Apple CryptoKit / SharedSecret

Structure

SharedSecret

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

iOS 13.0+ | iPadOS 13.0+ | Mac Catalyst 13.0+ | macOS 10.15+ | tvOS 13.0+ | visionOS 1.0+ | watchOS 6.0+

```
struct SharedSecret
```

Overview

Generate a shared secret by calling your private key's `sharedSecretFromKeyAgreement(publicKeyShare:)` method with the public key from another party. The other party computes the same secret by passing your public key to the the equivalent method on their own private key.

The shared secret isn't suitable as a symmetric cryptographic key (`SymmetricKey`) by itself. However, you use it to generate a key by calling either the `hkdfDerivedSymmetricKey(using:salt:sharedInfo:outputByteCount:)` or `x963DerivedSymmetricKey(using:sharedInfo:outputByteCount:)` method of the shared secret. After the other party does the same, then you both share a symmetric key suitable for creating a message authentication code like `HMAC`, or for opening and closing a sealed box with a cipher like `ChaChaPoly` or `AES`.

Topics

Deriving keys

```
func hkdfDerivedSymmetricKey<H, Salt, SI>(using: H.Type, salt: Salt, sharedInfo: SI, outputByteCount: Int) -> SymmetricKey
```

Derives a symmetric encryption key from the secret using HKDF key derivation.

```
func x963DerivedSymmetricKey<H, SI>(using: H.Type, sharedInfo: SI, outputByteCount: Int) -> SymmetricKey
```

Derives a symmetric encryption key from the secret using x9.63 key derivation.

Comparing shared secrets

```
static func == <D>(SharedSecret, D) -> Bool
```

Determines whether a shared secret is equivalent to a collection of contiguous bytes.

Relationships

Conforms To

```
ContiguousBytes
Copyable
CustomStringConvertible
Equatable
Hashable
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.

`enum SecureEnclave`

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

`enum HPKE`

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