libhmac Overview

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

1 Library Overview

Overview

libhmac is a library that is used to generate a digest value using the HMAC format as defined by FIPS 198.

Files

The following files are required to use libhmac.

Filename	Description
libhmac.h	Header file
libSceHmac.a	Static link library file
libSceHmac_stub.a	Stub library file
libSceHmac_stub_weak.a	weak import stub library file
libhmac.suprx	PRX module file

2 Using the Library

Basic Usage Procedure

(1) HMAC-SHA1 digest value computation (comprehensive)

No specific initialization is required to use libhmac.

```
SceUChar8 digest[SCE_HMAC_SHA1_DIGEST_SIZE];

sceHmacSha1Digest(key, keylen, plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceHmacSha1Digest()` function, as shown above.

(2) HMAC-SHA1 digest value computation (divided)

To compute a digest value for a large amount of data, the hash calculation can be broken up as shown below.

```
SceHmacSha1Context sha;
SceUChar8 digest[SCE_HMAC_SHA1_DIGEST_SIZE];

sceHmacSha1BlockInit(&sha, key, kenlen);
sceHmacSha1BlockUpdate(&sha, plain1, len1);
sceHmacSha1BlockUpdate(&sha, plain2, len2);
sceHmacSha1BlockUpdate(&sha, plain3, len3);
        :            Repeat an arbitrary number of times
sceHmacSha1BlockResult(&sha, digest);
```

First, call the `sceHmacSha1BlockInit()` function to initialize the `SceHmacSha1Context` structure. Then, call the `sceHmacSha1BlockUpdate()` function the desired number of times. Lastly, the digest value can be obtained by calling the `sceHmacSha1BlockResult()` function.

Digest Value Size

In libhmac, the size of the digest value is determined using each hash algorithm, but the size will be variable if SHA-512/224 or SHA-512/256 is used as the digest algorithm. Set either 224 or 256 in the argument *t* of the `sceHmacSha512tDigest()` and `sceHmacSha512tBlockInit()` functions.