libsha512t Reference

PlayStation®Vita Programmer Tool Runtime Library Release 3.50

Document serial number: 000004892117

Document serial number: 000004892117

Table of Contents

Datatypes

SceSha512tContext

Context information for SHA-512/t digest value computation

Definition

```
#include <libsha512t.h>
typedef struct SceSha512tContext {
        SceUInt64 h[8];
        SceUInt32 t;
        SceUInt16 usRemains;
        SceUInt16 usComputed;
        SceUInt64 ullTotalLen;
        SceUChar8 buf[SCE_SHA512T_BLOCK_SIZE];
        SceUChar8 result[SCE_SHA512T_MAX_DIGEST_SIZE];
} SceSha512tContext;
```

Members

h	Work area
t	Digest value size
usRemains	Less than 128 bytes of remaining data, which was temporarily copied within the `SceSha512tContext` 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-512t digest value is divided up. Since the `sceSha512tBlockInit()`, `sceSha512tBlockUpdate()`, and `sceSha512tBlockResult()` functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

`sceSha512tBlockInit()`, `sceSha512tBlockUpdate()`, `sceSha512tBlockResult()`

Digest Function (Comprehensive)

sceSha512tDigest

Compute SHA-512/t digest

Definition

```
#include <libsha512t.h>
SceInt32 sceSha512tDigest(
        SceUInt32 t,
        const void *plain,
        SceUInt32 len,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

t	Digest value size (bits). Specify 224 or 256.
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.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA512T_ERROR_INVALID_DIGEST_SIZE	Size of *t* is invalid

Description

This function computes the SHA-512/t 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.

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

Digest Functions (Divided)

sceSha512tBlockInit

Initialize digest value computation work area

Definition

```
#include <libsha512t.h>
SceInt32 sceSha512tBlockInit(
        SceSha512tContext *pContext,
        SceUInt32 t
);
```

Calling Conditions

Multithread safe

Arguments

pContext	Address of digest value computation work area.
t	Digest value size (bits). Specify 224 or 256.

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA512T_ERROR_INVALID_POINTER	Invalid *pContext* address
SCE_SHA512T_ERROR_INVALID_DIGEST_SIZE	Size of *t* is invalid

Description

This function initializes the work area that is used to compute the SHA-512/t digest value.
It should be called before `sceSha512tBlockUpdate()` function.

See Also

`SceSha512tContext`, `sceSha512tBlockUpdate()`, `sceSha512tBlockResult()`

sceSha512tBlockUpdate

SHA-512/t digest value computation processing

Definition

```
#include <libsha512t.h>
SceInt32 sceSha512tBlockUpdate(
        SceSha512tContext *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_SHA512T_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 SceSha512tContext structure. By dividing the computation into multiple steps, the sceSha512tBlockUpdate() function, which can be called any number of times between the sceSha512tBlockInit() and sceSha512tBlockResult() functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

See Also

SceSha512tContext, sceSha512tBlockInit(), sceSha512tBlockResult()

sceSha512tBlockResult

Get computed SHA-512/t digest

Definition

```
#include <libsha512t.h>
SceInt32 sceSha512tBlockResult(
        SceSha512tContext *pContext,
        SceUChar8 *digest
);
```

Calling Conditions

Multithread safe

Arguments

pContext	Address of digest value computation work area
digest	Returns the computed digest value

Return Values

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal termination
SCE_SHA512T_ERROR_INVALID_POINTER	Invalid *pContext* or *digest* address

Description

This function retrieves the computed digest value from the SceSha512tContext structure. The SHA-512/t 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 SceSha512tContext structure by the sceSha512tBlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling the sceSha512tBlockResult() function. Always use the sceSha512tBlockResult() function to obtain the digest value.

The size of the digest value that returns to *digest* varies depending on the size specified in the argument *t* of the sceSha512tBlockInit() function.

The digest value of the SceSha512tContext structure is valid until the next time sceSha512tBlockInit() function or sceSha512tBlockUpdate() function is called.

See Also

SceSha512tContext, sceSha512tBlockInit(), sceSha512tBlockUpdate()