Instruction – Certum EV Code Signing

Activation and installation of Certum EV Code Signing on cryptographic card

version 2.7

Certum
by asseco

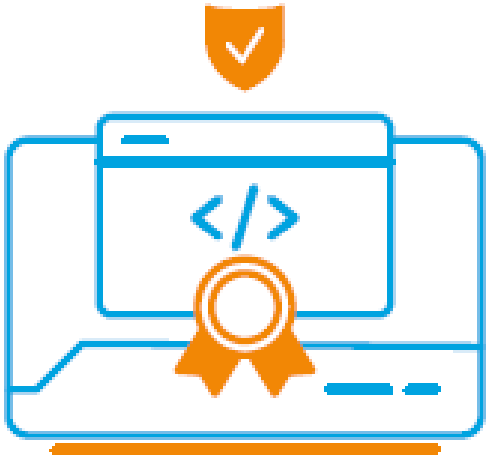


Table of Contents

1. Product description

A Code Signing certificate allows you to digitally sign your applications, drivers and programs, certifying their authenticity and security. This way, users of your software can be confident that it has not been modified, infected or corrupted by third parties.
Authentication of applications with Code Signing eliminates the problem of code anonymity on the network. With a digital signature, you gain confidence that users won't see an "unknown publisher" warning when they install or run your program and reassure them of its security.
Application certification allows you to protect both your users and your brand reputation.
Digitally signing the code makes the use of the application fully secure, which translates into greater trust in your brand and an expanded customer base.

The instruction describes the path of activation and installation of the Standard Code Signing certificate.

2. Software installation

The proCertum CardManager application is required for proper operation of the Code Signing certificate. The latest version of the software can be downloaded HERE.
To properly install the application you need to follow these steps:

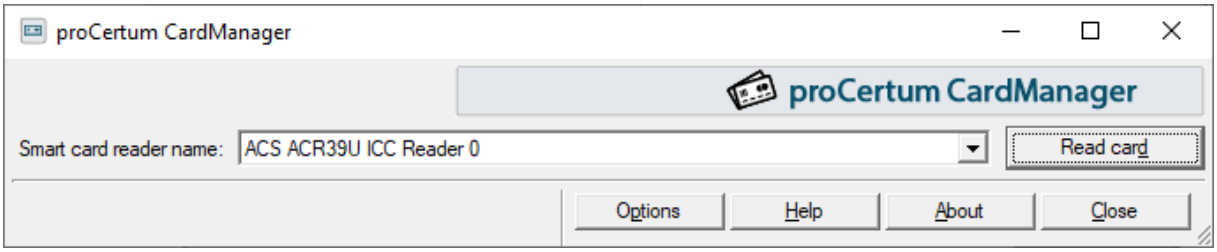
1. Download the latest software version from the official Certum website.
2. Run the downloaded installer.
3. When the installer starts, click Next.
4. When the next screen appears, select I accept the terms of the license agreement and click Next.
5. When the next screen appears, select the path in which to install the application.
6. In the next step click on the button Install.
7. At the end of the installation, restart your computer by selecting Yes, I want to restart my computer now.

Note
If the drivers do not install automatically after connecting the card reader, download them from the manufacturer's website HERE.

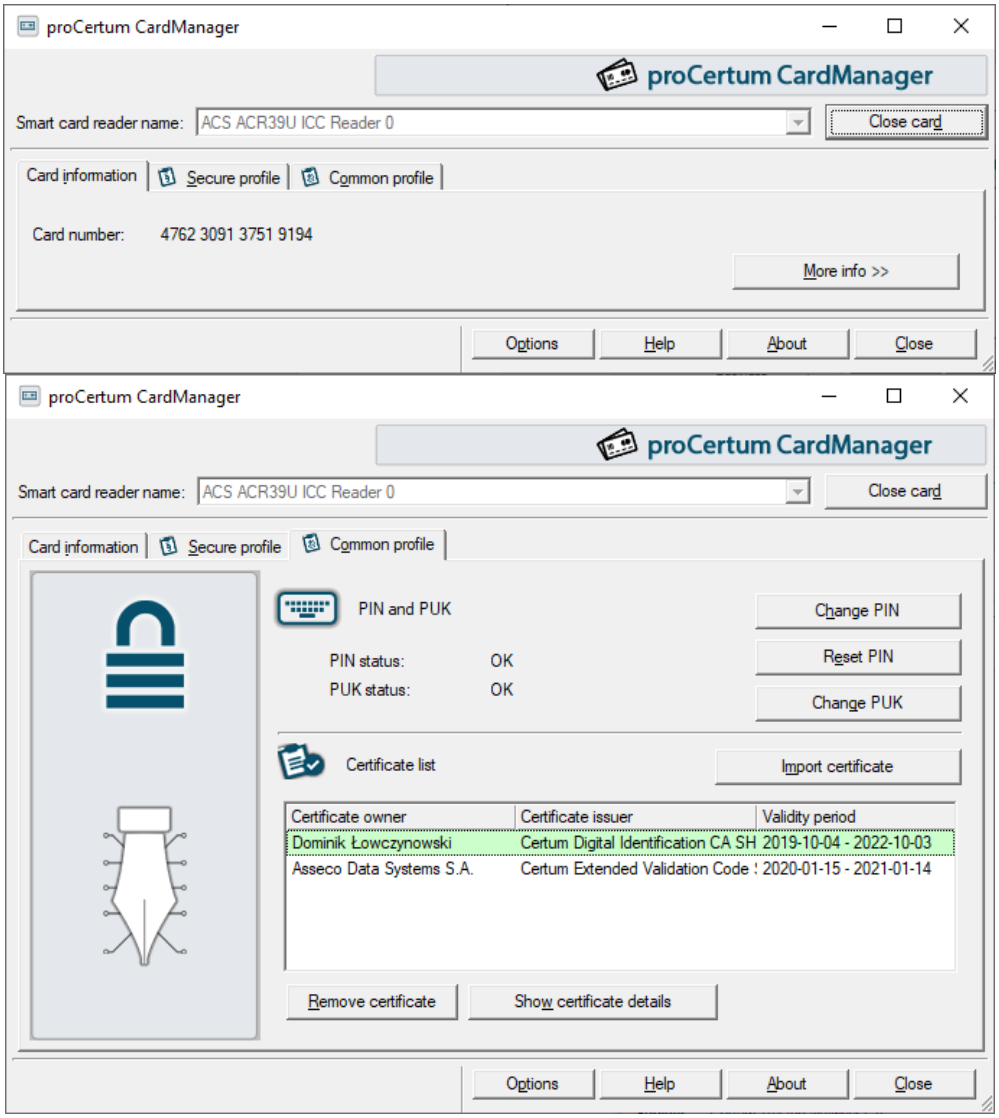
3. Necessary elements before activation and installation of a Code Signing certificate on a cryptographic card

To upload a Code Signing certificate onto a cryptographic card, follow the instructions below:

1. Start the proCertum CardManager software (the current version of the software is available HERE.)
2. If the card has been successfully read the following window should appear:



3. Go to the Common profile tab.
4. Check if the common profile is **active** - the software will display information about the selected profile and a list of certificates. If it is not active, go to section 5. The profile is active if the **PIN and PUK** code status is OK.



5. If the common profile is not **active**, press the Initialize profile button.

A processor card is always delivered with a “non-initialized” common profile, i.e. the PUK and PIN codes have not yet been assigned to it. To activate your profile, press the Initialize profile button.

The next step is to define a new PUK and a new PIN. The user will be asked to confirm the number entered. To confirm the changes, press the OK button. Once the profile is initialized, it is ready for use.

After assigning the PIN and PUK codes, the user may proceed to certificate activation.

NOTE
PIN and PUK codes are assigned by the user, in case of loss of the codes or their blocking the access to the service will be impossible. . In this situation, you must purchase a new cryptographic card and perform the reissue process.
To purchase a new card, go to the website: https://sklep.certum.pl/zestaw-cryptocertum-mini.html and select the variant without a reader.

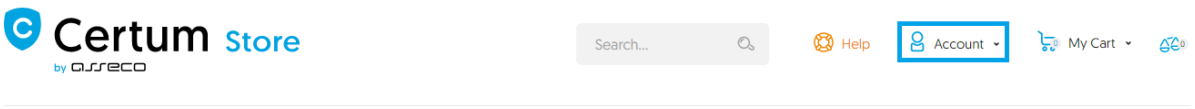
4. Product activation

The guide is prepared using the example of Google Chrome browser and concerns the process of activating the certificate.

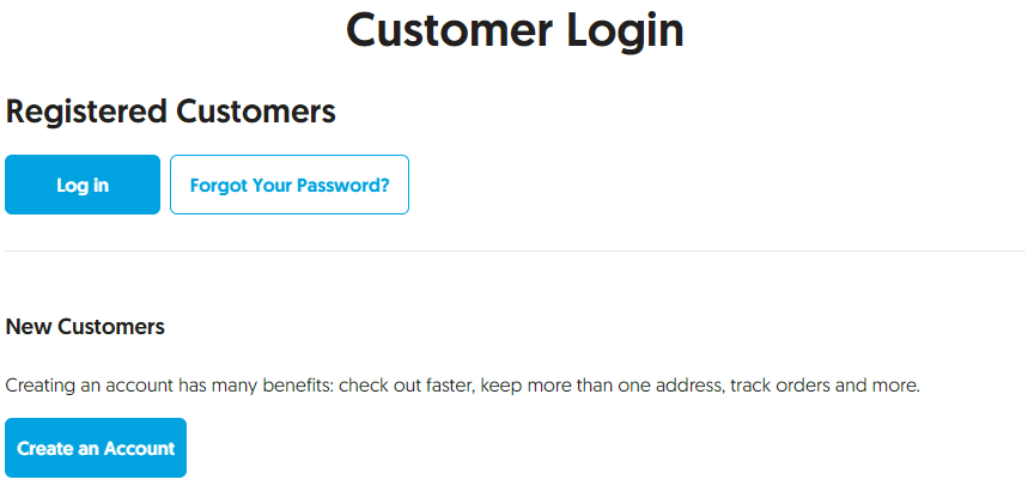
After placing an order in the Certum shop, activation will be available in the Activate Certificates tab (see section 4.2).

4.1. Adding the activation code

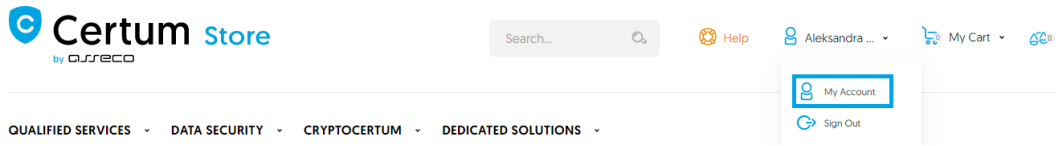
If you want to activate the product from an electronic code received e.g. on your e-mail address - before you begin the activation, add the code in the Electronic Codes tab. To do so, log in to your account on https://shop.certum.eu



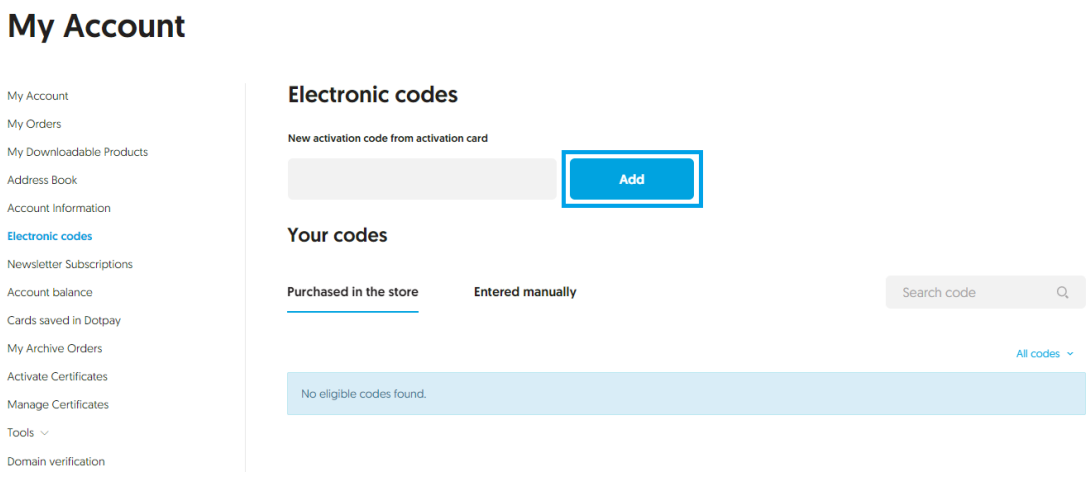
In case you do not have an account, click on the Create an Account button to create one. If you already have an account, select Log in.



After logging in, click on the customer panel - Your Account.



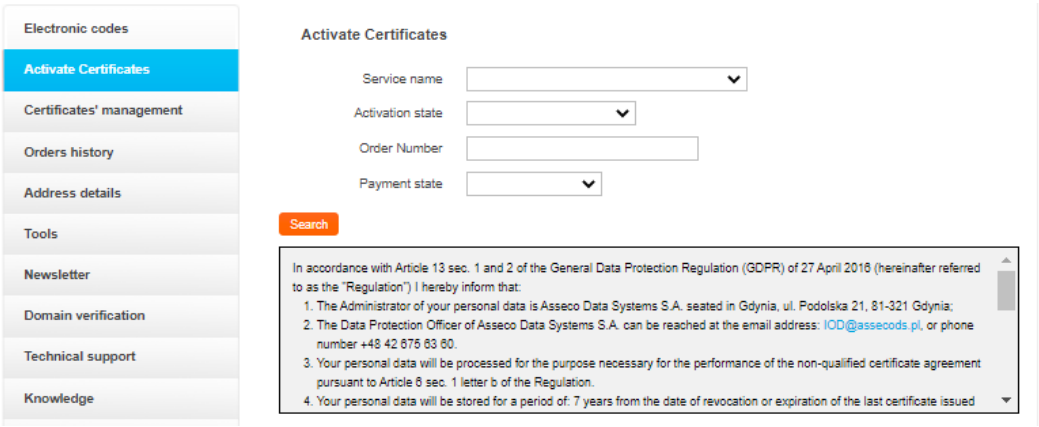
To add a code select the Electronic Codes tab. Enter the code in the Electronic code field and click Add button.
Note! Remember that the activation code consists of 16 characters. After entering or copying the code make sure that the number of characters is correct.



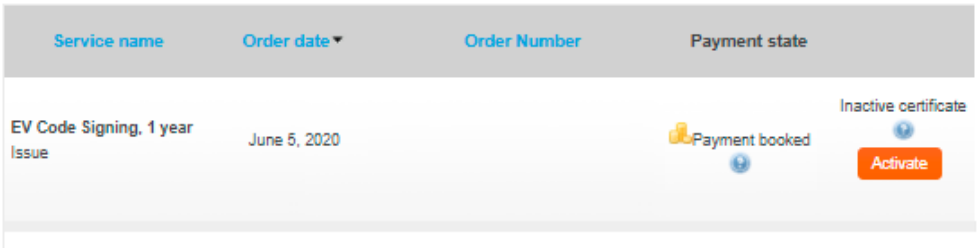
If you enter the code correctly, the product will appear on the list in the Your codes/Entered manually section. After processing the code, go to the Activate Certificates tab (see next point 4.2).

4.2. Start of certificate activation

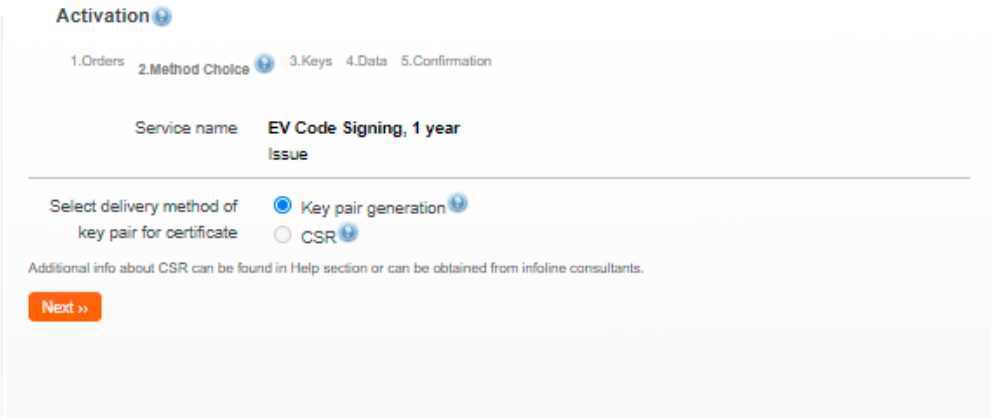
After placing an order or adding a code to your account, start activation in the Activate Certificates tab.



Find the correct certificate in the list and click Activate.

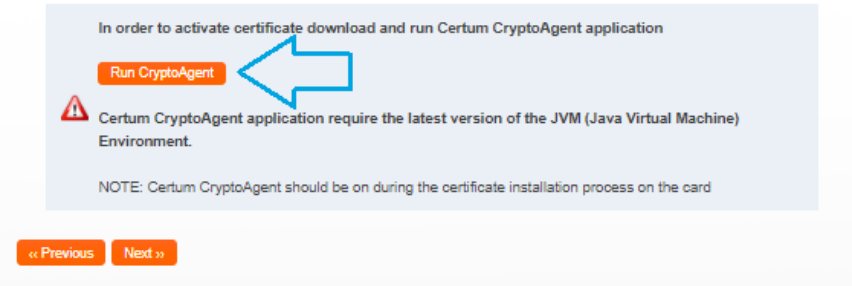


To generate a Sandard Code Signing certificate, select the Key Pair Generation method and click Next.



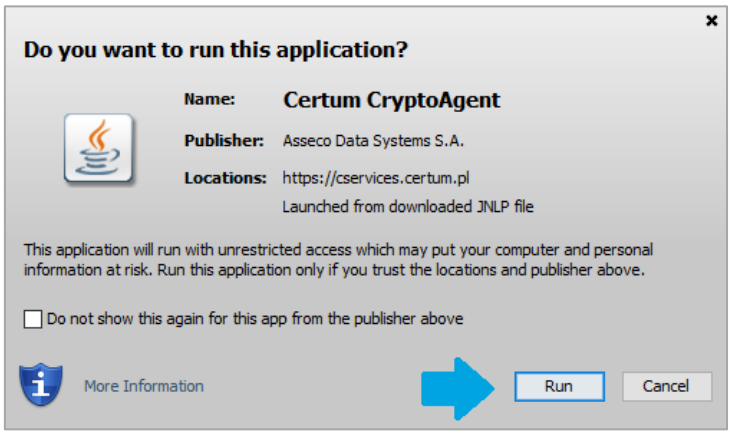
4.2.1.Key pair generation

In order to generate the keys, download and run the Certum CryptoAgent app (to run the app you need a Java environment installed on your computer https://www.java.com/).

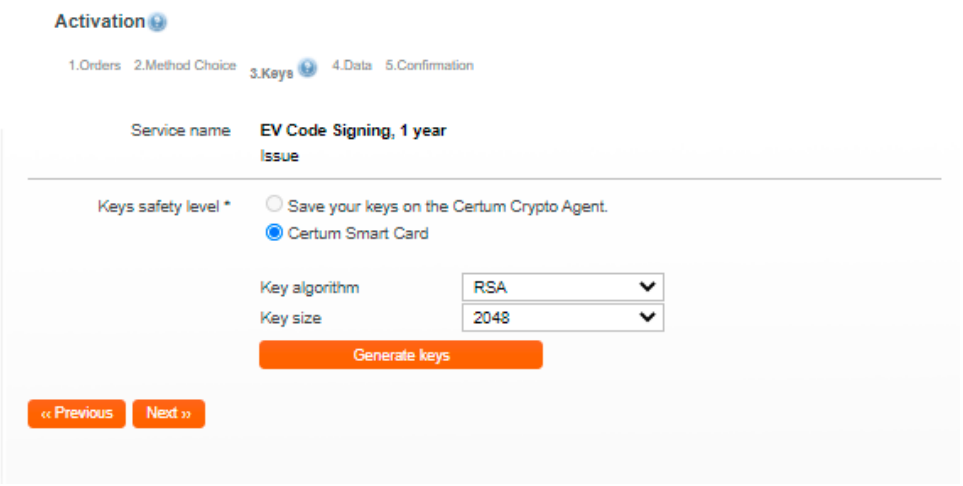


After clicking on the Run CryptoAgent Application button, a warning communicate will be displayed in the bottom bar of the browser, where you can click Save and run the downloaded Certum application.

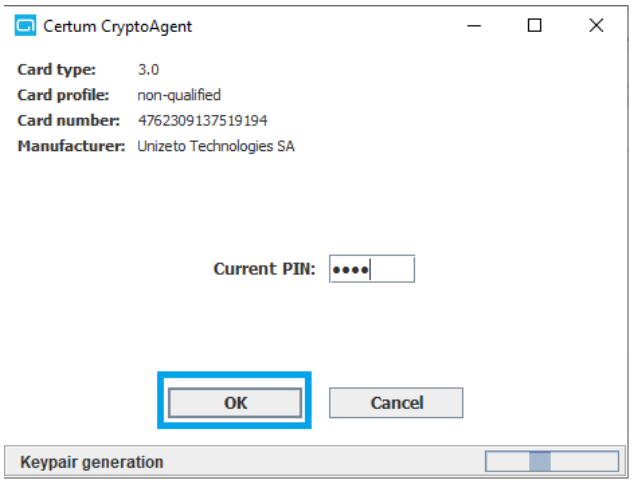
When the Certum CryptoAgent window appears, start the application by clicking Run.



After a short while, the application will run in the background and during the activation process there will be a possibility to save the keys on the Certum card. The default settings, i.e. **RSA key algorithm** and **2048 key length** are correct for the certificate operation.



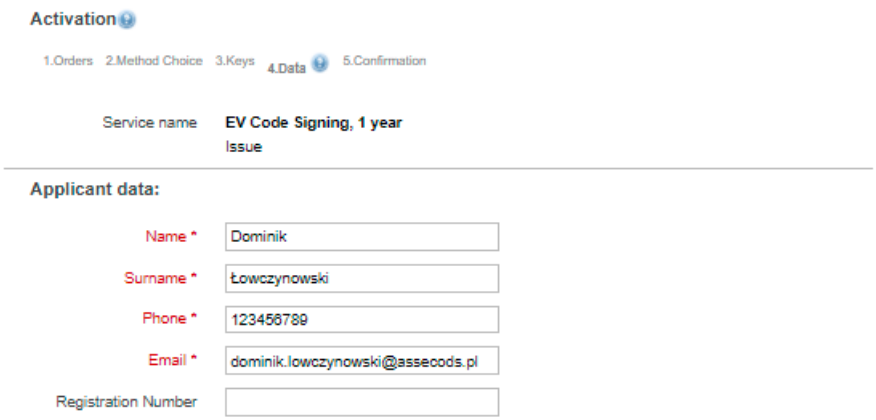
When you click on the Generate Keys button a window will be displayed, where you enter your previously assigned **PIN** code into the **Standard Profile** and confirm it with OK.



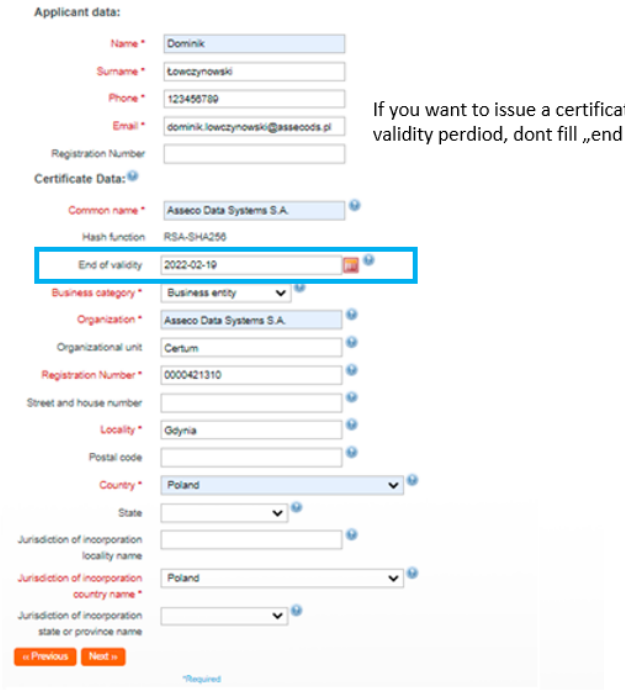
After receiving a communicate that the certificate keys have been generated. Click on the Next button to proceed to the next activation stage.

4.2.2.Filling in the form during activation

The next step is to complete the certification application form with the data that will be contained in the certificate. Please note that the fields with an asterisk * are required.

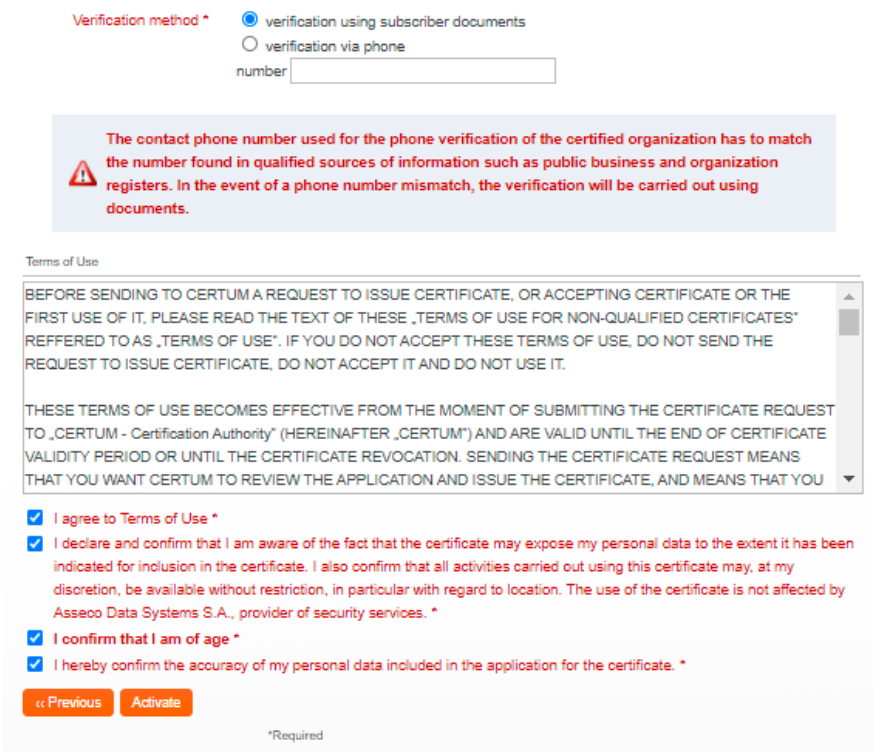


Then enter the data into the Certificate.



If you want to issue a certificate for maximum validity perdiod, dont fill „end of validity" field

In the last step (Summary), verify that the data is correct. Tick the required consents and confirmations and click Activate.



5. Verification

Depending on which verification method you have chosen, you will receive an email with verification instructions.

5.1. Document-based verification

Issuance of the Standard Code Signing certificate requires verification of the Subscriber and Organization identity. For this purpose, the person requesting the certificate should provide Certum with the following documents

- confirmation of identity at a Registration Desk or Identity Confirmation Point (details: https://shop.certum.eu/certum-reseller-points-map) or
- notary confirmation of identity
  or for faster issuance
- a copy of an identity document of the ordering person (ID card, passport, driver's license, permanent residence card). The copy should be a complete copy of the document (both sides).

Identity can also be confirmed with a valid qualified certificate issued for the Subscriber by Certum.

and

1. A bill issued to the certified organization (gas, electricity, water, telephone, etc.)
2. power of attorney or authorization confirming the relationship of the person ordering the certificate with the organization - when the ordering party is not listed in the relevant register as a person authorized to represent the company,
3. company registration document - when the company is not listed in the KRS/GUS/CEiDG register

In justified cases, Certum may ask you to send additional documents necessary for proper verification.

Please send all the documents collected to Certum in one of the following ways:

- by e-mail as a password-protected file to the address: ccp@certum.pl (recommended form),

In order to determine how to transfer your password, please contact the Certum technical support line

- by fax to: +48 91 4257 422
- by post to:

Certum
ul. Bajeczna 13
71-838 Szczecin

5.2. Verification with AriadNEXT

The entire process is performed using a computer or other device with access to a camera, from a maintenance-free interface. During scanning, the document Data are automatically extracted and analyzed as well as compared to the Owner's face. The process is based on comparison of a facial image with a photo extracted from an identity document. The biometric solution ensures that the User is present during the identity confirmation. The entire process is live, in real time, and does not require sending documents, they are only scanned during the process to extract the data needed for verification and

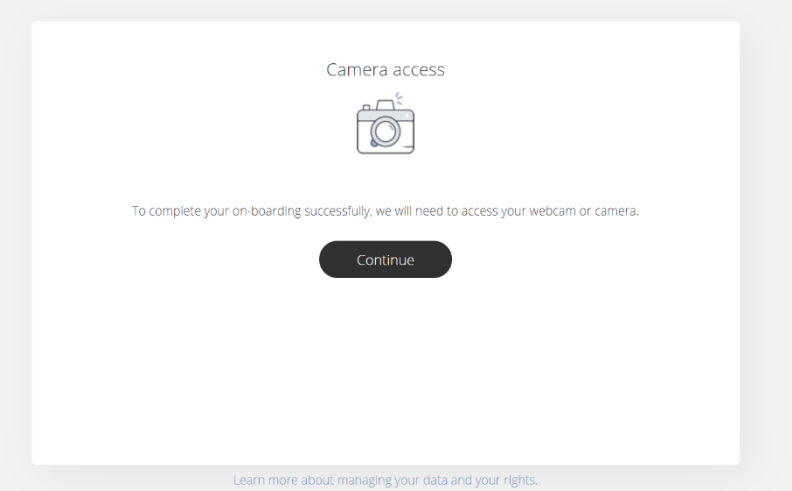
What does the process during certificate activation look like?

- In the certificate activation process, when selecting an identity verification method, select the method: **Automatic identity verification**
- After submitting the application, the User receives a unique link to the indicated email address
- After clicking on the link, the User is taken to the Certum screen on which the Automatic Verification process can be started. The User will then receive a link that initiates verification.
- Depending on the device on which the verification is performed, the process is different.

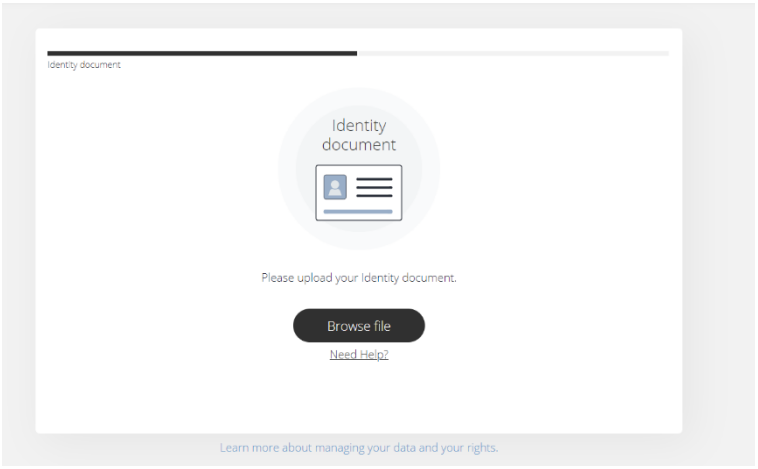
5.2.1.Verification using a computer

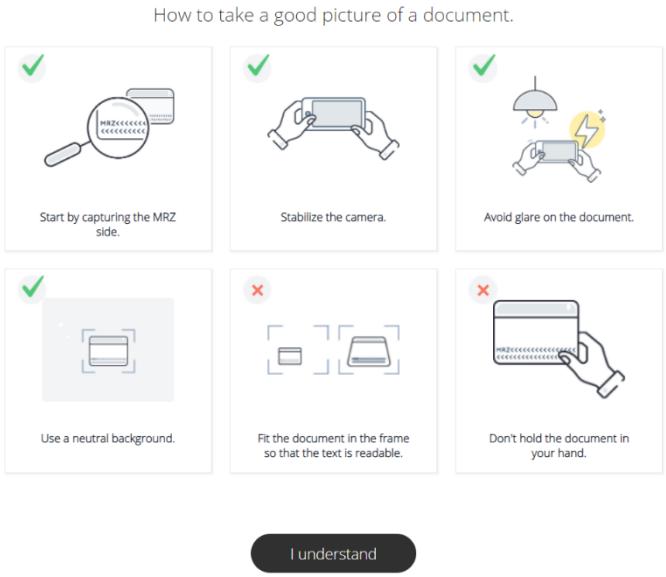
Step 1 — Document verification

After clicking the link to initiate verification, you will be prompted to turn on your camera, so your identity can be verified. Click "Continue" and proceed to the next step.



You will then be asked to upload a photo of your identification document. The photo provided should be taken according to the guidelines provided during the process.

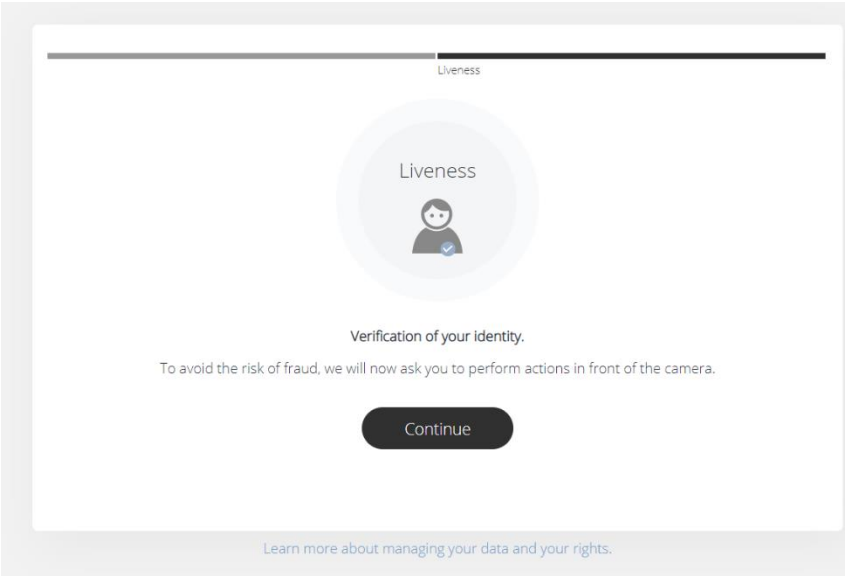




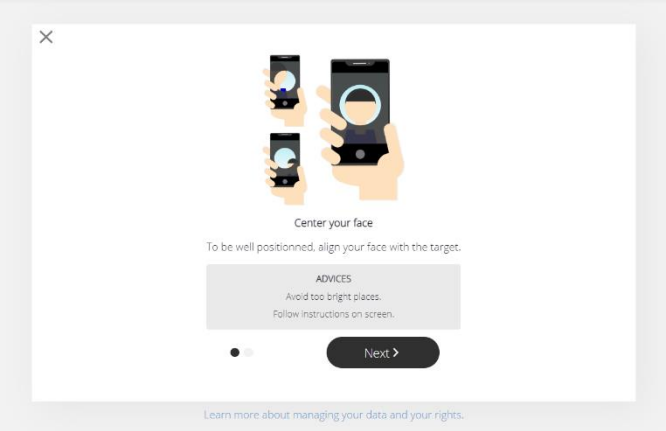
Once the data are submitted, the system will process it for approximately 12 seconds to extract the data from the document. After this process, the document image will be deleted.

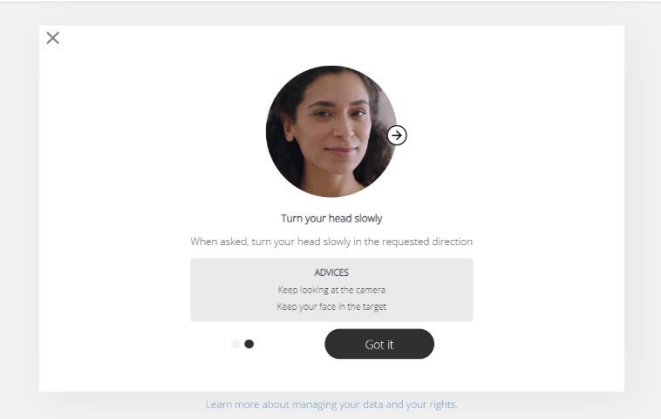
Step 2 — Facial comparison

During this step you will be asked to move your face in front of the camera. This biometric solution will ensure that the User is present during the identity confirmation and is the holder of the document.

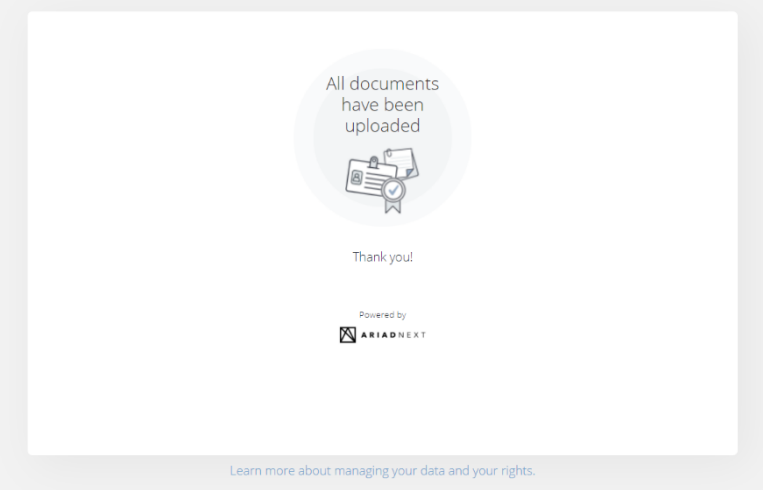


Performing this step requires you to point your face toward the center of the camera and then move your head toward the right side, looking at the camera the entire time.





After completing this step, a screen indicating that the verification was successful will be displayed. Your certificate will be issued shortly.



5.2.2.Mobile phone verification

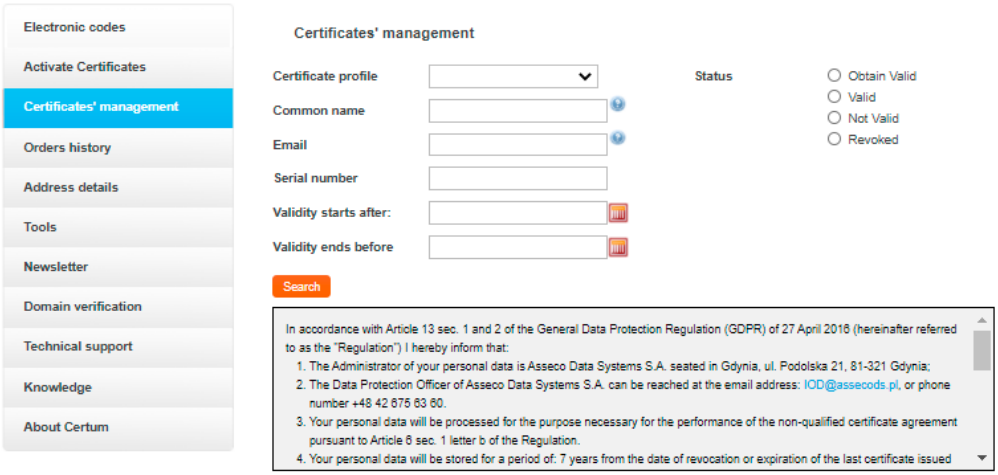
The verification process is similar, but in step one, the user does not provide a pre-made photo but takes one live during the process.

Note: In the case of an order placed by a traditional transfer, it is also necessary to register the payment in order to issue the certificate.

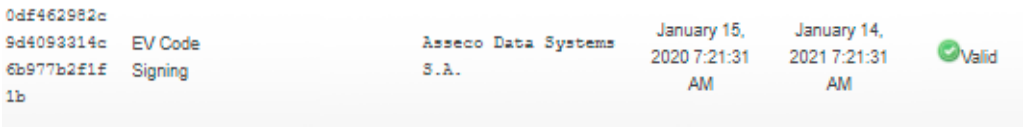
6. Downloading and uploading the certificate on the card

After going through the whole activation process, you need to upload a certificate to the card on which the keys were previously generated. To do this:

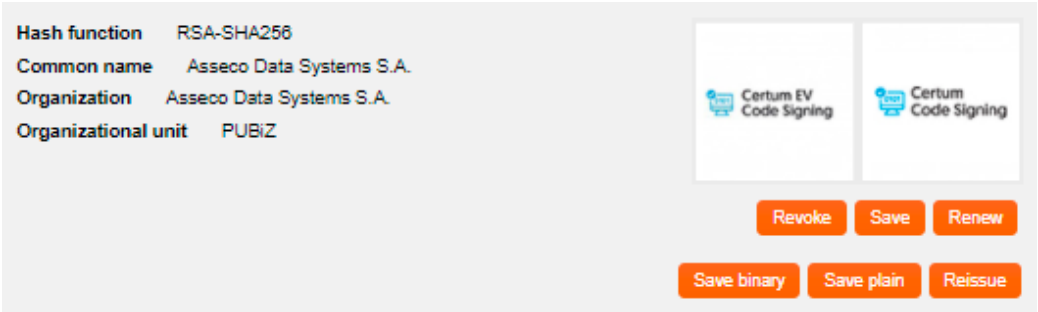
1. In Certum store, go to the Certificate Management tab:



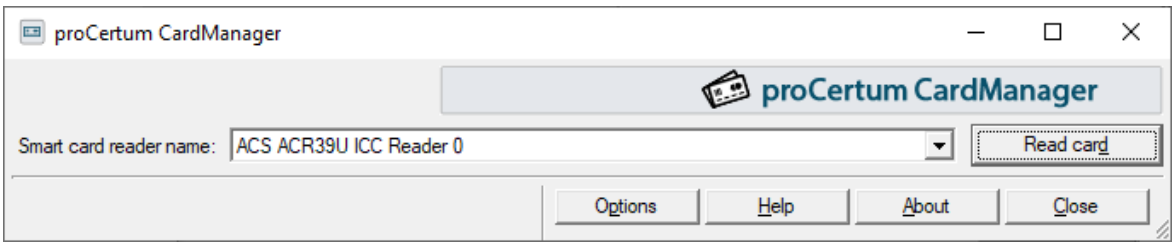
2. Locate the corresponding certificate for which the key pair was generated and click on it:



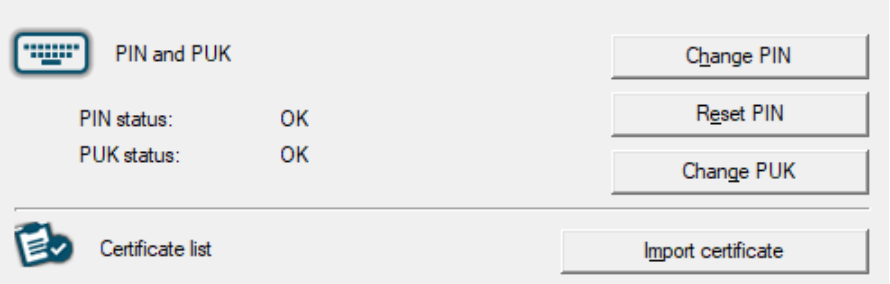
3. Click the Save Binary button:



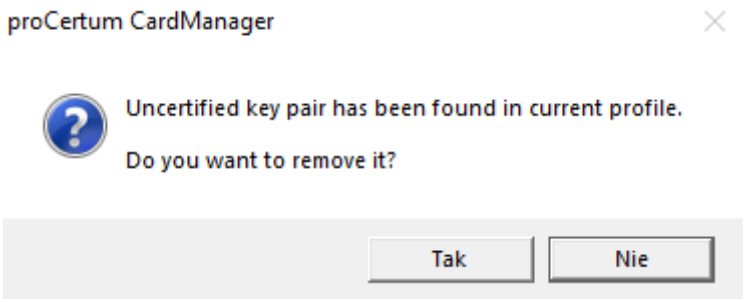
4. Download the certificate file to your computer.
5. Open proCertum CardManager:



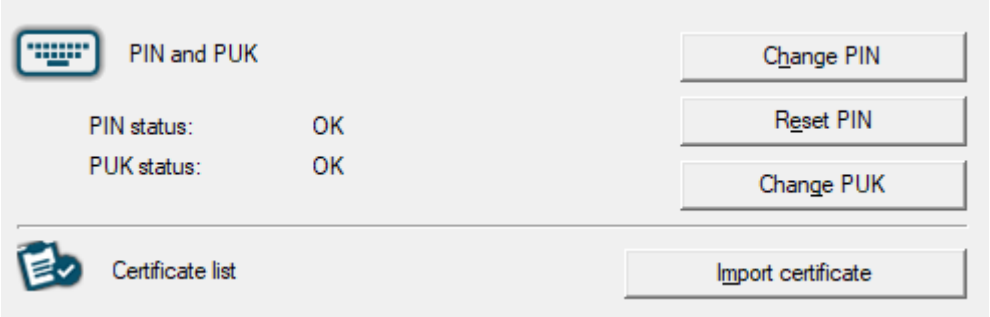
6. Go to the Common profile tab:



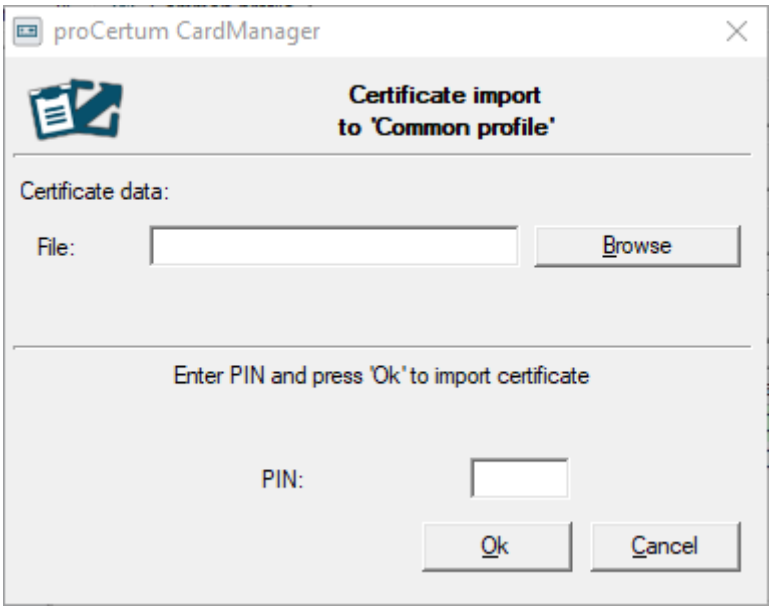
7. If you see a notification about uncertified keys on the card, press No:



8. Click Import Certificate:



9. Select the previously downloaded certificate file, enter the pin to the card (for Common Profile):



10. If the process of adding the certificate was successful, the Code Signing certificate should appear in the list: