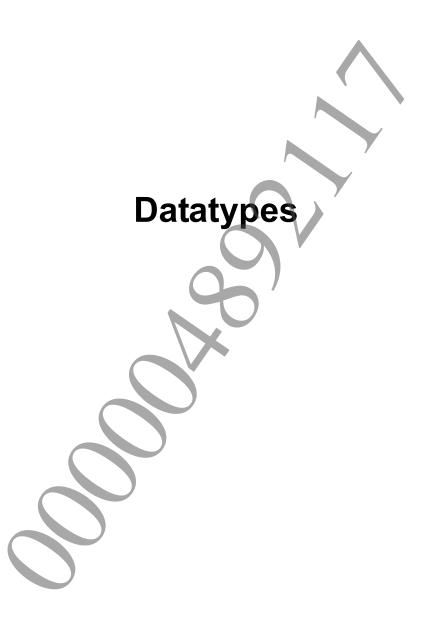


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

Datatypes	3
SceSha512Context	4
Digest Function (Comprehensive)	5
sceSha512Digest	6
Digest Functions (Divided)	8
sceSha512BlockResult	



SceSha512Context

Context information for SHA-512 digest value computation

Definition

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

usComputedDigest value computed flagullTotalLenTotal 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()



sceSha512Digest

Compute SHA-512 digest

Definition

Calling Conditions

Multithread safe

Arguments

Pointer to plaintext data for which digest value is to be computed.

Data size (bytes) of plaintext data for which digest value is to be computed.

Returns computed digest value (64 bytes).

Return Values

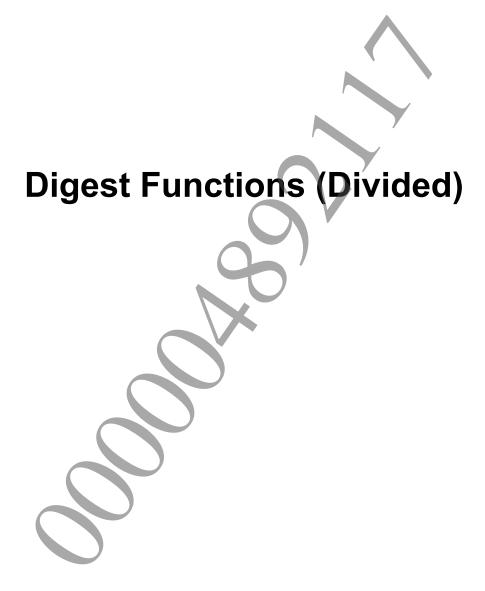
If an error occurs, a negative value is returned.

Value	
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.



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

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 <code>plain</code> and <code>len</code> to update the work area within the <code>SceSha512Context</code> structure. By dividing the computation into multiple steps, the <code>sceSha512BlockUpdate()</code> function, which can be called any number of times between the <code>sceSha512BlockInit()</code> and <code>sceSha512BlockResult()</code> 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()

©SCEI

sceSha512BlockResult

Get computed SHA-512 digest

Definition

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()