SK WEB CERTIFICATE CONFIGURATION, IIS 8

Specifications

TABLE OF CONTENTS

INTRODUCTION

This document describes the configuration of SK web certificates on Windows 2012 R2 server. In essence, a certificate request must be made to SK and the returned certificate must be bound to the desired website. The web server platform is IIS 8 for Windows Server 2012 R2 in these instructions. We examine how actions can be performed over a graphical user interface.

We address web server certificates issued from the "EE Certification Centre Root CA" / "KLASS3-SK 2010" level. (Test environment certificates are used in the demo.)

CREATING A CERTIFICATE REQUEST

In order to make a certificate request, the first step is to generate the request file (*Certificate Service Request* or *CSR*) using IIS server, which must be sent to SK.

Open *IIS Manager* to create the certificate request file and select the desired web server. In the details window, double-click on "*Server Certificates*".

Figure 1 - select the server certificates button and double-click it

In the new window, we see all the certificates attributed to the server and used by IIS. If we want to create a new certificate request file, we must click the button "*Create Certificate Request...*." in the menu on the right:

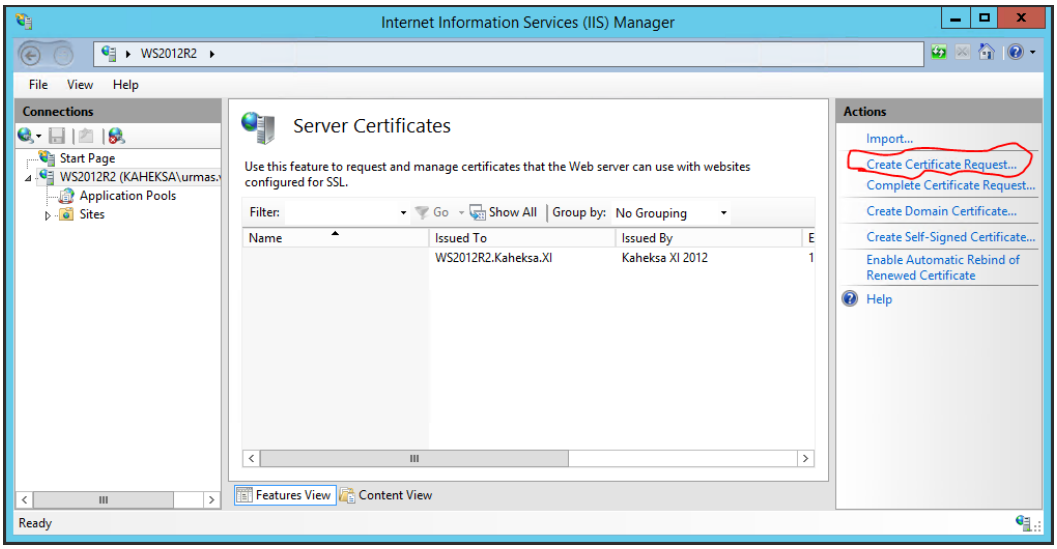


Figure 2 - selecting create new certificate request file

In a new window, a list of certificate properties must be defined:

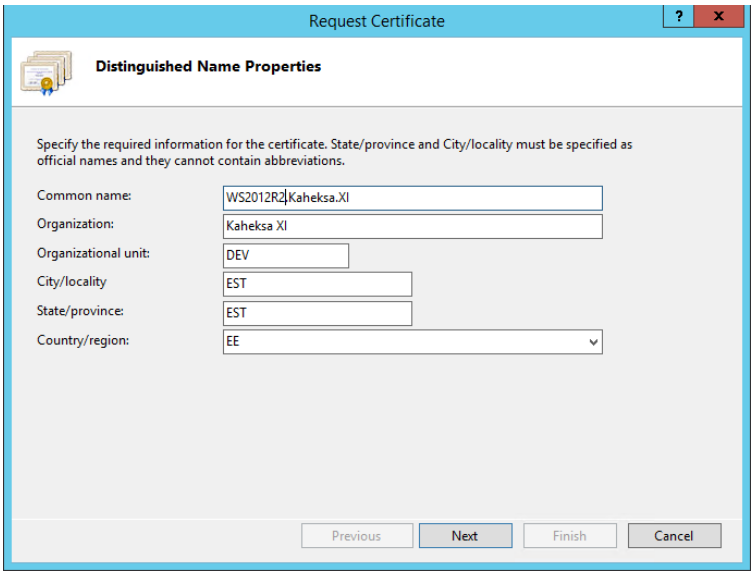


Figure 3 - filling out the certificate properties

It is important to make sure the "*Common Name*" field corresponds to the web server address. In our example it contains WS2012R2V.Kaheksa.XI, meaning that we will later contact the website https://WS2012R2.Kaheksa.XI

Moving on, CSP and bit length should be selected. Bit length should be set at 2048!

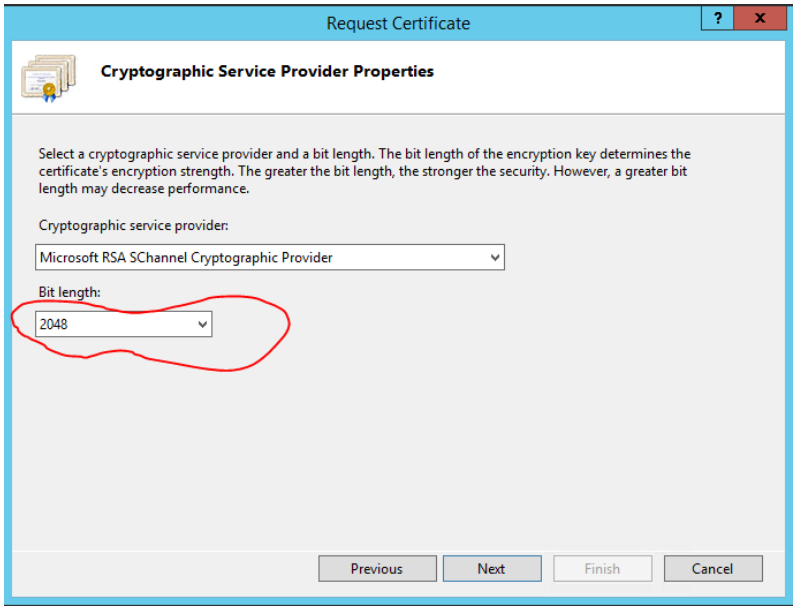


Figure 4 - adjusting certificate properties

As the last step, the name and location of the output file should be set:

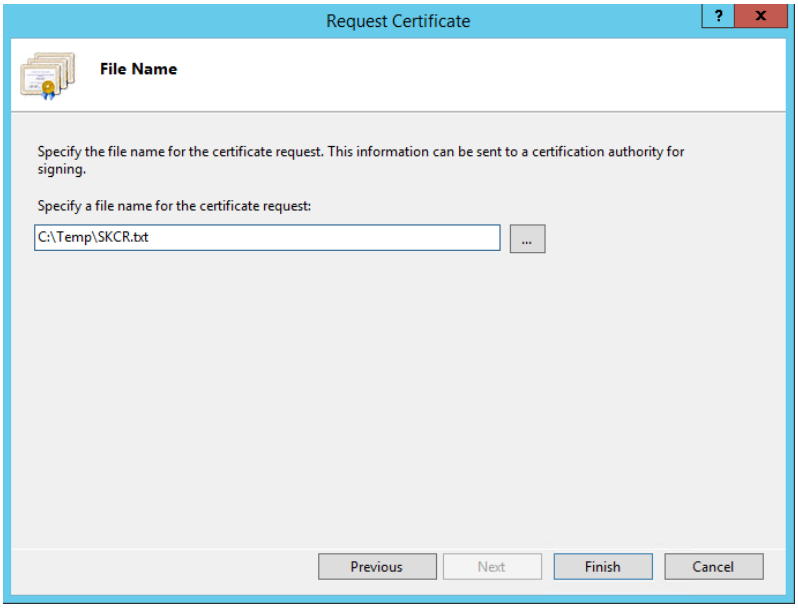


Figure 5 - saving the CSR

Now we have created a certificate request file that looks similar to below in text editor:

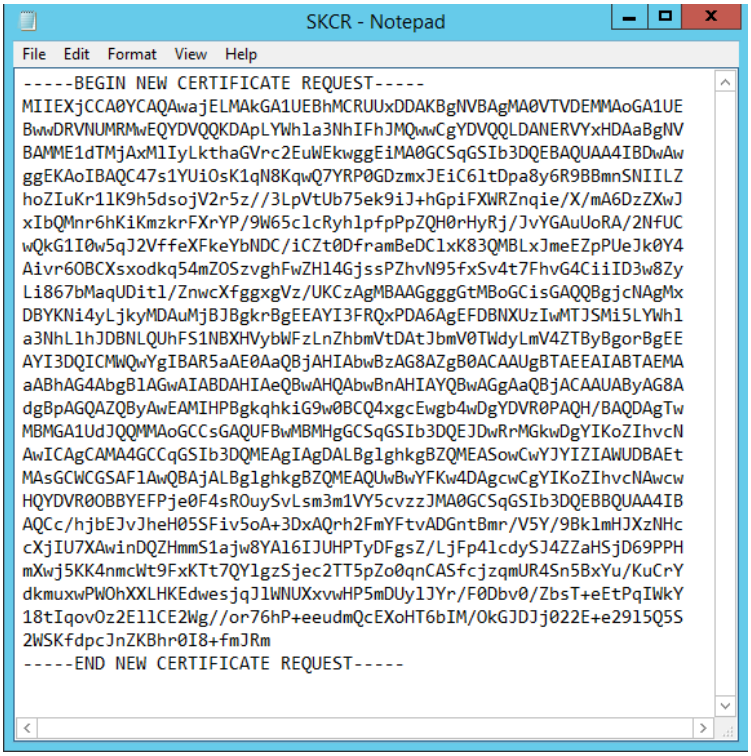
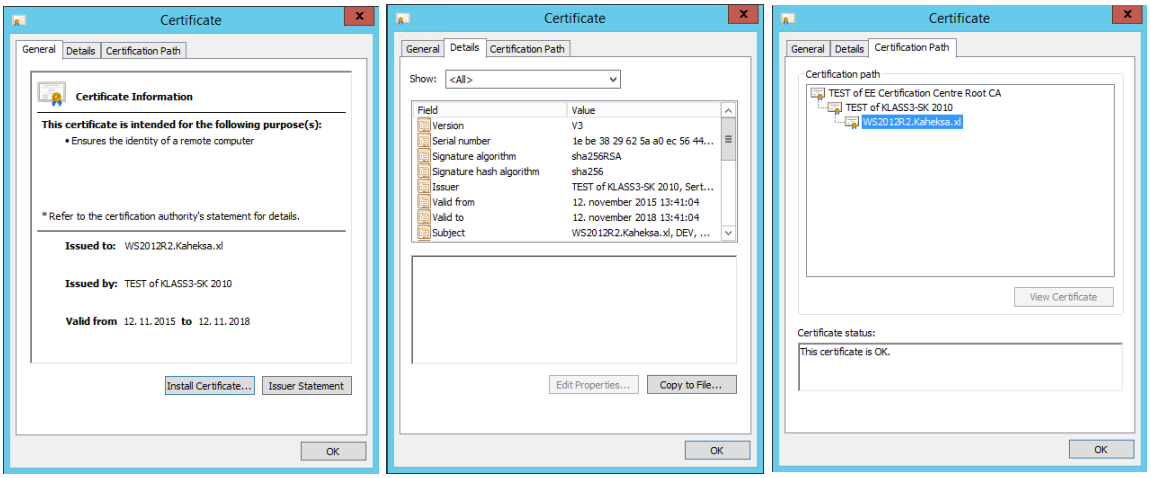


Figure 6 - CR as text

ORDER

The CSR or certificate request file generated in the previous chapter must be prepared/uploaded on SK's website https://sk.ee/en/services/ssl-certificates/?service/webserver_ssl[1].

SK will then respond with a certificate that looks like this:



Note that this certificate is issued to the website that we described in the request as *Common Name* – WS2012R2.Kaheksa.XI. We also see that the certificate is issued from the level "TEST of

[1] Web server certificates are issued to clients whose domain names and/or addresses are registered in the relevant public databases. Also see https://sk.ee/en/repository/conditions-for-use-of-certificates/

KLASS3-SK 2010", which in turn is issued from level "TEST of EE Certification Centre Root CA". In real life we obviously are dealing with actual and not test certificates and the certificate names are ""EE Certification Centre Root CA" and "KLASS3-SK 2010".

CERTIFICATE INSTALLATION

Preparation

In order for the web solution to function as expected, intermediate and root certificates must be published in the respective containers of IIS server:

1) The root certificate container is "*Trusted Root Certification Authorities" and* in case of Estonian-language Windows "Usaldusväärsed juursertimiskeskused".
2) The intermediate certificate container is "*Intermediate Certification Authorities" and* in case of Estonian-language Windows "Kesktaseme sertimiskeskused".

These certificates can be downloaded from SK's website at https://sk.ee/en/repository/certs/:

1) Root certificate "EE Certification Centre Root CA" - https://sk.ee/upload/files/EE_Certification_Centre_Root_CA.pem.crt
2) Intermediate certificate "KLASS3-SK 2010" - https://sk.ee/upload/files/KLASS3-SK_2010_EECCRCA_SHA384.pem.crt [2]

NON-DOMAIN ENVIRONMENT

In case of a non-domain environment, i.e. non-domain IIS servers, we add certificates using either management console, web browser or command line. In this case we will examine certificate management using management console.

Standalone IIS servers, management console

1) We run mmc.exe on IIS server with local administrator's permissions.
2) In the new window, click Ctrl+M[3], the snap-ins management window will open, select Certificates and click *Add* or "Lisa" if your version is in Estonian, thereafter select "*Computer Account"* and click *Next* or "Edasi":

[2] If an existing web certificate is issued via another intermediate level, that other intermediate level must obviously be published. See the issued certificate chain to ascertain correct certificate selection.
[3] Add Remove Snap-in

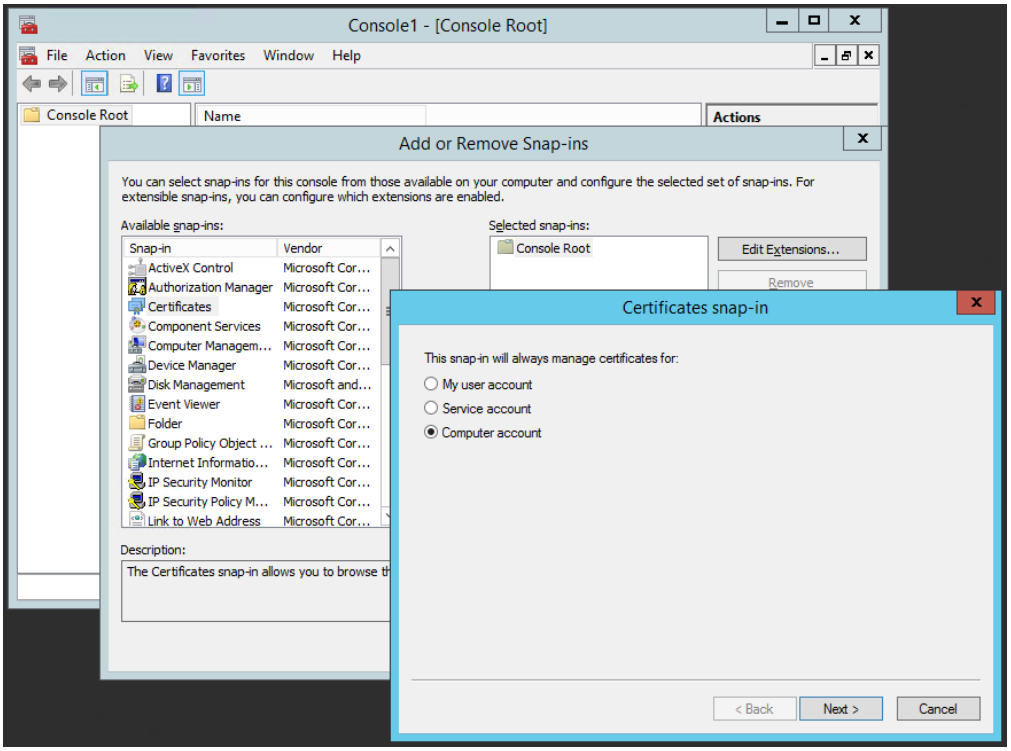


Figure 7 - Adding snap-ins

3) In the next window, "*Local Computer*" should remain selected if we are managing the same computer and click *Finish* or "Valmis", once again click OK to close the snap-in management window.

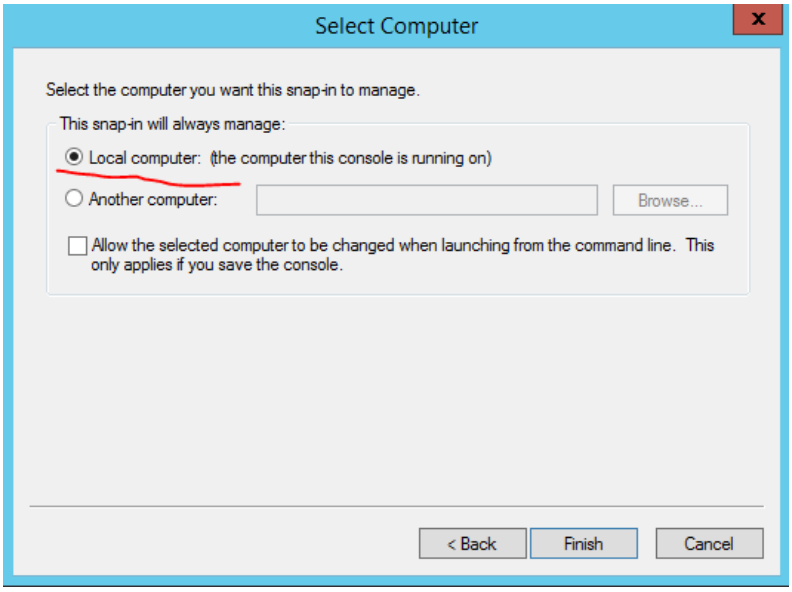


Figure 8 - local server selection

4) Open console root and browse to the Trusted Root Certification Authorities [4] certificates. Check if the "EE Certification Centre Root CA" certificate exists. If not, add

[4] *Trusted Root Certification Authorities*

the necessary certificate using the import command (see adding intermediate certificate, next section).

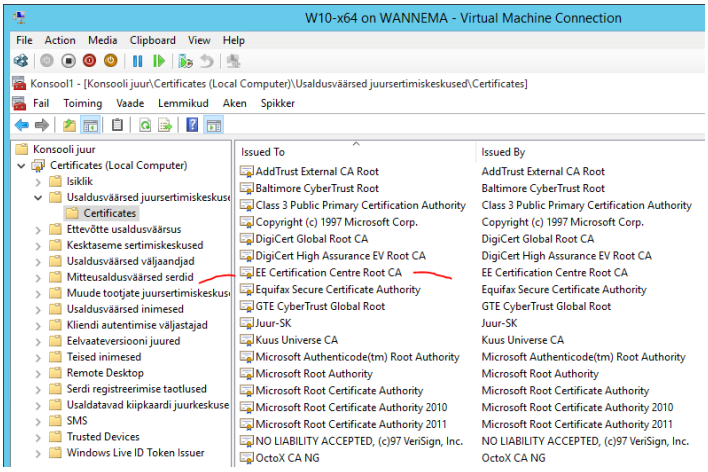


Figure 9 - root certificate verification

5) Open console root and browse to the Intermediate Certification Authorities [5] certificates. Add certificate "KLASS3-SK 2010" using the *Import* command:

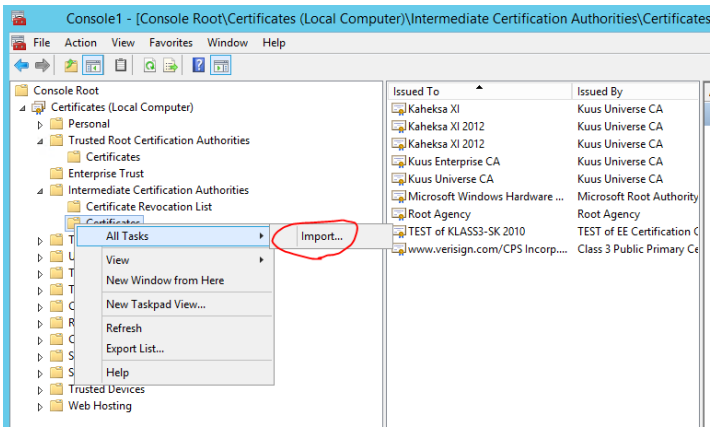


Figure 10 - starting to import

[5] *Intermediate Certification Authorities*

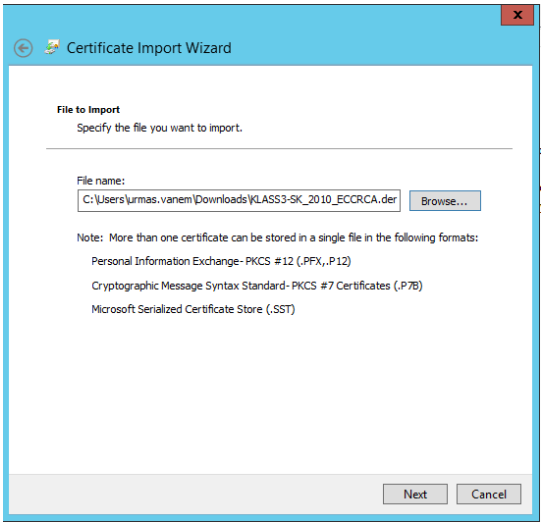


Figure 11 - certificate selection

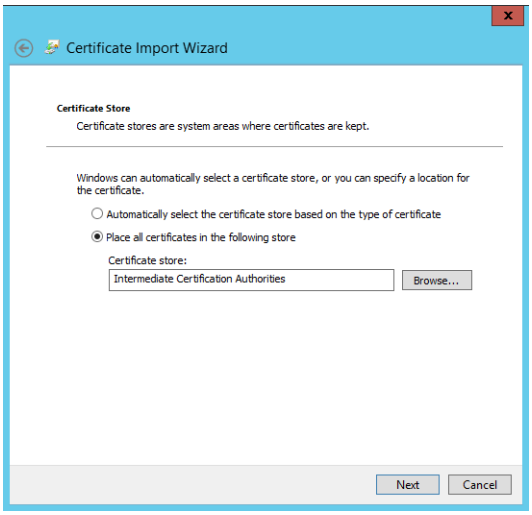


Figure 12 - store selection

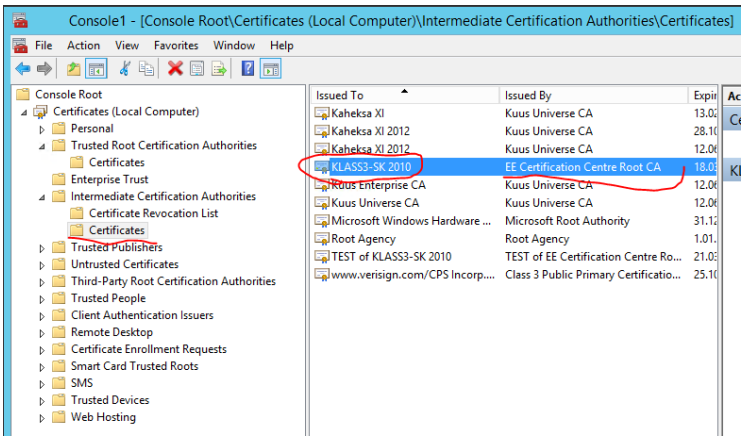


Figure 13 - results

If you see certificate "KLASS3-SK 2010" issued by "EE Certification Centre Root CA" in the list on the right, you have done everything correctly.

WINDOWS DOMAIN ENVIRONMENT

You can skip this section if you don't wish to manage your web servers using centralised policies and the method described in the previous section works well.

In Windows domain environment, if we have more IIS servers, we recommend root and intermediate certificates to be published to respective servers using "*Group Policy*"[6][7]:

1) Launch *Group Policy Management* console and select the policy that will be used for managing IIS server certificates, right-click it and select *Edit*. The policy management window will open. Select "Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Trusted Root Certification Authorities" and right-click it, from the right-click menu select *Import* and import the "EE Certification Centre Root CA" certificate like described above for single computer root certificate import.

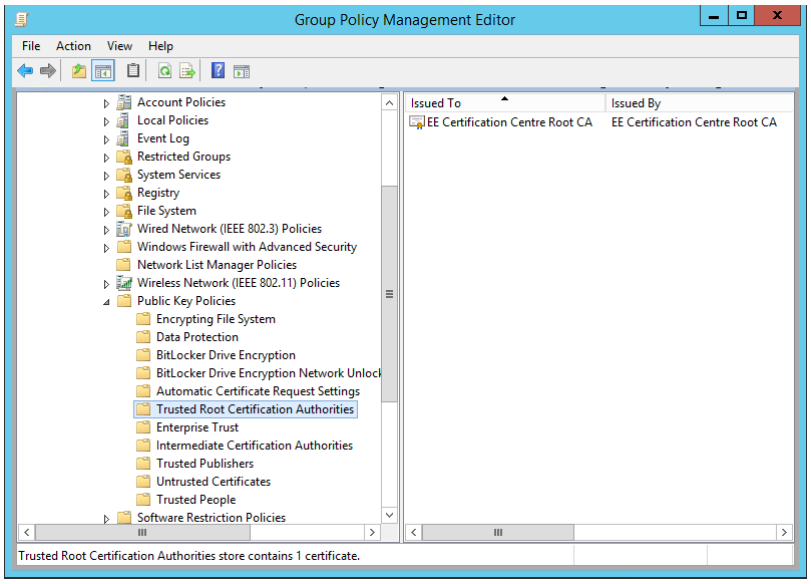


Figure 14 - results -the certificate "EE Certification Centre Root CA" is published

2) Launch *Group Policy Management* console and select the policy that will be used for managing IIS server certificates, right-click it and select *Edit*. The policy management window will open. Select "Computer Configuration/Policies/Windows Settings/Security Settings/Public Key Policies/Intermediate Certification Authorities" and right-click it, from the right-click menu select *Import* and import the "KLASS3-SK 2010" certificate like described above for single computer intermediate certificate import.

[6] In case of a single server, the "manual" approach is also fine, as described in the previous section.
[7] It is also not a problem if such certificates are published to all AD clients.

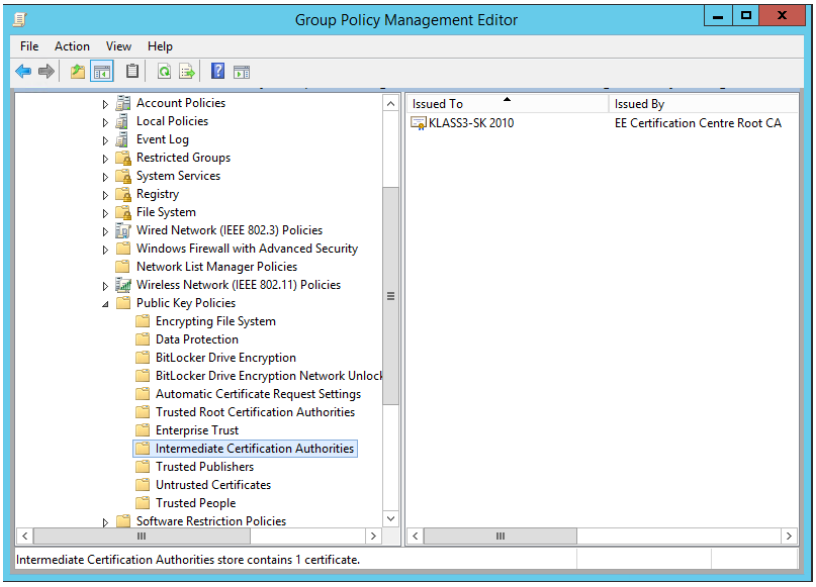


Figure 15 - results - the certificate KLASS3-SK 2010 is published

IIS SERVER CONFIGURATION IF CLIENT CERTIFICATE DOES NOT HAVE A COMPLETE CHAIN.

Starting from ID-card software version 3.10, a complete chain is no longer created for client certificates. Therefore, the default configuration no longer offers IIS service SK certificates to users. If we want to support a situation where the complete chain is not defined on the client side, we must make the following change to IIS server's registry: add to the key HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL DWORD the entry SendTrustedIssuerList with the value 0 :

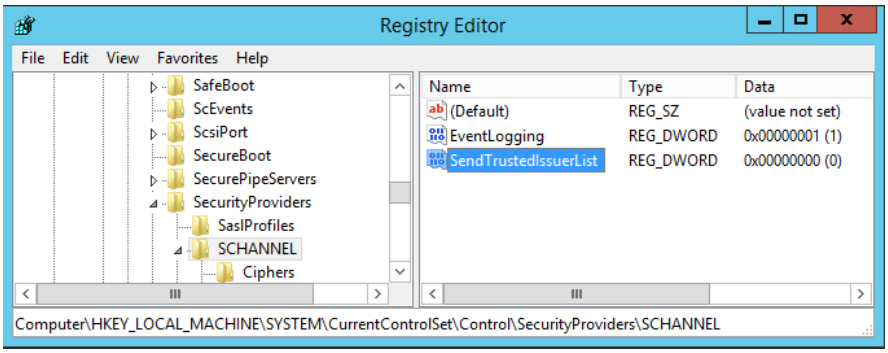


Figure 16 - support for clients with no chain

CLIENT CONFIGURATION

Clients must trust "EE Certification Centre Root CA" certificate, maintaining it in its "Trusted Root Certificates" store, depending on the final certificate in use. Trust occurs automatically in Windows operating systems because the "EE Certification Centre Root CA" certificate is automatically trusted. It can also be done using centralised policies by following the instructions described in previous sections on adding intermediate and root certificates or individually importing them.

Web certificate installation

In order to install the certificate obtained from SK, launch the IIS management console, select the server and click on "*Complete Certificate Request*":

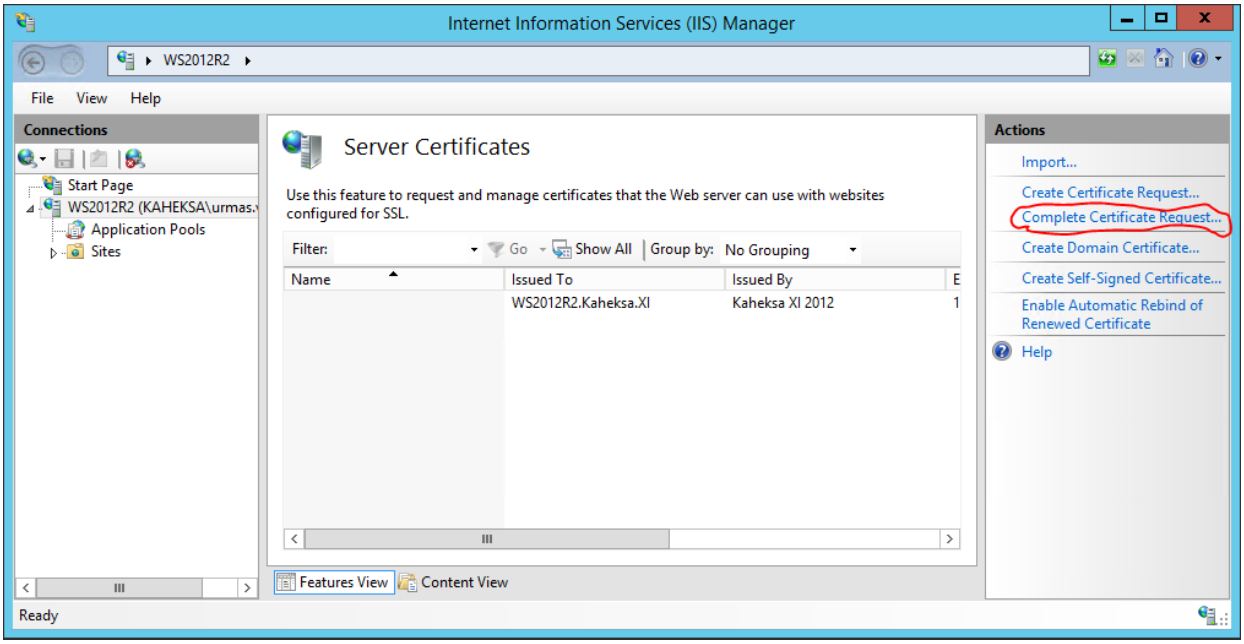


Figure 17 - *Complete Certificate Request button*

Then select the received certificate and set a friendly name (SK SSL certificate in the example), making it easier to select it afterwards. Leave *Personal* as the default store:

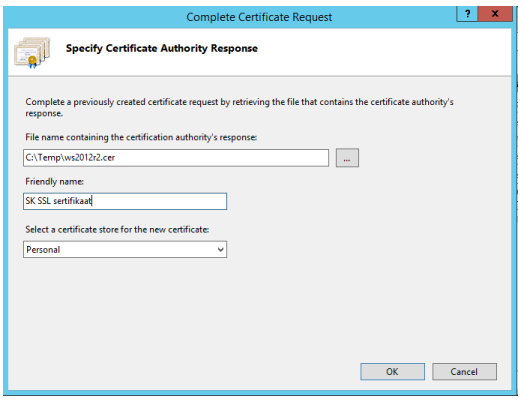


Figure 18 - certificate selection and setting friendly name

After you click OK, you'll see the certificate in the list of certificates:

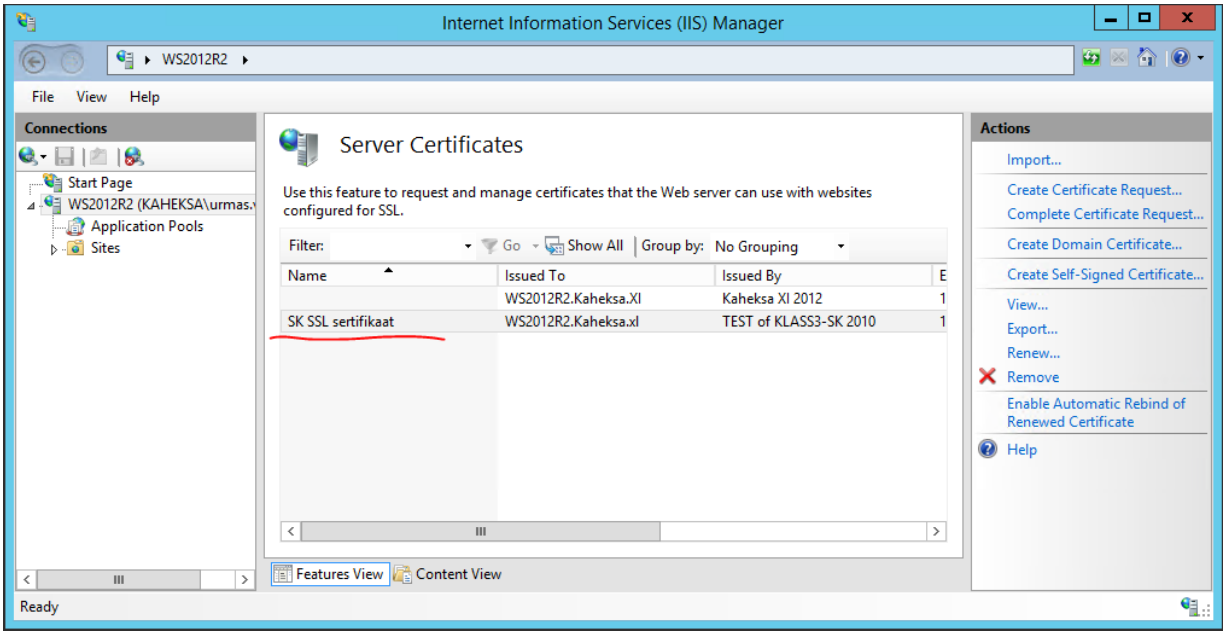


Figure 19 - the certificate with friendly name SK SSL certificate is now bound to the server

By opening this certificate from IIS window (by clicking *View*) you'll see that the service has the certificate private key:

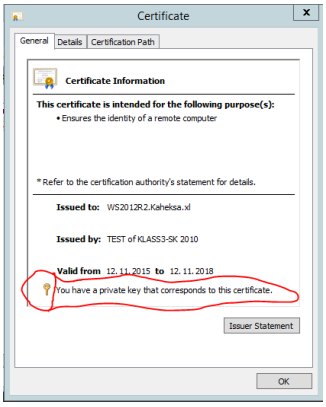


Figure 20 - certificate private key exists

Permitting SSL

The next step is to permit SSL on the desired website, communicating with it over the HTTPS protocol. First, select the desired website and then click on Bindings:

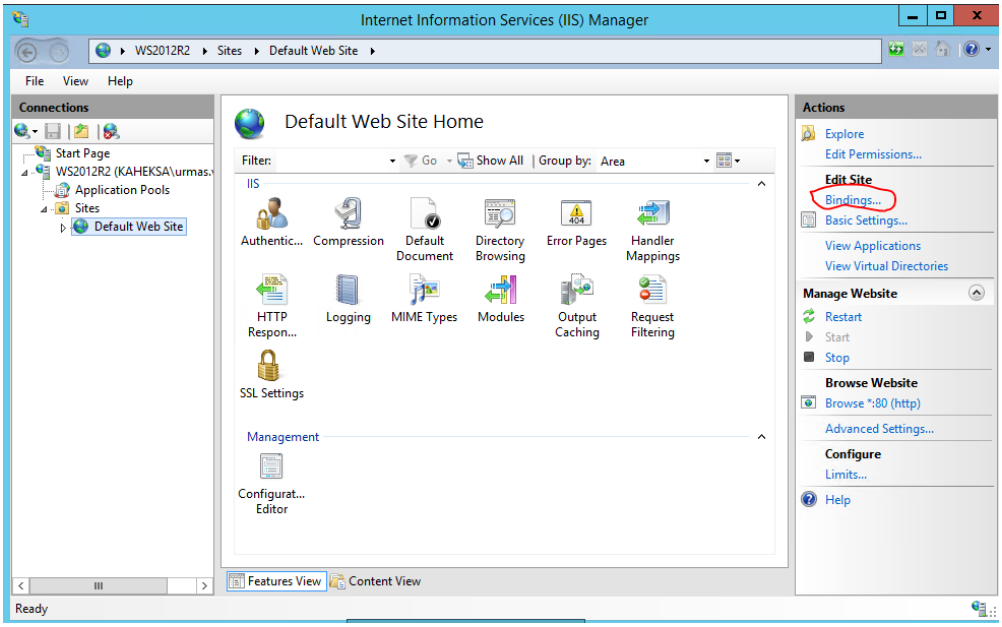


Figure 21 - Bindings selection

In the new window, click on *Add*, then select new type https, specific IP addresses and port are optional and the SSL certificate to be used (which is easy to recognise from the selection by the friendly name we have set):

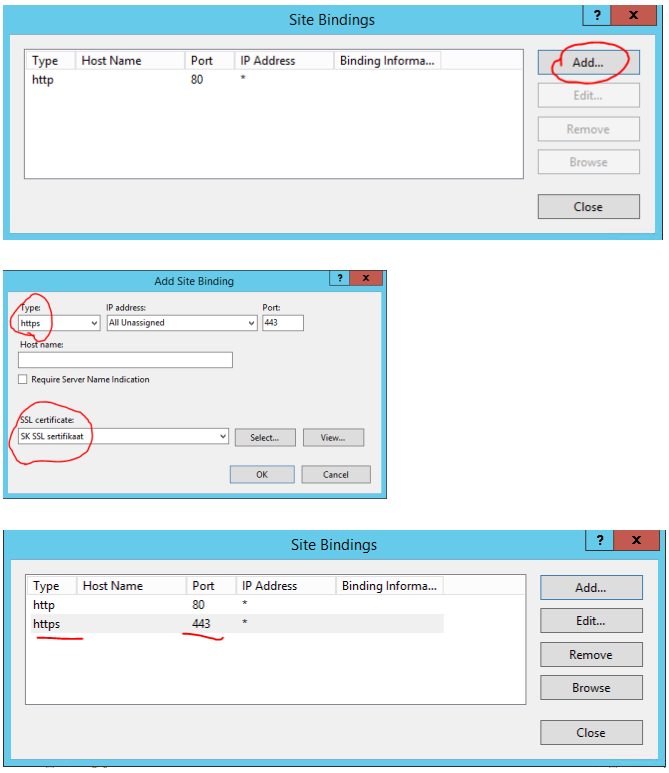


Figure 22 - Permitting https

Now, the website can be communicated with using the name https://ws2012r2.kaheksa.xi[8]

[8] Obviously, we assume the relevant entry exists in the domain name service.

RESULTS

The proper functioning of the certificate of an open website can be seen from the padlock sign. Clicking on it will give us more information:

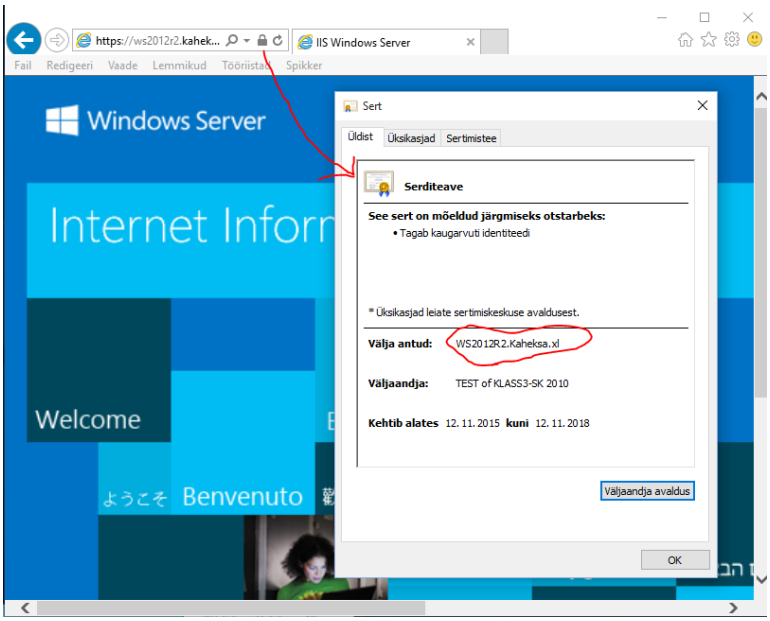


Figure 23 - the website can be trusted

POTENTIAL ISSUES

If we cannot see the above image and warnings are displayed when communicating with the website, it may be due to:

1) Wrong name - the website name must correspond to the name defined in the certificate
2) In some missing certificate to the extent of the whole chain - root and intermediate certificates must be properly published

ADDITIONAL OPTIONS

SSL requirement

In addition to the option to communicate with a website over HTTPS protocol, we can also establish this requirement by the IIS server. To do that, select the relevant website and click on "SSL Settings":

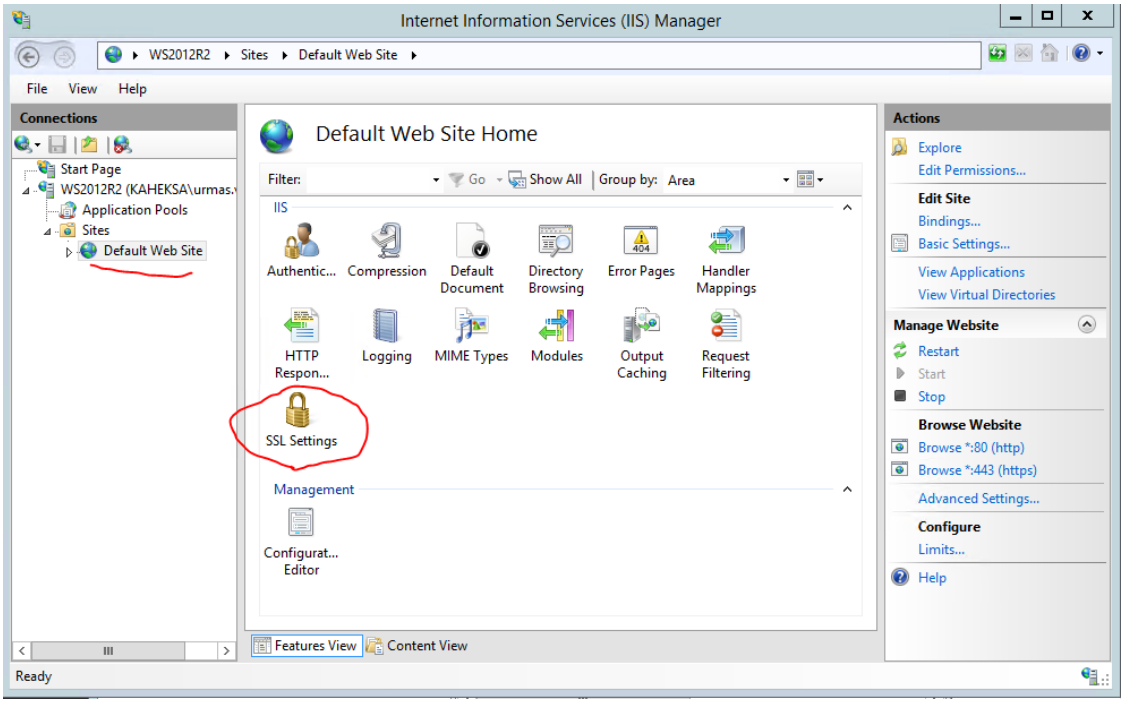


Figure 24 - *SSL Settings button*

Then we can switch on the SSL requirement and the website can no longer be communicated with over HTTP:

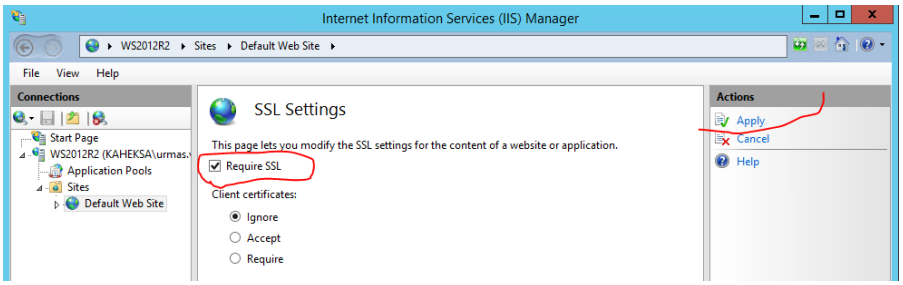


Figure 25 - SSL requirement

Now the site is only available over HTTPS!

Automatic redirecting

IIS makes it easy to redirect automatically from an HTTP site to HTTPS site. This article by Microsoft contains more details http://technet.microsoft.com/en-us/library/cc732969(WS.10).aspx

AUTHENTICATION USING ID-CARD

In addition to the one-way SSL authentication, we can also switch on mutual SSL authentication:

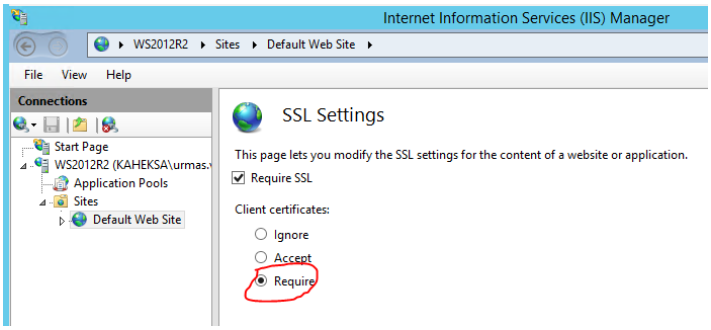


Figure 26 - mutual SSL authentication

In that case, certificate authentication by the web server will also be required. For example, the authentication certificate on the ID-card can be used for this purpose. In order for ID-card authentication to function on web server, we must add the ID-card certificate chain to the web server:

1) Open certificate console on IIS server and browse to the Intermediate Certification Authorities certificates. Add certificate "ESTEID-SK 2011" using the *Import* command:
2) If clients also use certificates issued from "Juur-SK" / "ESTEID-SK 2007" level:
    a. "ESTEID-SK 2007" must also be added to intermediate certificates;
    b. "Juur-SK" to trusted root certificates.

The listed certificates are available from:

1) Root certificate "Juur-SK" : https://sk.ee/upload/files/Juur-SK.der.crt
2) Intermediate certificate "ESTEID-SK 2011" - https://sk.ee/upload/files/ESTEID-SK_2011.der.crt
3) Intermediate certificate "ESTEID-SK 2007" - https://sk.ee/upload/files/ESTEID-SK_2007.der.crt [9]
4) Intermediate certificate "ESTEID-SK 2015" - https://sk.ee/upload/files/ESTEID-SK_2015.der.crt

Other options for using secure web solutions

If the Estonian ID-card certificate is bound to user in AD (for example if ID-login is used[10]), this may also be used for authentication on the website[11]. However, these cases depend on the exact configuration and needs and it is difficult to provide general guidelines.

[9] Valid until 26 August 2016.
[10] Also see http://www.sk.ee/upload/files/ID-login_juhend.pdf
[11] Web server additional properties installation is required.