libsha512t Overview

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

1 Library Overview

Overview

libsha512t is a library that is used to generate a digest value using the SHA-512/t Secure Hash Algorithm 512 format as defined by FIPS 180-4. 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 libsha512t.

Filename	Description
libsha512t.h	Header file
libSceSha512t.a	Static link library file
libSceSha512t_stub.a	Stub library file
libSceSha512t_stub_weak.a	weak import stub library file
libsha512t.suprx	PRX module file

2 Using the Library

Basic Usage Procedure

(1) SHA-512/224 digest value computation (comprehensive)

No specific initialization is required to use libsha512t.

```
SceUChar8 digest[224 / 8];

sceSha512tDigest(224, plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceSha512tDigest()` function, as shown above.

(2) SHA-512/224 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.

```
SceSha512tContext sha;
SceUChar8 digest[224 / 8];

sceSha512tBlockInit(&sha, 224);
sceSha512tBlockUpdate(&sha, plain1, len1);
sceSha512tBlockUpdate(&sha, plain2, len2);
sceSha512tBlockUpdate(&sha, plain3, len3);
        :            Repeat an arbitrary number of times
sceSha512tBlockResult(&sha, digest);
```

First, call the `sceSha512tBlockInit()` function to initialize the `SceSha512tContext` structure. Then, call the `sceSha512tBlockUpdate()` function the desired number of times. Lastly, the digest value can be obtained by calling the `sceSha512tBlockResult()` function.

Digest Value Size

In libsha512t, the size of the digest value is variable.

Set either 224 or 256 in the argument *t* of the `sceSha512tDigest()` and `sceSha512tBlockInit()` functions to use SHA-512/224 and SHA-512/256 defined by FIPS 180-4.