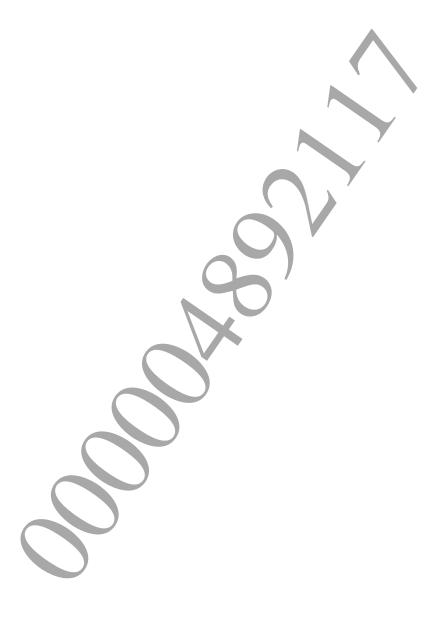


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

1 Library Overview		3
-		
	3	
	4	
Basic Usage Procedure	4	1
Digest Value Size		1



1 Library Overview

Overview

libhmac is a library that is used to generate a digest value using the HMAC format as defined by FIPS 198.

Files

The following files are required to use libhmac.

The following thes are requir	led to use infilliac.	
Filename	Description	
libhmac.h	Header file	
libSceHmac.a	Static link library file	
libSceHmac_stub.a	Stub library file	
libSceHmac_stub_weak.a	weak import stub library file	
libhmac.suprx	PRX module file	

2 Using the Library

Basic Usage Procedure

(1) HMAC-SHA1 digest value computation (comprehensive)

No specific initialization is required to use libhmac.

```
SceUChar8 digest[SCE_HMAC_SHA1_DIGEST_SIZE];
sceHmacShalDigest(key, keylen, plaintext, length, digest);
```

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

(2) HMAC-SHA1 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 sceHmacShalBlockInit() function to initialize the SceHmacShalContext structure. Then, call the sceHmacShalBlockUpdate() function the desired number of times. Lastly, the digest value can be obtained by calling the sceHmacShalBlockResult() function.

Digest Value Size

In libhmac, the size of the digest value is determined using each hash algorithm, but the size will be variable if SHA-512/224 or SHA-512/256 is used as the digest algorithm. Set either 224 or 256 in the argument t of the sceHmacSha512tDigest() and sceHmacSha512tBlockInit() functions.