

libsha384 Reference

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

Table of Contents

Datatypes..... 3

 SceSha384Context 4

Digest Function (Comprehensive)..... 5

 sceSha384Digest 6

Digest Functions (Divided)..... 7

 sceSha384BlockInit..... 8

 sceSha384BlockUpdate..... 9

 sceSha384BlockResult 10

000004892117

Datatypes

000004892117

SceSha384Context

Context information for SHA-384 digest value computation

Definition

```
#include <libsha384.h>
typedef struct SceSha384Context {
    SceUInt64 h[8];
    SceUInt32 pad;
    SceUInt16 usRemains;
    SceUInt16 usComputed;
    SceUInt64 ullTotalLen;
    SceUChar8 buf[SCE_SHA384_BLOCK_SIZE];
    SceUChar8 result[SCE_SHA384_DIGEST_SIZE];
} SceSha384Context;
```

Members

<i>h</i>	Work area
<i>pad</i>	Padding for adjusting alignment
<i>usRemains</i>	Less than 128 bytes of remaining data, which was temporarily copied within the <i>SceSha384Context</i> structure
<i>usComputed</i>	Digest value computed flag
<i>ullTotalLen</i>	Total data size (bytes)
<i>buf</i>	Temporary copy of less than 128 bytes of data
<i>result</i>	Temporary copy of the digest value computation result

Description

This structure is used as a work area when computation of the SHA-384 digest value is divided up. Since the *sceSha384BlockInit()*, *sceSha384BlockUpdate()*, and *sceSha384BlockResult()* functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

```
sceSha384BlockInit(), sceSha384BlockUpdate(), sceSha384BlockResult()
```

Digest Function (Comprehensive)

SCE CONFIDENTIAL

sceSha384Digest

Compute SHA-384 digest

Definition

```
#include <libsha384.h>
SceInt32 sceSha384Digest(
    const void *plain,
    SceUInt32 len,
    SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

<i>plain</i>	Pointer to plaintext data for which digest value is to be computed.
<i>len</i>	Data size (bytes) of plaintext data for which digest value is to be computed.
<i>digest</i>	Returns computed digest value (48 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination

Description

This function computes the SHA-384 digest value.

This function is used when all data of the plaintext for which the digest value is to be computed has been expanded in memory.

Digest Functions (Divided)

sceSha384BlockInit

Initialize digest value computation work area

Definition

```
#include <libsha384.h>
SceInt32 sceSha384BlockInit(
    SceSha384Context *pContext
);
```

Calling Conditions

Multithread safe

Arguments

pContext Address of digest value computation work area.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA384_ERROR_INVALID_POINTER	Invalid <i>pContext</i> address

Description

This function initializes the work area that is used to compute the SHA-384 digest value. It should be called before `sceSha384BlockUpdate()` function.

See Also

`SceSha384Context`, `sceSha384BlockUpdate()`, `sceSha384BlockResult()`

SCE CONFIDENTIAL

sceSha384BlockUpdate

SHA-384 digest value computation processing

Definition

```
#include <libsha384.h>
SceInt32 sceSha384BlockUpdate (
    SceSha384Context *pContext,
    const void *plain,
    SceUInt32 len
);
```

Calling Conditions

Multithread safe

Arguments

pContext Address of digest value computation work area.
plain Pointer to plaintext data for which digest value is to be computed.
len Data size (bytes) of plaintext data for which digest value is to be computed.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA384_ERROR_INVALID_POINTER	Invalid <i>pContext</i> or <i>plain</i> address

Description

This function uses the plaintext specified by *plain* and *len* to update the work area within the *SceSha384Context* structure. By dividing the computation into multiple steps, the *sceSha384BlockUpdate()* function, which can be called any number of times between the *sceSha384BlockInit()* and *sceSha384BlockResult()* functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

See Also

SceSha384Context, *sceSha384BlockInit()*, *sceSha384BlockResult()*

SCE CONFIDENTIAL

sceSha384BlockResult

Get computed SHA-384 digest

Definition

```
#include <libsha384.h>
SceInt32 sceSha384BlockResult(
    SceSha384Context *pContext,
    SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

pContext Address of digest value computation work area.
digest Returns the computed digest value (48 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA384_ERROR_INVALID_POINTER	Invalid <i>pContext</i> or <i>digest</i> address

Description

This function retrieves the computed digest value from the `SceSha384Context` structure. The SHA-384 algorithm computes a digest value in increments of 128 bytes, so a remaining amount less than 128 bytes may have been temporarily copied within the `SceSha384Context` structure by the `sceSha384BlockUpdate()` function. If this remaining data exists, the final digest value can be obtained by calling `sceSha384BlockResult()` function. Always use the `sceSha384BlockResult()` function to obtain the digest value.

The digest value of the `SceSha384Context` structure is valid until the next time `sceSha384BlockInit()` function or `sceSha384BlockUpdate()` function is called.

See Also

`SceSha384Context`, `sceSha384BlockInit()`, `sceSha384BlockUpdate()`