IIS VEEBISERVERILE ID-KAARDI TOE SEADISTAMINE

Dokumendi info	
Loomise aeg	21.01.2019
Tellija	Riigi Infosüsteemi Amet
Autor	Urmas Vanem, OctoX
Versioon	25.03/1

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 kohta 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 soovitused IISi turvamiseks. Muutja: Urmas Vanem
14.12.2020	20.12/1	Lisatud turvasätted ebasoovitavate CAde ligipääsu piiramiseks. Muutja: Urmas Vanem
17.12.2020	20.12/2	Lisatud mõned turvassoovitused peatükki „Ebavajalike CAde 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 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
28.02.2025	25.02/1	Lisatud Thales testkaart. Muutja: Urmas Vanem

Sissejuhatus

Käesolevas juhendis kirjeldatakse IIS veebiserveri konfiguratsiooni kahepoolse SSLi kasutamiseks, kus kasutajapoolseks sertifikaadiks on Eesti ID-kaardile (siin ja edaspidi: Eesti ID-kaardi mõiste all on mõeldud kodaniku ID-kaarti, elamisloakaarti, digi-IDd ja e-residendi digi-IDd) väljastatud sertifikaat. Uue asjana oleme siia juhendisse lisanud Thalese testkaardi konfiguratsiooni puudutava informatsiooni.

Juhendi loomisel on kasutatud Windows Server 2022 ja Windows 11 operatsioonisüsteeme. Näidisjuhendis on toetatud SK ID Solutions AS (edaspidi SK) „EE-GovCA2018“ ja Zetese „Test EEGovCA2025“ ahelatest pärinevad sertifikaadid. Tagamaks sertifikaatide äratundmist, peab klientarvutitel olema paigaldatud vajalik tarkvara:

- Idemia kaartide jaoks ID-tarkvara (soovitame kasutada värskeimat ID-tarkvara versiooni, mille saab veebilehelt id.ee).
- Thalese kaartide jaoks testkaardi toega ID-tarkvara, mille saab siit.

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 pärast sertifikaadi kehtivuse kontrolli lubatakse kasutaja eelnevalt määratud kasutaja (IUSR) õigustes veebilehele ligi.

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

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

Ühepoolse SSL/TLSi konfigureerimine

Windows serveri sertifikaadi konfiguratsioon

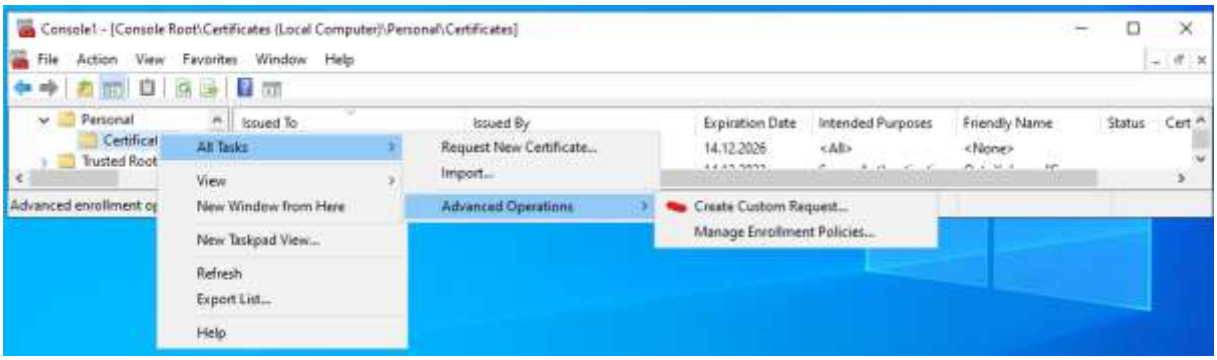
Pakkumaks turvalist veebiteenust peab IIS serverile olema määratud TLS sertifikaat - käesolevas näites on kasutusel OctoX testkeskkonnast väljastatud sertifikaat. Nii kasutajad kui veebiserver peavad seda sertifikaati usaldama.

Domeeni keskkonna ja domeeni (*enterprise*) sertifitseerimiskeskuse (CA) olemasolul on mõistlik küsida ka serveri sertifikaat domeeni CA-lt. Ent kui sellist võimalust ei ole või kui on vaja sertifikaati, mis on laiemalt usaldatud, siis tuleb luua sertifikaadi privaatvõti ja päringufail (CSR) ning lasta viimase alusel luua sertifikaat mõnel üldtuntud CA-l.

Serveri sertifikaadi hankimine

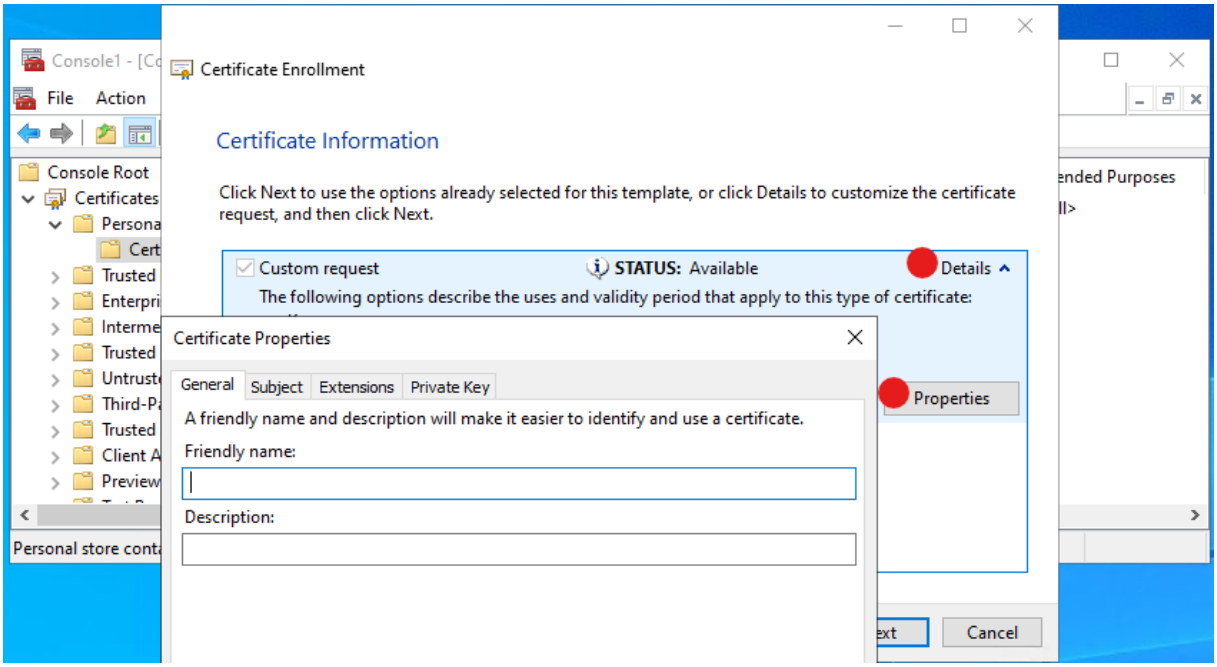
Kuna IIS halduskonsoolilt loodav sertifikaadi päringufail on üsna piiratud võimalustega, tuleks serveri sertifikaadi päringufaili loomiseks kasutada hoopis sertifikaatide halduskonsooli. (Märgin siinkohal veelkord selgituseks, et alltoodud juhendit on mõttekam kasutada pigem sellise IIS serveri loomiseks, mis kasutab mõne avaliku CA poolt väljastatud sertifikaati. Kui meile piisab oma CA lahenduse sertifikaadist, siis saame kasutada mõnd lokaalselt väljastatud sertifikaati millele EKU-sse on kirjutatud *Server Authentication*.)

1. Käivita IIS serveril mmc.exe ja lisa sinna lokaalse arvuti sertifikaatide vaade. Loo kohandatud päring:



Pilt 1 – kohandatud päringu loomine

2. Kliki kolm korda *Next, a*va *Details, Properties.* Avaneb sertifikaadi päringu omaduste aken:



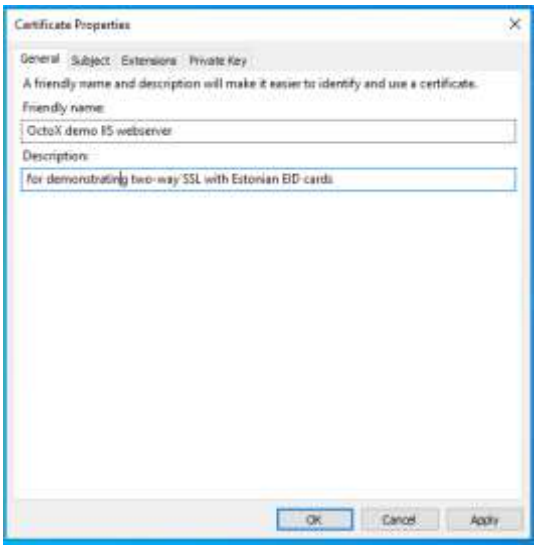
Pilt 2 – sertifikaadi päringu omaduste aken

3. Järgnevalt saab määrata päringufailile täpsed omadused, mida soovitakse hiljem veebiserveri sertifikaadi juures näha.

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

Sakk General

Siin saab soovi korral määrata sertifikaadi hüüdmine ja põgusa kirjelduse. Need väljad ei ole sertifikaadi sisulised osad ja need selgitused omavad tähendust hilisema lihtsama arusaamise jaoks.



Pilt 3 - sertifikaadi üldinfo

Sakk Subject

Aknas *Subject* saab tavapäraselt subjekti kirjeldada. Kui on soov kasutada erinevad SAN DNS nimesid või kasutada *common name* puhul midagi muud kui FQDN, siis tuleb üks või mitu DNS aliast siin ka kirjeldada.

Pilt 4 - subjekti näidiskonfiguratsioon

Sakk Extensions

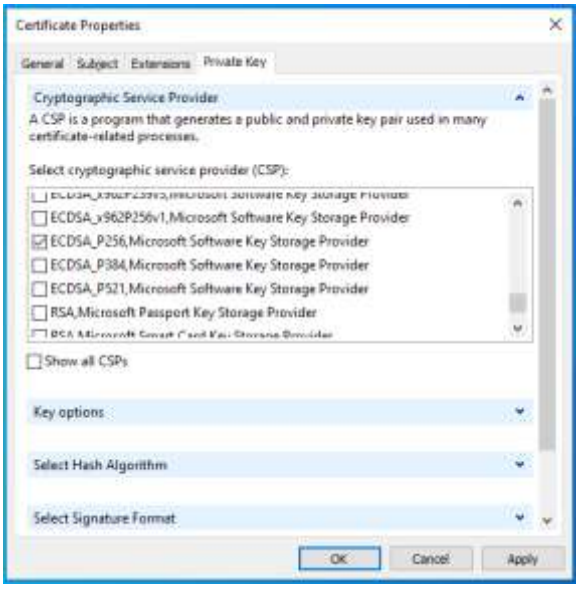
Aknas *Extensions* saab määrata järgmised omadused:

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

Pilt 5 - laienduste määramine

Sakk Private Key

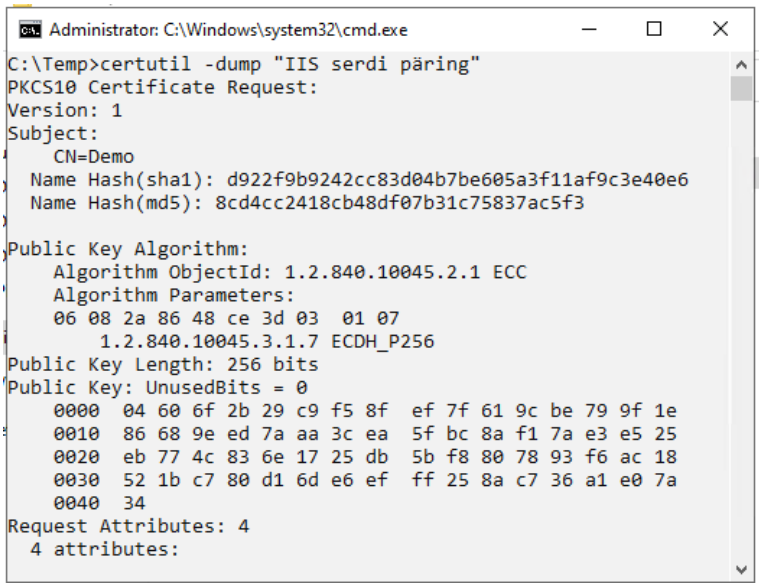
Siin tuleb valida CSP ehk sertifikaadi võtmete algoritm. Näidiskonfiguratsioonis on kasutatud algoritmi ECDSA_P256, seega tuleb valida loendist ECDSA_P256 ja eemaldada nimekirja alguses olev RSA.



Pilt 6 - CSP valimine

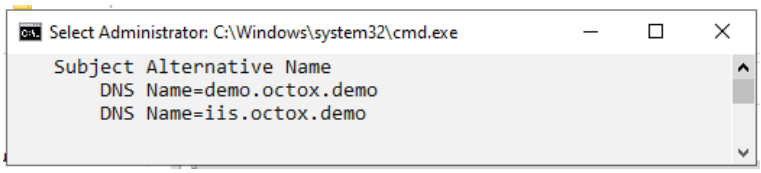
Kliki *OK* ja *Next*, määra kaust ja nimi ning salvesta sertifikaadi päringufail Base64 formaadis.

Värskelt loodud sertifikaadi päringufaili omadusi võib kontrollida käsuga „certutil -dump PÄRINGUFAILI_NIMI“.



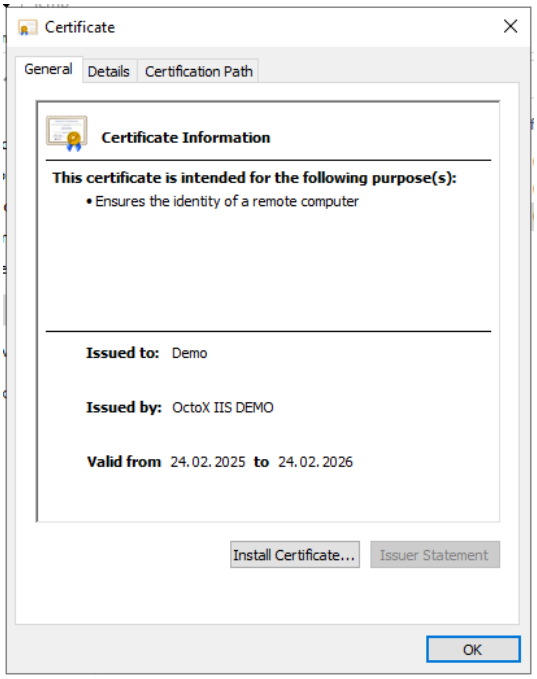
Pilt 7 - päringufaili sisu

Veendu, et ka DNS alternatiivsed nimed on päringufailis olemas:



Pilt 8 - DNS aliased päringufailis

Nüüd tuleb edastada sertifikaadi päringufail mõnele CA serverile ja paluda selle alusel genereerida sertifikaat. Tulemus on järgmine:



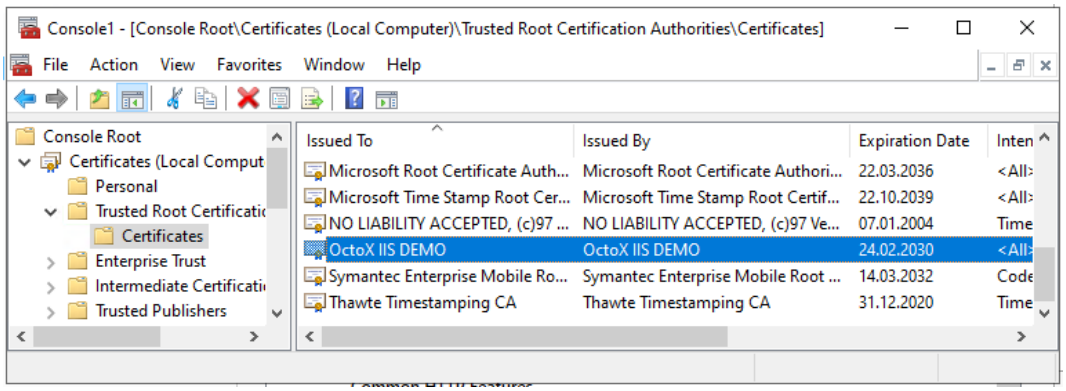
Pilt 9 – IIS serveri sertifikaat

Sertifikaadi paigaldamine

IIS server peab usaldama sertifikaati „OctoX IIS Demo“, mis on serveri IIS teenuse sertifikaadi väljastajaks. Selleks tuleb kontrollida selle sertifikaadi olemasolu usaldusväärsete juursertifikaatide[1] konteineris. Kui väljastaja CA sertifikaat seal puudub, tuleb see lisada.[2]

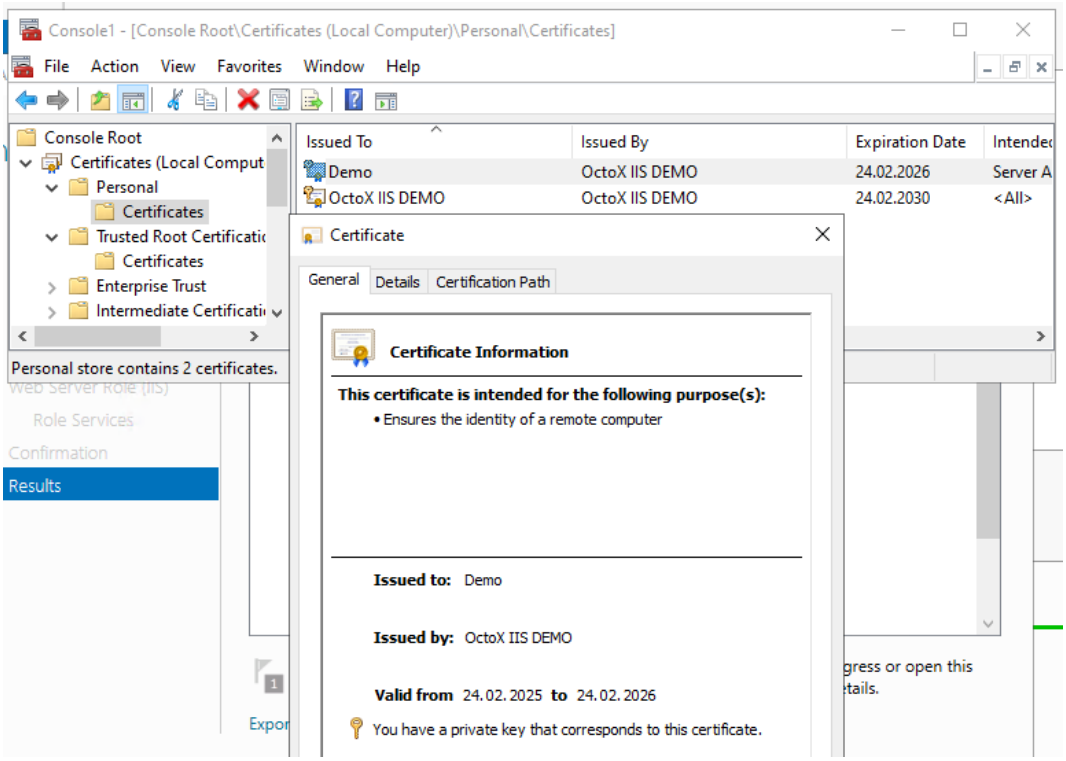
[1] *Trusted root certification authorities*

[2] Juhul, kui sertifikaadi on väljastanud mõni kesktaseme CA, siis tuleb see puudumisel lisada kesktaseme sertifitseerimiskeskuste konteinerisse. Ja kesktaseme CA sertifikaadi väljastanud juur-CA sertifikaat tuleb puudumisel lisada usaldusväärsete juursertifikaatide konteinerisse.



Pilt 10 - IIS server usaldab temale sertifikaadi väljastanud CAd

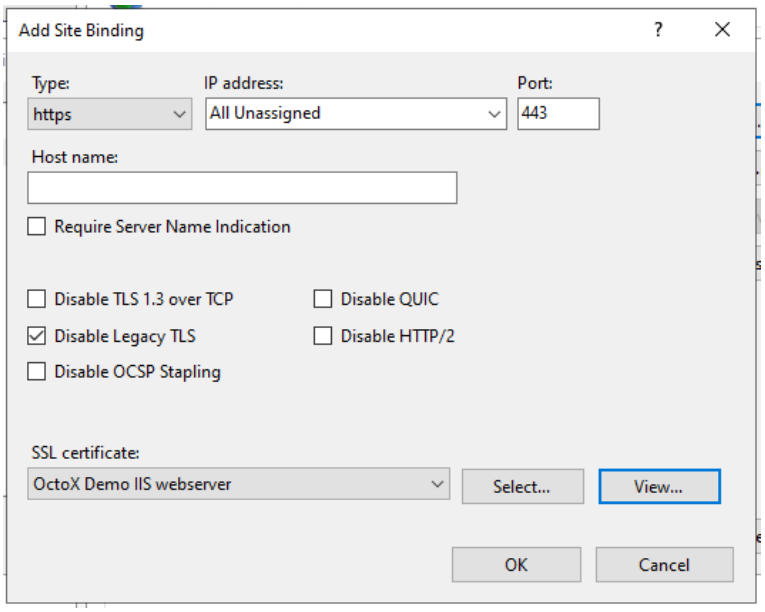
IIS serveri sertifikaat tuleb paigaldada IIS serveris lokaalse arvuti personaalsesse konteinerisse:



Pilt 11 - avades sertifikaadi on näha, et IIS server saab ootuspäraselt ka selle privaatvõtit kasutada

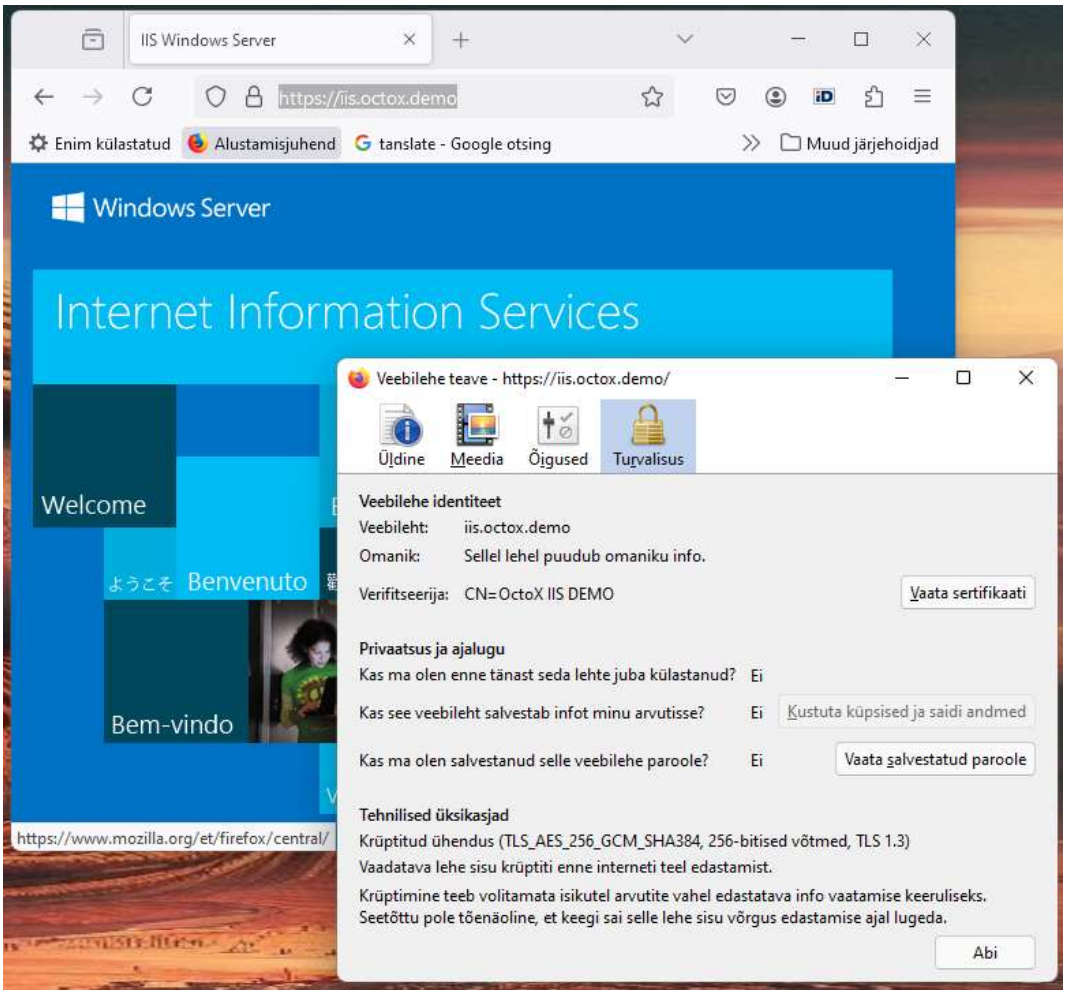
Ühepoolse SSLi konfiguratsiooni loomine

Ühepoolse SSLi kehtestamiseks peab veebilehel olema kirjeldatud SSL port (vaikimisi 443) ja see peab olema seotud soovitud sertifikaadiga. Koheselt tuleb keelata ka vanade SSL/TLS protokollide (vanemad kui 1.2) kasutamine.



Pilt 12 - veebilehel on lubatud 443 port ja kasutatavaks sertifikaadiks on „OctoX IIS Demo“, vanad TLS protokollid tuleb keelata

Peale määrangute kinnitamist ühepoolne SSL töötab.



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

Ühepoolse SSLi demonstreerimiseks kasutatud Firefox veebilehitseja näitab lisainfo akendes veel ka järgmist:

1. Kasutusel on värskelt paigaldatud sertifikaat iis.octox.demo;
2. Kasutusel on TLS 1.3 protokoll.

HTTP ligipääsu piiramine

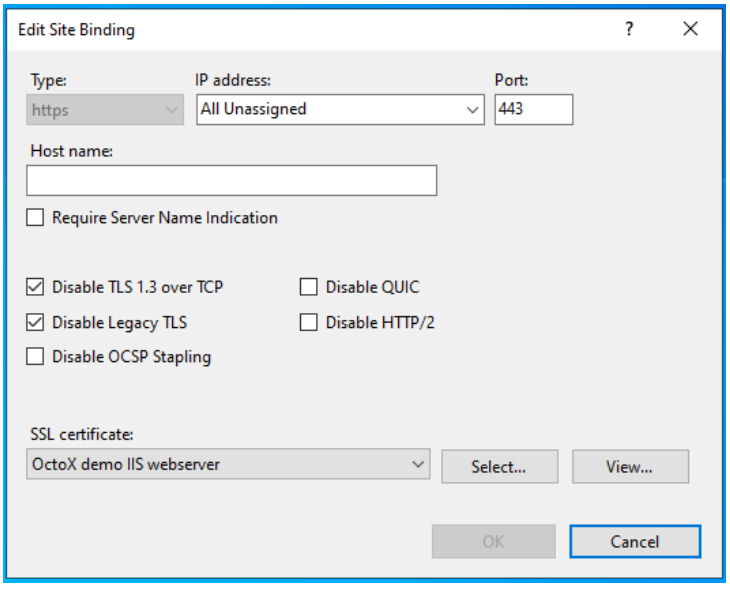
HTTP ligipääsu keelamiseks tuleb seotud protokollide loendist eemaldada port 80 ja keelata ka tulemüürist vastav ligipääs. Alternatiivina võib suunata HTTP liikluse automaatselt HTTPS veebilehele vältimaks probleemi, kus kasutajad kirjutavad ise veebilehitsejasse veebilehe aadressi ent ei lisa sinna ette HTTPS:// määrangut.

Kahepoolse SSLi konfigureerimine ehk sertifikaadiga autentimise nõudmine

Eelhäälestus

Juhime tähelepanu, et IIS 10/Schannel (seisuga 18.01.2022, mis kohandati Windows Server 2022 serverile,) kasutab protokolli TLS 1.3 abil sertifikaadiga autentimiseks vaikimisi *post-handshake* autentimismeetodit. Kuna enimlevinud veebilehitsejad seda ei toeta[3], siis see lahendus praktikas ei toimi. Juhul, kui TLS 1.3 on sisse lülitatud, ei saada server kasutajale vaikimisi konfiguratsioonis sertifikaadi päringut ja katkestab ühenduse. Sertifikaadiga autentimise tööle saamiseks tuleb keelata TLS 1.3 kasutamine. Alternatiivina saab sisse lülitada *in-handshake* autentimismeetodi, vt. peatükk „*In-handshake* autentimismeetodi lubamine".

TLS protokolli versiooni 1.3 saab välja lülitada IIS HTTPS seose lehelt, märkides linnuke lahtrisse „Disable TLS 1.3 over TCP":



Pilt 14 – sertifikaadiga autentimise lubamiseks peab TLS 1.3 protokolli keelama

Eesti eID sertifikaatide häälestus IIS serveril

Kahepoolse SSLi 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 EKUs kirjeldatud *client authentication* laiend. Korrektseks toimimiseks peab server suutma

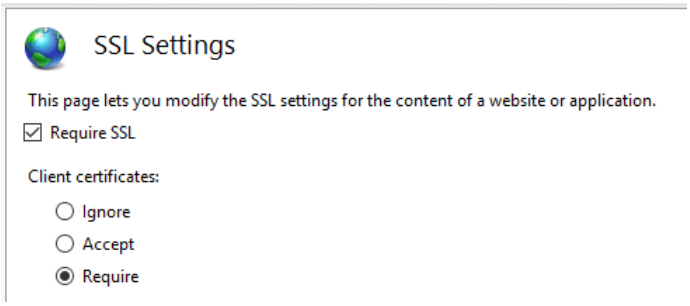
[3] Teadaolevalt Firefox veebilehitseja küll toetab, ent ka sellel veebilehitsejal ei ole see vaikimisi lubatud.

luua kogu sertifikaadiahela alates kasutajasertifikaadist kuni juursertifikaadini. See tähendab, et IIS serveris on vajalik lisaks juurtaseme sertifikaatide olemasolule ka kesktaseme (*intermediate*) sertifikaatide olemasolu.

Näidiskonfiguratsiooni puhul tuleb IIS serveris sertifikaadid publitseerida järgmiselt:

1) Idemia kaartide ahela sertifikaadid:
    a. Usaldusväärsete juursertifikaatide konteinerisse: EE-GovCA2018
    b. Kesktaseme sertifikaatide konteinerisse[4]: ESTEID2018
2) Thalese kaartide ahela sertifikaadid:
    a. Usaldusväärsete juursertifikaatide konteinerisse: Test EE-GovCA2025
    b. Kesktaseme sertifikaatide konteinerisse: Test ESTEID2025

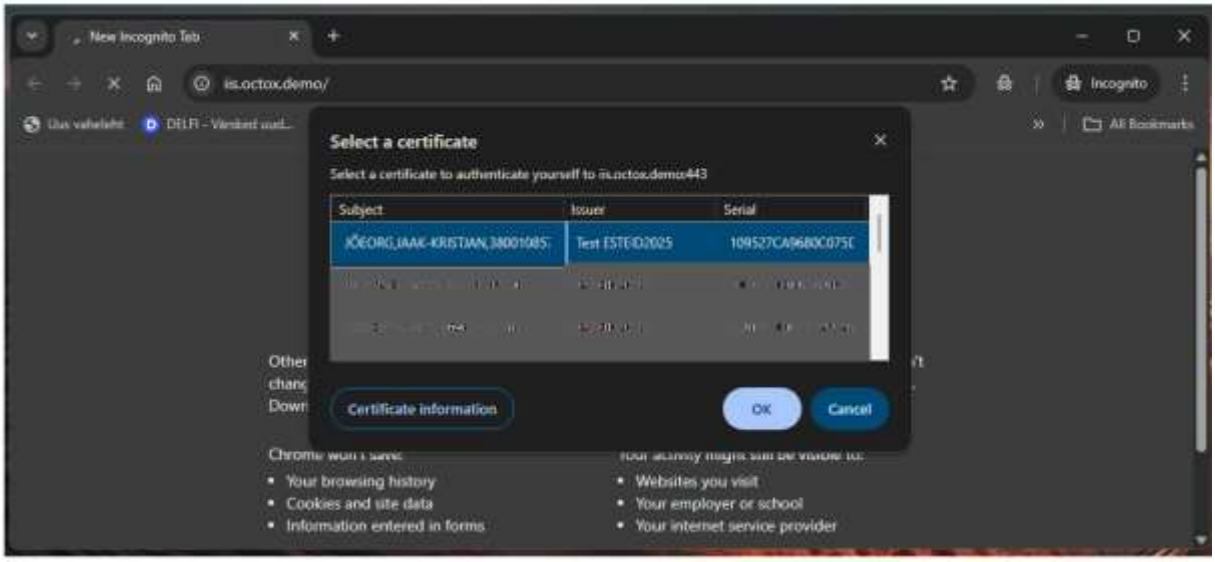
Veebilehe SSL omaduste all tuleb nõuda SSL protokolli ja kasutaja sertifikaatide kasutamist:



Pilt 15 - SSL ja sertifikaadi nõue

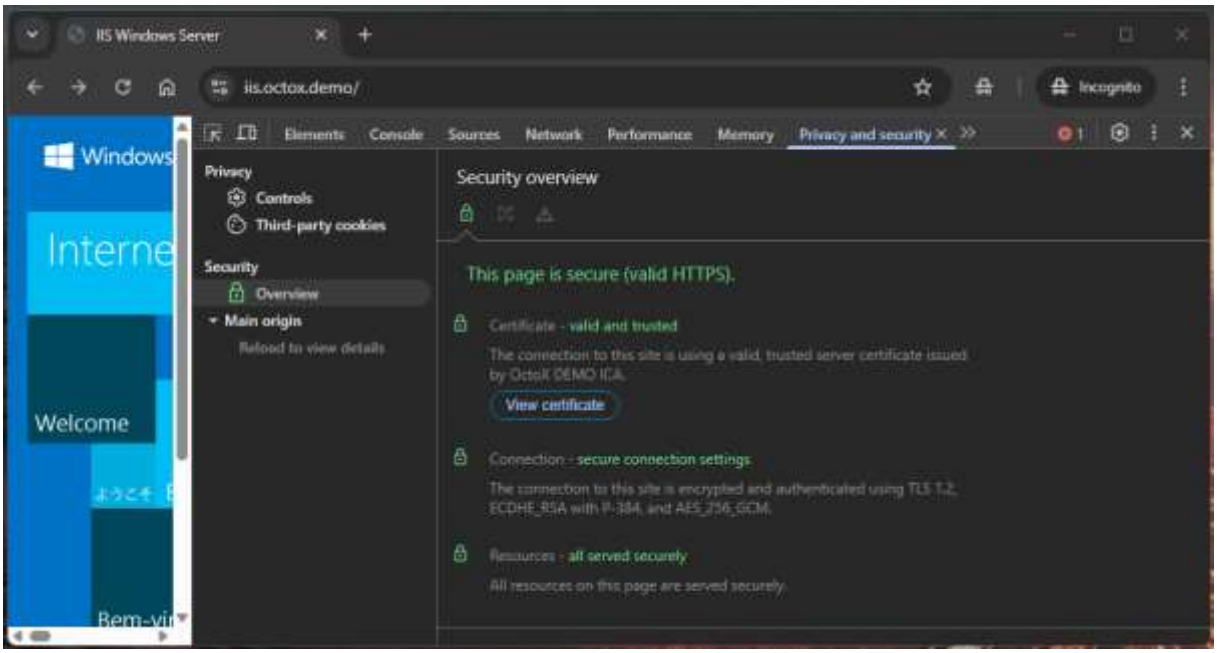
Loodud konfiguratsioon lubab veebilehele ligipääsu pordi 443 kaudu, kus kasutajalt nõutakse sertifikaati. Pöördudes veebilehe poole lubatakse valida serveri poolt aktsepteeritud soovitud sertifikaat:

[4] 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.



Pilt 16 - veebilehele pöördudes sertifikaadi küsimine Firefox veebilehitsejas

Pärast PIN-koodi sisestamist kontrollitakse veebiserveris sertifikaadi staatust ja kui kõik on korras, lubatakse kasutaja veebilehele.



Pilt 17 - autentimine õnnestus kasutades protokolli TLS 1.2

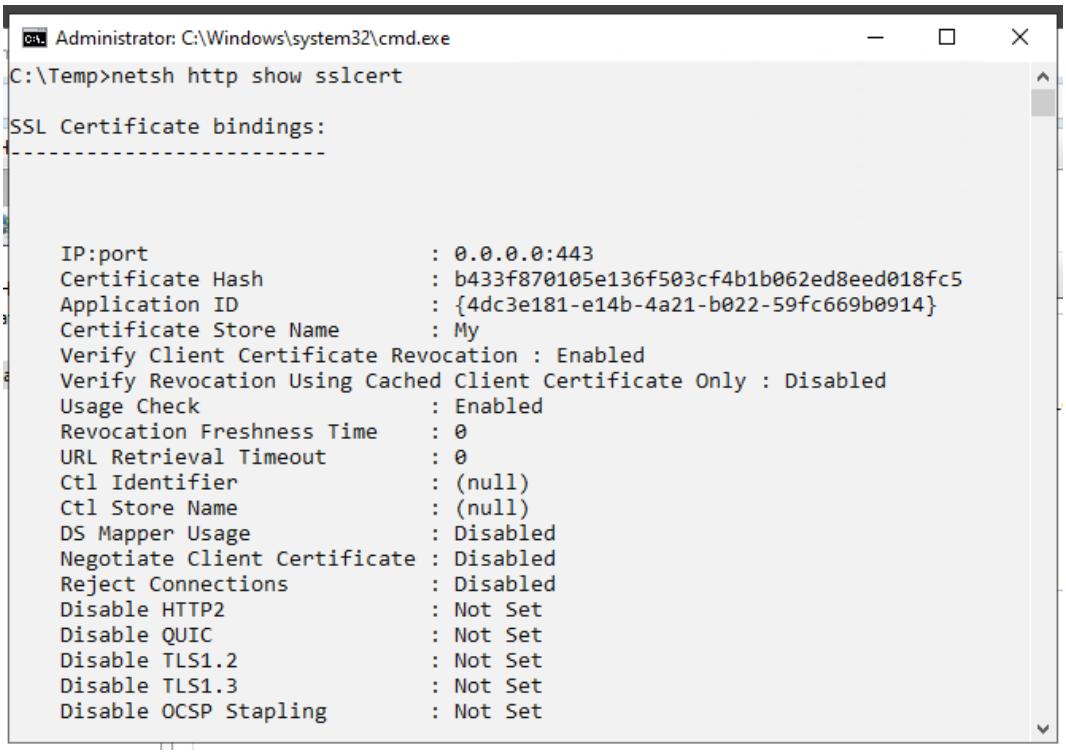
Alternatiivina võib IISi poolse sertifikaadinõude (*Require*) asemel kasutada ka lihtsat sertifikaadi aktsepteerimist (*Accept*) IIS serveri poolt – see võimaldab lisaks sertifikaadile saada serverile ligi ka kasutajanime ja parooliga või üldse autentimata.

In-handshake autentimismeetodi lubamine

Kui on soov kasutada TLS 1.3 protokolli ja kasutada sertifikaadiga autentimist, saab kasutada *in-handshake* autentimismeetodit. Selle meetodi puhul küsib server kasutajalt *Server Hello* saatmisel koheselt ka sertifikaati.

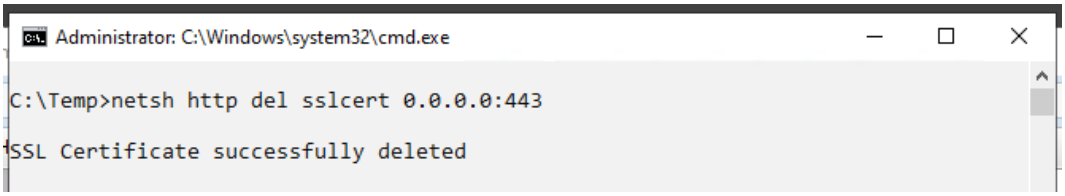
In-handshake autentimismeetodi lubamiseks tuleb teha järgmist:

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



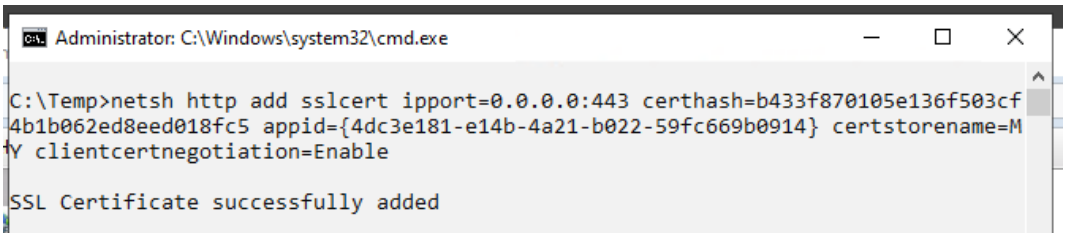
Pilt 18 - vaikimisi on määrang "negotiate client certificate" keelatud

2) Eemaldada sertifikaadi seotus pordiga 443 käsuga „netsh http del sslcert 0.0.0.0:443“:



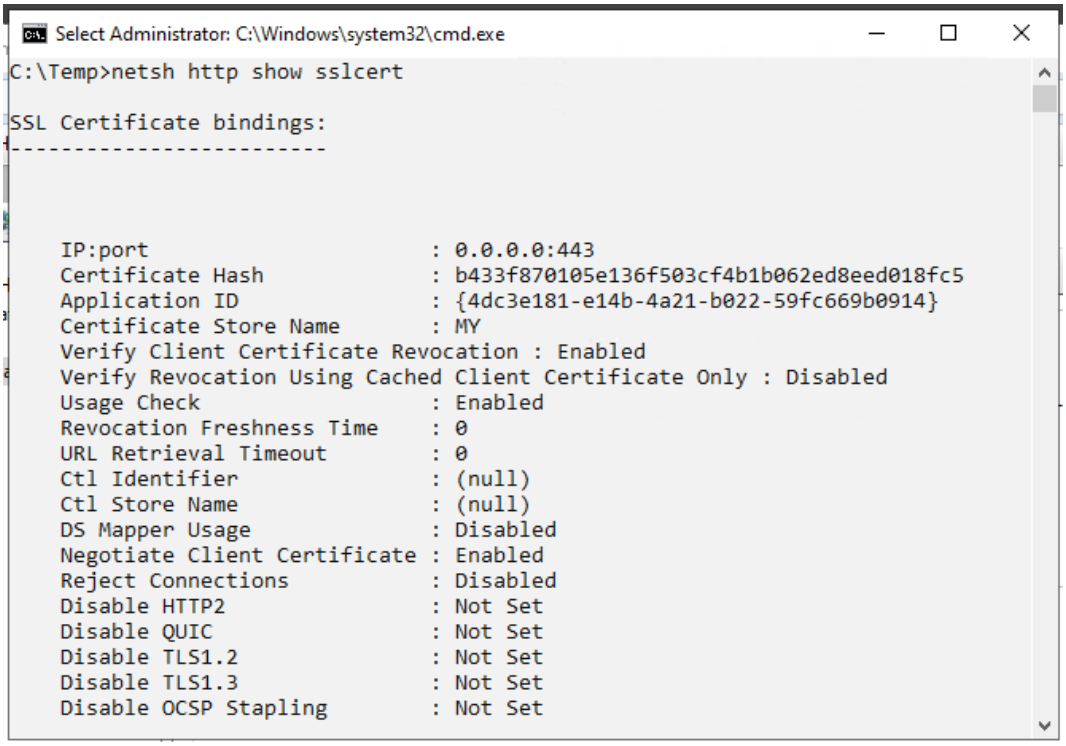
Pilt 19 - sertifikaadi eemaldamine pordi 443 küljest

3) Lisada sertifikaat uuesti lubades ühtlasi ka *in-handshake* autentimismeetod käsuga „netsh http add sslcert ipport=0.0.0.0:443 certhash=b433f870105e136f503cf4b1b062ed8eed018fc5 appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=MY **clientcertnegotiation=Enable**“:



Pilt 20 - clientcertnegotiation lubamine

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



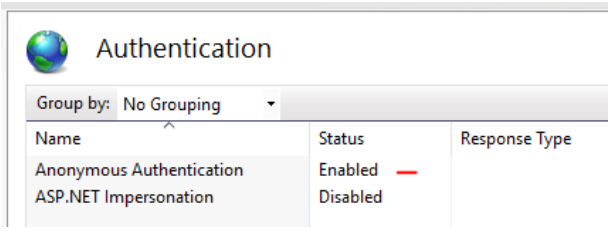
Pilt 21 - in-handshake autentimismeetod on nüüd sisse lülitatud

Märkus:

Kuna *session renegotiation* on TLS 1.3 puhul keelatud, siis selle meetodi puhul tuleb arvestada asjaoluga, et autentimine peab toimuma „esimesel lehel“. Kui kasutaja sertifikaadiga on juba autentimata ühepoolne SSL ühendus loodud ja soovitakse samal lehel mõnele kaitstud ressursile kasutaja sertifikaadiga autentides ligi pääseda, siis see ebaõnnestub, kuna TLS 1.3 ei toeta sellist lähenemist. Vajadusel tuleb see „maandumise“ probleem ühel või teisel viisil lahendada.

Autentimine

Käesolevas näites on lubatud ainult anonüümne autentimine:



Pilt 22 - anonüümne autentimine, kasutaja saab veebilehele ligi kasutaja (IUSR) õigustes

Võimalikud lisakonfiguratsioonid

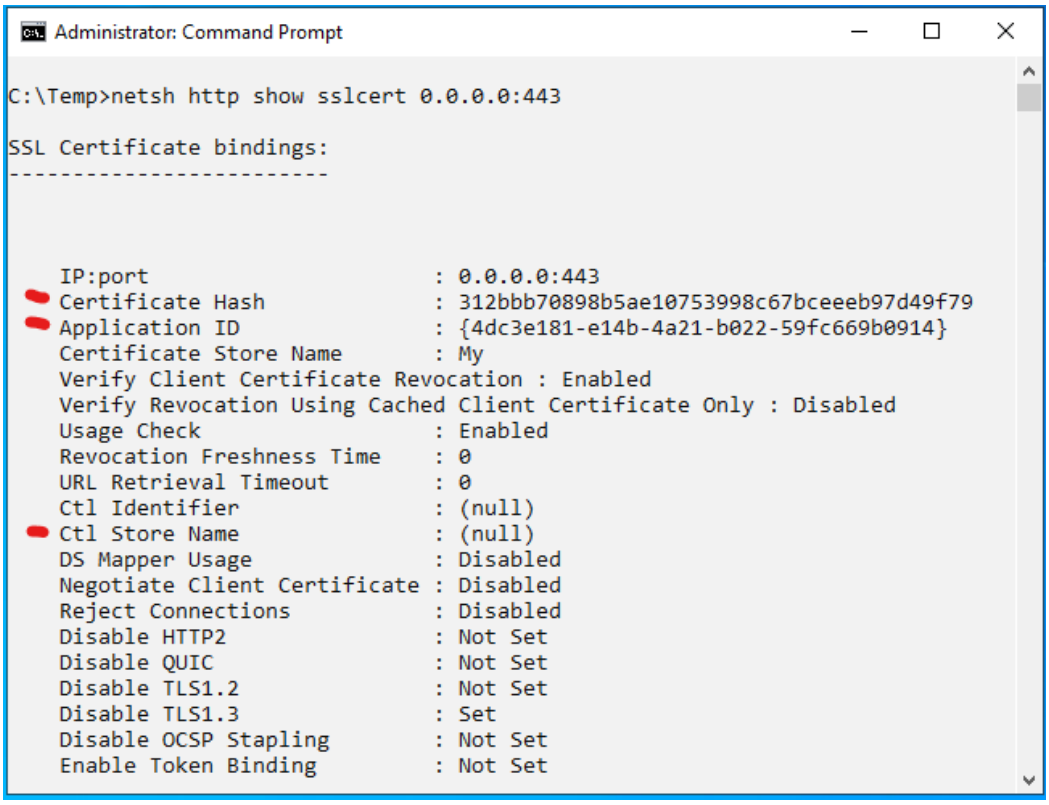
Käesoleva dokumendi eesmärk ei ole anda täpseid juhiseid optimaalseks veebilehtede konfigureerimiseks ega turvamiseks, vaid tutvustada konfiguratsiooni kahepoolse SSLi kasutamiseks Eesti ID-kaartidega. Siiski on oluline arvestada allolevaga.

Kasutajale kuvatavate sertifikaatide filtreerimine

Vaikimisi konfiguratsioonis ei piirata kasutajatele kuvatavate sertifikaatide valikut, mis tähendab, et veebiserverisse autentimisel näidatakse kasutajale kõiki kasutaja käsutuses olevaid sertifikaate, millel on EKU omaduste all kirjas kasutaja autentimine. IISi poolt on aga võimalik kasutajale ette anda loend lubatud autentimiskeskustest ja seeläbi kasutajale kuvada vaid toetatud ahelate sertifikaadid.

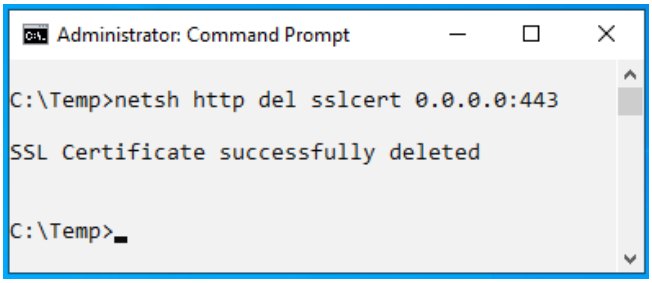
Kui eesmärk on kuvada kasutajale vaid sertifikaadid, mis pärinevad kindlate juursertifikaatide, „EE-GovCA2018“ või „Test EE-GovCA2025“ ahelatest, siis tuleb toimida järgmiselt:

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



Pilt 23 - vaikimisi seotud sertifikaadi omadused

2) Eemalda selle sertifikaadi seos käsuga “netsh http del sslcert 0.0.0.0:443”:



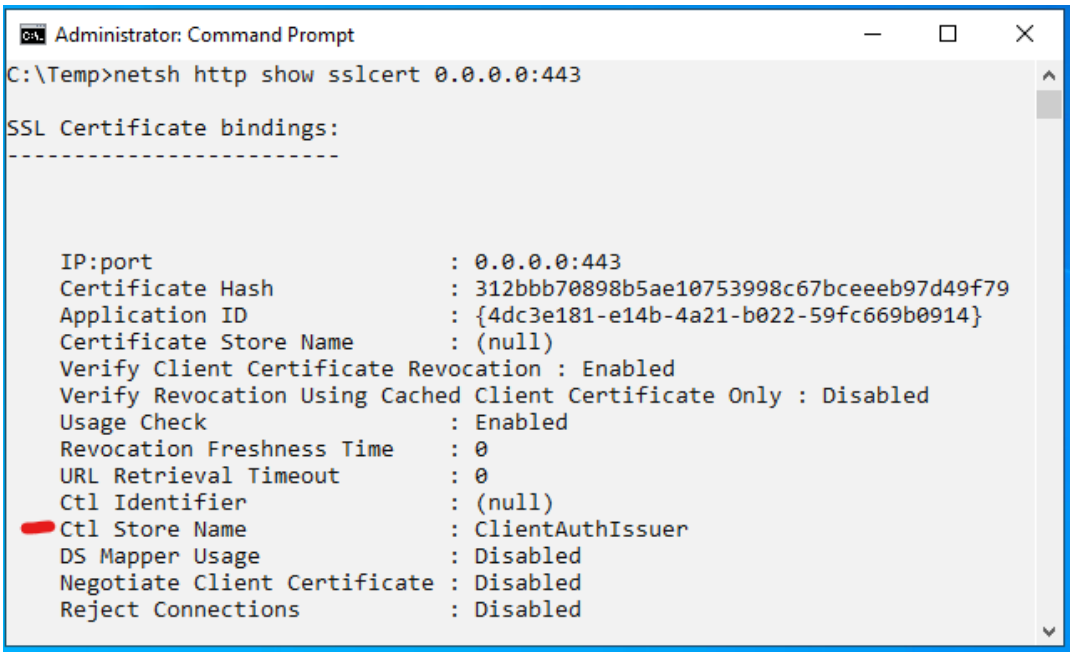
Pilt 24 - sertifikaadi eemaldamine

3) Lisa sertifikaat uuesti ja määra sertifikaatide filtreerimiseks arvuti sertifikaatide kaust *„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“:

Pilt 25 - uute omadustega sertifikaadi lisamine

Certhash ja *appid* väärtused saab esialgsest sertifikaadi väljavõttest, vt. „Pilt 23 - vaikimisi seotud sertifikaadi omadused“.

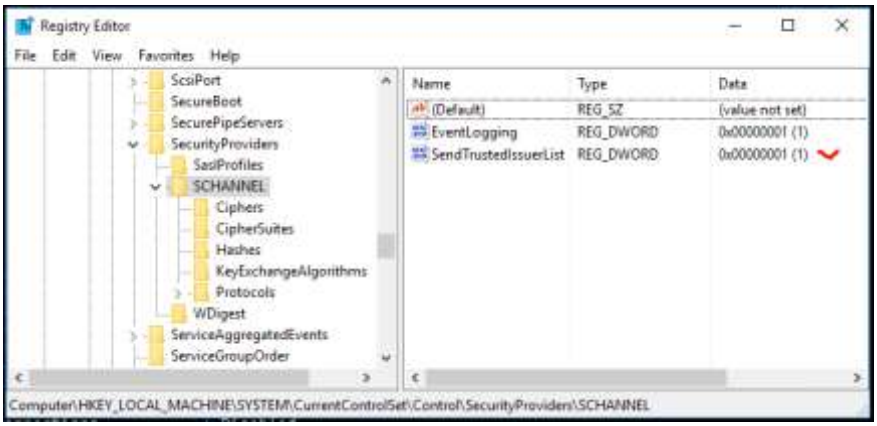
4) Kontrolli, et “*CTL Store Name*” on uuel sertifikaadi väljavõttel *ClientAuthIssuer*:



Pilt 26 - uuesti seotud sertifikaadi omadused

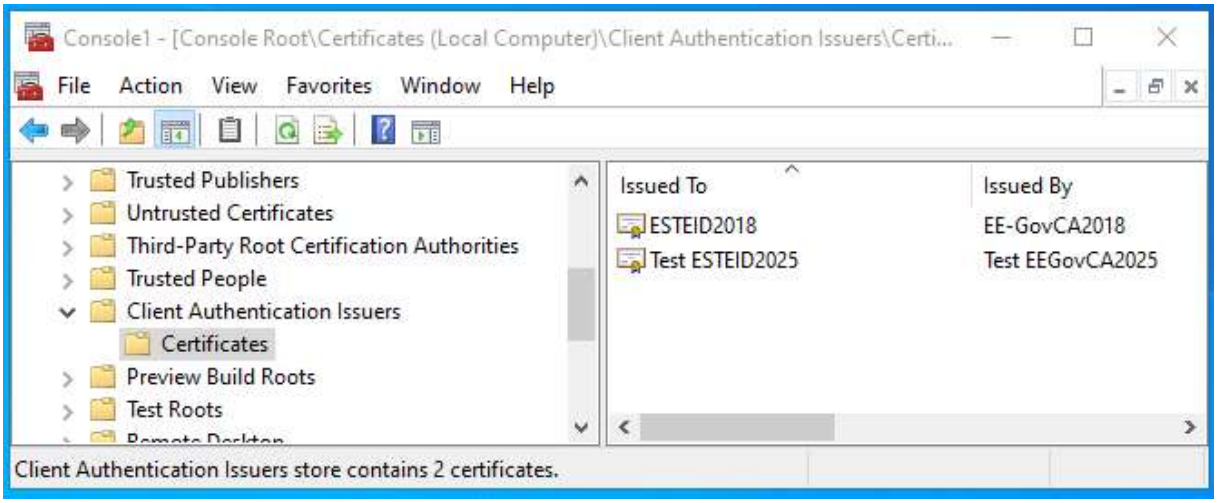
Soovi korral näeb ka IIS-i konfiguratsioonist, et SSL sertifikaat on uuesti korrektselt seotud 443 pordiga.

5) Luba IIS serveri registrist sertifikaatide filtreerimine lisades määrang “HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendTrustedIssuerList=1“:



Pilt 27 - sertifikaatide filtreerimise lubamine registris

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



Pilt 28 – siin näites on lisatud nii Idemia kui ka Thalese ahela sertifikaadid

7) Vajadusel taaskäivita IIS teenus või server ja kontrolli soovitud lahenduse toimimist.

Kasutaja sertifikaadi staatuse kontroll OCSP teenuse vastu

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

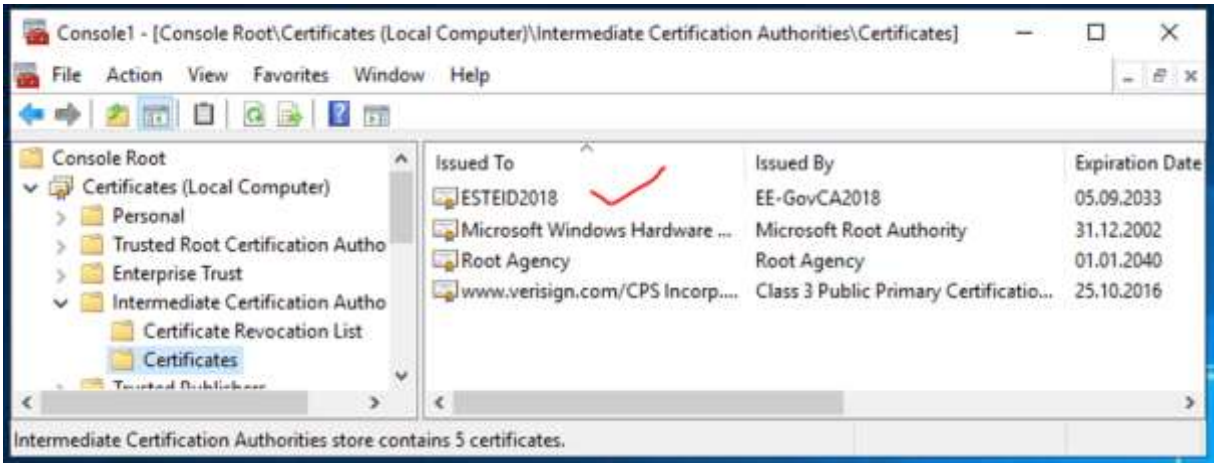
Garanteeritud (tasuline) OCSP teenus

Selleks, et kontrollida sertifikaadi staatust kasutades SK poolt pakutavat garanteeritud OCSP teenust, tuleb SKga esmalt leping sõlmida. Seejärel lubatakse tellijale ligipääs OCSP teenusele (aadressiga

http://ocsp.sk.ee) kas sertifikaadi või IP-aadressi põhiselt. **Seda funktsionaalust saab täna kasutada ainult Idemia kaartide vaates**.

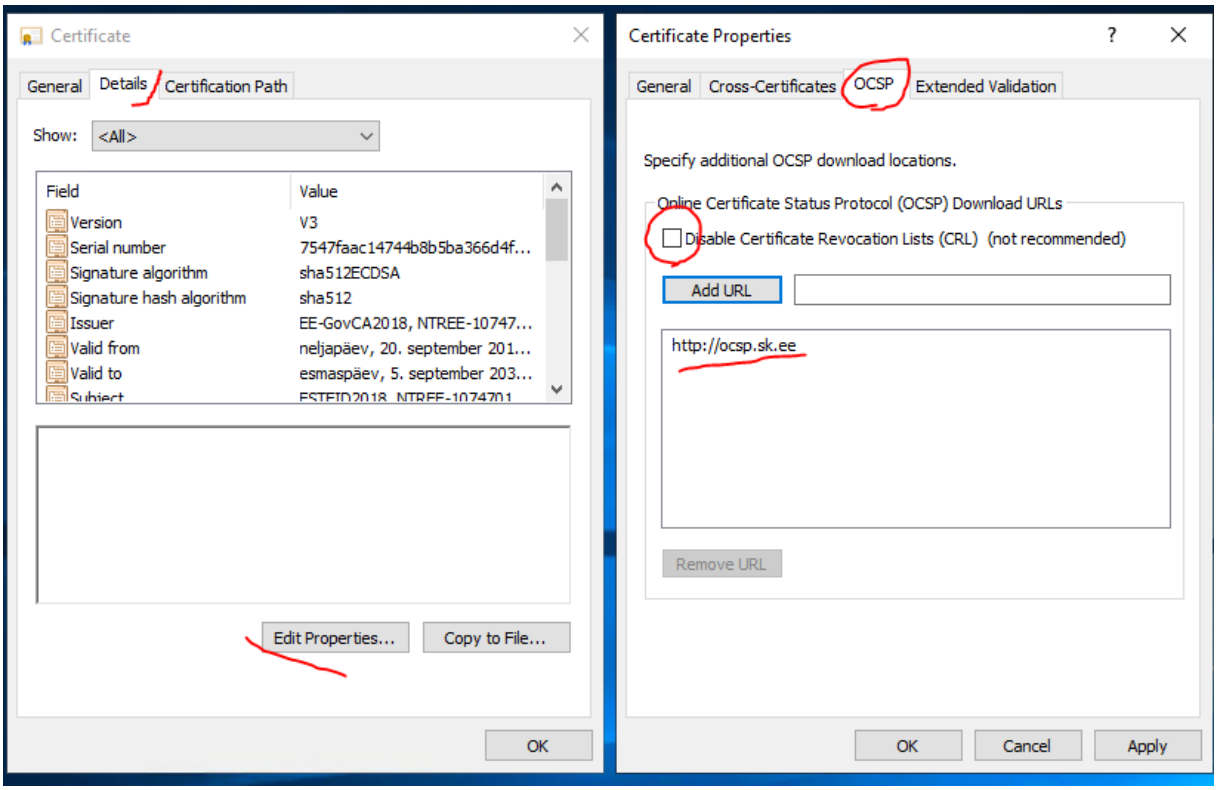
Konfiguratsioon

Garanteeritud OCSP teenuse kasutamiseks veebiserveril tuleb klientide sertifikaatide staatuse kontrolliks modifitseerida serveri operatsioonisüsteemis olevaid kesktaseme sertifikaate. Veebiserveril on Eesti eID kesktaseme CA-de sertifikaadid publitseeritud konteineris „Kesktaseme sertifitseerimiskeskused“.



Pilt 29 - sertifikaatide paigutus IIS serveris

Sertifikaatide OCSP omaduste muutmiseks tuleb avada sertifikaat, valida leht *Details*, klikkida nupul „*Edit Properties…*“ ja valida leht OCSP. OCSP URLde loendisse tuleb lisada OCSP teenuse aadress http://ocsp.sk.ee.

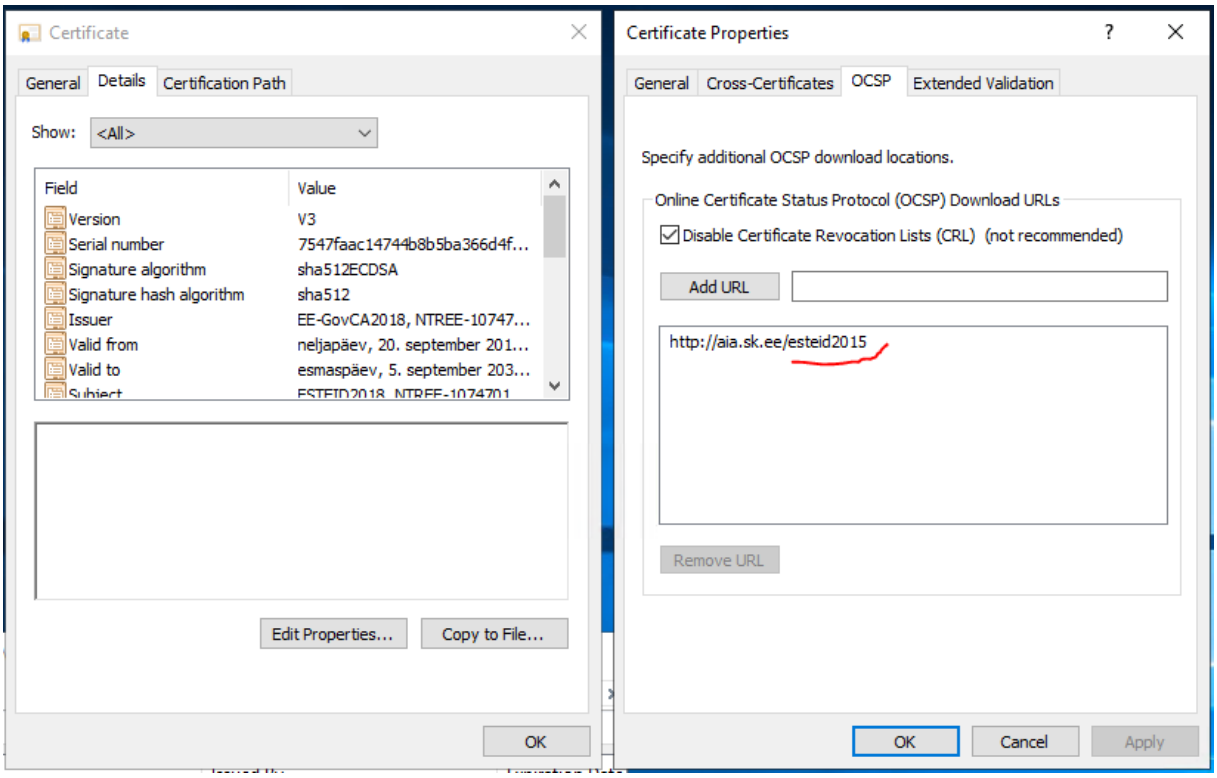


Pilt 30 - OCSP teenuse asukoha määramine kesktaseme sertifikaadi põhiselt

Ülaltoodud pildil suunatakse kasutaja sertifikaatide staatuse kontroll ESTEID2018 CA alt väljastatud sertifikaatide puhul garanteeritud OCSP teenuse aadressile (http://ocsp.sk.ee). Kui on soov CRLi kontrolli ID-kaartidel täielikult keelata (ESTEID2018 CA ahelast väljastatud kaartidel CRLi aadressi enam sertifikaadis kirjeldatud ei ole, nii et käesoleva konfiguratsiooni puhul puudub selleks vajadus), siis saab selle aktiveerida linnukesega „*Disable Certificate Revocation Lists (CRL) (not recommended)*“.

Vaba ligipääsuga (tasuta) AIA OCSP teenus

Lisaks garanteeritud (tasulisele) OCSP teenusele pakuvad usaldusteenuse osutajad ka vaba ligipääsuga (tasuta) AIA OCSP teenust, mille puhul sertifikaatide staatust kontrollitakse pisut lihtsama OCSP teenuse vastu. ESTEID2018 CA alt väljastatud sertifikaatide puhul on AIA OCSP aadress juba sertifikaadis kirjas (http://aia.sk.ee/esteid2018), nii et siin midagi eraldi konfigureerima ei peagi. Küll aga saab soovi korral kehtestada AIA OCSP kontrolli ka keskselt:

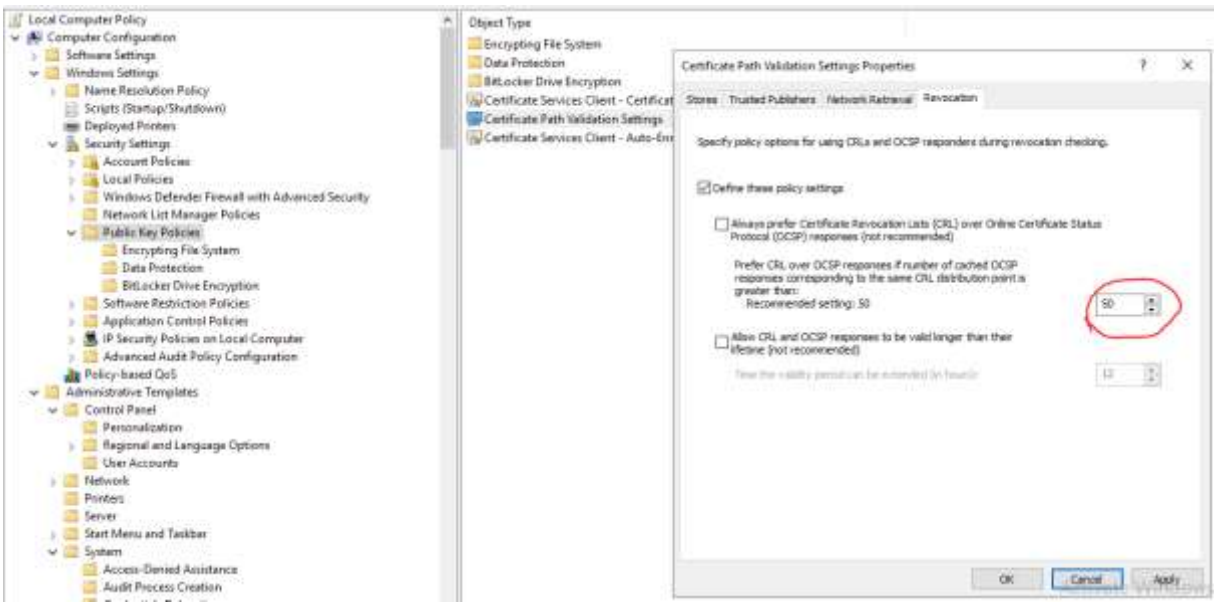


Pilt 31 - AIA OCSP aadressi konfigureerimine

Ka Thalese kaartide sertifikaatides on kirjeldatud AIA OCSP tee, seega mingeid lisategevusi selle kasutamiseks me tegema ei pea. Küll aga on täna neis sertifikaatides ka CRL tee. CRL kasutamisest saame vajaduse loobuda kasutades üleval kirjeldatud keskse AIA OCSP määramist koos CRL keelamisega.

Märkused:

- Kõikidel täna kasutusel olevate ID-kaartide sertifikaatidel on kehtivuskontrollina kasutusel AIA OCSP teenus, CRL aadressi neis kirjeldatud ei ole.
- Windows serveri puhul pöördutakse vaikimisi OCSP põhiselt sertifikaatide kehtivuse kontrollilt tagasi CRL põhisele kontrollile, kui vahemälus olevate OCSP päringute hulk ületab 50 piiri. Käesoleva näidiskonfiguratsiooni puhul ei ole see oluline, kuna CRLi ei kasutata. Muude konfiguratsioonide puhul on seda numbrit 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*.



Pilt 32 - maagilise OCSP numbri muutmine

Soovituslikud IISi turvasätted

SSL/TLS

IISi versioon 10 serveril 2022 kasutab vaikimisi kõiki TLS protokollide versioone, 1.0-1.3[5]. 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 ajutiselt keelatud TLS versioon 1.3 (loe täpsemalt lk 14: Kahepoolse SSLi, sertifikaadiga autentimise nõudmine - Eelhäälestus). Kui sertifikaadiga autentimine ei ole oluline, võiks olla lubatud vaid TLSi versioon 1.3.

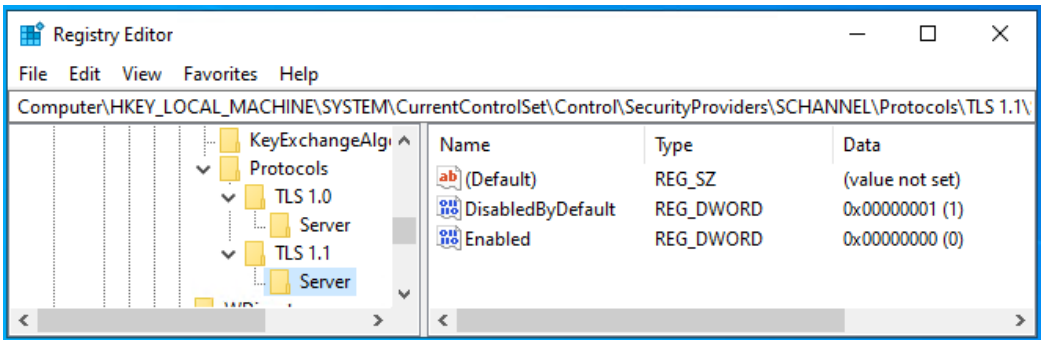
Rohkem infot TLS protokolli kasutamise soovituste kohta leiab RIA tellitud krüptograafiliste algoritmide elutsükli uuringust aadressil https://www.id.ee/artikkel/kruptograafiliste-algoritmide-elutsukli-uuringud-2/.

Vanade TLS protokollide keelamist saab lisaks IIS konfiguratsiooni kaudu keelamisele teha ka otse registris. Kui on soov keelata TLS versioonid 1.0 ja 1.1, tuleb lisada registrisse järgmine konfiguratsioon[6]:

[5] https://docs.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-?redirectedfrom=MSDN.

[6] Vaikimisi neid väärtuseid ei eksisteeri.

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\[7]:
  - TLS 1.0\Server
    - Enabled DWORD:0
    - DisabledByDefault = DWORD:1
  - TLS 1.1\Server
    - Enabled DWORD:0
    - DisabledByDefault = DWORD:1



Pilt 33 - TLS versioonide 1.0 ja 1.1 keelamine registris

Ülaltoodud registri konfiguratsiooni on muidugi võimalik levitada ka kesksete poliitikate abil.

Šifrikomplektid (*Cipher suites*)

Windows serveriga tuleb vaikimisi kaasa mitmeid šifrikomplekte. Kõiki neid saab vaadata näiteks PowerShell käsuga Get-TLSCipherSuite[8].

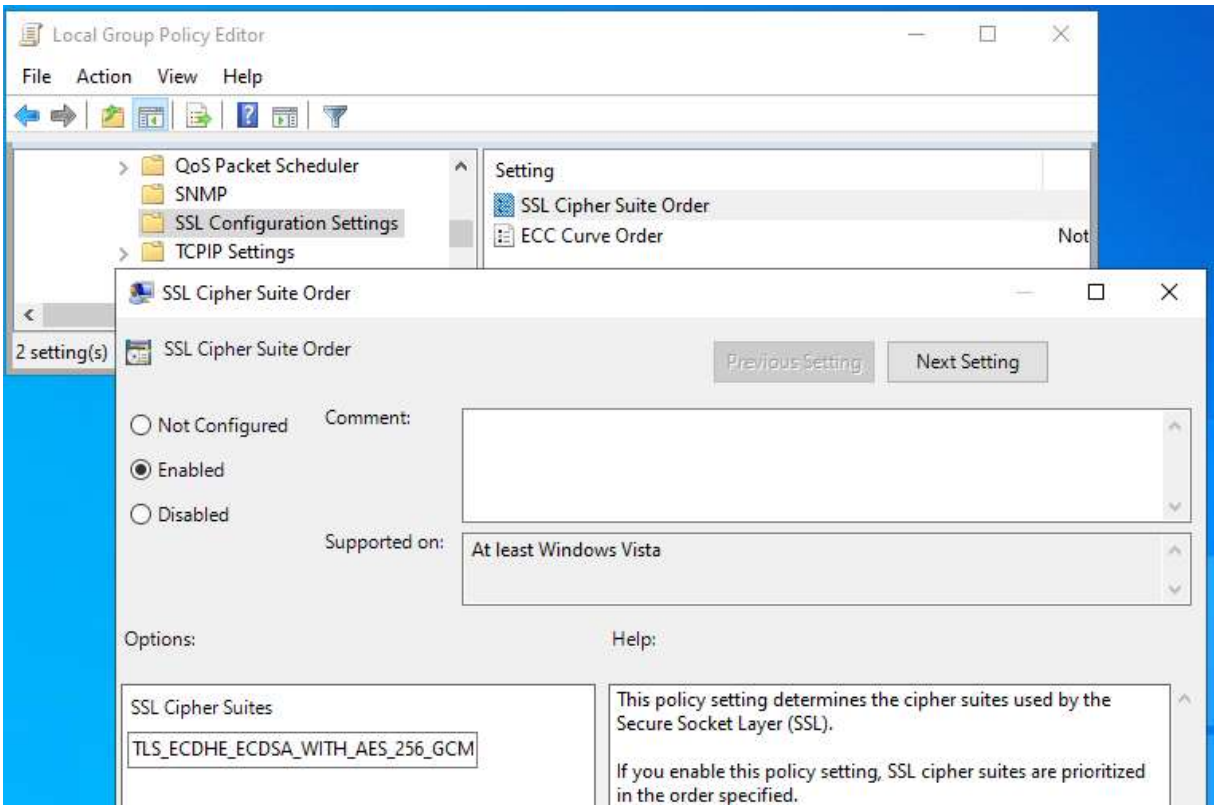
Kindlat soovitust erinevate šifrikomplektide kasutamiseks ei ole võimalik anda ilma veebilehele esitatavaid tingimusi teadmata. Küll aga tuleb kindlasti eemaldada loendist ebaturvalised šifrikomplektid. Enne konfiguratsiooniga jätkamist soovitame kindlasti tutvuda RIA tellitud krüptograafiliste algoritmide elutsükli uuringu soovitustega aadressil https://www.id.ee/artikkel/kruptograafiliste-algoritmide-elutsukli-uuringud-2/. Mõistlik on kirjeldada konkreetsed lubatud šifrikomplektid TLS 1.2 kasutamiseks.

Seega, kui on soov ise kasutatavaid šifrikomplekte määrata, on mõistlik selleks kasutada kohalikke või keskseid poliitikaid. Kasutamaks ainult šifrikomplekte ECDHE-ECDSA-AES256-GCM-SHA384 ja ECDHE-RSA-AES256-GCM-SHA384, tuleb modifitseerida määrangut “Computer Configuration/Administrative Templates/Network/SSL Configuration Settings: SSL Cipher Suite Order”. Šifrikomplektid tuleb eraldada komaga.[9]

[7] Võimalik on konfigureerida ka kasutaja osa SSL/TLS protokollide vaates. Käesolev juhis käsitleb küll ainult serveripoolset häälestust, kuid see ei tähenda, et kasutaja osa konfigureerimine ei ole soovitatav, see sõltub alati konkreetsest situatsioonist.

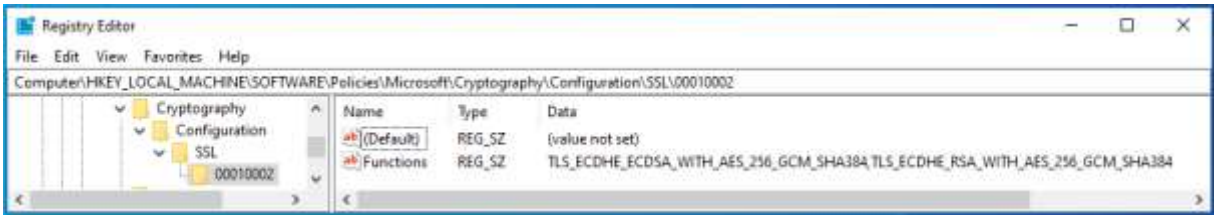
[8] https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel

[9] NB! Nende konkreetsete määrangutega TLS 1.3 ei toimi. Pigem võib nende määrangute kasutamine olla mõttekas juhul, kui ei soovita TLS 1.3 kasutada, näiteks sertifikaadiga autentimise lubamise puhul.



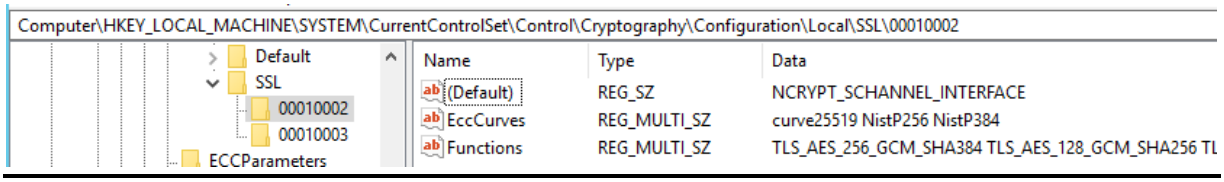
Pilt 34 – kindlate šifrikomplektide määramine keskse poliitikaga

Eelmises punktis määratud konfiguratsioon kirjutatakse registrisse:



Pilt 35 - poliitikaga määratud konfiguratsioon

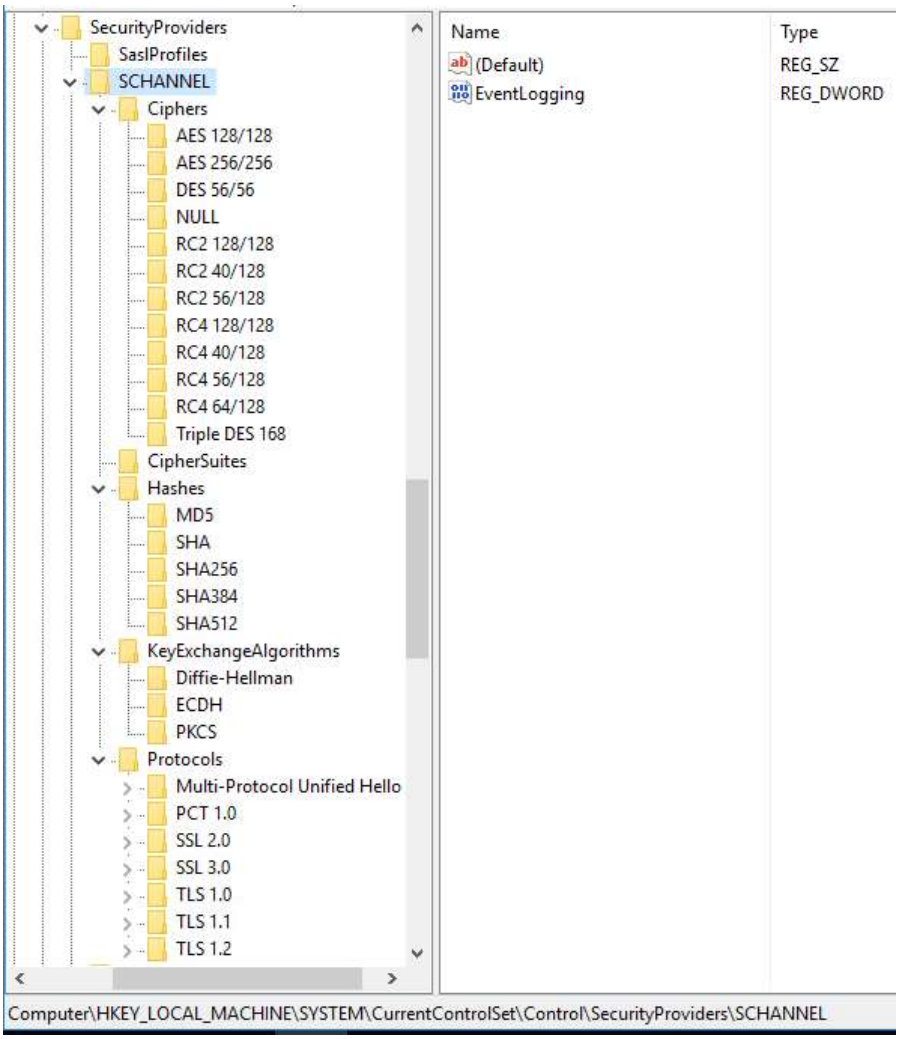
Vaikimisi on šifrikomplektid kirjeldatud järgmisel pildil kirjeldatud asukohas:



Pilt 36 - vaikimisi šifrikomplektide konfiguratsioon

Muud konfigureeritavad Schannel omadused

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



Pilt 37 - Schannel konfigureeritavad omadused

Muud võimalused

Lisaks TLS ja šifrikomplektide häälestusele on soovitav pöörata tähelepanu IISi serveri turvalisusele ka järgmiste punktide vaates:

- Hoida operatsioonisüsteemi ajakohasena.
- Keelata serveri info presenteerimine.
- Keelata HTTP päringud.
- Keelata failide lappamise võimaluse (*directory listing*).
- Kasutada mitte-süsteemseid ja mitte-administraator kontosid.
- Lubada HSTSi.
- …

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