

[Authentication Services](#) / `ASAuthorizationProviderExtensionEncryptionAlgorithm`

Structure

ASAuthorizationProviderExtensionEncryptionAlgorithm

macOS 15.0+

```
struct ASAuthorizationProviderExtensionEncryptionAlgorithm
```

Topics

Initializers

```
init(NSNumber)
```

```
init(rawValue: NSNumber)
```

Type Properties

```
static let ecdhe_A256GCM: ASAuthorizationProviderExtensionEncryptionAlgorithm
```

A encryption algorithm that uses NIST P-256 elliptic curve key agreement, ConcatKDF key derivation with a 256-bit digest, and the Advanced Encryption Standard cipher in Galois/Counter Mode with a key length of 256 bits.

```
static let hpke_Curve25519_SHA256_ChachaPoly: ASAuthorizationProviderExtensionEncryptionAlgorithm
```

A cipher suite for HPKE that uses X25519 elliptic curve key agreement, SHA-2 key derivation with a 256-bit digest, and the ChaCha20 stream cipher with the Poly1305 message authentication code.

```
static let hpke_P256_SHA256_AES_GCM_256: ASAuthorizationProvider  
ExtensionEncryptionAlgorithm
```

A cipher suite for HPKE that uses NIST P-256 elliptic curve key agreement, SHA-2 key derivation with a 256-bit digest, and the Advanced Encryption Standard cipher in Galois/Counter Mode with a key length of 256 bits.

```
static let hpke_P384_SHA384_AES_GCM_256: ASAuthorizationProvider  
ExtensionEncryptionAlgorithm
```

A cipher suite that you use for HPKE using NIST P-384 elliptic curve key agreement, SHA-2 key derivation with a 384-bit digest, and the Advanced Encryption Standard cipher in Galois/Counter Mode with a key length of 256 bits.

Relationships

Conforms To

RawRepresentable, Sendable, SendableMetatype