Priprava brskalnika MS Internet Explorer na operacijskem sistemu Windows Vista

1. Vključitev korenskih potrdil izdajateljev SIGEN-CA in SIGOV-CA overitelja na MJU

V brskalnik je potrebno najprej vključiti korenski potrdili izdajateljev SIGEN-CA in SIGOV-CA, da se tako izognete opozorilom o sumljivih izdajateljih potrdil pri dostopu do aplikacij javne uprave. Ti dve potrdili namreč nista že vnaprej naloženi v brskalnik.

a) Namestitev korenskega potrdila izdajatelja SIGEN-CA

Postopek vključitve korenskega potrdila SIGEN-CA v shrambo zaupanja vrednih izdajateljev začnete s klikom na <u>http://www.sigen-ca.si/sigen-ca.crt</u>.

Brskalnik vpraša, ali naj datoteko s potrdilom shrani ali odpre -- izberete "Open":

File Down	load - 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>			

Pokaže se varnostno opozorilo, kliknete na Dovoli (Allow).



Zažene se čarovnik za uvoz potrdil - kliknete Naprej (Next).



Izberete "Namesti vse certifikate v sledečo shrambo" (Place all certificates in the following store) in izberete "Zaupanja vredni izhodiščni certifikatni uradi" (Trusted Root Certification Authorities) v oknu "Izberi shrambo s certifikati" (Certificate Store) in kliknete Naprej (Next).

Certificate 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.
\bigcirc Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities Browse
Learn more about <u>certificate stores</u>
< <u>B</u> ack <u>N</u> ext > Cancel

Še enkrat se pokaže naš izbor shrambe za korensko potrdilo - kliknemo na Dokončaj (Finish).

Certificate Import Wizard				
	Completing the Certifi Wizard	ig the Certificate Import		
	The certificate will be imported after	r you click Finish.		
	You have specified the following set	tings:		
	Certificate Store Selected by User Content	Trusted Root Certifica Certificate		
	۲ III	4		
	< <u>B</u> ack F	inish Cancel		

Pokažejo se vam podatki o korenskem potrdilu izdajatelja SIGEN-CA:

Security Wa	arning	×		
<u>^</u>	'ou are about to install a certificate from a certification authority (CA) laiming to represent: igen-ca Vindows cannot validate that the certificate is actually from "sigen-ca". 'ou should confirm its origin by contacting "sigen-ca". The following number will assist you in this process: 'humbprint (sha1): 3E42A187 06BD0C9C CF594750 D2E4D6AB			
	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?	is root certificate, Windows will automatically trust any d by this CA. Installing a certificate with an unconfirmed security risk. If you click "Yes" you acknowledge this		
	<u>Y</u> es <u>N</u> o			

Preverite, da je razpoznavni odtis (sha1), ki ga vidite v opozorilu, enak nizu na zgornji sliki, torej:

3E42A187 06BD0C9C CF594750 D2E4D6AB 0048FDC4

Potem kliknete na gumb "Da" in dobite obvestilo, da ste potrdilo izdajatelja SIGEN-CA uspešno namestili.

b) Namestitev korenskega potrdila izdajatelja SIGOV-CA

Zdaj namestite še korensko potrdilo izdajatelja SIGOV-CA, ki izdaja potrdila strežnikom državnih organov. Postopek je enak kot za namestitev korenskega potrdila SIGEN-CA.

Začnete ga s klikom na spletno stran: <u>http://www.sigen-ca.si/sigov-ca.crt</u>. Brskalnik vpraša, ali naj datoteko s potrdilom shrani ali odpre -- izberemo "Open". Zažene se čarovnik za uvažanje certifikatov. Izberete "Namesti vse certifikate v sledečo shrambo" (Place all certificates in the following store) in izberete "Zaupanja vredni izhodiščni certifikatni uradi" (Trusted Root Certification Authorities) v oknu "Izberi shrambo s certifikati" (Certificate Store) in kliknete Naprej (Next).

Potrdite izbrane možnosti s klikom na gumb "Dokončaj". Pokažejo se podatki o potrdilu izdajatelja SIGOV-CA:



Preverite, da je razpoznavni odtis (sha1), ki ga vidite v opozorilu, enak nizu na zgornji sliki, torej:

7FB9E2C9 95C97A93 9F9E81A0 7AEA9B4D 70463496

Potem kliknete na gumb "Da" in dobite obvestilo, da ste potrdilo izdajatelja SIGOV-CA uspešno namestili.

Če zdaj odprete shrambo zaupanja vrednih izdajateljev (oziroma izhodiščnih certifikatnih uradov, kot so prevedli pri MS), v njej vidite obe potrdili:

Certificates				X
Intended purpose: <a>				•
Intermediate Certification Au	thorities Trusted Root Ce	ertification Aut	horities Trusted Pub	4 >
Issued To	Issued By	Expiratio	Friendly Name	
Copyright (c) 1997 GTE CyberTrust Glo Microsoft Authentic Microsoft Root Aut Microsoft Root Cert NO LIABILITY ACC	Copyright (c) 1997 Mi GTE CyberTrust Globa Microsoft Authenticod Microsoft Root Authority Microsoft Root Certifi NO LIABILITY ACCEP sigen-ca	30.12.1999 13.8.2018 31.12.1999 31.12.2020 9.5.2021 7.1.2004 29.6.2021	Microsoft Timest GTE CyberTrust Microsoft Authe Microsoft Root A Microsoft Root C VeriSign Time St <none></none>	III
Thawte Premium Se	sigov-ca Thawte Premium Serv	10.1.2021 31.12.2020	<none> thawte</none>	-
Import Export Certificate intended purpose	<u>R</u> emove		<u>A</u> dvar	nced
Learn more about <u>certificates</u>			Clos	se

Orodja (Tools) -> Internetne možnosti (Internet options) -> Vsebina (Content) -> Certifikati (Certificates)

Zdaj bi morala biti naslovna vrstica ob varni priključitvi (prek https) na katerikoli strežnik, ki uporablja digitalno potrdilo Overitelja na MJU, bela in brez opozoril:

🖉 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 p Ministrstv	otrdil Si o za javno upr				

Če ni tako, brskalnik zaprite in ga ponovno zaženite. Tako ga prisilite, da bo pravkar vključeni potrdili zaznal kot zaupanja vredni.

2. Vključitev strani e-Uprave med zaupanja vredne strani

Iz menija izberemo "Orodja" ->"Internetne možnosti"->"Varnost" (Tools -> Internet Options - > Security)

Izberemo zavihek Zaupanja vredne strani (Trusted sites), izberemo strani (Sites) in dodamo naslove strežnikov e-uprave za aplikacije, do katerih boste dostopali. Priporočamo, da dodate naslednje naslove URL:

- https://gov.si (kar se prikaže kot dodana domena https://*.gov.si)
- https://sigen-ca.si
- https://durs.si

Dodatno priporočamo, da dodate http://gov.si (kar se vidi kot http://*.gov.si), da se izognete nadležnemu opozarjanju brskalnika ob prehajanju med https in http povezavami. Za to pa morate najprej izključiti kljukico spodaj ob "Require Server Verification (https:)...". Ko ste dodali http://gov.si, možnost preverjanja strežnikov spet vključite, da ne bi kdaj kasneje nehote dodali nepreverjenih strežnikov med zaupanja vredne.

Internet Options	? 🛛			
General Security Privacy Content Connections Progra	ams Advanced			
Select a zone to view or change security settings.				
🛛 🎱 🔩 🗸 🚫				
Internet Local intranet Trusted sites Restricted sites				
Trusted sites				
Trusted sites	×			
You can add and remove websites from this zor this zone will use the zone's security settings. Add this website to the zone: http://gov.si	ne. All websites in			
Websites:				
http://*.gov.si	Remove			
https://*.durs.si				
https://*.gov.si				
https://*.sigen-ca.si				
Require server verification (https:) for all sites in this zone				
	Close			

3. Nastavitev ustreznih protokolov

Iz menija izberemo "Orodja" ->"Internetne možnosti"->"Napredno" (Tools -> Internet Options -> Advanced)

Pred zapisom "Uporabi TLS 1.0" (Use TLS 1.0) izbrišemo kljukico in kliknemo na gumb "OK".

Internet Options						
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 						
•			111			•
*Ta	kes effect a	after you	restart Int	ernet Explore	r	
				Restor	e advanced s	settings
Reset I	internet Ex	plorer set	tings			
Deletes all temporary files, disables browser add-ons, and resets all the changed settings.						
You should only use this if your browser is in an unusable state.						
OK Cancel Apply						

S to nastavitvijo prisilimo brskalnik, da za povezavo ne uporablja zgoraj omenjenega protokola, ker ni ustrezno podprt na nekaterih strežnikih e-Uprave.