HelloDevice
Device Server

RC4/SSL Encryption
Sample Program Guide

Version 1.0.0

2005-08-23

Copyright Information

Sena Technologies reserves the right to make any changes and improvements to its product without providing prior notice.

Trademark Information

HelloDevice™ is a trademark of Sena Technologies, Inc.

Technical Support

Sena Technologies, Inc.

210 Yangjae-dong, Seocho-gu

Seoul 137-130, Korea

Tel: (+82-2) 573-5422

Fax: (+82-2) 573-7710

E-Mail: support@sena.com

Website: http://www.sena.com

Revision history

Revision	Date	Name	Description
V1.0.0	**2005-08-23**	**H. Yeom**	Initial Release

Content

1. Overview

The HelloDevice Pro Series (PS110/410/810), Super Series (SS100/400/800) and STS Series (STS800/1600) support the RC4 and the SSL encryption methods in serial data communication.

The purpose of this guide is to describe how to use the RC4 and the SSL encryption sample program package.

For sample program package described in this guide, please contact the technical support of Sena Technologies, Inc.

2. Brief descriptions about RC4 and SSL encryption methods

2.1. RC4

RC4 is a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure.

2.2. SSL

SSL (Secured Sockets Layer) is a protocol that transmits communications over the Internet in an encrypted form. SSL ensures that the information is sent, unchanged, only to the server you intended to send it to. Online shopping sites frequently use SSL technology to safeguard your credit card information.

SSL (Secure Sockets Layer) is a protocol for encrypting TCP/IP traffic that also incorporates authentication and data integrity. The newest version of SSL is sometimes referred to as Transport Layer Security (TLS) (the specification for which can be found at www.ietf.org/rfc/rfc2246.txt) and TLS v1.0 is equivalent to SSL v3.1.

SSL runs on top of TCP/IP and can be applied to almost any sort of connection-oriented communication. It is most commonly used to secure HTTP. When HTTP is secured in this fashion, it is referred to as HTTPS. Most browsers now support HTTPS connections, allowing secure communication with a web server supporting SSL.

SSL is based on session-key encryption which adds a number of extra features, including authentication based on X.509 certificates and integrity checking with message authentication codes.

SSL is an extension of sockets, which allow a client and a server to establish a stream of

communication with each other. They begin with a handshake, which allows identities to be established and keys to be exchanged.

For more detail information about SSL, please refer to the following URLs,

http://www.openssl.org/

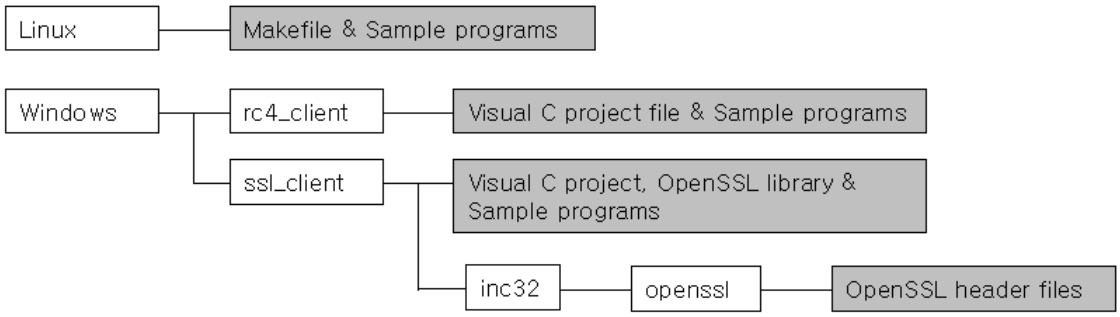
http://wp.netscape.com/eng/ssl3/ssl-toc.html

3. How to build sample programs?

3.1. Preparing

Decompress sample program package on your host.

The directory structure of the sample program package is as follows,



To build sample programs on Linux host, you need to install the OpenSSL package. But most Linux distribution has the OpenSSL installed by default.

3.2. Building and Executing

3.2.1 Linux Host

1. Build the sample programs as follows.

```
# cd Linux
# make all
```

2. Run the RC4 sample program as follows.

```
# ./rc4_client –host 192.168.1.1 –port 7001
```

or

```
# ./rc4_client –connect 192.168.1.1:7001
```

3. Run the SSL sample program as follows.

```
# ./ssl_client –host 192.168.1.1 –port 7002
```

or

```
# ./ssl_client –connect 192.168.1.1:7002
```

Please note that target serial port of the HelloDevice device server should be configured correctly

before testing sample program.

3.2.2 Windows Host

1. Run the Microsoft Visual C++ IDE and open the VC++ project file in sample package.
2. Modify the sample program.
   RC4 and SSL Window sample programs have the fixed variables for target host IP address and port number on the top of source program. (rc4_client.c, ssl_client.c)
   Modify these variables according to your environments.
3. Build the sample program in VC IDE.
   To build the SSL sample program, you should add the Windows\ssl_client\inc32 directory to the directory for include files by selecting Tools->Options->Directories tab of VC++ IDE.
4. Run the sample program in command prompt as follows,
   ```
   Windows\rc4_client\Debug\rc4_client
   ```
   Or
   ```
   Windows\ssl_client\Debug\ssl_client
   ```

Please note that target serial port of the HelloDevice device server should be configured correctly before testing sample program.

SSL libraries included in this sample package are built from the OpenSSL project source v0.9.6a (http://www.openssl.org/source/)

Download RC4/SSL Sample Program