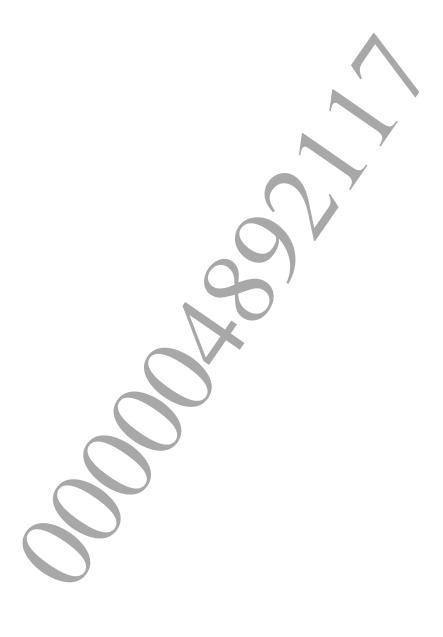


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

1 Library Overview		3
		-
Rasic Usage Proce		1



Library Overview

Overview

libsha384 is a library that is used to generate a digest value using the SHA-384 Secure Hash Algorithm 384 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 libsha384.

Description
Header file
Static link library file
Stub library file
weak import stub library file
PRX module file



2 Using the Library

Basic Usage Procedure

(1) SHA-384 digest value computation (comprehensive)

No specific initialization is required to use libsha384.

```
SceUChar8 digest[SCE_SHA384_DIGEST_SIZE];
sceSha384Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the sceSha384Digest () function, as shown above.

(2) SHA-384 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.

First, call the sceSha384BlockInit() function to initialize the SceSha384Context structure. Then, call the sceSha384BlockUpdate() function the desired number of times. Lastly, the digest value can be obtained by calling the sceSha384BlockResult() function.