Naslov dokumenta:	**Razlozi zbog kojih se sertifikat korisnika ne kopira sa smart kartice ili USB tokena u Windows skladište sertifikata i predlozi za rešenje problema**
Verzija:	2.51
Datum:	31.10.2024.
Autor:	Administratori Sertifikacionog tela Pošte

Napomena: Korisničko uputstvo je napisano za rad u operativnom sistemu Windows 10.

Posle instalacije neophodnog softvera i njegove konfiguracije, stavljanjem kartice u čitač smart kartica ili USB tokena u USB port računara, dolazi do automatskog kopiranja sertifikata korisnika u Windows skladište sertifikata. Tek kada je izvršeno navedeno kopiranje sertifikata korisnika, moguće je njegovo korišćenje u okviru različitih aplikacija (Google Chrome, MS Outlook, MS Word, Adobe Reader i druge).

Postoje različiti razlozi zbog kojih se sertifikat korisnika **ne** kopira sa smart kartice ili USB tokena u Windows skladište sertifikata:

1. Čitač smart kartica ili USB token je stavljen u USB port računara koji ne radi.

Predlog za rešenje problema: Čitač smart kartica ili USB token staviti u **ispravan** USB port računara.

2. Smart kartica nije ispravno stavljena u čitač smart kartica.

Predlog za rešenje problema: Proverite da li je smart kartica ubačena do kraja u čitač i da li se čip smart kartice nalazi sa odgovarajuće strane.

3. Nije ispravno instalisan drajver za čitač smart kartica ili USB token.

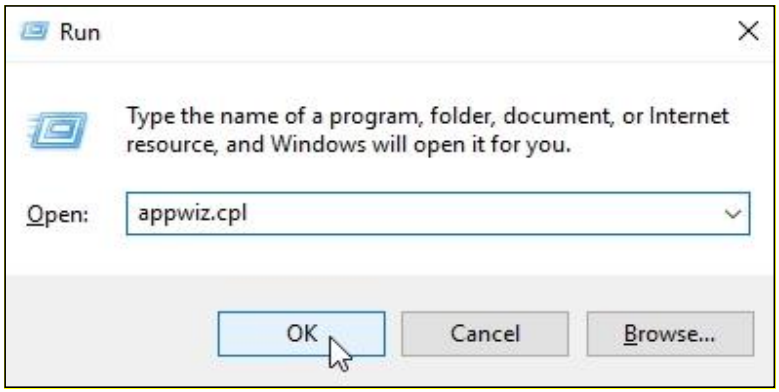
Predlog za rešenje problema: U *Device Manager*-u treba pogledati sekciju ***Smart card readers*** i proveriti da li je drajver ispravno instalisan.

Napomena: Detalje pročitati u dokumentu **Instalisanje klijentskog softvera A.E.T. SafeSign i korišćenje smart kartica i USB tokena**, koji se nalazi na veb strani https://www.ca.posta.rs/dokumentacija/#Uputstva.

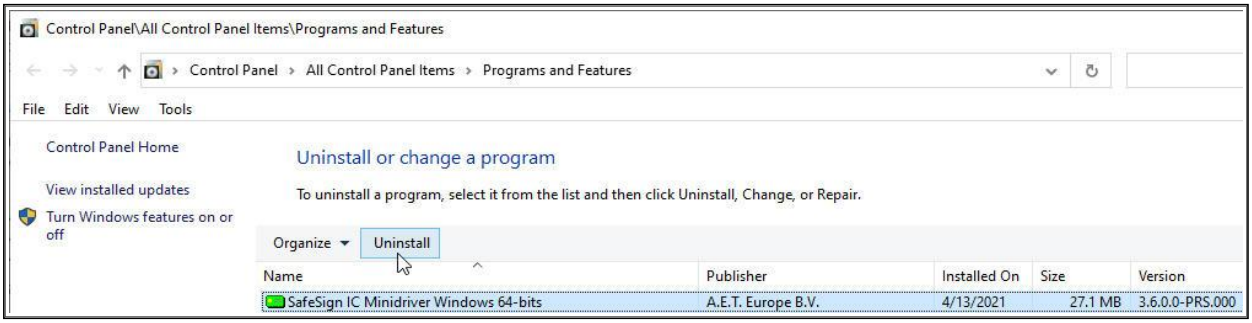
4. Nije ispravno instalisan klijentski softver A.E.T. SafeSign.

Predlog za rešenje problema: Ukloniti klijentski softver A.E.T. SafeSign. Da bi se uklonio klijentski softver A.E.T. SafeSign sa računara, najlakše je startovati formu *Run* pritiskom tastera Win+R na tastaturi. Kada se pokrene forma *Run*, u polje *Open* ukucati **appwiz.cpl** i nakon toga pritisnuti dugme *OK* (slika 1.). Tada se pojavljuje forma *Programs and Features*. Na listi

instalisanih aplikacija izabrati **SafeSign** i pritisnuti dugme ***Uninstall*** (slika 2.), pa ga ponovo instalisati i **restartovati računar**. **Na računaru korisnika osim klijentskog softvera A.E.T. SafeSign, NE sme da bude instalisan klijentski softver (middleware) bilo kog drugog sertifikacionog tela ili bilo koje banke, zbog moguće kolizije u radu.**



Slika 1. Forma *Run* za pokretanje forme *Programs and Features*

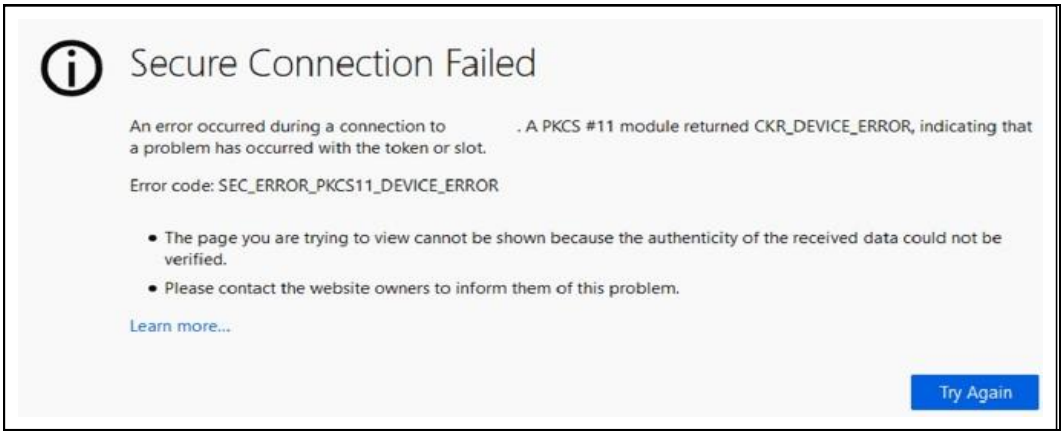


Slika 2. Forma *Programs and Features* za uklanjanje instalisanih aplikacija

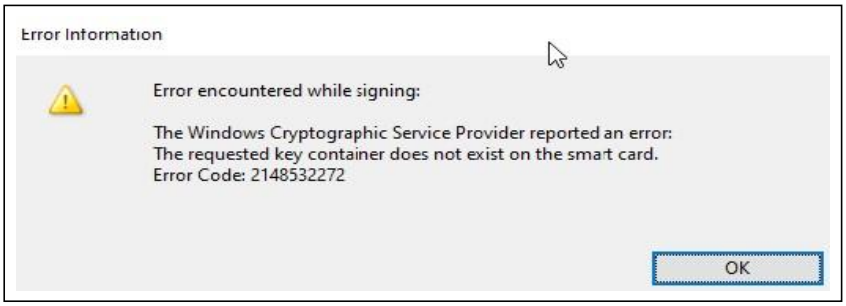
5. Nije aktivirana kartica/USB token.

U slučaju da se javio problem koji se manifestuje kao što je prikazano na slikama 2.1. i 2.2. on je posledica neaktivne kartice/USB tokena.

Predlog za rešenje problema: Aktivirati karticu/USB token. Primeniti uputstvo **Aktivacija QSCD kartica i tokena** koje može da se preuzme sa veb strane Sertifikacionog tela Pošte: https://www.ca.posta.rs/dokumentacija/#Uputstva



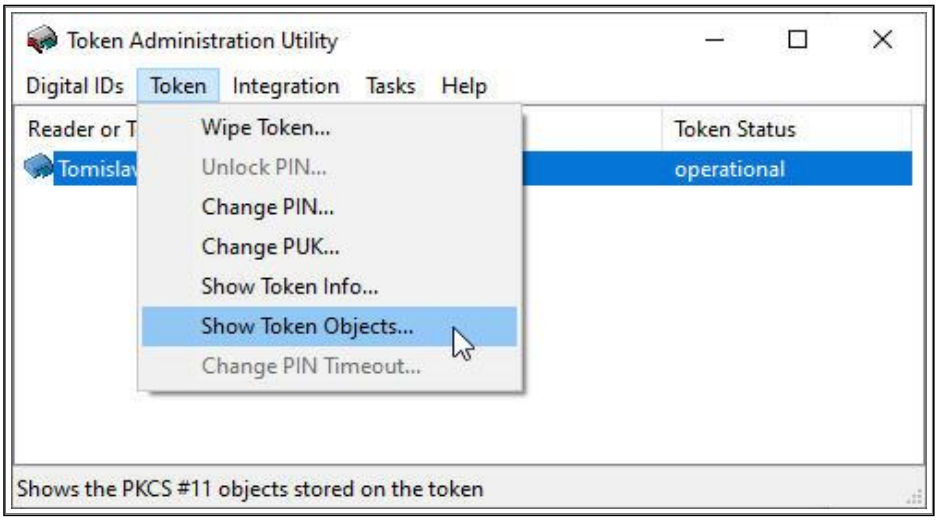
Slika 2.1. Neuspešna prijava sertifikata putem Web browser-a kada smart kartica/USB token nisu aktivirani



Slika 2.2. Greška koja se javlja prilikom pokušaja potpisivanja PDF dokumenta kada QSCD smart kartica/USB token nisu aktivirani

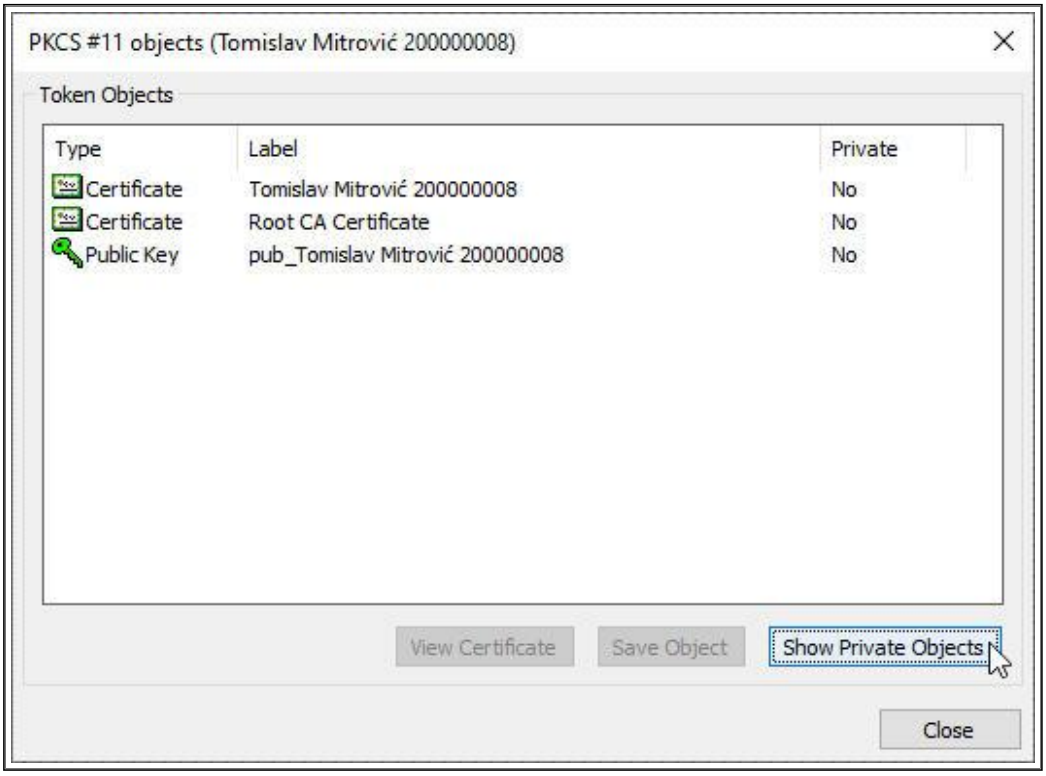
6. Oštećena je smart kartica (USB token) ili je obrisan sertifikat korisnika i pripadajući tajni (privatni) ključ korisnika sa smart kartice (USB tokena).

Predlog za rešenje problema: Korisnik može da proveri ispravnost smart kartice (USB tokena) i ispravnost svog sertifikata tako što će u *Token Administration Utility* iz menija *Token* izabrati opciju *Show Token Objects*, kao što je prikazano na slici 3.



Slika 3. Token Administration Utility, opcija Show Token Objects

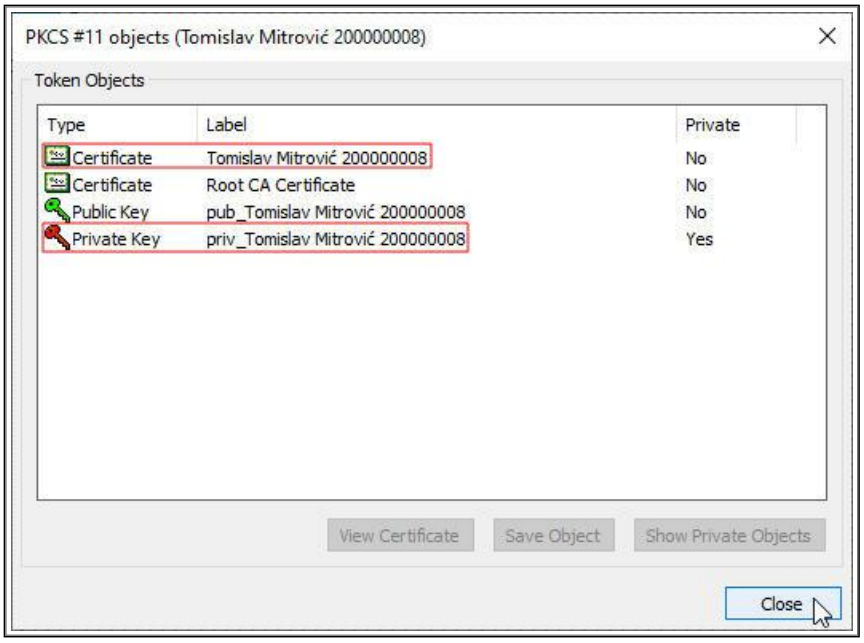
Zatim će se otvoriti forma PKCS#11 objects na kojoj je potrebno pritisnuti dugme Show Private Objects, kao što je prikazano na slici 4, a posle toga treba uneti lozinku kartice/tokena (PIN).



Slika 4. Forma PKCS#11 objects

Posle unošenja lozinke kartice/USB tokena, na formi PKCS#11 objects će biti prikazani svi objekti koji postoje na kartici/USB tokenu (slika 5.). Crvenom bojom su uokvireni sertifikat i privatni ključ, a ukoliko neki od njih ne postoji, neće biti moguće korišćenje kartice/USB tokena. Korisnik može da **obriše** sertifikat i/ili pripadajući tajni (privatni) ključ sa smart kartice (USB tokena) korišćenjem veb pretraživača **Mozilla Firefox** ili drugim aplikacijama koje pristupaju smart kartici (USB tokenu) preko PKCS#11 modula (aetpkss1.dll). Obrisani tajni (privatni) ključ **ne** može da se vrati na smart karticu (USB token). **Korisnik je odgovoran ako s namerom ili iz nehata obriše sertifikat i pripadajući tajni (privatni) ključ sa smart kartice (USB tokena). Smart kartica (USB token) sa koje je obrisan sertifikat i/ili pripadajući tajni (privatni) ključ ne podleže reklamaciji, ni garanciji.**

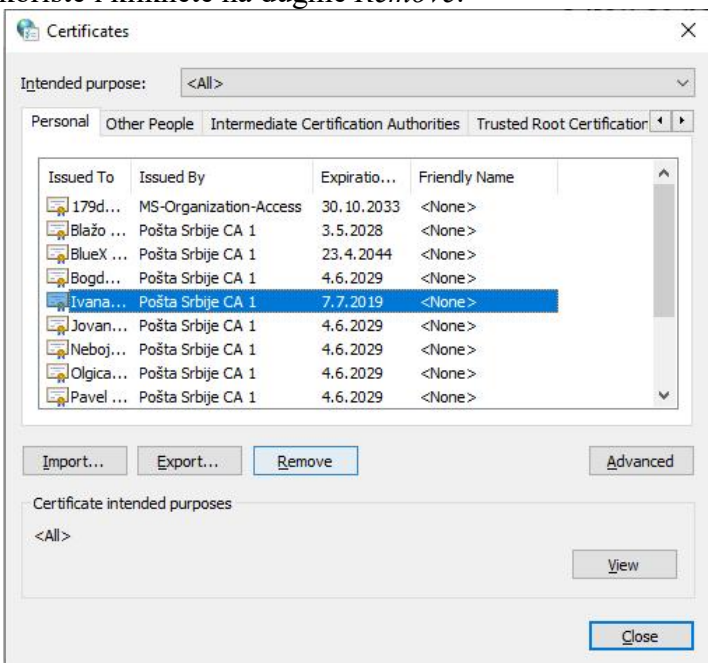
Obrisani sertifikat je u nekim slučajevima moguće vratiti na karticu/USB token. U slučaju kada je obrisan samo sertifikat, a na kartici/tokenu postoji privatni ključ, potrebno je da se obratite korisničkoj podršci Sertifikacionog tela Pošte na adresu E-pošte: ca-podrska@posta.rs radi dobijanja daljih instrukcija.



Slika 5. Forma PKCS#11 objects, prikazani svi objekti na kartici/USB tokenu

7. Problem sa keširanim podacima u Microsoft skladištu sertifikata.

U slučaju da se na jednom računaru koristi više sertifikata od strane Microsoft aplikacija i aplikacija drugih proizvođača softvera koje pristupaju sertifikatu preko Windows skladišta sertifikata, mogu da se dogode usporenja u radu. Potrebno je da se korisnički sertifikati koji se ne koriste, a nalaze se u skladištu sertifikata, obrišu. Do forme prikazane na slici 6. se najlakše dolazi prečicom, tako što se pritiskom tastera Win+R na tastaturi pokrene forma *Run*, u polje *Open* se upiše **inetcpl.cpl** i posle toga pritisne dugme *OK*. Kada se bude otvorila forma prikazana na slici 6. potrebno je da klikom miša na sertifikat obeležite sertifikat, ili više sertifikata koji se ne koriste i kliknete na dugme *Remove*.



Slika 6. Brisanje sertifikata koji se ne koriste iz Microsoft skladišta

8. Onemogućeno je kopiranje sertifikata korisnika u Windows skladište sertifikata.

Ako postoje svi potrebni objekti na kartici/USB tokenu (slika 5.) i instalisana je poslednja verzija klijentskog softvera A.E.T. SafeSign, a sertifikat korisnika se **nije** iskopirao u Windows skladište sertifikata, tada je verovatno onemogućen servis za kopiranje sertifikata korisnika.

Onemogućeno je Microsoft Windows kopiranje sertifikata korisnika, ako je:

- U Windows registru DWORD vrednost **CertPropEnabled** = **0**, na sledećoj lokaciji: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CertProp, a na 64-bitnom Windows-u dodatno i na sledećoj lokaciji: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\CertProp. Ako ova lokacija **ne** postoji, tada se podrazumeva da je **CertPropEnabled** = **1**.
- Stopiran servis **Certificate Propagation** ili **Smart Card**.

Predlog za rešenje problema: U Windows registru (Start→Run→regedit) **CertPropEnabled** = **1** i startovati navedene servise (slika 8. i 9.). Posle izvršenog podešavanja u Windows registru potrebno je **restartovati računar**.

Name	Description	Status	Startup Type	Log On As
Certificate Propagation	Copies user ...	Running	Automatic (Tri...	Local System

Slika 8. Startovan je servis **Certificate Propagation**

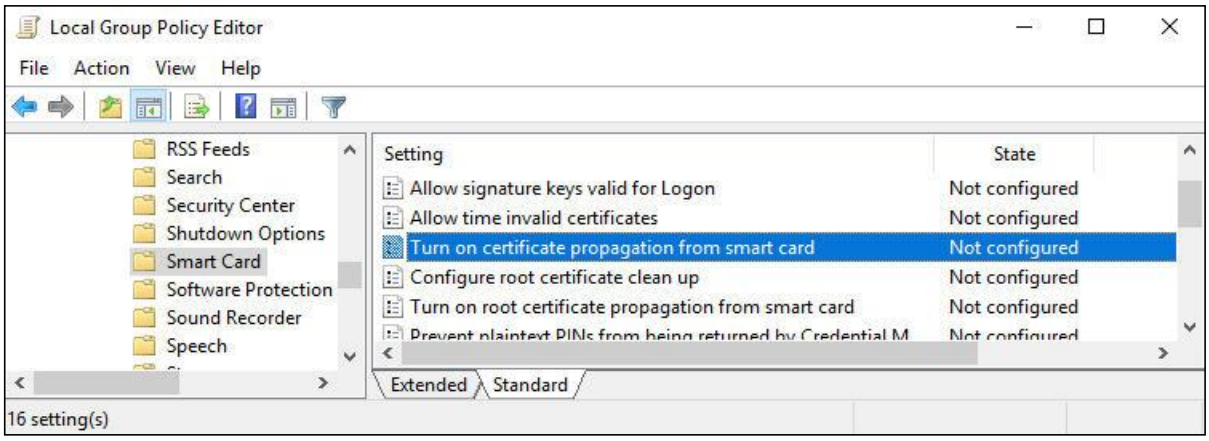
Name	Description	Status	Startup Type	Log On As
Smart Card	Manages ac...	Running	Automatic (Tri...	Local Service

Slika 9. Startovan je servis **Smart Card**

Vrednost **CertPropEnabled** može da se podesi i preko forme *Local Group Policy Editor* koja je prikazana na slici 10, do koje se dolazi na sledeći način: Pritiskom tastera *Win+R* na tastaturi→gpedit.msc→Computer Configuration→Administrative Templates→Windows Components→Smart Card→Turn on certificate propagation from smart card. Moguće su dve (2) vrednosti:

- **CertPropEnabled** = **1** ako je Turn on certificate propagation from smart card = **Not configured** ili **Enabled**.
- **CertPropEnabled** = **0** ako je Turn on certificate propagation from smart card = **Disabled**.

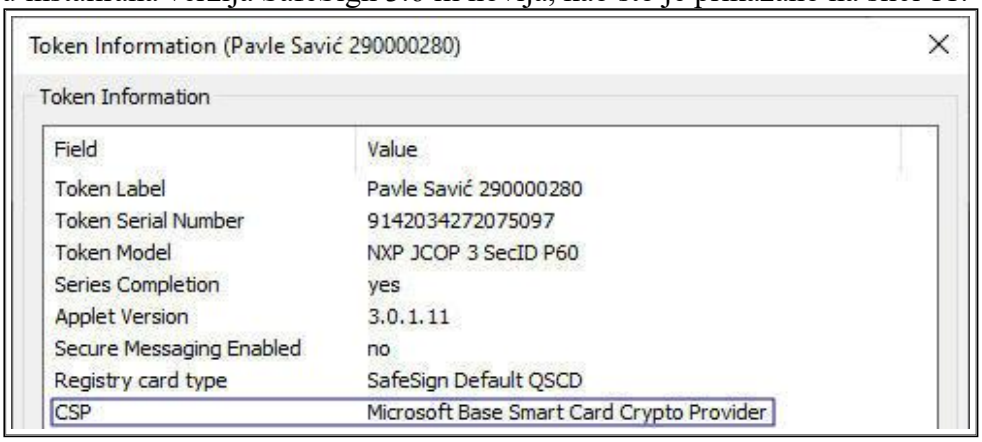
Ako se izvrše promene preko forme *Local Group Policy Editor*, treba **restartovati računar**.



Slika 10. Podešeno je kopiranje sertifikata korisnika sa smart kartice (USB tokena) u Windows skladište sertifikata

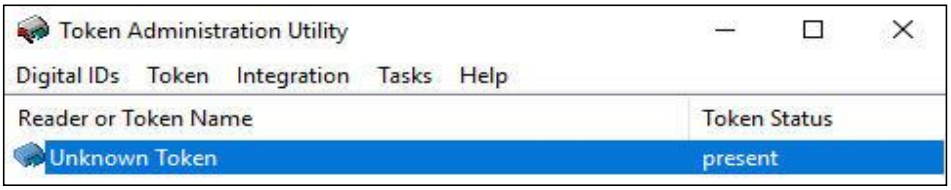
9. U Windows registru su oštećeni podaci koji se odnose na smart karticu ili USB token.

Korisnik može da proveri ispravnost podataka smart kartice (USB tokena) u Windows registru tako što će u *Token Administration Utility* i sa menija *Token* izabrati opciju ***Show Token Info*** za selektovanu karticu ili USB token. Ako su podaci smart kartice (USB tokena) ispravni, na formi ***Token Information*** će pisati: **CSP = Microsoft Base Smart Card Crypto Provider** ukoliko je na računaru instalirana verzija SafeSign 3.6 ili novija, kao što je prikazano na slici 11.



Slika 11. Smart kartica/USB token izdata posle 20.4.2021. godine

Ako su podaci oštećeni, ili pokušavate da koristite kartice ili tokene izdate od 21.04.2021. godine na verziji SafeSign nižoj od 3.6 biće prikazano: **Unknown Token** (slika 12.).



Slika 12. Podaci smart kartice (USB tokena) u Windows registru su oštećeni

Predlog za rešenje problema: Ponovo instalisati poslednju verziju softvera A.E.T. SafeSign i **restartovati računar**.

Napomena: Problemi opisani u tački 7. i 8. su najčešće posledica instalisanja klijentskog softvera (middleware) nekog drugog sertifikacionog tela ili neke banke. Na računaru korisnika osim klijentskog softvera A.E.T. SafeSign, NE sme da bude instalisan klijentski softver (middleware) bilo kog drugog sertifikacionog tela ili bilo koje banke, zbog moguće kolizije u radu. Ukloniti sa računara sve klijentske softvere (middleware) za rad sa sertifikatima, osim klijentskog softvera A.E.T. SafeSign Sertifikacionog tela Pošte.

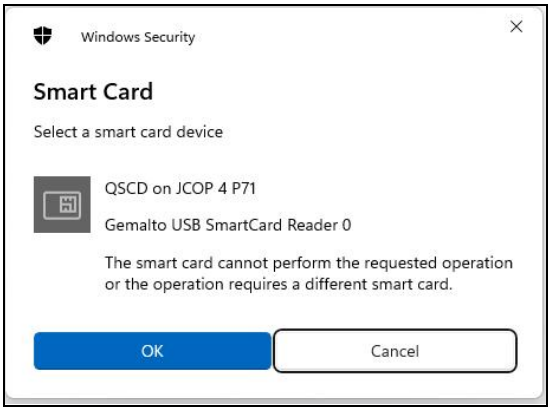
10. Antivirus softver blokira rad sa sertifikatom na smart kartici ili USB tokenu.

Predlog za rešenje problema: U nekim slučajevima, iako je sve prethodno korektno podešeno, antivirus softver može da blokira kopiranje sertifikata u Windows skladište, ili pristup ključevima. U tom slučaju, potrebno je da se privremeno onemogući ili u potpunosti isključi antivirus softver kako bi se problem izolovao. Posle toga treba ubaciti karticu u čitač/priključiti USB token i proveriti da li se sertifikat iskopirao u Windows skladište i da li je rezultat provere ispravnosti uspešan. Ukoliko se sertifikat iskopirao, odnosno ukoliko je rezultat provere ispravnosti uspešan to znači da je problem bio u antivirus softveru. Korisnik je odgovoran za podešavanje, odnosno ispravan rad antivirus softvera.

Ukoliko ni jedan od predloga ne dovede do rešenja problema, a korisnik upotrebljava sertifikat samo za rad u veb aplikacijama, preostaje da se koristi **Mozilla Firefox**, uz prethodno podešavanje prema dokumentu **Podešavanje veb pretraživača Mozilla Firefox za korišćenje sertifikata na smart kartici ili USB tokenu na Windows računaru**, jer pomenuti veb pretraživač koristi drugačiji način pristupa kartici/tokenu odnosno sertifikatu i ključevima koji se na njoj nalaze.

11. Zapamćen izbor prethodno korišćenog sertifikata korisnika u Mozilla Firefox

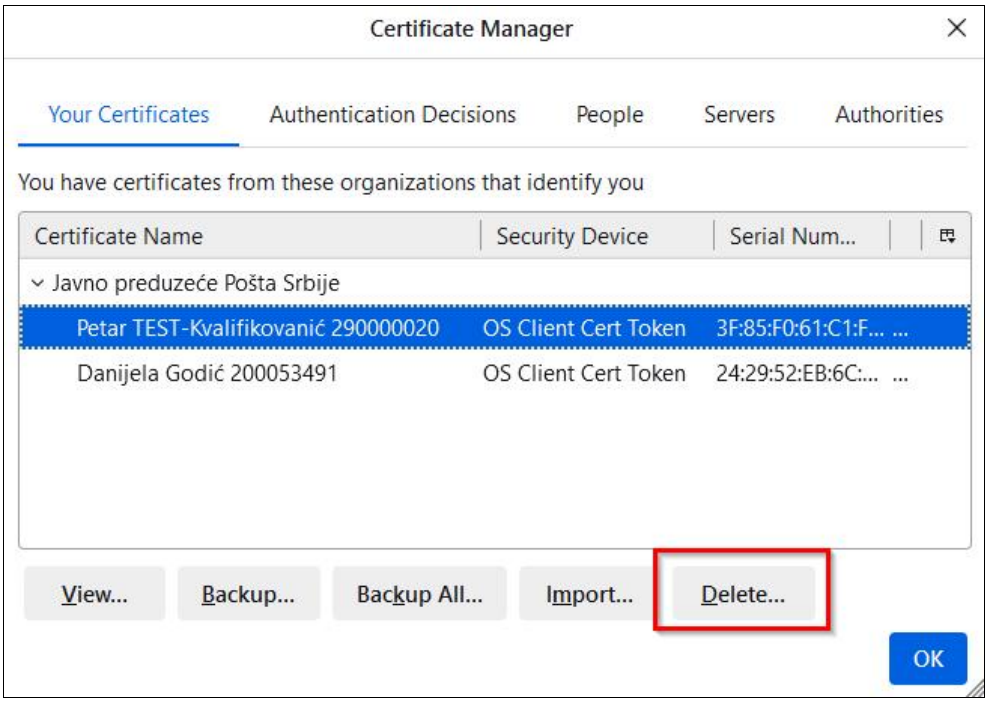
Ukoliko ste u Mozilla Firefox-u koristili neki drugi sertifikat moguće je da je ostao zapamćen kao podrazumevani izbor za prijavu što može da uzrokuje problem poput onog koji je prikazan na slici 13.



Slika 13. Problem izbora sertifikata

Da biste ovaj problem prevazišli, potrebno je da u Mozilla Firefox-a obrišite (uklonite) stari/nekorišćeni sertifikat koji je zapamćen kao podrazumevani izbor. **VAŽNO**: Pre brisanja izvucite sve kartice/izvucite sve tokene iz USB utičnice. Pristupite sledećoj formi: Menu bar → Settings → Privacy & Security → odeljak Security → dugme View Certificates. U

kartici Authentication Decisions, kao što je prikazano na Slici 14. potrebno je da sertifikat koji treba da se obriše obeležite klikom miša i da pritisnete dugme Delete.



Slika 14. Stari sertifikat korisnika

Posle brisanja ubacite karticu u čitač/priključite USB token i restartujte Firefox pa izvršite proveru ispravnosti sertifikata uz neophodan unos lozinke smart kartice/USB tokena: https://ra-front.ca.posta.rs/test/provera_ispravnosti.aspx

Prilikom izbora sertifikata dečekirajte checkbox tako da se ne pamti izbor podrazumevanog sertifikata kao na slici 15, jer njegovo pamćenje može da uzrokuje problem ukoliko ćete imati potrebu da koristite dva ili više sertifikata na istom računaru.

Slika 15. Dečekirati podrazumevani izbor sertifikat korisnika