A self-signed SSL Certificate can be used for testing purposes or on websites where the visitors are people who know you and trust you. For situations where you ask for credit card or other payment information I strongly advice you to use a signed certificate (Make sure openssl is installed on your system, on a typically installation of CentOs it is installed by default) The first step is to generate the private key: openssl genrsa -des3 -out server.key 1024

You will be asked for a password twice. Make it a stong password and don't forget this it. Once the private key has been generated you have to generate Certificate Signing Request

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

This will ask you serveral questions:

```
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:
Locality Name (eg, city) [Newbury]:
Organization Name (eg, company) [My Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []: FQDN of the server
Email Address []: myaddress at mydomain.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Make sure that the Common Name matches the Fully Qualified DomainName of your SSL website.

As we signed the key with a password we should remove it, otherwise Apache cann't start up withou prompting for this password. We can remove the password:

```
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
```

Generate the cerficate which will be valid for 365 days:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

Last step is to configure Apache to use the self-signed certificate. Make sure the mod_ssl is enabled in your config. Open /etc/httpd/conf/httpd.conf find and uncomment by removing the # in the line:

```
# LoadModule ssl_module modules/mod_ssl.so
```

Copy the certificate and the private key to the Apache conf directory:

```
  cp server.crt /etc/httpd/conf/ssl/server.crt
cp server.key /etc/httpd/conf/ssl/server.key
```

Now edit the directive in your config matching the server you created this certificate for and add:

```
  SSLEngine on
SSLCertificateFile /usr/local/apache/conf/ssl.crt/server.crt
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/server.key
SetEnvIf User-Agent ".*MSIE.*" nokeepalive ssl-unclean-shutdown
CustomLog logs/ssl_request_log "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x "%r" %b"
```

and restart Apache:

```
  /etc/init.d/apache restart
```