Protocol

KEMPrivateKey

The private key for a key encapsulation mechanism.

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

```
@preconcurrency
protocol KEMPrivateKey : Sendable
```

Topics

Associated Types

`associatedtype PublicKey : KEMPublicKey`

Required

Instance Properties

`var publicKey: Self.PublicKey`

The associated public key.

Required

Instance Methods

`func decapsulate(Data) throws -> SymmetricKey`

Recovers a shared secret from an encapsulated representation.

Required

Type Methods

```
static func generate() throws -> Self
```

Generates a new random private key.

Required

Relationships

Inherits From

`Sendable`, `SendableMetatype`

Inherited By

`HPKEKEMPrivateKey`, `HPKEKEMPrivateKeyGeneration`

Conforming Types

`MLKEM1024.PrivateKey`
`MLKEM768.PrivateKey`
`SecureEnclave.MLKEM1024.PrivateKey`
`SecureEnclave.MLKEM768.PrivateKey`
`XWingMLKEM768X25519.PrivateKey`

See Also

KEM keys

```
protocol KEMPublicKey
```

The public key for a key encapsulation mechanism.