Network Working Group
Internet-Draft
Intended status: Informational
Expires: 19 April 2026

D. Harkins
Hewlett-Packard Enterprise

16 October 2025

Deterministic Nonce-less Hybrid Public Key Encryption
draft-irtf-cfrg-dnhpke-07

Abstract

This document describes enhancements to the Hybrid Public Key Encryption standard published by CFRG. These include use of "compact representation" of relevant public keys, support for key-wrapping, and two ways to address the use of HPKE on lossy networks: a determinstic, nonce-less AEAD scheme, and use of a rolling sequence number with existing AEAD schemes.

Status of This Memo

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

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

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 19 April 2026.

Table of Contents

1. Introduction

[RFC9180], hereinafter simply HPKE, is a robust, provably-secure construct. It defines APIs to ensure proper use to retain its security guarantees. These APIs are therefore rigid and purposeful. While there are certainly use cases for HPKE as is, there are applications for which this rigidity is an impediment to use: networks with bandwidth constrained mediums, networks which cannot guarantee in-order delivery of every packet sent, and for key-wrapping applications.

This memo proposes three modifications to HPKE to make it more suitable for different use cases.

1.1. Compact Representation

HPKE generates an ephemeral keypair and uses it to perform a Diffie-Hellman with the static keypair of the proposed recipient of a secure message. The ephemeral public key is required to accompany the message, or at least the first of a stateful sequence of messages. HPKE therefore defines a serialization and deserialization for public keys used with defined KEMs.

HPKE defines KEMs that use three Weierstrass curves defined in [NISTCurves]. The serialization and deserialization for public keys in these KEMs use the uncompressed form of an elliptic curve from [SECG]. Unfortunately, this results in the string that accompanies the message to be over twice as long as it needs to be. This can be an issue for applications that have constrained bandwidth or that use the HPKE APIs in a stateless, "single shot" mode where the message being sent is dwarfed by the size of the serialized public key.

[RFC6090] defines a notion of "compact output" and "compact representation" for elliptic curves. Compact output means that the shared secret output from the ECDH operation is the x-coordinate of the resulting point, the y-coordinate is discarded. Compact representation is a way of communicating an elliptic curve Diffie-Hellman public key using the x-coordinate only. Compact representation will work if compact output is employed-- the sign of the ECDH secret is irrelevant so it doesn't matter what the sign of the peer's public key is

HPKE uses compact output, it passes the x-coordinate of the ECDH secret key to HKDF to derive a key to pass to the AEAD cipher. Since HPKE uses compact output, it can define serialization and deserialization that uses compact representation and thereby address use cases in which message size is important. Redefining the serialization and deserialization, though, requires definition of new KEMs that will use the new technique.

1.2. Addressing Lossy Networks

To prevent the possibility of misuse, management of AEAD counters are entirely constrained to the HPKE context. The sender and receiver have no ability to know what particular counter was used with a particular invocation or to manage how counters are used.

This restriction is not an issue for an applications that use HPKE which have a guarantee of in-order packet delivery, where sender and receiver HPKE contexts are kept in sync. But not everyone has a guarantee of in-order delivery of packets and this restriction makes use of HPKE impracticle by a great many use cases. Any undetected packet loss or reordering would result in the sender and receiver HPKE contexts getting out of sync. Since HPKE provides no way to resynchronize such a situation, the result would be tragic.

Therefore, two techiques are added to allow HPKE to be used in lossy networks or networks that reorder packets: a rolling window of received sequence numbers, and a determinstic mode of AEAD.

1.2.1. Rolling Sequence Window

The technique from [RFC2401] can be adopted which implements a rolling window that represents received messages (inside the window). As the sequence number advances, and a message is successfully opened thus validating the sequence number, the window advances to include it. The result is that reorder and loss is acceptable for a number of messages defined by the size of the window and messages deemed "too old" are dropped. Messages replayed with a used sequence number are also dropped.

To implement such a scheme, the receiver needs to know the counter used with the AEAD algorithm. Therefore, the sequence number used to construct the counter in HPKE (it is XOR’d with a secret base nonce) is pre-peneded to the ciphertext.

1.2.2. Deterministic Authenticated Encryption

[SIV] defines a provably secure mode of deterministic authenticated encryption (DAE). In this mode, a counter is optional. If one is used and it is guaranteed to be unique, SIV achieves the same level of IND-CCA2 security offered by other HPKE ciphers. But if the nonce is reused or, in the case proposed here, the nonce is not used, SIV will provide a different security guarantee, that of deterministic security.

Determinsitic authenticity in a DAE scheme provides the traditional inability of an adversary to come up with a non-trivial query that will return a non-FAIL response-- i.e. a valid forgery-- with non-negligible probability. Deterministic privacy in a DAE scheme provides for the typical indistinguishability from random guarantee of a traditional AEAD scheme, with a caveat: it cannot achieve the indistinguishability goal that requires concealment of whether or not a given plaintext was encrypted twice in a sequence of ciphertexts.

What this means is that the security of a DAE scheme is the same as a traditional AE scheme with the exception that encrypting the same AAD and the same plaintext twice will result in the same ciphertext, an outcome an adversary would notice. Unlike other AEAD schemes, after this misuse the privacy and authenticity guarantees remain, albeit with this consideration to traffic analysis. This is a reasonable price to pay for the ability to use the HPKE APIs as more than a "single shot".

DAE can achieve the equivalent of semantic security if the message space is random enough. This is the justification for the security of key wrap schemes (see Section 1.3) in which (a portion of) the plaintext is a random key.

SIV takes a vector of AAD. When a unique sequence number can be managed it can be part of that vector. It should be noted, therefore, that it is trivial for an application that has control of the AAD to add a nonce as a component of the AAD vector to ensure unique AAD per invocation of the HPKE API and achieve the IND-CCA2 notion of security.

Alternately, for some situations-- e.g. when the message protected by HPKE is idempotent-- DAE security can be acceptable.

See Section 6.

1.3. Key Wrapping

Key wrapping schemes utilize a symmetric encryption algorithm to provide privacy and integrity to cryptographic keying material. Additionally, such schemes should provide integrity protection of cleartext associated data which contains control information about the wrapped key. Due to the symmetric nature of the algorithm, it is assumed both sides possess a shared secret whose establishment is problematic. Therefore HPKE is naturally an attractive option to use to wrap a cryptographic key to a receipent’s public key.

Since the data being wrapped is, in effect, random, a probabalistic input like a nonce is not needed, hence the deterministic nature of proposed key-wrapping schemes (see [X9102] and [RFC5649]). [SIV] is superior to those schemes in a number of ways:

* it accepts associated data;

* it is more efficient;

* it accepts natural data lengths without requiring padding; and,

* it has a security proof.

Thus, making it well-suited for key wrapping use cases with HPKE.

2. Requirements Notation

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

3. Notation

This document re-uses the notation from HPKE and adds the following:

* or(a,b): logical OR of byte strings; or(0x9876, 0x1234) = 0x9cf6. It is an error to call this function with two arguments of unequal length.

* and(a,b): logical AND of byte strings; and(0x1234, 0x5678) = 0x1230. It is an error to call this function with two arguments of unequal length.

* a | b: concatenation of byte strings "a" and "b". The length of the resulting string is the sum of the lengths of "a" and "b". If this symbol is on the left side of an equation it represents distinct data, represented by "a" and "b", as the result of the equation.

4. Modifying HPKE

4.1. Adding Compact Representation

New DHKEMs are defined for the three NIST curves, P-256, P-384, and P-521. Being "compact", they are denoted here CP-256, CP-384, and CP-521 but are, for the purposes of cryptography, otherwise identical.

All KEM modes defined in HPKE are supported for these KEMs, including Auth and AuthPSK.

Value	KEM	Nsecret	Nenc	Npk	Nsk	Auth	Reference
0x0013	DHKEM(CP-256, HKDF-SHA256)	32	32	32	32	yes	[NISTCurves], [RFC6090], [this RFC]
0x0014	DHKEM(CP-384, HKDF-SHA384)	48	48	48	48	yes	[NISTCurves], [RFC6090], [this RFC]
0x0015	DHKEM(CP-521, HKDF-SHA512)	64	66	66	66	yes	[NISTCurves], [RFC6090], [this RFC]

Table 1: KEM IDs

These KEMs use the KDFs defined in HPKE and therefore are bound by the input length restrictions of the KDF used (see 7.2.1 of HPKE).

The security properties of these KEMs satisfy the security requirements of a KEM used in HPKE (see section 9.2 of HPKE).

4.1.1. SerializePublicKey and DeserializePublicKey

For CP-256, CP-384 and CP-521, the SerializePublicKey() function of the KEM performs the Integer-to-Octet-String conversion of the x-coordinate of the public key only, according to [RFC6090]. DeserializePublicKey() performs the Octet-String-to-Integer conversion of [RFC6090] to produce the x-coordinate of a the resulting point. Since all of these curves have a prime p = 3 mod 4, the y-coordindate can be computed using the equation of the curve and Shanks' method of computing the square root modulo p:

$$y = ((x^3 + a*x + b)^((p + 1)/4)) \bmod p$$

for a, b, and p defined for the curve in [NISTCurves]. There will be two distinct solutions for y that will differ only in sign but either one is acceptable to produce a Diffie-Hellman shared secret that is used in compact output.

These deserialized public keys MUST be validated before they can be used. See HPKE for specifics.

4.1.2. SerializePrivateKey and DeserializePrivateKey

As with HPKE, CP-256, CP-384, and CP-521 private keys are field elements in the scalar field of the curve being used. Serialization of the private key uses the Integer-to-OctetString function from [RFC6090] and deserialization uses the OctetString-to-Integer function from [RFC6090]. If the private key is an integer outside the range [0, order-1], where order for each curve is defined in [NISTCurves], the private key MUST be reduced, modulo the order, to [0, order-1] before being serialized.

To catch invalid keys early on, implementers of DHKEMs SHOULD check that deserialized private keys are not equivalent to 0 (mod order), where order is the order of the curve.

4.2. Adding A Rolling Window

A rolling receiver replay window is added by overloading the way a context encrypts and decrypts messages-- ContextS.Seal() and ContextR.Open(). The calling parameters remain the same but the internals change and, for ContextS.Seal(), the output differs.

The replay window is implemented as a bitmask check for a window whose size is implementation-specific. For illustration purposes only it is described here as being of size 32, meaning it can tolerate loss and reorder of the previous 31 messages. The following pseudo-code has separate routines for a quick check of a received sequence number and an update to the window for sequence numbers that have been validated.

The context encryption API template is the same as that in HPKE except it prepends the sequence number, used to construct the counter for the AEAD operation, to the data returned from Seal(). Therefore the single "ct" output is, in fact, a concatenation of the four octet sequence number and the returned ciphertext.

The context decryption API template is changed to extract the sequence number from the input ciphertext, and check whether the received sequence number is conditionally good. If it is and the message is successfully opened, the window is updated with the received sequence number.

Details are as follows:

```
windowSize = 32

def CheckSeq(num):
  if num > self.seq
      return Good
  diff = self.seq - num
  if diff > windowSize
      return Bad
  if and(self.window, (1 << diff)) == 0
      return Good
  else
      return Bad

def UpdateWindow(num)
  if num > self.seq
      diff = num - self.seq
      if diff < windowSize
          self.window <<= diff
          self.window = or(self.window, 1)
      else
          self.window = 1
      self.seq = num
  else
      diff = self.seq - num
      self.window = or(self.window, (1 << diff))
  return

def ContextS.DSeal(aad, pt):
  num = self.ComputeNonce(self.seq)
  ct = num | Seal(self.key, num, aad, pt)
  return ct

def ContextR.DOpen(aad, m):
  num | ct = m
  if CheckSeq(num) == Bad
      raise OpenReplay
  pt = Open(self.key, num, aad, ct)
  if pt == OpenError
      raise OpenError
  else
      UpdateWindow(num)
  return pt
```

The window is added to the Encryption Context as well as a single datum to indicate whether the rolling receiver replay window is used (1) or not (0). When the replay window is used, Context<ROLE>.DOpen() and Context<ROLE>.DSeal() are used, when it is not the encryption and decryption operations from HPKE are used.

4.3. Adding DAE

DAE ciphers MUST provably provide "determinstic authenticated encryption" as defined in [SIV]. A DAE cipher mode that satisfies those requirements is AES-SIV as defined in [RFC5297].

AES-SIV uses a "double-wide" key. A single large key is passed to AES-SIV which divides the key into two, one for encipherment and the other for authenticity. Unlike other AEAD schemes, AES-SIV takes a vector of AAD. The number of components of that vector is up to the application using AES-SIV in HPKE.

Value	DAE	Nk	Nt	Reference
0x8000	AES-256-SIV	32	16	[RFC5297], [this RFC]
0x8001	AES-512-SIV	64	16	[RFC5297], [this RFC]

Table 2: AEAD IDs

Since these cipher modes are being added in their deterministic, nonce-less varient, the nonce is not used and the encryption and decryption operations ContextS.Seal() and ContextR.Open() do not call IncrementSeq() for DAE ciphers.

Alternately a universal invocation of the call can be made as follows by setting Nn to zero (0) for DAE ciphers:

```
  def Context<ROLE>.IncrementSeq():
    if (Nn > 0) and (self.seq >= (1 << (8*Nn)) - 1):
      raise MessageLimitReachedError
    self.seq += 1
```

5. IANA Considerations

In the "Hybrid Public Key Encryption" repositories, IANA has assigned values 0x0013, 0x0014, and 0x0015 from the HPKE KEM Identifiers repository for the KEMs defined in Section 4.1.

This document requests the creation of a new IANA registry by extracting a portion of the two-byte value space from the existing "HPKE AEAD Identifiers" registry. The new registry should be under the existing "Hybrid Public Key Encryption" registries and entitled "DAE Identifiers" and administered under a Specification Required policy [RFC8126].

IANA is instructed to update the HPKE AEAD Identifiers and set the unassigned values to be 0x0004 to 0x7FFF. The values 0x8000 to 0xFFFE are the available values of the new "DAE Identifiers" registry.

Template:

* Value: The two-byte identifier for the algorithm

* DAE: The name of the algorithm

* Nk: The length in bytes of a key for this algorithm

* Nt: The length in bytes of an authentication tag for this algorithm

* Reference: Where this algorithm is defined

Initial contents as defined in Table 2.

6. Security Considerations

Since HPKE uses Diffie-Hellman in "compact output", the sign of the public keys is irrelevant. Discarding that which has no impact on the result, i.e. doing "compact representation", does not present a security issue.

See [SIV] for a formal security proof.

Uses of the DAE ciphers in HPKE can achieve the same level of security as the non-DAE ciphers if the calling application guarantees unique AAD per invocation or if the calling application can guarantee a random message space.

This opens up the possibility of misuse where an application inadvertently makes a non-unique invocation (which is a good reason to hide nonce management inside the HPKE context, as the existing AEAD ciphers do). For some use cases-- e.g. messages are idempotent, or a probabalistic operation can be achieved (e.g. key wrapping)-- the DAE ciphers provide an acceptable option.

It deserves to be mentioned again that even if a nonce is reused (i.e. misused) by an application wishing to manage the AAD of AES-SIV, the security of the cipher is not completely voided as it is with a non-DAE mode. The notion of deterministic privacy and determinstic authenticity are retained (see [SIV]).

7. Acknowledgements

The algorithm for the sliding window to address dropped and reordered messages was proposed by James Hughes and Harry Varnis in [RFC2401].

8. Test Vectors

The following test vectors have been generated using the registry value assignments from Table 2.

* AES-256-SIV: 32768

* AES-512-SIV: 32769

8.1. DHKEM(CP-256, HKDF-SHA256), HKDF-SHA256, AES-256-SIV

8.1.1. Base Setup Information

```
mode: 0
kem_id: 19
kdf_id: 1
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
4270e54f fd08d79d 5928020a f4686d8f 6b7d35db e470265f 1f5aa228 16ce860e

pkEm:
23cd4f6a 91f37b51 3480ff24 9b4a08fd 27a56651 cb359476 02073780 7d5ce831

ikmR:
668b3717 1f1072f3 cf12ea8a 236a45df 23fc13b8 2af3609a d1e354f6 ef817550

pkRm:
3dbc347a e6a2a467 5a6848b3 4e10bf28 ed957847 18b43f05 959b2034 039c9626

key:
801dd7a3 6f806da8 f37b46cd 45d61ca9 61d44829 5863f78f ddd4cb6e a7246582

enc:
23cd4f6a 91f37b51 3480ff24 9b4a08fd 27a56651 cb359476 02073780 7d5ce831

kem_context:
23cd4f6a 91f37b51 3480ff24 9b4a08fd 27a56651 cb359476 02073780 7d5ce831
3dbc347a e6a2a467 5a6848b3 4e10bf28 ed957847 18b43f05 959b2034 039c9626

shared_secret:
97d46fdd 749db253 1604b8b6 763897ef bd75aee0 d0fc361e 186e86e6 5511ac45

key sched context:
0055453c ca40c034 308f7e16 99de3e0a 1829c455 5e85e129 8f8ab2c9 24af8459
910ebc50 7e6381dc 28a47ac8 21e7d495 02474770 5dabfedd f171b642 fbeb99c5
c8

secret:
5f338824 f999f5bf d3f26412 0874d48b 5ba9e8e4 bfc54837 f57d2479 dcdc9e26

key:
801dd7a3 6f806da8 f37b46cd 45d61ca9 61d44829 5863f78f ddd4cb6e a7246582

exp:
3c4406ae 3b354001 24ddcb1e 87bda1ae 14abc4a4 248177fd 7910def3 2af339af
```

8.1.2. Encryption

```
pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
877324cc 10f1378d 9e362948 1fd8104f 2943bafc ddc0eb7d 6ad21cac a615992a
bae7aa02 06aadc72 f62af629 ce

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
623000a0 53a5824d cc87f85f 8a829e36 72953ef8 456c3e73 02112924 e3285bf5
cd94c88d c7544601 daa4b404 6b

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
3f9678d0 ae372f6f 8dc90965 be89dcbd b4f8f491 eb5de1bc 8a081b1a 0f0621e8
af12aae4 0dd4a4d9 5d7d94e0 39

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

ct:
cc943b50 aefd7eed b0bd5b78 9e60aeea 801608ca 2eaa67d9 d0318f55 67348289
c0712330 52b891c1 8bcbf479 57

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
1b02acb8 9d0e761e 757a2874 86e0625d be9982f6 5670f1b4 cf9cea54 3c06d066
```

565fc87d 36481905 82178de9 a4

8.2. DHKEM(CP-256, HKDF-SHA256), HKDF-SHA256, AES-256-SIV

8.2.1. Auth Setup Information

mode: 2
kem_id: 19
kdf_id: 1
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
798d82a8 d9ea19db c7f2c6df a54e8a67 06f7cdc1 19db0813 dacf8440 ab37c857

pkEm:
ba2b510d 3808c4be ced6b153 120b79d7 78c785f9 2c3b67b3 0e153d94 5b20727d

ikmR:
7bc93bde 8890d1fb 55220e7f 3b0c107a e7e6eda3 5ca4040b b6651284 bf0747ee

pkRm:
48b9c95a 72c53280 d19d5886 15b1f3a6 b1f607c8 111b9802 1441b9ad 709da767

ikmS:
874baa0d cf93595a 24a45a7f 042e0d22 d368747d aaa7e19f 80a802af 19204ba8

pkSm:
57fc29c0 7963a7bb ec000475 c11b4633 c51788fb d2fff55e 3b9cd8cb 31acb077

key:
d9458251 e1e1c04b 6d0dcd7b 54d2fdcc ac30fe93 4c6b2218 06000d32 135b9d51

enc:
ba2b510d 3808c4be ced6b153 120b79d7 78c785f9 2c3b67b3 0e153d94 5b20727d

kem_context:
ba2b510d 3808c4be ced6b153 120b79d7 78c785f9 2c3b67b3 0e153d94 5b20727d
48b9c95a 72c53280 d19d5886 15b1f3a6 b1f607c8 111b9802 1441b9ad 709da767
57fc29c0 7963a7bb ec000475 c11b4633 c51788fb d2fff55e 3b9cd8cb 31acb077

shared_secret:
ef299e8f 1be52e52 d66d3ee1 1b8a62f8 6a0b5e34 3508e6c4 8873f5ca 33926369

key sched context:
0255453c ca40c034 308f7e16 99de3e0a 1829c455 5e85e129 8f8ab2c9 24af8459
910ebc50 7e6381dc 28a47ac8 21e7d495 02474770 5dabfedd f171b642 fbeb99c5

c8

secret:
5abdd336 98923571 1a007ecc 1ef0b2cc c7d5176d 1eae4fc7 481c5f50 250a1c72

key:
d9458251 e1e1c04b 6d0dcd7b 54d2fdcc ac30fe93 4c6b2218 06000d32 135b9d51

exp:
4a25c401 ff8a4046 e577988f 28b912c7 aa7f7d74 663b1d2f fa5706e0 86ec2231

8.2.2. Encryption

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
505a34e4 cff47112 d7f4ac07 ec2b6bda a7de6d36 dd437d15 3be9b37e cdea0158
d7f2e5fc 1259889e 4301353e 71

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
2c5db18b 59e8b843 68edcbf7 de03e025 b16b10b9 454c54a6 542f4fae cbddd392
aceb13da ac477423 4729a810 f9

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
de8bbbf1 012fbbc1 a411330f c04b7f28 6525fba7 88aa1375 7bf123ac 537fefc8
1243e539 27d11228 79c3fa0b 9b

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

```
ct:
eae65954 6188c313 cd91a7fa 5c49c053 15e77586 83cbe87d 8425fd22 1134cc3c
3b6605b8 831d22d5 81d4536d 56

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
f91c6fb4 9375f180 fcbae250 93de6f9f 211aa0bc 9869b297 6825b781 3d04c7d2
d304d7b7 c78bc84b 38b8d9e9 dc
```

8.3. DHKEM(CP-256, HKDF-SHA256), HKDF-SHA256, AES-512-SIV

8.3.1. Base Setup Information

```
mode: 0
kem_id: 19
kdf_id: 1
aead_id: 32769
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
a90d3417 c3da9cb6 c6ae19b4 b5dd6cc9 529a4cc2 4efb7ae0 ace1f318 87a8cd6c

pkEm:
0c83751b 613bf3e6 3fa4ee1a e64ffa4c 86c997bc 97983c2a 7ec9546b ee856e0b

ikmR:
a0ce15d4 9e28bd47 a18a97e1 47582d81 4b08cbe0 0109fed5 ec27d1b4 e9f6f5e3

pkRm:
d6643f01 efee734d 147e78f7 9722012f 22dbc5bd 640348e4 dc7872fd 6afb2748

key:
b300523f 5ad519e0 7fd90a6b d6b16a56 aa97531f ea28b779 4e02cec1 6e24b1b2
6d89916a acd6c486 2e03fd2a 7a28ee57 33e02f68 ff0a6ded 90667938 ae7eeded

enc:
0c83751b 613bf3e6 3fa4ee1a e64ffa4c 86c997bc 97983c2a 7ec9546b ee856e0b

kem_context:
0c83751b 613bf3e6 3fa4ee1a e64ffa4c 86c997bc 97983c2a 7ec9546b ee856e0b
d6643f01 efee734d 147e78f7 9722012f 22dbc5bd 640348e4 dc7872fd 6afb2748

shared_secret:
81a5c8af 1952bbdf d200ca47 9b9b6433 fe3c1a13 55cb1381 8fa0a828 99e5746e

key sched context:
0080f298 71dabe08 a3047996 f23f4cd4 1d21a437 af194ad3 fa5c1ea9 d552279b
8af92a25 9ecfcf09 2d342660 00770763 04905f3c a6672705 857b2d9c 6a912e25
b1

secret:
d707b687 a3eecd32 fa7b1a1d 918a74f2 3fa9081f a26bde50 de67f3a3 c6691143

key:
b300523f 5ad519e0 7fd90a6b d6b16a56 aa97531f ea28b779 4e02cec1 6e24b1b2
6d89916a acd6c486 2e03fd2a 7a28ee57 33e02f68 ff0a6ded 90667938 ae7eeded

exp:
33e02f68 ff0a6ded 90667938 ae7eeded a9106dd0 6b35413d ae55a243 0f7f7294
```

8.3.2. Encryption

```
pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
3b7e8476 98758c33 7b424457 c97cd3ec d6abbbb9 a3ebdcf1 fd545950 19da1030
ef95f5d4 7366d7fa 9df86c5b 7a

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
c4f6869f 4d373412 3dd0b3d6 a7f2e83f 0bb48fd1 bf9df179 eed2b9a7 36675c5f
f8a1ade2 e422d2e7 bffca15f 15

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
b934d341 50a68412 b1ee9d00 86989c4c 3696fa83 a207e57e e7bb72b9 ab909503
4d53dd4e dbaaaa67 632b7bbf ca

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

ct:
fa429ab9 5b3b1121 f22d6595 6bcb3ab0 3cb81c65 29643329 391ba562 6ed29c95
cc3f0400 034aa884 7f8c8415 47

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34
```

ct:
b60a38bf f1e4ee98 9defa146 c299f95a 61a313c2 a2679cd1 9b24e3e8 60f2cb87
8e8394f4 10364533 842ba02b 46

8.4. DHKEM(CP-256, HKDF-SHA256), HKDF-SHA256, AES-512-SIV

8.4.1. Auth Setup Information

mode: 2
kem_id: 19
kdf_id: 1
aead_id: 32769
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
d6c49e44 2aad90bc c1bc0d16 6e5c4d3d f845c803 ba08b8a4 d891af2e eae4f97e

pkEm:
5fc3876c 0e3d841c 070d5c5b e41c048c e924f8d5 c8d11893 70955bbc 0fe349f0

ikmR:
3c567569 48f1c27a ed3eb27a 923c891d c073eccf 94bb6c1b 64a8bfaa 95f1f8f7

pkRm:
5ac93274 8d20c9aa af3c4126 51706a2a 08958a48 e7ed10f8 a944c556 9fbeca8c

ikmS:
0f3def8c c45967f8 6c566f2c 2a7deced ff0d5f8b 20a34ab6 5318144c 80cb6b2b

pkSm:
db74c19a 176482fe bad3e945 03c4b89d 622ddbf2 b1428cff 37627f6b e154011a

key:
8e6be96f b4b7e028 ea83f30f 776825e5 9f8c6627 a8f58fbd da95acd6 2f799cda
e7cfc768 43c1fff4 0dc928a7 a8e52554 1b32dbc0 f25ffd82 86cd3eaf 7a27c83b

enc:
5fc3876c 0e3d841c 070d5c5b e41c048c e924f8d5 c8d11893 70955bbc 0fe349f0

kem_context:
5fc3876c 0e3d841c 070d5c5b e41c048c e924f8d5 c8d11893 70955bbc 0fe349f0
5ac93274 8d20c9aa af3c4126 51706a2a 08958a48 e7ed10f8 a944c556 9fbeca8c
db74c19a 176482fe bad3e945 03c4b89d 622ddbf2 b1428cff 37627f6b e154011a

shared_secret:
a67f3222 eeb41eba 6c7a9f5a 10478fd7 a0e809e9 32ec4b8c f2edd01e cc96af50

```
key sched context:
0280f298 71dabe08 a3047996 f23f4cd4 1d21a437 af194ad3 fa5c1ea9 d552279b
8af92a25 9ecfcf09 2d342660 00770763 04905f3c a6672705 857b2d9c 6a912e25
b1

secret:
59982e49 962d4cfc 37487e6e 46b975b6 41537fb6 fe1182e0 12181ed4 5bfef239

key:
8e6be96f b4b7e028 ea83f30f 776825e5 9f8c6627 a8f58fbd da95acd6 2f799cda
e7cfc768 43c1fff4 0dc928a7 a8e52554 1b32dbc0 f25ffd82 86cd3eaf 7a27c83b

exp:
1b32dbc0 f25ffd82 86cd3eaf 7a27c83b 4ed2fb8f d0bb1e44 b46210fa 0ac10424
```

8.4.2. Encryption

```
pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
f3c0cc30 08f32d60 6ea800ef d71f397a 580a9869 03bdc087 b336507a 1d689d28
0cf3ed40 2d8db4e3 b80cc7ba 5a

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
5ec097aa 495b2b75 eb53b6a4 085a0f52 e99fa936 3a0941cc 1b2d2221 907af81f
f8b95a74 70891aa3 cee1ed02 b2

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
625d347f 346142b8 59282401 5881aa3c 06ed16f4 e33cbca9 afc39929 b4004330
1576570a ff885773 af124966 45

pt:
```

42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

ct:
93465758 e8dac5b8 9edd4cd6 9369a076 1853dfcb 36f215d7 48e09b75 1db893c0
f8888c5e 6e669df1 e9712b99 1e

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
38c0adc9 b275d964 2ba210ce 3f5fd2db b3f5a4a3 8fa6e698 6bfa7fce f9ef1936
d440682a 666d5cc5 0e27bc23 90

8.5. DHKEM(CP-256, HKDF-SHA256), HKDF-SHA512, AES-512-SIV

8.5.1. Auth PSK Setup Information

mode: 3
kem_id: 19
kdf_id: 3
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
37ae06a5 21cd5556 48c928d7 af58ad2a a4a85e34 b8cabd06 9e94ad55 ab872cc8

pkEm:
87e52765 608be760 1d402d76 fd0cef53 c79365b6 96f0217f 89165f90 f07fb191

ikmR:
7466024b 7e2d2366 c3914d78 33718f13 afb9e3e4 5bcfbb51 0594d614 ddd9b4e7

pkRm:
474f1abb 69c066b7 1c1c35c6 a67dccb1 8d3a6cfd 5bf95501 d6594c3e 144b7b9b

ikmS:
ee27aaf9 9bf5cd83 98e9de88 ac09a82a c22cdb8d 0905ab05 c0f5fa12 ba1709f3

pkSm:
a2076645 915893d8 df5d99b2 5368e1de 74de3b6b 070d8fbe b85b242c bf00a47c

```
psk:
0247fd33 b913760f a1fa51e1 892d9f30 7fbe65eb 171e8132 c2af1855 5a738b82

psk_id:
456e6e79 6e204475 72696e20 6172616e 204d6f72 6961

key:
24f50c2f 1a320631 18503ffa 17225f85 e7d85bb9 c14cc2f4 f07c2a0b 006dbd05

enc:
87e52765 608be760 1d402d76 fd0cef53 c79365b6 96f0217f 89165f90 f07fb191

kem_context:
87e52765 608be760 1d402d76 fd0cef53 c79365b6 96f0217f 89165f90 f07fb191
474f1abb 69c066b7 1c1c35c6 a67dccb1 8d3a6cfd 5bf95501 d6594c3e 144b7b9b
a2076645 915893d8 df5d99b2 5368e1de 74de3b6b 070d8fbe b85b242c bf00a47c

shared_secret:
0c554e67 af28a8cb 6548163c bba01e0c 882111cb 9a9d2b70 d52f27a6 b5da0e93

key sched context:
0351398b 9adc33df ee5d72ec d21b2d06 cd29fdbb 65b0bafb 43d8d15a 4c603cad
26b85548 a1f6981b 751cda8b 29f92d40 8d8825c6 54ddf912 f5c654a3 96f5514d
5116ed5b c72c1cdb 46f09985 3ff26e0e 3ed58c6f bafcff06 a71eb91a e494868a
ce5607c5 e9bb4749 c40c6e89 e158195c 68746a37 e31505e4 96fbcf78 6075c0e5
78

secret:
6b29d869 13db42ff 5c25fa45 0f69b7b5 cef715e2 16f0f3c7 19c601f0 0e641e17
2c5fcd45 856e0393 8c68861a 90190161 25564de5 77168cbd 555169ba 323d9048

key:
24f50c2f 1a320631 18503ffa 17225f85 e7d85bb9 c14cc2f4 f07c2a0b 006dbd05

exp:
b29bc9e5 174eaccf d04b2b42 24fcdaac df7a9077 0972dd3e 7bb7aa93 8e8ca08f
17b0cac1 97da3466 c4f28260 50fa8c69 0ce05059 d26edef2 449dc96d 9a1d20b9
```

8.5.2. Encryption

```
pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
6797df43 1aad8cf5 95772337 23ea34fc 4701b1c0 ed727801 6c93cf1c f534bbaa
```

```
 b79dcdab 58456b46 d319320c 0e

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d31

 ct:
 47a7e05e 638c5ae9 e61bf2d8 43e5ae5c db3d1598 e67eacf2 58d0b60d 3e2ad239
 7f65f01d 26a811f6 1448b229 10

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d32

 ct:
 1565278f 9c5e776b 1df1a635 c7050b4e eb734521 a3007eec 5602cc6d 20269fa5
 0f9f892a 20da105f 3e798802 97

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d33

 ct:
 5e9bee3f 33f80d45 c42f0aed c6d81ee0 a577e334 796e3089 dd2cf311 b506c1e0
 4cd8cedd 635b3690 f088a2f2 1a

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d34

 ct:
 791c982a 0c87e3a7 9c16e845 6cfd2e3d 71412615 88d7d300 64525c7a 7e91cc9d
 2e07d151 2107db04 0974dcf5 ca
```

8.6. DHKEM(CP-521, HKDF-SHA521), HKDF-SHA256, AES-256-SIV

8.6.1. Base Setup Information

```
mode: 0
kem_id: 21
kdf_id: 1
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
5040af7a 10269b11 f78bb884 812ad200 41866db8 bbd749a6 a69e3f33 e54da716
4598f005 bce09a9f e190e29c 2f42df9e 9e3aad04 0fccc625 ddbd7aa9 9063fc59
4f40

pkEm:
005208f9 56649e60 0e958116 ae05435a 6adb3a17 2e29bc3b 22818043 535ede1a
977bc486 40f4163e 8fc68c3c fb629380 cad13675 b93d186d 39e754ed 62055014
a5f5

ikmR:
39a28dc3 17c3e48b 908948f9 9d608059 f882d3d0 9c054182 4bc25f94 e6dee7aa
0df1c644 296b06fb b76e84ae f5008f8a 908e08fb abadf706 58538d74 753a85f8
856a

pkRm:
01d07d98 c86f123e 13a052cf 58d4d7f9 ac98ab62 aa0fccc6 a2354ab4 4abc0e33
8cf8ba8a 8a26225a a1bf023a 9d4db0a1 2135b7b7 c95aadc6 eec3fdc6 4eb4fdf0
e440

key:
857e671a 0d784ec3 a3123463 6aaa981a 383e2e38 af4f0465 d9c3400a 5be072bf

enc:
005208f9 56649e60 0e958116 ae05435a 6adb3a17 2e29bc3b 22818043 535ede1a
977bc486 40f4163e 8fc68c3c fb629380 cad13675 b93d186d 39e754ed 62055014
a5f5

kem_context:
005208f9 56649e60 0e958116 ae05435a 6adb3a17 2e29bc3b 22818043 535ede1a
977bc486 40f4163e 8fc68c3c fb629380 cad13675 b93d186d 39e754ed 62055014
a5f501d0 7d98c86f 123e13a0 52cf58d4 d7f9ac98 ab62aa0f ccc6a235 4ab44abc
0e338cf8 ba8a8a26 225aa1bf 023a9d4d b0a12135 b7b7c95a adc6eec3 fdc64eb4
fdf0e440

shared_secret:
01b5e494 8af1dae6 9fe69cf1 ff6c2f52 022ce691 6fa5e846 40351561 292f19c4
2fa6fd27 132d0414 dbc67d34 8f9efaaf 2064f76e b6e43f2c 0c59d72f 2b75b988

key sched context:
00ee8951 7f8b3b58 9c547937 838d2d3a 3bf69626 bf7315ac dbda6fd7 b69fd702
```

465a397e bf6ab9d3 4216b4b1 b4a58887 7735f07d 56abeee7 6a67f264 175f3c92
cd

secret:
1b9f34d5 3fc408b3 ef82f2e1 72bbe0f5 876a2b24 29b8d39c 9e8e73fc 12aa9b61

key:
857e671a 0d784ec3 a3123463 6aaa981a 383e2e38 af4f0465 d9c3400a 5be072bf

exp:
45c5d1ba 83843b8a 96e190e2 e8e2e711 c5014193 6b5e69bf 0b63a3cc 93f1f8f1

8.6.2. Encryption

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
5c96ded6 cda96dea 6e7a13a1 291da3c9 86c07965 76cf353a befca435 3912f56d
86639e60 501ef2f8 1902a1cc e4

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
89684304 6f073963 a0f005cb 652eea9e 7f8ac9fa e4a529fe e1e8ce20 4f9d48c1
59a25605 f004522d 80cfc2e7 0b

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
ce500e6f 53dfa802 efc3923b 7795221e 38ee8599 780a52f9 319f313e 774a8ead
4d61af92 77b6b85c 5d082f04 7f

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:

436f756e 742d33

ct:
f9ad960f 7077c4ff ad5f08c8 89c0c3bf 2161d04c 46d9f64b 5ffac5b5 a9b7734d
a102a625 551ecd89 74f93cb6 9a

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
db9e9db2 5531bdd4 70dab5ca 11288ef8 2139d968 b6bc0126 43be567a c0cf1ea1
c8b7ba5c c53ff255 e16eb6ce 27

8.7. DHKEM(CP-521, HKDF-SHA521), HKDF-SHA256, AES-256-SIV

8.7.1. PSK Setup Information

mode: 1
kem_id: 21
kdf_id: 1
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
19484305 36ca540c 53351ae5 9d7a2240 8f1a0f20 1c1387e2 38ca8c52 ea162da7
ffe27652 fbbfef9b 60b66a03 9c80853a 4224c01f d83155a1 7373c92f 3d41bc25
4943

pkEm:
012c55eb 18a3184f 8fefb856 f2f16d9d 2e7bb9bd bf0842c4 f4d5d668 17302753
ee239e72 627e724d a393436d 47d7dede 97734ce6 db12387b cfa5713b b20e0ccd
cbd6

ikmR:
3c9a57ce 2773fc44 d2b03a9f ed866e9f 8dfd18bf c844c4dd c254fe0c 836643b9
fd3f54ce 090caf5f 07829fd0 17ebdf4b 43408579 85f21056 d5a2dd46 1dd61da9
afce

pkRm:
016368a1 295c5fef 6f80fd82 98401040 c2960e4b 8db4c265 c2eb4832 8ac026c1
74075384 12be0251 35f88f66 50f61fe1 0a6bd91a f4b9e431 442bbfa2 3192c08c
757d

psk:

```
 0247fd33 b913760f a1fa51e1 892d9f30 7fbe65eb 171e8132 c2af1855 5a738b82

 psk_id:
 456e6e79 6e204475 72696e20 6172616e 204d6f72 6961

 key:
 57ef66fe 6b7acca5 a966d2d2 ed68dc01 066afac4 39b614a8 4009c111 9275fb26

 enc:
 012c55eb 18a3184f 8fefb856 f2f16d9d 2e7bb9bd bf0842c4 f4d5d668 17302753
 ee239e72 627e724d a393436d 47d7dede 97734ce6 db12387b cfa5713b b20e0ccd
 cbd6

 kem_context:
 012c55eb 18a3184f 8fefb856 f2f16d9d 2e7bb9bd bf0842c4 f4d5d668 17302753
 ee239e72 627e724d a393436d 47d7dede 97734ce6 db12387b cfa5713b b20e0ccd
 cbd60163 68a1295c 5fef6f80 fd829840 1040c296 0e4b8db4 c265c2eb 48328ac0
 26c17407 538412be 025135f8 8f6650f6 1fe10a6b d91af4b9 e431442b bfa23192
 c08c757d

 shared_secret:
 7dbf19ed dced8520 cf9f4f09 cbe09c67 c7493d6e 798d69f0 f13fc693 e3161d27
 8b37b1f7 78556a5d 293957bb 768a1567 75bded1e c835fc69 faeb6e01 d981110d

 key sched context:
 010e2e1b ede95a81 0b44d22b 7b7f7194 68f4ea41 bb1412cc 8e1bdce1 702317ad
 d95a397e bf6ab9d3 4216b4b1 b4a58887 7735f07d 56abeee7 6a67f264 175f3c92
 cd

 secret:
 18bb01aa bc613d1a b5e783cc e7961c5a 4401cc6c 1336afcf b166e2fd 5daf2c55

 key:
 57ef66fe 6b7acca5 a966d2d2 ed68dc01 066afac4 39b614a8 4009c111 9275fb26

 exp:
 f0654114 a142395d 43d51d1b 79d1af90 428c1d51 1d2dbc8d 8a3a6fd8 a4ae43d9
```

8.7.2. Encryption

```
 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d30

 ct:
 3e8ed8f1 9dc9a775 6dcf5ad0 2558e344 03d36c53 48c73774 d37fbfb8 217afb73
```

```
 9118d532 35fdd6a7 01066859 7e

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d31

 ct:
 a4e42c73 9fa3a5ad c25b14e6 7f685aa0 d45c900e be208e25 a94ffdf7 4f23a91a
 71452f81 e51a2a0b d4e3045e 6d

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d32

 ct:
 b5f3cc60 00fe8b7f fe2a8c9c 88291f3c 58b9e9ed b4fcf68b 8351d37e ba658360
 bbc3916b 9f2d3c8e 4380e013 56

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d33

 ct:
 c9bb324e a4b68104 5d43d2e1 4523da47 669bc5dc 93f9f53f 76adf991 f25817e9
 5268f94c 3b8c94a2 bb1b6ab1 e2

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d34

 ct:
 5cc04caf c840b053 9401718c c6a3e559 8a157889 090e59ba 5074481c 7e220f4d
 7776faa1 60c0b854 b93bc98c 88
```

8.8. DHKEM(CP-521, HKDF-SHA521), HKDF-SHA256, AES-256-SIV

8.8.1. Auth Setup Information

```
mode: 2
kem_id: 21
kdf_id: 1
aead_id: 32768
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
d45cc999 ba65eb6b ec00cf9b df308ae7 57558d62 8938ada2 d7bbf97b f58b401d
ea5710d5 c1f733fd 30dade61 6806669a cce09ba3 2cc57d58 02026955 3a19d632
d1f7

pkEm:
00941aa3 61e3df67 8316e950 f082f38d 972b4f5d 789d4abb ebb0bd10 7f3e1d77
66a02538 47840ec2 bb22dd43 6cbf9a8b fa90a38f 61e86ca1 44877699 8e1d7db7
33a3

ikmR:
fd95b48b 2a8e53cd 12da39ec c343c273 ce282b00 f185b6e9 80d3b4b8 55e938ea
0ba841e8 dfe5ac19 4ba830a5 23a7c5d1 faff6482 ff5e46ea 8f25b126 b8545c6d
eb11

pkRm:
01f7b479 fef9ddbf 10a12c7e 5d4e22f5 ca3745e6 12dc7007 96f80ecf 0a32e5d0
3b4e526d bc08234b 13740963 ea1e9de2 85a21647 72ae3fcf f7a513b8 f7c132f6
7b18

ikmS:
7c533451 b4b61ba8 ee879bb4 e11fb330 d0397244 2d74fd7c f5ebc0f8 84a90005
a87fcb0e 3401e9f7 24b45cec de6d9f6d d88f202e f23f790d a10867d6 bd8d9fb8
bf89

pkSm:
01715f0e 475571c9 9e0bfac5 eae86e08 fbea30db 23f670ed 471b053f f5f7c464
3daf384e 7714d25a 45170576 8d05ab73 00e0cb64 5d21c697 49a46680 f31eec0e
fc2a

key:
00b627bb ab7429ce ef678e18 e771d8ee c2dc1813 3c434d6f b0bb1508 74127366

enc:
00941aa3 61e3df67 8316e950 f082f38d 972b4f5d 789d4abb ebb0bd10 7f3e1d77
66a02538 47840ec2 bb22dd43 6cbf9a8b fa90a38f 61e86ca1 44877699 8e1d7db7
33a3

kem_context:
00941aa3 61e3df67 8316e950 f082f38d 972b4f5d 789d4abb ebb0bd10 7f3e1d77
66a02538 47840ec2 bb22dd43 6cbf9a8b fa90a38f 61e86ca1 44877699 8e1d7db7
```

```
 33a301f7 b479fef9 ddbf10a1 2c7e5d4e 22f5ca37 45e612dc 700796f8 0ecf0a32
 e5d03b4e 526dbc08 234b1374 0963ea1e 9de285a2 164772ae 3fcff7a5 13b8f7c1
 32f67b18 01715f0e 475571c9 9e0bfac5 eae86e08 fbea30db 23f670ed 471b053f
 f5f7c464 3daf384e 7714d25a 45170576 8d05ab73 00e0cb64 5d21c697 49a46680
 f31eec0e fc2a

 shared_secret:
 fd55afea 8cf91399 eab366b2 1f9c1c5e 1be2cc06 92a988d3 58884755 7eaebf4b
 1a85f6f1 150e34f5 0fa4faa8 2beba6b6 a06d97e7 8a63a43d 7c0369b4 851ddda4

 key sched context:
 02ee8951 7f8b3b58 9c547937 838d2d3a 3bf69626 bf7315ac dbda6fd7 b69fd702
 465a397e bf6ab9d3 4216b4b1 b4a58887 7735f07d 56abeee7 6a67f264 175f3c92
 cd

 secret:
 bd613083 0bc92898 68e03de9 b09031f2 2a188233 2fb2095f 3fea4f96 275011b3

 key:
 00b627bb ab7429ce ef678e18 e771d8ee c2dc1813 3c434d6f b0bb1508 74127366

 exp:
 a15a0692 3195b504 5569980f c93a67db 989c09b4 f133f4ec 9123ad8c c06e1ce2
```

8.8.2. Encryption

```
 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d30

 ct:
 811b7ff6 209baeb6 7aa1290b 98cb5cbc 8ad52356 4bbb0cce 8a70470f dac4ea07
 89ff3c5e b127e64a d4fce0e9 4e

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

 aad:
 436f756e 742d31

 ct:
 2c44010b 917d1b4f 404d93ce 98011d64 c2a84994 79c90901 32600303 ddaf14d8
 fa4a4bfd f787de6e 92cfb5ba d1

 pt:
 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79
```

aad:
436f756e 742d32

ct:
a66c2b58 f7842413 72d5fe78 eded9e1e 7706efd8 4fb9ac3d 1fd4ce20 5e6ca7f4
95ac5aba 58eda466 e104a4d0 ee

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

ct:
53432289 353275a1 43f1347a fe97d21d 4c2c6924 b10f2c9b 53d558b4 8d5c4cf9
f6b758fe 4b397d61 949a749c 94

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
41d12f9e e0725bfc 18548deb bd2b21a0 c72f85ad fe0444a2 167da71a 882b62cd
d2807c53 ee530b99 a1df10cc b1

8.9. DHKEM(CP-521, HKDF-SHA521), HKDF-SHA256, AES-512-SIV

8.9.1. Base Setup Information

mode: 0
kem_id: 21
kdf_id: 1
aead_id: 32769
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
9953fbd6 33be69d9 84fc4fff c4d7749f 007dbf97 102d36a6 47a8108b 0bb7c609
e826b026 aec1cd47 b93fc5ac b7518fa4 55ed38d0 c29e900c 56990635 612fd3d2
20d2

pkEm:
00fd79f7 20262f2f 38f6e164 3139fad0 58a07210 a0ded183 092de949 b70271ab
7fc59999 b9f13ce8 a0c79454 841be330 e0298d6b b3449e1b e6835f52 2963fdbe
2cbb

```
ikmR:
17320bc9 3d9bc1d4 22ba0c70 5bf693e9 a51a855d 6e09c11b ddea5687 adc1a112
2ec81384 dc7e4795 9cae01c4 20a69e8e 39337d9e bf9a9b2f 3905cb76 a35b0693
ac34

pkRm:
00685b94 a565c40e 44467ded 521e51dd 27062392 7f076cae 5d2ac51e daa00c08
0cb53932 a0f96476 7016be86 e1828c97 406a1c45 210bd72a 6a4db565 a0a2ede1
66bf

key:
509447ee d1a60907 bcbb58ca 4d67dd8e 0ced5605 1189a317 6420cb30 9a539bac
fa852d28 57f271f9 c362fc0f baac005b ad69cffe 33726417 2a4a8f2d b51a72b7

enc:
00fd79f7 20262f2f 38f6e164 3139fad0 58a07210 a0ded183 092de949 b70271ab
7fc59999 b9f13ce8 a0c79454 841be330 e0298d6b b3449e1b e6835f52 2963fdbe
2cbb

kem_context:
00fd79f7 20262f2f 38f6e164 3139fad0 58a07210 a0ded183 092de949 b70271ab
7fc59999 b9f13ce8 a0c79454 841be330 e0298d6b b3449e1b e6835f52 2963fdbe
2cbb0068 5b94a565 c40e4446 7ded521e 51dd2706 23927f07 6cae5d2a c51edaa0
0c080cb5 3932a0f9 64767016 be86e182 8c97406a 1c45210b d72a6a4d b565a0a2
ede166bf

shared_secret:
f4016476 1b23e62a 825c3a12 f00a300c 7fc0bca7 d63a4b4d 8decd9e3 e6665c77
72e5caa3 1d81b01c 83f85fad 171604a5 f5620d0e b3adc049 cf84a244 da1b66fc

key sched context:
0084582f ea7c6cbb 3a9be54c 06e8db3c 9665ad00 36975727 e014a93f 1db6ca99
61b76fd4 9e7c946d aa118995 dbf5be4b 4207a32d ef074588 da164a7c 64a16026
b1

secret:
7c205720 20b636ef ef05fad5 08bc322c d73fadb0 1518682a 8aba4e5b 1ec77915

key:
509447ee d1a60907 bcbb58ca 4d67dd8e 0ced5605 1189a317 6420cb30 9a539bac
fa852d28 57f271f9 c362fc0f baac005b ad69cffe 33726417 2a4a8f2d b51a72b7

exp:
ad69cffe 33726417 2a4a8f2d b51a72b7 1398b0b3 743254a7 365e7b43 b4bb4ff9
```

8.9.2. Encryption

```
pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d30

ct:
fe7d8ba9 602969e1 6456447c b4d1b887 9345f92c 453f5ce2 08ea7bad ef9bdd3c
f6107b1d 5f804cef 6d78de23 e3

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d31

ct:
0cd5d034 55b92378 6c35ea14 0f42eaa9 ff19e9fa 2eea0916 f78b4f78 b21f89ce
b33de5fd 98f75067 5e6ce5db 64

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d32

ct:
949d3b1c 96da376e 3865648b 344f606c a8640ca5 cb846801 eaa12009 875c1f59
2c7c3288 fab6a96a 4ab91620 3d

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d33

ct:
5774238b 80c0eefa cdbf5804 f9928e93 a600e9b4 460b0370 c70e94c8 c954ea25
6297974e 428257a3 75f0668e 82

pt:
42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad:
436f756e 742d34

ct:
b5bf6e37 38298058 a6f16b50 fef5dff6 59bcf5f5 65133849 646d04b4 756247fb
```

e88b248a d2da2540 2fddd27c 8f

8.10. DHKEM(CP-521, HKDF-SHA521), HKDF-SHA512, AES-512-SIV

8.10.1. Auth PSK Setup Information

mode: 3
kem_id: 21
kdf_id: 3
aead_id: 32769
info:
4f646520 6f6e2061 20477265 6369616e 2055726e

ikmE:
54272797 b1fbc128 a6967ff1 fd606e0c 67868f77 62ce1421 439cbc9e 90ce1b28
d566e6c2 acbce712 e48eebf2 36696eb6 80849d68 73e99593 95b29319 75d61d38
bd6c

pkEm:
01b716a3 3ef96baa 96761a89 0b08efc6 762f2f20 fe7db159 7c3e3663 4a3973e6
8bdb71f9 1cc2d701 ad4424a3 04554f12 efce4c25 991f2033 d51c1f3c 43d95564
4510

ikmR:
3db434a8 bc25b27e b0c590dc 64997ab1 378a99f5 2b2cb5a5 a5b2fa54 0888f6c0
f09794c6 54f44685 24e040e6 b4eca2c9 dcf229f9 08b9d318 f960cc9e 9baa92c5
eee6

pkRm:
01bf5b74 278612e1 cfa7a47c dbe24a6f be41b73c 32e98e98 6d40c849 0a9201d3
187483b8 b66e2710 5a3eb80c 394a889a 24841875 7425b0e3 a4b376f3 fd8ea087
daf4

ikmS:
65d523d9 b37e1273 eb25ad05 27d3a7bd 33f67208 dd1666d9 904c6bc0 4969ae58
31a8b849 e7ff6425 81f2c3e5 6be84609 600d3c6b bdaded3f 6989c37d 2892b1e9
78d5

pkSm:
01856189 0c5378f2 dedf9da7 8c082f22 01110f1c ca97637c e4ae528c af38ee87
5d70b77f a72c4b6f 2fb42466 f98852dc 8466c4de f387db3a 6514872f 616d7379
e27e

psk:
0247fd33 b913760f a1fa51e1 892d9f30 7fbe65eb 171e8132 c2af1855 5a738b82

psk_id:
456e6e79 6e204475 72696e20 6172616e 204d6f72 6961

```
key:
6a105ab1 ba14ce2b cc4642f1 8c3f9ed0 df9da5c4 c14912f7 1c232402 0529f8e8
b614eb2b ff8f6ee3 a04bb40f c669420d 296d9f9d 51fc4839 58909d12 7ce57c86

enc:
01b716a3 3ef96baa 96761a89 0b08efc6 762f2f20 fe7db159 7c3e3663 4a3973e6
8bdb71f9 1cc2d701 ad4424a3 04554f12 efce4c25 991f2033 d51c1f3c 43d95564
4510

kem_context:
01b716a3 3ef96baa 96761a89 0b08efc6 762f2f20 fe7db159 7c3e3663 4a3973e6
8bdb71f9 1cc2d701 ad4424a3 04554f12 efce4c25 991f2033 d51c1f3c 43d95564
451001bf 5b742786 12e1cfa7 a47cdbe2 4a6fbe41 b73c32e9 8e986d40 c8490a92
01d31874 83b8b66e 27105a3e b80c394a 889a2484 18757425 b0e3a4b3 76f3fd8e
a087daf4 01856189 0c5378f2 dedf9da7 8c082f22 01110f1c ca97637c e4ae528c
af38ee87 5d70b77f a72c4b6f 2fb42466 f98852dc 8466c4de f387db3a 6514872f
616d7379 e27e

shared_secret:
3c1c20e2 16a48012 e032127b af46a725 e55448f8 511a5ea2 ebffd891 473ebc8c
20373d88 8738685b 018e7310 066976bb b35ad27f 9392a870 42865aeb 354b2428

key sched context:
03b28b2b 7df96e43 3f4af4b3 578e3448 9e244d41 6b0b5f7a 0f5fb21f 5629c37a
4bafd80d fa613e70 86311242 98472b34 0feb0034 a430d8c3 1e25a3ca 304c7bd4
49bb5fa9 521626ec d409e935 bb6c1cc9 7e36868b 7340db4c d68c2438 afe2c5cc
bcb7cbb2 a5222dc4 53ff2e40 82a36356 9a1208a7 630a6234 95d29594 b2bd2539
0d

secret:
b9961790 85a65803 0a3c8644 ed77277b 63160d94 63ba2e4e 17057bbc 72f6cb9a
3d9de946 023d9a1a 299cb60b cf116c97 fd952362 499af097 6b7f432e b030bebd

key:
6a105ab1 ba14ce2b cc4642f1 8c3f9ed0 df9da5c4 c14912f7 1c232402 0529f8e8
b614eb2b ff8f6ee3 a04bb40f c669420d 296d9f9d 51fc4839 58909d12 7ce57c86

exp:
296d9f9d 51fc4839 58909d12 7ce57c86 c77e5cb4 5dcbefa0 1c34b7fe e4f68598
c2df16ec 9d007ba4 872c752b dfe54013 91608f52 e91a7141 b0ee7025 5ec07cf0
```

8.10.2. Encryption

~~~

pt: 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad: 436f756e 742d30
~~~

ct: 2c8bd708 935cc913 074060a2 ff5db0e1 563d0056 72557eba 18a0e582
60a99119 c164400e ccf409cd deea82fb f8

pt: 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad: 436f756e 742d31

ct: 7d6c5f46 c3d8e0f3 62efa1a3 2c230a75 a4bfbb47 46fd45de 6773740a
62a872a0 1b16e44a 1eb1f2dd 435add6e 68

pt: 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad: 436f756e 742d32

ct: bf43f1fd b74140f6 681f2321 5934cc24 dc4219b6 06951c40 c27fbd02
678aca0a 249311e8 f093a825 7c045dc7 22

pt: 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad: 436f756e 742d33

ct: a99e93b9 1c0b8327 ac0e795b 465c1b46 05c5e11c de85be69 33bf9f82
71492ca6 79ebaad9 c65bb192 9089c5e2 72

pt: 42656175 74792069 73207472 7574682c 20747275 74682062 65617574 79

aad: 436f756e 742d34

ct: 4e1d98dc 13a5af34 b4fbce6a bbab5de1 0deaa4a2 8a8f9c70 4db00592
63f6e113 490433d9 79456839 16abee42 0d

9. References

9.1. Normative References

[NISTCurves]
"Digital signature standard (DSS)", National Institute of Standards and Technology (U.S.) report, DOI 10.6028/nist.fips.186-4, 2013, <https://doi.org/10.6028/nist.fips.186-4>.

[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/info/rfc2119>.

[RFC5297] Harkins, D., "Synthetic Initialization Vector (SIV) Authenticated Encryption Using the Advanced Encryption Standard (AES)", RFC 5297, DOI 10.17487/RFC5297, October 2008, <https://www.rfc-editor.org/info/rfc5297>.

[RFC6090] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", RFC 6090, DOI 10.17487/RFC6090, February 2011, <https://www.rfc-editor.org/info/rfc6090>.

[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/info/rfc8174>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/info/rfc9180>.

9.2. Informative References

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, DOI 10.17487/RFC2401, November 1998, <https://www.rfc-editor.org/info/rfc2401>.

[RFC5649] Housley, R. and M. Dworkin, "Advanced Encryption Standard (AES) Key Wrap with Padding Algorithm", RFC 5649, DOI 10.17487/RFC5649, September 2009, <https://www.rfc-editor.org/info/rfc5649>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[SECG] "Elliptic Curve Cryptography, Standards for Efficient Cryptography Group, ver. 2", 2009, <https://secg.org/sec1-v2.pdf>.

[SIV] Rogaway, P. and T. Shrimpton, "Determinstic Authenticated Encryption: A Provable-Security Treatment of the Key-Wrap Problem", 2007, <https://www.cs.ucdavis.edu/~rogaway/papers/keywrap.pdf>.

[X9102] ANSI X9, "Symmetric Key Cryptography For The Financial Services Industry-- Wrapping of Keys and Associated Data", 2020.

Author’s Address

Dan Harkins
Hewlett-Packard Enterprise
Email: daniel.harkins@hpe.com