COSE
Internet-Draft
Intended status: Standards Track
Expires: 9 October 2026

H. Tschofenig
UniBw M.
M. Jones, Ed.
Self-Issued Consulting
O. Steele
Tradeverifyd
D. Ajitomi
bibital LLC
L. Lundblade
Security Theory LLC
7 April 2026

Use of Hybrid Public-Key Encryption (HPKE) with CBOR Object Signing and Encryption (COSE)
draft-ietf-cose-hpke-25

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 9 October 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() Single-Shot 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. The "psk_id" header parameter, when present, MUST be a protected header parameter of the COSE structure of the corresponding HPKE operation. The PSK value itself is an external input to HPKE and MUST NOT be encoded in the COSE structure.

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.

The use of the "kid" header parameter is RECOMMENDED 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 Single-Shot 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.

* psk: If 'mode_psk' has been selected, the externally supplied pre-shared key. Otherwise, the empty string.

* psk_id: If 'mode_psk' has been selected, the value of the protected "psk_id" header parameter. Otherwise, the empty string.

* 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 [RFC9052].

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.

* psk: If 'mode_psk' has been selected, the externally supplied pre-shared key. Otherwise, the empty string.

* psk_id: If 'mode_psk' has been selected, the value of the protected "psk_id" header parameter. Otherwise, the empty string.

* 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 [RFC9052]. 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 is a Content Key Distribution Method like those specified in Section 8.5 of [RFC9052]. It uses HPKE to protect the CEK. It is similar to the Key Agreement with Key Wrap method defined in Section 8.5.5 of [RFC9052]. Internally, HPKE performs a key agreement to derive a shared secret and then uses that secret to wrap the CEK.

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

When constructing a COSE_Recipient for COSE-HPKE, the Recipient_structure defined here is used in place of COSE_KDF_Context to aggregate the items that require protection. COSE-HPKE does not use the COSE_KDF_Context in any way.

The Recipient_structure works akin to Sig_structure and Enc_structure defined in [RFC9052]. It is constructed independently by the sender and the receiver only as an input to the cryptographic algorithms. It is not actually conveyed in the COSE message. A CDDL [RFC8610] description of the data structure is as follows:

```
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": Defaults to empty byte string. See Section 3.3.4.

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. Implementations may perform operations in this section in whichever order they choose, so long as the same bytes are produced as a result.

First, the CEK is generated, usually using a high-quality random number generator.

The CEK is used to encrypt the content. 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.

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

Next, assemble the protected headers. Note that they will be wrapped in a byte string.

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" header parameter is present, it MUST be a protected header parameter.

The protected header parameters MAY contain the "kid" header 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. If ’mode_psk’ has

been selected, then the protected header MUST also contain the "psk_id" parameter. If 'mode_base' has been chosen, then the protected header MUST NOT contain the "psk_id" parameter.

Next, construct a Recipeint_structure as described above.

Next, the HPKE Seal Single-Shot operation is invoked with the following inputs:

* 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.

* psk: If 'mode_psk' has been selected, the externally supplied pre-shared key. Otherwise, the empty string.

* psk_id: If 'mode_psk' has been selected, the value of the protected "psk_id" header parameter in the COSE_Recipient. Otherwise, the empty string.

* info: Deterministic encoding of the Recipient_structure. See Section 3.3.4.

* aad: SHOULD be empty. See Section 3.3.4.

* pt: The CEK.

The outputs go into 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.

The COSE_recipient structure is computed for each recipient.

Decrypting is largely the inverse of encrypting.

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.

* psk: If 'mode_psk' has been selected, the externally supplied pre-shared key. Otherwise, the empty string.

* psk_id: If 'mode_psk' has been selected, the value of the protected "psk_id" header parameter in the COSE_Recipient. Otherwise, the empty string.

* info: Deterministic encoding of the Recipient_structure. See Section 3.3.4.

* aad: SHOULD be empty. See Section 3.3.4.

* ct: The contents of the COSE_Recipient ciphertext field.

The plaintext output from the HPKE Open operation is the CEK.

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.

3.3.4. Context Binding and Additional Information

All header parameters in the protected bucket of the COSE_Recipient are incorporated into the HPKE Single-Shot Seal/Open info parameter via the Recipient_structure. As a result, these parameters are both integrity-protected and bound to the HPKE key schedule, since they influence the internal HPKE key setup.

In most cases, additional header parameters carry supplementary data such as a "kid". If a use case requires binding the encryption context to public information, placing that information in the protected header parameters is a straightforward approach: the value will be transmitted to the recipient and automatically incorporated into the HPKE key schedule. For example, a new header parameter identifying the application-level protocol that uses COSE-HPKE could be defined. Its value would be authenticated and would also influence the HPKE key setup.

Because all header parameters are transmitted in the clear, they cannot be used to bind information that must remain secret. The "recipient_extra_info" field in the Recipient_structure is also included in the HPKE Single-Shot Seal/Open info parameter, but unlike header parameters it is not transmitted. This makes it suitable for binding context information that is, for example, provided in other layers of the protocol stack or via out-of-band means. It is the responsibility of the specific use case to ensure that both sender and receiver possess this context information.

There are minor size considerations. HPKE guarantees support for at least 64 bytes in the info parameter, and implementations are expected to support up to 16,384 bytes. This indirectly imposes a

size limit on the COSE_Recipient protected header parameters and the "recipient_extra_info" field. In practice, this limit is unlikely to pose problems except in highly constrained environments or in use cases with unusually large header parameters.

Protection and binding of auxiliary information can generally be achieved using protected header parameters together with the "recipient_extra_info" field, so use of the Single-Shot Seal/Open aad parameter is rarely necessary. However, it remains available for special cases and has no practical size limit.

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	HPKE KDF	HPKE 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]

* Usage: This header parameter MUST be a protected header parameter of the COSE_Encrypt0 or COSE_Recipient structure for the HPKE operation. It MUST NOT be present as an unprotected header parameter.

* 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-03, 2 March 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-hpke-hpke-03>.

[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>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[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>.

[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>.

[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 Thomas Fossati, John Mattsson, Ivaylo Petrov, Mike Prorock, Michael Richardson, 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"

* PSK (for the PSK testvectors only): h'0247fd33b913760fa1fa51e1892d9f307fbe65eb171e8132c2af18555a738b82'

* PSK ID (for the PSK testvectors only): h'456e6e796e20447572696e206172616e204d6f726961' (= "Ennyn Durin aran Moria")

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\
044d626f622d68706b655f305f6b65a12358410481158 85e297b224f955c5ee9344c\
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: \
d8608443a10103a10558205972218d130ebd50902f975638867f4393a02ad5fec6ac\
ea3b5acc14b99e7d6f5821e0d433a3f90df4a6bf252d8375c02ed940ae6321ac1168\
65e8a698e3e9826ae00e818353a2011833044d626f622d68706b655f355f6b65a123\
5838a5617b199ab5a27633ca063f171039bbbbe50e1563630270f5608b1c80b3add4\
658ee958f71bef28abe39e20231df1b2a5fdc6e5c7cd4c4258302f8f8d8b1f3bc43d\
53dbb260c3930310300d4ed07d04702c4e2114e7fcbc27cffe87c754455bb52c2e0d\
77ffc49f3424

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

Ciphertext: \
d8608443a10103a10558200ea58687a765e595948d0a4f863ffe895ed35afcc292f8\
e5f09a59666c018f87582153e80b1f3f78c46d298c2d969bb438269f56fb0db3f8b0\
dfbc3ce64d9bdb910905818353a2011833044d626f622d68706b655f355f6b65a123\
5838d9d4ce1da2bb47ce71c092855f2982a108793dad43b58ad4f378c35e50ae9601\
24ec906f02e959783559b189d73b4245bf6d12a291a66f2b5830816961b03ac6df31\
f593d4e3b8cca193e330d5ad273cd8e4fe1355c685c0b2a804fd8b5871346c3a640d\
f51e2885aafb

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

Ciphertext: \
d8608443a10103a1055820febe825f97612663cb5b37322f6d27a4a69cfb984b7703\
91db1ddd4351c565ea582163f837fa3fc30525c6dcd8fd38b0fdf4cb0732726d4e48\
479faf4cd19c106cb61d818353a2011833044d626f622d68706b655f355f6b65a123\
58386d8ab86baef7eb8b1b4b9812b8ee20de9bb7665db246a4058d557ef7b5a17537\
8825d6c3878cfe4cded34a63cd3f23b0c0a486fd742824af5830a5ff5e55b20975bf\
b4288eed91aae3181599c9444f56bd7d845e537f75e0001b860939ff406e3de872af\
20939444fb97

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

Ciphertext: \
d8608443a10103a1055820e651daaf30ef27e8898bd2f0f71eb81105a65ca9d625de\

```
   ba0ff73efa5518a0fe58216f7ed02b0a8c3be5f2e2d15bd58c357c65b688cace33d2\
   e50e7a5e48a20b1612f2818353a2011833044d626f622d68706b655f355f6b65a123\
   58380f782ab1db5dbdff4310356362f1fd48c0cce05f4cf5f10ed17dd4ef5489513a\
   63d3f357875f8d4f80c8c44afcb46897b623ef3909a043e358304fdb1f7cc531e49f\
   f9d6fb934a0a56b0c39fb161802304ee2d6aa2e038b7a1f604c643cfd3ba046f8557\
                                                              9e06ad7e58db
```

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

```
   Ciphertext: \
   d8608443a10103a1055820bc667687a2c9ba3a67811138b684871cc443c3a656602b\
   8c7fa229e73fd873f358218bf0c9204e988d76554b1195baee96da10ac58867a1daa\
   775eefe9710307bc4cec818353a2011833044d626f622d68706b655f355f6b65a123\
   58380e5096bad10fa4fcdd440552c14da49d819eb5fb2dd333ee59cfa845f51406d7\
   cab97f61a5c852b3312fddbdf347cdd66d0ac3fd6aeba8825830a961291467b70f5b\
   a8e1c02417d0048f3f2000ac4dc11722d8cd88b75e0dbf7c084740adacb62fb7b10b\
                                                              8b15649dba17
```

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

```
   Ciphertext: \
   d8608443a10103a1055820330886cc981a8fc93e5f508127f1adfc8d4db541d3618c\
   887ddc4f8ac952b78c5821652e76d1029e9749fdc28bea647b1e3e3d62bd57676cfb\
   e857b84703a1c5a07b15818353a2011833044d626f622d68706b655f355f6b65a123\
   583846c302c3731504388199bc3e885b9fac2171f59c1f9cafd8b909f6b5f7d3360f\
   261101400b33c8c10b5be896d2b2bf2dc324018be31a46175830b11375f3eac8a4f5\
   69ea3e6c31f8a27deeb029d54597496db6fbd2e853b59e1ef1fc30c312e7d0b6f482\
                                                              558d95f9bb5c
```

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

```
   Ciphertext: \
   d8608443a10103a1055820968e5870eb26e9e8777dafb83becedb4c9ee1ac75e57b9\
   635739e7ba96925d7c5821d65d8d5bb8922d7e16a6ec3a0a2c7b6432c569510a9469\
   53c891442704e3dbba78818353a2011833044d626f622d68706b655f355f6b65a123\
   58385545cbe1853c1c43e456f5fefd73004bb1d21684970adf8f8fbaa9681b835767\
   80d138948bb82b1094fdbac6c3388cd8247acf1493e969f458306c2f2c32734dd4f6\
   af964e9546d0a642107831b5c4bbf0b8edb87e38e3755e2da85b1e8f14097d51159b\
                                                              7df7cafc34f8
```

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

```
   Ciphertext: \
   d8608443a10103a105582012c4b7c5277a67a1f0cd348eaead14678fbb47428daebc\
```

```
   43426b5630bbc08bbc58217d6af626389f2eecf2cdcff8d3716033aab7a922a1b3e6\
   ac66edead54f7c451284818353a2011833044d626f622d68706b655f355f6b65a123\
   583840a712d7894f87c5c5dd263a97bafb6fcf06e22e9ed801a1034aada201fe9c1a\
   49e8e073746f6c713306f00c4335ebe8c9159910c659610c58303b5eefa35efee50c\
   73134120b7f24bfe68936b628c782912086087441754d408fa877cf15e4374a8c3af\
                                                              19a048df2896
```

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

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

   Ciphertext: \
   d8608443a10103a10558202b413539e41b5be049097d8c7336c564da6910493f34ca\
   c7be758d9be0bbc2a45821895a2fe91419e7f4e56cdad089d97b4313fd4d64b50751\
   aa35b8ae2a5a1f0f49c0818353a2011834044d626f622d68706b655f365f6b65a123\
   58389e4bc52535fd7d7de199cd9d3bc1ead38132ce559491daa8291ae62e27a305cf\
   a0e5301c44ada163e8c6d003cc201d84d6e56a0fbbff09aa5830386b65b7d4658bb2\
   cc1cb93e05d94685cceec0f155d39f46b74fd67db0ede3aaf653f5d44a79b2bc0b5c\
                                                              5c186f42a0e4
```

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

   Ciphertext: \
   d8608443a10103a1055820c38056dd0acc795392719d75883a9efa306688289e317f\
   bcaa907a593ef7fbd058211d3a68fca3448e77c0350164e7ccef263ddf6e52c00b5d\
   7467137987d9322b0edd818353a2011834044d626f622d68706b655f365f6b65a123\
   583873272b13d50c86ade06ad70f4067d8b9dd546dea6699cb8937b79106a2d178c6\
   e3dab8b403b60a05efa417ddeb14e97dcb8b46c866ec027458302ac2d004b9a0a638\
   932cb41dfcf2980e731dc1e164e78755e54be305f821130e25bfd8f9e423132f9984\
                                                              e587ff58aea0
```

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

   Ciphertext: \
   d8608443a10103a105582054037148342b2929d4126a1daa1a5cf49963f07f4bcfc6\
   b125cc9569315d428158212c12be5f1b14cb0be9cbc7f89e7d17cf6332f978ed3ff2\
   8e6ecf4177b439911f1f818353a2011834044d626f622d68706b655f365f6b65a123\
   5838fe5677121bc5b939bd1f3183d63ca7a1eb9834655073980f22463e0f4347c823\
   ae7fbcb106311bfe1862b5d8fb09be30222d73a1aec51a6d583092c3aeb223577ce7\
```

```
   0c4eb6d3fbdde2507ab0eb66684450f313a6098782bc2b7042880301438d9d3b1a8f\
                                                                65b8103a611c


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

   Ciphertext: \
   d8608443a10103a10558204717640f13442de964fe2df975d1f5b9049338cdc79914\
   3725983f3aac5e3bc45821c259895cb58581bcccb17204a6b99ea05cb1c556420025\
   c4487f7df0d1a7ca89db818353a2011834044d626f622d68706b655f365f6b65a123\
   583835b83dad83bce401ecbc78215d29c362be31727d86d14d1a983ee709f9cf23b4\
   4d1be7146c2ebab629d5e9d3a78e7ddc3b2ae9490ffedb355830652b1c2e54232fd6\
   7da865383a4196b3081d6af8f3dce4cfb2cbf74cb631df27c4180e081c4456df72e3\
                                                                06b033871415


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

   Ciphertext: \
   d8608443a10103a1055820cf185363d088aa84b66d952d905d67801aac1692a51fd7\
   0c5198bfec655cc17958219df95a1b0832f6ba161f831da0511904d075628c42d88b\
   d96c6d051edd67d7082f818353a2011834044d626f622d68706b655f365f6b65a123\
   58385148182fcb71312bda648d9a7a4c4dd74ae840a0f0617f2d4b89c834eaa55b4e\
   9636334a53bb1821e0fa15c38590c75fd2e09a5c678c6f0758306a9450456cd531a0\
   b2d8215f7c6f67b8d8fee596d5093f9ae8e3d0fa4d606c6b9c06fbe22cc186807e20\
                                                                816d411a3c8c


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

   Ciphertext: \
   d8608443a10103a1055820561f96247e2ea00c85aac63bbeb1ee480f21ab3e9ebf2d\
   fc54c324e1440b8da158216ec7606341f7ca01b47a12f96b14b592a19acec35fc857\
   5a14e77c1120f62a9ace818353a2011834044d626f622d68706b655f365f6b65a123\
   5838f60e9ef789715248f9f31fb9436aecee7a2fea8799fe436a97b5ad25b5dfbb69\
   7f9965e6f446e91fcffc3ff5e682fcb4e7a4bffa596f0a395830dee903c258f9be6e\
   9019e2663c97b5912bac14ec09f814b9501dcc29c7211a60b0b15ecb21ea434c38dd\
                                                                8363d2783e3e


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

   Ciphertext: \
   d8608443a10103a1055820dc036988cb1a9f5c3c2ab7320fd3a38bacb9c23b034172\
   c59fbeb026dc9f744658210c6ba63dfb087141b507a55070900ea3ae097aaacd3a40\
   0c83148f55e85134032c818353a2011834044d626f622d68706b655f365f6b65a123\
   5838bdc971ce40e3e124a0145a622e1ec19182bfdc0cd66fbf8f6ff8fe7b43af1363\
   c26be033563da00e96c8008f8804884dff825beacc89f63858305a3af658bcc81a61\
```

```
   5f025485efd9925e243d9d3331f0a0fd1a65fc6f28a0895bc30eabac5cdb11e6cf82\
                                                           204d096e7489


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

   Ciphertext: \
   d8608443a10103a10558209bedce93fc7ff55e06af978546a3b48e5a4c46caf3c1dc\
   d70e14529d98c0278a582144091e536a28a763f4441b7432ea884c7ec2ac0b68e938\
   c8de8c05c5009e82d6e2818353a2011834044d626f622d68706b655f365f6b65a123\
   5838ed5e7fdd82a824dc43c87a72f84943d3d7ea70331dc513ebaa11136fce401eee\
   755106b7498ba2dcbf6180677b735796bd9ed654c23ac2215830802d61870ffd8238\
   13b63c670db3319374b040e6de9a9b14015d2d2de1601f13ddfb6e054c78e4bb3512\
                                                           7be2bb775803


   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: \
d08344a101182ba2044e626f622d68706b655f352d696e742358388f5af58e1f0db4\
43f7404b1ede00a32b977cd3a699b46928f5c571c306deed1f2d859381c0b6b6f666\
a78514b5041fb2e7f694d5692598ec58216a365c1bdcac86157cbacf68ac46d89597\
440a775607af455e754d42f98b197336

HPKE-5 Encrypt0 with external aad and default info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838981878c54475dc\
1e97661abdb4189c05b5063564297b3e6ac252412720eaf098cf854555ac70003537\
4a0cba8abc3bdcb70e42d202f55410582139fece2ab3dd76bb900ebec9c8436ff8b4\
e129499e10c703fce9099b962a2baf2e

HPKE-5 Encrypt0 with default aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838cfc56e2a7bc6e0\
968b29a13c995a2f1d6c14096facae8f6c4de89e5f59baf0c25dd5547034c2cb157b\
275b0f7dc74837b65f4092bc6bbfbf582162df9346e36efb8d4a3b55dff58ab2095a\
31b5de9973dd51f9c8859902566c345d

HPKE-5 Encrypt0 with external aad and external info

Ciphertext: \
d08344a101182ba2044e626f622d68706b655f352d696e74235838e7bfbb375d9d1e\
c703b8333d50f5bb62e5a8ebe093e207cc7f65b102f03706bce492b83be7d86b61c0\
0863e96edff00888dad9ba39e60143582112636db0edaa6c58de1b9029084a0dfb8c\
26b09f3e7bd8d0f962a1e8bac74f71cc

HPKE-6 COSE_Key: \
a60101024e626f622d68706b655f362d696e7403182c20052158380aff5f4a86fc46\
8a25b7715d066628125dad13e4243f242cd6585f89f7371a55cfc3cf42cd3405a78d\
d380b4e9f4d47880c684deaa3f8aa923583898b6c98f0d48162ecc4c0f5e09c97246\

```
   b03564a2672e12496f0f7a0d0576fbbdfb287b5a868e5b569a55b7d3765e5685feb7\
                                                              270471b13392


   HPKE-6 Encrypt0 with default aad and default info

   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e7423583805b7dc9742e800\
   cda70b5bf55e2cfafb1414b630dca621999897a223c6564295328f4d913deff488d7\
   a5ac70b089679e808b1b9ecf18e43458217bba22205a379a6af9cbc37dc608d0571c\
                                       a8f0146e4ddbe0bcacb5ffc259a3325f


   HPKE-6 Encrypt0 with external aad and default info

   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e742358385b964c5c2e9a12\
   226b649ceaf964a4e50a8fe428fb288756c59cb92bd03d4c0eaa8c2104907cb8fe74\
   87c14e4ef7ce11f39cd4d1f1b209d1582151c6acdfdc65920d6d047a7d47acdab642\
                                       493698a89444c5f32e6888047611c48b


   HPKE-6 Encrypt0 with default aad and external info

   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e74235838f601104f623603\
   38e929527dba71011acc9ea59ec3fe3fb5cc338a3ce03b75664111ac030a6260091a\
   80a4926447010c97b6079bd6cd33b75821fb8851b4c848830717589eedf46fc7dcd2\
                                       3af1de491a4c2273918bb78e7d8e232c


   HPKE-6 Encrypt0 with external aad and external info

   Ciphertext: \
   d08344a101182ca2044e626f622d68706b655f362d696e7423583869e66f4b70a130\
   6856a7f09e5d8b41fb808786c30a54e1627f2f65c33ce66212f0c2e5bf769391b7fd\
   7d691f1dfe7c8b131793e9727314f658216df8f6658779fc5f234cd58e6049f67955\
                                       24f9ba00549772ca617d6262b230b81d


   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: \
a70102024d626f622d68706b655f305f6b6503182e200121582064ea61f745f7deed\
186d697a4c8971593275517766348b0443a60aac450b5a622582088f53a4cbbcfcc\
1bf0b33d5dc60f789a7f495244f57c158a8ceed5179639152b235820e8de39325f3c\
0be02442076c470a46bca742de9bc2be453ec1dc049dda1f6ca3

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

Ciphertext: \
d8608443a10101a1054c3dbf02ad2a8cd300035a7f515821b91b343a050b5b839a60\
f7d903f1b9c851e4a8e6df03b0ae05db0d33674fb635498183581ca201182e245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
5f6b6523584104c6022db2bfc09def2e95b94f2dc917fe2c27cf202ad3860e6bda82\

```
   9b64f8b68c53b06b211dd166dfb7491ef6f45ad6db9003af5fbc4747074364c386c9\
   7dafc258202e54e91afca5ddb92636072b373ed2921942cd497d7ec8c611fdc9824b\
                                                                  41d738
```

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

```
   Ciphertext: \
   d8608443a10101a1054c9661e9a238abd6dc7cf50e1a5821306ea0fd082a6a323aa8\
   430356159fff4d7112c85033a906ad6dc172ef0a0b0cc88183581ca201182e245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
   5f6b6523584104dd68ce56333e69967c02ade32115948c2ec2d291a698c4bf16440e\
   37e1f5c8785e2aa3bf0b6ff8a6c4226dcd0521c789e581b1aa816747ce2d2457b812\
   24074f582016b41fcd4f8dd5b2d179a68ccecd21470067811e7c94667294bf968a4b\
                                                                  3d9b1d
```

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

```
   Ciphertext: \
   d8608443a10101a1054cef09c76235024a7f9d9bf764582185dd1f0c0f3f27c7cec2\
   d32860ef7821454b76ec3213372b829b732b3df38dc3ce8183581ca201182e245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
   5f6b6523584104d7bbddfc24dee2304bf8f5cf59bb295696692fe9adb0b12d184140\
   7056830f1a989f32dcf4b96d319b4b358cc49d83d3e3dc1577a3ceac66d17a83a786\
   0565eb58203b5a2826a45ff3e7ee7c426d17dcd06737068b8329ccca41b0f52e8118\
                                                                  43913f
```

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

```
   Ciphertext: \
   d8608443a10101a1054cf7578443df9e4b89d9698ec758214dcd300e1a35ac0baacd\
   c1413b52acd44faf96b7b73caaf898490e122c748b69c78183581ca201182e245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
   5f6b65235841048f9fce9bd99461ffa16d9d969c0cace07de67e5cccf0267003e4eb\
   ce9732f6d6a62607eaca4735cf14fb7d5413decfb8ffa2c87b1fefd6741111be541e\
   eef8e5582076841526c099256a270d7b77aeac627e27ead1da23cf783c8585277f83\
                                                                  27e4c3
```

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

```
   Ciphertext: \
   d8608443a10101a1054c80de2428978334c2e921460c5821119725181b9eb6cf0851\
   2569b4638d95cd85668aa08cc85f29c77fb8f4777a2a378183581ca201182e245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
   5f6b6523584104c7aae16935e9f136f07786fc22f7becba789fa01a6e3bbf3342972\
```

```
680b5f3dbe9861fe0f68ed368bf012b0146b921f24fa64b54ad4f8477f529457a9b0\
d157c958200d4ea3f34616d04a4e5e9491fcf06df18c0954370b5650d099ff78f434\
                                                                352c9f
```

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

```
Ciphertext: \
d8608443a10101a1054c8cb385b70d414c1a2fef26aa582193b9a87ab45b1df2bb31\
c170246531deeeab2f3181eb63b47c43e63e4dc1eed5cb8183581ca201182e245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
5f6b6523584104d7caaf6b399d19f972c7cd761c1f3579c8693e95c64ba6beea8e2a\
1087ed8a4c5e3ffa0d9fdd6ff5d8fdb57a5f4ad770411909683c0be7d4db953b9b21\
746ebd58205b4bf1bdb9832eb48fa1ec40376241ef20d90cc55c51a25e6eb4ac4fd1\
                                                                4c037d
```

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

```
Ciphertext: \
d8608443a10101a1054c36c9055f67c485b618259472582176d7939ffc02c8472e0b\
6db2815d59eccd554cfa22d9425499fe8cf0e46e8f94078183581ca201182e245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
5f6b6523584104bb4c4cf211c12bedd7809231c1f951996e1738c93e7d292b23737d\
1cfe63750f50058e1aefa5073aec064fd1df754cf3b38227fcc293c7c0fbcf93180f\
bbb2665820a1ce149592a87351f8ffcaa4a6794be3f5a412704f559e0100419271de\
                                                                9afb48
```

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

```
Ciphertext: \
d8608443a10101a1054ce9864cb8b12d64751ec05d4e5821a1801101d6df6f25e182\
43c4a6ce901836cd0b343ec0c41409f29421f3207f135b8183581ca201182e245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f30\
5f6b6523584104b8376193ac2da680fae1da7ac0e23d88963ef33e31c6b660386ec4\
5582a743df0e439fb9a3573e5054c858cf0cfe8d3f45b7819827316a86ec19939300\
62725e5820dc809e77433a2af8225f0aa81413f5ee6e5bc14f441dc3fa079dc9ffac\
                                                                b54f69
```

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

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

Ciphertext: \
d8608443a10103a1054cb5fcbe9b162b79e2777bff265821a88c6c682b8c4f9b22b5\
375f08af6267fa0cdd4bf24b7999f383881bd720672b948183581ca201182f245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
5f6b6523586104c4186784b91e570a0c3778fd8617e4474f00ac36e5a1fd02bcf068\
90dc592ee2cbd8347c5a8020b03dbe3936301a5039ff4c4971bf5e07d55224fd130a\
2e666a2ec083cab442a4ccd06848bd40ddf9fccbfcdbcd1d7253bf6b9363bb30200c\
3f5830a138d514b294bb96ae5606bcf913fbc6f00e3a044b69fe54178b6edc971eb6\
2e2499b26c07e2b263fe1187cda8252932

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

Ciphertext: \
d8608443a10103a1054c24c592d1ceed6a8ade059f42582145c47bb07f24e0a3a42f\
4bd434d5593ea2332b0da4f4eb80f07ed5eab36bea11f78183581ca201182f245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
5f6b6523586104088b774f5c5db0696a45c6f5e8a290511baf14539fd0dcfd75101b\
e33ad580709f6b6d2ad99ef6328051479f18bd679f32f798a88d481edf1d491eb5c9\
05aea736b8f5c99ae401649cbfcbc927e664f37a170c50493cd3e6d242cdcc6c90e4\
395830b1bb140eafb2ccf567096db4ba97f3b23d37e6a620686430cf51617b431efa\
e636c67b6614bda39d068edb391bd1cb09

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

Ciphertext: \
d8608443a10103a1054c1042aaa6dd01cd47dd1905745821d22cf5013aa59e873fb9\
0a4cbc95a45428331189dba1bdd38b089af740e2946cf28183581ca201182f245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
5f6b6523586104699fde2f9dbcc7302732d254a56ee3cd4893334a4fe7f6a736f6d7\
e40fa72202ded96ec8098a41e29665ab5780e79446647fa10a0c7b91db431c5501ae\
52be7466303de9899cec90c229a9c8be2040ad70e05c37acd5c3f2b2f791c50c12fa\
d3583060f91f213902b49af37d07536c280036d3445f1ed6345a2d4781c52d7e6f78\
9a7493f4b8603931463d857564117764c2

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

Ciphertext: \
d8608443a10103a1054c91da386c5f1eef07cbf85faa5821fd8dd400e8f684343462\
0607ee0c70e4e5f4f04976b76ce97f26d9f63ff93430f08183581ca201182f245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
5f6b652358610450712efc09a90bc816fccbabb506b5da926531e8525ffefbc2e8b2\
aa7cb9a8ce33028f2d3849d0dee2e87340cb8078b0dac9378931b166a039c27cc8dc\
9eef69f1c1c4796922bfab61a274456e7953d3527750090991fa55e9d2e490b10b74\

```
   025830bff35b89ea234b88df3455dc5c23ab1c9680de46317f878b84d5ceec67384a\
                                       4f79935db486194bec5513e4769a7f486f
```

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

```
   Ciphertext: \
   d8608443a10103a1054c21f4cf0bcdac7f3b2e19d5f158217c2ff717ab53001eb726\
   e47cbd5c252c05dca426c5fa34a08bd9a9a1f4b92cfa958183581ca201182f245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
   5f6b652358610468124eb79dca9a18b16820b27e3a0eec4e4e9576e12fd1ae569462\
   1f2bc99f93f427efd7df5ea753d07a0d043080f4ff44ac6bd7f067ffc4c92e8741ad\
   cc60f3f3964118fd68d5514d40c6bf47d9caa80dfb241e1fdd04615182cb82971e1c\
   4e58304046f1a10ebe9f22a2aea00b922cb16a4ef445b55a223076894caa801beb61\
                                       8482dc992c9d9bda658c19b768476065bd
```

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

```
   Ciphertext: \
   d8608443a10103a1054c4f69aca23c486075321ec2c1582175f0ac90bdf8519e8f9e\
   5f5d8045b870140e7e1b4fa3828a3ea66c8514afa336408183581ca201182f245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
   5f6b652358610496430 7d5842c5e6bd03b2d770ec24f20e2f468319fbda2ed929218\
   e449cbb1b25c7c9da0b48fd619544b550af078f0d3dd703929cfd1e239cd10702c91\
   a5a8486b16ebc447a20a159769c0cde0068bbe7a93a5829730e558b0c466f7525891\
   9e5830a8cb603a923d60fbcdc996033aac4a3dc7107ee045d54efb7a87211c64591c\
                                       5f8c911197e56bf7e4fd500cb80e49bf99
```

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

```
   Ciphertext: \
   d8608443a10103a1054c81f26d6e9c5f24ff84b68c4b5821d492076beb8b8c5192d0\
   d7ad7abf7f54decfa6e6cf738b1e41cd8bfa9334c246838183581ca201182f245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
   5f6b6523586104fca207561d14c2184bef2f81af341e7750c778dc86a094147d1200\
   67f5e198c4639f78ad0c0ad3aeb7fe03f03ac47ff19b4986759bc6d3856cf299f202\
   95190ae8818c6e728fc0b7d69a96a16d98ddc8a36848e4595ae6dd8691e950878ad4\
   9a58300b2e005b728326026508f708ba12d4a92664363af98c551b69a011b8a10de1\
                                       333e9410149cced7e942cb13eb11540b75
```

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

```
   Ciphertext: \
   d8608443a10103a1054cdf9689a08e9920334a9742325821b85ccdf0c17da4f616af\
   863cc44932b23f1ea1fdcc4a5d2e0055be5d788766eac28183581ca201182f245645\
```

```
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f31\
5f6b65235861040d44189c41d060baf45f61f71d8c61d2259c1a5fb6f2af9754a630\
7d3ac1b7aacf3b10c455738e130c678d76686bb3d581fe8a94ecd75901513aa88462\
9b9e9b801bf55251160fccded082b91e3bf24e24467695d55605e73d15878e216337\
f2583005352b50b6ac62dbce5dd04af8cf7a4c5fe24f2b1641cfc964f8f4275dad74\
                                    d0da9222135c2525db6d77e7d41eaeb4e2
```

```
HPKE-2-KE COSE_Key: \
a70102024d626f622d68706b655f325f6b650318302003215842003 3db899e500ac6\
f1fb7a9e23f16a363e41b6d1f6dd5562c4faaa0491f1a74cbdbd039ff2b5824842d4\
da26c36173bc31ba2d1672699d871fdca27b9af0020bb580225842012ecb4d569869\
085618ce0a4e0f82fe9b618dae8b678e26e7a1ed8d8b9bdf7ffcd32dfdee1bd85ee5\
2097866c4f493a3174e6abb6b365057d212ce3d84a5010a6df235842019f28872f68\
9d9c3a8018712e453a23beac37cb86c87e2c5a99d7e3901f2e4f4995fae274ca0774\
                  8a7076d0ecae6466a7c3cdbc55d233544a59d22d3e4dde1d4b5f
```

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

```
Ciphertext: \
d8608443a10103a1054ccc2242d4757e17d25a15ed3e5821365e04f0c6e4952c0b79\
454fccf76cbc28b74a46ef05cfff1b9f8fd9990c13cbb98183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b652358850401420aa4c4c627f798133196b5db1d875b2171c72e9b4a99040212\
cf7493b3e3bae6031b1404fb7310b87572d3f3c2cd47d6af96409898c6a0b23f9744\
881ffdf496002591f0a73a97e9bc10f816e7d6112c1453c641710d63ccea38cff636\
08acd7f422dfb1bf6a06eaf8faf2042ac02b2edaa99609d652bbae462023d3d2dde1\
3d502858300ff6a2d8cb8b938f26787174c9dbfc85b39f1482755dbbb83d0da19b92\
                                34b4317c2281ea39f18ba90ee0dc3ebac535ee
```

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

```
Ciphertext: \
d8608443a10103a1054c3ffa359ac3825a0c2494bd5a582181de3200580856ad1d32\
e3b048a1514f876175490eabaf16f8c77cdb29b5a72ff48183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b6523588504005a008e6048f592980a269593795a2477b6e2483bbd5c4905f8f2\
7a13da967bee0b14ef17267f10c09096e3b782c07040a835d11ef75b14e08adac9f7\
9dd99db0f800e024d2c2f77e6b7719801c8057e63c8d947698e414bc76f89c7aa9f9\
32facd739738093662b89225a5d6a8bb5837f94ff50d0cc87e220c33a2c3ee2b9558\
39c2b75830a973bd72652388fceafe8c27fabcf6cdf9d126925139036f0220f25cc9\
                                9116ef84c6a0973da27296cef25e15430dfc81
```

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

Ciphertext: \
d8608443a10103a1054cfe0a853f493e564b510e6da158211f3736313ee0ed512ac1\
0ab2ae6b285dd11e627ceaa05307c31685e136a0a13ff68183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b652358850400aea55d98ba99de025f46405517e8768d81c96d59bfd2fe3f9157\
ac4d8d32ea62ad3f67775fbba8ad83f29e86256df856bda826504f4c46f14283c3bd\
faa575075d001a20e9a1c8ec0dae6f77ae74c2247bc99d2aec355fe678556abd21ec\
c0a31d666667d9c043d36d29ca513af1cd4b6fe5f078de2b250663d966ba451a1fc6\
a1b28658308d5348c71c2e86d8f23cc19891ebf4730710612677b806ff0682d65127\
2a656327867fd99f427d053bf2f5c7865155d5

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

Ciphertext: \
d8608443a10103a1054c594ca1298043f224fa4b1822582127fe011f834d4b3c781c\
4543876d72b98706c79718946f250fcae28816f0c2ed308183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b6523588504010d31e782460f310a82303af9a65af3dd13f1c8751ce5fe0798fe\
c6551691037f9cc0911ecc072e1620a15dcef781f13d4149dcd50720ebe45d474304\
7625b8746100137e3fe917b538af7ca2fa64ea6344dc64ff1de4dc89224ee57c8081\
f0b0a9b0b3db6756fe7560d961c2fddcf1ea9a0095755c4856c1280089174a642961\
edb76f58305af395d823c5290ca4256b07ebb8313ad2fff37da1d27cbdfad189ad89\
356f38386ce4df7cab985061df152ef9e75498

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

Ciphertext: \
d8608443a10103a1054c0c5f9e93aa2b6b33064f0b615821d324eef552572ca180a5\
d0a842b0f99791ddfe4dbbac7c239edadaed6ba2d34dea8183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b652358850400271889251e67d6bedb6fb4d7b2a60f989dc445219b2e11990114\
bf199f4c03f37fa77f1b9d5afab0ad8e27c0b0419bdaf20c36e7f952b479755be4d9\
f1c718a66100fe990106e4618f44fb9dadf8eef57a40a4d4e827d4849bc043191bdb\
bcf127b190fe357b9537b4e29c13da16465e3d51a836833c7f379829b06fc88da62b\
ad337958301b9dc03b16d574206eec4dd105a466065ce9aff843c6ffff4faf74b843\
afa58a4f8ffa1d289589876eaea3e6d7fcd2bf

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

Ciphertext: \
d8608443a10103a1054cca7d6047cc45ccdd77f890035821a3aa9aa763c441334a09\
047e7fbf0fb29359f906e008721d7a8d2e5bc6f304c8c98183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b652358850401e15cf2cfd07ffc3711a2a3aa999275e22aa7293cd024b2d6c19a\
793dae6ba8cd6d7cd8e0ad09ca84d1989435bdb248bc354043ff16dbef35fd3976dd\

```
923eab027401c57e9e5ad3e23d0d8ebfd403fc5cf205d32d9cf9c34c39eeddff1e3e\
e9cb7e2b68b7d0ae96f476fe2574a98ca262afbc5d419bffdbc659a5351e2dc3f1a5\
8657b8583021539e5d740e58cb0d5a82ab9f05f2383ce78a3d2bbd6289482fe0c72d\
                                99094be91be74b2b321adf225b20a1fa4dc723
```

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

Ciphertext: \

```
d8608443a10103a1054c6a7f9ad577d1fda19f57eac558210613ac0fed5e66dcfc88\
8e1955ffbe59e991896f466ba4a36d35c8028cffc99ee98183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b6523588504006055fa4cb5b85e543dd03decb5aa21d4fa5df4f120e08b92380d\
9c101f6d18e9267c17ddce47fc2c9246c445f637aa74ec24221e731177951eb7def4\
1c81a0c7ab009c87c7eff17968be352f9f912f5eb2f02b56010b3bd42b99dd4e17bf\
479dc20ff9fe7fba5196bf05e2780ac19d06ab500f87ef340069ecd664ea7eec1f74\
7cfe3c583087cf7e83ea5377854ed51220ce62123fc976ca70198b37c5a73c6073d5\
                                201f887c5dc1cff08a83b57c56ad18807e5f89
```

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

Ciphertext: \

```
d8608443a10103a1054cbdaab86150919ae8b5b834845821e7e2cb618527db518b18\
375aa7edc6857f72978ad1385819a71eae01647779fcc78183581ca2011830245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f32\
5f6b652358850400e6d1c1707c66ff216bb5c23177b1d45da5178304e5bce401100e\
1692e00734b6274b607cc5ce673075c3d54f0711c4c0d7051f625f35f086a4962df3\
29777562a1018c3ab86a3f6be3bccf531413fd58ac66d7bdd1e0d9f9c57282282d4f\
2711b1f24d1cb342a8125edd9879dab0a9fd8e7f991a4d0ea25ded2d858393cb05b5\
4d44db583085da334be4a72731e8dbe28d2ff71e5fd3879a1f31ecac6604d52ac619\
                                2627a4d52e347743374aae7baa3f7b6a43f052
```

HPKE-3-KE COSE_Key: \

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

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

Ciphertext: \

```
d8608443a10101a1054c087f1d07a0e87c270e41d4e15821d1b47d46b6df77e9d3db\
5228d0af3f87ac7ded5a31f8b382e9b6389f9033bc53d78183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b65235820c1ccc94d662d3a8b07f50fc18624f8e100ff316c0ecf1bb40b5505bb\
9805186658209f7f855ca97be8661aec7bcd9224d1dfbfdb2d503097f2b17f909c3a\
```

8903c456

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

Ciphertext: \
d8608443a10101a1054cd33f6f7b5cdc8974a9a194c95821700162943b4f55c1b8fb\
de676a17b0e59d1bfced926db14b3f2522257a8439a0d08183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b65235820a64d042825f9b6c7ff0e2149c805e6e75846ff6d42e550d9e4345fe1\
e5e2b73e58209bfea8b775bfdc0ee1203b3299f942e0aa267b43ac9238dca623500a\
79e88c5b

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

Ciphertext: \
d8608443a10101a1054c221104011e8ea554d159fd435821bc7626f9f2859dcc701e\
4bbe528ac3f16397cb89218f12f929a9b8c479ab879e258183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b6523582003423f546a5756386f88f993e1f57afa983e9ac0f393dd35f2eb596e\
4b37214d582074ee55b4271f58420b59914df0c75ccf8f8245c98d1561f4b1e14137\
5ec3ef30

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

Ciphertext: \
d8608443a10101a1054c6e2426b72d3c281e3dd415855821d1c7b5b743119c68efc1\
4cd2306ef9608163ccb4e3bc01b56fb3dd76981d9d984b8183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b652358200ddb597c69ba1ca599277babdfc34d650723f821e4e8a701f1c965ab\
e678487658200b38e6ca680ab97618d2fd73ee7a6ef4e6dd90458440e7c814e20ad3\
02d1ab90

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

Ciphertext: \
d8608443a10101a1054c328509c1251bcb8d0dbc707e5821febe757b5d827288f28b\
d57e1889aae48b17371a9352bc147f27138bcb278a82008183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b65235820b497b974cb4d8e7abbf060530d6ad2802916867dcf94302bac134f3a\
e7dc080758209126e88207469f7fe243adc8390d58360f3da239336f2bd39d4036d6\
28edb2b5

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

Ciphertext: \
d8608443a10101a1054ce25671dc8b3a673b3e7a54785821d40477eddf43426a8dd6\
abfea7f1c3e4a76d555b0da7c4f937c9a928b1da2632238183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b65235820aa871be16845e8be952cb3112468056f34751da2b89c03455481fe24\
b4608d7a5820d484b6f27e33353092be7b4b8327e70b8c199cdd8b32ef05bb3301d7\
d7f979d1

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

Ciphertext: \
d8608443a10101a1054cc133201f78abad8f59a36d16582153d41d6e440506097061\
17926531f6db33cdae24e1d9893e267693b1358c7af1b28183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b652358204d60a40af7bbdad596c05f8aef4d2d59dd739daf7f2d8207a4f37a98\
7139f87958201a8ef70eb57a722695fe79a2fc172f3c1a02429a34d6c52480a0b1c6\
881fc120

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

Ciphertext: \
d8608443a10101a1054cf3790340c81ab5a03782c0765821c62bb5ba94087b77a776\
ccd8b36327ead7c07416d3942c70e73b8094423be8b8648183581ca2011831245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f33\
5f6b6523582091bf7afbdf0312af1d6ee46a07054d3190eb80f05a5fc89d04fba713\
7a87680a5820bd31be117b7a760601d2a93ad2b578fe7f95643ec56899f9ce28a373\
fbcca74c

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

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

Ciphertext: \
d8608444a1011818a1054c007db1e253c05a77c7960d2858211646cae1c09d7432bd\
4a42f6a9abc25b9a09defd157f0c8e880724d09b71bc49ac8183581ca20118322456\
456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
345f6b65235820f1ba3848ad6162363ad57952fb7870da525191f620b8fa5bb1d593\
174c17232d58304635ac73d6e33966ec443b7ab017f9185571ea010065d8862ace8e\
2566b7c0704fe947fe56db64b10e02766c427f83b3

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

Ciphertext: \
d8608444a1011818a1054c38d3d704efa38c029752ca1a5821592b56f3d76bf573b9\
1bc7e2454cfbd71c25377e99c59748d4cfe554d4feec68558183581ca20118322456\
456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
345f6b65235820a8c00e9025c381d4c2b9e4bfdea3f744b43966f22ae48e84521d64\
d89e66c810583007207152 80fb5e662bbac5700a8a59d9af170a68a0bec9b7f6fd3d\
3870fc164df3fe40e0078388b593b0b7d7400edaa9

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

Ciphertext: \
d8608444a1011818a1054c5bb9f3db5220811a48fa5dad5821c54c547cc13cb4ed50\
c07349cdb64bf523b5e260dacf61299ec84fd3628573c5108183581ca20118322456\
456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
345f6b652358206e9b9742fdb0f846332cf80cceb256dc243d4c71bf9dddc476ad58\
3b5935e94458304755506fb7b96fdde760f4bdfcb039313fbb817fa0250cbfd18179\
0239fb53a252486461ea900e2cfba2758444d2e0f4

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

Ciphertext: \
d8608444a1011818a1054c3891481162c2fc91acaa558558215f3161419f70905c9c\
a38cc7345e3f85bc80a805b53e7f972610a7b9fd50e92ed98183581ca20118322456\
456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
345f6b65235820e2013d9d7f842e6d1063fe388fd50ab4092840b59a8e1f6817adaf\
3be6102d69583047739a107287144a29a8778b534db91d3c12645188f6c90a57cd6a\
712bebaa8e975d19c0294a82ac570fb5ce7ca7dbf4

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

Ciphertext: \
d8608444a1011818a1054ced667294b551c91b234a775b5821a940898b738c95090c\
00dc03e16331da77e14cfe9378bfbfa6bc23b3520811bb798183581ca20118322456\
456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
345f6b65235820cd75b971e1d7b49e30dbaefa69e531d6edd27c67152eb92e87ab8b\
d63ec48a77583007ee898bbb19a31de857d5f763b5366d3ff2367774da1ad00ae9e4\
1606c55c662d6d76c79460c993be8658159d2f9e7c

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

Ciphertext: \
d8608444a1011818a1054cff75207da353490e289408f358213306e92a51bd77b669\

```
   5fe3a72087bea5609a47c1731ca9b0fc3a2e7e3b2187eed88183581ca20118322456\
   456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
   345f6b65235820f4211e14388db2706d40bd7f80dee278ee8fd586bc968d115e9ce8\
   e81cce695e583003ff5d044c2fc4091b8f686300035f17a60a60cc6189880fbef4b5\
                              e4d578e6044b713e91be66c7f3ff5574a22f1e2cee
```

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

```
   Ciphertext: \
   d8608444a1011818a1054cfa03887e5d1a0a3334a142605821f03ae21bf3aca4bc9a\
   62fa1afcf539408dc67c1cb6de84ad44753b0db7f0a0b0178183581ca20118322456\
   456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
   345f6b65235820ffb600a17c13480c8401088dc6428c9ef2f88db2c9dbd195fdad35\
   dc74f0370d58303e6b9e912295318716dd673b0baa9fd0ef59ac37b96049e09a1261\
                              39bb3271837327747b5082e45bf31dfe1e3fd90b76
```

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

```
   Ciphertext: \
   d8608444a1011818a1054c9d81b36afd28e2c8bb3246dc58217a74391bef4910236b\
   2dfc964450d14ebfcf93494f265b08423180d9c22974e5398183581ca20118322456\
   456e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f\
   345f6b65235820a0b49f8281353307c0dc52ae54ba90233e48354fcb0ece9a8161ba\
   ce12e3b12c58309aa5bccb1491687935dbd8fa4fceacfe8684863d7c8ced8cdbfca1\
                              b89d4fd1b0ec36fa8e9f11d2b74d33c8d05a3a3cc9
```

```
   HPKE-5-KE COSE_Key: \
   a60101024d626f622d68706b655f355f6b650318332005215838448 9c1479ccd3534\
   3a90b3e1cb4922f73d9d611f12bf4abe9f76fcac6a6a974c0941fa602dfc29fb5c52\
   b3191ea896162718d2ddbc97097e235838785cb877d73f034edaaa14d66dc3e10bc2\
   8d3ee5a290310c89eab7e347a82218874963600cf36850a389325fcbb6e4477dcc0f\
                                                              1b65e860d9
```

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

```
   Ciphertext: \
   d8608443a10103a1054c2949acdb90b1015072b80e675821ac065f314f080a5dfc2e\
   3e06f4f222a3e4968887957ed0eee16250ef785ce5e2d78183581ca2011833245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
   5f6b6523583802a6da874f6a2620194f7b731099296d1e9512e955fd0f50eaf2e5ae\
   23a000962e852ef245d8386aeee37cec14718fee3034fd01909f4d2e583099fdc2d2\
   ea5a9801fcd7f6bed9c8ef7d4d32cbd87f3f3bc70537647559a745c43a4af2ea38a9\
                                                    34592ef3e6b03c8f0268
```

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

Ciphertext: \
d8608443a10103a1054c53f4e2fb1df67a865219e0a2582152dacd88c76f015f633d\
6158cf8c539629c0693c3cb862ec9488c37b8eec30b9da8183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b65235838c98a8b4db3c46d89bfe93148b7dc65c9a4095b8641e14ae5e1fc14bc\
e80a297ff8db1c12a061583109bd53bf175b13c543013a79142c9f885830cc808a9e\
cd407be466e4920a325828358609f3d16f810ad88b555d414b114eff43796e25a98e\
4a81551e77c0db0be185

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

Ciphertext: \
d8608443a10103a1054c92e5591600c44ddb2a13c42a5821d07c0b52be682945ebc6\
4346c4c478a81c908bbcb0a899ac124db1a463f65daeae8183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b65235838b69945ef0932a2cc47092bddb812af68730f078f9743b0d208bb482a\
a3abe55ab342d848868ca56b6b44a1f0d5b510bae9731583c6e4c1245830aa6de151\
2ab91d07cd1564280d70414b85ddec670143870957a52dd14890ca68ff55616b31ab\
c9556f10f250cf531d17

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

Ciphertext: \
d8608443a10103a1054ce1ac34677cb6f7efca36107058215a8e9539e3bca5f0bef9\
447427d94dff836daa4d79b349bcff1bb0351f5bc787448183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b65235838909d1444000d3432175e9539ef75a1c41999b94456fb16668fc280a3\
32683cf4e972697291702272f56c9021a3b7f8024cc2a539c1c3a4cb5830fccf12ec\
bdab9273a37fc45d00fe4dac4888715816d5a47abeb0d8dab1d9e05e2667ced3873e\
afc2a98779ba3830a720

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

Ciphertext: \
d8608443a10103a1054c5195eb4a8fae34d39cadb9535821ae6af0ad922d27c668c1\
ab70e1d560fcb40a562872fc380335885e704bed0ddc258183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b6523583845ece7f96619b1a46a607a7d1a3005cd57d1405c605a19438b6fecad\
ff2bfd992dcc396e16acd67756fbb1e24dcf03c3c1332c468486fb6a5830e96b44da\
4b0a5c72d79a8dcabca9bb212e0d01cea57670e0b1c8185b8e69377454b89dfdb3c0\
b6dfe485b8128549509f

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

Ciphertext: \
d8608443a10103a1054cb10539a1192ed9218d34293e5821ae4e7c28fc0395a88075\
1804db96a3081d660d41249df20af74c52807aed082dac8183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b65235838d2eaf84753eeb391939fbbf417e80d11b083a91fc3f13655a5ea75b2\
b08c30b1659e7e9d09098b0ac50328b6a4ed2c261e515c7d1c9ac79f583065ec2f9c\
a4bd6cb2dfca13d897f67634f16262ef3aa0b000229670be2a8f2e454ff2084cba8c\
1e9699f19db62ea92c78

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

Ciphertext: \
d8608443a10103a1054ca12495344dac41a7c7c7ac8058215cefab72b215a994215d\
36688be01de3e90f585ad8b5a0f7855466cb0c7d3a72a08183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b6523583866c5d3d74fe18a530364ca2982b8a664e3ad3dac86fb2b0dc3fd66f0\
95ca475c4cdfad29ab1ab6fb5a8a514e30505ea0f4459c0c1d841c185830015871cb\
6615e642462a72d563289faaf0d287506824968e4f8f1b12688e48d19e5a2764a31f\
a4d5de64cc0becf9d1dc

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

Ciphertext: \
d8608443a10103a1054c72969c20928bc5e5f2668c745821f2643a6039958696c448\
ac0d63f55132b0830c66b0f3f7be73b76502ba252ca1858183581ca2011833245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f35\
5f6b652358381845442818d953dddeebb546a1df6e0d17eff174b627fd5595c39700\
ffd56b85b2b8283cdffa4a69d5a4b0c4245ebae0f1d6af52f1d242425830af4f63c1\
b416befb1545c9d023ca5fde88b5680ed8396af65e2bca55af6f97225d505dd202a2\
c2a45367985428568509

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

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

Ciphertext: \
d8608443a10103a1054ca69651786cd0897b5897691358219b6332bede2a83db731b\

```
   bd15d7a805bb862435d78dd5c1ff0122bb1ede839e8f728183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b652358389fdfccc85fbf60af97e178569d37d06c55d2aefad63a769d9358e4c7\
   a4db1e06cb2ff9126cf8ba125f42e41f2e0e7f53557096b018cfe657583094a8e0d3\
   9a7b9448fa610fa26114c5c2e86515b77db6006002d81d41f01c5c2cad99ebdcb246\
                                                   e5b7ea8cc14812fa1682
```

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

Ciphertext: \

```
   d8608443a10103a1054ca2559318b1e333c7e6274a4058212be18e3179d2c262b6d8\
   41a581ac30af8eb5bed1ab3cc05beea9c377bcb73ad738183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b65235838371bf6961ade4f634f071fe738b15f3627d82c5b6f76611ab45a2165\
   dccd33b5df3bbf616438b5164e19d164b745b1bf8212d1e5fd270ee058305871e52d\
   5794c7b8981d6b9c92f40addb7caacad5c81b85d887b096b7983a26854b7bfd3e336\
                                                   edf71ff4874f64d89d08
```

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

Ciphertext: \

```
   d8608443a10103a1054c2492b09ef4c564fd3079631458213b9529ae9c7356f2dedc\
   7a682efc6c24548e4bbf70f22931bf0822efdff05b4c448183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b6523583899433c8f53fb59a6cd1645e4370c1799f715035fd931b2704f821337\
   8530fab0f8f0457ba228704c27c720436161feda841b6c2491c73a0258306ead1c6c\
   35e13916e63b2aae6c0e265219647b9c86bdd9b77523c1f5f12050d72cfefb7dd45a\
                                                   691174a2d2dfa64b3c9b
```

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

Ciphertext: \

```
   d8608443a10103a1054c57140fbf12fe8ab78653abbd5821125018d5b069f071d283\
   da80c4188b2ca95d3b92df274640cdf691b9535261283c8183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b652358384b335276cad00164831bb40671b8cf443a600bc4c03fd5adc7593e83\
   277f9b9bc772cb5a4fa9c4cdfc0e8eee326a61b0cdc60706281221e458302d23c12c\
   20bb3f3e1d8e76be00f1d0d1c066529767b17b0d7d4bd050af65f6f45e8868374e71\
                                                   03aa077ec74b3a0af7ca
```

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

Ciphertext: \

```
   d8608443a10103a1054cf38d16e6fecb152da995e2cd5821135887b1829e5b6b38f8\
```

```
   4dd33a8c6fa4be19e2effdf014e29cd4a3a42e19bf2e648183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b652358385a727ab6eb38b0db15c0078048f91b333bc3b16ef5bf27129afd4638\
   7d92e0d494fe19b2133b6f4118ab54fb0396cd135907a8da82de7421583056175cb8\
   e000b71129adfe4a90f00ea734ccd524a2009c076dae4de3ee4563a94b67b245a019\
                                                   23f28931565e17fb4c70
```

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

```
   Ciphertext: \
   d8608443a10103a1054c9ec5330828f36f9d71a63dc158210433f428f9490b8d61b8\
   1b140df333101bea7a89a44227ce04525110ca3f9c331e8183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b652358380d8caed0c439f7296a4af94201673ff65dad8b54d2ec7af206bba9ee\
   672ead43641a5d1ce8441c3ac80e171396065092a0f12d76e5a5c3d35830f0a825ba\
   05c5d3ac504188ddf5fd6f786c0ee8cb03b13a459acdbc87584ac4c466959687efb5\
                                                   40a488d778145841c247
```

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

```
   Ciphertext: \
   d8608443a10103a1054caa3c1c35c826e19ed11adbd35821cdd02a3b3f8483b9e837\
   ca924628eb7e434f1f61e3361e2930dc6df8c04342d2398183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b65235838df5ea2f46560f2d895b441235a4a944dde842322935dc758b775ba6b\
   e2a80ec2072e04e6c6594020794a51584de7010f533f48330fa6761958306ea42d6e\
   0eea23f9173d4e05d0b9408acbf10a4284de448c75408cf9efd2b2d000c2e9c8923e\
                                                   3b1267a754f3f671df13
```

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

```
   Ciphertext: \
   d8608443a10103a1054c157d92252756da81f082fea3582145f89806900cb69df104\
   94c1fd9e2550f1f4a727fc11356cefb8d833cc8a3317fc8183581ca2011834245645\
   6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f36\
   5f6b65235838e40310ac02a7a041b6f1e62001739a09d604144f957563c6f7663e5a\
   106ea7d30bedf843c178d0f02150a81136cda53f931332d6fc30d8a6583094f8e00a\
   8109463bce68bcb9df796b353c5a54bb71adba0ac8ac3cf4180e4053a9770d063aff\
                                                   6dae41e131a4bfb66fe1
```

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

08becf7358ea89c0cda596cbd9705a6b7c6f0ae8d70a9a85a913

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

Ciphertext: \
d8608443a10103a1054c167316d0b8458d63c4deac1e5821330245b359b114ca9101\
d44351e6ccc673abd75b21f94eae183d2c71c3abc4a03e8183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b65235841049910ff21e19614d69e43ff5cb5f5ba1d017385c390fe7958df9431\
26826a8d03ffe527471581cfe065fbf3145625e7cff9a649eb4aefd8be949db9c1aa\
9a89df5830234e18c3566d93a9791fb4b5d1f206199fe89bbc92d6c7d58166bdfa09\
bb32b310cd345d869ac15fd5cc895e2e3a18bc

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

Ciphertext: \
d8608443a10103a1054c75253a8c0de6d5ec21c3269f5821039f752d03e974aaf22b\
e52d88d692f33db25f5984a4fb8ce34232e0bfeab9f57a8183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b65235841049668a18483f3698645cc106c9ab6929dc7b48c088fd1ef331848ce\
479909e51e54da829de26b2cbb57b83c4413f7744eeb484126571369651808f18271\
c1fa8d583090c340157fe5691712b968b9686ca6156aa80165f03aa5167da1d1e868\
168a76af54f05d9847fbc15033f8eb45a1b9b0

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

Ciphertext: \
d8608443a10103a1054cf941d22e87d020bef0c3406758216de86b483f1b5eee2126\
a57b56e0db30cf4d9bcf99599ef8f18074490e3c0eb6dd8183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b652358410445094b593064e8aa69284356909e281d2ff1e9903fd1fefe4e4d55\
c885c445ef68ce8dd15b84107a2f36187a243e342a42f651f71131d6c9b1f7e55de9\
671977583038f9fc778ce6c87feffefab16662aee353050ace99291c9ed952842c85\
87f4eacd9d8ca91b05d05b0006fd0c908eb65f

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

Ciphertext: \
d8608443a10103a1054ca426b061751bffde093a4e145821acca6ff86354e4a5b466\
bcb37c639413688e854801f7f1b95bf2e122c3f63fe8fc8183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b65235841043bfa3b80b70072d4fbe1bca1883775e80ffa456f197314432eca7e\
297bffb66ba02b91e8ec45b027c54b1c4a2446e66ab706e84d764a7eff7a6010fb35\
fe4f1b58302c390dc76fa2c1c2fe81386483c50399c2493e04fa8fd21f2b588432ff\

7abcdfb39be10d952b1e085f2d7d4ec16a91d4

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

Ciphertext: \
d8608443a10103a1054c4cb112a7d93701df4be38e355821bc0e02527b0f9522166d\
cd969cf78a3ea79a531bf6e1225a585d8808ca7f9b0aa08183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b6523584104f07eb61cf10bb413bab1a74e55aef40d872d1510622b7c94c680a5\
9c48633fd389937703cdf7997adb367e3295bba8dbcc4fe6c7ae2fe6df96c4e72210\
a9311f5830a73675d9a635829fa39b185d260dc98648d7590f8df23e7f0b5e20c4ed\
d146ba4e1a5cc213508c74abe6ab196fc01b3e

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

Ciphertext: \
d8608443a10103a1054c24a18c15e63d780186b738a8582165b980d65f6ea607febc\
873a4c7c350a02a2626b1716c2877ea275ccc14758003d8183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b652358410441346709ba380de20e4a2b57f0220aa97f4e3424a8a54565ea7277\
12b3380887bed1ad53ea2a7f7b3e3df5ec3fbd3deebd25d2cee60523ce1a49aa1d82\
91d1ef5830d9794b996b0a36405bddaa95c2ef92cdd18ba3fa7c089e020228aceef3\
cb5f8599901c7549f0b6b91a9428e3de9c7388

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

Ciphertext: \
d8608443a10103a1054c820bd36d521e62ccbba28175582110888bce69074ac614a4\
d26b196dd8891a562fde2e4b9b2e80f15ac90f1414e4c08183581ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b6523584104651dddd8671626af493d4f7c2a2df9621831977651dd6bfa4d6c26\
65ca34bc2760b34ba705189d11dceb9df64ebcc1d729c32f707f2c4fcae679f6eae5\
3611595830b2ce3d5b51cd60521ebd558bd9a35da1c6967341be0c95074b5835fe83\
9b391630d2ec12a90fe2023d7e407fb4688833

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

Ciphertext: \
d8608443a10103a1054c3dc36ba4b79a00a477ff9e305821890243f0ba9651f3ec49\
cd49295e2e373c4e59c5e66e06603f0894741327071123818358 1ca2011835245645\
6e6e796e20447572696e206172616e204d6f726961a2044d626f622d68706b655f37\
5f6b6523584104e63b411c176d4f6bbfdf68c8a0d4d3523111f51e0907559ef602aa\
8a8380bc307e6e5085ad17d6ebf55c53234d8884218c32dc6773b58b6a6b78d801a5\
3123815830986e51fdac91f5101a2630e4dd1a01dbfbeb4cfbff62fcf922fe416250\

761e1dac5e1ffd0c1912da9a7d09e1e7b56a31

HPKE-0 COSE_Key:: \
a70102024e626f622d68706b655f302d696e74031823200121582066 99b067898b7d\
2d37db0da3aecad4bdac1558870b47d67d080d6049fb81752f225820b0 1b6da1f210\
f46e20e2b552a80f4f6b9a3adad34a6701f73fbbeffb174cf7412358206 716e93d65\
94fbfd27016daada9ccc8e6ba2eea0e103e3d7ae22278f6dfe124a

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

Ciphertext: \
d083581ca20118232456456e6e796e20447572696e206172616e204d6f 726961a204\
4e626f622d68706b655f302d696e7423584104f23febee7bb712b9a862 cdd08ddda8\
55633e198a906ac36ab202ee33f059238c96684f3a85e3d042aeb4ad1 f12b4af79f6\
0817dbdd4878abdac88639d291aafe5821c9d9d8be25960450b25b126 e8bf9053153\
d617d9497e56daeae9e267d25237fc90

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

Ciphertext: \
d083581ca20118232456456e6e796e20447572696e206172616e204d6f 726961a204\
4e626f622d68706b655f302d696e74235841048bd0bc0dd8fa65cf4dbd b127b61b47\
2f2c41fc343b51e80394b208e36ec8273b0ffa88cffd9647fc2012af61 708beeb901\
a21f38f4714113ab032497aa2680285821e239e5097383def6a168e02 e417c58c45f\
f0949235ceb3478a34def09f91f95d98

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

Ciphertext: \
d083581ca20118232456456e6e796e20447572696e206172616e204d6f 726961a204\
4e626f622d68706b655f302d696e7423584104ff56eb1cdcfc285094 720a12f95b87\
f715cef62ad4e12da36388a6e33d2331055b0551e377ae048e8f7c6bf baa1bb2a4ac\
c9d644f9f215902248ab72853c9ef25821c9dbff1e9c96dfc8857b6f 4686761765aa\
9f9ffa6ed11f47412395de7d127b782d

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

Ciphertext: \
d083581ca20118232456456e6e796e20447572696e206172616e204d6f 726961a204\
4e626f622d68706b655f302d696e74235841040750562be6042d2d49de 49f425c93a\
bb762db06c21e65c44a2faf9a7a619152763979d1cf766e7b6f0eaadf 6993bb6fc35\
2fcb66220ddb6b73a13fcef6a8d092582175c8906db9fdb31de6a474 cb93dcb8b026\
9f607b0503cd37ae0d47fe1ad5589271

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

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

Ciphertext: \
d083581ca20118252456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f312d696e742358610462a69a790932356229ec34f5d53f65\
b38353d6a99973dbd2bab59bba608c3756173688a473bab9eda926655187d8e30ad0\
f72c91892022ffee4a9a49fac0bc0df172073964a310ef201c62438fd3ebbd8a297d\
ca717fc9972c977330efc5bfd458216e8e7db08234904f3620219f45ec852d4a0b12\
3be5e7cffd5c75cf6816f0cedc17

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

Ciphertext: \
d083581ca20118252456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f312d696e7423586104a4a2ec754d0f4a811668e6ac3c52b0\
ae313b7b7361334503c4be9566b8af64e5af14ff7d723b5dc8af9a573f8d6f66dd51\
86d8dafadf77e40b94180a2a2e8647dc195c571f4601b121a733234ca8c0f556aeee\
b4b151e8cdfb493fc620b9935e58212a6cb14bc91b926626a793eda9e6c0e5328112\
d3067bfc766f0eab6cdb5570cfb9

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

Ciphertext: \
d083581ca20118252456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f312d696e7423586104bf2824ee4a475b7c58aea6c9e0fa13\
f2da420c0f5b08a104d9ae5fbd51a2b3fe932030c54238941dfdd88c9cbde1d0f330\
54eb5a441af509809245214b77aa58ab82152d239ef754ebdf73864e16dcfd2e1c29\
5f1c65e6c237e3a9255f78d8225821e179b44ac3c887139401039f42d25ff710fe3b\
80328f9b371f62146667aa2d7210

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

Ciphertext: \
d083581ca20118252456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f312d696e7423586104bffe07fb09f56fdd1baa874b6bc909\
706e373c676e5dea6d8d1f8c92e5063ea46129a110f36a53068b56627a32947502d8\

```
   abbe0ce240b32f3a0c75ca117491d9515b129ba8913d8da8176dba79b0b241773a99\
   5afeba1d81d01a04453801fd855821b95252647cd812a2b38feb687a3564d09cb099\
                                          ac4590056dcd88729fd7be71c6c2
```

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

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

   Ciphertext: \
   d083581ca20118272456456e6e796e20447572696e206172616e204d6f726961a204\
   4e626f622d68706b655f322d696e742358850401d74570333d518fa837730d40d7ac\
   86f0503b464874f1843f870ed2f57cf08da1913be657de9714dab042f8483e15ba03\
   49b807288b97cce9a8ca14e5c66d9a6ff1014fcffc12c393534fb7d2929a2b26184f\
   911b3089f579e106f7743c0eaaabb789d22ba7b420fb37a5037ec926db6a85b5bde5\
   b43a253529e8a12e9578228453553458211b370f77471c30e197b98ebc48e6662661\
                                       827a2c6d664797b27967cd176b6867ca
```

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

   Ciphertext: \
   d083581ca20118272456456e6e796e20447572696e206172616e204d6f726961a204\
   4e626f622d68706b655f322d696e74235885040062 8d4c1019cb421541cdf46606e0\
   d80206211523ef5b76d0655f410d4204f04dab82e9462ce30169a10741d158169e06\
   caecaed8542218bf7842de8e36cebc5335008b663469d754d5f160ad6303801f9d17\
   af2ea7556b5940c544c3e3a017303c2e04ab4834f1d6753fe20338f361a3f2dc24ab\
   3e41b36a0dc0b5ece3b99acdec4d735821ed51b9a3be09019d5177962b516b50c8f0\
                                       00fea6f24f3b39a5c921ab5d2662c8b4
```

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

   Ciphertext: \
   d083581ca20118272456456e6e796e20447572696e206172616e204d6f726961a204\
   4e626f622d68706b655f322d696e74235885040141316 8c034153ff5412b056f786e\
   ee6a2c2ffa3ab0afce8b3cc0a3f66c751acf0f7a9ebd02df7814ecb78e8fde1b13a5\
   e529ac52c5d7fbf68c399c5ee8197f1a12008d327a2257fa5a8cecfb7da717b6f366\
   125b85152d2f13bf105cd9cd4820c5eb5bcb518eab1fb1d5b273b64cfff07b01c412\
   0ff5896a793f2ee4fea6096d8e174658214e9009d4dc438d26e0f9516d123c900978\
```

```
                                        03d0168787f131f708c7ce6457130ecb
```

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

```
Ciphertext: \
d083581ca20118272456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f322d696e7423588504018bb999dbe22b1b3439edfeb27f4c\
447927bd05a5e417da740dbb7b60fda62f035ad91e1e79c8a9282086ba5e42309ecd\
2f8123b74fe57a65ad423b118572ef2c60010b4896df57ad95464726b1309b4ca1e1\
222e753f8285be735c5a6556c5e624a31fb47ab960ea6d94832540fc1bae8f3d7f61\
4b16f9c227d416a45080a27107f7d6582127bf341ec0b515b66dd33dfbe2687d310d\
                                        f8f660ee56a09d0d0b2406f852b81504
```

HPKE-3 COSE_Key:: \

```
a60101024e626f622d68706b655f332d696e74031829200421582085eb6351a4e93a\
49953e1e23ade9504af68a73196a823c9a0654bf98c7536a7f235820f0b8ece6e393\
                    8430f36798eeea8206d0ac5e0577349ad63843cbbb63bc90b849
```

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

```
Ciphertext: \
d083581ca20118292456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f332d696e74235820108597ab12b01fa48c04f122eb9aacbe\
cccd0d3fb876cde3460a3aebf2ca712958217bd15efc2d505abdf10216048a586189\
                                        1b848f57578c2d2144602f623055c807f3
```

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

```
Ciphertext: \
d083581ca20118292456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f332d696e742358201121e279e47b8dbc3720437ee4530966\
c3136da22aed801b9918087f726b021d58216b525075513ac8eb0f4d5ea9d1558236\
                                        8992d4efaaea28918cde2d243e720632f6
```

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

```
Ciphertext: \
d083581ca20118292456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f332d696e74235820f48e404935a13a691a960e26f446a5f2\
b4d1d0da4d166c3a35644dfff2b670055821952f4c6fe9dfb90194a0c69a01927927\
                                        e557aa89ce70295dca0367a588e287cd1a
```

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

Ciphertext: \
d083581ca20118292456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f332d696e74235820508de89bedf2b67100e6cda1be48c28b\
9cc5b2b35ac951703bb8ce78f3c9134a582199b36466c873a8e09d140ef6c714dfb3\
92b079002bbb2b9078321c846af830f15c

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

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

Ciphertext: \
d083581ca201182a2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f342d696e7423582021d0e4cff502197444d775f94384b220\
a2f05c058bcc999eae5ae598e1492b2f5821ac10355029121d9666d250c90f889545\
2f71eabba23a797275f9491864edc6983c

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

Ciphertext: \
d083581ca201182a2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f342d696e74235820aa11dc7e968766fb860294a3ce1df34d\
66f19e5128694831f075d00649f7ef2d5821fefd34a5d08d53a6bb59f735b1c8d0f6\
ad4938e349aa5329146bed3ba2a3c35c23

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

Ciphertext: \
d083581ca201182a2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f342d696e74235820ea46850a7abf6443ca09ce93ee25404b\
2c76fe67d067c7a09470daf2e0e962765821fc8b71522f844cd814183552248a3778\
a8abe86029092f50549a74b7b9bcfe59b4

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

Ciphertext: \
d083581ca201182a2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f342d696e742358204898db0dcd020eb3b101def38ce47f88\
4b05ad99f0c7541af1d048ed85aefb19582144cbd534df529e438aae8ba4f7bd1590\

7593980252f825104785539fef883bf532

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

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

Ciphertext: \
d083581ca201182b2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f352d696e7423583848a105f9ef8438be88dc302e977dacd0\
57c1847ed994787bd77cb0a36148ee6496eeb7c78b7c46a4e7f66078dcfee87baf18\
1a93dc453a8b5821eb573faaeeaa2195fa6b461df314aa82a6ccb3ce06b497513397\
7c1fc425841e82

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

Ciphertext: \
d083581ca201182b2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f352d696e742358382993eda49b1207346e331a8d97050c40\
82d5c8506ec403bdf3de493d0989f5342739dcb1b5de3f0bce3980ce10dc0e0b041b\
86521ab2e0d558214eb68192111b742534dd53c202aafab429248e0e6e152ee89ccc\
5f5d38a514fa31

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

Ciphertext: \
d083581ca201182b2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f352d696e742358389e526c2549221fe7c5e39e34205fe8e3\
46c8414c359d62369294f6ac5dfa36299a062fc9f3e40c86cea7266de238e3ee0fbe\
c18836f0334a5821a4cceddd1a61d7a61e8c16857174b66f833f54bc3c6a70bfc586\
93a3e18dea0e63

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

Ciphertext: \
d083581ca201182b2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f352d696e742358384730bef518b80ad11cab35015141acc3\
fd91f7df38d02584c6b7a213ecad0e84ebfaa7035f1a7b2cef0d44d3edafe03fb416\
c6aab77322ba5821fc71cd39005d4727a1d0a5ee7e7b33535720744b072daf5274e4\

c15fd076878d11

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

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

Ciphertext: \
d083581ca201182c2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f362d696e74235838b79eff5e559b7be693277ef53c4886e4\
3d2b4a53674e213cd9fdc6b76352f6227d1f6656998e5968f413a3a53bbd251cbcfe\
cb5e8f3e89d958211da2c58902ff48e32b395bc7bdc111dce9a66f78e3277ee8694f\
3e16d20893c8e9

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

Ciphertext: \
d083581ca201182c2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f362d696e74235838c705abfaf2741be3da6f8385c9b90164\
a4e7ac0a6d7f941fbe6f8fe2cef7e00e1478cb359a38cc1a61b78e1a5af0583bf4ea\
c3e02c6f4bf75821a7289d191e854577e7b71c621b0dca07bdd3f139e12f9a7792cc\
40fb38587357e9

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

Ciphertext: \
d083581ca201182c2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f362d696e7423583894b33ece4084fc00af8003fb810c2619\
7ce6181210fc0cd706dd43a02b1b04c58218de64a265a6c87db8745d90e94e740ce8\
02783343c27b582154206a5d8e5b940d456e4ccddc19d7875ebc91df5964524c1dc1\
ddd593aa56e075

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

Ciphertext: \
d083581ca201182c2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f362d696e74235838b7dae578a90ef5fa3b5952fdb40e2feb\
10c7dfb47ae805873993d77cab86c47dad9e7b8d017022fa4d00c885dd359423f9df\
564dfa69eedd58217480864cefd0fb34401807d03a6d11a8f0a328039cd4aaf4822b\

32a99cd6880e5c

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

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

Ciphertext: \
d083581ca201182d2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f372d696e7423584104a5cb0610c7bf25f9af9ab8d7508a96\
cba8069cd04fdf13d7cad84b410e1499d5197f78a3284a201c302405af795db80780\
2b82edecbdcd96b57d6fc41d7466375821dd6eb02287a86994b4022263e77c70a82e\
55b29e3cbe7c20156b1e9ab451c97269

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

Ciphertext: \
d083581ca201182d2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f372d696e74235841041091 90d60f33234c8224c6785d5a03\
3bc301a02a0c773913d1fe7f9d25116212580f7b8a67517ca92be6b91e3da32fefae\
edb5d398586b8815a8d92412955788582166e4d17e22319951c9da4caf712f2f650f\
1db362a6b51aaa2ed9e8dd88bcbe39d9

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

Ciphertext: \
d083581ca201182d2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f372d696e74235841045072 5e39e4e1c9bac07b94fd977ccc\
2025210263267d2348d21efb8d47aabf0555f25c3a735b501c6fca4d2b10b9fa73d3\
de4b8778a491382e9432402197c74a5821d81c6327208ae1a0d73be50621127e0b40\
750b9c49ddff164630c377270093f48c

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

Ciphertext: \
d083581ca201182d2456456e6e796e20447572696e206172616e204d6f726961a204\
4e626f622d68706b655f372d696e7423584104c326776c0c10487f4f24cce1fdae6f\
dd8fddc3bc7bd4782832682a42162f33b067393c7262f23e260af725240635cde3ca\
b01e46ea722124b7216259c684bba3582119d96af9e02ba358bdcada6543c8996866\
5d3886d4911e57ca198f031da7b57fea

Authors' Addresses

Hannes Tschofenig
University of the Bundeswehr Munich
85577 Neubiberg
Germany
Email: hannes.tschofenig@gmx.net

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

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

Daisuke Ajitomi
bibital LLC
Japan
Email: dajiaji@gmail.com

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