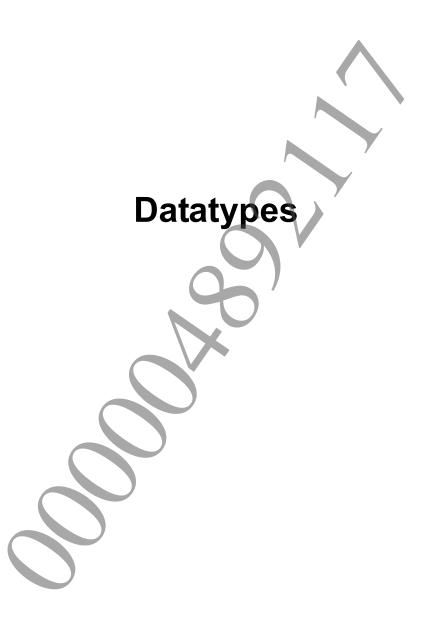


© 2011 Sony Computer Entertainment Inc. All Rights Reserved. SCE Confidential

# **Table of Contents**

	3
	5
sceMd5Digest	6
Digest Functions (Divided)	7
sceMd5BlockInit	8
sceMd5BlockUpdate	9
sceMd5BlockResult	10



## SceMd5Context

Context information for MD5 digest value computation

#### **Definition**

#### **Members**

h Work area pad Padding

usRemains Number of bytes of remaining data (less than 64), temporarily copied to the

SceMd5Context structure

usComputed Flag set at the end of the digest value computation

ullTotalLen Total data size

buf Temporary copy of less than 64 bytes of data

result Temporary copy of the digest value computation result

#### Description

This structure is used as a work area for dividing up the MD5 digest value computation. Since the sceMd5BlockInit() function, sceMd5BlockUpdate() function, and sceMd5BlockResult() function use this structure as a work area, the application must not directly access the members of this structure.

#### See Also

sceMd5BlockInit(),sceMd5BlockUpdate(),sceMd5BlockResult()





# sceMd5Digest

## Compute MD5 digest

#### **Definition**

```
#include <libmd5.h>
SceInt32 sceMd5Digest (
        const void *plain,
        SceUInt32 len,
        SceUChar8 *digest
);
```

## **Calling Conditions**

Multithread safe.

## **Arguments**

plain Pointer to text data for which digest value is to be computed. len Size of text data (in bytes) for which digest value is to be computed. digest Pointer to 16-byte area where computed digest value is returned. Be sure to provide a 16-byte area.

#### **Return Values**

If an error occurs, a negative value is returned.

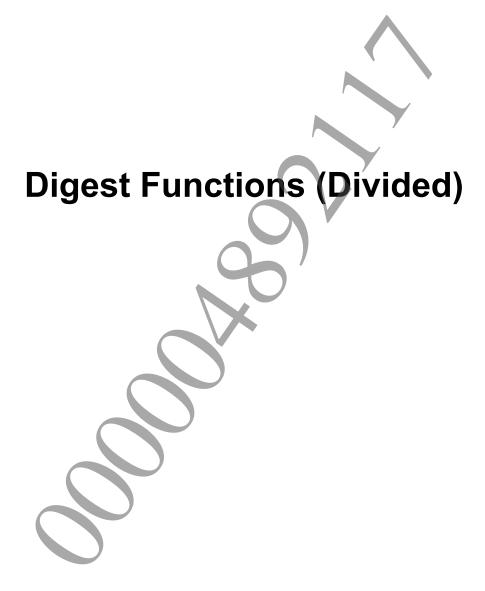
Value	
SCE OK	Normal completion

## **Description**

This function computes the MD5 digest value.

Use this function when all the text data for which the digest value is to be computed is available in memory.





## sceMd5BlockInit

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 completion
SCE_MD5_ERROR_INVALID_P	POINTER Invalid pContext address

## **Description**

This function initializes the work area that is used to compute the MD5 digest value. Call this function before calling the sceMd5BlockUpdate() function.

#### See Also

SceMd5Context, sceMd5BlockUpdate(), sceMd5BlockResult()



# sceMd5BlockUpdate

MD5 digest value computation processing

#### **Definition**

## **Calling Conditions**

Multithread safe.

## **Arguments**

pContext Address of digest value computation work area.

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

len Size of text data (in bytes) for which digest value is to be computed.

#### **Return Values**

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Normal completion
SCE_MD5_ERROR_INVALID_POINTER	Invalid pContext or plain address

## **Description**

This function updates the work area in the SceMd5Context structure using the text data specified by <code>plain</code> and <code>len</code>. It can be called any number of times between the <code>sceMd5BlockInit()</code> and <code>sceMd5BlockResult()</code> functions, enabling the digest value to be computed for a large amount of data that is too big to fit in memory, by breaking up the computation.

#### See Also

SceMd5Context, sceMd5BlockInit(), sceMd5BlockResult()

## sceMd5BlockResult

## Get computed MD5 digest

#### **Definition**

#### **Calling Conditions**

Multithread safe.

## **Arguments**

pContext Address of digest value computation work area.

Pointer to 16-byte area where computed digest value is returned.

Be sure to provide a 16-byte area.

#### **Return Values**

If an error occurs, a negative value is returned.

Value	Result
SCE_OK	Success
SCE_MD5_ERROR_INVALID_POINTER	Invalid pContext or digest address

#### **Description**

This function extracts the computed digest value from the SceMd5Context structure. Since the MD5 algorithm computes the digest value in units of 64 bytes, less than 64 bytes may still be remaining at the end of the computation. In this case, the extra bytes will have been temporarily copied to the SceMd5Context structure by the sceMd5BlockUpdate() function. When extra data is left over, the final digest value can be obtained by calling the sceMd5BlockResult() function. The sceMd5BlockResult() function should always be used to obtain the digest value.

The digest value maintained by the SceMd5Context structure is valid until the next time that the sceMd5BlockInit() function or sceMd5BlockUpdate() function is called.

#### See Also

SceMd5Context, sceMd5BlockInit(), sceMd5BlockUpdate()