COSE
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

H. Tschofenig
H-BRS
O. Steele, Ed.
Tradeverifyd
D. Ajitomi
bibital
L. Lundblade
Security Theory LLC
M. Jones
Self-Issued Consulting
2 March 2026

Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)
draft-ietf-cose-hpke-23

Abstract

This specification defines hybrid public-key encryption (HPKE) for use with CBOR Object Signing and Encryption (COSE). HPKE offers a variant of public-key encryption of arbitrary-sized plaintexts for a recipient public key.

HPKE is a general encryption framework utilizing an asymmetric key encapsulation mechanism (KEM), a key derivation function (KDF), and an Authenticated Encryption with Associated Data (AEAD) algorithm.

This document defines the use of HPKE with COSE. Authentication for HPKE in COSE is provided by COSE-native security mechanisms or by the pre-shared key authenticated variant of HPKE.

Discussion Venues

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

Discussion of this document takes place on the CBOR Object Signing and Encryption Working Group mailing list (cose@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/cose/.

Source for this draft and an issue tracker can be found at https://github.com/cose-wg/draft-ietf-cose-hpke.

Status of This Memo

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

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

Hybrid public-key encryption (HPKE) [I-D.ietf-hpke-hpke] is a scheme that provides public key encryption of arbitrary-sized plaintexts given a recipient's public key.

This document defines the use of HPKE with COSE ([RFC9052], [RFC9053]) with the single-shot APIs defined in Section 6 of [I-D.ietf-hpke-hpke]. Multiple invocations of Open() / Seal() on the same context, as discussed in Section 9.7.1 of [I-D.ietf-hpke-hpke] are not supported.

Algorithm identifiers follow a ciphersuite scheme in which a single COSE algorithm ID maps to the three algorithm IDs required for HPKE: the Key Encapsulation Mechanism (KEM), the Key Derivation Function (KDF), and the Authenticated Encryption with Associated Data (AEAD) algorithm.

2. Conventions and Terminology

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

This specification uses the following abbreviations and terms:

* Content-encryption key (CEK), as described in Section 2 of [RFC9052].

* Hybrid Public Key Encryption (HPKE) as defined in [I-D.ietf-hpke-hpke].

* pkR is the public key of the recipient, as defined in [I-D.ietf-hpke-hpke].

* skR is the private key of the recipient, as defined in [I-D.ietf-hpke-hpke].

* Key Encapsulation Mechanism (KEM), see [I-D.ietf-hpke-hpke].

* Key Derivation Function (KDF), see [I-D.ietf-hpke-hpke].

* Authenticated Encryption with Associated Data (AEAD), see [I-D.ietf-hpke-hpke].

* Additional Authenticated Data (AAD), see [I-D.ietf-hpke-hpke].

3. HPKE for COSE

3.1. Overview

This specification supports two modes of using HPKE in COSE, namely:

* HPKE Integrated Encryption mode, where HPKE is used to encrypt the plaintext. This mode can only be used with a single recipient. Section 3.2 provides the details.

* HPKE Key Encryption mode, where HPKE is used to encrypt a content encryption key (CEK), which then encrypts the content. This mode supports multiple recipients. Section 3.3 provides the details.

Distinct algorithm identifiers are defined and registered that are specific to each COSE HPKE mode so that they are fully specified, as required by [RFC9864]. Algorithm identifiers MUST only be used in the COSE HPKE mode that is specified for them.

In both cases, the new COSE header parameter "ek" MUST be present. It contains the encapsulated KEM shared secret. The value of this parameter MUST be the "enc" value output by the HPKE Seal() operation, as defined in Section 6.1 of [I-D.ietf-hpke-hpke]. The "ek" header parameter MUST be encoded as a CBOR byte string.

HPKE defines several authentication modes, as described in Table 1 of [I-D.ietf-hpke-hpke]. This specification uses both ’mode_base’ and ’mode_psk’. The mode is ’mode_psk’ if the "psk_id" header parameter is present; otherwise, the mode defaults to ’mode_base’. ’mode_base’ is described in Section 5.1.1 of [I-D.ietf-hpke-hpke], which only enables encryption to the holder of a given KEM private key. ’mode_psk’ is described in Section 5.1.2 of [I-D.ietf-hpke-hpke], which authenticates using a pre-shared key.

3.2. HPKE Integrated Encryption Mode

This mode applies if the COSE_Encrypt0 structure uses a COSE-HPKE algorithm and has no recipient structure(s).

Because COSE-HPKE supports header protection, if the "alg" parameter is present, it MUST be included in the protected header and MUST be a COSE-HPKE algorithm.

Although the use of the "kid" parameter in COSE_Encrypt0 is discouraged by RFC 9052, this document RECOMMENDS the use of the "kid" parameter (or other parameters) to explicitly identify the static recipient public key used by the sender. If the COSE_Encrypt0 structure includes a "kid" parameter, the recipient MAY use it to select the corresponding private key.

When encrypting, the inputs to the HPKE Seal operation are set as follows:

* kem_id: From the ciphersuite. See Section 4.

* pkR: The recipient public key, converted into an HPKE public key.

* kdf_id: From the ciphersuite. See Section 4.

* info: Defaults to the empty string; externally provided information MAY be used instead.

* aad: MUST contain the byte string for the authenticated data structure according to the steps defined in Section 5.3 of RFC 9052.

For the Integrated Encryption mode the context string will be "Encrypt0". Externally provided AAD information MAY be provided and MUST be passed into the Enc_structure via the external_aad field.

* aead_id: From the ciphersuite. See Section 4.

* pt: The raw message plaintext.

The outputs are used as follows:

* enc: MUST be placed raw into the "ek" (encapsulated key) parameter in the unprotected bucket.

* ct: MUST be used as layer ciphertext. If not using detached content, this is directly placed as ciphertext in COSE_Encrypt0 structure. Otherwise, it is transported separately and the ciphertext field is nil. See Section 5 of [RFC9052] for a description of detached payloads.

If ’mode_psk’ has been selected, then the "psk_id" parameter MUST be present. If ’mode_base’ has been chosen, then the "psk_id" parameter MUST NOT be present.

When decrypting, the inputs to the HPKE Open operation are set as follows:

* kem_id: From the ciphersuite. See Section 4.

* skR: The recipient private key, converted into an HPKE private key.

* kdf_id: From the ciphersuite. See Section 4.

* aead_id: From the ciphersuite. See Section 4.

* info: Defaults to the empty string; externally provided information MAY be used instead.

* aad: MUST contain the byte string for the authenticated data structure according to the steps defined in Section 5.3 of RFC 9052. For the Integrated Encryption mode the context string will be "Encrypt0". Externally provided AAD information MAY be provided and MUST be passed into the Enc_structure via the external_aad field.

* enc: The contents of the layer "ek" parameter.

* ct: The contents of the layer ciphertext.

The plaintext output is the raw message plaintext.

The COSE_Encrypt0 MAY be tagged or untagged.

An example is shown in Section 5.1.

3.3. HPKE Key Encryption Mode

This mode specifies a method for constructing a COSE_Recipient using HPKE. In this construction, both key agreement and key wrapping are performed within HPKE.

A COSE_Encrypt structure is used with two logical layers:

* Layer 0 contains the content (plaintext) encrypted with the CEK. This ciphertext may be detached, and if not detached, then it is included in the COSE_Encrypt structure.

* Layer 1 contains a COSE_Recipient with the parameters needed for HPKE to generate a shared secret used to encrypt the CEK. This layer conveys the encrypted CEK in the COSE_recipient structure using a COSE-HPKE algorithm.

This two-layer structure is used to encrypt content that can also be shared with multiple recipients at the expense of a single additional encryption operation. The content is encrypted once with the CEK, then the CEK is encrypted for each recipient. Layer 1 may also contain other COSE_Recipients using other content key distribution methods that also encrypt the CEK.

3.3.1. Recipient_structure

This section defines the Recipient_structure, which is used in place of COSE_KDF_Context for COSE-HPKE recipients. It MUST be used for COSE-HPKE recipients, as it provides integrity protection for recipient-protected header parameters.

The Recipient_structure is modeled after the Enc_structure defined in [RFC9052], but is specific to COSE_recipient structures and MUST NOT be used with COSE_Encrypt.

Furthermore, the use of COSE_KDF_Context is prohibited in COSE-HPKE; it MUST NOT be used.

```
Recipient_structure = [
    context: "HPKE Recipient",
    next_layer_alg: int/tstr,
    recipient_protected_header: empty_or_serialized_map,
    recipient_extra_info: bstr
]
```

"next_layer_alg": The algorithm ID of the COSE layer for which the COSE_recipient is encrypting a key. It is the algorithm that the key MUST be used with. This value MUST match the "alg" parameter in the next lower COSE layer.

"recipient_protected_header": The protected header parameters from the COSE_recipient.

"recipient_extra_info": Any additional context the application wishes to include in the key derivation via the HPKE info parameter. If none, it is a zero-length string.

The Recipient_structure MUST be serialized deterministically in accordance with the Core Deterministic Encoding Requirements defined in Section 4.2.1 of [RFC8949]. This requirement applies only to the Recipient_structure itself — the array and its four members. It does not extend into the byte-string wrapped protected headers.

3.3.2. COSE-HPKE Recipient Construction

This section gives the steps for constructing a COSE_Recipient using HPKE.

When encrypting, the inputs to the HPKE Seal operation are set as follows:

* kem_id: From the ciphersuite. See Section 4.

* kdf_id: From the ciphersuite. See Section 4.

* aead_id: From the ciphersuite. See Section 4.

* pkR: The recipient public key, converted into HPKE public key.

* info: Deterministic encoding of the Recipient_structure. Externally provided context information MAY be provided and MUST be passed into the Recipient_structure via the recipient_extra_info field.

* aad: Defaults to the empty string; externally provided information MAY be used instead.

* pt: The CEK.

The outputs are put in the COSE_Recipient as follows:

* enc: MUST be placed into the "ek" (encapsulated key) header parameter in the unprotected bucket.

* ct: MUST be placed in the ciphertext field.

While the "alg" header parameter is not strictly required in the COSE_Recipient, if present, it must be the ciphersuite used to specify the HPKE algorithms. See Section 4. If the "alg" parameter is present it MUST be a protected header parameter.

The protected header MAY contain the "kid" parameter to identify the static recipient public key that the sender used. Use of the "kid" parameter is RECOMMENDED to explicitly identify the static recipient public key used by the sender. Including it in the protected header parameters ensures that it is input into the key derivation function of HPKE.

When decrypting, the inputs to the HPKE Open operation are as follows:

* kdf_id: From the "alg" parameter ciphersuite. See Section 4.

* aead_id: From the "alg" parameter ciphersuite. See Section 4.

* kem_id: From the "alg" parameter ciphersuite. See Section 4.

* enc: From the "ek" parameter in the COSE_Recipient headers.

* skR: The recipient private key, converted into an HPKE private key.

* info: Deterministic encoding of the Recipient_structure. Externally provided context information MAY be provided and MUST be passed into the Recipient_structure via the recipient_extra_info field.

* aad: Defaults to the empty string; externally provided information MAY be used instead.

* ct: The contents of the COSE_Recipient ciphertext field.

The plaintext output is the CEK.

It is not necessary to populate recipient_aad, as HPKE inherently mitigates the classes of attacks that COSE_KDF_Context, and SP800-56A are designed to address. COSE-HPKE use cases may still utilize recipient_aad for other purposes as needed; however, it is generally intended for small values such as identifiers, contextual information, or secrets. It is not designed for protecting large or bulk external data.

Any bulk external data that requires protection should be handled at layer 0 using external_aad.

The COSE_recipient structure is computed for each recipient.

When encrypting the content at layer 0, the instructions in Section 5.3 of [RFC9052] MUST be followed, including the calculation of the authenticated data structure.

An example is shown in Section 5.2.

3.3.3. Security Design Rationale

COSE-HPKE does not use COSE_KDF_Context, which is defined in Section 5.2 of [RFC9053], for the following reasons:

* HPKE is a well-analyzed and widely reviewed construction that already incorporates the protections provided by COSE_KDF_Context.

* The HPKE design avoids many of the weaknesses present in earlier key agreement protocols that COSE_KDF_Context was designed to mitigate.

* Use of the COSE_KDF_Context would introduce unnecessary complexity; many of the fields typically go unused.

* It is difficult to know what to put in the COSE_KDF_Context fields.

The algorithm identifier for the bulk content encryption algorithm can be manipulated, since it is neither integrity-protected nor incorporated into the key derivation. In particular, the layer 0 algorithm identifier is not integrity protected by the COSE_Recipient and is therefore not cryptographically bound to the key agreement algorithm. This class of attack has been demonstrated against CMS; a corresponding mitigation is described in [I-D.ietf-lamps-cms-cek-hkdf-sha256].

The "next_layer_alg" member of the Recipient_structure mitigates this attack by explicitly binding the bulk content encryption algorithm identifier with the COSE_Recipient. The "next_layer_alg" member is explicitly defined to identify the algorithm for the immediately following COSE layer. Such explicit layering semantics were not provided for the AlgorithmID field in COSE_KDF_Context, where the intended interpretation was ambiguous.

3.4. Key Representation

The COSE_Key with the existing key types can be used to represent KEM private or public keys. When using a COSE_Key for COSE-HPKE, the following checks are made:

* If the "kty" field is "AKP", then the public and private keys SHALL be the raw HPKE public and private keys (respectively) for the KEM used by the algorithm.

* Otherwise, the key MUST be suitable for the KEM used by the algorithm. In case the "kty" parameter is "EC2" or "OKP", this means the value of "crv" parameter is suitable. The valid combinations of KEM, "kty" and "crv" for the algorithms defined in this document are shown in Figure 1.

* If the "key_ops" field is present, it MUST include only "derive bits" for the private key and MUST be empty for the public key.

Examples of the COSE_Key for COSE-HPKE are shown in Section 5.3.

4. Ciphersuite Registration

A ciphersuite is a set of cryptographic algorithms selected to achieve a specific security level. For COSE-HPKE, a single COSE algorithm ID represents a ciphersuite that maps to the following HPKE algorithm identifiers:

* KEM algorithm
* KDF algorithm
* AEAD algorithm

Each COSE algorithm ID registered for COSE-HPKE MUST indicate the three HPKE algorithm IDs mapped by the ciphersuite.

The HPKE mode is determined by the presence or absence of the "psk_id" parameter and is therefore not explicitly indicated in the ciphersuite.

For a list of ciphersuite registrations, please see Section 7. The following table summarizes the relationship between the ciphersuites registered in this document and the values registered in the HPKE IANA registry [HPKE-IANA].

COSE-HPKE Ciphersuite Label	COSE HPKE Mode	HPKE		
		KEM	KDF	AEAD
HPKE-0	Integrated Encryption	0x10	0x1	0x1
HPKE-1	Integrated Encryption	0x11	0x2	0x2
HPKE-2	Integrated Encryption	0x12	0x3	0x2
HPKE-3	Integrated Encryption	0x20	0x1	0x1
HPKE-4	Integrated Encryption	0x20	0x1	0x3
HPKE-5	Integrated Encryption	0x21	0x3	0x2
HPKE-6	Integrated Encryption	0x21	0x3	0x3
HPKE-7	Integrated Encryption	0x10	0x1	0x2
HPKE-0-KE	Key Encryption	0x10	0x1	0x1
HPKE-1-KE	Key Encryption	0x11	0x2	0x2
HPKE-2-KE	Key Encryption	0x12	0x3	0x2
HPKE-3-KE	Key Encryption	0x20	0x1	0x1
HPKE-4-KE	Key Encryption	0x20	0x1	0x3
HPKE-5-KE	Key Encryption	0x21	0x3	0x2
HPKE-6-KE	Key Encryption	0x21	0x3	0x3
HPKE-7-KE	Key Encryption	0x10	0x1	0x2

The following list maps the ciphersuite labels to their textual description.

* HPKE-0: Integrated Encryption with DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* HPKE-1: Integrated Encryption with DHKEM(P-384, HKDF-SHA384) KEM, HKDF-SHA384 KDF, and AES-256-GCM AEAD.

* HPKE-2: Integrated Encryption with DHKEM(P-521, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* HPKE-3: Integrated Encryption with DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* HPKE-4: Integrated Encryption with DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and ChaCha20Poly1305 AEAD.

* HPKE-5: Integrated Encryption with DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* HPKE-6: Integrated Encryption with DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and ChaCha20Poly1305 AEAD.

* HPKE-7: Integrated Encryption with DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-256-GCM AEAD.

* HPKE-0: Key Encryption with DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* HPKE-1: Key Encryption with DHKEM(P-384, HKDF-SHA384) KEM, HKDF-SHA384 KDF, and AES-256-GCM AEAD.

* HPKE-2: Key Encryption with DHKEM(P-521, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* HPKE-3: Key Encryption with DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* HPKE-4: Key Encryption with DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and ChaCha20Poly1305 AEAD.

* HPKE-5: Key Encryption with DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* HPKE-6: Key Encryption with DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and ChaCha20Poly1305 AEAD.

* HPKE-7: Key Encryption with DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-256-GCM AEAD.

As the list indicates, the ciphersuite labels have been abbreviated at least to some extent to strike a balance between readability and length.

The ciphersuite list above is a minimal starting point. Additional ciphersuites can be registered into the already existing registry. For example, once post-quantum cryptographic algorithms have been standardized it might be beneficial to register ciphersuites for use with COSE-HPKE. Additionally, ciphersuites utilizing the compact encoding of the public keys, as defined in [I-D.irtf-cfrg-dnhpke], may be standardized for use in constrained environments.

As a guideline for ciphersuite submissions to the IANA COSE algorithm registry, the designated experts must only register combinations of (KEM, KDF, AEAD) triple that constitute valid combinations for use with HPKE, the KDF used should (if possible) match one internally used by the KEM, and components should not be mixed between global and national standards.

4.1. COSE_Keys for COSE-HPKE Ciphersuites

The COSE-HPKE algorithm uniquely determines the KEM for which a COSE_Key is used. The following mapping table shows the valid combinations of the KEM used, COSE_Key type, and its curve/key subtype. This holds for COSE algorithms using either of the COSE HPKE modes (Integrated Encryption and Key Encryption).

HPKE KEM id	COSE_Key	
	kty	crv
0x0010, 0x0013	EC2	P-256
0x0011, 0x0014	EC2	P-384
0x0012, 0x0015	EC2	P-521
0x0020	OKP	X25519
0x0021	OKP	X448

Figure 1: COSE_Key Types and Curves for COSE-HPKE Ciphersuites

5. Examples

This section provides a set of examples that show the HPKE Integrated Encryption Mode and the HPKE Key Encryption Mode, and illustrates the use of key representations for HPKE KEM.

5.1. COSE HPKE Integrated Encryption Mode

This example assumes that a sender wants to communicate an encrypted payload to a single recipient, named "bob".

An example of the HPKE Integrated Encryption Mode is shown in Figure 3. Line breaks and comments have been inserted for better readability.

This example uses the following:

* Suite: HPKE-0 (P-256 / HKDF-SHA256 / AES-128-GCM)

* Plaintext: "This is the content."

* External AAD: empty

* External Info: empty

* Recipient kid: "bob"

The ciphertext (hex) transmitted to "bob" is:

```
d08344a1011823a20443626f622358410457229bdd99407b384a9e59fa15
53224d58b106e9ebebdaa06d2126bd96757674847669966ecb0dcdf21af5
623f19f0b799b0cddf3ee930b739dd474f6282de0158253f3c1595e9d252
e816215a9ce73f47ba4b57acb06ecc39ca5a03a14108bbe7807af5688d61
```

Figure 2: Hex-Encoding of COSE_Encrypt0

COSE_Encrypt0 pretty-printed:

```
16([
  h'A1011823',
  {
    4: 'bob',
    -4: h'0457229BDD99407B384A9E59FA1553224D58B106E9EBEBDA
    A06D2126BD96757674847669966ECB0DCDF21AF5623F19F0B799B0
    CDDF3EE930B739DD474F6282DE01'
  },
  h'3F3C1595E9D252E816215A9CE73F47BA4B57ACB06ECC39CA5A03A1
  4108BBE7807AF5688D61'
  ])
```

Figure 3: COSE_Encrypt0 Example for HPKE

The following COSE Key was used in this example:

```
{
  1 /kty/: 2,
  2 /kid/: h'626f62',
  3 /alg/: 35 /HPKE-0  (P-256 + HKDF-SHA256 + AES-128-GCM)/,
 -1 /crv/: 1 /P-256/,
 -2 /x/:
  h'02a8e3315f96bc7355dbf85740c6d8e53fb070cd8ba5c419be49a91d789ef55c',
 -3 /y/:
  h'96b6621abf5ca532e042dc5c346c1ef0c9186b83cb122e50a46f1458de023d35',
 -4 /d/:
  h'eca39300147c91a2a65d17e00ea278b57a14178245bf5686d9a404cca1816b8e'
}
```

Figure 4: COSE Key

5.2. COSE HPKE Key Encryption Mode

An example of key encryption using the COSE_Encrypt structure using HPKE is shown in below. Line breaks and comments have been inserted for better readability.

This example uses the following input parameters:

* Content encryption algorithm: AES-128-GCM
* plaintext: "This is the content."
* kid:"bob"
* alg: HPKE-0-KE (assumed 46) - Key Encryption, DHKEM(P-256, HKDF-SHA256), KDF: HKDF-SHA256, AEAD: AES-128-GCM
* external aad and info are empty

The following COSE Key is used:

```
a701020243626f6203182e2001215820d832916778598ea6203af974c97b
45970ac0266fc6a3b7f213ba9f8b591b92972258208d9410599a8e83d00e
b46d67b34d4dac8fbd4b8b1f08864599659cee9ef09184235820b1162c56
8efcba91c8e4e82f66e36b45aa10bc55228cf65ecd3bb29cfb09f989
```

As a pretty-printed version:

```
   {
      1 /kty/: 2,
      2 /kid/: h'626f62' /"bob"/,
      3 /alg/: 46 /HPKE-0-KE/,
     -1 /crv/: 1 /P-256/,
     -2 /x/:
        h'd832916778598ea6203af974c97b45970ac0266fc6a3b7f213ba9
   f8b591b9297',
     -3 /y/:
       h'8d9410599a8e83d00eb46d67b34d4dac8fbd4b8b1f08864599659c
   ee9ef09184',
     -4 /d/:
       h'b1162c568efcba91c8e4e82f66e36b45aa10bc55228cf65ecd3bb2
   9cfb09f989'
   }
```

As a result, the following COSE_Encrypt payload is produced:

```
d8608443a10101a1055089115f10ecc1c7fd834442cb87929bc15825534d
b92f5366e3cadd096774a9576bb8d8867e75ea38c329ecfc7b8793c5a4ae
9603e5b0b6818349a201182e0443626f62a12358410417cd85837981ddb1
4963061ab5fb7308988eb922f87cf6cf6ef83556f7657922c9815947e41b
9bc932e48c6f1c4677d9a5506a30d694587628b5193a4cde2f3f58204b50
8a340e463c317f4e62fb8d08c887cac4788087ad022562d05855a50ca4a0
```

Pretty-printed, this hex-sequence has the following content:

```
96([
  h'A10101',
  {5: h'89115F10ECC1C7FD834442CB87929BC1'}, h'534DB92F5366E3CADD096774A9576BB8D8867E75EA3
8C329ECFC7B87
  93C5A4AE9603E5B0B6',
  [
    [
    h'A201182E0443626F62',
    {-4: h'0417CD85837981DDB14963061AB5FB7308988EB922F87CF6C
    F6EF83556F7657922C9815947E41B9BC932E48C6F1C4677D9A5506A3
    0D694587628B5193A4CDE2F3F'}, h'4B508A340E463C317F4E62FB8D08C887CAC4788087AD022562D058
    55A50CA4A0']]
  ])
```

5.3. Key Representation

Examples of private and public KEM key representation are shown below.

5.3.1. Public Key for HPKE-0

```
{
    / kty = 'EC2' /
    1: 2,
    / kid = '01' /
    2: h'3031',
    / alg = HPKE-0 (Assumed: 35) /
    3: 35,
    / crv = 'P-256' /
    -1: 1,
    / x /
    -2: h'65eda5a12577c2bae829437fe338701a10aaa375
          e1bb5b5de108de439c08551d',
    / y /
    -3: h'1e52ed75701163f7f9e40ddf9f341b3dc9ba860af
          7e0ca7ca7e9eecd0084d19c'
}
```

Figure 5: Public Key Representation Example for HPKE-0

5.3.2. Private Key for HPKE-0

```
{
    / kty = 'EC2' /
    1: 2,
    / kid = '01' /
    2: h'3031',
    / alg = HPKE-0 (Assumed: 35) /
    3: 35,
    / key_ops = ['derive_bits'] /
    4: [8],
    / crv = 'P-256' /
    -1: 1,
    / x /
    -2: h'bac5b11cad8f99f9c72b05cf4b9e26d244dc189f7
          45228255a219a86d6a09eff',
    / y /
    -3: h'20138bf82dc1b6d562be0fa54ab7804a3a64b6d72
          ccfed6b6fb6ed28bbfc117e',
    / d /
    -4: h'57c92077664146e876760c9520d054aa93c3afb04
          e306705db6090308507b4d3',
}
```

Figure 6: Private Key Representation Example for HPKE-0

5.3.3. KEM Public Key for HPKE-4

```
{
    / kty = 'OKP' /
    1: 1,
    / kid = '11' /
    2: h'3131',
    / alg = HPKE-4 (Assumed: 42) /
    3: 42,
    / crv = 'X25519' /
    -1: 4,
    / x /
    -2: h'cb7c09ab7b973c77a808ee05b9bbd373b55c06eaa
          9bd4ad2bd4e9931b1c34c22',
}
```

Figure 7: Public Key Representation Example for HPKE-4

6. Security Considerations

This specification is based on HPKE and the security considerations of [I-D.ietf-hpke-hpke] are therefore applicable also to this specification.

Both HPKE and HPKE COSE assume that the sender possesses the recipient's public key. Therefore, some form of public key distribution mechanism is assumed to exist, but this is outside the scope of this document.

HPKE relies on a source of randomness to be available on the device. Additionally, with the two layer structure the CEK is randomly generated and it MUST be ensured that the guidelines in [RFC8937] for random number generation are followed.

HPKE in Base mode does not offer authentication as part of the HPKE KEM. In this case COSE constructs like COSE_Sign, COSE_Sign1, COSE_Mac, or COSE_Mac0 can be used to add authentication.

If COSE_Encrypt or COSE_Encrypt0 is used with a detached ciphertext then the subsequently applied integrity protection via COSE_Sign, COSE_Sign1, COSE_Mac, or COSE_Mac0 does not cover this detached ciphertext. Implementers MUST ensure that the detached ciphertext also experiences integrity protection. This is, for example, the case when an AEAD cipher is used to produce the detached ciphertext but may not be guaranteed by non-AEAD ciphers.

7. IANA Considerations

This document requests IANA to add new values to the 'COSE Algorithms' and to the 'COSE Header Parameters' registries.

7.1. COSE Algorithms Registry

7.1.1. HPKE-0

* Name: HPKE-0
* Value: TBD1 (Assumed: 35)
* Description: COSE HPKE Integrated Encryption using DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.2. HPKE-1

* Name: HPKE-1
* Value: TBD3 (Assumed: 37)
* Description: COSE HPKE Integrated Encryption using DHKEM(P-384, HKDF-SHA384) KEM, HKDF-SHA384 KDF, and AES-256-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.3. HPKE-2

* Name: HPKE-2
* Value: TBD5 (Assumed: 39)
* Description: COSE HPKE Integrated Encryption using DHKEM(P-521, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.4. HPKE-3

* Name: HPKE-3

* Value: TBD7 (Assumed: 41)

* Description: COSE HPKE Integrated Encryption using DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.5. HPKE-4

* Name: HPKE-4

* Value: TBD8 (Assumed: 42)

* Description: COSE HPKE Integrated Encryption using DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and ChaCha20Poly1305 AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.6. HPKE-5

* Name: HPKE-5

* Value: TBD9 (Assumed: 43)

* Description: COSE HPKE Integrated Encryption using DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.7. HPKE-6

* Name: HPKE-6

* Value: TBD10 (Assumed: 44)

* Description: COSE HPKE Integrated Encryption using DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and ChaCha20Poly1305 AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.8. HPKE-7

* Name: HPKE-7

* Value: TBD13 (Assumed: 45)

* Description: COSE HPKE Integrated Encryption using DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.9. HPKE-0-KE

* Name: HPKE-0-KE

* Value: TBD14 (Assumed: 46)

* Description: COSE HPKE Key Encryption using DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.10. HPKE-1-KE

* Name: HPKE-1-KE

* Value: TBD15 (Assumed: 47)

* Description: COSE HPKE Key Encryption using DHKEM(P-384, HKDF-SHA384) KEM, HKDF-SHA384 KDF, and AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.11. HPKE-2-KE

* Name: HPKE-2-KE

* Value: TBD16 (Assumed: 48)

* Description: COSE HPKE Key Encryption using DHKEM(P-521, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.

* Capabilities: [kty]

* Change Controller: IESG

* Reference: [[TBD: This RFC]]

* Recommended: Yes

7.1.12. HPKE-3-KE

* Name: HPKE-3-KE

* Value: TBD17 (Assumed: 49)

* Description: COSE HPKE Key Encryption using DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-128-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.13. HPKE-4-KE

* Name: HPKE-4-KE
* Value: TBD18 (Assumed: 50)
* Description: COSE HPKE Key Encryption using DHKEM(X25519, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and ChaCha20Poly1305 AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.14. HPKE-5-KE

* Name: HPKE-5-KE
* Value: TBD19 (Assumed: 51)
* Description: COSE HPKE Key Encryption using DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and AES-256-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.15. HPKE-6-KE

* Name: HPKE-6-KE
* Value: TBD20 (Assumed: 52)
* Description: COSE HPKE Key Encryption using DHKEM(X448, HKDF-SHA512) KEM, HKDF-SHA512 KDF, and ChaCha20Poly1305 AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.1.16. HPKE-7-KE

* Name: HPKE-7-KE
* Value: TBD21 (Assumed: 53)
* Description: COSE HPKE Key Encryption using DHKEM(P-256, HKDF-SHA256) KEM, HKDF-SHA256 KDF, and AES-256-GCM AEAD.
* Capabilities: [kty]
* Change Controller: IESG
* Reference: [[TBD: This RFC]]
* Recommended: Yes

7.2. COSE Header Parameters

7.2.1. ek Header Parameter

* Name: ek
* Label: TBD11 (Assumed: -4)
* Value type: bstr
* Value Registry: N/A
* Description: HPKE encapsulated key

* Reference: [[TBD: This RFC]]

7.2.2. psk_id Header Parameter

* Name: psk_id

* Label: TBD12 (Assumed: -5)

* Value type: bstr

* Value Registry: N/A

* Description: A key identifier (kid) for the pre-shared key as defined in Section 5.1.2 of [I-D.ietf-hpke-hpke]

* Reference: [[TBD: This RFC]]

8. References

8.1. Normative References

[I-D.ietf-hpke-hpke] Barnes, R., Bhargavan, K., Lipp, B., and C. A. Wood, "Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-ietf-hpke-hpke-02, 4 November 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-02>.

[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>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

[RFC9053] Schaad, J., "CBOR Object Signing and Encryption (COSE): Initial Algorithms", RFC 9053, DOI 10.17487/RFC9053, August 2022, <https://www.rfc-editor.org/rfc/rfc9053>.

8.2. Informative References

[HPKE-IANA]
IANA, "Hybrid Public Key Encryption (HPKE) IANA Registry", October 2023, <https://www.iana.org/assignments/hpke/hpke.xhtml>.

[I-D.ietf-lamps-cms-cek-hkdf-sha256]
Housley, R., "Encryption Key Derivation in the Cryptographic Message Syntax (CMS) using HKDF with SHA-256", Work in Progress, Internet-Draft, draft-ietf-lamps-cms-cek-hkdf-sha256-05, 19 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-cms-cek-hkdf-sha256-05>.

[I-D.irtf-cfrg-dnhpke]
Harkins, D., "Deterministic Nonce-less Hybrid Public Key Encryption", Work in Progress, Internet-Draft, draft-irtf-cfrg-dnhpke-07, 16 October 2025, <https://datatracker.ietf.org/doc/html/draft-irtf-cfrg-dnhpke-07>.

[RFC8937] Cremers, C., Garratt, L., Smyshlyaev, S., Sullivan, N., and C. Wood, "Randomness Improvements for Security Protocols", RFC 8937, DOI 10.17487/RFC8937, October 2020, <https://www.rfc-editor.org/rfc/rfc8937>.

[RFC9864] Jones, M.B. and O. Steele, "Fully-Specified Algorithms for JSON Object Signing and Encryption (JOSE) and CBOR Object Signing and Encryption (COSE)", RFC 9864, DOI 10.17487/RFC9864, October 2025, <https://www.rfc-editor.org/rfc/rfc9864>.

Appendix A. Contributors

We would like to thank the following individuals for their contributions to the design of embedding the HPKE output into the COSE structure following a long and lively mailing list discussion:

* Richard Barnes

* Ilari Liusvaara

Finally, we would like to thank Russ Housley and Brendan Moran for their contributions to the draft as co-authors of initial versions.

Appendix B. Acknowledgements

We would like to thank John Mattsson, Mike Prorock, Michael Richardson, Thomas Fossati, and Gran Selander for their contributions to the specification.

Appendix C. Testvectors

The testvectors use the following input:

* Plaintext: "hpke test payload"
* AAD: "external-aad"
* Info: "external-info"
* HPKE AAD: "external-hpke-aad"

AAD is the COSE Enc_structure.external_aad. It is used as AAD for the COSE AEAD in Encrypt0/Encrypt (Layer 0). HPKE AAD is the HPKE AAD for CEK wrap/unwrap in Key Encryption (Layer 1). It is only passed to the HPKE Seal/Open of the CEK.

```
=============== NOTE: '\' line wrapping per RFC 8792 ================


HPKE-0-KE COSE_Key:: \
a70102024d626f622d68706b655f305f6b6503182e200121582064ea61f745f7deed\
186d697a4c8971593275501776634 8b0443a60aac450b5a622582088f53a4cbbcfcc\
1bf0b33d5dc60f789a7f495244f57c158a8ceed5179639152b235820e8de39325f3c\
                 0be02442076c470a46bca742de9bc2be453ec1dc049dda1f6ca3


HPKE-0-KE with default aad, default info, default hpke aad

Ciphertext: \
d8608443a10101a105507af5398f1827c014f68bdb9fe84152eb5821d25b7b5eb83d\
c30f3a4d9ddadd9bd2726e88c621182d88ff53b39c5688c558f732818353a201182e\
044d626f622d68706b655f305f6b65a1235841040189cdaf807a039007db9e298471\
7cff68554f1bbe372d73a7af89cad1b3b1ecdcfca75e2c3786ac3a7f61bf303395e2\
768b114ded2f4be39d40fff7917bb987582011a6de6b6c1e5240a1035c1239c7a8b3\
                                      000e7dc383818a97099f19b6c2b73b1b


HPKE-0-KE with default aad, default info, external hpke aad
```

```
   Ciphertext: \
   d8608443a10101a10550d68d7921fc2bf04d033edc091c7045f2582167788960ecb8\
   6bc44a71b67d4fffabaa94c032e7b7f639cd28574b9080b817e324818353a201182e\
   044d626f622d68706b655f305f6b65a123584104c73249f22b8c4171fecb3bd1093d\
   3c6a1288aab904db50cb7c688a5dcb02ef22fc734d6091472016fe087bd0eaa71694\
   821314321c6d193d842c220c7f58d819582075ea467d773d97db62deb5fd1507607e\
                                       e7ca47e467cedcd79f16a4072678713a
```

HPKE-0-KE with external aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a105506a6c63e17b739c728d65b66d39e85174582118b37ca471a5\
   306ba4745b9578e6a8cf618bc01d7f4f9f16c28049dcb12027677d818353a201182e\
   044d626f622d68706b655f305f6b65a1235841048115885e297b224f955c5ee9344c\
   944801e8633e9305763125bd0739656f6f0495af6bccb2c1e34d06ae586b186bdb61\
   8913e718456be702c2c84196ffee06245820e62641de898fa0534bfbaa671949554f\
                                       6d9db266270b0cdd8b53ff4255353a1b
```

HPKE-0-KE with external aad, default info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a10550f07d00afe300fe71beb752cadca5bb245821beed09dcab8c\
   16c6ac26ddf5df3d47c6638467cb231ba934882499db30a5073d7b818353a201182e\
   044d626f622d68706b655f305f6b65a123584104b1d54393905a8551df3a675032b5\
   97ce40fa18dee7a4b11fe0ca93524e4f20cd6de652360acc99e72f8b620039d33a9a\
   1bdd542158a1a16b6d152264ddb701f95820602d1e4fac1cd619fd5f54bd625dd186\
                                       1d80ddf6f4e220922616a05cc86018cc
```

HPKE-0-KE with default aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a1055089035dbd98078aac856737fc9ce06eba58210c356b57b017\
   0d371bf2cfc4c5d648164036726f33498ff2c99b1cee42257a197a818353a201182e\
   044d626f622d68706b655f305f6b65a1235841047ef0f70acf119a83c24b967af181\
   514fae47996bd0eafb4d8641e967802f28d58940fcfb4d28b4df4745a30700036b3b\
   ccc2ced18c1375865f421e583fb0a77958202f93933dd09fb3db2cd287b738664d34\
                                       bc263c89fab8aa6d46fa1d431814cd5f
```

HPKE-0-KE with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a10550edb91df2666a50b438779cbcd25ab4b158212b48ca390e8e\
   5903e467390347a8f4da0710ae6c66d90693083d8d62265b72fd5a818353a201182e\
   044d626f622d68706b655f305f6b65a1235841041fb11d2984ca125db16fd99fd8c3\
```

```
   f64862daee939a212fc68ddd275ee75b5c25a4b71c73d9620951d9897410c2a9f2f1\
   9aa5932446ac9b36b0ae1e913fe7bcc458200eec5d2195d413e32a60b593008a85a0\
                                        cc1ae74c63823feadd35eca3aba3786b
```

HPKE-0-KE with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a105509ab67637694ffe1f4420ededf9a3e4ed582110b9cfa11046\
   c75524433a693b8bcafea8522939afa042519495e46e1c40996869818353a201182e\
   044d626f622d68706b655f305f6b65a123584104ae1c16e230410ce4f385288a7d83\
   ebd0d12fa6760362e98c2c42dde16f8caaea74971025d8b39bae72a127fd795068d7\
   f3447a282d37295609e9b60dfa1a672958207ddfc787b9372d6ec0215a8504765947\
                                        271074e6e81c48e2c6d5de95ac306526
```

HPKE-0-KE with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a1055012c4d08a6cb6da8dff2c072a152858875821064264f2652b\
   166a88373bd9cedd96d38cb65c650726578910ae6e6e6313258f94818353a201182e\
   044d626f622d68706b655f305f6b65a1235841043bf1b7f2d106d364416c27f3d7cc\
   d03c3d803b9bd473c521456c51f8c1a37b917584b861c100c42eb0eb048519bc10d6\
   75ac8013174e669af6bed0f814cb614e58205c9e7e8f86b7ef1ba9f94425c9b0d8a7\
                                        f43fc56df49da6b414629c2b7c96f489
```

```
   HPKE-1-KE COSE_Key:: \
   a70102024d626f622d68706b655f315f6b6503182f200221583003fcd256d1fd79ce\
   8d6d29e3cb72a823380e1c655aa2ce211721245873bacb76eacd6e28f4557fed2552\
   46a76fdd61b82258304dd4aa71088792b44e00970c2f269c1eb546e848a6df2946e4\
   409777deb6d7b77803a383c9e87757cef9f18910a1f76423583035172a2ccec0f1d1\
   af547b811754e01de5406257ca808f2fabcbca5cbf7a4d22b951fc1d4da0e89e8608\
                                                            fde30d2f6706
```

HPKE-1-KE with default aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820aac05a4dcbdd92e82befd10b4724ef077579404dd106c4\
   bc33c69cb549cac1ed58214597a425b09b4ab5f169143378a5ff92169be65260098c\
   5ae834659444d753f672818353a201182f044d626f622d68706b655f315f6b65a123\
   586104bc7ed2fa3f73a546de2bae35fee30c39cad00e7883f85f2670a9eceb547262\
   dfb8f676f701b7143a6ff693380b397c23572dd677fc7bd6a5de005662ef9f8a3c33\
   5c81b69b59fa585a70e449ae581421ead6f7a0a6d9c05e9fdcac0db1f60605583008\
   e7f0466569e452d0f3e45aa99aa9dddeb04de6398fd55100578046c27e15ba13fd2c\
                                              abc5a33202ecd547a4c7b0c99e
```

HPKE-1-KE with default aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820c8ee79fb915867c74d950d05f6ca9d43d47f714936684c\
a7f0254d7df92ba68f5821e74e07295b12fc4a8e518c5cff4d05df0bcfe55d29804c\
6eaf2a176ddec72249f4818353a201182f044d626f622d68706b655f315f6b65a123\
58610463a670ebf1628d5a6238c131aa98bee619c1d007aa703e3312eff22c2145a9\
1f0dcb1e4787082e81720649780786e409fb9be9b7589d9d78e1d735cf1c664d4721\
4bc1d4dfd06216c07a8ada1b3fe0f41fb759965d65755dd59e74247561b19a583021\
15a5dcd6d165a7b30736723a4da24df149a89c0decde47e554abfc995b55a3eb89dd\
52d5059b96449ccd243fd93665

HPKE-1-KE with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a1055820ac71a5659fe597a604fcc77a3d5b2b52bcd0d7d00fc5e1\
57caf21ea9666a1f685821052f34eacd31e88626a199ac533fd0308b74268a3cd320\
df3e8697e5cc9ec6d211818353a201182f044d626f622d68706b655f315f6b65a123\
586104639aaa2fe678c4186e9578c16dc72d6006ca8f7df7946b67843d7c4248da84\
d6a8ebb0f58fb84689c54b1f23c8390b41e77d4bc4c93159ebc3a7810316ce505544\
ac2d81309fb45eb64a3401558921e37cd861aeaf895e9606b066be1a609bea5830bb\
266370fdb5c56669e4c88c86329ea9a84dde052c9482e4c6b305945d7c27e081b1d7\
cd5cd39c65ad4a4bd4bbeee875

HPKE-1-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820172e4e1b4df69bb472d261bfb43c78433c330625eae7f4\
a4e31cf10b2ceeb94d5821ebfa1a3352ed030fc5fef08ae1c1066bc7d9108fd45def\
05396a6b4cd3401af48d818353a201182f044d626f622d68706b655f315f6b65a123\
586104a355c7e5fa4a166ff68825bf094e81b9744aa2518ce381721c329952f26bbd\
de60f5fbde96fa47258684bd7277e545d3320b367ca06f42a56f6cf0afaaf1cb8ea9\
6e4fa46b9db1dca72fd19988d9af9234d2b02a251eee800fcc03c260fa23205830d5\
f92ee2d4eff9323732c0fa70a071fa068c1572188b67ce1401657ff32c1cf4d3bcb7\
0d2144ba4cfc323e4f93d8b8bf

HPKE-1-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820393f4c0886145f63d4de2012757a496b46f80da705c4fc\
7f045618b2b1bbe74d5821a580ae1f89bd1b84e546d94628c97c3548118e74c5026e\
ec543442b0bdf92f1d01818353a201182f044d626f622d68706b655f315f6b65a123\
58610483ad6cd4932f0fc73a7e0640b5db583082b0d741b64a948404adc5624e67e9\
167e9d81fd8d98e47afc006c2a366ff8f1c4062565c8b1e9a2cfe791120addfa86ef\
6b444e957982a3f194fa2e932f6987b8ebf674b8a96d5ebdde8a4edcd1fefd583088\

```
   f136f57fa98c10df0b8a09d1ed6833a25e197ee653652f104265e20acf723bb2ff7d\
                                                   aefc9db56f2120186c1d991978
```

HPKE-1-KE with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a105582086dbfa77caffcdcbc96b45ba891dd2b61a88ad0940ce5f\
   dadf44526eb3b043ac5821a558899a7bc196b4b252f5cbf13a6d1ab2b45a083719ae\
   0bcd3ac3cf16a45f911a818353a201182f044d626f622d68706b655f315f6b65a123\
   5861045cd0a1afae98177f0f2fc52d75eb0acc5b4b8464ef7f14e8b0d90410f88449\
   6f21747e0b589b1fba09b0da8312476cfa7492e4dff1258128b9be4cf6d8e94e9725\
   75935075767d186029a34d19115d4fd908565389ecfd21a4a528eeecb1a704583095\
   8ff6ee18bd7aca20198ba18b220658c1db5c67a2251600c1eb698fd85812c271a5ec\
                                                   61be430a8c985c9d0922815e3a
```

HPKE-1-KE with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820d19b7e6c324f92b83ee77477d5a646cd88b986b8c6f83c\
   dec36c7d4892f7ba7958212d06813db517713f343ff5125ef2ac14c41b574b931cce\
   50bd48b4ed3e2c5dc8e8818353a201182f044d626f622d68706b655f315f6b65a123\
   58610499890247ae97c42ff00408e71396e17ff114ac35f35849da6452c1cab3cc78\
   186a65bfbf7a7c79e12c78f7c562af7ab5c06ac4066f175c49d5992efab2c521c5d2\
   90549caee7d175e32d3f9bf1212b438c61eb8a010ea5956ff51d207d197fbb583064\
   b27d50df0f0305c139c7545bb339b4341c099d40294b55fe31ffd10d53ea9c6a58ad\
                                                   a98a89b5b7a2419434df7e6f16
```

HPKE-1-KE with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a10558209f03b841a61b17bf41e3afb0109933abc9750cf9a5f6d6\
   90a96283c9a8b30cf05821613a6eda5df30ef01a9d5974dd0f28598f587803a0e644\
   cf22f5b78e42f38a9259818353a201182f044d626f622d68706b655f315f6b65a123\
   586104f85e706f0b1469fcc2bad6a25cb801418954d78344bf56e855e4d0241dc654\
   d4050e224480e99644949875243cdb0cce4ab352e6e9ff3106fec195fa4bebe994da\
   650208b34b55b2f6a433609d6343d43e5a8abe8db28dc06f665cdef59984a15830a8\
   17dd751be11ed8596225bed31887383299ee632cbe319443a2b6f3bab515884c423e\
                                                   0af2a29e7db0ee13daad9d69f8
```

```
   HPKE-2-KE COSE_Key:: \
   a70102024d626f622d68706b655f325f6b650318302003215842003 3db899e500ac6\
   f1fb7a9e23f16a363e41b6d1f6dd5562c4faaa0491f1a74cbdbd039ff2b5824842d4\
   da26c36173bc31ba2d1672699d871fdca27b9af0020bb580225842012ecb4d569869\
   085618ce0a4e0f82fe9b618dae8b678e26e7a1ed8d8b9bdf7ffcd32dfdee1bd85ee5\
```

```
2097866c4f493a3174e6abb6b365057d212ce3d84a5010a6df235842019f28872f68\
9d9c3a8018712e453a23beac37cb86c87e2c5a99d7e3901f2e4f4995fae274ca0774\
                8a7076d0ecae6466a7c3cdbc55d233544a59d22d3e4dde1d4b5f
```

HPKE-2-KE with default aad, default info, default hpke aad

```
Ciphertext: \
d8608443a10103a105582036694bc81347438c501dc55add947708ba52ce8bb52aa7\
b2878d26a0b9878d855821e6032422deb9c62db49d50c0011197c39b586660b7a018\
443f1ab285f707019f69818353a2011830044d626f622d68706b655f325f6b65a123\
58850400d55b883bb4f6f54cb0f147826fb706f01ccb19d67a8df4ce4bdf451f39ae\
2c4e77370558c529c2022dd39e07f36e315705cafe57249ac9abd1fe0fd821a366bc\
e6013a2b390c1d3bf50f47cf19df06ee0564716dbc589c325a46fb66526167710a82\
a4e40c55629fb48619dde005fa002b994b240ab481c37aa4170f7d38c61674eee958\
30933543fd556de228367ef1d4b1b6407461bd4a7acede97d25ebf67590078cc3fe4\
                                        9408300ed29d23be1c27b2902317a8
```

HPKE-2-KE with default aad, default info, external hpke aad

```
Ciphertext: \
d8608443a10103a10558201d84edbb7cdff030f465bfce04a1e69e888bb092d660fc\
7837754591aef06e4158218fdcf224296ba502062f6029071f5f120ce2f8f3ba20e8\
1052a9e34dbda21026ec818353a2011830044d626f622d68706b655f325f6b65a123\
58850400c2d331ea52e37a71ca3b32abf85f25ef92ac398c806de067fa344a97b111\
f00677a62ed2eac2d540e5685279ec03ee69a6b23ed78baf8229b7aa83d76318d86b\
7a0142ad7baf09f065fafa8c887a5151272fd219d9c0b7caebf4f4e1532e261b5df4\
e5ce1b6ccb5dbfd86f5a6d7f0c34eb7f2da17b89831ebbf56791d18fb305c0197f58\
3076cf3e4a3ff03606752d6b7e09806c02aa35a4677452bfd0dbd1a8abb9de682978\
                                        a6d0ae2be5685d4ca48c85b5b2c0e4
```

HPKE-2-KE with external aad, default info, default hpke aad

```
Ciphertext: \
d8608443a10103a1055820ef1d313af4d977ec69da4dec5fb387920fb5f0e1843dab\
998a24ee94aa47a119582186a225225aadeed9ed918e6d1f48c4697e10a07085aa6f\
cbc0fdff18189b85f361818353a2011830044d626f622d68706b655f325f6b65a123\
588504004074fd0f72b7237966abf252c0e41a21c5566e0f8c94c2a86c6d21e16035\
c57a887e5f69a3adf44a1580992bac716f2693a8fd3771043b022d016771b0498569\
390168f4cd133158b2da000169f8676e3499161f35be790f7c26bd984b339b00ce50\
5c18b3470f0e159741d63a1fe106eb1ecb6ca50c8130670f28c97bfc625ff33eaf58\
30935ea79f6e36fd6785bcdbcdcfc737f01400d1262aadf8f2814a123cbd5a498550\
                                        f3f30978aad8c71b5dec58238e9d61
```

HPKE-2-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a105582050ffa1a4eddc067fa06db21366dc53f4746d1d7b4f9fdb\
9e02532c80591e621258217c27fb226998f944de516cd7a13509aed1070e72bd4639\
f955efe6626a202ec97f818353a2011830044d626f622d68706b655f325f6b65a123\
588504004a73a294d7a1c96685a9ca89dd657afddb2fd8263474d5d020d46a59ed66\
290770b6e7989c60f800eeef64de8f823c9e40c99b5deee652b5c5d450b9ea127dc0\
06009e49e147db35cae26ab891572765c4fc588962d0f71c046c3f7f627f09a41e9e\
682d0d1740720ee8b73adb777c44fdcf4c343b08aaf01849c32ae4cdaa56e04a8958\
30609a822ab35ac0e183c1049d0e80556d443c8a6f80a27da55f8c34605c240b720d\
beafe4961fd95eac09dafa4c090de0

HPKE-2-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a10558208abd74a6f6494dca72c2dbdbd5f7771a508fb43adf7772\
08e7dc828a9ccf024d582133db1cbe20bb05829a6f1a2d4bdad78d4b3c9e10dd9d3d\
e106454fbd6b967361ee818353a2011830044d626f622d68706b655f325f6b65a123\
588504012af1fa72a02b73aa86229266d417f82dc19c55ff550f122e354dc3c7866a\
ef669f26cf2b57f9b9d3f373903dd1d0ef0c5189d41aa7cbfd4bfc4c955e5727420b\
980076484702ecfbf448298ffa72d1d31f36d9dfd629104e5bd5f226c6fb992fa754\
51d0114144b1908e93a3d5c5db83064bf973c9ae2f7876b669a55e49a3dc9bab2158\
3040424efb8c1c3827fe491bc7e426dff929402372dcb44e5b29103ab7254204367d\
72f56df75003b07fe4294b93fdc2a6

HPKE-2-KE with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a10558203099a01f838a003fc9119ee15835749011e099d23026f1\
34a96b0ec2a99711005821aa17b650a15695339c627f95080f37b0e27bdd56d75863\
6cedf5ffa1028490f407818353a2011830044d626f622d68706b655f325f6b65a123\
588504015b3422b8aa732b57dba50e817eacef848ac0f6f9d41fe2496512442044cf\
5cea24778deff337c76b26fe23f7f3820d95e22766d72e2ddfc54750c6c1089b585e\
250043c612eeaf05c49b1df18066f8b4925d287c3b36b6177206b8964bcb9d2aab62\
c77117444ccb4164c7e60e07df0a00ccd28f19747c3d1b4999055a215e06dd0efc58\
3046501065f28c600ff9872eadec2c958d4435edbf3c6aef7fe8b01b6b7fe625e53e\
0186a9d52b26573031b49009ae1808

HPKE-2-KE with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820d6571aef69ca1d95c29f8e32138f3b4cf73d6de02bd42f\
21c5c245dd1281e95d5821aaeb110acefa649d60730cdf59fdfbfe99d4cd468f0af7\
9912a996d6fc62946107818353a2011830044d626f622d68706b655f325f6b65a123\
58850401a18bb1ccfe76360447ac01c17cfef513f41ab8a9d621aac0c3f1cd523fc1\
5748ba0aa4526745260f918826fac568c9c1788db3ef20cabcb60d057ec4d01f7146\

```
cd005e52a1743fce60440f6a7e630165bee4bd7059ea01781488bf397416920d33f5\
5f1cf0d01c89a90611c5a5a07cf493d693b02266d743a972652ca94e8652fa52ef58\
3011f8320f59b91a8aee140d2edf61e0da9db310e42759577c3254f927b7d83d85d2\
                                    632a955ab4e1bb2c5093b37a8ea138
```

HPKE-2-KE with external aad, external info, external hpke aad

Ciphertext: \

```
d8608443a10103a1055820ebd94a697400c2eb88607a0bc538915e63f5fdbe4f528a\
11e559244b773da7115821af4eb2942d7596739651bb60b4de3c456cf74296af3cf0\
665de158cfaabba1b188818353a2011830044d626f622d68706b655f325f6b65a123\
58850401db35d812f17987c11a82fcc40bb40c540a7ace9c35b4da9b65dc03ef67e2\
199b066a3ce082f9da9f596b73daf89b643756f8e29df45d0b78b002ba1d96f2661b\
78005472f944fd1172c93c04df2e8a6452ddf5ba4c932d17604b58591903de3f60c2\
8557a781269ce31779c1f2d752ec1fe9fc6ffdcdb6f21a71e6ae5969d07fffc0fe58\
30d96f3bf5629c8c9cf315cac23cdf75c72c013df31434f9999eb2852111faa0d3c3\
                                    6c5e7f1b5ebd81b0644c38ee8e3bec
```

HPKE-3-KE COSE_Key:: \

```
a60101024d626f622d68706b655f335f6b650318312004215820 2d925acfd0ee359a\
68565b619165985a7108f7b1771131e26f11d24177dc9a3c23582060cb9ff63744ac\
                    dac02a48527dfc2810fc49bc1223a240d870fa2d668c891155
```

HPKE-3-KE with default aad, default info, default hpke aad

Ciphertext: \

```
d8608443a10101a1055057c9f2b6225deca6982d8f501953628a582168e4b863ae09\
e0179dfe7368d92c0e998ba891791004ac55f05b81fca899dcb975818353a2011831\
044d626f622d68706b655f335f6b65a123582071075e8a1b304ef9edbc2936f6e5be\
4ac2e4e7ad59ad37d748fb580bb5fc5c5858205b3704e4c7fd8f05c51fde7f159e70\
                                    1aeba21c55b82dec0e42b9bf9a6a9634c4
```

HPKE-3-KE with default aad, default info, external hpke aad

Ciphertext: \

```
d8608443a10101a10550320b164a39702b84ad08f8e9b741445658210a1cda2aa5fa\
b6fde7026ef7fbef3faab763d7e3ef2b06aa09ca08b4de09a15d84818353a2011831\
044d626f622d68706b655f335f6b65a12358209e0d94bb2d354bd6a83b9374d9984b\
e125bde4ae96230eff1d10d0254e96a97d5820b3aee0a1d634043403d61ba332ddf8\
                                    fa899430e0221ba127eec76399a026a359
```

HPKE-3-KE with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10101a105508c0eca59bd53bffe5ef3b539c4ea5d6b5821e60895c561cf\
c588bbd124dbdab7bd2a19590f93e712f6bb3f745c6c8912366ce2818353a2011831\
044d626f622d68706b655f335f6b65a1235820a141613c5ce54168fc1b9d76a4a28b\
6461c8b65a14220086c3da2704ca0406695820bdd73f84ffb4d11d4d92391dbb34fa\
8db2ee4f81299203f529f98ce52e49de86

HPKE-3-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10101a105502ff672957f5586fd4a08d0fb045c6639582122758f93e861\
925e3e40dab68a550046043c0b6183690696116b93093888e52ed1818353a2011831\
044d626f622d68706b655f335f6b65a1235820a95c290e4366159abd514194334177\
5f58521efc1ab15015bd368f10bbd5a53f5820c540b2af48b165f272a72d3a133846\
d6915627cbf3a37db34a312cd86cb5a9f7

HPKE-3-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10101a105503a42e93d02472760b51fb62b464b4b9a5821ac8e71b022b2\
4b2288579ef0c1c854afd28b74e9e784fa5d2f1528c477a0c90740818353a2011831\
044d626f622d68706b655f335f6b65a12358203c9268ad53ea237b648a1806d667a4\
5f74dcb725c7777fc558d4566cdeaadf605820dd50847d57ba2906c45b3365153bf9\
3cad6dc9dc049fca46d91ac07a5354c069

HPKE-3-KE with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10101a10550dc32f24a9fcb7dd8da12372b7ccdf3505821ad11bf317640\
a6c1051ac0453ef9994a9a8a21dc34f2bb8ad17ac17bd902dc420c818353a2011831\
044d626f622d68706b655f335f6b65a1235820bbca5f776f840f0c4eb5f1994c9989\
2fd595f9df6e45787550a1624d3a3468255820140a9c10b359b476982d18f7f0fe38\
63845501a020fc311b8a8a513df115acd6

HPKE-3-KE with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10101a10550b224ec850a723d60cd6fade231f03a7058210e151c37f85b\
ff7b382fd4158339d10bc1746a7d26dccf21d37e122f45456641a0818353a2011831\
044d626f622d68706b655f335f6b65a123582056e5dc366ead34698fc0b4071a7406\
c6910beb1e8292b3dd9436ae34b653a0055820edd2498d3dae8e148360ea18f07d59\
e0adb4d283519d9d4b3820c9148f5bcd5f

HPKE-3-KE with external aad, external info, external hpke aad

Ciphertext: \
d8608443a10101a1055062670829c5fc6f5cdc48faab828dc09e58211ed421e07f98\
eca98f1155790c790e6710a53484310a47f3b7afdbc77b5a7cb5a4818353a2011831\
044d626f622d68706b655f335f6b65a12358204370a8614e9d71a82998498493fedb\
d974def1ba2f3ff34feb5c8bbb1898484c58201e284bb8a5f35206429c5326036316\
a4c4dcd5772b7ed9dffdd1e3cfe02ad9fb

HPKE-4-KE COSE_Key:: \
a60101024d626f622d68706b655f345f6b650318322004215820a5922a701eebdf66\
5a7877e32b0651db5d3ad8eb4be792f2dfd9d9ac5d04956123582000f28ee18a4ddc\
dd4f318dd88ba71efe0bb68002015e9c4879e99edf4e9c4b60

HPKE-4-KE with default aad, default info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c06361aad32854c99401d9613582107f6ed7364a443fab2\
dc1710de081e8e535d621ab98d45e92cd15ecfac213dff6d818353a2011832044d62\
6f622d68706b655f345f6b65a1235820ba1cbbf9ccacde066147b54ea4c28806c41a\
dd5495c37295d520d5332d247102583022d9d848d1e3603de56c4a3a0ece5ca75e6a\
51b929d28142a53067f6169001da5320bbe23facb5c4f6f428f35c4af1cb

HPKE-4-KE with default aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c9c4cbe7dc327ce468d50bd9e58216f145b2851c502d5b0\
c3ce4bcd99e96299e2aba606e2af70338c91b31c68a7613b818353a2011832044d62\
6f622d68706b655f345f6b65a1235820e1e167e1917be9aa3090108e145a03d0fd20\
4242800da4cab096573fb5f4f164583071397ad12d2a974dd23eaa363f40d3c59c6e\
706b6b4c8d2a4ec4a6de92e860c30552336591bec0a8e51fe293bca83740

HPKE-4-KE with external aad, default info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c3d211831f229feb2b70db089582105a0acb03ea75dd18d\
53bf05e648260c91c890355985a11d527eb8c4189590b08d818353a2011832044d62\
6f622d68706b655f345f6b65a1235820c18fb4814d1f116b82836aeb213bd3528ae6\
a2417da08cc5abb6b15575217b345830ec408b0789d9097e9be5101e9e84a3076089\
55570547964d2d840aecef45909361477ce85b012d4ad0d3bd9b2fad9101

HPKE-4-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054ca3a0a911408279f90ca90b0858214cbe2773a824c0e526\
c75dfd20285b2cef1d39605ff9b64e4f3e16ba943e237263818353a2011832044d62\
6f622d68706b655f345f6b65a1235820e2d8f154d1a40c518058770f0f345b9d448b\
418397ccc42d2af887ae9c137210583016932c4f4a574d2ab03dc02729dbaf404330\
a21df11e1ebc2e52c462e48fed0a0cd3219bff3e9eef5fdc19d92aad161c

HPKE-4-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054cd7ab613f6cc110a022aaba5958210a1b3f842a6c339bc9\
39bea0ec5a0f265777f67d8bb4b826252b6252ba4cdfc6db818353a2011832044d62\
6f622d68706b655f345f6b65a1235820f8fec4f5ada1c6f6a6b1ee9b89092200c8a4\
81daccfb51fd47b4fa99709427465830cd5b8342f3727d7afa5b981c7be6edeaada7\
28833f801ec658cc77763d6de36af71122a250c5edf7df853c54dc486fe9

HPKE-4-KE with default aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054cff6ec38f45005c1d36229a2858212291e110fe7cca10f0\
258abfa31dbb9c8d019f88dc297f7a1641474650db40ec82818353a2011832044d62\
6f622d68706b655f345f6b65a1235820e6fec434687bc3b5cd0597c4a56d76c325fb\
8c21d4dfe8e7aaa47b4572c58f4a5830167720e484a884f32f961544bc2fa865cbbe\
e622c73bc98424871e7dcc9e7dbeb8b50edc8f6bd499a0e08b9bdb916841

HPKE-4-KE with external aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054cbde082e4f5995e02d5ecfa6d582116efe45e6ac45104ad\
f41a3d46a627ad743f8178a0a326ddc1431d030172bcd35e818353a2011832044d62\
6f622d68706b655f345f6b65a1235820a7252d0db32722de877846fefc59ceadd29e\
698db423ebe3577cd6c0af195f675830520b088ea067725bfeb093abd31bb7516423\
3a499171855f3d68cd93cad466d56fc29119c475b10e29a69951163383a1

HPKE-4-KE with external aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c2bf44cdd95f7de613426342c58210fee2d9d95bf69355f\
f885451849a0dad422dcb3cac652e11413bb87a16da8c333818353a2011832044d62\
6f622d68706b655f345f6b65a123582063915e953e2d4a681251ae4e19fb61d4d059\
1cb6cba32d989ec97d0d9c65841a5830c8fc0abec5ee853241c63be826b682119856\
d9dcc511a0aa4ae5121555afe61980716cd793312fa52ca130649e8b69f9

HPKE-5-KE COSE_Key:: \
a60101024d626f622d68706b655f355f6b650318332005215838448 9c1479ccd3534\
3a90b3e1cb4922f73d9d611f12bf4abe9f76fcac6a6a974c0941fa602dfc29fb5c52\
b3191ea896162718d2ddbc97097e235838785cb877d73f034edaaa14d66dc3e10bc2\
8d3ee5a290310c89eab7e347a8221887496360 0cf36850a389325fcbb6e4477dcc0f\
1b65e860d9

HPKE-5-KE with default aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a10558204ff93b1cf652bd6b3a78aa66aff3cf0763c4607fec098d\
0ca74a6036f299ebb2582146d06eb19d65874a09970bcd52bca5d1ae70aef68302b9\
5771ca57914b3100bcd4818353a2011833044d626f622d68706b655f355f6b65a123\
58384099e311ea6ecb8c1bb579b3192634863e32c15374551b7cd76f38278cb25065\
4fc7bd8d5d10d3bf020f5338fc89cb27b1be472ef2687617583092b0973eecebaefc\
480ad5e606d6def1e78d22ee546831e49df7b91382b5d34e41e9262303525bbbe921\
afce1d3b4c25

HPKE-5-KE with default aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820ee0407489df27075ea6c15d2c798ea0610e969b18d3d30\
1867abfc60d14c571f582102485c143d33f60e3e3e6bf52e24a317991ef505085bee\
6b593d85bfd763dc7593818353a2011833044d626f622d68706b655f355f6b65a123\
58381e027e0f01b9ce80513f2945e81582922f593186a4ba6f015bea962a5856e321\
00552f29a141e7ea288f379a2a3e6a6204ee5cbc37970c955830082a8b17e3e65548\
20c31107b8b50d97caca42f6fde213a4c7494257d019e7d3bb00410301d3113d8114\
6f64b1d649f7

HPKE-5-KE with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a1055820add0563a9487a69fd84c520c1b403ca469bfd31b3888a7\
badf1ace338489cc9e5821e5f53fb6e1baeb79c1e42bc88e414d25bb0deecb3fb75b\
5e5ccc71a5c514b1b33c818353a2011833044d626f622d68706b655f355f6b65a123\
5838a1cb8855ddead0ae82b4e87df4b399b7197b2f06d5ba0f4b053b104b760db9e9\
b2d53d924d403bb243cc2fa51d9d0eabf20150db69ad419b583014330834835b5951\
ee83fd58ebea9bb375ec5df0b373eec65c15a1f59ae7fddc8d16eaf11f67d98dcf4a\
b833b21e2669

HPKE-5-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a10558204427ccf295f6163509a646b90fd9c40ed7a0fe9384cb10\

```
   36a17b813b237524f2582103723c06533e16224e98d151063d708c7dc4c09b53b872\
   346c6083adee8b2fb43f818353a2011833044d626f622d68706b655f355f6b65a123\
   5838d6b7013b4c9f9b44ea55d9edaec03be7591cda435670066f3878c89ea5d49005\
   f683d0dc1a8c85dddd9a79c8ff5993876b25dbc5e1231b275830ddafd2a0712a6845\
   f11970adaf619f844eff75c8a381f80533c393fc5dc114b83a902c672af3d5390a4e\
                                                              478ec6897ede
```

HPKE-5-KE with default aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558208919fd6f31b0cbbdda4875af585af67e0c0823cef6d0be\
   cd6802ea3ecef0c9a55821fb88175fd00fdda16def7f4110899c4f9017c63ec4b375\
   73f0dc4a97b6d9527b22818353a2011833044d626f622d68706b655f355f6b65a123\
   5838203f42bbdb8cfeb59f7c05a1580a885554f5ef8848c76a04a011b2b9521f08a4\
   bf7d159b8f01762ab304ff57637400acc22d62746a942ffa5830ad7cb3c1c79711a1\
   1aff71f09a29228341485376d569fae65673c5a0ba0a4dbd5b7904ad2cea0ce1aa2d\
                                                              af37adc25e73
```

HPKE-5-KE with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a105582085aa9e38bdbf1f258426becc819a929c55e719cc75227b\
   a515ae09a8267bf4925821f5d3bd70c82cdcd96595efbc671919c2698af5ef96667a\
   b16894f6dd7ec5dc6a95818353a2011833044d626f622d68706b655f355f6b65a123\
   58384d97b5bc0f662d782b9122f113ca655d156674d3381b45f61a55f6f670771bba\
   eff2187824469740f49ed0ec5bcebcf991851bd41fa95d5858306e0bd0c92cd5e4f6\
   c74a34319a4738051e96cc3ddb69b6ef8dc0710918d02940c10688cd828b303b4b35\
                                                              95d8bf2c0056
```

HPKE-5-KE with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558201806b9f94e356ed2f2c10b0822ff35b1504dba0b5a1db8\
   af9b8e0d5c3792068058210a5eabd5d60b81eeff382c7598898e4fca0efcad5b27b3\
   cdc05ae412b771495d4f818353a2011833044d626f622d68706b655f355f6b65a123\
   5838e3fbd237c85215a1d247176714e27f198a0f7a76e83f5116c97b218b5204c300\
   06dd08abf94892a44bf00a358f67822d3bf92d331b6430ba58307fd5803d162ea9ea\
   adb8fc37b327d6b4a526a07ce4a13697195579ba6d7230f444568d1b731443f3bf6f\
                                                              f5d4f2c4e375
```

HPKE-5-KE with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820de43c2aa8af6fcaf531231f6403cee6800fe1e3d0fc614\
```

```
   7e090c1595fe8467ae5821f29e9f566935b3ef34e043891c935094dc1fe4984dd30a\
   ac5877f98b0759055303818353a2011833044d626f622d68706b655f355f6b65a123\
   583803884f02e4d336a193959844a73db0b95f2511121886dc7bf82b945f8337c025\
   56efa96811b63cba029b13c60e9581a38366d6366177db4e5830eb8e0f189adaaf28\
   7119963680320da63ee1dc219982e7145cbef6437472b977344bdf141ceac4c4521b\
                                                          cd971c154ee1
```

```
   HPKE-6-KE COSE_Key:: \
   a60101024d626f622d68706b655f365f6b650318342005215838253b435291775cff\
   909b2227b8bd6f539f521368b33871022f95713b4433df21becfffeaba9d63e839e4\
   3413e92689ead254feae3d7aa8e72358382c6894f63ec5d05047370d9415d4c0cd53\
   ee2633926596788a41b5ff5368733b7d9499c391b08ed7c1c3d750c4c5af2ff03a44\
                                                          278c7c40b6
```

```
   HPKE-6-KE with default aad, default info, default hpke aad

   Ciphertext: \
   d8608444a1011818a1054cdc91705d85a0564634c28b9458210a72029b5ce3c44b85\
   28862f5f5764e438c7d723cd412bf65f681f7382b2084ecc818353a2011834044d62\
   6f622d68706b655f365f6b65a1235838e2d1ffe83d043f7fde6f14658e6ea3827e57\
   8bd060def6491ada7311a260c4b3f0734b97d3c3b8cd50c6f667df518c3d6a9d60c1\
   d2563e8058300dc6bf0ce7314032e954f5eac21d5646b3d8a0f50a1beb3414da3e60\
                                 333d15b9edc7b8f9615bbb411b053268968b0be3
```

```
   HPKE-6-KE with default aad, default info, external hpke aad

   Ciphertext: \
   d8608444a1011818a1054c161f8d0c535147d452345f7b582105686a0762c213b2ab\
   775b71f5752e91a14ea742afc9be7d4dcef77408cbb3b474818353a2011834044d62\
   6f622d68706b655f365f6b65a1235838a06b9b5d98702887a49304d2cd174da29014\
   08c3a012cbc97c8548afd5e113a8fbbafa02df731f4f9ec314aacb389766defccbe5\
   087da31d5830395054dceb31dbac2381c37bf04f1db0f79b184482fba8f92a7ce31c\
                                 b4fae7ebd9c4f52a1730ca3cb76695af047ff6cc
```

```
   HPKE-6-KE with external aad, default info, default hpke aad

   Ciphertext: \
   d8608444a1011818a1054c2eaa13b8a25bf8e0971fbaaa5821abe79da1ef9aa997ec\
   00bcfbad70283b1c82874557c74f6d411742f0f35534c232818353a2011834044d62\
   6f622d68706b655f365f6b65a1235838c88eb6e1e4a8901cdda6340b0f6f0a22aef1\
   eb93b8c9b0396e0390e4e11ceace150773c38614076b4a65890cfd87376117e92925\
   80ce9ba55830a1fc1274c68b001884bcc2c0bacfcd1c16ae3bd12366edf28da11adc\
                                 ede0a5ba7b02550ac305f74e0c2e6993eb980617
```

HPKE-6-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c777589e4029d40667c3f5113582178d2b8e3a9b4b7a676\
0a5d442476370bb171134189415ce45957c2325ad5e6e8fa818353a2011834044d62\
6f622d68706b655f365f6b65a123583805ab0e5f240b5a0add796adcf658a865eac3\
b661b19b45ec84d19d87eb4ce789f11e51a6641907d71a79a7e9e00372f8b03185a0\
aaafc23158303e0e1cf5cbe04cd7c99c804ab120374f4a53aa31cf867cdc6222e1c3\
3329e271e2b10723e09c3e58e0d5440ff1674877

HPKE-6-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c79c3898eee0f5d0c139ea9d1582122c443c0fb066dddd0\
05678ab35d2409e37145f3a2c660212b307c567107d481e8818353a2011834044d62\
6f622d68706b655f365f6b65a1235838c0d3df69fd572cc5b4ea701c50d3251b9aa2\
8620a0885b9377b2287c52ac6a25381921c735c82f0d471ccf8eff4f7096336db9d7\
6231c8fd5830152b3a5f3833c4aed2d9d5a8e15b782543dc84709ac4706379eee3e5\
e334b0b9f56aec8770765c7b26bde266af673208

HPKE-6-KE with default aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c342275d497bd01b56282649c58219cedf5c89b5f3e1bca\
d64725c0d90a2184eedd1e8b7138b80d8c0f5cc1abf89e33818353a2011834044d62\
6f622d68706b655f365f6b65a12358386e741c2825336f78c666cc7ad296920b25c1\
1b6d482b235ad243172ce301dcbcaee23a076beabc6c282f2ba757d50fec9c6af0d0\
706d98275830e89f61c2fbdafb5573cfd12220dbd4545fa54b4d1412833db1b56ab4\
84f486164138d9b84a2b16bdba3c7993ed8bd4a6

HPKE-6-KE with external aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054ca9fa34a4e5f1846e9afeb0a258219e4b6d9512d4d4fde5\
c5ca94d3babd478132a1ba3f92448fd25dcd26a483c2cb25818353a2011834044d62\
6f622d68706b655f365f6b65a1235838a23c08691c61200eb23cf535ba0f0252f7f0\
09f9ce24f7df7ad71a974536a01ff52d2ba12345d74bf751fd5382166aed53b2a786\
35d4aa7d5830691f2d587f1748e87ba11dc1c10dd7602712789e85eaf63990d36a00\
5ceb9041c119c8629d0cb366a8aafe0473a56b4f

HPKE-6-KE with external aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c226a8d618d7ce2f1a116e7a8582120c2989b87f908e508\

```
443d80c3c7d35c3860da0fdf77edd51846874e38153d9b43818353a2011834044d62\
6f622d68706b655f365f6b65a1235838ae833f2ab29229c1fe66f025d30facde2e87\
71940275f0b67934cad41822a7325ae9669f3cf8dc11c034c9105d67188a40d0343b\
ce70bcdd58301e78d4468b91719a6f1e6f6a2e98efa55f92a0713984e4fa677f44f3\
                              9acacf65559af142b5216786588123e8fa3d73d8
```

```
HPKE-7-KE COSE_Key:: \
a70102024d626f622d68706b655f375f6b650318352001215820551 37ef3179b4bba\
4326a5e73ae0966d92d2ccc7e1714a66fba562a1c597a08d2258201daa17ff95d717\
128dc944069f4060af5981575734f1f847e6bd6bc30603cd6123582073294f0f394f\
                  08becf7358ea89c0cda596cbd9705a6b7c6f0ae8d70a9a85a913
```

HPKE-7-KE with default aad, default info, default hpke aad

```
Ciphertext: \
d8608443a10103a1055820b4ad67bdb6937286a5983cc45f54b41e3c7a0df82e12f1\
b7e7925bde628eca6a582142b48f53df1fcc1caf84bc4820476082e55146a04e1726\
aabea65114de8329bda5818353a2011835044d626f622d68706b655f375f6b65a123\
58410433c37c35e3c3c333aff1bc62edfa2765518c7cd4e025a8b23ffb3fcf78f13d\
051cdb830d89f97e1567f27362420b63d0cbc4c1dcf6df18f2c599e763c575c3f058\
3029ee7739a3699d79e1ffbb652f99741a1e2d15cc05bf68d8a9f55bf3b77e33c22f\
                                        5c7bdd3a842031325f385f6ed972c4
```

HPKE-7-KE with default aad, default info, external hpke aad

```
Ciphertext: \
d8608443a10103a1055820812362136428 0f31244476af7ba86971aee01f51ec197f\
63127acc2845c1c23e5821f71f66a19a63bf08eeae9cab07ab5c8454816f7370a6c4\
f58630647a5988d5b823818353a2011835044d626f622d68706b655f375f6b65a123\
584104ba669a6cdf24f9eb902c0647fa7011c764d210f10c4de956188b2137829b73\
6b1d0ec5e6d71ca286d279391a4d129ba3cd904edc3d61ee98cf45528b81e3f9db58\
30b2e8ad669f478914862185c6ec6f70593d29b8e2ec523b7d89f9cd914ad34ca775\
                                        2fe3629b4680c8466942adf7a14ac2
```

HPKE-7-KE with external aad, default info, default hpke aad

```
Ciphertext: \
d8608443a10103a105582073a819dcb519a63355b711e7ba4bd278a25a5065983b94\
90f0169c3ca1a6c446582159ef651b16dd3eccb599906d27a3f3d06e09efeb0bae14\
7f5cc3cd8ad876697401818353a2011835044d626f622d68706b655f375f6b65a123\
5841044fd069ae9dc9a029979615eddba8e946dc4087817c8e02680dce2b0415fa88\
39904afe73c3c045f32a010603ee158deb96e3c5a97c501fecf9b29b8914d4a71658\
304c694a5e09eecc922621d3dfe02b7e5dd0ff7c174ad6001f24a0764867f8a3c18d\
                                        ad15a51d85542ef85b0753f4654cee
```

HPKE-7-KE with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820bd1930d292a90e8c717057f53fa6bf9058e0b9d3e6c013\
c6e19061ad839a47cd58215bc9e46ef5be53dea520078ae2e41ccd5b9b5419f273b5\
dd8c35459184eb8a8512818353a2011835044d626f622d68706b655f375f6b65a123\
58410438bd711f6e6cea92c0008fa4b6e6874d6466ed63ae3031a87ed03d074b236f\
1b07526363c63f5d90ef5ee45a41e00f726f3bf1c61a0de461f1da41545f055c2558\
30795f8c1b78115df8af58f49b8f5fd94df744f50f6f36836cd15441dceb88c196d0\
a4014ac8ed81832a6a106dc974591f

HPKE-7-KE with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820921ada478a6296b81674ec480e27ff77ef0cc691967b23\
5920c45be58079f1fb5821bc50d6b7348a33fac2aff9d9b289dce83c8a60050309fb\
6f432d564a6e6b909366818353a2011835044d626f622d68706b655f375f6b65a123\
5841046d92481c24059c5d5ae998048868ac975a2d87136c62dd53fca5cce700f45c\
2c7da093dbf84545880f8f81fd51b9d73622153324ffe35ff80ab9edc828b6db9458\
30f6c919e08dc6f0dddb0bec457ceb6726f5a3c18d97389d96d894b553e602f0d484\
49740735f900b1d6fd7e4003457ee8

HPKE-7-KE with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a105582003a092a86b3432027f1eff4e1cad509aa786f73a5148a1\
7d0071b7798a5b2206582153bbf01e70aaec7dfddea48b28dd511afadc6edc7524bb\
e449ac677c2136c994a5818353a2011835044d626f622d68706b655f375f6b65a123\
58410481bc8c8fd41e43207e76e38a808c04c69ac716e4e95d712732df1bfacaf548\
039db70e5ec9374f6744eb88b8d4480de1caa03f6fb7a3c9ae7b60f7715e4bada858\
309d22782eedf0f851fa507b74fd05d1bd7d995e15bbd5162ef0ab08840cda5b6b55\
a7ed79500990cefe94a8f312518bb0

HPKE-7-KE with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a10558208e23d1384869e09d81b29aca4a6c914f5b6e1fab762986\
00146e7b82bcd3349558218784389faa384d51bb2488fa493d63f2e3fe72634c9994\
4c5a8b7bb32e6ad4b5fa818353a2011835044d626f622d68706b655f375f6b65a123\
5841041542669339ff82f8c64acb331de9103d339042bf8bd61d75056cd05d70d136\
c2b481b1dd2b220196228a1f4a8f70991176deb68ca4900a698878900cd3bf763958\
30f611c9c31785c2d7bcca2638da2375131fe2287b72f4b4b93ba1d8424ba12fe6a4\
8bb8ac5d0bad1cf7b8f81cf9d11bcc

HPKE-7-KE with external aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a10558200014fd43c613aaa6578d3001abeef3c028cb1c3079f21f\
f6da777a9c586b985f5821333e109d32d4cb58224e3cc3958b0696233e4a824586fc\
953056b55fb0f988f9e3818353a2011835044d626f622d68706b655f375f6b65a123\
584104cfd2686a4ab624d792050d5fefd9f128467196fc437fccc02643ed770b1944\
502d9515c98bad76e6b4c3c982ea8192124bc3dfd61901af0bd9676e5e189a93a158\
30334cdf07561053063f668bb025f4d46cbab5202de419d34ce5e49290c886763b17\
0fcc5586f9eec223a6a94ae484542c

HPKE-0 COSE_Key: \
a70102024e626f622d68706b655f302d696e74031823200121582066 99b067898b7d\
2d37db0da3aecad4bdac1558870b47d67d080d6049fb81752f225820b01b6da1f210\
f46e20e2b552a80f4f6b9a3adad34a6701f73fbbeffb174cf7412358206716e93d65\
94fbfd27016daada9ccc8e6ba2eea0e103e3d7ae22278f6dfe124a

HPKE-0 Encrypt0 with default aad and default info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e7423584104bb6385b1cd50\
09597006380ba2de0f66d293007755640f57b13a234bbe7241cf6f91f45469f85e99\
a13b9567257b7025298bcf6e7f4c1f29ab5229381f4b99e65821ed584cb52cb37201\
35d1aed21adeca560e00effb931cf17f9b60542abc92e80b63

HPKE-0 Encrypt0 with external aad and default info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e74235841040c483c4a0f7e\
41e98c585fdb19ab95789ec6f7f6fe3e7e4943e3e0ce147e42c0688808a3284f779b\
d374d2a83e72d0248e3c6339a932cabb35c084071b75670a58218c9fd85ac5f111b2\
ef077872bcf72a7222a8ed8bdcf6f4036f304eb03c75450067

HPKE-0 Encrypt0 with default aad and external info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e74235841048ab08975a473\
b7e85a8796479a986b1d57270074ab819bbea2eb48a666c78fd4cfa1558f56dbde81\
848b19b1a2bf9a8438dcf8e4a2d800bb155cbb6e9b41956e58217a8a794081022469\
dab987927fff8e642d7f2f44b96eab7bb5b78b8fe7b5e6f2a5

HPKE-0 Encrypt0 with external aad and external info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e74235841049d1716049cee\
3aa5f23d2b3bbc96fd251262a97d3b0dbc53eac742b8c89fe887af7ab816ca8aee7a\
bacacd1a2ab0495e57aeff22611139d1cf894a666529b1615821590565fd461c31ed\
bfb529c208c29b87c7c924b9c570d8308cb006f1c86b646544

HPKE-1 COSE_Key: \
a70102024e626f622d68706b655f312d696e74031825200221583083 09a370b333f9\
56c1cff9d94e1ef8aacc2808ca898fec0476d9c132893704a2a4ecc88bd002e2c713\
83b97bb3ab65822258304b2a3e1b2fc832c136aee1632f967b31f5afd0a32c8c9766\
d0e9d0e4e2560a905278b0d9965898b3fe4d2165cfa1b1c0235830bde0361bbbf278\
ff3286a36897b2e674286870981ef471c2c81b55a3b82827800d32b34da68993cd59\
0ff06e0788aeaf

HPKE-1 Encrypt0 with default aad and default info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e7423586104652d74d6ded6\
32be58dfdf81aeb3e7f365f86ad170c509dac27c2107551538c5b4ea89f36b6aa431\
5b39ec96528c7b0d049f5c70d801e6d522e7a91f559b52eb2b706d93f3f11d1cfbd1\
906a5c4c3380150d46926c3f469526389ecd0e1f9db6582144c5fd46930ccf302b53\
15faa3337d76c8622fe8ec6df824ad7e376007d52e02ac

HPKE-1 Encrypt0 with external aad and default info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e74235861041063 88d784f2\
cdaab13c77b6f67d0229d552ce2e7707dc5a17ec01f74637d4275ad2a931ca7d0062\
f7bf45be096cc29b7b2ba96efc974ce673c29d47a7a2db63eb0a5c55aa6c5abf9f72\
8f7b4f29435437c59409584a61cbcd4a83a1f876fe1c582174d9cbc04fd6fcc0ad6a\
a587a38f21be70e381f4b8de184c4e7e3fffa246418ac6

HPKE-1 Encrypt0 with default aad and external info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e7423586104fdd2d7553bc3\
1201851cacb28ec135df4ba6f4cbc92362a18d3024ba3944a74ff46bad3cedca9721\
5c8e5c337aee23a04bf42d777fc2a38e14ffb0337a983de8e6fdc28714b527180733\
33aa374bca263d1b270bb61098be1032271cf5e166fd5821124c3c9acc6700f6faab\
0503ea8306ccafa6ad341e69017b5d57877bba7c8d7c4c

HPKE-1 Encrypt0 with external aad and external info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e74235861047a2c8b275dd4\
8bba7666452c6ee4db7e4d9c53790344b446223753d4fd6c15b6a513cf223af09355\
62820f9336396edd5a096498dd7c49cd7dab87a86cfa03ef507bdfc3de2403569cf0\
2bd702afd76c756d9aae114ba4dc5b94ecd29f62d383582171c1a6219cf72d7446a5\
9c00c5fa692d17c0efc3b92c34a2ff0cc56adcea9b65e7

HPKE-2 COSE_Key: \
a70102024e626f622d68706b655f322d696e74031827200321584200 3c20a6d2990d\
ac871dec57d8f31283ca99b9958a00e92ba43b1ff9186813f750b01333ef1f311960\
1875065599aa48884425480a4d20e8e39bc84e98f745d91ed72258420058edb9dbcc\
ddc1594dc9003ab39886babd7ef7d0046aa72eae0f9c67b794c251c8a2309ae05f6f\
1cf4ac06045ecd45bc335d5c316936e3968e6ed42211bfdaa859235842010c50be4e\
0322d8bcb1424750f6ed3b22bcbe25ae9745a868688dcbbab97f522f5a95d0712b8d\
9ff48a5be6650179fd4e59913c76b1b28af9605ddb294756c2effd

HPKE-2 Encrypt0 with default aad and default info

Ciphertext: \
d08344a1011827a2044e626f622d68706b655f322d696e7423588504009a6b229af0\
1086f3d269bc53e80af50c51fa34d7919137f7ee341773859909eb8a42d528d3cb4a\
a8d11e2b0456a1eea80b77a5ac960c22899e96bcd5a41b57277101eb8043867d62f6\
4de2c6400d5239b17d5fc1c1544eba22ee4c2f464fbb88a0b24d532b7587727cca8d\
93f5a39997a3cb9ef2490ea1d1fe46a45fa96fb2b26bf6ec582199e3fd2ccf2add11\
cd4be8ea6819e00af7b3a37d46e674ab6028376ff99125ce2e

HPKE-2 Encrypt0 with external aad and default info

Ciphertext: \
d08344a1011827a2044e626f622d68706b655f322d696e7423588504008f1fbff7e1\
c3960d04ed74bdd86b19c995af96468008b7ad62e9ca2d060c222fda6bd30831e04f\
e797b6a87f7b0eb325a2b0b0e5331d302aaf69aa386ec9276fa901dc4056f6331d58\
093273ed605c1e1e32b2e368afe71390246f8fa20d7ffc6e790a06d86e588f658bb0\
bee30c523101b351433ea1c611cd0d2fdf6e924fce55eed2582120bb19765d3444e4\
3325d1c8a7d4a510c4a85a88cf3b9a2763e477f9e064e08510

HPKE-2 Encrypt0 with default aad and external info

Ciphertext: \
d08344a1011827a2044e626f622d68706b655f322d696e7423588504006dba8c9caa\
d42c743aebca073875e1e5780c828162072850df9a8c83975f64dc4466152a8bbd12\
d7bef79c00a589a0b8bced83b8fa82fbc1a50a33e0a54a1420ae010b5dd6dcc9bd0b\
af5101485f37d011fdd902dad39843343bb57be244e566047a60d54a15ec9c8d25d9\
1b97ea7be7a1ae118898ec8c273d88198ba4d0f5e74ec14b58218e160a01123c22b9\

a4f4859a9d101bdad6ce576c6cc68343ec54f32f644facdba2

HPKE-2 Encrypt0 with external aad and external info

Ciphertext: \
d08344a1011827a2044e626f622d68706b655f322d696e74235885040100fffac417\
f1ddde4c2f9316e7031d73aeb7e21e2223da751c310971d8d78861fe437facaad58c\
2a72abc8ffd5c9c052ce345c7dd7a871204f8d90669bc8a3679f016ef52865c7bc9a\
221dc67c1a9c12405943772a7db4658c8855b80b6883812ba92017f8fb98bf9bad12\
ac14a7e2eaea2c7fb3a9513e117ccf69c3e6998abd0e3e2a5821657d17e9ca01ee51\
f7a88a870ac0719e2c1ae8d0881e6e9c03ffb4834d586aa98a

HPKE-3 COSE_Key: \
a60101024e626f622d68706b655f332d696e74031829200421582085eb6351a4e93a\
49953e1e23ade9504af68a73196a823c9a0654bf98c7536a7f235820f0b8ece6e393\
8430f36798eeea8206d0ac5e0577349ad63843cbbb63bc90b849

HPKE-3 Encrypt0 with default aad and default info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358200a97fc27b9542a\
666479ad6635d9d5988e2bb187db4f8b3b48f60f2d06bac46b5821f058dcbad9bad8\
553fd6cbccfd50486e33dd96557d5805c6327af6624760bc7a1b

HPKE-3 Encrypt0 with external aad and default info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e7423582093a055592c2978\
fe4c7424e649938700ead043668b0a12c4233350f7927a250958216ec61f83f6fab2\
79d636bbc78bccaf9d06d34b9f39b0d615b26066c1c584fc05e4

HPKE-3 Encrypt0 with default aad and external info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e74235820b9a5e203033c7c\
5d15bce2c35cd59e24db38db2114b9c5d16edc5d7ec4cfb54f5821807a3046ee8c72\
5701d5e9bf5472772e84b5a2cffbd4b296d55af264da8b14b87e

HPKE-3 Encrypt0 with external aad and external info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358201d6124b3462a25\

```
   d3ed374b88a4702afa7831aafd81af5c8774eceef569f0234658210fcbc960c3f6a0\
                    49cbff49d881fff00a86152cfbbeccdeec111fdadc848665b9f0


   HPKE-4 COSE_Key: \
   a60101024e626f622d68706b655f342d696e7403182a20042158200191a45e724023\
   3a4bda72ac8b38283aea336c863c7d5856b7df263038bc69072358200838e90c3407\
                    649faf0bd7eeb3e5a9fd7c643e4cb72b91997fc81d26d2f1de49


   HPKE-4 Encrypt0 with default aad and default info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e7423582081cbeefeef0b8a\
   8b736f700fe52ff25f0cfc7302e5075a44b95e7cf5a82a96775821e5c0ebf3de1016\
                    b0fd33f41c0774d6b283dd494537c729ad7decab64bd5c1f43e5


   HPKE-4 Encrypt0 with external aad and default info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e742358204c41250100e5f5\
   05dd0acf8830ff1d22e7954d8f6d88d59c809c95d903849c4658218c99cbbe71f8f6\
                    95e6e79dc6f412793c3ea9d1464066e2d08aaa27b5fef24ec144


   HPKE-4 Encrypt0 with default aad and external info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e7423582004aa6884ce80e1\
   88a0ef5496c24f6798afde8c8dc623bc2654ce836bb2b9be4158211bc91f4db16f81\
                    fdab012e74c00ae5353eb258e433b8ea4b28893d7436fe7615f2


   HPKE-4 Encrypt0 with external aad and external info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e74235820bcf1e847f43e3f\
   4244751ce5e4ac782fc5270310590a3cf8fb825e5ad6be54145821e9c1313608956f\
                    65a12558a94ce3fa04ec84ecdeb2eed4eee2a4fbbe783cfcfdd7


   HPKE-5 COSE_Key: \
   a60101024e626f622d68706b655f352d696e7403182b2005215838fa09d4a5d1fa3a\
   7b2b6de43b08c715283d7425b80bf8b628b07d0d077283aa9c1507354e98c087688e\
   8cfe7220be5e2d44509b2fd53b24e9235838b07f1d8cb1d2f3d5ba62c0ad5a1791e0\
   fe79f6fdb9f49910274aa184855b67850ab2a53b39b131d07bc3d4e80a4f83b1c9f8\
                                                        f5f97f1fa598
```

HPKE-5 Encrypt0 with default aad and default info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838a7887685085eef\
bcf8230ce60ab6d18c01044807413f38ef1203b73b8083d37c3474fe2e822945c77f\
a011a4c808f55fbed005c8e90a90e4582101dd9b944c4e051fa9214aa99296a83f81\
c04642f1f6aecd6f9304bbe5a92954f8

HPKE-5 Encrypt0 with external aad and default info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e742358388cde9ba79de945\
37b33e121f3c8d3c5a720c9d3e5eaad0f0e0f84e323d592d20afa87a09657765d5ea\
57b27659366cfde26a80d817e5b6ed58213794aa4fbbc9807f953c23eed30e575d16\
e83b488a521b03a7e737ce9a6f7e90e4

HPKE-5 Encrypt0 with default aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838ca713a0271741c\
ac564ae35b5278b343ce9b3f0f2a5379a0f20f6f759b682ad9884926185e7f2fb9db\
a541bc2a41034392e430c3f429f16a58211b393d9ba77bf79efa231d87033cf8a407\
ba249891c098abf834b63e222aa744b3

HPKE-5 Encrypt0 with external aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e742358388c4b45493d8b3a\
5cd88bb3022e3e0a3777ac3b5f480e448b509089bb801608654a984e85200a70476f\
206b0bdf045063a57f472d63c69b1a58212a35247d2dd06d3bcdf02f6d26e751420e\
a966907612e4431f44d7f792e91818a2

HPKE-6 COSE_Key: \
a60101024e626f622d68706b655f362d696e7403182c20052158380aff5f4a86fc46\
8a25b7715d066628125dad13e4243f242cd6585f89f7371a55cfc3cf42cd3405a78d\
d380b4e9f4d47880c684deaa3f8aa923583898b6c98f0d48162ecc4c0f5e09c97246\
b03564a2672e12496f0f7a0d0576fbbdfb287b5a868e5b569a55b7d3765e5685feb7\
270471b13392

HPKE-6 Encrypt0 with default aad and default info

Ciphertext: \
d08344a101182ca2044e626f622d68706b655f362d696e74235838a17baa842458b4\

```
   d082f042e5598e072bbe19b9970963ca0428a577add73c7a8d275e63f53971f4ba96\
   bf842201d1c4776122dfffbc04e6cc582157e46f77fd6c2f2cab3d0810d67b7eac73\
                                       41c0726ebaf978a8fafda78f295fad0e
```

HPKE-6 Encrypt0 with external aad and default info

```
   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e7423583851e914d34210e5\
   fe233283c2755b6a42cfb1ada1139d9ece7664e57336b03892bdc67cec396c13dae4\
   37801cca5c885901fb616a96166ce75821fb3979eea60600d09bb76b4f3a5596ad5b\
                                       194b21e713070fe7b0fa1443b809f65d
```

HPKE-6 Encrypt0 with default aad and external info

```
   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e7423583842ad024c1f764c\
   bb797b3558d9c8ed9c3559c65870620c7b56f3367fdc65bc7b696d96411b57cd47a1\
   56fb945a939aca63f1a168f1a7d96a582197c449697f868ac6a708a8f9a1b1c32537\
                                       2edf6333c87e8d5f1853e8599a7848d2
```

HPKE-6 Encrypt0 with external aad and external info

```
   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e742358380a100686fd1f04\
   0155a64da572a9e9109487a55c7fed63c68c7bb38311a7b9c48d1555e006f0db2884\
   bb4306703a9c5cb7c4a0e4afd1297b582199c40b5fcba3fa474ebd9f44326e308b46\
                                       2a2171a5c50294329284f0e333ed5f15
```

```
   HPKE-7 COSE_Key: \
   a70102024e626f622d68706b655f372d696e7403182d2001215820df717fb8deae1b\
   58b754487c5432c8ec9a140dd11bcc7cd65cbe4b728e9263d6225820a8528d614367\
   3203144a9636ea065c60761390916f2218c8db958a64e263d3e02358202343a73ed3\
                   dc2b5e110d734c8d5e7a8b7fea63849e78a8db3da48a65ecdb720e
```

HPKE-7 Encrypt0 with default aad and default info

```
   Ciphertext: \
   d08344a101182da2044e626f622d68706b655f372d696e74235841040ae250a36575\
   d60ebcd50444d99d1f1546438585fc807338d0a69cffad14d45b28047e5e4d7429f6\
   28e9f8313058535375dcf1ce1804a83b8745b2d63064cf6b5821847f648fbeb8e386\
                       89248933366fe6929e36843d7855e318c48383f54022b7bac7
```

HPKE-7 Encrypt0 with external aad and default info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e74235841046a563d7eea74\
4ccbacc9ea6df50e002d8b235fabc7023d51c75e5ba22af4102c1c20954d6cc1b2b6\
3f893d504301c94fc37ba89084d04ca59f96581d87435f215821d619e5c0189533c3\
9c353cab4db8a939225c170e840915b27503b9de88f5451beb

HPKE-7 Encrypt0 with default aad and external info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e7423584104e5f56b98441f\
710117e3d9019b5d09cde61b1d4f228353062b8a7667aa58dab2e511b922f740eb7b\
8850a5a838bcb6c16ddc1cb6d7000e7d2e2d69867e11d73a582107834d1f44591c01\
db20acb0d7f71faa793e11f7c83619a9410a97991eef3a56eb

HPKE-7 Encrypt0 with external aad and external info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e74235841047258745 1cdc6\
5749b6724a78484c69e4a7092edec45c31aaf13a1b725b388820efb2b381bab4b52e\
feb9d6d65ff69c49b765426a6a4fd7872b3691149069394a582142a32c0ba176b205\
3b114682189982e07506a4ac383067aa9920552e452be123b8

HPKE-0-KE COSE_Key: \
a70102024d626f622d68706b655f305f6b6503182e2001215820f135aa53a7b8d080\
1eefc6545a8b6262d74b74015f246c11b37762767ef201ff225820ed6afc34bc882d\
17d025cc79723caaec97006411b6b975add484362196948c4e235820182a2a509e56\
778bf678dbc5ca76cc18fce47300815540c82d4a624b17bbe437

HPKE-0-KE KE+PSK with default aad, default info, default hpke aad

Ciphertext: \
d8608443a10101a1055055ef57a8c8f1e2cd792f9e9c253a7adb5821e7dde67c8df6\
36eb9b2349527a6bab7bd575e46995b3cb45b7edfb339ef6dbd903818353a201182e\
044d626f622d68706b655f305f6b65a1235841042436c6d0ff2176e1a1a808737781\
a7fc7376014919b539aace84114fe6dccfb82c327719721efc5e8df87cebe7d0c28b\
74770a2c816781a5c88f8b6ef83110a158204ca4cc64d178000d42aa6092f7c8ef5b\
d5995a33ef7c4b6d9490b105215d6293

HPKE-0-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \

```
   d8608443a10101a10550ca918484db7e57fcd6a451579d04a91058218f4e49d4242d\
   4b03092402de93ba613f64d3546334581d75f09781a917eb64b5c9818353a201182e\
   044d626f622d68706b655f305f6b65a1235841043f245ce79f1a6674314e44010377\
   c817b3e52e31767c45143824ebdd4275a8c02f6037267b7de937ef1e3d5331000305\
   0311b33826469b3f7213a7d3a518d1b95820efe256263376b60f788d17a590b31464\
                                        903587f5ef8708016697bdd27e793424
```

HPKE-0-KE KE+PSK with external aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a1055008d4b4ba3a6b7fab94fea740ddfea6ae582145dfe705c3a8\
   85a23c92abce2e9a4ceee4913ca54c12e3c7df39a5239012ce15a1818353a201182e\
   044d626f622d68706b655f305f6b65a1235841043e734095428789dee24b83790686\
   3ad7bcef86c3fb6c4839eb76463a081dc0b1c64c504ecb319ae0c64f6a6a8b7294a5\
   b7d68c2cd12493673ecb9719a01343e7582061aa26e99c15baa82edd40265236cad4\
                                        511aa05519617cc0c22f56d455ec7e26
```

HPKE-0-KE KE+PSK with external aad, default info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a10550db52db662f81a9ae2c1cec60b79abb125821ff4bf2e65f87\
   d17e74432da6da46f264543c5662a34da8b1d63c7a04f92cf4a2e3818353a201182e\
   044d626f622d68706b655f305f6b65a123584104ac44c7268c1790ef423d607b2ff7\
   5320667e20695387db9c1fe7ec4bb97b74001f33dc58c9e56353bc67a4d6820226cc\
   36e98452e912a325755537a6429c65e9582043c8fcd50f343797fc2350b7e22476a3\
                                        9b6370fa338a7f8cb90df438409b407c
```

HPKE-0-KE KE+PSK with default aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a10550b0d6c7caf307e05561f106e44a54742f582143713d533c1f\
   b2c96071d30efd30633d18ed3891e3cc6338d05fdf922a1fc82ff3818353a201182e\
   044d626f622d68706b655f305f6b65a123584104212d6e5b8b376b279515d1337519\
   7b64d18b311d1adad0df5c72480ac5b4ce87c68016824b2a952c745132132d417498\
   15d7696a117d77384188fdd7cc6176f9582059ed1ddcfd922588e541aaaf4bd89f70\
                                        a360adfd109da2a83c5eb7b20732579c
```

HPKE-0-KE KE+PSK with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a105506024ab7fed3cf00950e794951efbfe415821eced08e89a89\
   e6184147e56c1650fd57ff514233042b6e9001170dbc060a66ab89818353a201182e\
   044d626f622d68706b655f305f6b65a1235841047aab9097da3d4c17f4bb5504d8d4\
   5f4c28ebbeccccb77b2f7a4f8f3674700554578c7a0f19586a2cf4fb0cd5926eb0e9\
```

```
   db6733752e4f43dd9bd5996554e522ba5820839a506ff751227d9ec4db931f73517f\
                                       65a3ccc9d84a9595c06f7cf07fc6bd19
```

HPKE-0-KE KE+PSK with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10101a10550fda46441c4560291a6eec9da655289de5821a6b9b3342ee5\
   49f2f6dee9ab165d7631cb2a29f0d923378638cb7f5c8e648a193f818353a201182e\
   044d626f622d68706b655f305f6b65a123584104b378a7e3362bb1becf24ae2e8562\
   66da9784e20f7aaddda2a536cc355595d888e9737891b32e29c3ab5c07eb55e4f44a\
   2631529f9a2dadbcd1c5e32d8fa46ddc58203b391f81a9aabb2683dc6a371d6824d7\
                                       8812595cba6c97fb83798fd87eef75c7
```

HPKE-0-KE KE+PSK with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10101a105507a78d1bfef768bd0739fad341f49039658210a5f55ba415f\
   a3c240ef60eab590bd91cce926c92a8762e9362bca167fd8fad844818353a201182e\
   044d626f622d68706b655f305f6b65a123584104df01fe0e86de46fcbdf83569d3be\
   4892fcbf66172b953fa5af4a4da3175b825a0a68a2497f779dae5430522942e77518\
   4c0403b6a3f57b5c49ea93775667c86c58204f835e149377345d40bddfd3e7e24793\
                                       19518a11b44ede7f24cfd059652094cd
```

```
   HPKE-1-KE COSE_Key: \
   a70102024d626f622d68706b655f315f6b6503182f20022158304f65f3e8ce5db1ff\
   24f49fe236ffdcfba3214bde3c1c0bdec78d6e35b0d59d15edb4f497a1b440c7e37a\
   29f99de5bfb922583076653c742f9eb5a42d6d4f88a01ba09cb8cadad0eb570b312f\
   60ea5ff6aec15c927af3fa6976c77dec3141b893a9a697235830ec601bec4dffc923\
   9b6a0bbcdf52c9acf322a125af9658b4d145a0d2738229f21f4454e4f4a18e5c2240\
                                                           437e66d0f6bb
```

HPKE-1-KE KE+PSK with default aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558203f9020bb7917aad988ac4ce28ba557125cbca073f47b92\
   d62ac626faea8e99d358219db8e5036cc04c9c1fdca5193d326bd865c2cf17f26a9c\
   7389e8f3db5d48753896818353a201182f044d626f622d68706b655f315f6b65a123\
   586104b224dde0932ad62723c9e8898a4c1559aaae3a6b13ebad3e39f956219a98b4\
   25430f04b20c91d206e09fc2444f9052f5683f37ee65fd3848fe7a4dc1f76add725e\
   3017e83c8d12a84845cd1d2d82d1166ee680a1bacf199a73031111d84e948858302e\
   5d980137bc7495b6a0d6b71601c1a1e75256df9d629fe05fa6e62d42e17ddcb008f3\
                                               62b52c2febd892232e16c2497c
```

HPKE-1-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a105582037216bdf248d82945b87a3c84435f20301e9df3b374406\
88d24b21679a7a0ab85821a931981ba8d07236e891fbb39c0618999e67c80f6a2628\
23a6d129c56aaf4d508c818353a201182f044d626f622d68706b655f315f6b65a123\
5861048cd2c5b128525c051760ca792ae38c60f5d9be83091d4e904eaca8e0075df6\
d8f30738de090c203535bebcf1a6e9b6bf36e224bcd8fb5967e0a0eca0a0fbfdf5b3\
5da3a69e3c7caac50f266a3fc11e42d087511f1b0fad6d523ae53a0bfe604c5830cc\
cd606f644126bc917ae03ba7cefb34a38a8a4e00f51b830fb459018b009c78348094\
1f73800fc8e0b112002a07fc52

HPKE-1-KE KE+PSK with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a105582066815f04df75e4baa646152f2460695b200df8a50bbd0e\
299dafefaf15c0532a58212dc67fc86f0206f279930dced3b6dfe726250cff8354c0\
b657fe6bcdaa6488daa9818353a201182f044d626f622d68706b655f315f6b65a123\
5861047c52bead4335a216813ae6e4dee2659ca7105ea850317c25b0cea602c8f3f2\
2e0141b58893ec356f33c20d6330bbaf836f158ba1ed714a04847a7813c64ac6c702\
9674035b6bca9c78f558746e669627970d8ac3b87800e4afe2d64db3dcb57f5830b6\
6689f6f4d536439d6b2e3f8240ae704c17679f94c63590fd6a29a03b1e32d40e2af8\
e664f622d0e5877f002882d558

HPKE-1-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a10558209eddef4455129ccbc494aff056fe52b251224e272da90c\
7ecd54ce94c7d45169582188ace3811de11efcd2085d7ae48ffeaa7ce401e9c991e2\
25044c8359190d997283818353a201182f044d626f622d68706b655f315f6b65a123\
5861046ed1710cfe5f23c768f69ae5124ea8baa65b18a1981c64e157e8f324619215\
c7878a697c004a612fe20f66c89b7b2af741cfb7e867b7c2a1b35273c2bc947ecbfc\
868377795c296592759d3bc722bcd62bd1ca6e9fd0c70a9b16908da9b2c8445830c6\
199481077ac37f2ec1d4b1ef1fef392e4fb9141df4293dafb794b54bdc4064a81d8d\
8e373ad1d3e92e246066d5738f

HPKE-1-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820f47c3ba696c350eaf5dfe64827bf68b315ef8cdd02f6eb\
79b86c025f16c9b4a1582197c7f2ecf7c3f2b716ab7d4b73f97b481b222e60716210\
534f78016c9b03413f38818353a201182f044d626f622d68706b655f315f6b65a123\
586104507accfed015dcf0df6d1306def2ceb0452ba174ecd3e06b9d30e347e07364\
b3235ddd156f6501ab8f96a27ddd65fa2b0d54326b38c3bc6ccb592bb72a41561fea\
fa7ba3d707a9f8723c96c0c849fac454603f148c45525dfa19582e76c9a0c3583003\

```
   caa89c05e657bc89efbad8e98477e85fb02ec395c0afc94547ebdca64d653e80923b\
                                                   95fca02adf07a7e017693e68e5
```

HPKE-1-KE KE+PSK with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a105582018e63fad49110f7ca669baa530a3ec034c2f1770d1eaa2\
   ce2a341f217d896bb558211815fb8683836dfb3704d766cb4b40dc4b1fd3ac1b2d24\
   9f8bf391d3a555169506818353a201182f044d626f622d68706b655f315f6b65a123\
   586104a4f4e17c89b7c0b522e8ec28bd24c0bab416f94b30c5fe34ac861dfb25235b\
   67aa6e5b3a9ae6e716165091f673b89e42d34c159d3017dc6278c94552927b864c18\
   918855547bd105e52143bf40d918ace0909d175c4762e0148a160db874ca0a5830aa\
   4d85b740d6f6374b5e2badfee77f4785b09fb924f08e66f5fefe36475452c4afd6b8\
                                                   21d2709f5475a4f2e4e425757c
```

HPKE-1-KE KE+PSK with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820ef49dff5d5ba7d895181eb84e0559e17064ff6149bc74b\
   3b1cc707edffb10ed058218b25783a9d5efebf68c9a32535d50dea5335af4b28683d\
   ddea0238b7ac864efe65818353a201182f044d626f622d68706b655f315f6b65a123\
   586104acb79124f34d2f82b6816d4ef4f835f6ac056fa3ed49b631136e416de1a7da\
   5b13d77ef3e99b5c3af89c4335fcec4d0b52063e3669de03469d8f65069dae4484cf\
   58027f0d1c0414575db5e4ae47d302f49aad5d6efb7eb1c827502688f245af58306c\
   ca7863e2e0b35193bad7c08677f15c9497ed073df29ff1c7acb784a2d9d5c5184d9c\
                                                   8ef64218d1561a9f36b7c38d09
```

HPKE-1-KE KE+PSK with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820b6813d3b91fd420ce0fbb282282a0781e928bba1f2ed65\
   55ac3876ccb79139605821278ef63f7bef40a20188e88d8072a35fa49b421dfc7106\
   9a0f01abf8632b5a188f818353a201182f044d626f622d68706b655f315f6b65a123\
   5861046f6718ba3d9581817b7d6e8ba572577ca2b4c426db2e83273af0b8bbf1ee33\
   d54afd913c341bbb8d3115d7b6d08b6d1fee711131c1c908877accc0214cb2c86670\
   cfb647cedc0d3de474397691ff71a9f72ddfd0d8a7bea15c6ab8b1035fb723583013\
   444234c83126f8a62772aa4b9a6e7a702255557cd726a740ee18a1766ad48148d00f\
                                                   87f6e9d418d3c68f8f8411b77a
```

```
   HPKE-2-KE COSE_Key: \
   a70102024d626f622d68706b655f325f6b650318302003215842 00d79ba4c6f1f0cf\
   b40eb165353f19725907afc3d302e466f937fcd14fb3be4eb50e2d13502642e691ee\
   2f9a6ff8f9639f2af3291fdb7c3b4c2d48b9ba6963d7762e22584201d842560d1937\
   0441abf9819003efbe8ebfb6ea2d6c53eff1952aab6abd9956aa8d35642bd3b1fc8e\
```

```
   99e5a55a8e5615240e1f5c8d3e83481307215f71d7eb06734b23584201565854ad14\
   06345de77c2a4df3715f29c2bea30b86c08ca2b756118969f5c7aeea0ed0aa10ce20\
                    5ccb5428e4ffb476bf1524a3905ecb7381fef8c5011e5870b9f8
```

HPKE-2-KE KE+PSK with default aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558203138bee2c7c5222a490f6dc8afc1b3928d44db2df56fb4\
   032acfe1079ff9c52a5821093d059b8e0684b04d4a7a4eaeae24cbea063414467e45\
   89417511e7468410298e818353a2011830044d626f622d68706b655f325f6b65a123\
   5885040162b43abd5b8846801b7de98072cb9603536ec3a7bd30668528dc75707804\
   dbca8a71e3adcae9ad7635e1107ab85441b63acb86d0252488ac7c24157460955da4\
   22010eed01508bc178962b45cb26d06d484ee72b4ac2cfc937e1d171e42483a5a5ac\
   080b83a0aa25b376facc15607d9a2ef91ebd233e2f35ef08b4dca8fb0efbe1676158\
   306417055e20b3c85bd42c94377af8ff21b5da0bacd1f62da7e0b91499158eda595b\
                                          40d1c9fe83361bf739577e2cc7b847
```

HPKE-2-KE KE+PSK with default aad, default info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820215850dbf837415f3822d8f5d26cd15a0c146c92359b11\
   b1782867d457d4378a5821dca9a96193d94c1d1a6875471f113dfa4c623fd0ce711b\
   f7d4c1109bdf7930895b818353a2011830044d626f622d68706b655f325f6b65a123\
   58850400c6e8136d09b7a8acb620c13b17ac1afef18ed180cd259be1d3dda1072d96\
   40371b05e7c56911fa97aeb1c7ad54c8fd396f40e75cb5f67f17a2ea70e873b56f0e\
   5501372452c80572470b4cc341434b023b8f7d421ef1a6560670d9ac7510dc6d6cc4\
   4d4c2454ef702313759494bd5dc1198aaee2ba8005bbbcde75d688f59b15a88e1f58\
   30c17f1cae979c5ce953c68b778f0a774bcee5af484f6c59c35cfef9c811cfc87959\
                                          334a1c4475034e2b780ec7bb53499e
```

HPKE-2-KE KE+PSK with external aad, default info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820fdb5784ac8e133937727e19374513e964a7d940e4f5684\
   b73ffccddc843df4445821abc32701a38c1c36b3cdd98683474ac9d01237f4a61013\
   7905c75be8520a7e7a4e818353a2011830044d626f622d68706b655f325f6b65a123\
   58850400652d2c6aad232448534aa1fbf6318956a3ca8fe3a581bc264cfb74b5c4b5\
   9675b5852f7b28c515413414faf01474c45c4111711ffab4d1541cfcaaa0a6136dbf\
   78017cdab90f57f246ba74fdbad5218bb7e57e4f645253c3802417f91587beb94af2\
   3423eb0fc295c74b42fe64d5c033bbf29a3b18548788de1010bdcc076254dd30ed58\
   3063e1f93cb9087ee33598b22f6b5f77008b4798345c4a8004b42565dc5a753dc39d\
                                          280117494fec9fb5ae0e28ac358470
```

HPKE-2-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a10558206a802ccb1bd4d388862b5fe0afce78dc7fc3c08a4ee1c4\
97fc03e2a92db02da45821329c4d048a5c81485fff9540d9ddc083d31b59c6eee09e\
8b3787e0f50424eff01d818353a2011830044d626f622d68706b655f325f6b65a123\
58850401f32ef361c8b9435fd85f2a762bff35d49407738e645893bc38938a046553\
9beaa0867b3c32eb993ce0a8599e684b22fbe06527d7ea5f23809bf2a340e4310bd9\
20005d05b63e8fdaa1428ae3bbf70e8b606b8bb364c897a1edcf54d27e56dc0fb4e4\
c89b35099465048b10531dff3101167eb081f4ce1198d66361773ce83f1420cff658\
300189869866e44e995db469e07664386d86680cf0afba7ed0506d893124347ed12c\
05277d04eb5ca818a83ef7d2abed40

HPKE-2-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820ca66488980e271eb113bab9c87c532ab964778274b14fd\
d1498f43760660cbdb58215915445e1b1592fc3ca8a10e066770df837e8dcf627b2d\
cdb303350a8cfdc15181818353a2011830044d626f622d68706b655f325f6b65a123\
58850400af9a27daf713ab290e06f323585fe4e378adb3da71ee3f913d4df0ff6432\
34d5096298388e0385b6791583dae223df7a2395c739be3456d877f2c22a60db7079\
3b019e97cb108e5ed8a4dcc92e708f9010f0ae64410aba36ef66edb45275f4c22e61\
3352d0ad6e2a94c645ddca1c3db4df47b0453de357c91f6dfafacb11221462060058\
3060acf6929d7bf0496ef34937a3bea4a83b92e7ac223b9cb7b1389eac5a6fe52f62\
a7e16186005c5d9c7e3aa052b66c4f

HPKE-2-KE KE+PSK with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a1055820c12e10e83ffb5d684b5dbc8987f36227b0ae5356f60eab\
1c5cfc07733972713e5821625dad1ac818ddcd4f5847d09b661f6a80bb3ee80c85c7\
11d1eb1fd57e6b6e9bbc818353a2011830044d626f622d68706b655f325f6b65a123\
5885040163399875d2f44c2b62f6a241dc4e5d2d77ae2f71d48b8a4ff7015cfea98c\
25573ca31b1fecc15ab570c6d848a9dd6cf65791cebd6fafa43b85a997caae43a6ed\
6d000f7b7e6f33ee305779bcdb560112e82663715bacb5b5b46a17e00fbc1c7e48dd\
eea2cf7f79d6a8db02baf64ec466244d206ae933eb4ec2559603a306c5a43a36f758\
30151440d327f5b4301017aa88a5c07df896c565e5dda60e71594c9a07dd95d16ea9\
7f780977fe2b5e1ec9a3bb2899ec0d

HPKE-2-KE KE+PSK with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820d2d3de0c045b580ca7065a0b6ee0ee4a99b16df064c8c3\
b94f080503ae1bf96b58217b530401f8dfe8b7f938929169f31054f4c1b077d874da\
e6357e0299523cf309ff818353a2011830044d626f622d68706b655f325f6b65a123\
588504001c84d1eedbed866132867ed9cb7468462f9c9a149fe92f8b719d6b2c02c1\
10e04b1cefbdf10604a0426a24e0a11b2f1b519b1344629344a4f54bc0fe2996e9b4\

```
9e01478110bb40c4050e47d7bb2d2f99233dbc6bb71a1a60a2ccefde398fd6eaaa10\
c940825ef3f2bd824399139b9f55ba7d8c0f600c4208867778f7bd596c3c95afc758\
3063330387cd24664cc5ebc2ad1d1f9e785c9c1c8682ab61e810595b99f6af562ca9\
                                        751eaef8949b746005a8aabb3d73bf
```

HPKE-2-KE KE+PSK with external aad, external info, external hpke aad

Ciphertext: \

```
d8608443a10103a105582035a8bd741dd4bc4eb339dcc69e91214badd6d79fff2cca\
4088e6733b80f7d4e25821a2b8d2e530b9939d2bc3e478ca797afb14453151e294c1\
dc4a2bbaba356949dd95818353a2011830044d626f622d68706b655f325f6b65a123\
58850401dfb9d20c07e0ba4fcc4b93e66bd94ea0b8ea94f4b336912b0d676b5367d6\
97801e668f598dadbfbda8c375478d368209e09d51f7cfa2ad283f8d211ae13b7d23\
d801b2f56718deba752f33c8ba0aef918db14d6b901ac55072a781eb26b04cf55363\
461604f6b0b6931f0da446f5d55fb56c82ce6989fc88129b1918335efd0fcda03558\
30afc3fd0466c8696180429b63cc76880e877e2da59f20411572cffe8ce15ceff86e\
                                        78a18472c78a6286127290caf6f15f
```

HPKE-3-KE COSE_Key: \

```
a60101024d626f622d68706b655f335f6b650318312004215820 32df6a916a5f6f14\
5cacd3755783f65f7f5b35ddfdc6bbe6e699c1012f296c70235820e8acbd4b527e76\
                    6136f0e0ae266dafaca435e2c4326f6be8aeeea30d4ce91070
```

HPKE-3-KE KE+PSK with default aad, default info, default hpke aad

Ciphertext: \

```
d8608443a10101a105508fde94810cf9df2b8f3e011dd014866458211e3b36874e1b\
8fa028f8805bbb1f88cd29125b6cb229292eed3949060323114f26818353a2011831\
044d626f622d68706b655f335f6b65a1235820fd114c5c260726726405b3983e92b8\
24c76ff415bfb3a85d43266be85e436d605820db8a62e96f13814fb6b391fbd07868\
                                    7ec01e5430408a1ba130b8aa561106d36c
```

HPKE-3-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \

```
d8608443a10101a10550e7eb3c12fba8f1a84360649e00228c035821188af3afa5ea\
10ee723e40b0aefa2a7c1b1b05ca778c613ecc0c1f846595a5a7b5818353a2011831\
044d626f622d68706b655f335f6b65a123582020f2e48c5b6cd52cc560c8c345050f\
1bfd3756259bbd321704a963614646656c582002ca2aca70d04f750f32805cfc440f\
                                    e78591f3a5c1fe6a931870ba6cad61244d
```

HPKE-3-KE KE+PSK with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10101a105506c5121bb87c9c2f62b2c868403be8a38582113c72fe8aba5\
5de94b9f0cea23854e8fb4dfdf87d034f0b17e366fb05f94be4364818353a2011831\
044d626f622d68706b655f335f6b65a12358201cb2a61bbc134a03b6ba241f0bf47f\
71a65a3b67e948f7974f94e05e2569c97458209e8495b63496b92c5bab86e7f34b55\
5b6a3677397bf408835500188c3df93b39

HPKE-3-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10101a10550f9a3efc56621cd0fa9c173feb8d486ea5821bc91169ed9a8\
17fefa394582affb4f019ecf50cdbfc46e52ef437d08907854447818353a2011831\
044d626f622d68706b655f335f6b65a1235820e33a5d0f7a885988058daa06eb6895\
961f41e6b93e07314e8319ec60dd0ca8635820d38344948ce6c0fcae23835a7b3059\
dcca67057ebbb3628b30c7a44af246ca2a

HPKE-3-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10101a10550e21e4f3f711e3d4a40233210b6c7cb18582153dae8d74b8f\
f4377890721f44b576e9cde9c069796daa0ee1606b21b868d72560818353a2011831\
044d626f622d68706b655f335f6b65a12358202d4c865b322326d0c42970da331d64\
0be580266d1ff5bd48fe2d5851bac0fe7358203325793599c3f217f84542bc2523ad\
beec95c931eb53e71145f1a3f8f78843e6

HPKE-3-KE KE+PSK with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10101a10550784f25d8b3b8e28c2ee57f8034c2d63558213d35627b8906\
a2c6325f0bc1dcbeff96a66f00d2326b7bc347631f356dc79a1c37818353a2011831\
044d626f622d68706b655f335f6b65a12358207ebbf54428b2c7ab5cfbb1aade2cc6\
a9556a0e58528ae576258f0d7c126585315820b610571bba5facae1b75386f5ee98e\
3c370fd7b7070b58794e4ebfbedd876543

HPKE-3-KE KE+PSK with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10101a10550b0e54f4eb4dbc8d74d0403151a4c9ab65821bb0bf21a799e\
13f522fd5d6efd495e1e0715ad541388557b9baaabd6c4f7105280818353a2011831\
044d626f622d68706b655f335f6b65a1235820bc2dd6a7498209f6a16ce2cb8ad311\
46e1d7601f3b7a7d916e9b8f0c4b280c1858206335338627bda61773b8abc05330f2\
d86744561fc9705df85392c3979a34aa82

HPKE-3-KE KE+PSK with external aad, external info, external hpke aad

Ciphertext: \
d8608443a10101a105505e5a35587511620d9c95dbda458414285821ca24cea1349e\
a1bd6610cf7d64fbae3809c17b48870a1e33fae2daefe83b16caef818353a2011831\
044d626f622d68706b655f335f6b65a12358204f16be73404f6130ce36f25b3abf38\
f1f8d574330257a3715a44182d74611c715820cf43a27483d12a7fc5a01ba05cf0b7\
9bc9fb6c5b7108f7469c2ab8fc437d514d

HPKE-4-KE COSE_Key: \
a60101024d626f622d68706b655f345f6b650318322004215820 00c2029ec474be36\
8261a61ef7dc4a3cb7951209fcc66dbab39c14ff85400320235820d01a98ed714cf0\
8ad96c793edbae5e1f5258dd98e94a1a94d6a08adbd56ea74a

HPKE-4-KE KE+PSK with default aad, default info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c2fb741d0c5c6977aaa2b01c35821b738d24609bcaa98ee\
1f5f7b77eb38b9d64e5aba602154c58c12c61824631a4f0c818353a2011832044d62\
6f622d68706b655f345f6b65a1235820a2310170dbec7095eefb7d35107c425ec256\
6a5e859cfd80e6a56fc91cb37e3c5830635a41f1026dd93b27b73d30c9a5391c7e05\
bfc8b0ca766933f62257781c79fe6e4c2c0d1cb17edaee344fc33322a9f1

HPKE-4-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c3cf3405adaa9331e2706668458216e3a5631d75766cb70\
8fbda036a6e5b654f4bc3c19bfcbb7ad9ed3e5574115381a818353a2011832044d62\
6f622d68706b655f345f6b65a123582009fe08cb84624452f285537cbc0671477338\
7689960a3584b05cbb4ac70acb705830db74a5f8b12ea239755500670d38b3c63eae\
4a1f0ba21b25876c427422a70a7f3cbf26a43570d266d28418c914394d2f

HPKE-4-KE KE+PSK with external aad, default info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c6d73414c64bbef1b945b35a9582118530c7ff2e58db941\
e48ba7b1876e88a3e019bb1b92789dba0309cae6cb74ee2a818353a2011832044d62\
6f622d68706b655f345f6b65a123582047267ddb7a6a5788a506b37d450aadffe786\
164e6f94cf5253c8e023f181a73a583034362ce15946e700fd8bc9dccdf1cc504822\
e76e2a9250866378e85b8d1c8faeade8e5657fa9dd9e36ebaa46c3ad923e

HPKE-4-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c8bac033f30bf465b3c8184c25821ed9ea80bfb07d11a20\
399d92e4d757179ae6e4ce1d9d5db67ca20fd0c85ffe35e3818353a2011832044d62\
6f622d68706b655f345f6b65a12358200e6087d030b1e8520574f884baafdafddba7\
1c558705cf4872aeca4629c7403758308f95cf34c40fb9ff6f3cae1f9a8e9f99058d\
249f5feacb091b0e615e0e9f46a5bd1435439b1bd5844ee7775840003c36

HPKE-4-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054cc32577820e9fc7f1dfaaef16582146e402f02e4c45bf8d\
e3c32d36b16f520faf735f90ab843f23796880fcbd549d07818353a2011832044d62\
6f622d68706b655f345f6b65a1235820d524b1636dd7796be27a080a9167ddf362e8\
a06eff5549572a04eaf9bbb46604583009ed3173e50ea69bd2a3f60a7252e81e1225\
6016ae3a762b05e28174cdc853a80909b6f0be8db0aba24a48b2c975c153

HPKE-4-KE KE+PSK with default aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c733a1396a5fe52e4014a80355821d5b08336a933b87f03\
26832badf4f522c942c95f0bac27c9e47bd99039360dbe5f818353a2011832044d62\
6f622d68706b655f345f6b65a123582096d993edbd974f70b36f89a5833f745c5f2d\
ba2c34e2dd25254ab4c3309078235830244a6ae5269b99fcf817f921dfbb914a3e7a\
8d98d7effa565c1a38b6607c5ce29a0a6ea78cd3e00a1dc1c1191f715edd

HPKE-4-KE KE+PSK with external aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c6508d2450db84d5aafdf22645821979e63ed8bfdb38b82\
8b5c495aa0eed1257eb0dd8784d52efc6acdb450ab3c00ec818353a2011832044d62\
6f622d68706b655f345f6b65a1235820ff60abdde8677257c587be0228e616bfbbfc\
b2ed5c311e112fffece0ae28d4585830299c4de0445f2f588b8f9dad87b10f5195bd\
c20a65f1b0021c138304477ed35ed752694fde15c21cb4cbf5b49b8affb7

HPKE-4-KE KE+PSK with external aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c6a9fa48284941a3c00aaf7c8582173bfd8633fcb167664\
09f713a4d6345c4331834876130bc6fa8e3b382914ec68b0818353a2011832044d62\
6f622d68706b655f345f6b65a1235820a78b256072f458027fa9790f0689eb492f40\
d28622e07c6ecb81fc30c02f894c583065f9ded5cdbc30262debac57505803bce0a2\
879a354171668ef8378bad1f2e09e84ac1cc79fd7dfbf03a773a99d8a6dc

HPKE-5-KE COSE_Key: \
a60101024d626f622d68706b655f355f6b650318332005215838 4e237eb6c934b5d9\
48aee5db58e71b73becc1fdc6c90d45eb68975b0008ba24976fa622dbdf0848e80a6\
a222e4b0e1f85b99631307bc4b01235838940bb8c6bf6882564f1138fc7805677a68\
d2422492d3de009740f973e4e29cdd92e1942dd2f2d23526c410522376bc0c0890a6\
425097f4a9

HPKE-5-KE KE+PSK with default aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a10558205adbcb6e0ff034e4c7fb8f57d8684d48a0713ccd9d9ea8\
07e0414efee28a983758212b781241cafbce0ddc141d16a4fbb48f64eb2aed749aff\
992400a081c9719a3d98818353a2011833044d626f622d68706b655f355f6b65a123\
5838dd342034c2bef0bb830c781530623f7dfae57752409b4c063c08c670bc5003be\
86d45941075d2e38e35d6b5c8da084b1eba2e05119c48d26583023ec6199b0bbf9cc\
776ea35e34fdaa85786090f62f738179128cb37aff35f95e5d12417ea84df23daef6\
eb78117a4f8c

HPKE-5-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820c801c70cd6c15c0ed4c5d31095a3d9ea5dd35a3b7ff85c\
effb49ebac170a9ff95821ab85a76a92a692a53161168a3beb7a051346cb4859d3e0\
f2047f9fe4c90131de12818353a2011833044d626f622d68706b655f355f6b65a123\
5838b6c90aad8c11cbcb475b01f9544219dc466f6ec119d4108d35bc31cb12b2db26\
e1c8eafc5362e696490c06129a5cb4f7fecaffa5bd0d00b958307a1ff17acb7d872e\
c2bf968d6ecf7be5194175e98531359bc26db8a0293100649d3ff5dc80261c5c80fc\
1384c17e418b

HPKE-5-KE KE+PSK with external aad, default info, default hpke aad

Ciphertext: \
d8608443a10103a1055820b55199d8da2f1d98276b8a6c0a6db64fde7f45c75fc468\
10465cbe324072dee45821745d2621a784e938f5b81a742ccb209ad642502fb63210\
0c3af8c2c9cbe013646f818353a2011833044d626f622d68706b655f355f6b65a123\
58389cd5c81cf76b3be50a1ab36c6875d89b65f2d26355311f5c76c32ebb5fee324f\
8faaa70fe97eaa8346edf8191529f21c58afe92d8dc56a3658309adba68d36c24323\
0b6615bd68a7af1bc1ec51902ef11e4779dd2168fd515319fe60d7dfb4c0345fa9fa\
f53525a1d68e

HPKE-5-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820ada57fa4de7c380f19c3e5b2b929b64cd838f46a8c5087\

```
   3c7b84c076e8cfaa3a582185a638115f9e6036d3845bb96ccc12ff6d506200a7264e\
   524a316ec496d419c99f818353a2011833044d626f622d68706b655f355f6b65a123\
   583832dfdc226ec0637124dbf5a5c82795b860d0b80a1d6c50bbe2181ce1c8fccb7b\
   f4014340a3588af77a231124e7863278e44c082dd86495f25830d386e2f8408fcb05\
   d8898380101486ac601901774e065220f485f2049b11a01b0992f0ded73dfdb2341d\
                                                              4b53d6fdf3c1
```

HPKE-5-KE KE+PSK with default aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558205a2b4259c8726f7b27c76ecbab67b873b5d6d4a70b0cd3\
   486d71f14236b296e4582102e54618043019f8934c2c8c56db8d92189bf4ec1f5296\
   2bcf51fc02a965ba1440818353a2011833044d626f622d68706b655f355f6b65a123\
   58381213b34c1040aa5de533d5af7cc401a7824683762da048933a292ede982a9722\
   c6110351b1e98cd058705fbcca2818cff9f7b6b5bb8881f858305ab144940664bbc1\
   bf1c5b3c8c76d57520d871f7238b4cd34f8a53ff72b9980ad2d05a51403df6f8e926\
                                                              bea5780cf0c3
```

HPKE-5-KE KE+PSK with default aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a10558207f86dff69987f153f499c0511ed65e655d4d34430a81bc\
   95cdacc6a107f7bfd95821142a231e1c831730c99cb634850ec08c47305bb342b279\
   4ff27c6490d3d0c3036b818353a2011833044d626f622d68706b655f355f6b65a123\
   5838fc4618571971c112d55fef10f82d2114c2fb73dc0a94182cde7bfefea6d82685\
   b4bdfa1ee1947cf0d76a224c496f282e75694efcc4af5abf5830d074a192df2905b0\
   3183195149c13bf83c1dddbd2d76b40d5ef0ead641103b01ed5bb88de9a7e00e7924\
                                                              4343231a0207
```

HPKE-5-KE KE+PSK with external aad, external info, default hpke aad

```
   Ciphertext: \
   d8608443a10103a10558201e95d431b06ea4021049ea2eaf75546ddf41f390ddb9e7\
   376863a904c769a5b058215929dd46a1996ea5323720abd290796727915d670e6bec\
   9192317d40e7e905be79818353a2011833044d626f622d68706b655f355f6b65a123\
   583856e102688b82fcd05585bf0cdfce4e7b749dcc4c8c5e5f0afffe1987accee459\
   369e30092519b382aeb395d121467af61fb7e344bc8397ea58301776ac6367407286\
   282a9f3bb645b42d0b77b35c17190bfa18489b5d11de38cebc9ae74e845ddbd76958\
                                                              38765da32724
```

HPKE-5-KE KE+PSK with external aad, external info, external hpke aad

```
   Ciphertext: \
   d8608443a10103a1055820ccc5a28c0fc6ce3a77b3287c4bfa39527836d4d977ddca\
```

```
2995f9f231c1aa3e5858211c8d84c7bc5b41632d045448b3dd303be1facaf8308dc4\
520ecb141f366786903e818353a2011833044d626f622d68706b655f355f6b65a123\
5838577f7fb7d14b3cbcf4cc8cc987c9fdb8c37e4c7787091720b16ca8ce1a1eb64\
ff394100b5e30ebe141c1728c44bbe50111ed2b3cdfe80465830129a07f73d90eecc\
a1fd2c6b57dde0cf7e35e08dbfec45195576143610932eb18a65a625d83ab2932861\
                                                        a06ffafecf92
```

HPKE-6-KE COSE_Key: \

```
a60101024d626f622d68706b655f365f6b650318342005215838 7a73481c0220c785\
b74d64c163e1de5d44e5390bd0fa08ee15073b58530e4085ffc8864e7a515d472177\
58719376b1450d97bf2a669ab9b3235838dca30972462039bf863de85351d9190e87\
938dfc8e84d55036d3ab77b8f8c75d9ce58b9cde255a254d70194cb4853134e6e375\
                                                        583df14190
```

HPKE-6-KE KE+PSK with default aad, default info, default hpke aad

Ciphertext: \

```
d8608444a1011818a1054c36d04a7d19dc55e80075d23a5821e574da31d97960f6ab\
7175d1a5532d59c14394e24f51df359de4db10b12714e9d9818353a2011834044d62\
6f622d68706b655f365f6b65a1235838748632655487c9a95f46258ccdfa90d04f8b\
434fa91810c86afacef5648cafbad2ed82ea7e2c2dfab8addcc335796fec210e0fe2\
6ec10488583020b73a418c7419830b7f9d8b6e06a645b404fb35e6cd7ce7e7e74601\
                                abb1d5b66ed53e823517a315cd8ce27b2fd71a48
```

HPKE-6-KE KE+PSK with default aad, default info, external hpke aad

Ciphertext: \

```
d8608444a1011818a1054c797818adbf0a654fb32d614758219fdd3c0be43a6ca9eb\
b33af5563d90620ef2ae69bc9777c1d42862874b0a4ffb26818353a2011834044d62\
6f622d68706b655f365f6b65a123583890100c00c48cb2531016da4f3a3d3094f1c2\
f03451d76e992f540147bbd8e9ccc3b3538168856cd0ce5d772fdb299f9427793fa7\
727d9dad5830cb8dcf359251188b60eca487fb14ee1c3914cf347c6fe223dbe5fef7\
                                d36de4ca2ceec64ba0a50fe5296451d51b53c4a7
```

HPKE-6-KE KE+PSK with external aad, default info, default hpke aad

Ciphertext: \

```
d8608444a1011818a1054c82d73212f41a6d160736112458215de02558566868de98\
6e6bd01ecba81b47bc67dab079c69519e9f020884172c3d0818353a2011834044d62\
6f622d68706b655f365f6b65a123583842f56ab3e5441e6c65634346a2cfb13ae8b1\
afc9a8b833d045045b57015f9e9ab7fafe6a05671e9ee29187e20cc1b5b0acf2a90b\
402b5df1583078cf0aef816b9e8fc4f94678c98bfd1fd7999b5e44edfa2aecb64fc1\
                                5a17a94350eea486dffa00a9c7ca99224d46a09a
```

HPKE-6-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c2a6fd56a8b3f6908e1111c255821b1a6735f8870342bcc\
0906e85561781ee0126a5efe9aa8ed18d28533449f152e1b818353a2011834044d62\
6f622d68706b655f365f6b65a12358388769dcc3b3ec1956dec6a7f75367a59c6387\
0f2f7b3762ec7f32432495c5e73c2c23781033a9d364591a3d300426615e9f320422\
35f42c035830604150f58d908a033a617ad608c6bc2ee2eecd55bd50571ff2472a5e\
523a09e2a6f85818c4466836d99331a35bc410a7

HPKE-6-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c44d92785fbf3070bb1becfde58214c17f577725046e044\
f809adda3ecc238d697c20e728bdcc4bb3720ad4765a5538818353a2011834044d62\
6f622d68706b655f365f6b65a1235838bfc6a49e284186a6fa33ce0e7cd97e9b69f7\
20a81559a4b3297705219bba25c54b0ab70cc38a1ddb67446c3e448167546c4620bd\
8736a3e55830ea379d8848709112c1eef6366ab91cf6d4cf256d3c216c7733a6eae9\
c8557ca478a147db040def50e7955c1ab5819379

HPKE-6-KE KE+PSK with default aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054cf38ab7422245935d23a66d8758212dbe21e54161712a49\
1581fe3820e5aa386a07fc64a324fc692d455e7aa07bacea818353a2011834044d62\
6f622d68706b655f365f6b65a12358383bc0cc314a33ffdb4e87eaf5d52d5ced617f\
0896300c63bc25390bdcf5ff6b9f9cd4800f05864a1bae10c3b941205bd5b7b3afcb\
1ba898c458308a745bf13677cf7ec0d2ac9a65e14bc5641ea9727d143a30f2535589\
1572f6958f5bc9898e33c5b926deb1f1ceba2da8

HPKE-6-KE KE+PSK with external aad, external info, default hpke aad

Ciphertext: \
d8608444a1011818a1054c7913f581c059c8ec72f9ab5a58214e023cd8ca3239fd2d\
9b29a580edd711e981551abd7751a004ff47057162b4a184818353a2011834044d62\
6f622d68706b655f365f6b65a123583872af48d87d997690e3cfaa920dac46dc6095\
216d05b58a5323d814ea5ee6f471b4fd99d996a9663ef0148aec8904acc6ea0ddda1\
3c7315765830bf103402453fc9b6d846ad6f3a435aae99f628b7f323552e9136cfaf\
64a7a95de8e2656ad6b706c94e002f2410092c56

HPKE-6-KE KE+PSK with external aad, external info, external hpke aad

Ciphertext: \
d8608444a1011818a1054c3b24712df521ce6daeb16d79582157122c22bb26402e9c\

```
   c64b46f817ec3b11d648f1de72499442efa7ffd13b07af1c818353a2011834044d62\
   6f622d68706b655f365f6b65a12358388cb8b6f65144bc3f730feb3c40dbbe759f8a\
   db2fc96a67552a431efdc7c5ec4ec78a415823e1422b532f35c7b8ee75619e46d6fc\
   9e4455a458308f628129208d995a3e5e7234680907ebcf15add2fa9579f910ad0e55\
                                b43e3faf5f8e8e41e1849d3e91a6ad8a5f07ef6e
```

```
   HPKE-7-KE COSE_Key: \
   a70102024d626f622d68706b655f375f6b650318352001215820235da0a3f782d1d6\
   3883301a1f465ce5ecb9ee21b5c956dc33af969716ac10122258200bd7226e1968f5\
   fca824b05749377e347ebab34dafb752941204ae153e18a7723582 08c6710cca617\
                    4b6c57ab2f3166a3e12d18d5915201c98b4e48ddf65568f3a73a
```

```
   HPKE-7-KE KE+PSK with default aad, default info, default hpke aad

   Ciphertext: \
   d8608443a10103a10558201e7f005d9034fd70b784b478151f569c9e4116e8d9a6a8\
   71370be98fa1e2452d5821b51716881bdd056919af5fb588eefcb06200f220f48f50\
   0931bbbab04a82e03c3b818353a2011835044d626f622d68706b655f375f6b65a123\
   5841041479f005908668cb2492fb8cb8afcb9df4c0c89c11ccd18c2c3bc7fb42c931\
   2797245d5a3ab4eac0c0a87dc2cb0a2b8ce770c5757a44880257a48841639ca31e58\
   30e0ab73659cbbd3b6a43bcce5169a041599af3a8485e32d01264a0b134f11f9dcc9\
                                         7324b54127972b0fb93d9c11469602
```

```
   HPKE-7-KE KE+PSK with default aad, default info, external hpke aad

   Ciphertext: \
   d8608443a10103a1055820b1ffe35d48b498f0288ff46d6a61a4e90ff0befd1e1ec3\
   c94537b5f9af9920955821c23e3d1f53e82f94eeddd1588c5cadf50bfaf31f1d28d2\
   96c9047ba9727ee6b22d818353a2011835044d626f622d68706b655f375f6b65a123\
   58410424929f8f874446d29dcb78c37e6a5b50f1a4680e7a23d8f0014717645a90bd\
   a7b7f4bc6b920ea8ee042a644f6b1b5af8cd7e5fea40e424e3000b4c2532e3883d58\
   300bc1e619a7ff8f5b67c7e110e01f9e1018239c3c4bb3a1f63389453bdf3249b266\
                                         a321843aba2401d42804f627d5e457
```

```
   HPKE-7-KE KE+PSK with external aad, default info, default hpke aad

   Ciphertext: \
   d8608443a10103a105582064a16aad701de8efec4c898d53d75e273dab2ee7720d54\
   4700f3f26dc1e8b4aa58212cd39835cff3f3f303dd9dae20e79c789e0d425ee04112\
   f26962be476a94f0654f818353a2011835044d626f622d68706b655f375f6b65a123\
   5841047443a801c2579cc3a9683828ac1720d133dc0ea1d9c34b72dc3225aa1b203c\
   7eced7aafcca86dbda61dcc95efaacae431fe02626f390a7e97e4a8319c9d20c7f58\
   30cb47c1f7c40efdf049f874f9fe75ac7d1a494f2cf4882bfd492cc402822ab8f52a\
                                         51848f7e60e798dfb969c89bb44e61
```

HPKE-7-KE KE+PSK with external aad, default info, external hpke aad

Ciphertext: \
d8608443a10103a1055820e413d828a5dfcfb33b686ba36a5d155327b096140f23e5\
2b675731f2fa06ba3558213438a2918171fd8534f9e65fcc902f9cb117821f059b59\
fdd76490a37a44aeaea8818353a2011835044d626f622d68706b655f375f6b65a123\
5841047056fd1244388c2b611cde8e10585a66974fd59724cb6bdd82f8e576c6de06\
dec1fec70238f7f0f83f13c58cad88bc38af95456427597d5314055cb67ef0380d58\
308a5acd6f28e689c7b750291bf0a771863a0b38bb6e3d972522e0c4e96d2fac613f\
c907615e4ec8df18f0923c2488e674

HPKE-7-KE KE+PSK with default aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a10558207e358aa4427767452becb89d519e0fa6896ae3c41019bf\
5ec8ef6700fe248ad858216d1f77b27b44718c523d0fd25d532546678578e5b6ded4\
f20a6a030367b673908d818353a2011835044d626f622d68706b655f375f6b65a123\
5841042bb09d00627ab8c7ad3c224485f3b81a9a3f696f8c216b7543c37065860c86\
5f9e18ab32654bcbb69e4a63797b838b6c040b24a6707a39f720486fa9f24c8e9658\
30e2727f5ae33e384b37c80a9357dd2eedf9351b1422604d5883b1aeb4f32b227d1f\
5d1c7328475ede37196bc2aaf6e131

HPKE-7-KE KE+PSK with default aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a1055820bbffb795e60de4a819c29f426c403685d125b32b67dadb\
ba80218ffd00faa64658217b4d6953483445bd9a5dbf07d4fd2bea23e17806e02bbc\
8e9a042ab73c7bbd9e82818353a2011835044d626f622d68706b655f375f6b65a123\
5841045c1d347a472f3967d2c92324fd5dca6aa26df991a06de353e2b9eb4f4cccb4\
2e098feadd4bd9f20f109a0c78e6a3c1d4af9a86e2243a68e331fd5352b993d7c758\
3037d79f7df4f5d20aed2922e5a449125e977b209706b8e63bc194ec3d72a29e00bb\
d0b7ab54fbb8e9619e2a57ebadce39

HPKE-7-KE KE+PSK with external aad, external info, default hpke aad

Ciphertext: \
d8608443a10103a1055820a2d6dfc0464ecb11dcea7d68e5e6789f43a6361f5d59c3\
7ed6f7bdf1e1a570b45821efc33ca5a6bc622204945b925063e7e9430792d637876b\
b4f722238d9faa33fdd7818353a2011835044d626f622d68706b655f375f6b65a123\
58410410a71911e9fff4710a3d2e9958a7514396351bd4782e1444e221c50e59d85b\
e8831870513c71217d9047291de48f3b3ec0e92a4937ed32a7d5221a9e752f8b6f58\
3023879441649cf5dbfc65318c6b844f250cac5b80f5c5bcc1c79549765c9ff79e54\
f26f08aa83cce9ce80f24ed134ebf7

HPKE-7-KE KE+PSK with external aad, external info, external hpke aad

Ciphertext: \
d8608443a10103a105582002a2da5a958beef87ad0ba08837b444a2f123187df56ee\
2f102fdc26c1520788582124ad5a1dff05de46743fa4285a4c8296b9b402798ff585\
617b99d71483a1e872c0818353a2011835044d626f622d68706b655f375f6b65a123\
584104cda61f9062ce00aba834383c974eaa1f10f05515861073265508f5834c0980\
d586f88cb101d7bcf8c39408bfac13004746c96ecb33974d98869b5be16d6cfb9358\
30677210dede124a21c73b75d43d70597b512e6dd7b467bcd3f809347c039ebfab97\
2c41db766608113bf178aeeef89b62

HPKE-0 COSE_Key:: \
a70102024e626f622d68706b655f302d696e74031823200121582019788 38d5d7cec\
cf63ef1b5206e7bf6e7878eda9fffef7f9372174559bb915b5225820ce11b8ec4906\
471126f125f8309fa6d535b88bc2902659b2ec311f2210a0ecf1235820d584d0f00d\
9ac070e310e07af82af13f8f5ccf8c48feb74a9f5e9ac7e434d012

HPKE-0 Encrypt0+PSK with default aad and default info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e742358410436497c25f707\
c15c87f902d1e21c3cabb8d298511eb5a23aa5ca54846d296923539927ccb6e12c5d\
2ea31e0322be9052881e1908463f74218759abaeb7acc8ee5821460f6df2872c7719\
0f2d109b40f9387738b161a11af42af43806afa23a2f43ea8c

HPKE-0 Encrypt0+PSK with external aad and default info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e742358410408e74886e267\
b409c5813e6ed9a5f8b142397b64d3266c03d124a4899265465d6d1c3d85e72ca170\
c59f6748d6a314b81e065affa6c2a6a2b17d7f5e991a9f3258213fee4c1fb2daf759\
7130bf6777ff4c617e474ab4ae87df303f8c24575022f76f55

HPKE-0 Encrypt0+PSK with default aad and external info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e7423584104d27a3f163efa\
768558406af61bde46d8ddedf9ac6fbb21d737eabf5906c7f7f68f469b027d22d396\
8692279cc4d45d937823486e0f3a118605778921b9e4d0775821d33af1cf7b36a32c\
21263ddf2257f85ace2257797fc9ce3b8362f7a71d7775c618

HPKE-0 Encrypt0+PSK with external aad and external info

Ciphertext: \
d08344a1011823a2044e626f622d68706b655f302d696e7423584104a1dbd4acd8f6\
9bc5e38f4bdaff6101aa8ecee2d637eee96f495174209a1e7fb27a934f3b17329a0f\
b93c3cd76ceb339c6ea4bee4b950792c060ff686b50147135821c9ecd3b87eb93f19\
c7f220a9afbf7c3f0d8bc35766818c9f49148563ded4cd5de0

HPKE-1 COSE_Key:: \
a70102024e626f622d68706b655f312d696e74031825200221583 0a07787376d7be3\
aefad3a37787f366fb5b9db711ea52da6007d6c0415edea639a3749f35e20b5db7fd\
3f1acfa94fe88d22583093e13666684a788a3ddbdb3747923fccd850f072574b7a3f\
bc4ce7bd810de7d0754ee5e0763061e3615ccac4a6231490235830a29d238c81ec58\
17c4ad1b8f6e6f796ba76d6ed3bff6c730531c8469bf7e08c30e8645f690d6adc12a\
4411953082467a

HPKE-1 Encrypt0+PSK with default aad and default info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e7423586104df5de432eca4\
006ac093375950771fb12d1b61b1bc8498c2a04a4b0ea42130afb07fed7ae45e0de4\
f51f872897440f16c06fe23c768f2663def46b6c5340261f45a8427d9da07e058e69\
599b62e6712ed7e04704194900cd4f7a13e5d600b2e558212ed9d3916151acc3cc24\
7a6b5cfff03595f4bffb5e26d4a98ecdac227ffbd2d211

HPKE-1 Encrypt0+PSK with external aad and default info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e7423586104a218f4c737e2\
53d3b87094017731469274d9df3eb676192ad68e9fbad4523b51d1555b82e8780a79\
49055188fe745234d1d75574f2b5ba944c5e3faab398d44477d579d7bdd6389e55f3\
48d119eb9c022d465002381be0c3afb9674fbe016f4058217d4b45a3b68278465c57\
cc1b3acac76b9271213ff89dc7ee1208cbfa5d9ef47607

HPKE-1 Encrypt0+PSK with default aad and external info

Ciphertext: \
d08344a1011825a2044e626f622d68706b655f312d696e7423586104d116a00b8ee8\
24c1b6781c91d9fb4830928b963feacd9824c232f0f4f5b71a04a5e0be4149086381\
32ab4c758db22f4c6e37bfe8d2903812cceef4c386e65529d102693f8c0c88ef9b94\
8e06d9a6d6afdb29a8b781947af95b5ea00c99ca56ed582160e20429a820e789310f\
9af083fbf818141cf5a8ee186109f003941c3f05194d92

HPKE-1 Encrypt0+PSK with external aad and external info

```
   Ciphertext: \
   d08344a1011825a2044e626f622d68706b655f312d696e74235861044aae7f5eb6ff\
   9aa01746b686d6d3fb70a899992c85387d81419ca412e3321863e89a3f758e8e0454\
   dadf8da49d510dcedea55f5bd4a21c05ac8d5adee32c3885b50592bdb10840840e16\
   9aa9617e53f919d03a9e4eee8ba9cedeea06296a59d75821ad5a3f69d0bc2502d480\
                          ba69622367278507ed68ff5c96ce5cfc742450e52cdb6a


   HPKE-2 COSE_Key:: \
   a70102024e626f622d68706b655f322d696e74031827200321584201 0ff539d3b9e6\
   fc491c324a1fccf71e4b3dca99c4ca3bbcdd715cb7732109b846f2c7a08b96fec81f\
   04a34c5fb694adb551a4f8e11cc336441378bd05471b79b70b22584200ebefdb1bff\
   b05f3eff770ec11b2b880a0a8f9f853297006e8db147b5e5cf34709e3ce71930d3c6\
   1ca1ddc7f33322323aa8dcec47748a503162aab814698f504a272358420164e63b64\
   4aeb24c393ba75243505a6f77f9c3acaf4f45925ec0d9a93f2838c46665449adae9d\
                  4f68fd02e504bc01032fff52c57281fd9f01dff04bc714d80a1b1f


   HPKE-2 Encrypt0+PSK with default aad and default info

   Ciphertext: \
   d08344a1011827a2044e626f622d68706b655f322d696e74235885040019b47bcd96\
   dddd5feb25b470146d1cf0c09f20d8e642468160835db40e29f25f2d25664afe2bbb\
   90daaebda1238ef5bb19ff321bde00da48764cd8a7270476e5e000fa4f7a92e769f7\
   aa71c06dda3397ef0f9a2b11e26571604d034b3c7c3ec07e0df4c6366377053e7230\
   efcb77cb123d40ad0e9513e54338c8d20443e4fc6aff2b27582115e3bbca19faa6f6\
                       1a7582db14aa58433d6876716c796e39b156e97fa4e0f5ecfd


   HPKE-2 Encrypt0+PSK with external aad and default info

   Ciphertext: \
   d08344a1011827a2044e626f622d68706b655f322d696e742358850401abc01f5afc\
   1dfbc2b40adf647f863bfa62c9ac2bc059e8678c3d1666acd150f4a0b7eb3a9b71e9\
   f5c617d89744ff529370d55a9ef4176b1265882611232e484d4701690e2e3dd1d184\
   b6e5cf202d1983d39e396f3ad776cd97f2760e1a570ca71f8ae29902a80c2f462eaf\
   da610ff9f03867fff20742816838efb536fd501f6ca10dc058213245639008b74fc5\
                       c71f37f3c302f94d54e95061dc14b86c59681d2b242c1d1de8


   HPKE-2 Encrypt0+PSK with default aad and external info

   Ciphertext: \
   d08344a1011827a2044e626f622d68706b655f322d696e742358850401b85a75afd2\
   d4832df126acb39630b1ecf97cfeba280bfbed6f0c3008daa590635740d7b4fdff28\
   070e2936a5b7bbb4772b897c548da2133133a6da63de96ef87a60013d6fb0195b5eb\
   9559b8f8d9a6fa12ae3bda7e3f7b75eef0e420c3fff312044c6a87a33e429408a8d0\
   7d27099cd4e1c0d1f61c38133b821ab1881a419a395f32d85821640e4aac586afbc9\
```

489818406f1f69bb30884cd01f5dbcf8bc8fc7ab6b26edebbb

HPKE-2 Encrypt0+PSK with external aad and external info

Ciphertext: \
d08344a1011827a2044e626f622d68706b655f322d696e7423588504001f4e8064b1\
74c08064fb07a48e73c92ec41073f74fd043a33cac2eb2b5a39679c15e20b8d228ce\
93964a77f0766e460614114ac3beb2f6baec2675823821e81ef200e0b9c902e74524\
1db2a85e3cf7717e2e61f8824a3fd8fb0d1403b367da7bb42fe63a2ed1ac4ce42aa2\
9853d4a1dae37f4eef0a1193225d78811f1692943a81c5c15821188905cf7d36da69\
3355ba05457fd6039d5c1cd1f49185817d70e737b8da629978

HPKE-3 COSE_Key:: \
a60101024e626f622d68706b655f332d696e74031829200421582 09f898a80cc4290\
dfdf261d0a90571095afccd022b65f609fb7cbfc144b721539235820881c29bbf697\
0ef15bef05e2b6350ceed8cfcc77a7ce141e9a8ff99b0d998043

HPKE-3 Encrypt0+PSK with default aad and default info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358202bf99fd198dfe5\
0851ad960a2d593fe8ad32a9b84a304e7eaa3feef510609d105821322a3cb0425a6b\
9735ec81020f7a8f124de35b9c6788623bca0309d239677985b8

HPKE-3 Encrypt0+PSK with external aad and default info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358205df8c7147ca3a6\
5d94fffcacc61ed49a3790cad79534f31df74a91fb74b60f0c58219ed975688367df\
7f8264585cc25ea668cad87824b0b2eadd9984e530b904961c8a

HPKE-3 Encrypt0+PSK with default aad and external info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358202a3900a4fbdd71\
4b7624be04df2b031c63d9c9a852b788b0572da47b56a11b4e5821ac8087a1bbb462\
ccfa9b78f7c4e040e6041014ca783af8b754dddf52b72b0ca3f1

HPKE-3 Encrypt0+PSK with external aad and external info

Ciphertext: \
d08344a1011829a2044e626f622d68706b655f332d696e742358208bed4488608e6e\

```
   a3e3b10e33d7cb35d106a378e56ceddb9b421201254516285b58214a1304836a432f\
                   c64fbfd0f445ae464a686c950e0fefc6ca1d6cef99b9ad8a7865


   HPKE-4 COSE_Key:: \
   a60101024e626f622d68706b655f342d696e7403182a20421582098f335c76496e8\
   1d70b464b7168ca9331ca28bf6077db774fb8a652a98466151235820e06b4e6d7d1e\
                   7c5feabc632c61cfb7761163608b5d5e1c82a1d9ffbc4b449f4c


   HPKE-4 Encrypt0+PSK with default aad and default info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e7423582077376805957 1f7\
   487c63dbbb6684932a13f8782a8865a721c1f91899efb91958582109794195e1ccbc\
                   f3a4091254df0b980e3dc2a4f76a16f91d10106bccd4e17ec0b1


   HPKE-4 Encrypt0+PSK with external aad and default info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e742358204972c7ccf0072b\
   fcca44cd334b6170895e59bc08ac24598b9dc024c8537ba234582185c48849033c56\
                   2fe8cd0fb110b96546b1f9fb0a956462b8803501a0f342b36f1b


   HPKE-4 Encrypt0+PSK with default aad and external info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e74235820edeabe2d694177\
   e36bd06120e11c45a1d78f64336c5a9ef6f3a09f5adfc42b0b582188d2a43d93aacc\
                   89bd29e3efd7be8b56d8d3c02b3be1da7f5ce8b55f4b93190334


   HPKE-4 Encrypt0+PSK with external aad and external info

   Ciphertext: \
   d08344a101182aa2044e626f622d68706b655f342d696e74235820a4bcb538ad59e8\
   6e0e1cf8b615eee457eee2ce659c88fb263fc9d064a3022f145821ded166fc8867b6\
                   b45628630ee777df2e47a03a81f00c961c1443d225182b01b835


   HPKE-5 COSE_Key:: \
   a60101024e626f622d68706b655f352d696e7403182b20052158388a68a40d28b469\
   ca93ef6ab8f4095e0c467ed7da367ec674ea966d23773dfc3ad39765409f9c9f1c34\
   900c355777a9a76ddbf3e2e06e0141235838e86c18e103423df47ed171fc82f8d398\
   adfb61bebc17ed35eb85246bfba090e46841dadedf5f1049433ed3a875882a934fb7\
                                                           07588a2d12d5
```

HPKE-5 Encrypt0+PSK with default aad and default info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e742358386925a3a6a036a2\
d76e66ca435f712055a771c3d2b744e8b8e0ad01534ac236b1d8c3b7741876e7a92f\
8646f3b7cefc4236914698fe93c7785821965d22abb1540da8024724d12a8fd848e7\
9e2b9cd2f74c44e0e85166853e98b1d8

HPKE-5 Encrypt0+PSK with external aad and default info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e742358387b8c8969d60d6f\
a9668453cf4dd9e73d769a362a0892e754ee091ed7de93964648795a35613eda69a4\
b164d43abee4560c7c3604fa9dafcc5821c82bea6fd7f13c29f3a4931159eb8caf52\
9cbafdd677c2354ed5e6accf84a55999

HPKE-5 Encrypt0+PSK with default aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e742358389a4882d84ca735\
9da36adf7a80a72feaed07e32014aacabdebea553868f3482b15cc42c573c6185f3b\
a4744d22df70ad99b74e68702944a858210a23b921a2a884507b661239bd79302701\
f3a5b479f97f3260681b9d4185da5920

HPKE-5 Encrypt0+PSK with external aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838bdfc9d7a69532d\
605cd20c454713f2bba183566e7d5814535e4648b239fb2a1845e8030718ff0243de\
3d854d25dc0cb3fc87fc692224c79558213c73d2bcf43ec29f3a91306567d2903532\
b03e4224948d702e5be80ee9e9644f9d

HPKE-6 COSE_Key:: \
a60101024e626f622d68706b655f362d696e7403182c2005215838958b1eb8523293\
b880d8744265760378b4f9a72f9ab31c9147205207bfcc114186347f030f3fd894d7\
a5b9e385154141d6e5c41e06e977032358387063a27888d7919aff93704896ec21a4\
d36312d5a101fac8f75183603fbd718b5aa68a33eeaa5c8ac1d4e400c938976c6e0d\
a5080f2e33ad

HPKE-6 Encrypt0+PSK with default aad and default info

Ciphertext: \
d08344a101182ca2044e626f622d68706b655f362d696e74235838e5b4599601b2bb\

```
a65b4eccd053a4163c70ba55c47b6b2cdbcbd7da4301ba954aa2e106e342acf4557a\
68ef1d9fed298ce10a5489fb01006f5821aab8bdac5bb7e89199c16293caa5ce057a\
                                    0a03de3b643d885665866fdf9548b6b2
```

HPKE-6 Encrypt0+PSK with external aad and default info

```
Ciphertext: \
d08344a101182ca2044e626f622d68706b655f362d696e74235838535c3766b98650\
daeef42882dfe251e4502faa645a315fad0eaf0daa08c68366cf281b3a0e0924fc87\
f83d8e6462cd039907b9ee7fccbadd5821d10bfa98fbff244a4a7ff6940bad877fad\
                                    8e7bab901a503a51b365f50ee6baaada
```

HPKE-6 Encrypt0+PSK with default aad and external info

```
Ciphertext: \
d08344a101182ca2044e626f622d68706b655f362d696e742358387b1e949b71d32c\
02236d08f29afebc7f12c14e5e21e5909683ee9ce2cb804b42d6134a88290a38f92f\
163934329c01d70b855aa0127f660658214860e64ac9613b9188fbe659a89fde3fbb\
                                    f87e05d828bed3112e039ee1060c5914
```

HPKE-6 Encrypt0+PSK with external aad and external info

```
Ciphertext: \
d08344a101182ca2044e626f622d68706b655f362d696e74235838f8133adda20c17\
be5cce697b83cd305a9304f596f663440a2547cdd86afc4ec3b061b8ab18e886bfdc\
aad18164f35da4337dad314e63ba5a58216023c82c3ae28723cc8396d523d6946948\
                                    1b67edbfaca4df0a6bde5f472398716b
```

HPKE-7 COSE_Key:: \

```
a70102024e626f622d68706b655f372d696e7403182d2001215820a60f63d47f6e4a\
9010c65140f827f05cd04bc45ba2f75e8d9aee0ebb6d519ffe225820b1e33d1b7202\
11dcbb7b58694fd45bad75f494656ffa754505d80044c1d1f5fd235820cff95cf1ce\
                5c67edcb20881bc02829d870f5f50cdaa03d1e1522c67505b6d5f4
```

HPKE-7 Encrypt0+PSK with default aad and default info

```
Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e7423584104df99cbe182c0\
41a6502415fdedfc22b90bfcd33879dc9bc9e30b9ddc74b3a837acc71f09ad252180\
bd01da4df7b7487701ef6a80b35738e9c1f37cf40675bc4b58213da7027ac0e3943f\
                    df967e75bac20fd621d1726220813b416361c95e32557b4dbc
```

HPKE-7 Encrypt0+PSK with external aad and default info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e74235841041cb6cdbeb778\
329f4812be9da0169ac0510646a5b7d63d7ca845241c8d6200d9489be511fdc12892\
0a3bc0998312dc0db82b314fbb2e046c7bc20ff5afe767f7582112b9b197cabfd884\
55936d8037908bffe7b07c2953bec1c0b3b963c9fc74a8716d

HPKE-7 Encrypt0+PSK with default aad and external info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e7423584104467cc0f1d194\
ea0dde9dc946d67ef89b7bb4026617bf68cef65d8127077a5209334a057e2674d213\
3278d729595fd51a1556ee8f9df91acdae106671bdbaf2885821d2786254e1311ca4\
f884717a60d1b493b98cfe44be88d2820c7585e57cdcb2c8be

HPKE-7 Encrypt0+PSK with external aad and external info

Ciphertext: \
d08344a101182da2044e626f622d68706b655f372d696e7423584104f62055c9d997\
d492879363ee13e4cdf676172c7cdf24d27e18befab5886fe93228306646f05a06c7\
ac2d807301ea997374a3aee90b4c12c8dca348ea93fae5425821e831f27b7d99e448\
97f409648e54594cc5f3ff1fb184979d97a5af5799b6c0ca64

Authors' Addresses

Hannes Tschofenig
University of Applied Sciences Bonn-Rhein-Sieg
Germany
Email: hannes.tschofenig@gmx.net

Orie Steele (editor)
Tradeverifyd
United States
Email: orie@or13.io

Daisuke Ajitomi
bibital
Japan
Email: dajiaji@gmail.com

Laurence Lundblade
Security Theory LLC
United States
Email: lgl@securitytheory.com

Michael B. Jones
Self-Issued Consulting
United States
Email: michael_b_jones@hotmail.com
URI: https://self-issued.info/