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-305

Document code

Instructions for installing and using the ESS QCA qualified certificate for electronic seals

Table of Contents

1. Terms & Conditions for using the ESS QCA qualified certificate for electronic seals

Instructions presented in this document are intended for use with qualified certificates for electronic seals on the Microsoft Windows OS. If you intend to use the qualified certificate on Mac or Linux operating systems, please, send us a ticket using the web form or write us an e-mail at qca@esshitsupport.zohodesk.eu and we shall contact you at the earliest convenience.

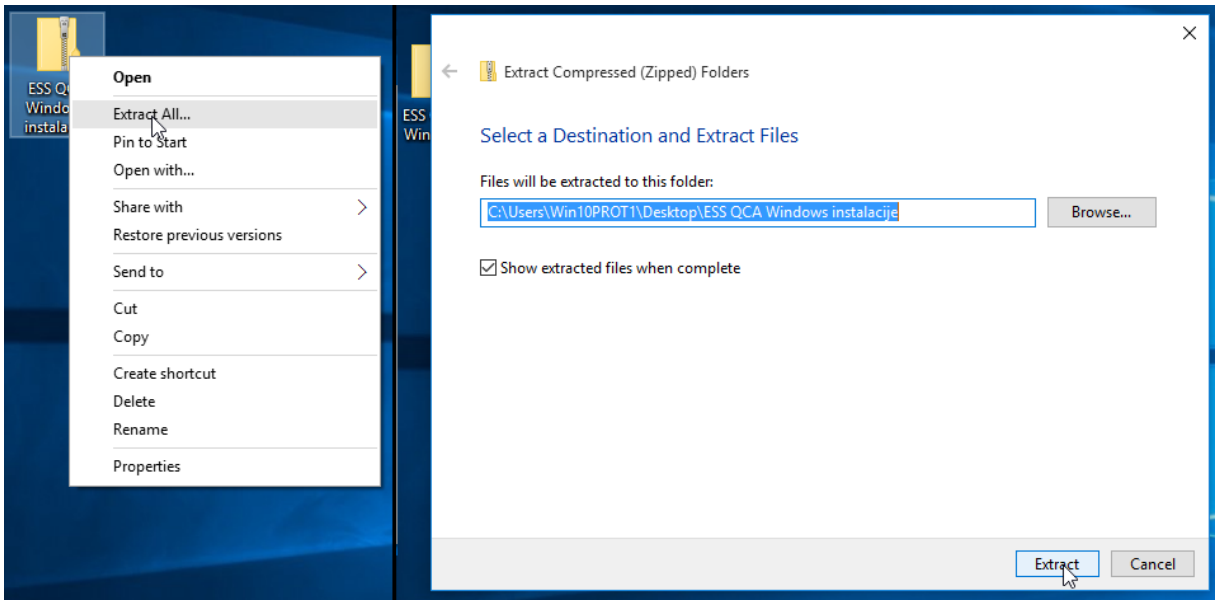
For successful usage of the ESS QCA qualified certificate it is necessary to have the ESS QCA "chain of trust" installed (The root and issuer certificate of the ESS QCA certificate authority), the Thales SafeNet Minidriver with PKCS#11 middleware and a driver for reading smart cards or USB tokens (usually automatically detected by Windows).

2. Downloading the ESS QCA Installation package for Windows

The installation package with all necessary components can be download from the ESS QCA website - https://essqca.e-smartsys.com on the page „Preuzimanje softvera".

Before use extract the zip file by doing the following:

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



After this step it is possible to begin installing the necessary software components for using the ESS QCA qualified certificate for electronic seals.

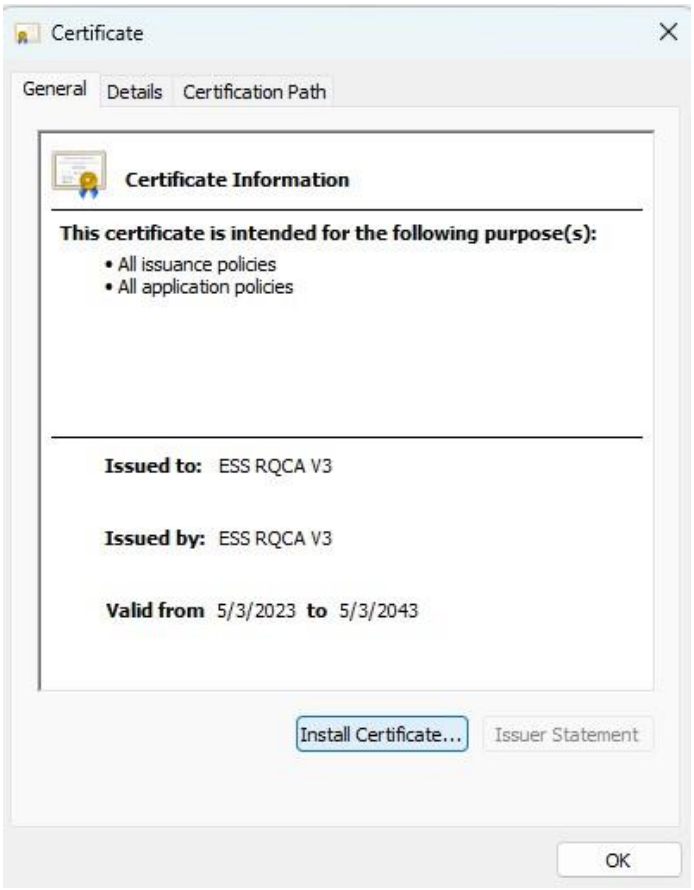
3. Installing the ESS QCA “chain of trust”

The ESS QCA “chain of trust” consists of the CA Root and Issuer certificate located in the “Certificates” installation package. These certificates must be imported in the local computer on the Windows PC so trust could be established between the machine and the certificate user.

3.1. Importing the CA Root certificate

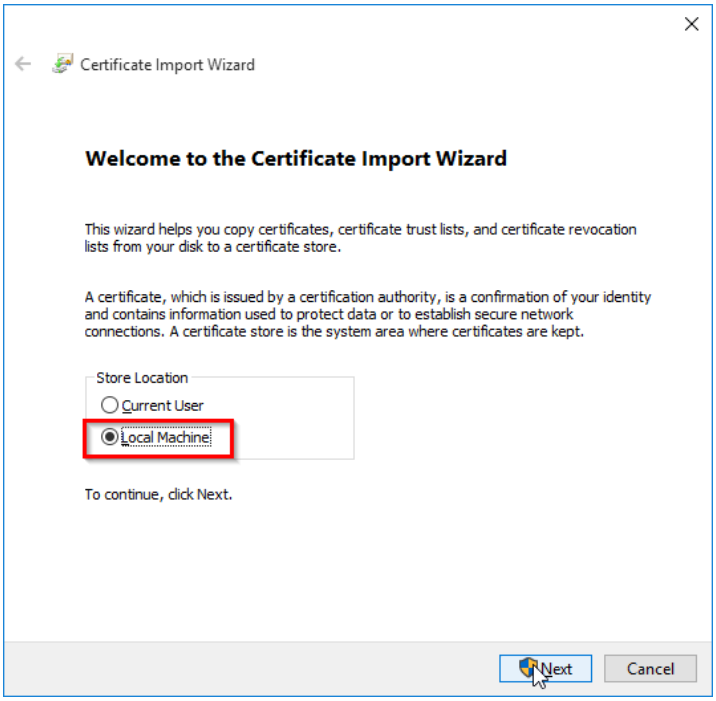
The CA Root (ESS RQCA V3) certificate can be imported in the following way:

1. Double-click the **”ESS RQCA v3.cer”** and the following window will appear.

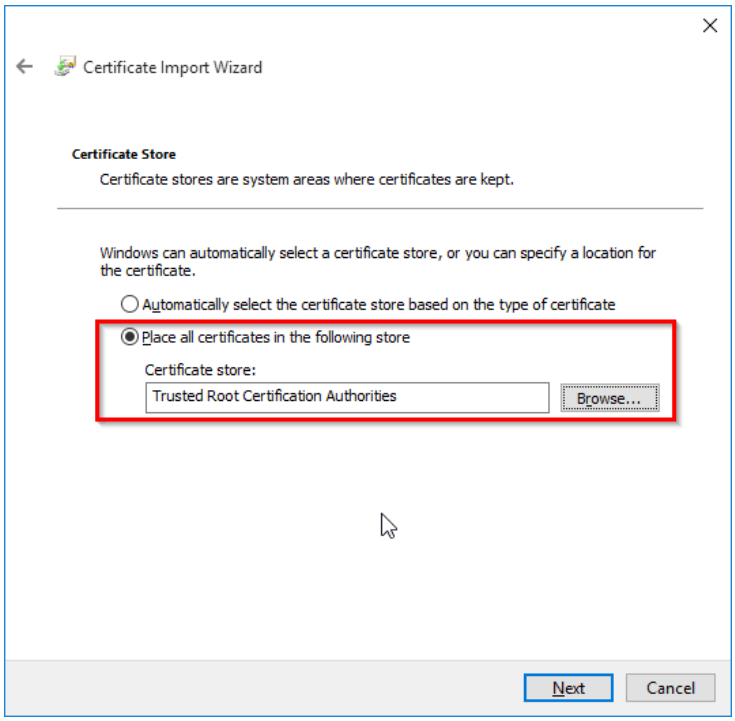


2. By clicking **„Install Certificate...“** we begin the import process.

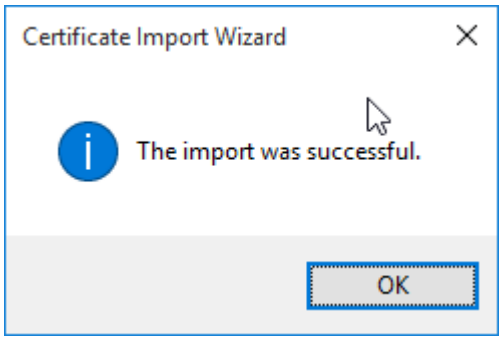
On the following prompt select **„Local Machine“** and press the **„Next“** button.



3. 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**. „Trusted Root Certification Authorities“** should be selected.



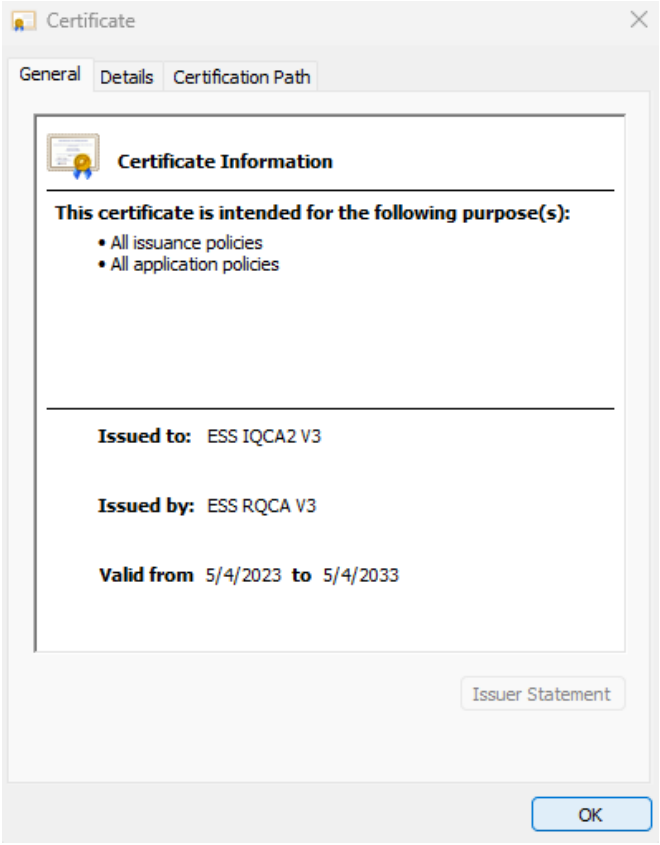
4. Clicking **„Next“**, a final prompt appears and by pressing **„Finish“** the process concludes**.** After that a message will display notifying us that the CA Root certificate has been imported successfully.



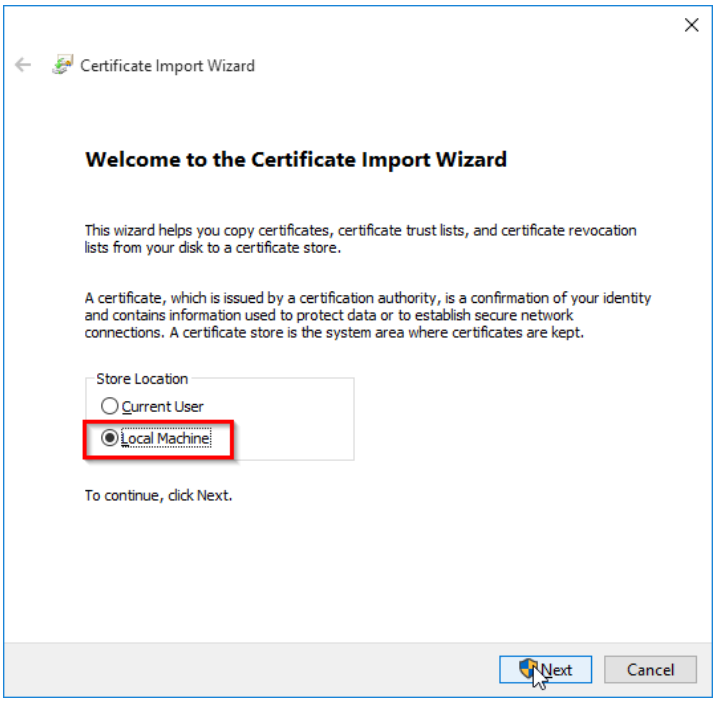
3.2. Importing the CA Issuer certificate

In the “Certificates” folder, more than one CA certificates can be found. To ensure a reliable working environment with the PKI infrastructure, all certificates of the CA should be installed. The names of these certificates start with ESS IQCA1 and can be imported by doing the following:

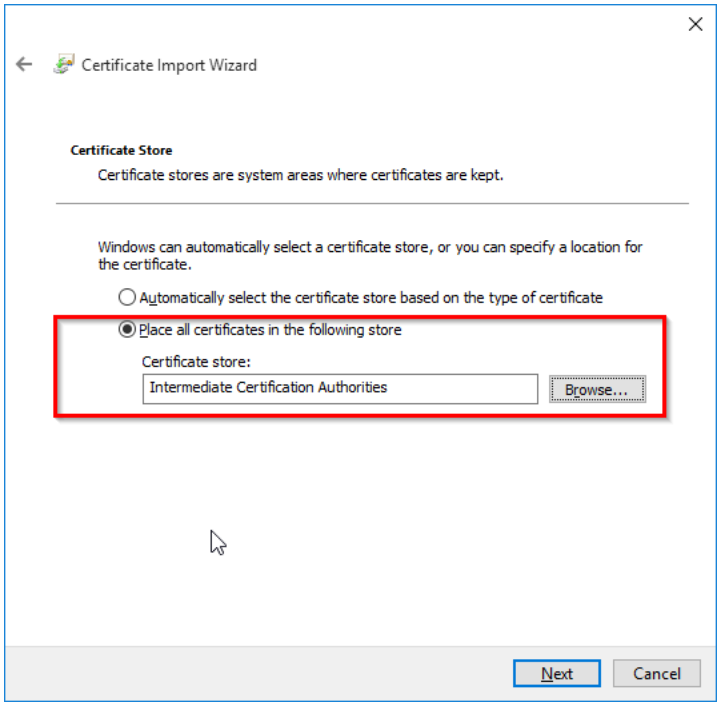
1. Double-click the **„ESS IQCA2 V3.cer“** and the following window will appear.



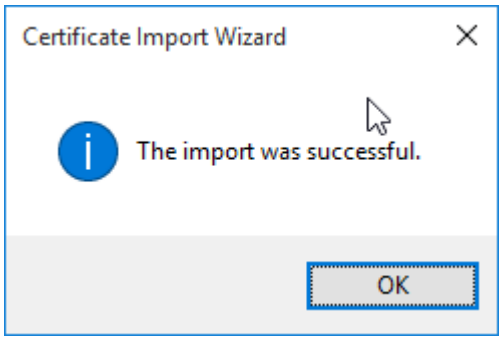
2. The import process begins by clicking **„Install Certificate...“**.
   After that, a window appears where **„Local Machine“** should be selected and after that **„Next**“ should be clicked.



3. 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.



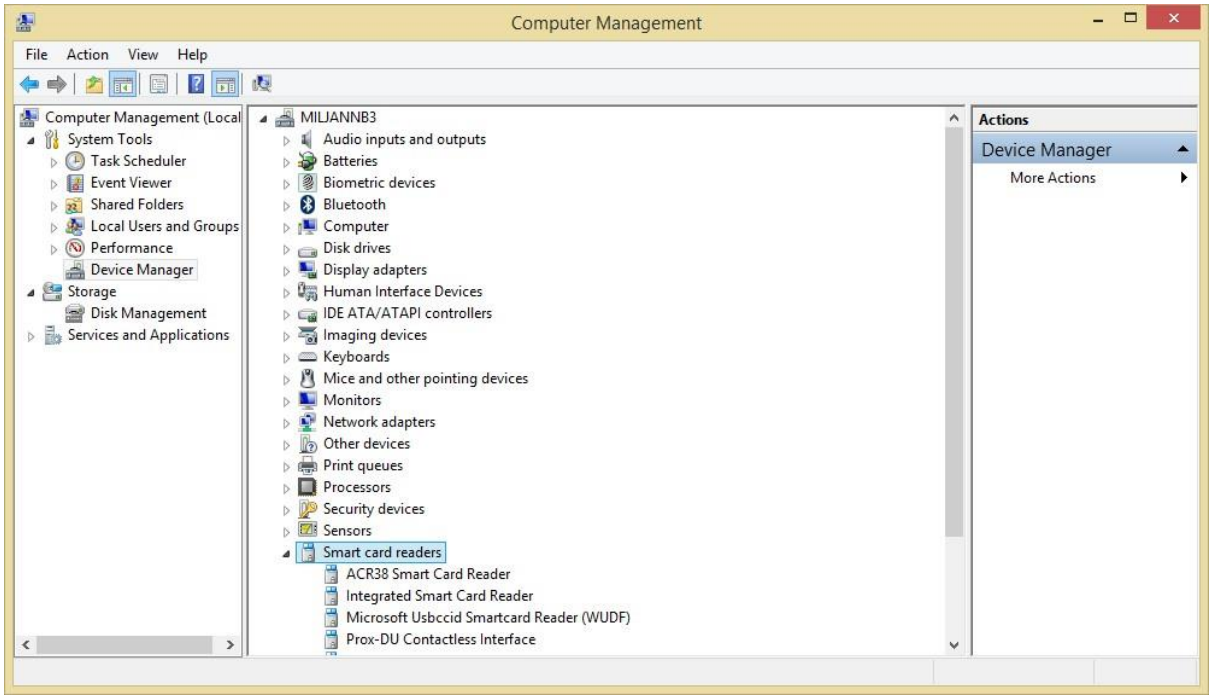
4. Clicking **„Next“**, a final prompt appears and by pressing **„Finish“** the process concludes**.** After that a message will display notifying us that the CA Issuer certificate has been imported successfully.



4. Installing the Smart Card reader drivers

Drivers for smart card readers, which can be purchased alongside the qualified certificates, are usually automatically installed on Windows PCs (10 and 11) when the reader is connected to the PC via USB.

If the installation has been successful, in “Device Manager” under the “Smart card readers” node, the name of the connected reader will appear, as shown in the picture below.



In case of an error during the automatic installation of drivers, the drivers can always be manually installed using the file in the folder “Smart Card Reader Drivers” inside the installation package. Depending on the manufacturer of the smart card reader, appropriate drivers will be located in the folder.

- For ACS smart card readers, the drivers can be found in the “ACS Drivers (ACR39U - ACR39T)” folder,

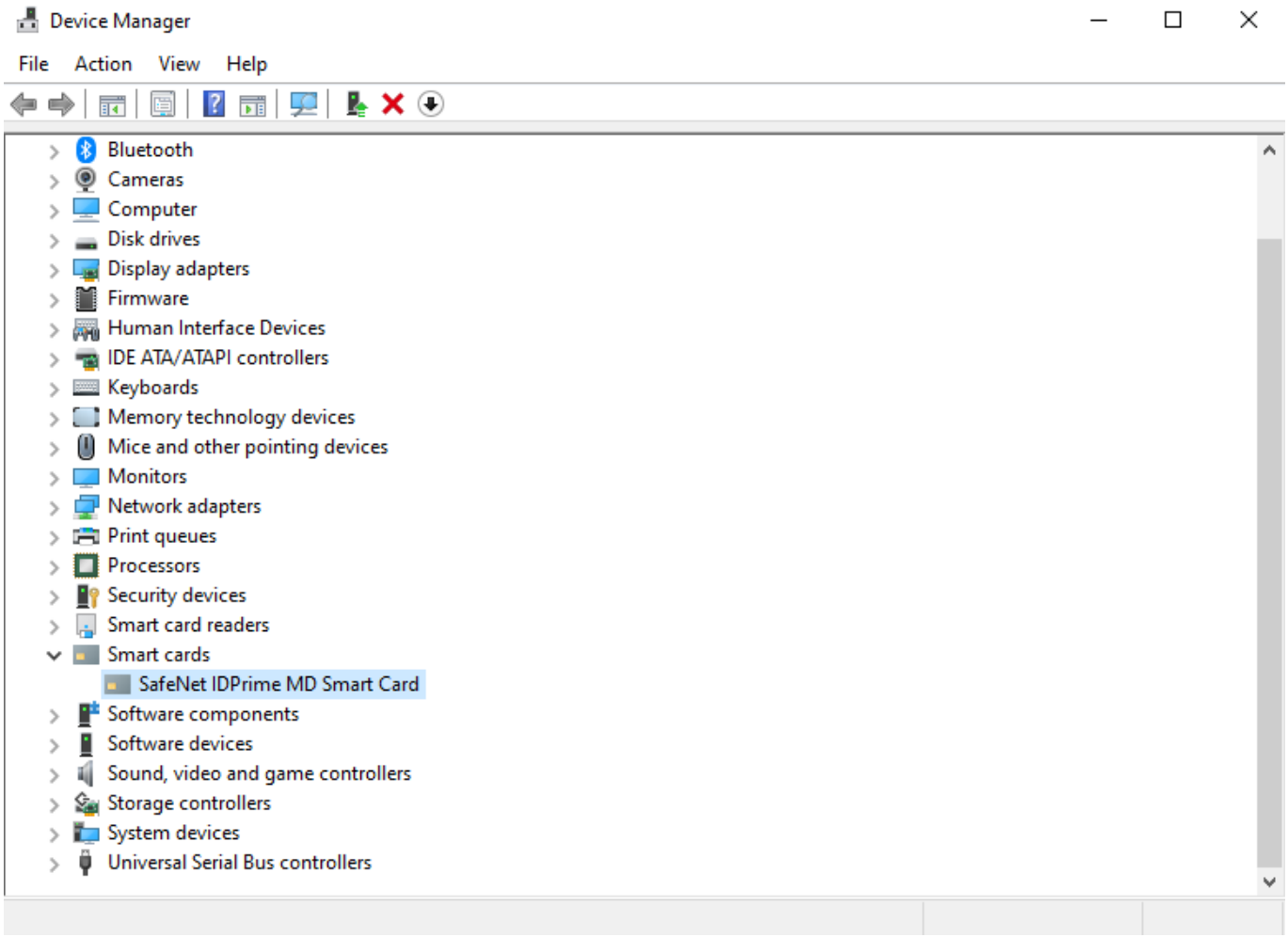
- For Thales/Gemalto smart card readers, the drivers can be found in the “Thales - Gemalto Drivers (CT30-CT40-K50-K30)” folder.

5. Installing the ESS QCA windows software package

In order for Windows (10,11) to recognize the chip on which the qualified certificate for electronic seals is located it is necessary to install the (MiniDriver) driver.

In the folder „**ESS QCA Windows QSCD**“ there is a folder called „**QSCD Minidriver i PKCS11**“ where MSI packages for 32-bit and 64-bit versions of Windows are located. Included in the packages is also the PKCS11 library which is used for signing with third-party apps.

After the successful installation of the MiniDriver, in “Device Manager” under the node “Smart Cards” a card which has been inserted in the USB smart reader will appear.



If any problems arise, please, send us a ticket using the web form or write us an e-mail at qca@esshitsupport.zohodesk.eu and we shall contact you at the earliest convenience.

6. App for changing and deblocking PINs

Depending on the OS version, on the page Preuzimanje i instalacija softvera under "**Korisničke aplikacije"** two versions of the PIN deblocking app can be found:

- for Windows 11 - QCA QSCD Manager W11
- for other OSs (Windows 10) - QCA QSCD Manager

CAUTION: the process of changing and deblocking the PIN is the same regardless of the app version or OS.

Necessary pre-requisites for using the app are .net framework 4.5 (or higher) and the latest version of the Thales Safener Minidriver for IDPrime smart cards (check chapter 5 and 6). If the aforementioned requirements are not met the following window will appear :

6.1. PIN Change

It is recommended to change the initial PIN code received in the PIN envelope after first use. The PIN can be changed at any moment during the life-span of the certificate.

It is necessary to have the QSCD device with the qualified certificate – the smart card (and appropriate reader) or USB token, as well as the PIN envelope where the PIN code is located..

By launching the APP all smart card readers are detected. If you do not have any or if you have more QSCD devices connected, some of the following windows will appear.

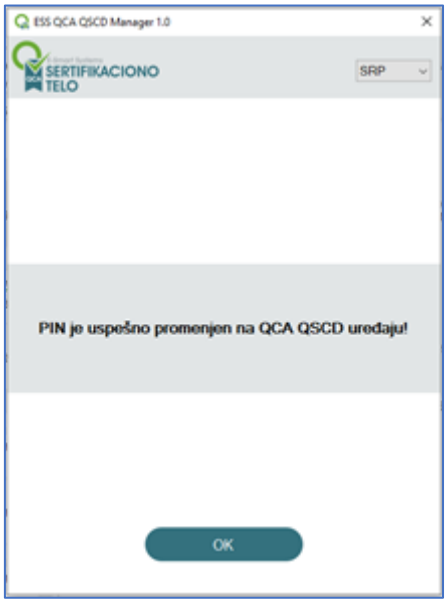
The app goes into active mode only when it detects **ONE** personalized QSCD device with the ESS QCA qualified certificate.

The app will automatically display data about the connected device, data from the Subject of the certificate as well as remaining attempts to enter the PIN and PUK for QSCD V3 devices.

By clicking the **Promeni PIN** button, a window appears where it is necessary to fill in the blanks, so the pin could be changed : **Trenutni PIN** (if you didn't change it before, this is the PIN located inside the PIN envelope which you received alongside the QSCD device), **Novi PIN** the new PIN field **Potvrda PIN-a** confirm the new PIN we just entered.

On every field there is an eye icon on the side which, when pressed, displays the data entered, to ensure no mistakes are made.

If every blank field has been filled accordingly following the instructions, by clicking the Potvrdi button, the PIN of your QSCD device will be adjusted to the new, desired Value. A Message saying„PIN je uspešno promenjen na QCA QSCD uređaju!“ will appear.



If all current PIN input attempts have been used up unsuccessfully, the QSCD device will be blocked.

Deblocking/unlocking all types of devices can be done at the ESS QCA. It is necessary to submit a deblocking request and get in touch with the ESS QCA support so that the deblocking of the device at the ESS premises with personal presence required, can take place.

Deblocking the PIN on devices type **QCA QSCD V3** can also be done by using the app – **QCA QSCD Manager**, described below.

6.2. Deblocking the PIN

NOTICE: only devices type **QCA QSCD V3** can be deblocked using the **QCA QSCD Manager** app.

It is necessary to have the blocked device as well as the PIN envelope you received with the device, in which, apart from the PIN, a PUK code is located used for deblocking/unlocking these types of devices.

The app goes into active mode only when it detects **ONE** personalized QSCD device with the **ESS QCA** qualified certificate.

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

Clicking the **Otključaj uređaj** button a window appears where can deblock the PIN. It is necessary to fill in the empty fields, first and foremost the PUK code which can be found in the PIN envelope which you received with the device and the **Novi PIN** i **Potvrda PIN-a fiels (New Pin and Confirm the New Pin).** On every field there is an eye icon on the side which, when pressed, displays the data entered, to ensure no mistakes are made.

If every blank field has been filled accordingly following the instructions, by clicking the Potvrdi button, the PIN of your QSCD device will be adjusted to the new, desired Value. A Message saying „QCA QSCD uređaj je uspešno otključan!“ will appear.

In case you entered the wrong PUK two (2) times during the deblocking process, independently changing the PIN will no longer be possible.

In this case, deblocking/unlocking the device will only be possible by ESS QCA. It is necessary to submit a deblocking request and get in touch with the ESS QCA support so that the deblocking of the device at the ESS premises with personal presence required, can take place. During this time a new PIN envelope with new Pin and Puk values will be issued.

By clicking the button **Pomoć,** contact information of ESS QCA support will be displayed.