



Version info		
Date	Version	Changes/Updates/Amendments
01.2012	1.03	Removed ESTEID-SK part as this CA expired 13.01.2012 and there are no more active ID-card certificates issued under this CA.
06.2011	1.02	First public edition

Configuring Apache web server to support ID-card certificates

In order to configure Apache to use SSL apache mod_ssl module has to be installed and enabled. This module relies on OpenSSL to provide the cryptography engine.

This document is based on <http://www.colleduc.ee/id.html> article, author [Taniel Kirikal](#).

Following is tested with:

Parameter	Value	Compatibility Notes
Operating system	CentOS 5.4	should apply to other Linux platforms
Web server	Apache HTTP server 2.2	

1.1 Configuring from beginning

- 1) If you do not have public and private keys, then generate them using openssl:

Generate private key:

```
openssl genrsa -out server.key 1024
```

Create a CSR (SSL Certificate Signing Request)

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

Simply answer the following questions and it is done:

Country Name (2 letter code) [Unknown]:ee
 State or Province Name (full name) [Unknown]:Harju
 Locality Name (eg, city) [Unknown]:Tallinn
 Organization Name (eg, company) [Unknown]:My Company
 Organizational Unit Name (eg, section) []:Software Development
 Common Name (eg, your name or your server's hostname) []:www.myserver.com
 Email Address []:



Please enter the following 'extra' attributes
to be sent with your certificate request

A challenge password []:

An optional company name []:

ENTER

NB! The value of Common Name attribute should be the DNS name of your web server (for example www.myserver.com or id.sk.ee).

2) Order web server SSL certificate

You can order Web Server SSL certificate from AS Sertifitseerimiskeskus:
<http://www.sk.ee/en/services/ssl-certificates> or any other public Certification Authority.

For development and testing purposes you can generate self signed SSL certificate using OpenSSL:

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

NB! In production environment it's strongly recommended not to use self signed SSL certificates and order web server certificate from trusted CA-s.

3) Download following certificates¹ with .pem extension from <http://sk.ee/repositoorium/sk-sertifikaadid/>:

- **Juur-SK**
- **EE Certification Centre Root CA**
- **ESTEID-SK 2007**
- **ESTEID-SK 2011**

```
wget http://sk.ee/upload/files/JUUR-SK.PEM.cer  
wget http://sk.ee/upload/files/EECCRCA.pem.cer  
wget http://sk.ee/upload/files/ESTEID-SK%202007.PEM.cer  
wget http://sk.ee/upload/files/ESTEID-SK%202011.pem.cer
```

4) Merge downloaded certificates in to one file:

¹ ESTEID-SK which was the first CA to issue certificates for ID-card expired 13.01.2012 and there is no need to configure ESTEID-SK in your system. If it is still configured please remove it. The last issued CRL will remain available from SK homepage <http://www.sk.ee/crls/esteid/esteid.crl> and is not longer renewed. There is no need after 13.01.2012 for CRL-s users to download ESTEID-SK CRL. Check your query rules set for fetching CRL-s and make sure that queries for ESTEID-SK CRL are not made after 13.01.2012.



```
cat JUUR-SK.PEM.cer EECRCA.pem.cer ESTEID-SK\ 2007.PEM.cer ESTEID-SK\
2011.pem.cer > id.crt
```

5) Download certificate revocation list files from <http://sk.ee/repositoorium/CRL/>

```
wget http://www.sk.ee/crls/esteid/esteid2007.crl
wget http://www.sk.ee/crls/juur/crl.crl
wget http://www.sk.ee/crls/eecrca/eecrca.crl
wget http://www.sk.ee/repository/crls/esteid2011.crl
```

Convert crl's to PEM

```
openssl crl -in esteid2007.crl -out esteid2007.crl -inform DER
openssl crl -in crl.crl -out crl.crl -inform DER
openssl crl -in eecrca.crl -out eecrca.crl -inform DER
openssl crl -in esteid2011.crl -out esteid2011.crl -inform DER
```

make a symlink of the CRL file in the CRL directory, with a filename based on a hash of the CRL file:

```
ln -s crl.crl `openssl crl -hash -noout -in crl.crl`.r0
ln -s esteid2007.crl `openssl crl -hash -noout -in esteid2007.crl`.r0
ln -s eecrca.crl `openssl crl -hash -noout -in eecrca.crl`.r0
ln -s esteid2011.crl `openssl crl -hash -noout -in esteid2011.crl`.r0
```

Every CRL file in the SSLCARevocationPath must have one of these symlinks.

It is important to regularly update certificate revocation files.

Check script which automatically renews CRL's for reference:

```
http://id.ee/public/renew.sh
```

After adding or renewing certificate revocation files apache http server must be restarted, otherwise new CRL's will not be used. If the web server SSL Private Key is encrypted, the Pass Phrase dialog is forced after restart.

NB! Our recommendation is to use at application level OCSP service for certificate validation instead of using CRL-s. For more information please look at <http://www.sk.ee/en/services/validity-confirmation-services>.

6) Replace bold selected paths in the example config with correct paths on your server:

```
NameVirtualHost *:443
Listen 443

<VirtualHost *:443>
    ServerName idtest
```



```
SSLEngine On
# change to correct path on your server
SSLCertificateFile /etc/httpd/conf/ssl/crt/server.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl/key/server.key
SSLCACertificateFile /etc/httpd/conf/ssl/crt/id.crt
SSLCARevocationPath /etc/httpd/conf/ssl/revocation/
DocumentRoot /etc/httpd/temp/idhome
<Directory "/etc/httpd/temp/idhome/">
    Options Indexes FollowSymLinks MultiViews
    SSLVerifyClient require
    SSLVerifyDepth 2
</Directory>
</VirtualHost>
```

Save config to file with .conf extension and and move it to /etc/httpd/conf.d directory

- 7) To use certificates of server and client for the current HTTPS connection in CGI scripts put the following to .htaccess file

```
<Files ~ "\.(cgi|shtml|php)$">
    SSLOptions +StdEnvVars +ExportCertData
</Files>
```

- 8) Restart apache httpd server

```
/etc/init.d/httpd restart
```

- 9) Put your ID-card into card reader and open Web Server ULR (in example <https://www.myserver.com/>) in a browser if you started Apache httpd server on local machine. PIN1 will be asked and content will be shown.

If you generated your own private and public keys and you have not signed them in valid authorities then security certificate problem is displayed in Internet Explorer. Just click "Continue to this website (not recommended)."

1.2 Configuring Apache to support new 2011 root certificate and ESTEID-SK 2011 CA certificate.

If you had apache http server configured before and you just want add new 2011 root certificate support then download "EE Certification Centre Root CA" and "ESTEID-SK 2011" from <http://sk.ee/repositoorium/sk-sertifikaadid/>.

```
wget http://sk.ee/upload/files/EECCRCA.pem.cer
wget http://sk.ee/upload/files/ESTEID-SK%202011.pem.cer
```

New certificate support can be done in two ways. This depends on way other certificates were configured before.

- 1) Open your host configuration file.
- 2) Find if SSLCACertificateFile directive is used.



For example:

```
<VirtualHost www.myserver.com:443>
  SSLEngine On
  ...
  SSLCACertificateFile /etc/httpd/conf/ssl/crt/id.crt
  ...
</VirtualHost>
```

This means that CA certificates are merged into one file. Simply add downloaded certificates to end of this file:

```
cat id.crt EECCRCA.pem.cer ESTEID-SK\ 2011.pem.cer > id.crt
```

restart apache httpd server:

```
/etc/init.d/httpd restart
```

3) Find if SSLCACertificatePath directive is used.

For example:

```
<VirtualHost www.myserver.com:443>
  SSLEngine On
  ...
  SSLCACertificatePath /etc/httpd/conf/ssl/crt/
  ...
</VirtualHost>
```

Copy downloaded certificates to certificate path directory. Make a symlink of certificate file in this directory, with a filename based on a hash of the certificate file:

In bulk:

```
for f in *.cer;do ln -sf "$f" `openssl x509 -hash -noout -in "$f"`.0; done
```

Individually:

```
ln -s EECCRCA.pem.cer `openssl x509 -hash -noout -in EECCRCA.pem.cer`.0
ln -s ESTEID-SK\ 2011.pem.cer `openssl x509 -hash -noout -in ESTEID-SK\
2011.pem.cer`.0
```

restart apache httpd server:

```
/etc/init.d/httpd restart
```

4) Update certificate revocation information checking configuration

a. Certificate validation checking based on OCSP service



SK OSCP service (<http://ocsp.sk.ee>) signs ESTEID-SK 2011 certificate validity confirmations using „SK OSCP RESPONDER 2011“ OSCP responder certificate. This certificate is available at <https://www.sk.ee/certs/>

For checking ESTEID-SK 2011 certificates validity „ESTEID-SK 2011“ and „SK OSCP RESPONDER 2011“ certificates should be added OSCP client application configuration.

Example PHP application with OSCP certificate validation (including ESTEID-SK 2011 CA) is available from <http://www.id.ee/>

b. Checking Certificate revocation information based on CRLs:

Download ESTEID-SK 2011 CRL

```
wget http://www.sk.ee/repository/crls/esteid2011.crl
```

Convert the downloaded CRL to PEM

```
openssl crl -in esteid2011.crl -out esteid2011.crl -inform DER
```

make a symlink of the CRL file in the CRL directory (SSLCARevocationPath), with a filename based on a hash of the CRL file:

```
ln -s esteid2011.crl `openssl crl -hash -noout -in esteid2011.crl`.r0
```

NB! Add esteid2011.crl to automatic CRL update script. Renewal interval of ESTEID-SK 2011 CRL is the same as ESTEID-SK 2007 CRL-s (12 hours).