



UBUNTU APACHE2 VEEBISERVERI KAHEPOOLSE SSLi HÄÄLESTUS EESTI ID-KAARTIDE VAATES

Dokumendi info	
Loomise aeg	06.02.2019
Tellijä	Riigi Infosüsteemi Amet
Autor	Urmas Vanem, OctoX
Versioon	25.10/1

Versiooni info		
Kuupäev	Versioon	Muutused/märkused
06.02.2019	19.02/1	Avalik versioon
20.02.2019	19.02/1	Lisatud võimalike lisakonfiguratsioonide peatükk: tulemüüri ja OCSP seadistus ning vaikimisi veebilehe eemaldamine. Muutja: Urmas Vanem
12.12.2019	19.12/1	Lisatud Apache soovituslikud turvasätted. Muutja: Urmas Vanem
16.12.2020	20.12/1	Lisatud kasutajasertifikaadile nõue omada korrektset <i>extendedKeyUsage</i> välja ja õiget sertifikaadi väljastajat. Vt. peatükk „Kasutajasertifikaatide lisafiltreerimine“. Muutja: Urmas Vanem
17.12.2020	20.12/2	Lisatud direktiiv SSLCADNRequestPath, vt. peatükk „Kasutajale kuvatavate sertifikaatide filtreerimine“. Muutja: Urmas Vanem
13.01.2021	21.01/1	Lisatud demo-konfiguratsiooni fail lingina. Lisatud HSTS konfiguratsioon. Muutja: Urmas Vanem
21.01.2021	21.01/2	Parandatud SSLOCSPEnable parameeter: on->leaf. Uuendatud TLS 1.2 <i>cipherte</i> ja TLS protokollide kasutamise soovitused. Demokonfi ja dokumendi muutujate nimed on sünkroniseeritud. Muutja: Urmas Vanem
27.01.2021	21.01/3	Lisatud mobiil-ID filter. Muutja: Urmas Vanem



26.02.2021	21.02/1	Lisatud alternatiivne kesktaseme sertifitseerimiskeskuste filtreerimisvõimalus SSLCADNRequestFile direktiivi abil. Muutja: Urmas Vanem
27.04.2021	21.04/1	Eemaldatud aegunud ESTEID-SK 2011 sertifikaatide tugi. Muutja: Urmas Vanem
25.11.2021	21.11/1	Ubuntu uuendatud versioonile Ubuntu Server 21.10 ja Apache versioonile 2.4.48. Lisatud ECC sertifikaatide loomine veebiserveril. Täiendatud TLS ja Cipher soovitusi. Muutja: Urmas Vanem
21.02.2023	23.02/1	Ubuntu uuendatud versioonile Ubuntu Server 22.04 ja Apache versioonile 2.4.55. Uuendatud virtuaalhosti konfiguratsiooni. Muutja: Urmas Vanem
27.12.2023	23.12/1	Eemaldatud ESTEID-SK 2015 ahel. Muutja: Urmas Vanem
27.12.2023	23.12/2	Eemaldatud aegunud OCSP responderi sertifikaat. Muutja: Urmas Vanem
22.08.2024	24.08/1	Ubuntu uuendatud versioonile Ubuntu Server 24.04 ja Apache versioonile 2.4.62. Muutja: Urmas Vanem
31.10.2025	25.10/1	Lisatud Zetes ahelad Muutja: Raul Kaidro



Sissejuhatus

Käesolevas juhendis kirjeldatakse:

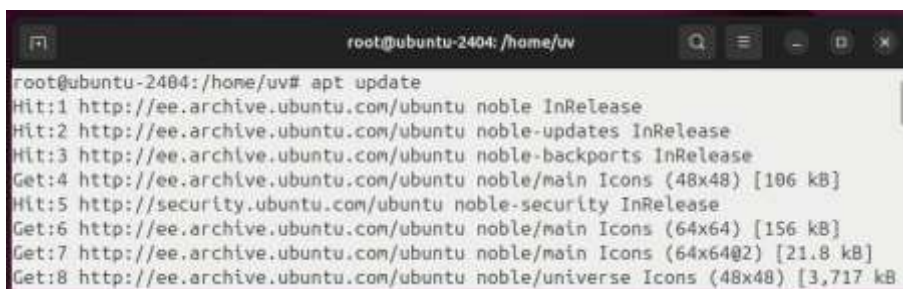
- Kuidas paigaldada ja häälestada Apache2 (v. 2.4.65) veebiserver Ubuntu 24.04 serveril.
- Kuidas häälestada HTTPS (ühepoolne SSL) veebiserveril.
- Kuidas häälestada ID-kaartidega autentimine (kahepoolne SSL) veebiserveril.
- Muud võimalused serveri konfigureerimiseks ja soovitusel turvalisuse tagamiseks.

Apache2 paigaldus ja häälestus

Paigaldus

1. Uuenda Ubuntu pakke andmed terminalis käsuga:

apt update

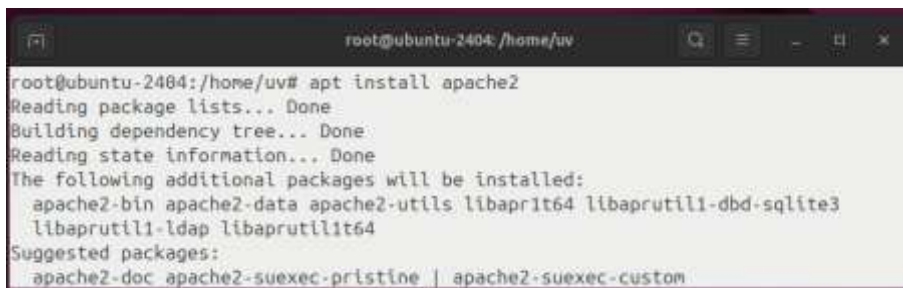


```
root@ubuntu-2404: /home/uv# apt update
Hit:1 http://ee.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://ee.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://ee.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:4 http://ee.archive.ubuntu.com/ubuntu noble/main Icons (48x48) [106 kB]
Hit:5 http://security.ubuntu.com/ubuntu noble-security InRelease
Get:6 http://ee.archive.ubuntu.com/ubuntu noble/main Icons (64x64) [156 kB]
Get:7 http://ee.archive.ubuntu.com/ubuntu noble/main Icons (64x64@2) [21.8 kB]
Get:8 http://ee.archive.ubuntu.com/ubuntu noble/universe Icons (48x48) [3,717 kB]
```

Pilt 1 – pakke uuendamine

2. Paigalda Apache2 käsuga:

apt install apache2



```
root@ubuntu-2404: /home/uv# apt install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  apache2-bin apache2-data apache2-utils libapr1t64 libaprutil1-dbd-sqlite3
  libaprutil1-ldap libaprutil1t64
Suggested packages:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
```

Pilt 2 - Apache2 paigaldus



Eelneva tegevuse tulemusena on Apache server paigaldatud¹.

```
parallels@ubuntu-linux-24-04-desktop:~$ apache2 -v
Server version: Apache/2.4.58 (Ubuntu)
Server built:   2025-08-11T11:10:09
parallels@ubuntu-linux-24-04-desktop:~$
```

Pilt 3 - Apache versiooni päring

Uuenda Apache versioonile 2.4.65, järgmiste käskude abil saad seda teha:

```
add-apt-repository ppa:ondrej/apache2
```

```
apt update
```

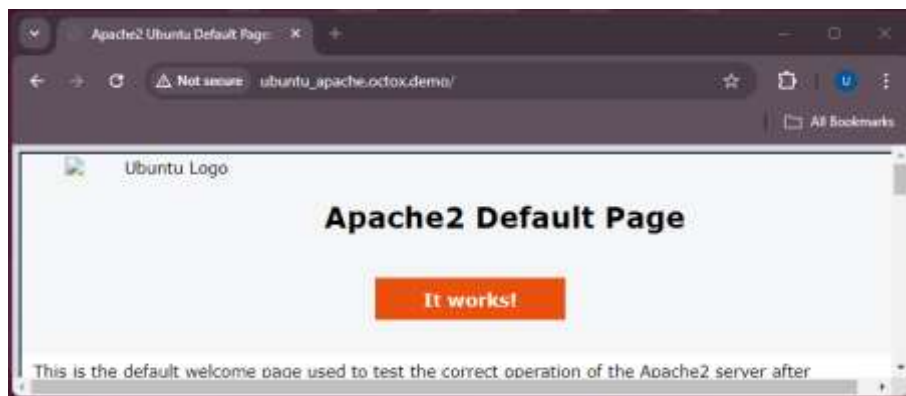
```
apt upgrade
```

Nüüd on Apache versiooniks ootuspäraselt 2.4.65:

```
parallels@ubuntu-linux-24-04-desktop:~$ apache2 -v
Server version: Apache/2.4.65 (Ubuntu)
Server built:   2025-07-26T17:41:22
parallels@ubuntu-linux-24-04-desktop:~$
```

Pilt 4 – Apache versiooniks peale uuendamist on 2.4.65

Versiooniga 2.4.65 töötab Apache2 veebiserver nüüd ebaturvalises http režiimis:



Pilt 5 – Apache veebiserver vaikimisi konfiguratsioonis

Konfiguratsioon

Ühepoolse SSLi lubamine

Luba Apache serveril SSL mooduli käsuga:

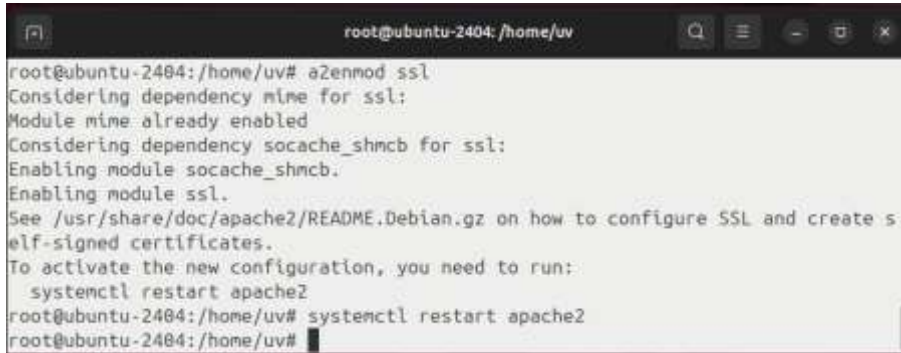
```
a2enmod ssl
```

¹ Hetkeseisuga (30.10.2025) on Ubuntu'ga vaikimisi kaasas versioon 2.4.58, viimane Apache versioon on 2.4.65.



ja taaskäivita Apache2 teenus:

```
systemctl restart apache2
```



```
root@ubuntu-2404:/home/uv# a2enmod ssl
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu-2404:/home/uv# systemctl restart apache2
root@ubuntu-2404:/home/uv#
```

Pilt 6 - SSL lubamine ja teenuse taaskäivitus

SSL sertifikaadi privaatvõtme ja päringufaili (CSR) loomine

ECC (Elliptic Curve Cryptography)

Esmalt tuleb luua ECC algoritmil baseeruv privaatvõti:

```
openssl ecparam -name secp384r1 -genkey -noout -out Apache2404.key
```

ja seejärel privaatvõtme baasil sertifikaadi päringufail:

```
openssl req -new -key Apache2404.key -out Apache2404.csr -subj
/C=EE/O=OctoX/CN=Apache2404.octox.demo -reqexts SAN -config <(cat
/etc/ssl/openssl.cnf <(printf
"[SAN]\nsubjectAltName=DNS:Apache2404.octox.demo,DNS:MYWEBSERVER.oct
ox.demo"))2
```



```
root@ubuntu-2404:/home/uv# openssl ecparam -name secp384r1 -genkey -noout -out A
pache2404.key
root@ubuntu-2404:/home/uv# openssl req -new -key Apache2404.key -out Apache2404.
csr -subj /C=EE/O=OctoX/CN=Apache2404.octox.demo -reqexts SAN -config <(cat /etc
/ssl/openssl.cnf <(printf "[SAN]\nsubjectAltName=DNS:Apache2404.octox.demo,DNS:M
YWEBSERVER.octox.demo"))
root@ubuntu-2404:/home/uv#
```

Pilt 7 – ECC privaatvõtme ja sertifikaadi päringufaili loomine

Kollase taustaga parameetrid:

1. Apache2404.key on sertifikaadi privaatvõti;
2. Apache2404.csr on sertifikaadi päringufail, mis edastatakse sertifitseerimiskeskusele;

² Lisaks käsuraal kirjeldatud sertifikaadi atribuutidele C, O ja CN on võimalik soovi korral lisaks kirjeldada atribuudid L, OU ja S. Võib kasutada ka ainult CNI.



3. CN=Apache2404.octox.demo on väljastatava sertifikaadi *common name*;
4. DNS:Apache2404.octox.demo ja DNS:MYWEBSERVER.octox.demo on sertifikaadil olevad SAN DNS nimed, mis peavad kindlasti vastama veebilehe tegelikule aadressile³. Need nimed peavad ka nimeserveris lahenema.

Loodud sertifikaadi päringufaili sisu on võimalik vaadata käsuga

openssl req -in Apache2404.csr -noout -text

```
root@ubuntu-2404: /home/uv
root@ubuntu-2404:/home/uv# openssl req -in Apache2404.csr -noout -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = EE, O = OctoX, CN = Apache2404.octox.demo
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (384 bit)
    pub:
      04:db:9b:fe:8c:11:87:00:b1:71:9b:54:06:3a:49:
      71:b0:89:04:dc:a9:75:52:54:42:39:07:21:84:51:
      b7:5b:07:61:09:5b:e7:82:ff:60:58:b3:af:5e:73:
      ee:03:47:1d:9d:26:e6:fe:92:e0:60:df:71:23:8e:
      24:2b:11:be:68:f6:60:6c:3e:be:dc:7d:f4:32:6e:
      9e:ae:5e:73:5f:fd:43:74:ab:8d:7d:d8:91:b6:e1:
      52:f9:f6:53:aa:df:64
    ASN1 OID: secp384r1
    NIST CURVE: P-384
  Attributes:
    Requested Extensions:
      X509v3 Subject Alternative Name:
        DNS:Apache2404.octox.demo, DNS:MYWEBSERVER.octox.demo
  Signature Algorithm: ecdsa-with-SHA256
  Signature Value:
```

Pilt 8 – loodud sertifikaadi päringufaili sisu

RSA

Juhul, kui mingil põhjusel on soov jätkata RSA algoritmiga, siis on siin juhendis ka vana, üle-eelmise juhendi õpetus RSA sertifikaadipäringu loomiseks. Edasistes punktides selles juhendis jätkatakse eelmises punktis kirjeldatud ECC algoritmil põhineva sertifikaadiga.

Loo sertifikaadi päring ja privaatvõti käsuga

```
openssl req -newkey rsa:2048 -keyout Apache2021.key -sha256 -subj
"/CN=Apache5.kaheksa.xi" -reqexts SAN -config <(cat
/etc/ssl/openssl.cnf <(printf
"[SAN]\nsubjectAltName=DNS:Apache2021.kaheksa.xi,DNS:
Apache5.kaheksa.xi")) -out Apache2021.csr -nodes
```

³ Kaasaegsed veebilehitsejad ei pea veebilehte usaldusväärseks, kui vähemalt üks SAN DNS ei vasta veebilehe tegelikule aadressile.



```
uv@Ubuntu8: ~$ openssl req -newkey rsa:2048 -keyout Apache2021.key -sha256 -subj
"/CN=Apache5.kaheksa.xi" -reqexts SAN -config <(cat /etc/ssl/openssl.cnf <(print
F "[SAN]\nsubjectAltName=DNS:Apache2021.kaheksa.xi,DNS:Apache5.kaheksa.xi")) -ou
t Apache2021.csr -nodes
Generating a RSA private key
.....+++++
.+++++
writing new private key to 'Apache2021.key'
-----
uv@Ubuntu8:~$
```

Pilt 9 - privaatvõtme ja sertifikaadi päringu genereerimine

Kollase taustaga parameetrid:

1. Apache2021.key on sertifikaadi privaatvõti;
2. Apache2021.csr on sertifikaadi päringufail, mis edastatakse sertifitseerimiskeskusele;
3. Apache5.kaheksa.xi on väljastatava sertifikaadi subjekt;
4. Apache2021.kaheksa.xi ja Apache5.kaheksa.xi on sertifikaadil olevad SAN DNS nimed, mis peavad kindlasti vastama veebilehe tegelikule aadressile⁴. Need nimed peavad ka nimeserveris lahenema.

Loodud sertifikaadi päringufaili sisu on võimalik vaadata käsuga

```
openssl req -in Apache2021.csr -noout -text
```

⁴ Kaasaegsed veebilehitsejad ei pea veebilehte usaldusväärseks, kui vähemalt üks SAN DNS ei vasta veebilehe tegelikule aadressile.



Ubuntu/Apache2 SSL häälestus

Lihtne konfiguratsioonijuhend Eesti ID-kaartide vaates

```
uv@Ubuntu8: ~  
File Edit View Search Terminal Help  
uv@Ubuntu8:~$ openssl req -in Apache2021.csr -noout -text  
Certificate Request:  
Data:  
  Verston: 1 (0x0)  
  Subject: CN = Apache5.kaheksa.xl  
  Subject Public Key Info:  
    Public Key Algorithm: rsaEncryption  
    RSA Public-Key: (2048 bit)  
    Modulus:  
      00:c9:4f:a2:54:bd:1a:bb:88:a6:ec:16:c9:3e:28:  
      ee:f6:f6:09:3a:d7:e6:8f:a6:7a:4e:57:3b:38:70:  
      70:73:b0:01:95:7a:8d:c3:47:46:49:b9:12:52:20:  
      08:0c:ed:f5:ec:c5:4e:25:3e:27:9b:98:67:b0:bd:  
      c2:cd:00:98:54:36:d4:bf:b8:60:d9:aa:26:de:6a:  
      da:11:23:2e:a9:05:94:ff:e8:bb:d2:5e:c2:68:8d:  
      63:97:71:5e:0a:a0:49:fc:27:c7:28:c4:7d:53:12:  
      1c:e6:2e:9d:bd:81:5b:ff:6a:e5:cf:b5:1a:1b:a3:  
      5a:2e:9b:bd:0c:fe:c8:8f:ed:ff:b6:08:9a:1a:69:  
      4f:88:a1:1c:c7:9d:84:53:f0:77:2f:db:ba:2a:9a:  
      16:f4:78:02:ca:e2:29:f7:f0:f3:61:df:00:ce:3f:  
      fa:80:c5:ca:2d:37:a4:2e:a4:8c:be:a2:b3:c9:fd:  
      46:4e:20:fb:18:8b:3d:09:6a:be:01:3d:af:29:dd:  
      e2:b6:63:3c:3e:46:c1:7a:9b:08:83:c9:32:c5:54:  
      b2:e6:3d:a3:68:b6:8d:53:cb:36:c2:20:7d:77:63:  
      c7:cf:c9:11:36:b3:47:9b:10:8f:19:66:cb:a4:0f:  
      50:f5:35:bf:0d:53:82:cb:ad:3c:1f:5a:1a:2b:70:  
      a4:8f  
    Exponent: 65537 (0x10001)  
  Attributes:  
  Requested Extensions:  
    X509v3 Subject Alternative Name:  
      DNS:Apache2021.kaheksa.xl, DNS:Apache5.kaheksa.xl  
  Signature Algorithm: sha256WithRSAEncryption
```

Pilt 10 – loodud sertifikaadi päringufaili sisu

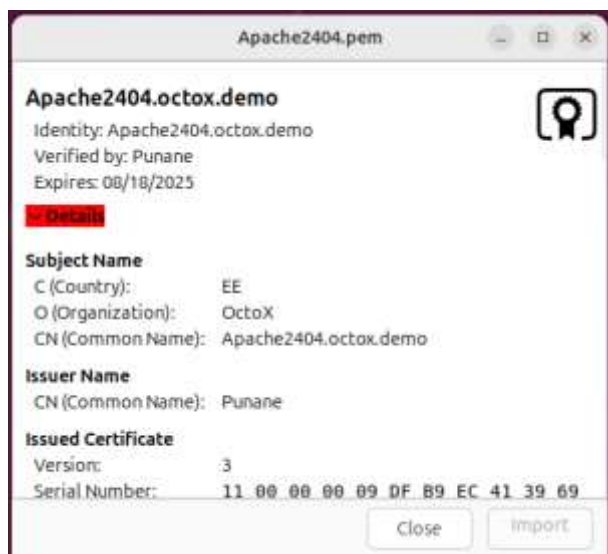
SSL sertifikaadi tellimine ja paigaldamine

Järgnevalt tuleb saata sertifikaadi päringufail **Apache2404.csr** mõnele usaldusväärsele sertifitseerimiskeskele. Näidiskonfiguratsiooni tingimustes on sertifikaadi väljastajaks testkeskkonna sertifitseerimiskeskus. Allkirjastatud sertifikaat väljastatakse Base64 kodeeritud formaadis:

```
-----BEGIN CERTIFICATE-----  
MIICGQCCA26gAwIBAgITEQAAAAAnFuexBOWmmSgAAAAAACTAKBggqhkJOPQQAzAR  
MQ8wDQYDVQQDEwZkdW5hbmUwHhcNMjQwODE0MTQ0MzUzW3hcnmJwODE0MTQ1MzU3  
WjA9MQswCQYDVQQGEwJFRTEOMwGA1UEChMFT2N0b1gxHjAcBgNVBAMTFUFwYWN0  
ZTI0MDQub2N0b3guZGVtbzB2MBAgByqGSM49AgEG8SuBBAIA2IABNub/owRhwCx  
cZtUBjpbcbCJBNypdVJUQjkHIYRRt1sHYQ1b54L/YF1zn15z7gNHZ0m5v6S4Gdf  
cS00JCsRvwj2Ygw+vtx99DJunq5ec1/9Q3Sr-jX3YkbbhUvn2U6nfZK0B1zCB1DA4  
BgNVHREEMTAvgHVBcGFjaGUyNDh0Lm9jdG94LmR1bW+CFk1ZV8VCUR8V5VksVLe9j  
dG94LmR1bWbWbHQYDVR80BBYFAzQZ0UgEIJvGNYZ7qtHYVe5bcyIMB8GA1UdIwQY  
MBaAFNwUsh5iVKVBo6FY8ap5K16W+9UTMAwGA1UdEwEB/wQMAAwCGYIKoZIzj0E  
AwMDAFAwZQIwdn+C8whTsYVnZ4axxQhtAx5ak0/kZGEtpWe32x2kyjE1Z0W+RIyn  
cuFwt1CgYIHLAjeAqj69bKlQ5DhQr4FBVMr1V56fp6FjPH7qsHw5USUgYnFAL51u  
o6DunYynxvZsunE5  
-----END CERTIFICATE-----  
Rid 3, Vig 27 786 täkki 100% Windows (CRLF) UTF-8
```

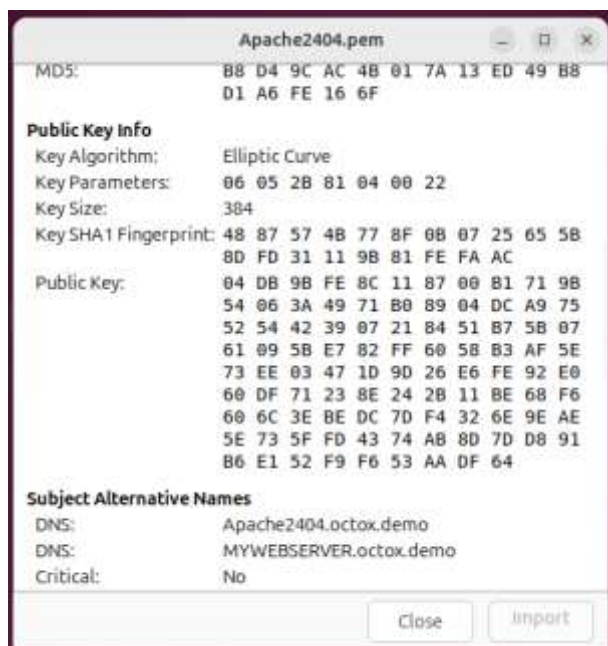
Pilt 11 – sertifikaat pem-formaadis tekstiredaktoris

Avades sertifikaadi Ubuntu failihalduris on näha järgmist:



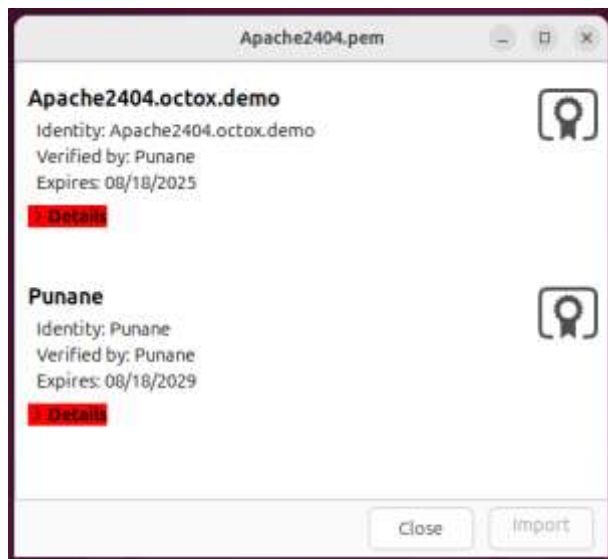
Pilt 12 – ECC sertifikaat Ubuntu failihalduris

Sertifikaadis on kirjas ka algoritm ja alternatiivsed subjekti DNS nimed:



Pilt 13 – algoritm ja SAN DNS nimed

Nagu näha, on sertifikaadi väljaandjaks sertifitseerimiskeskus nimega „Punane“. Nüüd tuleb luua sertifikaadi fail, milles paiknevad nii tulevane veebiserveri TLS sertifikaat kui ka selle väljaandjate ahel. Selleks tuleb lisada veebiserveri sertifikaadifailile pem formaadis ka väljastaja sertifikaat pem formaadis ja salvestada faili nimega **Apache2404.pem**.



Pilt 14 – veebiserveri sertifikaadiahel Ubuntu

Loodud fail tuleb paigaldada kausta **/etc/ssl/certs**. Lisaks peab veebiserveri sertifikaadi privaatvõtme paigaldama kausta **/etc/ssl/private**.



Pilt 15 - sertifikaadi ja selle privaatvõtme asetamine konteinerisse

Nüüd on Apache2 serveripoolsed sertifikaadid olemas ja korrektselt failisüsteemi paigaldatud.

Virtuaalse veebilehe loomine

Loo enda konfiguratsioonile eraldiseisev virtuaalne veebileht. Esmalt tuleb luua kaust **/var/www/Apache2404**, kuhu paigaldada veebilehe sisu.



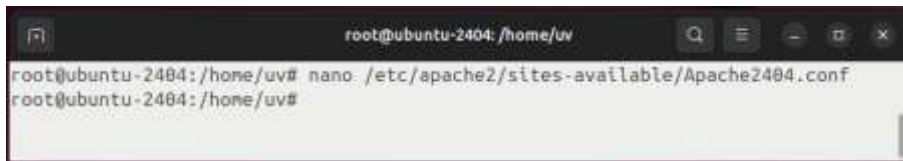
Pilt 16 - kausta loomine veebifailidele

Paigalda loodud kausta mõni lihtne ja äratuntav veebileht. Siin näites võtame testimiseks vaikimisi lehe kaustast **/var/www/html/index.html**. Oma näites muudame pisut kopeeritud lehe päist ja sisu veendumaks, et veebileht võetakse ikka õigest kohast.

Järgmiseks tee valmis virtuaalse veebilehe konfiguratsioonifail. Tee uus fail nimega **/etc/apache2/sites-available/Apache2404.conf** käsuga



```
nano /etc/apache2/sites-available/Apache2404.conf
```



```
root@ubuntu-2404: /home/uv
root@ubuntu-2404: /home/uv# nano /etc/apache2/sites-available/Apache2404.conf
root@ubuntu-2404: /home/uv#
```

Pilt 17 – uue konfiguratsioonifaili tegemine

Nüüd muuda uut konfiguratsioonifaili vastavalt oma soovidele. Lisa sinna järgmine sisu:

```
# Faili algus
```

```
<Virtualhost Apache2404.octox.demo:80>
```

```
# Pöördudes http saidi poole juhatakse meid kahe järgmise rea abil
automaatselt https saidile.
```

```
    ServerName Apache2404.octox.demo
    redirect / https://Apache2404.octox.demo
```

```
</Virtualhost>
```

```
<VirtualHost Apache2404.octox.demo:443>
```

```
# Üldinfo
```

```
    ServerName Apache2404.octox.demo:443
    DocumentRoot /var/www/Apache2404
```

```
# SSL häälestus
```

```
    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/Apache2404.pem
    SSLCertificateKeyFile /etc/ssl/private/Apache2404.key
```

```
# Vigade kogumise häälestus
```

```
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
```

```
</Virtualhost>
```

```
# Faili lõpp
```

Aktiveeri loodud konfiguratsioon käsuga

```
a2ensite Apache2404.conf
```

ja taaskäivita Apache2 teenus.



```
root@ubuntu-2404: /home/uv
root@ubuntu-2404: /home/uv# a2ensite Apache2404.conf
Enabling site Apache2404.
To activate the new configuration, you need to run:
systemctl reload apache2
root@ubuntu-2404: /home/uv# systemctl reload apache2
root@ubuntu-2404: /home/uv#
```

Pilt 18 - veebilehe lubamine ja Apache2 taaskäivitus

Nüüd saab veebilehe poole pöördumiseks kasutada ühepoolset SSLi. Samuti suunatakse automaatselt aadressilt <http://Apache2404.octox.demo> aadressile <https://Apache2404.octox.demo>.



Pilt 19 - Apache veebiserver töötab ja kasutab ühepoolset SSLi

Märkus: Sarnaseid virtuaalseid veebilehti erinevate nimede ja sama IP-aadressiga võib Apache2 veebiserverile luua mitmeid.

Kahepoolse sertifikaadinõude (SSLi) kehtestamine

Kui on soov võimaldada veebilehele ligipääs Eesti ID-kaardiga autentides, tuleb olemasolevat konfiguratsiooni pisut täiendada.

Lisa Apache2404.conf failile järgmised read SSL sektsiooni:

```
SSLVerifyClient                                require
SSLVerifyDepth                                2
SSLCACertificateFile /etc/ssl/certs/EID_Bundle.pem
```



```
root@ubuntu2204: ~
GNU nano 6.2 /etc/apache2/sites-available/Apache2204.conf *
# Certificates
  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/Apache2204.pem
  SSLCertificateKeyFile /etc/ssl/private/Apache2204.key
# Revocation and filtering.
  SSLVerifyClient require
  SSLVerifyDepth 2
  SSLCACertificateFile /etc/ssl/certs/EID_Bundle.pem
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

Pilt 20 - selline on uus konfiguratsioonifaili SSL osa

Nüüd tuleb luua uus tekstifail **EID_Bundle.pem**⁵, kuhu tuleb lisada eID juur- ja kesktaseme sertifikaadid Base64 kodeeritud kujul (EE-GovCA2018, ESTEID2018, EEGovCA2025, ESTEID2025). Selle faili abil saab välja filtreerida kõik sertifitseerimiskeskused, mille alt väljastatud sertifikaate uus loodud veebileht toetab. Kasutajale näidatakse vaid neid sertifikaate, mis on väljastatud eelloetletud ahelatest. Ubuntu avatuna näeb fail välja järgmine:

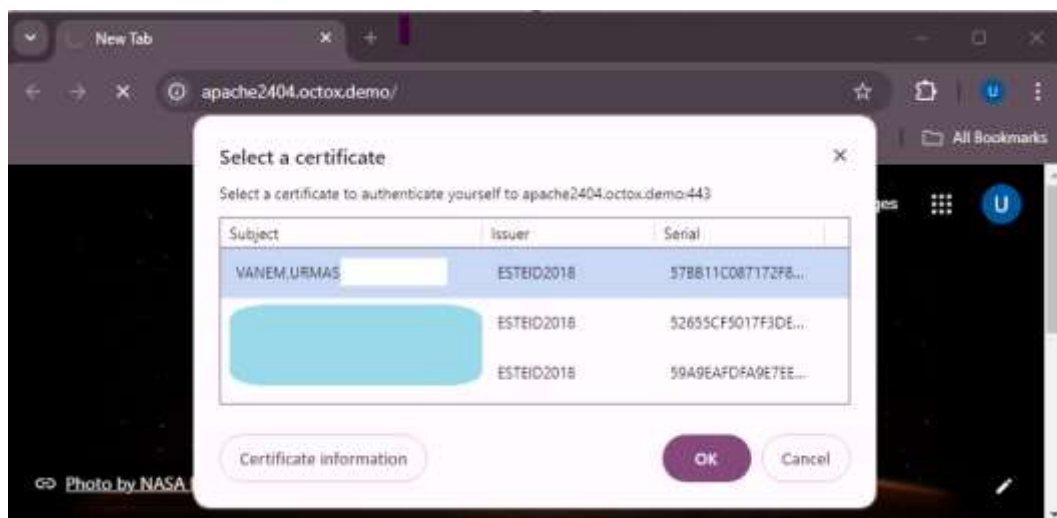
⁵ Saadaval: EIDBundle.pem



Pilt 21 – juur- ja kesktaseme sertifikaadid ühes failis

Salvesta loodud fail nimega **EID_Bundle.pem** ja kopeeri see kausta **/etc/ssl/certs**. Veebiserveris muudatuse jõustumiseks taaskäivita Apache2 käsuga „systemctl reload apache2“.

Pöördudes pärast muudatuse jõustumist uuesti veebilehe **Apache2404.octox.demo** poole, küsitakse kasutaja sertifikaati.



Pilt 22 - kasutaja sertifikaadi päring



Server pakub kasutajale välja sertifikaadid, mille väljastajad on kirjeldatud failis **EID_Bundle.pem**. Pärast sertifikaadi kinnitamist ja PIN-koodi sisestamist lubatakse kasutaja veebilehele - kahepoolne SSL töötab.

Võimalikud lisakonfiguratsioonid

Käesoleva dokumendi eesmärk ei ole anda täpseid juhiseid optimaalseks veebilehete konfiguratsiooniks ega turvamiseks, vaid tutvustada konfiguratsiooni kahepoolse SSLi kasutamiseks Eesti ID-kaartidega. Siiski on oluline arvestada allolevaga.

Tulemüüri reegli loomine (vajadusel)

Tulemüüri reegli loomiseks tuleb terminalis käivitada käsk

```
ufw allow 'SOOVITAV REEGEL'
```

Näiteks ainult HTTPS liikluse lubamiseks tuleb käivitada

```
ufw allow 443/tcp
```

```
root@ubuntu-2404: /home/uv
root@ubuntu-2404:/home/uv# ufw enable
Firewall is active and enabled on system startup
root@ubuntu-2404:/home/uv# ufw allow 443/tcp
Rule added
Rule added (v6)
root@ubuntu-2404:/home/uv#
```

Pilt 23 - tulemüüri aktiveerimine ja HTTPS reegli loomine

Kui tulemüüri staatus on aktiivne (**ufw enable**), siis päring **ufw status** näitab olemasolevaid reegleid.

```
root@ubuntu-2404: /home/uv
root@ubuntu-2404:/home/uv# ufw status
Status: active

To Action From
--
443/tcp ALLOW Anywhere
443/tcp (v6) ALLOW Anywhere (v6)

root@ubuntu-2404:/home/uv#
```

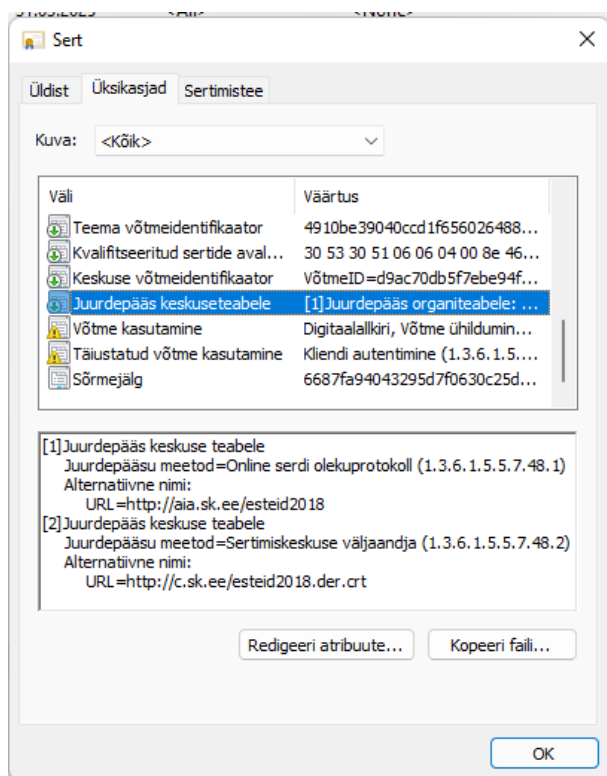
Pilt 24 - tulemüür on aktiivne ja ainult HTTPS liiklus on lubatud



Kasutaja sertifikaadi staatuse kontroll OCSP teenuse vastu⁶

OCSP (*Online Certificate Status Protocol*) teenuse abil saab kasutaja sertifikaadi staatust kontrollida reaajas. Iga kasutaja autentimisel saadab veebiserver päringu OCSP teenusele, mis tagastab sertifikaadi staatuse info.

SK ja Zetes pakuvad vaba ligipääsuga (tasuta) AIA OCSP teenust. ESTEID2018 ja ESTEID2025 CA alt väljastatud sertifikaatide puhul on AIA OCSP aadress juba sertifikaadis kirjas (<http://aia.sk.ee/esteid2018>, <http://ocsp.eidpki.ee>).



Pilt 25 – ESTEID2018 AIA OCSP aadress sertifikaadis

Lubamaks kasutaja sertifikaadi staatuse kontrolli sertifikaadis määratud AIA OCSP teenuse abil, tuleb Apache2 SSL konfiguratsiooni lisada järgmised read:

```
SSLCOSEnable leaf # - lubab OCSP kontrolli kasutaja sertifikaatidele.  
SSLCOSEnableUseRequestNonce off # - lülitab välja OCSP teenuse vastuse nonce nõude.
```

⁶ Sertifikaatide kehtivust on võimalik kontrollida ka sertifikaatide tühistusnimekirjade (CRL) abil, ent sellel käesolevas dokumendis ei peatuta, kuna OCSP-põhine lahendus on eelistatum.



```
root@ubuntu2204: -
GNU nano 6.2 /etc/apache2/sites-available/Apache2204.conf
# Certificates
  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/Apache2204.pem
  SSLCertificateKeyFile /etc/ssl/private/Apache2204.key

# Revocation and filtering.
  SSLVerifyClient require
  SSLVerifyDepth 2
  SSLCACertificateFile /etc/ssl/certs/EID_Bundle.pem

# AIA-OCSP
  SSLOCSPEnable leaf
  SSLOCSPUseRequestNonce off

G Help      O Write Out  W Where Is  K Cut       T Execute   C Location
X Exit      R Read File  N Replace   U Paste     J Justify   / Go To Line
```

Pilt 26 – AIA OCSP konfiguratsioon on lisatud

Taaskäivita Apache2 veebiteenus käsuga **systemctl reload apache2**. Ülaltoodud konfiguratsiooni puhul võetakse OCSP teenuse aadress kasutaja sertifikaadist.

Vaikimisi veebilehe eemaldamine

Apache2 paigaldusega paigaldatakse ka vaikimisi veebileht. Selle eemaldamiseks lahendusest tuleb terminalis anda käsk **a2dissite 000-default.conf** ja aktiveerida muudatus käsuga **systemctl reload apache2**.

```
root@ubuntu2204:/home/uv/temp
root@ubuntu2204:/home/uv/temp# a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
systemctl reload apache2
root@ubuntu2204:/home/uv/temp# systemctl reload apache2
root@ubuntu2204:/home/uv/temp#
```

Pilt 27 – vaikimisi veebilehe eemaldamine

Soovituslikud Apache turvasätted

SSL/TLS

Apache versioonil 2.4.55 on vaikimisi lubatud kõik SSL/TLS protokollid, mis on uuemad kui SSL3:

```
root@ubuntu2204:/home/uv/temp
root@ubuntu2204:/home/uv/temp# grep -I -r "SSLProtocol" /etc/apache2/nods-availa
ble/
/etc/apache2/nods-available/ssl.conf:SSLProtocol all -SSLv3
root@ubuntu2204:/home/uv/temp#
```

Pilt 28 - Apache SSL/TLS vaikimisi konfiguratsioon

Tänapäeval on tungivalt soovitatav mitte kasutada TLS protokollid versioonist 1.2 madalamaid versioone. Juba mõnda aega on kasutusel ka TLS versioon 1.3.



Kui puudub spetsiifiline nõue TLS 1.2 versiooni lubamiseks, siis on soovitatav kasutada vaid TLS versiooni 1.3. TLS 1.2 on küll korrektse konfiguratsiooni puhul väga stabiilne ja turvaline, ent TLS 1.3 on kiirem, vaikumisi turvalisem ja nõuab vähem konfigureerimist. Standardlahendustes võiks TLS 1.2 olla toetatud vaid tõestatud vajaduse puhul ja sel juhul tuleb olla veendunud, et kasutusel on vaid turvalised šifrikomplektid ja laiendused.

Kui on soov Apache serveris kasutada vaid protokoll TLS 1.3, tuleb konfiguratsioonifaili lisada rida

```
SSLPROTOCOL -all +TLSv1.3
```

```
SSLPROTOCOL -all +TLSv1.3
```

Pilt 29 - konfiguratsioonifailis lubatakse ainsa protokollina TLS 1.3

Toetamaks TLS versioone 1.2 ja 1.3, tuleb konfiguratsioonireale lisada **+TLSv1.2**

Alternatiivina saab sama muudatuse teha serveripõhiselt konfigureerides parameetrit SSLPROTOCOL failis `/etc/apache2/mods-available/ssl.conf`.

Rohkem infot TLS protokollide kasutamise soovitude kohta leiab RIA tellitud krüptograafiliste algoritmide elutsükli uuringust aadressil <https://www.id.ee/artikkel/krüptograafiliste-algoritmide-elutsükli-uuringud-2/>.

Šifrikomplektid (*Cipher suites*)

TLS 1.3 versiooni kõiki šifreid peetakse hetkeseisuga turvaliseks, seega turvakaalutlustel selle protokolliga jaoks lisakonfiguratsiooni looma ei pea.

TLS 1.2 puhul see päris nii ei ole. Apache 2.4.55 versiooniga on vaikumisi kasutusel suur hulk erinevaid TLS šifreid⁷, mida näeb käsuga

```
openssl ciphers -v
```

Vaikumisi on šifrite kasutamise osas defineeritud ainult kaks reeglit:

- 1) HIGH – lubatud on mõned šifrid võtme pikkusega 128 bitti ja kõik tugevamad;
- 2) !aNULL – keelatud on šifrite komplektid, mis ei toeta autentimist.

```
SSLCipherSuite HIGH:!aNULL
```

Pilt 30 - serveripõhise konfiguratsiooni kirjeldus failis /etc/apache2/mods-available/ssl.conf

Kui on soov määrata täpsemalt TLS 1.2 protokolliga kasutatavaid šifrikomplekte, saab Apache kaustapõhises konfiguratsioonifailis kasutada käsku SSLCIPHERSUITE. Siin omakorda saab kasutada kas eeldefineeritud muutujaid või täpseid šifrikomplektide kirjeldusi.

⁷ Siin ei käsitleta teiste TLS protokollide šifreid, kuna versioonist 1.2 vanemad protokollid on eelduslikult keelatud ja 1.3 versioon on hetkel eelistatim.



Kindlat soovitus erinevate šifrikomplektide kasutamiseks ei ole võimalik ilma veebilehele esitatavaid tingimusi teadmata anda. Küll aga tuleb kindlasti eemaldada loendist ebaturvalised šifrikomplektid. Mõistlik on kirjeldada konkreetseid lubatud šifrikomplektid TLS 1.2 kasutamiseks.

Näide:

- Kasutades konfiguratsioonifailis järgmist käsurida:
SSLCIPHERSUITE 'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384'
lubatakse vaid kirjeldatud šifrikomplektide kasutamine.

Alternatiivina saab kasutatavaid šifreid konfigurereida serveripõhiselt failis /etc/apache2/mods-available/ssl.conf muutes selles parameetrit SSLCIPHERSUITE.

Rohkem infot šifrikomplektide soovitusete kohta leiab RIA tellitud krüptograafiliste algoritmide elutsükli uuringust aadressil <https://www.id.ee/artikkel/krüptograafiliste-algoritmide-elutsykli-uuringud-2/>.

SSLHONORCIPHERORDER

Oluline šifritega seotud parameeter on ka SSLHONORCIPHERORDER, mille väärtus on soovitatav konfiguratsioonifailis määrata ON asendisse. Sel juhul eelistatakse serveri šifrikomplektide valikut kasutaja omale. Vaikimisi on see parameeter määramata ja vaikimisi väärtuseks on määratud „off“.

Kasutajasertifikaatide lisafiltreerimine

Oluline! Kindlustamaks, et veebiteenuse poole saavad pöörduda vaid korrektsete sertifikaatidega kasutajad, tuleb serveri konfiguratsioonis kehtestada järgmised nõuded:

- 1) sertifikaadis peab olema korrektne väli *extendedKeyUsage*;
- 2) sertifikaadi väljastaja peab olema ESTEID2018 või ESTEID2025.

Selleks tuleb lisada Apache konfiguratsiooni read:

```
<Location "/">
Require expr ( \
  (%{SSL_CLIENT_I_DN_CN} == "ESTEID2018" || %{SSL_CLIENT_I_DN_CN} ==
  "ESTEID2025") \
  and "TLS Web Client Authentication, E-mail Protection" in
  PeerExtList('extendedKeyUsage') \
)
</Location>
```

Selle konfiguratsiooni võib lisada kas virtuaalse hosti või Apache serveri üld-konfiguratsiooni juurde. Pärast ülaltoodud tingimuste lisamist on teenuse poole lubatud pöörduda vaid sertifikaatidega millel on korrektne *extendedKeyUsage* väli ning mis on väljastatud serveri poolt lubatud ahelast.

Märkused:

- Kui on kasutusel mõni muu liikluse filtreerimise vahend/võimalus, siis on soovitatav turvaline konfiguratsioon juurutada ka seal. SK on F5 konfiguratsiooni osas publitseerinud järgmise



informatsiooni (vt. peakükki „Only accept certificates with trusted key usage“): <https://github.com/SK-EID/smart-id-documentation/wiki/Secure-Implementation-Guide>

- SK soovitusel turvaliseks autentimiseks ID-kaardiga on leitavad peatükist „Defence: implement ID-card authentication securely“: <https://github.com/SK-EID/smart-id-documentation/wiki/Secure-Implementation-Guide>
- Soovituslik meetod ebakorreksete sertifikaatide vältimiseks on kasutada sertifikaatides olevaid OIDE. Paraku ei ole hetkeseisuga teada meetodit, kuidas seda serveri tasemel teha. Võimalusel tuleks võtta autentimise sertifikaat veebirakenduse tasemel lahti ja kontrollida, kas see sisaldab mõnda korrektset OIDI ning kui ei sisalda, siis mitte autentida. Hetkeseisuga teadaolevad OIIDid on SK publitseerinud peatükis „Only accept certificates with trusted issuance policy“: <https://github.com/SK-EID/smart-id-documentation/wiki/Secure-Implementation-Guide>

Kasutajale kuvatavate sertifikaatide filtreerimine

Vaikimisi konfiguratsioonis ei piirata kasutajale kuvatavate sertifikaatide valikut, mis tähendab, et veebiserverisse autentimisel näidatakse kasutajale kõiki kasutaja käsutuses olevaid autentimise sertifikaate. Korrektne on kasutajale näidata aga vaid neid sertifikaate, mis on väljastatud ahelatest ESTEID2018 või ESTEID2025. Selleks tuleb:

- 1) luua aktsepteeritud ahelate fail **/etc/ssl/certs/DN_Bundle.pem**⁸
- 2) panna sinna ESTEID2018 ja ESTEID2025 sertifikaadid Base64 kodeeringus
- 3) lisada Apache SSL häälestuse sektsiooni direktiiv
SSLCADNRequestFile /etc/ssl/certs/DN_Bundle.pem
ja uus konfiguratsioon salvestada
- 4) taaskäivitada Apache server käsuga
systemctl reload apache2

Nüüd saadab Apache server kasutajale info, et toetatud on ainult ESTEID2018 ja ESTEID2025 ahelatest väljastatud sertifikaadid ning kasutajale kuvataksegi ainult selle CA poolt väljastatud sertifikaate.

HTTP Strict Transport Security (HSTS) lubamine

1. Luba terminalis *mod-headers* käsuga
a2enmod headers

⁸ Saadaval DN_Bundle.pem



```
root@ubuntu2204: ~
root@ubuntu2204:~# a2enmod headers
Enabling module headers.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@ubuntu2204:~# systemctl restart apache2
root@ubuntu2204:~#
```

Pilt 31 – mod-headers lubamine (käesolevas näites HSTS tarbeks)

2. Lisa Apache konfiguratsioonifaili rida

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains"
```

```
# Enable HSTS.
Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"
```

Pilt 32 – HSTS aktiveerimine 30-ks päevaks

3. Konfiguratsiooni jõustamiseks taaskäivita Apache teenus.

Muud võimalused

Lisaks TLS ja šifrikomplektide häälestusele on soovitatav pöörata tähelepanu Apache serveri turvalisusele ka järgmiste punktide vaates:

- Hoida operatsioonisüsteem uuendatuna.
- Hoida Apache uuendatuna.
- Käidelda Apachet tavakasutaja õigustes.
- Keelata serveri info presenteerimine.
- Eemaldada ebaolulised moodulid.
- Lisada ja konfigureerida *Mod Security*.
- Lisada ja konfigureerida *Mod Evasive*.
- Keelata *listing* ligipääs vaikimisi kataloogile.
- Lubada logimine.
- ...

Ülaltoodu on näidisloend võimalustest Apache turvalisemaks muutmiseks. Põhjalikumaid soovitusi on võimalik leida internetist: <https://www.google.com/search?q=how+to+secure+apache+server>.



Appendix

EIDBundle.pem

```
EE-GovCA2018
-----BEGIN CERTIFICATE-----
MIIE+DCCBfmgAwIBAgIQMLOWlXoR0oFbj52nmRsneZAKBggqhkJOPQQDBDBaMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRCwFQYDVQRh
DA5OVFJFRS0xMDC0NzAxMzEVMBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkw
NTA5MTEwM1oXDTMzMDkwNTA5MTEwM1owWjELMAkGA1UEBhMCRUUXGzAZBgNVBAoM
E1NLElE1E1FNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOT1RSRUUtMTA3NDcwMTMxFTAT
BgNVBAMMDEVFLUdvdnkNBMjAxODCBmzAQBgqhkJOPQIBBgUrgQQAiwoBhgAEAMcb
/dmAcVo/b2azEPS6CFW7fEA2KuHKC53D7ShVnVlz4QUjCdTXjds/4u99jUoYEQec
luVVzmlgEJR1nkN2eOrLAZYxPjwG5Hi1liZEyW9QKVdeEgyvzhWWTNHGjV3HdZRv
7L9o4533PtJAYqJ90tIB9zCCAfmwCAYGBACPEgECMAkGBwQAL+xAAQIwMgYLKwYB
BAGDkSEBAQEwIzAhBggrBgEFBQCcARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMA0G
CysGAQQBg5EhAQECMA0GCysGAQQBg5F/AQEEMA0GCysGAQQBg5EhAQEFMA0GCysG
AQQBg5EhAQEGMA0GCysGAQQBg5EhAQEHMA0GCysGAQQBg5EhAQEDMA0GCysGAQQB
g5EhAQEEA0GCysGAQQBg5EhAQEIMA0GCysGAQQBg5EhAQEJMA0GCysGAQQBg5Eh
AQEKMA0GCysGAQQBg5EhAQELMA0GCysGAQQBg5EhAQEMMA0GCysGAQQBg5EhAQEN
MA0GCysGAQQBg5EhAQEOMA0GCysGAQQBg5EhAQEPMA0GCysGAQQBg5EhAQEQMA0G
CysGAQQBg5EhAQERMA0GCysGAQQBg5EhAQESMA0GCysGAQQBg5EhAQETMA0GCysG
AQQBg5EhAQEU0GCysGAQQBg5F/AQEEMA0GCysGAQQBg5F/AQEDMA0GCysGAQQB
g5F/AQEEA0GCysGAQQBg5F/AQEFMA0GCysGAQQBg5F/AQEGMA0GCysGAQQBg5Eh
CgEwIzAhBggrBgEFBQCcARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMBGCCSQAUF
BwEDBAwwCjAIBgYEA15GAQEwCgYIKoZIzj0EAwQDgYwAMIGIAkIBk698EquetY9Tt
6Hw050CfzdI1jKmlfCl34xkdU7J+wz1tNVu2tHJwEhdsH0e92i969sRDp1RNP1Vh
4XFJzI3oQFQCQgVxmcuVnsy7NUScDZ0erwovmbFOsNxELCANxNSWx5xMqzEiHv8
46opxu10UFDIBBPzkbBenL4h+g/WU71G78fIhA==
-----END CERTIFICATE-----
ESTEID2018
-----BEGIN CERTIFICATE-----
MIIFVzCCBliGAWIBAgIQdUf6rBR0S4tbo2bU/mZV7TAKBggqhkJOPQQDBDBaMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRCwFQYDVQRh
DA5OVFJFRS0xMDC0NzAxMzEVMBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkw
NTA5MTEwM1oXDTMzMDkwNTA5MTEwM1owWDELMAkGA1UEBhMCRUUXGzAZBgNVBAoM
E1NLElE1E1FNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOT1RSRUUtMTA3NDcwMTMxFTAT
BgNVBAMMCKVTVEVJRDIwMTgwgZswEAYHkoZiZj0CAQYFK4EEACMDgYYABAHHOB1v
7URPYP1yHhOb7RA/YBDbtgygnSVmQYdxnFrKHUXh6tFkghvHuA1k2DSom1he5kqh
B5VspDembwWDJBOQWGOI/0t3EtccLjYeM7F9xOPdzUbZaIbpNRHpQgVbPFX0xpL
TgW27MpImH08DHBWfPeAaNX3eUpD4gC5cvhsK0RFEqOCAx0wggMZMB8GA1UdIwQY
MBaAFH4pVuc0knhOd+FvLjMqmHhB/TSfMB0GA1UdDgQWBbTzrHDbx36+1Pig5L5H
otA0rZoaqEjAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAAQH/BAGwBgEB/wIBADCCAc0G
A1UdIASCAcQwggHAMAGBGAj3oBAJAjBgCEAIVsQAECMDIGCysGAQQBg5EhAQEB
MCMwIQYIKwYBBQUHAgEWFwh0dHBz0i8vd3d3LnNrLmV1L0NQUzANBgsrBgEEAYOR
IQEBAjANBgsrBgEEAYORfweBATANBgsrBgEEAYORIQEBBTANBgsrBgEEAYORIQEB
BjANBgsrBgEEAYORfweBBAZANBgsrBgEEAYORIQEBBzANBgsrBgEEAYORIQEBBDAN
BgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEBBTANBgsrBgEEAYORIQEBBzANBgsr
BgEEAYORIQEBBzANBgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEBBTANBgsrBgEE
AYORIQEBBzANBgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEBBTANBgsrBgEEAYOR
IQEBBTANBgsrBgEEAYORIQEBBzANBgsrBgEEAYORIQEBBDANBgsrBgEEAYORIQEB
FDANBgsrBgEEAYORfweBAJANBgsrBgEEAYORfweBAZANBgsrBgEEAYORfweBBBDAN
BgsrBgEEAYORfweBBBTANBgsrBgEEAYORfweBBzAqBgNVHSUBAf8EIDAeBggrBgEF
BQCDCQYIKwYBBQUHAgIGCCSQAUFBwMEMGoGCCSQAUFBwEBBF4wXDAPBggrBgEF
BQCcAwYydaHR0cDovL2FpY290Y290Y290Y290Y290Y290Y290Y290Y290Y290Y290
I2h0dHA6Ly9jLnNrLmV1L0VFLUdvdnkNBMjAxOC5kZXIuY3J0M0BgGCCSQAUFBwED
BAwwCjAIBgYEA15GAQEwMAYDVR0fBCKwJzAlc0CgIYYfaHR0cDovL2Muc2suZWUv
RUUtR292Q0EyMDE4LmNybDAKBggqhkJOPQQDBA0BjAAwGyGcQgDeUUY4HczUbFKS
002HZ88gclgYdzthqglENyTmtXE6dMBRnCbGUmhBCAA0mJSHbyFJ8W9iKLiSyurm
kJM0hDE9KgJCSAQa405Ia5nKjTJPNsHQ1mi7KZsIcTH0oBccx+54N8ZX1MgBozJ
mT59rZY/2/OeE163BAwD0UduQUAnMPP6+W3Vd
-----END CERTIFICATE-----
EEGovCA2025
```




```
002HZ88gclgYdzthgglENyTMtXE6dMBRnCbGUmhBCAA0mJSHbyFJ8W9ikLiSyurm
kJM0hDE9KgJCASOqA405Ia5nKjTJPNsHQ1Mi7KZsIcTHOoBccx+54N8ZX1MgBozJ
mT59rZY/2/OeE163BAwD0UduQAAnMPP6+W3Vd
-----END CERTIFICATE-----
ESTEID2025
-----BEGIN CERTIFICATE-----
MIIDDzCCApagAwIBAgIUUFQrcGtK7/jCP+GyAOTFvbglGlcwCgYIKoZIzj0EAwMw
WDEUMBIGAlUEAwWLRUVHb3ZDQTIwMjUxUzAVBGNVbGEMdk5UUKVFLTE3MDY2MDQ5
MR0wGAYDVQQKDBFhZXRlc3RvbmlhIE/DnDELMAkGA1UEBhMCRUUWHhcNMjUw
NTA3MTMyMDA3WhcNNDAwNTA3ZTM3MDY2MDQ5WjBXRMRwEQYDVQDDApFU1RFSUQyMDI1
MRcwFQYDVQRhDA50VFFFRS0xNzA2NjA0OTEaMBGGA1UECgwRWmV0ZXMGdXN0b25p
YSBPw5wxCzAJBgNVBAYTAkVFMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEdSEmb1An
xN7G22CCEQ3ts2YZNIEtUZP4Vc4iObhmL/um4EXkia4HgyCiR5T6o1KAEkPdxFBs
fmcLoPN+TmBO8ZpLGEqy1Vwf59ahDW7dQiLXTIAEiGCoXSWI9MvtHDZ2o4IBIDCC
ARwwEgYDVR0TAAQH/BAgwBgEB/wIBADAFBgNVHSMEGDAWgBSqgKibD7tLpn7FAvRy
zSxpSnZtzBABggrBgEFBQCBAQQ0MDIwMAYIKwYBBQUHMAKGJGh0dHA6Ly9jcncQu
ZWLkccGtpLmVlL0VFR292Q0EyMDI1LmNydDA9BgNVHSAENjA0MDIGBFUdIAAwKjAo
BggrBgEFBQCcARYcaHR0cHM6Ly9yZXBvc210b3J5LmVpZHBraS51ZTA1BgNVHR8E
LjAsMCcGqKAmhiRodHRwOi8vY3JsLmVpZHBraS51ZS9FRUdvdkmNBMjAyNS5jcmww
HQYDVR0OBBYEFJLAOLC4NhJo9crtZu5HKohtpo3oMA4GA1UdDwEB/wQEAWIBBjAK
BggqhkjOPQDAwNnADBKAjANipgLQqdM985dSFZfKvU9A7Sz2YdmmUSZBxu01L7Q
XKzqa0ZDyXmf03NPLNAC6dICMBQiROZbLoPezO9LD1847UbENx85hloLlzwEwjqp
rY++Xj8FjCD1C9hnb1sVgj3XAA==
-----END CERTIFICATE-----
```