

U-QCA-221

Šifra dokumenta

Uputstvo za instalaciju i korišćenje ESS QCA kvalifikovanog sertifikata za elektronski potpis i pečat - Windows

Sadržaj

1. Uslovi za korišćenje ESS QCA kvalifikovanog sertifikata za elektronski potpis.....	3
2. Preuzimanje ESS QCA instalacionog paketa za Windows.....	3
3. Instalacija ESS QCA „lanca poverenja“	4
3.1. Importovanje Root CA sertifikata	4
3.1.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.....	4
3.1.2. Za kvalifikovane sertifikate za elektronski potpis i pečat izdate posle 08.04.2024.....	6
3.2. Importovanje Issuer CA sertifikata	8
3.2.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.....	8
3.2.2. Za kvalifikovane sertifikate za elektronski potpis izdate posle 08.04.2024.	10
3.2.3. Za kvalifikovane sertifikate za elektronski pečat.....	12
4. Instalacija drajvera za Smart Card čitače	14
5. Instalacija ESS QCA SafeNet Minidriver & PKCS11 paketa	15
6. Aplikacija za promenu i deblokadu PIN-a	16
6.1. Promena PIN-a.....	16
6.2. Deblokada PIN-a	19

1. Uslovi za korišćenje ESS QCA kvalifikovanog sertifikata za elektronski potpis

Instrukcije prezentovane unutar ovog dokumenta namenjene su upotrebi kvalifikovanih sertifikata za elektronski potpis na Microsoft Windows OS. Ukoliko želite da koristite kvalifikovani sertifikat na macOS ili Linux operativnim sistemima, molimo Vas, pošaljite tiket putem [web forme](#) ili napišite mail na gca@esshitsupport.zohodesk.eu, a mi ćemo Vas u najkraćem roku kontaktirati.

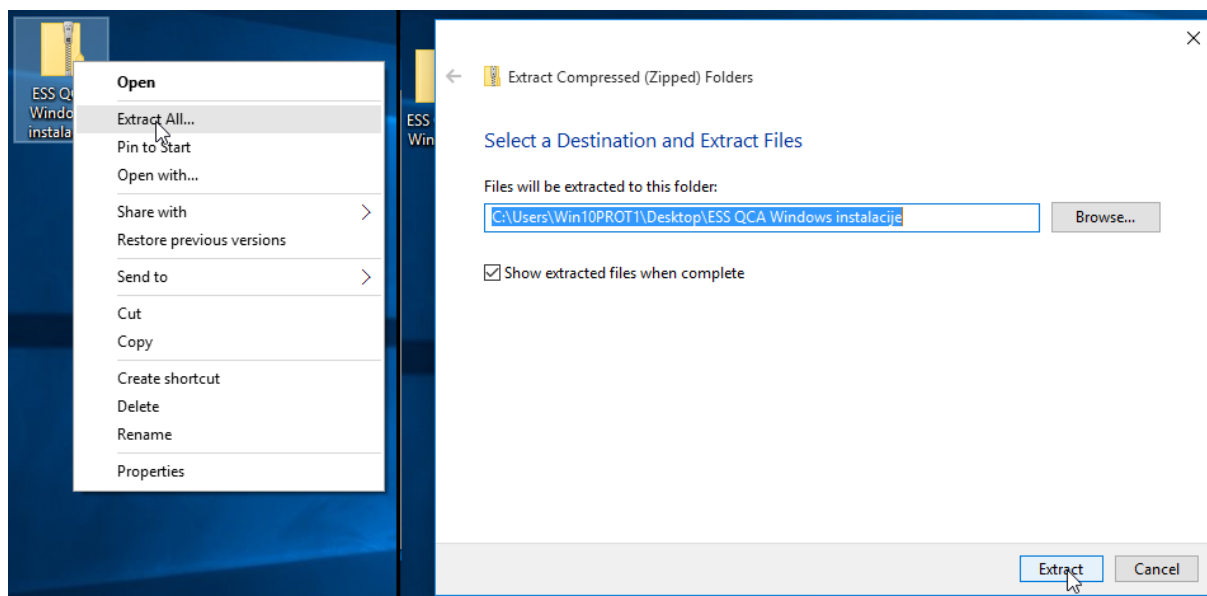
Da biste mogli uspešno da koristite ESS QCA kvalifikovani sertifikat, neophodno je da instalirate ESS QCA „lanac poverenja“ (Root i Issuer sertifikat ESS QCA sertifikacionog tela), SafeNet Minidriver sa PKCS#11 middleware-a i drajvera za čitače smart kartica ili USB tokena (obično ih Windows automatski detektuje).

2. Preuzimanje ESS QCA instalacionog paketa za Windows

Instalacioni paket sa svim neophodnim komponentama može biti preuzet sa ESS QCA web stranice – [Preuzimanje softvera](#), klikom na link „ESS QCA Windows Instalacion paket“.

Pre same upotrebe zip datoteku treba otpakovati:

1. Otvoriti padajući meni desnim klikom na zip datoteku „ESS QCA Windows...“
2. Izabrati opciju „Extract All...“
3. Potvrditi ekstrakciju klikom na dugme „Extract“.



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

3. Instalacija ESS QCA „lanca poverenja“

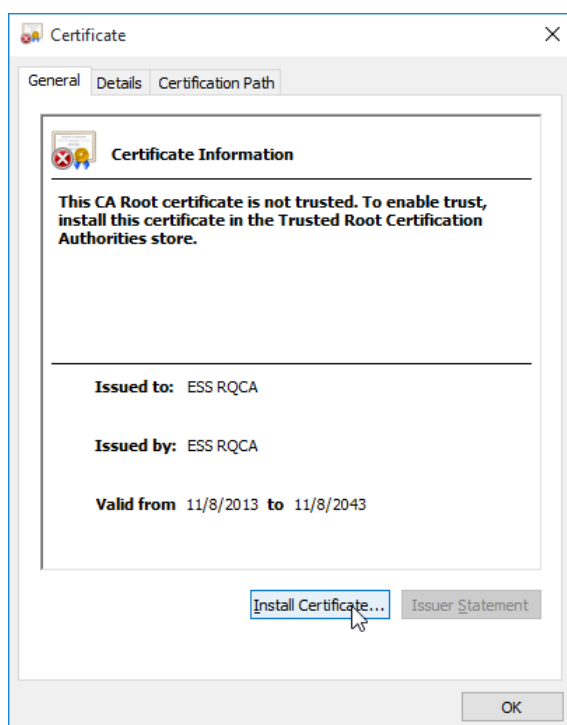
ESS QCA „lanac poverenja“ sastoji se od Root CA i Issuer CA sertifikata koji se nalaze unutar „Certificates“ instalacionog paketa. Ovi sertifikati moraju biti importovani u lokalni računar na Windows mašini kako bi se uspostavilo poverenje između mašine i sertifikata korisnika.

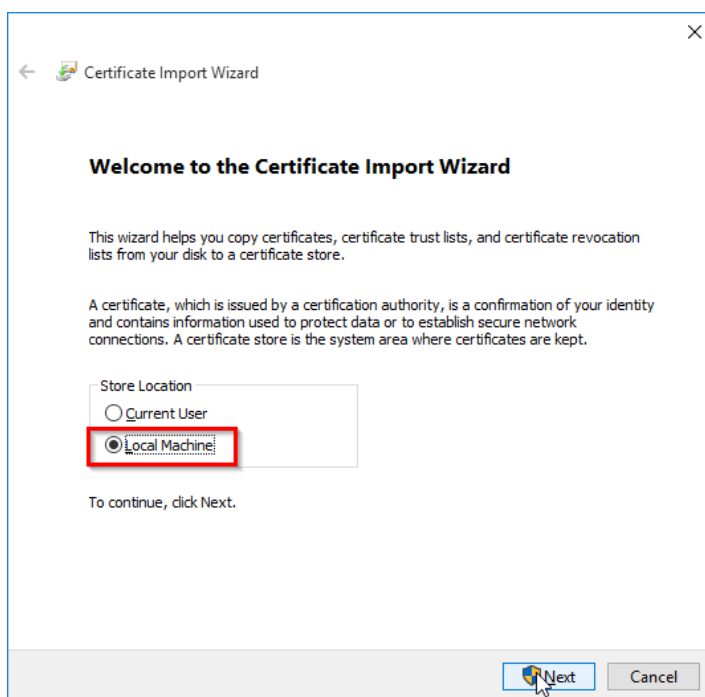
3.1. Importovanje Root CA sertifikata

3.1.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.

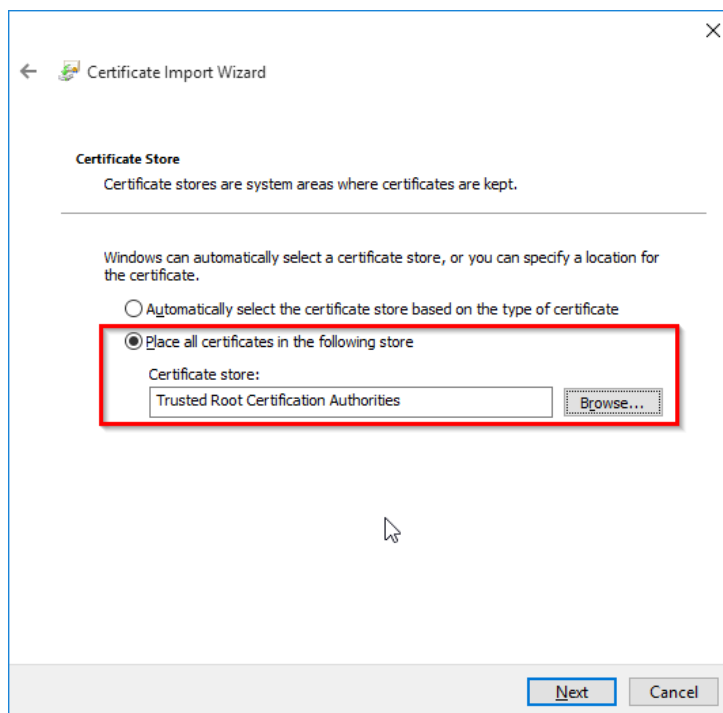
Root CA (ESS RQCA) sertifikat je moguće importovati na sledeći način:

1. Potrebno je dvoklikom otvoriti „**ESS RQCA.cer**“ sertifikat, nakon čega će se pojaviti prozor kao na slici ispod.
2. Importovanje sertifikata se pokreće klikom na dugme „**Install Certificate...**“.
Nakon toga se otvara prozor na kome je potrebno izabrati opciju „**Local Machine**“ i kliknuti na dugme „**Next**“.

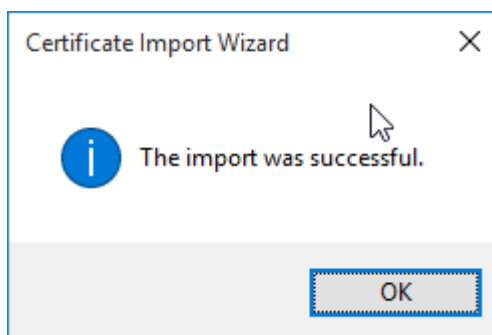




3. Na narednom prozoru potrebno je odabrati opciju „**Place all certificates in the following store**“, a nakon toga treba izabrati naziv „**Certificate store:**“ pomoću „**Browse...**“ dugmeta. „**Trusted Root Certification Authorities**“ je namenjen certificate store za Root CA.



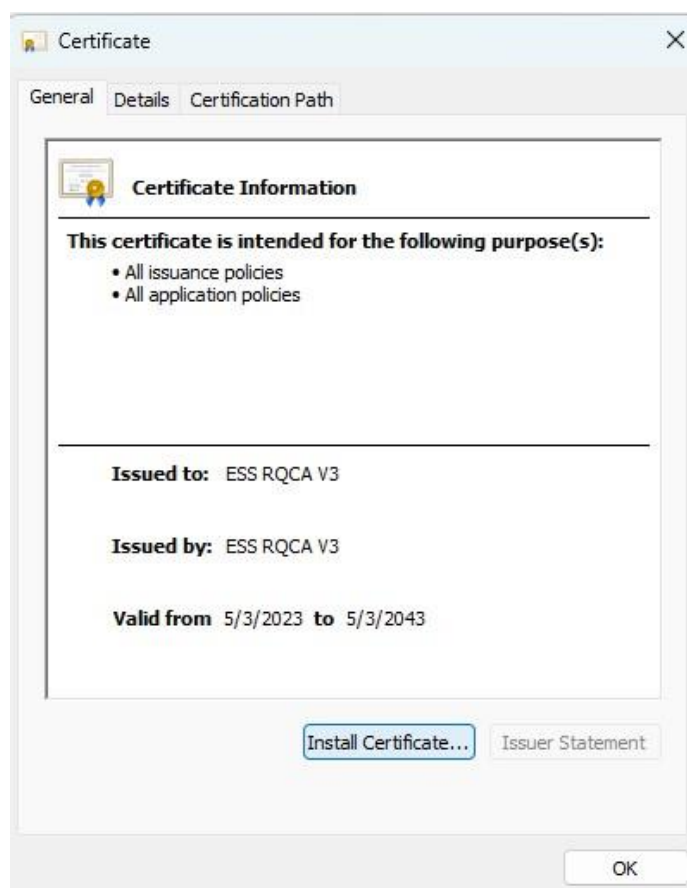
4. Klikom na dugme „**Next**“, otvara se finalni ekran na kome je potrebno kliknuti dugme „**Finish**“. Nakon toga prikazaće se poruka o uspešno izvršenom importu Root CA sertifikata, kao na slici ispod.

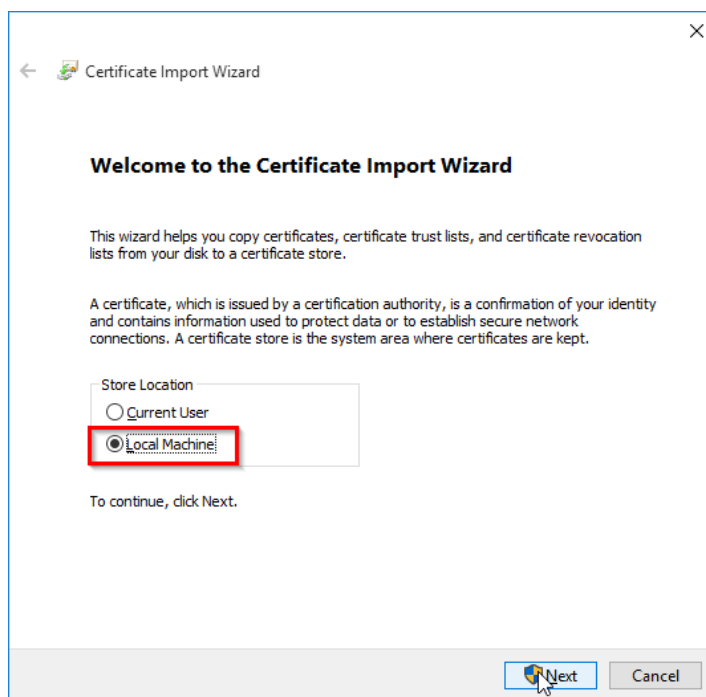


3.1.2. Za kvalifikovane sertifikate za elektronski potpis i pečat izdate posle 08.04.2024.

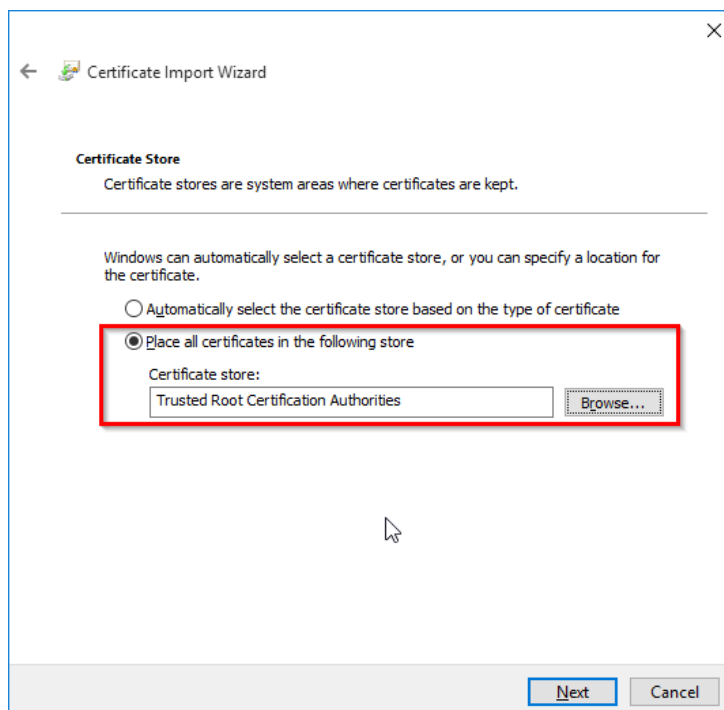
Root CA (ESS RQCA V3) sertifikat je moguće importovati na sledeći način:

1. Potrebno je dvoklikom otvoriti „**ESS RQCA V3.cer**“ sertifikat, nakon čega će se pojaviti prozor kao na slici ispod.
2. Importovanje sertifikata se pokreće klikom na dugme „**Install Certificate...**“. Nakon toga se otvara prozor na kome je potrebno izabrati opciju „**Local Machine**“ i kliknuti na dugme „**Next**“.

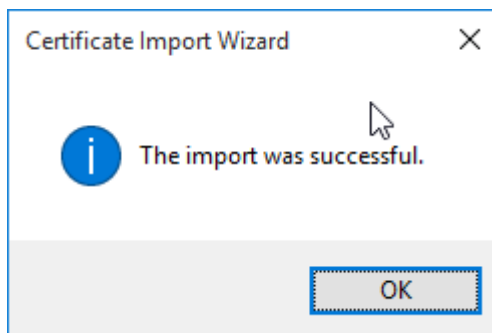




3. Na narednom prozoru potrebno je odabrati opciju „**Place all certificates in the following store**“, a nakon toga treba izabrati naziv „**Certificate store:**“ pomoću „**Browse...**“ dugmeta. „**Trusted Root Certification Authorities**“ je namenjen certificate store za Root CA.



4. Klikom na dugme „**Next**“, otvara se finalni ekran na kome je potrebno kliknuti dugme „**Finish**“. Nakon toga prikazaće se poruka o uspešno izvršenom importu Root CA sertifikata, kao na slici ispod.

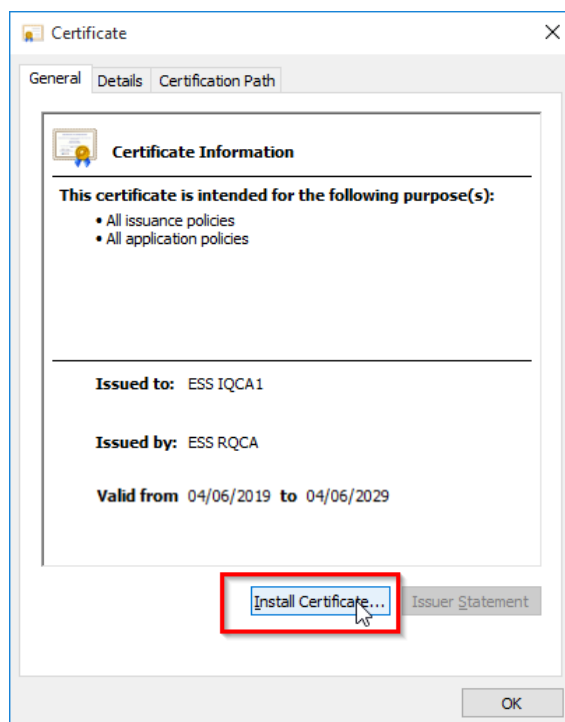


3.2. Importovanje Issuer CA sertifikata

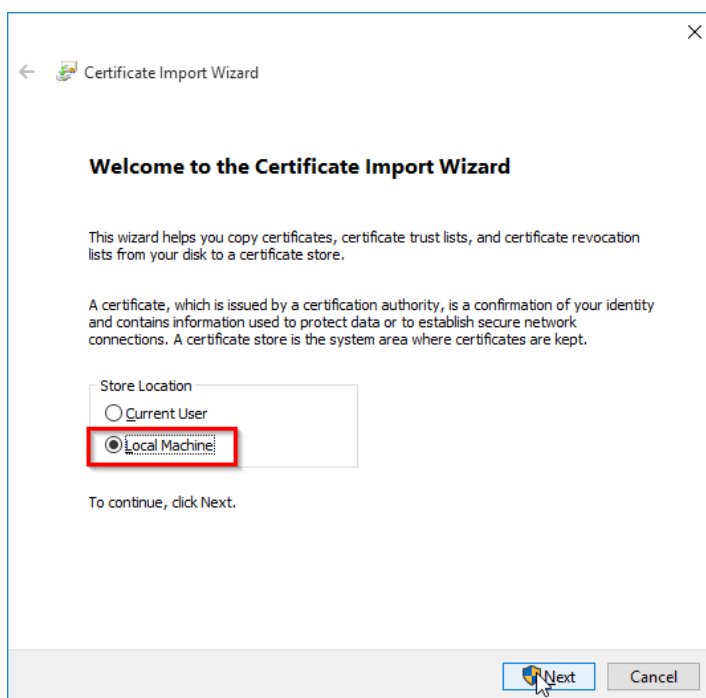
3.2.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.

Issuer CA (ESS IQCA) sertifikat je moguće importovati na sledeći način:

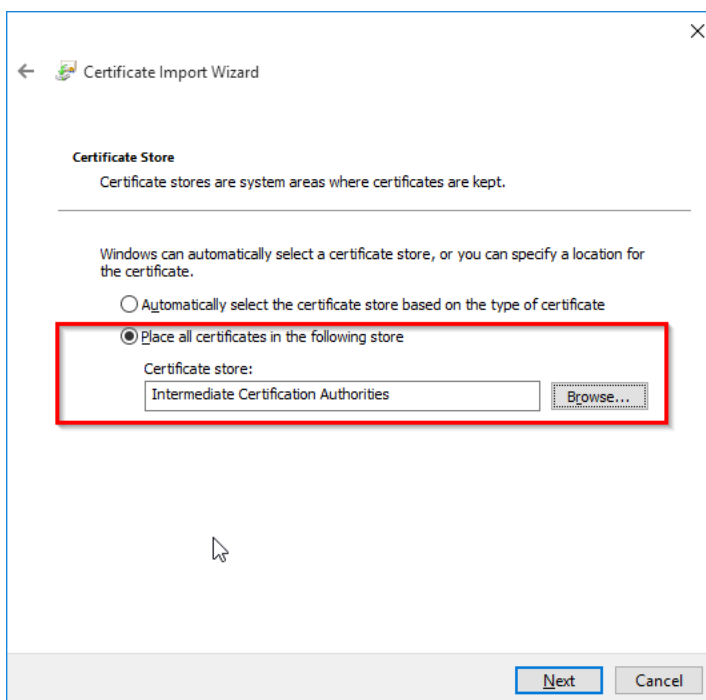
1. Potrebno je dvoklikom otvoriti „**ESS IQCA1(3).cer**“ sertifikat, nakon čega će se pojaviti prozor kao na slici ispod.



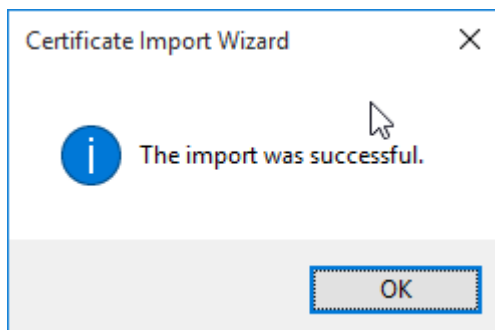
2. Importovanje sertifikata se pokreće klikom na dugme „**Install Certificate...**“.
Nakon toga se otvara prozor na kome je potrebno izabrati opciju „**Local Machine**“ i kliknuti na dugme „**Next**“.



3. Na narednom prozoru potrebno je odabrati opciju „**Place all certificates in the following store**“, a nakon toga treba izabrati naziv „**Certificate store:**“ pomoću „**Browse...**“ dugmeta. „**Intermediate Certification Authorities**“ je namenjen certificate store za Issuer CA.

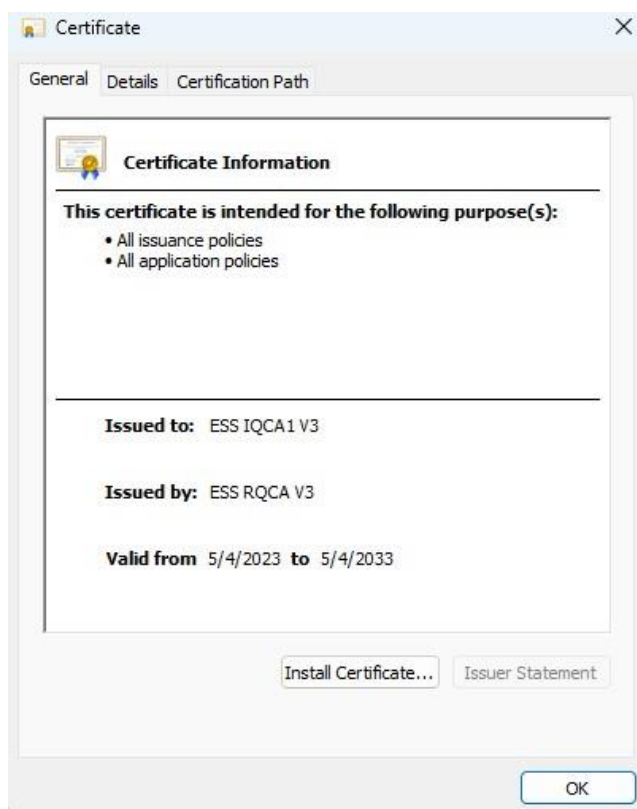


4. Klikom na dugme „**Next**“, otvara se finalni ekran na kome je potrebno kliknuti dugme „**Finish**“. Nakon toga prikazaće se poruka o uspešno izvršenom importu Issuer CA sertifikata, kao na slici ispod.

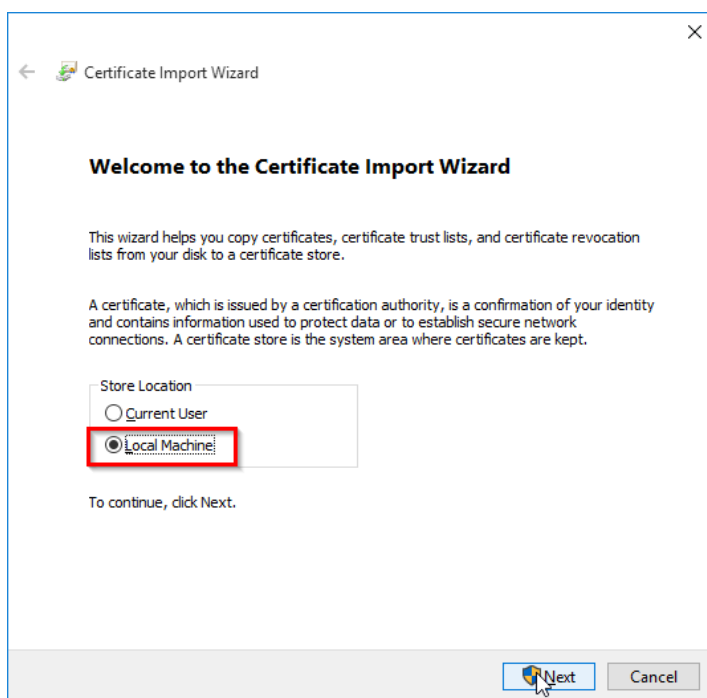


3.2.2. Za kvalifikovane sertifikate za elektronski potpis izdate posle 08.04.2024.

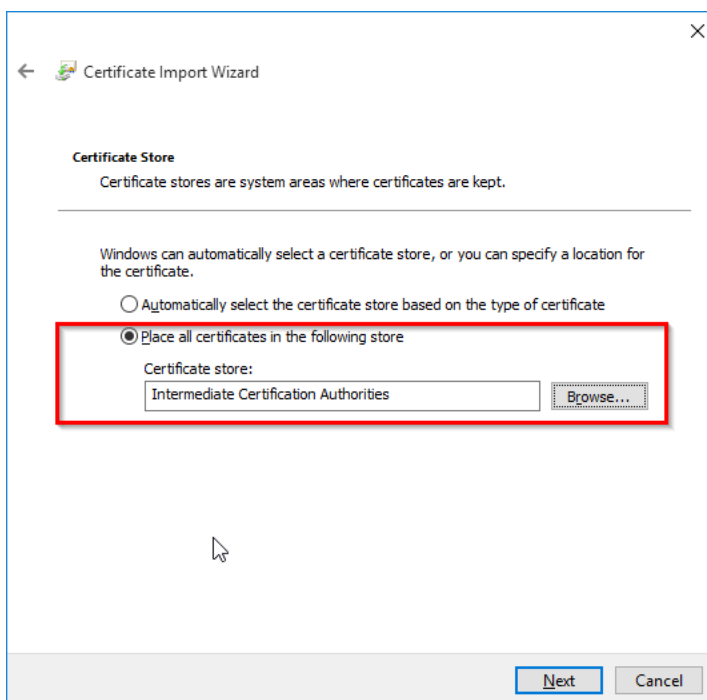
1. Potrebno je dvoklikom otvoriti „**ESS IQCA1 V3.cer**“ sertifikat, nakon čega će se pojaviti prozor kao na slici ispod.



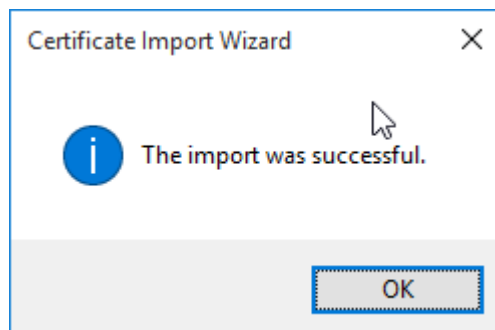
2. Importovanje sertifikata se pokreće klikom na dugme „**Install Certificate...**“.
Nakon toga se otvara prozor na kome je potrebno izabrati opciju „**Local Machine**“ i kliknuti na dugme „**Next**“.



3. Na narednom prozoru potrebno je odabrati opciju „**Place all certificates in the following store**“, a nakon toga treba izabrati naziv „**Certificate store:**“ pomoću „**Browse...**“ dugmeta. „**Intermediate Certification Authorities**“ je namenjen certificate store za Issuer CA.



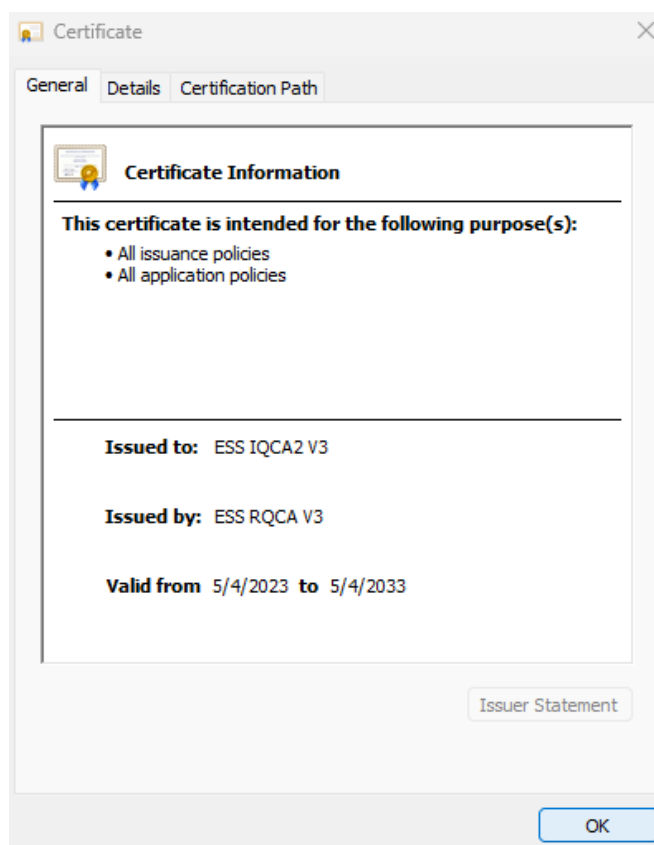
4. Klikom na dugme „**Next**“, otvara se finalni ekran na kome je potrebno kliknuti dugme „**Finish**“. Nakon toga prikazaće se poruka o uspešno izvršenom importu Issuer CA sertifikata, kao na slici ispod.



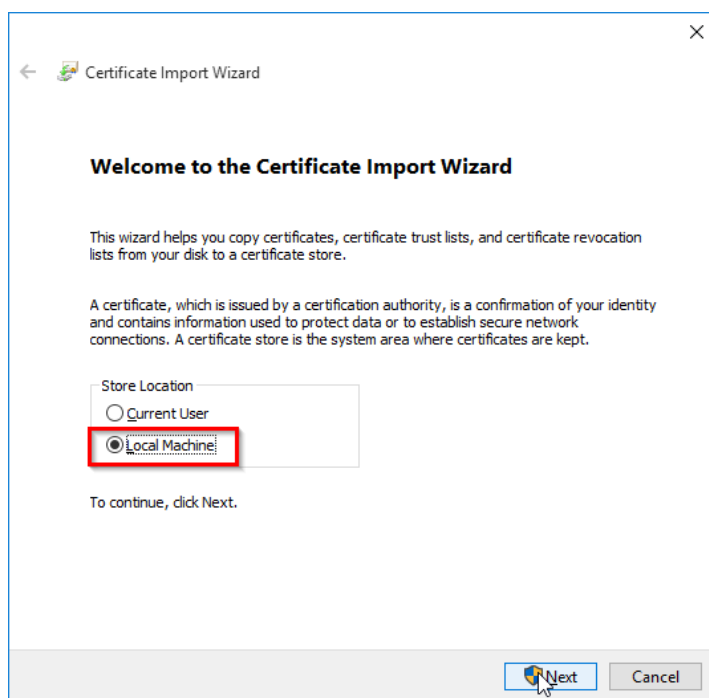
3.2.3. Za kvalifikovane sertifikate za elektronski pečat

Issuer CA (ESS IQCA) sertifikat je moguće importovati na sledeći način:

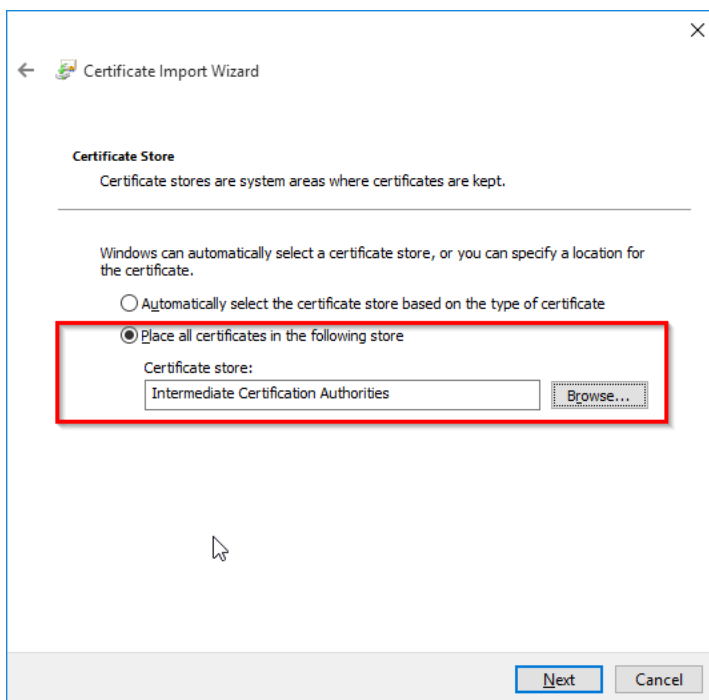
1. Potrebno je dvoklikom otvoriti „**ESS IQCA2 V3.cer**“ sertifikat, nakon čega će se pojaviti prozor kao na slici ispod.



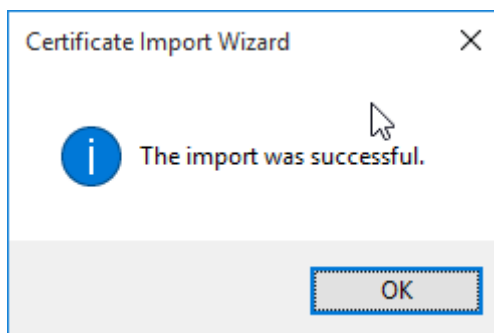
2. Importovanje sertifikata se pokreće klikom na dugme „**Install Certificate...**“. Nakon toga se otvara prozor na kome je potrebno izabrati opciju „**Local Machine**“ i kliknuti na dugme „**Next**“.



3. Na narednom prozoru potrebno je odabrati opciju „**Place all certificates in the following store**“, a nakon toga treba izabrati naziv „**Certificate store:**“ pomoću „**Browse...**“ dugmeta. „**Intermediate Certification Authorities**“ je namenjen certificate store za Issuer CA.



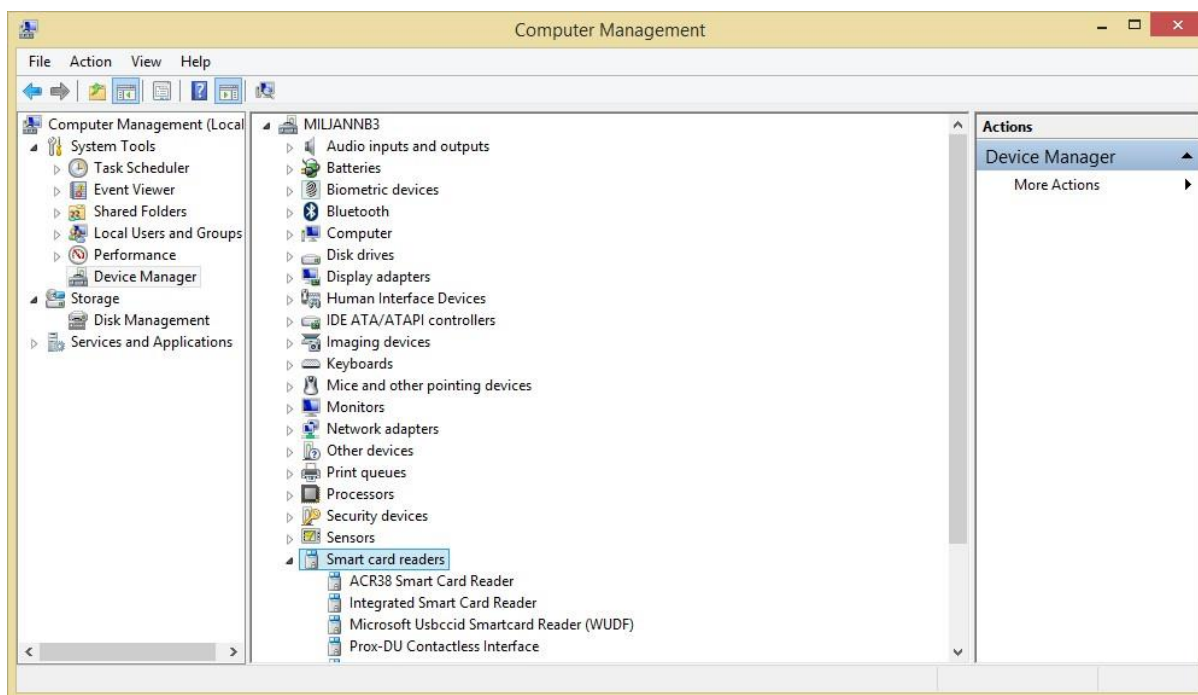
4. Klikom na dugme „**Next**“, otvara se finalni ekran na kome je potrebno kliknuti dugme „**Finish**“. Nakon toga prikazaće se poruka o uspešno izvršenom importu Issuer CA sertifikata, kao na slici ispod.



4. Instalacija drajvera za Smart Card čitače

Drajveri za Smart Card čitače, koje je moguće kupiti uz kvalifikovane sertifikate, se uglavnom automatski instaliraju na Windows računarima (10 i 11) prilikom prvog priključivanja čitača putem USB-a.

Ukoliko je instalacija uspešna, u „Device Manager-u“ pod nodom „Smart card readers“ prikazaće se ime priključenog čitača, kao na slici ispod.



U slučaju da nastane problem prilikom automatske instalacije drajvera, uvek možete drajvere instalirati ručno koristeći datoteku koja se nalazi u folderu "Smart Card Reader Drivers" unutar instalacionog paketa. U zavisnosti od proizvođača smart card čitača, odgovarajući drajveri se nalaze u folderima:

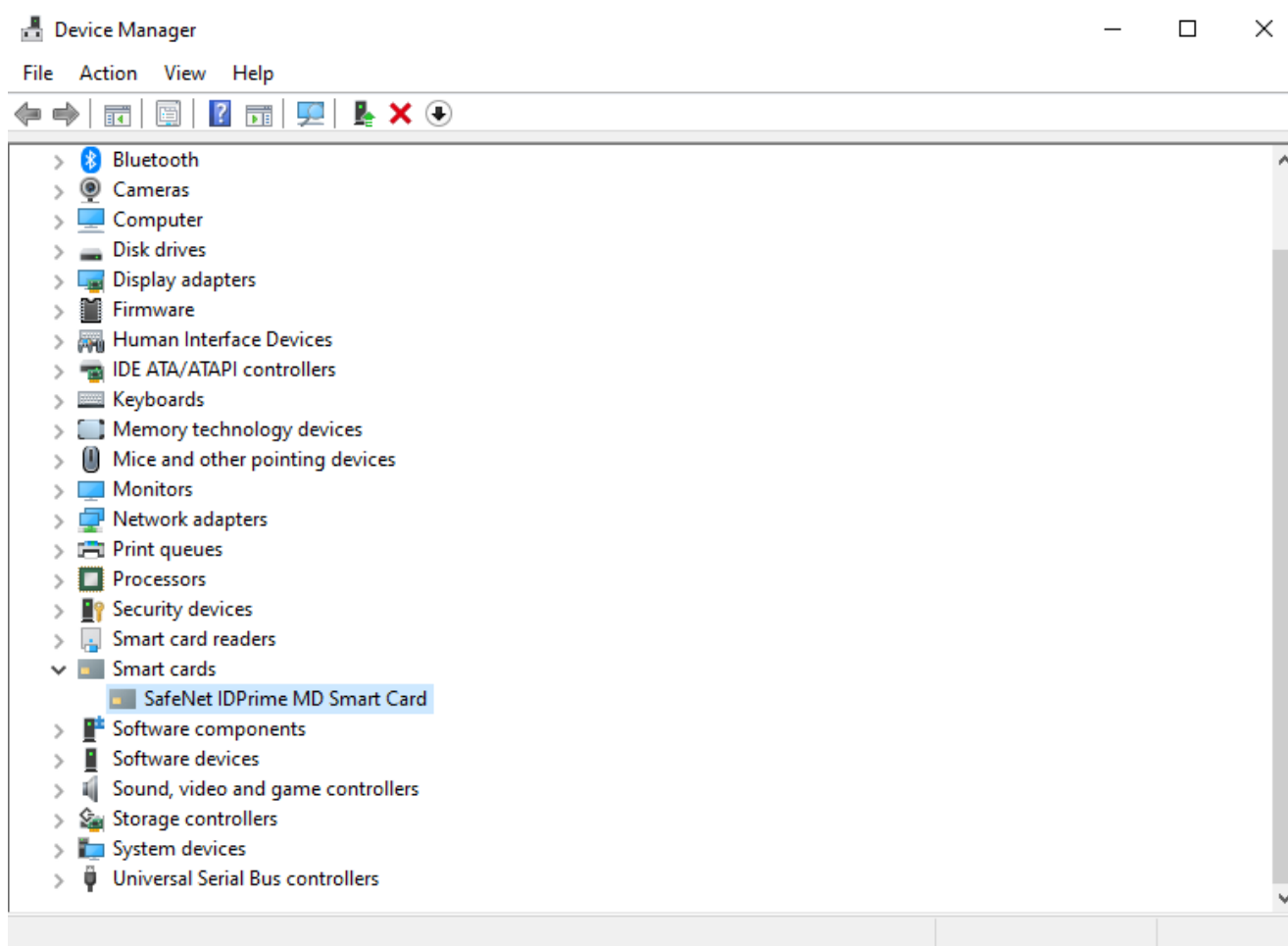
- Za ACS smart card čitače instalirajte drajver koji se nalazi u folderu "ACS Drivers",
- Za Thales/Gemalto smart card čitače instalirajte drajver koji se nalazi u folderu "Thales - Gemalto Drivers (CT30-CT40-K50-K30)".

5. Instalacija ESS QCA SafeNet Minidriver & PKCS11 paketa

Kako bi Windows 10 i 11 računar prepoznao čip na kome se nalazi kvalifikovani sertifikat za elektronski potpis neophodno je instalirati drajver (MiniDriver).

U folderu „**ESS_QCA_Windows_Installer**“ se nalazi folder „**SafeNet Minidriver & PKCS11**“ u kome se nalaze MSI paketi za 32-bit, 64-bit i arm64 verziju Windows operativnog sistema. U okviru paketa se instalira i PKCS11 biblioteka koja služi za potrebe potpisivanja na aplikacijama kao što su: ePorezi, eUprava, NexU-APR, CROSO, CEOP, itd...

Nakon uspešne instalacije, u „Device Manager-u“ pod nodom „Smart cards“ prikazaće se ime kartice koja je prethodno ubačena u povezan USB smart card čitač.



Ukoliko dođe do eventualnih problema, molimo Vas, pošaljite tiket putem [web forme](#) ili napišite mail na gca@esshitsupport.zohodesk.eu, a mi ćemo Vas u najkraćem roku kontaktirati.

6. Aplikacija za promenu i deblokadu PIN-a

Na ESS QCA web strani za [Preuzimanje i instalacija softvera](#) u delu **Korisničke aplikacije** možete pronaći link za preuzimanje [aplikacije za promenu i deblokadu PIN-a](#).

Neophodni preduslovi za korišćenje aplikacije su .net framework 4.5 (ili viši) i poslednja verzija SafeNet Minidrivera za IDPrime smart kartice (videti poglavlje 5 i 6). Ukoliko ovi uslovi nisu ispunjeni, prilikom pokretanja aplikacije, otvoriće Vam se sledeći prozor:



6.1. Promena PIN-a

Preporuka je da se inicijalni PIN kod, koji uz uređaj dobijete u PIN koverti, nakon prve upotrebe promeni. Promenu PIN-a možete izvršiti i bilo kada u toku trajanja sertifikata.

Potrebno je da uz sebe imate svoj QSCD uređaj sa kvalifikovanim sertifikatom - smart karticu (i odgovarajući čitač) ili USB token, kao i PIN kovertu u kojoj se nalazi PIN kod.

Pokretanjem aplikacije, vrši se detekcija svih čitača smart kartica. Ukoliko nemate nijedan ili imate više QSCD uređaja koji su u čitačima ili računaru, pojaviće Vam se jedan od prozora sa slike.

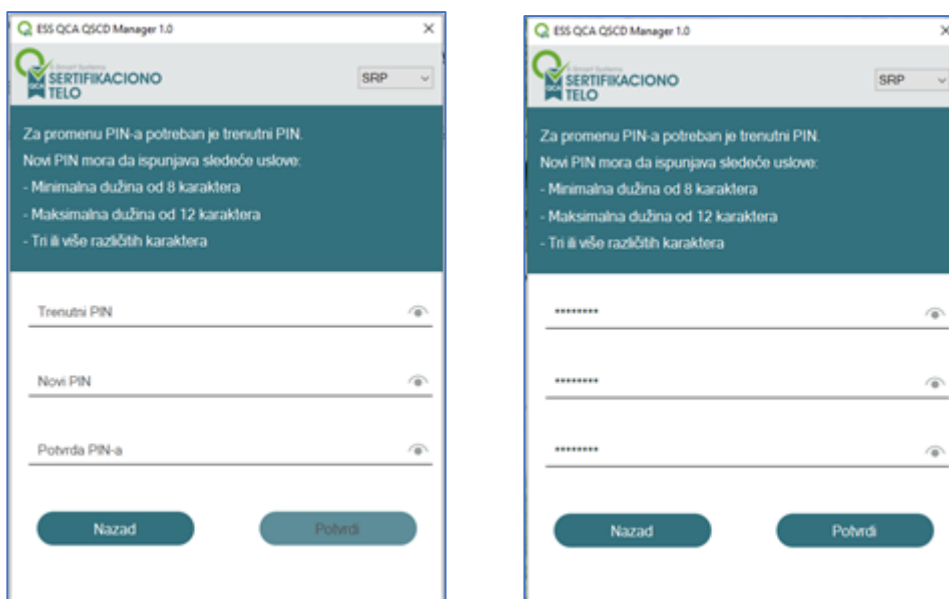


Aplikacija prelazi u aktivan režim rada samo kada pronade **jedan** personalizovani QSCD uređaj sa ESS QCA kvalifikovanim sertifikatom.

Aplikacija će automatski prikazati podatke o tipu povezanog uređaja, podatke iz Subject-a sertifikata kao i preostali broj unosa PIN-a (za **SSCD V1** i **SSCD V2** uređaje – leva slika ispod) ili preostali broj unosa PIN-a i PUK-a za uređaje **QSCD V3** (desna slika ispod).

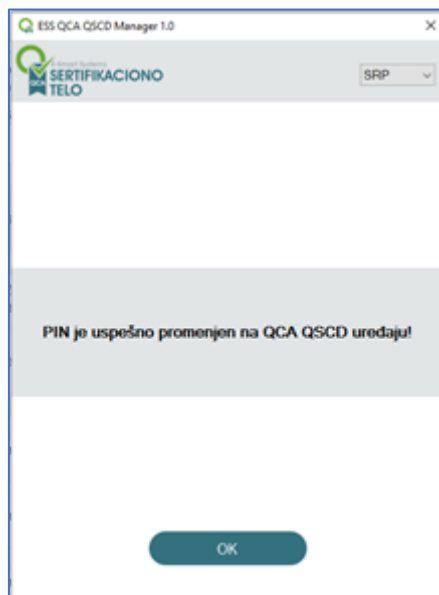


Klikom na dugme **Promeni PIN**, otvara se prozor za promenu PIN-a gde je potrebno popuniti prazna polja, i to: **Trenutni PIN** (ukoliko ga niste ranije menjali, onda je to PIN koji se nalazi u PIN koverti koju ste dobili uz QSCD uređaj), **Novi PIN** i još jednom je potrebno u polje **Potvrda PIN-a** uneti vrednost novog PIN-a.



Na svakom polju koje popunjavate postoji opcija pregleda (klikom na „oko“) i izmene unetih podataka čime se smanjuje mogućnost greške.

Ukoliko ste popunili sva potrebna polja prateći i poštujući uputstva na samoj aplikaciji, klikom na dugme **Potvrdi**, PIN Vašeg QSCD uređaja biće podešen na novu, željenu vrednost. U prozoru će se pojaviti poruka „PIN je uspešno promenjen na QCA QSCD uređaju!“.



Ukoliko ste iskoristili dozvoljen maksimalan broj za pogrešan unos trenutnog PIN-a, PIN kod, samim tim i QSCD uređaj, će biti blokiran.

Deblokadu/otključavanje svih tipova uređaja možete izvršiti u ESS QCA. Potrebno je da podnesete [zahtev za deblokadu](#) i javite se ESS QCA podršci, kako biste u ESS QCA prostorijama, uz lično prisustvo i donet blokirani uređaj izvršili deblokadu istog. Tom prilikom će Vam biti izdata nova PIN koverta.

Deblokada PIN-a na uređajima tipa **QCA QSCD V3** može se takođe izvršiti preko aplikacije - **QCA QSCD Manager**, a opis ovog postupka nalazi se u nastavku ovog dokumenta.

6.2. Deblokada PIN-a

NAPOMENA: Samo za uređaje tipa **QCA QSCD V3** deblokadu možete izvršiti i preko aplikacije **QCA QSCD Manager**. Neophodno je da uz sebe imate blokirani uređaj, kao i PIN kovertu koju ste dobili uz uređaj, a u kojoj se, osim PIN-a, nalazi i PUK kod koji se koristi za deblokadu/otključavanje ovog tipa uređaja.

Pokretanjem aplikacije, vrši se detekcija svih čitača smart kartica. Aplikacija prelazi u aktivan režim rada samo kada pronađe jedan personalizovani QSCD uređaj sa **ESS QCA** kvalifikovanim sertifikatom.

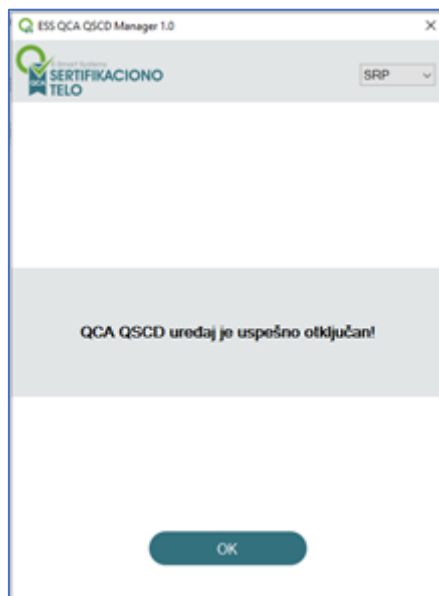


Aplikacija će automatski prikazati tip povezanog uređaja i podatke iz Subject-a sertifikata, preostali broj pokušaja unosa PIN-a koji je u ovom slučaju 0 (nula), kao i preostali broj pokušaja unosa PUK-a.

Klikom na dugme **Otključaj uređaj** otvara se prozor za deblokadu PIN-a. Potrebno je popuniti prazna polja, pre svega **PUK** kod koji se nalazi u PIN koverti koju ste dobili uz uređaj, zatim polja **Novi PIN** i **Potvrda PIN-a**. Na svakom polju koje popunjavate postoji i opcija pregleda unetih podataka (klikom na „oko“) koja smanjuje mogućnost greške.



Ukoliko ste popunili sva potrebna polja prateći i poštujući uputstva na samoj aplikaciji, klikom na dugme **Potvrdi**, PIN kod Vašeg QSCD uređaja biće podešen na novu, željenu vrednost, a sam uređaj otključan. U prozoru će se pojaviti i poruka „QCA QSCD uređaj je uspešno otključan!“.



U slučaju da ste u procesu deblokade PIN-a uneli pogrešan PUK dva (2) puta, samostalna deblokada PIN-a više nije moguća.



U tom slučaju, deblokada/otključavanje uređaja može se izvršiti samo od strane ESS QCA. Potrebno je da podnesete [zahtev za deblokadu](#) i javite se ESS QCA podršci, kako biste u ESS QCA prostorijama, uz lično prisustvo i donet blokirani uređaj, izvršili deblokadu istog. Tom prilikom će Vam biti izdata nova PIN koverta sa novim vrednostima PIN i PUK koda.

Klikom na dugme **Pomoć**, otvoriće se kontakt podaci ESS QCA podrške.