libsha0 Overview

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

1 Library Overview

Overview

libsha0 is a library for generating an SHA-0-format digest value, where SHA is the Secure Hash Algorithm. It can be used to detect data corruption and prevent data tampering by applying Keyed-Hashing for Message Authentication (HMAC).

Use of SHA-0 is not recommended since it is known to cause collisions.

Files

The following files are required to use libsha0.

Filename	Description
libsha0.h	Header file
libSceSha0.a	Static link library file
libSceSha0_stub.a	Stub library file
libSceSha0_stub_weak.a	weak import stub library file
libsha0.suprx	PRX module file

2 Using the Library

Basic Usage Procedure

(1) SHA-0 digest value computation (comprehensive)

No specific initialization is required to use libsha0.

```
SceUChar8 digest[SCE_SHA0_DIGEST_SIZE];

sceSha0Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceSha0Digest()` function, as shown above.

(2) SHA-0 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.

```
SceSha0Context sha;
SceUChar8 digest[SCE_SHA0_DIGEST_SIZE];

sceSha0BlockInit(&sha);
sceSha0BlockUpdate(&sha, plain1, len1);
sceSha0BlockUpdate(&sha, plain2, len2);
sceSha0BlockUpdate(&sha, plain3, len3);
        :            Repeat an arbitrary number of times
sceSha0BlockResult(&sha, digest);
```

First, call the `sceSha0BlockInit()` function to initialize the `SceSha0Context` structure. Then, call the `sceSha0BlockUpdate()` function the desired number of times. Lastly, the digest value can be obtained by calling the `sceSha0BlockResult()` function.