Structure

HMAC

A hash-based message authentication algorithm.

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

```
struct HMAC<H> where H : HashFunction
```

Overview

Use hash-based message authentication to create a code with a value that's dependent on both a block of data and a symmetric cryptographic key. Another party with access to the data and the same secret key can compute the code again and compare it to the original to detect whether the data changed. This serves a purpose similar to digital signing and verification, but depends on a shared symmetric key instead of public-key cryptography.

As with digital signing, the data isn't hidden by this process. When you need to encrypt the data as well as authenticate it, use a cipher like `AES` or `ChaChaPoly` to put the data into a sealed box (an instance of `AES.GCM.SealedBox` or `ChaChaPoly.SealedBox`).

Topics

Getting a key

`typealias Key`

An alias for the symmetric key type used to compute or verify a message authentication code.

`struct SymmetricKey`

A symmetric cryptographic key.

Working with codes

`typealias MAC`

An alias for a hash-based message authentication code.

`struct HashedAuthenticationCode`

A hash-based message authentication code.

`protocol MessageAuthenticationCode`

A type that represents a message authentication code.

Creating an authentication code with one call

`static func authenticationCode<D>(for: D, using: SymmetricKey) -> HMAC<H>.MAC`

Computes a message authentication code for the given data.

Creating an authentication code iteratively

`init(key: SymmetricKey)`

Creates a message authentication code generator.

`func update<D>(data: D)`

Updates the message authentication code computation with a block of data.

`func finalize() -> HMAC<H>.MAC`

Finalizes the message authentication computation and returns the computed code.

Checking an authentication code

`static func isValidAuthenticationCode<D>(HMAC<H>.MAC, authenticating: D, using: SymmetricKey) -> Bool`

Returns a Boolean value indicating whether the given message authentication code is valid for a block of data.

`static func isValidAuthenticationCode(HMAC<H>.MAC, authenticating: UnsafeRawBufferPointer, using: SymmetricKey) -> Bool`

Returns a Boolean value indicating whether the given message authentication code is valid for a block of data stored in a buffer.

```
static func isValidAuthenticationCode<C, D>(C, authenticating: D, using
: SymmetricKey) -> Bool
```

Returns a Boolean value indicating whether the given message authentication code represented as contiguous bytes is valid for a block of data.

Relationships

Conforms To

`Sendable`, `SendableMetatype`

See Also

Message authentication codes

`struct SymmetricKey`

A symmetric cryptographic key.

`struct SymmetricKeySize`

The sizes that a symmetric cryptographic key can take.