

libssl Overview

© 2013 Sony Computer Entertainment Inc.
All Rights Reserved.
SCE Confidential

Table of Contents

1 Library Overview..... 3

 Purpose and Features.....3

 Main Functions3

 Used Resources.....3

 Embedding into a Program3

 Sample Programs.....3

2 Using the Library 4

 Basic Usage Procedure4

 Preparation.....4

000004892117

1 Library Overview

Purpose and Features

libssl is a module that is necessary for libhttp to perform HTTPS communication. Also, it provides a function for retrieving certificate information. Note that it is not possible to perform SSL communication with libssl alone.

Main Functions

The main functions offered by the libssl are as follows:

- HTTPS communication function through combination with libhttp
- Function for retrieving certificate information

Used Resources

The libssl uses the following system resources.

Resource	Description
Work memory	Differs widely based on communication destination and content. It is possible to obtain the maximum value with the <code>sceSslGetMemoryPoolStats()</code> function.

Embedding into a Program

Include `libssl.h` in the source program. Various header files will be automatically included as well.

Load also the PRX module in the program as follows.

```
if ( sceSysmoduleLoadModule(SCE_SYSMODULE_HTTPS) != SCE_OK ) {
    // Error processing
}
```

Upon building the program, link `libSceSsl_stub.a` or `libSceSsl_stub_weak.a`.

Sample Programs

The following program is provided as a libssl sample program for reference purposes.

sample_code/network/api_libhttp/http_get/https/

This is a sample of basic HTTPS communication with the libssl and libhttp.

sample_code/network/api_libhttp/root_ca_list/

This sample shows how to retrieve the root CA certificate list with the libssl and libhttp.

2 Using the Library

Basic Usage Procedure

This section explains the basic procedure of HTTPS communication. The following is an outline of the processing flow.

- (1) Load the SSL module in the module utility API
- (2) Initialize the library
- (3) Perform communication using libhttp
- (4) Terminate

Preparation

Load the SSL module with the module utility API.

(1) initializing library

Call `sceSslInit()` to initialize libssl after the libnet has been initialized but before initializing libhttp.

(2) Communication with libhttp

Perform HTTPS communication using libhttp. If necessary, during communication it is possible to verify certificates received from the server by using the function for retrieving certificate information.

(3) Terminating library

Call `sceSslTerm()` to terminate libssl after libhttp has been terminated but before libnet termination.

Main APIs used for basic processing

API	Description
<code>sceSslInit()</code>	Initializes the library
<code>sceSslTerm()</code>	Terminates the library