Document serial number: 000004892117

libsha1 Reference

000004892117

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

© 2012 Sony Computer Entertainment Inc.
All Rights Reserved.
SCE Confidential

Document serial number: 000004892117

Document serial number: 000004892117

Table of Contents

000004892117

Document serial number: 000004892117

Datatypes

000004892117

Document serial number: 000004892117

©SCEI

SceSha1Context

Context information for SHA-1 digest value computation

Definition

```
#include <libsha1.h>
typedef struct SceSha1Context {
        SceUInt32 h[5];
        SceUInt16 usRemains;
        SceUInt16 usComputed;
        SceUInt64 ullTotalLen;
        SceUChar8 buf[SCE_SHA1_BLOCK_SIZE];
        SceUChar8 result[SCE_SHA1_DIGEST_SIZE];
        SceUInt32 pad;
} SceSha1Context;
```

Members

h	Work area
usRemains	Less than 64 bytes of remaining data, which was temporarily copied within the SceSha1Context structure
usComputed	Digest value computed flag
ullTotalLen	Total data size (bytes)
buf	Temporary copy of less than 64 bytes of data
result	Temporary copy of the digest value computation result
pad	Padding for adjusting alignment

Description

This structure is used as a work area when computation of the SHA-1 digest value is divided up. Since the sceSha1BlockInit(), sceSha1BlockUpdate(), and sceSha1BlockResult() functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

sceSha1BlockInit(), sceSha1BlockUpdate(), sceSha1BlockResult()

000004892117

Document serial number: 000004892117

Digest Function (Comprehensive)

000004892117

Document serial number: 000004892117

©SCEI

sceSha1Digest

Compute SHA-1 digest

Definition

```
#include <libsha1.h>
SceInt32 sceSha1Digest(
        const void *plain,
        SceUInt32 len,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

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.
digest	Returns computed digest value (20 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination

Description

This function computes the SHA-1 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.

000004892117

Document serial number: 000004892117

Digest Functions (Divided)

000004892117

Document serial number: 000004892117

sceSha1BlockInit

Initialize digest value computation work area

Definition

```
#include <libsha1.h>
SceInt32 sceSha1BlockInit(
        SceSha1Context *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_SHA1_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the SHA-1 digest value.
It should be called before `sceSha1BlockUpdate()` function.

See Also

`SceSha1Context`, `sceSha1BlockUpdate()`, `sceSha1BlockResult()`

000004892117

Document serial number: 000004892117

sceSha1BlockUpdate

SHA-1 digest value computation processing

Definition

```
#include <libsha1.h>
SceInt32 sceSha1BlockUpdate(
        SceSha1Context *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_SHA1_ERROR_INVALID_POINTER	Invalid *pContext* or *plain* address

Description

This function uses the plaintext specified by *plain* and *len* to update the work area within the SceSha1Context structure. By dividing the computation into multiple steps, the sceSha1BlockUpdate() function, which can be called any number of times between the sceSha1BlockInit() and sceSha1BlockResult() functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

See Also

SceSha1Context, sceSha1BlockInit(), sceSha1BlockResult()

000004892117

Document serial number: 000004892117

sceSha1BlockResult

Get computed SHA-1 digest

Definition

```
#include <libsha1.h>
SceInt32 sceSha1BlockResult(
        SceSha1Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

pContext	Address of digest value computation work area.
digest	Returns the computed digest value (20 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA1_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function retrieves the computed digest value from the SceSha1Context structure. The SHA-1 algorithm computes a digest value in increments of 64 bytes, so a remaining amount less than 64 bytes may have been temporarily copied within the SceSha1Context structure by the sceSha1BlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling sceSha1BlockResult() function. Always use the sceSha1BlockResult() function to obtain the digest value.

The digest value of the SceSha1Context structure is valid until the next time sceSha1BlockInit() function or sceSha1BlockUpdate() function is called.

See Also

SceSha1Context, sceSha1BlockInit(), sceSha1BlockUpdate()

000004892117

Document serial number: 000004892117

©SCEI