# Asymmetric (Public/Private Key) Encryption

**OpenSSL Tutorial**:

<http://i.amniels.com/mysql-database-encryption-using-public-private-keys#comments>

**Download OpenSSL** - <http://www.php.net/manual/en/openssl.setup.php>

**Direct link** - <http://gnuwin32.sourceforge.net/packages/openssl.htm>

**WAMP & OpenSSL Configuration:**

<http://www.phpjoel.com/2011/04/07/installing-ssl-using-openssl-on-a-wamp-localhost/>

**Original:** <http://forum.wampserver.com/read.php?2,28731,page=1>

**How to Create a Certificate Signing Request on the CSS SCA:**

<http://www.cisco.com/en/US/products/hw/contnetw/ps2083/products_tech_note09186a0080094b2d.shtml>

**Wamp2 HTTPS and SSL Setup Step-by-Step guide:**

<http://forum.wampserver.com/read.php?2,32986,page=1>

# HTTPS SSL on WAMPServer2

Based on Guide from: <http://guides.jlbn.net/setssl/setssl1.html>

## What You Need

* [WampServer](http://www.wampserver.com/en/) version 2.2D (Tutorial based off of Apache 2.2.21)
* A web-browser ([Firefox](http://www.mozilla.org/en-US/firefox/new/), [Chrome](https://www.google.com/chrome), [Opera](http://www.opera.com/))
* A text-editor ([Notepad++](http://notepad-plus-plus.org/download/v6.1.1.html), [Crimson Editor](http://www.crimsoneditor.com/), [Programmer’s Notepad](http://www.pnotepad.org/download/))

## Steps

1. Open Command Prompt
2. Navigate to the binary folder located in the Apache folder in WAMP

***cd C:\wamp\bin\apache\apache2.2.21\bin***

1. Generate an 256 bit AES passkey

***openssl genrsa -aes256 -out pass.key 2048***

1. Enter a passphrase it will be used in step #7
2. Verify passphrase
3. Create key for server

**openssl rsa -in pass.key -out server.key**

1. Enter passphrase from step #4
2. Create self-signed SSL certificate

***openssl req -new -x509 -nodes -sha1 -key server.key -out server.crt -days 365 -config C:\wamp\bin\apache\apache2.2.21\conf\openssl.cnf***

1. Fill out the certificate
2. Create a new folder called “ssl” in the Apache configuration folder

***cd C:\wamp\bin\apache\apache2.2.21\conf***

***mkdir ssl***

1. Copy the key: *server.key* and certificate: *server.crt* to the new location

***cd C:\wamp\bin\apache\apache2.2.21\bin***

***copy server.crt C:\wamp\bin\apache\apache2.2.21\conf\ssl***

***copy server.key C:\wamp\bin\apache\apache2.2.21\conf\ssl***

1. Create a new folder called “logs” in the new ssl folder

***cd C:\wamp\bin\apache\apache2.2.21\conf\ssl***

***mkdir logs***

1. Go to the extra folder in the Apache configuration folder and open *httpd-ssl.conf*

***cd C:\wamp\bin\apache\apache2.2.21\conf\extra***

1. Replace line 62 with this (this is all on 1 line)

***SSLSessionCache "shmcb:C:/wamp/bin/apache/Apache2.2.21/conf/ssl/logs/ssl\_scache(512000)"***

1. Replace line 99 with this

***SSLCertificateFile "C:/wamp/bin/apache/Apache2.2.21/conf/ssl/server.crt"***

1. Replace line 107 with this

***SSLCertificateKeyFile "C:/wamp/bin/apache/Apache2.2.21/conf/ssl/server.key"***

1. Replace line 68 with this (if not already)

***SSLMutex default***

1. Replace lines 77-81 with these lines

***DocumentRoot "C:/wamp/www”***

***ServerName localhost:443***

***ServerAdmin admin@localhost***

***ErrorLog "C:/wamp/bin/apache/Apache2.2.21/conf/ssl/logs/ssl\_error.log"***

***TransferLog "C:/wamp/bin/apache/Apache2.2.21/conf/ssl/logs/ssl\_access.log"***

1. On line 193 replace the Directory with

***<Directory "C:/wamp/www">***

***SSLOptions +StdEnvVars***

***Options Indexes FollowSymLinks MultiViews***

***AllowOverride All***

***Order allow,deny***

***allow from all***

***</Directory>***

1. Replace line 232 (used to be line 228 before step 19) with this

***CustomLog "C:/wamp/logs/ssl\_request.log" \***

1. Go back a directory or use this and open *httpd.conf*

***cd C:\wamp\bin\apache\apache2.2.21\conf***

1. On line 479 uncomment (remove the #) this statement

***Include conf/extra/httpd-ssl.conf***

1. Left-click the WAMP tray icon and check off the ssl module (WAMP may stop working, if this happens you can download my *httpd-ssl.conf* file upon request)

***Apache > Apache modules > ssl\_module***

1. Click on WAMP again but this time enable php openssl

***PHP > PHP extensions > php\_openssl***

1. Copy these 2 libraries into the System32 folder (Make sure you are running Command prompt as Administrator)

***cd C:\wamp\bin\apache\apache2.2.21\bin***

***copy libeay32.dll C:\windows\System32***

***copy ssleay32.dll C:\windows\System32***

1. Create a test file called *index.php* in your www folder or WAMP and open a web-browser.
2. Type the following URL in the web browser

https://localhost

1. You will get a warning, just click the following (Based on Firfox)

**Add Exception**

**Get Certificate**

**Confirm Security Exception**

1. You are done! You've just finished setup HTTPS SSL on WAMP, and much better, you can obtain a free SSL certificate through these <http://www.cacert.org> or <http://cert.startcom.org>

After SSL is set up you can use this tutorial: [MySQL Database Encryption Using Public/Private Keys](http://i.amniels.com/mysql-database-encryption-using-public-private-keys) for asymmetric encryption in PHP