Secure HTTP (SSL/TLS) encrypts all the data passed between the web browser and the web server, so it has become a must have if you web page contains user authentication code and your server is critical.

Here is the tutorial on how to setup a secure HTTP on Apache web server in general, different OS could be different, but the principle is similar.

Required software:

- apache2 (Web Server)
- openssl

1: Create a self-signed certificate
You need to create a self-signed certificate with *openssl*. To do that you will need to generate the server key.

```
openssl genrsa –aes256 -out server-sec.key 4096
```

…and certificate signing request (CSR)

```
openssl req -new -key server-sec.key -out server.csr
```

After that, generate the server certificate by signing it with the server key.

```
openssl x509 -req -days 3650 -in server.csr -signkey server-
sec.key -out server.crt
```

Keep the server-sec.key in a secure location, with read/write permission assigned only to root. Then generate a password-less copy of the key for Apache use.

```
openssl rsa -in server-sec.key -out server.key
```

By this time, you should have :

- server.key (passwordless key for Apache)
- server.csr (certificate signing request)
- server.crt (certificate)
- server-sec.key (server key)

2: Update SSL config in Apache

Check on your server's apache configuration directory, for 2.x version, you will probably find it under /etc/httpd/conf.d

Save a copy of the ssl.conf:

```
cp ssl.conf ssl.conf.ORIG
```

then edit the ssl.conf file, search the '<VirtualHost *:443>' and change the config to something similar to these:

```
 <VirtualHost *:443>

ServerName ServerName

DocumentRoot /var/www-ssl/html/
```

Then, in the same file, find a line starting with ‘SSLCertificateFile’ and a line starting with ‘SSLCertificateKeyFile’, for example, on RHEL 6.3, the 2 lines look like following:

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt

SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

and use earlier generated ‘server.key’ and ‘server.crt’ to replace the 2 files:

```
SSLCertificateFile /etc/pki/tls/certs/ServerName.crt

SSLCertificateKeyFile /etc/pki/tls/private/ServerName.key
```

```
cp server.crt /etc/pki/tls/certs/ServerName.crt

cp server.key /etc/pki/tls/private/ServerName.key
```

then restart the web server.

Thanks: This document is derived from materials available from internet.