SK veebisertide häälestus, IIS 6

Tehniline kirjeldus

Urmas Vanem

2010

SERTIFITSEERIMISKESKUS

SISUKORD

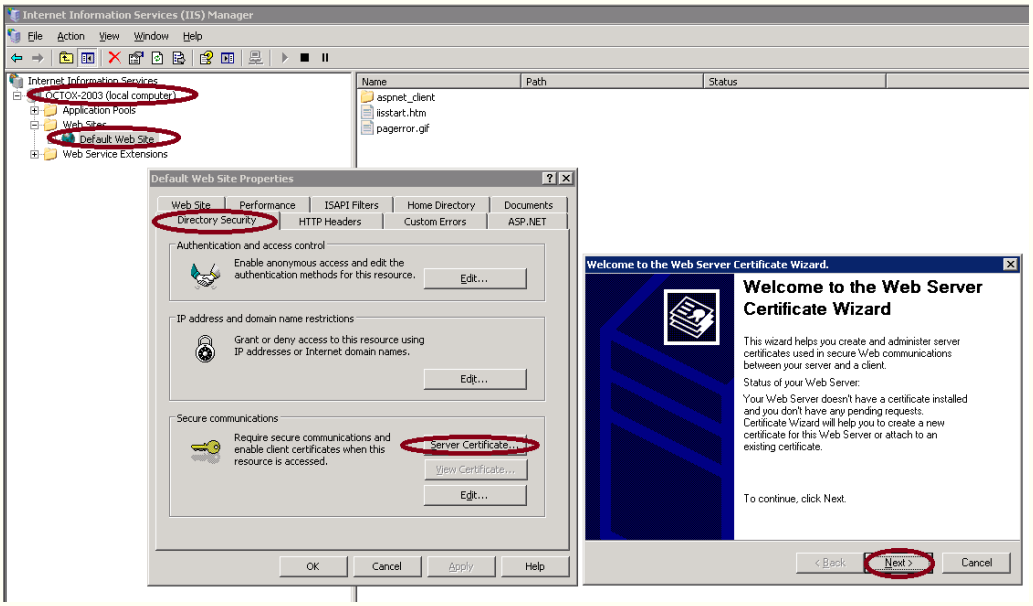
SISSEJUHATAVALT

Käesolev dokument kirjeldab Sertifitseerimiskeskuse veebisertide häälestamist Windows 2003 serveril. Põhimõtteliselt on vaja teha sertifikaadi päring SK-sse ja tagasisaadud sertifikaat siduda soovitava veebisaidiga. Veebiserveri platvormiks on IIS 6. Vaatleme, kuidas soovitavaid tegevusi saab sooritada üle graafilise kasutajakeskkonna.

SERTIFIKAADI PÄRINGU LOOMINE

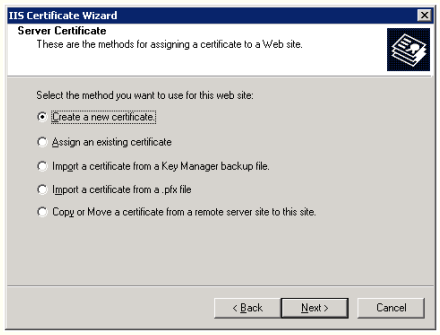
Sertifikaadi päringuks tuleb esimese sammuna IIS serveri abil genereerida päringufail (*Certificate Service Request* elik *CSR*), mis tuleb edastada sertifitseerimiskeskusesse.

Sertifikaadi päringufaili loomiseks tuleb avada IIS Manager ja sealt valida soovitav veebiserver ja veebisait. Veebisaidil tuleb klikkida parempoolset hiirenuppu ja valida *Properties*. Seejärel avanevas aknas tuleb valida leht *„Directory Security“* ja klikkida nupul *„Server Certificate“*. Seejärel klikkida nupul *Next*:



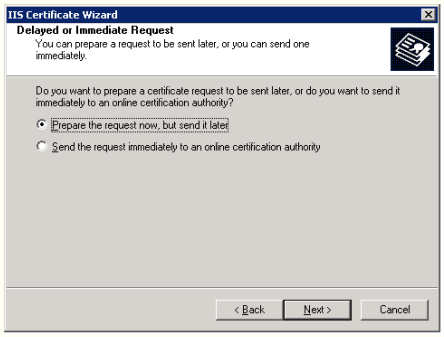
Joonis 1 – päringufaili loomine, esimesed sammud

Järgnevalt avanevas aknas tuleb valida *„Create a new certificate“*:



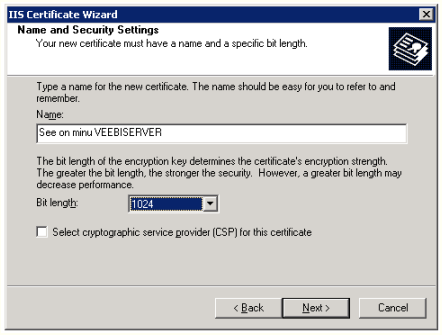
Joonis 2 – loome uut sertifikaadi

Seejärel valime *„Prepare the request now, but send it later“*:



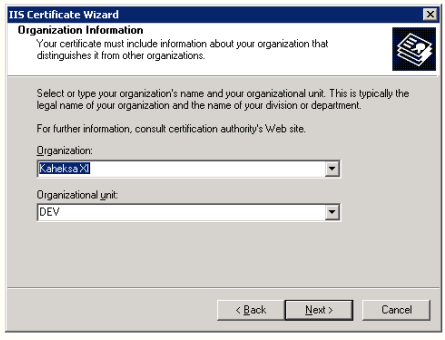
Joonis 3 - päringufaili loomise valik

Valime oma sertifikaadile esimesed omadused ja klikime *Next*:



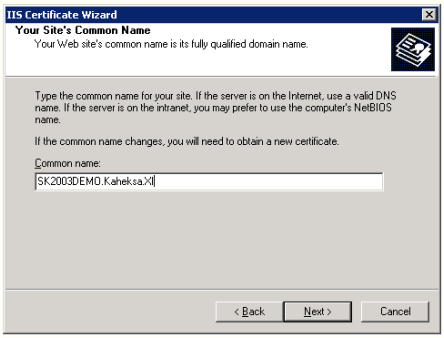
Joonis 4 - sõbralik nimi ja muu

Järgnevalt kirjeldame organisatsiooni ja OU:



Joonis 5 - organisatsioon ja OU

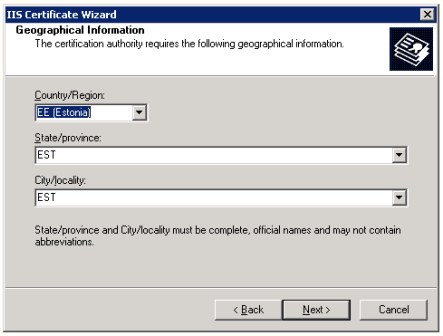
Siis määrame nime, mille abil hakkame serveri poole pöörduma:



Joonis 6 - veebiserveri nime määramine

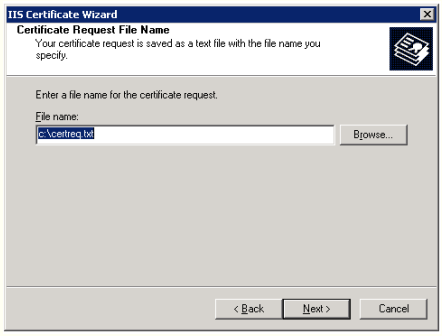
Oluline: see peab tegelikult ka olema nimi, mida hiljem reaalselt kasutama hakkame. Muidu saame üle https protokolli leheküljele minnes veateate, kus öeldakse et nimi pole õige.

Täidame asukohaga seotud parameetrid:



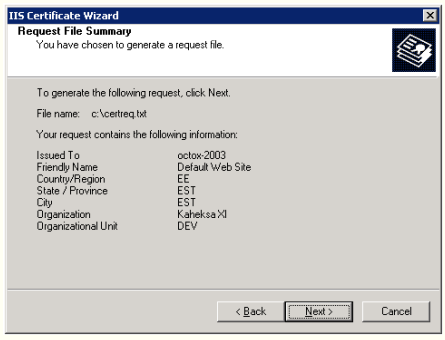
Joonis 7 – asukoha info

Määrame salvestatava päringufaili nime ja asukoha:



Joonis 8 - päringufaili nimi ja asukoht

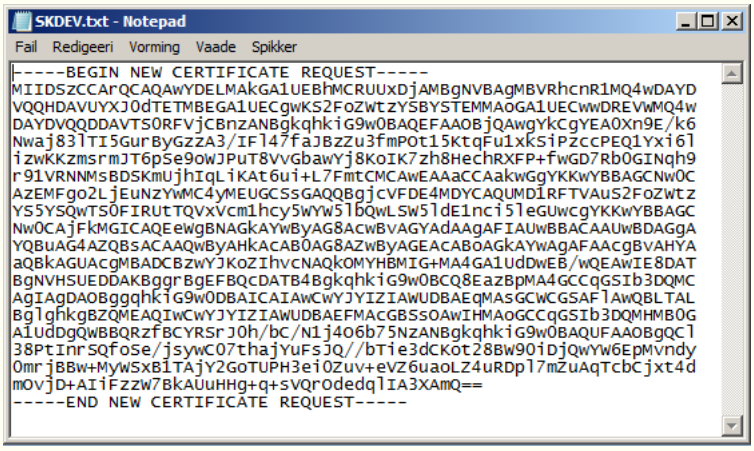
Vaatame üle sisestatud informatsiooni:



Joonis 9 – kokkuvõtvalt

Ja klikime *Next* ja *Finish* päringufaili loomiseks.

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

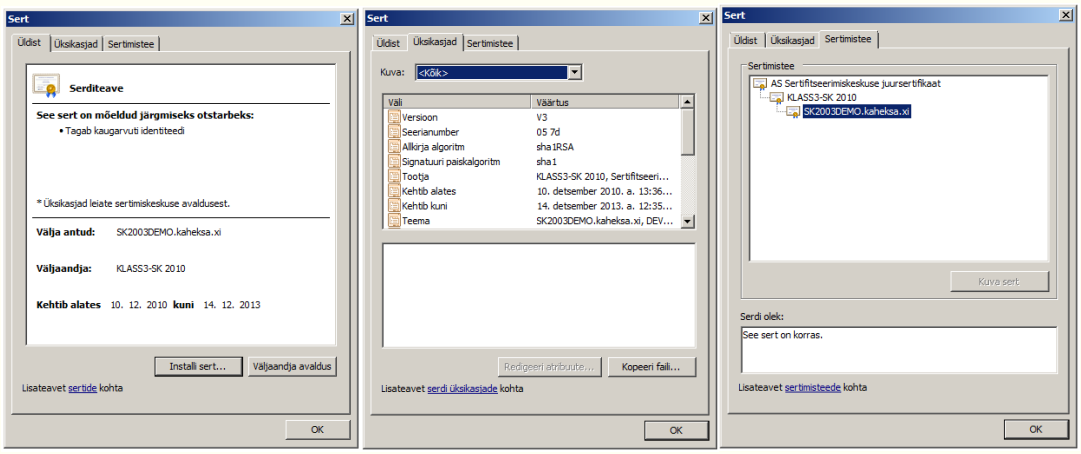


Joonis 10 - CSR tekstina

TELLIMUS

Eelnevas peatükis tekkinud CSR elik sertifikaadi päringufail tuleb edastada sertifitseerimiskeskuse müügiosakonnale aadressil sales@sk.ee[1]. Sertifitseerimiskeskus vastab seepeale sertifikaadiga, mis näeb välja järgmine:

[1] SK on loomas uut veebiteenust sertifikaatide tellimiseks.



Pange tähele, et välja on see sertifikaat antud veebilehele, mille kirjeldasime päringus kui *Common Name* – SK2003DEMO.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

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

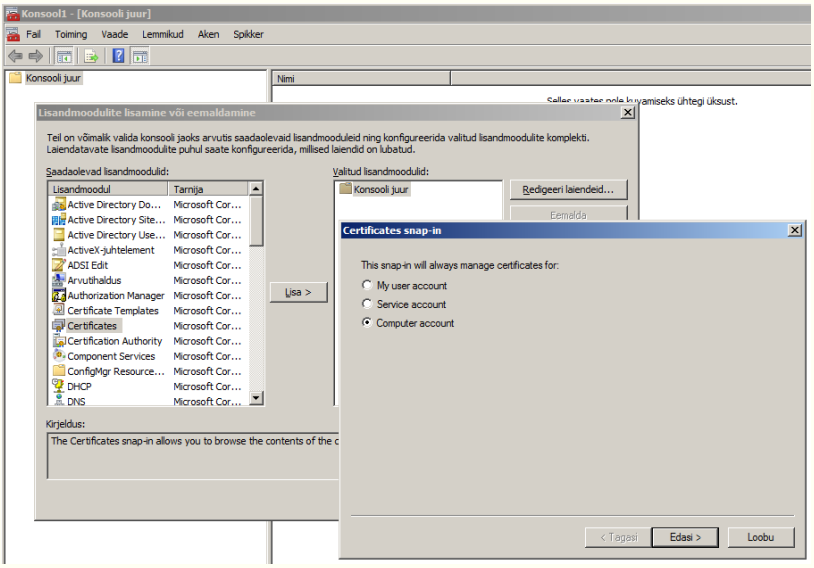
Haldamata keskkonna elik domeeniväliste IIS serverite puhul lisame sertifikaadid kas halduskonsooli, veebibrauseri või käsurea abil. Vaatleme siin sertifikaatide haldamist halduskonsooli abil.

ERALDISEISVAD IIS SERVERID, HALDUSKONSOOL

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

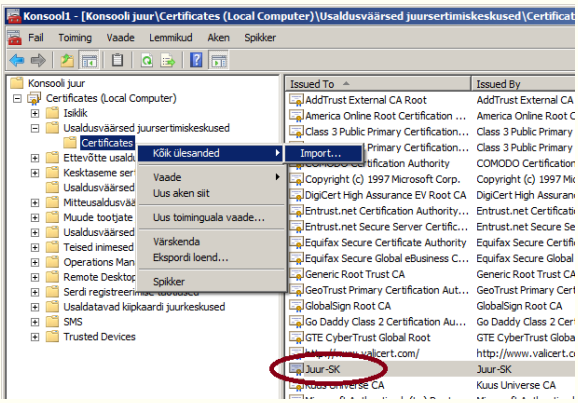
[3] Juhul, kui olemasolev veebisert on antud välja mõne teise kesktaseme kaudu, tuleb loomulikult publitseerida see teine kesktase. Vaata väljastatud sertifikaadi ahelat veendumaks õige sertifikaadi valikus.

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“:



Joonis 11 - 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. ka kesktaseme sertifikaadi lisamine, järgmine punkt).

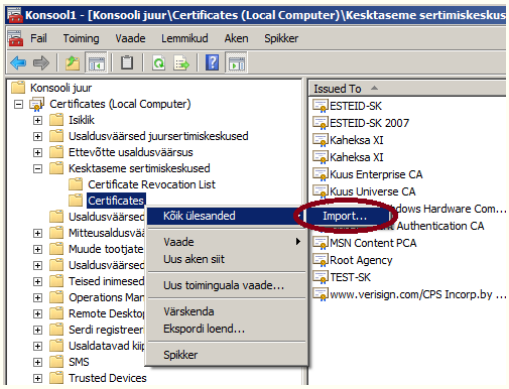


Joonis 12 - juursertifikaadi kontroll

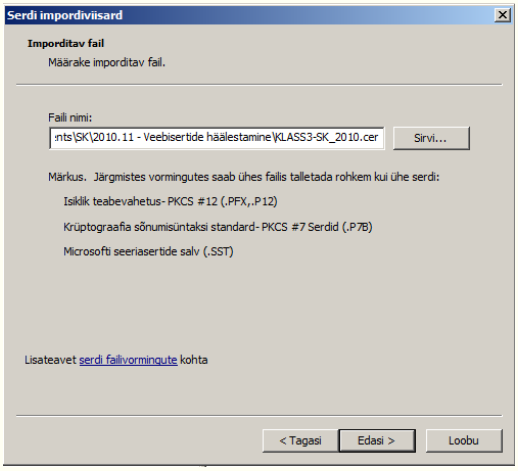
[4] Add-Remove Snap-in / Lisa-Eemalda lisandmoodul

[5] *Trusted Root Certification Authorities*

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

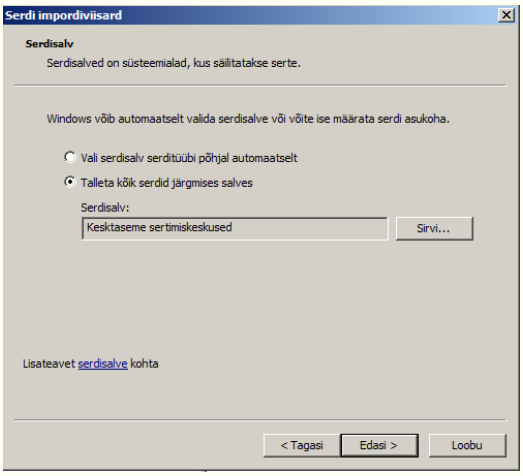


Joonis 13 - importimise algus

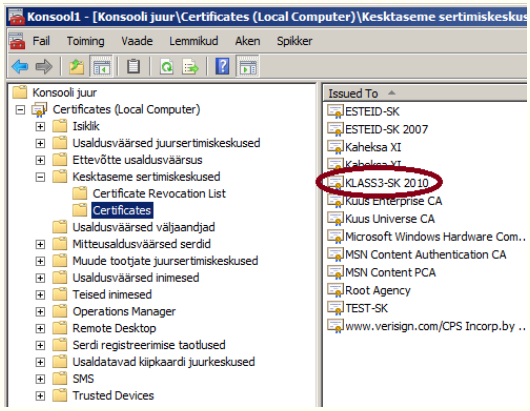


Joonis 14 - sertifikaadi valik

[6] *Intermediate Certification Authorities*



Joonis 15 - salve valik



Joonis 16 – 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!

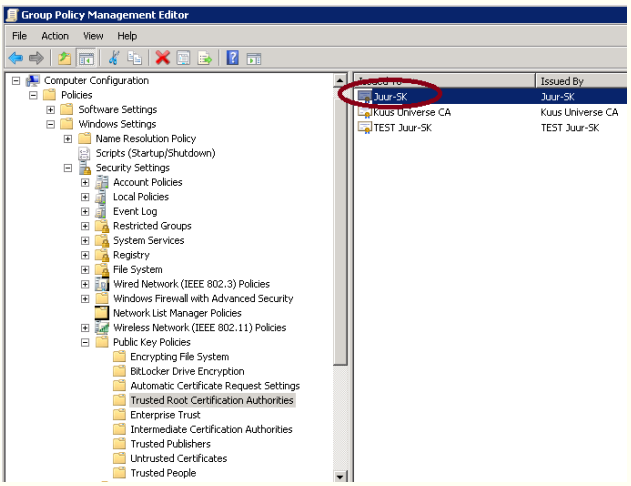
Windows domeeni keskkonnas, kui meil on rohkem IIS servereid, soovitame publitseerida nii juur- kui kesktaseme sertifikaadid vastavatele serveritele „*Group Policy*“ abil[7][8]:

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

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

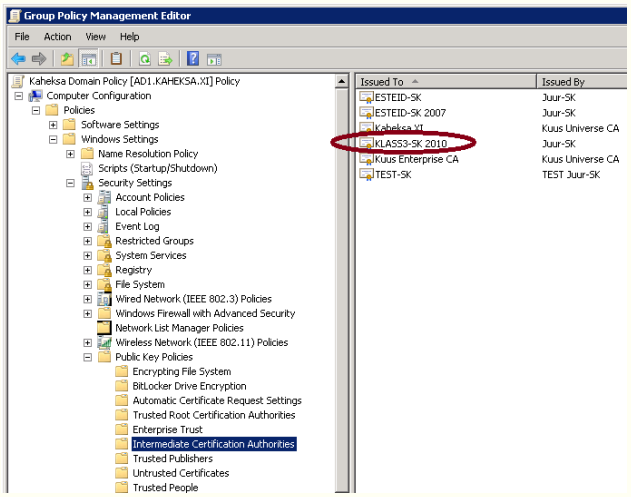
[8] Pole ka midagi halvasti, kui nimetatud sertifikaadid kõikidele AD klientidele publitseerime.

Certification Authorities“ ja paremklikime sellel, avanenud menüüst valime *Import* ja impordime Juur-SK sertifikaadi sarnaselt eelnevalt kirjeldatud üksikarvuti kesktaseme sertifikaadi impordile.



Joonis 17 - 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.



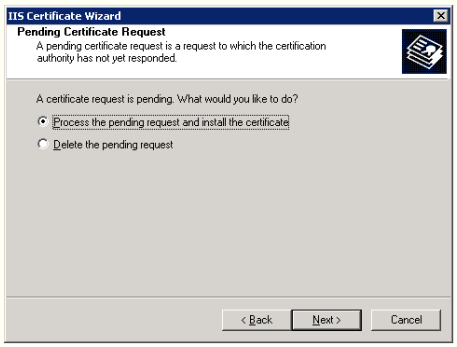
Joonis 18 - tulemus - sertifikaat KLASS3-SK 2010 on publitseeritud

KLIENTIDE HÄÄLESTUS

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

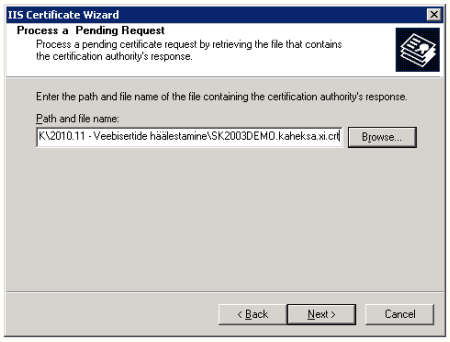
VEEBISERTIFIKAADI INSTALLEERIMINE

Saadud sertifikaadi installeerimiseks tuleb avada IIS Manager ja sealt valida soovitav veebiserver ja veebisait. Veebisaidil tuleb klikkida parempoolset hiirenuppu ja valida *Properties*[9]. Seejärel klikime *Next*, jätame vaikimisi valikuks „*Process the pending request and install the certificate*“:



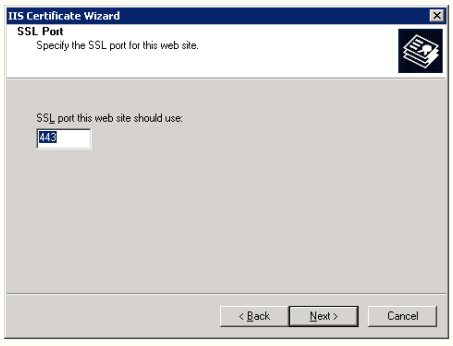
Joonis 19–sertifikaadi installatsiooni algus

Siis valime saadud sertifikaadifaili:



Joonis 20 - sertifikaadifaili valik

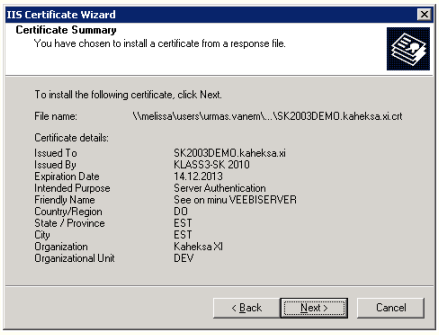
Valime pordi (vaikimisi 443 on standard):



Joonis 21 - SSL pordi valik

Kontrollime andmete õigsust:

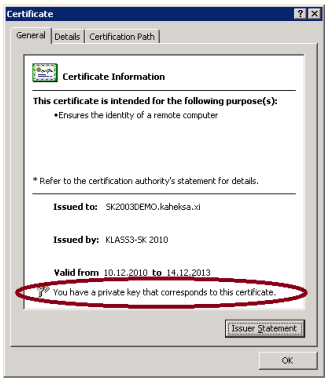
[9]Vt. joonis 1



Joonis 22 – kokkuvõte

Ja klikime *Next* ning *Finish* sertifikaadi omastamiseks.

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



Joonis 23 - sertifikaadi privaatvõti on olemas

SSL LUBAMINE

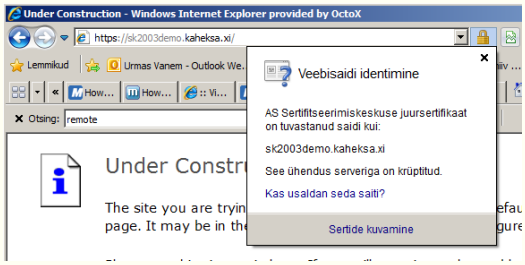
SSL nimetatud veebisaidi poole on automaatselt lubatud.

Nüüdsest on saidi poole võimalik pöörduda nimega https://SK2003Demo.kaheksa.xi[10]

TULEMUS

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

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



Joonis 24 - veebisait on usaldusväärne

VÕIMALIKUD PROBLEEMID

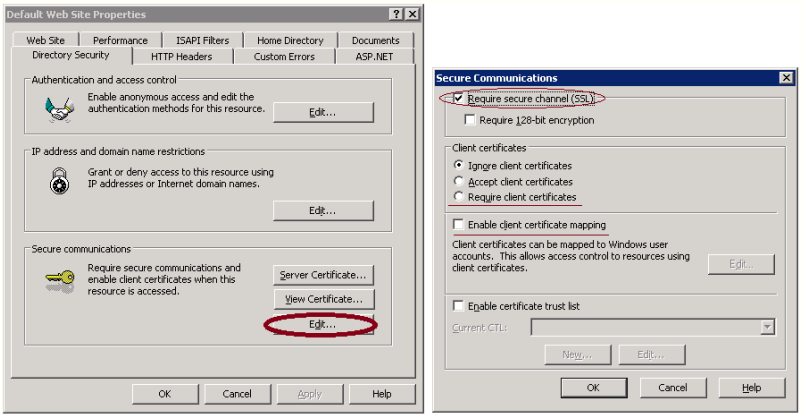
Kui me ei näe ülaltoodud pilti ja veebilehe poole pöördudes saame hoiatusi võib asi olla:

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 omadused, sealt valima „*Secure Communications* „ alamosast *Edit* ja märgime ära nupu „*Require secure channel*“:



Joonis 25–SSL nõude kehtestamine

Nüüdsest on sait kättesaadav ainult üle HTTPS protokolli!

Lisaks võime avanenud aknas häälestada ka kliendipoolse sertifikaadi omamise nõude.

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

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