

[Apple CryptoKit](#) / MLKEM768

Enumeration

MLKEM768

The Module-Lattice key encapsulation mechanism (KEM).

iOS 26.0+ | iPadOS 26.0+ | Mac Catalyst 26.0+ | macOS 26.0+ | tvOS 26.0+ | visionOS 26.0+ | watchOS 26.0+

`enum` MLKEM768

Topics

Keys

`struct` PrivateKey

A private key you use to decapsulate shared secrets with the Module-Lattice key encapsulation mechanism.

`struct` PublicKey

A public key you use to encapsulate shared secrets with the Module-Lattice key encapsulation mechanism.

Relationships

Conforms To

Sendable, SendableMetatype

See Also

Key encapsulation mechanisms (KEM)

enum KEM

A key encapsulation mechanism.

enum MLKEM1024

The Module-Lattice key encapsulation mechanism (KEM).

enum XWingMLKEM768X25519

The X-Wing (ML-KEM768 with X25519) Key Encapsulation Mechanism, defined in <https://datatracker.ietf.org/doc/html/draft-connolly-cfrg-xwing-kem-06>