

U-QCA-221

Document code

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

Content

1. Requirements for using ESS QCA Qualified certificate for electronic signature	3
2. Downloading the ESS QCA Windows installation package.....	3
3. Installation of ESS QCA trust chain	4
3.1. Importing the Root CA certificate for Signature and Seal	4
3.1.1. For qualified certificates for electronic signature issued before 04/08/2024	4
3.1.2. For qualified certificates for electronic signature and seal issued after 04/08/2024	6
3.2. Importing Issuer CA certificates	8
3.2.1. For qualified certificates for electronic signature issued before 04/08/2024	8
3.2.2. For qualified certificates for electronic signature issued after 04/08/2024	10
3.2.3. For qualified certificates for electronic seal	12
4. Installation of the driver for the Smart Card reader	14
5. Installation of ESS QCA SafeNet Minidriver & PKCS11 package	15
6. Application for changing and unblocking PIN	16
6.1. Changing PIN.....	16
6.2. PIN unlocking	19

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@esshitsuport.zohodesk.eu and we will contact you as soon as possible.

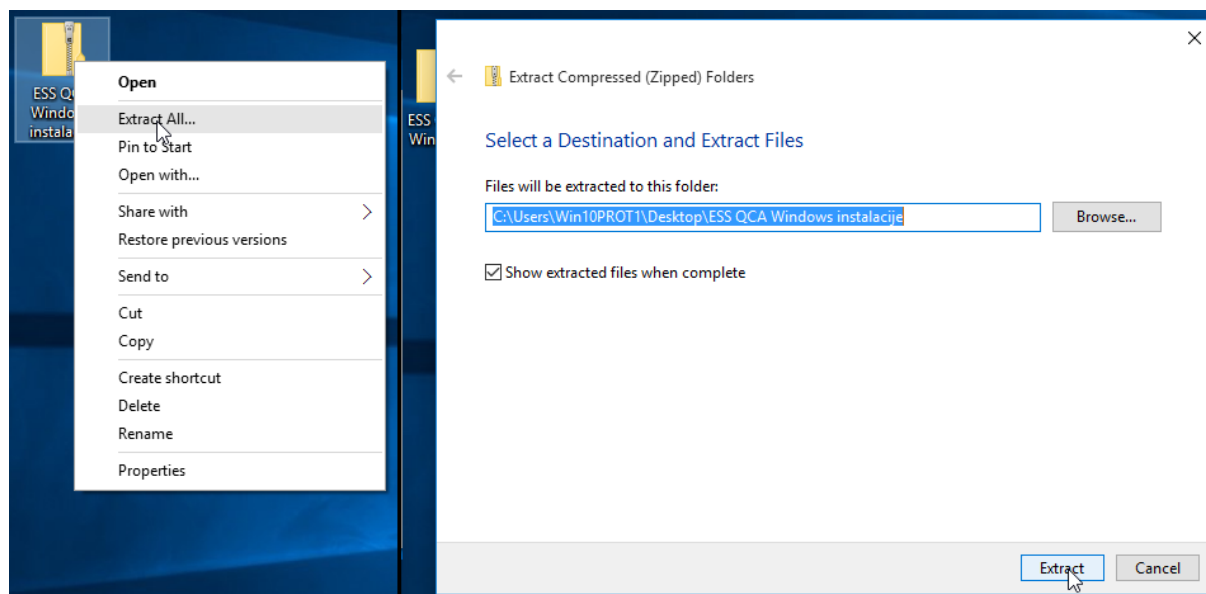
To be able to use ESS QCA Qualified certificate successfully you will have to install ESS QCA trust chain (Certification Authority root and issuer certificates), SafeNet Midriver with PKCS#11 middleware and drivers for the smart card reader or the USB token (usually automatically detected by the Windows).

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/en/> on the "Download Software" page, by clicking the link "ESS QCA Windows Installation Package".

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.



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 chain of trust

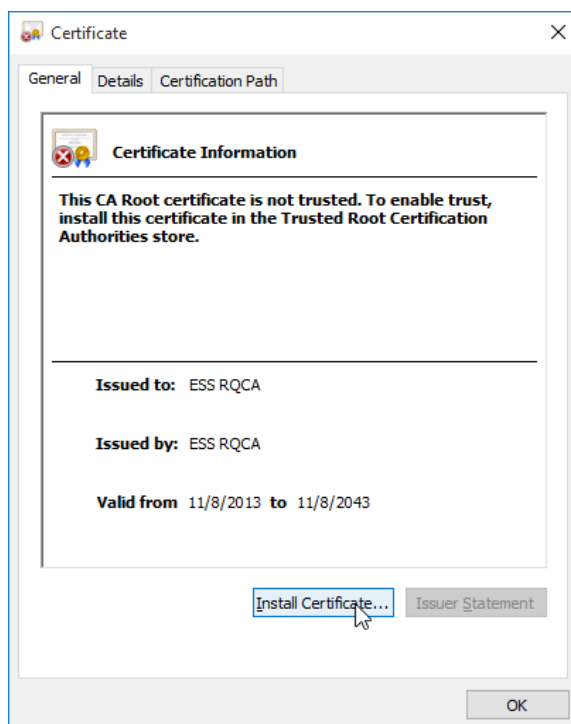
The ESS QCA chain of trust consists of Root CA and Issuer CA certificates which are located inside the "Certificates" folder of the installation package. These certificates need to be imported into the local certificate store on the Windows machine in order to establish trust between that machine and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

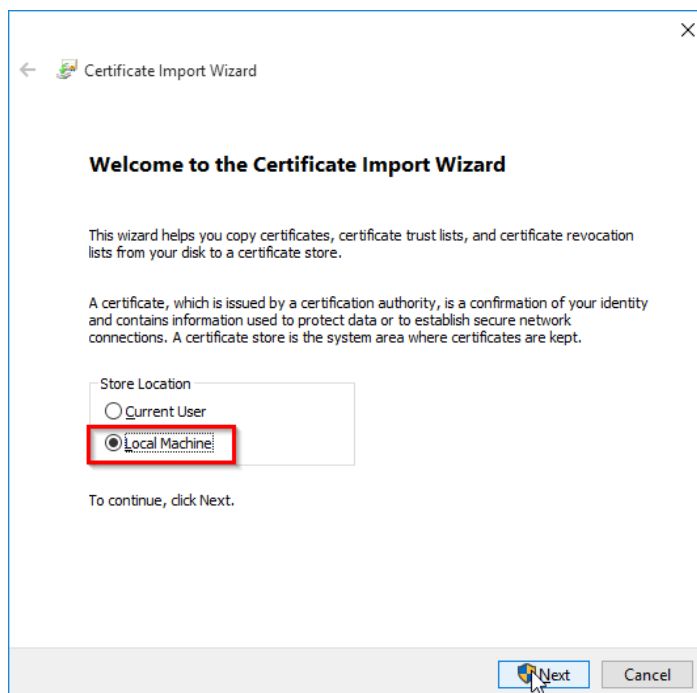
3.1. Importing the Root CA certificate for Signature and Seal

3.1.1. For qualified certificates for electronic signature issued before 04/08/2024

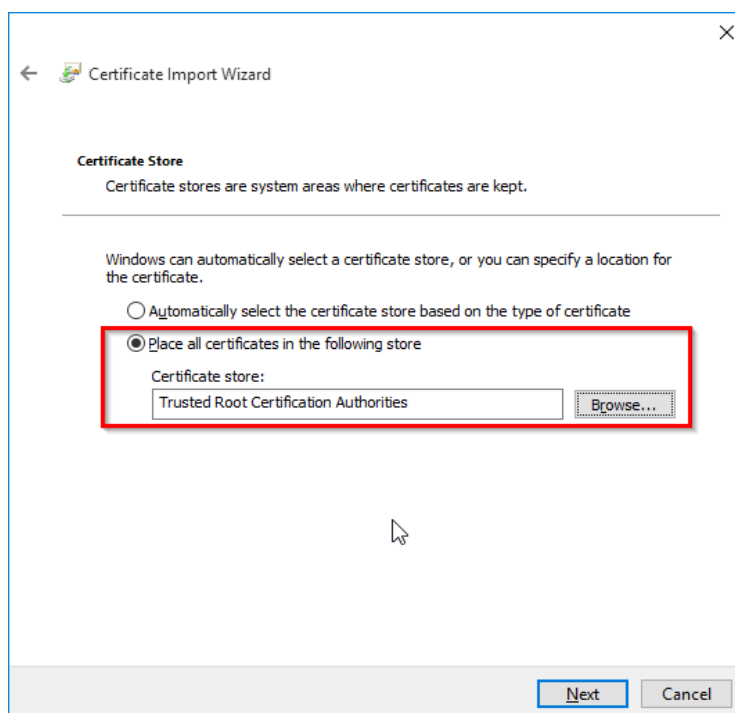
The Root CA (ESS RQCA) certificate can be imported as follows:

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.

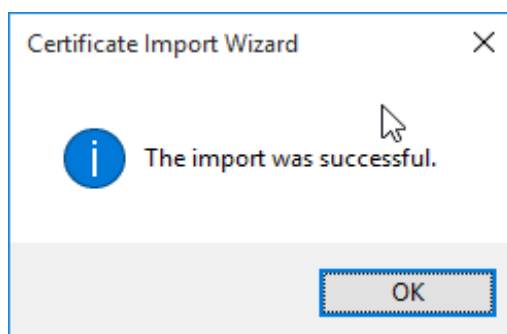




3. In the next window, you need to select the option **"Place all certificates in the following store"**, and after that you need to select the name **"Certificate store:"** using the **"Browse..."** button. **"Trusted Root Certification Authorities"** is intended as a certificate store for Root CA.



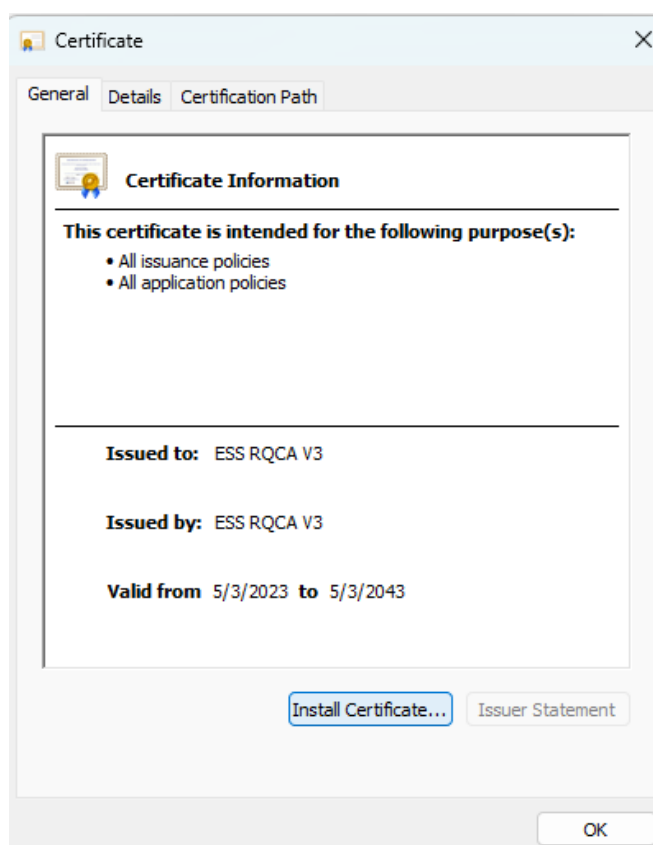
4. By clicking the **"Next"** button, the final screen opens, where you need to click the **"Finish"** button. After that, a message about the successful import of the Root CA certificate will be displayed, as in the image below.

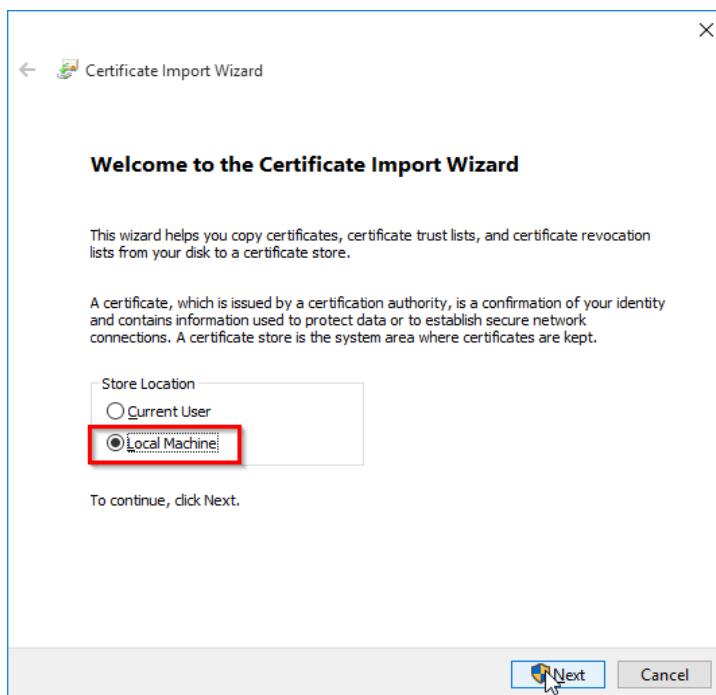


3.1.2. For qualified certificates for electronic signature and seal issued after 04/08/2024

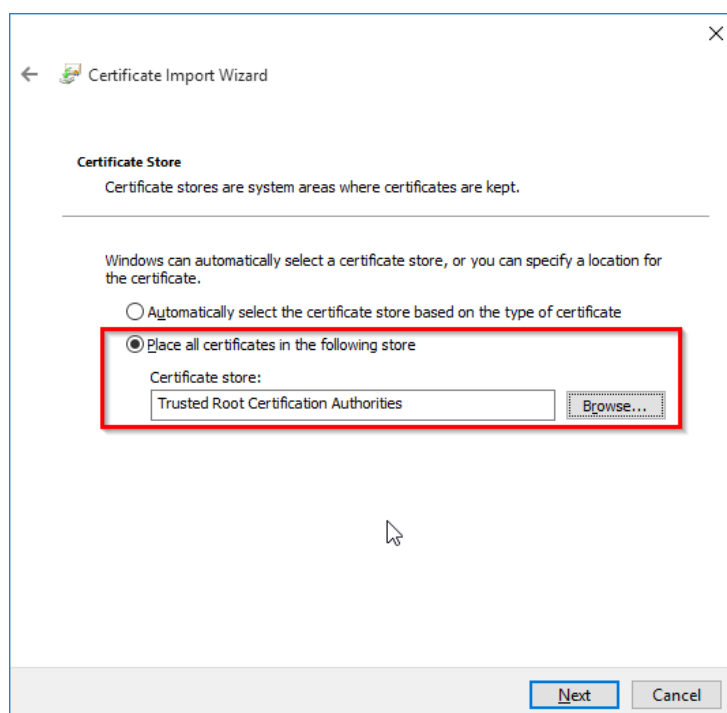
The Root CA (ESS RQCA) certificate can be imported as follows:

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.

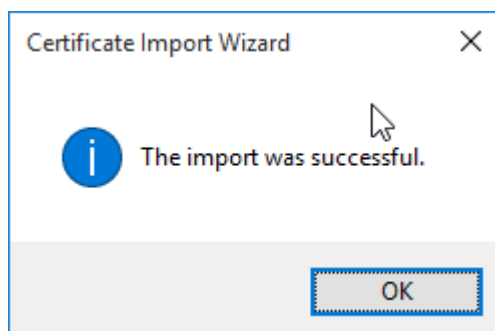




3. In the next window, you need to select the option "Place all certificates in the following store", and after that you need to select the name "Certificate store:" using the "Browse..." button. "Trusted Root Certification Authorities" is intended as a certificate store for Root CA.



- 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 Root CA certificate will be displayed, as in the image below.

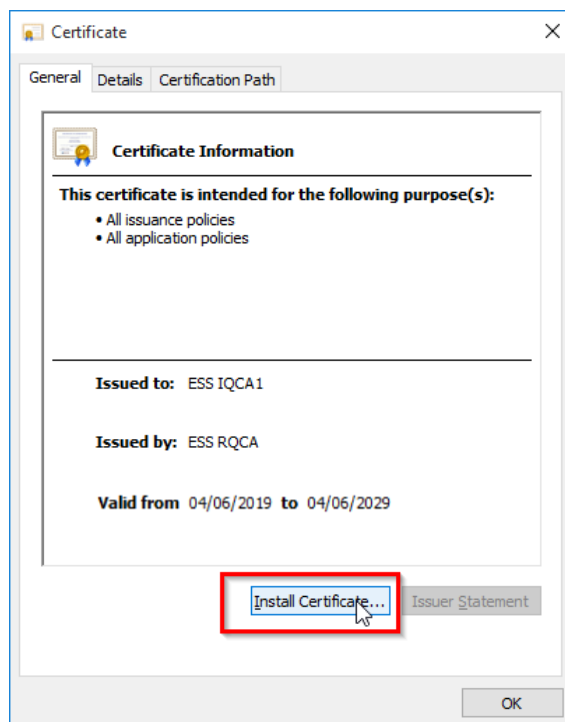


3.2. Importing Issuer CA certificates

3.2.1. For qualified certificates for electronic signature issued before 04/08/2024

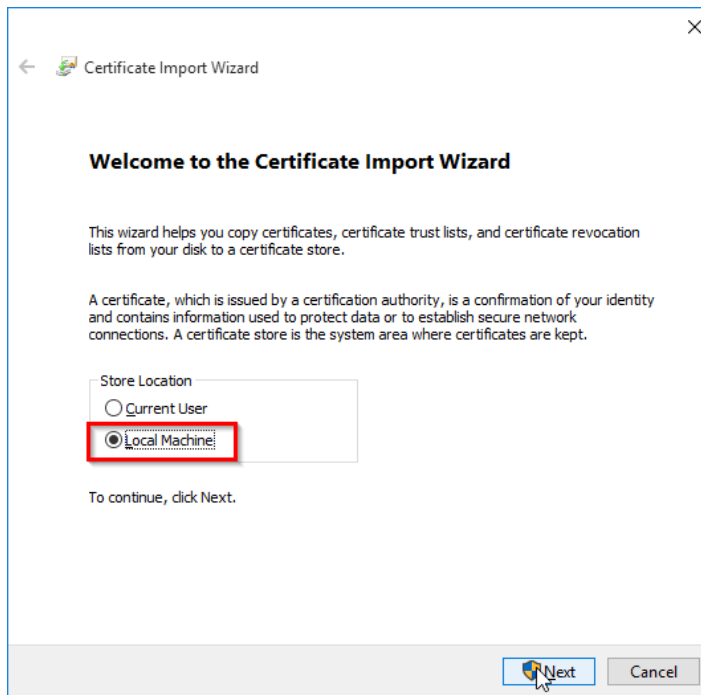
The Issuer CA (ESS IQCA) certificate can be imported as follows:

- It is necessary to open the **"ESS IQCA1(3).cer"** certificate with a double click, after which a window will appear as in the picture below.

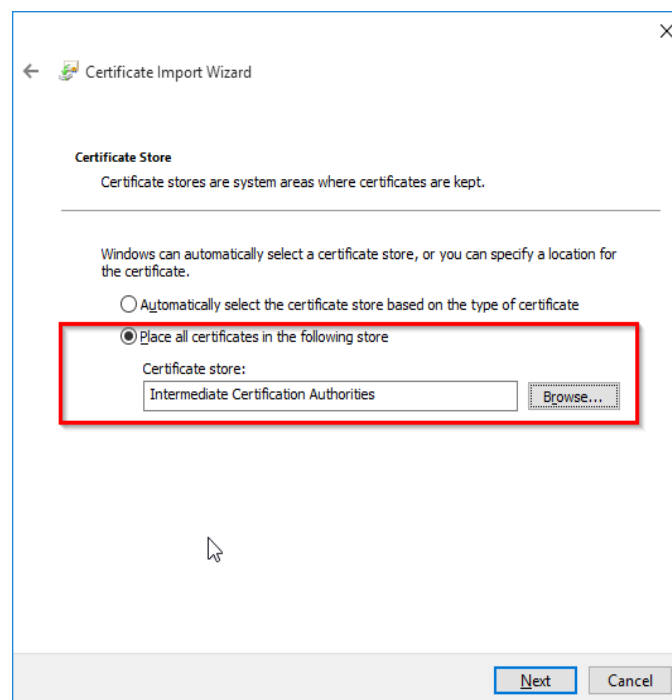


Importing the certificate is started by clicking the **"Install Certificate..."** button.

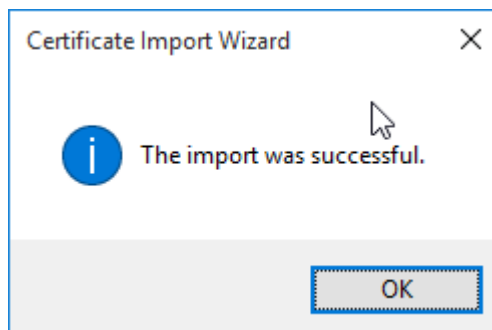
After that, a window opens where you need to select the **"Local Machine"** option and click on the **"Next"** button.



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 Issuer CA.



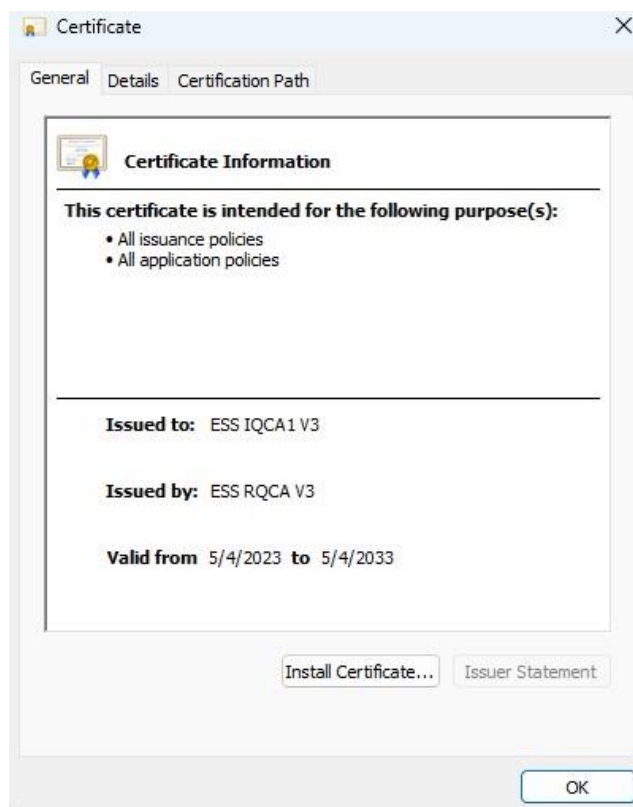
3. By clicking the **"Next"** button, the final screen opens, where you need to click the **"Finish"** button. After that, a message about the successful import of the Issuer CA certificate will be displayed, as in the picture below.



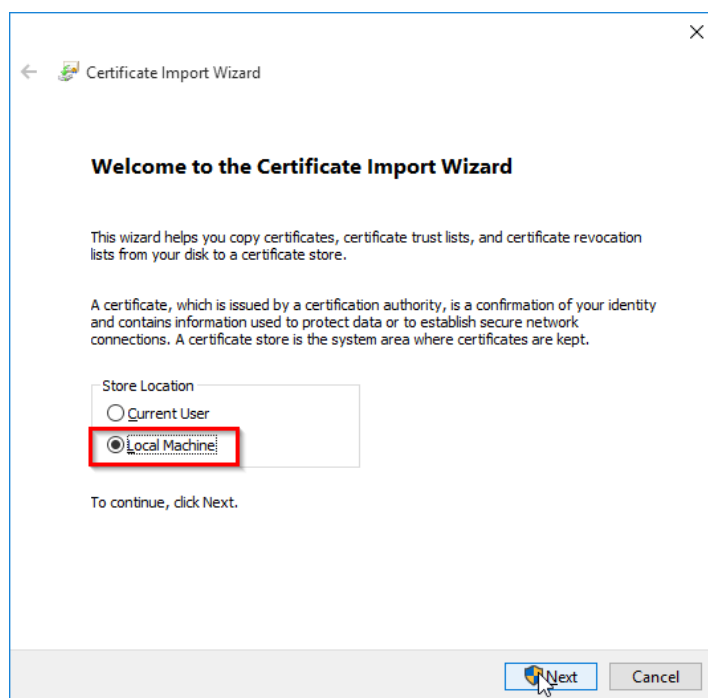
3.2.2. For qualified certificates for electronic signature issued after 04/08/2024

The Issuer CA (ESS IQCA) certificate can be imported as follows:

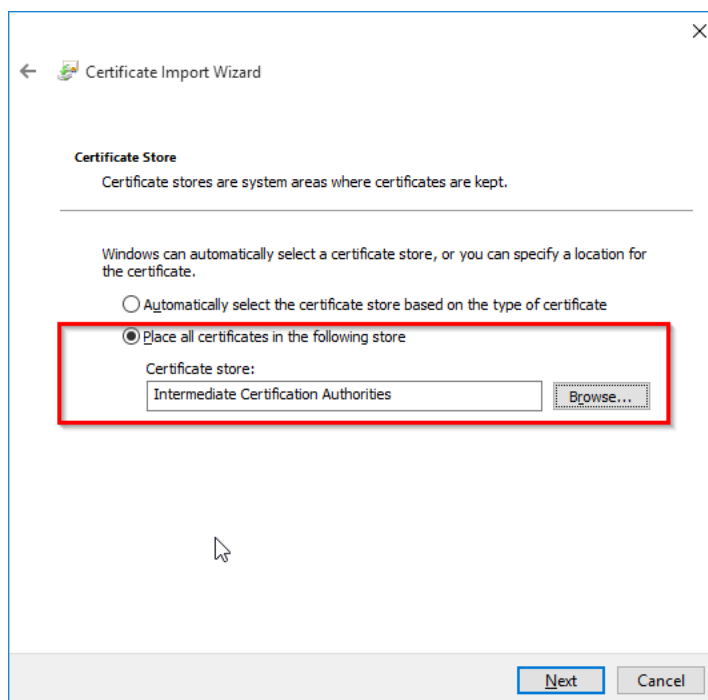
1. It is necessary to open the **"ESS IQCA1 V3.cer"** certificate with a double click, after which a window will appear as in the picture below.



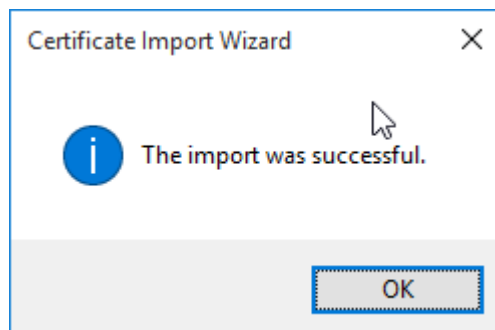
- Importing the certificate is started by clicking the **"Install Certificate..."** button.
After that, a window opens where you need to select the **"Local Machine"** option and click on the **"Next"** button.



- 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 Issuer CA.



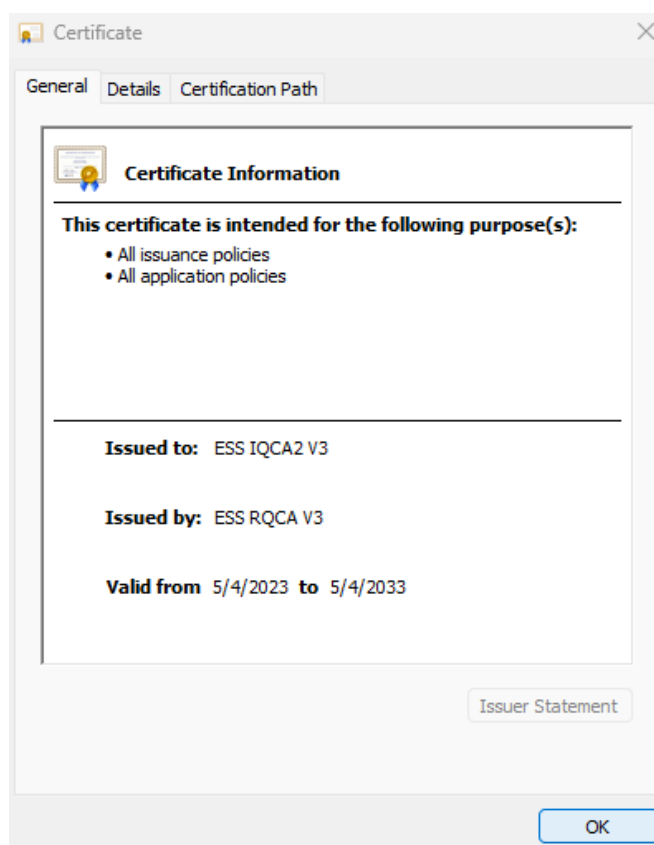
- By clicking the **"Next"** button, the final screen opens, where you need to click the **"Finish"** button. After that, a message about the successful import of the Issuer CA certificate will be displayed, as in the picture below.



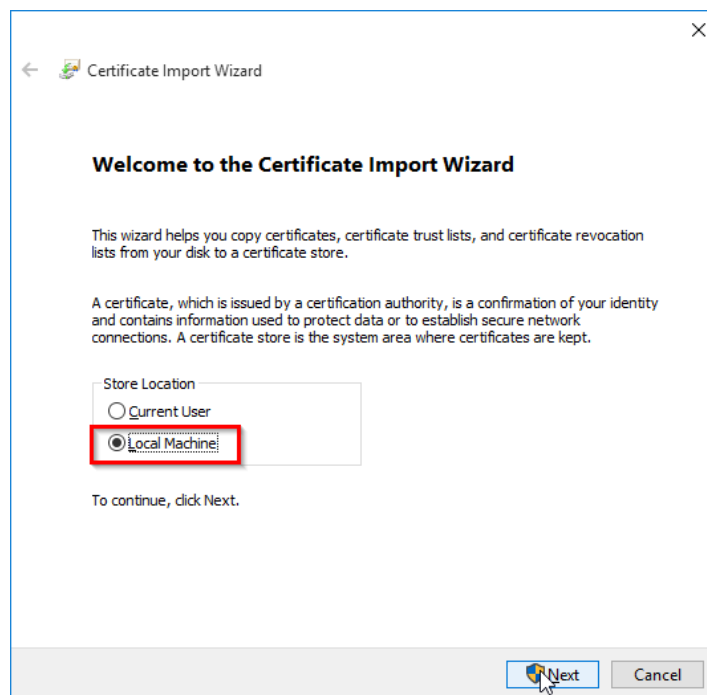
3.2.3. For qualified certificates for electronic seal

The Issuer CA (ESS IQCA) certificate can be imported as follows:

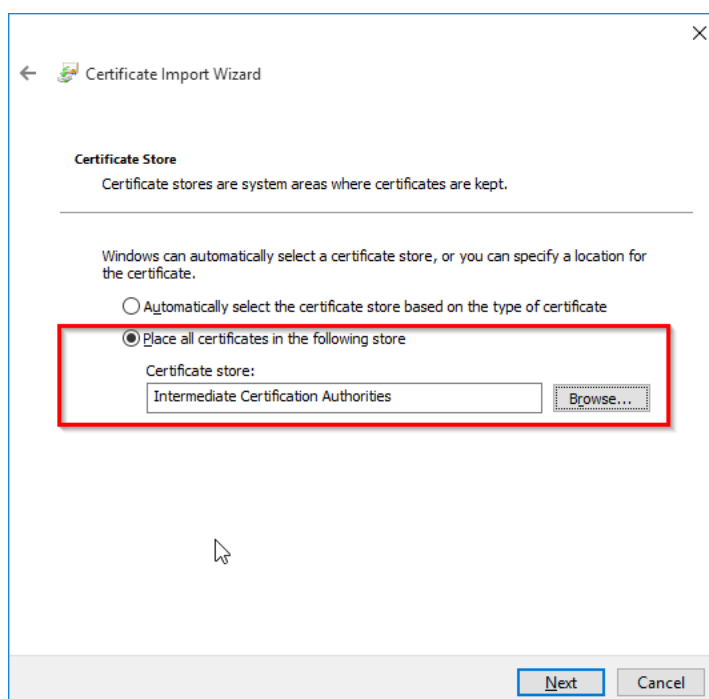
- Double-click the „ESS IQCA2 V3.cer“ and the following window will appear.



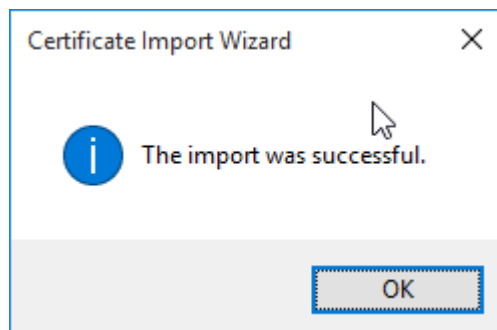
- The import process begins by clicking „**Install Certificate...**“.
After that, a window appears where „**Local Machine**“ should be selected and after that „**Next**“ should be clicked.



- On the following window it is necessary to select „**Place all certificates in the following store**“ and after that select the „**Certificate store:**“ using the „**Browse...**“ button. „**Intermediate Certification Authorities**“ should be selected.



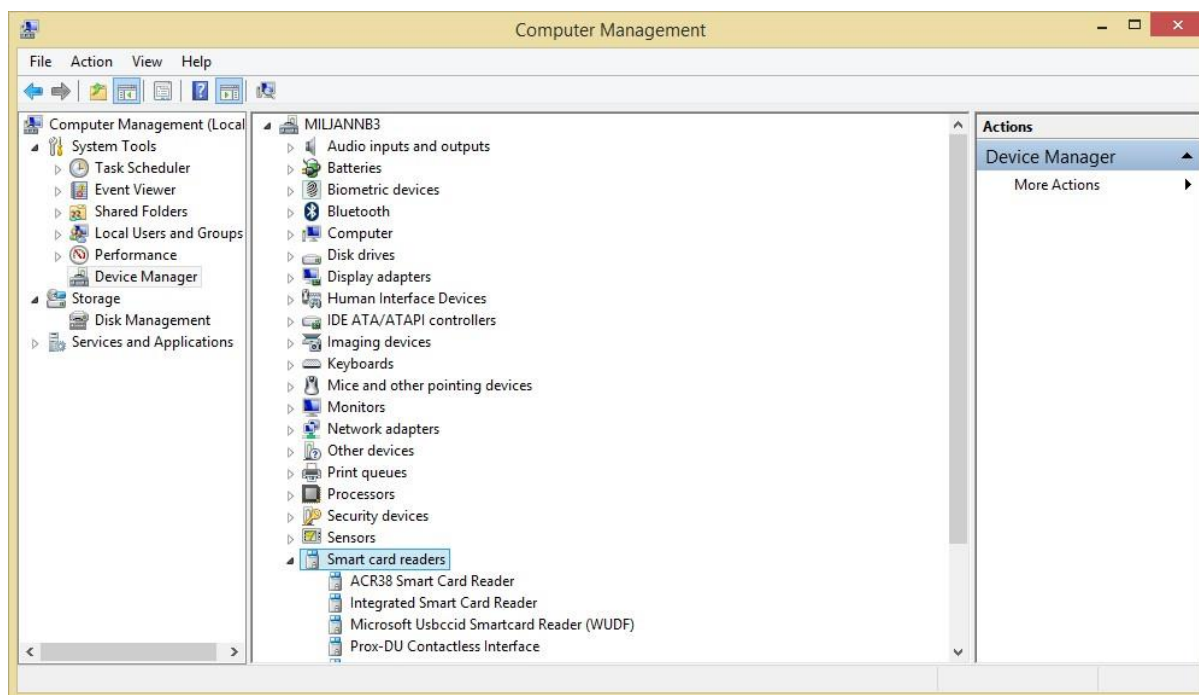
4. Clicking „Next“, a final prompt appears and by pressing „Finish“ the process concludes. After that a message will display notifying us that the Issuer CA certificate has been imported successfully.



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:

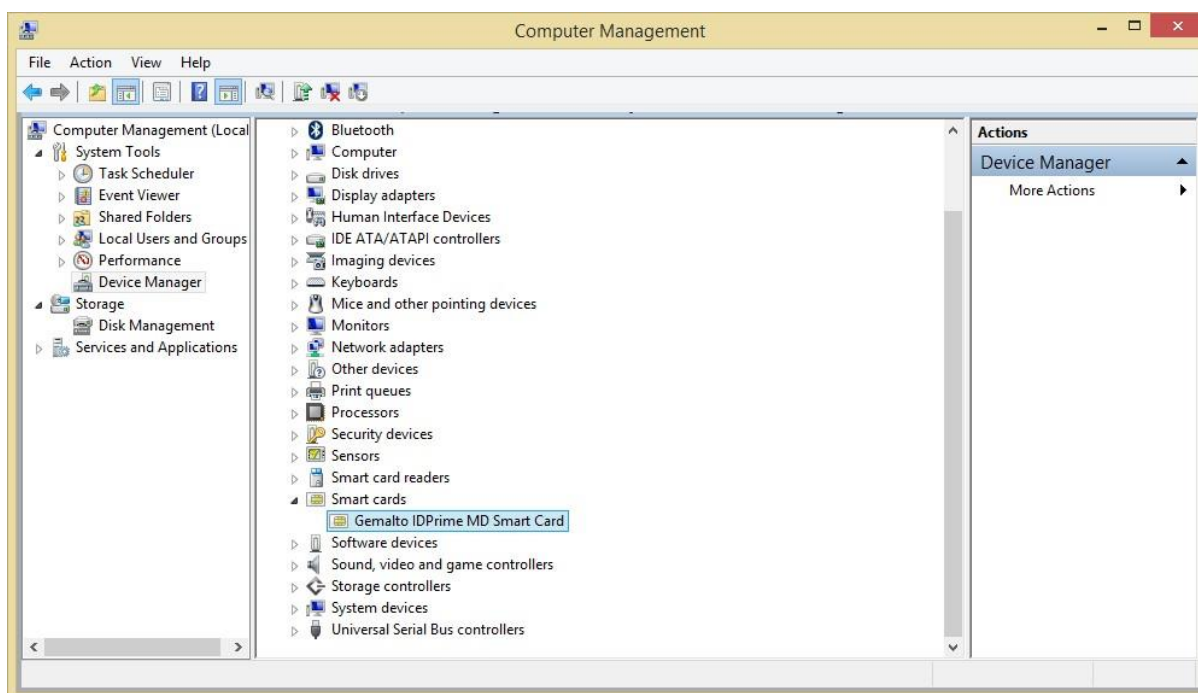
- For the ACS smart card readers install the drivers from the folder "ACS Drivers",
- For Thales/Gemalto smart card readers install the drivers from the folder "Thales - Gemalto Drivers (CT30-CT40-K50-K30)".

5. Installation of ESS QCA SafeNet Minidriver & PKCS11 package

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_Installer**" folder, there is a "**SafeNet Minidriver & PKCS11**" folder that contains MSI packages for 32-bit, 64-bit and arm64 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.

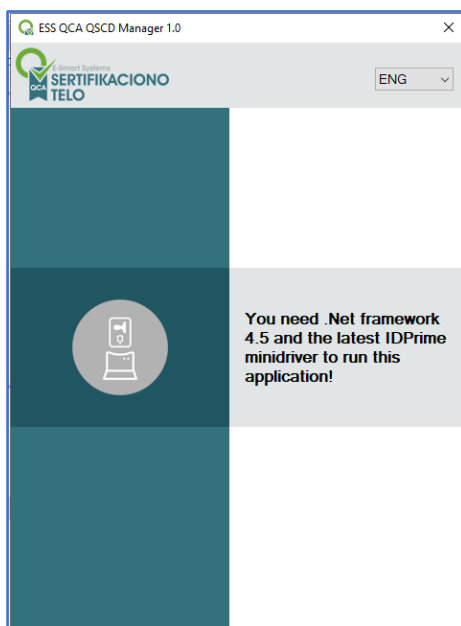


If any problems occur, please contact ESS QCA support via [web form](#) or email gca@esshitsuport.zohodesk.eu and we will contact you as soon as possible.

6. Application for changing and unblocking PIN

On the ESS QCA [Software download and installation](#) webpage under the **User applications** section, you can find the link for the download of the [application for changing and unblocking the PIN](#).

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:



6.1. 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.

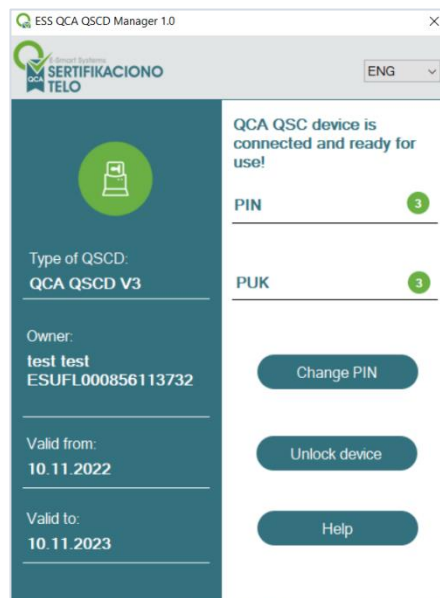
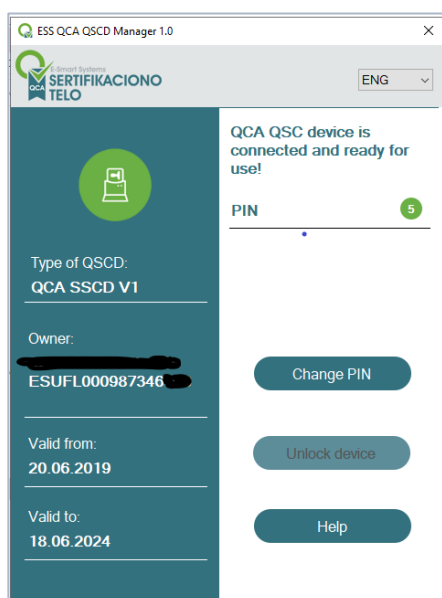
You need to have your QSCD device with a qualified certificate with you - a smart card (and a suitable reader) or USB token, as well as a PIN envelope containing the PIN code.

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.

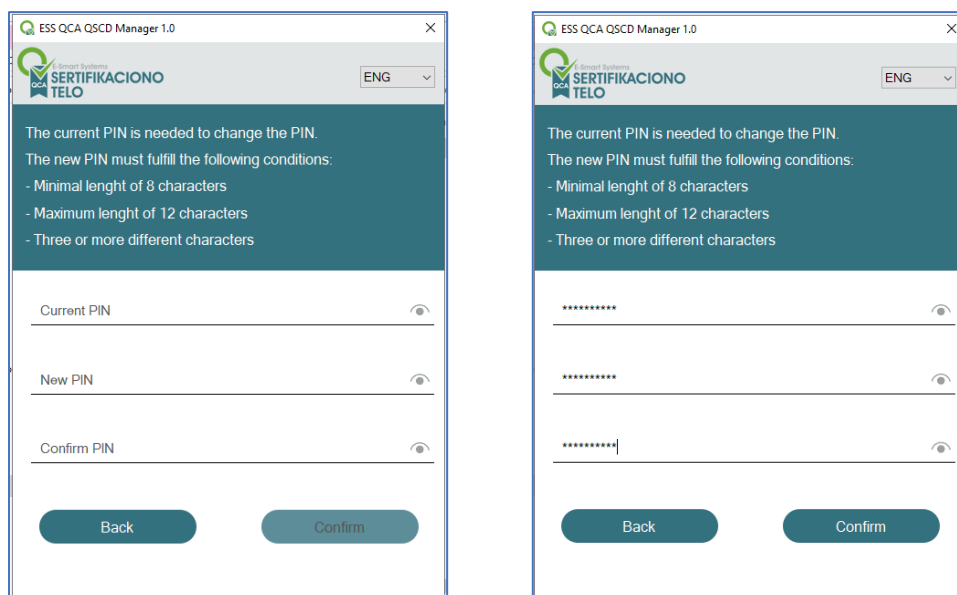


The application is in active mode only when it finds **ONE** personalized QSCD device with an **ESS QCA** qualified certificate.

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).

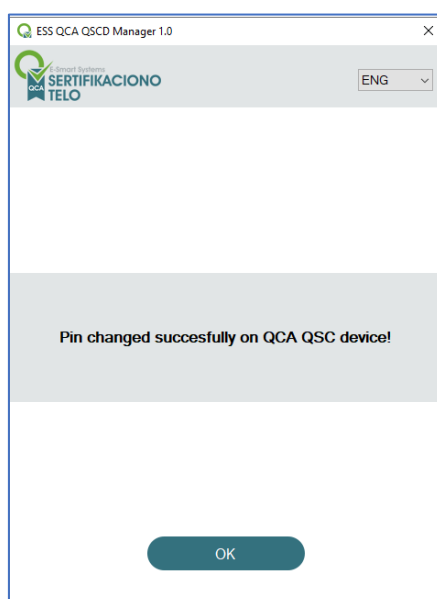


By clicking a button **Change PIN**, a window for changing the PIN opens, where you need to fill in the empty fields, namely: **Current PIN** (if you haven't changed it before, then it's the PIN found in the PIN envelope you received with the QSCD device), **New PIN** and once again it is necessary in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



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.



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.

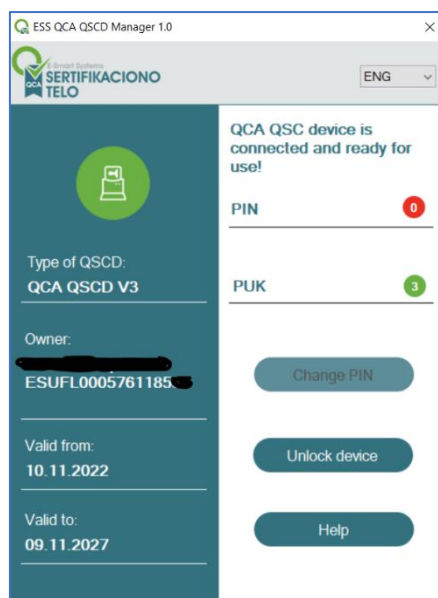
PIN unlocking on **QCA QSCD V3** type devices can also be done via the application - **QCA QSCD Manager**, and the description of this procedure can be found in the rest of this document.

6.2. PIN unlocking

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

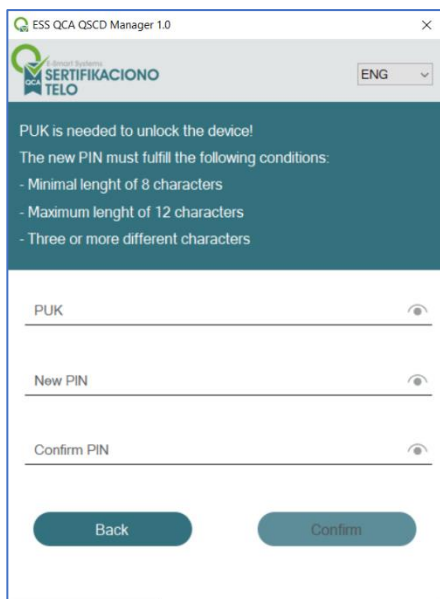
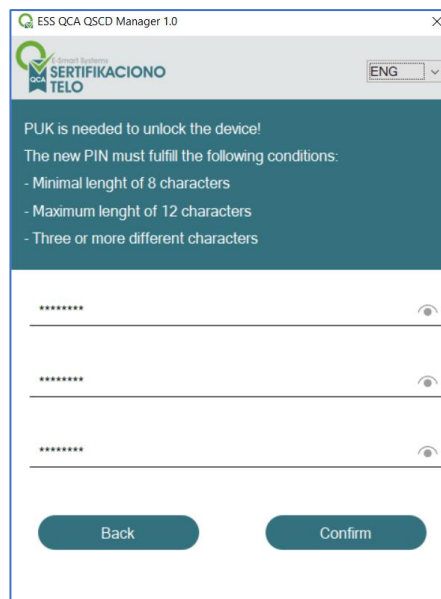
It is necessary to have with you the blocked device, as well as the PIN envelope that came with the device, which, in addition to the PIN, also contains the PUK code used to unblock/unlock this type of device.

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.

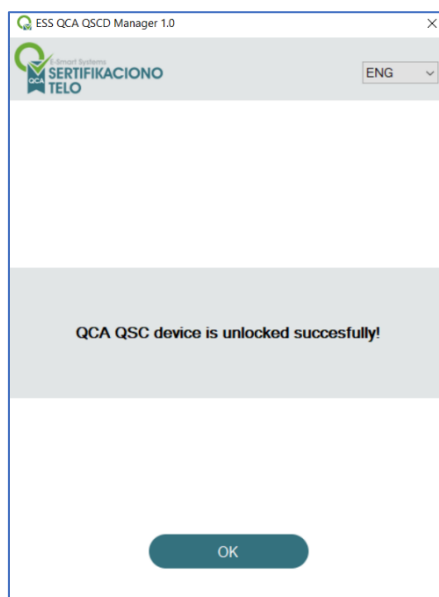


The application will automatically display the type of connected device and data from the Subject of the certificate, the remaining number of PIN entry attempts, which in this case is 0 (zero), as well as the remaining number of PUK entry attempts.

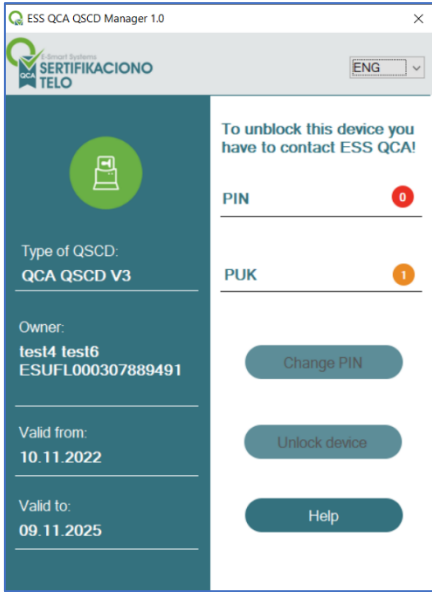
Clicking the **Unlock device** button opens the PIN unlock window. It is necessary to fill in the empty fields, first of all the PUK code found in the PIN envelope that you received with the device, then the New PIN and **Confirm PIN** fields. In each field you fill in, there is also an option to view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

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.



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

ENG

To unblock this device you have to contact ESS QCA!

PIN 0

PUK 1

Change PIN

Unlock device

Help

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.