Documentation

Language: Swift

Apple CryptoKit / HPKE / HPKE.Sender

Structure

HPKE.Sender

A type that represents the sending 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 Sender
```

Overview

To create encrypted messages, initialize a `Sender` specifying the appropriate cipher suite, the recipient's public key, and the additional cryptographic material relevant to your chosen mode of operation. Call `seal(_:)` or `seal(_:authenticating:)` on the `Sender` instance for each message in turn to retrieve its ciphertext. The recipient of the messages needs to process them in the same order as the `Sender`, using the same encryption mode, cipher suite, and key schedule information (`info`), as well as the `Sender`'s `encapsulatedKey`.

Topics

Initializers

`init<PK>(recipientKey: PK, ciphersuite: HPKE.Ciphersuite, info: Data) throws`

Creates a sender in base mode.

`init<PK>(recipientKey: PK, ciphersuite: HPKE.Ciphersuite, info: Data) throws`

Creates a sender in base mode.

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

Creates a sender in authentication mode.

```
init<SK>(recipientKey: SK.PublicKey, ciphersuite: HPKE.Ciphersuite,
info: Data, authenticatedBy: SK, presharedKey: SymmetricKey, preshared
KeyIdentifier: Data) throws
```

Creates a sender in authentication and preshared key mode.

```
init<PK>(recipientKey: PK, ciphersuite: HPKE.Ciphersuite, info: Data,
presharedKey: SymmetricKey, presharedKeyIdentifier: Data) throws
```

Creates a sender in preshared key (PSK) mode.

Instance Properties

```
let encapsulatedKey: Data
```

The encapsulated symmetric key that the recipient uses to decrypt messages.

Instance Methods

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

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

```
func seal<M>(M) throws -> Data
```

Encrypts the given cleartext message.

```
func seal<M, AD>(M, authenticating: AD) throws -> Data
```

Encrypts the given cleartext message and attaches additional authenticated data.

Relationships

Conforms To

`Sendable`, `SendableMetatype`

See Also

Sending and receiving messages

`struct Recipient`

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