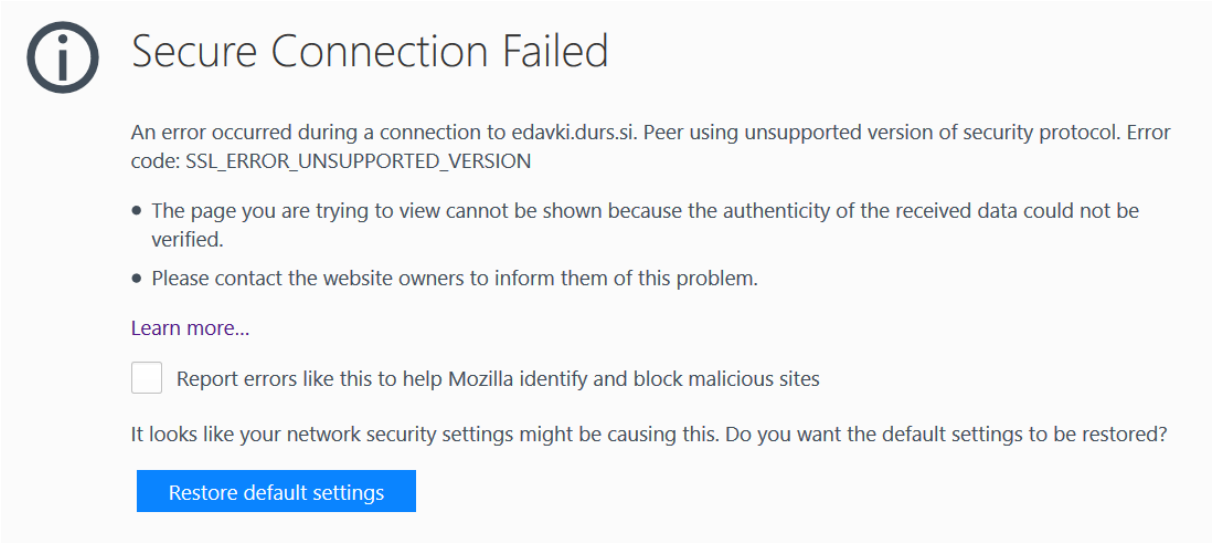
Nadgradnja varnostnih elementov storitve eDavki

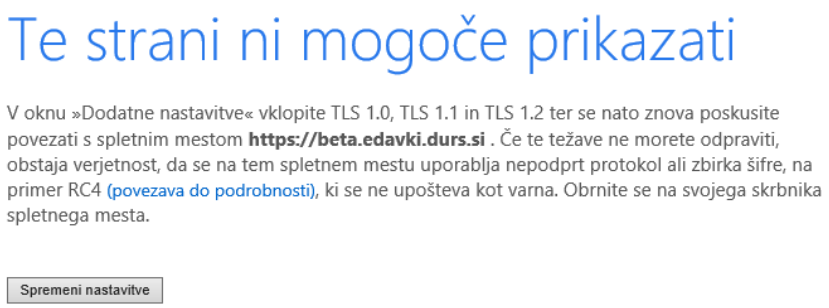
Portal eDavki za zagotavljanje varne komunikacije med brskalnikom zavezanca in strežniki eDavki uporablja protokol SSL (Secure Sockets Layer). Za zagotavljanje višjega nivoja varnosti bo Finančna uprava 01.09.2017 implementirala kriptografski protokol TLS (Transport Layer Security) 1.2. Protokol TLS 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 tej strani. Novosti lahko spremljate na njihovi spletni strani.

1. **V primeru, da vam pri odpiranju strani http://edavki.durs.si 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).**

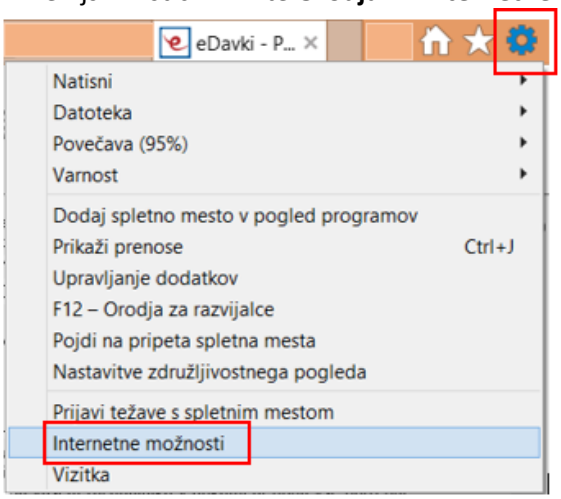




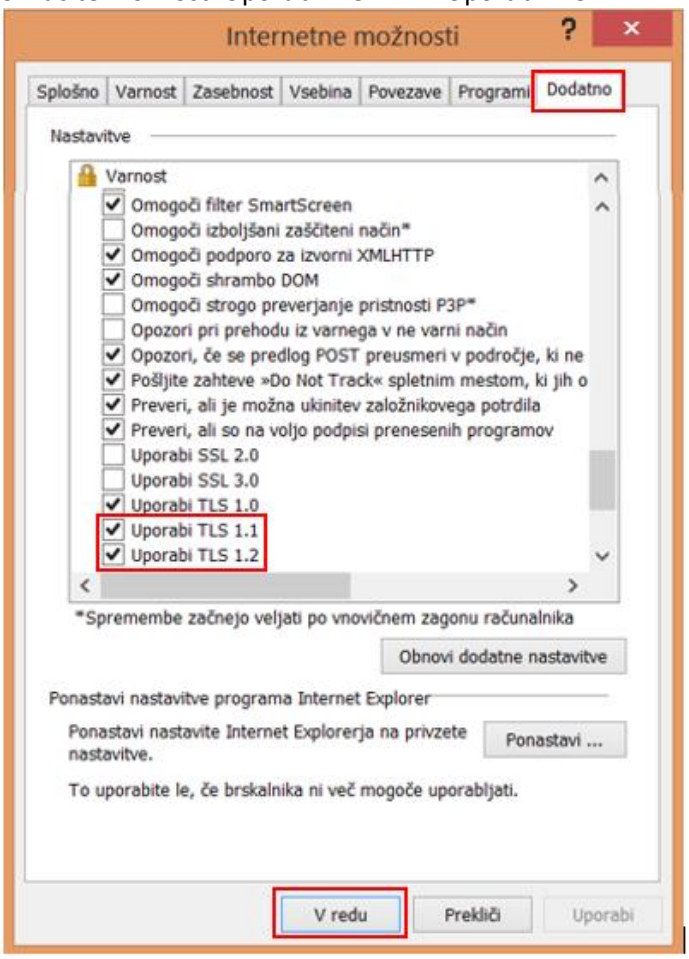
2. Kako omogočiti TLS 1.2 v brskalniku

2.1.Microsoft Internet Explorer

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



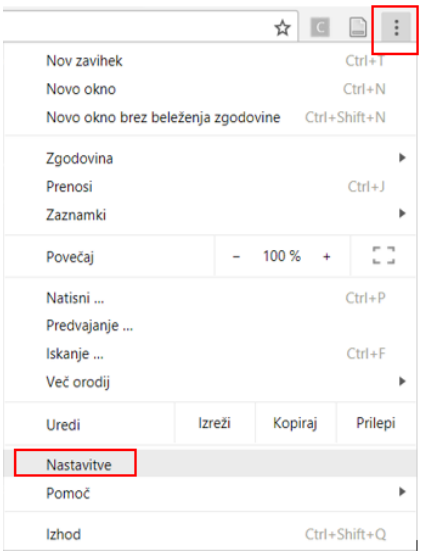
3. Kliknite na zavihek **Dodatno** → Pomaknite se navzdol do kategorije **Varnost** in ročno označite možnosti Uporabi TLS 1.1 in Uporabi TLS 1.2



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

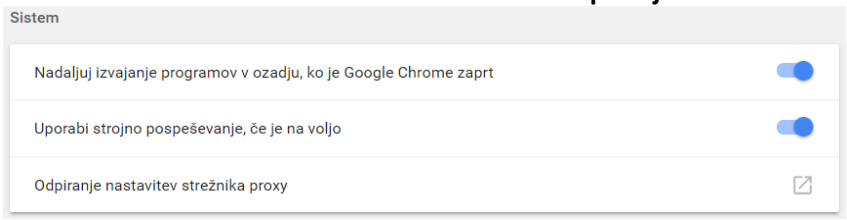
2.2 Google Chrome

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

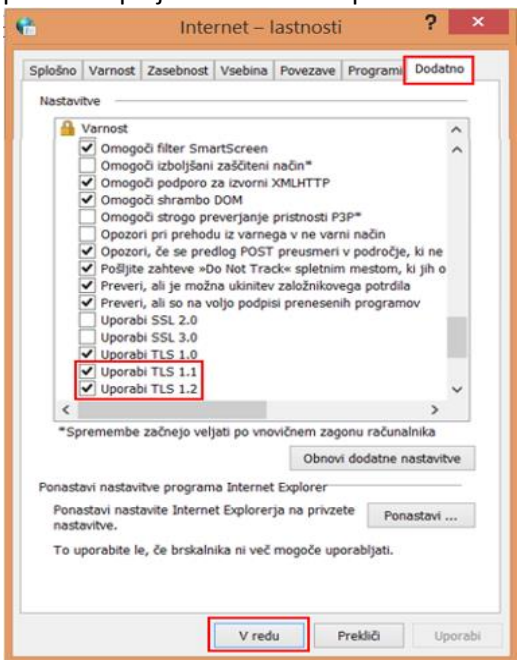


3. Pomaknite se navzdol in izberite **Dodatno** ...

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

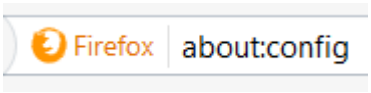


6. Kliknite V redu

7. Zaprite brskalnik in znova zaženite Google Chrome

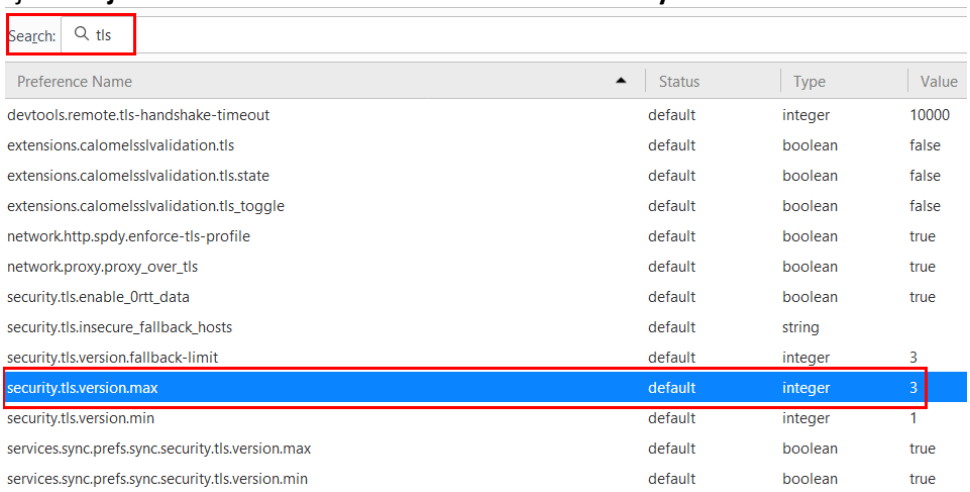
Mozilla Firefox

1. Odprite **Firefox**
2. V naslovno vrstico vnesite **about:config** in pritisnite Enter

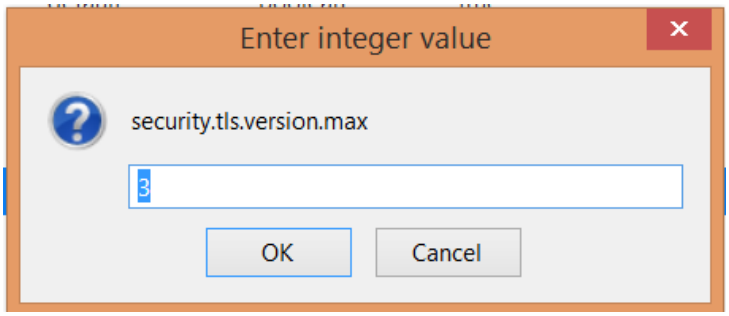


Odpre se opozorilo ˝This might void your warranty˝ , za nadaljevanje kliknite ˝I accept the risk!˝

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



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



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