E-Smart Systems d.o.o. | **Adress:** Kneza Višeslava 70a, 11030 Belgrade, Serbia | **Sertification authority (ESS QCA)** | **Tel:** 011 3050280| **E-mail:** qca@e-smartsys.com | MB: **17247565 , Reg.No: 01117247565 , Bussiness code: 6201, VAT: 101833141**

U-QCA-304

Document code

Instructions for installing prerequisites for working with qualified certificate for electronic signature and seal – macOS

Contents

1. Downloading the ESS QCA installation package for macOS

The installation package with all necessary components can be downloaded from the ESS QCA website - https://essqca.e-smartsys.com on the "**Download software"** page, by clicking the link "**ESS QCA macOS Installation package"**.

Before use make sure to unpack the zip package. Locate the file in the Downloads folder or in the desktop folder and double click the file to unpack it. After this step you can begin installing the necessary software components for using the ESS QCA qualified certificate for electronic signatures.

2. Installing the ESS QCA chain of trust

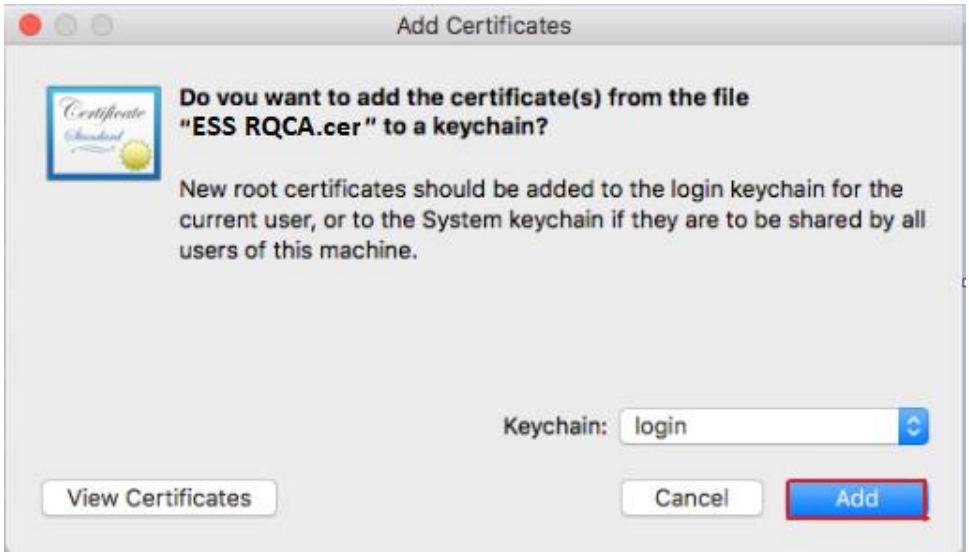
ESS QCA **chain of trust** consists of the Root CA and Issuer CA certificates which are located inside the „**Ceritificates"** folder inside the installation package. These certificates must be imported to the local MACOS computer to establish the trust between the machine and user certificate.

2.1. Importing the Root CA certificate

2.1.1. For qualified certificates for electronic signature issued before 08.04.2024.

Root CA (ESS RQCA) can be imported in the following way:

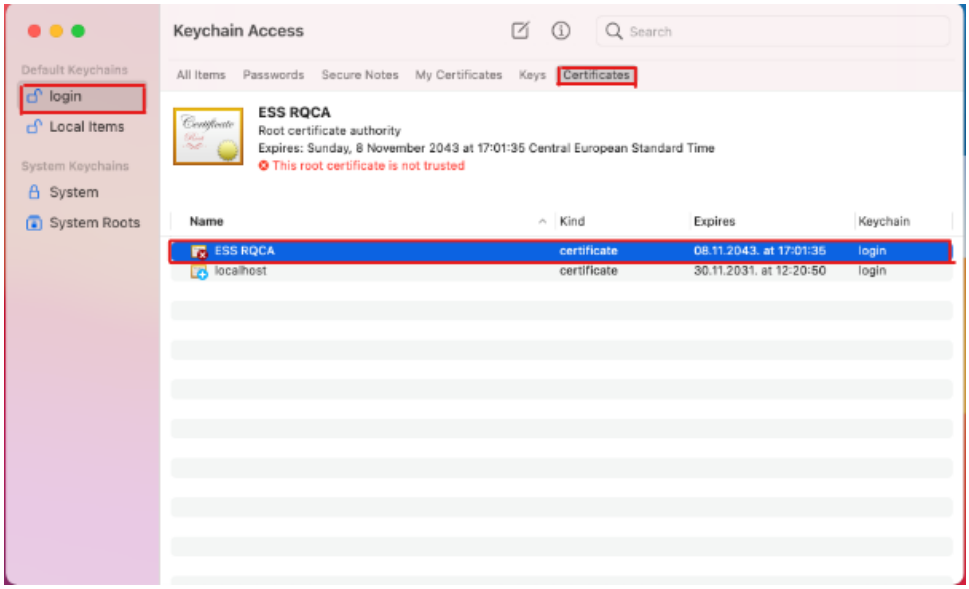
1. Double-clicking the "ESS RQCA.cer" certificate. Depending on the rights of the user and the number of users present on the machine, importing can be done in two ways:
   a) If there is only 1 user account and/or if you have all user rights on the machine, double-clicking the "ESS RQCA.cer" certificate, importing begins automatically.
   b) If there are more accounts and/or you don't have all the user rights on the machine, double-clicking the "ESS RQCA.cer" certificate will open the import verification window where you must choose the Keychain "Login" as shown in picture 1 and click on the "Add" button.



Picture 1.

2. In order for the certificate "ESS RQCA.cer" to be valid, it is necessary to open the app "Keychain Access" which can be accessed by doing the following: Launchpad > Other (folder) > Keychain Access. For the certificate to be trusted it necessary to do the following:

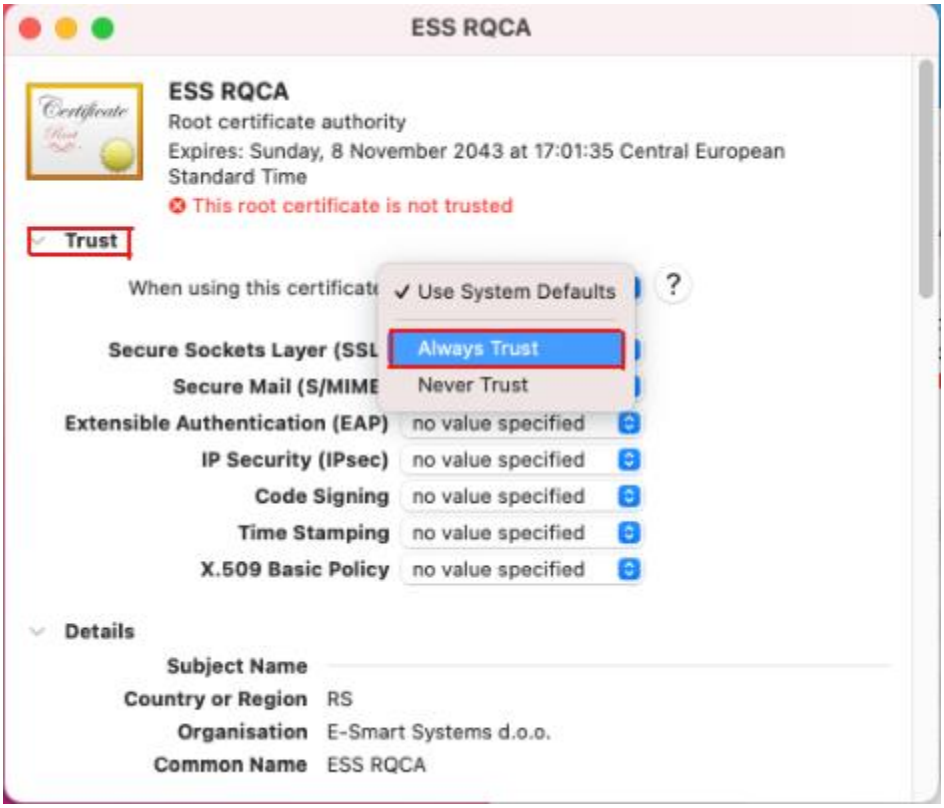
a) Locate the “ESS RQCA.cer” certificate, Keychain Login > Certificates > ESS RQCA, as shown in picture 2.



Picture 2.

b) Double-clicking the certificate “ESS RQCA.cer” will open the certificate details, expand the field “Trust” to see additional settings.

c) Click the field “When using this certificate” and select the option “Always trust”, as shown in picture 3.



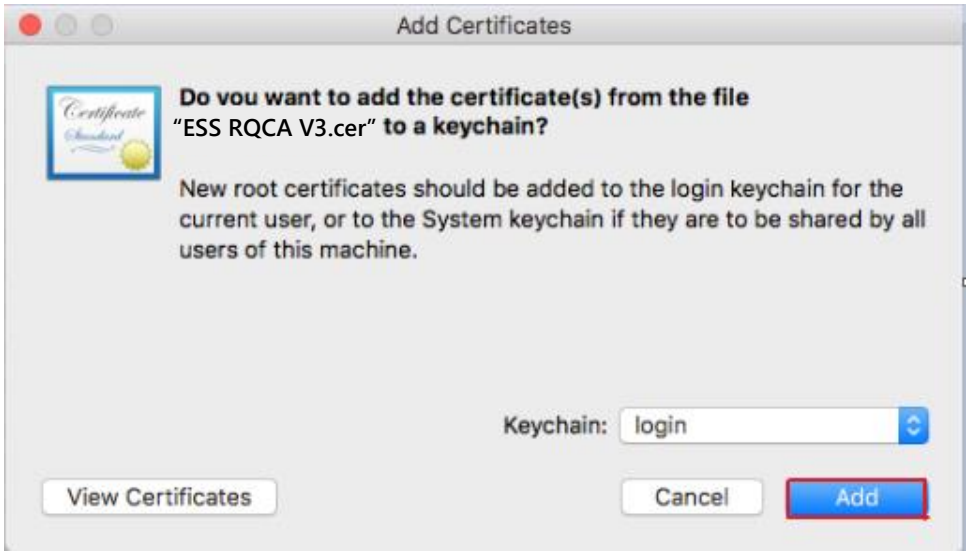
Picture 3.

Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS RQCA importing process.

2.1.2. For qualified certificates for electronic signature and seal issued after 08.04.2024.

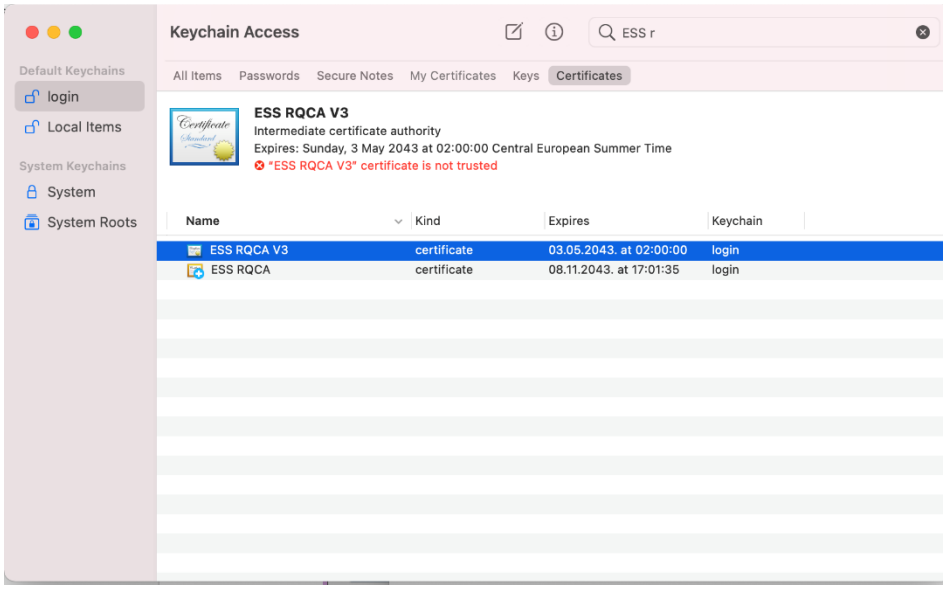
Root CA (ESS RQCA) can be imported in the following way:

1. Double-clicking the "ESS RQCA V3.cer" certificate. Depending on the rights of the user and the number of users present on the machine, importing can be done in two ways:
   a) If there is only 1 user account and/or if you have all user rights on the machine, double-clicking the "ESS RQCA V3.cer" certificate, importing begins automatically.
   b) If there are more accounts and/or you don't have all the user rights on the machine, double-clicking the "ESS RQCA V3.cer" certificate will open the import verification window where you must choose the Keychain "Login" as shown in picture 4 and click on the "Add" button.



Picture 4.

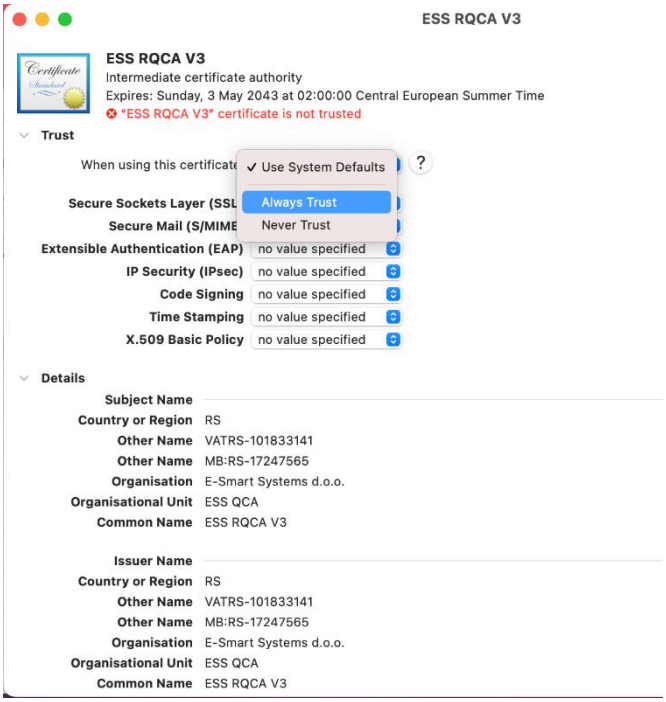
2. In order for the certificate "ESS RQCA V3.cer" to be valid, it is necessary to open the app "Keychain Access" which can be accessed by doing the following: Launchpad > Other (folder) > Keychain Access. For the certificate to be trusted it necessary to do the following:
   a) Locate the „ESS RQCA V3.cer"certificate, Keychain Login > Certificates > ESS RQCA V3, as shown in picture 5.



Picture 5.

b) Double-clicking the certificate “ESS RQCA V3.cer” will open the certificate details, expand the field “Trust” to see additional settings.

c) Click the field “When using this certificate” and select the option “Always trust”, as shown in picture 6.



Picture 6.

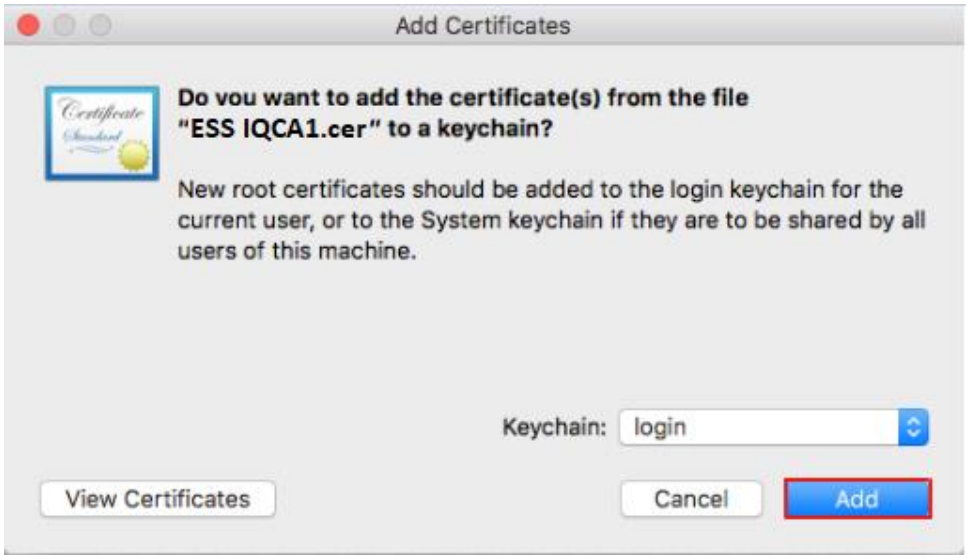
Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS RQCA V3 importing process.

2.2. Importing the Issuer CA certificate

2.2.1. For qualified certificates for electronic signature issued before 08.04.2024.

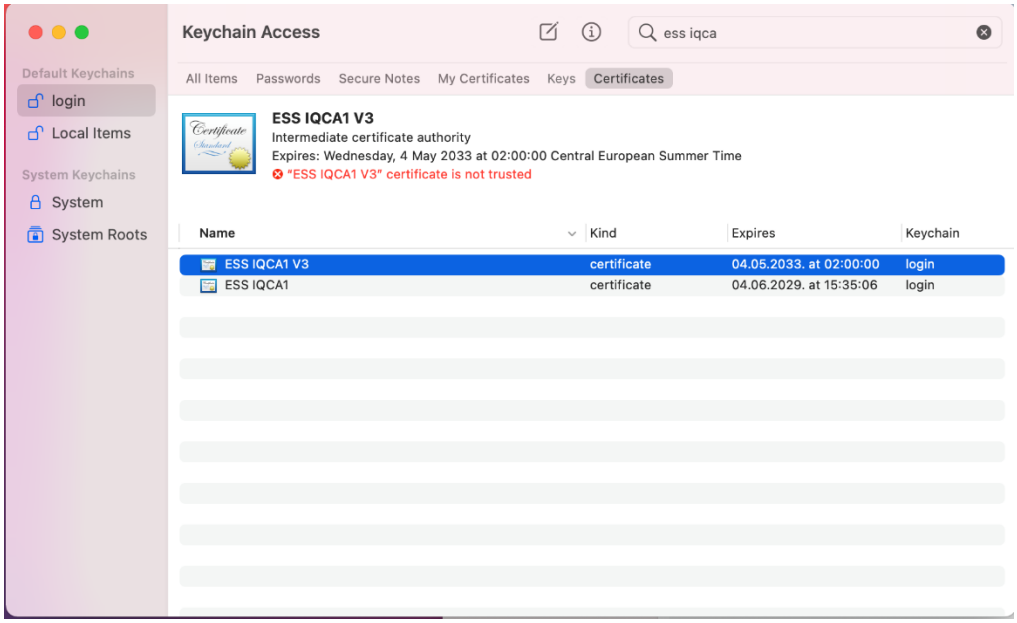
Issuer CA (ESS IQCA) can be imported in the following way:

1) It is necessary to double-click the “ESS IQCA1(3).cer” certificate and perform the importing process. Depending on the rights of your user account and the number of users on the machine, importing can be done in two ways:
   a) If there is only one user and/or you have all the user rights on the machine, double-clicking the “ESS IQCA1(3).cer” certificate starts the process automatically.
   b) If there are more user accounts and/or you don’t have all the user rights on the machine, double-clicking the “ESS IQCA1(3).cer” certificate will open the certificate import window where you must choose the Keychain “Login” option, as shown in picture 7 and click the “Add” button which will start the import process.



Picture 7.

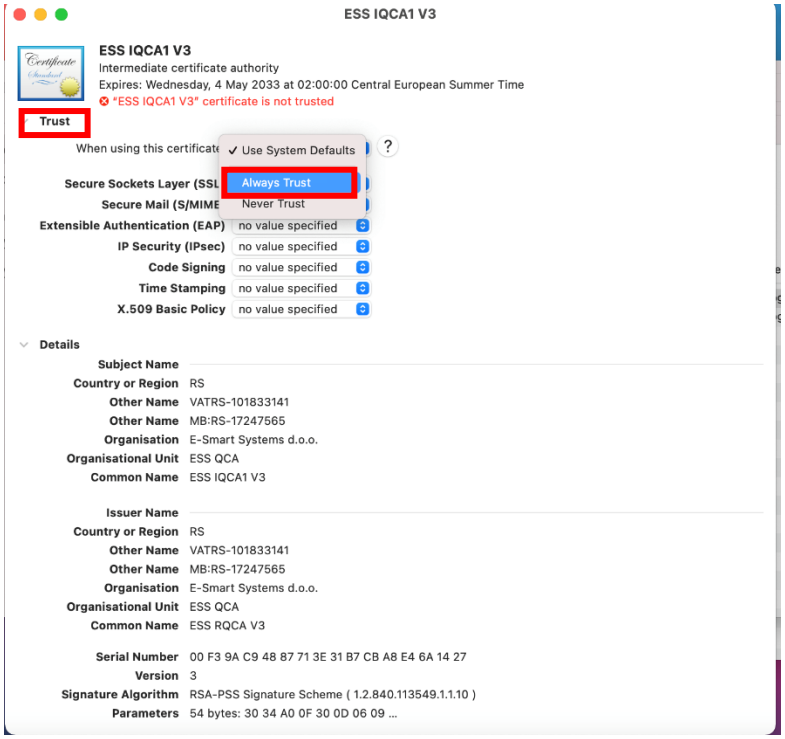
2) In order for the certificate “ESS IQCA1(3).cer” to be valid, it is necessary to open the app “Keychain Access” which can be accessed by doing the following: Launchpad > Other (folder) > Keychain Access. For the certificate to be trusted it necessary to do the following:
   a) Locate the „ESS IQCA1(3).cer“certificate, Keychain Login > Certificates > ESS IQCA1, as shown in picture 8.



Picture 8.

b) Double-clicking the certificate “ESS IQCA1(3).cer” will open the certificate details, expand the field “Trust” to see additional settings.

c) Click the field “When using this certificate” and select the option “Always trust”, as shown in picture 9.



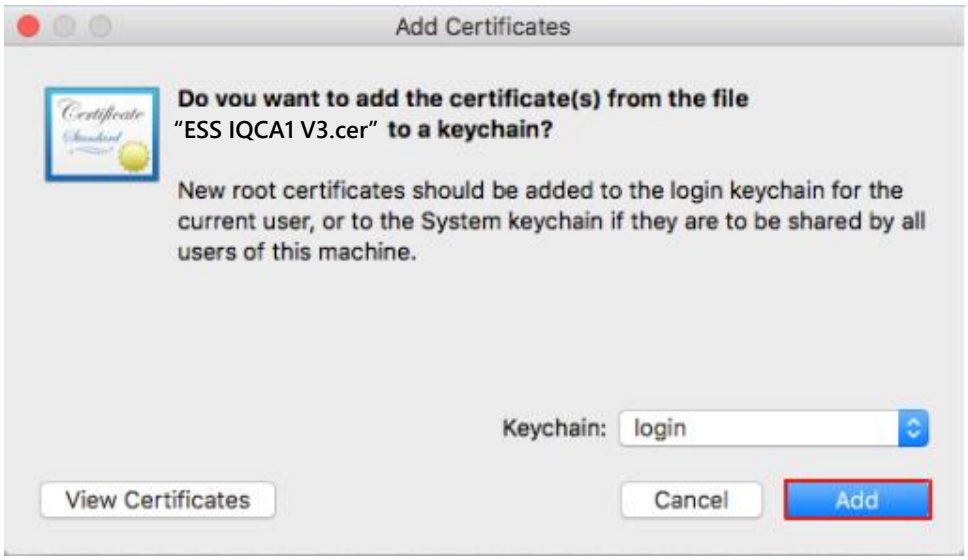
Picture 9.

Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS IQCA1(3) importing process.

2.2.2. For qualified certificates for electronic signature issued after 08.04.2024.

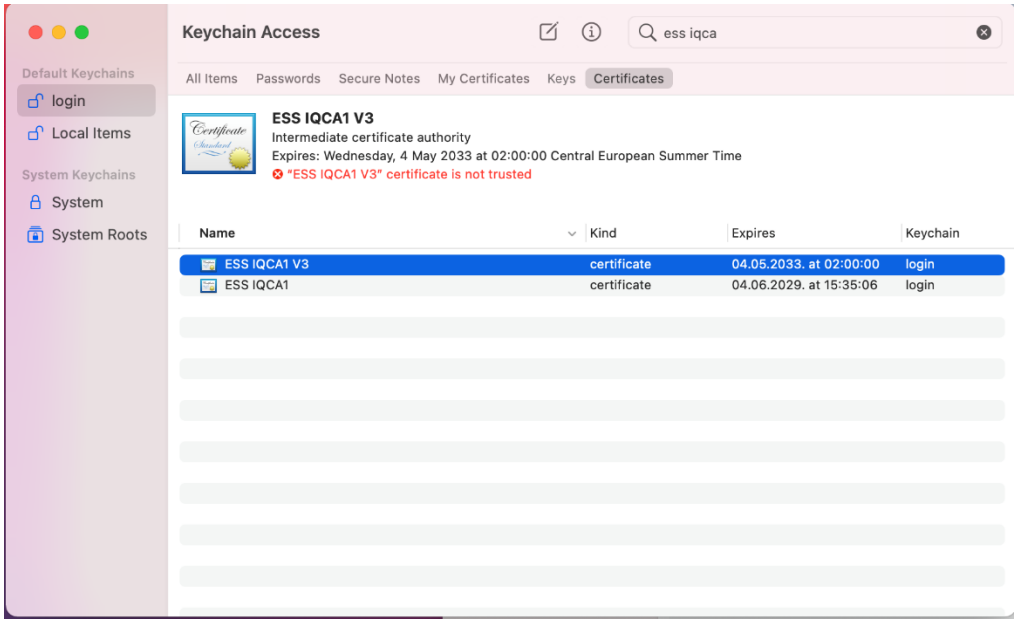
Issuer CA (ESS IQCA) can be imported in the following way:

1) It is necessary to double-click the “ESS IQCA1 V3.cer” certificate and perform the importing process. Depending on the rights of your user account and the number of users on the machine, importing can be done in two ways:
   a) If there is only one user and/or you have all the user rights on the machine, double-clicking the “ESS IQCA1 V3.cer” certificate starts the process automatically.
   b) If there are more user accounts and/or you don’t have all the user rights on the machine, double-clicking the “ESS IQCA1 V3.cer” certificate will open the certificate import window where you must choose the Keychain “Login” option, as shown in picture 10 and click the “Add” button which will start the import process.



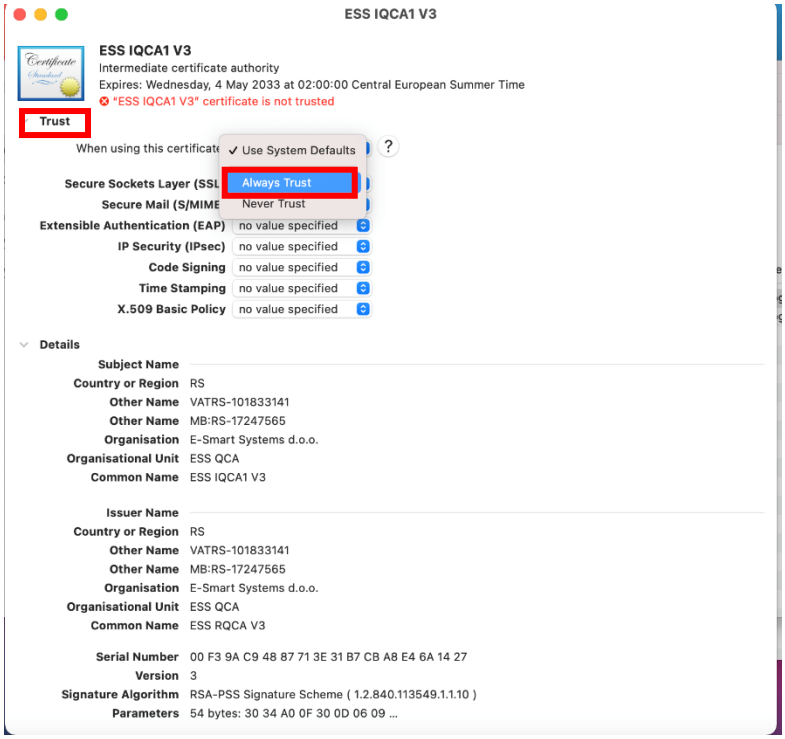
Picture 10.

2) In order for the certificate “ESS IQCA1 V3.cer” to be valid, it is necessary to open the app “Keychain Access” which can be accessed by doing the following: Launchpad > Other (folder) > Keychain Access. For the certificate to be trusted it necessary to do the following:
   a) Locate the „ESS IQCA1 V3.cer“certificate, Keychain Login > Certificates > ESS IQCA1 V3, as shown in picture 11.



Picture 11.

b) Double-clicking the certificate “ESS IQCA1 V3.cer” will open the certificate details, expand the field “Trust” to see additional settings.
c) Click the field “When using this certificate” and select the option “Always trust”, as shown in picture 12.



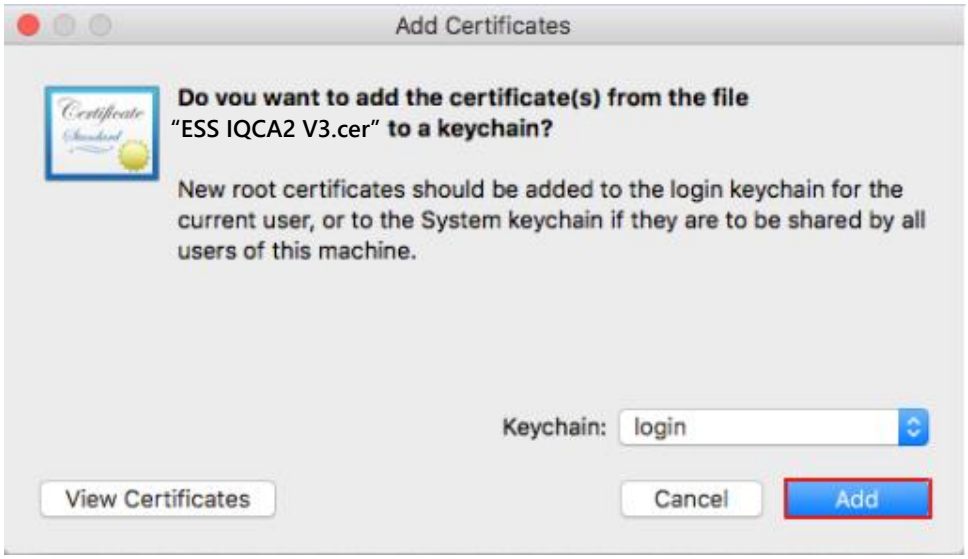
Picture 12.

Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS IQCA1 V3 importing process.

2.2.3. For qualified certificates for electronic seal

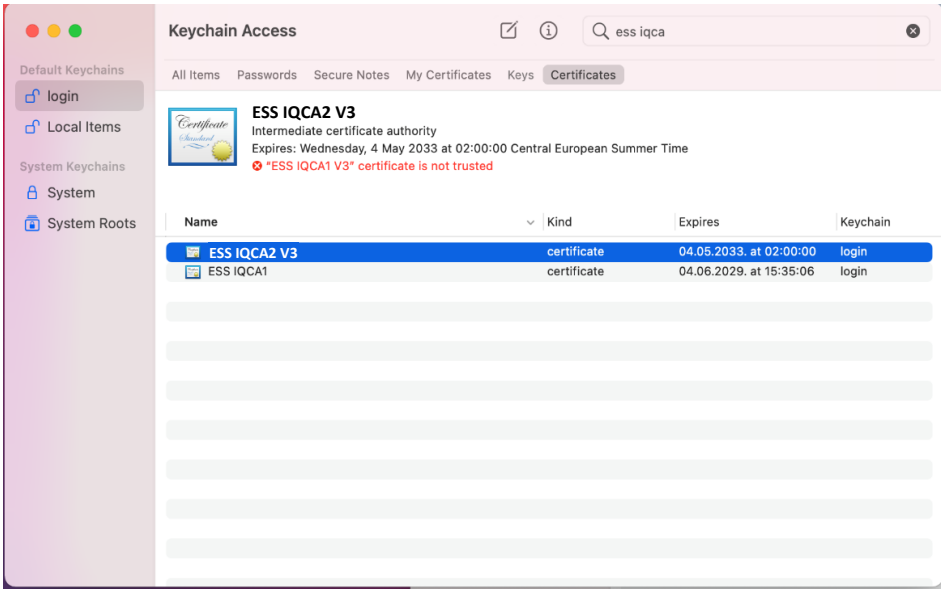
Issuer CA (ESS IQCA) can be imported in the following way:

1) It is necessary to double-click the “ESS IQCA2 V3.cer” certificate and perform the importing process. Depending on the rights of your user account and the number of users on the machine, importing can be done in two ways:
   a) If there is only one user and/or you have all the user rights on the machine, double-clicking the “ESS IQCA2 V3.cer” certificate starts the process automatically.
   b) If there are more user accounts and/or you don’t have all the user rights on the machine, double-clicking the “ESS IQCA2 V3.cer” certificate will open the certificate import window where you must choose the Keychain “Login” option, as shown in picture 13 and click the “Add” button which will start the import process.



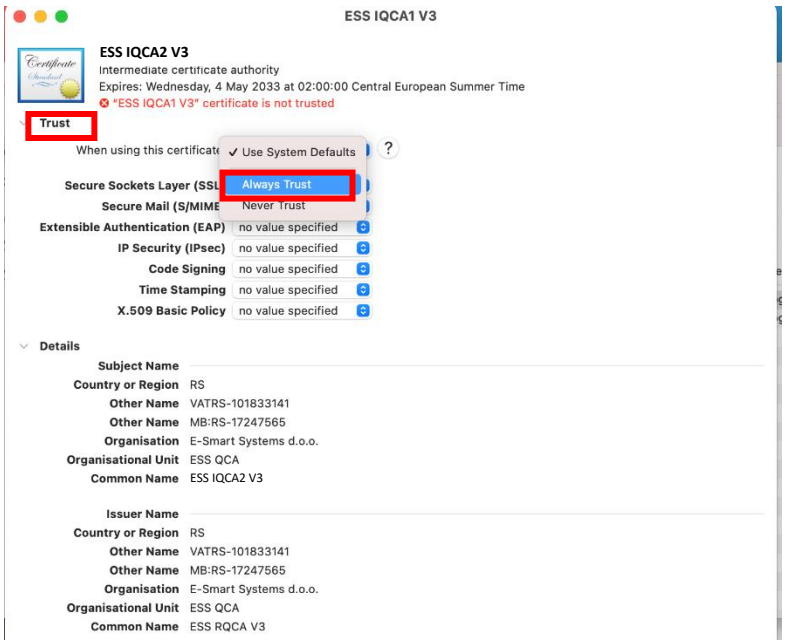
Picture 13.

2) In order for the certificate “ESS IQCA2 V3.cer” to be valid, it is necessary to open the app “Keychain Access” which can be accessed by doing the following: Launchpad > Other (folder) > Keychain Access. For the certificate to be trusted it necessary to do the following:
   a) Locate the „ESS IQCA2 V3.cer“certificate, Keychain Login > Certificates > ESS IQCA2 V3, as shown in picture 14.



Picture 14.

b) Double-clicking the certificate “ESS IQCA2 V3.cer” will open the certificate details, expand the field “Trust” to see additional settings.
c) Click the field “When using this certificate” and select the option “Always trust”, as shown in picture 15.



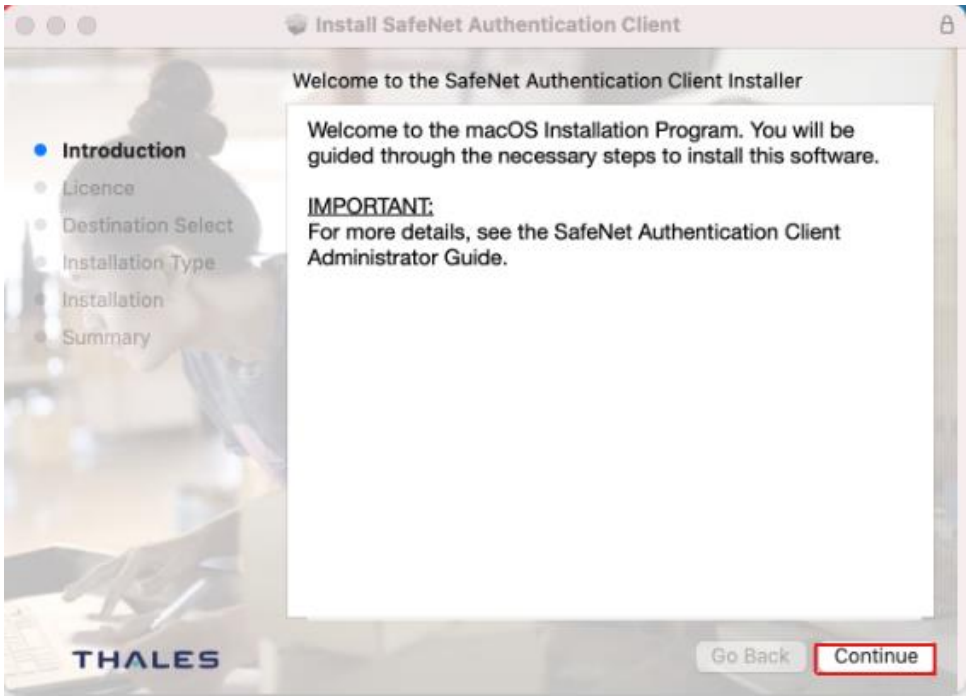
Slika 15.

Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS IQCA2 V3 importing process.

3. Installing the ESS QCA SafeNet Authentication Client middleware on macOS

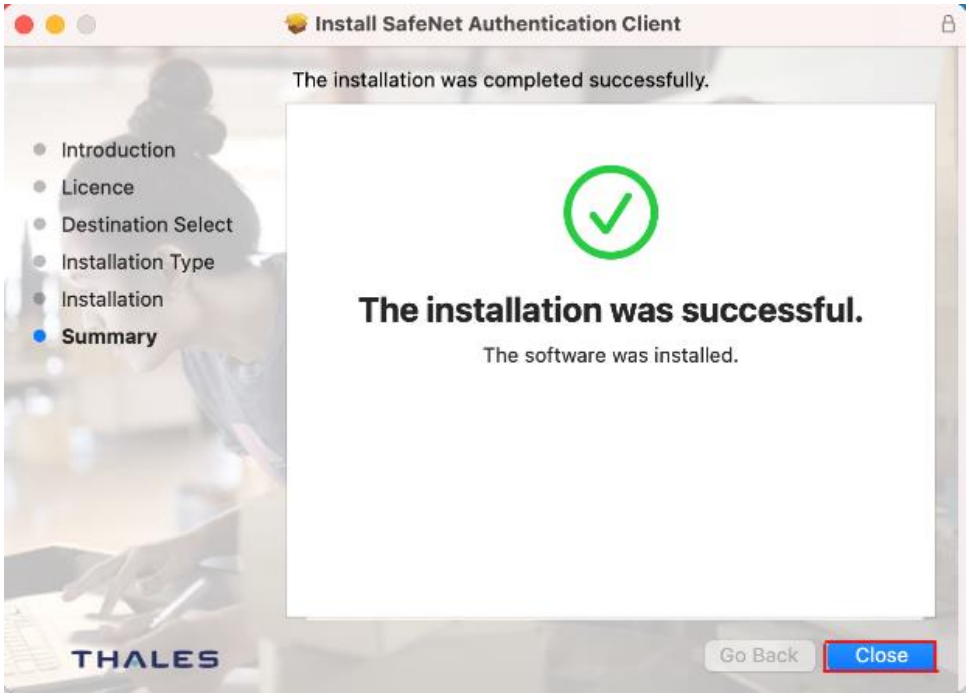
For the macOS computer to recognize the chip on which the qualified certificates are located it is necessary to install the SafeNet driver (SafeNet Authentication Client). The “SafeNet Authentication Client macOS” folder contains installation packages for macOS middleware.

Double-clicking the “SafeNetAuthenticationClient.10.9.4565.0.dmg” file will unpack the installation files. (“SafeNetAuthenticationClient.10.9.4565.0 Core.dmg” is version without UI client) After this it is required to double-click the package “SafeNet Authentication Client 10.9.pkg” which will start the installation process as shown in picture 16.



Picture 16.

For the installation to be successful it is necessary to click “Continue”, then “Continue” again, after this click “Agree” on the license agreement window and finally “Install” (If you have a login password or pin, a prompt will appear where you will have to enter it to continue with the installation). If the installation process has finished, you will see a “The installation was successful” window as shown in picture 17. Click “Close” and carry on.



Picture 17.

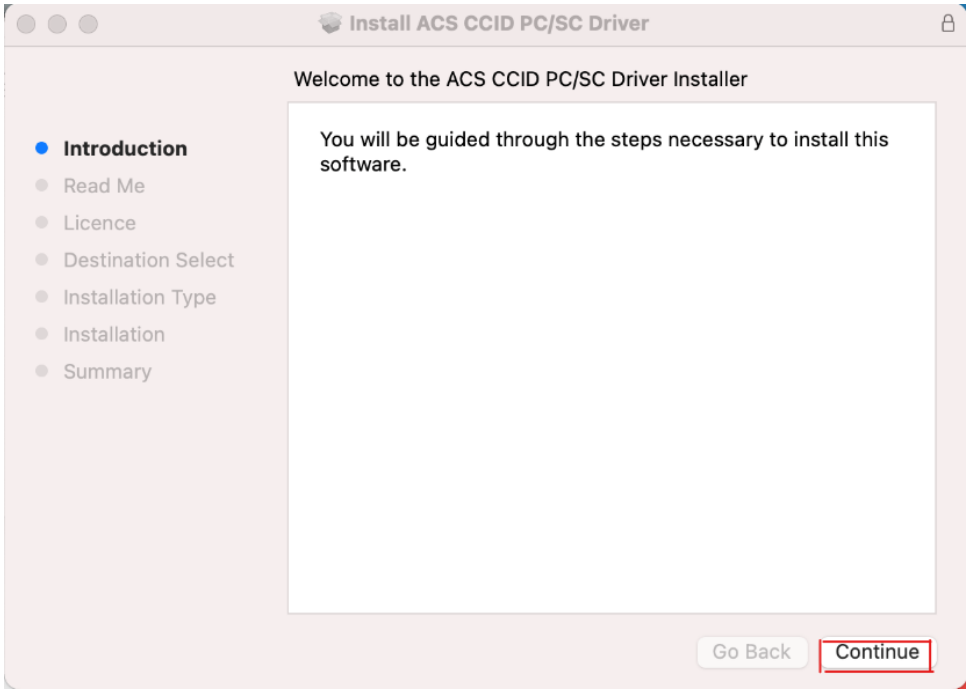
If any problems occur, please, submit a ticket through our web form or write a mail to: qca@esshitsupport.zohodesk.eu – our team will respond as soon as possible.

4. Installing the Thales-Gemalto Smart Card Reader Driver on macOS

In case that macOS is not able to recognize Thales/Gemalto Smart Card Reader it is recommended to install the provided driver. The macOS driver for Thales-Gemalto smart card readers is in „Thales - Gemalto Driver macOS“ folder, and it is installed by unpacking and running „ccid-installer1.7.0.dmg“.

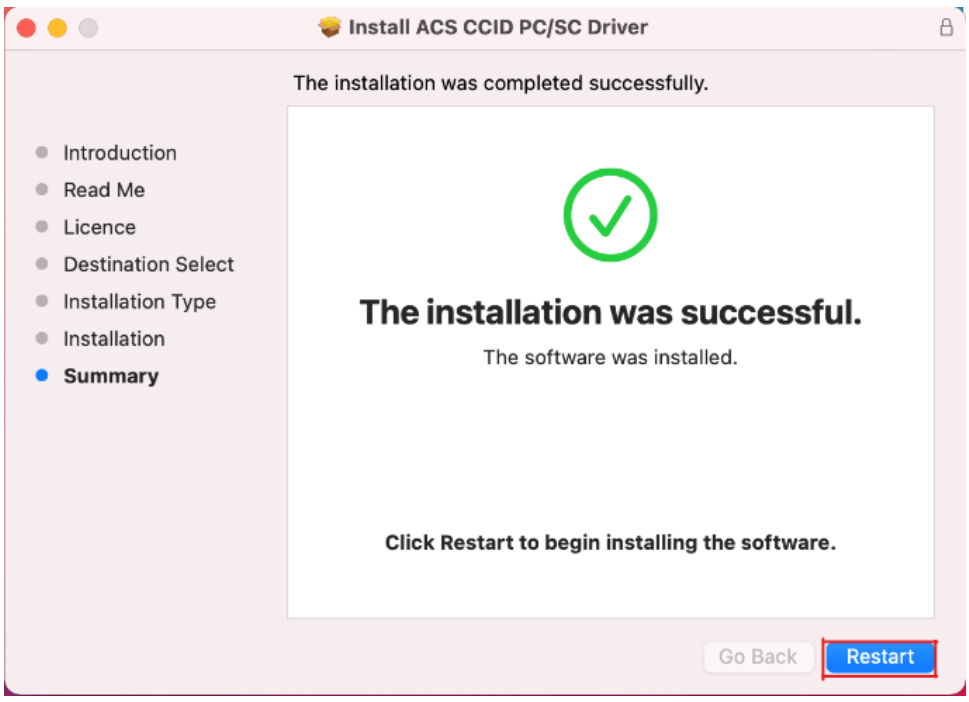
5. Installing the ACS Smart Card Reader Driver on macOS

If the MAC OS version is 14.1 or higher (macOS Sonoma), it may be necessary to install the ACS ACR Smart Card Reader Driver. The ACS driver is in the “ACS Driver macOS” folder. Double-clicking the “acsccid_installer-1.1.13” will unpack the files. After this, it is required to double-click the package “acsccid_installer.pkg” which will start the installation process as shown in picture 18.



Picture 18.

For the installation to be successful it is necessary to click “Continue”, then “Continue” again, after this click “Agree” on the license agreement window and finally “Install” (If you have a login password or pin, a prompt will appear where you will have to enter it to continue with the installation). If the installation process has finished, you will see a “The installation was successful” window as shown in picture 19. Click “Restart” and after restarting the computer you can tryout working with your certificate.



Picture 19.

6. Prerequisite package verification test for working with certificates on macOS

As a confirmation of the success of the installation of all prerequisites for working with certificates on MacOS machines, after installation, you will see a SafeNet icon on the header as shown in picture 20(Note: if you do not have this icon, it is necessary to locate the SafeNet client in the launchpad and launch it.

Picture 20.

When you import the certificate to your computer, the SafeNet icon in the header will light-up as shown in picture 21 which means the certificate is ready to be utilized.

Picture 21.

If any problems occur, please, submit a ticket through our web form or write a mail to: qca@esshitsupport.zohodesk.eu – our team will respond as soon as possible.