

U-QCA-304

Šifra dokumenta

Uputstvo za instalaciju prerekvizita za rad sa kvalifikovanim sertifikatom za elektronski potpis i pečat - macOS

Sadržaj

1. Preuzimanje ESS QCA instalacionog paketa za macOS	3
2. Instalacija ESS QCA „lanca poverenja“	3
2.1. Importovanje Root CA sertifikata	3
2.1.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.....	3
2.1.2. Za kvalifikovane sertifikate za elektronski potpis i pečat izdate posle 08.04.2024.....	5
2.2. Importovanje Issuer CA sertifikata	7
2.2.1. Za kvalifikovane sertifikate za elektronski potpis izdate pre 08.04.2024.....	7
2.2.2. Za kvalifikovane sertifikate za elektronski potpis izdate posle 08.04.2024.	9
2.2.3. Za kvalifikovane sertifikate za elektronski pečat.....	11
3. Instalacija ESS QCA SafeNet Authentication Client middleware na macOS	12
4. Instalacija drajvera za Thales-Gemalto čitače pametnih kartica na macOS	14
5. Instalacija drajvera za ACS čitače pametnih kartica na macOS	14
6. Test uspešnosti instalacije prerekvizita za rad sertifikata na macOS	15

1. Preuzimanje ESS QCA instalacionog paketa za macOS

Instalacioni paket sa svim neophodnim komponentama može biti preuzet sa ESS QCA sajta - <https://essqca.e-smartsys.com> na stranici "Preuzimanje softvera", klikom na link "ESS QCA macOS instalacioni paket".

Pre same upotrebe zip datoteku treba otpakovati. Pronaći datoteku u folderu Downloads ili na Desktopu i dvoklikom na nju počinje postupak otpakivanja.

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

2. Instalacija ESS QCA „lanca poverenja“

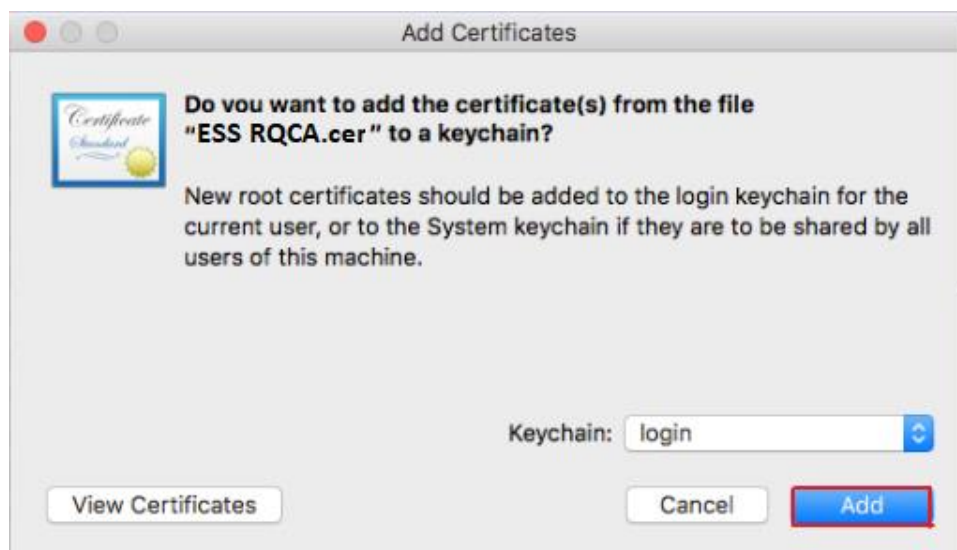
ESS QCA „lanac poverenja“ sastoji se od Root CA i Issuer CA sertifikata koji se nalaze unutar foldera „Certificates“ instalacionog paketa. Ovi sertifikati moraju biti importovani u lokalni računar na macOS mašini kako bi se uspostavilo poverenje između mašine i sertifikata korisnika.

2.1. Importovanje Root CA sertifikata

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

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

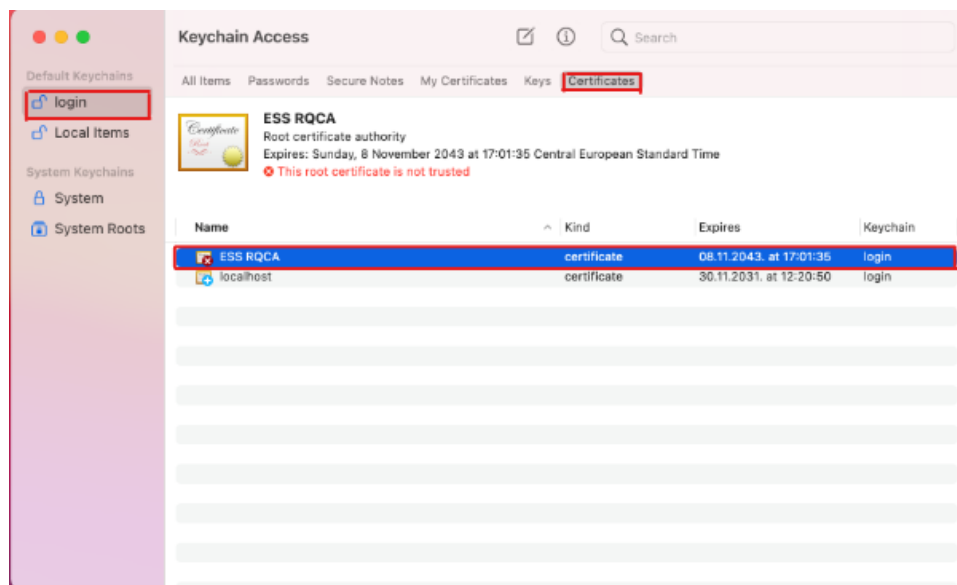
- 1) Potrebno je dvoklikom otvoriti „ESS RQCA.cer“ sertifikat. U zavisnosti od prava vašeg naloga i broja korisnika na toj mašini, importovanje je moguće na 2 načina I to:
 - a) Ukoliko ima samo 1 nalog I/ili imate sva prava na toj mašini, dvoklik na „ESS RQCA.cer“ sertifikat, importovanje započinje automatski.
 - b) Ukoliko ima više naloga I/ili nemate sva prava na toj mašini, dvoklik na „ESS RQCA.cer“ sertifikat, otvara se prozor verifikacije importa, na kojem morate izabrati opciju Keychain-a "Login", kao što je prikazano na slici 1, I klikom na dugme "Add" započinje se proces importovanja.



Slika 1.

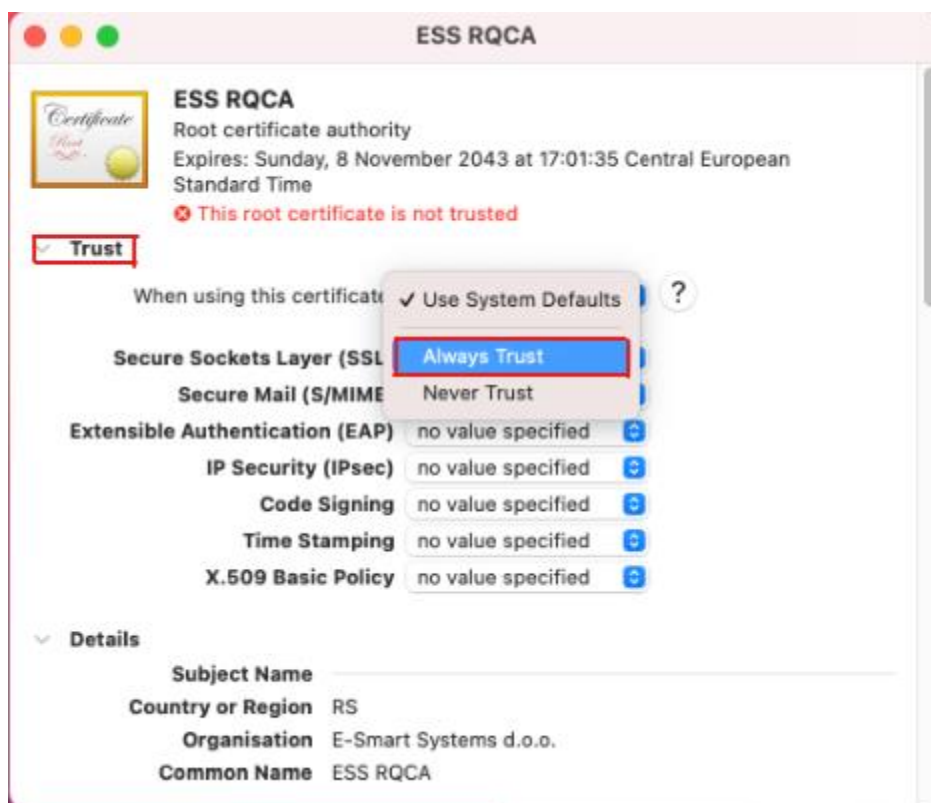
- 2) Da bi sertifikat „ESS RQCA.cer“ bio validan, potrebno je otići u aplikaciju "Keychain Access", a nju možete pronaći na sledeći način, Launchpad > Other (folder) > Keychain Access. Da bi stavili sertifikat kao trusted, potrebno je uraditi sledeće:

- a) Pronaći sertifikat „ESS RQCA.cer“, Keychain Login > Certificates > ESS RQCA, prikazano na slici 2.



Slika 2.

- b) Dvoklikom na sertifikat „ESS RQCA.cer“ otvaraju se detalji sertifikata, raširite polje “Trust” kako bi videli dodatna podešavanja.
a) Kliknite na polje “When using this certificate” izaberite opciju “Always trust”, prikazano na slici 3.



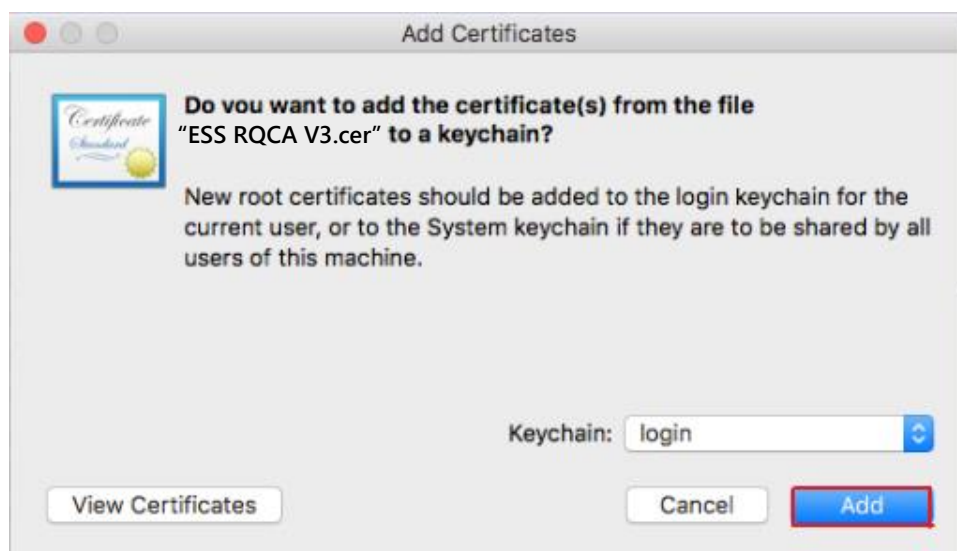
Slika 3.

Izađite na **x** iz tog prozora da bi se podešavanja sačuvala, unesite password vašeg usera ako mašina to bude tražila i samim tim, proces importovanja ESS RQCA bi bio završen.

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

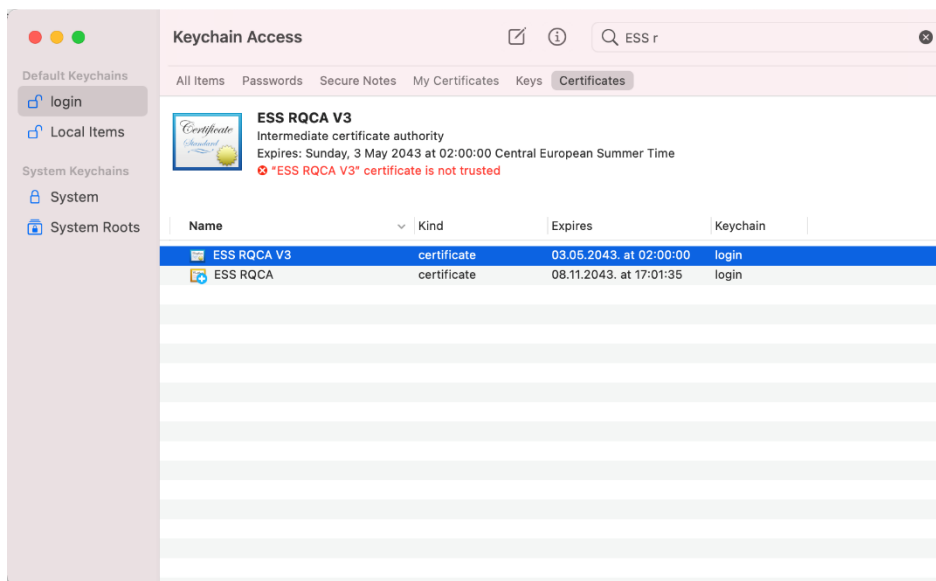
Root CA (ESS RQCA) sertifikat je moguće importovati na sledeći način:

- 1) Potrebno je dvoklikom otvoriti „ESS RQCA V3.cer“ sertifikat. U zavisnosti od prava vašeg naloga i broja korisnika na toj mašini, importovanje je moguće na 2 načina I to:
 - a) Ukoliko ima samo 1 nalog I/ili imate sva prava na toj mašini, dvoklik na „ESS RQCA V3.cer“ sertifikat, importovanje započinje automatski.
 - b) Ukoliko ima više naloga I/ili nemate sva prava na toj mašini, dvoklik na „ESS RQCA V3.cer“ sertifikat, otvara se prozor verifikacije importa, na kojem morate izabrati opciju Keychain-a “Login”, kao što je prikazano na slici 4, I klikom na dugme “Add” započinje se proces importovanja.



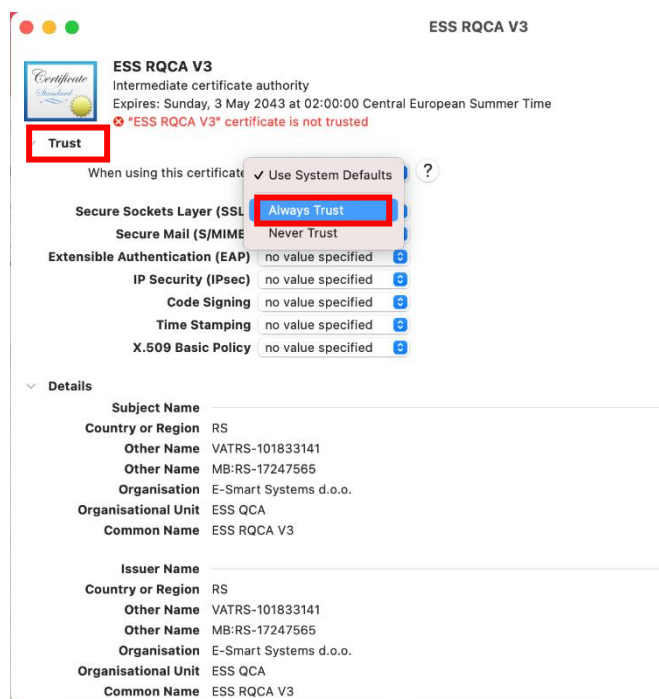
Slika 4.

- 2) Da bi sertifikat „ESS RQCA V3.cer“ bio validan, potrebno je otići u aplikaciju “Keychain Access”, a nju možete pronaći na sledeći način, Lauchpad > Other (folder) > Keychain Access. Da bi stavili sertifikat kao trusted, potrebno je uraditi sledeće:
 - a) Pronaći sertifikat „ESS RQCA V3.cer“, Keychain Login > Certificates > ESS RQCA V3, prikazano na slici 5.



Slika 5.

- Dvoklikom na sertifikat „ESS RQCA V3.cer“ otvaraju se detalji sertifikata, raširite polje “Trust” kako bi videli dodatna podešavanja.
- Kliknite na polje “When using this certificate” izaberite opciju “Always trust”, prikazano na slici 6.



Slika 6.

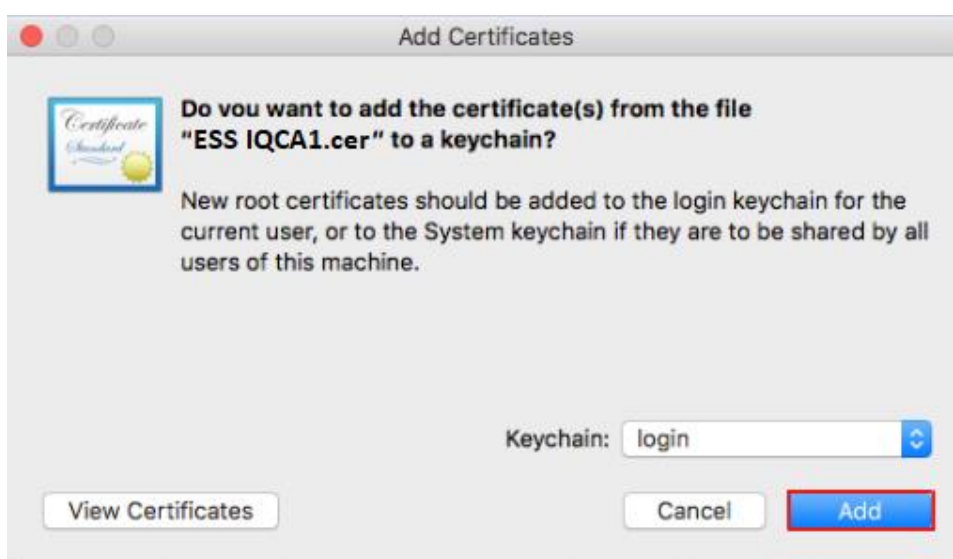
Izađite na x iz tog prozora da bi se podešavanja sačuvala, unesite password vašeg usera ako mašina to bude tražila i samim tim, proces importovanja ESS RQCA V3 bi bio završen.

2.2. Importovanje Issuer CA sertifikata

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

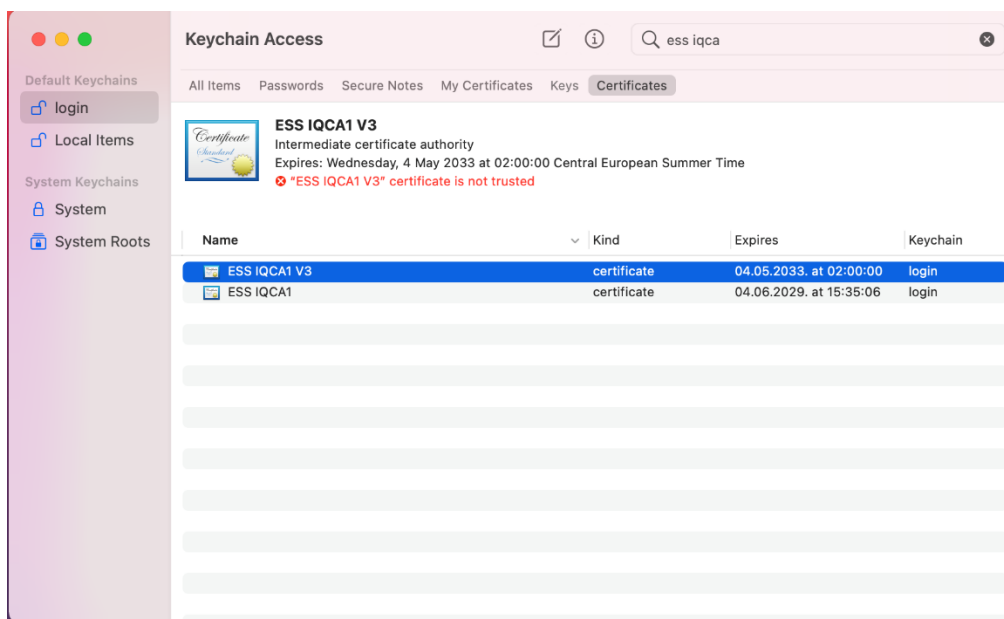
Issuer CA (ESS IQCA) sertifikat je moguće importovati na sledeći način:

- 1) Potrebno je dvoklikom otvoriti „ESS IQCA1(3).cer“ sertifikat i izvršiti postupak importovanja. U zavisnosti od prava vašeg naloga i broja korisnika na toj mašini, importovanje je moguće na 2 načina i to:
 - a) Ukoliko ima samo 1 nalog i/ili imate sva prava na toj mašini, dvoklik na „ESS IQCA1(3).cer“ sertifikat, importovanje započinje automatski.
 - b) Ukoliko ima više naloga i/ili nemate sva prava na toj mašini, dvoklik na „ESS IQCA1(3).cer“ sertifikat, otvara se prozor verifikacije importa, na kojem morate izabrati opciju Keychain-a “Login”, kao što je prikazano na slici 7, i klikom na dugme “Add” započinje se proces importovanja.



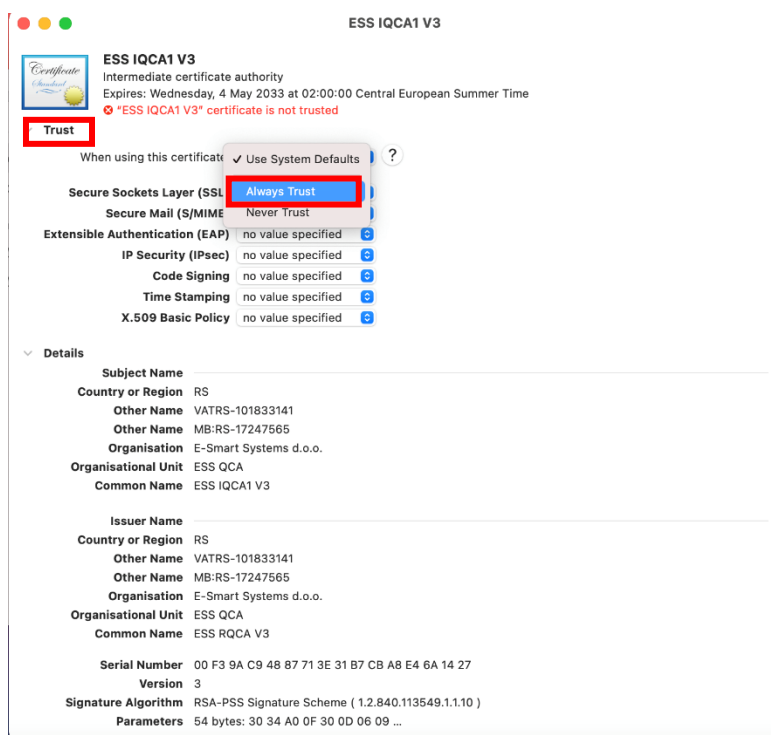
Slika 7.

- 2) Da bi sertifikat „ESS IQCA1(3).cer“ bio validan, potrebno je otići u aplikaciju “Keychain Access”, a nju možete pronaći na sledeći način, Launchpad > Other (folder) > Keychain Access. Da bi stavili sertifikat kao trusted, potrebno je uraditi sledeće:
 - a) Pronaći sertifikat „ESS IQCA1(3).cer“, Keychain Login > Certificates > ESS IQCA1, prikazano na slici 8.



Slika 8.

- b) Dvoklikom na sertifikat „ESS IQCA1(3).cer“ otvaraju se detalji sertifikata, raširite polje “Trust” kako bi videli dodatna podešavanja.
- c) Kliknite na polje “When using this certificate” izaberite opciju “Always trust”, prikazano na slici 9.



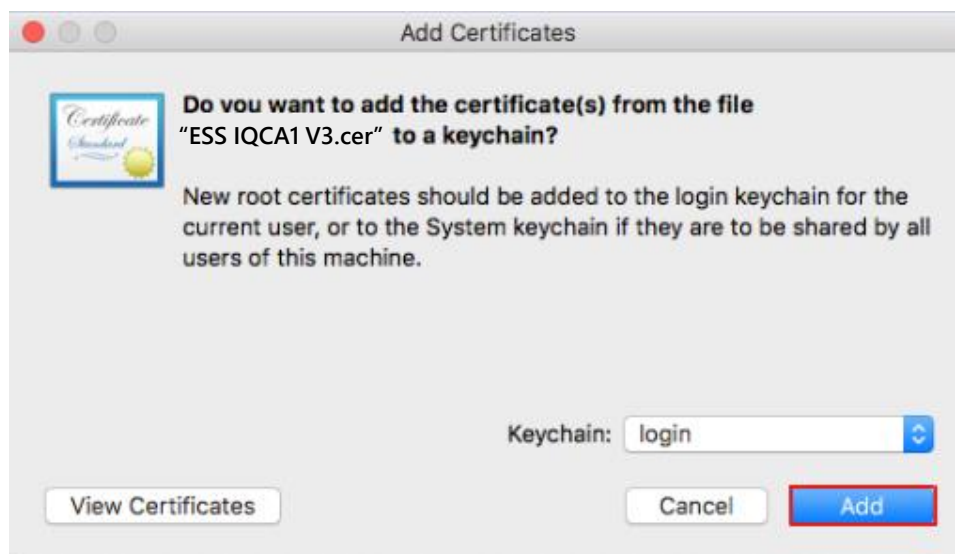
Slika 9.

Izađite na **x** iz tog prozora da bi se podešavanja sačuvala, unesite password vašeg usera ako mašina to bude tražila i samim tim, proces importovanja ESS IQCA1(3) bi bio završen.

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

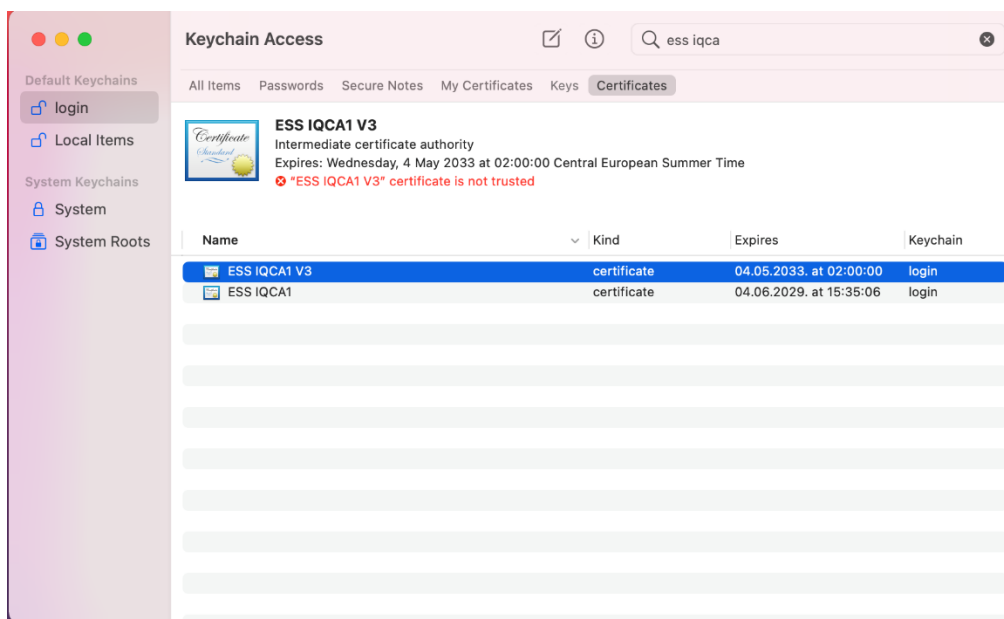
Issuer CA (ESS IQCA) sertifikat je moguće importovati na sledeći način:

- 1) Potrebno je dvoklikom otvoriti „ESS IQCA1 V3.cer“ sertifikat i izvršiti postupak importovanja. U zavisnosti od prava vašeg naloga i broja korisnika na toj mašini, importovanje je moguće na 2 načina i to:
 - a) Ukoliko ima samo 1 nalog i/ili imate sva prava na toj mašini, dvoklik na „ESS IQCA1 V3.cer“ sertifikat, importovanje započinje automatski.
 - b) Ukoliko ima više naloga i/ili nemate sva prava na toj mašini, dvoklik na „ESS IQCA1 V3.cer“ sertifikat, otvara se prozor verifikacije importa, na kojem morate izabrati opciju Keychain-a „Login“, kao što je prikazano na slici 10, i klikom na dugme „Add“ započinje se proces importovanja.



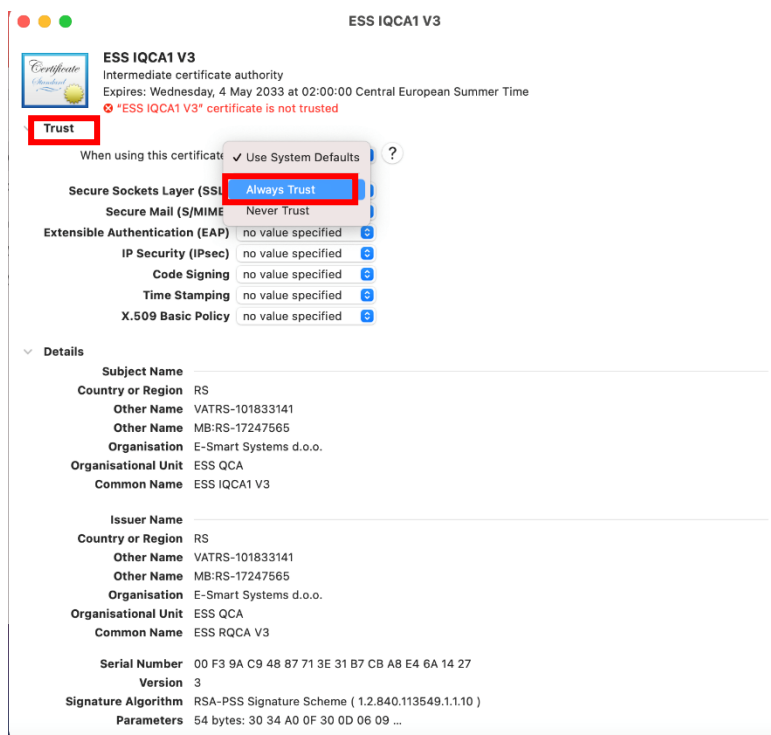
Slika 10.

- 2) Da bi sertifikat „ESS IQCA1 V3.cer“ bio validan, potrebno je otići u aplikaciju „Keychain Access“, a nju možete pronaći na sledeći način, Launchpad > Other (folder) > Keychain Access. Da bi stavili sertifikat kao trusted, potrebno je uraditi sledeće:
 - a) Pronaći sertifikat „ESS IQCA1 V3.cer“, Keychain Login > Certificates > ESS IQCA1 V3, prikazano na slici 11.



Slika 11.

- b) Dvoklikom na sertifikat „ESS IQCA1 V3.cer“ otvaraju se detalji sertifikata, raširite polje “Trust” kako bi videli dodatna podešavanja.
- c) Kliknite na polje “When using this certificate” izaberite opciju “Always trust”, prikazano na slici 12.



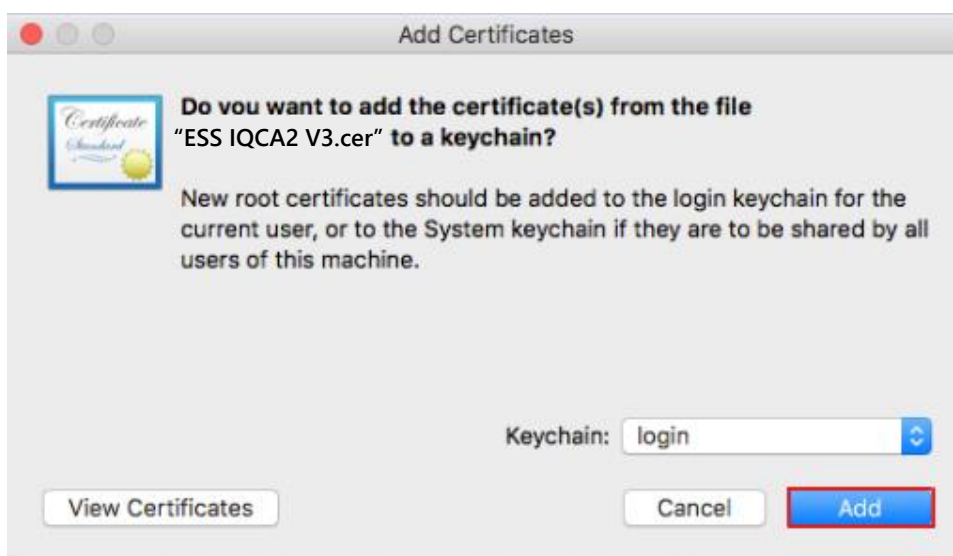
Slika 12.

Izađite na x iz tog prozora da bi se podešavanja sačuvala, unesite password vašeg usera ako mašina to bude tražila i samim tim, proces importovanja ESS IQCA1 V3 bi bio završen.

2.2.3. Za kvalifikovane sertifikate za elektronski pečat

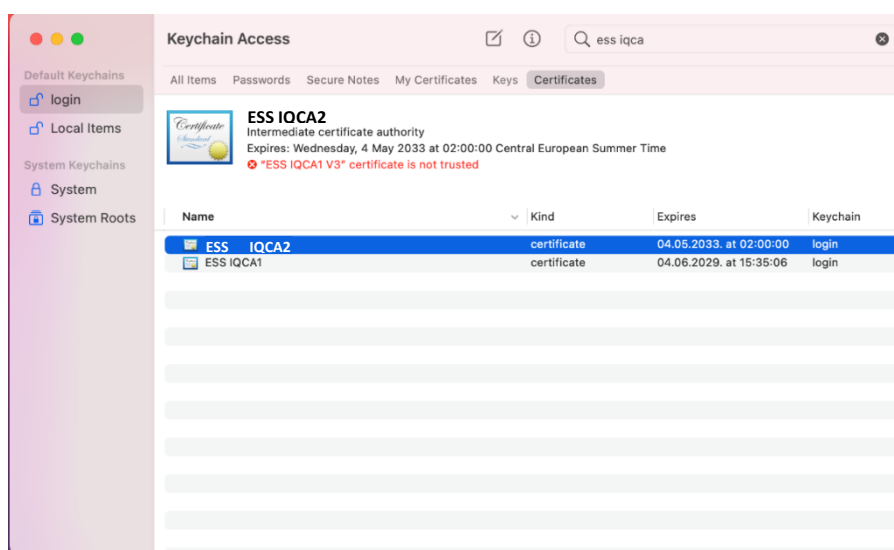
Issuer CA (ESS IQCA) sertifikat je moguće importovati na sledeći način:

- 1) Potrebno je dvoklikom otvoriti „ESS IQCA2 V3.cer“ sertifikat i izvršiti postupak importovanja. U zavisnosti od prava vašeg naloga i broja korisnika na toj mašini, importovanje je moguće na 2 načina i to:
 - a) Ukoliko ima samo 1 nalog i/ili imate sva prava na toj mašini, dvoklik na „ESS IQCA2 V3.cer“ sertifikat, importovanje započinje automatski.
 - b) Ukoliko ima više naloga i/ili nemate sva prava na toj mašini, dvoklik na „ESS IQCA2 V3.cer“ sertifikat, otvara se prozor verifikacije importa, na kojem morate izabrati opciju Keychain-a „Login“, kao što je prikazano na slici 13, i klikom na dugme „Add“ započinje se proces importovanja.



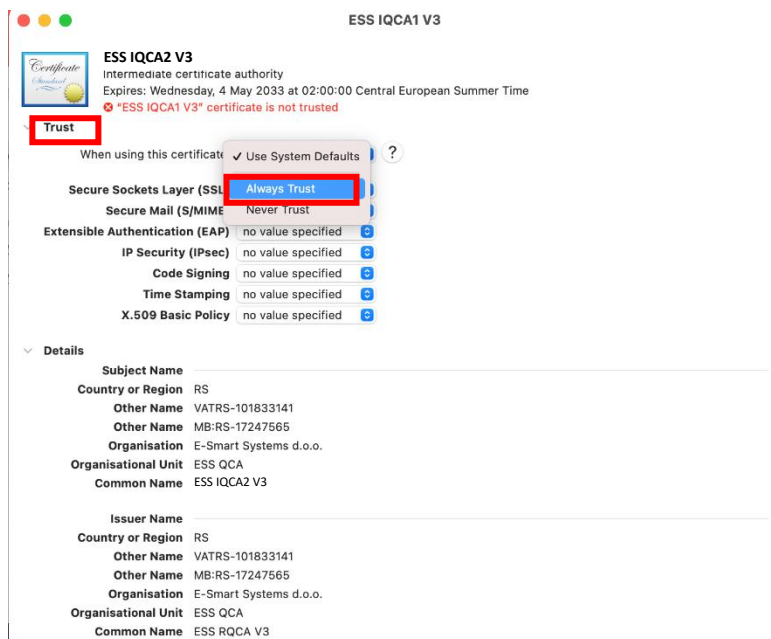
Slika 13.

- 2) Da bi sertifikat „ESS IQCA2 V3.cer“ bio validan, potrebno je otići u aplikaciju „Keychain Access“, a nju možete pronaći na sledeći način, Lauchpad > Other (folder) > Keychain Access. Da bi stavili sertifikat kao trusted, potrebno je uraditi sledeće:
 - a) Pronaći sertifikat „ESS IQCA2 V3.cer“, Keychain Login > Certificates > ESS IQCA2 V3, prikazano na slici 14.



Slika 14.

- b) Dvoklikom na sertifikat „ESS IQCA1 V3.cer“ otvaraju se detalji sertifikata, raširite polje “Trust” kako bi videli dodatna podešavanja.
- c) Kliknite na polje “When using this certificate” izaberite opciju “Always trust”, prikazano na slici 15.



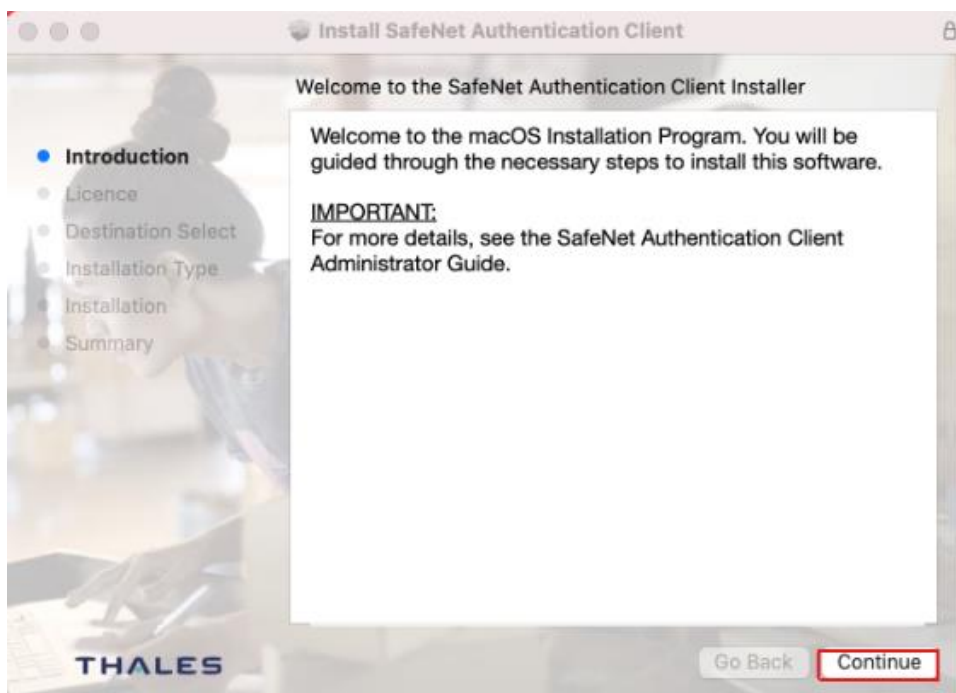
Slika 15.

Izađite na **x** iz tog prozora da bi se podešavanja sačuvala, unesite password vašeg usera ako mašina to bude tražila i samim tim, proces importovanja ESS IQCA1 V3 bi bio završen.

3. Instalacija ESS QCA SafeNet Authentication Client middleware na macOS

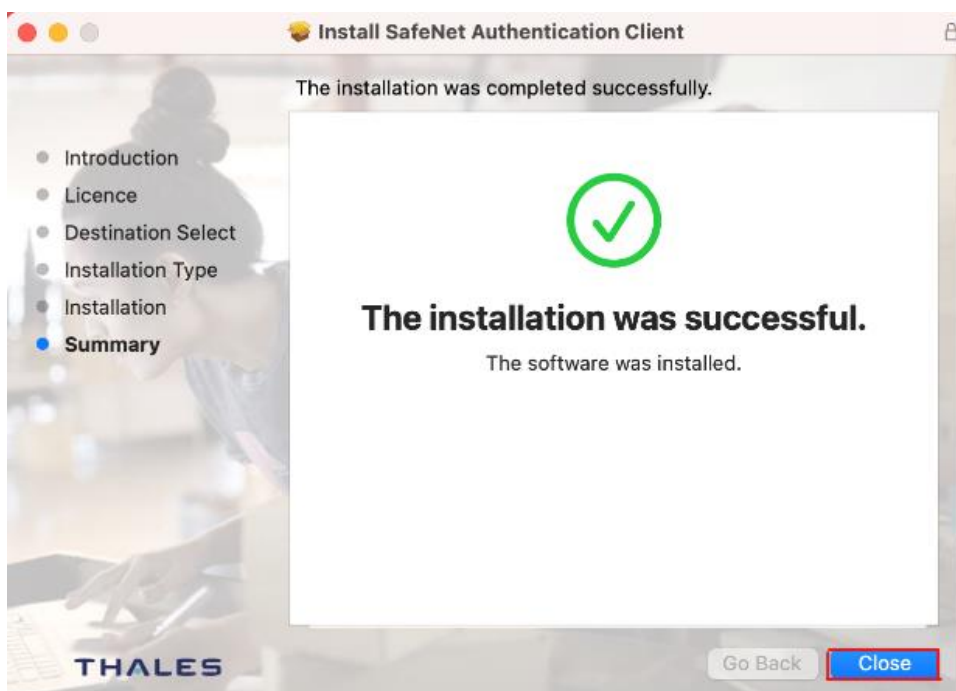
Kako bi macOS računar prepoznao čip na kome se nalazi kvalifikovani sertifikat za elektronski potpis neophodno je instalirati drajver (SafeNet Authentication Client). U folderu „SafeNet Authentication Client macOS“ se nalazi instalacioni paket za middleware.

Dvoklikom na fajl “SafeNetAuthenticationClient.10.9.4565.0.dmg” izvršava se odpakovanje fajla, a zatim je potrebno pokrenuti instalacioni paket. (“SafeNetAuthenticationClient.10.9.4565.0 Core.dmg” je verzija bez UI Client-a) Dvoklikom na paket “SafeNet Authentication Client 10.9.pkg” pokreće se instalacija kao što je prikazano na slici 16.



Slika 16.

Da bi instalacija bila uspešna potrebno je kliknuti na “Continue”, opet “Continue”, izlazi prozor verifikacije koraka, kliknuti na “Agree”, i konačno na dugme “Install” (Ukoliko imate login password ili pin, izaći će I taj prozor i samo unesite kako bi nastavili sa instalacijom). Ukoliko je proces instalacije završen, videćete uspešno instaliranje prvog paketa, kao što je prikazano na slici 17. Kliknite na dugme “Close” i nastavite dalje.



Slika 17.

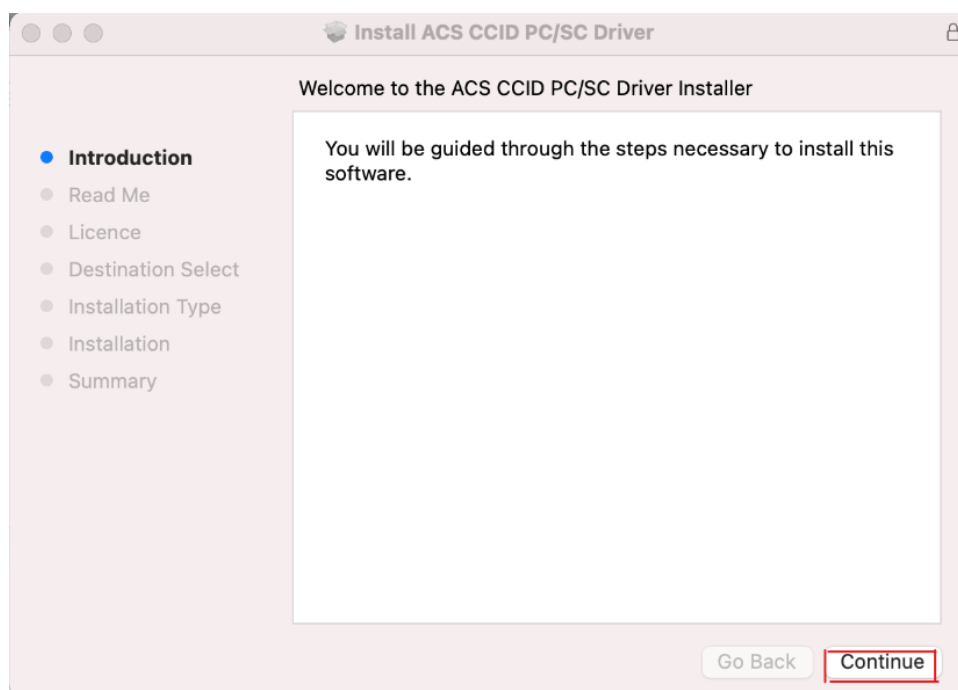
Ukoliko dođe do eventualnih problema, molimo Vas, pošaljite tiket putem [web forme](#) ili napišite mail na gca@esshitsuport.zohodesk.eu, a mi ćemo Vas u najkraćem roku kontaktirati.

4. Instalacija drajvera za Thales-Gemalto čitače pametnih kartica na macOS

U slučaju da macOS ne prepozna Thales/Gemalto čitač pametnih kartica, preporučuje se instalacija priloženog drajvera. MacOS drajver za Thales-Gemalto čitače pametnih kartica nalazi se u folderu „Thales - Gemalto Driver macOS“, a instalira se tako što se raspakuje i pokrene „ccid-installer1.7.0.dmg“.

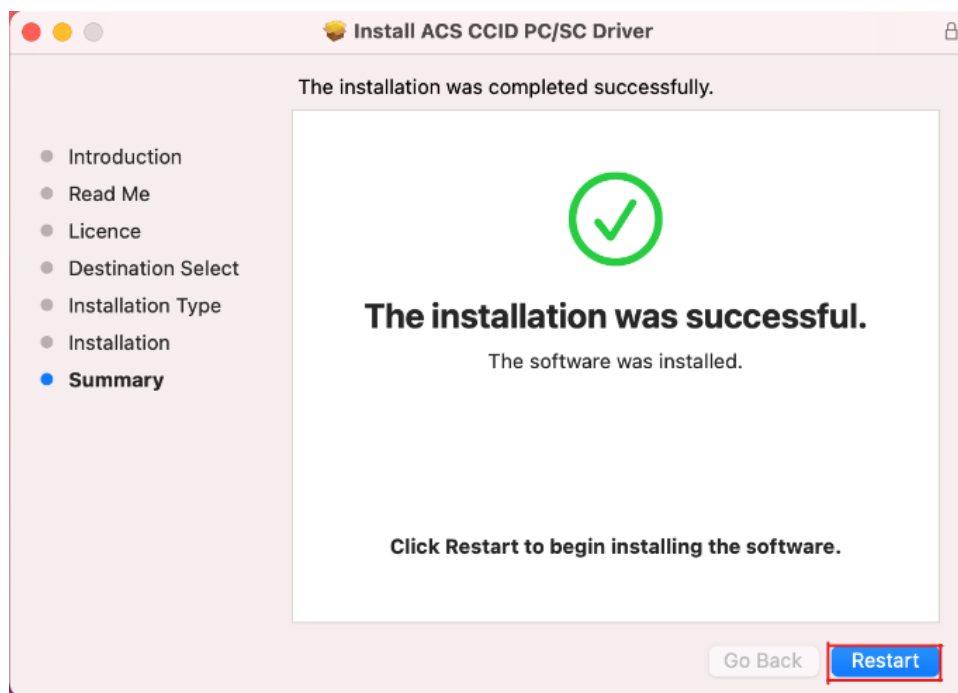
5. Instalacija drajvera za ACS čitače pametnih kartica na macOS

Ukoliko imate verziju macOS 14.1 i više (macOS Sonoma), možda će biti potrebno instalirati drajver za ACS ACR čitače pametnih kartica. Paket za ACS Driver se nalazi u folderu „ACS driver macOS“. Dvoklik na fajl „acscid_installer-1.1.13“ izvršava se odpakovanje fajla i zatim je potrebno pokrenuti instalacioni paket, dvoklikom na paket „acscid_installer.pkg“ pokreće se instalacija kao što je prikazano na slici 18.



Slika 18.

Da bi instalacija bila uspešna potrebno je kliknuti na “Continue”, zatim “Continue”, opet “Continue” da bi potvrdili polisu, izlazi prozor verifikacije koraka, kliknuti na “Agree”, i konačno na dugme “Install” (Ukoliko imate login password ili pin, izaći će i taj prozor i samo unesite kako bi nastavili sa instalacijom). Ukoliko je proces instalacije završen, videćete uspešno instaliranje prvog paketa, kao što je prikazano na slici 19. Kliknite na dugme “Restart” i nakon restarta možete isprobati rad sa sertifikatom.



Slika 19.

6. Test uspešnosti instalacije prerekvizita za rad sertifikata na macOS

Kao potvrda uspešnosti instalacije svih neophodnih prerekvizita za rad na MAC OS mašini, nakon instalacije prikazaže se ikonica SafeNeta u headeru, kao što je prikazano na slici 20 (Napomena: ukoliko nemate ovu ikonicu, potrebno je pronaći SafeNet klijenta u launchpadu i pokrenuti ga).



Slika 20.

Kada ubacite u računar vaš sertifikat, SafeNeta u headeru će zasvetleti kao što je prikazano na slici 21, to znači da računar spreman za rad sa sertifikatom.



Slika 21.

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