Structure

HPKE.Recipient

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

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

```
struct Recipient
```

Overview

To decrypt and verify the identity of encrypted messages, initialize a `Recipient` specifying the appropriate cipher suite, the receiver's private key, the encapsulated symmetric key, and the additional cryptographic material relevant to your chosen mode of operation. Call `open(_:)` or `open(_:authenticating:)` on the `Recipient` instance for each message in turn to retrieve its cleartext. The recipient of the messages needs to process them in the same order as the `Sender`, using the same cipher suite, encryption mode, and key schedule information (`info` data). Use a separate `Recipient` instance for each stream of messages.

Topics

Initializers

`init<SK>(privateKey: SK, ciphersuite: HPKE.Ciphersuite, info: Data, encapsulatedKey: Data) throws`

Creates a recipient in base mode.

`init<SK>(privateKey: SK, ciphersuite: HPKE.Ciphersuite, info: Data, encapsulatedKey: Data) throws`

Creates a recipient in base mode.

```
init<SK>(privateKey: SK, ciphersuite: HPKE.Ciphersuite, info: Data, encapsulatedKey: Data, authenticatedBy: SK.PublicKey) throws
```

Creates a recipient in authentication mode.

```
init<SK>(privateKey: SK, ciphersuite: HPKE.Ciphersuite, info: Data, encapsulatedKey: Data, authenticatedBy: SK.PublicKey, presharedKey: SymmetricKey, presharedKeyIdentifier: Data) throws
```

Creates a recipient in authentication and preshared key mode.

```
init<SK>(privateKey: SK, ciphersuite: HPKE.Ciphersuite, info: Data, encapsulatedKey: Data, presharedKey: SymmetricKey, presharedKey Identifier: Data) throws
```

Creates a recipient in preshared key (PSK) mode.

Instance Methods

```
func exportSecret<Context>(context: Context, outputByteCount: Int) throws -> SymmetricKey
```

Exports a secret given domain-separation context and the desired output length.

```
func open<C>(C) throws -> Data
```

Decrypts a message, if the ciphertext is valid.

```
func open<C, AD>(C, authenticating: AD) throws -> Data
```

Decrypts a message, if the ciphertext is valid, verifying the integrity of additional authentication data.

Relationships

Conforms To

`Sendable`, `SendableMetatype`

See Also

Sending and receiving messages

`struct` Sender

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