IIS VEEBISERVERILE ID-KAARDI TOE SEADISTAMINE

Dokumendi info	
Loomise aeg	21.01.2019
Tellija	RIA
Autor	Urmas Vanem, OctoX
Versioon	19.12/1

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 soovitused IIS'i turvamiseks. Muutja: Urmas Vanem

Juhend, kuidas autentida kasutajat IIS veebiserveril.

Sissejuhatus

Käesolevas juhendis kirjeldame IIS veebiserveri konfiguratsiooni kahepoolse SSL-i kasutamiseks, kusjuures kliendi poolseks sertifikaadiks on mõni kiipkaardile paigaldatud Eesti PPA poolt väljastatud sertifikaat (ID-kaart, elamisloakaart, digi-ID ja e-residendi digi-ID).

Juhendi loomisel on kasutatud Windows Server 2019 ja Windows 10 operatsioonisüsteeme. Näidisjuhendis on toetatud Sertifitseerimiskeskuse „EE Certification Centre Root CA" ja EE-GovCA2018 ahelatest pärinevad sertifikaadid. Tagamaks sertifikaatide äratundmist on kohustuslikuks komponendiks nii serveri kui kliendi poolel ka ID kaardi tarkvara[1]. Serveri sertifikaat on väljastatud OctoX testkeskkonnast.

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

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

1) Microsoft Edge
2) Microsoft Internet Explorer
3) Mozilla Firefox
4) Google Chrome

Microsofti IIS ja Google Chrome kombinatsioon töötab uue ID kaardiga (EE-GovCA2018 ahel, IDEMIA) juhul, kui Windows serverile on installeeritud järgmine uuendus:

- **Versioon 2016 (LTSC) töötab uuendusega KB4516061!**
- **Versioon 2019 (LTSC) töötab uuendusega KB4520062!**
- **Versioon 1903 (SAC) töötab uuendusega KB4524570![2]**

Versioonidele 2012 ja 2012R2 parandust ei tehta, kuna need ei kuulu peavoolu serverite versioonide hulka.

IIS serveri nõutav konfiguratsioon

IIS server peab olema häälestatud nõudmaks kasutajalt sertifikaati. IIS server lubab vaikimisi enda poole pöördumisel kasutada kõiki sertifikaate, milliste EKU-s on kirjeldatud *client authentication*. IIS server peab suutma luua kogu sertifikaadiahela alates kasutajasertifikaadist kuni juursertifikaadini – see tähendab, et lisaks juurtaseme sertifikaatide olemasolule IIS serveris on vajalik ka kesktaseme

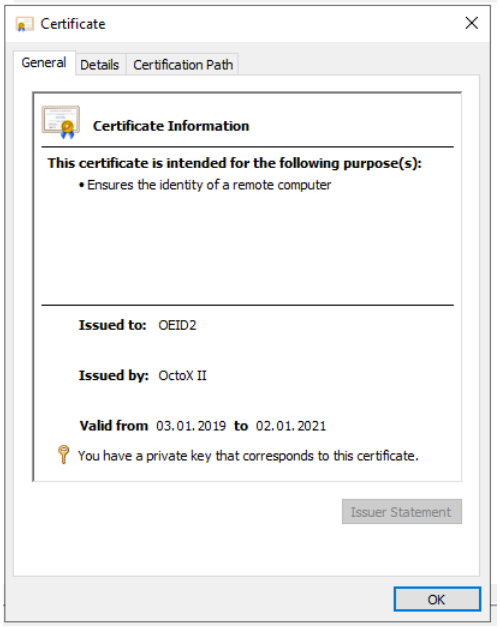
[1] https://installer.id.ee/?lang=est

[2] Serveri 1909 (SAC) versioonile on kättesaadav sama uuendus juhuks, kui probleem IIS/Chrome autentimisega seal vaikimisi pole parandatud!

(*intermediate*) sertifikaatide olemasolu. Meie konfiguratsiooni puhul tuleb IIS serveris sertifikaadid publitseerida järgmiselt:

1) Usaldusväärsete sertifikaatide konteinerisse:
   a. „EE Certification Centre Root CA“ (https://sk.ee/upload/files/EE_Certification_Centre_Root_CA.der.crt)
   b. EE-GovCA2018 (http://c.sk.ee/EE-GovCA2018.der.crt)
2) Kesktaseme sertifikaatide konteinerisse[3]:
   a. „ESTEID-SK 2011“ (https://sk.ee/upload/files/ESTEID-SK_2011.der.crt)
   b. „ESTEID-SK 2015“ (https://sk.ee/upload/files/ESTEID-SK_2015.der.crt)
   c. ESTEID2018 (http://c.sk.ee/esteid2018.der.crt)

Lisaks peab ka IIS serveril endal olema määratud SSL sertifikaat - meie näites on kasutusel OctoX testkeskkonnast väljastatud sertifikaat nõutava omadusega *Server Authentication*. Samuti peavad nii kliendid kui ka veebiserver usaldama nimetatud sertifikaati:

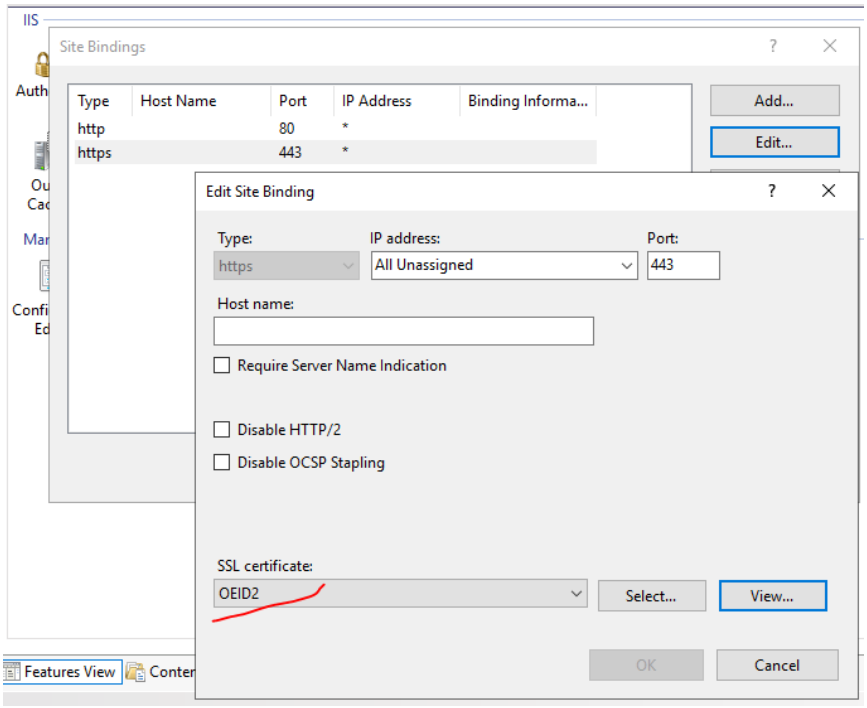


Pilt 1 - IISi sertifikaat

Sertifikaadi nimi (issued to) ei viita serveri „päris“ aadressile/nimele. Serveri aadress on kirjeldatud SAN atribuudi all DNS nimena ja selleks on id.octox.eu. Server usaldab ka sertifikaati „OctoX II“, mis on serveri sertifikaadi väljastajaks.

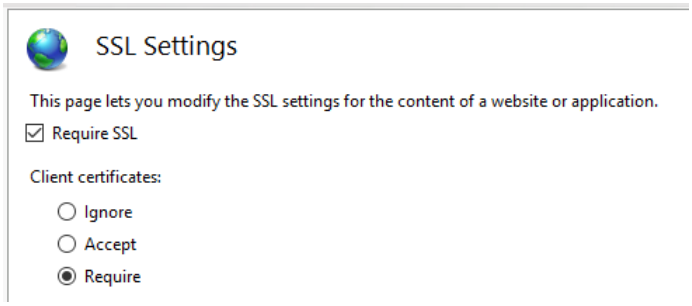
[3] SK poolt väljastatud organisatsioonide kaartide kasutuse puhul peavad kesktaseme sertifikaatide hulka olema häälestatud ka EID-SK 2011 (https://sk.ee/upload/files/EID-SK_2011.der.crt) EID-SK 2016 (https://www.sk.ee/upload/files/EID-SK_2016.der.crt) sertifikaadid!

Soovitud veebisaidil peab olema lubatud SSL port (vaikimisi 443) ja see peab olema seotud soovitava sertifikaadiga:



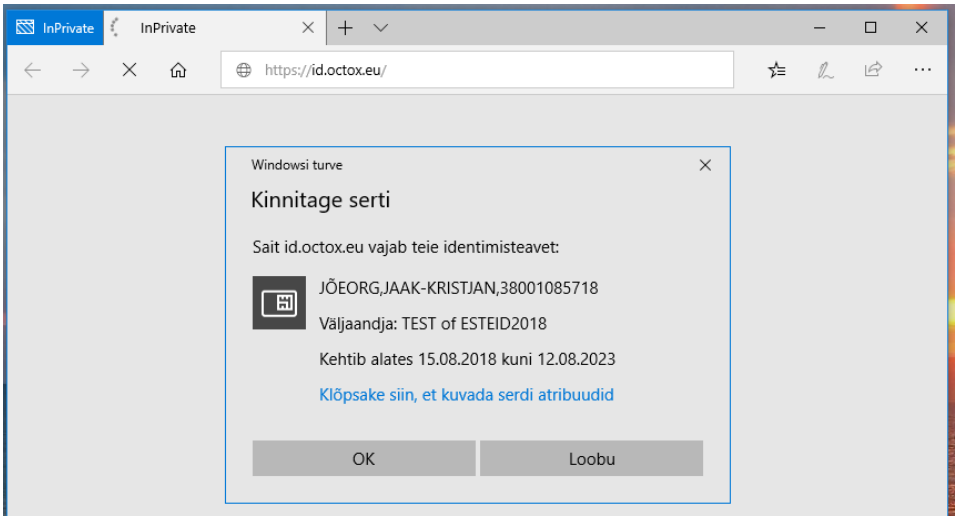
Pilt 2 - veebisaidil on lubatud 443 port ja kasutatavaks sertifikaadiks on OEID2 (id.octox.eu)

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



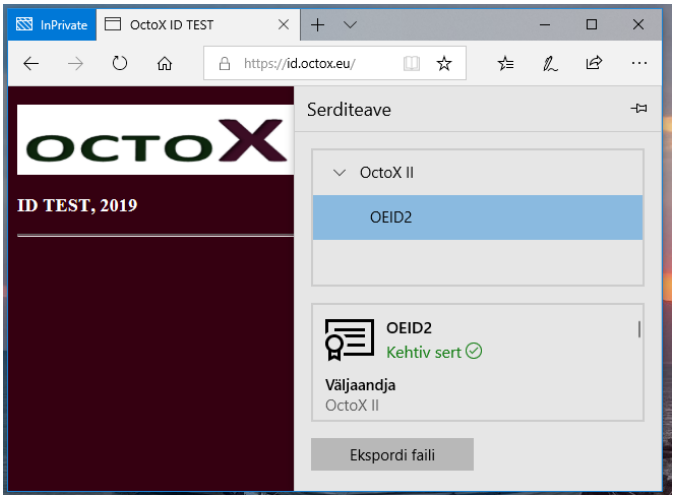
Pilt 3 - SSL ja sertifikaadi nõue

Loodud konfiguratsioon nõuab veebisaidile ligipääsu 443 pordi kaudu ja kasutaja sertifikaati. Pöördudes veebisaidi poole lubatakse valida soovitav serveri poolt aktsepteeritav sertifikaat:



Pilt 4 - sertifikaadi küsimine veebisaidile pöördudes, Edge

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

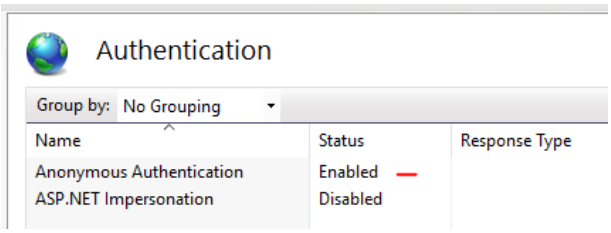


Pilt 5 - autentimine õnnestus

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.

Autentimine

Meie näites on lubatud ainult anonüümne autentimine:



Pilt 6 - anonüümne autentimine, kasutaja saab saidile ligi kasutaja IUSR õigustes

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 võimalik ette anda loend autentimiskeskustest, millised on toetatud ja seeläbi kuvatakse edaspidi klientidele serveri poolt vaid toetatud sertifikaadid.

Kuidas filtreerida kliendi poolt pakutavaid sertifikaate

Seame eesmärgiks kuvada kasutaja pool vaid sertifikaadid mis pärinevad juurserverite EE-GOV-CA2018 ja “EE Certification Centre Root CA” ahelatest..

1) Häälestame IIS-ile veebiserdi kasutamaks SSL-i ja dokumenteerime selle omadused käsuga “netsh http show sslcert 0.0.0.0:443”:

```
C:\Windows\system32>netsh http show sslcert 0.0.0.0:443

SSL Certificate bindings:
-------------------------

    IP:port                      : 0.0.0.0:443
    Certificate Hash             : 1e75c77c696aa4d49686bb1ef73ac3b07fdff38a
    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 7 - vaikimisi seotud sertifikaadi omadused

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

```
C:\Windows\system32>netsh http del sslcert 0.0.0.0:443

SSL Certificate successfully deleted
```

Pilt 8 - sertifikaadi eemaldamine

3) Lisame sertifikaadi uuest 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“:

```
C:\Windows\system32>netsh http add sslcert ipport=0.0.0.0:443 certhash=1e75c77c696aa4d49686bb1ef73ac3b07fdff38a appid={4
dc3e181-e14b-4a21-b022-59fc669b0914} sslctlstorename=ClientAuthIssuer

SSL Certificate successfully added
```

Pilt 9 - lisame sertifikaadi uute omadustega

Certhash ja appid väärtused saame esialgsest sertifikaadi väljavõttest, vt. „Pilt 7 - vaikimisi seotud sertifikaadi omadused“.

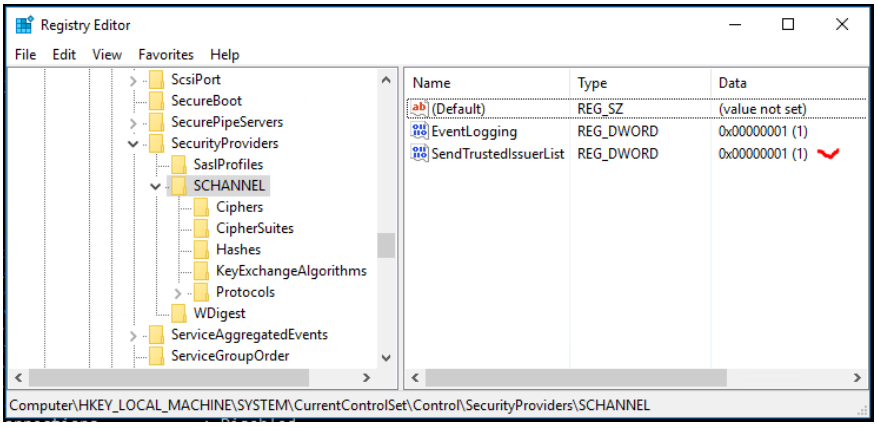
4) Kontrollime, et “CTL Store Name” on uuel sertifikaadi väljavõttel ClientAuthIssuer:

```
C:\Windows\system32>netsh http show sslcert 0.0.0.0:443

SSL Certificate bindings:
-------------------------

    IP:port                      : 0.0.0.0:443
    Certificate Hash             : 1e75c77c696aa4d49686bb1ef73ac3b07fdff38a
    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 10 - uuesti seotud sertifikaadi omadused

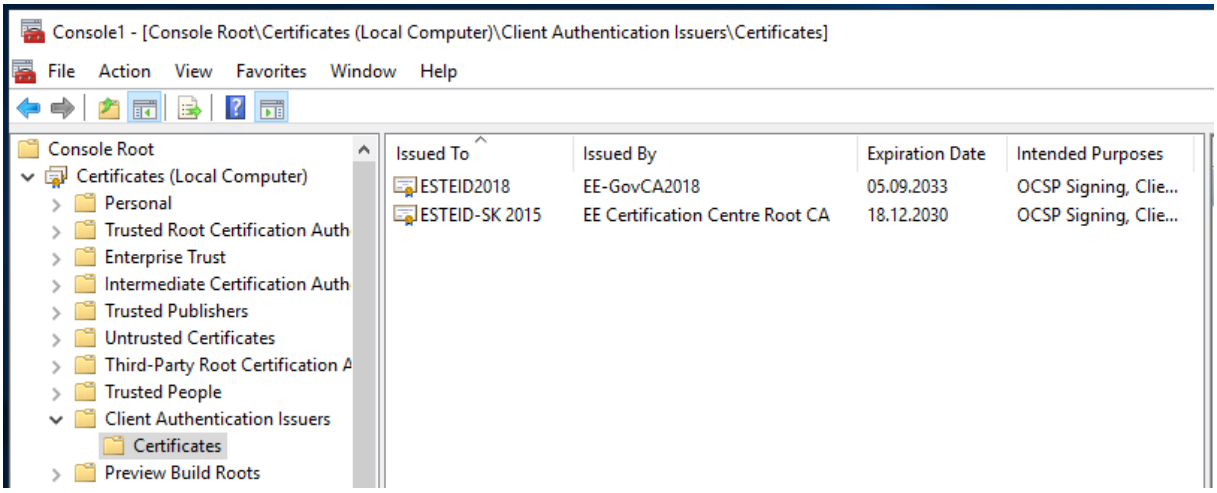
Näeme soovi korral ka IIS-i konfiguratsioonist, et SSL sertifikaat on uuesti korrektselt seotud 443 pordiga.

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



Pilt 11 - sertifikaatide filtreerimise lubamine registris

6) Lisame SK kesktaseme sertifikaadid arvuti sertifikaatide konteinerisse *„Client Authentication Issuers“*:



Pilt 12 - kliendi jaoks lubatud sertifikaatide lisamine õigesse konteinerisse

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

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.

Kliendisertifikaatide kehtivuse kontroll OCSP teenuse vastu

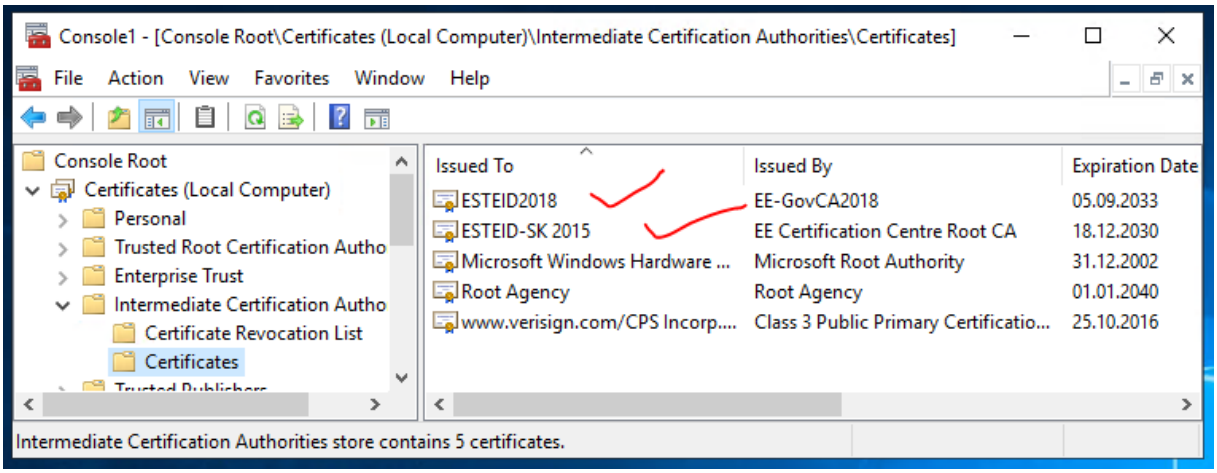
OCSP teenuse abil saame kasutaja sertifikaadi kehtivust kontrollida praktiliselt reaalajas. Iga kasutaja autentimisel saadab veebiserver päringu OCSP teenusele, mis tagastab sertifikaadi kehtivuse info.

Garanteeritud SK OCSP teenus

Garanteeritud SK OCSP teenus töötab aadressil http://ocsp.sk.ee ja on ühine kõikidele Eesti EID ahelatest väljastatud sertifikaatidele. **Selle teenuse kasutamiseks peab kliendil olema sõlmitud leping SK-ga – seejärel lubatakse teenusele ligipääs kas sertifikaadi alusel või IP aadressi põhiselt!**[4]

Konfiguratsioon

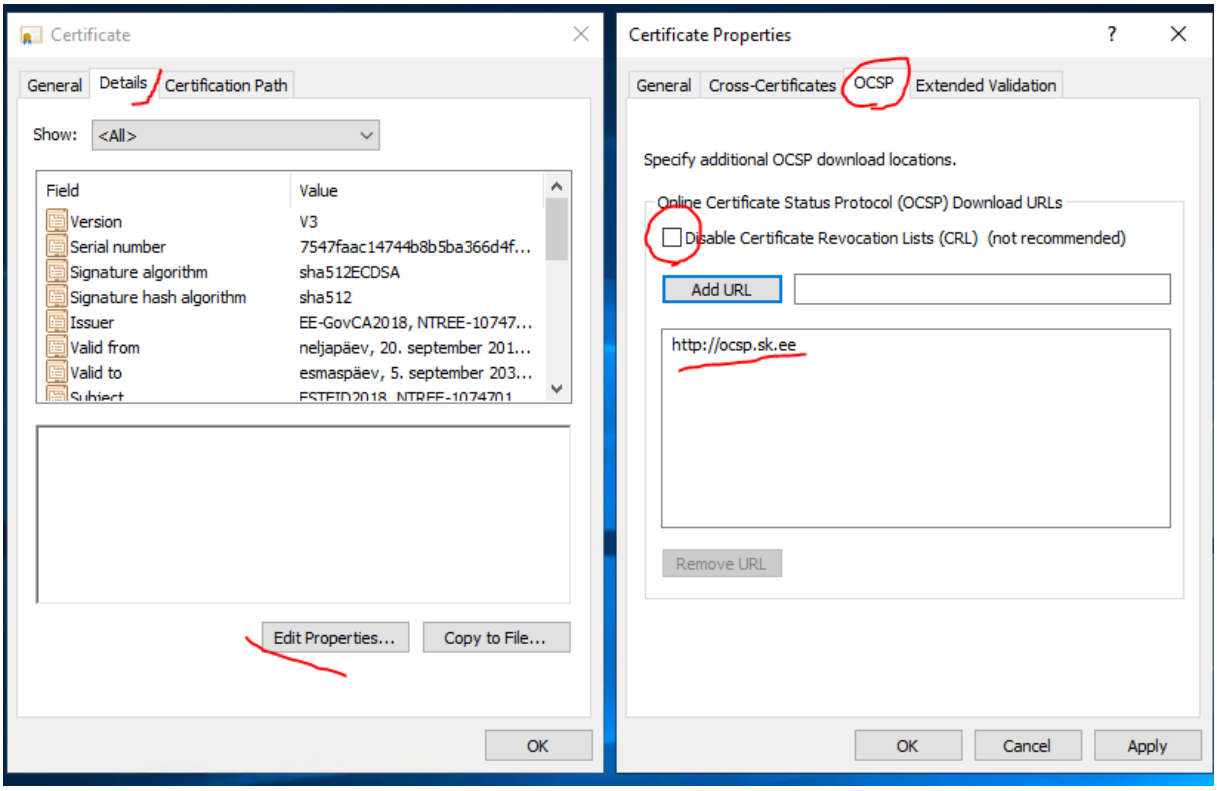
Tasulise OCSP häälestuseks veebiserveril klientide sertifikaatide kontrolliks tuleb meil modifitseerida serveri operatsioonisüstemis olevate kesktaseme sertifikaate. Veebiserveril on Eesti EID kesktaseme CA-de sertifikaadid publitseeritud konteineris „Kesktaseme sertimiskeskused“.



Pilt 13 - sertifikaatide paigutus IIS serveris

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

[4] https://www.sk.ee/upload/files/Teenuse_kasutamise_uldtingimused_4_0.pdf

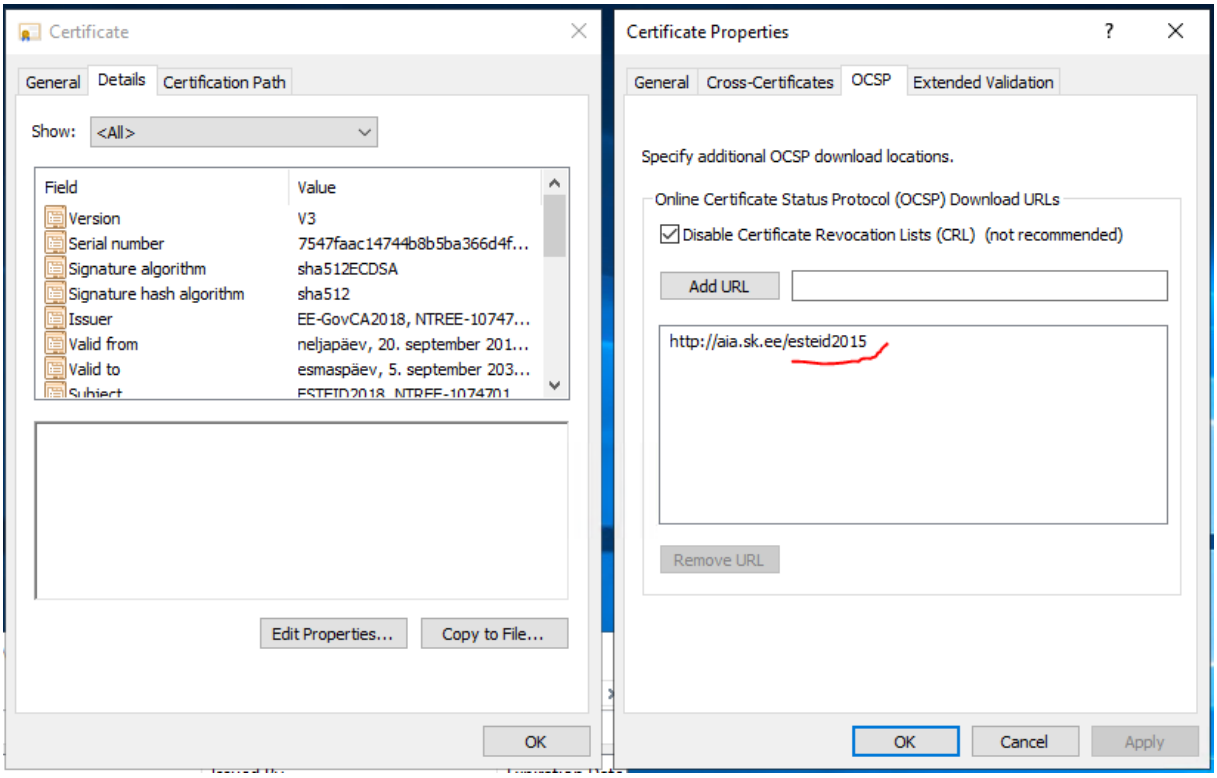


Pilt 14 - OCSP teenuse asukoha määramine kesktaseme sertifikaadi põhiselt

Ülaltoodud pildil suuname kliendisertifikaatide kehtivuse kontrolli ESTEID2018 CA alt väljastatud lepingu sõlmimist sertifikaatide puhul OCSP garanteeritud teenusele http://ocsp.sk.ee. „ESTEID-SK 2015“ CA alt väljastatud sertifikaatidele sama konfiguratsiooni rakendamiseks tuleb ka selle sertifikaadi (ESTEID-SK 2015) omadustega teha samasugune toiming! Kui me soovime CRL-i kontrolli vanematel kaartidel üldse välja lülitada (uutel, ESTEID2018 CA alt väljastatud kaartidel CRL-i teed enam sertifikaadis kirjeldatud ei ole), siis saame aktiveerida ka linnukese „Disable Certificate Revocation Lists (CRL) (not recommended)“.

AIA-SK OCSP teenus

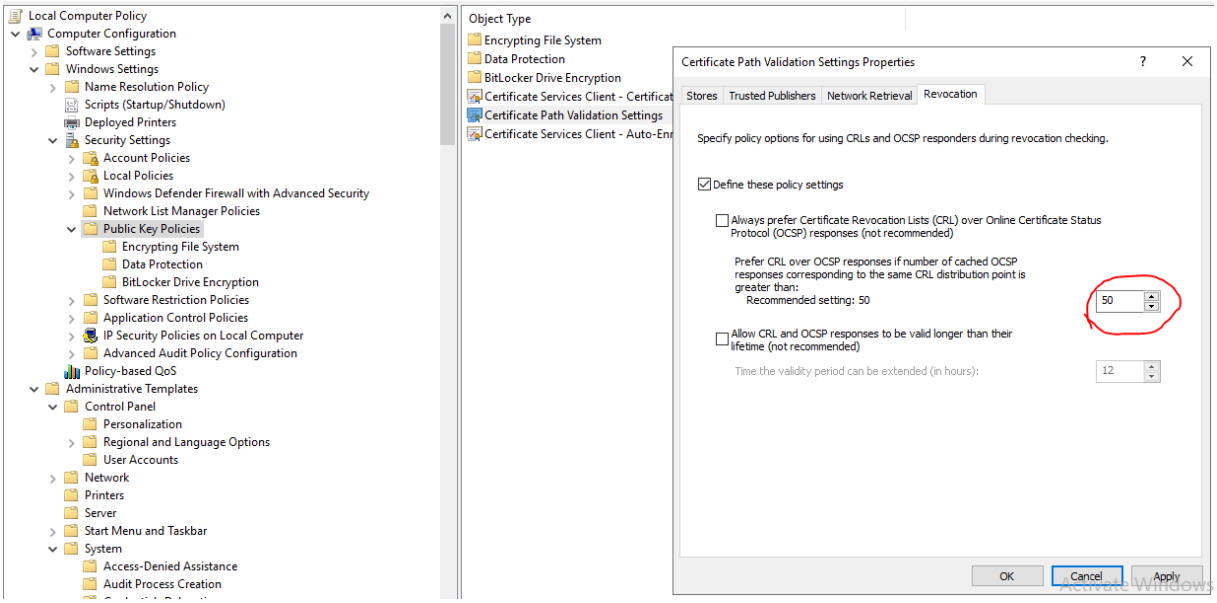
Lisaks garanteeritud OCSP teenusele pakub SK ka nö. vaba, AIA-OCSP teenust, mille käideldavusele ei ole kehtestatud nii kõrgeid nõudeid ja mis pakub ka vähem funktsionaalsust ning ka käitub pisut erinevalt – nimelt antakse ka aegunud sertifikaatidele staatuseks GOOD. ESTEID2018 CA alt väljastatud sertifikaatide puhul on vaba AIA-OCSP aadress juba sertifikaadis kirjas (http://aia.sk.ee/esteid2018), nii et siin me midagi eraldi konfigureerima ei pea. Küll aga saame „ESTEID-SK 2015“ CA alt väljastatud sertifikaatidele kehtestada samuti OCSP kontrolli, määrates kesktaseme sertifikaadis AIA-OCSP serveri aadressiks http://aia.sk.ee/esteid2015:



Pilt 15 - "ESTEID-SK 2015" kasktaseme sertifikaadi konfigureerimine

Märkuseid

- ESTEID2018 CA alt väljastatud sertifikaatidel on kehtivuskontrollina kasutusel OCSP teenus aadressiga http://aia.sk.ee/esteid2018. CRL-i neis kirjeldatud ei ole.
- „ESTEID-SK 2015“ CA alt väljastatud sertifikaatidel on kehtivuskontrolliks kirjeldatud CRL URL http://www.sk.ee/crls/esteid/esteid2015.crl. OCSP-d 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-ne piiri. 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*:



Pilt 16 - maagilise OCSP numbri muutmine

Soovituslikud IIS'i turvasätted

SSL/TLS

IIS'i versioon 10 kasutab vaikimisi TLS protokolli versioone 1.0, 1,1 and 1.2[5]. Vanemad SSL versioonid ei ole kasutusel.

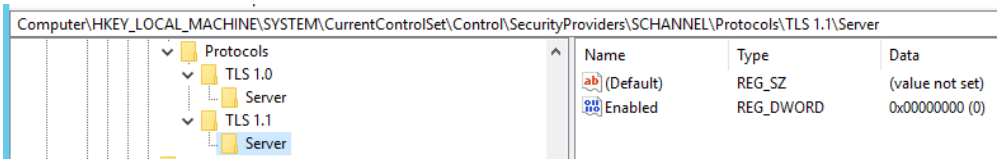
Tänasel päeval aga ei ole enam soovitatav ega tõenäoliselt ka reaalselt vaja kasutada ka TLS versioone 1.0 ja 1.1. Kindlasti peab olema lubatud stabiilne TLS versioon 1.2. Võimalusel võiks lubada ka TLS versiooni 1.3, aga paraku Microsoft seda täna (12.12.2019) veel ei toeta.

Kui me soovime keelata TLS versioonid 1.0 ja 1.1, tuleb meil 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\[78]:
  - TLS 1.0\Server
    - Enabled 0
  - TLS 1.1\Server
    - Enabled 0



Pilt 17 - TLS versioonide 1.0 ja 1.1 keelamine registris

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

Šifrid (Ciphers)

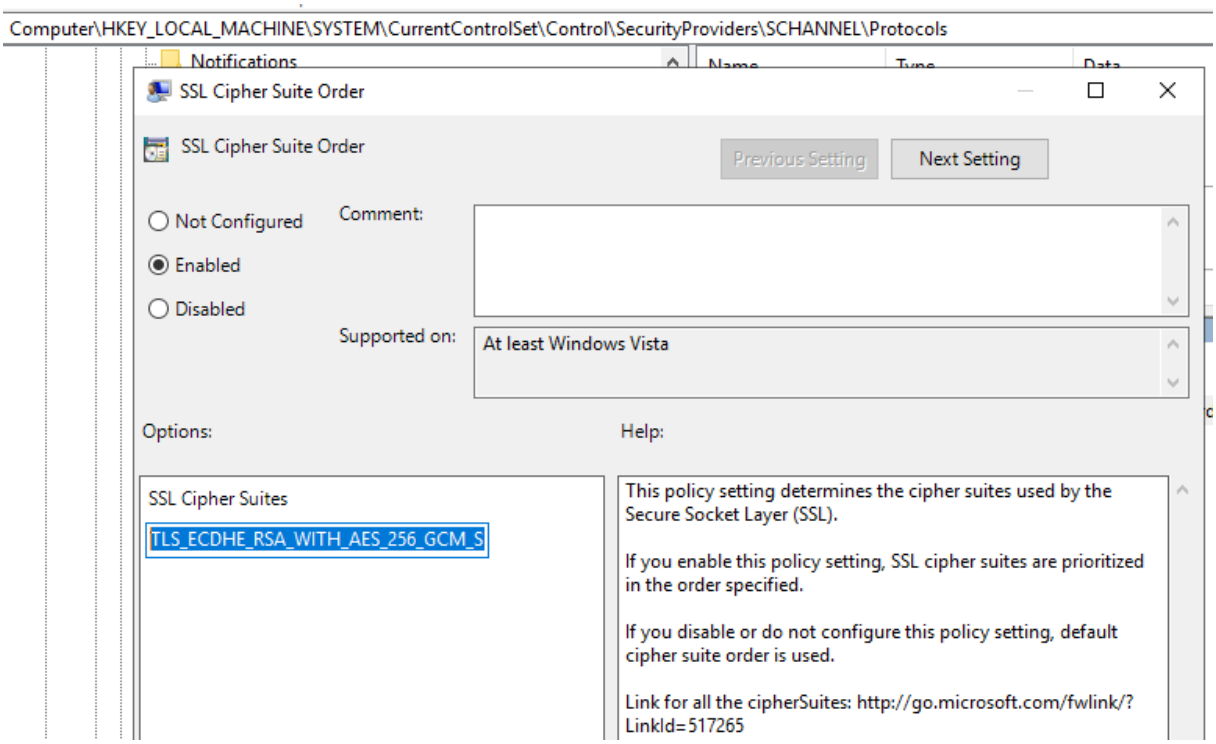
Windows serveriga tuleb vaikimisi kaasa mitmeid erinevaid TLS 1.2 šifrite komplekte.[9] Kõiki neid saame vaadata näiteks PowerShell käsuga Get-TLSCipherSuite[10].

Tavapäraselt võib selline konfiguratsioon olla täiesti piisav, kuna see ei sisalda täna ebaturvalisi šifrite komplekte. Küll aga on seal šifrite komplekte märgisega *WEAK*, millistest me täna aga ilmselt veel lõplikult loobuda ei saa toetamaks kõiksugu vanu kliente.

Kindlat soovitust erinevate šifrite kasutamiseks ei ole veebisaidile esitatavaid tingimusi teadmata võimalik anda. Küll aga tundub mõistlik eemaldada loendist ebaturvalised šifrite komplektid (juhul, kui neid seal on).

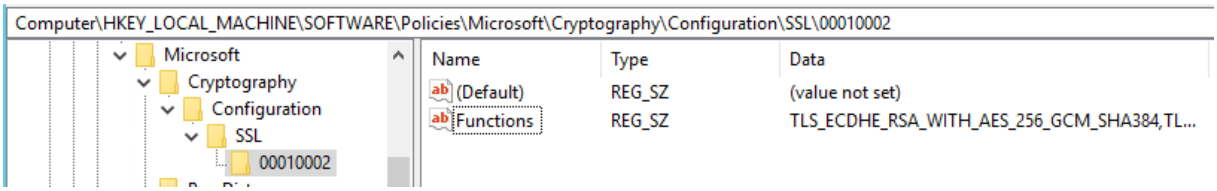
Kuid kui soovime ise täpsemalt määrata kasutatavaid šifrite komplekte, on ilmselt parim selleks kasutada keskseid poliitikaid. Kasutamaks ainult šifrite komplekte TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ja TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, tuleb meil modifitseerida määrangut “Computer Configuration/Administrative Templates/Network/SSL Configuration Settings: SSL Cipher Suite Order”. Šifrite komplektid tuleb eraldada komaga.

[7] Oleme teadlikud, et eksisteerib ka parameeter *disabledbydefault*. Tundub aga, et selle konfigureerimine lisaks ei anna protokollide keelamisele midagi juurde.
[8] Võimalik on konfigureerida eraldi ka kliendi osa SSL/TLS protokollide vaates. Hetkel aga räägime ainult serveri poole häälestusest. See ei tähenda, et kliendi osa konfigureerimine ei ole soovitatav, see sõltub alati konkreetsest situatsioonist.
[9] Selles dokumendis käsitleme me ainult TLS 1.2 šifreid, kuna eeldatavasti on vanemad protokollid keelatud ja TLS 1.3 ei ole veel toetatud.
[10] https://docs.microsoft.com/en-us/windows/win32/secauthn/cipher-suites-in-schannel



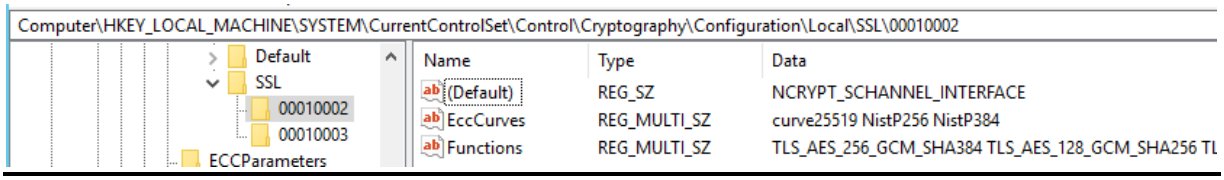
Pilt 18 – kindlate šifrite komplektida määramine keskse poliitikaga

Eelmises punktis määratud konfiguratsioon kirjutatakse registrisse:



Pilt 19 - poliitikaga määratud konfiguratsioon

Vaikimisi on šifrite komplektid kirjeldatud järgmisel pildil kirjeldatud asukohas:



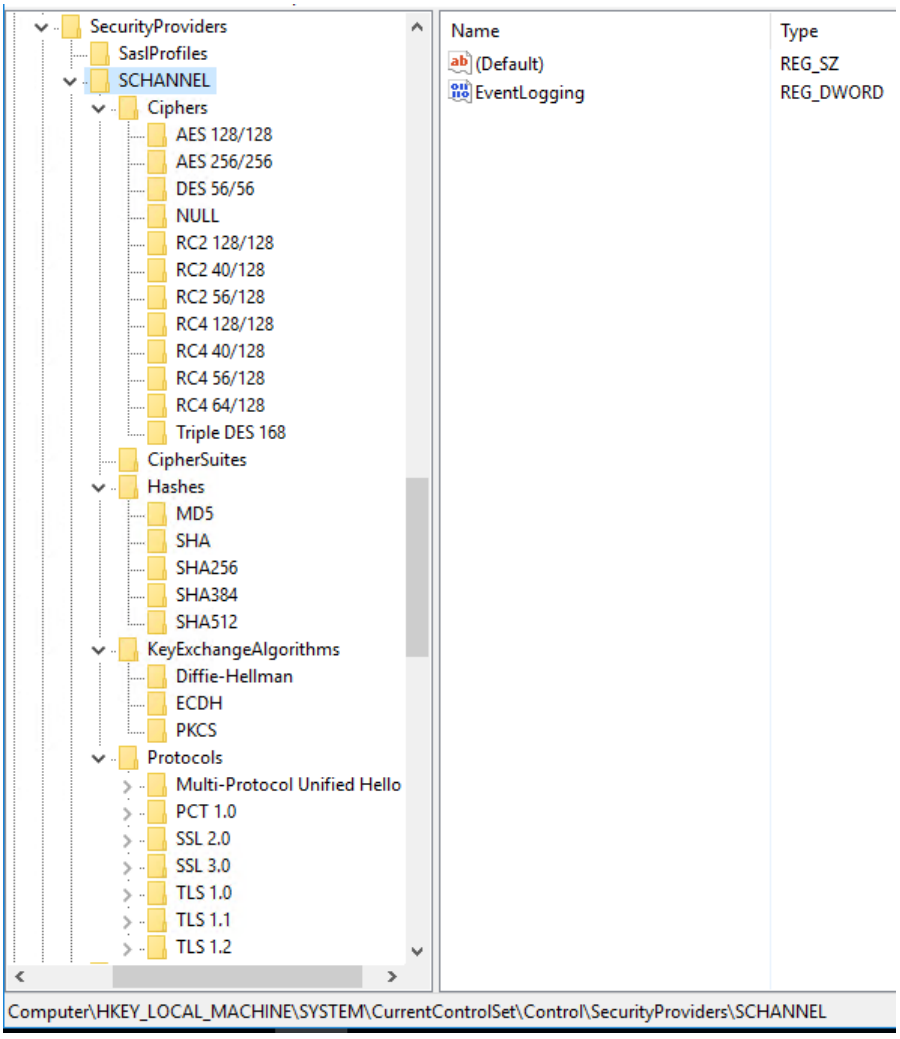
Pilt 20 - vaikimisi šifrite komplektide konfiguratsioon

Palun mitte võtta ülaltoodud näidiskonfiguratsioone aluseks ja konfigureerida šifritega seotud osa vaid juhul, kui sellest tegevusest on selge arusaam ning tegevusel on kindel eesmärk. Eesmärkideks võib

olla näiteks kas ebaturvaliste šifrite eemaldamine või saidi optimeerimine asetades ettepoole kiiremad turvalised šifrid või midagi kolmandat-neljandat.

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, kirjutada üle vaikimisi konfiguratsiooni.



Pilt 21 - Schannel konfigureeritavad omadused

Muud võimalused

Lisaks TLS-i ja šifrite komplektide konfigureerimisele, saame palu 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.
- …

Palun suhtuda ülaltoodusse kui näidisloendisse demonstreerimaks, mida veel saab IIS'i turvalisemaks muutmise jaoks ära teha. Põhjalikemaid soovitusi on leida paljudel internetilehtedel: https://www.google.com/search?q=how+to+secure+IIS+server.