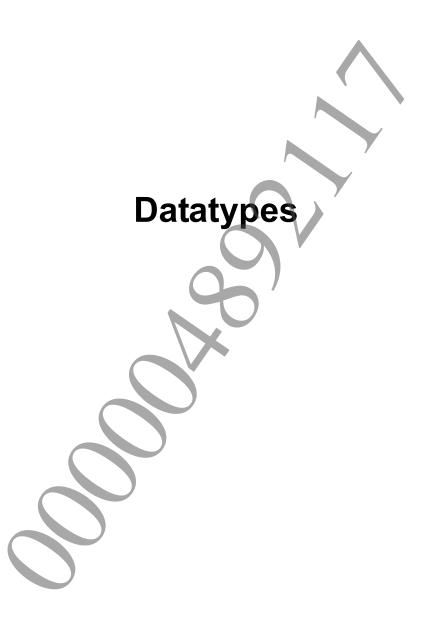


© 2012 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

Datatyp	Des	3
	SceSha1Context	4
Digest	Function (Comprehensive)	5
	sceSha1DigestsceSha1Digest	6
Dinest	Functions (Divided)	
Digest	sceSha1BlockInit	
	sceSha1BlockUpdate	
	sceSha1BlockResult	



SceSha1Context

Context information for SHA-1 digest value computation

Definition

Members

Mork area
usRemains
Less than 64 bytes of remaining data, which was temporarily copied within the
SceShalContext 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 sceShalBlockInit(), sceShalBlockUpdate(), and sceShalBlockResult() functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

sceShalBlockInit(), sceShalBlockUpdate(), sceShalBlockResult()





sceSha1Digest

Compute SHA-1 digest

Definition

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

Calling Conditions

Multithread safe

Arguments

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

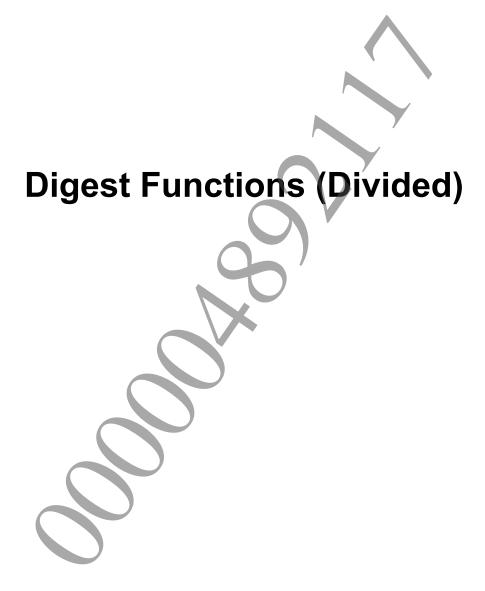
Value	
SCE OK	Normal termination

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





sceSha1BlockInit

Initialize digest value computation work area

Definition

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 sceShalBlockUpdate() function.

See Also

SceShalContext, sceShalBlockUpdate(), sceShalBlockResult()



sceSha1BlockUpdate

SHA-1 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_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 SceShalContext structure. By dividing the computation into multiple steps, the sceShalBlockUpdate() function, which can be called any number of times between the sceShalBlockInit() and sceShalBlockResult() 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()

sceSha1BlockResult

Get computed SHA-1 digest

Definition

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 SceShalContext 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 SceShalContext structure by the sceShalBlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling sceShalBlockResult() function. Always use the sceShalBlockResult() function to obtain the digest value.

The digest value of the SceShalContext structure is valid until the next time sceShalBlockInit() function or sceShalBlockUpdate() function is called.

See Also

SceShalContext, sceShalBlockInit(), sceShalBlockUpdate()