Setting up MS Internet Explorer on Windows Vista

1. Installing root certificates from SIGEN-CA and SIGOV-CA, the certification authorities at the Ministry of Public Administration

The SIGEN-CA and SIGOV-CA root certificates must be installed to prevent warnings about suspicious certification authorities (CAs) when accessing public administration applications. The two certificates are not pre-installed in the browser.

a) Installing the SIGEN-CA root certificate

Install the SIGEN-CA root certificate in the 'Trusted Root Certification Authorities' by clicking on the following link: <u>http://www.sigen-ca.si/sigen-ca.crt</u>.

After the browser prompts you whether to Open or Save the file, click 'Open'.

File Download - Security Warning						
Do you want to open or save this file?						
	Name: sigen-ca.cer Type: Security Certificate, 1,02KB From: www.sigen-ca.si					
	Open Save Cancel					
۲	While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. <u>What's the risk?</u>					

A security message appears. Click 'Allow'.

Internet I	Explorer Security	×
1	A website wants to open web content using this program on your computer	
	This program will open outside of Protected mode. Internet Explorer's <u>Protected mode</u> helps protect your computer. If you do not trust this website, do not open this program.	
	Name: Crypto Shell Extensions Publisher: Microsoft Windows	
	Do not show me the warning for this program again	
ତ	Details Don't allo	w

The Certificate Import Wizard is launched. Click 'Next'.



In the 'Certificate Store' window select 'Place all certificates in the following store', then click 'Browse' and select 'Trusted Root Certification Authorities'. Click 'Next'.

Certificate Import Wizard	x
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.	
\bigcirc Automatically select the certificate store based on the type of certificate	
<u> </u>	
Certificate store:	
Trusted Root Certification Authorities Browse	
Learn more about <u>certificate stores</u>	
< <u>B</u> ack <u>N</u> ext > Cance	

Complete the procedure by clicking 'Finish'.

Certificate Import Wizard				
	Completing the Certificate Import Wizard			
	The certificate will be imported after you click Finish.			
	You have specified the following settings:			
	Certificate Store Selected by User Trusted Root Certifica Content Certificate			
	4			
	< <u>B</u> ack Finish Cancel			

A security warning appears, containing information about the SIGEN-CA root certificate.



Make sure that the thumbprint (sha1) in the warning message matches the one on the picture above, i.e.:

3E42A187 06BD0C9C CF594750 D2E4D6AB 0048FDC4

After clicking '**Yes**' you will receive a confirmation the installation of the SIGEN-CA root certificate has been successful.

b) Installing the SIGOV-CA root certificate

Now install the SIGOV-CA root certificate, which issues server hostkey certificates to Government servers. The procedure is identical to installing the SIGEN-CA certificate. Begin by clicking on <u>http://www.sigen-ca.si/sigov-ca.crt</u>.

After the browser prompts you whether to Open or Save the file, click '**Open**'. The Certificate Import Wizard is launched. Click '**Next**'.

In the 'Certificate Store' window select 'Place all certificates in the following store', then click 'Browse' and select 'Trusted Root Certification Authorities'. Click 'Next'. Confirm your selection by clicking 'Finish'.

A security warning appears, containing information about the SIGOV-CA root certificate.

Security W	'arning	×
<u> </u>	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	sigov-ca	
	Windows cannot validate that the certificate is actually from "sigov-ca". You should confirm its origin by contacting "sigov-ca". The following number will assist you in this process:	
	Thumbprint (sha1): 7FB9E2C9 95C97A93 9F9E81A0 7AEA9B4D 70463496	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	
	Yes No	

Make sure that the thumbprint (sha1) in the warning message matches the one picture above, i.e.:

7FB9E2C9 95C97A93 9F9E81A0 7AEA9B4D 70463496

After clicking **'Yes'** you will receive a confirmation the installation of the SIGOV-CA root certificate has been successful.

If you open the 'Trusted Root Certification Authorities' folder, you will see that it contains both certificates. To open the folder click 'Tools' -> 'Internet Options' -> 'Content' -> 'Certificates'.

Certificates				X				
I <u>n</u> tended purpose: <a>A	>			•				
Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publ								
Issued To	Issued By	Expiratio	Friendly Name	•				
Copyright (c) 1997 GTE CyberTrust Glo Microsoft Authentic Microsoft Root Aut Microsoft Root Cert NO LIABILITY ACC sigen-ca sigov-ca Thawte Premium Se	Copyright (c) 1997 Mi GTE CyberTrust Globa Microsoft Authenticod Microsoft Root Authority Microsoft Root Certifi NO LIABILITY ACCEP sigen-ca sigov-ca . Thawte Premium Serv	30.12.1999 13.8.2018 31.12.1999 31.12.2020 9.5.2021 7.1.2004 29.6.2021 10.1.2021 31.12.2020	Microsoft Timest GTE CyberTrust Microsoft Authe Microsoft Root A Microsoft Root C VeriSign Time St <none> <none> thawte</none></none>	4				
Import Export	es		<u>A</u> dva <u>V</u> iew	nced				
Learn more about <u>certificate</u>	<u>s</u>		Clo	se				

With the certificates installed and a secure HTTPS connection established to any server that uses a digital certificate from the certification authorities at the Ministry of Public Administration, the URL bar should be white and without warnings.

🥻 Ministrstvo za javno upravo R5 - SIGEN-CA - Windows Internet Explorer	
😋 💽 👻 🔛 https://www.sigen-ca.si/	• 🔒 ++ 🗙
🚖 🍄 🏭 Ministrstvo za javno upravo RS - SIGEN-CA	6
Overitelj digitalnih potro Ministrstvo za	sii Si a javno upr

If this does not happen, close and reopen the web browser, so that it identifies the two new certificates as trusted.

2. Making the e-Uprava web site a trusted site

In the menu select 'Tools' -> 'Internet Options' -> 'Security'

In the 'Trusted Sites' tab select **'Sites'**, and add the addresses of e-Uprava servers you wish to access. We recommend you to add the following URLs:

- <u>https://gov.si</u> (displayed as an additional domain https://*.gov.si)
- https://sigen-ca.si
- <u>https://durs.si</u>

We also recommend you to add <u>http://gov.si</u> (displayed as <u>http://*.gov.si</u>), to avoid annoying browser warning messages when the connection is switched between http and https. To do this, first uncheck the box at the bottom ('Require server verification (https:) for all sites in this zone'). Once you have added the URL <u>http://gov.si</u>, check the box so as to prevent the possibility of unintentionally adding unverified servers among trusted ones.

Internet (ptions					8 🛛
General	Security	Privacy	Content	Connections	Programs	Advanced
Select	a zone to v	iew or cha	ange securi	ty settings.		
	2				0	
Int	ærnet L	ocal intrar	net Trust	ed sites Re	estricted sites	
	Trustee	sites				
Tru	sted sites					X
Ac	You of this z dd this webs http://gov.s	an add ai one will u ite to the i	nd remove se the zone zone:	websites from e's security se	this zone. ttings.	All websites in Add
	nttp://*.gov nttps://*.du nttps://*.go	/.si irs.si iv.si				Remove
	Require se	rver verif	ication (ht	ps:) for all site	es in this zo	ne
						Close

3. Protocol settings

In the menu select 'Tools' -> 'Internet Options' -> 'Advanced'

Uncheck the box next to 'Use TLS 1.0' and click 'OK'.

Internet O	ptions					? <mark>X</mark>		
General	Security	Privacy	Content	Connections	Programs	Advanced		
Setting	s]		
	 Enable Integrated Windows Authentication* Enable memory protection to help mitigate online attacks Enable native XMLHTTP support Phishing Filter Disable Phishing Filter Turn off automatic website checking Turn on automatic website checking Use SSL 2.0 Use SSL 3.0 Use TLS 1.0 Warn about certificate address mismatch* Warn if changing between secure and not secure mode Warn if POST submittal is redirected to a zone that does n 							
•			III			P.		
*Tal	kes effect a	after you i	restart Inte	ernet Explorer				
				Restore	advanced s	settings		
Reset I	Reset Internet Explorer settings							
Deletes all temporary files, disables browser add-ons, and resets all the changed settings.								
You	You should only use this if your browser is in an unusable state.							
L			Ok	Ci	ancel	Apply		

This setting prevents the browser from using the above-mentioned protocol, which some e-Uprava servers do not support.