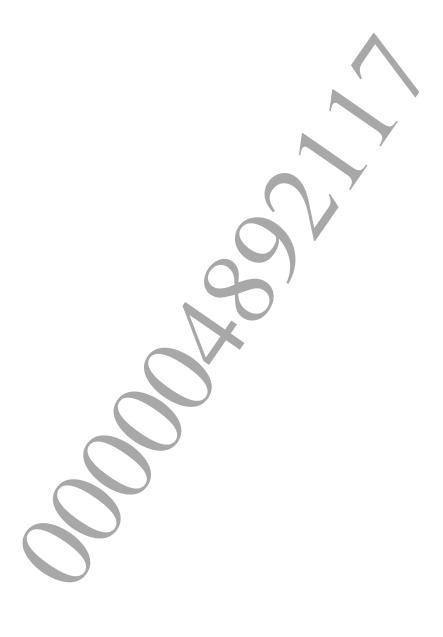


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

### **Table of Contents**

1 Library Overview		3
		-
Rasic Usage Proce		1



# **Library Overview**

### Overview

libsha224 is a library that is used to generate a digest value using the SHA-224 Secure Hash Algorithm 224 format as defined by RFC3874. 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 libsha224.

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



## f 2 Using the Library

### **Basic Usage Procedure**

### (1) SHA-224 digest value computation (comprehensive)

No specific initialization is required to use libsha224.

```
SceUChar8 digest[SCE SHA224 DIGEST SIZE];
sceSha224Digest(plaintext, length, digest);
```

You can compute the digest value simply by calling the sceSha224Digest () function, as shown above.

#### (2) SHA-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.

```
SceSha224Context sha;
SceUChar8 digest[SCE SHA224 DIGEST SIZE];
sceSha224BlockInit(&sha);
sceSha224BlockUpdate(&sha, plain1, len1);
sceSha224BlockUpdate(&sha, plain2, len2);
sceSha224BlockUpdate(&sha, plain3, len3);
                     Repeat an arbitrary number of times
sceSha224BlockResult(&sha, digest);
```

First, call the sceSha224BlockInit() function to initialize the SceSha224Context structure. Then, call the sceSha224BlockUpdate() function the desired number of times. Lastly, the digest value can be obtained by calling the sceSha224BlockResult () function.

