# Securing Your Apache Web Server With a Thawte Digital Certificate

## Contents



## 1. Overview

In this document you’ll find out how to purchase, install and use a Thawte SSL digital certificate on your Apache web server. We will also touch on the role of Thawte as a trusted third party.

## 2. Research

The latest Web Server Survey released by E-Soft [www.securityspace.com] reveals that the most popular web server in use today is the Apache Server. Apache serves over 56% of the market. Trailing the Apache server are the Microsoft, Netscape, WebSite, WebStar, and Zeus web servers. For more detailed information on this survey please see: http://www.securityspace.com/s_survey/data/200006/index.html

Thawte SSL certificates and SuperCerts are compatible with all of the above browsers.

## 3. System requirements

Before you can install an SSL certificate on your Apache web server you must have installed the required SSL components. You will need to install OpenSSL, as well as either ModSSL or Apache-SSL. OpenSSL and its libraries provide the SSL back-end, while ModSSL or Apache-SSL provide the interface between Apache and OpenSSL. ModSSL and Apache-SSL are fairly similar. Thawte makes no recommendation between the two, and it’s up to you which one you choose.

Apache users should find the following web sites useful:

- **Apache** is available at www.apache.org
- **ModSSL** is available at www.modssl.org
- **Apache-SSL** is available at www.apache-ssl.org
- **OpenSSL** is available at www.openssl.org

## 4. Generate your Private Key

Use the "openssl" binary to generate your **private key**. This key will be kept on your web server so you may want to encrypt it. If you encrypt it, you should be aware that you would have to type in the pass-phrase for that key every time you restart your secure server. The private key can be generated with or without cryptographic protection as follows:

- **With encryption**:

  "openssl genrsa -des3 -rand /dev/urandom -out www.domain.com.key 1024"

- **Without encryption**:

  "openssl genrsa -rand /dev/urandom -out www.domain.com.key 1024"

If you get stuck, or need further options, please go to:

"openssl genrsa–help"

## 5. Generate your Certificate Signing Request

You'll need to send Thawte a CSR (Certificate Signing Request) before your certificate can be issued. To generate the CSR, use "openssl" and your private key as follows: "openssl req-new-key www.domain.com.key-out www.domain.com.csr".

This step creates a CSR that has the same "modulus" as the private key.

## 6. Using a test certificate

To familiarize yourself with the workings of a Thawte certificate on an Apache Server, you can set up a test certificate on your server using a self-signed certificate or a Thawte test certificate:

### 6.1. Self-signed test certificate

If you use a self-signed test certificate, your CSR will be signed by your own private key as follows: "openssl req -x509 -key www.domain.com.key -in www.domain.com.csr-out www.xxx.com.crt"

### 6.2. Thawte test certificate

You can get a Thawte test certificate online from Thawte at: https://www.thawte.com/cgi/server/test.exe. Test certificates are intended for you to test your server configuration before you buy a "trusted" certificate from a CA (Certificate Authority).

Paste in your CSR (Certificate Signing Request) into the test certificate request. Within minutes, you should receive an "un-trusted" test certificate via mail. Save the test certificate to a file called "www.domain.com.crt". You can get your

browser to “trust” that test certificate by clicking on http://www.thawte.com/servertest.crt and installing the Test Certificate CA root.

Before you can use the test certificate you will have to configure your Apache web server properly. To do this, edit the “httpd.conf” file so that the web server points to the private key and test certificate. To do this, you will use the “SSLCertificateKeyFile” and “SSLCertificateFile” directives. Enable SSL and make sure that the server is listening on port 443 with the "Listen 443" directive. Once you have done this, you can restart your server and connect to it on https://www.domain.com/

## 7. Request a “trusted” certificate

Thawte SSL certificates and SuperCerts are requested online from Thawte. During the certificate request process, you will be asked to copy and paste your CSR (Certificate Signing Request) into a text area on the online enrollment form. Please ensure that you are submitting the correct CSR, if you have generated more than one (you can check your CSR as follows: “openssl req–text–noout–in csrfilename.csr”).

You will have to provide all the requested information during the enrollment process, and send us documentation proving your, or your company’s, identity (a company registration certificate for instance). You can view detailed instructions for obtaining a Thawte SSL certificate at: https://www.thawte.com/certs/server/request.html

The enrollment process for SuperCerts is the same as for SSL certificates. However, during the process you will need to check the box that indicates that you would like a SuperCert. You will also have to generate a 1024-bit key, and make sure your Apache Server is 128-bit enabled.

Once you have completed the online request process, Thawte will take a number of steps to verify your identity and the other details you provided in the CSR. Thawte performs a considerable amount of background checking before it issues the certificate. As a result, it could take a few days to verify your company identity and details, and issue the certificate. During that period, you can track the progress of your request on your personal status page at http://www.thawte.com/cgi/server/status.exe

***SuperCerts*** *are SSL certificates that allow “international” browsers to “step-up” to 128-bit encryption. Internet Explorer 5.01, Netscape Communicator 4.7 and later browsers recognize Thawte’s SuperCerts. 128-bit encryption is regarded as being impossible to “crack”. For more information on SuperCerts please see: http://www.thawte.com/certs/server/128bit/contents.html*

## 8. Download your certificate

Once the certificate has been issued, you will be able to download it from your status page by clicking on the “Fetch Certificate” button (which only appears once the certificate has been issued).

## 9. Install your certificate

Once the certificate has been issued, you can install it by simply copying it and pasting it into a file on your server. The certificate is stored in Thawte’s database indefinitely, and can be downloaded again at any stage. For consistency, you should probably save it to a file called “www.domain.com.crt”.

If you generated a self-signed certificate or requested a test certificate earlier in the process and you configured your web server to use that test/self-signed certificate, then you do not need to make any changes to your configuration file. You can simply copy the real (“trusted”) certificate file over the test/self-signed certificate.

If you did not configure your server to look for the self-signed test certificate, then you'll need to update your “httpd.conf” file to look for the new certificate. Open the “httpd.conf” configuration file and make sure that you have the “SSLCertificateFile” and “SSLCertificateKeyFile” directives associated with the correct file paths. For example, if you have your certificate in the “/usr/local/ssl/certs/” directory and your private key in the “/usr/local/ssl/private/” directory, then you will have the following in your httpd.conf file:

- SSLCertificateFile /usr/local/ssl/certs/www.domain.com.crt
- SSLCertificateKeyFile /usr/local/ssl/private/www.domain.com.key

You will also need to make sure your Apache Server is listening on port 443 and "switch on" SSL with the "SSLEngine on" or SSLEnable directives in ModSSL or Apache-SSL respectively.

## 10. Securing virtual hosts

If you have secure virtual hosts, each will need its own IP, as SSL does not support name-based virtual hosts.

## 11. Useful URLs

- Common problems experienced with Apache are dealt with in our FAQs:http://www.thawte.com/support/server/apachessl.html
- You’ll find a key generation guide for Apache at: http://www.thawte.com/certs/server/keygen/apachessl.html
- The certificate enrollment process for SSL and SuperCerts begins at: https://www.thawte.com/certs/server/request.html
- How to generate a test certificate: https://www.thawte.com/cgi/server/test.exe
- Installing the test certificate CA root into your browser: http://www.thawte.com/servertest.crt

## 12. What role does Thawte play?

Thawte Consulting issues server certificates to organizations and individuals worldwide. Thawte verifies that the company ordering the certificate is a registered organization and that the person in the company who orders the certificate is authorized to do so.

Thawte also checks that the company in question owns the relevant domain. Thawte digital certificates interoperate smoothly with Apache and the latest software from Microsoft and Netscape, so you can rest assured that your purchase of a Thawte Server Certificate will give your customers confidence in your system and integrity; they will feel secure about transacting with you online.

## 13. Conclusion

Apache web servers, together with Apache-SSL, or ModSSL provide an excellent platform on which to base an e-commerce website, and Thawte certificates provide the necessary security.

## 14. Contact Thawte

If you would like more information about Thawte's SSL and other online security products, please visit http://www.thawte.com. If you have any questions, please e-mail info@thawte.com.