E-Smart Systems d.o.o. | **Adresa:** Kneza Višeslava 70a, 11030 Beograd, Srbija | **Sertifikaciono telo (ESS QCA)** | **Tel:** 011 3050280, **Fax:** 011 3050222 | **E-mail:** qca@e-smartsys.com | **Matični broj:** 17247565, **PIB:** 101833141, **Šifra delatnosti:** 6201

U-QCA-221

Šifra dokumenta

Instructions for installing and using the ESS QCA Qualified Certificate for Electronic Signature

Content

1. Requirements for using ESS QCA Qualified certificate for electronic signature

Presented instructions inside of this document are meant for use of the Qualified certificate for electronic signature on Microsoft Windows OS. If you need to use the qualified certificate on macOS or Linux operating systems please contact our support team via web form or email qca@esshitsupport.zohodesk.eu and we will contact yuo as soon as posible.

To be able to use ESS QCA Qualified certificate succesfully you will have to install ESS QCA trust chain (Certification Authority root and issuer certificates), Thales SafeNet Midriver with PKCS#11 middleware and drivers for the smart card reader or the USB token (usually automatically detected by the Windows).

2. Downloading the ESS QCA Windows installation package

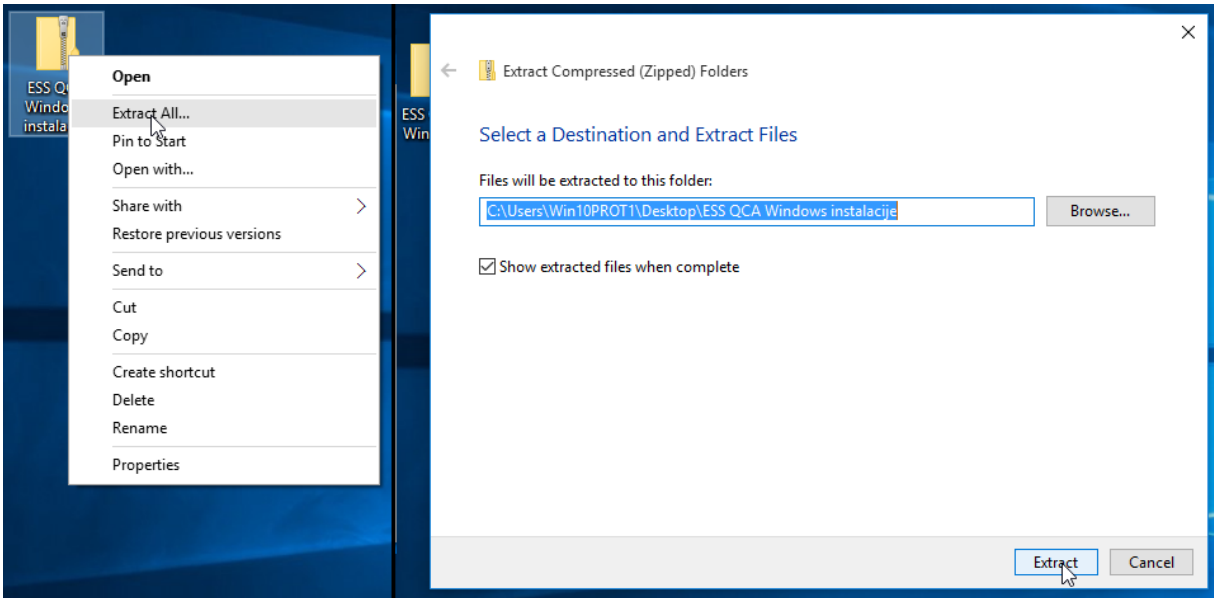
The installation package with all necessary files can be downloaded from ESS QCA website - https://essqca.e-smartsys.com under the section “Download Software”.

If you have a qualified certificate that was issued:

- **after 04/08/2024** please download the ZIP file labelled as Windows Installation package (QSCD) – for certificates issued after 04/08/2024
- **from 04/05/2021 until 04/08/2024** please download the ZIP file labelled as Windows Installation package (QSCD) - – for certificates issued from 04/05/2021 until 04/08/2024
- **before 04/05/2021**, please download ZIP file labelled as Windows Installation package (SSCD) - for certificates issued before 04/05/2021.

Before using any of the files in the package, you need to unzip it:

1. Open the drop-down menu by right-clicking on the zip file "ESS QCA Windows..."
2. Select the option "**Extract All**..."
3. Confirm the extraction by clicking the **"Extract"** button.



Select a Destination and Extract Files

Files will be extracted to this folder: C:\Users\Win10PROT1\Desktop\ESS QCA Windows instalacije

☑ Show extracted files when complete

After this step, it is possible to proceed with the installation of the necessary software components for using the ESS QCA qualified certificate for electronic signature.

3. Installation of ESS QCA trust chain

The ESS QCA trust chain consists of Certification Authority Root and Issuer certificates which are located inside the “Certificates” folder of the installation package. These certificates need to be imported into the local certificate store on the Windows machine in order to establish trust between that machine and the user's certificate.

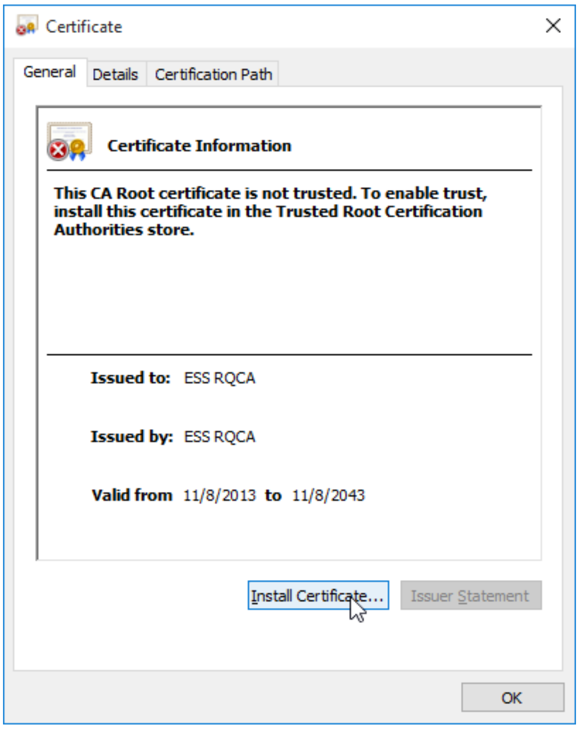
3.1. Importing the CA Root certificate

3.1.1. For qualified certificates issued before 04/08/2024

The CA Root (ESS RQCA) certificate can be imported as follows:

1. It is necessary to open the "**ESS RQCA.cer**" certificate with a double click, after which a window will appear as in the picture below.

2. Importing the certificate is started by clicking the "**Install Certificate...**" button.
   After that, a window opens where you need to select the "**Local Machine**" option and click on the "**Next**" button.

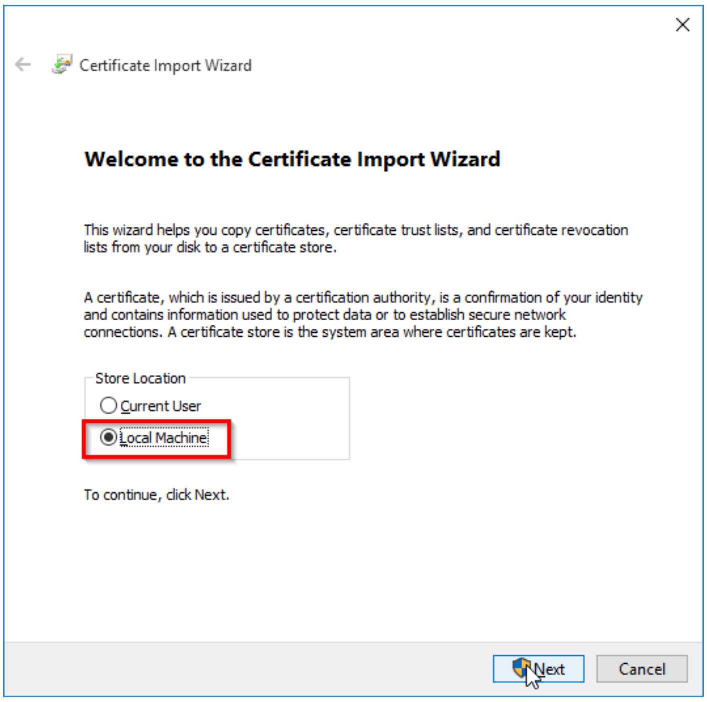


This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: ESS RQCA

Issued by: ESS RQCA

Valid from 11/8/2013 to 11/8/2043



Certificate Import Wizard

Welcome to the Certificate Import Wizard

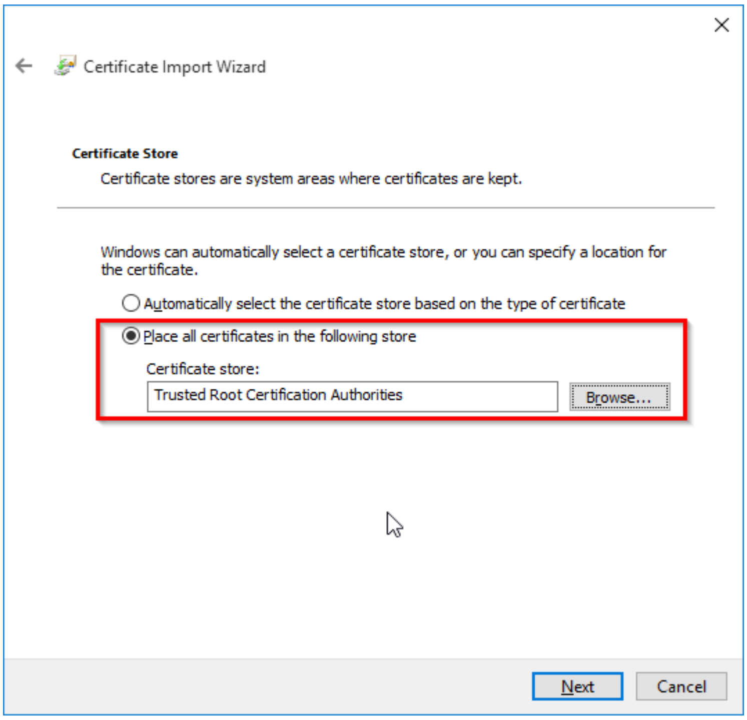
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

3. In the next window, you need to select the option "**Place all certificates in the following store**", and after that you need to select the name "**Certificate store**:" using the "B**rowse**..." button. "**Trusted Root Certification Authorities**" is intended as a certificate store for CA Root.



Certificate Import Wizard

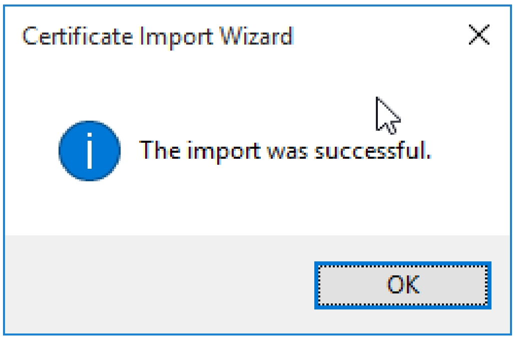
Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

4. By clicking the "**Next**" button, the final screen opens, where you need to click the "**Finish**" button. After that, a message about the successful import of the CA Root certificate will be displayed, as in the image below.



Certificate Import Wizard

The import was successful.

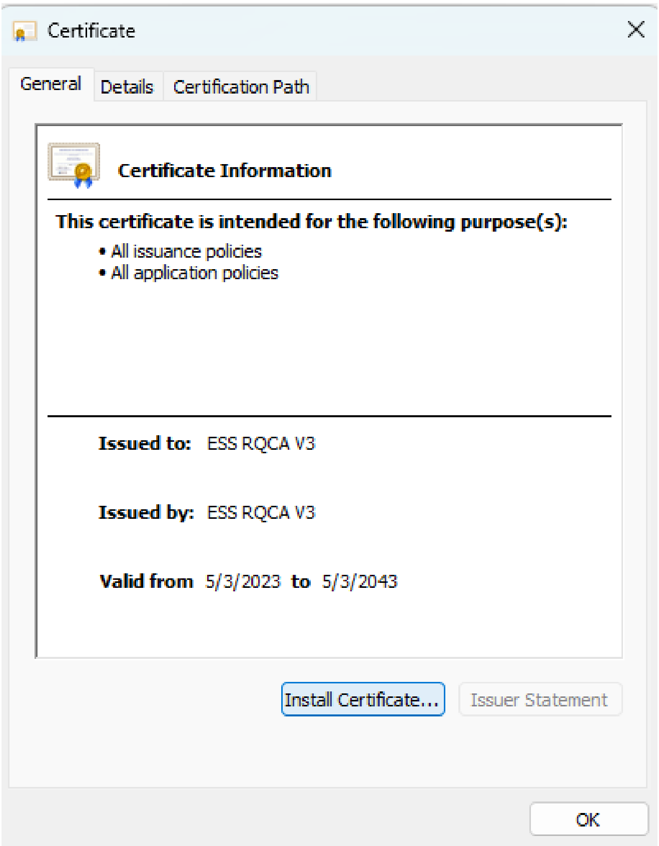
3.1.2. For qualified certificates issued after 04/08/2024

The CA Root (ESS RQCA) certificate can be imported as follows:

1. It is necessary to open the "**ESS RQCA V3.cer**" certificate with a double click, after which a window will appear as in the picture below.

2. Importing the certificate is started by clicking the "**Install Certificate...**" button.

After that, a window opens where you need to select the "**Local Machine**" option and click on the "**Next**" button.



Certificate Information

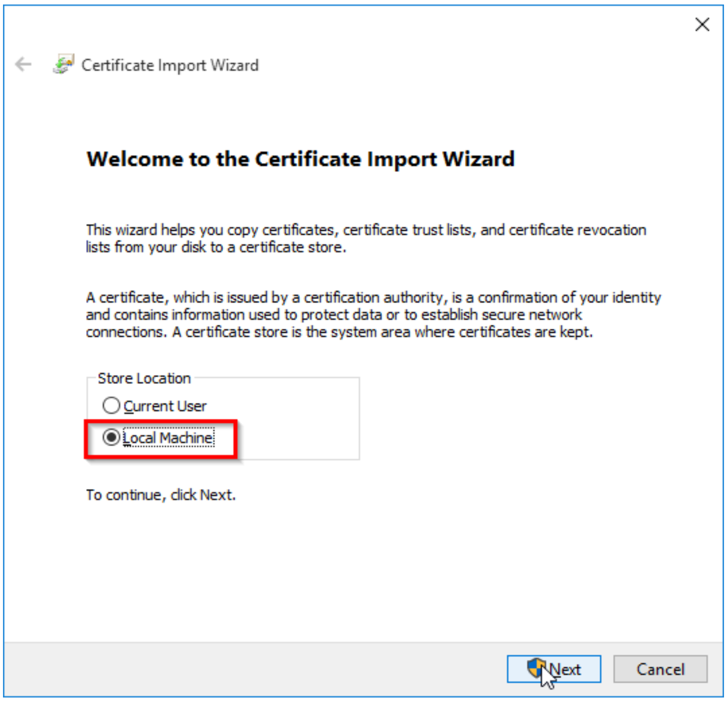
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: ESS RQCA V3

Issued by: ESS RQCA V3

Valid from 5/3/2023 to 5/3/2043



Certificate Import Wizard

Welcome to the Certificate Import Wizard

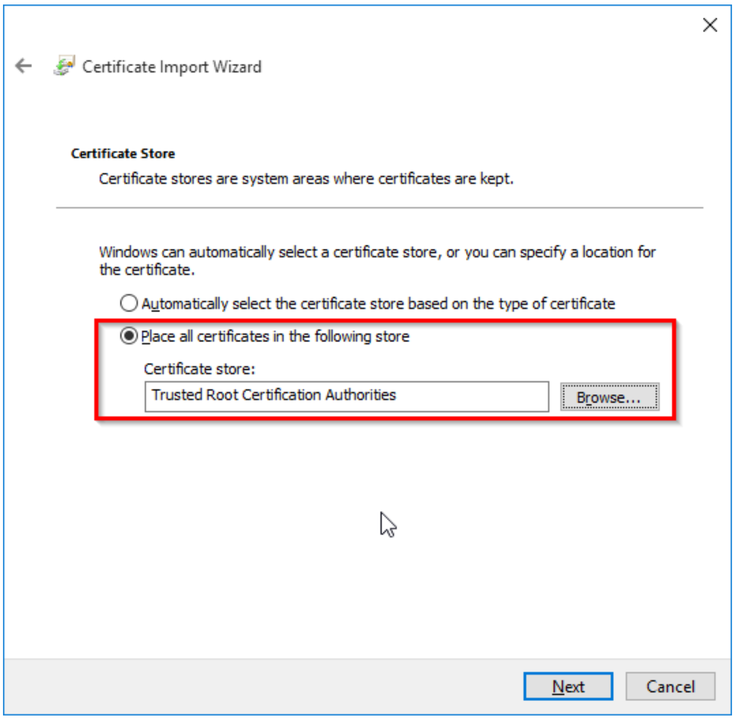
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

3. In the next window, you need to select the option "**Place all certificates in the following store**", and after that you need to select the name "**Certificate store**:" using the "**Browse**..." button. "**Trusted Root Certification Authorities**" is intended as a certificate store for CA Root.



Certificate Import Wizard

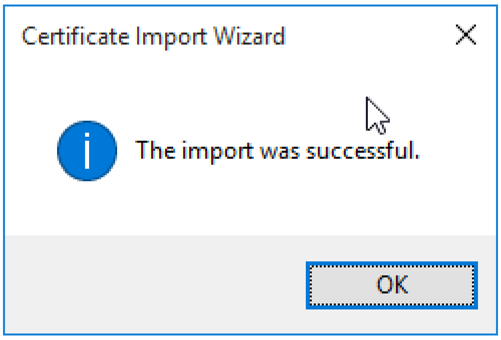
Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate
● Place all certificates in the following store

Certificate store:
Trusted Root Certification Authorities

4. By clicking the "**Next**" button, the final screen opens, where you need to click the "**Finish**" button. After that, a message about the successful import of the CA Root certificate will be displayed, as in the image below.


Certificate Import Wizard

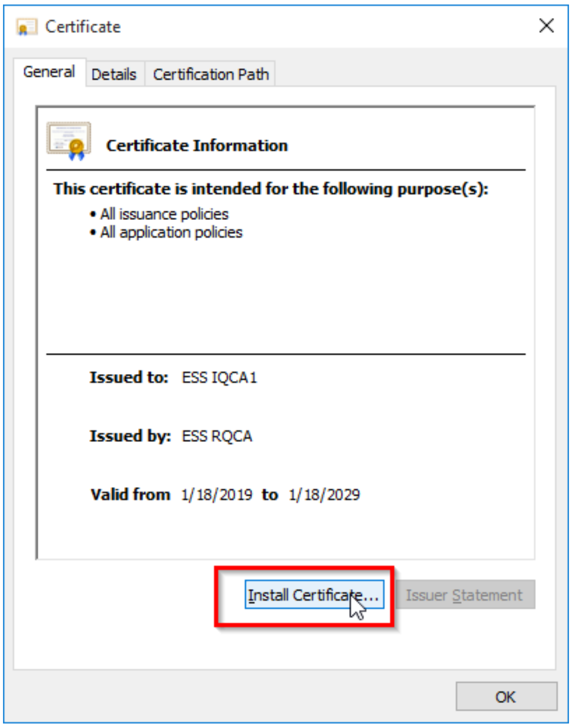
The import was successful.

3.2. Importing CA Issuer certificates

3.2.1. For qualified certificates issued before 04/08/2024

There is more than one certificates for CA Issuer in the “Certificates” folder. In order to have highest level of reliability with the PKI infrastructure of ESS QCA, it is necessary to install all certificates of the Issuer authority. The names of these certificates start with ESS IQCA1 and can be imported as follows:

1. It is necessary to open the "**ESS IQCA1.cer**" certificate with a double click, after which a window will appear as in the picture below.



Certificate Information

This certificate is intended for the following purpose(s):
- All issuance policies
- All application policies

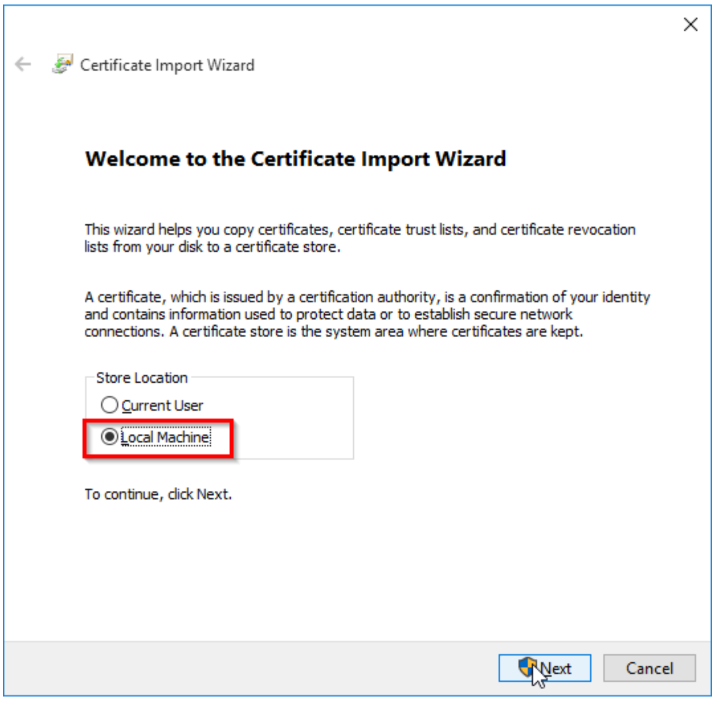
Issued to: ESS IQCA1

Issued by: ESS RQCA

Valid from 1/18/2019 to 1/18/2029

Importing the certificate is started by clicking the "**Install Certificate...**" button.

After that, a window opens where you need to select the "**Local Machine**" option and click on the "**Next**" button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

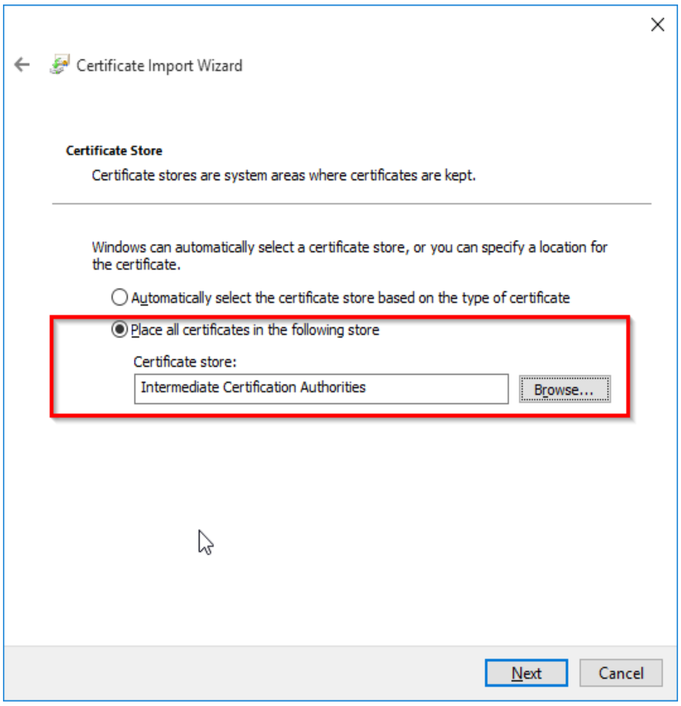
Store Location

○ Current User

● Local Machine

To continue, click Next.

2. In the next window, you need to select the option "**Place all certificates in the following store**", and after that you need to select the name "**Certificate store**:" using the "**Browse**..." button "**Intermediate Certification Authorities**" is intended for certificate store for CA Issuer.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

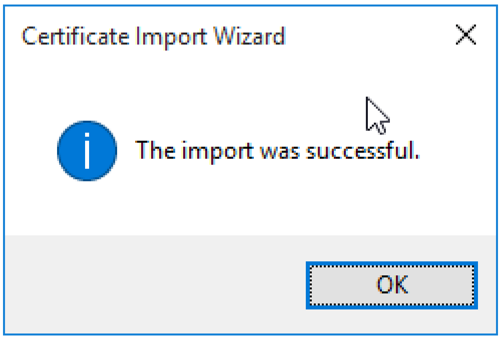
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

3. By clicking the "**Next**" button, the final screen opens, where you need to click the "**Finish**" button. After that, a message about the successful import of the CA Issuer certificate will be displayed, as in the picture below.

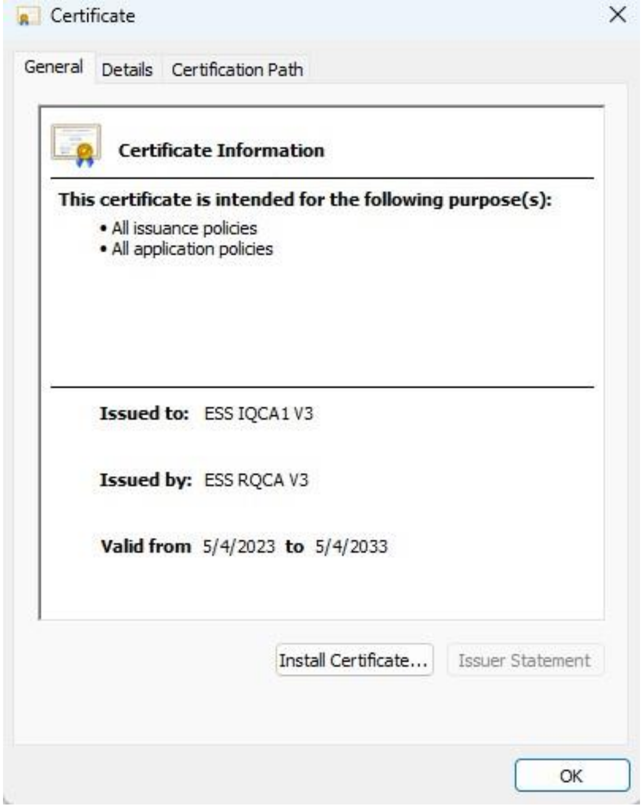


Certificate Import Wizard

The import was successful.

3.2.2. For qualified certificates issued after 04/08/2024

1. It is necessary to open the "**ESS IQCA1.cer**" certificate with a double click, after which a window will appear as in the picture below.



Certificate Information

This certificate is intended for the following purpose(s):

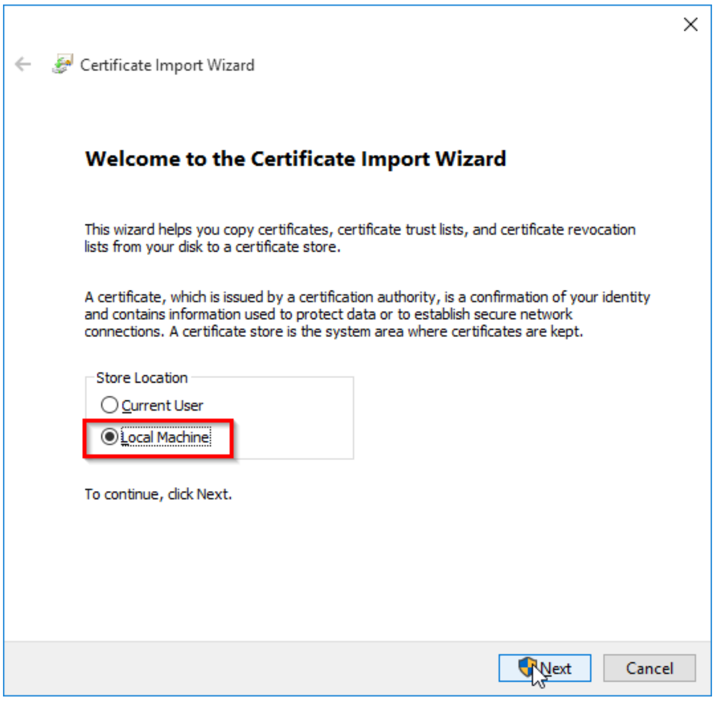
- All issuance policies
- All application policies

Issued to: ESS IQCA1 V3

Issued by: ESS RQCA V3

Valid from 5/4/2023 to 5/4/2033

2. Importing the certificate is started by clicking the "**Install Certificate...**" button.
   After that, a window opens where you need to select the "**Local Machine**" option and click on the "**Next**" button.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

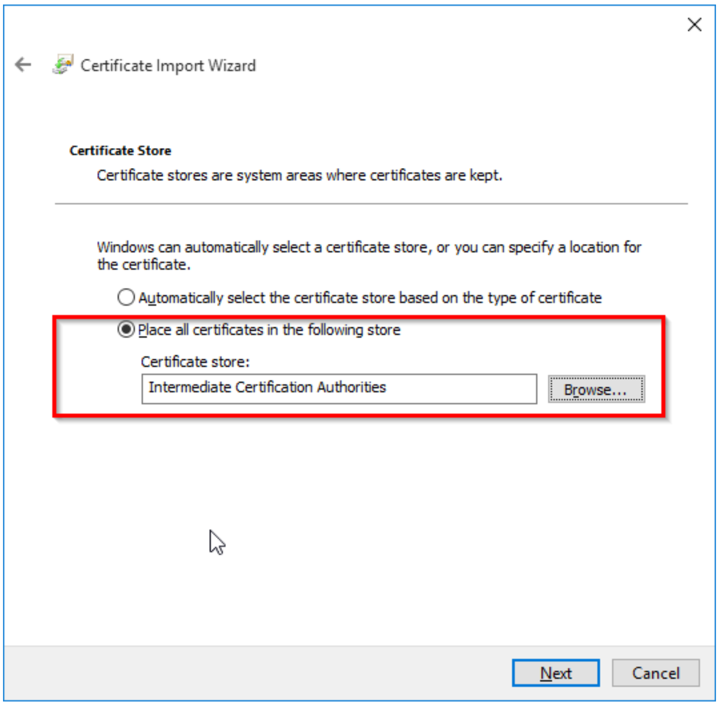
Store Location

○ Current User

● Local Machine

To continue, click Next.

3. In the next window, you need to select the option "**Place all certificates in the following store**", and after that you need to select the name "**Certificate store**:" using the "**Browse**..." button "**Intermediate Certification Authorities**" is intended for certificate store for CA Issuer.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

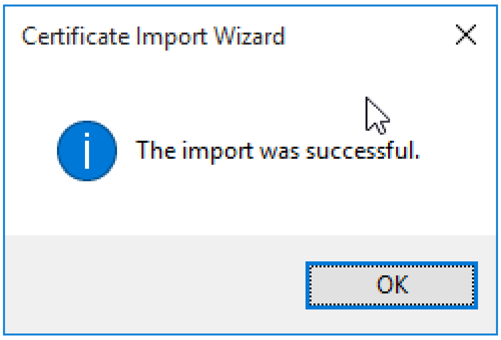
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

4. By clicking the "**Next**" button, the final screen opens, where you need to click the "**Finish**" button. After that, a message about the successful import of the CA Issuer certificate will be displayed, as in the picture below.

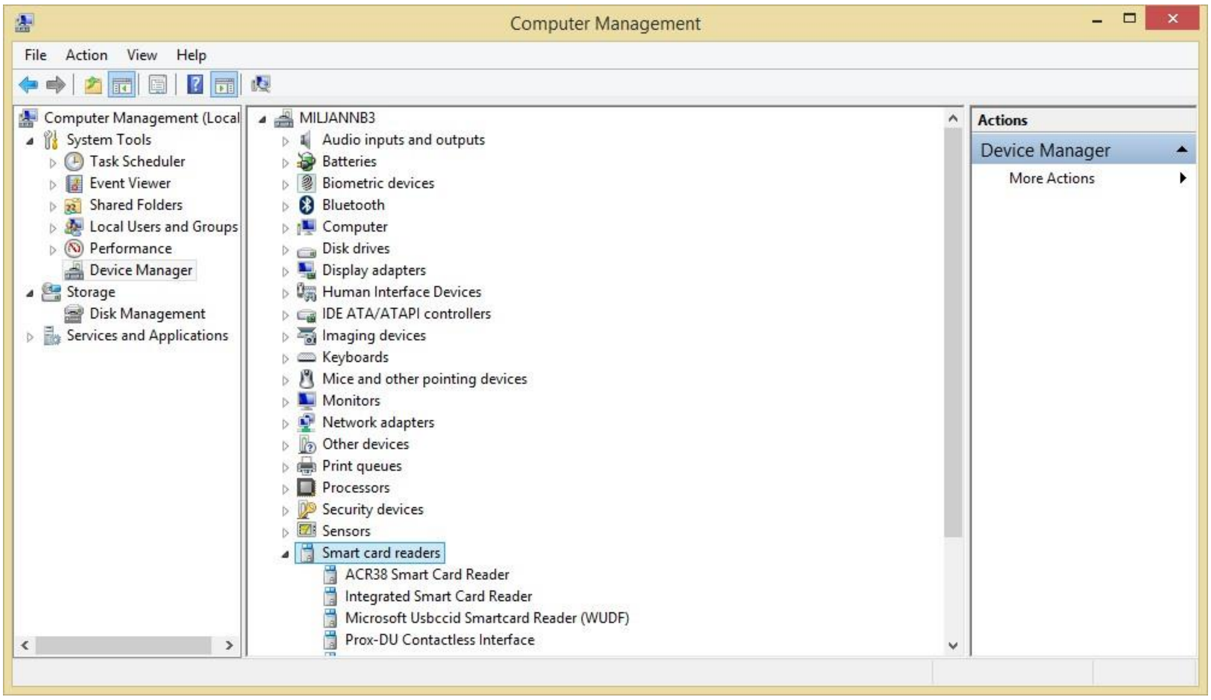

Certificate Import Wizard

The import was successful.

4. Installation of the driver for the Smart Card reader

Drivers for Smart Card readers and tokens, which can be purchased with qualified certificates, are generally automatically installed on Windows computers (10 and 11) when the smart card reader is connected via USB for the first time.

If the installation is successful, the name of the connected smart card reader will be displayed in the "Device Manager" under the node "Smart card readers", as in the picture below.



In case there is a problem with the automatic installation you can always install drivers manually by using the files that are located in the folder "Smart Card Reader Drivers” inside the installation package:

- For the ACS smart card readers install the drivers from the folder “ACS Drivers (ACR39U - ACR39T)”,
- For Thales/Gemalto smart card readers install the drivers from the folder “Thales - Gemalto Drivers (CT30-CT40-K50-K30)”.

5. Installation of ESS QCA Windows software package - SSCD version

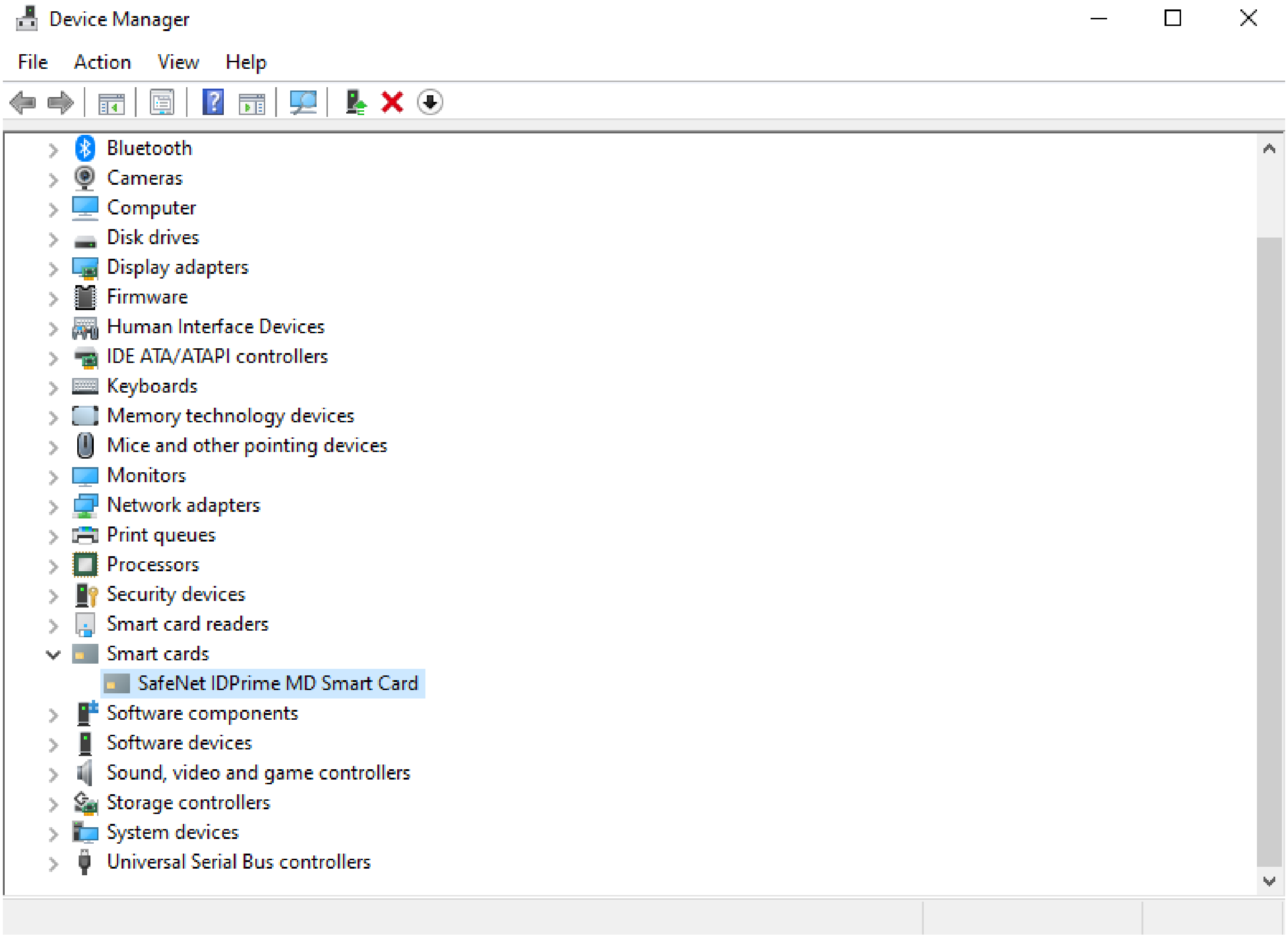
5.1. Installation of Smart Card MiniDriver

In order for a Windows 10 and 11 computers to recognize a chip with a qualified certificate for electronic signature, it is necessary to install a Safenet Minidriver for Windows.

In the "**ESS QCA Windows SSCD**" folder there is a "**Smart Card Minidriver**" folder which contains MSI packages for 32-bit and 64-bit versions of the Windows operating system.

After successful installation of Minidriver, the name of the smart card inserted into the connected USB smart card reader will be displayed in the "Device Manager" under the "Smart cards" node.

If any problems occur, please contact ESS QCA support via web form or email qca@esshitsupport.zohodesk.eu and we will contact yuo as soon as posible.

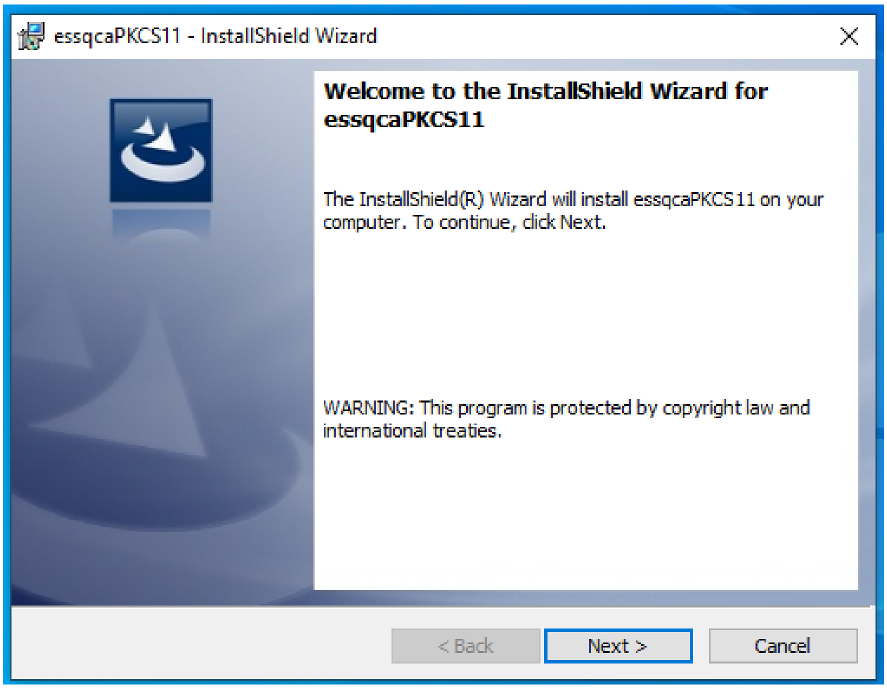


- Bluetooth
- Cameras
- Computer
- Disk drives
- Display adapters
- Firmware
- Human Interface Devices
- IDE ATA/ATAPI controllers
- Keyboards
- Memory technology devices
- Mice and other pointing devices
- Monitors
- Network adapters
- Print queues
- Processors
- Security devices
- Smart card readers
- Smart cards
  - SafeNet IDPrime MD Smart Card
- Software components
- Software devices
- Sound, video and game controllers
- Storage controllers
- System devices
- Universal Serial Bus controllers

5.2. Installation of ESS QCA PKCS11

The installation of this package is necessary if the qualified certificate will be used for signing on applications and portals of state authorities such as: ePorezi, eUprava NexU-APR, CROSO, CEOP etc... The installation package is located in the "**PKCS11**" folder.

1. The installation process is started by double-clicking"**essqcaPKCS11.**
2. Clicking the "**Next**" button continues the installation.



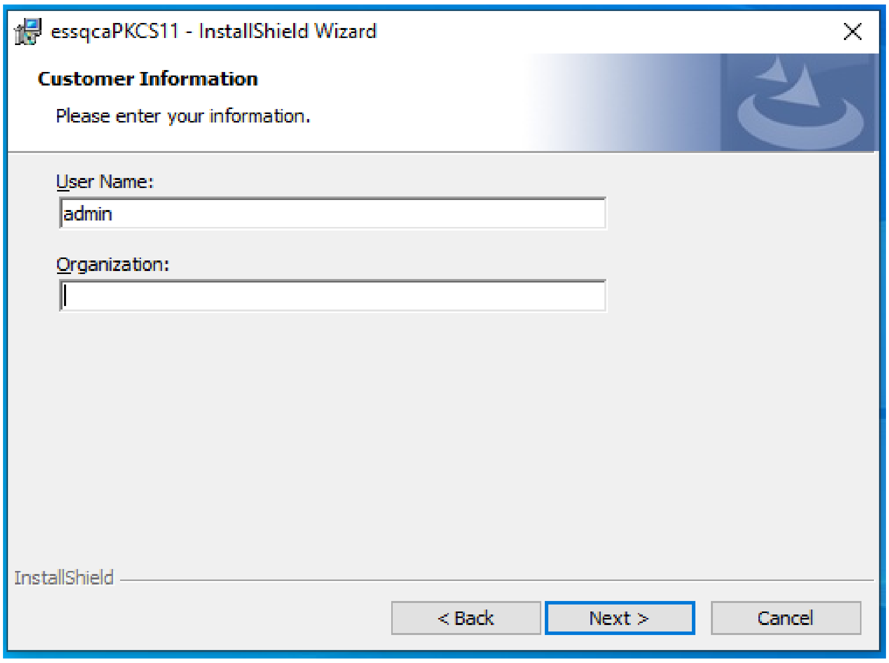
essqcaPKCS11 - InstallShield Wizard

Welcome to the InstallShield Wizard for essqcaPKCS11

The InstallShield(R) Wizard will install essqcaPKCS11 on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

3. Entering or changing the "**User Name**" and "**Organization**" fields is optional. Click on the "Next" button.



essqcaPKCS11 - InstallShield Wizard

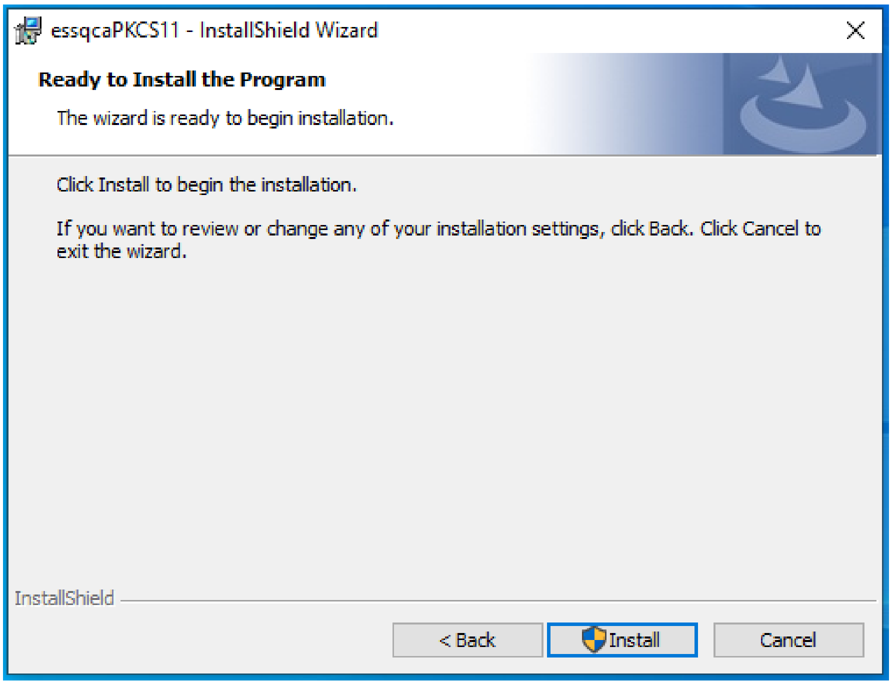
Customer Information

Please enter your information.

User Name: admin

Organization:

4. Clicking the "**Install**" button starts the installation.



essqcaPKCS11 - InstallShield Wizard

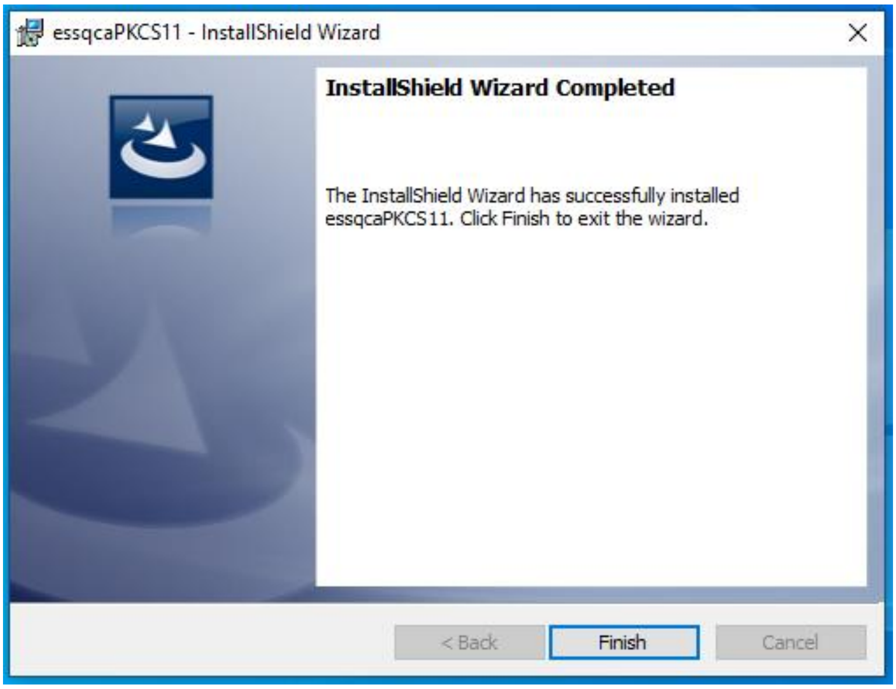
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

5. The installation is completed successfully and clicking the "**Finish**" button closes the window.



essqcaPKCS11 - InstallShield Wizard

InstallShield Wizard Completed

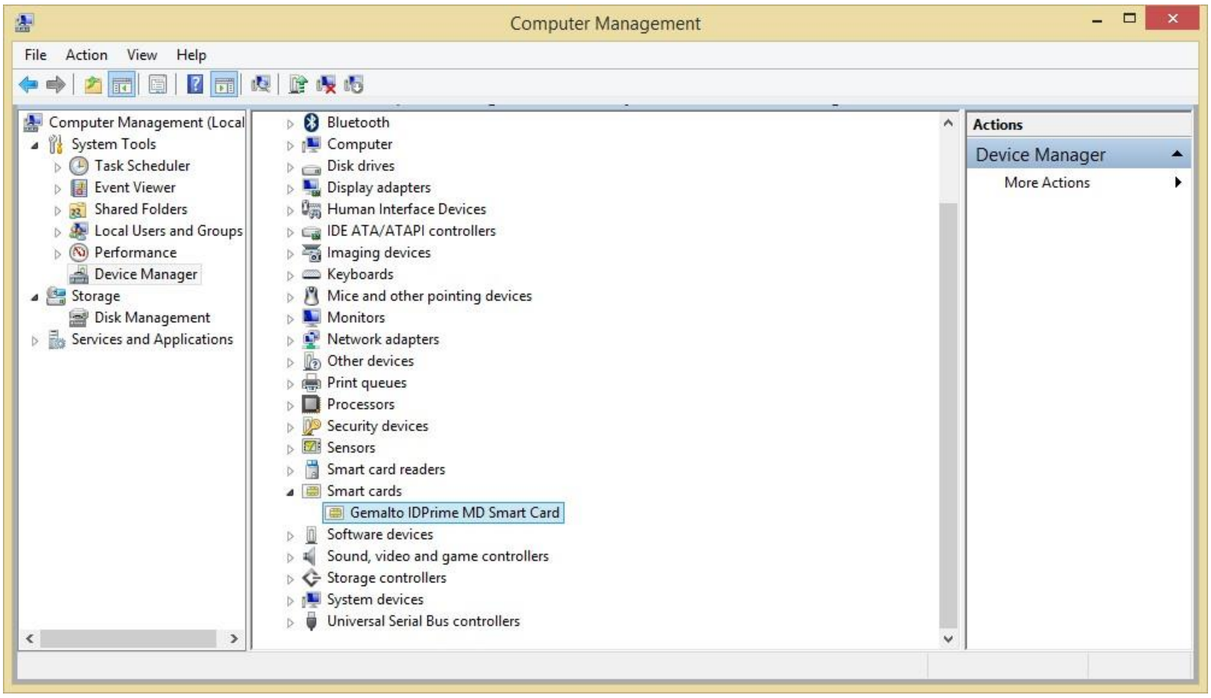
The InstallShield Wizard has successfully installed essqcaPKCS11. Click Finish to exit the wizard.

6. Installation of ESS QCA Windows software package - QSCD version

In order for a Windows 10 and 11 computers to recognize a chip with a qualified certificate for electronic signature, it is necessary to install Thales SafeNet Minidriver and PKCS#11.

In the "**ESS QCA Windows QSCD**" folder, there is a "**QSCD Minidriver and PKCS11**" folder that contains MSI packages for 32-bit and 64-bit versions for Windows OS. The PKCS11 library is also installed within the package, which serves the needs of signing to public service applications such as: ePorezi, eUprava, NexU-APR, CROSO, CEOP, etc...

After the successful installation, the name of smart card inserted into the connected USB smart card reader will be displayed in the "Device Manager" under the "Smart cards" node.



If any problems occur, please contact ESS QCA support via web form or email qca@esshitsupport.zohodesk.eu and we will contact yuo as soon as posible.

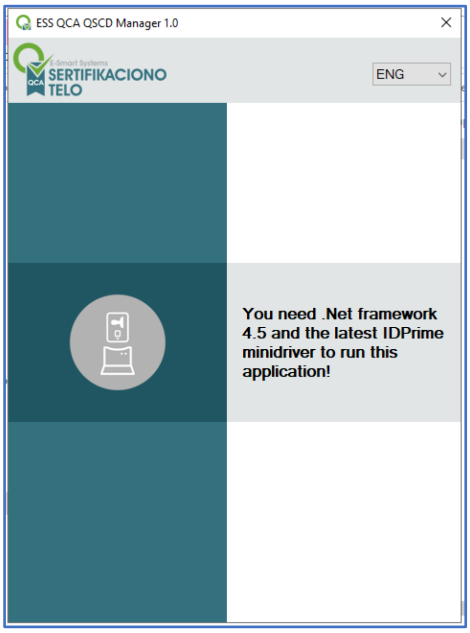
7. Application for changing and unblocking PIN

Depending on the versions of the operating system, on the Software download and installation page in the User applications section, you can find two versions of the application for changing and unblocking the PIN, namely:

- For Windows 11 - QCA QSCD Manager W11
- For other operating systems (Windows 10) - QCA QSCD Manager

NOTE: The procedure for changing and unlocking the PIN is the same regardless of the version of the application or OS.

Necessary prerequisites for using the application are .net framework 4.5 (or higher) and the latest version of the Thales SafeNet Minidriver for IDPrime smart cards (see chapter 5 and 6). If these conditions are not met, when starting the application, the following window will open:



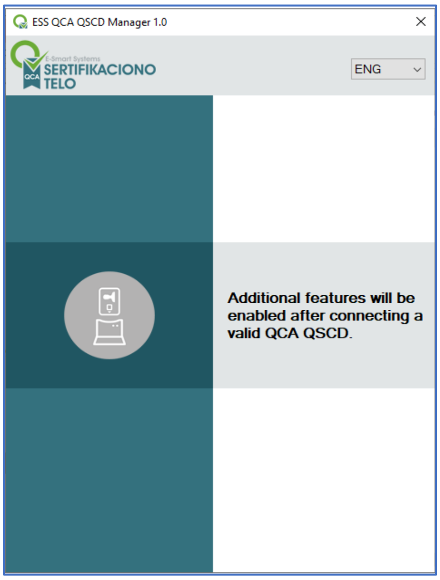
You need .Net framework 4.5 and the latest IDPrime minidriver to run this application!

7.1. Changing PIN

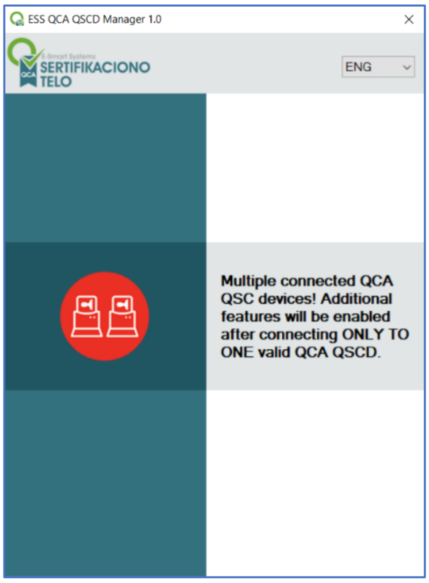
It is recommended that the initial PIN code, which you receive in the PIN envelope with the device, should be changed after the first use. You can change your PIN at any time during the validity of the certificate.

You need to have your QSCD device with a qualified certificate with you - a smart card (and a suitable reader) or USB token, as well as a PIN envelope containing the PIN code.

By starting the application, all smart card readers are detected automatically. If you don't have any or you have several QSCD devices that are connected to your computer, one of the windows from the picture will appear.



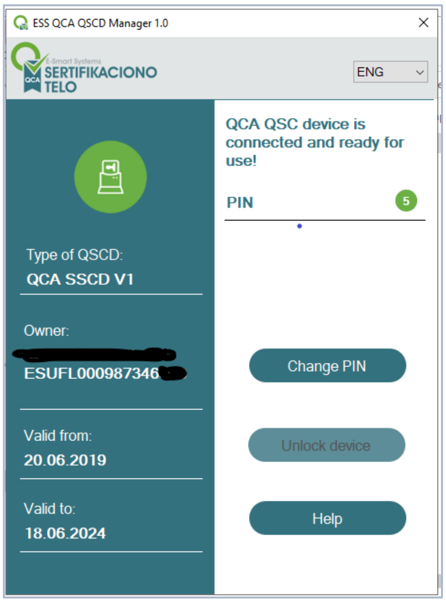
Additional features will be enabled after connecting a valid QCA QSCD.



Multiple connected QCA QSC devices! Additional features will be enabled after connecting ONLY TO ONE valid QCA QSCD.

The application is in active mode only when it finds **ONE** personalized QSCD device with an **ESS QCA** qualified certificate.

The application will automatically display data on the type of connected device, data from the subject of the certificate as well as the remaining number of PIN entries (for **SSCD V1** and **SSCD V2** devices - left image below) or the remaining number of PIN and PUK entries for devices **QSCD V3** (right image below).



QCA QSC device is connected and ready for use!

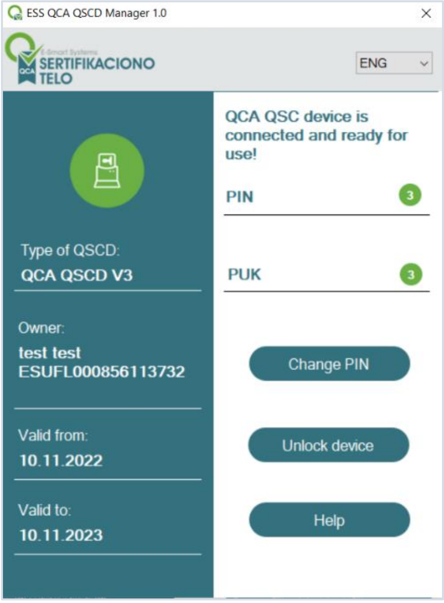
PIN 5

Type of QSCD:
QCA SSCD V1

Owner:
[redacted]
ESUFL000987346[redacted]

Valid from:
20.06.2019

Valid to:
18.06.2024



QCA QSC device is connected and ready for use!

PIN 3

PUK 3

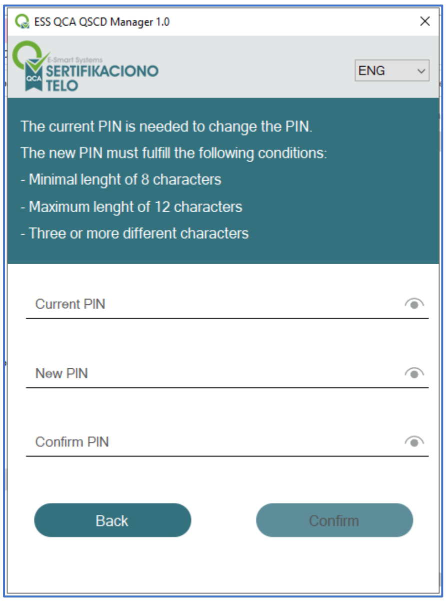
Type of QSCD:
QCA QSCD V3

Owner:
test test
ESUFL000856113732

Valid from:
10.11.2022

Valid to:
10.11.2023

By clicking a button **Change PIN**, a window for changing the PIN opens, where you need to fill in the empty fields, namely: **Current PIN** (if you haven't changed it before, then it's the PIN found in the PIN envelope you received with the QSCD device), **New PIN** and once again it is necessary in the field **PIN confirmation** to enter the new PIN value.



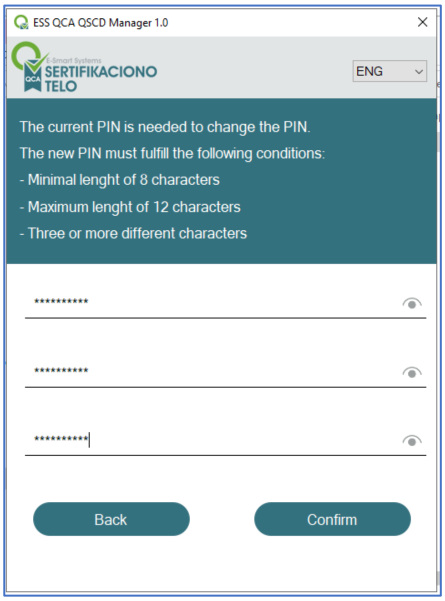
ESS QCA QSCD Manager 1.0

The current PIN is needed to change the PIN.
The new PIN must fulfill the following conditions:
- Minimal lenght of 8 characters
- Maximum lenght of 12 characters
- Three or more different characters

Current PIN

New PIN

Confirm PIN



ESS QCA QSCD Manager 1.0

The current PIN is needed to change the PIN.
The new PIN must fulfill the following conditions:
- Minimal lenght of 8 characters
- Maximum lenght of 12 characters
- Three or more different characters

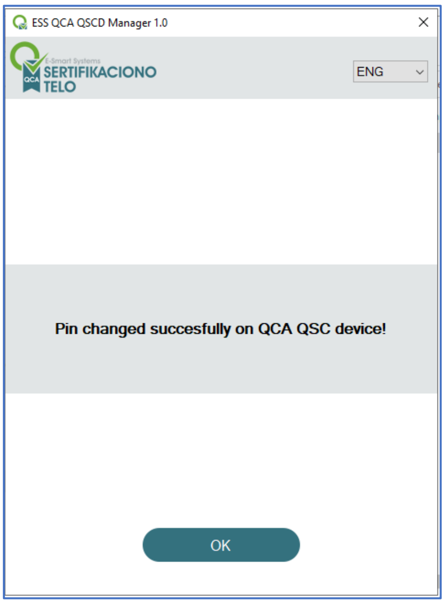
****

****

****

In each field you fill in, there is an option to view (by clicking on the "eye") and change the entered data, which reduces the possibility of errors.

If you have filled in all the required fields following the instructions on the application itself, by clicking the **Confirm** button, the PIN of your QSCD device will be set to the new, desired value. The message "PIN changed successfully on QCA QSCD device!" will appear in the window.



ESS QCA QSCD Manager 1.0

Pin changed succesfully on QCA QSC device!

If you have used the maximum allowed number for the incorrect entry of the current PIN, the PIN code, and thus the QSCD device, will be blocked.

You can unblock all types of devices in **ESS QCA**. In order to unblock device in ESS QCA, you need to submit a request for unblocking and contact ESS QCA support. Your personal presence and device are requested. On that occasion, you will be issued a new PIN envelope with new PIN code value.

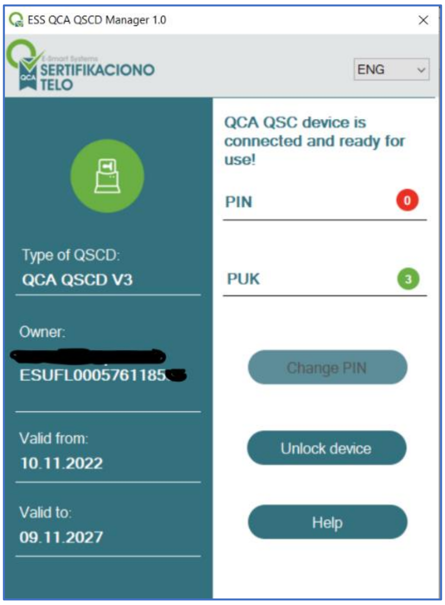
PIN unlocking on **QCA QSCD V3** type devices can also be done via the application - **QCA QSCD Manager**, and the description of this procedure can be found in the rest of this document.

7.2. PIN unlocking

NOTE: Only for devices of the **QCA QSCD V3** type, you can perform the unblocking via the **QCA QSCD Manager** application**.**

It is necessary to have with you the blocked device, as well as the PIN envelope that came with the device, which, in addition to the PIN, also contains the PUK code used to unblock/unlock this type of device.

By starting the application, all smart card readers are detected. The application enters active mode only when it finds one personalized QSCD device with an **ESS QCA** qualified certificate.



ESS QCA QSCD Manager 1.0

QCA QSC device is connected and ready for use!

PIN 0

PUK 3

Type of QSCD:
QCA QSCD V3

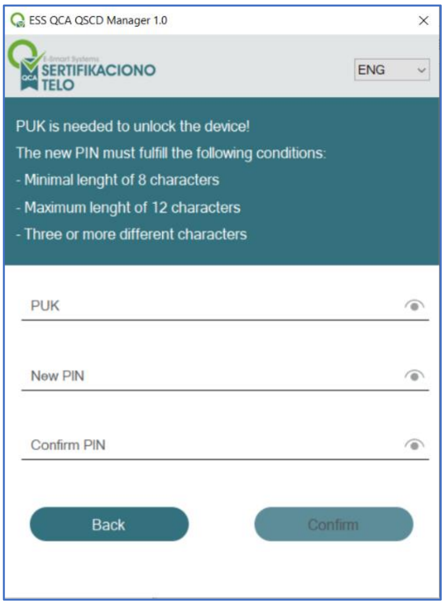
Owner:
[redacted]
ESUFL0005761185[redacted]

Valid from:
10.11.2022

Valid to:
09.11.2027

The application will automatically display the type of connected device and data from the Subject of the certificate, the remaining number of PIN entry attempts, which in this case is 0 (zero), as well as the remaining number of PUK entry attempts.

Clicking the **Unlock device** button opens the PIN unlock window. It is necessary to fill in the empty fields, first of all the PUK code found in the PIN envelope that you received with the device, then the New PIN and **Confirm PIN** fields. In each field you fill in, there is also an option to view the entered data (by clicking on the "eye"), which reduces the possibility of errors.

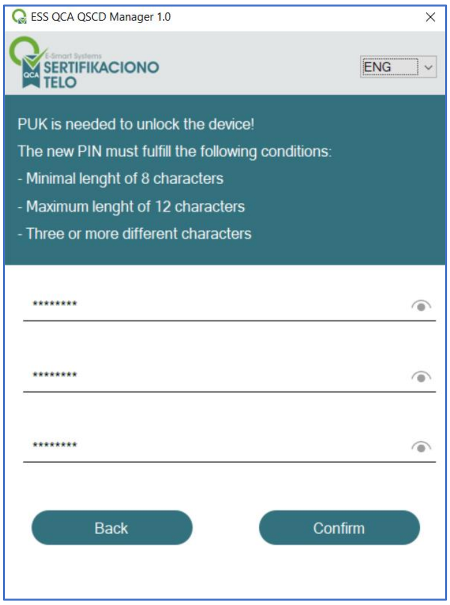


ESS QCA QSCD Manager 1.0

PUK is needed to unlock the device!

The new PIN must fulfill the following conditions:

- Minimal lenght of 8 characters
- Maximum lenght of 12 characters
- Three or more different characters



ESS QCA QSCD Manager 1.0

PUK is needed to unlock the device!

The new PIN must fulfill the following conditions:

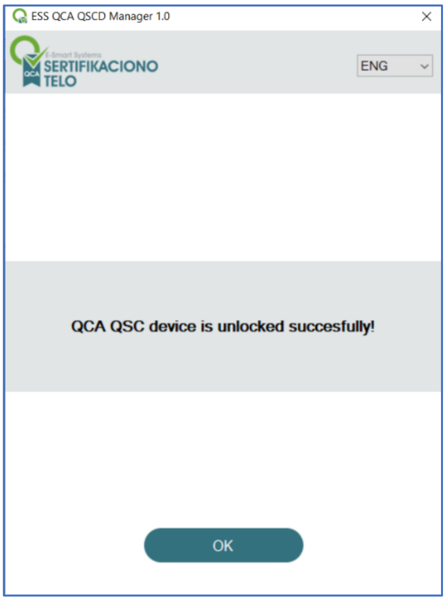
- Minimal lenght of 8 characters
- Maximum lenght of 12 characters
- Three or more different characters

****

****

****

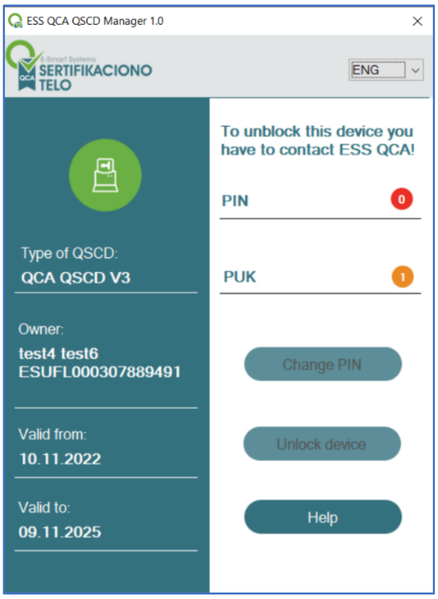
If you have filled in all the required fields by following and following the instructions on the application itself, by clicking the **Confirm** button, the PIN code of your QSCD device will be set to the new, desired value, and the device itself will be unlocked. The message "QCA QSCD device successfully unlocked!" will also appear in the window.



ESS QCA QSCD Manager 1.0

QCA QSC device is unlocked succesfully!

In case you entered the wrong PUK two (2) times during the PIN unblocking process, independent PIN unblocking is no longer possible.



ESS QCA QSCD Manager 1.0

To unblock this device you have to contact ESS QCA!

Type of QSCD: QCA QSCD V3

Owner: test4 test6 ESUFL000307889491

Valid from: 10.11.2022

Valid to: 09.11.2025

In this case, unlocking the device can only be done by the ESS QCA. In order to unblock device in ESS QCA, you need to submit a request for unblocking and contact ESS QCA support. Your personal presence and device are requested. On that occasion, you will be issued a new PIN envelope with new PIN and PUK code values.

Clicking the **Help** button will open the ESS QCA support contact details.