Hybrid Public Key Encryption
draft-irtf-cfrg-hpke-00

Abstract

This document describes a scheme for hybrid public-key encryption (HPKE). This scheme provides authenticated public key encryption of arbitrary-sized plaintexts for a recipient public key. HPKE works for any combination of an asymmetric key encapsulation mechanism (KEM), key derivation function (KDF), and authenticated encryption with additional data (AEAD) encryption function. We provide instantiations of the scheme using widely-used and efficient primitives.

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 January 4, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 2
2. Requirements Notation ........................................... 3
3. Security Properties .............................................. 3
4. Notation .......................................................... 3
5. Cryptographic Dependencies ..................................... 4
   5.1. DH-Based KEM ............................................... 5
6. Hybrid Public Key Encryption .................................... 6
   6.1. Creating an Encryption Context ............................. 7
   6.2. Encryption to a Public Key .................................. 10
   6.3. Authentication using a Pre-Shared Key ..................... 10
   6.4. Authentication using an Asymmetric Key ................... 11
   6.5. Authentication using both a PSK and an Asymmetric Key .. 12
   6.6. Encryption and Decryption .................................. 12
7. Algorithm Identifiers ............................................ 13
   7.1. Key Encapsulation Mechanisms (KEMs) ....................... 13
   7.2. Key Derivation Functions (KDFs) ......................... 14
   7.3. Authentication Encryption with Associated Data (AEAD) Functions .................................. 14
8. Security Considerations ......................................... 15
9. IANA Considerations ............................................. 15
10. References ...................................................... 15
    10.1. Normative References .................................... 15
    10.2. Informative References .................................. 15
Appendix A. Possible TODOs ......................................... 17
Authors’ Addresses ................................................ 17

1. Introduction

"Hybrid" public-key encryption schemes (HPKE) that combine asymmetric and symmetric algorithms are a substantially more efficient solution than traditional public key encryption techniques such as those based on RSA or ElGamal. Encrypted messages convey a single ciphertext and authentication tag alongside a short public key, which may be further compressed. The key size and computational complexity of elliptic curve cryptographic primitives for authenticated encryption therefore make it compelling for a variety of use cases. This type of public key encryption has many applications in practice, for example:

- PGP [RFC6637]
- Messaging Layer Security [I-D.ietf-mls-protocol]
Currently, there are numerous competing and non-interoperable standards and variants for hybrid encryption, including ANSI X9.63 [ANSI], IEEE 1363a [IEEE], ISO/IEC 18033-2 [ISO], and SECG SEC 1 [SECG]. All of these existing schemes have problems, e.g., because they rely on outdated primitives, lack proofs of IND-CCA2 security, or fail to provide test vectors.

This document defines an HPKE scheme that provides a subset of the functions provided by the collection of schemes above, but specified with sufficient clarity that they can be interoperably implemented and formally verified.

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 BCP14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Security Properties

As a hybrid authentication encryption algorithm, we desire security against (adaptive) chosen ciphertext attacks (IND-CCA2 secure). The HPKE variants described in this document achieve this property under the Random Oracle model assuming the gap Computational Diffie Hellman (CDH) problem is hard [S01].

[[ TODO - Provide citations to these proofs once they exist ]]

4. Notation

The following terms are used throughout this document to describe the operations, roles, and behaviors of HPKE:

- Initiator (I): Sender of an encrypted message.
- Responder (R): Receiver of an encrypted message.
- Ephemeral (E): A fresh random value meant for one-time use.
- 
  "(skX, pkX)": A KEM key pair used in role X; "skX" is the private key and "pkX" is the public key.
5. Cryptographic Dependencies

HPKE variants rely on the following primitives:

- **A Key Encapsulation Mechanism (KEM):**
  - GenerateKeyPair(): Generate a key pair (sk, pk)
  - Marshal(pk): Produce a fixed-length octet string encoding the public key "pk"
  - Unmarshal(enc): Parse a fixed-length octet string to recover a public key
  - Encap(pk): Generate an ephemeral symmetric key and a fixed-length encapsulation of that key that can be decapsulated by the holder of the private key corresponding to pk
  - Decap(enc, sk): Use the private key "sk" to recover the ephemeral symmetric key from its encapsulated representation "enc"
  - AuthEncap(pkR, skI) (optional): Same as Encap(), but the outputs encode an assurance that the ephemeral shared key is known only to the holder of the private key "skI"
  - AuthDecap(skR, pkI) (optional): Same as Decap(), but the holder of the private key "skR" is assured that the ephemeral shared key is known only to the holder of the private key corresponding to "pkI"
* Nenc: The length in octets of an encapsulated key from this KEM

* Npk: The length in octets of a public key for this KEM

- A Key Derivation Function:
  - Extract(salt, IKM): Extract a pseudorandom key of fixed length from input keying material "IKM" and an optional octet string "salt"
  - Expand(PRK, info, L): Expand a pseudorandom key "PRK" using optional string "info" into "L" bytes of output keying material
  - Nh: The output size of the Extract function

- An AEAD encryption algorithm [RFC5116]:
  - Seal(key, nonce, aad, pt): Encrypt and authenticate plaintext "pt" with associated data "aad" using secret key "key" and nonce "nonce", yielding ciphertext and tag "ct"
  - Open(key, nonce, aad, ct): Decrypt ciphertext "ct" using associated data "aad" with secret key "key" and nonce "nonce", returning plaintext message "pt" or the error value "OpenError"
  - Nk: The length in octets of a key for this algorithm
  - Nn: The length in octets of a nonce for this algorithm

A set of algorithm identifiers for concrete instantiations of these primitives is provided in Section 7. Algorithm identifier values are two octets long.

5.1. DH-Based KEM

Suppose we are given a Diffie-Hellman group that provides the following operations:

- GenerateKeyPair(): Generate an ephemeral key pair "(sk, pk)" for the DH group in use
- DH(sk, pk): Perform a non-interactive DH exchange using the private key sk and public key pk to produce a fixed-length shared secret
- Marshal(pk): Produce a fixed-length octet string encoding the public key "pk"
Then we can construct a KEM (which we’ll call "DHKEM") in the following way:

```python
def Encap(pkR):
    skE, pkE = GenerateKeyPair()
    zz = DH(skE, pkR)
    enc = Marshal(pkE)
    return zz, enc

def Decap(enc, skR):
    pkE = Unmarshal(enc)
    return DH(skR, pkE)

def AuthEncap(pkR, skI):
    skE, pkE = GenerateKeyPair()
    zz = concat(DH(skE, pkR), DH(skI, pkR))
    enc = Marshal(pkE)
    return zz, enc

def AuthDecap(enc, skR, pkI):
    pkE = Unmarshal(enc)
    return concat(DH(skR, pkE), DH(skR, pkI))
```

The GenerateKeyPair, Marshal, and Unmarshal functions are the same as for the underlying DH group. The Marshal functions for the curves referenced in (#ciphersuites) are as follows:

- **P-256**: The X-coordinate of the point, encoded as a 32-octet big-endian integer
- **P-521**: The X-coordinate of the point, encoded as a 66-octet big-endian integer
- **Curve25519**: The standard 32-octet representation of the public key
- **Curve448**: The standard 56-octet representation of the public key

### 6. Hybrid Public Key Encryption

In this section, we define a few HPKE variants. All variants take a recipient public key and a sequence of plaintexts "pt", and produce an encapsulated key "enc" and a sequence of ciphertexts "ct". These outputs are constructed so that only the holder of the private key corresponding to "pkR" can decapsulate the key from "enc" and decrypt the ciphertexts. All of the algorithms also take an "info" parameter.
that can be used to influence the generation of keys (e.g., to fold in identity information) and an "aad" parameter that provides Additional Authenticated Data to the AEAD algorithm in use.

In addition to the base case of encrypting to a public key, we include two authenticated variants, one of which authenticates possession of a pre-shared key, and one of which authenticates possession of a KEM private key. The following one-octet values will be used to distinguish between modes:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mode_base</td>
<td>0x00</td>
</tr>
<tr>
<td>mode_psk</td>
<td>0x01</td>
</tr>
<tr>
<td>mode_auth</td>
<td>0x02</td>
</tr>
<tr>
<td>mode_psk_auth</td>
<td>0x03</td>
</tr>
</tbody>
</table>

All of these cases follow the same basic two-step pattern:

1. Set up an encryption context that is shared between the sender and the recipient

2. Use that context to encrypt or decrypt content

A "context" encodes the AEAD algorithm and key in use, and manages the nonces used so that the same nonce is not used with multiple plaintexts.

The procedures described in this session are laid out in a Python-like pseudocode. The algorithms in use are left implicit.

6.1. Creating an Encryption Context

The variants of HPKE defined in this document share a common mechanism for translating the protocol inputs into an encryption context. The key schedule inputs are as follows:

- "pkR" - The receiver’s public key
- "zz" - A shared secret generated via the KEM for this transaction
- "enc" - An encapsulated key produced by the KEM for the receiver
o "info" - Application-supplied information (optional; default value "")

o "psk" - A pre-shared secret held by both the initiator and the receiver (optional; default value "zero(Nh)").

o "pskID" - An identifier for the PSK (optional; default value "" = zero(0)"

o "pkI" - The initiator’s public key (optional; default value "zero(Npk)"

The "psk" and "pskID" fields MUST appear together or not at all. That is, if a non-default value is provided for one of them, then the other MUST be set to a non-default value.

The key and nonce computed by this algorithm have the property that they are only known to the holder of the recipient private key, and the party that ran the KEM to generate "zz" and "enc". If the "psk" and "pskID" arguments are provided, then the recipient is assured that the initiator held the PSK. If the "pkIm" argument is provided, then the recipient is assured that the initiator held the corresponding private key (assuming that "zz" and "enc" were generated using the AuthEncap / AuthDecap methods; see below).
default_pkIm = zero(Npk)
default_psk = zero(Nh)
default_pskID = zero(0)

def VerifyMode(mode, psk, pskID, pkIm):
  got_psk = (psk != default_psk and pskID != default_pskID)
  no_psk = (psk == default_psk and pskID == default_pskID)
  got_pkIm = (pkIm != default_pkIm)
  no_pkIm = (pkIm == default_pkIm)

  if mode == mode_base and (got_psk or got_pkIm):
    raise Exception("Invalid configuration for mode_base")
  if mode == mode_psk and (no_psk or got_pkIm):
    raise Exception("Invalid configuration for mode_psk")
  if mode == mode_auth and (got_psk or no_pkIm):
    raise Exception("Invalid configuration for mode_auth")
  if mode == mode_psk_auth and (no_psk or no_pkIm):
    raise Exception("Invalid configuration for mode_psk_auth")

def EncryptionContext(mode, pkRm, zz, enc, info, psk, pskID, pkIm):
  VerifyMode(mode, psk, pskID, pkIm)

  pkRm = Marshal(pkR)
  context = concat(mode, ciphersuite, enc, pkRm, pkIm,
                   len(pskID), pskID, len(info), info)

  secret = Extract(psk, zz)
  key = Expand(secret, concat("hpke key", context), Nk)
  nonce = Expand(secret, concat("hpke nonce", context), Nn)
  return Context(key, nonce)

Note that the context construction in the KeySchedule procedure is equivalent to serializing a structure of the following form in the TLS presentation syntax:
struct {
    // Mode and algorithms
    uint8 mode;
    uint16 ciphersuite;

    // Public inputs to this key exchange
    opaque enc[Nenc];
    opaque pkR[Npk];
    opaque pkI[Npk];
    opaque pskID<0..2^16-1>;

    // Application-supplied info
    opaque info<0..2^16-1>;
} HPKEContext;

6.2. Encryption to a Public Key

The most basic function of an HPKE scheme is to enable encryption for
the holder of a given KEM private key. The "SetupBaseI()" and
"SetupBaseR()" procedures establish contexts that can be used to
e encrypt and decrypt, respectively, for a given private key.

The the shared secret produced by the KEM is combined via the KDF
with information describing the key exchange, as well as the explicit
"info" parameter provided by the caller.

    def SetupBaseI(pkR, info):
        zz, enc = Encap(pkR)
        return enc, KeySchedule(mode_base, pkR, zz, enc, info, 
                                default_psk, default_pskID, default_pkIm)

    def SetupBaseR(enc, skR, info):
        zz = Decap(enc, skR)
        return KeySchedule(mode_base, pk(skR), zz, enc, info, 
                            default_psk, default_pskID, default_pkIm)

6.3. Authentication using a Pre-Shared Key

This variant extends the base mechanism by allowing the recipient to
authenticate that the sender possessed a given pre-shared key (PSK).
We assume that both parties have been provisioned with both the PSK
value "psk" and another octet string "pskID" that is used to identify
which PSK should be used.

The primary differences from the base case are:

  o The PSK is used as the "salt" input to the KDF (instead of 0)
o The PSK ID is added to the context string used as the "info" input to the KDF

This mechanism is not suitable for use with a low-entropy password as the PSK. A malicious recipient that does not possess the PSK can use decryption of a plaintext as an oracle for performing offline dictionary attacks.

```
def SetupPSKI(pkR, psk, pskID, info):
    zz, enc = Encap(pkR)
    return enc, KeySchedule(pkR, zz, enc, info, psk, pskId, default_pkIm)

def SetupPSKR(enc, skR, psk, pskID, info):
    zz = Decap(enc, skR)
    return KeySchedule(pk(skR), zz, enc, info, psk, pskId, default_pkIm)
```

6.4. Authentication using an Asymmetric Key

This variant extends the base mechanism by allowing the recipient to authenticate that the sender possessed a given KEM private key. This assurance is based on the assumption that "AuthDecap(enc, skR, pkI)" produces the correct shared secret only if the encapsulated value "enc" was produced by "AuthEncap(pkR, skI)", where "skI" is the private key corresponding to "pkI". In other words, only two people could have produced this secret, so if the recipient is one, then the sender must be the other.

The primary differences from the base case are:

o The calls to "Encap" and "Decap" are replaced with calls to "AuthEncap" and "AuthDecap".

o The initiator public key is added to the context string

Obviously, this variant can only be used with a KEM that provides "AuthEncap()" and "AuthDecap()" procedures.

This mechanism authenticates only the key pair of the initiator, not any other identity. If an application wishes to authenticate some other identity for the sender (e.g., an email address or domain name), then this identity should be included in the "info" parameter to avoid unknown key share attacks.
def SetupAuthI(pkR, skI, info):
    zz, enc = AuthEncap(pkR, skI)
    pkIm = Marshal(pk(skI))
    return enc, KeySchedule(pkR, zz, enc, info,
                            default_psk, default_pskID, pkIm)

def SetupAuthR(enc, skR, pkI, info):
    zz = AuthDecap(enc, skR, pkI)
    pkIm = Marshal(pkI)
    return KeySchedule(pk(skR), zz, enc, info, 
                       default_psk, default_pskID, pkIm)

6.5. Authentication using both a PSK and an Asymmetric Key

This mode is a straightforward combination of the PSK and authenticated modes. The PSK is passed through to the key schedule as in the former, and as in the latter, we use the authenticated KEM variants.

def SetupAuthI(pkR, psk, pskID, skI, info):
    zz, enc = AuthEncap(pkR, skI)
    pkIm = Marshal(pk(skI))
    return enc, KeySchedule(pkR, zz, enc, info, psk, pskID, pkIm)

def SetupAuthR(enc, skR, psk, pskID, pkI, info):
    zz = AuthDecap(enc, skR, pkI)
    pkIm = Marshal(pkI)
    return KeySchedule(pk(skR), zz, enc, info, psk, pskID, pkIm)

6.6. Encryption and Decryption

HPKE allows multiple encryption operations to be done based on a given setup transaction. Since the public-key operations involved in setup are typically more expensive than symmetric encryption or decryption, this allows applications to "amortize" the cost of the public-key operations, reducing the overall overhead.

In order to avoid nonce reuse, however, this decryption must be stateful. Each of the setup procedures above produces a context object that stores the required state:

- The AEAD algorithm in use
- The key to be used with the AEAD algorithm
- A base nonce value
- A sequence number (initially 0)
All of these fields except the sequence number are constant. The sequence number is used to provide nonce uniqueness: The nonce used for each encryption or decryption operation is the result of XORing the base nonce with the current sequence number, encoded as a big-endian integer of the same length as the nonce. Implementations MAY use a sequence number that is shorter than the nonce (padding on the left with zero), but MUST return an error if the sequence number overflows.

Each encryption or decryption operation increments the sequence number for the context in use. A given context SHOULD be used either only for encryption or only for decryption.

It is up to the application to ensure that encryptions and decryptions are done in the proper sequence, so that the nonce values used for encryption and decryption line up.

```python
def Context.Nonce(seq):
    encSeq = encode_big_endian(seq, len(self.nonce))
    return xor(self.nonce, encSeq)

def Context.Seal(aad, pt):
    ct = Seal(self.key, self.Nonce(self.seq), aad, pt)
    self.seq += 1
    return ct

def Context.Open(aad, ct):
    pt = Open(self.key, self.Nonce(self.seq), aad, ct)
    if pt == OpenError:
        return OpenError
    self.seq += 1
    return pt
```

7. Algorithm Identifiers

7.1. Key Encapsulation Mechanisms (KEMs)
For the NIST curves P-256 and P-521, the Marshal function of the DH scheme produces the normal (non-compressed) representation of the public key, according to [SECG]. When these curves are used, the recipient of an HPKE ciphertext MUST validate that the ephemeral public key "pkE" is on the curve. The relevant validation procedures are defined in [keyagreement].

For the CFRG curves Curve25519 and Curve448, the Marshal function is the identity function, since these curves already use fixed-length octet strings for public keys.

7.2. Key Derivation Functions (KDFs)

<table>
<thead>
<tr>
<th>Value</th>
<th>KDF</th>
<th>Nh</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>(reserved)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>0x0001</td>
<td>HKDF-SHA256</td>
<td>32</td>
<td>[RFC5869]</td>
</tr>
<tr>
<td>0x0002</td>
<td>HKDF-SHA512</td>
<td>64</td>
<td>[RFC5869]</td>
</tr>
</tbody>
</table>

7.3. Authentication Encryption with Associated Data (AEAD) Functions

<table>
<thead>
<tr>
<th>Value</th>
<th>KDF</th>
<th>Nh</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>(reserved)</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>0x0001</td>
<td>HKDF-SHA256</td>
<td>32</td>
<td>[RFC5869]</td>
</tr>
<tr>
<td>0x0002</td>
<td>HKDF-SHA512</td>
<td>64</td>
<td>[RFC5869]</td>
</tr>
</tbody>
</table>
8. Security Considerations

[[ TODO ]]

9. IANA Considerations

[[ TODO: Make IANA registries for the above ]]

10. References

10.1. Normative References


10.2. Informative References

[ANSI] "Public Key Cryptography for the Financial Services Industry -- Key Agreement and Key Transport Using Elliptic Curve Cryptography", n.d..


[IEEE] "IEEE 1363a, Standard Specifications for Public Key Cryptography - Amendment 1 -- Additional Techniques", n.d..


Appendix A. Possible TODOs

The following extensions might be worth specifying:

- Multiple recipients - It might be possible to add some simplifications / assurances for the case where the same value is being encrypted to multiple recipients.

- Test vectors - Obviously, we can provide decryption test vectors in this document. In order to provide known-answer tests, we would have to introduce a non-secure deterministic mode where the ephemeral key pair is derived from the inputs. And to do that safely, we would need to augment the decrypt function to detect the deterministic mode and fail.

- A reference implementation in hacspec or similar

Authors’ Addresses

Richard L. Barnes
Cisco

Email: rlb@ipv.sx

Karthik Bhargavan
Inria

Email: karthikeyan.bhargavan@inria.fr