SK WEB CERTIFICATE CONFIGURATION, IIS 8

Specifications



TABLE OF CONTENTS

Introduction
Creating a certificate request2
Order5
Certificate installation
Preparation
Non-domain environment6
Windows domain environment10
IIS server configuration if client certificate does not have a complete chain
Client configuration
Web certificate installation
Permitting SSL
Results
Potential issues
Additional options
SSL requirement
Automatic redirecting
Authentication using ID-card
Other options for using secure web solutions17



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:



8]	Interne	et Information Services (IIS) Manager		_ 🗆 X
					ど 🐼 🚱 •
File View Help					
Connections	Server Certifica Use this feature to request and m configured for SSL. Filter: Name	tes anage certificates that the Web s Go - Show All Group by Issued To WS2012R2.Kaheksa.XI	erver can use with websites No Grouping Issued By Kaheksa XI 2012	E 1	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate Enable Automatic Rebind of Renewed Certificate P Help
Ready					• <u>1</u> .:

Figure 2 - selecting create new certificate request file

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

Request Certificate ? ×								
Distinguished Name Properties								
Specify the required information official names and they can	Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.							
Common name:	WS2012R2Kaheksa.XI							
Organization:	Kaheksa XI							
Organizational unit:	DEV							
City/locality	EST							
State/province:	EST							
Country/region:	EE v							
	Previous Next Finish Cancel							

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 <u>https://WS2012R2.Kaheksa.XI</u>

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



Request Certificate	? X
Cryptographic Service Provider Properties	
Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.	
Cryptographic service provider:	
Bit length:	
Previous Next Finish Ca	ncel

Figure 4 - adjusting certificate properties

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

Request Certificate	?)	C
File Name			
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.			
C:\Temp\SKCR.txt			
Draviour Next Finish	Canco	1	1
Previous Next Finish	Cance]

Figure 5 - saving the CSR

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

				SKCR -	Notepa	ad			-		X	:
File	Edit Format	View He	lp									
	-BEGIN NEW	CERTIF	ICATE	REQUES	T							^
MIIE	XjCCAØYCAQ	AwajELM	AkGA1L	JEBhMCR	UUxDDA	KBgNVBA	gMA0VT\	/DEMM	AoG/	1UE		
BwwD	RVNUMRMwEQ	YDVQQKD	ApLYW	nla3NhI	FhJMQw	vCgYDVQ	QLDANEF	RVYxH	DAat	BgNV		
BAMM	E1dTMjAxM1	IyLktha	GVrc2E	EuWEkwg	gEiMA00	GCSqGSI	b3DQEB4	AQUAA	41B0	DwAw		
ggEK	AoIBAQC47s	1YUiOsK	1qN8Kc	γwQ7YRP	0GDzmx	JEiC6lt	Dpa8y6F	R9BBm	nSN]	ILZ		
hoZI	uKr11K9h5d	lsojV2r5	z//3Lp	VtUb75	ek9iJ+	hGpiFXW	RZnqie/	/X/mA	6Dz2	ZXwJ		
xIbQ	Mnr6hKiKmz	krFXrYP	/9W65c	:lcRyhl	.pfpPpZ(QH0rHyR	j/JvYG4	\uUoR	A/21	IfUC		
wQkG	1I0w5qJ2Vf	feXFkeY	bNDC/i	LCZt0Df	ramBeDO	C1xK83Q	MBLxJme	EZpP	UeJl	(0Y4		
Aivr	60BCXsxodk	q54mZOS	zvghF⊮	vZH14Gj	ssPZhvl	V95fxSv	4t7Fhv0	G4Cii	ID3v	v8Zy		
Li86	7bMaqUDitl	./ZnwcXf	ggxgVz	z/UKCzA	gMBAAG	gggGtMB	oGCisG4	4QQBg	jcN/	٩gМx		
DBYK	Ni4yLjkyMD	AuMjBJB	gkrBgE	EAYI3F	RQxPDA	5AgEFDB	NXUzIw	ITJSM	i5L\	/Whl		
a3Nh	L1hJDBNLQU	hFS1NBX	HVybWF	zLnZhb	mVtDAt	JbmV0TW	dyLmV42	ZTByB	gorE	BgEE		
AYI3	DQICMWQwYg	IBAR5aA	EØAaQE	BjAHIAb	wBzAG8/	AZgBØAC	AAUgBT4	AEEAI	ABTA	AEMA		
aABh	AG4AbgB1AG	WAIABDA	HIAeQE	Bwahqad	wBnAHI	AYQBwAG	gAaQBj4	ACAAU	ABy/	AG8A		
dgBp	AGQAZQByAw	EAMIHPB	gkqhki	LG9w0BC	Q4xgcE	vgb4wDg	YDVRØP#	AQH/B	AQD/	4gTw		
MBMG	A1UdJQQMMA	oGCCsGA	QUFB₩M	ABMHgGC	SqGSIb	BDQEJDw	RrMGkwE)gYIK	oZI	nvcN		
AwIC	AgCAMA4GCC	qGSIb3D	QMEAg1	[AgDALB	glghkgl	BZQMEAS	οωϹωϒϽ	IZIA	WUDE	BAEt		
MAsG	CWCGSAF1Aw	QBAjALB	glghkg	gBZQMEA	QUwBwYI	FKw4DAg	cwCgYI	(oZIh	vcN/	Awcw		
HQYD	VRØOBBYEFF	je0F4sR	DuySvL	.sm3m1V	Y5cvzz	JMAØGCS	qGSIb3D	OQEBB	QUAA	41B		
AQCc	/hjbEJvJhe	H05SFiv	50A+30)xAQrh2	FmYFtv	ADGntBm	r/V5Y/9	9Bklm	HJX2	zNHc		
cXjI	U7XAwinDQZ	HmmS1aj	v8YA16	SIJUHPT	yDFgsZ,	/LjFp41	cdySJ42	ZZaHS	jD69	PPH		
mXwj	5KK4nmcWt9	FxKTt7Q	YlgzSj	jec2TT5	pZo0qn(CASfcjz	qmUR4Sr	15BxY	u/Kı	ıCrY		
dkmu	xwPWOhXXLH	KEdwesj	qJ1WNU	JXxvwHP	5mDUy1	JYr/F0D	bv0/Zbs	sT+eE	tPq]	[WkY		
18tI	qovOz2E110	E2Wg//o	r76hP⊣	⊦eeudmQ	cEXoHT	5bIM/Ok	GJDJj02	22E+e	2915	5Q5S		
2WSK	fdpcJnZKBh	r018+fm	JRm									
	-END NEW C	ERTIFIC	ATE RE	EQUEST -								
												\sim
<											$\left \right\rangle$	

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 <u>https://sk.ee/en/services/ssl-</u>certificates/?service/webserver_ssl¹.

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

Certificate X	Certificate X	Certificate X
General Details Certification Path	General Details Certification Path	General Details Certification Path
Certificate Information	Show: <al></al>	Certification path
This certificate is intended for the following purpose(s):	Version V3	WS2012R2.Kaheksa.xl
Ensures the identity of a remote computer	🔄 Serial number 1e be 38 29 62 5a a0 ec 56 44 ≡	
	Signature algorithm sha256RSA	
	Signature hash algorithm sha256	
	Issuer TEST of KLASS3-SK 2010, Sert	
	Valid from 12. november 2015 13:41:04	
* Refer to the certification authority's statement for details.	Valid to 12. november 2018 13:41:04	
Issued to: WS2012R2.Kaheksa.xl	Subject WS2012R2.Kaheksa.xd, DEV, V	
Issued by: TEST of KLASS3-SK 2010		View Certificate
Valid from 12.11.2015 to 12.11.2018		
		Certificate status:
		This certificate is OK.
Instal Certificate Issuer Statement	Edit Properties Copy to File	
ОК	ОК	ОК

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 <u>https://sk.ee/en/repository/conditions-for-use-of-certificates/</u>



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" <u>https://sk.ee/upload/files/KLASS3-</u> <u>SK_2010_EECCRCA_SHA384.pem.crt</u>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+M³, 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

-		Console1	- [Console Root]	_ 🗆 X	
🚰 File 🛛	Action View Favorites W	indow Help		_ & ×	
Consol	e Root Name e Root Name You can select snap-ins for i extensible snap-ins, you can Available gnap-ins: Snap-in ActiveX Control ActiveX	Add this console from those ava configure which extension Microsoft Cor Microsoft Cor	d or Remove Snap-ins ilable on your computer and configure the selects is are enabled. Selected snap-ins: Console Root Certificate Certificates My user account Service account Computer account	Actions	X
				< Back Next >	Cancel

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.

Select Computer	x					
Select the computer you want this snap-in to manage. This snap-in will always manage:						
O Another computer: Browse						
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.						
< Back Finish Ca	ancel					



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

⁵Intermediate Certification Authorities



Figure 11 - certificate selection

Sertificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
O Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Intermediate Certification Authorities Browse
Next Cancel

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*"⁶⁷:

 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.

🧃 Group Policy Management Editor 📃 🗖 🗙								
File Action View Help								
Account Policies	^	Issued To 📩	Issued By					
Local Policies		EE Certification Centre Root CA	EE Certification Centre Root CA					
Event Log								
Restricted Groups								
System Services								
Registry								
File System								
Wired Network (IEEE 802.3) Policies								
Windows Firewall with Advanced Security								
Network List Manager Policies								
Wireless Network (IEEE 802.11) Policies	=							
Public Key Policies								
Encrypting File System								
Data Protection								
BitLocker Drive Encryption								
BitLocker Drive Encryption Network Unloc								
Automatic Certificate Request Settings								
Trusted Root Certification Authorities								
Enterprise Trust								
Trusted Bublishers								
Intrusted Publishers								
Trusted People								
Software Restriction Policies	$\overline{\mathbf{v}}$							
	1	<	>					
Trusted Root Certification Authorities store contains 1 certificate		<u> </u>						

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 :

ġ		_ 🗆 X					
File	Edit	View Favorites Help					
		Name Type ScEvents Image: Construction of the sector of t	Data (value not set) 0x00000001 (1) 0x00000000 (0)				
<	:		>				
Com	Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL						

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:

Complete Certificate Request ? X
Specify Certificate Authority Response
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.
File name containing the certification authority's response:
C:\Temp\ws2012r2.cer
Friendly name:
SK SSL sertifikaat
Salact a cartificate store for the new cartificate
Personal Y
1 Coontra
OK Cancel

Figure 18 - certificate selection and setting friendly name

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



8)	Interr	net Information Services	(IIS) Manager		_ D X
ⓒ ○ ♥ WS2012R2 ▶					🖸 🛛 🟠 🔞 🗸
File View Help					
Connections	Server Certific. Use this feature to request and r configured for SSL. Filter:	ates manage certificates that the We Go V Show All Group Issued To WS2012R2.Kaheksa.XI WS2012R2.Kaheksa.xI	b server can use with websites by: No Grouping Issued By Kaheksa XI 2012 TEST of KLASS3-SK 2010	E 1 1	Actions Import Create Certificate Request Complete Certificate Request Create Domain Certificate Create Self-Signed Certificate View Export Renew Renew Renewed Enable Automatic Rebind of Renewed Certificate Relp Help
	< III	ew		>	
Ready					•1.:

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:

€j	Internet Information Services (IIS) Manager	_ 🗆 X
€ • WS2012R2 • S	ites 🕨 Default Web Site 🍑	😰 🖾 🟠 i 😧 🗸
File View Help		
Connections Start Page Start Page WS2012R2 (KAHEKSA\urmas. WS2012R2 (KAHEKSA\urmas. Default Web Site	Default Web Site Home Filter: • • •	Actions
< III >	Features View 💦 Content View	
Ready		¶.:

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):

			Site	Bindings	? X
Type http	Host Name	Port 80	IP Address *	Binding Informa	Edit Remove Browse
/pe: ttps ost name:	Ade IP address: V All Unassigned	d Site Bindin	9 Port: v 443	2 *	
Kequire se		~	Select	View	
			Site	Bindings	?)
Type http https	Host Name	Port 80 443	IP Address * *	Binding Informa	Add Edit
	-	~			Remove Browse
					Close

Figure 22 - Permitting https

Now, the website can be communicated with using the name <u>https://ws2012r2.kaheksa.xi⁸</u>

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":



V	Internet Information Services (IIS) Manager	_ 🗆 X
(€) (€) WS2012R2 → Sites → Default Web Sites	te 🕨	📴 🖂 🔞 🗸
File View Help		
Connections	Web Site Home	Actions
Start Page WS2012R2 (KAHEKSA\urmas)	🗸 🐺 Go 👒 🕁 Show All Group by: Area	Edit Permissions
Application Pools	9	Edit Site Bindings Basic Settings
Default Web Site Muthentic Comp	ession Default Directory Error Pages Handler Document Browsing Mappings	View Applications View Virtual Directories
] 🏂 📬 🎼	Manage Website
HTTP Log Respon	ging MIME Types Modules Output Request Caching Filtering	Image: Start Image: Start
		Stop
SSL Settings		Browse *:80 (http) Browse *:443 (https)
Management		Advanced Settings
Configurat		Configure Limits
Editor		Help
C III > Features View	Content View	
ready		*1 .:

Figure 24 - SSL Settings button

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

<i>6</i> ³	Internet Information Services (IIS) Manager	_ _ ×
€ • WS2012R2 •	Sites Default Web Site	🐷 🗟 🖗 •
File View Help		
Connections	SSL Settings This page lets you modify the SSL settings for the content of a website or application. Client certificates: G Ignore Accept Require	Actions



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 <u>http://technet.microsoft.com/en-us/library/cc732969(WS.10).aspx</u>

AUTHENTICATION USING ID-CARD

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

8	Internet Information Services (IIS) Manager
	Sites 🔸 Default Web Site 🔺
File View Help	
Connections	SSL Settings This page lets you modify the SSL settings for the content of a website or application. Require SSL Client certificates: Ignore Accept Require

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

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 used¹⁰), this may also be used for authentication on the website¹¹. 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 <u>http://www.sk.ee/upload/files/ID-login_juhend.pdf</u>

¹¹ Web server additional properties installation is required.