SSL Certification Installation on WAMP Server

Implementation of PFX certificate on WAMP server (Our Case) :

WAMP Apache on Windows does not support .pfx certificates. The Apache server will require the following two files:

1 **- server.key** : the private key associated with the certificate
2 - **server.crt** : the public SSL certificate issued by Entrust

Install openssl from following website :

- http://slproweb.com/products/Win32OpenSSL.html

With openssl you can convert pfx to Apache compatible format with next commands:

```
openssl pkcs12 -in domain.pfx -clcerts -nokeys -out domain.cer
openssl pkcs12 -in domain.pfx -nocerts -nodes  -out domain.key
```

First command extracts public key to domain.cer.
Second command extracts private key to domain.key.

Update your Apache configuration file with:

```
<VirtualHost 192.168.0.1:443>
 ...
 SSLEngine on
 SSLCertificateFile /path/to/domain.cer
 SSLCertificateKeyFile /path/to/domain.key
 ...
</VirtualHost>
```

Ensure SSL is Enabled
Make sure that Apache is setup to even use SSL.
Do this by clicking the WAMP icon in your tray,
hovering to: Apache > Apache Modules,
scroll through the list and make sure that ssl_module has a check next to it.
If not, then click it.

TEST HTTPS

Run **httpd –t** and make sure the syntax is OK.

Restart Apache.

Check that port 443 is open by running the following in the command prompt:

```
netstat -an | more
```

Test the https connection from your web browser.

General Case – Installing SSL certificate on WAMP Server :

Step 1 : Create SSL Certificate and Key

1a) Open the DOS command window and change directory to bin directory of wamp apache directory by using the DOS command without quotes: "cd /d c:\" and then "cd wamp\bin\apache\apache2.2.8\bin". apache2.2.8 should be changed to what apache folder your wamp server has.

After done, the DOS prompt should look like: **C:\wamp\bin\apache\apache2.2.8\bin**>

1b) Create a server private key with 1024 bits encryption. You should enter this command without quotes:
"**openssl genrsa -des3 -out server.key 1024**". It'll ask you a pass phrase (password), just enter any password you like '
1c) Remove the pass phrase from the RSA private key (while keeping a backup copy of the original file). Enter this command without quotes: "copy server.key server.key.org" and then "openssl rsa -in server.key.org -out server.key". It'll ask you the pass phrase, just type it.

1d) Create a self-signed Certificate (X509 structure) with the RSA key you just created. Enter the command without quotes: "**openssl req -new -x509 -nodes -sha1 -days 365 -key server.key -out server.crt -config C:\wamp\bin\apache\apache2.2.8\conf\openssl.cnf**".

You might combine step1b, 1c and 1d into one step by using this command, no quotes:
"**openssl req -new -x509 -nodes -out server.crt -keyout server.key**" if you have trouble following through.

You'll fill in the information after entering this command. The correct location of config file, openssl.cnf may need to be changed. In windows, you won't see ".cnf" extension of the file openssl, but in DOS you'll see the full name openssl.cnf.

1e) Create a real SSL server certifcate (Optional): if you don't want step 1a to 1d
A. Create a server RSA private key for your Apache server (**Triple-DES encrypted and PEM formatted**):
Type command: **openssl genrsa -des3 -out server.key 1024**

You might keep the backup of server private key in a maximum secure place and guard it well (e.g your digital wallet).

B. Create a Certificate Signing Request (CSR) for public (output will be PEM formatted). A CSR is a file containing your certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the webform in the enrollment process at your certificate authority website:
Type the command: **openssl req -new -key server.key -out server.csr**

You will now be asked to enter details to be entered into your CSR. What you are about to enter is what is called a Distinguished Name or a DN. For some fields there will be a default value, If you enter '.', the field will be left blank. Use the name of the webserver as Common Name (CN). If the domain name (Common Name) is mydomain.com append the domain to the hostname (use the fully qualified domain name).

Depending on a specific certifying authority (CA) you might have to enter the details as specified by them. Normally, the CA authority will provide specific instructions for you.

C. Now all you have to do is sending this Certificate Signing Request (CSR) to a Certifying Authority (CA) to be signed. A trusted CA means all major web browsers recognize it without giving you a warning when you install your CA-signed SSL certificate on your webserver. Once the CSR has been signed, you will have a REAL Certificate, which can be used by Apache. You can have a CSR signed by a commercial CA (fees are required). Then they will send you the signed certificate which you can store in a server.crt file.

D. Once, your CSR certificate has been signed and returned to you, you can view the details by using this command: **openssl x509 -noout -text -in server.crt**

Step 2 : Copy the server.key and server.crt files.

2a) In the conf folder of apache2.2.8 folder, create two folders named as ssl.key and ssl.crt

2b) copy the server.key file to ssl.key folder and server.crt file to ssl.crt

Step 3 : Edit the httpd.conf file and php.ini

3a) In httpd.conf file, remove the comment '#' at the line which says:

LoadModule ssl_module modules/mod_ssl.so

3b) In httpd.conf, remove the comment '#' at the line which says:

Include conf/extra/httpd_ssl.conf
Then move that line after this block **<IfModule ssl_module>.... </IfModule>**

3c) open the php.ini file located in apache2.2....\bin folder, remove the comment ';' at the line which says:

extension=php_openssl.dll

Step 4 : Edit the httpd_ssl.conf file in the folder name, extra

4a) Find the line which says "**SSLMutex** ...." and change it to "SSLMutex default" without quotes

4b) Find the line which says**:**

<VirtualHost _default_:443>.

Right after it, change the line which says

"**DocumentRoot** ..." to **DocumentRoot "C:/wamp/www/"** with quotes.

Change the line ServerName localhost:443

Change the line "**ErrorLog...."** to Errorlog **logs/sslerror_log**.

Change the line "**TransferLog** ...." to **TransferLog logs/sslaccess_log**

4c) SSL crt file: Change the line "**SSLCertificateFile** ...." to **SSLCertificateFile "conf/ssl.crt/server.crt"**

4d) SSL key file: Change the line "**SSLCertificateKeyFile** ...." to **SSLCertificateKeyFile "conf/ssl.key/server.key"**

4e) Change the line which says

<Directory "C:/Program Files/Apache Software Foundation/Apache2.2/cgi-bin"> or something similar to **<Directory "C:/wamp/www/">** and add the following lines inside those **<Directory ... >...</Directory>** tags:

Options Indexes FollowSymLinks MultiViews
AllowOverride All
Order allow,deny
allow from all

4f) Make sure the **line CustomLog "logs/ssl_request_log" **
is uncommented (remove the #). This step is suggested by wmorse1.

Step 5 : In the previous DOS Command windows, enter httpd -t . If it displays Sysntax is OK, then go to Step 6. If not, then correct the wrong syntax and redo step 5.

Step 6 : Restart the Apache server

Step 7 : if restart is successful, then open the browser and enter "[localhost"]; without quotes.

Step 8 (Optional) :

If you want to allow world wide web access to your HTTPS secure server, then in the httpd_ssl.conf file, change the line which says 'ServerName localhost:443' to '**ServerName** www.maharashtra.gov.in:443' without quotes. yourwebsitename is your registered internet domain name. If you don't have it, then just use your WAN IP address. For example '**ServerName 10.208.11.x:443**'. Make sure these setups are correct to allow outside access to secured www server.

8.a The DocumentRoot you modified in step 4b points to the correct website folder on your computer.

8.b If your computer's connected to the router, setup the router to allow port 443 forwarding to your computer.

8.c If your computer has a firewall enabled or behind a network firewall, set up the firewall to allow incoming port 443 connection.