SK veebisertide häälestus, IIS 7

Tehniline kirjeldus

Urmas Vanem

2011

SERTIFITSEERIMISKESKUS

SISUKORD

SISSEJUHATAVALT

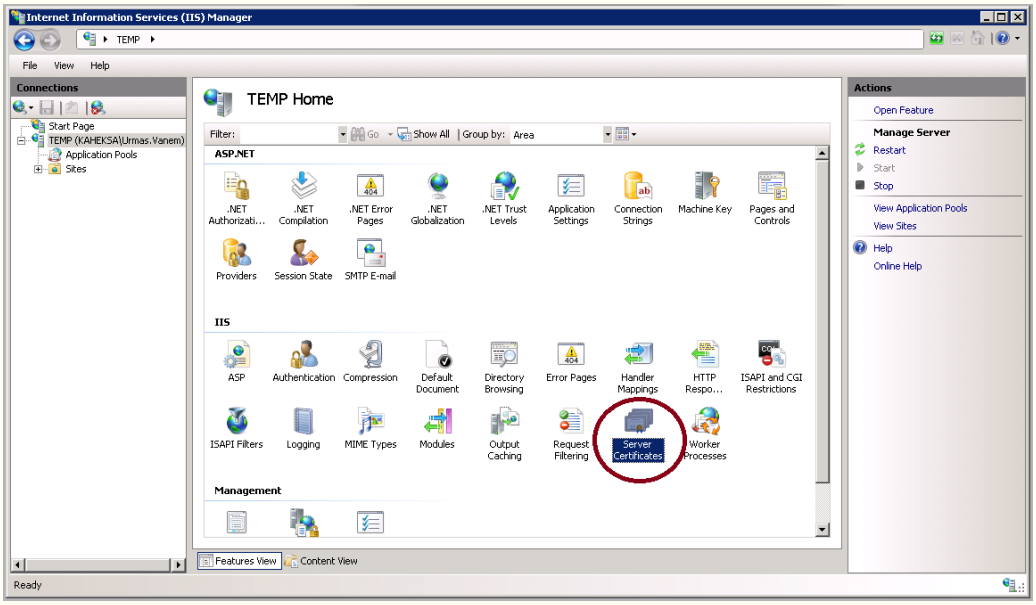
Käesolev dokument kirjeldab Sertifitseerimiskeskuse veebisertide häälestamist Windows 2008 serveril. Põhimõtteliselt on vaja teha sertifikaadi päring SK-sse ja tagasisaadud sertifikaat siduda soovitava veebisaidiga. Veebiserveri platvormiks on IIS 7. Vaatleme, kuidas soovitavaid tegevusi saab sooritada üle graafilise kasutajakeskkonna.

Käsitleme siin veebiserveri sertifikaate, mis on välja antud KLASS3-SK 2010 tasemelt.

SERTIFIKAADI PÄRINGU LOOMINE

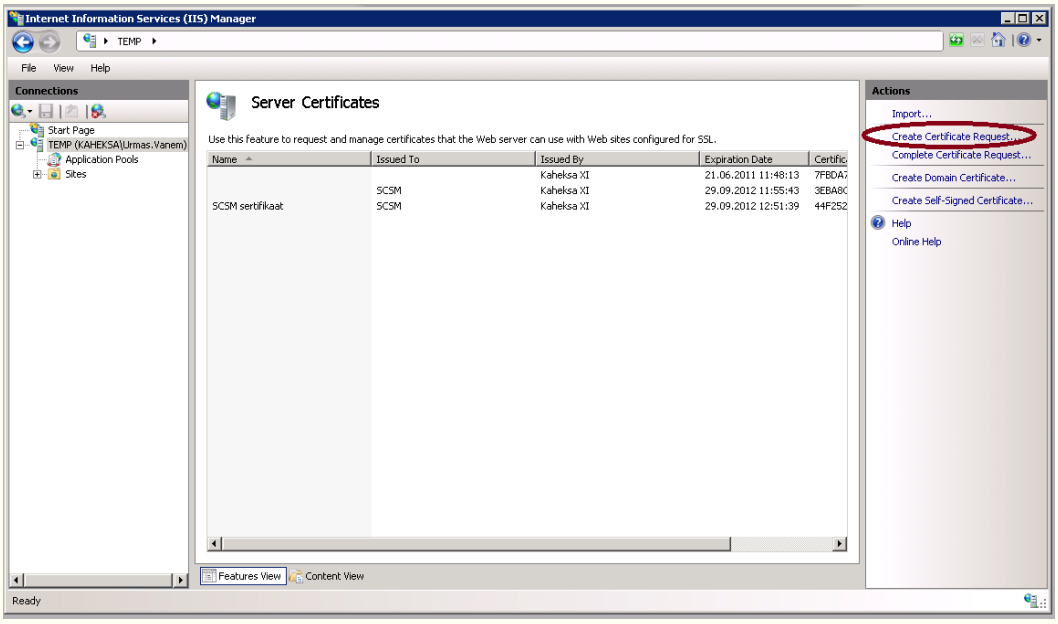
Sertifikaadi päringuks tuleb esimese sammuna IIS serveri abil genereerida päringufail (*Certificate Service Request* elik *CSR*), mis tuleb edastada sertifitseerimiskeskusesse.

Sertifikaadi päringufaili loomiseks avame *IIS Manager'i* ja valime soovitava veebiserveri. Detailide aknas topeltklikime nupul *„Server Certificates".*



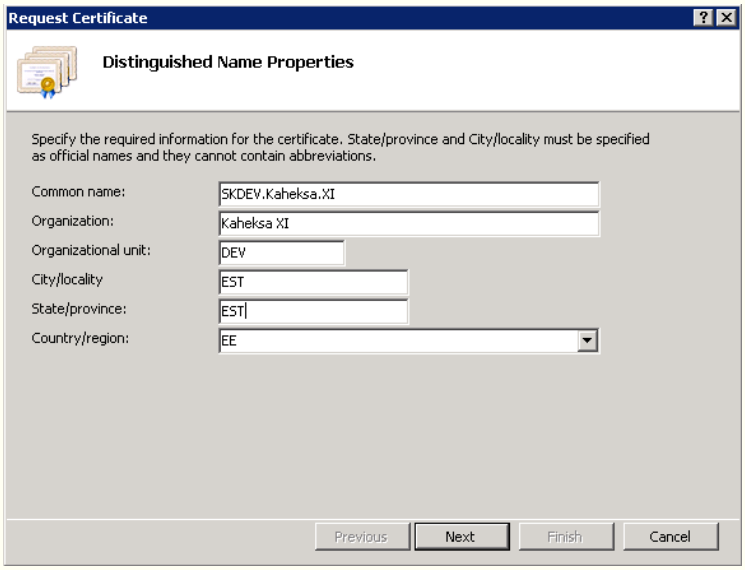
Joonis 1 - valime serveri sertifikaatide nupu ja topeltklikime sellel

Avanenud aknas näeme kõiki serverile omastatud ja IIS-i poolt kasutatavaid sertifikaate. Kui soovime teha uut sertifikaadi päringufaili tuleb parempoolses käsujada-aknas klikkida nupule *„Create Certificate Request...."*:



Joonis 2 - valime uue sertifikaadi päringufaili loomise

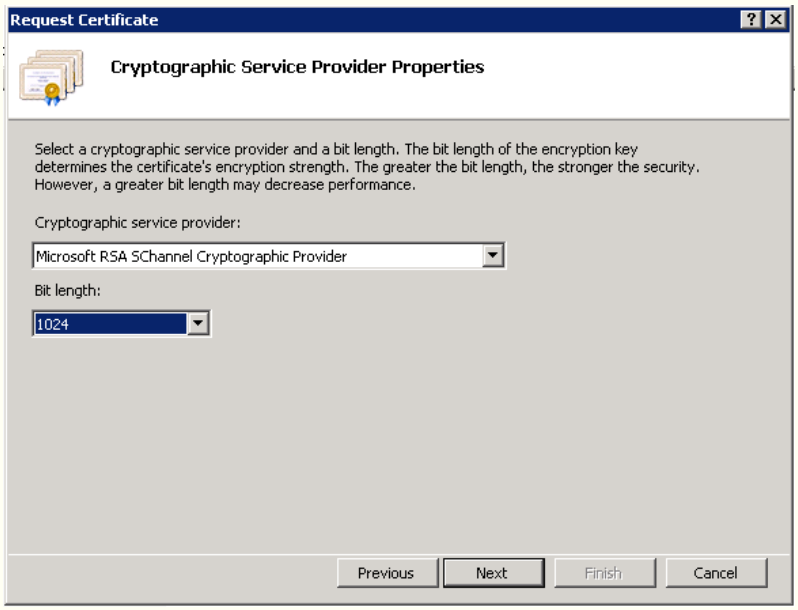
Avanevas aknas tuleb kirjeldada kogum tellitava sertifikaadi välju:



Joonis 3 - täidame sertifikaadi väljad

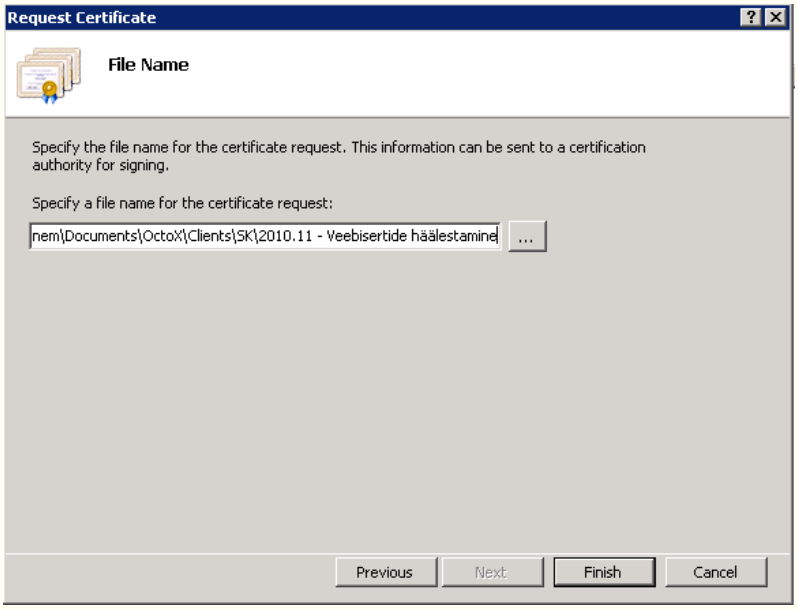
Oluline on siin pöörata tähelepanu väljale *„Common Name"* – see väli peab vastama veebiserveri aadressile. Meie näites on siia kirjutatud SKDEV.Kaheksa.XI mis tähendab, et hiljem pöördume veebisaidi poole nimega https://SKDEV.Kaheksa.XI

Liikudes edasi tuleb valida CSP ja võtme pikkus. Parema mõtte puudumisel võib siia jätta vaikimisi väärtused:



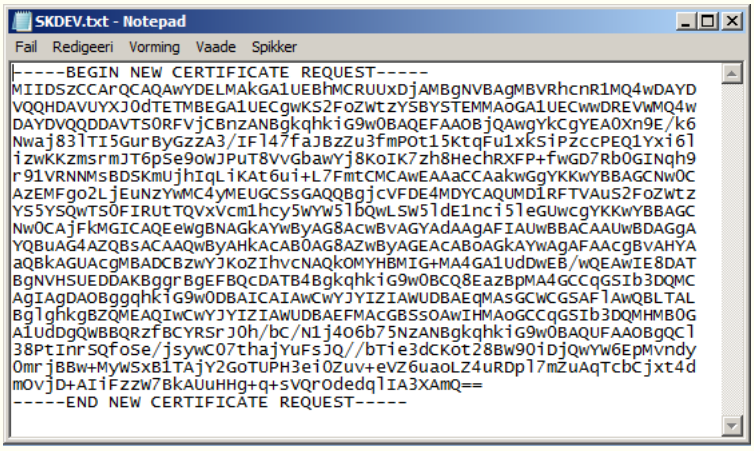
Joonis 4 - sertifikaadi omaduste kohandamine

Viimase sammuna tuleb valida väljundfaili nimi ja asukoht:



Joonis 5 - CSR-i salvestamine

Nüüd on meil tekkinud sertifikaadi päringufail, mis tekstiredaktoris näeb välja sarnaselt järgmisele:



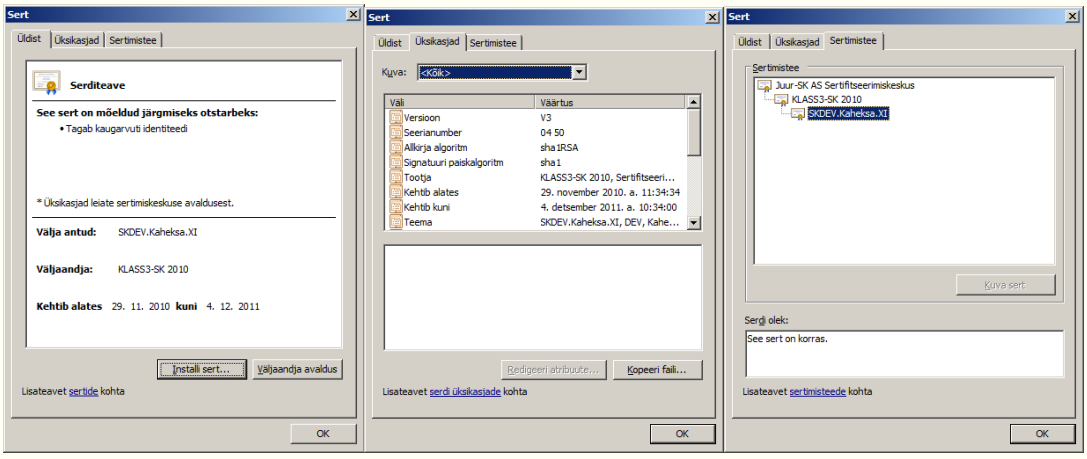
Joonis 6 - CSR tekstina

TELLIMUS

Eelnevas peatükis tekkinud CSR elik sertifikaadi päringufail tuleb:

1) Tellida sertifitseerimiskeskuse lehel http://www.sk.ee/teenused/veebiserveri-sertifikaadid/ või
2) Edastada sertifitseerimiskeskuse müügiosakonnale aadressil sales@sk.ee[1].

Sertifitseerimiskeskus vastab seepeale sertifikaadiga, mis näeb välja järgmine:



Paneme tähele, et välja on see sertifikaat antud veebilehele, mille kirjeldasime päringus kui *Common Name* – SKDEV.Kaheksa.XI. Lisaks näeme, et sertifikaat on välja antud „KLASS3-SK 2010“ tasemelt, mis omakorda on välja antud Juur-SK tasemelt.

SERTIFIKAADI INSTALLEERIMINE

KESKKONNA ETTEVALMISTUS

[1] SK on loomas uut veebiteenust sertifikaatide tellimiseks.

Selleks, et klientarvutite keskkond ootuspäraselt toimiks on vajalik nii kesk- kui juurtaseme sertifikaatide publitseerimine IIS serveri vastavates konteinerites[2]:

1) Juurtaseme sertifikaadi konteiner on *„Trusted Root Certification Authorities“,* eestikeelse Windowsi puhul „Usaldusväärsed juursertimiskeskused“.
2) *Kesktaseme sertifikaadi konteiner on „Intermediate Certification Authorities“,* eestikeelse Windowsi puhul „Kesktaseme sertimiskeskused“.

Vastavad sertifikaadid on allalaetavad Sertifitseerimiskeskuse veebilehelt http://www.sk.ee/certs :

1) Juursertifikaat Juur-SK – https://www.sk.ee/upload/files/Juur-SK.der.crt
2) Kesktaseme sertifikaat KLASS3-SK 2010 - https://www.sk.ee/upload/files/KLASS3-SK_2010.der.crt[3]

HALDAMATA KESKKOND

Haldamata keskkonna elik domeeniväliste IIS serverite puhul lisame sertifikaadid kas halduskonsooli, veebibrauseri või käsurea abil. Vaatleme siin sertifikaatide haldamist halduskonsooli abil.

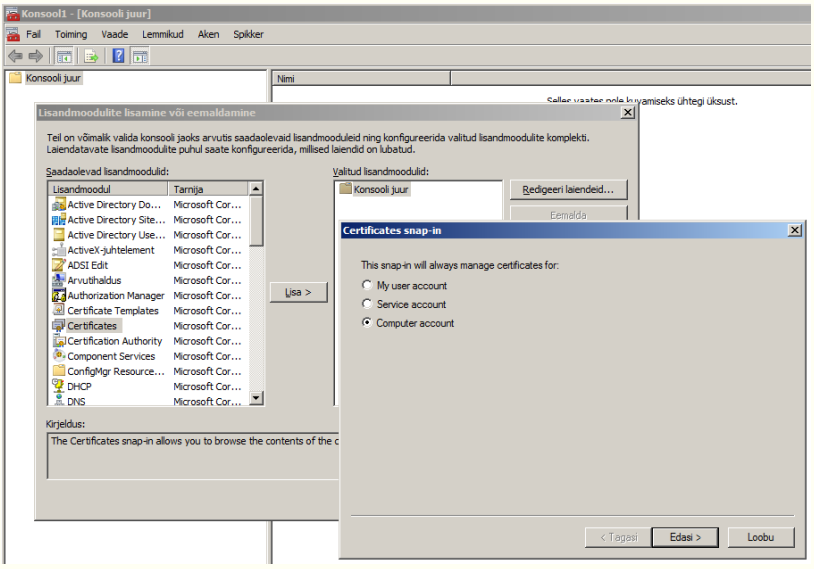
ERALDISEISVAD IIS SERVERID, HALDUSKONSOOL

1) Käivitame IIS serveril lokaalse administraatori õigustes mmc.exe
2) Avanenud aknas olles klikime Ctrl+M[4], avaneb lisandmoodulite haldusaken, kust valime Certificates ja klikime *Add* või „Lisa“ eestikeelse versiooni puhul, seejärel valime *„Computer Account“* ja klikime *Next* või „Edasi“:

[2] Juurtaseme sertifikaadid publitseeritakse ka automaatselt – need on Windows operatsioonisüsteemis vaikimisi olemas.

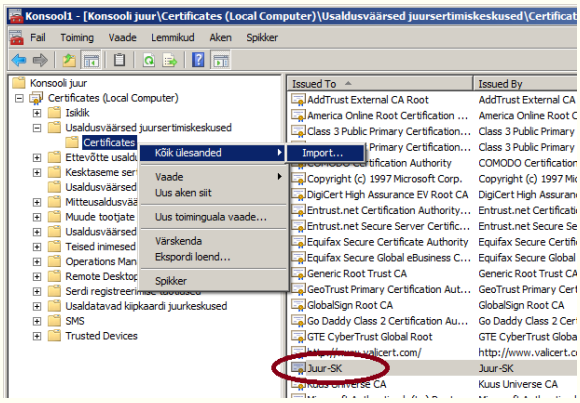
[3] Juhul, kui olemasolev veebisert on antud välja mõne teise kesktaseme kaudu, tuleb loomulikult publitseerida see teine kesktase. Vaata väljastatud sertifikaadi ahelat veendumaks õige sertifikaadi valikus.

[4] Add Remove Snap-in/Lisa/Eemalda lisandmoodul



Joonis 7 - Lisandmooduli lisamine

3) Järgnevas aknas jätame valituks „*Local Computer*“ kui tegeleme sama arvutiga ja klikime *Finish* või „Valmis“, klikime veelkord OK sulgemaks lisandmoodulita haldusakent.
4) Avame konsooli juure ja brausime Usaldusväärsete juursertimiskeskuste [5] sertifikaatide juurde. Kontrollime Juur-SK sertifikaadi olemasolu. Selle puudumisel lisame selle import käsu abil (vt. kesktaseme sertifikaadi lisamine, järgmine punkt).

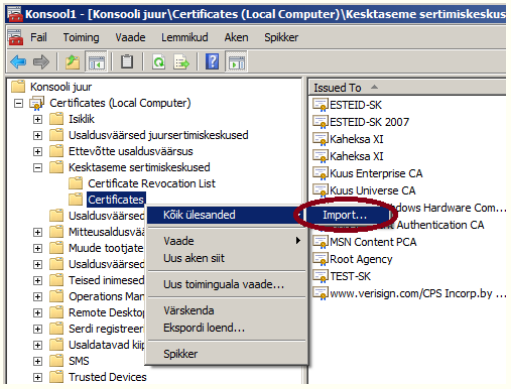


Joonis 8 - juursertifikaadi kontroll

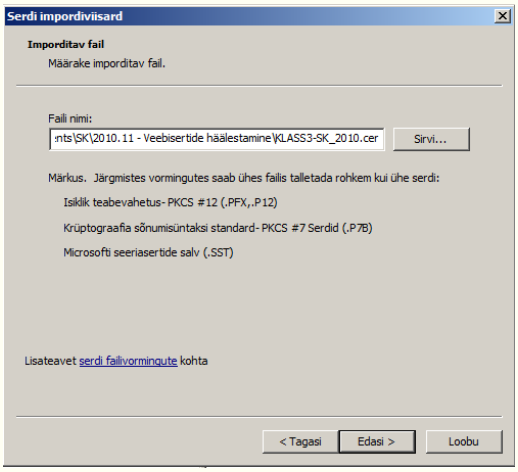
5) Avame konsooli juure ja brausime kesktaseme sertimiskeskuste [6] sertifikaatide juurde. Lisame sertifikaadi „KLASS3-SK 2010“ kasutades *Import* käsku:

[5] *Trusted Root Certification Authorities*

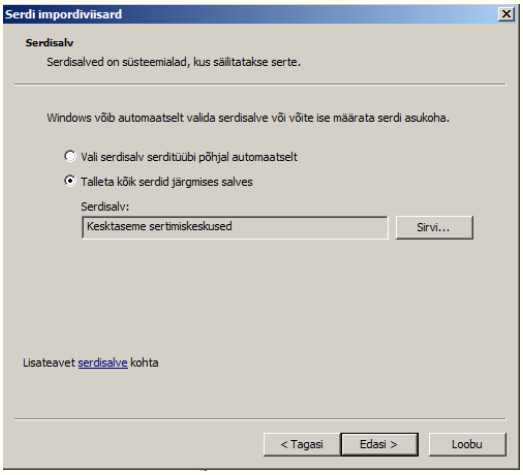
[6] *Intermediate Certification Authorities*



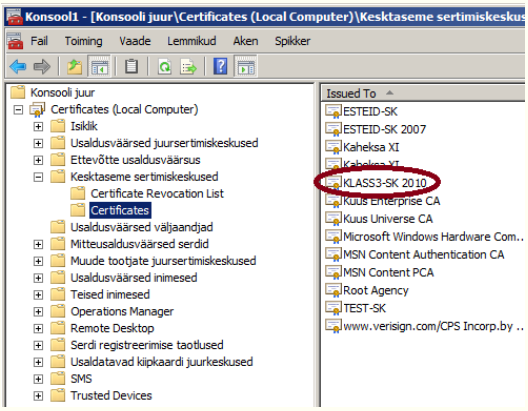
Joonis 9 - importimise algus



Joonis 10 - sertifikaadi valik



Joonis 11 - salve valik



Joonis 12 – tulemus

Kui näeme sertifikaati „KLASS3-SK 2010“ parempoolses loetelus oleme kõik õieti teinud.

WINDOWS DOMEENI KESKKOND

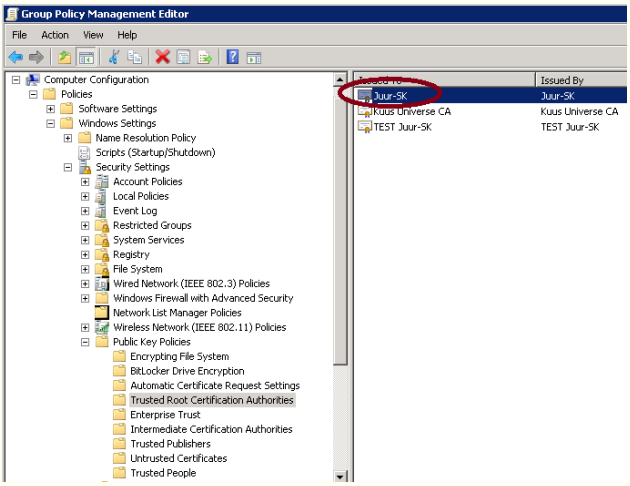
Selle punkti võime kindlasti vahele jätta, kui ei soovi oma veebiservereid kesksete poliitikatega hallata ja eelmises punktis kirjeldatud meetod on piisavalt hea!

Windows domeeni keskkonnas, kui meil on rohkem IIS servereid, soovitame publitseerida nii juur- kui kesktaseme sertifikaadid vastavatele serveritele *„Group Policy“* abil[7][8]:

1) Käivitame *Group Policy Management* konsooli ja valime sealt poliitika, mille abil alustame IIS serverite sertifikaatide haldamist, paremklikime sellel ja valime *Edit*. Avaneb poliitika haldusaken. Valime sealt „Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Trusted Root Certification Authorities“ ja paremklikime sellel, avanenud menüüst valime *Import* ja impordime Juur-SK sertifikaadi sarnaselt eelnevalt kirjeldatud üksikarvuti kesktaseme sertifikaadi impordile.

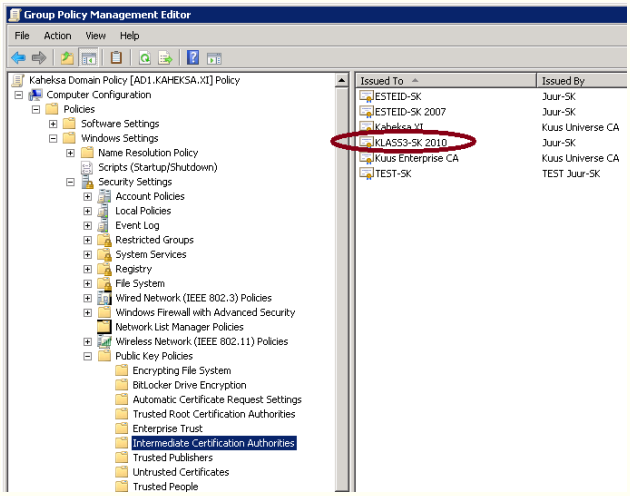
[7] Üksiku serveri puhul võime kasutada ka „käsitsi“ lisamist, nagu kirjeldatud eelmises punktis.

[8] Pole ka midagi halvasti, kui nimetatud sertifikaadid kõikidele AD klientidele publitseerime.



Joonis 13 - tulemus –sertifikaat Juur-SK on publitseeritud

2) Käivitame *Group Policy Management* konsooli ja valime sealt poliitika, mille abil alustame IIS serverite sertifikaatide haldamist, paremklikime sellel ja valime *Edit*. Avaneb poliitika haldusaken. Valime sealt „Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Intermediate Certification Authorities“ ja paremklikime sellel, avanenud menüüst valime *Import* ja impordime „KLASS3-SK 2010“ sertifikaadi sarnaselt eelnevalt kirjeldatud üksikarvuti kesktaseme sertifikaadi impordile.



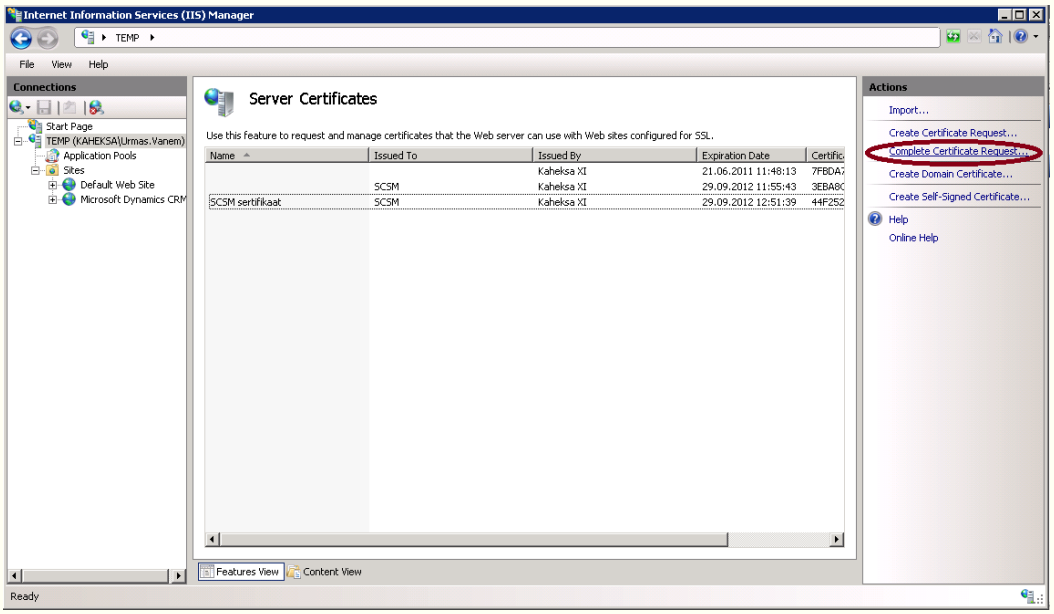
Joonis 14 - tulemus - sertifikaat KLASS3-SK 2010 on publitseeritud

KLIENTIDE HÄÄLESTUS

Kliendid peavad usaldama Juur-SK sertifikaati elik hoidma seda enda „Usaldusväärsete Juursertifikaatide“ salves. Kaasaegsetes Windows operatsioonisüsteemides on see häälestus vaikimisi korras.

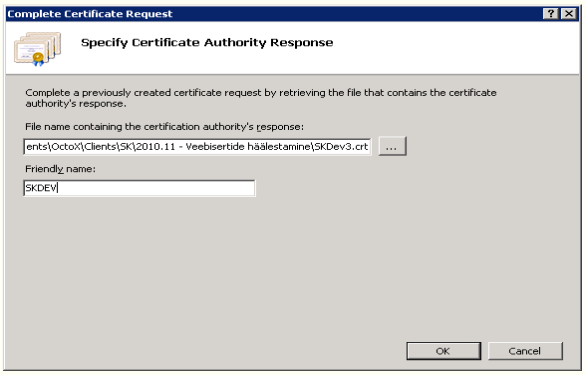
VEEBISERTIFIKAADI INSTALLEERIMINE

Sertifitseerimiskeskusest saadud sertifikaadi installeerimiseks käivitame IIS halduskonsooli, valime serveri ja klikime nupul „*Complete Certificate Request*“:



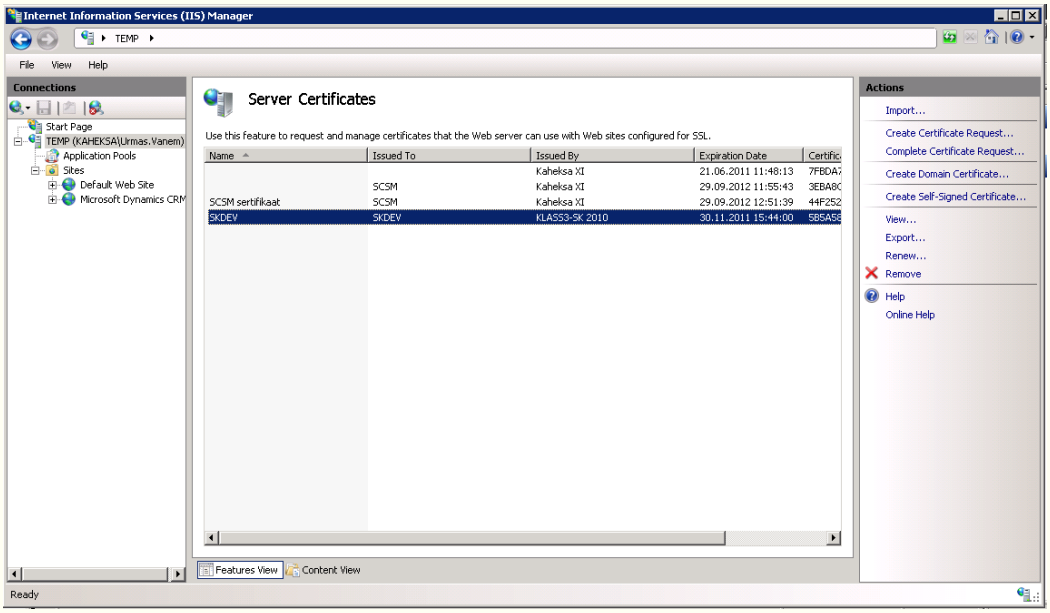
Joonis 15 - nupp *Complete Certificate Request*

Seejärel valime saadud sertifikaadi ja määrame sellele sõbraliku nime (näite valik on SKDEV), mis teeb selle hilisema valiku lihtsamaks:



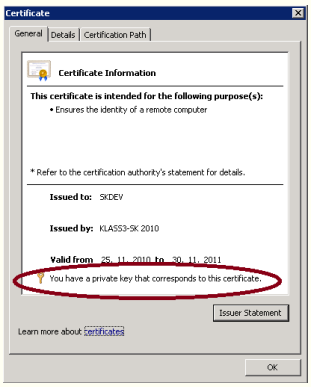
Joonis 16 - sertifikaadi valik ja sõbraliku nime määramine

Peale OK klikkimist näeme sertifikaati muude sertifikaatide loendis:



Joonis 17 - sõbraliku nimega SKDEV on nüüd serveriga seotud

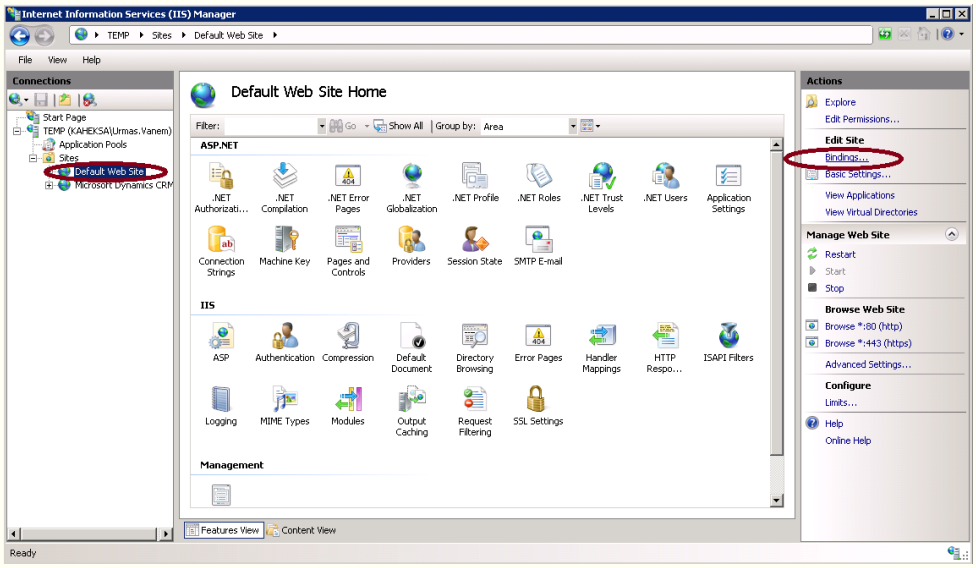
Avades selle sertifikaadi IIS aknast (klikkides V*iew*) näeme, et teenusel on sertifikaadi privaatvõti:



Joonis 18 - sertifikaadi privaatvõti on olemas

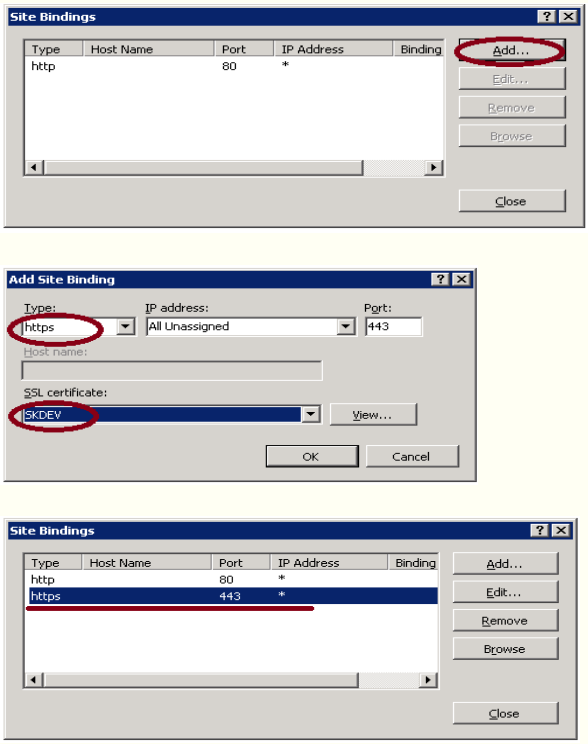
SSL LUBAMINE

Järgmise sammuna tuleb soovitud saidil lubada SSL elik selle poole pöördumine üle HTTPS protokolli. Selleks valime esmalt soovitud veebisaidi ja seejärel klikime käsul *Bindings:*



Joonis 19 - Bindings valik

Avanevas aknas klikime nupule *Add*, seejärel valime uue tüübi https, soovi korral spetsiifilised IP aadressid ja pordi ning kasutusele võetava SSL sertifikaadi (mida on valikust lihtne ära tunda meie määratud sõbraliku nime järgi):



Joonis 20 - https lubamine

Nüüdsest on saidi poole võimalik pöörduda nimega https://skdev.kaheksa.xi[9]

TULEMUS

Avanenud veebisaidi sertifikaadi korrasolu iseloomustab tabaluku märk, millele klikkimine annab meile ka enamat informatsiooni:

Joonis 21 - veebisait on usaldusväärne

VÕIMALIKUD PROBLEEMID

Kui me ei näe ülaltoodud pilti ja veebilehe poole pöördudes saame hoiatusi võib asi olla:

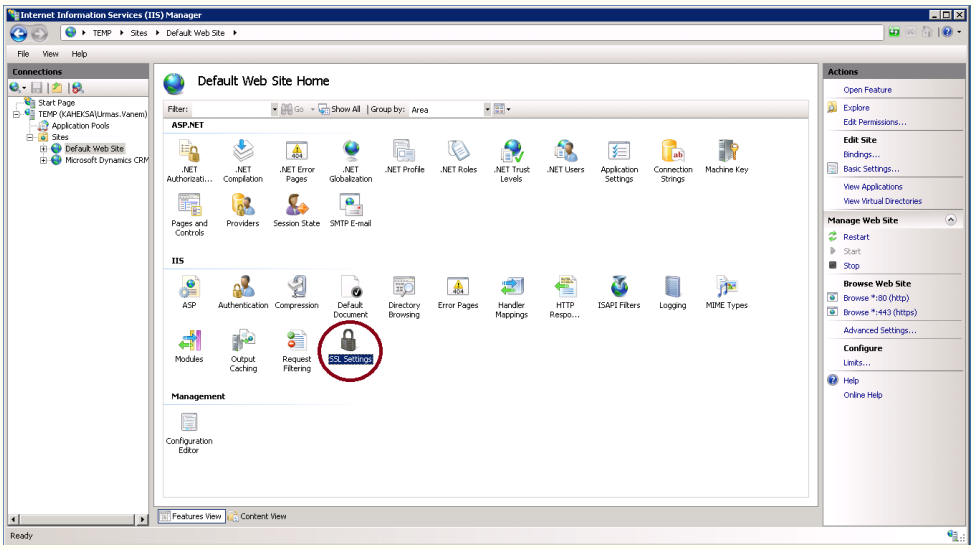
1) Vales nimes – veebisaidi nimi peab vastama sertifikaadis kirjeldatud nimele
2) Mõnes puuduvas sertifikaadis terve ahela ulatuses – juur- ja kesktaseme sertifikaadid peavad olema korralikult publitseeritud

LISAVÕIMALUSED

SSL NÕUE

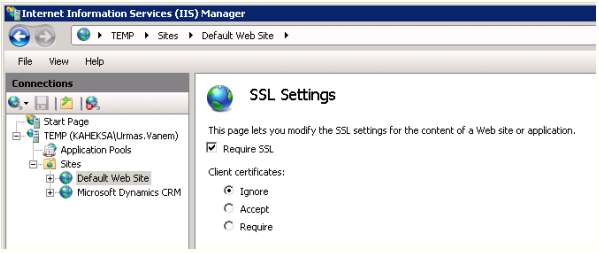
Lisaks võimalusele üle HTTPS protokolli veebisaidi poole pöörduda saame vastava nõude ka IIS serveri poolt kehtestada. Selleks valime meid huvitava saidi ja klikime nupul „*SSL Settings*“:

[9] Muidugi eeldame, et vastav kirje eksisteerib nimelahendusteenuses.



Joonis 22 - NUPP *SSL Settings*

Seejärel saame lülitada sisse SSL nõude, mille järel üle HTTP protokolli enam veebisaidi poole pöörduda ei saa:



Joonis 23 - SSL nõue

Nüüdsest on sait kättesaadav ainult üle HTTPS protokolli!

MUUD VÕIMALUSED

AUTOMAATNE ÜMBERSUUNAMINE

IIS'i abil on lihtne sooritada automaatset ümbersuunamist HTTP saidilt HTTPS saidile. Täpsemad viited on Microsofti artiklis http://technet.microsoft.com/en-us/library/cc732969(WS.10).aspx

MUUD VÕIMALUSED TURVALISE VEEBILAHENDUSE KASUTUSEKS

IIS veebisaidil võib kehtestada nõude, et kasutaja võib saidi poole pöörduda vaid kehtivat sertifikaati omades. Kui Eesti ID kaardi sertifikaat on seotud kasutajaga AD-s (näiteks juhul, kui on kasutusel „puhas" ID-login[10]), on

[10] Vt ka. http://www.sk.ee/upload/files/ID-login_juhend.pdf

võimalik end ka selle abil veebisaidil autentida[11]. Need juhtumid aga sõltuvad täpsemalt konfiguratsioonist ja vajadustest ning üldiseid suuniseid on siin raske anda.

[11] Vajalik on veebiserveri lisaomaduse installatsioon.