**HOW TO SETUP AN SSL CONNECTION ON APACHE**

### Step 1 - What You Need

* A installation of Apache that includes SSL support.
* A installation of OpenSSL.
* An openssl.cnf file.

**Step 2 –** **In order to create a SELF-SIGNED CERTIFICATE (** We don’t have the time or the money to go to a competent authority)

i. We first generate the CSR (Certificate Signing Request) and the private key.

**openssl req -config openssl.cnf -new -out srik.csr -keyout srik.pem**

It will ask you a bunch of questions and you can ignore most of them, except two

a. Pass phrase (which will be used in the next step)

b. Common name: This will be the full domain name you will publish.

For ex: If we are using <https://localhost/somefiles>, we need Common name to be “localhost”.

Else, it could be a full name such as “www.myserver.com”

ii . Now we have the CSR and the public/private key. (srik.csr and srik.pem) . We now encrypt the key using RSA.

**openssl rsa -in srik.pem -out srik.key**

This will generate srik.key. (encrypted private/public key-pair)

iii. Now in normal conditions we should send the CSR file and the public key to a certifying authority. IN our case, we are the authority. So we will now generate a certificate using the above info. We will use the hugely popular X.509 standard for generating certificates.

**openssl** **x509 -in srik.csr -out srik.cert -req -signkey srik.key -days 365**

**(valid for 365 days)**

At the end of this exercise, we have a certificate, issued by US OFCOURSE….. ☺

**CONFIGURING APACHE**

Uncomment the following in **httpd.conf**

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

**#LoadModule ssl\_module modules/mod\_ssl.so**

SSL works on port 443 by default. So now open **http-ssl.conf.** Search for **“<VirtualHost \_default\_:443>”.**

Fill up the following fields. The example below will clarify everything.

**DocumentRoot "C:/Program Files/Apache Software Foundation/Apache2.2/htdocs"**

**ServerName localhost:443**

**ServerAdmin srikanth@localhost.com**

**ErrorLog "C:/Program Files/Apache Software Foundation/Apache2.2/logs/error.log"**

**TransferLog "C:/Program Files/Apache Software Foundation/Apache2.2/logs/access.log"**

Move down and look for: (change the directory if needed)

**SSLCertificateFile "C:/Program Files/Apache Software Foundation/Apache2.2/bin/srik.cert"**

**SSLCertificateKeyFile "C:/Program Files/Apache Software Foundation/Apache2.2/bin/srik.key"**

**Restart Apache and you are all set. Try** [**https://localhost**](https://localhost) **and things should be a breeze.**

**NOTE: YOU CAN USE:**

**openssl req -in srik.csr -noout -pubkey** to get the public-key out of the CSR

**openssl req -in srik.csr -noout –text** to decrypt the CSR