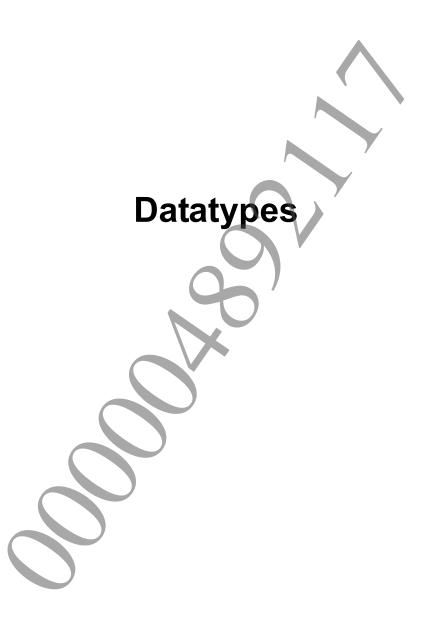


© 2012 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

Table of Contents

| Datatyp | esSceSha0Context | |
|----------|---------------------------------------|-------|
| Digest | Function (Comprehensive) | |
| J | sceSha0Digest | |
| Digest | sceSha0BlockUpdate sceSha0BlockResult | 9 |
| | | |



SceSha0Context

Context information for SHA-0 digest value computation

Definition

```
#include <libsha0.h>
typedef struct SceSha0Context {
        SceUInt32 h[5];
        SceUInt16 usRemains;
        SceUInt16 usComputed;
        SceUInt64 ullTotalLen;
        SceUChar8 buf[SCE SHA0 BLOCK SIZE];
        SceUChar8 result[SCE SHA0 DIGEST SIZE];
        SceUInt32 pad;
} SceSha0Context;
```

Members

h Work area usRemains Less than 64 bytes of remaining data, which was temporarily copied within the SceSha0Context 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-0 digest value is divided up. Since the sceShaOBlockInit(), sceShaOBlockUpdate(), and sceShaOBlockResult() functions use this structure as a work area, an application must not directly access the members of this structure.

See Also

sceShaOBlockInit(), sceShaOBlockUpdate(), sceShaOBlockResult()





sceSha0Digest

Compute SHA-0 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 (20 bytes).

Return Values

If an error occurs, a negative value is returned.

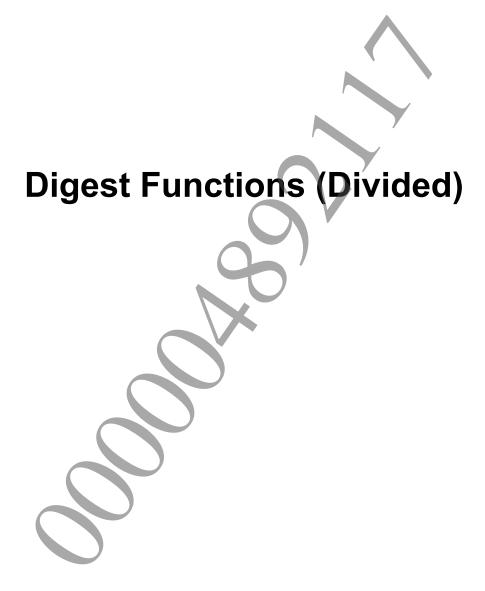
| Value | Result | |
|--------|--------------------|--|
| SCE OK | Normal termination | |

Description

This function computes the SHA-0 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.

©SCEI



sceSha0BlockInit

Initialize digest value computation work area

Definition

```
#include <libsha0.h>
SceInt32 sceShaOBlockInit(
        SceSha0Context *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_SHAO_ERROR_INVALID_POINTER | Invalid pContext address |

Description

This function initializes the work area that is used to compute the SHA-0 digest value. It should be called before sceShaOBlockUpdate() function.

See Also

SceShaOContext, sceShaOBlockUpdate(), sceShaOBlockResult()



sceSha0BlockUpdate

SHA-0 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_ | | | | | Normal termination |
| SCE_ | SHA0 | 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 SceSha0Context structure. By dividing the computation into multiple steps, the sceSha0BlockUpdate() function, which can be called any number of times between the sceSha0BlockInit() and sceSha0BlockResult() functions, enables the digest value to be computed even for a large amount of data that cannot fit in memory.

See Also

SceSha0Context, sceSha0BlockInit(), sceSha0BlockResult()

sceSha0BlockResult

Get computed SHA-0 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 |
|--------------------------------|------------------------------------|
| _ | Normal termination |
| SCE_SHAO_ERROR_INVALID_POINTER | Invalid pContext or digest address |

Description

This function retrieves the computed digest value from the SceSha0Context structure. The SHA-0 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 SceSha0Context structure by the sceSha0BlockUpdate() function. If this remaining data exists, the final digest value can be obtained by calling the sceSha0BlockResult() function. Always use the sceSha0BlockResult() function to obtain the digest value.

The digest value of the SceShaOContext structure is valid until the next time sceShaOBlockInit() function or sceShaOBlockUpdate() function is called.

See Also

SceSha0Context, sceSha0BlockInit(), sceSha0BlockUpdate()