



Version info		
Date	Version	Changes/Updates/Amendments
09.2016	1.07	Removed instructions for KLASS3-SK 2010 certificate revocation list (CRL) installation (reason: KLASS3-SK 2010 certificates are not used on personal eID documents). Added installation instructions for EID-SK 2011 certificate.
08.2016	1.06	Removed installation instructions for Juur-SK, ESTEID-SK 2007, EID-2007 and KLASS3-SK 2010 (Juur-SK) due to expiration of root certificate (Juur-SK) on 26 <sup>th</sup> of August 2016.
03.2016	1.05	Removed KLASS3-SK 2010 (EECCRCA, SHA1) from instructions. There is no need for mentioned certificate. Changed SSLCertificateChainFile value to /etc/apache2/ssl.crt/ca.crt
12.2015	1.04	Added new certificate ESTEID-SK 2015. Tested with latest software (Apache+CentOs).
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 7.2	should apply to other Linux platforms
Web server	Apache HTTP server 2.4	

### 1.1 Configuring from beginning

- 1) If you do not have public and private keys, then use this [TLS Server Certificate manual](#) for generating public and private keys and installing TLS Server Certificate on Apache.
- 2) Download following certificates with .pem extension from <https://sk.ee/en/repository/certs/>:
  - EE Certification Centre Root CA



- ESTEID-SK 2011
- ESTEID-SK 2015
- EID-SK 2011

```
wget http://www.sk.ee/upload/files/EE_Certification_Centre_Root_CA.pem.crt
wget http://www.sk.ee/upload/files/ESTEID-SK_2011.pem.crt
wget http://www.sk.ee/upload/files/ESTEID-SK_2015.pem.crt
wget http://www.sk.ee/upload/files/EID-SK_2011.pem.crt
```

3) Merge downloaded certificates in to one file (folder contains only these files):

```
cat *.crt > id.crt
```

Revoked SSL certificates. There is two ways to check revoked certificates: OSCP (Online Certificate Status Protocol) or CRL (Certificate Revocation Lists).

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

## 1.1.1 Using OSCP (OCSP Stapling)

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

```
Listen 443

SSLUseStapling On
SSLStaplingCache shmcb:/run/httpd/ssl_stapling(128000)

<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
    SSLCertificateChainFile /etc/apache2/ssl.crt/ca.crt

    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.

## Configuring Apache web server to support ID-card certificates



Version 1.07

You can see the URLs used to connect to a CA's OCSP server by opening up a certificate. Then, in the certificates **Details** in the **Certificate Extensions**, select **Authority Information Access** to see the issuing CA's URL for their OCSP.



## 1.1.2 Using CRL

- a) Download certificate revocation list files from <https://sk.ee/en/repository/CRL/>

```
wget https://sk.ee/crls/eccrca/eccrca.crl
wget https://sk.ee/repository/crls/esteid2011.crl
wget http://www.sk.ee/crls/esteid/esteid2015.crl
wget https://sk.ee/repository/crls/eid2011.crl
```

- b) Convert crl's to PEM:

```
for f in *.crl; do openssl crl -in $f -out $f -inform DER; done
```

- c) Make a symlink of the CRL file in the CRL directory, with a filename based on a hash of the CRL file:

```
for f in *.crl; do ln -s $f `openssl crl -hash -noout -in $f`.r0; done
```

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.

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

```
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/
    SSLCARevocationCheck leaf
    SSLCertificateChainFile /etc/apache2/ssl.crt/ca.crt

    DocumentRoot /etc/httpd/temp/idhome
    <Directory "/etc/httpd/temp/idhome/">
```



Version 1.07

```
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.

- 4) 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>
```

- 5) Restart apache httpd server

```
apachectl restart
```

- 6) 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 ESTEID-SK 2015 CA certificate.

If you had apache http server configured before and you just want add new ESTEID-SK 2015 certificate support then download from <http://sk.ee/repositoorium/sk-sertifikaadid/>.

```
wget http://www.sk.ee/upload/files/ESTEID-SK_2015.pem.crt
```

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 SSLCertificateFile directive is used.

For example:

```
<VirtualHost www.myserver.com:443>
    SSLEngine On
    ...
    SSLCertificateFile /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 ESTEID-SK_2015.pem.crt >> id.crt
```

restart apache httpd server:

```
apachectl 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:

```
ln -s ESTEID-SK_2015.pem.crt `openssl x509 -hash -noout -in ESTEID-  
SK_2015.pem.crt`.0
```

restart apache httpd server:

```
apachectl restart
```

### 4) Update certificate revocation information checking configuration

#### a. Certificate validation checking based on OCSP service

SK OCSP service (<http://ocsp.sk.ee>) signs ESTEID-SK 2015 certificate validity confirmations using „SK OCSP RESPONDER 2011“ OCSP responder certificate. This certificate is available at <https://sk.ee/en/repository/certs/>

For checking ESTEID-SK 2015 certificates validity „ESTEID-SK 2015“ certificate should be added OCSP client application configuration.

Example PHP application with OCSP certificate validation (including ESTEID-SK 2015 CA) is available from <http://id.ee/index.php?id=35795>.

#### b. Checking Certificate revocation information based on CRLs:



### Download ESTEID-SK 2015 CRL

```
wget http://www.sk.ee/crls/esteid/esteid2015.crl
```

### Convert the downloaded CRL to PEM

```
openssl crl -in esteid2015.crl -out esteid2015.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 esteid2015.crl `openssl crl -hash -noout -in esteid2015.crl`.r0
```

NB! Add esteid2015.crl to automatic CRL update script. Renewal interval of ESTEID-SK 2015 CRL is the same as ESTEID-SK 2011 CRL-s (12 hours).