Nadgradnja varnostnih elementov storitve eDavki

Portal eDavki za zagotavljanje varne komunikacije med brskalnikom zavezanca in strežniki eDavki uporablja protokol SSL (Secure Sockets Layer). Za zagotavljanje višjega nivoja varnosti bo Finančna uprava 01.09.2017 implementirala kriptografski protokol TLS (Transport Layer Security) 1.2. Protokol TLS 1.2 omogoča višji nivo varnosti medmrežne komunikacije in je njegova uvedba nujna za doseganje visokega nivoja varnosti elektronskega poslovanja zavezancev s FURS.

Za večino zavezancev nadgradnja na protokol TLS 1.2 ne bo imela vpliva pri dostopu do portala eDavki. Problemi bodo nastali pri zavezancih, ki uporabljajo stare operacijske sisteme (Windows XP ali starejši) ali stare verzije brskalnikov, ki ne podpirajo TLS1.2, saj bo le-tem onemogočen dostop do portala eDavki. Posledično pozivamo vse tiste zavezance, ki imajo ali zastareli operacijski sistem ali stare verzije brskalnikov, da izvedete ustrezne nadgradnje programske opreme, da boste po 31.8.2017 lahko nemoteno vstopali v portal eDavki.

Zavezancem, ki bodo kljub zgornjim priporočilom uporabljali operacijski sistem Windows XP predlagamo, da za delo v sistemu eDavki uporabljajo brskalnik Firefox (verzijo 52 ESR), katerega bo organizacija Mozilla podpirala do nadaljnjega. Namestitev izvedete na <u>tej strani</u>. Novosti lahko spremljate na njihovi <u>spletni strani</u>.

1. V primeru, da vam pri odpiranju strani <u>http://edavki.durs.si</u> javi napako "Secure Connection Failed" ali "Te strani ni mogoče prikazati", preverite ali vaš brskalnik omogoča varnostni protokol TLS 1.2 (za nastavitev glej navodila pod točko 2).

()	Secure Connection Failed
	An error occurred during a connection to edavki.durs.si. Peer using unsupported version of security protocol. Error code: SSL_ERROR_UNSUPPORTED_VERSION
	• The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
	• Please contact the website owners to inform them of this problem.
	Learn more
	Report errors like this to help Mozilla identify and block malicious sites
	It looks like your network security settings might be causing this. Do you want the default settings to be restored?
	Restore default settings

Te strani ni mogoče prikazati

V oknu »Dodatne nastavitve« vklopite TLS 1.0, TLS 1.1 in TLS 1.2 ter se nato znova poskusite povezati s spletnim mestom **https://beta.edavki.durs.si** . Če te težave ne morete odpraviti, obstaja verjetnost, da se na tem spletnem mestu uporablja nepodprt protokol ali zbirka šifre, na primer RC4 (povezava do podrobnosti), ki se ne upošteva kot varna. Obrnite se na svojega skrbnika spletnega mesta.

Spremeni nastavitve

2. Kako omogočiti TLS 1.2 v brskalniku

- 2.1.Microsoft Internet Explorer
- 1. Odprite Internet Explorer
- 2. V menijski vrstici kliknite **Orodja** → **Internetne možnosti**

eDavki - P × 🗈 🏠 📩					
Natisni	7				
Datoteka	→				
Povečava (95%)	→				
Varnost	→				
Dodaj spletno mesto v pogled programov					
Prikaži prenose Ctrl-	+J				
Upravljanje dodatkov	- 1				
F12 – Orodja za razvijalce	- 1				
Pojdi na pripeta spletna mesta	- 1				
Nastavitve združljivostnega pogleda					
Prijavi težave s spletnim mestom					
Internetne možnosti					
Vizitka					

3. Kliknite na zavihek **Dodatno** → Pomaknite se navzdol do kategorije **Varnost** in ročno označite možnosti Uporabi TLS 1.1 in Uporabi TLS 1.2

Splošno	Varnost	Zasebnost	Vsebina	Povezave	Programi	Dodatno		
Nastav	itve —							
	Varnost					^		
	V Omogo	ă filter Sma	rtScreen			^		
	Omogo	oči izboljšani	zaščiteni	način*				
	✓ Omogo	oči podporo z	za izvorni	XMLHTTP				
	✓ Omoge	ci shrambo	DOM	prictpocti D	20*			
	000200	ri pri prehod	u iz varne	da v ne var	ni način			
	V Opozor	ri, če se pred	dlog POST	preusmeri	v področje	, ki ne		
	✓ Pošljite	zahteve »D	o Not Tra	ck« spletnin	n mestom,	ki jih o		
	 Prever 	i, ali je možr	na ukinitev	založnikov	ega potrdila	3		
	 Prever 	i, ali so na vi	oljo podpi	si prenesen	ih program	ov		
	Uporat	SSL 2.0						
	✓ Uporat	TIS 10						
	✓ Uporab	TLS 1.1						
	✔ Uporab	TLS 1.2				~		
<		26				>		
*Sp	*Spremembe začnejo veljati po vnovičnem zagonu računalnika							
				Obnov	ri dodatne n	astavitve		
Ponast	avi nastavi	tve program	a Internet	Explorer		-		
Pona	astavi nast	avite Interne	t Explorer	ja na privze	ete Pon	astavi		
nast	avitve.							
To u	iporabite le	e, če brskaln	ika ni več	mogoče up	orabljati.			

- 4. Kliknite V redu
- 5. Zaprite brskalnik in znova zaženite Internet Explorer

2.2 Google Chrome

- 1. Odprite Google Chrome
- 2. Kliknite Alt F in izberite Nastavitve/Settings



3. Pomaknite se navzdol in izberite Dodatno ...

Dodatno 🔺

4. Pomaknite se do razdelka Sistem in kliknite Odpiranje nastavitev strežnika proxy...



5. Izberite jeziček **Dodatno/Advanced** → pomaknite se navzdol do kategorije Varnost, ročno preverite polje za možnosti Uporabi TLS 1.1 in Uporabi TLS 1.2

Nastav	itve					
	Varnost V Omoge Omoge V Omoge V Omoge Opozoi V Opozoi V Posljite V Prever Uporat Uporat V Uporat V Uporat V Uporat	ci filter Sma ci izboljšani ci izboljšani ci podporo : ci shrambo ci shra	artScreen zaščiteni za izvorni DOM everjanje u iz varne dlog POST o Not Tra a ukinitev oljo podpi	način" XMLHTTP ga v ne varr preusmeri ck« spletnim založnikov si preneseni	sp* ni način v področje i mestom, ga potrdil h program	, ki ne ki jih o ov
	vemembe	začnejo vel	ati no uno	vičnam zao	งกม รลดับกล	>
***	remembe	zachejo ver	lan bo and	Obaw	dodatne n	astavitve
*Sp				Obnov	dougane n	
*Sp Ponast	avi nastavi	tve program	a Internet	Explorer	ooodine i	
*Sp Ponast Pona	avi nastavi astavi nast avitve.	tve program avite Interne	a Internet t Explorer	Explorer ja na privze	te Pon	astavi

- 6. Kliknite V redu
- 7. Zaprite brskalnik in znova zaženite Google Chrome

Mozilla Firefox

1. Odprite Firefox

2. V naslovno vrstico vnesite about:config in pritisnite Enter



Odpre se opozorilo "This might void your warranty", za nadaljevanje kliknite "I accept the risk!"

3. V polje Iskanje vnesite tls. Poiščite in dvokliknite na security.tls.version.max

Search: Q tis			
Preference Name	Status	Туре	Value
devtools.remote.tls-handshake-timeout	default	integer	10000
extensions.calomelsslvalidation.tls	default	boolean	false
extensions.calomelsslvalidation.tls.state	default	boolean	false
extensions.calomelsslvalidation.tls_toggle	default	boolean	false
network.http.spdy.enforce-tls-profile	default	boolean	true
network.proxy.proxy_over_tls	default	boolean	true
security.tls.enable_0rtt_data	default	boolean	true
security.tls.insecure_fallback_hosts	default	string	
security.tls.version.fallback-limit	default	integer	3
security.tls.version.max	default	integer	3
security.tls.version.min	default	integer	1
services.sync.prefs.sync.security.tls.version.max	default	boolean	true
services.sync.prefs.sync.security.tls.version.min	default	boolean	true

4. Vrednost nastavite na max. 3 (če že ni nastavljena po defaultu), kar pomeni protokol TLS 1.2 in kliknite OK.

	Enter integer value	×
?	security.tls.version.max	
	8	
	OK Cancel	

5. Zaprite brskalnik in znova zaženite Mozilla Firefox

Apple Safari

TLS 1.1 in TLS 1.2 sta samodejno omogočena v Safari od 7 različice naprej.

***Več o delovanju TLS protokola si lahko ogledati na tej strani.

3. Zahtevana programska oprema

V eDavkih se podpisovanje dokumentov lahko izvaja na enem od naslednjih operacijskih sistemov in brskalnikov, ki jih podpira tudi zadnja različica komponente za elektronski podpis DigSig.

Dne 31.05.2017 smo izdali komponento DigSig 2.0.91.0, ki je ob ustrezni konfiguraciji sistema,

delovala na navedenih okoljih:

- Podprti operacijski sistemi (preverite tudi omejitve v delovanju):
 - o Windows 7 32/64bit
 - o Windows 8.1 32/64bit
 - o Windows 10 32/64bit
 - o Linux Ubuntu 16.04 LTS 32/64bit, 17.04 32/64bit
 - o Linux Fedora 24 25 32/64bit
 - o Mac OS X 10.11.6 10.12.4 64bit
- Podprti brskalniki v operacijskem sistemu Windows (preverite tudi omejitve v delovanju):
 - o Internet Explorer 11
 - o Firefox 52 ESR, 53 54
 - o Chrome 58 59
- Podprti brskalniki v operacijskem sistemu Linux (preverite tudi omejitve v delovanju):
 - o Firefox 52 ESR, 53 54
 - o Chrome 58 59 za 64 bitne operacijske sisteme
- Podprti brskalniki v operacijskem sistemu Mac OS (preverite tudi omejitve v delovanju):
 - o Safari 10
 - o Firefox 52 ESR, 53 54
 - o Chrome 58 59