Apache with mod_ssl – Guide to Installing Root Certificates, Generating CSR and Installing certificate

Trustis Limited

Building 273 New Greenham Park Greenham Common Thatcham RG19 6HN

E: info@trustis.com W: www.trustis.com

Registered in England No: 03613613

Table of Contents

1 Introduction

This document specifies instructions for installing the Root, Intermediate and SSL certificates. Some parts of the process will require you to refer to the OpenSSL Tool guide.

2 Install Root and Intermediate Certificates

You will need to install the CA certificates in order for your webserver to use your SSL certificate properly. Apache users do not need to install these certificates individually. Instead you can install the CA certificates using a 'bundle' method.

In the Virtual Host settings for your site, in the httpd.conf file, you will need to complete the following:

1. Copy the PEM format Bundled CA certificate file (full CA chain) found at http://www.trustis.com/pki/healthcare/ops/healthcarett-chain-pem.txt to the directory in which the CA-bundled file is stored e.g. /usr/local/apache/conf/ca-bundle/ or /etc/httpd/conf/ca-bundle/
2. Add the following line to the SSL section of the httpd.conf (assuming /etc/httpd/conf/ca-bundle/ is the directory where you have copied the CA Bundle file). if the line already exists amend it to read the following:

```
SSLCACertificateFile /etc/httpd/conf/ca-
bundle/healthcarett-chain-pem.txt
```

If you are using a different location and certificate file names you will need to change the path and filename to reflect your server.

The SSL section of the updated httpd config file should now read something similar to this example (depending on your naming convention and directory structure):

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/myserver.cert

SSLCertificateKeyFile /etc/httpd/conf/ssl.key/privkey.pem

SSLCACertificateFile /etc/httpd/conf/ca-
bundle/healthcarett-chain-pem.txt
```

Save your httpd.conf file and **restart** Apache.

3 Certificate Signing Request (CSR) Generation

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 enrolment process:

Follow the Certificate Signing Request (CSR) Generation process found in the OpenSSL Tools guide – this is located on the Help page.

4 Installing your SSL Server Certificate

You will receive an email from the Registration Authority when your certificate request has been approved, that contains a link to a location where your certificate may be obtained. Clicking on this link will bring up a browser window that contains the details of your issued certificate, and includes a section which will appear similar to the following:

```
-----BEGIN CERTIFICATE-----
MIAGCSqGSIb3DQEHAqCAMIACAQExADALBgkqhkiG9w0BB
wGggDCCAmowggHXAhAFUbM77e50M63v1Z2A/5O5MA0GCS
qGSIb3DQEOBAUAMF8xCzAJBgNVBAYTAlVTMSAw...
...E+cFEpf0WForA+eRP6XraWw8rTN8102zGrcJgg4P6X
VS4l39+l5aCEGGbauLP5W6K99c42ku3QrlX2+KeDi+xBG
2cEIsdSiXeQS/16S36ITclu4AADEAAAAAAAAA
-----END CERTIFICATE-----
```

Copy everything you see **between and including** the lines:

```
-----BEGIN CERTIFICATE-----
...
-----END CERTIFICATE-----
```

and paste it into an appropriately named text file e.g. myserver.cert

Copy this certificate file into the directory that you will be using to store the certificate.

e.g. `/usr/local/apache/conf/ssl.crt/` **or**
`/etc/httpd/conf/ssl.crt/`

It is recommended that the directory containing privkey.pem is only readable by root.