



IIS VEEBISERVERILE ID-KAARDI TOE SEADISTAMINE

Dokumendi info	
Loomise aeg	21.01.2019
Tellija	RIA
Autor	Urmas Vanem, OctoX
Versioon	25.10/1

Versiooni info		
Kuupäev	Versioon	Muutused/märkused
21.01.2019	19.01/1	Avalik versioon, baseerub 18.12 tarkvaral.
12.02.2019	19.02/1	Lisatud OCSP konfiguratsioonivõimalused. Muutja: Urmas Vanem
01.10.2019	19.10/1	Lisatud info Windows serveri (IIS) paranduste staatuse ja tulevase kättesaadavuse osas versioonide lõikes. Vt. sissejuhatuse viimane lõik. Muutja: Urmas Vanem
18.10.2019	19.10/2	Kirjeldatud Windows Server 2016 uuendus KB4516061, mis lahendab Chrome-IIS probleemi. Muutja: Urmas Vanem
08.11.2019	19.11/1	Kirjeldatud Windows Server 2019 uuendus KB4520062, mis lahendab Chrome-IIS probleemi. Muutja: Urmas Vanem
14.11.2019	19.11/2	Kirjeldatud Windows Server 1903 (SAC) uuendus KB4524570, mis lahendab Chrome-IIS probleemi. Muutja: Urmas Vanem
12.12.2019	19.12/1	Lisatud soovitusel IIS'i turvamiseks. Muutja: Urmas Vanem



MS IIS ja eID kaardi tugi

Juhend administraatorile

14.12.2020	20.12/1	Lisatud turvasätted ebasoovitavate CA-de ligipääsu piiramiseks. Muutja: Urmas Vanem
17.12.2020	20.12/2	Lisatud mõned turvasoovitused peatükki „Ebavajalike CA-de juurdepääsu piiramine“. Muutja: Urmas Vanem
03.03.2021	21.03/1	Eemaldatud aegunud IIS ja Google Chrome autentimise probleem ning täpsustatud infot. Vt. Sissejuhatuse viimane lõik. Muutja: Kristjan Vaikla
30.04.2021	21.04/1	Eemaldatud aegunud ESTEID-SK 2011 sertifikaatide tugi. Muutja: Urmas Vanem
14.12.2021	21.12/1	Muudetud Windows platvorm versioonile Server 2022. Lisatud kolmandalt osapoolelt ECDSA algoritmil põhineva sertifikaadi päringu protseduur. Täiendatud on TLS ja Cipher soovitusi. Muutja: Urmas Vanem
18.01.2022	22.01/1	Lisatud Windows Server 2022 ja TLS 1.3 protokolliga seotud informatsioon, k.a. in-handshake autentimismeetodi konfigureerimise protseduur sertifikaadiga autentimise lubamiseks TLS 1.3 protokolliga. Muutja: Urmas Vanem
18.12.2023	23.12/1	Eemaldatud ESTEID-SK 2015 ahel. Muutja: Urmas Vanem
31.10.2025	25.10/1	Lisatud Zetes ahelad. Muutja: Raul Kaidro



MS IIS ja eID kaardi tugi

Juhend administraatorile

Juhend, kuidas autentida kasutajat IIS veebiserveril Eesti eID kaartidega.

Sissejuhatus

Käesolevas juhendis kirjeldame IIS veebiserveri konfiguratsiooni kahepoolse SSL-i kasutamiseks, kus kliendi poolseks sertifikaadiks on Eesti eID kaardile (ID-kaart, elamisloakaart, digi-ID ja e-residendi digi-ID) väljastatud sertifikaat.

Juhendi loomisel on kasutatud Windows Server 2022 ja Windows 10 operatsioonisüsteeme. Näidisjuhendis on toetatud SK ID Solutions EE-GovCA2018 ja Zetes EEGovCA2025 ahelast pärinevad sertifikaadid. Tagamaks sertifikaatide äratundmist on kohustuslikuks komponendiks kliendi poolel ka ID-tarkvara¹. Näidisjuhendi serveri sertifikaat on väljastatud OctoX testkeskkonnast.

IIS kasutamisel on võimalik rakendada erinevaid autentimismeetodeid. Käesolev dokument vaatleb sertifikaadi nõude kehtestamist IIS anonüümse autentimise jaoks – st. peale sertifikaadi kehtivuse kontrolli lubatakse kasutaja eelnevalt määratud kasutaja (IUSR) õigustes veebisaidile ligi.

Hetkel on testid edukalt läbi viidud järgmiste brauseritega (viimased versioonid):

- 1) Microsoft Edge
- 2) Mozilla Firefox
- 3) Google Chrome

Ühepoolse SSL/TLS-i konfigureerimine

Windows serveri sertifikaadi konfiguratsioon

Pakkumaks turvalist veebiteenust peab IIS serverile olema määratud TLS sertifikaat - meie näites on kasutusel OctoX testkeskkonnast väljastatud sertifikaat. Samuti peavad nii kliendid kui ka veebiserver ise usaldama nimetatud sertifikaati.

Domeeni keskkonnas ja domeeni (*enterprise*) CA olemasolul on tõenäoliselt kõige mõistlikum küsida ka serveri sertifikaat domeeni CA-lt. Ent juhul, kui meid ei rahulda domeeni taseme turvalisus ja võimalused või kui vajame sertifikaati, mis on laiemalt usaldatud, tuleb luua privaatvõti ning sertifikaadi päring ja lasta viimase alusel luua sertifikaat mõnel üldtuntud CA-l.

Serveri sertifikaadi hankimine

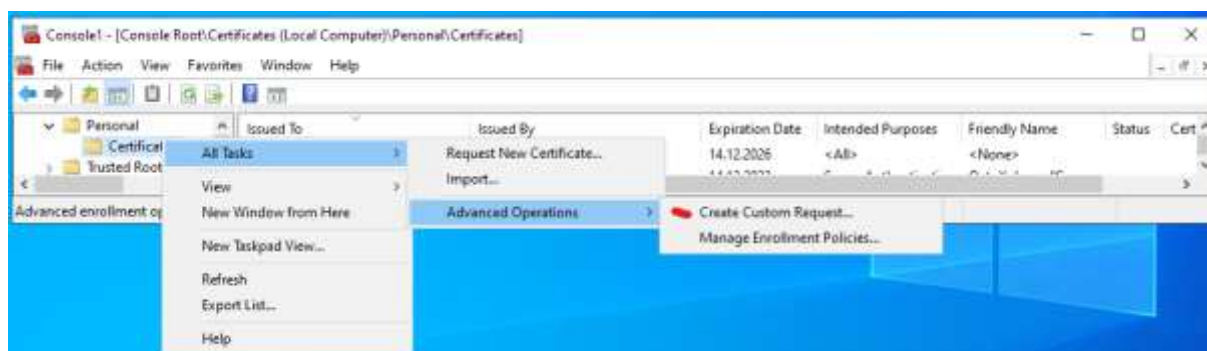
Kuna IIS halduskonsoolilt loodav sertifikaadi päring on üsna piiratud võimalustega, kasutame serveri sertifikaadi loomiseks hoopis sertifikaatide halduskonsooli. Käivitame IIS serveril mmc.exe ja lisame sinna lokaalse arvuti sertifikaadid. Loome kohandatud päringu:

¹ <https://www.id.ee/artikkel/paigalda-id-tarkvara/>



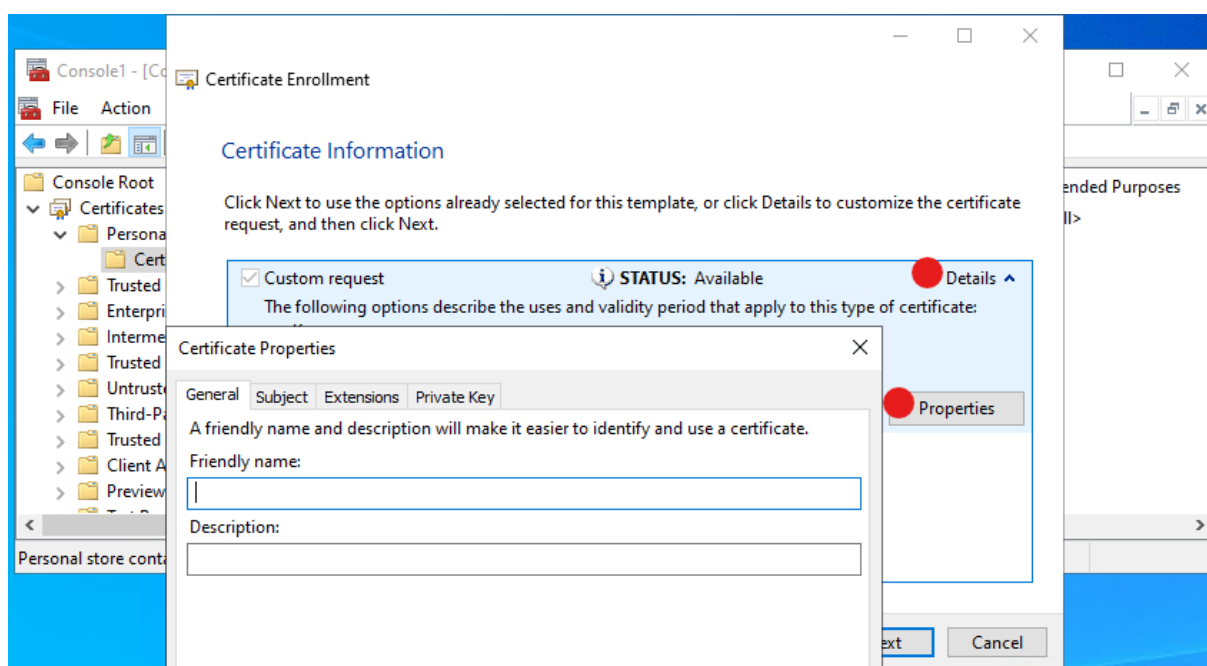
MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 1 – alustame kohandatud päringu loomisega

Klikime kolm korda *Next* ja valime *Details*, *Properties*. Avaneb sertifikaadi päringu omaduste aken:



Pilt 2 – sertifikaadi päringu omaduste aken

Järgnevalt saame määrata päringufailile täpsed omadused, milliseid tahame hiljem oma veebiserveri sertifikaadi juures näha.

Juhul, kui meil on tarvis sarnaseid päringufaile tihedamini luua, soovitame tegevuse automatiseerimiseks tutvuda *PowerShell* võimalustega.

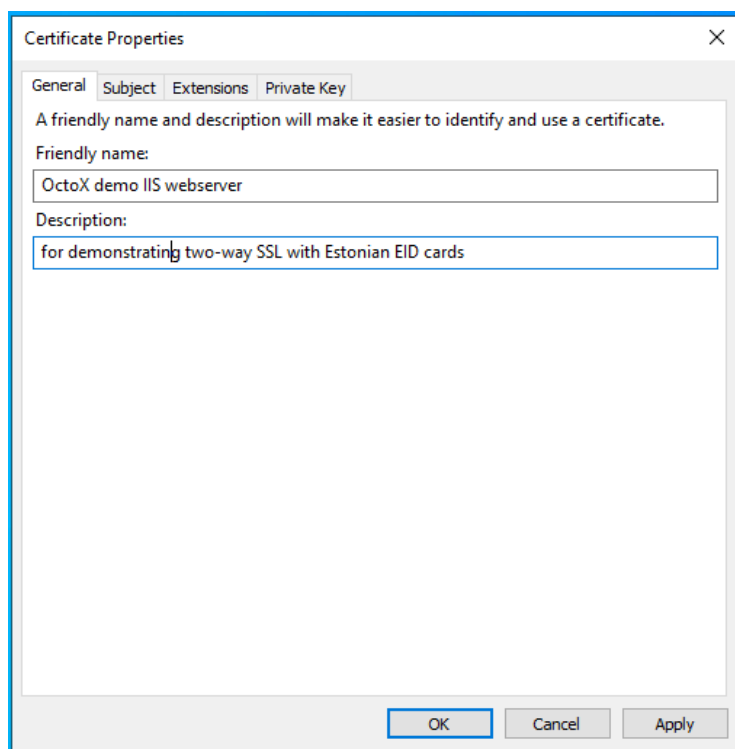
Sakk General

Siin määrame soovi korral sertifikaadi hüüdmine ja põgusa kirjelduse. Need väljad ei ole sertifikaadi sisulised osad ja omavad tähendust selgituse, hilisema lihtsama arusaama mõttes.



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 3 - sertifikaadi üldinfo

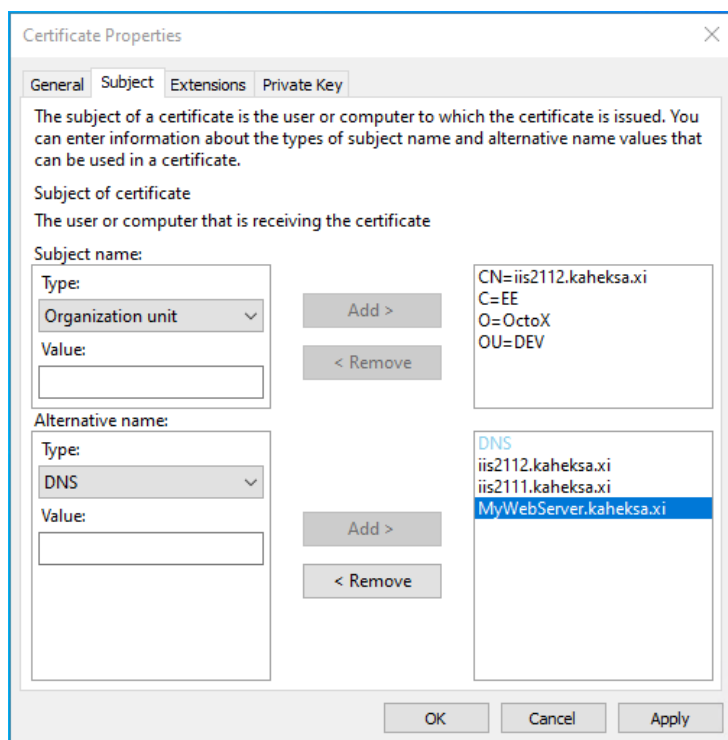
Sakk Subject

Aknas *Subject* kirjeldame subjekti nagu ikka. Kui soovime kasutada erinevad SAN DNS nimesid või kasutame *common name* puhul midagi muud kui FQDN, siis tuleb üks või mitu DNS aliaast siin ka kirjeldada.



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 4 - subjekti näidiskonfiguratsioon

Sakk Extensions

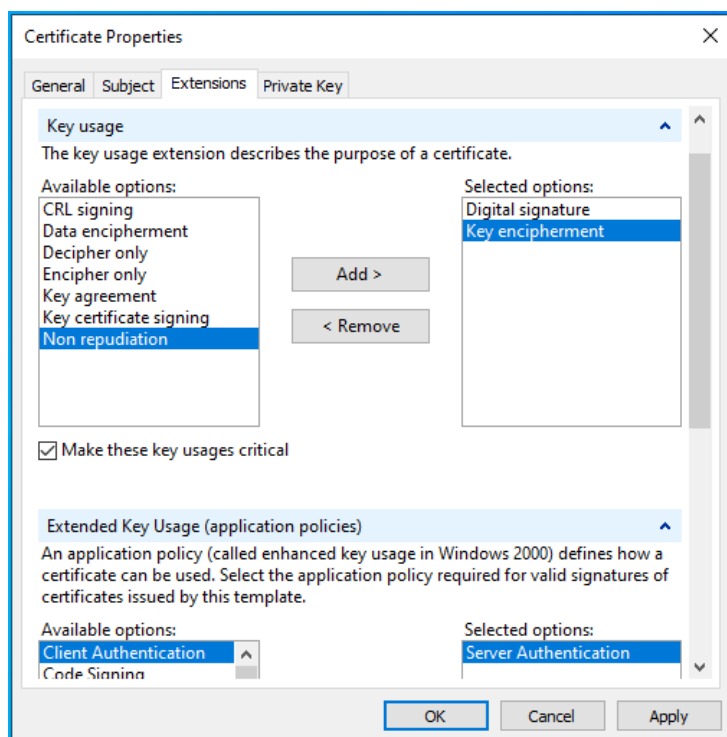
Aknas *Extensions* määrame järgmised omadused:

1. Key Usage:
 - a. Digital signature;
 - b. Key encipherment.
2. Extended Key Usage:
 - a. Server Authentication.



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 5 - laienduste määramine

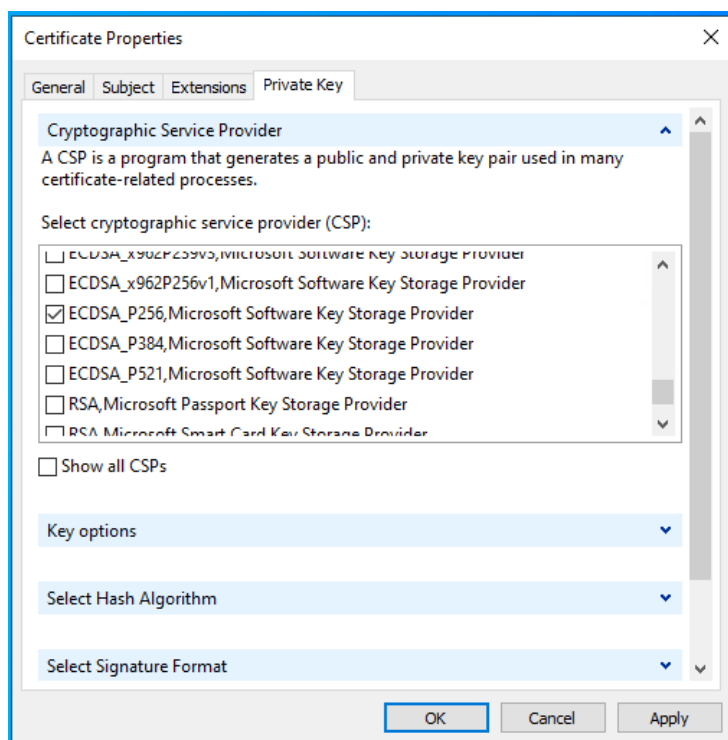
Sakk Private Key

Siit aknast valime CSP ehk sertifikaadi võtmete algoritmi. Näidis-konfiguratsioonis kasutame algoritmi ECDSA_P256, seega valime loendist ECDSA_P256 ja eemaldame nimekirja alguses oleva RSA.



MS IIS ja eID kaardi tugi

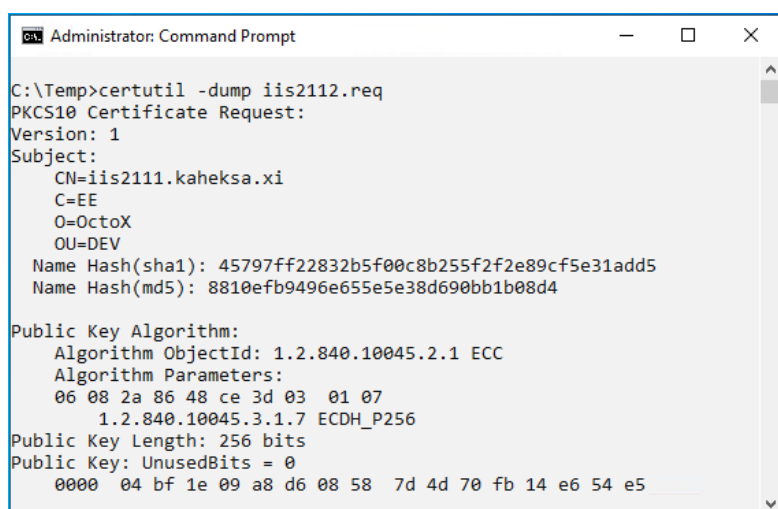
Juhend administraatorile



Pilt 6 - CSP valimine

Klikime *OK* ja *Next*, määrame kausta ning nime ja salvestame sertifikaadi päringu „Base64“ formaadis.

Võime värskelt loodud sertifikaadi päringufaili omadused kontrollida üle käsuga „certutil -dump PÄRINGUFAILI_NIMI“.



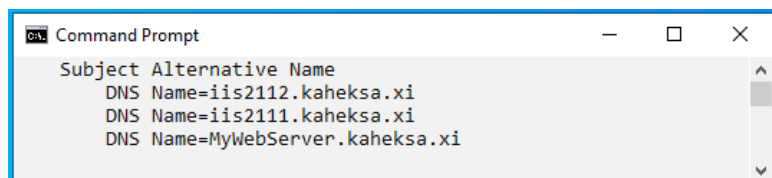
Pilt 7 - päringufaili sisu



MS IIS ja eID kaardi tugi

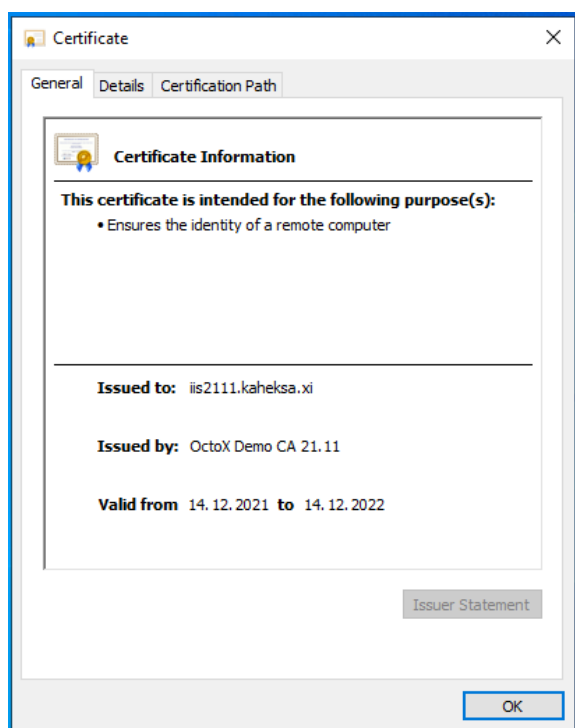
Juhend administraatorile

Veendume, et ka DNS alternatiivsed nimed on päringufailis olemas:



Pilt 8 - DNS aliased päringufailis

Nüüd edastame sertifikaadi päringufaili mõnele CA serverile ja palume selle alusel endale sertifikaadi genereerida. Tulemus on järgmine:



Pilt 9 – IIS serveri sertifikaat

Sertifikaadi installeerimine

IIS server peab usaldama sertifikaati „OctoX Demo CA 21.11“, mis on serveri sertifikaadi väljastajaks. Selleks peame kontrollima selle sertifikaadi olemasolu *usaldusväärsete juursertifikaatide*² konteineris. Kui väljastaja CA sertifikaat sealt puudub, tuleb see lisada!³

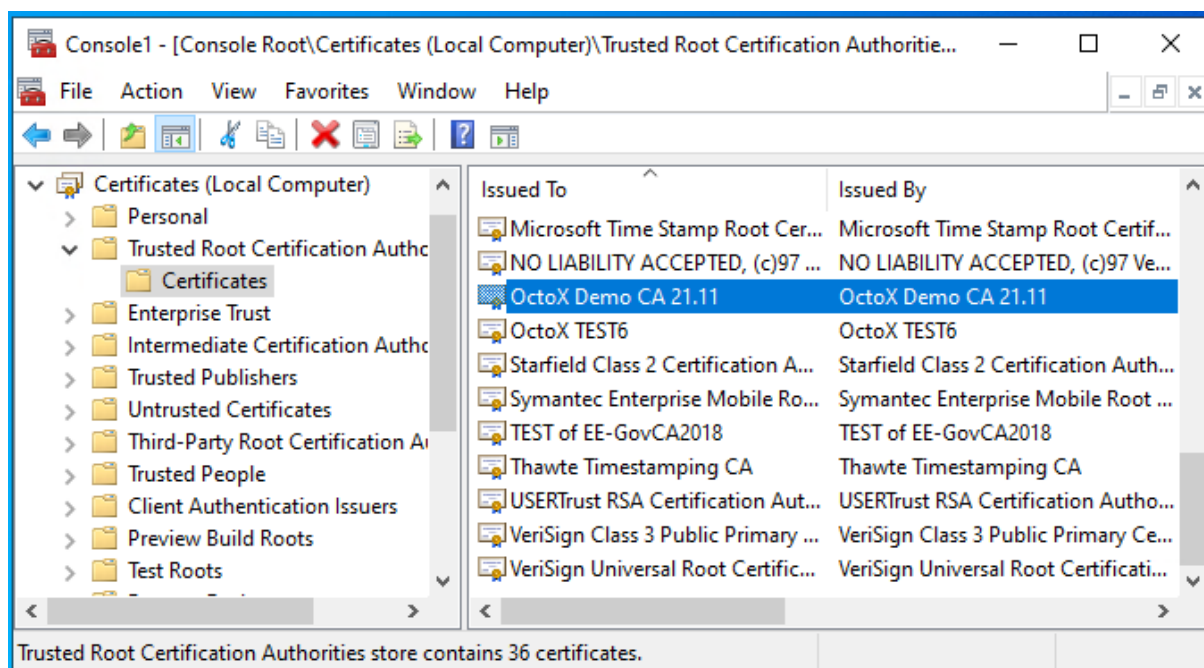
² Trusted root certification authorities

³ Juhul, kui sertifikaadi on väljastanud mõni kesktaseme CA, siis tuleb see puudumisel lisada *kesktaseme sertimiskeskuste* konteinerisse. Ja kesktaseme CA sertifikaadi väljastanud juur-CA sertifikaat tuleb puudumisel lisada *usaldusväärsete juursertifikaatide* konteinerisse.



MS IIS ja eID kaardi tugi

Juhend administraatorile



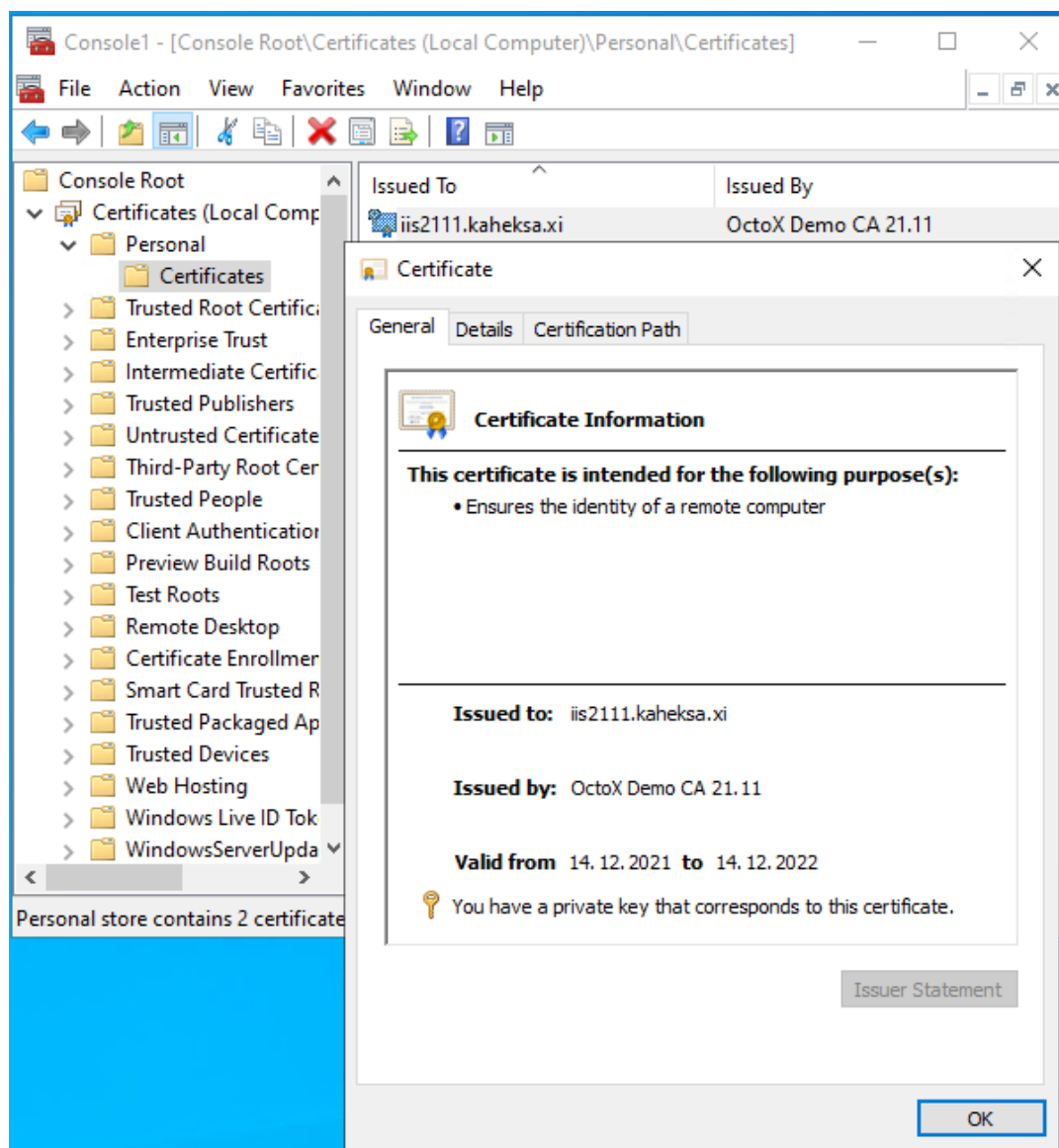
Pilt 10 - IIS server usaldab temale sertifikaadi väljastanud CA-d.

IIS serveri sertifikaat ise tuleb paigaldada IIS serveril lokaalse arvuti personaalsesse konteinerisse:



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 11 - avades sertifikaadi näeme, et IIS serveril on ka selle privaatvõti kasutada!

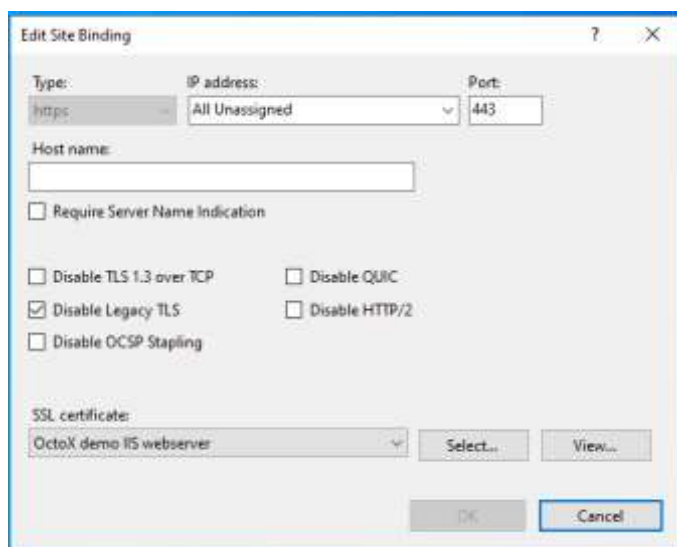
Ühepoolse SSL-konfiguratsiooni loomine

Ühepoolse SSL-i kehtestamiseks peab veebisaidil olema kirjeldatud SSL port (vaikimisi 443) ja see peab olema seotud soovitava sertifikaadiga. Koheselt keelame ka vanade SSL/TLS protokollide (vanemad kui 1.2) kasutamise!



MS IIS ja eID kaardi tugi

Juhend administraatorile



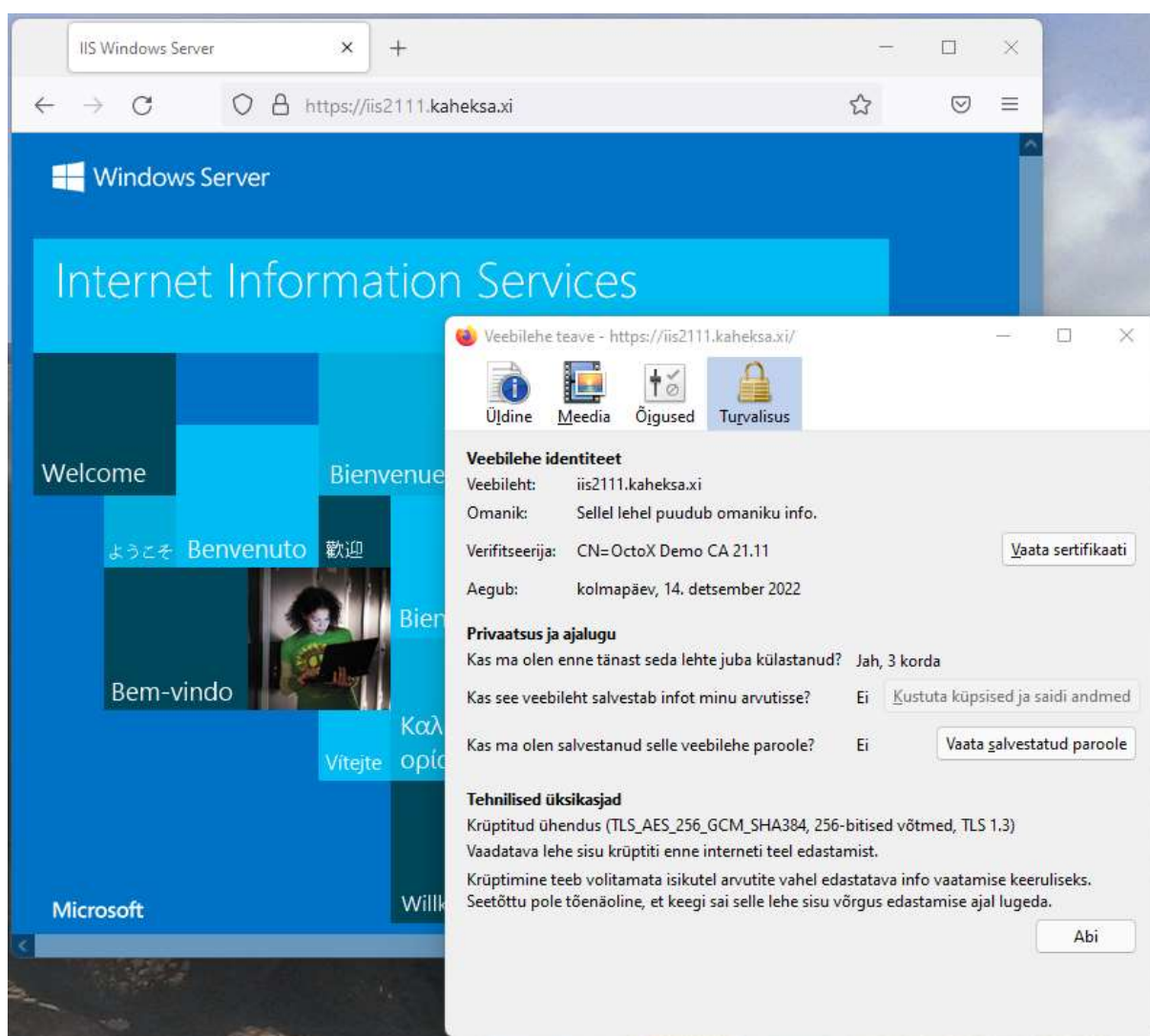
Pilt 12 - veebisaidil on lubatud 443 port ja kasutatavaks sertifikaadiks on iis2111.kaheksa.xi, vanad TLS protokollid tuleb keelata!

Peale määrangute kinnitamist ühepoolne SSL töötab!



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 13 - ühepoolne SSL töötab TLS 1.3 protokolliga, veebilehitsejaks on Firefox!

Ühepoolse SSL-i demonstreerimiseks kasutatud Firefox veebilehitseja näitab lisainfo akendes meile veel ka järgmist:

1. Kasutusel on meie värskest installeeritud sertifikaat 2111.kaheksa.xi;
2. Kasutusel on TLS 1.3 protokoll.

HTTP ligipääsu piiramine

HTTP ligipääsu keelamiseks eemaldame pordi 80 seotud protokollide loendist ja keelame tulemürist ka vastava ligipääsu. Alternatiivina võime suunata HTTP liikluse automaatselt HTTPS saidile vältimaks probleemi, kus kasutajad kirjutavad ise brauserisse saidi aadressi ent ei taipa sinna ette HTTPS:// määrangut panna.



MS IIS ja eID kaardi tugi

Juhend administraatorile

Kahepoolse SSL-i, sertifikaadiga autentimise nõudmine

Eelhäälestus

Juhime tähelepanu, et IIS 10/Schannel (seisuga 18.01.2022), mis töötab Windows Server 2022 platvormil, kasutab sertifikaadiga autentimiseks protokollit TLS 1.3 abil vaikimisi post-handshake autentimismeetodit. Kuna aga enimlevinud brauserid seda ei toeta⁴, siis see lahendus paraku praktikas ei tööta! Juhul, kui TLS 1.3 on sisse lülitatud, ei saada server kliendile vaikimisi konfiguratsioonis sertifikaadi päringut ja katkestab ühenduse! Sertifikaadiga autentimise tööle saamiseks tuleb keelata TLS 1.3 kasutamine. Alternatiivina saame sisse lülitada in-handshake autentimismeetodi, vt. peatükk „In-handshake autentimismeetodi lubamine“.

TLS protokollit versiooni 1.3 saame välja lülitada IIS HTTPS seose lehel, märkides linnukese lahtrisse „Disable TLS 1.3 over TCP“:

The screenshot shows the 'Edit Site Binding' dialog box. The 'Type' is set to 'https', the 'IP address' is 'All Unassigned', and the 'Port' is '443'. The 'Host name' field is empty. The 'Require Server Name Indication' checkbox is unchecked. The 'Disable TLS 1.3 over TCP' checkbox is checked. The 'Disable Legacy TLS' checkbox is checked. The 'Disable OCSP Stapling' checkbox is unchecked. The 'Disable QUIC' checkbox is unchecked. The 'Disable HTTP/2' checkbox is unchecked. The 'SSL certificate' dropdown is set to 'OctoX demo IIS webserver'. There are 'Select...' and 'View...' buttons next to the dropdown. At the bottom, there are 'OK' and 'Cancel' buttons.

Pilt 14 – sertifikaadiga autentimise lubamiseks peame paraku TLS 1.3 protokollit keelama

⁴ Firefox teadaolevalt toetab, ent ka sellel brauseril ei ole see vaikimisi lubatud.



MS IIS ja eID kaardi tugi

Juhend administraatorile

Eesti eID sertifikaatide häälestus IIS serveril

Kahepoolse SSL-i lubamiseks tuleb IIS serveri poolt nõuda sertifikaadiga autentimist. Vaikimisi lubab server enda poole pöördumisel kasutada kõiki sertifikaate, mis on tema poolt usaldatud ja millel on EKU-s kirjeldatud *client authentication* laiend. Korrektseks toimimiseks peab server suutma luua kogu sertifikaadiahela alates kasutajasertifikaadist kuni juursertifikaadini – see tähendab, et lisaks juurtaseme sertifikaatide olemasolule IIS serveris on vajalik ka kesktaseme (*intermediate*) sertifikaatide olemasolu.

Meie konfiguratsiooni puhul tuleb IIS serveris sertifikaadid publitseerida järgmiselt:

- 1) Usaldusväärsete juursertifikaatide konteinerisse:
 - a. EE-GovCA2018 (<https://c.sk.ee/EE-GovCA2018.der.crt>)
 - b. EEGovCA2025 (<https://crt.eidpki.ee/EEGovCA2025.crt>)
- 2) Kesktaseme sertifikaatide konteinerisse⁵:
 - a. ESTEID2018 (<http://c.sk.ee/esteid2018.der.crt>)
 - b. ESTEID2025 (<https://crt.eidpki.ee/ESTEID2025.crt>)

Veebisaidi SSL omaduste alt tuleb nõuda SSL protokollu ja kliendi sertifikaatide kasutamist:

SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

Require SSL

Client certificates:

Ignore

Accept

Require

Pilt 15 - SSL ja sertifikaadi nõue

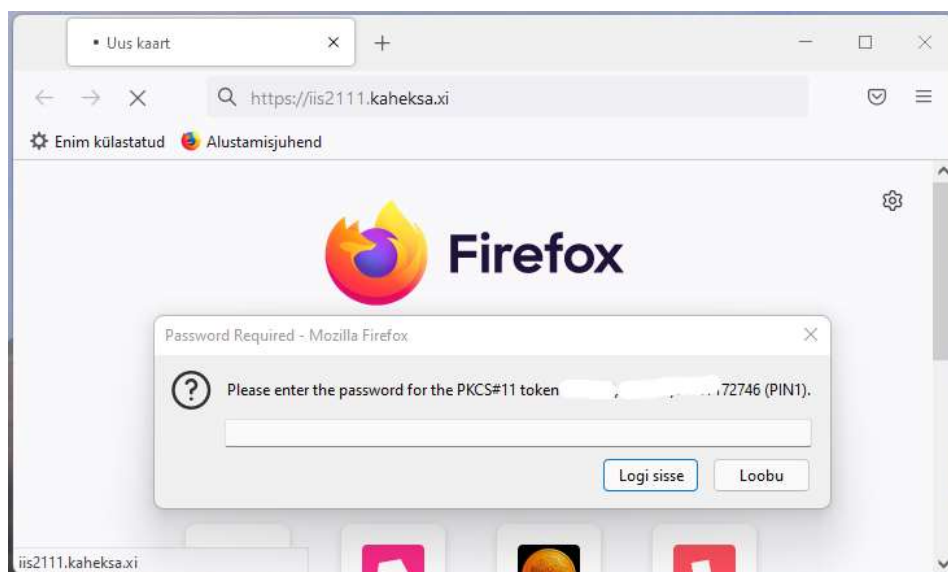
Loodud konfiguratsioon lubab veebisaidile ligipääsu 443 pordi kaudu, kasutajalt nõutakse sertifikaati. Pöördudes veebisaidi poole lubatakse valida soovitatav serveri poolt aktsepteeritud sertifikaat:

⁵ SK poolt väljastatud organisatsioonide kaartide kasutuse puhul peavad kesktaseme sertifikaatide hulka olema häälestatud ka EID-SK 2016 (https://www.sk.ee/upload/files/EID-SK_2016.der.crt) sertifikaadid!



MS IIS ja eID kaardi tugi

Juhend administraatorile



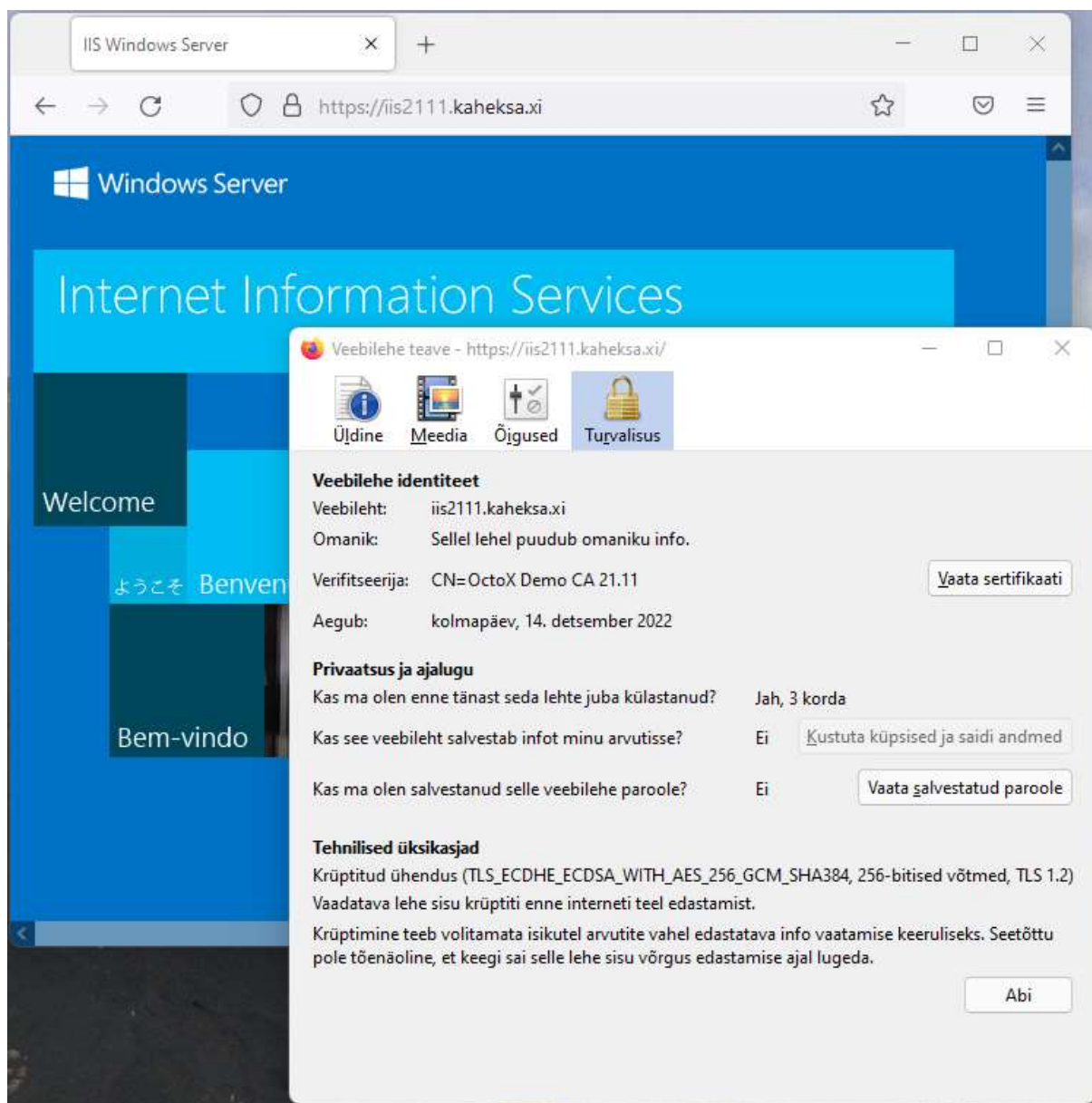
Pilt 16 - sertifikaadi küsimine veebisaidile pöördudes Firefox brauseris

Peale PIN-i sisestamist kontrollitakse sertifikaadi kehtivust veebiserveri poolt ja kui kõik on korras, lastakse kasutaja veebisaidile ligi.



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 17 - autentimine õnnestus kasutades protokollit TLS 1.2

Alternatiivina võib IIS-i poolse sertifikaadinõude (*Require*) asemel kasutada ka lihtsat sertifikaadi aktsepteerimist (*Accept*) IIS serveri poolt – see võimaldab lisaks sertifikaadile saada serverile ligi ka kasutajanime ja parooliga või üldse autentimata.

In-handshake autentimismeetodi lubamine

Kui soovime siiski kasutada TLS 1.3 protokollit ja kasutada sertifikaadiga autentimist, saame lubada in-handshake autentimismeetodi. Selle meetodi puhul küsib server kliendilt *Server Hello* saatmisel kohe ka sertifikaati.



MS IIS ja eID kaardi tugi

Juhend administraatorile

In-handshake autentimismeetodi lubamiseks tuleb teha järgmist:

- 1) Dokumenteerida olemasoleva sertifikaadi määrangud käsuga "netsh http show sslcert".
Oluline on üles märkida *Certificate Hash* ja *Application ID*:

```
Administrator: Command Prompt
C:\Users\Administrator>netsh http show sslcert

SSL Certificate bindings:
-----

IP:port                : 0.0.0.0:443
Certificate Hash       : 312bbb70898b5ae10753998c67bceeeb97d49f79
Application ID        : {4dc3e181-e14b-4a21-b022-59fc669b0914}
Certificate Store Name : MY
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier         : (null)
Ctl Store Name        : (null)
DS Mapper Usage       : Disabled
Negotiate Client Certificate : Disabled
Reject Connections    : Disabled
```

Pilt 18 - vaikumisi on määrang "negotiate client certificate" keelatud

- 2) Eemaldame sertifikaadi seotuse 443 pordiga käsuga „netsh http del sslcert 0.0.0.0:443“:

```
Administrator: Command Prompt
C:\Temp>netsh http del sslcert 0.0.0.0:443

SSL Certificate successfully deleted

C:\Temp>
```

Pilt 19 - sertifikaadi eemaldamine 443 pordi küljest.

- 3) Ja lisame selle uuesti lubades ühtlasi ka in-handshake autentimismeetodi käsuga „netsh http add sslcert ipport=0.0.0.0:443 certhash=312bbb70898b5ae10753998c67bceeeb97d49f79 appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=MY **clientcertnegotiation=Enable**“:



MS IIS ja eID kaardi tugi

Juhend administraatorile

```
Administrator: Command Prompt
C:\Users\Administrator>netsh http add sslcert ipport=0.0.0.0:443 certhash=312bbb708
98b5ae10753998c67bceeeb97d49f79 appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certst
orename=MY clientcertnegotiation=Enable
SSL Certificate successfully added
```

Pilt 20 - clientcertnegotiation lubamine

Vaadates uuesti sertifikaadi infot näeme, et *Negotiate Client Certificate* on nüüd lubatud:

```
Administrator: Command Prompt
C:\Users\Administrator>netsh http show sslcert
SSL Certificate bindings:
-----
IP:port                : 0.0.0.0:443
Certificate Hash       : 312bbb70898b5ae10753998c67bceeeb97d49f79
Application ID        : {4dc3e181-e14b-4a21-b022-59fc669b0914}
Certificate Store Name : MY
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : (null)
Ctl Store Name       : (null)
DS Mapper Usage      : Disabled
Negotiate Client Certificate : Enabled
Reject Connections   : Disabled
```

Pilt 21 - in-handshake autentimismeetod on nüüd sees

Märkus. Kuna *session renegotiation* on TLS 1.3 puhul keelatud, siis selle meetodi puhul tuleb arvestada asjaoluga, et autentimine peab toimuma „esimesel lehel“. Kui oleme juba kliendi sertifikaadiga autentimata ühepoolse SSL ühenduse loonud ja samal lehel soovime kliendi sertifikaadiga autentides mõnele kaitstud ressursile ligi pääseda, siis me ebaõnnestume, kuna TLS 1.3 ei toeta sellist lähenemist. Vajadusel tuleb see „maandumise“ probleem ühel või teisel viisil lahendada.

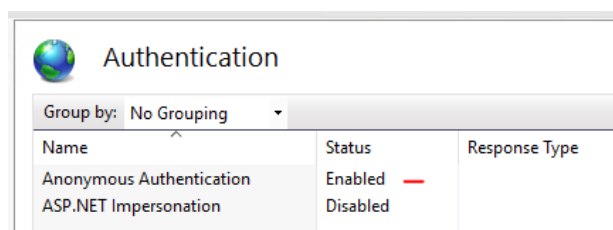
Autentimine

Meie näites on lubatud ainult anonüümne autentimine:



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 22 - anonüümne autentimine, kasutaja saab saidile ligi kasutaja IUSR õigustes

Võimalikud lisakonfiguratsioonid

Selle dokumendi eesmärgiks ei ole anda täpseid juhiseid optimaalseks veebisaitide konfigureerimiseks ega turvamiseks. Pigem tahame tutvustada konfiguratsiooni kahepoolse SSL-i kasutamiseks Eesti eID kaartidega. Siiski toome järgnevalt välja punktid, mida peame oluliseks mainida.

Kasutajapoolsete sertifikaatide filtreerimine

Vaikimisi pakutakse kasutajapoolse kahepoolse SSL sessiooni alustamisel IIS puhul kliendile välja kõik sertifikaadid, millistel on EKU omaduste all kirjas kliendi autentimine (ja loomulikult peab olema ka sertifikaadi privaatvõti). IIS-i poolt on aga kliendile võimalik ette anda loend autentimiskeskustest millised on lubatud ja seeläbi kuvatakse edaspidi klientidele vaid toetatud ahelate sertifikaadid.

Seame eesmärgiks kuvada kasutaja pool vaid sertifikaadid, mis pärinevad kindla juurserveri „EE-GovCA2018“ ja „EEGovCA2025“ ahelast.

- 1) Kuvame aktiivse IIS sertifikaadi info käsuga “netsh http show sslcert 0.0.0.0:443”:



MS IIS ja eID kaardi tugi

Juhend administraatorile

```
Administrator: Command Prompt
C:\Temp>netsh http show sslcert 0.0.0.0:443

SSL Certificate bindings:
-----
IP:port                : 0.0.0.0:443
Certificate Hash       : 312bbb70898b5ae10753998c67bceeeb97d49f79
Application ID        : {4dc3e181-e14b-4a21-b022-59fc669b0914}
Certificate Store Name : My
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : (null)
Ctl Store Name       : (null)
DS Mapper Usage      : Disabled
Negotiate Client Certificate : Disabled
Reject Connections   : Disabled
Disable HTTP2        : Not Set
Disable QUIC         : Not Set
Disable TLS1.2       : Not Set
Disable TLS1.3       : Set
Disable OCSP Stapling : Not Set
Enable Token Binding : Not Set
```

Pilt 23 - vaikimisi seotud sertifikaadi omadused

2) Eemaldame selle sertifikaadi seose käsuga “netsh http del sslcert 0.0.0.0:443”:

```
Administrator: Command Prompt
C:\Temp>netsh http del sslcert 0.0.0.0:443

SSL Certificate successfully deleted

C:\Temp>
```

Pilt 24 - sertifikaadi eemaldamine

3) Lisame sertifikaadi uuesti ja ütleme, et sertifikaatide filtreerimiseks kasutame arvuti sertifikaatide kausta „*Client Authentication Issuers*“. Käsuks on „netsh http add sslcert ipport=0.0.0.0:443 certhash=1e75c77c696aa4d49686bb1ef73ac3b07fdff38a appid={4dc3e181-e14b-4a21-b022-59fc669b0914} sslctlstorename=ClientAuthIssuer“:



MS IIS ja eID kaardi tugi

Juhend administraatorile

```
Administrator: Command Prompt
C:\Temp>netsh http add sslcert ipport=0.0.0.0:443 certhash=312bbb70898b5ae10753998c67bceeeb97d49f79 appid={4dc3e181-e14b-4a21-b022-59fc669b0914} sslctls
torename=ClientAuthIssuer
SSL Certificate successfully added
C:\Temp>
```

Pilt 25 - lisame sertifikaadi uute omadustega

Certhash ja appid väärtused saame esialgselt sertifikaadi väljavõttest, vt. „Pilt 23 - vaikimisi seotud sertifikaadi omadused“.

4) Kontrollime, et “CTL Store Name” on uuel sertifikaadi väljavõttel ClientAuthIssuer:

```
Administrator: Command Prompt
C:\Temp>netsh http show sslcert 0.0.0.0:443
SSL Certificate bindings:
-----
IP:port                : 0.0.0.0:443
Certificate Hash       : 312bbb70898b5ae10753998c67bceeeb97d49f79
Application ID        : {4dc3e181-e14b-4a21-b022-59fc669b0914}
Certificate Store Name : (null)
Verify Client Certificate Revocation : Enabled
Verify Revocation Using Cached Client Certificate Only : Disabled
Usage Check           : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout : 0
Ctl Identifier        : (null)
Ctl Store Name       : ClientAuthIssuer
DS Mapper Usage       : Disabled
Negotiate Client Certificate : Disabled
Reject Connections    : Disabled
```

Pilt 26 - uuesti seotud sertifikaadi omadused

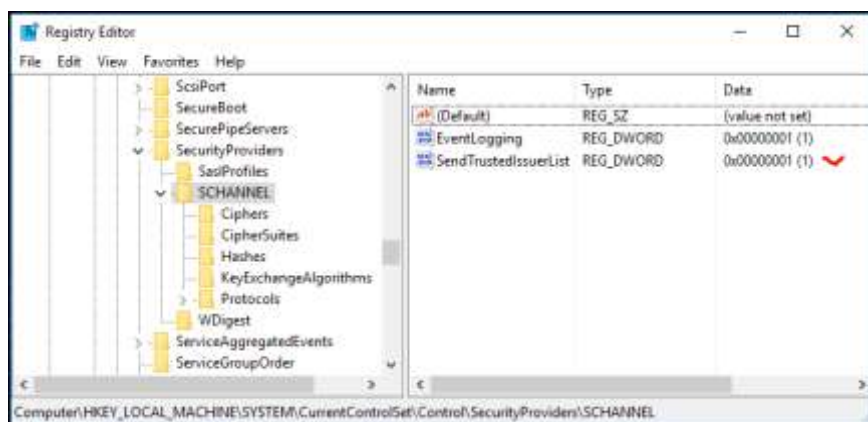
Näeme soovi korral ka IIS-i konfiguratsioonist, et SSL sertifikaat on uuesti korrektselt seotud 443 pordiga.

5) Lubame IIS serveri registrist sertifikaatide filtreerimise lisades määrangu “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Send TrustedIssuerList=1“:



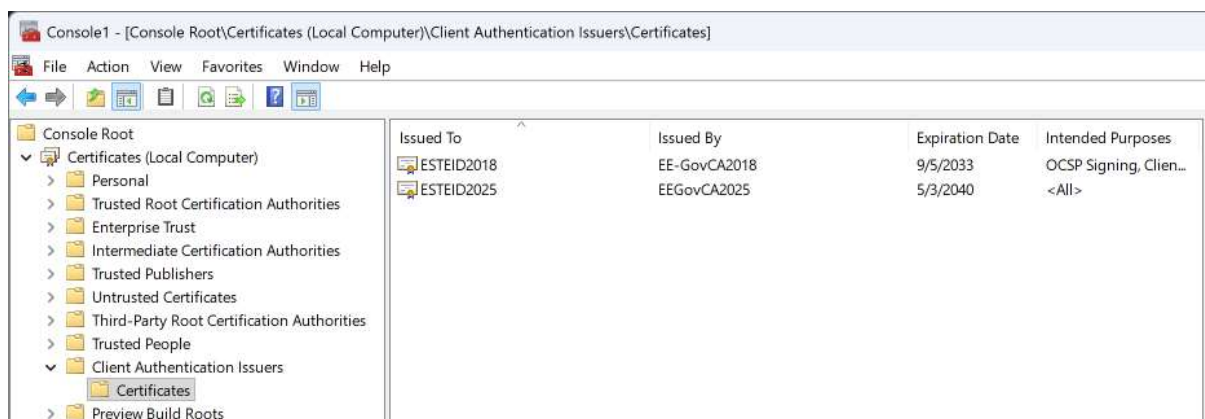
MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 27 - sertifikaatide filtreerimise lubamine registris

- 6) Lisame kesktaseme sertifikaadid IIS serveri sertifikaatide konteinerisse „*Client Authentication Issuers*“:



Pilt 28 - kliendi jaoks lubatud sertifikaatide lisamine õigesse konteinerisse

- 7) Vajadusel taaskäivitame IIS teenuse või serveri ja kontrollime soovitud lahenduse toimimist!

Kliendisertifikaatide kehtivuse kontroll OCSP teenuse vastu

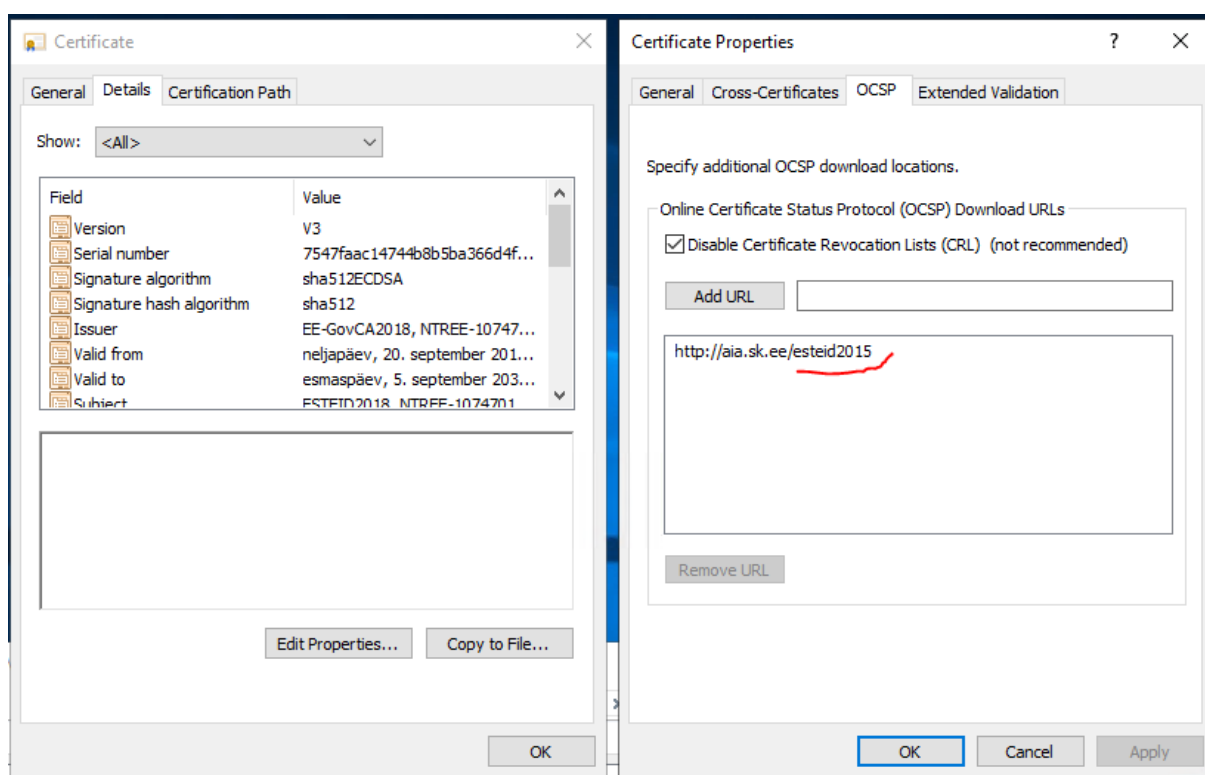
OCSP teenuse abil saame kasutaja sertifikaadi kehtivust kontrollida praktiliselt reaalajas. Iga kasutaja autentimisel saadab veebiserver päringu OCSP teenusele, mis tagastab sertifikaadi kehtivuse info.

ESTEID2018 ja ESTEID2025 CA alt väljastatud sertifikaatide puhul on AIA OCSP aadress juba sertifikaadis kirjas (<http://aia.sk.ee/esteid2018> ja <http://ocsp.eidpki.ee>), nii et siin me tegelikult midagi eraldi konfigureerima ei pea. Küll aga saame soovi korral kehtestada ka keskelt AIA OCSP kontrolli:



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 29 - AIA OCSP tee konfigureerimine

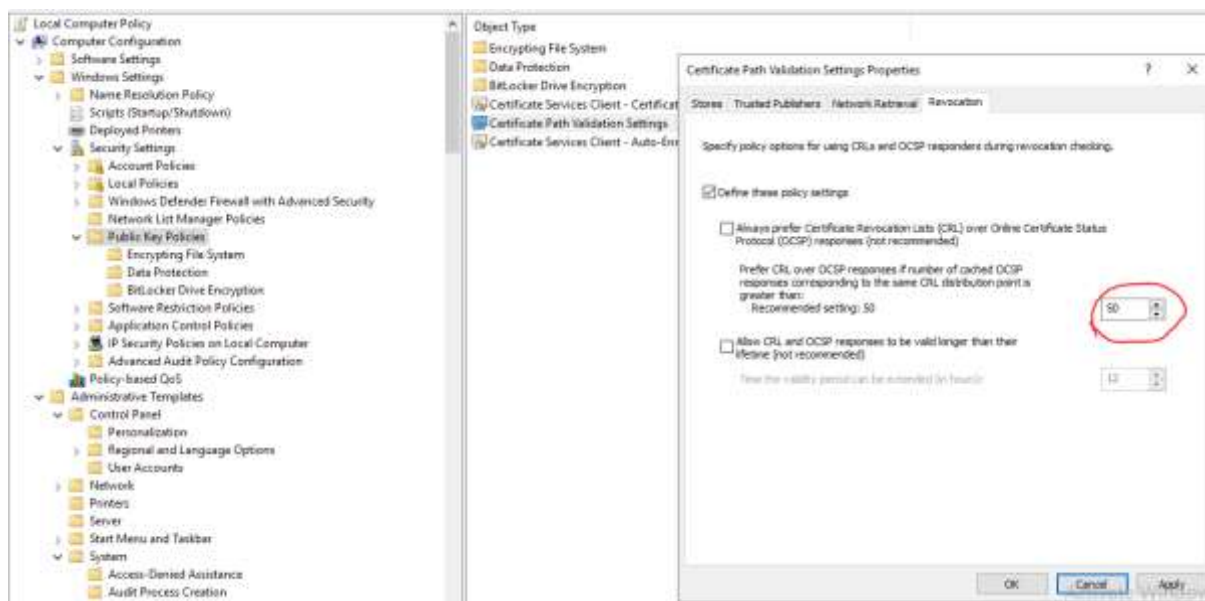
Märkuseid

- Kordan siin selguse mõttes, et ESTEID2018 / ESTEID2025 CA alt väljastatud sertifikaatidel on kehtivuskontrollina kasutusel AIA OCSP teenus aadressiga <http://aia.sk.ee/esteid2018> ja <http://ocsp.eidpki.ee>. CRL teed neis kirjeldatud ei ole.
- Windows serveri puhul pöörduakse vaikumisi OCSP põhiselt sertifikaatide kehtivuse kontrollilt tagasi CRL põhisele kontrollile, kui vahemälus olevate OCSP päringute hulk ületab 50-ne piiri. Meie konfiguratsiooni puhul ei ole see tegelikul oluline, kuna CRL-i me üldse ei kasuta. Muude konfiguratsioonide puhuks mainin, et seda numbrit on võimalik muuta luues registri väärtuse HKEY_LOCAL_MACHINE/Software/Policies/Microsoft/SystemCertificates/ChainEngine/Config/CryptnetCachedOcspswitchToCrlCount ja määrates sinna uue väärtuse. Vt. ka OCSP *magic count* või *magic number*. Ehk aga lihtsamgi tee selle omaduse muutmiseks on *windows policy*:



MS IIS ja eID kaardi tugi

Juhend administraatorile



Pilt 30 - maagilise OCSP numbri muutmine

Soovituslikud IIS'i sätted

SSL/TLS

IIS'i versioon 10 serveril 2022 kasutab vaikimisi kõiki TLS protokollide versioone, 1.0-1.3⁶. Vanemad SSL protokollid ei ole vaikimisi kasutusel.

Tänapäeval ei tohiks kindlasti enam kasutada TLS versioone 1.0 ja 1.1. Kahepoolse autentimise toimimiseks peab olema lubatud TLS versioon 1.2 ja loodetavasti ajutiselt keelatud TLS versioon 1.3 (loe täpsemalt lk 14 – Kahepoolse SSL-i, sertifikaadiga autentimise nõudmine - Eelhäälestus). Kui sertifikaadiga autentimine ei ole oluline, võib hea mõte olla lubada vaid TLSi versioon 1.3.

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/>.

Lisaks IIS konfiguratsiooni juures vanade TLS protokollide keelamisele saame seda teha ka otse registris. Kui me soovime keelata TLS versioonid 1.0 ja 1.1, tuleb meil lisada registrisse järgmine konfiguratsioon⁷:

⁶ <https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-?redirectedfrom=MSDN>.

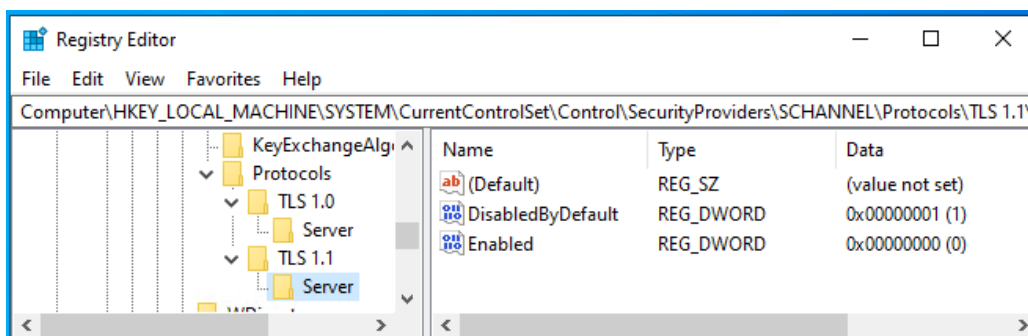
⁷ Vaikimisi neid väärtuseid ei eksisteeri.



MS IIS ja eID kaardi tugi

Juhend administraatorile

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\^8:
 - TLS 1.0\Server
 - Enabled DWORD:0
 - DisabledByDefault = DWORD:1
 - TLS 1.1\Server
 - Enabled DWORD:0
 - DisabledByDefault = DWORD:1



Pilt 31 - TLS versioonide 1.0 ja 1.1 keelamine registris

Ja muidugi on võimalik ülaltoodud registri konfiguratsiooni levitada ka kesksete poliitikate abil.

Šifrikomplektid (Cipher suites)

Windows serveriga tuleb vaikselt kaasa mitmeid šifrikomplekte. Kõiki neid saame vaadata näiteks PowerShell käsuga `Get-TLSCipherSuite`⁹.

Kindlat soovitus erinevate šifrikomplektide kasutamiseks ei ole veebisaidile esitatavaid tingimusi teadmata võimalik anda. Küll aga tundub mõistlik eemaldada loendist ebaturvalised šifrikomplektid (juhul, kui neid seal on). Enne konfiguratsiooniga jätkamist soovitage kindlasti tutvuda RIA tellitud krüptograafiliste algoritmide elutsükli uuringu soovitusetega aadressil <https://www.id.ee/artikkel/krüptograafiliste-algoritmide-elutsükli-uuringud-2/>. Mõistlik võib olla konkreetsete šifrikomplektide lubamine.

Seega, kui soovime ise täpsemalt määrata kasutatavaid šifrikomplekte, on ilmselt parim selleks kasutada kohalikke või keskseid poliitika. Kasutamaks ainult šifrikomplekte ECDHE-ECDSA-AES256-GCM-SHA384 ja ECDHE-RSA-AES256-GCM-SHA384, tuleb meil modifitseerida määrangut "Computer

⁸ Võimalik on konfiguratsioon eraldi ka kliendi osa SSL/TLS protokollide vaates. Hetkel aga räägime ainult serveri poole häälestusest. See ei tähenda, et kliendi osa konfiguratsioon ei ole soovitatav, see sõltub alati konkreetsest situatsioonist.

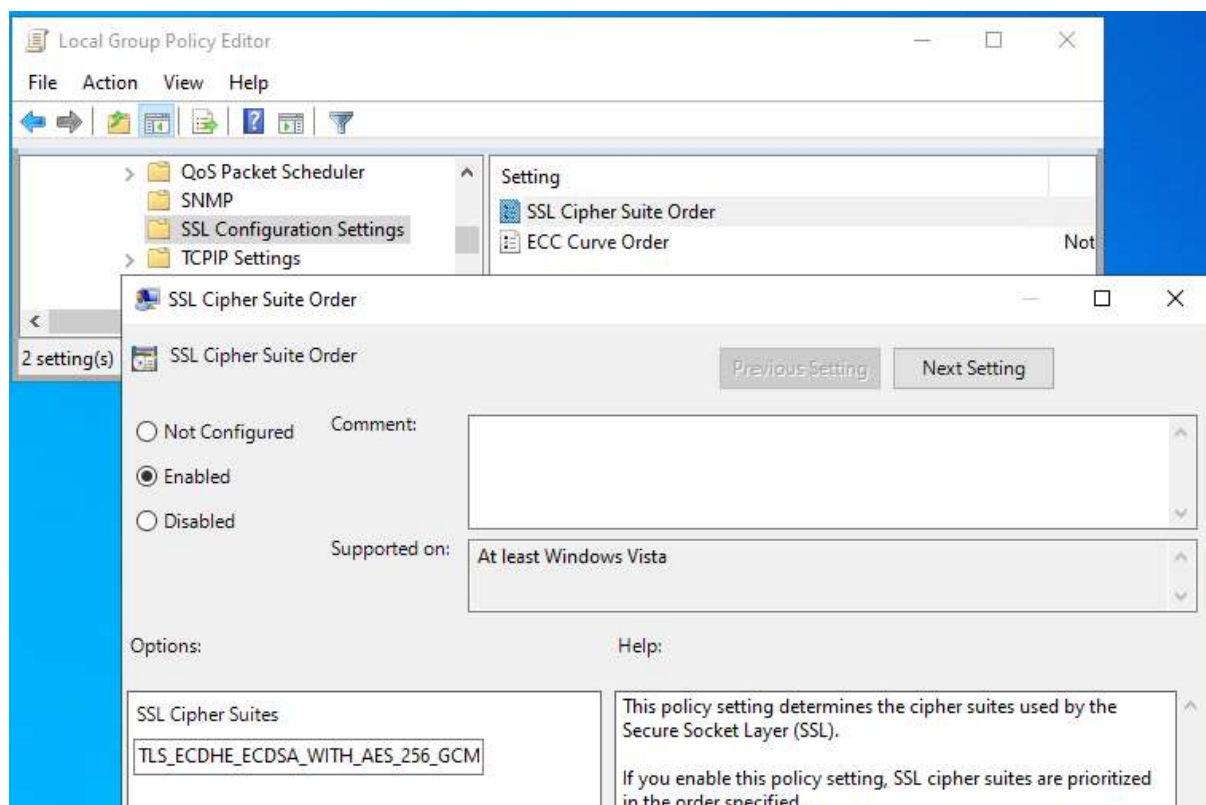
⁹ <https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel>



MS IIS ja eID kaardi tugi

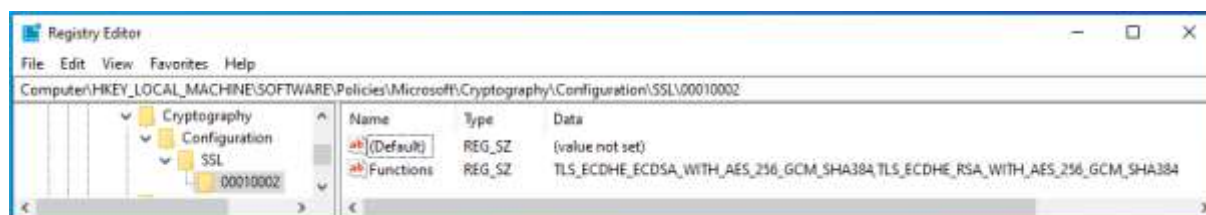
Juhend administraatorile

Configuration/Administrative Templates/Network/SSL Configuration Settings: SSL Cipher Suite Order". Šifrikomplektid tuleb eraldada komaga.¹⁰



Pilt 32 – kindlate šifrikomplektide määramine keskse poliitikaga

Eelmises punktis määratud konfiguratsioon kirjutatakse registrisse:



Pilt 33 - poliitikaga määratud konfiguratsioon

Vaikimisi on šifrikomplektid kirjeldatud järgmisel pildil kirjeldatud asukohas:

¹⁰ Märkime siinkohal, nende konkreetsete määrangutega TLS 1.3 ei toimi! Pigem võib nende määrangute kasutamine olla mõttekas juhul, kui me ei soovi TLS 1.3-e kasutada, kasvõi näiteks sertifikaadiga autentimise lubamise puhul.



MS IIS ja eID kaardi tugi

Juhend administraatorile

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Cryptography\Configuration\Local\SSL\00010002

Name	Type	Data
(Default)	REG_SZ	NCRYPT_SCHANNEL_INTERFACE
EccCurves	REG_MULTI_SZ	curve25519 NistP256 NistP384
Functions	REG_MULTI_SZ	TLS_AES_256_GCM_SHA384 TLS_AES_128_GCM_SHA256 TL

Pilt 34 - vaikimisi šifrikomplektide konfiguratsioon

Muud konfigureeritavad Schannel omadused

Vaikimisi asukoht Schanneli konfigureeritavatele omadustele on registris: HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL. Siin on võimalik erinevaid komponente lubada või keelata, kirjutada vajadusel üle vaikimisi konfiguratsiooni määranguid.

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL

Name	Type
(Default)	REG_SZ
EventLogging	REG_DWORD

Pilt 35 - Schannel konfigureeritavad omadused



MS IIS ja eID kaardi tugi

Juhend administraatorile

Muud võimalused

Lisaks TLS-i ja šifrikomplektide konfigureerimisele, saame palju muudki ära teha oma IIS-i serveri turvamiseks:

- Hoiame operatsioonisüsteemi ajakohasena
- Keelame serveri info presenteerimise.
- Keelame HTTP päringud.
- Keelame failide lappamise võimaluse (*directory listing*).
- Kasutame mitte-süsteemseid ja mitte-administraator kontosid.
- Lubame HSTS'i.
- ...

Palume suhtuda ülalloodusse kui näidisloendisse demonstreerimaks, mida veel saab IIS'i turvalisemaks muutmise jaoks ära teha. Põhjalikemaid soovitusi on võimalik leida paljudelt internetilehtedelt: <https://www.google.com/search?q=how+to+secure+IIS+server>.