



UBUNTU NGNIX VEEBISERVERI KAHEPOOLSE SSLi HÄÄLESTUS EESTI ID-KAARTIDE VAATES

Dokumendi info	
Loomise aeg	08.02.2019
Tellijä	Riigi Infosüsteemi Amet
Autor	Urmas Vanem, OctoX
Versioon	25.10/1

Versiooni info		
Kuupäev	Versioon	Muutused/märkused
08.02.2019	19.02/1	Avalik versioon.
28.02.2019	19.02/2	Lisatud märkused kasutaja sertifikaatide kehtivuse kontrolli kohta. Vaikimisi veebilehe eemaldamine. Muutja: Urmas Vanem
12.12.2019	19.12/1	Lisatud Nginx soovituslikud turvasätted. Muutja: Urmas Vanem
30.12.2020	20.12/1	Ubuntu uuendatud versioonile 20.04.1. Nginx uuendatud versioonile 1.19.6. Muudetud konfiguratsiooni haldamine (sites-... -> conf.d). Lisatud OCSP-põhiste tühistusnimekirjade kasutamise võimalus, soovituslikud turvasätted ja valede CAde sertifikaatide blokeerimise kirjeldus. Muutja: Urmas Vanem
13.01.2021	21.01/1	Lisatud demo-konfiguratsiooni fail. Lisatud HSTS konfiguratsioon. Muutja: Urmas Vanem
25.01.2021	21.01/2	Muudetud HSTS, SSL/TLS ja šifrite kasutamise soovitusi, lisatud täiendava turvalisuse tõstmise soovitusel. Muutja: Urmas Vanem
28.04.2021	21.04/1	Eemaldatud aegunud ESTEID-SK 2011 sertifikaatide tugi. Muutja: Urmas Vanem
25.11.2021	21.11/1	Uuendatud Ubuntu platvorm versioonile Ubuntu Server 21.10 ja Nginx platvorm versioonile 1.21.4,

Ubuntu/Nginx SSL häälestus



Lihtne konfiguratsioonijuhend Eesti ID-kaartide vaates

		lisatud ECC sertifikaatide loomine veebiserveril, täiendatud TLS ja Cipher soovitusi. Muutja: Urmas Vanem
22.02.2023	23.02/1	Ubuntu uuendatud versioonile Ubuntu Server 22.04 ja Nginx versioonile 1.23.3, uuendatud on ka virtuaalhosti konfiguratsioon. Muutja: Urmas Vanem
18.12.2023	23.12/1	Eemaldatud ESTEID-SK 2015 ahel. Muutja: Urmas Vanem
22.08.2024	24.08/1	Ubuntu uuendatud versioonile Ubuntu Server 24.04 ja Nginx versioonile 1.27.1. Muutja: Urmas Vanem
31.10.2025	25.10/1	Lisatud Zetes ahelad, eemaldatud SK OCSP lõik Muutja: Lauris Kaplinski



Sissejuhatus

Käesolevas juhendis kirjeldatakse:

- Kuidas paigaldada ja häälestada Nginx 1.28.0 veebiserver Ubuntu 24.04 serveril.
- Kuidas häälestada HTTPS (ühepoolne SSL) veebiserveril.
- Kuidas häälestada ID-kaartidega autentimine (kahepoolne SSL) veebiserveril.
- Kuidas turvata oma veebiserverit.

Lisaks on käsitletud muid konfiguratsioonivõimalusi, nt kuidas HTTP liiklus suunata HTTPS kanalisse jpm.

Nginx paigaldus ja häälestus

Paigaldus

Ubuntu 24.04 versiooni puhul paigaldatakse vaikumisi juhiste puhul Nginx versioon 1.24. Kuna aga soovime oma demojuhendis kasutada viimast versiooni 1.28.0, siis tuleb enne paigaldust teha täiendavaid muudatusi.

Nginx versiooni 1.28.0 paigaldamiseks Ubuntu versioonile 24.04 tuleb teha järgmised sammud (oktoober 2025):

1. Käivita terminalis käsk

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

```
parallels@ubuntu-linux-24-04-desktop: ~  
parallels@ubuntu-linux-24-04-desktop:~$ sudo add-apt-repository ppa:ondrej/nginx  
PPA publishes dbgshim, you may need to include 'main/debug' component  
Repository: 'Types: deb  
URIs: https://ppa.launchpadcontent.net/ondrej/nginx/ubuntu/  
Suites: noble  
Components: main  
'  
Description:  
This branch follows latest NGINX Stable packages compiled against latest OpenSSL for  
HTTP/2 and TLS 1.3 support.  
BUGS&FEATURES: This PPA now has a issue tracker: https://deb.sury.org/#bug-reporting
```

Pilt 1 – Nginx mainline paki lisamine

2. Käivita terminalis käsk



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
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:5 https://ppa.launchpadcontent.net/ondrej/apache2/ubuntu noble InRelease
Hit:6 https://ppa.launchpadcontent.net/ondrej/nginx-mainline/ubuntu noble InRelease
```

Pilt 2 - pakside uuendamine

3. Käivita terminalis käsk

apt install nginx-full

```
root@ubuntu-2404:/home/uv# apt install nginx-full
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libnginx-mod-http-auth-pam libnginx-mod-http-dav-ext libnginx-mod-http-echo
  libnginx-mod-http-geoip2 libnginx-mod-http-subst-filter
  libnginx-mod-http-upstream-fair libnginx-mod-stream
  libnginx-mod-stream-geoip2 nginx nginx-common
```

Pilt 3 - Nginx install

Nginx versiooni saab kontrollida ka käsuga

nginx -v

```
root@ubuntu-2404:/home/uv# nginx -v
nginx version: nginx/1.27.1
```

Pilt 4 - Nginx versioon on ootuspäraselt 1.27.1

Konfiguratsioon

Ühepoolse SSLi lubamine

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 Nginx2404.key
```

Seejärel genereeri privaatvõtme baasil sertifikaadi päringufail:



```
openssl req -new -key Nginx2404.key -out Nginx2404.csr -subj  
/C=EE/O=OctoX/CN=Nginx2404.octox.demo -reqexts SAN -config <(cat  
/etc/ssl/openssl.cnf <(printf  
"[SAN]\nsubjectAltName=DNS:Nginx2404.octox.demo,DNS:MYWEBSERVER.octo  
x.demo"))1
```

```
root@ubuntu-2404: /home/uv  
root@ubuntu-2404: /home/uv# openssl eparam -name secp384r1 -genkey -noout -out N  
ginx2404.key  
root@ubuntu-2404: /home/uv# openssl req -new -key Nginx2404.key -out Nginx2404.cs  
r -subj /C=EE/O=OctoX/CN=Nginx2404.octox.demo -reqexts SAN -config <(cat /etc/ss  
l/openssl.cnf <(printf "[SAN]\nsubjectAltName=DNS:Nginx2404.octox.demo,DNS:MYWEB  
SERVER.octox.demo"))  
root@ubuntu-2404: /home/uv#
```

Pilt 5 – ECC privaatvõtme ja sertifikaadi päringufaili loomine

Kollase taustaga argumendid:

1. Nginx2404.key on sertifikaadi privaatvõti;
2. Nginx2404.csr on sertifikaadi päringufail, mis edastatakse sertifitseerimiskeskusele;
3. CN=Nginx2404.octox.demo on väljastatava sertifikaadi *common name*;
4. DNS:Nginx2404.octox.demo ja DNS:MYWEBSERVER.octox.demo on sertifikaadil olevad SAN DNS nimed, mis peavad kindlasti vastama veebilehe tegelikule aadressile². Need nimed peavad ka nimeserveris lahenema.

Loodud sertifikaadi päringufaili sisu on võimalik vaadata käsuga

```
openssl req -in Nginx2404.csr -noout -text
```

¹ 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.

² Kaasaegsed veebilehitsejad ei pea veebilehte usaldusväärseks, kui vähemalt üks SAN DNS ei vasta veebilehe tegelikule aadressile.



```
root@ubuntu-2404:/home/uv# openssl req -ln Nginx2404.csr -noout -text
Certificate Request:
Data:
  Version: 1 (0x0)
  Subject: C = EE, O = OctoX, CN = Nginx2404.octox.demo
  Subject Public Key Info:
    Public Key Algorithm: id-ecPublicKey
    Public-Key: (384 bit)
    pub:
      04:83:8a:77:21:33:00:ac:6a:66:28:f4:7e:8e:98:
      fa:52:09:ed:bb:83:f9:98:ee:24:3b:48:b1:e2:ad:
      ae:1d:57:78:b1:9a:5c:c7:9c:4c:cb:95:f9:ff:b1:
      89:4f:d8:c9:e1:39:0e:5d:ac:c6:d3:92:64:39:23:
      5c:d0:fc:0e:38:17:22:3c:bb:e0:fb:ca:2c:8e:55:
      65:2b:7c:56:6a:55:4a:b8:ae:a4:8c:e5:81:b7:a9:
      d6:e4:5a:1a:aa:af:37
    ASN1 OID: secp384r1
    NIST CURVE: P-384
  Attributes:
    Requested Extensions:
      X509v3 Subject Alternative Name:
        DNS:Nginx2404.octox.demo, DNS:MYWEBSERVER.octox.demo
  Signature Algorithm: ecdsa-with-SHA256
  Signature Value:
```

Pilt 6 – 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 NGINX20PRIV.key -sha256 -subj
"/CN=Nginx20.kaheksa.xi" -reqexts SAN -config <(cat
/etc/ssl/openssl.cnf <(printf "[SAN]\nsubjectAltName=DNS:
Nginx20.kaheksa.xi,DNS: Nginx22.kaheksa.xi ")) -out NGINX20.csr -
nodes
```

```
root@Ubuntu2020:/home/uv# openssl req -newkey rsa:2048 -keyout NGINX20PRIV.key -
sha256 -subj "/CN=Nginx20.kaheksa.xi" -reqexts SAN -config <(cat /etc/ssl/openssl
l.cnf <(printf "[SAN]\nsubjectAltName=DNS: Nginx20.kaheksa.xi,DNS: Nginx22.kahek
sa.xi ")) -out NGINX20.csr -nodes
Generating a RSA private key
.....+++++
.....+++++
writing new private key to 'NGINX20PRIV.key'
-----
```

Pilt 7 - privaatvõtme ja sertifikaadi päringufaili genereerimine

Kollase taustaga muutujad:

1. NGINX20PRIV.key on sertifikaadi privaatvõti;



2. NGINX20.csr on sertifikaadi päringufail, mis edastatakse sertifitseerimiskeskusele;
3. Nginx20.kaheksa.xi on väljastatava sertifikaadi subjekt;
4. Nginx20.kaheksa.xi ja Nginx22.kaheksa.xi on sertifikaadil olevad SAN DNS nimed, mis peavad kindlasti vastama veebilehe tegelikule aadressile³. Need nimed peavad ka nimeserveris lahenema (piisab ka ühest nimest).

Loodud sertifikaadi päringufaili sisu on võimalik vaadata käsuga

openssl req -in NGINX20.csr -noout -text

```
root@Ubuntu2020:/home/uv# openssl req -in NGINX20.csr -noout -text
Certificate Request:
  Data:
    Version: 1 (0x0)
    Subject: CN = Nginx20.kaheksa.xi
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:f1:62:c3:ed:1d:0b:ea:cb:7c:22:17:41:1e:e3:
        c1:02:a6:7b:f3:72:13:ae:8d:72:72:6f:09:77:d6:
        51:84:4b:2a:f0:7b:65:9d:9f:f3:2a:0c:16:e5:26:
        47:79:aa:3e:c8:4c:50:62:5b:6c:2a:49:ea:51:81:
        68:5c:94:2c:d6:1d:78:70:eb:41:88:6c:09:c8:2f:
        e4:d5:bb:2f:fb:ec:2f:9d:0c:42:66:b5:de:91:e3:
        60:62:ff:94:11:21:aa:de:bb:52:bd:20:a6:ff:b4:
        c3:92:0a:5b:b5:fc:2f:8b:bc:44:3e:b4:5b:a4:ec:
        de:49:16:b6:c9:13:ed:d6:e2:ee:d0:58:bc:cb:36:
        32:c9:1b:6d:8f:79:db:83:22:fd:fe:a7:9a:b2:cd:
        26:b1:d7:52:c4:0c:40:6d:6e:49:b5:18:07:c2:3c:
        c8:c9:70:5d:06:da:0a:e6:01:1a:a4:78:19:aa:a7:
        38:1c:9d:36:07:4d:db:d2:b5:7b:50:f1:4b:d0:c7:
        5d:90:06:92:2d:a6:ea:d7:d2:09:8f:51:e8:b6:52:
        07:b1:1e:5e:ca:65:f3:d4:09:52:f1:d9:47:02:24:
        98:42:70:83:bc:49:13:c1:92:51:f7:ca:b2:fa:f6:
        a7:88:13:c1:74:23:d6:58:ab:27:d5:e5:02:20:3f:
        11:3b
      Exponent: 65537 (0x10001)
    Attributes:
    Requested Extensions:
      X509v3 Subject Alternative Name:
        DNS:Nginx20.kaheksa.xi, DNS:Nginx22.kaheksa.xi
    Signature Algorithm: sha256WithRSAEncryption
      5c:ad:79:7d:be:e1:e0:02:a5:26:11:73:76:b0:77:63:5a:47:
```

Pilt 8 - loodud sertifikaadi päringufaili sisu

SSL sertifikaadi tellimine ja paigaldamine

Järgnevalt tuleb saata sertifikaadi päringufail Nginx2404.csr mõnele usaldusväärsele sertifitseerimiskeskusele allkirjastamiseks. Näidiskonfiguratsiooni tingimustes on sertifikaadi väljastajaks testkeskkonna sertifitseerimiskeskus. Allkirjastatud sertifikaat väljastatakse Base64 kodeeritud formaadis:

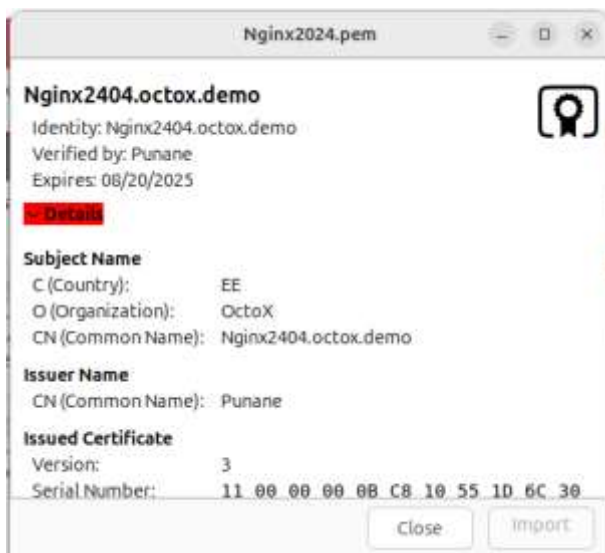
³ Veebilehitsejad ei pea veebilehte usaldusväärseks, kui vähemalt üks SAN DNS ei vasta veebilehe tegelikule aadressile.



```
-----BEGIN CERTIFICATE-----
MIICFjCCAZygAwIBAgITEQAAAAvIEFUdBDdFKgAAAAACzAKBggqhkJOPQDAzAR
MQ8wDQYDVQQDEwZzdW5hbnUwHhcNMjQwODIwMDc0OTQ0WncNMjUwODIwMDc1
OTQ0WjABMQswCQYDVQQGEwJFRTEOMAwGA1UEChMFT2N0b1gxHTAbBgNVBAMTFE5naH54
MjQwNjY3RveC5kZW1vMHYwEAYHKoZIzj0CAQYFK4EEACIDYgAEg4p3ITMARGpm
KPR+JpJ6Ugntu4P5m04k00ix4q2uHVdwsZpcx5xMy5X5/7GJT90J4Tk0XazG05Jk
OSMc0Pw00BciPLvg+8osj1V1K3xla1VKuK6kj0WBt6nW5Foaqq83o4GKMIGHMDcG
A1UdEQQwMC6CFE5naH54MjQwNjY3RveC5kZW1vghZmVdFQ1NFU1ZFU15vY3Rv
eC5kZW1vMB0GA1UdDgQwBBR5jkd+X31F1zoz4Fd6DEBFJjEe8jA4f8gNVHSMEGDAW
gBTrcF1U1o1S1fK0hWPgqeSou1vvVeZAMBgNVHRMBAf8EAjAAMAoGCCqGSM49BAMD
A2gAMGUCMQCqQAekCmo11qwgABz0BeDs14qjRKR1WcMhRA/Ph+7IFyBu/u57Nc/
uBviiid4ToFQCMAXHsVmuFh6jT2n4sW17j0owPJU0S7b411ExyRn1/LoDOCnew2T
Hz3/vZjy73t2ag==
-----END CERTIFICATE-----
```

Pilt 9 - sertifikaat Base64 formaadis tekstiredaktoris

Avades sertifikaadi Ubuntu failihalduris on näha järgmist:



Pilt 10 - ECC sertifikaat Ubuntu failihalduris

Sertifikaadis on kirjas ka algoritm ja alternatiivsed subjekti DNS nimed:



Pilt 11 – algoritm ja SAN DNS nimed

Nagu näha, on sertifikaadi väljaandjaks sertifitseerimiskeskus nimega „Punane“. Nüüd tuleb hankida väljaandja CA sertifikaat Base64 kodeeringus ja salvestada see kasutaja kodukausta nimega Punane.pem.

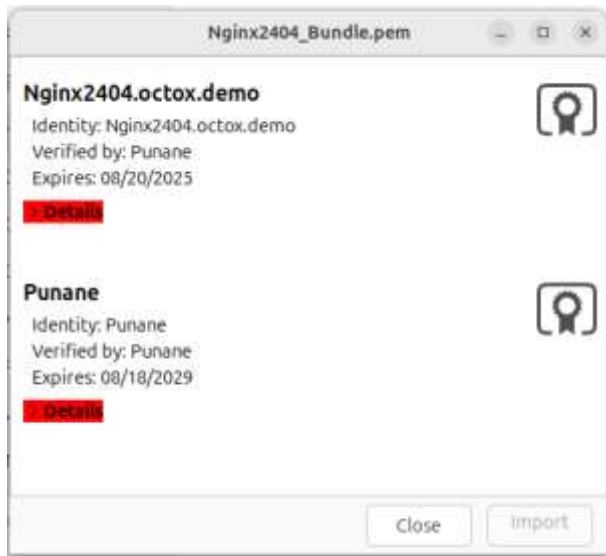
Pane kõik ühepoolseks SSL'iks kasutatavad sertifikaadid ühte faili, kusjuures esimene sertifikaat selles failis peab olema veebiserveri sertifikaat. Käesolevas näites peab faili kokku tõstma väljastatud veebiserveri sertifikaadi Nginx2404.pem ja selle väljastaja sertifikaadi Punane.pem. Seda saab teha kas tekstiredaktoris (sertifikaadid Base64 kodeeritud formaadis üksteise järel asetades) või kasutades käsku

```
cat Nginx2404.pem Punane.pem > Nginx2404_Bundle.pem
```



Pilt 12 - sertifikaatide koondamine ühte faili

Ubuntu avades näeb koondfail välja järgmine:



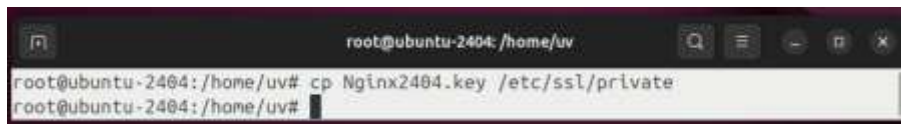
Pilt 13 - sertifikaadid on koondatud ühte faili

Sertifikaatide koondfaili **Nginx2404_Bundle.pem** tuleb kopeerida kausta **/etc/ssl/certs**



Pilt 14 - sertifikaatide koondfaili kopeerimine sertifikaatide konteinerisse

Lisaks peab paigaldama ka sertifikaadi privaatvõtme kausta **/etc/ssl/private**

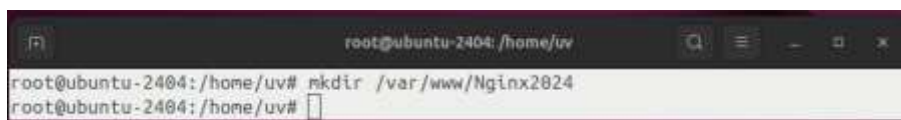


Pilt 15 - privaatvõtme paigaldamine

Nüüd on Nginx serveripoolsed sertifikaadi olemas ja korrektselt failisüsteemi paigaldatud.

Virtuaalse veebilehe loomine

Loo enda konfiguratsioonile eraldiseisev virtuaalne veebileht. Esmalt tuleb luua kaust **/var/www/Nginx2404**, kuhu paigaldada veebilehe sisu.



Pilt 16 - kaustad loomine veebisaidile

Paigalda loodud kausta mõni lihtne ja äratuntav veebileht nimega **index.html**.

Järgmiseks tee valmis virtuaalse veebilehe konfiguratsioonifail. Tee uus fail nimega **/etc/nginx/conf.d/Nginx2024.conf** (näiteks käsuga **nano /etc/nginx/conf.d/Nginx2404.conf**).



Nüüd muuda uut konfiguratsioonifaili vastavalt oma soovidele. Lisa sinna järgmine sisu⁴:

```
# Start
server {
    listen 80;
    listen [::]:80;
    server_name Nginx2404.octox.demo;
    return 301 https://Nginx2404.octox.demo ;
}
server{
    # SSL configuration
    listen 443 ssl;
    listen [::]:443 ssl;
        root /var/www/Nginx2404;
        index index.html;
        server_name Nginx2404.octox.demo ;

    # Certificates
    ssl_certificate /etc/ssl/certs/Nginx2404_Bundle.pem;
    ssl_certificate_key /etc/ssl/private/Nginx2404.key;

    location / {
        try_files $uri $uri/ =404;
    }
}
# End
```

Konfiguratsiooni korrektsust saab kontrollida käsuga **nginx -t**. Kui konfiguratsiooniga probleeme ei ole, siis aktiveeri uus konfiguratsioon käivitades Nginx teenuse:

```
systemctl start nginx
```

Juhul kui teenus juba töötab, saab selle taaskäivitada käsuga

```
systemctl reload nginx
```

Tulemus

Nüüd saab veebilehe poole pöördumiseks kasutada ühepoolset SSLi. Samuti suunatakse automaatselt aadressilt <http://Nginx2404.octox.demo> aadressile <https://Nginx2404.octox.demo>.

⁴ HTTP osa siin konfiguratsioonifailis ei ole tegelikult vajalik ja on toodud lihtsalt HTTP ->HTTPS ümbersuunamise näitena.



Pilt 17 - Nginx veebiserver töötab ja kasutab ühepoolset SSL-i, index.html on kohandatud

Kahepoolse sertifikaadinõude (SSLi) kehtestamine

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

Lisa Nginx2404.conf failile järgmised read SSL sektsiooni:

```
ssl_client_certificate /etc/ssl/certs/EID_Bundle.pem;  
ssl_verify_client on;  
ssl_verify_depth 2;
```

```
# Certificates  
ssl_certificate /etc/ssl/certs/Nginx2404_Bundle.pem;  
ssl_certificate_key /etc/ssl/private/Nginx2404.key;  
ssl_client_certificate /etc/ssl/certs/EID_Bundle.pem;  
ssl_verify_client on;  
ssl_verify_depth 2;
```

Pilt 18 - 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 veebileht toetab. Kasutajale näidatakse vaid neid sertifikaate, mis on väljastatud eelloetletud ahelatest. Faili loomiseks saab kasutada cat käsku, aga töötab ka kopeeri-ja-kleebi tekstiredaktorite vahel. Ubuntu avatuna näeb fail välja järgmine:

⁵ Saadaval: EID_Bundle.pem

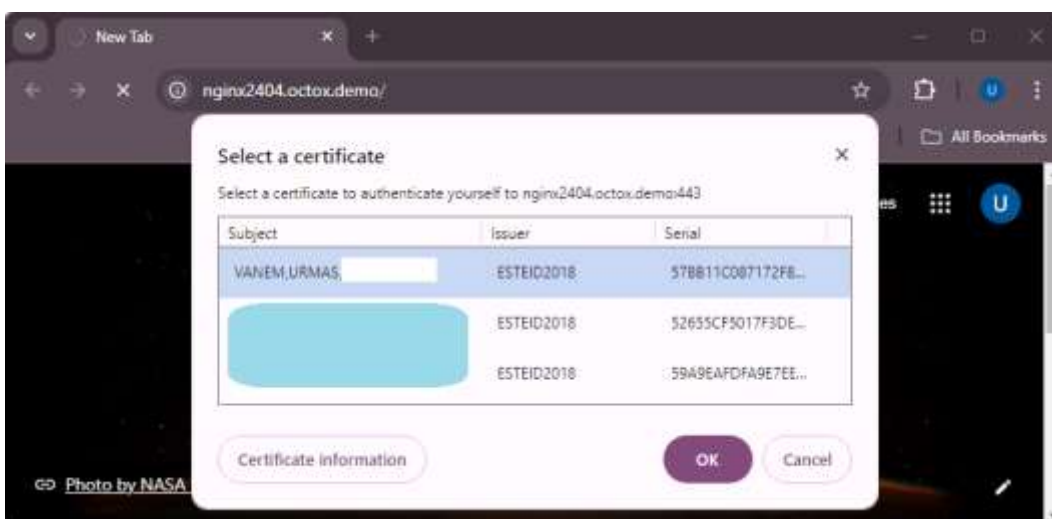


Pilt 19 – juur- ja kesktaseme sertifikaadid ühes failis

Salvesta loodud faili nimega EID_Bundle.pem ja kopeeri see kausta `/etc/ssl/certs`. Veebiserveris muudatuse jõustumiseks taaskäivita Nginx käsuga

```
systemctl reload nginx
```

Pöördudes pärast muudatuse jõustumist uuesti veebilehe `Nginx2404.octox.demo` poole, küsitakse kasutaja sertifikaati.



Pilt 20 - 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 veebilehede konfigureerimiseks 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 21 - 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# ufw status
Status: active

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

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

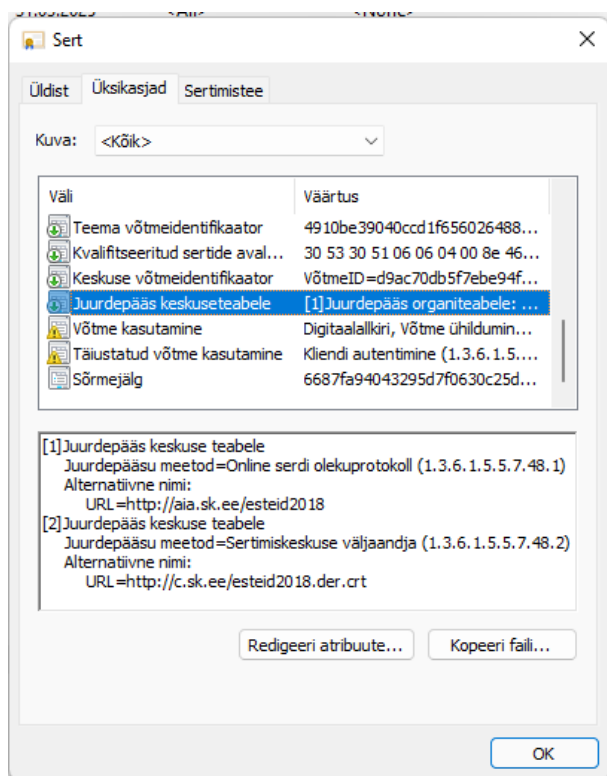
Pilt 22 - tulemüür on aktiivne ja ainult HTTPS liiklus on lubatud



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 23 - ESTEID2018 AIA OCSP aadress sertifikaadis

Lubamaks kasutaja sertifikaadi staatuse kontrolli vastu sertifikaadis olevat AIA OCSP teenust, tuleb Nginx SSL konfiguratsiooni lisada järgmised read:

```
ssl_ocsp leaf;  
ssl_ocsp_cache off;  
resolver 194.126.115.18;7
```

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

⁷ *Resolver* – asendage see soovi korral mõne DNS serveriga, mis on võimeline avalikke DNS aadresse lahendada. Selliseks serveriks võib olla ka teie enda sisevõrgu DNS server.



```
# Certificates
ssl_certificate /etc/ssl/certs/nginx123_bundle.pem;
ssl_certificate_key /etc/ssl/private/nginx123.key;
ssl_client_certificate /etc/ssl/certs/EID_Bundle.pem;
ssl_verify_client on;
ssl_verify_depth 2;
ssl_ocsp leaf;
resolver 194.16.115.18;
```

Pilt 24 - AIA OCSP konfiguratsioon on lisatud

Ülaltoodud konfiguratsiooni puhul võetakse OCSP teenuse aadress kasutaja sertifikaadist.

Soovituslikud Nginxi turvasätted

SSL/TLS

Ubuntu platvormil töötav Nginx server versiooniga 1.24 võib toetada aegunud TLS versioone nagu TLS 1.0 või TLS 1.1. 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 Nginx serveris kasutada vaid TLS protokollid versiooni 1.3, tuleb konfiguratsioonifaili lisada rida:

```
ssl_protocols TLSv1.3;
```

```
ssl_protocols TLSv1.3;
```

Pilt 25 – TLS 1.3 lubamine konfiguratsioonifailis

Toetamiseks ka TLS versiooni 1.2, tuleb konfiguratsioonireale lisada **TLSv1.2**.

Kui on soov sama muudatust kehtestada serveri tasemel, tuleb `ssl_protocols` käsku kohandada failis **/etc/nginx/nginx.conf**.

Rohkem infot TLS protokollid 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 protokollid jaoks lisakonfiguratsiooni looma ei pea.



TLS 1.2 puhul see päris nii ei ole. Nginx 1.24 versiooniga on vaikimisi kasutusel suur hulk erinevaid TLS šifreid⁸, mida näeb käsuga

```
openssl ciphers -v
```

Kui on soov määrata täpsemalt TLS 1.2 protokolliga kasutatavaid šifrikomplekte, saab Nginx kaustapõhises konfiguratsioonifailis kasutada käsku **ssl_ciphers**. Siin omakorda saab kasutada kas eeldefineeritud *aliasi* või täpseid šifrikomplektide kirjeldusi.

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

Näide:

- Kasutades konfiguratsioonifailis käsurida:
`ssl_ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384;`
lubatakse vaid kirjeldatud šifrikomplektide kasutamine.

Alternatiivina saab kasutatavaid šifreid konfigureerida serveripõhiselt failis **/etc/nginx/nginx.conf** muutes selles parameetrit **ssl_ciphers**.

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

ssl_prefer_server_ciphers

Eelistamiseks serveri šifrikomplektide valikut kasutaja omale, tuleb Nginx konfiguratsioonifailis defineerida määrang **ssl_prefer_server_ciphers** ja panna selle väärtuseks **on**.

Kasutajasertifikaatide lisafiltreerimine

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

- 1) sertifikaadis peab olema korrektne OID väärtus;
- 2) sertifikaadi väljastaja peab olema ESTEID2018 või ESTEID2025.

Paraku ei ole hetkeseisuga teada, kuidas Nginx puhul oleks esimest punkti serveri tasemel võimalik saavutada. Seetõttu on esimese punkti kontrolli soovitatav teha veebirakenduse tasemel.

Teise nõude täitmiseks saab luua konfiguratsiooni, kus ühendus katkestatakse, kui sertifikaat ei ole väljastatud serveris lubatud CAde poolt. Selleks tuleb lisada konfiguratsioonifaili (serveri sektsiooni, näiteks SSL kirjeldusele järgnevalt) järgmised tingimused:

⁸ Siin ei käsitleta teiste TLS protokollide šifreid, kuna versioonist 1.2 vanemad protokollid on eelduslikult keelatud ja 1.3 versioon on hetkel eelistatim.



```
#Determine IMCA and cancel, if not trusted
    set $ocspr "";
    if ($ssl_client_i_dn = "CN=ESTEID2018,organizationIdentifier=NTREE-10747013,O=SK ID Solutions AS,C=EE") {
        set $ocspr "http://aia.sk.ee/esteid2018";
    }
    if ($ssl_client_i_dn = "CN=ESTEID2025, organizationIdentifier=NTREE-17066049, O=Zetes Estonia OÜ, C=EE") {
        set $ocspr "http://ocsp.eidpki.ee";
    }
    if ($ocspr = "") {
        return 403;
    }
}
```

Pärast ülaltoodud tingimuste lisamist sessioon katkestatakse kui kasutaja sertifikaat ei ole väljastatud ülalkirjeldatud ESTEID2018 või ESTEID2025 CA poolt.

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>

HTTP Strict Transport Security (HSTS) lubamine

HSTS teenuse Nginx veebilehele konfigureerimiseks lisa konfiguratsioonifaili rida

```
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
```

```
# Other recommended security and optimization settings
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains; preload" always;
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 1h;
ssl_session_tickets on;
```

Pilt 26 - HSTS aktiveerimine



Muud võimalused

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

- Hoida operatsioonisüsteem uuendatuna.
- Hoida Nginx uuendatuna.
- Keelata serveri info presenteerimine.
- Keelata HTTP päringud.
- Paigaldada ja konfigureerida Naxsi.
- Monitoorida Monit abil.
- Konfigureerida X-XSS kaitse.
- Konfigureerida X-Frame-Options.
- Konfigureerida X-Content-Type-Options.
- Konfigureerida Content Security Policy (CSP).
- ...

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



Appendix

EID_Bundle.pem

```
EE-GovCA2018
-----BEGIN CERTIFICATE-----
MIIE+DCCBfmgAwIBAgIQMLOWlXoR0oFbj52nmRsneZAKBggqhkJOPQQDBDBaMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRh
DA5OVFJFRS0xMDC0NzAxMzEVMBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkw
NTA5MTEwM1oXDTMzMDkxNTA5MTEwM1owWjELMAkGA1UEBhMCRUUXGzAZBGNVBAoM
E1NLEIEIEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOT1RSRUUtMTA3NDcwMTMxFTAT
BgNVBAMMDEVFLUdvdnkNBMjAxODCBmzAQBgqhkJOPQIBBjUrgQQAiwoBhgAEAMcb
/dmAcVo/b2azEPS6CFW7fEA2KuHKC53D7ShVNVLz4QUjCdTXjds/4u99jUoYEQec
luVVzmlgEJR1nkN2eOrLAZYxPjwG5Hi1liZEyW9QKVdeEgyvzhWWTNHGjV3HdZRv
7L9o4533PtJAYqJ9Q0tIB9zCCAfmwCAYGBACPEgECMAkGBwQAL+xAAQIwMgYLKwYB
BAGDkSEBAQEwIzAhBggrBgEFBQcCARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMA0G
CysGAQQBQg5EhAQEEMA0GCysGAQQBQg5F/AQEEMA0GCysGAQQBQg5EhAQEFMA0GCysG
AQQBQg5EhAQEGMA0GCysGAQQBQg5EhAQEHMA0GCysGAQQBQg5EhAQEDMA0GCysGAQQB
Qg5EhAQEEMA0GCysGAQQBQg5EhAQEIMA0GCysGAQQBQg5EhAQEJMA0GCysGAQQBQg5Eh
AQEKMA0GCysGAQQBQg5EhAQELMA0GCysGAQQBQg5EhAQEMMA0GCysGAQQBQg5EhAQEN
MA0GCysGAQQBQg5EhAQEOMA0GCysGAQQBQg5EhAQEPMA0GCysGAQQBQg5EhAQEQMA0G
CysGAQQBQg5EhAQERMA0GCysGAQQBQg5EhAQESMA0GCysGAQQBQg5EhAQETMA0GCysG
AQQBQg5EhAQEUMA0GCysGAQQBQg5F/AQEEMA0GCysGAQQBQg5F/AQEDMA0GCysGAQQB
g5F/AQEEMA0GCysGAQQBQg5F/AQEFMA0GCysGAQQBQg5F/AQEGMDEGCisGAQQBQg5Eh
CgEwIzAhBggrBgEFBQcCARYVaHR0cHM6Ly93d3cuc2suZWUvQ1BTMBGDCSQAQUF
BwEDBAwwCjAIBgYEAISGAQEwCgYIKoZIzj0EAwQDgYwAMIGIAkIBk698EquetY9Tt
6Hw050CfzdIjKmlfCI34xkdU7J+wz1tNVu2tHJwEhdsH0e92i969sRDp1RNP1Vh
4XFJzI3oQFQCQgVxmcuVnsy7NUScDZ0erwovmbFOsNxELCANxNSWx5xMqzEiHv8
46opxu10UFDIBBPzkbBenL4h+g/WU71G78fIhA==
-----END CERTIFICATE-----
ESTEID2018
-----BEGIN CERTIFICATE-----
MIIFVzCCBLigAwIBAgIQdUf6rBR0S4tbo2bU/mZV7TAKBggqhkJOPQQDBDBaMQsw
CQYDVQQGEwJFRTEbMBkGA1UECgwSU0sgSUQgU29sdXRpb25zIEFTMRcwFQYDVQRh
DA5OVFJFRS0xMDC0NzAxMzEVMBMGA1UEAwwMRUUtR292Q0EyMDE4MB4XDTE4MDkw
NTA5MTEwM1oXDTMzMDkxNTA5MTEwM1owWDELMAkGA1UEBhMCRUUXGzAZBGNVBAoM
E1NLEIEIEIFNvbHV0aW9ucyBBUzEXMBUGA1UEYQwOT1RSRUUtMTA3NDcwMTMxFTAT
BgNVBAMMCKVTVEVJRDIwMTgwgZswEAYHkoZiZj0CAQYFK4EEACMDgYYABAHHOB1v
7URPYP1yHhOb7RA/YBDbtgyNSVMqYdxnFrKHUXh6tFkghvHuA1k2DSom1he5kqh
B5VspDembwWDJBOQWGOI/0t3EtcCLyjem7F9xOPdzUbZaIbpNRHpQgVbPFX0xpL
TgW27MpImH08DHBWfPeAaNX3eUpD4gC5cvhsK0RFEqOCAx0wggMZMB8GA1UdIwQY
MBaAFH4pVuc0knhOd+FvLjMqmHHB/TSfMB0GA1UdDgQWBbTzrHDbx36+1Pig5L5H
otA0rZoaqEjAOBgnVHQ8BAf8EBAMCAQYwEgYDVR0TAAQH/BAgwBgEB/wIBADCCAc0G
A1UdIASCAcQwggHAMAGBGAj3oBAjAIBgcEAIVsQAECMDIGCysGAQQBQg5EhAQEB
MCMwIQYIKwYBBQUHAgEWFWh0dHBzOi8vd3d3LnNrLmV1L0NQUzANBg9rBgEEAYOR
IQEBjANBg9rBgEEAYORfwbEBATANBg9rBgEEAYORIQEBBTANBg9rBgEEAYORIQEB
BjANBg9rBgEEAYORfwbEBATANBg9rBgEEAYORIQEBBzANBg9rBgEEAYORIQEBBDAN
Bg9rBgEEAYORIQEBBDANBg9rBgEEAYORIQEBCTANBg9rBgEEAYORIQEBcANBg9r
BgEEAYORIQEBcZANBg9rBgEEAYORIQEBDDANBg9rBgEEAYORIQEBDTANBg9rBgEE
AYORIQEBDjANBg9rBgEEAYORIQEBDzANBg9rBgEEAYORIQEBEDANBg9rBgEEAYOR
IQEBETANBg9rBgEEAYORIQEBEjANBg9rBgEEAYORIQEBEzANBg9rBgEEAYORIQEB
FDANBg9rBgEEAYORfwbEBAjANBg9rBgEEAYORfwbEBAzANBg9rBgEEAYORfwbEBBDAN
Bg9rBgEEAYORfwbEBBTANBg9rBgEEAYORfwbEBBjAqBgNVHSUBAf8EIDAeBggrBgEF
BQcDCQYIKwYBBQUHAgIGCCSQAQUBwMEMGoGCCSQAQUBwEBBF4wXDAPBggrBgEF
BQcAwYydaHR0cDovL2FpY55zay5lZS9lZS1nb3ZjYTYwMTgWYwYIKwYBBQUHMAKG
I2h0dHA6Ly9jLnNrLmV1L0VFLUdvdnkNBMjAxOC5kZXIuY3J0MBGDCSQAQUBwED
BAwwCjAIBgYEAISGAQEwMAYDVR0fBCKwJzAlc0CgIYYfaHR0cDovL2Muc2suZWUv
RUUtR292Q0EyMDE4LmNybdAKBggqhkJOPQQDBAObjAAwGyGcQgDeUUY4HczUbfKS
002HZ88gclgYdzthgglENyTmtXE6dMBRnCbGUmhBCAAOmJSHbyFJ8W9ikLiSyurm
kJM0hDE9KgJCASOqA405Ia5nKjTJPNsHQ1Mi7KZsIcTHOoBccx+54N8ZX1MgBozJ
mT59rZy/2/OeE163BAwD0UduQUAnMPP6+W3Vd
-----END CERTIFICATE-----
EEGovCA2025
```



```
-----BEGIN CERTIFICATE-----
MIIC1jCCAhYgAwIBAgIUkKbXJo8FWjthNs7Hgduq1RiXqswsCgYIKoZIzj0EAwMw
WDEUMBIGA1UEAwLRUVHb3ZDQTIwMjUxZjZAVBgnVNBGEEMk5UUKVFLTE3MDY2MDQ5
MRowGAYDVQQKDBFaZXRlcYBfc3RvbmlhIE/DnDELMAkGA1UEBhMCRUUwHhcNMjUw
NTA2MDgxODEzWWhcNDAwNTA1MDgxODEyWjBYMRQwEgYDVQDDAtFRUdvdKNBMjAy
NTEYMBUGA1UEYQwOT1RSRUUtMTcwNjYwNDkxGjAYBgNVBAoMEVpldGVzIEVzZG9u
aWEgT8OcMQswCQYDVQQGEwJFRTRB2MBAGByqGSM49AgEGBSuBBAAiA2IABH0zMU4D
UN/Ay6gUdWzMUdAYFau0flpuuicO2bfK7kHNGw+psRRn6DaF/4cVQd8qHxbDF2x
N4jJf1bSpQHlsc2RZHSCi8qb4E9GmB5MDovVxiXnBHOOW3+55Qm/BfvcwaOBpjCB
ozASBgNVHRMBAf8ECDAGAQH/AgEBMB8GA1UdIwQYMBaAFKqAqJsPu0umfsUC9HLN
LPG1Kdm3MD0GA1UdIAQ2MDQwMgYEVROgADAqMCgGCCsGAQUFBwIBFhxodHRwczov
L3JlcG9zaXRvcnkuaW1kcGtpLmVlL0VFR292Q0EyMDI1LmNydDA9BgnVHSAENjA0MDIGBFUdIAAwKjAo
BgggrBgEFBQcCARYcaHR0cHM6Ly9yZXBvc210b3J5LmVpZHBraS51ZTA1BgnVHR8E
LjAsMCcGKKAhR0dHRwOi8vY3JsLmVpZHBraS51ZS9FRUdvdKNBMjAyNS5jcmww
HQYDVRO0BBYEFJLAOLC4NhJo9crtZu5HKohtpo3oMA4GA1UdDwEB/wQEAWIBBjAK
BggqhkJOPQDAwNnADBKAjANipgLQgdM985dSFZfKvU9A7Sz2YdmmUSZBxu01L7Q
XKzqa0ZDyXmf03NPLNAC6dICMBQiROZbLoPezO9LD1847UbENx85hloLlzeWjqp
rY++Xj8FjCD1C9hnb1sVgJ3XAA==
-----END CERTIFICATE-----
ESTEID2025
-----BEGIN CERTIFICATE-----
MIIDDzCCApagAwIBAgIUUFQrcGtK7/jCP+GyAOTFvbg1G1cwCgYIKoZIzj0EAwMw
WDEUMBIGA1UEAwLRUVHb3ZDQTIwMjUxZjZAVBgnVNBGEEMk5UUKVFLTE3MDY2MDQ5
MRowGAYDVQQKDBFaZXRlcYBfc3RvbmlhIE/DnDELMAkGA1UEBhMCRUUwHhcNMjUw
NTA3MTMyMDA3WWhcNDAwNTA2MDgxODEyWjBYMRMwEQYDVQDDApFU1RFSUQyMDI1
MRcWFQYDVQRhDA5OVFJFRS0xNzA2NjA0OTEaMBgGA1UECgwRWmV0ZXMGdXN0b25p
YSBPPw5wCzAjbG9uVBAyTAKvFMHYwEAYHKOZIzj0CAQYFK4EEACIDYgAEdSEmb1An
xN7G22CCEQ3ts2YZNiETUZP4Vc4iObhmL/um4EXkia4HgyCiR5T6o1KAekPdxFBs
fmcLoPN+TmBO8ZpLGEqy1Vwf59ahDW7dQiLXTIAEiGCoXSWI9MvtHDZ2o4IBIDCC
ARwwEgYDVR0TAQH/BAgwBgEB/wIBADAFBgNVHSMEGDAWgBSqgKibD7tLpn7FAvRy
zSzxpsnZtzBABggrBgEFBQcBAQQ0MDIwMAYIKwYBBQUHMAKJGh0dHA6Ly9jcnQu
ZW1kcGtpLmVlL0VFR292Q0EyMDI1LmNydDA9BgnVHSAENjA0MDIGBFUdIAAwKjAo
BgggrBgEFBQcCARYcaHR0cHM6Ly9yZXBvc210b3J5LmVpZHBraS51ZTA1BgnVHR8E
LjAsMCcGKKAhR0dHRwOi8vY3JsLmVpZHBraS51ZS9FRUdvdKNBMjAyNS5jcmww
HQYDVRO0BBYEFJLAOLC4NhJo9crtZu5HKohtpo3oMA4GA1UdDwEB/wQEAWIBBjAK
BggqhkJOPQDAwNnADBKAjANipgLQgdM985dSFZfKvU9A7Sz2YdmmUSZBxu01L7Q
XKzqa0ZDyXmf03NPLNAC6dICMBQiROZbLoPezO9LD1847UbENx85hloLlzeWjqp
rY++Xj8FjCD1C9hnb1sVgJ3XAA==
-----END CERTIFICATE-----
```