SK VEEBISERTIFIKAATIDE SEADISTAMISE JUHEND APACHE SERVERIL

Tehniline kirjeldus

2016

SERTIFITSEERIMISKESKUS

SISUKORD

SISUST

Käesolev juhend käsitleb Sertifitseerimiskeskus poolt väljastatavate SSL sertifikaatide installeerimist Apache veebiserverisse, et tagada turvaline internetisuhtlus veebilehe külastaja ja serveri vahel. Juhendi eelnõudeteks on internetiühendus ja root ligipääs veebiserveri konsoolile.

SERTIFIKAADIPÄRINGU LOOMINE

Kasutame openssl programmi privaatvõtme ja sertifikaadipäringu loomiseks.
Käivitades openssl programmi, ette näidatud käsuga, küsitakse informatsiooni päringu loomiseks. Serveri aadress mida tahetakse turvata tuleb sisestada "Common Name" järele. Näites on selleks **www.domain.ee** aadress. Sertifikaadi päring, mis tuleb edastada Sertifitseerimiskeskusele salvestatakse Linuxi puhul faili **/root/www.domain.ee.csr,** serveri privaatvõti salvestatakse faili **/root/www.domain.ee.key**. Microsoft Windowsi puhul salvestatakse serveri privaatvõti **www.domain.ee.key** ja sertifikaadipäring **www.domain.ee.csr** kasutaja Desktopile.

Linuxi puhul avame konsooli root õigustes ja käivitame käsu: "**openssl req -nodes -newkey rsa:2048 -keyout /root/www.domain.ee.key -out /root/www.domain.ee.csr**"

Microsoft Windowsi puhul käivitame OpenSSL programmi käsurealt:
„"%programfiles%\Apache Software Foundation\Apache2.2\bin\openssl.exe" req -nodes -newkey rsa:2048 -keyout "%HOMEPATH%\desktop\www.domain.ee.key" -out "%HOMEPATH\desktop\www.domain.ee.csr" -config "%programfiles%\Apache Software Foundation\Apache2.2\conf\openssl.cnf""

Järgnevalt avanevas dialoogis tuleb määrata sertifikaadi päringu parameetrid (näidisparameetrid märgitud punasega):

Generating a 2048 bit RSA private key
.....+++
..+++
writing new private key to '/root/www.domain.ee.key'

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:EE
State or Province Name (full name) [Some-State]:Harjumaa
Locality Name (eg, city) []:Tallinn
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AS Serverid
Organizational Unit Name (eg, section) []:Äri
Common Name (eg, YOUR name) []:www.domain.ee
Email Address []:webmaster@domain.ee

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

A challenge password []:
An optional company name []:

SERTIFIKAADI KÜSIMINE SK-ST

Päringu loomise käigus genereeritud fail tulab edastada Sertifitseerimiskeskusse, vastavalt kokkulepetele väljastatakse teile vastav sertifikaat. Veebiserveri sertifikaadi saab tellida veebilehelt http://www.sk.ee/teenused/veebiserveri-sertifikaadid.

SERTIFIKAADI INSTALLEERIMINE

Järgnevalt tuleb installeerida serveri privaatvõti ja Sertifitseerimiskeskusest saadud sertifikaat **www.domain.ee.crt,** mille oleme kopeerinud **/root** kataloogi.
Märkus: SK sertifikaadid on allalaetavad aadressilt http://www.sk.ee/certs

NB! Allpool kajastatud op. süsteemide juhendites kasutatud SSLCertificateChainFile on alates Apache 2.4.8 versioonist deprecated. KLASS3-SK 2010 sertifikaat tuleks Apache 2.4.8 või uuema kasutamisel lisada SSLCertificateFile'i (wget -q https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt -O - > /etc/httpd/conf/ssl/crt/server.crt)

DEBIAN JA UBUNTU

Veendume näites toodu käsuga, et vajalik tarkvara on serverisse installeeritud:
„apt-get install apache2 openssl nano wget"

Oodatud väljund sellele käsule on sarnane järgnevale:
Reading package lists... Done
Building dependency tree
Reading state information... Done
nano is already the newest version.
openssl is already the newest version.
openssl set to manually installed.
wget is already the newest version.
apache2 is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

Installeerime Sertifitseerimiskeskusest saadud sertifikaadi:
„cp /root/www.domain.ee.crt /etc/ssl/certs/www.domain.ee.crt"

Installeerime serveri privaatvõtme:
„cp /root/www.domain.ee.key /etc/ssl/private/www.domain.ee.key"

Installeerime Sertifitseerimiskeskuse kesktaseme sertifikaadi:
„wget -q https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt -O - > /etc/ssl/certs/ca.crt"

Lülitame sisse ssl toetuse Apache veebiserveris:
„a2enmod ssl"

Loome Apache veebiserveri seadistuste faili ja kopeerime sinna sisse näites toodud seaded. Seda on võimalik teha otse konsoolist nano tekstiredaktoriga:
„nano /etc/apache2/sites-available/www.domain.ee":

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerName www.domain.ee:443
        ServerAdmin webmaster@domain.ee

        DocumentRoot /var/www

        ErrorLog ${APACHE_LOG_DIR}/error.log
        LogLevel warn
        CustomLog ${APACHE_LOG_DIR}/ssl_access.log combined

        SSLEngine on
        SSLCertificateFile    /etc/ssl/certs/domain.ee.crt
        SSLCertificateKeyFile /etc/ssl/private/domain.ee.key
        SSLCertificateChainFile /etc/ssl/certs/ca.crt

        BrowserMatch "MSIE [2-6]" \
                nokeepalive ssl-unclean-shutdown \
                downgrade-1.0 force-response-1.0
        BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost>
</IfModule>
```

Lülitame sisse uue veebiserveri seadistuse:
„a2ensite www.domain.ee"

Loeme sisse uue seadistuse:
„/etc/init.d/apache2 reload"

CENTOS, RED HAT ENTERPRISE LINUX JA FEDORA

Veendume näites toodu käsuga, et vajalik tarkvara on serverisse installeeritud:
„yum install httpd mod_ssl openssl nano wget"

Oodatud väljund sellele käsule on sarnane järgnevale:

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.estpak.ee
 * epel: ftp.funet.fi
 * extras: ftp.estpak.ee
 * updates: ftp.estpak.ee
Setting up Install Process
Package httpd-2.2.3-45.el5.centos.1.i386 already installed and latest version
Package 1:mod_ssl-2.2.3-45.el5.centos.1.i386 already installed and latest version
Package nano-1.3.12-1.1.i386 already installed and latest version
Package wget-1.11.4-2.el5_4.1.i386 already installed and latest version
Package openssl-0.9.8e-12.el5_5.7.i386 already installed and latest version
Nothing to do
```

Installeerime Sertifitseerimiskeskusest saadud sertifikaadi:
„cp /root/www.domain.ee.crt /etc/pki/tls/certs/www.domain.ee.crt"

Installeerime serveri privaatvõtme:
„cp /root/www.domain.ee.key /etc/pki/tls/private/www.domain.ee.key"

Installeerime Sertifitseerimiskeskuse kesktaseme sertifikaadi:
„wget -q https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt -O - > /etc/pki/tls/certs/ca.crt"

Muudame Apache veebiserveri seadistuste faili. Seda on võimalik teha otse konsoolist nano tekstiredaktoriga:
„nano /etc/httpd/conf.d/ssl.conf"

Otsime üles **SSLCertificateFile** algusega rea ja muudame selle järgnevaks:
SSLCertificateFile /etc/pki/tls/certs/www.domain.ee.crt

Otsime üles **SSLCertificateKeyFile** algusega rea ja muudame selle järgnevaks:
SSLCertificateKeyFile /etc/pki/tls/private/www.domain.ee.key

Otsime üles **#SSLCertificateChainFile** algusega rea ja muudame selle järgnevaks:
SSLCertificateChainFile /etc/pki/tls/certs/ca.crt

Loeme sisse uue seadistuse:
„/etc/init.d/httpd restart"

OPENSUSE JA SUSE

Veendume näites toodu käsuga, et vajalik tarkvara on serverisse installeeritud:
„yast --install apache2 openssl nano wget"

Oodatud väljundina avaneb tekst mode programm, mis ei tohiks enam midagi üle küsida ja lõppedes ei jäta mingit väljundit.

Installeerime Sertifitseerimiskeskusest saadud sertifikaadi:
„cp /root/www.domain.ee.crt /etc/apache2/ssl.crt/server.crt"

Installeerime serveri privaatvõtme:
„cp /root/www.domain.ee.key /etc/apache2/ssl.key/server.key"

Installeerime Sertifitseerimiskeskuse kesktaseme sertifikaadi:
„wget -q https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt -O - > /etc/apache2/ssl.crt/ca.crt"

Lülitame sisse ssl toetuse Apache veebiserveris:
„a2enmod ssl"
„a2enflag SSL"

Loome Apache veebiserveri seadistuste faili ja kopeerime sinna sisse näites toodud seaded. Seda on võimalik teha otse konsoolist nano tekstiredaktoriga:
„nano /etc/apache2/vhosts.d/www.domain.ee.conf":

```
<IfDefine SSL>
<IfDefine !NOSSL>
<VirtualHost _default_:443>
    DocumentRoot "/srv/www/htdocs"
    ServerName www.domain.ee:443
```

ServerAdmin webmaster@domain.ee
ErrorLog /var/log/apache2/error_log
TransferLog /var/log/apache2/access_log

SSLEngine on
SSLCipherSuite „EECDH+ECDSA+AESGCM EECDH+aRSA+AESGCM EECDH+ECDSA+SHA384 EECDH+ECDSA+SHA256 EECDH+aRSA+SHA384 EECDH+aRSA+SHA256 EECDH EDH+aRSA !aNULL !eNULL !LOW !3DES !MD5 !EXP !PSK !SRP !DSS !RC4"

SSLProtocol All -SSLv2 -SSLv3
SSLHonorCipherOrder on

SSLCertificateFile /etc/apache2/ssl.crt/server.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
SSLCertificateChainFile /etc/apache2/ssl.crt/ca.crt

**SetEnvIf User-Agent ".*MSIE.*" **
**nokeepalive ssl-unclean-shutdown **
downgrade-1.0 force-response-1.0

CustomLog /var/log/apache2/ssl_request_log ssl_combined
</VirtualHost>
</IfDefine>
</IfDefine>

Loeme sisse uue seadistuse:
„/etc/init.d/apache2 restart"

MICROSOFT WINDOWS

Eelnevalt peab olema installeeritud Apache veebiserver OpenSSL toetusega. Server on tasuta allalaetav aadressilt http://httpd.apache.org/download.cgi

Lülitame sisse ssl toetuse:
1) Start -> Run
2) Avanenud aknasse kirjutame **notepad "%programfiles%\Apache Software Foundation\Apache2.2\conf\httpd.conf"**
3) Avanenud failis teeme järgmised muudatused:
a) Asendame rea **#LoadModule ssl_module modules/mod_ssl.so** uue reaga **LoadModule ssl_module modules/mod_ssl.so**
b) Asendame rea **#Include conf/extra/httpd-ssl.conf** uue reaga **Include conf/extra/httpd-ssl.conf**

Installeerime sertifikaadid:
1) Start -> Run
2) Avanenud aknasse kirjutame **notepad "%programfiles%\Apache Software Foundation\Apache2.2\conf\extra\httpd-ssl.conf"**
3) Asendame rea **#SSLCertificateChainFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/server-ca.crt"** uue reaga **SSLCertificateChainFile "C:/Program Files/Apache Software Foundation/Apache2.2/conf/ca.crt"**
4) Start -> Run
5) Avanenud aknasse kirjutame **"%programfiles%\Apache Software**

Foundation\Apache2.2\conf\"
6) Avanenud kataloogi kopeerime Sertifitseerimiskeskusest saadud sertifikaadi nimega **server.crt** ja Desktopile salvestatud serveri privaatvõtme nimega **server.key**
7) Järgnevalt laeme alla kesktaseme sertifikaadi https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt ning avame notepadis, et selle sisu kopeerida ja salvestada punktis 5 avatud kataloogis **ca.crt** faili.

Loeme sisse uued Apache seadistused:
1) Start -> All Programs -> Apache HTTP Server -> Control Apache Server -> Restart