

U-QCA-304

Document code

Instructions for installing prerequisites for working with qualified certificates for electronic signatures – MAC edition

1. Downloading the ESS QCA installation package for MAC

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. Clicking the link [ESSQCA installation package for MACOS](#) will begin the download.

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.

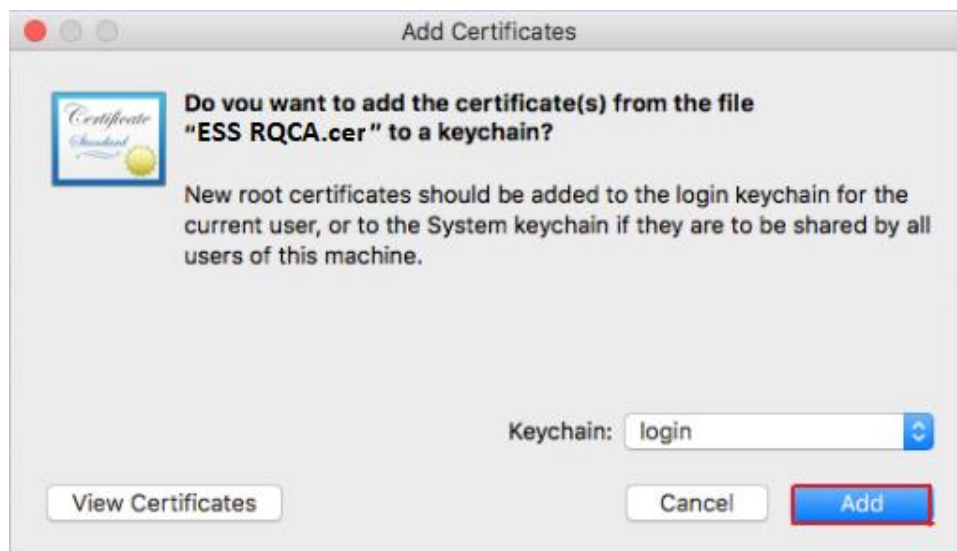
2. Installing the ESS QCA „chain of verification“

ESS QCA „chain of verification“ consists of the CA Root and Issuer certificates which are located inside the „Certificates“ 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 CA root certificate

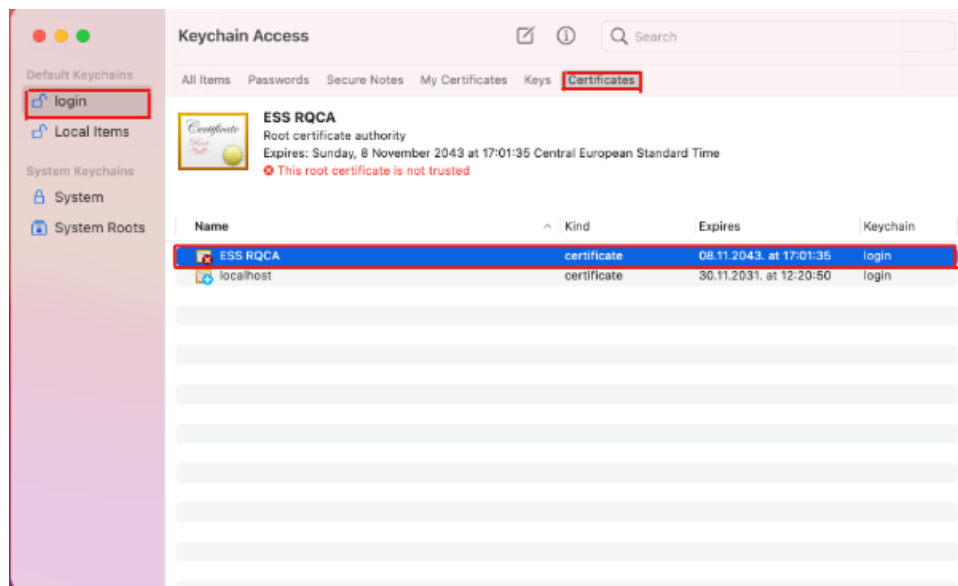
CA Root (ESS RQCA) can be imported in the following way:

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.



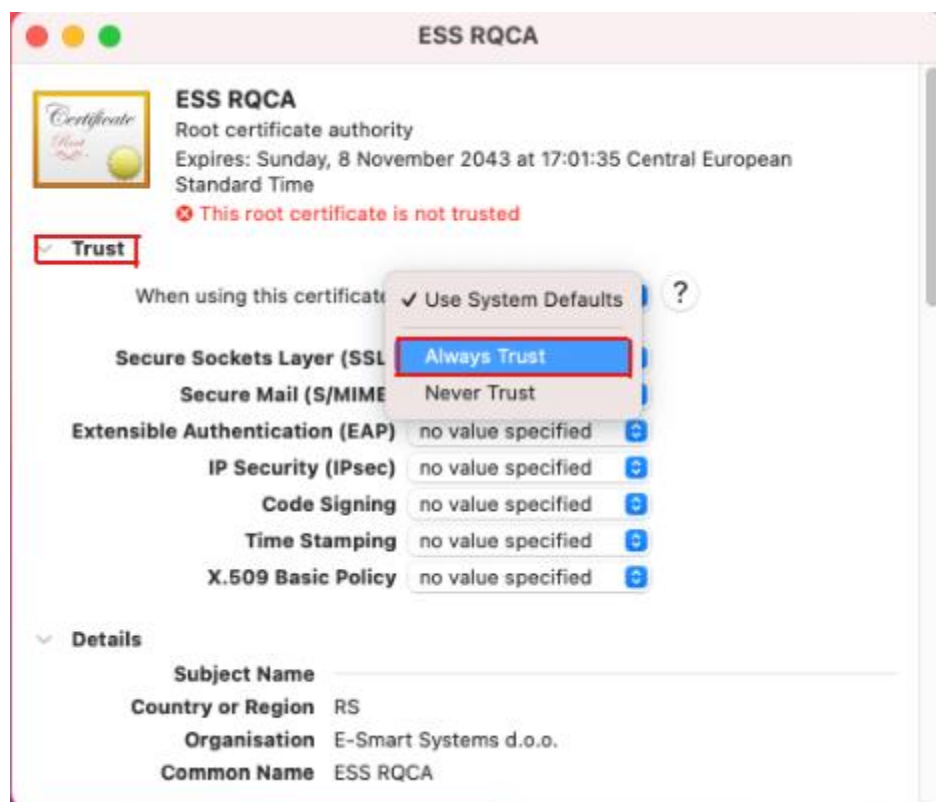
Picture 1.

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.

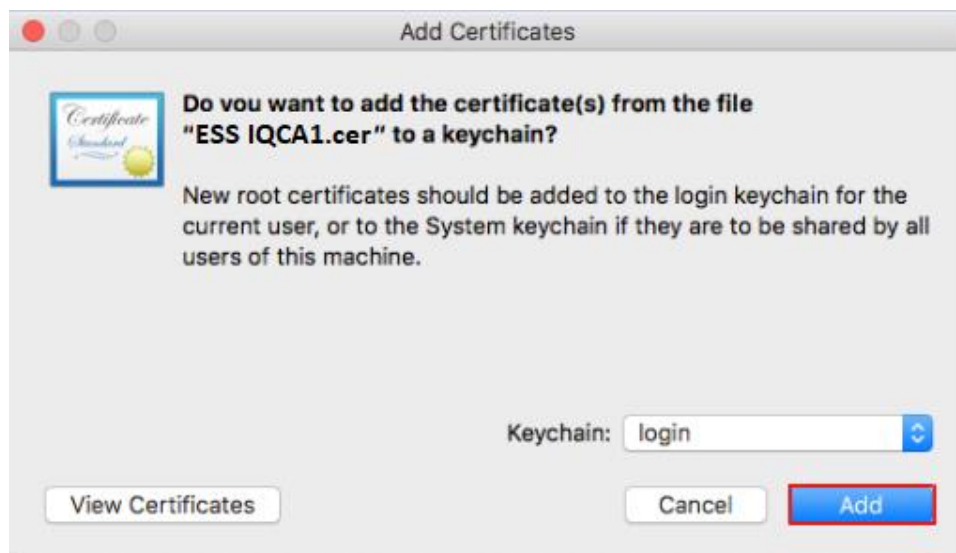
Exit the window by clicking on the X for the settings to be saved and enter the password of your user account if necessary. Finishing these steps completes the ESS RQCA importing process.

2.2. Importing the CA Issuer certificate

There are multiple certificate authority certificates in the “Sertifikati” folder. For the workflow with the PKI infrastructure ESS QCA to be flawless, it is necessary to install all the certificate authority certificates. The names of these certificates begin with ESS IQCA1, and they can be imported in the following way:

It is necessary to double-click each “ESS IQCA1.cer” certificate separately and perform the importing process (Note: certificates that can’t be imported should be ignored, they have probably expired, just continue importing the ones you can). 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.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.cer” certificate will open the certificate import window where you must choose the Keychain “Login” option, as shown in picture 4 and click the “Add” button which will start the import process.



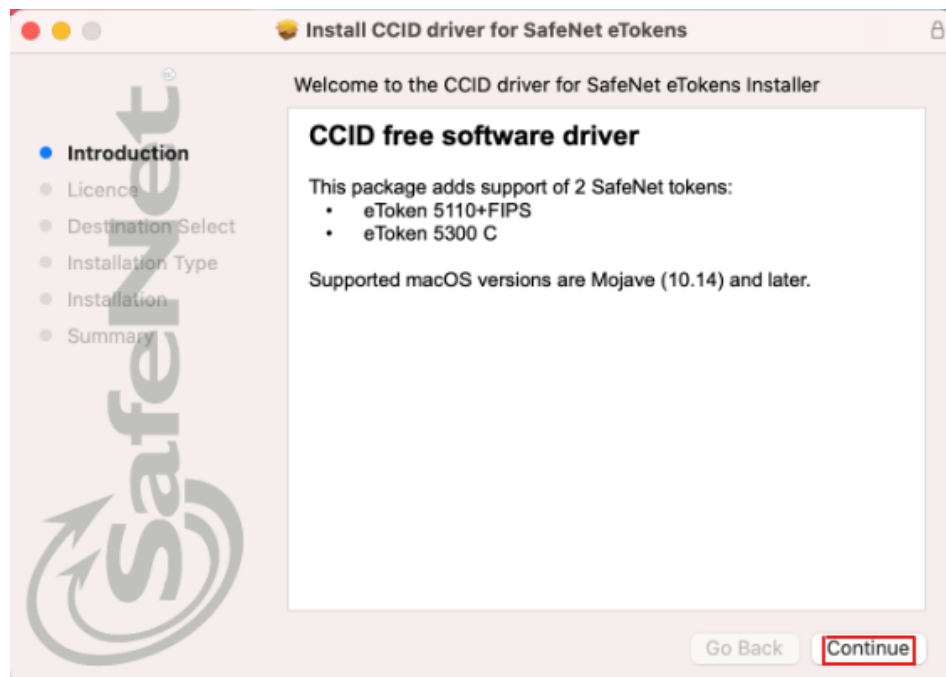
Picture 4.

3. Installing the ESS QCA software package– MAC OS

For the MAC computer to recognize the chip on which the qualified certificates are located it is necessary to install the SafeNet driver. In the “MacOS SafeNet Authentication Client(QSCD)” folder there is a folder named “Installation (Notarized)” which contains 3 installation packages for MAC OS. It is necessary to install all three packages for the certificate to work. All files need to be unpacked by double-clicking them.

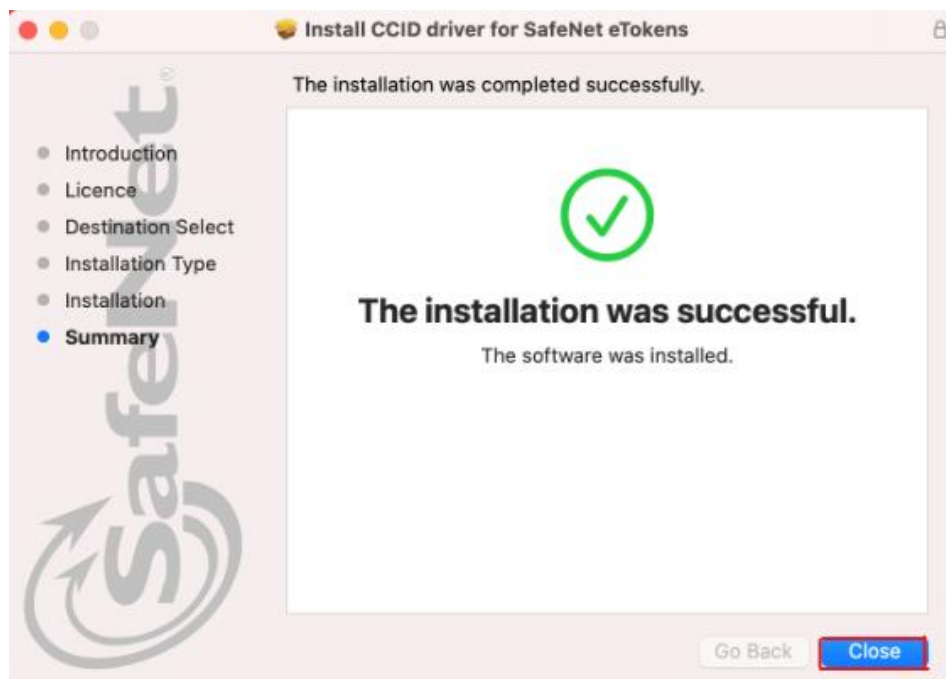
3.1. Installing the “ccid-installer.dmg” package.

Double-clicking the “ccid-installer.dmg” will unpack the files. After this it is required to double-click the package “ccid-installer-1.4.36.pkg” which will start the installation process as shown in picture 5.



Picture 5.

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 6. Click “Close” and carry on.

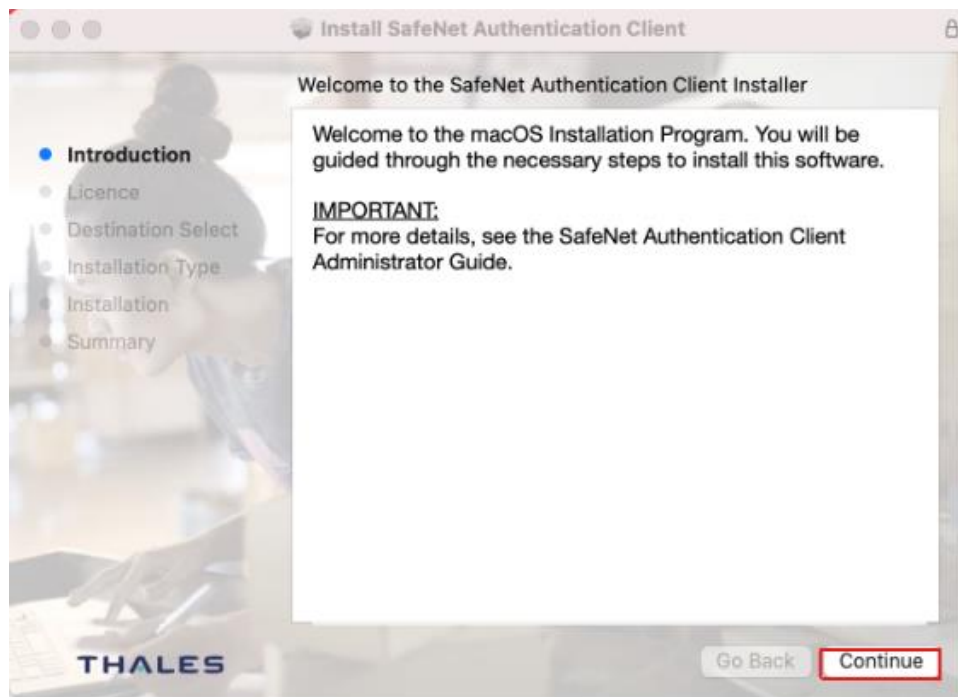


Picture 6.

If any problems occur, please, submit a ticket through our [web form](#) or write a mail to: gca@esshitsuport.zohodesk.eu – our team will respond as soon as possible.

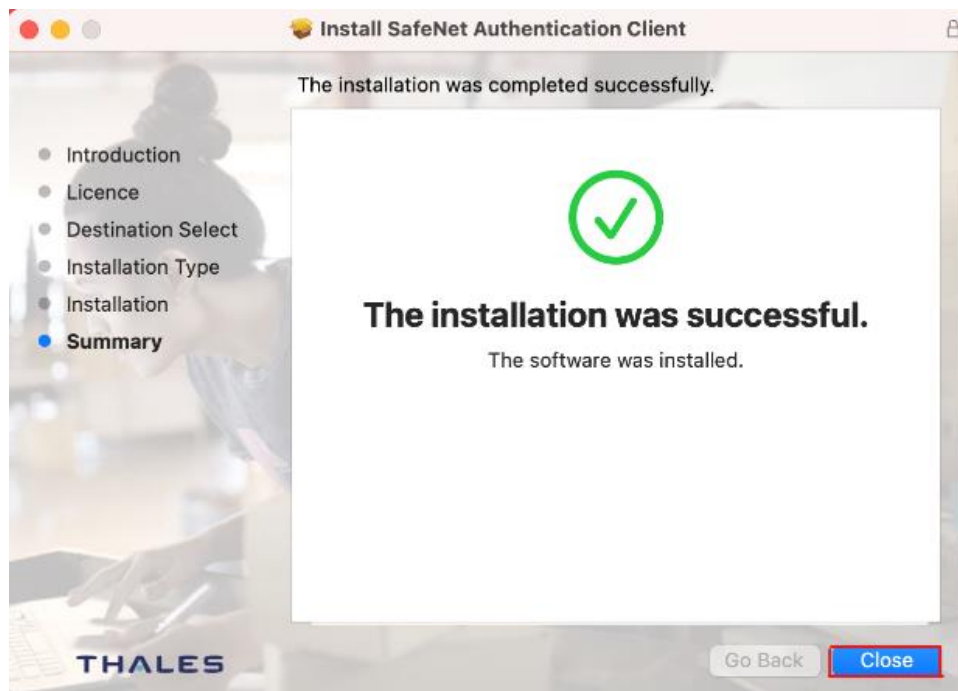
3.2. Installing the Safe Net Authentication Client package

Double-clicking the “SafeNetAuthenticationClient.10.8.267.0 Core.dmg” will unpack the files. After this it is required to double-click the package “SafeNetAuthenticationClient.10.8.267.0 Core.dmg” which will start the installation process as shown in picture 7. After installing the CORE client, the user should install the regular Client “SafeNetAuthenticationClient.10.8.267.0.dmg” in the same manner as explained above and shown below.



Picture 7.

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 8. Click “Close” and carry on.

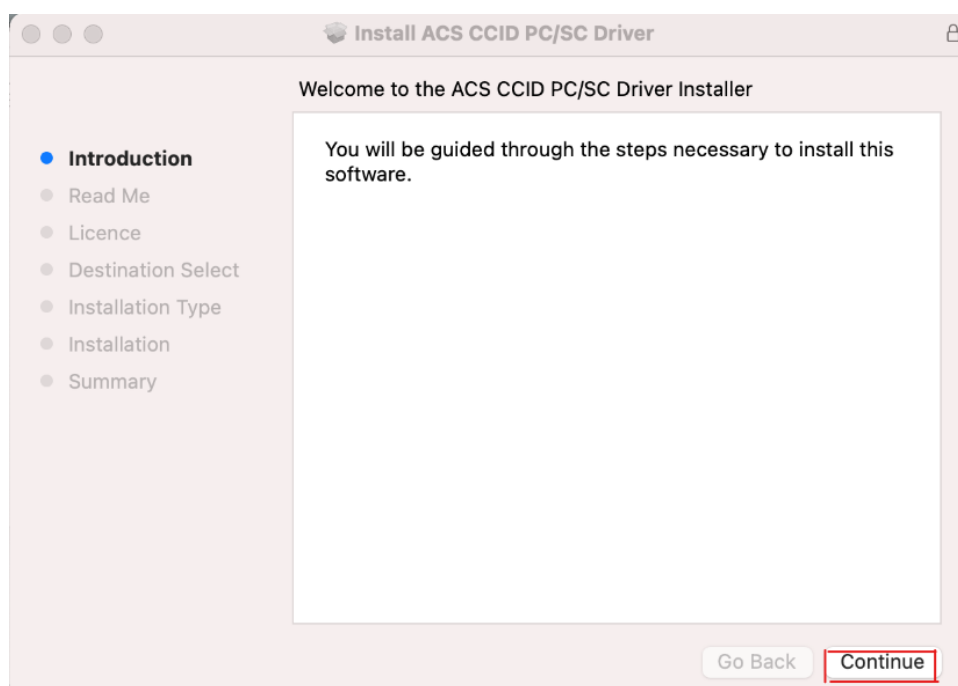


Picture 8.

If any problems occur, please, submit a ticket through our [web form](https://esshitsuport.zohodesk.eu) or write a mail to: gca@esshitsuport.zohodesk.eu – our team will respond as soon as possible.

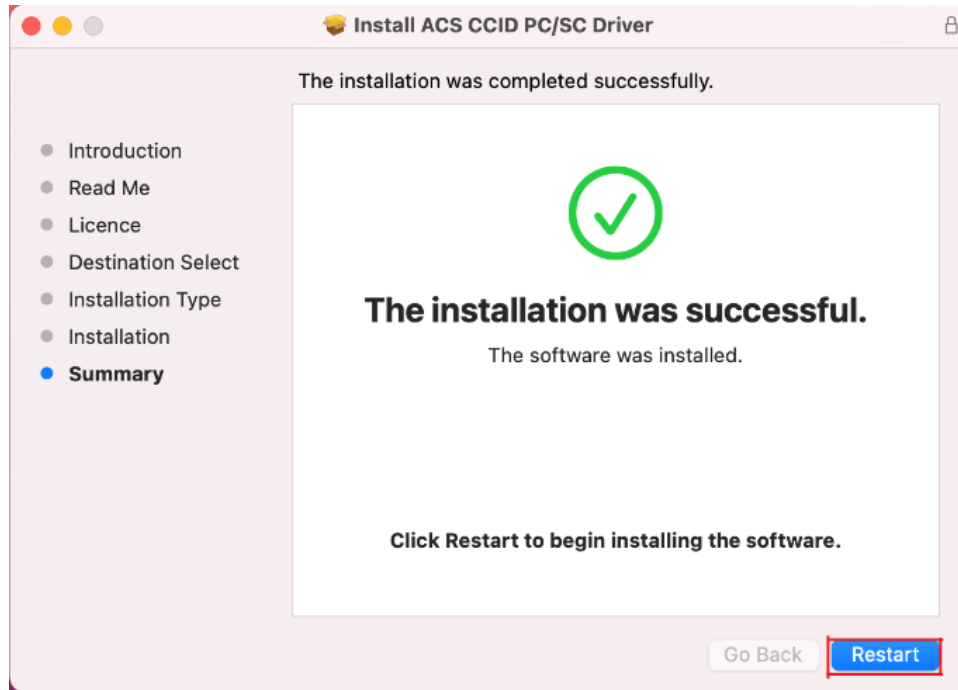
4. Installing the ACS Drivers – MAC OS

If the MAC OS version is 14.1 or higher (macOS Sonoma), it is necessary to install the ACS Driver package. The ACS driver package is in the "ACS driver macOS" folder. Double-clicking the "acscid_installer-1.1.8.3.dmg" will unpack the files. After this, it is required to double-click the package "acscid_installer.pkg" which will start the installation process as shown in picture 9.



Picture 9.

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 10. Click “Restart” and after restarting the computer you can tryout working with your certificate.



Picture 10.

5. Prerequisite package verification test for working with certificates on MAC OS

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 11 (Note: if you do not have this icon, it is necessary to locate the SafeNet client in the launchpad and launch it).



Picture 11.

When you import the certificate to your computer, the SafeNet icon in the header will light-up as shown in picture 12 which means the certificate is ready to be utilized.



Picture 12.

If any problems occur, please, submit a ticket through our [web form](#) or write a mail to: gca@esshitsuport.zohodesk.eu – our team will respond as soon as possible.