libsha512 Overview

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

1 Library Overview

Overview

libsha512 is a library that is used to generate a digest value using the SHA-512 Secure Hash Algorithm 512 format as defined by FIPS 180-2. It can be used to detect data corruption and prevent data tampering through the use of Keyed-Hashing for Message Authentication (HMAC).

Files

The following files are required to use libsha512.

Filename	Description
libsha512.h	Header file
libSceSha512.a	Static link library file
libSceSha512_stub.a	Stub library file
libSceSha512_stub_weak.a	weak import stub library file
libsha512.suprx	PRX module file

2 Using the Library

Basic Usage Procedure

(1) SHA-512 digest value computation (comprehensive)

No specific initialization is required to use libsha512.

```
SceUChar8 digest[SCE_SHA512_DIGEST_SIZE];

sceSha512Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceSha512Digest()` function, as shown above.

(2) SHA-512 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.

```
SceSha512Context sha;
SceUChar8 digest[SCE_SHA512_DIGEST_SIZE];

sceSha512BlockInit(&sha);
sceSha512BlockUpdate(&sha, plain1, len1);
sceSha512BlockUpdate(&sha, plain2, len2);
sceSha512BlockUpdate(&sha, plain3, len3);
        :            Repeat an arbitrary number of times
sceSha512BlockResult(&sha, digest);
```

First, call the `sceSha512BlockInit()` function to initialize the `SceSha512Context` structure. Then, call the `sceSha512BlockUpdate()` function the desired number of times. Lastly, the digest value can be obtained by calling the `sceSha512BlockResult()` function.