Protocol

DiffieHellmanKeyAgreement

A Diffie-Hellman Key Agreement Key

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

```
@preconcurrency
protocol DiffieHellmanKeyAgreement : Sendable
```

Topics

Associated Types

`associatedtype PublicKey : Sendable`

The public key share type to perform the DH Key Agreement

Required

Instance Properties

`var publicKey: Self.PublicKey`

Required

Instance Methods

`func sharedSecretFromKeyAgreement(with: Self.PublicKey) throws -> SharedSecret`

Performs a Diffie-Hellman Key Agreement.

Required

Relationships

Inherits From

Sendable, SendableMetatype

Inherited By

HPKEDiffieHellmanPrivateKey, HPKEDiffieHellmanPrivateKeyGeneration

Conforming Types

Curve25519.KeyAgreement.PrivateKey
P256.KeyAgreement.PrivateKey
P384.KeyAgreement.PrivateKey
P521.KeyAgreement.PrivateKey
SecureEnclave.P256.KeyAgreement.PrivateKey