



Instruction – Certum EV Code Signing

Activation and installation of Certum EV Code Signing on cryptographic card

version 2.7

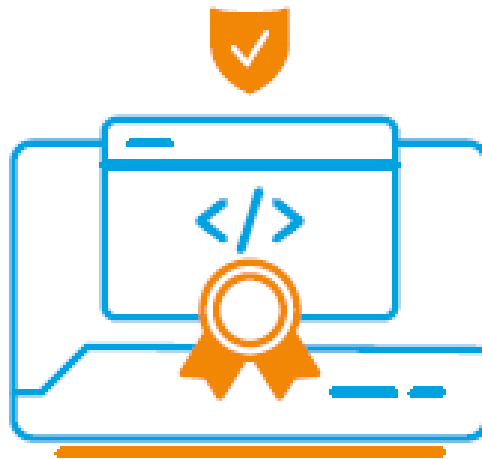


Table of Contents

1. Product description	3
2. Software installation	3
3. Necessary elements before activation and installation of a Code Signing certificate on a cryptographic card.....	3
4. Product activation	4
4.1. Adding the activation code.....	5
4.2. Start of certificate activation.....	6
4.2.1. Key pair generation	7
4.2.2. Filling in the form during activation	9
5. Verification	10
5.1. Document-based verification	10
5.2. Verification with AriadNEXT	11
5.2.1. Verification using a computer	11
5.2.2. Mobile phone verification	13
6. Downloading and uploading the certificate on the card.....	13

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](#).

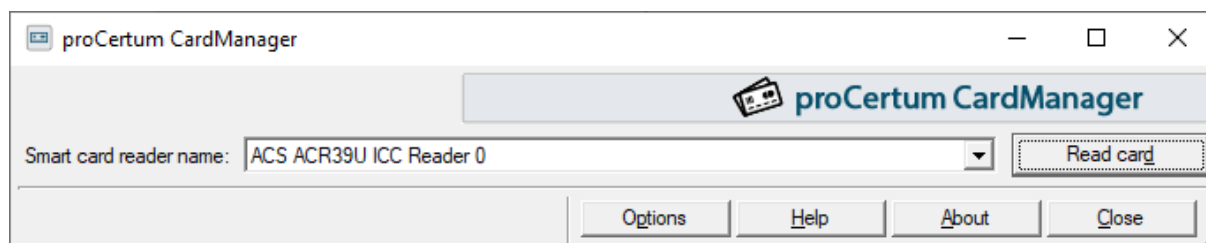
Note

If the drivers do not install automatically after connecting the card reader, download them from the manufacturer's website [HERE](#).

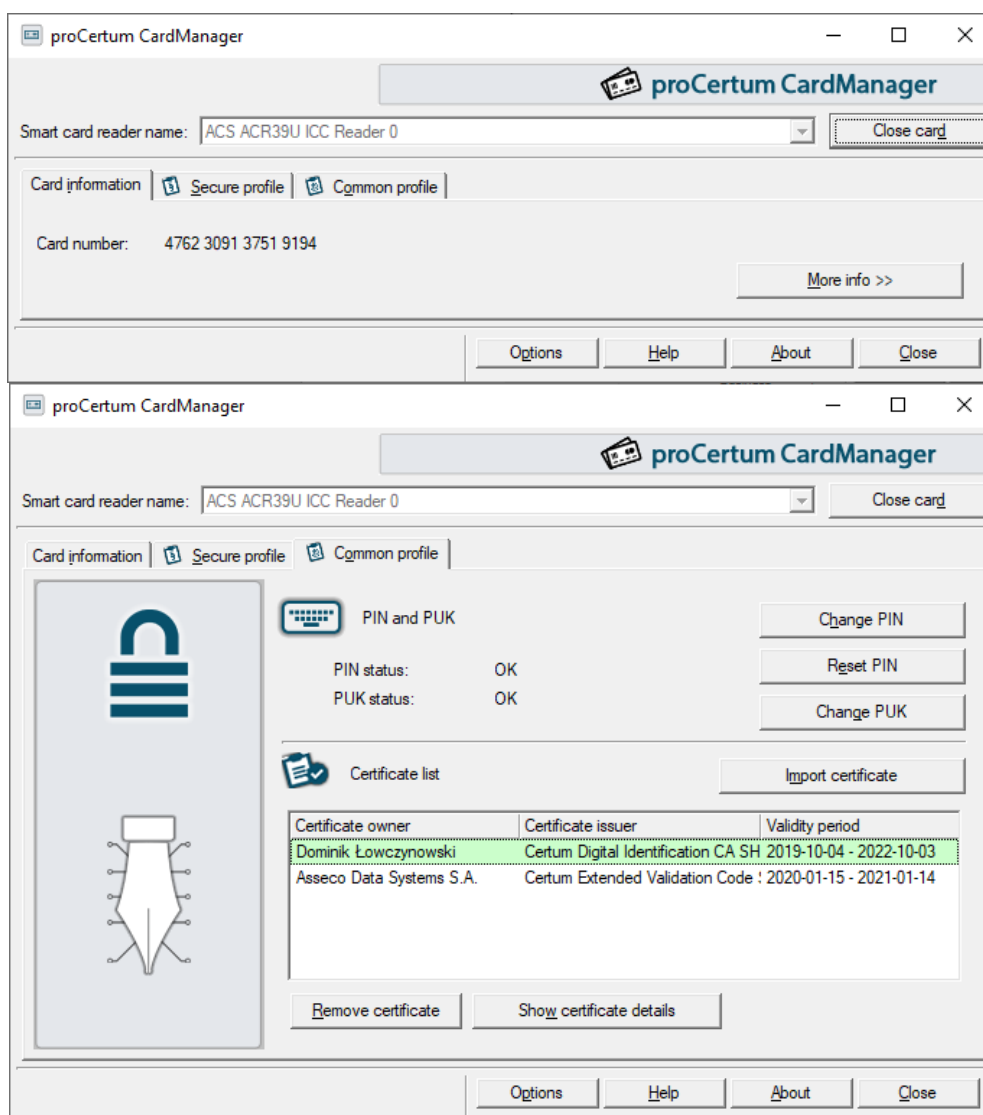
3. Necessary elements before activation and installation of a Code Signing certificate on a cryptographic card

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](#).



- 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.

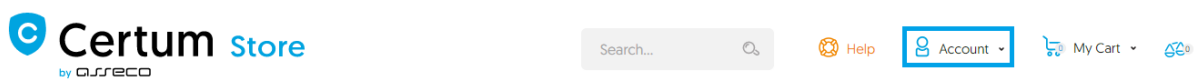
4. Product activation

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](#).

Customer Login

Registered Customers

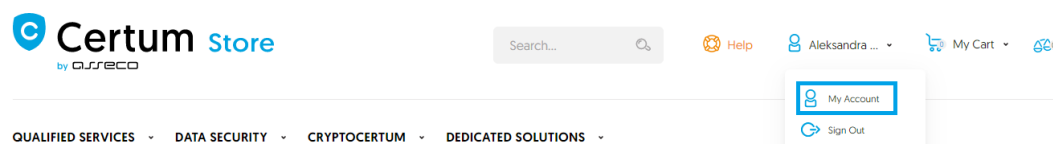


New Customers

Creating an account has many benefits: check out faster, keep more than one address, track orders and more.



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.

My Account

My Account
 My Orders
 My Downloadable Products
 Address Book
 Account Information
Electronic codes
 Newsletter Subscriptions
 Account balance
 Cards saved in Dotpay
 My Archive Orders
 Activate Certificates
 Manage Certificates
 Tools ▾
 Domain verification

Electronic codes

New activation code from activation card

Your codes

Purchased in the store

Entered manually

Search code

All codes ▾

No eligible codes found.

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.

- Electronic codes
- Activate Certificates**
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Domain verification
- Technical support
- Knowledge

Activate Certificates

Service name

Activation state

Order Number

Payment state

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

- The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
- The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: IOD@assecoods.pl, or phone number +48 42 875 63 60.
- Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
- Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued

Find the correct certificate in the list and click [Activate](#).

Service name	Order date ▾	Order Number	Payment state
EV Code Signing, 1 year Issue	June 5, 2020		Inactive certificate Payment booked <input type="button" value="Activate"/>

To generate a Standard Code Signing certificate, select the [Key Pair Generation](#) method and click [Next](#).

Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **EV Code Signing, 1 year Issue**

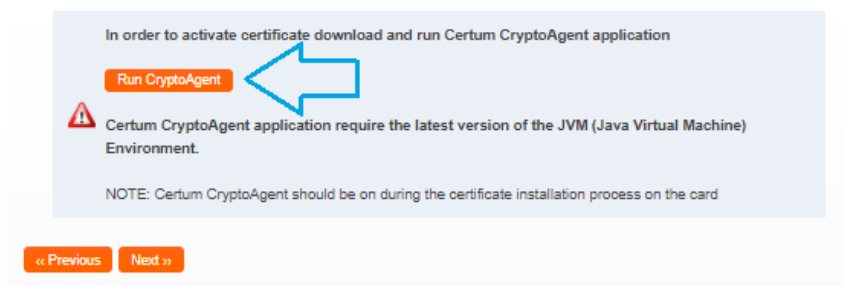
Select delivery method of key pair for certificate Key pair generation CSR

Additional info about CSR can be found in Help section or can be obtained from infoline consultants.

Next >>

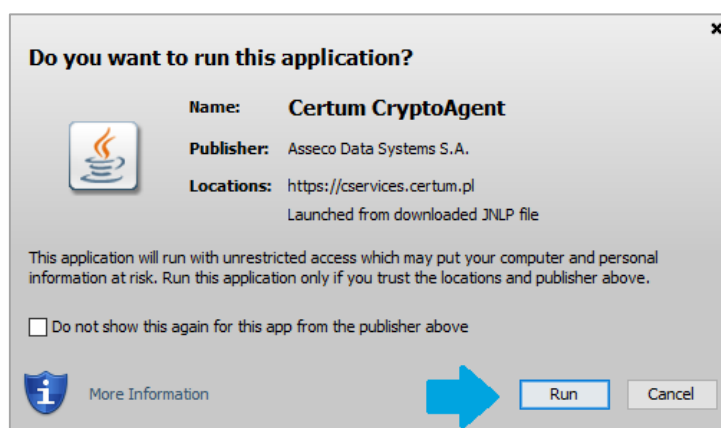
4.2.1.Key pair generation

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.

Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **EV Code Signing, 1 year Issue**

Keys safety level * Save your keys on the Certum Crypto Agent.
 Certum Smart Card

Key algorithm

Key size

Generate keys

<< Previous **Next >>**

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**.

Certum CryptoAgent

Card type: 3.0
Card profile: non-qualified
Card number: 4762309137519194
Manufacturer: Unizeto Technologies SA

Current PIN:

OK **Cancel**

Keypair generation

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

Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **EV Code Signing, 1 year Issue**

Keys safety level * Certificate keys have been generated

<< Previous **Next >>**

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.

Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **EV Code Signing, 1 year Issue**

Applicant data:

Name *

Surname *

Phone *

Email *

Registration Number

Then enter the data into the Certificate.

Applicant data:

Name *

Surname *

Phone *

Email *

Registration Number

Certificate Data:

Common name *

Hash function RSA-SHA256

End of validity

Business category *

Organization *

Organizational unit

Registration Number *

Street and house number

Locality *

Postal code

Country *

State

Jurisdiction of incorporation locality name

Jurisdiction of incorporation country name *

Jurisdiction of incorporation state or province name

*Required

If you want to issue a certificate for maximum validity period, 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](#).

Verification method * verification using subscriber documents
 verification via phone
 number

The contact phone number used for the phone verification of the certified organization has to match the number found in qualified sources of information such as public business and organization registers. In the event of a phone number mismatch, the verification will be carried out using documents.

Terms of Use

BEFORE SENDING TO CERTUM A REQUEST TO ISSUE CERTIFICATE, OR ACCEPTING CERTIFICATE OR THE FIRST USE OF IT, PLEASE READ THE TEXT OF THESE „TERMS OF USE FOR NON-QUALIFIED CERTIFICATES“ REFERRED TO AS „TERMS OF USE“. IF YOU DO NOT ACCEPT THESE TERMS OF USE, DO NOT SEND THE REQUEST TO ISSUE CERTIFICATE, DO NOT ACCEPT IT AND DO NOT USE IT.

THESE TERMS OF USE BECOMES EFFECTIVE FROM THE MOMENT OF SUBMITTING THE CERTIFICATE REQUEST TO „CERTUM - Certification Authority“ (HEREINAFTER „CERTUM“) AND ARE VALID UNTIL THE END OF CERTIFICATE VALIDITY PERIOD OR UNTIL THE CERTIFICATE REVOCATION. SENDING THE CERTIFICATE REQUEST MEANS THAT YOU WANT CERTUM TO REVIEW THE APPLICATION AND ISSUE THE CERTIFICATE, AND MEANS THAT YOU

I agree to Terms of Use *

I declare and confirm that I am aware of the fact that the certificate may expose my personal data to the extent it has been indicated for inclusion in the certificate. I also confirm that all activities carried out using this certificate may, at my discretion, be available without restriction, in particular with regard to location. The use of the certificate is not affected by Asseco Data Systems S.A., provider of security services. *

I confirm that I am of age *

I hereby confirm the accuracy of my personal data included in the application for the certificate. *

*Required

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

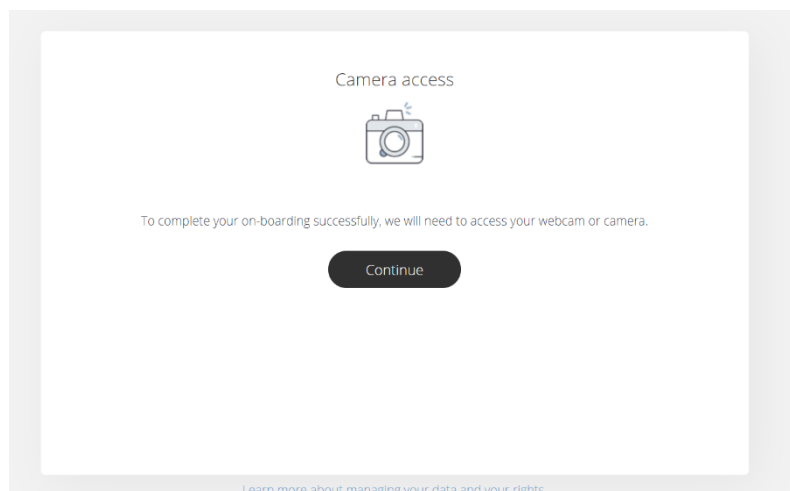
What does the process during certificate activation look like?

- 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.

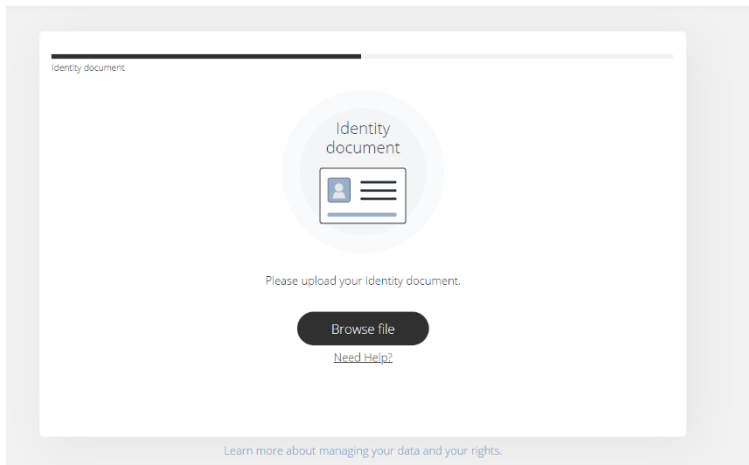
5.2.1. Verification using a computer

Step 1 — Document verification

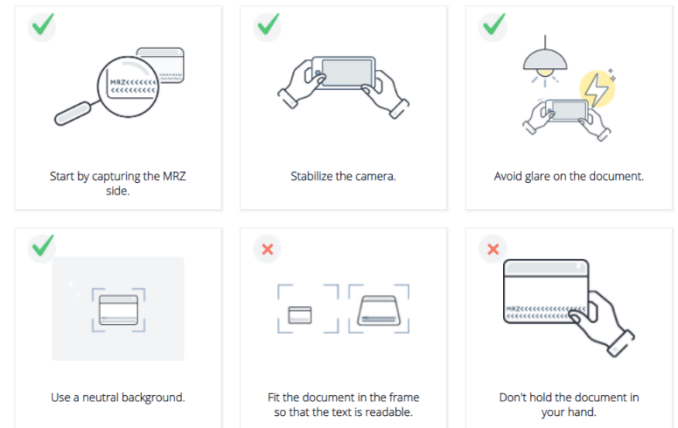
After clicking the link to initiate verification, you will be prompted to turn on your camera, so your identity can be verified. Click "Continue" and proceed to the next step.



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.



How to take a good picture of a document.

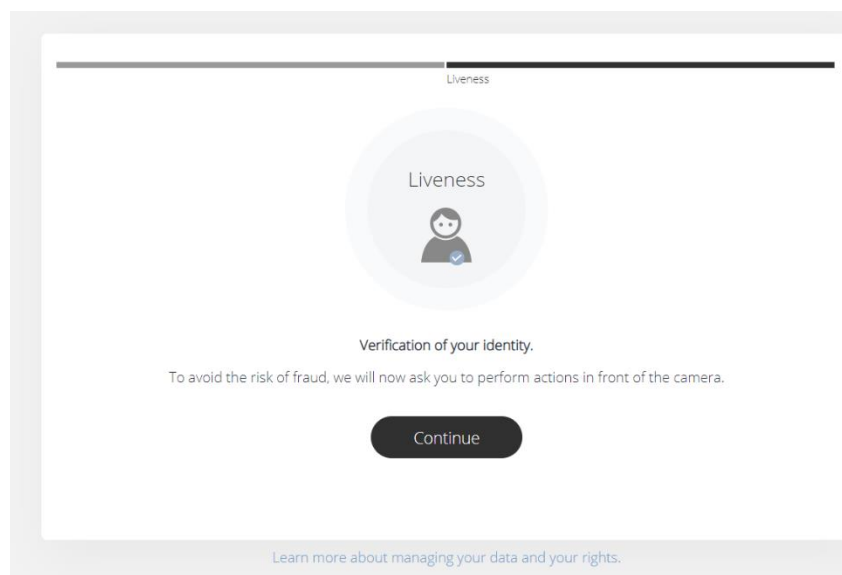


I understand

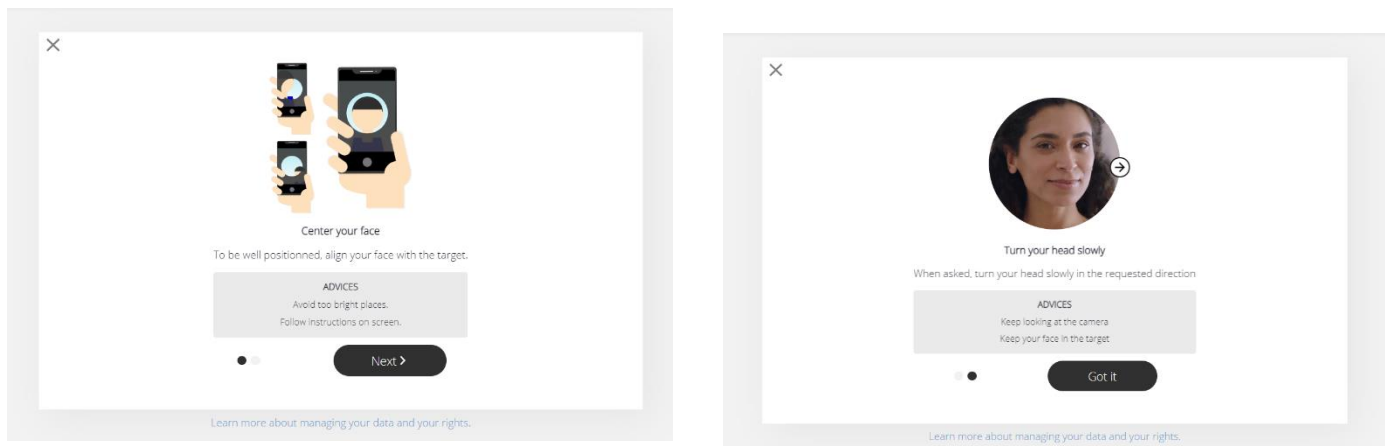
Once the data are submitted, the system will process it for approximately 12 seconds to extract the data from the document. After this process, the document image will be deleted.

Step 2 — Facial comparison

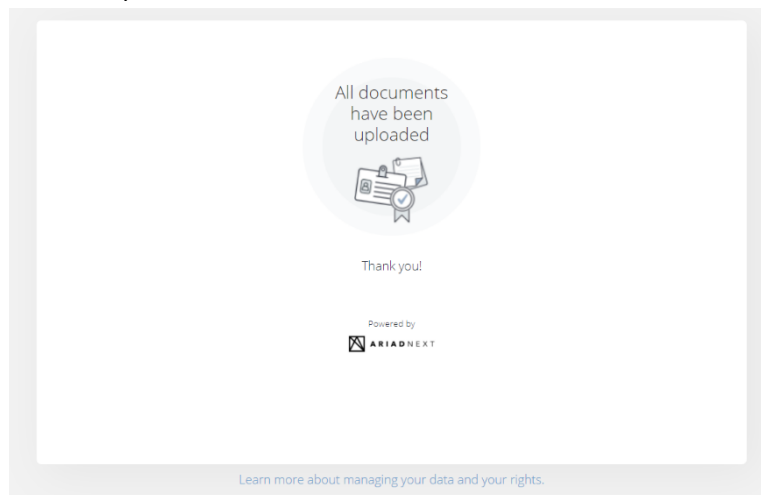
During this step you will be asked to move your face in front of the camera. This biometric solution will ensure that the User is present during the identity confirmation and is the holder of the document.



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:

- Electronic codes
- Activate Certificates
- Certificates' management
- Orders history
- Address details
- Tools
- Newsletter
- Domain verification
- Technical support
- Knowledge
- About Certum

Certificates' management

Certificate profile:

Common name:

Email:

Serial number:

Validity starts after:

Validity ends before:

[Search](#)

Status:

Obtain Valid

Valid

Not Valid

Revoked

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

1. The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdynia, ul. Podolska 21, 81-321 Gdynia;
2. The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: IOD@asseccods.pl, or phone number +48 42 876 63 60.
3. Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
4. Your personal data will be stored for a period of 7 years from the date of revocation or expiration of the last certificate issued

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

0df462982e					
9d4093314c	EV Code	Asseco Data Systems	January 15,	January 14,	Valid
6b977b2f1f	Signing	S.A.	2020 7:21:31	2021 7:21:31	
1b			AM	AM	


- Click the [Save Binary](#) button:

Hash function RSA-SHA256


Common name Asseco Data Systems S.A.

Organization Asseco Data Systems S.A.

Organizational unit PUBIZ



Certum EV Code Signing



Certum Code Signing

[Revoke](#)

[Save](#)

[Renew](#)

[Save binary](#)


[Save plain](#)

[Reissue](#)

- Download the certificate file to your computer.
- Open [proCertum CardManager](#):

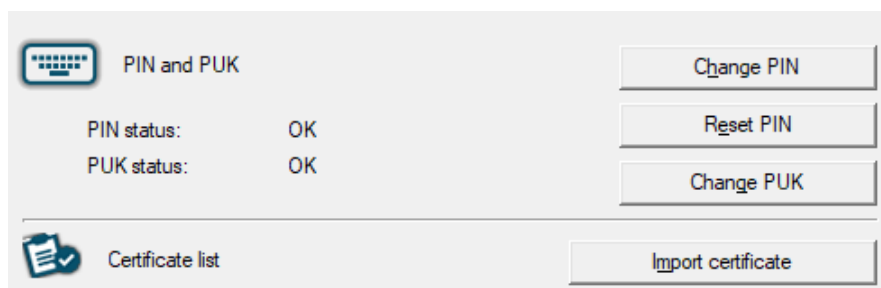
proCertum CardManager

— □ ×

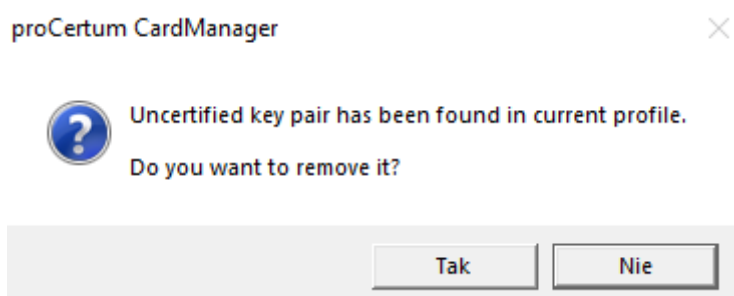


Smart card reader name:

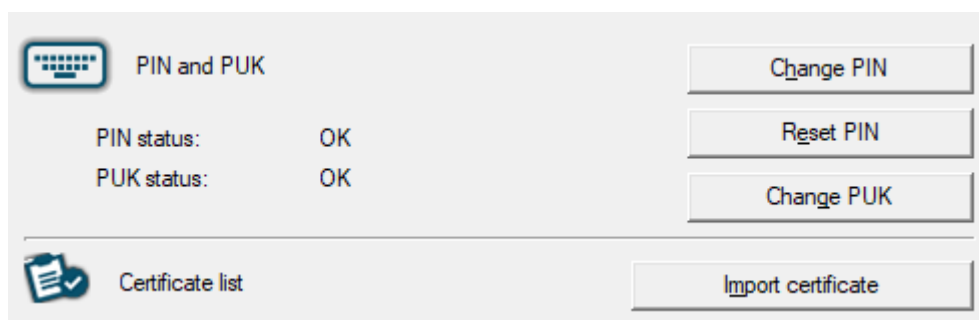
- Go to the [Common profile](#) tab:



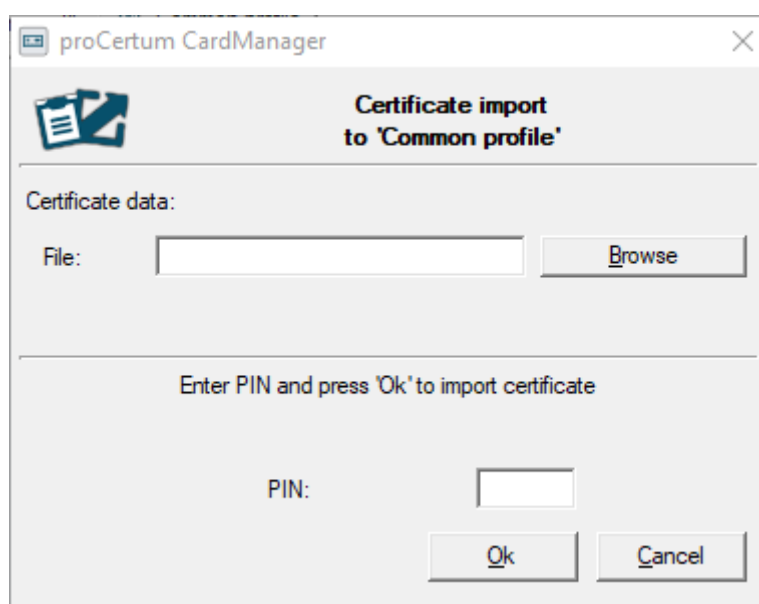
7. If you see a notification about uncertified keys on the card, press [No](#):



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:

