libsha1 Overview

SCE CONFIDENTIAL

Table of Contents

©SCEI

SCE CONFIDENTIAL

1 Library Overview

Overview

libsha1 is a library that is used to generate a digest value using the SHA-1 Secure Hash Algorithm 1 format as defined by RFC3417 (FIPS 180-1). 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 libsha1.

Filename	Description
libsha1.h	Header file
libSceSha1.a	Static link library file
libSceSha1_stub.a	Stub library file
libSceSha1_stub_weak.a	weak import stub library file
libsha1.suprx	PRX module file

2 Using the Library

Basic Usage Procedure

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

No specific initialization is required to use libsha1.

```
SceUChar8 digest[SCE_SHA1_DIGEST_SIZE];

sceSha1Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the `sceSha1Digest()` function, as shown above.

(2) SHA-1 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.

```
SceSha1Context sha;
SceUChar8 digest[SCE_SHA1_DIGEST_SIZE];

sceSha1BlockInit(&sha);
sceSha1BlockUpdate(&sha, plain1, len1);
sceSha1BlockUpdate(&sha, plain2, len2);
sceSha1BlockUpdate(&sha, plain3, len3);
        :            Repeat an arbitrary number of times
sceSha1BlockResult(&sha, digest);
```

First, call the `sceSha1BlockInit()` function to initialize the `SceSha1Context` structure. Then, call the `sceSha1BlockUpdate()` function the desired number of times. Lastly, the digest value can be obtained by calling the `sceSha1BlockResult()` function.