SSL Communication with Apache Server

2170030

Author:	Sierra Wireless	Date:	August 1, 2013

APN Content Level	BASIC		INTERMEDIATE		ADVANCED	✓	Confidentiality	Public	✓	Private	

Hardware Compatibility	Product Line	AirPrime	Series	Q26xx	SL60xx
				WMPxx	SL808x

Software Compatibility	Series	ALL

1 Version

Application Notes may be updated over their lifetime. To ensure you design with the correct version, please check the application notes page in www.sierrawireless.com for latest versions.

2 Introduction

This Application Note (APN) is provided to Sierra Wireless distributors and clients to aid more rapid development of embedded applications using the Sierra Wireless portfolio of cellular solutions. To request a new application note, contact your regional Sierra Wireless Product Marketing Manager.

3 Overview

The OpenSSL Project is a robust, commercial-grade, full-featured, and Open-Source toolkit implementing the Secure Sockets Layer protocols as well as a full-strength general purpose cryptography library. Detailed explanation about OpenSSL is present at http://www.openssl.org.

OpenSSL is used in the Internet & TCP/IP Libraries provided by Sierra Wireless to establish secure communication. The OpenSSL version used in the Libraries is v0.9.6c.

Screenshots have been added to help you relate to the steps that are explained.

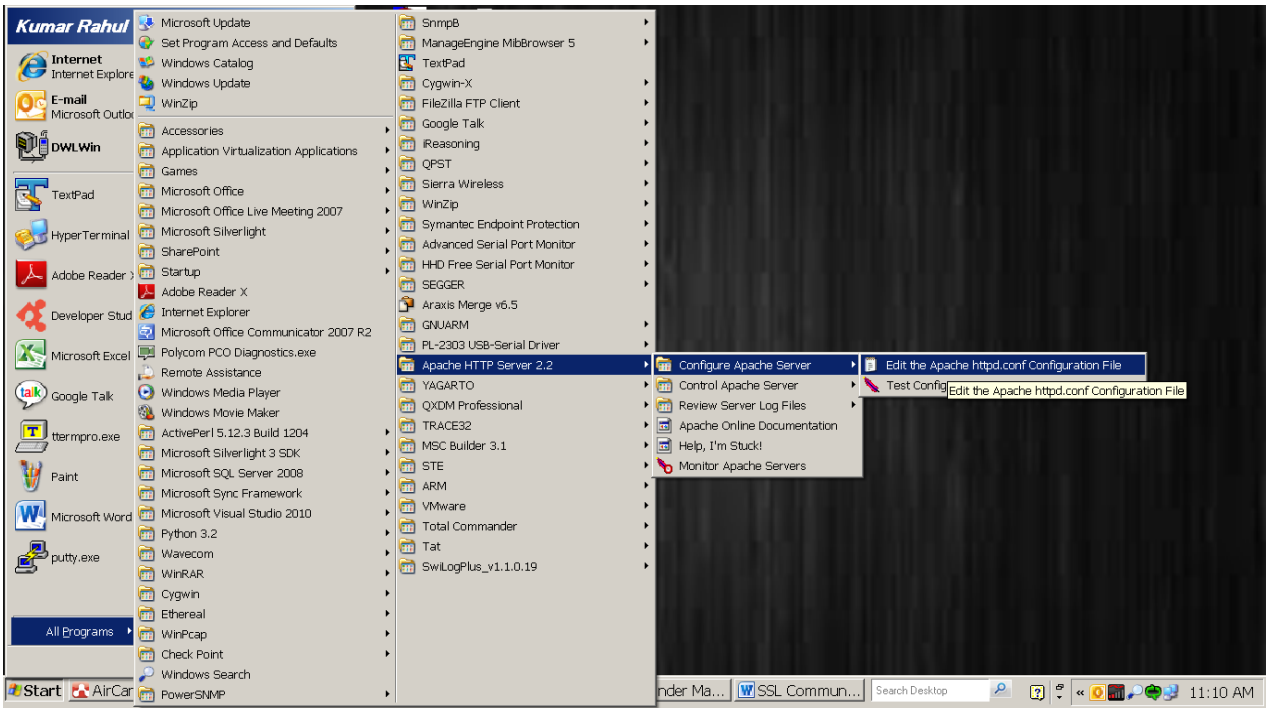
4 Glossary

Initials	Definition
GSM	Global System for Mobile Communication
HTTP	Hyper Text Transfer Protocol
PPP	Point to Point Protocol
TMT	Target Monitoring Tool
UART	Universal Asynchronous Receiver/Transmitter

5 Apache Server Installation and Configuration

Apache HTTP Server Project is a HTTP web server for modern operating systems including UNIX and Windows NT. This project provides a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards. Information regarding the Apache HTTP web server installation and configuration is available at **http://httpd.apache.org/docs/2.2/**.

With respect to the sample application “wipssl_https_client”; the following changes will be required in the httpd.conf file:



5.1.1 Modification 1

Listen to IP 192.168.1.5 and PORT 4433, which is assigned by the application running on the AirPrime module.

#Listen 80 /* This Line is commented */

Listen 192.168.1.5:4433

Keepalive off

Timeout 10

5.1.2 Modificaiton 2

The server is running on 192.168.1.5, which is assigned by the AirPrime module.

#ServerName BLRKEC216936D.ad.infosys.com:80 /* This Line is commented */

ServerName 192.168.1.5

6 Setting Up SSL Secured Communication Channels Using Apache Server

In the application note, Open AT Framework Sample Application “wipssl_https_client” is used to explain the steps to set up a SSL-Secured Communication channels using Apache server over UART PPP and the OS used is Windows. Please note that the Open AT Framework Sample Application “wipssl_https_client” can be used to set up secured communication over GSM PPP or GPRS. In order to communicate over GSM or GPRS; uncomment one of the followings according to the requirement, which is available in the “appli.c” file of the Open AT Framework Sample Application “wipssl_https_client”.

//#define OVER_UART_PPP_SERV

//#define OVER_UART_PPP_CLIENT

//#define OVER_GSM_PPP_SERV

//#define OVER_GSM_PPP_CLIENT

//#define OVER_GPRS

This application establishes a connection with an HTTPS server. When the negotiation is complete, the application displays the page (source code in HTML) of the root page of the server.

With respect to the sample application “wipssl_https_client”, use the option “OVER_UART_PPP_SERV”.

6.1 Setting-Up Apache Server

6.1.1 Cryptographic Keys and Certificates

When two parties want to communicate over an insecure channel, they might use cryptographic keys as follows. Both parties agree to use one particular algorithm with a particular key. The first party composes a message and creates a network stream on which to send the message. Then the text is encrypted using the key, and is sent across the Internet to the second party. Please note that the key is not sent across with the encrypted text. The second party receives the encrypted text and decrypts it using the previously agreed upon key. However, if the transmission is intercepted, the interceptor cannot recover the original message because the interceptor does not know the key. Thus cryptographic keys are used for authentication (e.g. through Secure Shell) or signing (e.g. web server certificates).

Thus, the key and certificate files, which are included in the source directory of the Open AT Framework Sample Application “wipssl_https_client” (path: C:\OpenAT\Plug-ins\Security\1.00.2030\Security\samples\wipssl_https_client\ src) has to be copied to the Apache Software.

Foundation (Path: C:\Program Files\Apache Software Foundation\Apache2.2\bin). The key and certificate files are:

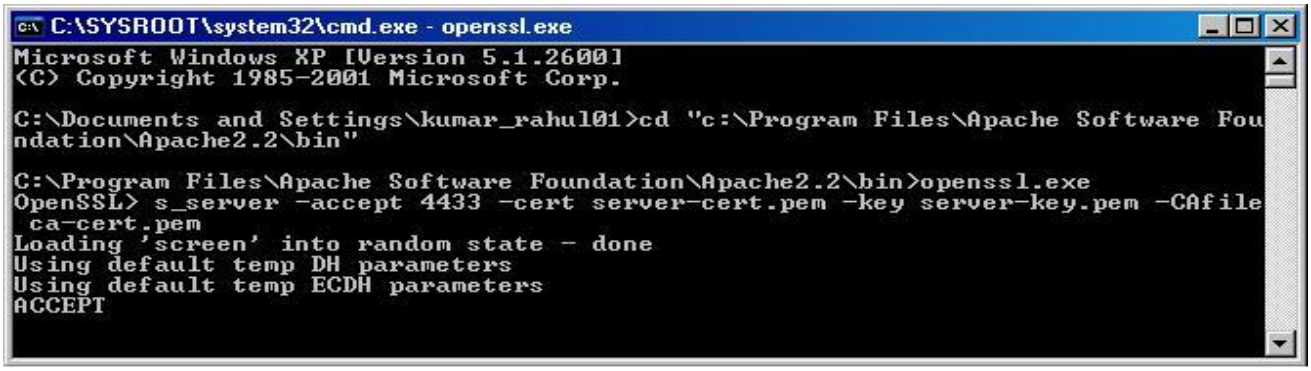
a. ca-cert.pem
b. client-cert.pem
c. client-key.pem
d. server-cert.pem
e. server-key.pem

6.2 Run OpenSSL as Server

In order to run the OpenSSL as server, open the command prompt. Command prompt can be opened by typing “cmd” in the run window (Start->Run). The appropriate command to run it is:

```
s_server -accept 4433 -cert server-cert.pem -key server-key.pem -CAfile ca-cert.pem -www
```

The key and certificate files are included in the source directory of the sample application as mentioned earlier.



6.3 Setting Up Windows PPP Server

6.3.1 Step 1

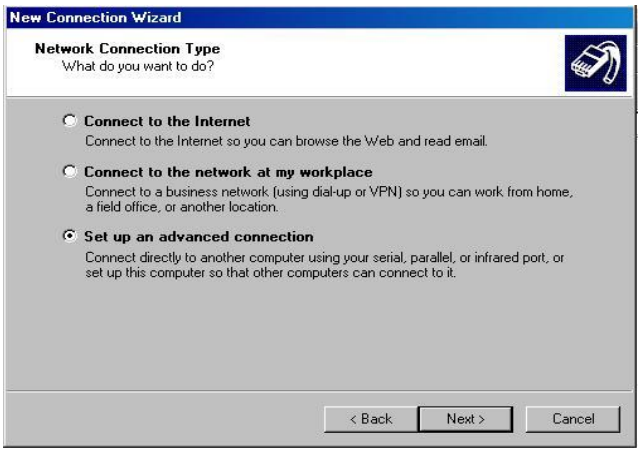
PC dial-up connection is used to connect to a network such as your workplace network. Steps to create a dial up connection (serial computer to computer) are given below:

6.3.2 Step 2

Run the “New Connection” wizard and click on “Next” button.

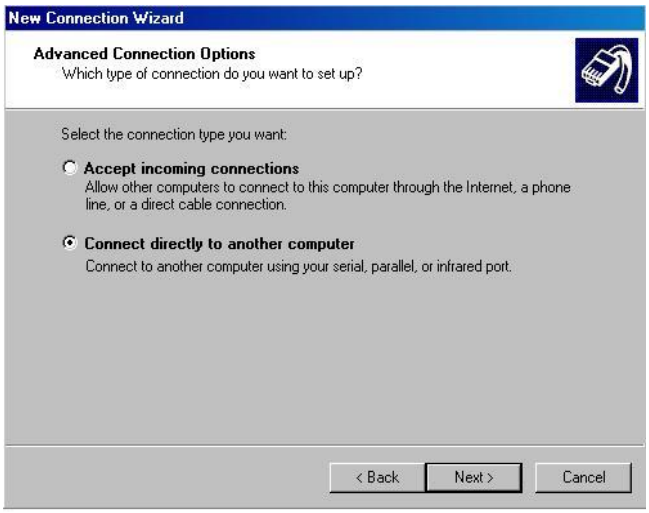
6.3.3 Step 3

Select “Set up an advanced connection” and click “Next”.



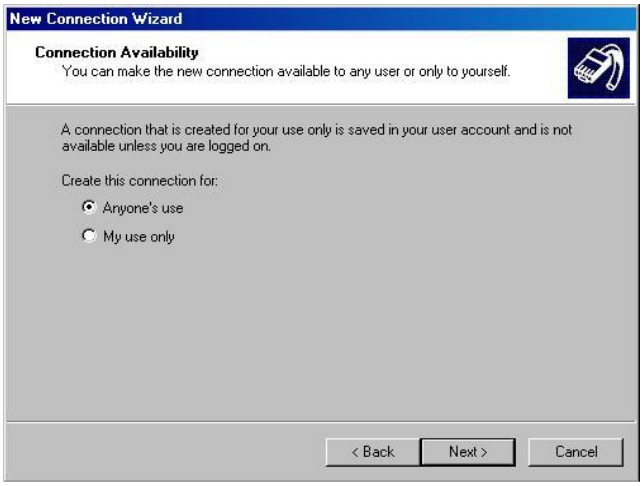
6.3.4 Step 4

Select “Connect directly to another computer” and click “Next”.



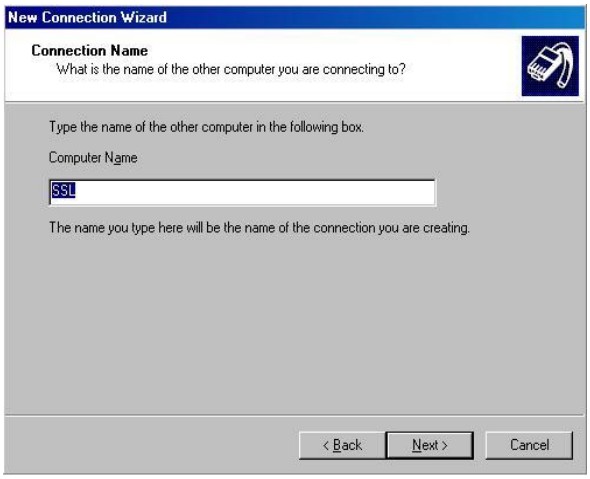
6.3.5 Step 5

Select “Anyone’s use” and click “Next”.



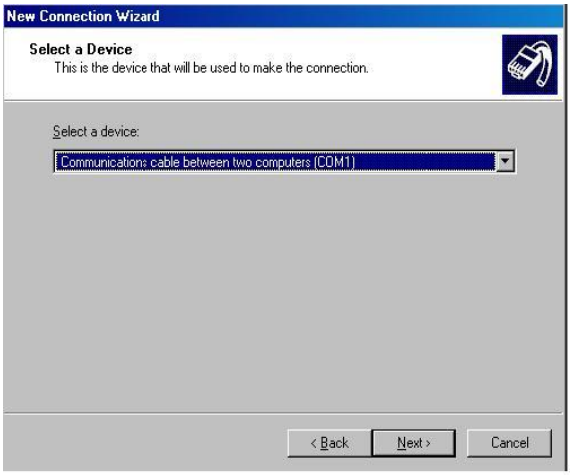
6.3.6 Step 6

Type the Computer Name and click “Next”.



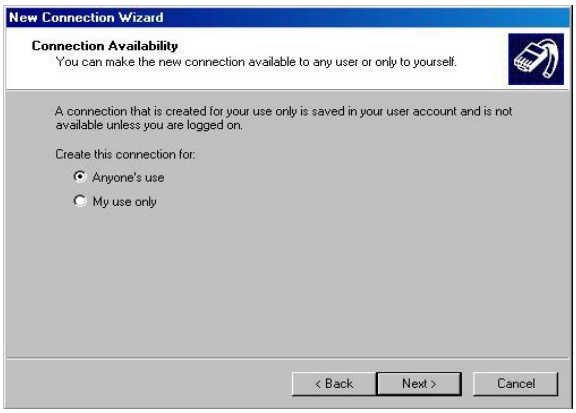
6.3.7 Step 7

Select “Communication cable between two computers (COM1)” as device and click “Next”.



6.3.8 Step 8

Create the connection as per the requirement and click “Next”.



6.3.9 Step 9

The new connection is created. Click “Finish” to complete the set-up.

6.3.10 Step 10

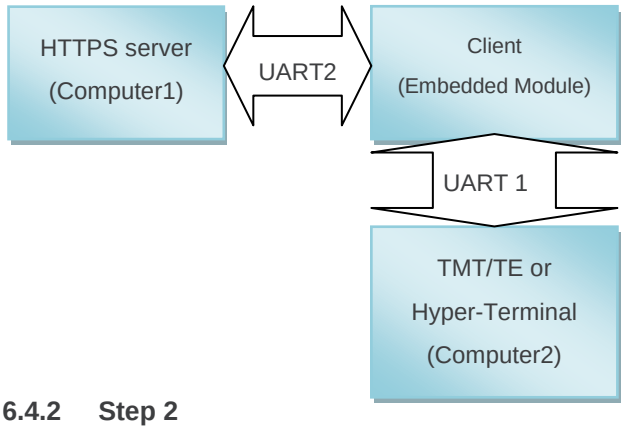
Once the ‘‘Finish’’ button is clicked, the following window will appear where username and password have to be provided for dial-up connection. Access point parameters are provided in the Open AT Framework Sample Application ‘‘wipssl_https_client’’. Username and password for the PPP connection are ‘‘wipuser’’ and ‘‘WU#passwd’’ respectively.

6.4 Setting Up Client Connection

6.4.1 Step 1

Now a client needs to be created to attach to the server. Hence, after the set up of Apache server and Windows PPP server above, run the Open AT Framework Sample Application "wipssl_https_client" from UART1 using "AT+WOPEN=1" command as this application establishes a connection with an HTTPS server.

Make sure that the clock is properly set before running the application. The command to set the clock is "AT+CCLK"



6.4.2 Step 2

Run the Apache server (Start→ All Programs→ Apache HTTP Server→ Control Apache Server→ Start)

With respect to the sample application "wipssl_https_client"; there is the chance that the Apache server will NOT start on the IP on which it is listing. So,

a. Start the application "wipssl_https_client".

b. Start the PPP over UART connection. This will assign the IP address to the peer.

c. Now start the Apache server.

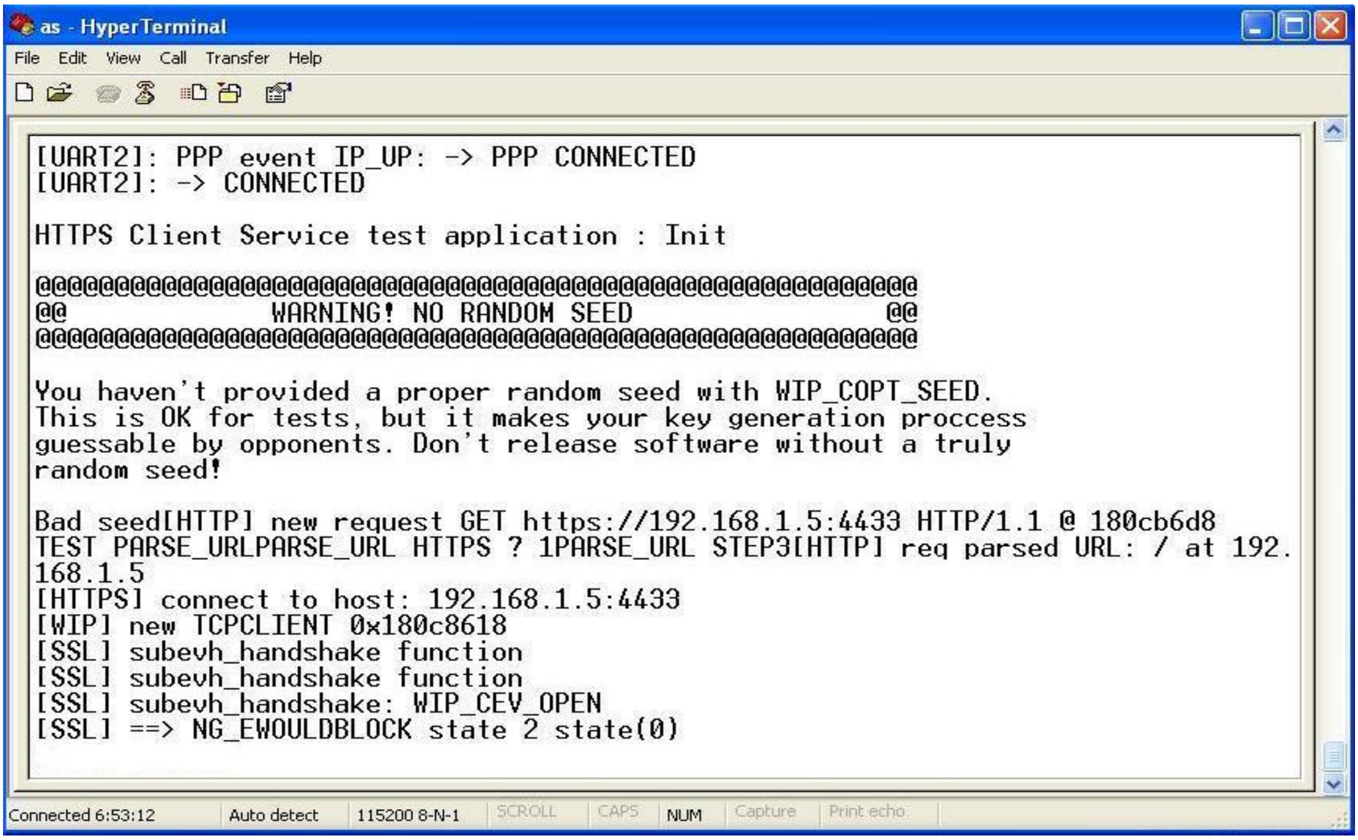
After this we can CLOSE(dis-connect) the PPP and reset the Airprime Moodule.

6.4.3 Step 3

Next is setting-up a PPP over UART. Enter access point parameter and click "Connect". Once this is done, the client connects to the Apache server which is in the listing stage.

6.4.4 Step 4

The sample application establishes a connection between the client (embedded module) and the HTTPS server. When the negotiation is complete, the application shows us the page of the root page of the server as shown in figure below.



6.4.5 Step 5

On PC side you can open the Internet Explorer and enter the HTTPS address (https://192.168.1.5:4433/) to view the page.

7 Software Compatibility Matrix

FW	Open AT Framework/SDK	Open AT Framework Libraries
R7.x	Open AT Application Framework v2.x	Internet Library

8 Reference Documents

	Document Name	Comment
[1]	Security Library User Manual-Internet Library SSL	This document describes the Internet Library SSL Security Library, which provides SSL-secured communication channels to Internet Library.

9 Support

For direct clients: contact your Sierra Wireless FAE

For distributor clients: contact your distributor FAE

For distributors: contact your Sierra Wireless FAE

10 Document History

Level	Date	History
001	October 9, 2009	Creation
002	February 18, 2010	Update

Level	Date	History
3.0	January 13, 2012	Updated legal boilerplate contents New reference: 2170030 Old reference: WM_DEV_OAT_APN_018
4.0	August 1, 2013	Updated Apache settings with respect to “wipssl_https_client” application.

11 Legal Notice