Enumeration

HPKE

A container for hybrid public key encryption (HPKE) operations.

iOS 17.0+ | iPadOS 17.0+ | Mac Catalyst 17.0+ | macOS 14.0+ | tvOS 17.0+ | visionOS 1.0+ | watchOS 10.0+

```
enum HPKE
```

Overview

Hybrid public key encryption (HPKE) uses a symmetric encryption algorithm to encrypt data, and encapsulates the symmetric encryption material using a public key encryption algorithm.

HPKE ensures that the ciphertext wasn't tampered with after its creation. It can also check the validity of additional cleartext data in apps where you need to send headers or other metadata as cleartext.

HPKE optionally incorporates sender authentication, allowing the recipient to validate the authenticity of messages using the sender's public key.

HPKE is described in the Internet Research Task Force (IRTF) document RFC 9180.

Topics

Sending and receiving messages

`struct` Sender

A type that represents the sending side of an HPKE message exchange.

`struct Recipient`

A type that represents the receiving side of an HPKE message exchange.

Choosing cryptographic algorithms

`struct Ciphersuite`

Cipher suites to use in hybrid public key encryption (HPKE).

`enum AEAD`

The authenticated encryption with associated data (AEAD) algorithms to use in HPKE.

`enum KDF`

The key derivation functions to use in HPKE.

`enum KEM`

The key encapsulation mechanisms to use in HPKE.

`enum DHKEM`

A container for Diffie-Hellman key encapsulation mechanisms (KEMs).

Handling errors

`enum Errors`

Hybrid public key encryption (HPKE) errors that CryptoKit uses.

Relationships

Conforms To

`Sendable`, `SendableMetatype`

See Also

Public key cryptography

`enum` Curve25519

An elliptic curve that enables X25519 key agreement and Ed25519 signatures.

`enum` P521

An elliptic curve that enables NIST P-521 signatures and key agreement.

`enum` P384

An elliptic curve that enables NIST P-384 signatures and key agreement.

`enum` P256

An elliptic curve that enables NIST P-256 signatures and key agreement.

`struct` SharedSecret

A key agreement result from which you can derive a symmetric cryptographic key.

`enum` SecureEnclave

A representation of a device's hardware-based key manager.