libhmac Reference

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Document serial number: 000004892117

Table of Contents

Datatypes

SceHmacMd5Context

Context information for HMAC-MD5 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacMd5Context {
        SceMd5Context md5;
        SceUChar8 keybuf[SCE_MD5_BLOCK_SIZE];
} SceHmacMd5Context;
```

Members

md5	MD5 work area
keybuf	Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-MD5 digest value computation. Since the `sceHmacMd5BlockInit()` function, `sceHmacMd5BlockUpdate()` function, and `sceHmacMd5BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacMd5BlockInit()`, `sceHmacMd5BlockUpdate()`, `sceHmacMd5BlockResult()`

SceHmacSha0Context

Context information for HMAC-SHA0 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha0Context {
        SceSha0Context sha0;
        SceUChar8 keybuf[SCE_SHA0_BLOCK_SIZE];
} SceHmacSha0Context;
```

Members

sha0 SHA0 work area
keybuf Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA0 digest value computation. Since the `sceHmacSha0BlockInit()` function, `sceHmacSha0BlockUpdate()` function, and `sceHmacSha0BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha0BlockInit()`, `sceHmacSha0BlockUpdate()`, `sceHmacSha0BlockResult()`

SceHmacSha1Context

Context information for HMAC-SHA1 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha1Context {
        SceSha1Context sha1;
        SceUChar8 keybuf[SCE_SHA1_BLOCK_SIZE];
} SceHmacSha1Context;
```

Members

sha1	SHA1 work area
keybuf	Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA1 digest value computation. Since the `sceHmacSha1BlockInit()` function, `sceHmacSha1BlockUpdate()` function, and `sceHmacSha1BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha1BlockInit()`, `sceHmacSha1BlockUpdate()`, `sceHmacSha1BlockResult()`

SceHmacSha224Context

Context information for HMAC-SHA224 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha224Context {
        SceSha224Context sha224;
        SceUChar8 keybuf[SCE_SHA224_BLOCK_SIZE];
} SceHmacSha224Context;
```

Members

sha224 SHA224 work area
keybuf Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA224 digest value computation. Since the `sceHmacSha224BlockInit()` function, `sceHmacSha224BlockUpdate()` function, and `sceHmacSha224BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha224BlockInit()`, `sceHmacSha224BlockUpdate()`, `sceHmacSha224BlockResult()`

SceHmacSha256Context

Context information for HMAC-SHA256 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha256Context {
        SceSha256Context sha256;
        SceUChar8 keybuf[SCE_SHA256_BLOCK_SIZE];
} SceHmacSha256Context;
```

Members

sha256 SHA256 work area
keybuf Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA256 digest value computation. Since the `sceHmacSha256BlockInit()` function, `sceHmacSha256BlockUpdate()` function, and `sceHmacSha256BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha256BlockInit()`, `sceHmacSha256BlockUpdate()`, `sceHmacSha256BlockResult()`

SceHmacSha384Context

Context information for HMAC-SHA384 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha384Context {
        SceSha384Context sha384;
        SceUChar8 keybuf[SCE_SHA384_BLOCK_SIZE];
} SceHmacSha384Context;
```

Members

sha384 SHA384 work area
keybuf Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA384 digest value computation. Since the `sceHmacSha384BlockInit()` function, `sceHmacSha384BlockUpdate()` function, and `sceHmacSha384BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha384BlockInit()`, `sceHmacSha384BlockUpdate()`, `sceHmacSha384BlockResult()`

SceHmacSha512Context

Context information for HMAC-SHA512 computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha512Context {
        SceSha512Context sha512;
        SceUChar8 keybuf[SCE_SHA512_BLOCK_SIZE];
} SceHmacSha512Context;
```

Members

sha512 SHA512 work area
keybuf Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA512 digest value computation. Since the `sceHmacSha512BlockInit()` function, `sceHmacSha512BlockUpdate()` function, and `sceHmacSha512BlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha512BlockInit()`, `sceHmacSha512BlockUpdate()`, `sceHmacSha512BlockResult()`

SceHmacSha512tContext

Context information for HMAC-SHA512/t computation

Definition

```
#include <libhmac.h>
typedef struct SceHmacSha512tContext {
        SceSha512tContext sha512t;
        SceUInt32 t;
        SceUInt32 padding;
        SceUChar8 keybuf[SCE_SHA512T_BLOCK_SIZE];
} SceHmacSha512tContext;
```

Members

sha512t	SHA-512/t work area
t	SHA-512/t digest size
padding	Work area for adjusting alignment
keybuf	Temporary copy of the key information

Description

This structure is used as a work area for dividing up the HMAC-SHA512/t digest value computation. Since the `sceHmacSha512tBlockInit()` function, `sceHmacSha512tBlockUpdate()` function, and `sceHmacSha512tBlockResult()` function use this structure as a work area, the application must not directly access the members of this structure.

See Also

`sceHmacSha512tBlockInit()`, `sceHmacSha512tBlockUpdate()`, `sceHmacSha512tBlockResult()`

HMAC Functions (Comprehensive)

sceHmacMd5Digest

Compute HMAC-MD5

Definition

```
#include <libhmac.h>
int sceHmacMd5Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-MD5
keylen	Number of bytes of key for HMAC-MD5
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (16 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-MD5.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha0Digest

Compute HMAC-SHA0

Definition

```
#include <libhmac.h>
int sceHmacSha0Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA0
keylen	Number of bytes of key for HMAC-SHA0
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (20 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA0.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha1Digest

Compute HMAC-SHA1

Definition

```
#include <libhmac.h>
int sceHmacSha1Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA1
keylen	Number of bytes of key for HMAC-SHA1
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (20 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA1.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha224Digest

Compute HMAC-SHA224

Definition

```
#include <libhmac.h>
int sceHmacSha224Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA224
keylen	Number of bytes of key for HMAC-SHA224
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (28 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA224.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha256Digest

Compute HMAC-SHA256

Definition

```
#include <libhmac.h>
int sceHmacSha256Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA256
keylen	Number of bytes of key for HMAC-SHA256
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (32 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA256.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha384Digest

Compute HMAC-SHA384

Definition

```
#include <libhmac.h>
int sceHmacSha384Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA384
keylen	Number of bytes of key for HMAC-SHA384
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (48 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA384.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha512Digest

Compute HMAC-SHA512

Definition

```
#include <libhmac.h>
int sceHmacSha512Digest(
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

secretkey	Pointer to key for HMAC-SHA512
keylen	Number of bytes of key for HMAC-SHA512
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (64 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion

Description

This function computes the HMAC-SHA512.

Use this function when all the text data for which the digest value is to be computed is available in memory.

sceHmacSha512tDigest

Compute HMAC-SHA512/t

Definition

```
#include <libhmac.h>
int sceHmacSha512tDigest(
        SceUInt32 t,
        const void *secretkey,
        SceUInt32 keylen,
        const void *plain,
        SceUInt32 datalen,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

t	Digest value size (bits). Specify 224 or 256.
secretkey	Pointer to key for HMAC-SHA512/t
keylen	Number of bytes of key for HMAC-SHA512/t
plain	Pointer to text data for which digest value is to be computed
datalen	Size of text data (in bytes) for which digest value is to be computed
digest	Computed digest value (28 or 32 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_DIGEST_SIZE	Size of *t* is invalid

Description

This function computes the HMAC-SHA512/t.

Use this function when all the text data for which the digest value is to be computed is available in memory.

The size of the digest value that returns to *digest* varies depending on the size specified in the argument *t*.

HMAC Functions (Divided)

sceHmacMd5BlockInit

Initialize HMAC-MD5 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacMd5BlockInit(
        SceHmacMd5Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-MD5
keylen	Number of bytes of key for HMAC-MD5

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-MD5 digest value.
Call this function before calling the `sceHmacMd5BlockUpdate()` function.

See Also

`SceHmacMd5Context`, `sceHmacMd5BlockUpdate()`, `sceHmacMd5BlockResult()`

sceHmacMd5BlockUpdate

HMAC-MD5 computation processing

Definition

```
#include <libhmac.h>
int sceHmacMd5BlockUpdate(
        SceHmacMd5Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacMd5Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacMd5BlockInit() and sceHmacMd5BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacMd5Context, sceHmacMd5BlockInit(), sceHmacMd5BlockResult()

sceHmacMd5BlockResult

Get computed HMAC-MD5 digest

Definition

```
#include <libhmac.h>
int sceHmacMd5BlockResult(
        SceHmacMd5Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (16 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacMd5Context structure.

See Also

SceHmacMd5Context, sceHmacMd5BlockInit(), sceHmacMd5BlockUpdate()

sceHmacSha0BlockInit

Initialize HMAC-SHA0 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha0BlockInit(
        SceHmacSha0Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA0
keylen	Number of bytes of key for HMAC-SHA0

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA0 digest value.
Call this function before calling the `sceHmacSha0BlockUpdate()` function.

See Also

`SceHmacSha0Context`, `sceHmacSha0BlockUpdate()`, `sceHmacSha0BlockResult()`

sceHmacSha0BlockUpdate

HMAC-SHA0 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha0BlockUpdate(
        SceHmacSha0Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha0Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha0BlockInit() and sceHmacSha0BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha0Context, sceHmacSha0BlockInit(), sceHmacSha0BlockResult()

sceHmacSha0BlockResult

Get computed HMAC-SHA0 digest

Definition

```
#include <libhmac.h>
int sceHmacSha0BlockResult(
        SceHmacSha0Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (20 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha0Context structure.

See Also

SceHmacSha0Context, sceHmacSha0BlockInit(), sceHmacSha0BlockUpdate()

sceHmacSha1BlockInit

Initialize HMAC-SHA1 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha1BlockInit(
        SceHmacSha1Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA1
keylen	Number of bytes of key for HMAC-SHA1

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA1 digest value. Call this function before calling the `sceHmacSha1BlockUpdate()` function.

See Also

`SceHmacSha1Context`, `sceHmacSha1BlockUpdate()`, `sceHmacSha1BlockResult()`

sceHmacSha1BlockUpdate

HMAC-SHA1 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha1BlockUpdate(
        SceHmacSha1Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha1Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha1BlockInit() and sceHmacSha1BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha1Context, sceHmacSha1BlockInit(), sceHmacSha1BlockResult()

sceHmacSha1BlockResult

Get computed HMAC-SHA1 digest

Definition

```
#include <libhmac.h>
int sceHmacSha1BlockResult(
        SceHmacSha1Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (20 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha1Context structure.

See Also

SceHmacSha1Context, sceHmacSha1BlockInit(), sceHmacSha1BlockUpdate()

sceHmacSha224BlockInit

Initialize HMAC-SHA224 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha224BlockInit(
        SceHmacSha224Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA224
keylen	Number of bytes of key for HMAC-SHA224

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA224 digest value.
Call this function before calling the `sceHmacSha224BlockUpdate()` function.

See Also

`SceHmacSha224Context`, `sceHmacSha224BlockUpdate()`, `sceHmacSha224BlockResult()`

sceHmacSha224BlockUpdate

HMAC-SHA224 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha224BlockUpdate(
        SceHmacSha224Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha224Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha224BlockInit() and sceHmacSha224BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha224Context, sceHmacSha224BlockInit(), sceHmacSha224BlockResult()

sceHmacSha224BlockResult

Get computed HMAC-SHA224 digest

Definition

```
#include <libhmac.h>
int sceHmacSha224BlockResult(
        SceHmacSha224Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (28 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha224Context structure.

See Also

SceHmacSha224Context, sceHmacSha224BlockInit(), sceHmacSha224BlockUpdate()

sceHmacSha256BlockInit

Initialize HMAC-SHA256 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha256BlockInit(
        SceHmacSha256Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA256
keylen	Number of bytes of key for HMAC-SHA256

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA256 digest value.
Call this function before calling the `sceHmacSha256BlockUpdate()` function.

See Also

`SceHmacSha256Context`, `sceHmacSha256BlockUpdate()`, `sceHmacSha256BlockResult()`

sceHmacSha256BlockUpdate

HMAC-SHA256 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha256BlockUpdate(
        SceHmacSha256Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha256Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha256BlockInit() and sceHmacSha256BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha256Context, sceHmacSha256BlockInit(), sceHmacSha256BlockResult()

sceHmacSha256BlockResult

Get computed HMAC-SHA256 digest

Definition

```
#include <libhmac.h>
int sceHmacSha256BlockResult(
        SceHmacSha256Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (32 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha256Context structure.

See Also

SceHmacSha256Context, sceHmacSha256BlockInit(), sceHmacSha256BlockUpdate()

sceHmacSha384BlockInit

Initialize HMAC-SHA384 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha384BlockInit(
        SceHmacSha384Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA384
keylen	Number of bytes of key for HMAC-SHA384

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA384 digest value.
Call this function before calling the `sceHmacSha384BlockUpdate()` function.

See Also

`SceHmacSha384Context`, `sceHmacSha384BlockUpdate()`, `sceHmacSha384BlockResult()`

sceHmacSha384BlockUpdate

HMAC-SHA384 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha384BlockUpdate(
        SceHmacSha384Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha384Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha384BlockInit() and sceHmacSha384BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha384Context, sceHmacSha384BlockInit(), sceHmacSha384BlockResult()

sceHmacSha384BlockResult

Get computed HMAC-SHA384 digest

Definition

```
#include <libhmac.h>
int sceHmacSha384BlockResult(
        SceHmacSha384Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (48 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha384Context structure.

See Also

SceHmacSha384Context, sceHmacSha384BlockInit(), sceHmacSha384BlockUpdate()

sceHmacSha512BlockInit

Initialize HMAC-SHA512 digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha512BlockInit(
        SceHmacSha512Context *pContext,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
secretkey	Pointer to key for HMAC-SHA512
keylen	Number of bytes of key for HMAC-SHA512

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the HMAC-SHA512 digest value.
Call this function before calling the `sceHmacSha512BlockUpdate()` function.

See Also

`SceHmacSha512Context`, `sceHmacSha512BlockUpdate()`, `sceHmacSha512BlockResult()`

sceHmacSha512BlockUpdate

HMAC-SHA512 computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha512BlockUpdate(
        SceHmacSha512Context *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha512Context structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha512BlockInit() and sceHmacSha512BlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha512Context, sceHmacSha512BlockInit(), sceHmacSha512BlockResult()

sceHmacSha512BlockResult

Get computed HMAC-SHA512 digest

Definition

```
#include <libhmac.h>
int sceHmacSha512BlockResult(
        SceHmacSha512Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value (64 bytes) is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha512Context structure.

See Also

SceHmacSha512Context, sceHmacSha512BlockInit(), sceHmacSha512BlockUpdate()

sceHmacSha512tBlockInit

Initialize HMAC-SHA512/t digest value computation work area

Definition

```
#include <libhmac.h>
int sceHmacSha512tBlockInit(
        SceHmacSha512tContext *pContext,
        SceUInt32 t,
        const void *secretkey,
        SceUInt32 keylen
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
t	Digest value size (bits). Specify 224 or 256
secretkey	Pointer to key for HMAC-SHA512/t
keylen	Number of bytes of key for HMAC-SHA512/t

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* address
SCE_HMAC_ERROR_INVALID_DIGEST_SIZE	Size of *t* is invalid

Description

This function initializes the work area that is used to compute the HMAC-SHA512/t digest value.

Call this function before calling the `sceHmacSha512tBlockUpdate()` function.

See Also

`SceHmacSha512tContext`, `sceHmacSha512tBlockUpdate()`, `sceHmacSha512tBlockResult()`

sceHmacSha512tBlockUpdate

HMAC-SHA512/t computation processing

Definition

```
#include <libhmac.h>
int sceHmacSha512tBlockUpdate(
        SceHmacSha512tContext *pContext,
        const void *plain,
        SceUInt32 len
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
plain	Pointer to text data for which digest value is to be computed
len	Size of text data (in bytes) for which digest value is to be computed

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function updates the work area in the SceHmacSha512tContext structure using the text data specified by *plain* and *len*. It can be called any number of times between the sceHmacSha512tBlockInit() and sceHmacSha512tBlockResult() functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

See Also

SceHmacSha512tContext, sceHmacSha512tBlockInit(), sceHmacSha512tBlockResult()

sceHmacSha512tBlockResult

Get computed HMAC-SHA512/t digest

Definition

```
#include <libhmac.h>
int sceHmacSha512tBlockResult(
        SceHmacSha512tContext *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe.

Arguments

pContext	Address of digest value computation work area
digest	Computed digest value is returned

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_HMAC_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function extracts the computed digest value from the SceHmacSha512tContext structure.

The size of the digest value that returns to *digest* varies depending on the size specified in the argument *t* of the sceHmacSha512tBlockInit() function.

See Also

SceHmacSha512tContext, sceHmacSha512tBlockInit(), sceHmacSha512tBlockUpdate()