

U-QCA-354

Šifra dokumenta

Uputstvo za instalaciju prerekvizita za rad sa kvalifikovanim sertifikatom za elektronski potpis i pečat – LINUX

Sadržaj

1. Preuzimanje ESS QCA instalacionog paketa	3
2. Instalacija ESS QCA „lanca poverenja“	3
3. Instalacija ESS QCA SafeNet Authentication Client midlvera	5
4. Dodatna konfiguracija za korišćenje kvalifikovanih sertifikata u veb pretraživačima	6
5. Instalacija drajvera za ACS čitače pametnih kartica	7
6. Instalacija drajvera za Thales-Gemalto čitače pametnih kartica	7
7. Test uspešnosti instalacije prerekvizita za rad kvalifikovanih sertifikata na Linux-u	8

1. Preuzimanje ESS QCA instalacionog paketa

Instalacioni paket sa svim neophodnim komponentama može biti preuzet sa ESS QCA sajta - <https://essqca.esmartsys.com> na stranici "Preuzimanje softvera", klikom na link ESS QCA Linux instalacioni paket pokreće se postupak preuzimanja paketa.

Pre same upotrebe zip datoteku treba otpakovati dvoklikom. Pronaći datoteku u folderu Downloads dvoklikom na nju počinje postupak odpakivanja.

Nakon ovog koraka moguće je krenuti sa instalacijom neophodnih softverskih komponenti za korišćenje ESS QCA kvalifikovanog sertifikata za elektronski potpis i pečat.

Napomena: Softver za sertifikate je trenutno moguće koristiti samo na Ubuntu i CentOS distribucijama i instalacije se vrše puštanjem komandi u Terminalu.

2. Instalacija ESS QCA „lanca poverenja“

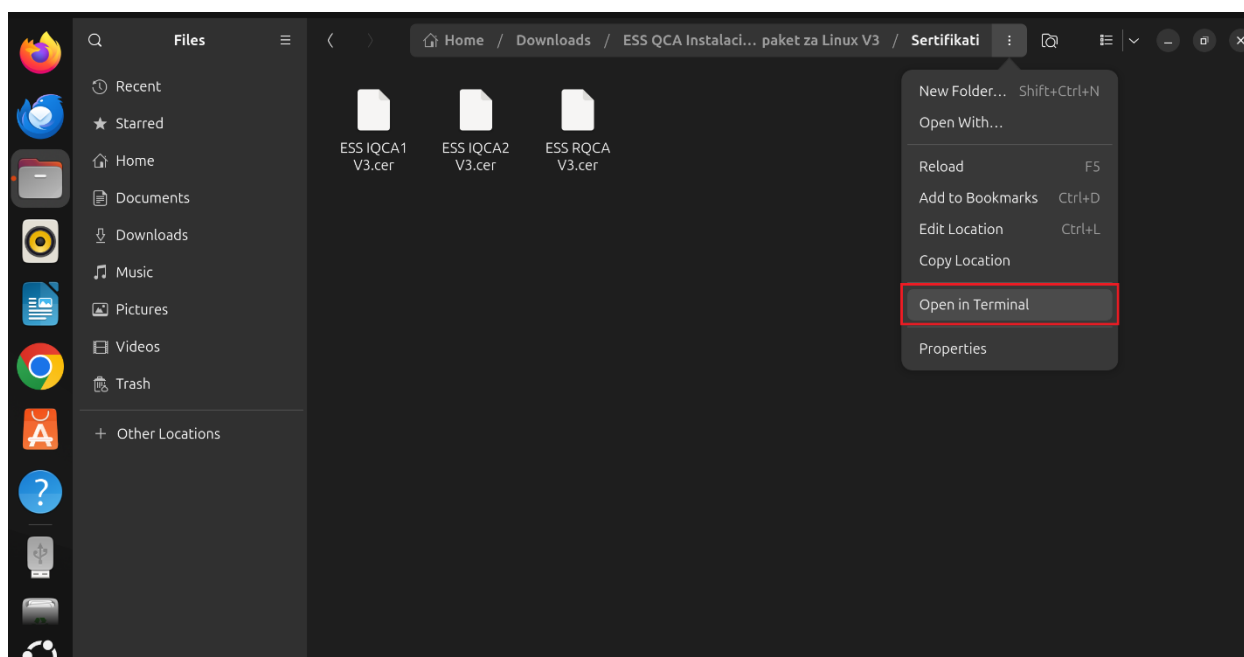
ESS QCA „lanac poverenja“ sastoji se od Root CA i Issuer CA sertifikata koji se nalaze unutar foldera „Certificates“ Linux instalacionog paketa. U zavisnosti od datuma izdavanja i tipa kvalifikovanog sertifikata, potrebno je instalirati odgovarajući skup navedenih sertifikata.

- Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024., potrebno je instalirati sledeće CA sertifikate:
 - "ESS RQCA.cer"
 - "ESS IQCA1(3).cer"
- Za kvalifikovane sertifikate za elektronski potpis izdate posle 08.04.2024., potrebno je instalirati sledeće CA sertifikate:
 - "ESS RQCA V3.cer"
 - "ESS IQCA1 V3.cer"
- Za kvalifikovane sertifikate za elektronski pečat, potrebno je instalirati sledeće CA sertifikate:
 - "ESS RQCA V3.cer"
 - "ESS IQCA2 V3.cer"

Ovi sertifikati se moraju importovati u lokalni Linux sistem na sledeće dve lokacije:

- a) `/usr/local/share/ca-certificates/`,
- b) `/etc/ssl/certs/`

Pre svega, potrebno je otvoriti Terminal na lokaciji gde su sačuvani CA sertifikati, kao što je prikazano na slici 1.



Slika 1.

Nakon toga, instalacija sertifikata se izvršava pokretanjem sledećih komandi:

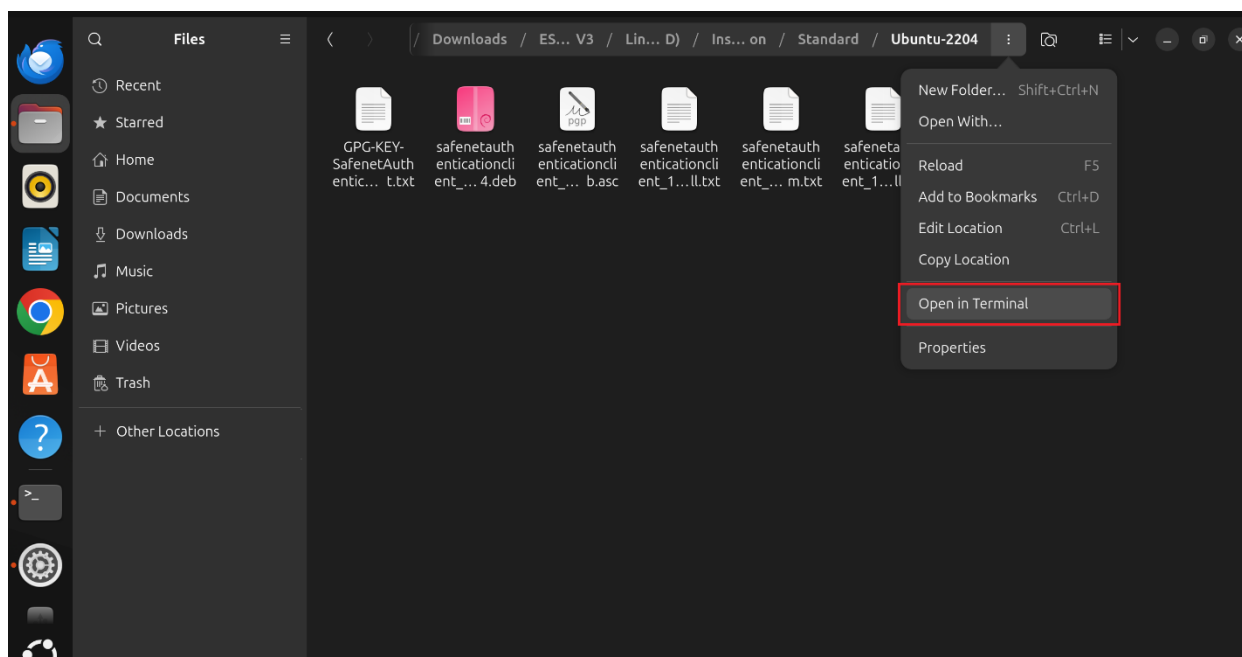
- a) **`sudo cp "ESS RQCA V3.cer" /usr/local/share/ca-certificates/`**
- b) **`sudo cp "/usr/local/share/ca-certificates/ESS RQCA V3.cer" /etc/ssl/certs/`**
- c) **`sudo update-ca-certificates`**

Napomena:

- Komandu pod **a)** je potrebno izvršiti za svaki CA sertifikat u lancu poverenja koji se importuje. Na primer, za V3 Root CA i Issuer CA, izvršavaju se sledeće komande:
 - `sudo cp "ESS RQCA V3.cer" /usr/local/share/ca-certificates/`
 - `sudo cp "ESS IQCA1 V3.cer" /usr/local/share/ca-certificates/`
- Komandu pod **b)** je potrebno izvršiti za svaki CA sertifikat koji je prethodno importovan putem komande **a)**, kako bi te sertifikate prebacili sa lokacije `/usr/local/share/ca-certificates/` na lokaciju `/etc/ssl/certs/`. Ukoliko imate problem sa izvršavanjem komande pod **b)**, i ne uspevate da prebacite sertifikate, to znači da trenutni **korisnik** nema prava da prebacuje sertifikate na lokaciju `/etc/ssl/certs/`. U tom slučaju potrebno je dodeliti odgovarajuća prava nad sertifikatima pokretanjem komande `sudo chmod 644 "/usr/local/share/ca-certificates/ESS RQCA V3.cer"`. Nakon pokretanja ove komande, potrebno je ponovo izvršiti komandu pod **b)** za svaki problematičan CA sertifikat.
- Komanda pod c) se pokreće samo jednom na kraju, nakon uspešnog izvršenja komandi pod a) i b).

3. Instalacija ESS QCA SafeNet Authentication Client midlvera

Kako bi Linux sistem prepoznao čip na kome se nalazi kvalifikovani sertifikat za elektronski potpis ili pečat, neophodno je instalirati SafeNet Authentication Client midlver (middleware). U folderu „SafeNet Authentication Client Linux“ nalaze se podfolderi za odabir verzije Linux operativnog sistema: „Ubuntu“ ili „CentOS“. Svaki od ova dva foldera sadrži direktorijum „Installation“, unutar kojeg se nalaze opcije za odabir tipa instalacije: „Standard“ i „withoutUI“ (bez SAC Tool-a). Preporuka je da se uvek instalira „Standard“ verzija. Ukoliko koristite Ubuntu mašinu, otvorite folder „Ubuntu“ u kome se nalazi fajl sa .deb ekstenzijom. Odabrani fajl je potrebno pokrenuti iz Terminala. Kao što je prikazano na slici 2, otvorite Terminal pomoću prečice:



Slika 2.

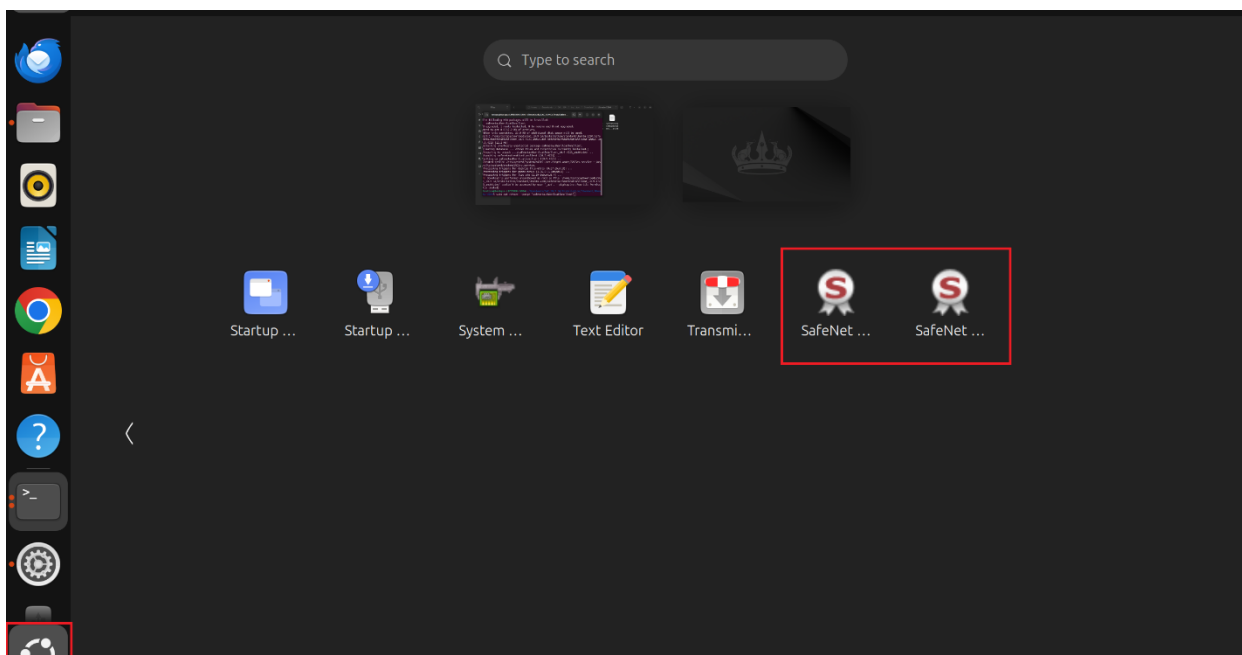
Pokrenuti komanda za instalaciju: **sudo apt install ./safenetauthenticationclient_10.9.6885_amd64.deb**

Ukoliko je instalacija neuspešna i dobijete grešku poput: **couldn't be accessed by user "_apt" pkgAcquire::run (13: Permission denied)**, potrebno je pokrenuti sledeću komandu za dodeljivanje prava: **sudo chmod 644 ./safenetauthenticationclient_10.9.6885_amd64.deb**.

Zatim, pokušajte ponovo sa komandom za instalaciju. Tokom ovog procesa sistem će vam najverovatnije tražiti da unesete korisničku lozinku (password). Kada je unesete, pritisnite Enter i nastavite sa instalacijom. Ukoliko ste greškom instalirali pogrešnu verziju paketa, otvorite Terminal i pokrenite komandu za potpuno uklanjanje: **sudo apt remove --purge safenetauthenticationclient**.

Nakon toga restartujte računar i pokušajte ponovo sa instalacijom ispravnog paketa.

Ukoliko je uspešno instaliran SafeNet Authentication Client midlver, možete to proveriti u App Manageru. Potrebno je da aplikacija bude vidljiva, kao što je prikazano na slici 3.



Slika 3.

4. Dodatna konfiguracija za korišćenje kvalifikovanih sertifikata u veb pretraživačima

Da bi veb pretraživači mogli da prepoznaju kvalifikovan sertifikat, potrebno je pokrenuti sledeće 3 komande:

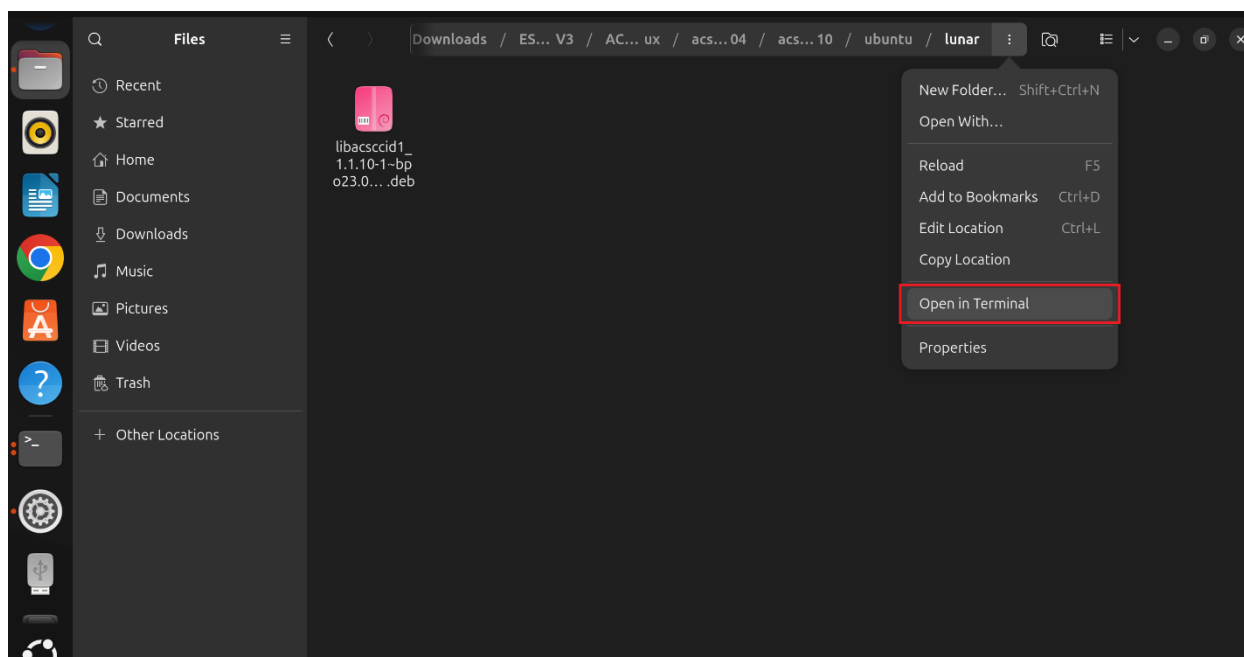
- a) **sudo apt update,**
- b) **sudo apt install libnss3-tools,**
- c) **modutil -dbdir sql:\$HOME/.pki/nssdb -add "SafeNet PKCS11" -libfile /opt/SafeNetAuthenticationClient/lib/libeToken.so**

Napomena: Ovi koraci su neophodni jer pretraživači sami po sebi ne prepoznaju tokene i pametne kartice, već se za pristup njima oslanjaju na PKCS#11 module. Ova konfiguracija omogućava korisniku da koristi sertifikat za autentifikaciju u pretraživačima kao što su Firefox i Chrome.

5. Instalacija drajvera za ACS čitače pametnih kartica

Pre nego što započnete ovaj korak, idite na korak 7 kako biste utvrdili da li je uopšte potrebno instalirati drajvere za ACS čitače pametnih kartica. Ukoliko čitač pametne kartice nije prepoznat (smatra se da sertifikat ne radi jer sistem ne vidi sam čitač), potrebno je nastaviti sa instalacijom ACS drajvera.

Instalacioni paket za ACS drajver nalazi se u folderu **Smart Card Reader Drivers Linux / ACS Driver linux**. Slično kao i kod instalacije SafeNet midlvera, potrebno je pronaći folder sa odgovarajućom verzijom, odnosno distribucijom Linux operativnog sistema. Otvorite taj folder i ukoliko vidite fajl sa .deb ekstenzijom, otvorite Terminal pomoću prečice prikazane na slici 4.



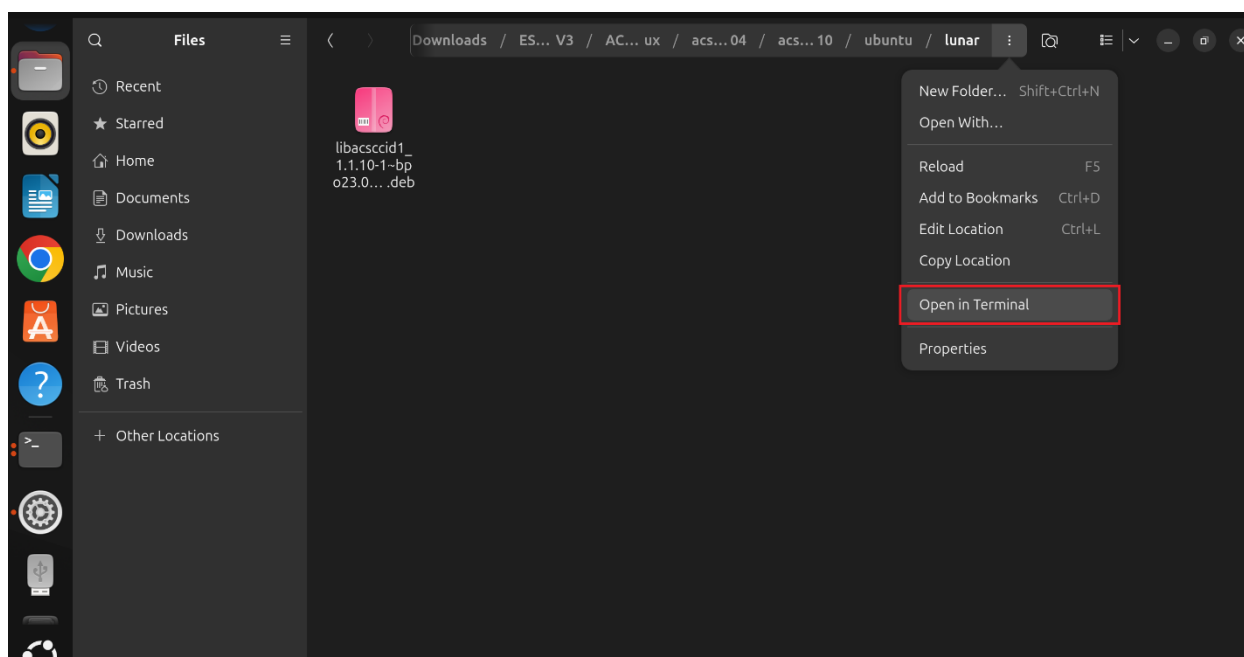
Slika 4.

Pokrenite komandu: ***sudo apt install ./[naziv paket (driver-ver,linux-ver)].deb***, zatim restartujte računar i pređite na korak 7.

6. Instalacija drajvera za Thales-Gemalto čitače pametnih kartica

Pre nego što započnete ovaj korak, idite na korak 7 kako biste utvrdili da li je uopšte potrebno instalirati drajvere za Thales-Gemalto čitače pametnih kartica. Ukoliko čitač pametne kartice nije prepoznat (smatra se da sertifikat ne radi jer sistem ne vidi sam čitač), potrebno je nastaviti sa instalacijom Thales-Gemalto drajvera.

Instalacioni paket za Thales-Gemalto drajver nalazi se u folderu **Smart Card Reader Drivers Linux / Thales - Gemalto Driver linux**. Slično kao i kod instalacije SafeNet midlvera, potrebno je pronaći folder sa odgovarajućom verzijom, odnosno distribucijom Linux operativnog sistema. Otvorite taj folder i ukoliko vidite fajl sa .deb ekstenzijom, otvorite Terminal pomoću prečice prikazane na slici 5.

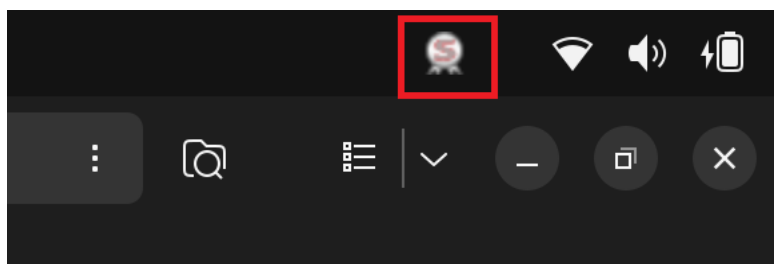


Slika 5.

Pokrenite komandu: **`sudo apt install ./[naziv paket (driver-ver,linux-ver)].deb`**, zatim restartujte računar i pređite na korak 7.

7. Test uspešnosti instalacije prerekvizita za rad kvalifikovanih sertifikata na Linux-u

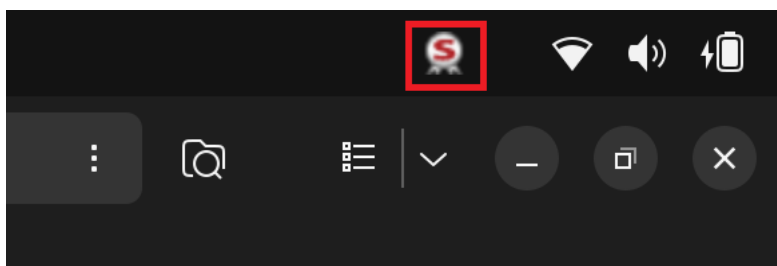
Kao potvrda uspešnosti instalacije svih neophodnih prerekvizita za rad na Linux sistemu, u gornjoj traci (header-u) prikazaće se ikonica SafeNet Authentication Client-a, kao što je prikazano na slici 6.



Slika 6.

(Napomena: ukoliko nemate ovu ikonicu, potrebno je pronaći SafeNet Authentication Client u meniju sa aplikacijama (App Manager) i pokrenuti ga).

Kada ubacite vaš kvalifikovani sertifikat u računar, ikonica SafeNet-a u gornjoj traci će zasvetleti kao što je prikazano na slici 7. To znači da je računar spreman za rad sa kvalifikovanim sertifikatom. Ukoliko je čitač neispravan ili kvalifikovani sertifikat nije pravilno ubačen, ikonica će ostati sive boje (kao na slici 6) i potrebno je proveriti da li je kvalifikovan sertifikat dobro postavljen u čitač.



Slika 7.

Ukoliko dođe do eventualnih problema, molimo Vas da pošaljete tiket putem [veb forme](#) ili napišete imejl na gca@esshitsuport.zohodesk.eu, a mi ćemo Vas kontaktirati u najkraćem roku.