Certificate generated

Your self-signed certificate has been generated. Download the files below and store in a folder reachable by the web server, for example /etc/apache2/ssl.

» localhost.key

» localhost.cert

Apache Configuration

You need the following ssl configuration in your VirtualHost:

```
<VirtualHost localhost:443>
        ServerName localhost

        SSLEngine on
        SSLCertificateKeyFile /etc/apache2/ssl/localhost.key
        SSLCertificateFile /etc/apache2/ssl/localhost.cert
        SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown

        # ...
</VirtualHost>
```

You will also need all the settings and sections required for a regular HTTP host, such as `DocumentRoot` and `<Directory>`. You must also enable apache to listen on port 443, which is done using the directive `Listen 443`.

How to repeat

You can create a key and certificate yourself instead of downloading them from this page. This makes your key more secure. To generate a key:

```
openssl genrsa -out localhost.key 2048
```

And the certificate:

```
openssl req -new -x509 -key localhost.key -out localhost.cert -days 3650 -subj /CN=localhost
```

Buy a real certificate

Consider buying a real certificate to get a secure solution. Click here to buy.

For secure installations, I recommend that you buy a professional ssl certificate using a key that you generated yourself.
Any keys and certificates provided from this website is provided "as is" without warranty of any kind.