCbETcfwKWsQEIpKd6sB
SKEimV-eeLmyqaSRFt8Kgh9y7FibUX_BvYXIK-z5FSnUpg8EL94QHuEvjt0WxhzObaN5W49pNQ71JKlkCeI0bXbeM
kroDWUw6X8t94IEkV9Ac9LHmOf2T3SL2YYed1BMgHMObvpWDzg"
   }
```

Figure 56: HPKE-17 Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE3Iiwia2lkIjoiUVdaZGtqYXNILXFySWxZVzFmSWswaXFmU01KUUJoWTQtRmJiZUlNVkVyW
SJ9.3iLs6N4egds_CZl-d-0Mt76d0ErYtpSV0Qu8HTPQLvmyoU1yyyF5M55bv2RzuFueVdLENXcHqwAsEVofAH-U8
LlujEKijzd9NObtDFlkUl5P97WyoyMMSQ0CXom-frHR0xve1hijlA1Vtdwgs9uQyzZvH1tUih3KmNpkM0QlcT8xQp
D3Ro5wLzNTDVwFkjf3Sv2aZpg0mj7DnHUBYqML1B4IlbjyVmGRbPMMH1ZL-uV5pLNvS2WBbQIIwD0-vRLSWak3Qda
m-dCRXuCqIEp6E4VlURlvvteQIMmxTSMS3BGuLwwFkIgtavEYR9JbO9Fhny-im4LPiuaAiqHK5upGzKZ9IeRg7Biq
zl4hgAIwGDQiZBJdAQ0-sEQYn0oH6D1hmMPExVgC3EDQlbvrtTjbZUD1ycWlUtYaigHn-zrY0_ovfTFBR3_1RFw4M
hvtII259t3MVCoirMhmCBnbQuiCutbU3DonOlb3SRP7p4h8s8JeKugeLrSPYG_ynikcClgESl_oYu26sC-um0j5vm
1Ltr5bY2wUE1RAZgEIy345bhaXabxlPo5s1KviPge1thsy7Os2cAcaeqyjPvSmyBpuNHpp4PtgOurA1DYKVKOIc6V
oOuLzUeVfnr5VEt8_0uAJbRHgIM7-lCvN5yzhGj2TMhFtxcgfmYzsk7C-jPbJ0JwOWEYAUcwesqLVg89kRkBWz30A
Ty8uQ8NPqz7MhR6Tkj6VPu2YPk6Y-RKtBvuuSNXeVOUfo-oelFlnOA2POoDnz_0Zr2OA06HYOzhMc7yaSt2zNh7ic
YIeZ6qG_97G9oOboc l06PTDDX8iEsLcIJPDInXP3UZWMpT_mzqvlpy6sC5rko87pX2e6FqAViTnxlbIaEM35Dxb2L
iKR2zmQTGw6bYlKtTurEJWku-H59n9aFM2EVp1jIH4AbsGHJdpi6LeK3P4RIQ3yhaNSzgdc7JSqKpnf8QAZYtIPJy
2xLfzZ3YVqUrcYdlQpj6Ez2SOsvaa_pqM5sMbwpx5YcgD3kAIpVAu3ZlDz4EoZdCW8WJuzhWmQPLRrRR-MMiIKjwq
JtY-s43YGrPgru6MmOb1aSE2OiJh5RyF9PIEagMsWhfMMtGbfMaTLCPMu_EITMbdwW1qcP3Wi0bimOQb2gbbUWYxd
KKNeYhPZgBOxW1ng-adQ9KbxsQuXcH-mObn74D_CI5QO1icAFcM6W-nJJZ1lq9ldD9VrO78AVrDR3oysIattMiSR-
ywp4swJQ2pSSOr6EclxksVycr5tmAjH0gct_zCb97pebZzi2dD8Sd5t6gkUi_qEi_FnQPwqj7kcaC2VyI4oIWsgGO
_oI-iqyAHlA-ERXUB3vcrR1IhJ70Vv3Bz6OuNyDFWkH3FGr9WuIzr-_l4FPq1KZXZsUAeX6mKvVaKNraeGgkYlWv4
e-I7Q3Fuuj6M2iX9KORpJVjC9FOnMuVRZkWVLacBoS-Z-t1MsHNYURWWYPj-4ZvrdJKnIJSG3LlV-taCcw4IKNHeM
hU-PkpVcFhNUEOML_eRwm_UVsAelxtNM0zN4qyLSShvSrEWAaWc8c2jzzcGrIjlzJTQt7WxBYOZQrO8sqLpGlK_ie
affcm0FEQX4HmJs1896ndrCNkjbvNWSCqbLuXxeiHdwk6KKvxNnNKFaxAHqTrym4UROngVB06_oqIRPdhcQRYKcMv
X0hedM7s_AU3C6SwoZjJLUL_5cnBnEOyJV1Mf5JKAbnof_Uz4e1kjUkBZd2slc2c7enxl-0kp5SQWoFHpuTMd6VM1
LX7lEubps2XwRZMh7U4RppNcnGVsfHkQ_GoEaVrPeuH8XyMHxh_qzGOvbstt6gLh2iRYeb91PoxpOw_BIBTp-_n36
uGLSjUELyOwXkp2gmvcf6hkwImunHL1VZrH4CORWD1Av6_1jWxpP_glHtoJ3CuAkxCg-D2lBze2FAJefsbIi_oWAt
3EXA_Vxm4CKYzvtZDcgQklQI2knSI5qq-W3I0mgsROEDJ1bo5VLyUVURDL1TljScmuE4HDf7n4wpGGPMEPdtTuQwh
D0jghfUsKkCYoxHWlhnzvhGWS7CIW7FJOZaAt2leXfVWAtFY..xT0jK9-UAy7iiTnBKyPGUrWVvJCO1d6OhvZpy7A
nTnEnQmPsv7k7LgNPMvfbbKT4Q1n7cVgTpXcQhclLtYd3_S0PpSbgeAAJA99ty1UIBYd1SSNMX3fWRboS2UXziAm6
clXDPWPVuf5DaqsnzSsC1WFLoLXSgl8NMo6rnST9eu0b-cSOp766f5e2sry7P37TeD6on7f3Z84SVBsJp4Zv76pf1
KKAK-43cebvBklP0v6AawtsBdEg3GYKN8weoiWh_lK3nhyhAbfNb3GTVTIlBdpDi3Kjb0r8j0hLOQEIIH3AYPdSiq
yOVqLELTV2Cj4r8AKLRpCcstg5s54WSUTDgyW1DT1cI2XiEEXn3lfUmozXWK2QrWwODaGsLTGOq23K8g.
```

Figure 57: HPKE-17 JWE Compact Serialization

A.20. HPKE-17-KE


```
{
  "kty": "AKP",
  "alg": "HPKE-17-KE",
  "kid": "ScO5bGaDpICDY2GH0-AgPOdiiBZ64b3GMYgK_DCipW8",
  "pub": "w0BJS-I7K6edZlsmZ6QLO5uejlBh3qa0GjVQnhygRiaJ9PJR8jECQYlMCKK72jVVzIK0fQevfnKZ
kkFp7kiPoLbMmmBjouGPEmjDgfMJTOCeKpyewrlX_Ahc0KaYwvM1E5pscjYRrQwoq8YO0HlzCdWpUTCwaehoX1kXm
-gVSmhBReN6OPfL0vWE7NKxifEmVGLPW-aoyBTB1sUzVARZCTesM4cNrRNfA4aY7Ce1DzQ5qpZBrHVsf6ODu4kC7d
dbVaOvueqBwbAg5BZ-oWRSauqHczrG_JWb2YJ00EoTrsRZ0GMr4LczqFk0XPTOJSweoAFeniRmBitmzGyRjwDO1za
vG_ibZua4BHvMPygVqTQR83xY3vFbhKpMOMyec1QyyNJsnqpmowVSi0A0P0tGcPx3PHUfQ4c_LpjJiIeXPTQqWNlt
2OfLqAMG9-GiJ8WmdwXOYfglpDS5oRLJ_GmB3shHxpOzrno7_eq3dsKpKrB0oZdoLNlVRWBiSBdal6FaCWKD98R9m
6koxFw9jVFOF5IcYSm3sPC4aXpcxClfWRZIttYT2UReLKemckNij9zGFfEM68u7C5fM8HYvKQTOP5MrFEdMxteIYV
Ot9JJmaYCNXApMOHG3SLYq7cWVRJdIgDaxL_W9_BNW9ZyYfnh6PxzAW_ZimxYgj3p7_twlJGNG8PM0zKRtJ9G2Igm
1Y6qHXlxTM0dMFWo1VETEdmmgJxIMstG17vw_gjtmKnw69KHGZ0IjrpAeUNgQekVjotQXCqinbMjLaqAHCiButOUI
S5IXG9JvdwIeuFeRnjlwj9mdY0KQp4AByAGBl1Mc2nof57KhZIRUrMEMpQpMuSCkfsRfv2JFIJQ6bqyneUVcjYRKO
FcCiOBCPrF8wcd6zDvHbDd9JUU3wZIvjlp_4oFy7ptaRGkLotqXqyoC86FvgXJs-gBLUgpam_bDgoeaDMYxERG6jE
ZPF5WnyagKdtzIBFlJURknJtvK86U1Cqi3qQM37zOoOYhe3AQpDAsb3QVNxOlGavt3J2kwi0lbp1YQa3gO1MJi_KE
YQgkWTDWT_YdoC3w8IvsbFDCpsShfp-VIFXYV_AuOv0NY2DmPg6OQpvwQ8McFrek_XfWGBvEPcnzLAkdaXSaZgNcY
9YNC7zIwkBSEI2EeE-MTCBQDVSCm5mYBYBQgoTWsOSmG3Ow4dRqANzKbhbKLHVZIeIUdYfRVY8wVU5EHLIEue4RIJ
JJH4Zh88AyvdBhP5nqUvUObQBhzTrMWeqVlccUVuVsghNZl5rUJpudtFlRgLUYC-jGAW6ozgUuTCjqSbJR1WjF1zz
dbspaT0rotuOddEhguXfmMPCsTosidjhiwN3ZkTrx5cSCIj8Y-9QrD_SFtULcHf7s7U2NwSuHH5EMaoRiXv7UpgbZ
D8Xt49aZtdXuCpWxIfYI8pyAG57eogQMhg1wj9cVc67pvvbVn4kFv0hCSEiZRbek5ZYadXcJUOgSZFdAAlAxSq2wg
rZlG0_QaU-A2_By3HRA9bVvEsjxz-RaSNZFjubynj3sql-ZxKNkW0IqF-Vs-7uZIzNgOK8aV1ZwCWzCHdkIzMykoV
CW-CRPLm7TGZitlQgtVu5Fs6gs5UnSem_lcnGA52QpwK3s7X8bMFTBJ7cUDznh7_Cky41DA3qDPp1BW4hSKZ7hK_v
gNeVURwvBP7GdweHs5K6TOJAyje5pU9ATEF_q_caVUZ4l_OhZg9Ed8otB-FEJC85W7Oqy4o9cFJaOBuqUZmZXGt9N
qQCEZQJVI2ToNpUVKHVZqaGKKU4zOLGbK6FxU74zPQQYpfElevAdPrWYJk_wKxgpuVJggqKm_w5IOyhwavbUJVWJS
9tiw3va-Z_bLPAW0_tm3afYw1JvBDxeLlNnIOGxPJChVQmMg2VBdIPc2fYhwvmGwmlN4q9Ca8zcZ2qtWHwVYgJQ3A
7gGH1g48lk0UklMvxllt7kTwue7CmscRkgGcEHHo5wTyaacsEc8LumQn5J1BiUpptKtRmWAGuGrFcq407Ro27s5PU
SJCum-LBEQbIKASXubtSvP6wrgowcNp3nga7FFJ6mCZDU6hlZEmyLLSHk",
  "priv": "wuj6hhHH-LFGeeNM1F5RBG35DVA6WD7wBwMw9KwvPRtaS0XEDDIPp4gP9cpp9BjaqlwLvEKhZR2
sXlJYD95fBg"
}
```


Figure 58: HPKE-17-KE Private JWK


```
{
  "protected": "eyJhbGciOiJIUEtFLTE3LUtFIiwia2lkIjoiU2NPNWJHYURwSUNEWTJHSDAtQWdQT2RpaU
JaNjRiM0dNWWdLX0RDaXBXOCIsImVuYyI6IkEyNTZHQ00iLCJlayI6ImYwS0VsUmQzNk9VeUQ2NmUwdDktN2h0ZVB
pZzVKZ2FzbzFjTG1WVUlNWnp5eW9qQnF6NWZqV2NoT2VXYkZPQ0JqVGxZYWxkYWE4bXd4bk82VHVUWnlxb3EzT2dy
UGRUUW9zVllIVXRrWHUxNkZTTzdpOTFrVndDWDJvdkljOEtOQmlTbFBqalFFTFY4OGR6ODdONEFieHRtSjJ6SzlPZ
Uh0NHZLZ0RtZkJkcjFqMFJXSnNXZ2xNUVkySVRGZTgzTGZSTDROczNoX1pkdGhzVF96MVg2SVJ0bExjcEZhUjlJTT
RBcVRnN1R2NmJ2SzRHOGNCaHZKRldzaFAxVW02VmttTFh1NUdCcXlzUGRKNkVwa296Y1hPZERKaFBVSEhpSUxWTkl
HYmUzTEdJRzE5SVFFRy1lOUZuWW8wRURLQW1oQnBlTEJCLVZmY2RjZV92QlBoX3J3S0VnOTBha21UVEc3SGo4Ykp1
STBvRlZ0YUlpOFI4X2FnNmlpYklGQUFvY1ROc3pVVFVaN2ZMNnIzQ1NUWTBzeDFsQ1VGZEN4dFBjY2tueGt1WFVkV
Esxa25Tb01nbVVadHN1Q2h3d0ZWcFlxTmpEUnpNaXdyMlBrZVhRNmMzeDRYSTZXZEtNN2I5VS1wU0txenowdEZXOU
tvNVBFTUNrd0xwZG4zbDA2WnhDWEpyNmk2bThKRGg5ZUNWQldOdWFialY5SF9hNzVDSTVmN1FZVEZvYXhJbllZTEN
sUDNCTXNEMzlBeXM4LXcyM2VPZURyeDBEQ2M0QUVtRVY2a2NrS2FhVUNndENfTXFLQ2ZXQ0tISE9MYmtnOUh4d0tl
V0pmbVJFZjFLdzF3V1d4TFpnQ3NlQlpEa2JvSXBic3Atd1FrdHhwQUZaei1YTlo0UjdGNGtaMHIxbXBRUUVRODRIa
XNER2tubU8xTTh1eWh3MDFQblJQcmo3U2l3QzB6ZjZ6SVpmZnRoZFRfTjFmQUlhU2lYdVBfaVJMTXcwZFZNZVQ4eF
BFN2RObWE4emxRS3F1MHpGd1VkaV9BMk9PVEZWUXo3YWMwZ3JZVXB2Wmx5NnNIeHVSVnFsQ0xzUVQ3YlRHUWVDNVh
EdExVVWdBeGlsZzYxWjJsa2JqSUYxeWFMQzRtektCWUhJM09jYXp5cGpxNDFyOWhJUEVMdm54TGJpUVlxWXVYeU5m
U09DcHo1Yk82NExTa2FqV0ptdkZDdzNkRVJuNUhfY3FmMWdVbVhHMGExYXB3ejRhd3ZCU3dqTWE5RVRoR0c3X1hjT
W5CTDNtNVR2Q2ZZd0VzQVdDWU53X2I0UHFEQldLRmgwUktyMHZQSTlqeXBLbHp4X1hlRmVZazlFUWhacUtWSXdrWV
FkZXh1UE5HeWwtc3hXTXhaTEZXZ29vV1NWOFpsbW5GblhWN3F0d0RaOVFMVFYxdlFtalItQUFlV1hseEVSVkN3dE9
PTk9udUdLSU5xN3FPa1ZzWXgzQklOMko4MjVjQV8yRlpTemtwaDd0eEYyX1JBOGdnM0FOM1M4Z1R2UGF0MDgycXJ4
VEtVNDVaSGlHenUyclp4X3I1YmllckNDNEUwMllaNXBxdW55Ym10LTd3N3BmNUVIUlEtYnpMSzJaT2dLcXVueUVkW
C0wYTB2VXo0V2pLSzhVc1FSYVd1QUVVOW5NenpURXhibTE3OHF4OVNtY1otT3F3NW5FdE1RVGZhNzUzZXN1cHBWV2
VTSzgwOGtNc3dTMUo5Qmx6WlN1cmoweTk5MHI4Zm05VGk1M0hjVENmajdYZFlrZE5BSGU3dTlpNjFoeGVDdXhuTjZ
vNHFsQ3ZRVXhPcmJNVnFVWTRPLV9ha1NDY3VRRlF2RnZ4TE1ITnRYSXRJcGp2YWpuZXRGZ2xzZjBUWE5DTFVlWGlB
```

```
SWJYMEt5YThPbFFiaTl3dWZtZ3Bpdk5LLUppdWkxT0VqNXhJWDQ4akRhYjNONmtTUDNSRmhhd3BpZk5oanJKRFR4O
C1FYl9CRFZhT2RfNTNObGh3MTZnQlVVZVM2V1BfOWJiNGJXNUUwY1VQSHIwaDNndzAtbzRrdG9oMVJaNEZ1ZDBFMW
1VdGFhMlV4ZTNFbEVTa05PeVRyalJBcTBEdDhfeTZ1UXEwVmJmR19yMkV1LS1HZXVnSHE5WWtPVUY3dGlYUFUxUGt
rTzdFZHU1NGRuMVpZZ05fWWNmYVhtb2duNTNLNktfdnVaaUdHMDYycFVaWUlheWRKeTdJZlRyNE1pMFAweFd2aWdU
WHBPWE0tby1PUXdSLXFxa0x3UnZ2UTRIR1BycXdiRzFGTjNNQVFtMXMyZVc0eGRlRDIyc2FsOGJxZWJhcDdBSVk5T
kVXQU16M1liS0J0V1oxSUFfcUxYTEhCTmg2YkFwQ29iR0ZLWDFmWlNJbXUxS21rOFdKdlZLdnZxS19KdWpSTTgySk
NES25RMWR2M2ZuTGY5cTMxYkRSWUFpRGhYay11UWR4OGg2bFBkN2JyVzdLWS1TMFlZem9nSzgzSjhpdjVmbmNoVXV
Xd1ZoZ2o0V3k0N2J4aGlqX1VDTFo1czBfaU5SQ2ZqckExak91ZXZpVlg1eHhnal8wQzNEZWV1Nk1IdUdUTUFUVXdl
cXQ1SlZFT3E4VTlmZlpkSUtkSFJCQWtQcW01V2RQY2dpM2JGcS1adW00OGNOelFPekgydklla29aRFVjSURuc0lCb
jB6a0xhWGR2X1loTUY1V1BiQ1FUTEpUdEhTUkhRSmlLc0l2aXF0clRva2d1SElvanJGbVdhcTdZSG9GYnlQYyJ9",
     "aad": "VGhlIEZlbGxvd3NoaXAgb2YgdGhlIFJpbmc",
     "iv": "ie1uRIh1QAjzBCMP",
     "ciphertext": "BQyNsRtSyKye3PchLTA-F57QxBKPz0ybfT4OjErHPVgw_YhXq8E1cf0Ic5X4U0AYRDiPk
M-oiPI9cH5de3yMyp7HpE63vJFon0NcmQIW_PfaKYwHLC-lMCfWak0G7KknHrgJVdxJEcM32xNY1Jdt169ALYhXuX
0zsoQXXLGjMAkqx2KYg3i3V8LR-bOkvtDNvmD76ERksJyxlRQ9WlWV3YIwdNI51Ukb7W3OkB-Ru8SgmNgFxl6v3qh
VHcxSaCom8d7mvUzL39ZFAEJ4Ptym-RBTeFnN-JSC-h7daY8YgvXJ8KN43qz5xjmNlS3N7_lYihQcFYoctLx3i2uK
ol5DtsAXBuzXnP0FwfNc3D6pf_mH",
     "tag": "MoT1JqpZDCUTTO_E5gvVGA",
     "encrypted_key": "T7l2Fu6qI82x4z2D-C8Yr3X9tnenDn3Dn-fECMFHyyepjgST8-V6g90R4J5UXPOV"
   }
```


Figure 59: HPKE-17-KE Flattened JWE JSON Serialization


```
eyJhbGciOiJIUEtFLTE3LUtFIiwia2lkIjoiU2NPNWJHYURwSUNEWTJHSDAtQWdQT2RpaUJaNjRiM0dNWWdLX0RDa
XBXOCIsImVuYyI6IkEyNTZHQ00iLCJlayI6IjViS1Y2SGhqWFdvSGp2UlkwNDdUVkJkOXZmMzV0Y2dKd0hGZUlGUE
ZWc2VackJYUjA1bDB5SkpzY0dqcVFWRmlUZmJzN1p2RjFtdjdXWHRUX1RLdmh1SHVnbzE0MWdJZzY4OW5scmtSRzN
SUEVSU0NJb3dLdTVYcUM4YncwbElPUnB2aFByd2JiZE5iUHBHZzVySFdtZUZLa1d1WGxrR0pkUGEyazFVOU96a21E
eEhmYU9ZZjVjTjdpM0VwSk9jMlRIQ212OVBQaXY3TG1Sdi1PMmE4RU9CaDlLaGNnbVRlQnlrbG4xSGY1ZDI0THphY
0xRby1GWnBnX25ma0xZcklwSi15blFGRVZQZHNBcWxfNU1YWjlBM2pCdGlHaDZFLTlzWXo1WVZMTVpFaENzUjU2WU
g3cXd4XzdCYjlYc3VISTZVVV9xZnduMlBVcURER1NjY2VTWktySVNnRGJMTUJvWE9kQm9ZSTdqQUpFVWJieHA3dUx
nVHBYUnZ2X0U5eFpUeWVkYjJhZllIY0RkVGI1b2lxRWVlU3k0NlZLbmlNRDVOaHYxNkg5MTFqQnRBNDNhX0gzUnA5
Z1RJLVhGcDZQUmdxN2VpY2F4VWVJa1pyTlVwWFRoM2JsQjFpeXdDNkZhdUxvRnFFTkk1VVpraGxIZXR4b3I5UXlyU
npEenF0UllVV1VFTDlJbm9EWFgtOE9qRjBWakU3Tm9xUGNCam00N3Y2UzZ4RWdkVUlwdXdGZHB6ZW44eWUwZ1lGNl
NaalRiY2xBTEthVTJaUUdYa2ZsTWNrTkJVZGxGMXRMTmFzTGJXQ0dwMkIybHBnempTbUg4UWtfTkd0WXp0ZFZWVWg
3YzgteWxnN2dlRnhXWXQwYWtNdEx3RU85bFRXVUdoV004b1g2eFRORfhvQ19oRGgwVFM1QU1KZzVsZlV0ZU1sbWFq
Z3VpS0owZU9FUE9ManJBa3hiclE3TkRrdnRjalFGZHdMREJoNGcweG9TUmNtbzZmNGYtS1pCUzBoYUZ6QmtrT2pzN
Gg4S255NEE4M1RHZlBxQVZGeDNwb0JESkx3SXlCVWd4cG9adERISXVKSERTSEoyR0hIRlVoaWxJX3RvTUZQd2hkVF
hnVmphd2FDV0JqUXNQTk81MjZMeDB6YUZWN3pnM3U5Qjl0eC10RDZZVWZ1NXU3aG92QVRPay1HVHZ0cjdrMUhhV2F
NdlhIdlZlakJUcENUQ3hBZmZBdTA4blNmVHBWWTBQV3h3Q0FlaUlIWjNxTVFBZDMwNk5fYzIzSEIzSVNkelFYX1ox
QjJBb0E3a3lENlVlZGdndXIxOTB6TmpOYjhWam5ld3ducWNMeVdYTXhianZZRVNiRXhSVG83RDZyU0VqeHpkcmlYR
UU4NXRQNDBGYVg5N2xWT1JPeXhVZGU4a0s4dHEwdC03WG9nTXZCbDYwbVQ2M2o4blU4Rk5WU2ZOczFUOU1NTTlSTk
VFR2JQY1ZxeFdiZkt2RWtzb3Q4MzQ2UXlXX0tJuM2FlQ1dpOUhYRmRjekpQQmI3Qk5MT21OMDc3Ui02WWZMdk9rcXJ
BWlhGXzIxZERxTGlxeDRBRlllONHNHTTFUNmVFVTJQWkN1S3ZzOUtjdzdIbEJFV3NwejdDTG82S2c5cEVzN1o2VDAw
akQteXZWbkpkQWEtUlIwcUFmYUNUYjgyWWdEendHNEZmWkVQZ1pPcmFsci1Ha3dBMEYzdjFGUWliUlk4dDZKSHBOM
TJZZEFPRlVCbEF3clpaeXdGLXdtUjFrWUwteVBCOURhcUNVbDRGYXVOcGFualNIOUxTN0hMTTFnVVpEYU5RQVQ0bH
J4SWpjSUFOc0ptbXJKaU5SRG9LYmd2NHVmcFNmQVNvdjVPWHNGZFNQZGRZZlZiMkhWZlluVE1aaFh4OWgzRmJlYVZ
HaFJQb0I1bTV1ZHlkdmJNRS0wSVRrc3pBUTY4LVNnaTdQOFJOdzl2WDlTbGZEa0NpZjJ2c25XRHdQbndyZzBPbHRp
eU1PeU1mWjV0T0tocV9zNk1oVHBpalpXcDJkamdiVk9oejRZbk1Dby03NXkxTDNlTWtNelVqRGttMTJoWERqU0ZKS
3dOMG10akdDLTNaT0NQY25BcElyTnRDRGhiTDBOMWxHYjhqbDB3Vnl3YnJwZGpsTjhQbzB0djMyblA2ZTdISUlCXz
JpQmpmQ21TVzRkTWtfYklpYmhkb0VRYkhoY3RjLWxzZEJPTENMUlVnZlVuY0s4VjlzT0pCV3Q4dEZlZUkzeGpwTkZ
qYjNmUUt0Wk5ULW43M3VESjJWd09OcVB4WTRReWRXbXZTUHZNWXZ6dlZldFJfYldXOWF5R0g1c3pOOXpsN2R2bzl3
VHlVVkRqQmpCWFZxSnJ4ZDZ2OE9iWlBQeUkyR2FMelV1ckhSVGxnXzk1ZW5MMUk5aWhYMEZBelVETnpwR1NRdGg4M
zVYS29WOFhNNnI1NDlnNDA5cHF4bnN4dm1iQUpxdjRQY3NFcTlJdGlMd0UtRTdpWHhPOFNDV0dwY09HZDFfVnAyeV
ZiVDJBMjJKU2gzb09RS1ExYlZXcWdFTmJhalVuUzNiU2FNcXpJanB2N3EyUDNZU093SU1DWWhXbXBRY2pDUllOMTR
sNVk2TU83ZzdlSWxpR0EzdlZkSTlhaFJwYzJyT3ZGQ3hvMlFDdF9mQVdJVTd0RWVrdnhlcjBocG5kanBfbGcxRlNY
Z2JpNDk5VDBFVXBNZjl1X1RjRjVPZWhBdmNwaWV6cnVSMXZBQ0tQY05sc1ZJNHQxOCJ9.cqktZbmzNM6suR35Fo58
t8TX1Va2coa3nBew_9zPYCN4U7U3OBJSVBp9xzkHyWjb.vLZG2Bhl70LQ3Czq.HKHHAMX9ZCDFDWlAFDAS6v1F8kG
a87Z_fOMEom-i7RsJ78egA4v7KRjRW6khjBQe6shQyaBwsfUi8q1gmf7KAkVBL3KmqspIkr6hB5rXyXhqRx4qnDdA
BMGguqjT7f0d-vdI8L7sbqyMZIS8bq-NFQcPVX1ZCl0-8Mf6-W3KIYFro14-baQ5Xm_voWGvqnv4-GPbpQOBuhWiV
obwbeIZnSKZyv389WCuDP9FvsmH26_rdPjHPw_rKe1gFUp_DnGsvgbwPYLE-rMCQC6X6TYBxG2uYJxizx2ZRVBQFF
ObQE9hF7CFZqEQYXYXtNvDIKeLX6l9yjxLl7ex51i7LmeK_BElee7HyAjN6GIXYCErQTXn.b2q_tDZNhXze_1JIv9
ZQew
```


Figure 60: HPKE-17-KE JWE Compact Serialization

Acknowledgments

TODO acknowledge.

Document History

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