libsha512 Reference

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Table of Contents

Datatypes

SceSha512Context

Context information for SHA-512 digest value computation

Definition

```
#include <libsha512.h>
typedef struct SceSha512Context {
        SceUInt64 h[8];
        SceUInt32 pad;
        SceUInt16 usRemains;
        SceUInt16 usComputed;
        SceUInt64 ullTotalLen;
        SceUChar8 buf[SCE_SHA512_BLOCK_SIZE];
        SceUChar8 result[SCE_SHA512_DIGEST_SIZE];
} SceSha512Context;
```

Members

h	Work area
pad	Padding for adjusting alignment
usRemains	Less than 128 bytes of remaining data, which was temporarily copied within the `SceSha512Context` structure
usComputed	Digest value computed flag
ullTotalLen	Total data size (bytes)
buf	Temporary copy of less than 128 bytes of data
result	Temporary copy of the digest value computation result

Description

This structure is used as a work area when computation of the SHA-512 digest value is divided up. Since the `sceSha512BlockInit()`, `sceSha512BlockUpdate()`, and `sceSha512BlockResult()` functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

`sceSha512BlockInit()`, `sceSha512BlockUpdate()`, `sceSha512BlockResult()`

Digest Function (Comprehensive)

sceSha512Digest

Compute SHA-512 digest

Definition

```
#include <libsha512.h>
SceInt32 sceSha512Digest(
        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 (64 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination

Description

This function computes the SHA-512 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)

sceSha512BlockInit

Initialize digest value computation work area

Definition

```
#include <libsha512.h>
SceInt32 sceSha512BlockInit(
        SceSha512Context *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_SHA512_ERROR_INVALID_POINTER	Invalid *pContext* address

Description

This function initializes the work area that is used to compute the SHA-512 digest value.

It should be called before sceSha512BlockUpdate() function.

See Also

SceSha512Context, sceSha512BlockUpdate(), sceSha512BlockResult()

sceSha512BlockUpdate

SHA-512 digest value computation processing

Definition

```
#include <libsha512.h>
SceInt32 sceSha512BlockUpdate(
        SceSha512Context *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_SHA512_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 SceSha512Context structure. By dividing the computation into multiple steps, the sceSha512BlockUpdate() function, which can be called any number of times between the sceSha512BlockInit() and sceSha512BlockResult() functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

See Also

SceSha512Context, sceSha512BlockInit(), sceSha512BlockResult()

sceSha512BlockResult

Get computed SHA-512 digest

Definition

```
#include <libsha512.h>
SceInt32 sceSha512BlockResult(
        SceSha512Context *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

pContext	Address of digest value computation work area.
digest	Returns the computed digest value (64 bytes).

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA512_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function retrieves the computed digest value from the SceSha512Context structure. The SHA-512 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 SceSha512Context structure by the sceSha512BlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling the sceSha512BlockResult() function. Always use the sceSha512BlockResult() function to obtain the digest value.

The digest value of the SceSha512Context structure is valid until the next time sceSha512BlockInit() function or sceSha512BlockUpdate() function is called.

See Also

SceSha512Context, sceSha512BlockInit(), sceSha512BlockUpdate()