AN054 –

SERIAL TO WI-FI (S2W) HTTPS (SSL) AND EAP SECURITY

AT COMMANDS/CONFIGURATION EXAMPLES

Table of Contents

1 Pre-Requirement

Verify that the appropriate "Serial To Wi-Fi" application firmware binaries are loaded on the Gainspan module.

For EAP tests, ensure that the binaries loaded support the EAP feature, else ERROR or INVALID INPUT responses may be seen.

For more details on the usage of AT commands described in this document, please refer to the "Serial-to-Wi-Fi Adapter Programming Guide.pdf" document. For which binaries version supports EAP, refer to the release notes or build the binary using the SDK Builder tool from the GainSpan website support section.

2 HTTPS Examples

This section provides instructions to generate self signed certificates and provides HTTPS GET/POST examples using the Serial to Wi-Fi application.

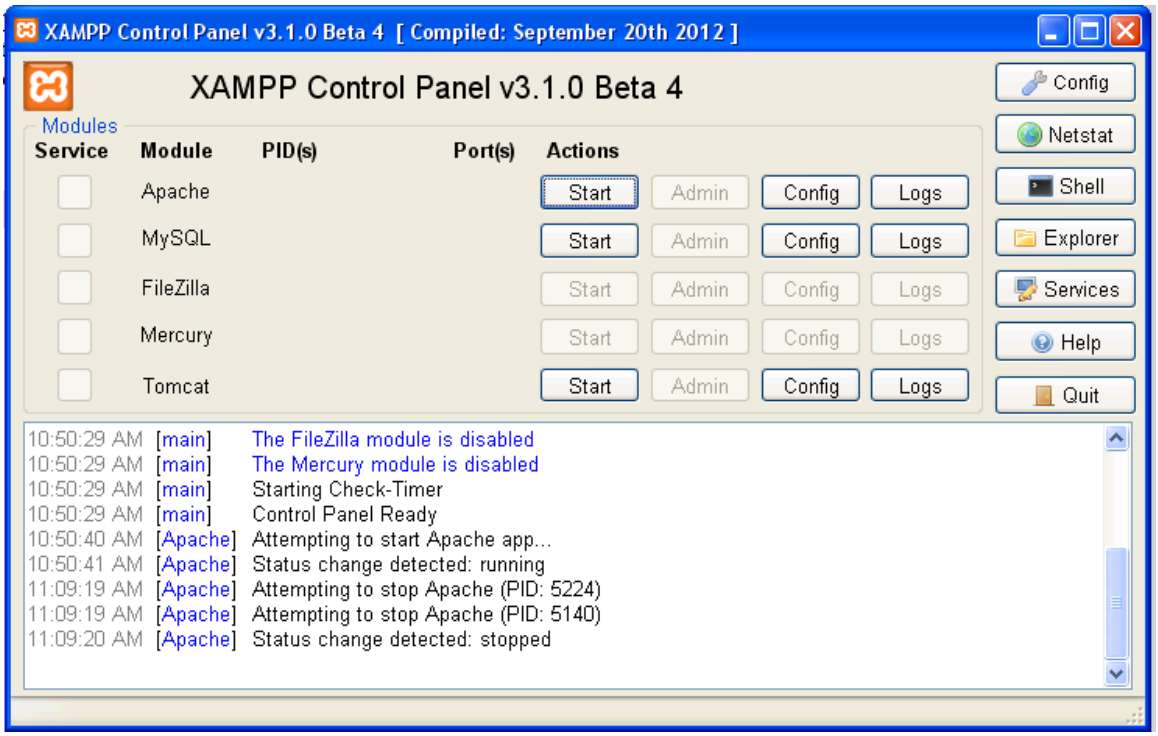
2.1 Installing Apache Server

2.1.1 Install Apache Server in Windows

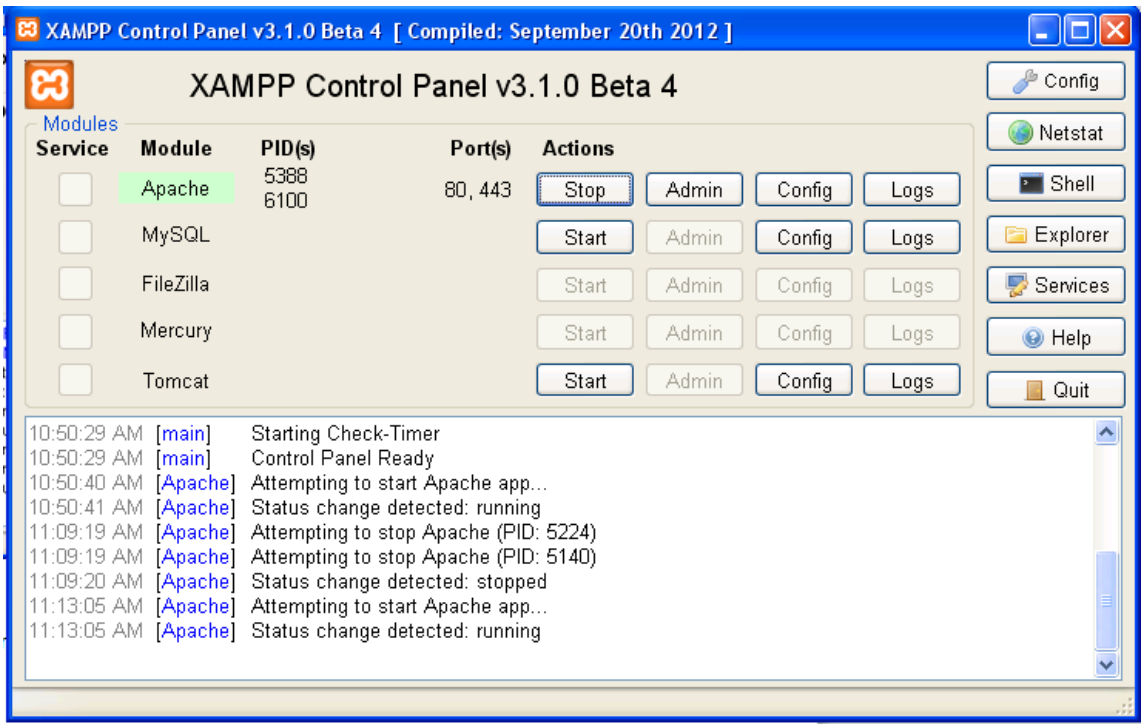
1. Download XAMPP for Windows from the following web link http://www.apachefriends.org/en/xampp-windows.html
2. Run the setup file to install XAMPP. All the files would be extracted to C:\xampp\. Please note to turn off your network connections and all web browsers to avoid any error during the installation process.

2.1.2 Run Apache Web Server

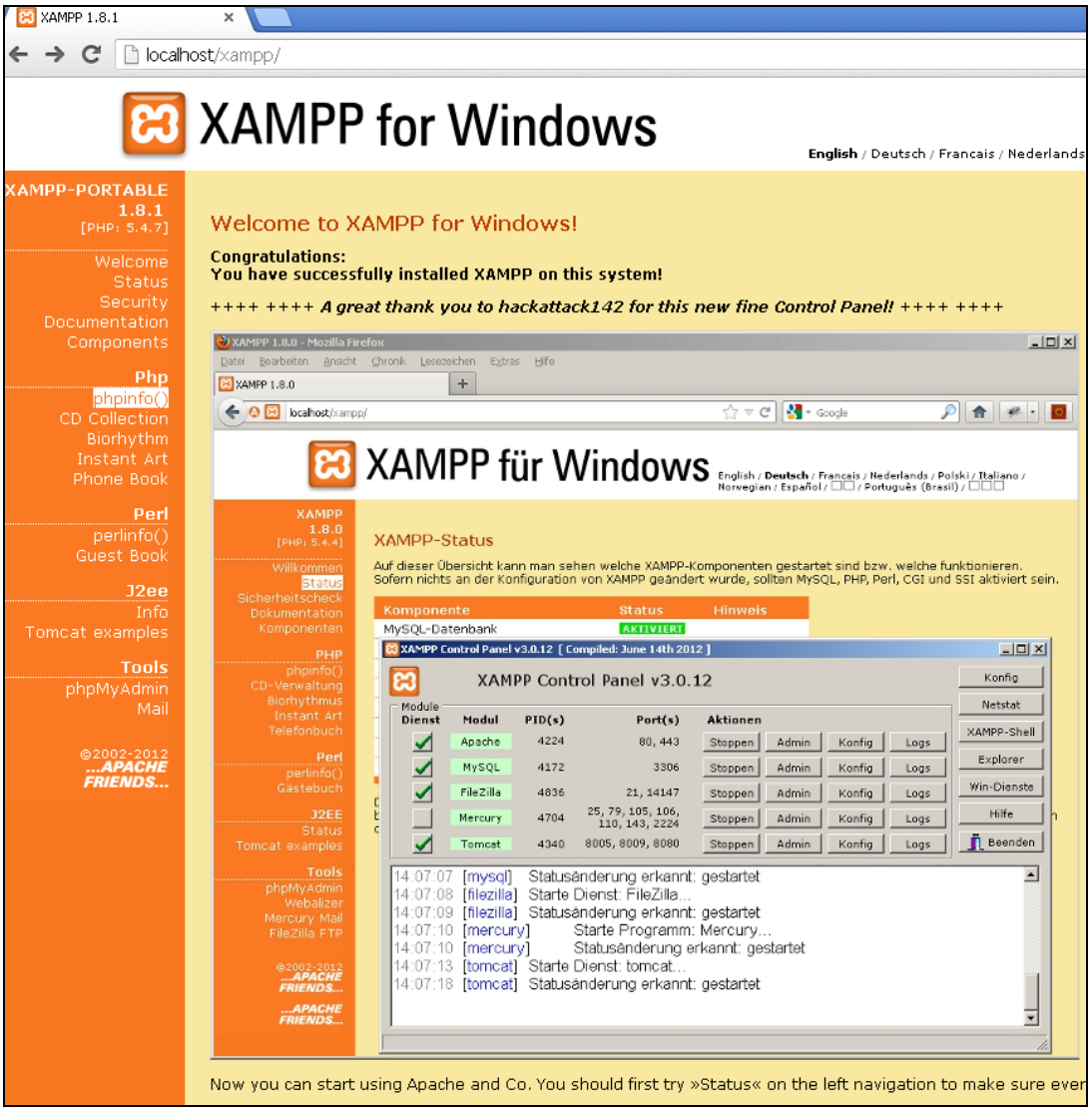
1. Browse to C:\xampp\ and run xampp-control.exe. The xampp control panel is as shown



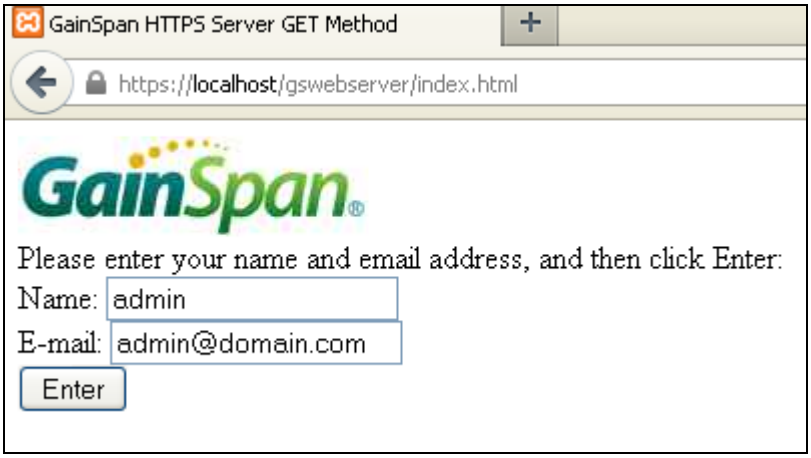
2. Click on the 'Start' button to start the Apache Web server.



3. After starting of Apache, go to the address http://localhost/ or http://127.0.0.1/ in your browser. This verifies that the web server is running properly.



4. GainSpan provides several example web pages for users to verify that the apache server is configured properly to access the web pages. Copy the Gainspan example "gswebserver" folder into C:\xampp\htdocs\.
    a. To test the index.html web page, open a web browser and go to the address http://localhost/gswebserver/index.html or http://127.0.0.1/gswebserver/index.html.



Enter the Name and E-mail details and click on Enter.

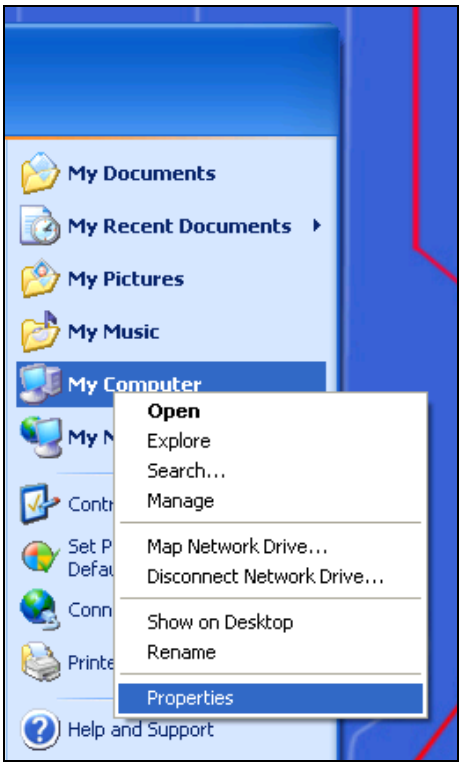
b. To test the post.html web page, open a web browser and go to the address http://localhost/gswebserver/post.html or http://127.0.0.1/gswebserver/post.html.

Enter the Name and click on Enter.

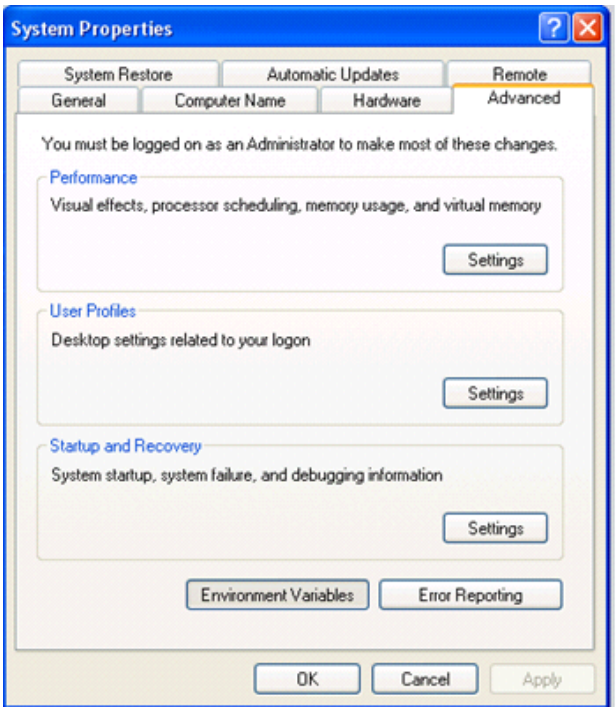
2.2 HTTPS Server Configuration

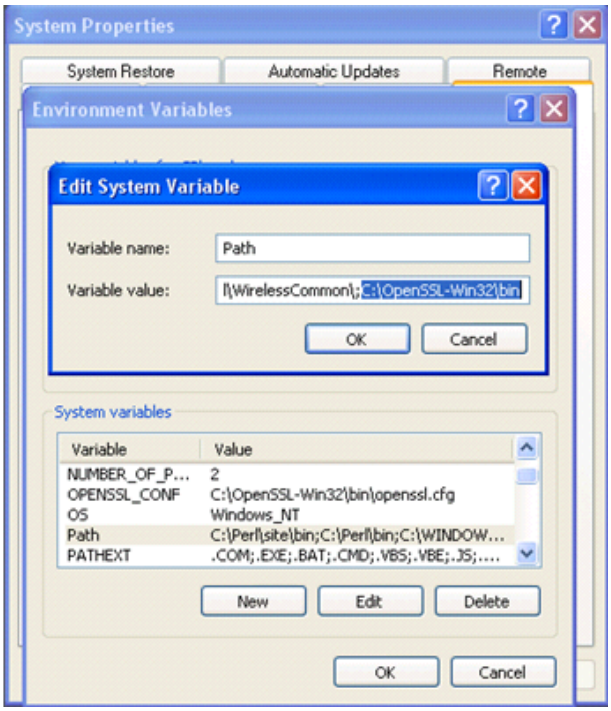
2.2.1 How To Install Openssl

1. Download and Install Perl from the following link: http://activestate.com/Products/activeperl/
   The installation is simple. Just follow the instructions on the screen.
2. Download and install Visual C++ 2008 Redistributables from:
   http://www.slproweb.com/products/Win32OpenSSL.html
   Download the appropriate version for your operating system. For example, if using WinXP 32-bit machine, one would download the "Visual C++ 2008 Redistributables"
3. Download the OpenSSL installer from:
   http://www.slproweb.com/products/Win32OpenSSL.html
   Download the appropriate version for your operating system. For example, if using WinXP 32-bit machine, one would download the "Win32 OpenSSL v1.0.1c".
4. Add C:\OpenSSL-Win32\bin to Windows system PATH variable as shown in the steps below:
   i. Right click My Computer icon, and click Properties.



ii. Go Advanced tab, and click Environment Variables. Search for 'Path' in System variables, and add "C:\OpenSSL-Win32\bin;" to the Variable value.





2.2.2 Generating Certificates

This sections describes steps to generate the following set of certificates for one-way or two-way authentication.

SSL Entity	Description	Generated Files
Certificate Authority	The CA(Certificate Authority) is the entity that issues trusted digital certificates. The CA issues public key certificates, which is used to verify a certificate's public key and that it belongs to the owner mentioned in the certificate. The CA could be a third party or implemented by the owner.	• ca.crt • ca.key • cacer.der
Server	The Server provides its certificate to the browser and can also request for a certificate from the Client. The Client validates the Server certificate using the CA's public key .	• server.crt • server.key
Client	The Client provides its certificates if the Server requests for Client authentication. The Server verifies the Client certificate using the CA's public key.	• client.crt • client.key.der

To genereate your own certiciates on a windows machine, open Command Prompt and run the following Commands:

2.2.3 Creating Own Certificate Authority

1. Creating Own Certificate Authority:

```
openssl genrsa -des3 -out ca.key 1024
openssl req -new -x509 -days 30 -key ca.key -out ca.crt
```

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out ca.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....................++++++
............++++++
e is 65537 (0x10001)
Enter pass phrase for ca.key:
Verifying - Enter pass phrase for ca.key:

C:\OpenSSL-Win32\certificates>openssl req -new -x509 -days 30 -key ca.key -out c
a.crt
Enter pass phrase for ca.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gainspanCA
Email Address []:gainspanca@gainspan.com

C:\OpenSSL-Win32\certificates>
```

2. Converting the CA Certificate from PEM to DER format:

openssl x509 –in ca.crt –inform PEM –out cacert.der –outform der

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl x509 -in ca.crt -inform PEM -out cacert.de
r -outform der

C:\OpenSSL-Win32\certificates>_
```

2.2.4 Generating Server Certificate

1. Generating Server Certificate:

openssl genrsa -des3 -out server.key 1024
openssl req -new -key server.key -out server.csr

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out server.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.............................................++++++
.........++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:

C:\OpenSSL-Win32\certificates>openssl req -new -key server.key -out server.csr
Enter pass phrase for server.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gssslserver.com
Email Address []:gssslserver@gainspan.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:gainspan
An optional company name []:gainspan

C:\OpenSSL-Win32\certificates>_
```

2. Signing the Server Certificate using own CA:

   openssl x509 -req -days 30 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl x509 -req -days 30 -in server.csr -CA ca.c
rt -CAkey ca.key -set_serial 01 -out server.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Gainspan/OU=APENG/CN=gssslserver.com/em
ailAddress=gssslserver@gainspan.com
Getting CA Private Key
Enter pass phrase for ca.key:

C:\OpenSSL-Win32\certificates>_
```

3. Remove the password from your key (first rename server.key to serverorg.key):

   openssl rsa -in serverorg.key -out server.key

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl rsa -in serverorg.key -out server.key
Enter pass phrase for serverorg.key:
writing RSA key

C:\OpenSSL-Win32\certificates>_
```

2.2.5 Generating Client Certificate

1. Generating Client Certificate:

   openssl genrsa -des3 -out client.key 1024
   openssl req -new -key client.key -out client.csr

```
Command Prompt

C:\OpenSSL-Win32\certificates>openssl genrsa -des3 -out client.key 1024
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
...................++++++
.....++++++
e is 65537 (0x10001)
Enter pass phrase for client.key:
Verifying - Enter pass phrase for client.key:

C:\OpenSSL-Win32\certificates>openssl req -new -key client.key -out client.csr
Enter pass phrase for client.key:
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Gainspan
Organizational Unit Name (eg, section) []:APENG
Common Name (e.g. server FQDN or YOUR name) []:gssslclient.com
Email Address []:gssslclient@gainspan.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:gainspan
An optional company name []:gainspan

C:\OpenSSL-Win32\certificates>
```

2. Signing the Client Certificate using own CA:

   openssl x509 -req -days 30 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out client.crt

```
Command Prompt
C:\OpenSSL-Win32\certificates>openssl x509 -req -days 30 -in client.csr -CA ca.c
rt -CAkey ca.key -set_serial 01 -out client.crt
Loading 'screen' into random state - done
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Gainspan/OU=APENG/CN=gssslclient.com/em
ailAddress=gssslclient@gainspan.com
Getting CA Private Key
Enter pass phrase for ca.key:

C:\OpenSSL-Win32\certificates>
```

3. Converting the Client Certificate from PEM to DER format:

openssl x509 –in client.crt –inform PEM –out client.der –outform der

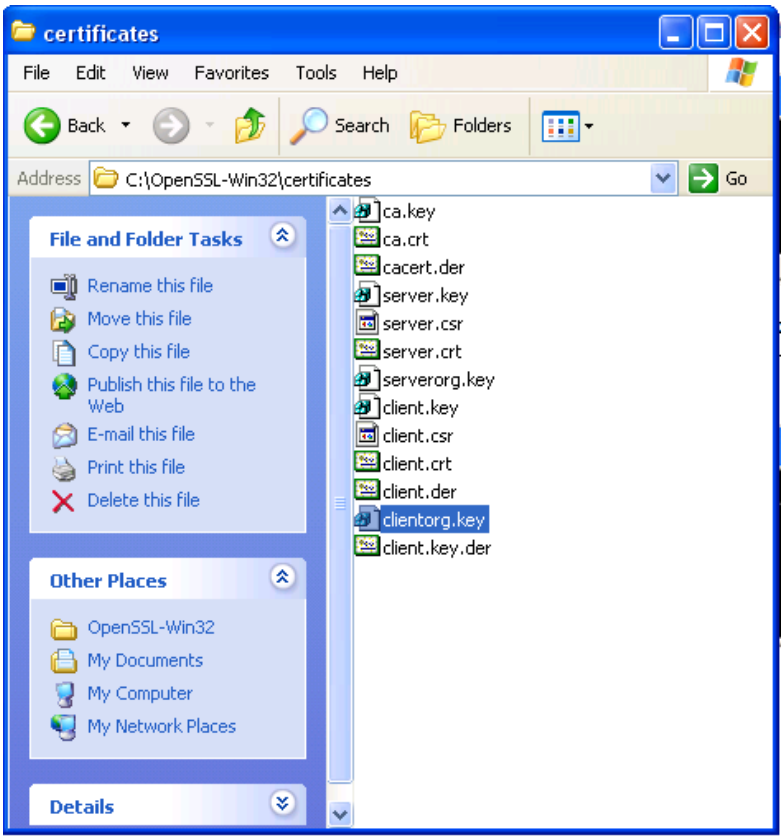
```
Command Prompt
C:\OpenSSL-Win32\certificates>openssl x509 -in client.crt -inform PEM -out cli
t.der -outform der

C:\OpenSSL-Win32\certificates>
```

4. Remove the password from your key (first rename client.key to clientorg.key):

openssl rsa -in clientorg.key -out client.key.der

```
Command Prompt
C:\OpenSSL-Win32\certificates>openssl rsa -in clientorg.key -out client.key.der
Enter pass phrase for clientorg.key:
writing RSA key

C:\OpenSSL-Win32\certificates>_
```

The following screenshot shows the files generated.

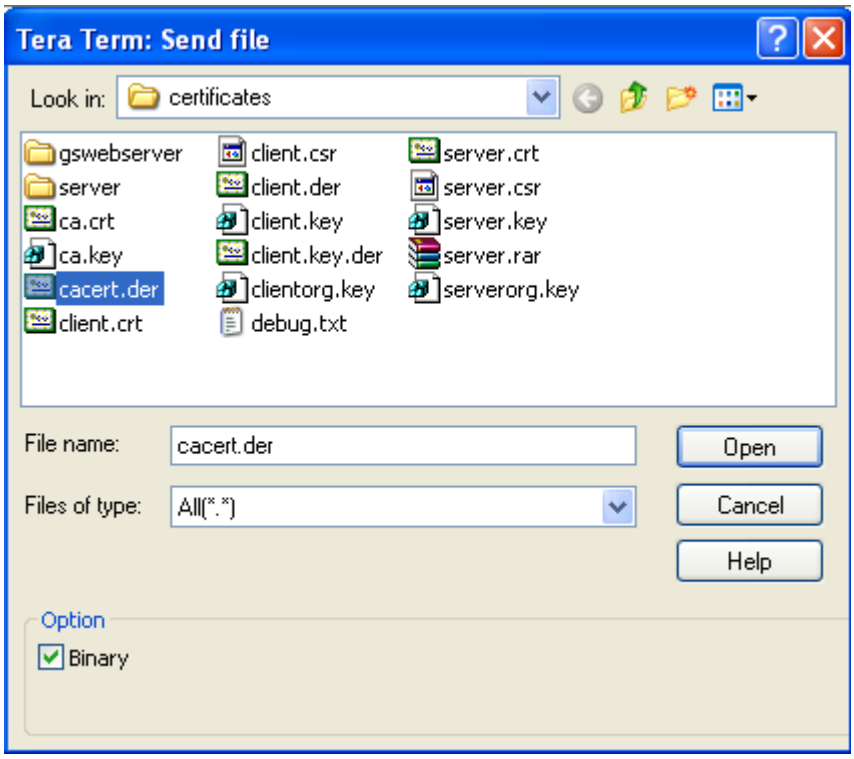


2.3 HTTPS GET Example

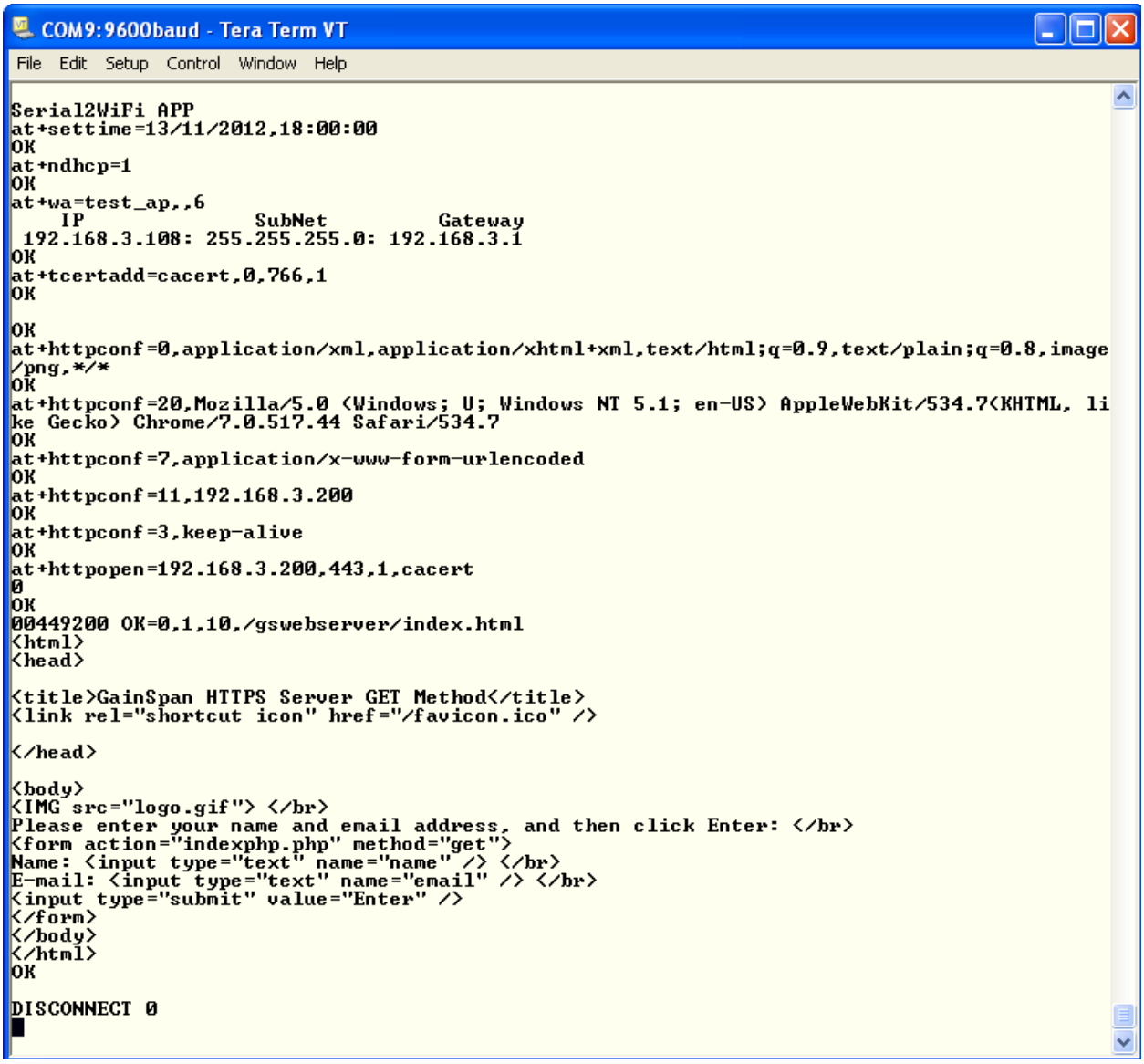
To have a secured apache server you need to put 'server.crt' in /xampp/apache/conf/ssl.crt and the 'server.key' in /xampp/apache/conf/ssl.key. Make sure that the 'httpd-ssl.conf' configuration file located in /xampp/apache/conf/extra is configured to allow SSL connection (SSL Engine should be On).

1. Set the system time
   at+settime=13/11/2012,18:00:00
2. Associate with AP
   at+ndhcp=1
   at+wa=test_ap,,6
3. Configure the certificate for HTTPS connection.
   at+tcertadd=cacert,0,766,1
4. Add the certificate:
   - Enter the [ESC] key
   - Enter the [W] key

- If you are using Tera Term, click on “File” and then select “Send File”, and select the “cacert.der” file. Make sure you check the “Binary option”. Then click “open” to send the certificate.



5. Configure thte HTTP parameters:
   at+httpconf=0,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*
   at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7 (KHTML, like Gecko) Chrome/7.0.517.44 Safari/534.7
   at+httpconf=7,application/x-www-form-urlencoded
   at+httpconf=11,192.168.3.200
   at+httpconf=3,keep-alive
6. Initiate HTTP client connection to the server
   at+httpopen=192.168.3.200,443,1, cacert
7. Do HTTP GET
   at+httpsend=0,1,10,/gswebserver/index.html



2.4 HTTPS POST Example

1. Set the system time
   at+settime=13/11/2012,18:00:00
2. Associate with AP
   at+ndhcp=1
   at+wa=test_ap,,6
3. Configure the certificate for HTTPS connection.
   at+tcertadd=cacert,0,766,1
4. Add the certificate:
   - Enter the [ESC] key
   - Enter the [W] key

- If you are using Tera Term, click on “File” and then select “Send File”, and select the “cacert.der” file. Make sure you check the “Binary option”. Then click “open” to send the certificate.

5. Configure thte HTTP parameters:

   at+httpconf=10,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*
   at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7 (KHTML, like Gecko) Chrome/7.0.517.44 Safari/534.7
   at+httpconf=7,application/x-www-form-urlencoded
   at+httpconf=11,192.168.3.200
   at+httpconf=3,keep-alive

6. Initiate HTTP client connection to the server

   at+httpopen=192.168.3.200,443,1,cacert

7. Do HTTP POST

   at+httpsend=0,3,10,/gswebserver/post.html,5

   - Enter the [ESC] key
   - Enter the [H] key
   - Enter the CID
   - Enter the text you want to POST.

COM9:9600baud - Tera Term VT

File Edit Setup Control Window Help

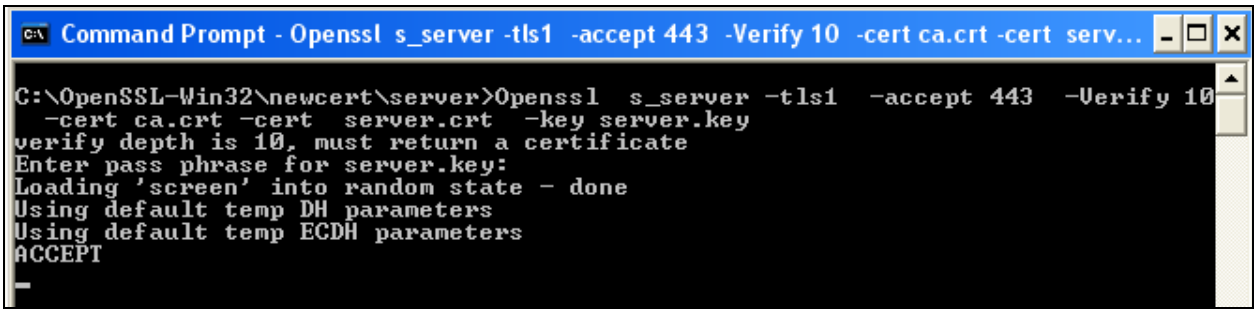
```
Serial2WiFi APP
at+settime=13/11/2012,18:00:00
OK
at+ndhcp=1
OK
at+wa=test_ap,,6
    IP              SubNet          Gateway
 192.168.3.108: 255.255.255.0: 192.168.3.1
OK
at+tcertadd=cacert,0,766,1
OK

OK
at+httpconf=0,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image
/png,*/*
OK
at+httpconf=20,Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7(KHTML, li
ke Gecko) Chrome/7.0.517.44 Safari/534.7
OK
at+httpconf=7,application/x-www-form-urlencoded
OK
at+httpconf=11,192.168.3.200
OK
at+httpconf=3,keep-alive
OK
at+httpopen=192.168.3.200,443,1,cacert
0
OK
at+httpsend=0,1,10,/gswebserver/post.html,5
OK
00383200 OK
<html>
<head>

<title>GainSpan HTTPS Server POST Method</title>
<link rel="shortcut icon" href="/favicon.ico" />

</head>

<body>
<IMG src="logo.gif"> </br>
Please enter your name and then click Enter: </br>
<form action="postphp.php" method="post">
Name: <input type="text" name="name" /> </br>
<input type="submit" value="Enter" />
</form>

</body>
</html>
OK

DISCONNECT 0
```

2.5 Using SSLOPEN Command

2.5.1 Starting a SSL Server

$ openssl s_server -cert server.crt -key server.key -CAfile cacert.der -verify 10 -accept 443

NOTE: 'server.crt' is the server certificate, 'server.key is the server key and 'cacert' is the CA certificate



2.5.2 Configuring GS Node as HTTPs Client (One-way Authentication)

1. Load CA Certificate: *AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>*

   at+tcertadd=cacert,0,760,1

   Enter the [ESC] key

   Enter the [W] key

   On Tera Term, click on "File" and then select "Send File", and select the "cacert.der" file, With "Binary option" checked. Then click "open" to send the certificate.

3. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

   at+settime=12/03/2012,18:00:00

4. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

   at+ndhcp=1

5. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*

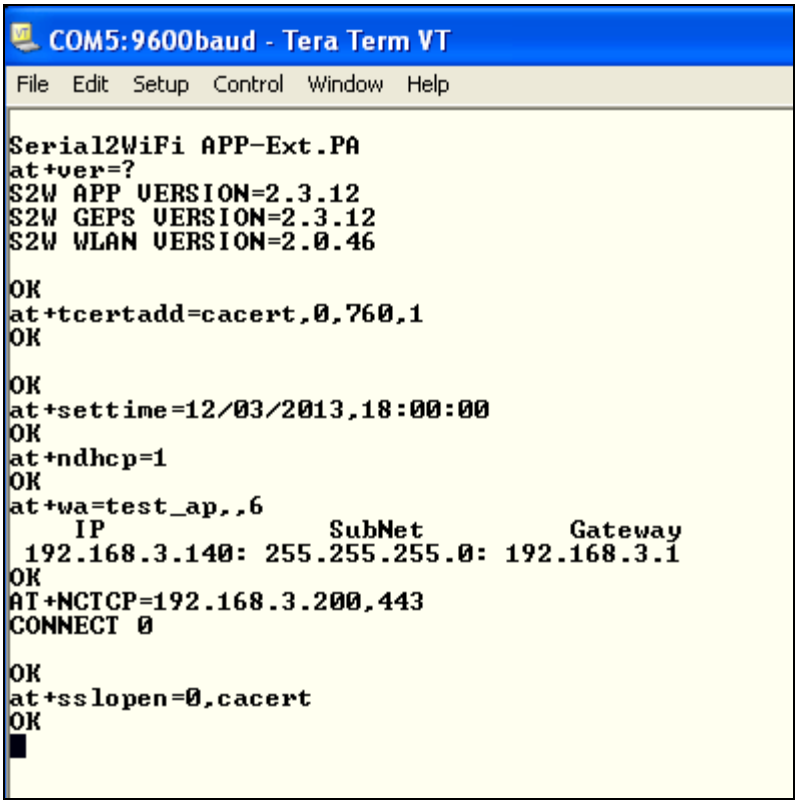
   at+wa=test_ap,,6

6. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[<,Src.Port>]*

   at+nctcp=192.168.3.200,443

7. Open a SSL Connection: *AT+SSLOPEN=<CID>,[<CA certificate name>]*

   at+sslopen=0,cacert



2.5.3 Configuring GS Node as HTTPs Client (Mutual Authentication)

Two way-authentication is supported only in GEPS 2.4.x and GEPS 3.4.x versions and newer.

1. Load CA Certificate: *AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>*

   at+tcertadd=cacert,0,868,1

   Enter the [ESC] key

   Enter the [W] key

   On Tera Term, click on "File" and then select "Send File", and select the "cacert.der" file, With "Binary option" checked. Then click "open" to send the certificate.

2. Load Client Certificate: *AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>*

   at+tcertadd=clientcert,0,621,1

   Enter the [ESC] key

Enter the [W] key

On Tera Term, click on “File” and then select “Send File”, and select the “client.der” file, With “Binary option” checked. Then click “open” to send the certificate.

3. Load Client Key: *AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>*

   at+tcertadd=at+tcertadd=clientkey,0,607,1

   Enter the [ESC] key

   Enter the [W] key

   On Tera Term, click on “File” and then select “Send File”, and select the “client.key.der” file, With “Binary option” checked. Then click “open” to send the certificate.

3. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

   at+settime=15/11/2012,10:15:00

4. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

   at+ndhcp=1

5. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*

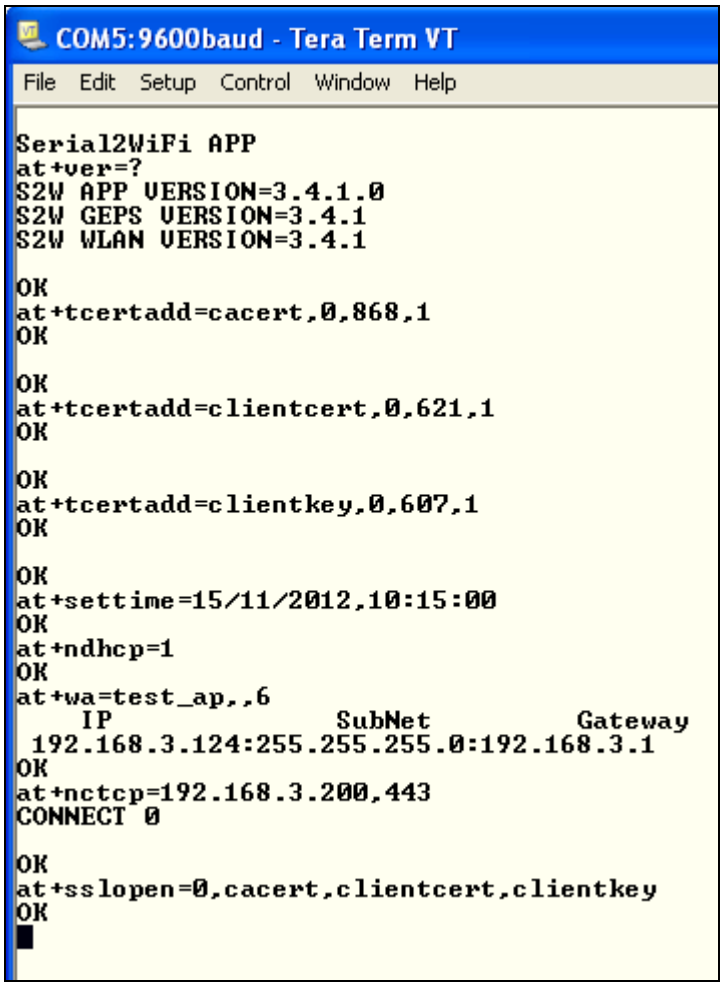
   at+wa=test_ap,,6

6. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[<,Src.Port>]*

   at+nctcp=192.168.3.200,443

7. Open a SSL Connection: *AT+SSLOPEN=<CID>,[<CA certificate name>,Client Certificate>, <Client Key>]*

   at+sslopen=0,cacert,clientcert,clientkey



2.5.4 HTTPs POST using AT+SSLOPEN Command

1. Load CA Certificate: *AT+TCERTADD=<Name>,<Format>,<Size>,<Location><ESC>W <data of size above>*

   at+tcertadd=cacert,0,868,1

   Enter the [ESC] key

   Enter the [W] key

   On Tera Term, click on "File" and then select "Send File", and select the "cacert.der" file, With "Binary option" checked. Then click "open" to send the certificate.

2. Set System Time: *AT+SETTIME=[<dd/mm/yyyy>,<HH:MM:SS>]*

   at+settime=19/03/2013,18:00:00

3. Enable DHCP: *AT+NDHCP=<disable=0/enable=1>*

   at+ndhcp=1

4. Associate to an access point: *AT+WA=<SSID>[,[<BSSID>][,<Ch>]]*

   at+wa=test_ap,,6

5. Start a TCP server: *AT+NCTCP=<Dest-Address>,<Port>>[<,Src.Port>]*

   at+nctcp=192.168.3.200,443

6. Open a SSL Connection: *AT+SSLOPEN=<CID>,[<CA certificate name>,Client Certificate>, <Client Key>]*

   at+sslopen=0,cacert

7. Send data to remote server by using the <ESC>S sequence and the CID number:

   Enter the [ESC] key
   Enter the [S] key
   Enter the [CID number from step 5]

8. Copy the highlighted text, and paste it on TeraTerm (via the "Edit" menu, choose "Paste" Option)

   POST /gswebserver/post.html HTTP/1.1
   User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7(KHTML, like Gecko) Chrome/7.0.517.44 Safari/534.7
   Content-Type: application/x-www-form-urlencoded
   Content-Length: 4
   Host: 192.168.3.200
   Connection: keep-alive

   John

9.. Indicate end of transmission by using the <ESC>E sequence

   Enter the [ESC] key
   Enter the [E] key

```
COM5:9600baud - Tera Term VT
File  Edit  Setup  Control  Window  Help

Serial2WiFi APP
at+ver=??
S2W APP VERSION=3.4.1.0
S2W GEPS VERSION=3.4.1
S2W WLAN VERSION=3.4.1
S2W BIN TYPE=WEB PROV APP WITH OTAFU ADK
S2W RELEASE TYPE=GA
BUILD TIME=15:11:50
BUILD DATE=Jul  4 2012
WLAN EXT VERSION=7
OK
at+tcertadd=cacert,0,868,1
OK

OK
at+settime=19/03/2013,18:00:00
OK
at+ndhcp=1
OK
at+wa=test_ap,,6
    IP              SubNet          Gateway
 192.168.3.120:255.255.255.0:192.168.3.1
OK
at+nctcp=192.168.3.200,443
CONNECT 0

OK
at+sslopen=0,cacert
OK
```

Over the air capture showing HTTP POST message.

```
⊟ Hypertext Transfer Protocol
  ⊞ POST /gswebserver/post.html HTTP/1.1\r
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/534.7(KHTML, like Gecko) Chrome/7.0.517.44 Safari/534.7\r
    Content-Type: application/x-www-form-urlencoded\r
    Content-Length: 4
    Host: 192.168.3.200\r
    Connection: keep-alive\r
    \r
⊟ Line-based text data: application/x-www-form-urlencoded
    John
```

3 EAP Examples

In order to support EAP associations, user must program the Serial to WiFi "Enterprise Security (EAP)" application firmware onto the Gainspan module. The EAP firmware can be found in the official Gainspan software EVK release, or customer can build it using the Gainspan SDK-Builder tool.

3.1 PEAP Without Certificate

The example shown in this section is demonstrated with the following authentication server and EAP method:

Outer Authentication: PEAP V0 (25)

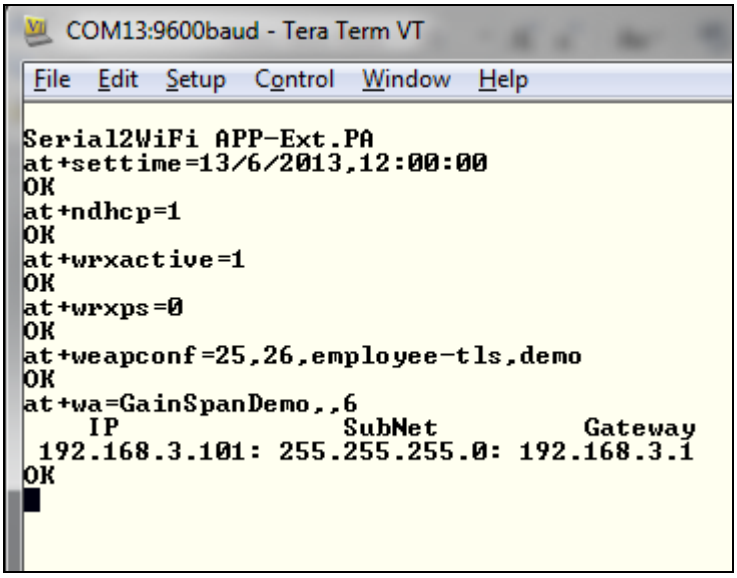
Inner Authentication: MSCHAP V2 (26)

Authentication Server: Free Radius Demo v2.2.3 by Enterasys Networks

The following AT command sequence are used:

1. at+settime=13/6/2013,12:00:00
2. at+ndhcp=1
3. at+wrxactive=1
4. at+wrxps=0
5. at+weapconf=25,26,employee-tls,demo
6. at+wa=GainSpanDemo,,6

Below is a screen capture of the above AT commands executed in a Tera Terminal:



Below is an over the air wireless capture showing the Key Exchange frame sequence:

No.	Time	Source	Destination	Protocol	Info
17181	28.084278	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
17190	28.095023	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
17191	28.095268		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
17206	28.110519	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
17223	28.127392	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
17224	28.127644		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
17229	28.144019	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Server Hello Done
18293	29.876563	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
18294	29.876934		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18316	29.913434	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
18325	29.932538	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
18326	29.932783		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18329	29.942685	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
18339	29.951302	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
18340	29.951675		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18345	29.960938	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
18360	29.980570	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
18361	29.980936		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18363	29.990325	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
18373	29.998809	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
18374	29.999182		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18379	30.009933	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
18386	30.016059	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
18387	30.016310		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
18396	30.031421	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Success
18402	30.033809	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key

```
⊞ Frame 18293 (394 bytes on wire, 394 bytes captured)
⊞ Radiotap Header v0, Length 20
⊞ IEEE 802.11 QoS Data, Flags: .......TC
⊞ Logical-Link Control
⊞ 802.1X Authentication
```

3.2 PEAP With Certificate

The example shown in this section is demonstrated with the following authentication server and EAP method with certificate:

Outer Authentication: PEAP V0 (25)

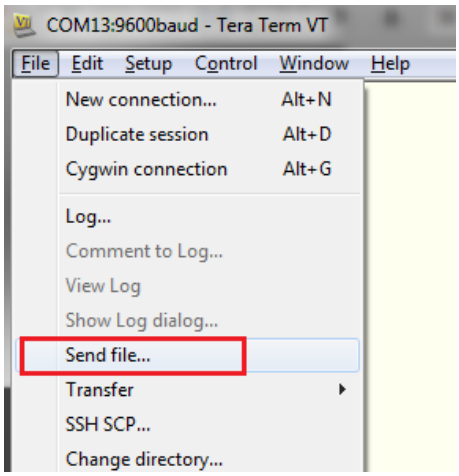
Inner Authentication: MSCHAP V2 (26)

Authentication Server: Free Radius Demo v2.2.3 by Enterasys Networks

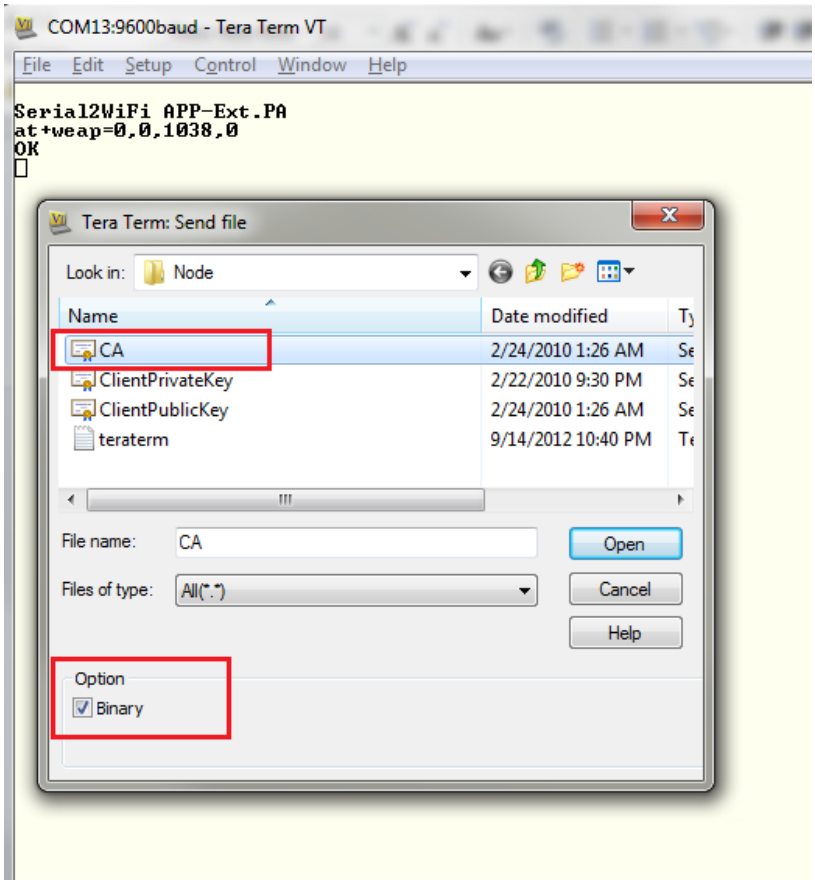
Certificate Format: DER

The following AT command sequence are used:

1. at+weap=0,0,1038,0
2. Now, load the CA certificate into the Gainspan module. If you are using Tera Term, please add the certificate by doing the following steps:
   - Enter the [ESC] key
   - Enter the [shift W] key
   - On Tera Term, click on “File” and then select “Send File”:

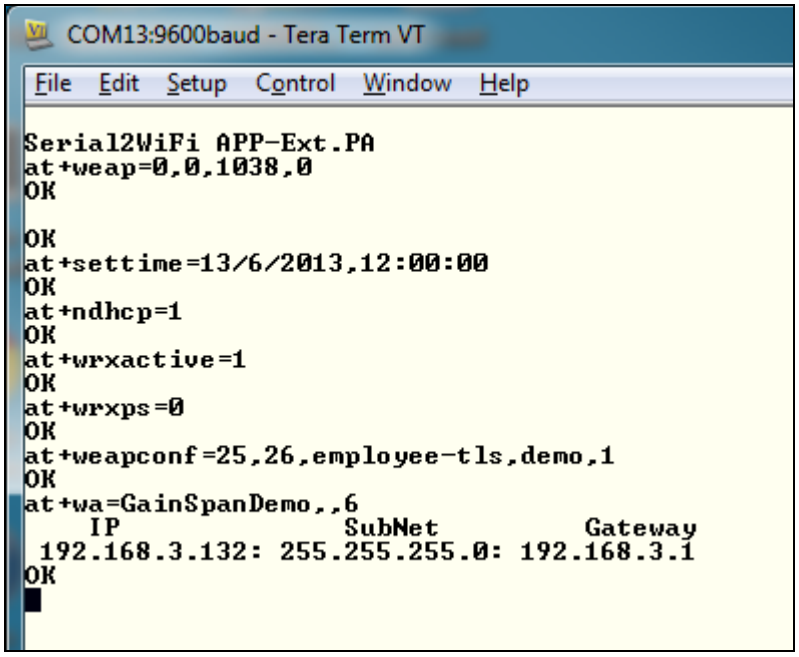


- Select the CA file. Make sure "Binary option" is checked. Then click "open" to add the certificate to the Gainspan module.



3. at+settime=13/6/2013,12:00:00
4. at+ndhcp=1
5. at+wrxactive=1
6. at+wrxps=0
7. at+weapconf=25,26,employee-tls,demo,1
8. at+wa=GainSpanDemo,,6

Below is a screen capture of the above AT commands executed in a Tera Terminal:



Below is an over the air wireless capture showing the Key Exchange frame sequence:

No.	Time	Source	Destination	Protocol	Info
58201	91.983076	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	SSL	Client Hello
58202	91.983448		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
58215	92.002825	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
58232	92.015059	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
58233	92.015314		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
58235	92.031576	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, PEAP [Palekar]
58248	92.041319		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
58267	92.054944	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Server Hello Done
59665	94.328452	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
59666	94.328797		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
59683	94.360674	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
59694	94.380180	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59695	94.380556		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
59699	94.391297	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59710	94.399679	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59711	94.400048		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
59722	94.417930	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59743	94.444150	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59744	94.444418		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
59750	94.451276	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59758	94.459773	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Application Data
59759	94.460166		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
59766	94.470776	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Application Data, Application Data
59770	94.476924	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59771	94.477653	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]
59772	94.478918	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, PEAP [Palekar]

```
⊞ Frame 59665 (394 bytes on wire, 394 bytes captured)
⊞ Radiotap Header v0, Length 20
⊞ IEEE 802.11 QoS Data, Flags: .......TC
⊞ Logical-Link Control
⊞ 802.1X Authentication
```

3.3 EAP-TLS

The example shown in this section is demonstrated with the following authentication server and EAP method with certificates:

Outer Authentication: EAP-TLS (13)

Inner Authentication: MSCHAP V2 (26)

Authentication Server: Free Radius Demo v2.2.3 by Enterasys Networks

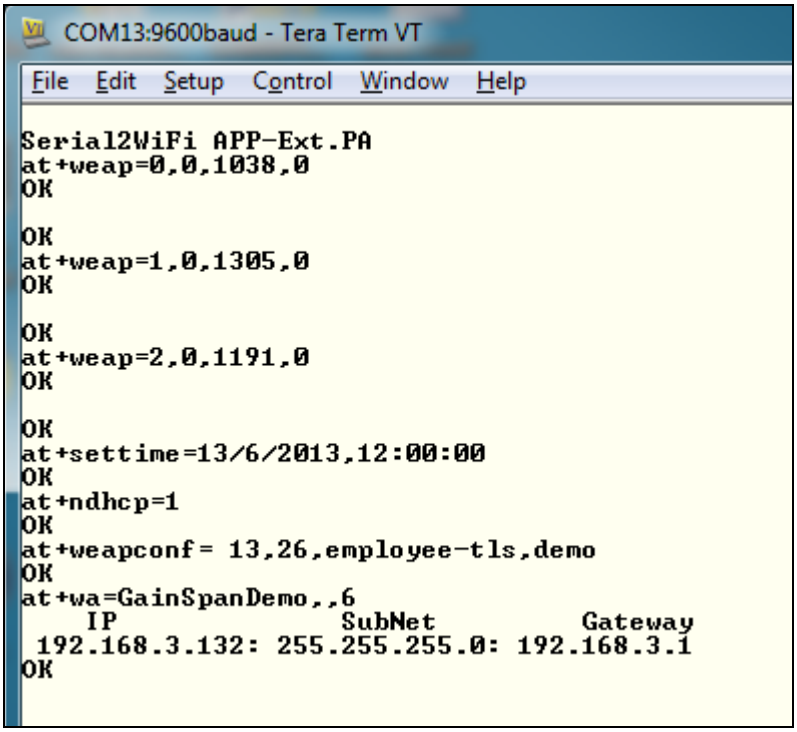
Certificate Format: DER

The following AT command sequence are used:

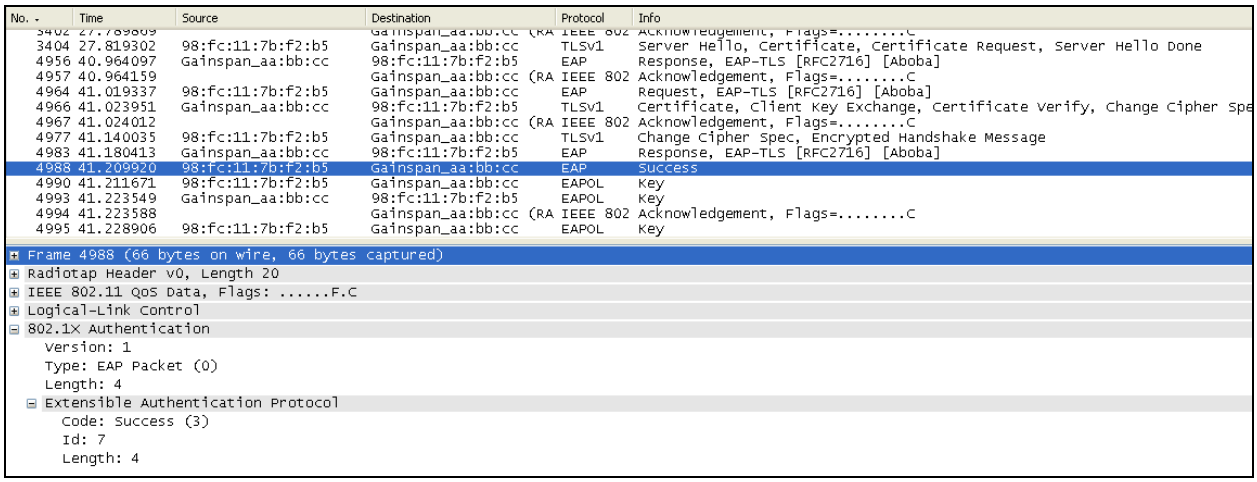
1. at+weap=0,0,1038,0
2. Now, load the **CA certificate** into the Gainspan module. Please refer to example in section 3.2 on how to load the certificate using Tera Term.
3. at+weap=1,0,1305,0
4. Now, load the **client certificate** into the Gainspan module. Please refer to example in section 3.2 on how to load the certificate using Tera Term.
5. at+weap=2,0,1191,0
6. Now, load the **client private key** into the Gainspan module. Please refer to example in section 3.2 on how to load the key using Tera Term.

7. at+settime=02/01/2013,06:38:00
8. at+ndhcp=1
9. at+weapconf= 13,26,employee-tls,demo
10. at+wa=test_ap,,6

Below is a screen capture of the above AT commands executed in a Tera Terminal:



Below is an over the air wireless capture showing the Key Exchange frame sequence:

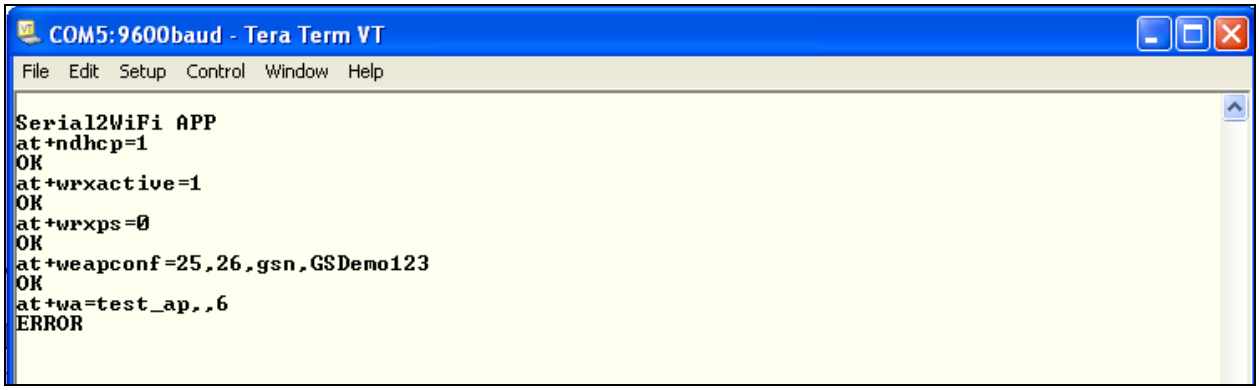


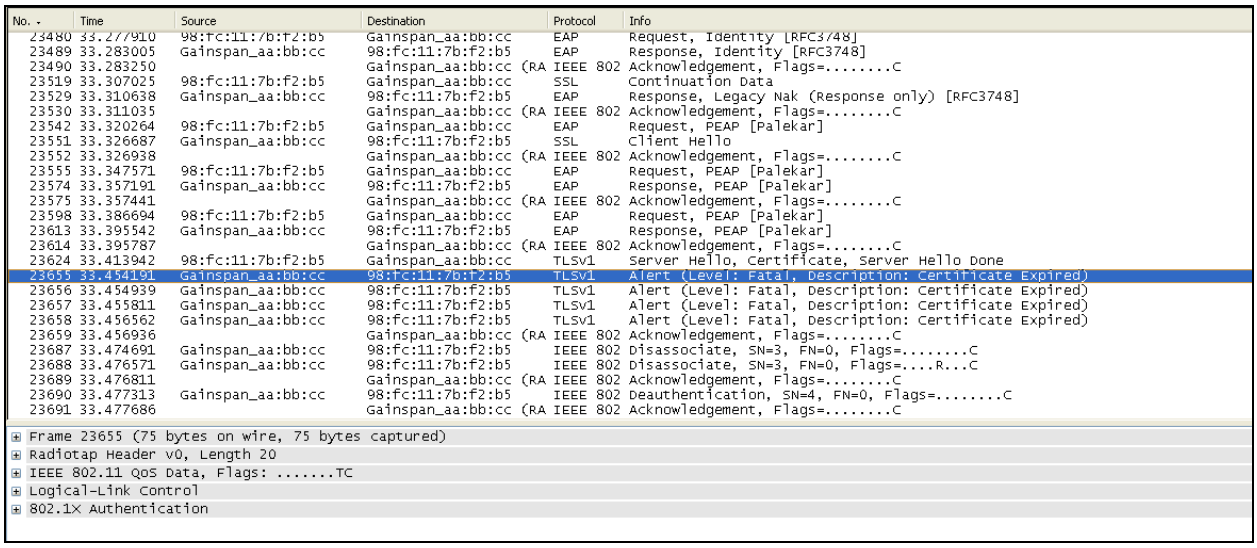
No.	Time	Source	Destination	Protocol	Info
3402	27.789809		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
3404	27.819302	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Server Hello, Certificate, Certificate Request, Server Hello Done
4956	40.964097	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, EAP-TLS [RFC2716] [Aboba]
4957	40.964159		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
4964	41.019337	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Request, EAP-TLS [RFC2716] [Aboba]
4966	41.023951	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	TLSv1	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spe
4967	41.024012		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
4977	41.140035	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	TLSv1	Change Cipher Spec, Encrypted Handshake Message
4983	41.180413	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAP	Response, EAP-TLS [RFC2716] [Aboba]
4988	41.209920	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAP	Success
4990	41.211671	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key
4993	41.223549	Gainspan_aa:bb:cc	98:fc:11:7b:f2:b5	EAPOL	Key
4994	41.223588		Gainspan_aa:bb:cc (RA	IEEE 802	Acknowledgement, Flags=.....C
4995	41.228906	98:fc:11:7b:f2:b5	Gainspan_aa:bb:cc	EAPOL	Key

```
⊞ Frame 4988 (66 bytes on wire, 66 bytes captured)
⊞ Radiotap Header v0, Length 20
⊞ IEEE 802.11 QoS Data, Flags: ......F.C
⊞ Logical-Link Control
⊟ 802.1X Authentication
    Version: 1
    Type: EAP Packet (0)
    Length: 4
  ⊟ Extensible Authentication Protocol
      Code: Success (3)
      Id: 7
      Length: 4
```

4 Troubleshooting

If you don't do a "SETTIME", you will see the following failures in the authentication process:





Make sure you issue the "AT+GETTIME" command to verify if the date and time on the module does not lie outside the expiration period of the certificate .

If the date and time is not within the expiration period issue the "AT+SETTIME" commands. Then issue the rest of the commands as shown in the examples.

5 Additional References

Serial to Wi-Fi Evaluation Kit Startup Guide.pdf

Serial to WiFi_Adapter_Guide.pdf

Detail description of the AT commands supported

Serial to WiFi_Command_Reference.pdf

List of the various AT commands supported

Serial to Provisioning Methods with S2W App Note AN039.pdf

Example of provisioning method supported as well as the steps necessary to connect to the infrastructure (i.e. Access Point) using either Web Based Provisioning or Wi-Fi Protected Setup (WPS).

Serial to WiFi Bridge App Note AN025.pdf

The GainSpan Ultra-Low-Power Wi-Fi System-On-Chip may be used as a transparent bridge to carry serial (UART) traffic over an 802.11 wireless link. Serial commands are used to manage the wireless network configuration. This application note will give the details necessary to setup this bridge.

Version	Date	Remarks
1.5	16-August-2013	EAP-TLS examples added with steps for certificate loading

GainSpan Corporation • +1 (408) 673-2900 • info@GainSpan.com • www.GainSpan.com

SP- 1.5