ZTP Network Security Plug-In (SSL)

Quick Start Guide

QS005906-1211

Introduction

ZTP Network Security Plug-In (SSL) software version 2.2.0 provides secure sockets layer (SSL) support to any TCP-based application that uses the Zilog TCP/IP (ZTP) software suite. This Quick Start Guide helps you install, compile, and execute the sample application included in this package.

The ZTP Network Security Plug-In (SSL) package can only be used with the ZTP software suite as the SSL protocols require the TCP/IP-enabled platform. This package is compatible with ZTP v2.2.0 and is an optional add-on to the ZTP software suite.

Although ZTP Network Security Plug-In (SSL) runs on the same processors as the ZTP software suite, you get the best performance when using faster platforms such as RAM-based eZ80F91 system instead of a Flash-based eZ80F92 system.

About SSL

The SSL is a suite of protocols which provides authentication, privacy, and data integrity over an insecure channel such as a TCP connection. Authentication ensures that communication occurs only with the intended target and not with an attacker masquerading as the target. Privacy prevents eavesdroppers from understanding the communication. Data integrity provides a mechanism which allows the participants to identify if the message is altered by an attacker.

This package provides support for the SSL version 2, SSL version 3, and TLS version 1 protocols. To secure communication with a peer device, existing TCP server or client applications can use one or more of these protocols. Later versions of the SSL protocol provide better security than earlier versions of the protocol at the expense of increased code size and slightly slower operation.

Package Contents

The ZTP Network Security Plug-In (SSL) package contains the following components:

- *Pre-compiled libraries*, which implement the SSL handshake protocols and cryptographic algorithms.
- Source code for all versions of the SSL handshake protocols.
- ZTP Network Security Plug-In (SSL) Quick Start Guide (QS0059).
- ZTP Network Security Plug-In (SSL) User Manual (UM0201).
- ZTP Network Security Plug-In (SSL) Reference Manual (RM0047).
- Release Notes.

Note: *The ZTP Network Security Plug-In (SSL) package is available in two versions, United States (US) version and International (INT) version. The US version of the ZTP Network Security Plug-In (SSL) package includes the source code to the cryptographic library and the INT version includes only the cryptographic library.*

System Requirements and Pre-requisites

This section describes the hardware and software system requirements and pre-requisites for installing and using the ZTP Network Security Plug-In (SSL) package.

Target Hardware Requirements

This package runs on the development kits similar to the ZTP software suite which includes:

- eZ80F910300ZCOG
- eZ80F910200KITG
- eZ80F920200ZCO
- eZ80L920210ZCO

Note: *Full implementation of ZTP Network Security Plug-In (SSL) requires approximately 100 KB of code memory on the target platform. The dynamic RAM requirements vary depending on the application and the amount of data transferred. Ensure at least 20 KB of RAM per active SSL session.*

In addition, this package requires all cables, power supplies, and emulator hardware supplied with one of the supported development platforms. For information on setting up the ZDS II development kit hardware, refer to *eZ80Acclaim!® Development Kits Quick Start Guide (QS0020)*.

Target Software Requirements

The target system must be running ZTP v2.2.0 to ensure compatibility with this package. It is necessary to rebuild the existing ZTP application with SSL components included in this package to enable secure communications.

For information on Host Machine Hardware and Software requirements, refer to System Requirements and Pre-requisites section in *Zilog TCP/IP Software Suite Quick Start Guide (QS0049)*.

Installing the ZTP Network Security Plug-In (SSL)

Before installing ZTP Network Security Plug-In (SSL), ensure that ZTP v2.2.0 is installed on the host PC. The default folder for various ZTP installation are as follows:

- Object code of ZTP v2.2.0—`C:\Program Files\Zilog\ZTP_2.2.0_Lib_ZDS`
- Source code of ZTP v2.2.0—`C:\Program Files\Zilog\ZTP_2.2.0_Src_ZDS`

Follow the steps below to install the ZTP Network Security Plug-In (SSL):

1. Insert the CD containing ZTP Network Security Plug-In (SSL) software in your PC. If the setup program does not start automatically, use Windows Explorer to browse the contents of the CD and then double click on either the `ZTP_SSL_v2.2.0_US.exe` or `ZTP_SSL_v2.2.0_INT.exe` setup program available in the root directory and follow the instructions.

   Note: *Only one of these setup programs is present on the CD depending on whether the US or International version of the ZTP Network Security Plug-In (SSL) software is purchased. If the CD does not contain the updated version of the SSL package, contact Zilog Customer Support.*

2. When the installation program starts executing, it prompts you to accept or decline the license agreement. To complete the installation, accept the terms of the license agreement.
3. Enter a user name and serial number. The user name is optional and arbitrary, but enter a valid serial number to unlock the installation CD.

Note: *If a valid serial number is not received along with the installation CD, contact Zilog Customer Support.*

4. Select a folder to copy the package contents. The default path is `C:\Program Files\Zilog`. If the underlying ZTP package is installed in another folder, click **Change** to select the folder in which the ZTP software is installed.
5. Click **Install** to complete the installation of the selected software components.

Uninstalling the ZTP Network Security Plug-In (SSL)

To uninstall ZTP Network Security Plug-In (SSL), start the installation program by repeating step 1 of the installation section. When the InstallShield wizard finds an already installed version of SSL, it allows you to modify, repair, or remove the previous installation. Alternatively, navigate to **Start → Settings → Control Panel → Add and Remove Programs** to select the installed version of SSL and uninstall it from your PC.

ZTP Directory Structure

After ZTP Network Security Plug-In (SSL) is installed, several new folders and files are added to the directory in which the underlying ZTP software suite is installed.

Figure 1 displays the directory structure of a ZTP based source system after installation of the SSL plug-in package. The following folders are added to the original ZTP installation:

- `Apps\crypto`
- `Apps\SSL`
- `Build\SSLDemo`

SSL related configuration files are added to the `\ZTP\Apps\crypto\Src\Conf` and `\ZTP\Apps\SSL\Src\Conf` folders, for the ZTP source package.

Note: *In Figure 1 and Figure 2,* `X.Y.Z` *refers to the ZTP release version 2.2.0.*

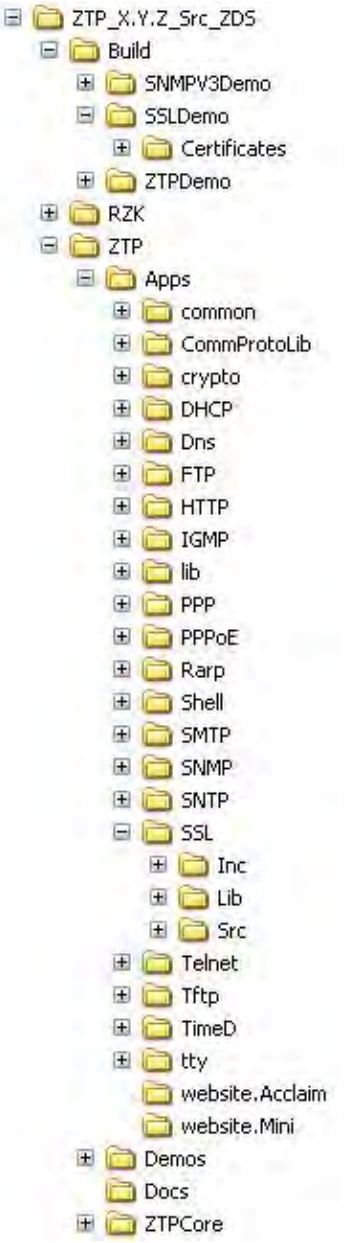

Figure 1. Directory Structure for ZTP-Based Source System

Figure 2 displays the directory structure of the ZTP-based library system after installation of the SSL plug-in package. The `SSLDemo` folder is added to the original ZTP installation. SSL related configuration files are added to the `\ZTP\Conf` folder of the ZTP library package.

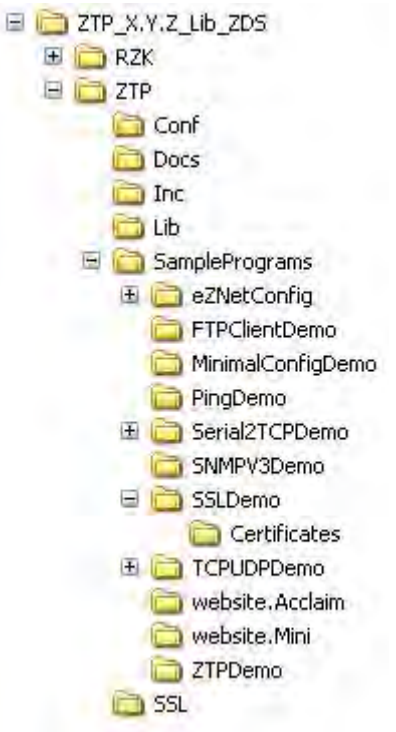

Figure 2. Directory Structure for ZTP-Based Library System

Executing the SSLDemo Project

The ZTP Network Security Plug-In (SSL) package contains an HTTPS server which adds SSL security to the HTTP web server included in the ZTP software suite. In addition, the sample SSL server application and SSL client application allows two eZ80® development platforms to communicate using SSL. These sample programs can also be used to communicate with applications on a PC that use the SSL protocol. Zilog® does not provide any PC-based applications that use SSL.

Building the SSLDemo Sample Program

Follow the steps below to build the SSLDemo program and download the compiled image to the target development kit.

1. Open the SSLDemo folder from the Windows Explorer. The default location of the folder for various installation is as follows:
   - ZTP-based systems using the object code package

     `C:\Program Files\Zilog\ZTP_2.2.0_Lib_ZDS\ZTP\SamplePrograms`
   - ZTP-based systems using the source code package

     `C:\Program Files\Zilog\ZTP_2.2.0_Src_ZDS\Build`
2. Double click the ZDS II project file in the SSLDemo folder that corresponds to the development kit platform being used. For example, if ZTP (source) is installed, click `ZTP_FULL_SSL_F91_LIB.zdsproj` or `ZTP_FULL_SSL_F91.zdsproj` file; and if ZTP (library) is installed, click `ZTPSSLDemo_F91.zdsproj`.
   For ZTP-based systems using source code package, the sample projects are present in `Build` folder.
3. Select the appropriate project configuration from the configuration pull-down menu of the ZDS II project file. Depending on the target hardware platform, select one of the three configuration options available:
   - RAM
   - FLASH
   - COPY TO RAM

In this example, the RAM configuration is selected.

4. To rebuild all source code modules included in the project, select the **Build → Rebuild All** menu option from the ZDS II interface.

Note: *Ensure that the target development kit has been powered on and the necessary cables are connected. For more information on ZDS II interface, refer to the Quick Start Guide included in the development kit.*

5. To download the executable image to the target platform, click **Download Code** on the ZDS II toolbar or select the **Build → Debug → Download Code** menu option.

6. To run the application on the target platform after the project code is downloaded, click the **Run** icon on the ZDS II toolbar or select the **Build** → **Debug** → **Go** menu option.

Using the HTTPS Server

When you start the SSLDemo sample program on the target development platform, an HTTPS server is started on port 443. Follow the steps below to view the website using Internet Explorer:

1. Open Internet Explorer and enable at least one of the SSL handshake protocols. To view the SSL handshake protocols, select **Tools** → **Internet Options** menu from the Internet Explorer.
2. Select the **Advanced** tab from the **Internet Options** dialog box.
3. From the **Security settings** section in the **Advanced** tab, select any of the following options:
   - Use SSL 2.0
   - Use SSL 3.0
   - Use TLS 1.0
4. Enter the URL for the SSL-enabled ZTP system in the address field of the browser. Use the IP address obtained from the first step as the URL. For example, if the sample ZTP system is using IP address 192.168.1.23, enter the following URL in the browser: `https:\\192.168.1.23.` After entering the IP address, the browser displays a security alert.

Figure 3 displays the security alert on a browser.

Figure 3. Security Alert

This security alert indicates the successful completion of the first SSL handshake protocol in an SSL-enabled ZTP system.

The warning is due to a self-signed test certificate included in the ZTP Network Security Plug-In (SSL). This message does not appear when you obtain a real certificate from a valid certificate authority (CA) for your eZ80® based product.

5. Click **Yes** to continue. The browser then uses the additional SSL session(s) to download the web page.

Once the transfer is complete, you can notice the padlock at the bottom right hand corner of the browser indicating that the data has been secured. Figure 4 displays the padlock on the browser window.

Figure 4. Padlock on the Browser Window

Using the SSL Client and SSL Server Programs

The sample program described in this section requires two eZ80® development platforms running the SSLDemo application. One system acts as SSL client and the other acts as SSL server. The `ssldemo` console command added to the underlying ZTP system by the SSLDemo application determines the role of each system.

The SSL client initiates an SSL session with the server and sends an encrypted message to the server. The server displays the message on the console and then echoes the same message back to the client. The client displays the message received from the server on its console and verifies if the message is identical to the original one.

Note: *Each development platforms must have an unique IP address in the same network or subnetwork. Dynamic host configuration protocol (DHCP) must be used or the static IP parameters must be manually configured as appropriate. In addition, the two eZ80 development platforms must be assigned a unique Ethernet MAC address. For information on how to make these changes, refer to the ZTP documents included in the* `Docs` *directory of the underlying ZTP system.*

Executing the SSLDemo Application

The server application on the first ZTP system must be started before executing the client application on the second system. Follow the steps below to run the server application:

1. Compile, build, and download the SSLDemo sample program on the first ZTP system (see Building the SSLDemo Sample Program on page 7).

2. Enter the following command on the command prompt:

```
ssldemo server 5000
```

This command launches the `ssldemo` program. The `server` parameter indicates to the program that the system must operate in server mode. The last parameter (5000 in this example) is the TCP port number on which the application waits for a connection from a remote client. Once the server has been created, it displays a message on the console as shown below:

```
Server listening on port 5000
```

Follow the steps below to run the client application:

1. Compile, build, and download the SSLDemo sample program on the second ZTP system (see Building the SSLDemo Sample Program on page 7).
2. Enter the following command on the command prompt:

```
ssldemo client 192.168.1.23:5000 “Hello server”
```

This command launches the `ssldemo` program. The `client` parameter indicates to the program that the system operates in client mode. The next parameter (`192.168.1.23:5000`) is the socket of the `ssldemo` server program running on the first eZ80® development platform. Text within the quotation marks is interpreted as the message sent to the server. The maximum length of the message in the SSLDemo application is restricted to 40 characters.

3. Enter a message on the command prompt of the client system. The client sends this message to the server.

The server displays the message on its console and echoes the same message back to the client. The client verifies whether the message received from the server is identical to the message entered on the command line. The client terminates the SSL session after verifying the message.

4. To stop the SSL server application, enter the following command on the server’s console:

```
ssldemo server stop
```

This sample program is an example of how to use SSL to enable secure data transfer in your applications. You can modify the test program to send large or multiple messages. For information on how to reconfigure ZTP Network Security Plug-In (SSL), refer to *ZTP Network Security Plug-In (SSL) User Manual (UM0201)* and *ZTP Network Security Plug-In (SSL) Reference Manual (RM0047)*.

It is also possible to use the SSLDemo sample program to communicate with PC-based applications using SSL.

Creating a New ZTP Project with SSL Support

The simplest way to create a new ZTP project with SSL support is to copy one of the existing sample projects into a new folder and modify it to suit your requirements. For information on how to add and remove files from a project as well as description of the advanced features of the tool, refer to *Zilog Developer Studio II–eZ80Acclaim!® User Manual (UM0144)*.

For information on ZDS II project settings required by SSL, refer to *ZTP Network Security Plug-In (SSL) User Manual (UM0201)* included in this package.

Related Documentation

For more information on the eZ80Acclaim!® family of microcontrollers, which includes the eZ80F91, eZ80F92, and eZ80F93 microcontrollers, and the eZ80L92 microprocessor, refer to the following documents:

- eZ80® CPU User Manual (UM0077)
- eZ80F91 Product Specification (PS0192)
- eZ80F92/F93 Product Specification (PS0153)
- eZ80L92 Product Specification (PS0130)

For more information on the ZDS II development tools for the eZ80Acclaim! family, refer to the following documents:

- Zilog Developer Studio II–eZ80Acclaim!® User Manual (UM0144)
- eZ80Acclaim!® External Flash Loader Product User Guide (PUG0016)
- ZPAK II Debug Interface Tool Product User Guide (PUG0015)
- eZ80Acclaim!® Development Kits Quick Start Guide (QS0020)

For more information on the ZTP software suite, refer to the following documents:

- Zilog TCP/IP Software Suite Programmers Guide (RM0041)
- Zilog TCP/IP Stack API Reference Manual (RM0040)

For more information on the ZTP Network Security Plug-In (SSL), refer to the following documents:

- ZTP Network Security Plug-In (SSL) User Manual (UM0201)
- ZTP Network Security Plug-In (SSL) Reference Manual (RM0047)

Warning: DO NOT USE IN LIFE SUPPORT

LIFE SUPPORT POLICY

ZILOG'S PRODUCTS ARE NOT AUTHORIZED FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE EXPRESS PRIOR WRITTEN APPROVAL OF THE PRESIDENT AND GENERAL COUNSEL OF ZILOG CORPORATION.

As used herein

Life support devices or systems are devices which (a) are intended for surgical implant into the body, or (b) support or sustain life and whose failure to perform when properly used in accordance with instructions for use provided in the labeling can be reasonably expected to result in a significant injury to the user. A critical component is any component in a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system or to affect its safety or effectiveness.

Document Disclaimer

 Information in this publication concerning the devices, applications, or technology described is intended to suggest possible uses and may be superseded. ZILOG, INC. DOES NOT ASSUME LIABILITY FOR OR PROVIDE A REPRESENTATION OF ACCURACY OF THE INFORMATION, DEVICES, OR TECHNOLOGY DESCRIBED IN THIS DOCUMENT. ZILOG ALSO DOES NOT ASSUME LIABILITY FOR INTELLECTUAL PROPERTY INFRINGEMENT RELATED IN ANY MANNER TO USE OF INFORMATION, DEVICES, OR TECHNOLOGY DESCRIBED HEREIN OR OTHERWISE. The information contained within this document has been verified according to the general principles of electrical and mechanical engineering.