

# EV Code Signing on a card certificate activation

Ver. 2.8

assecO

 **Certum**  
by assecO

## Table of contents

1. Product description .....	3
2. Certificate activation .....	3
Data verification step .....	4
Key generation step .....	10
Certificate activation step .....	14

## 1. Product description

The Code Signing certificate allows you to digitally sign applications and drivers, certifying their authenticity and security. Thanks to this, users of your software can be sure that it has not been modified, infected or damaged by third parties.

Signing the application with Code Signing eliminates the problem of code anonymity on the internet. With a digital signature you can be sure that users will not see an "unknown publisher" warning when installing or running your program and they will be ensured about its security. Signing your app helps protect both: your users and your brand's reputation.

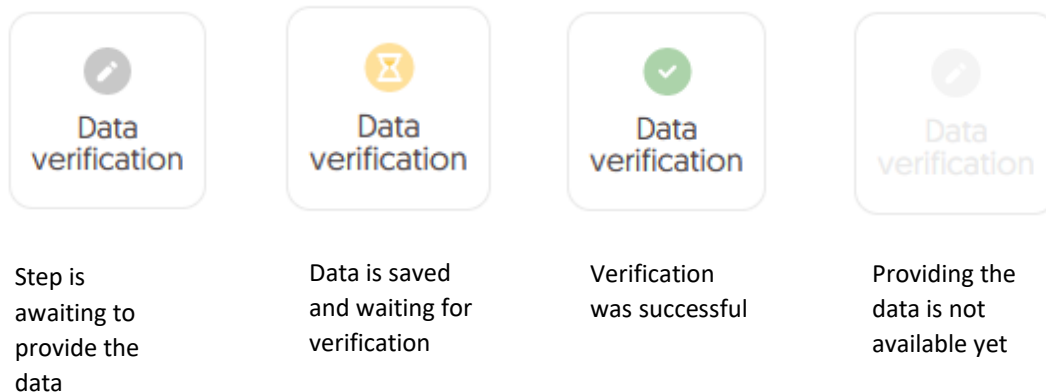
Digital code signing makes using the application safe, which translates into greater trust in your brand and an expansion of your group of users.

## 2. Certificate activation

You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **Data verification** – providing the Subscriber and/or organization's data and the verification
- **Key generation** – key pair generation
- **Certificate activation** – choosing the fields to include in the certificate and submit to issue.

As the activation process goes, each step will go through the next statuses:



## Data verification step

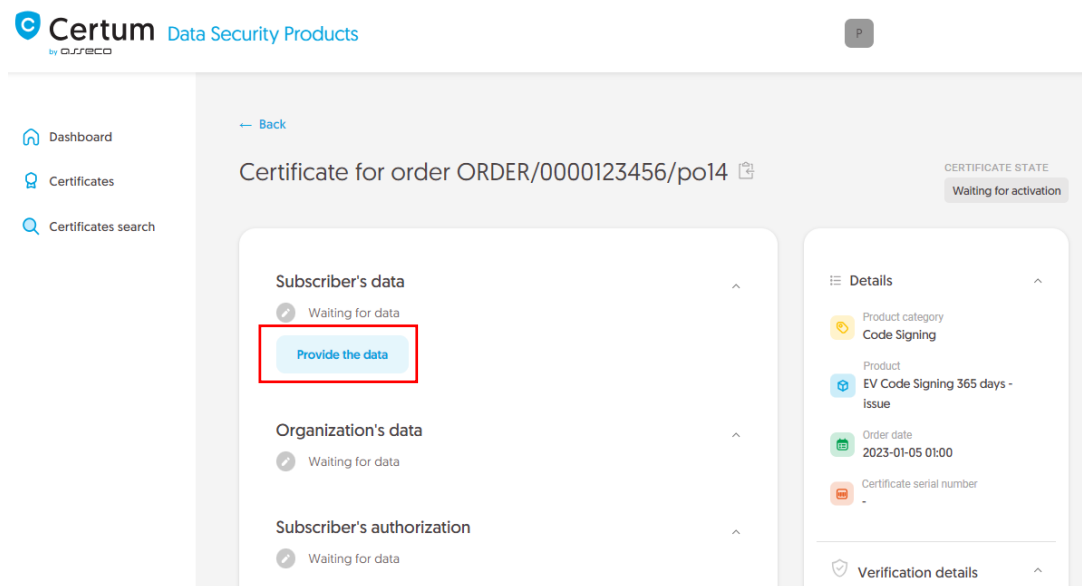
Providing data to be verified is the step in which you provide the data of the organization for which the certificate will be issued, the data of the Subscriber (the person who represents the organization and will be the owner of the certificate) and the data of the Subscriber's authorization to represent the organization. From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

The list of supported verification documents you can check at [Information about required documents](#).

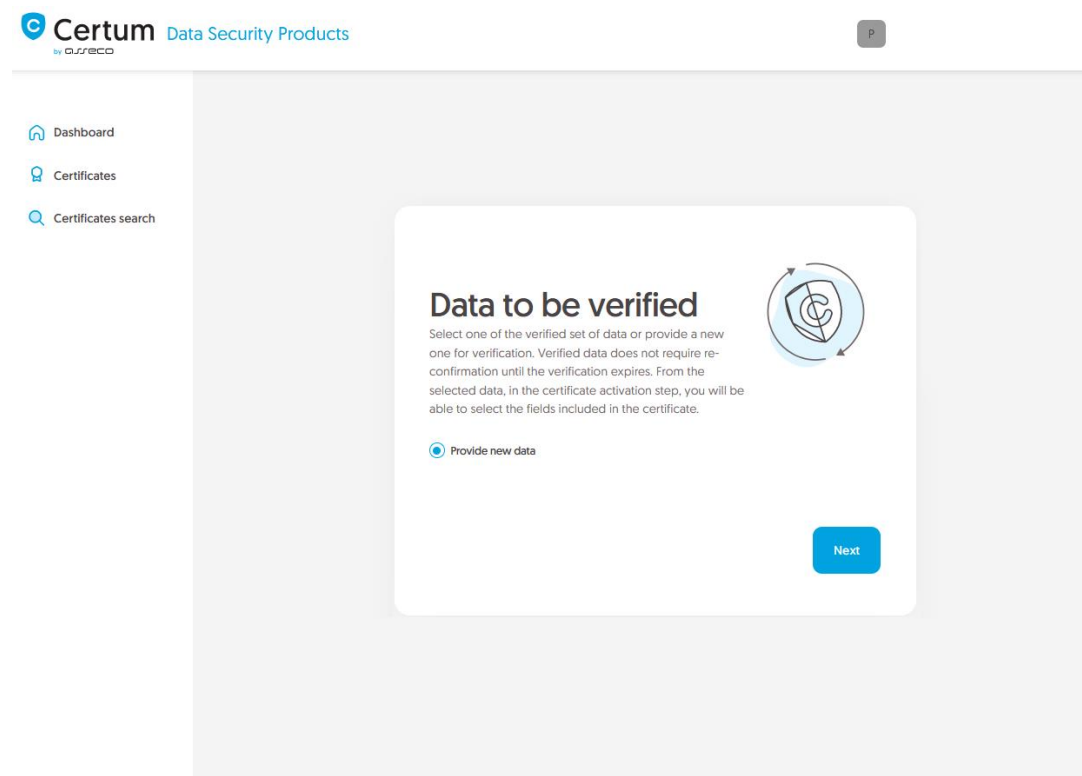
You will be able to start the data verification step from **Dashboard**, using **Data verification** option:

The screenshot displays the Certum Data Security Products dashboard. On the left, there is a navigation menu with 'Dashboard', 'Certificates', and 'Certificates search'. The main content area includes a 'Hello' message, an 'Events' table, and a 'Code Signing' card. The 'Code Signing' card shows the 'Data verification' step highlighted with a red box, indicating it is the current step. Below the steps, the product details are listed: 'EV Code Signing 365 days - issue', 'Status: Waiting for activation', 'Common name: -', and 'Certificate expires: -'. A 'Show more' link is visible at the bottom of the card. On the right side, there is a 'Useful information' section with a description of the product activation process and a 'Useful sources' section with links to 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'.

or from the **Certificates** list – choose the certificate you want to activate and use **Provide the data** option in the Subscriber's data section:



The wizard will guide you through the process of providing the data. In the first stage, choose **Provide new data**. In the future, it will be possible to use them to issue another certificate.

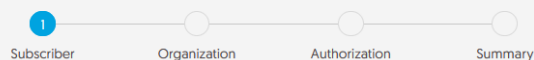


In the next stage, provide the details of the Subscriber, which means the person who represents the organization and will be the owner of the certificate. Please write the names and surnames in the form as they appear on the Subscriber's identity document.

Also choose a method for verifying the Subscriber's identity from the available ones:

- **Automatic identity verification** – the Subscriber will receive an e-mail with a link to the identity verification service to use with a computer or phone camera and an ID document
- **Attaching a document** – you will add a scan of the Subscriber's identity document or an identity confirmation.

- [Dashboard](#)
- [Certificates](#)
- [Certificates search](#)



## Subscriber data

The Subscriber is a person who will be the owner of the certificate: the data of him or her or related organization that he or she can represent will be available to include in the certificate (depending on the product type). After completing the step of providing the data to be verified, Subscriber will be asked to verify his/her identity with an **identity document** using one of the available verification methods.

NAME\*

Joe

SURNAME\*

Doe

### Verification method

- Automatic identity verification   
  Add the document to verify Subscriber's identity

E-MAIL ADDRESS OF THE SUBSCRIBER\*

joedoe@yourdomain.com

In the case of **automatic identity verification**, the Subscriber will receive a link and instructions to start the process to this e-mail address. The link will be sent after saving the data to be verified.

[Back](#)

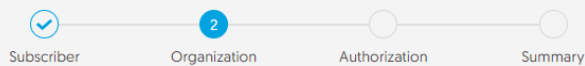
[Next](#)

After providing the Subscriber's data, go to the next stage: providing the organization's data. Here provide the organization's details and the address of its headquarters. The data will be used to verify the existence of the organization.

Choose also how Certum will verify the existence of the organization:

- **By registration number** – Certum will search for information about the organization in the public register using the provided number
- **Attaching a document** – you will add a document confirming the establishment of the organization.

- Dashboard
- Certificates
- Certificates search



## Organization data

Provide the data to let us verify your organization existence. From this data you will be able to choose the fields to include in the certificate.

### The data of the organization

ORGANIZATION\*

Your company

BUSINESS CATEGORY\*

Private Organization

REGISTRATION NUMBER\*

12345678

### Headquarters of the organization

COUNTRY\*

Poland

STATE OR PROVINCE\*

mazowieckie

LOCALITY\*

Warszawa

POSTAL CODE\*

10-100

STREET AND HOUSE NUMBER\*

Jana Kochanowskiego 1

Jurisdiction of incorporation

JURISDICTION OF INCORPORATION COUNTRY NAME\*

Poland

JURISDICTION OF INCORPORATION STATE OR PROVINCE NAME\*

mazowieckie

JURISDICTION OF INCORPORATION LOCALITY NAME\*

Warszawa

Verification method

Search the information about the organization by registration number

Add the document to verify organization existence

REGISTRATION NUMBER TYPE\*

DUNS

REGISTRATION NUMBER IN THE REGISTRY\*

12345678

[Back](#) [Next](#)

After providing all the required organization's data, proceed to the last stage of providing data for verification step, which is choosing the method of verifying the Subscriber's authorization to represent the organization.

There are two methods to choose from:

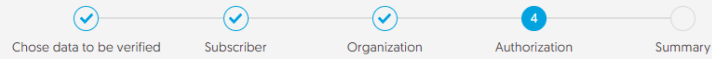
- **The Subscriber is visible in the registry** – the person given as the Subscriber appears in one of the given registers as a representative of the organization
- **Attaching a document** – you will add a document confirming authorization. You can download an example of such document by the **Download ready to sign authorization document** link.

The method of verifying the Subscriber's authorization is also influenced by the organization's chosen verification method. If the registration number and its type have been provided there, Certum will first check whether the Subscriber is listed in the register and the system will automatically mark the method of verifying the Subscriber's authorization as "The Subscriber is visible in the register". However, this does not prevent you from adding a document confirming the Subscriber's authorization.





- Dashboard
- Certificates
- Certificates search



## Authorization data

Choose the verification method to confirm the Subscriber's relationship with the organization.

### Subscriber data

Name   Surname  
Joe   Doe

### Verification method

- Subscriber is visible in DUNS, LEI or other registry as organization's representative    Add the document to verify Subscriber's relationship with the organization

### Chosen registry type




DUNS  
12345678

[Back](#)

[Next](#)

After selecting the authorization verification method and proceeding, verify provided information on the summary screen. If the data is correct, mark the required statements and complete the step of providing data to be verified.

The success screen will inform you that the data have been saved for verification. Certum will verify them. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the Subscriber's identity, if such verification method has been chosen. You may check the [instruction for automatic identity verification](#).

-  Dashboard
-  Certificates
-  Certificates search



## Success!

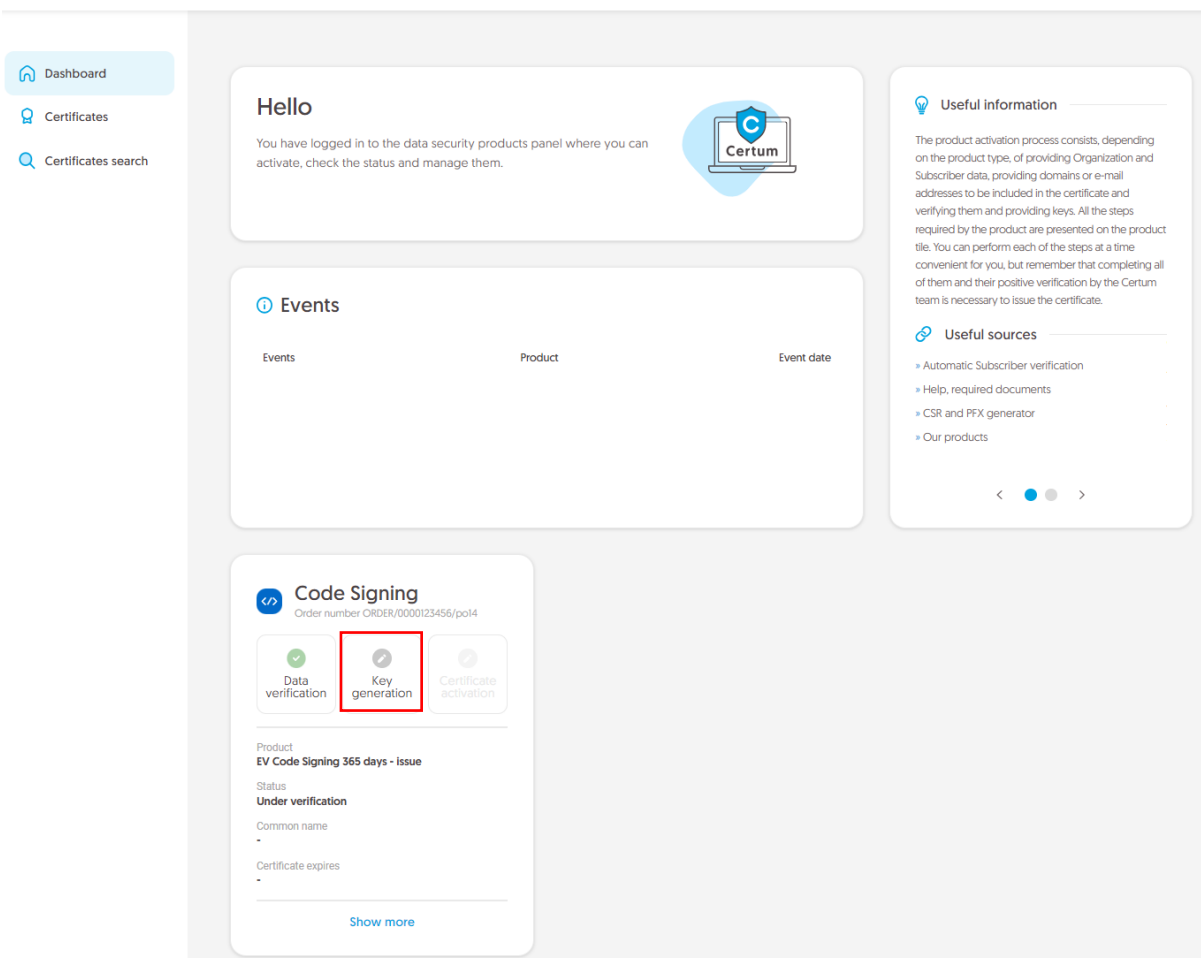
The data was saved and submitted for verification. The verification usually takes from 1 to 7 days. Positive data verification will allow you to proceed to the next step of the certificate activation.

[Go to dashboard](#)

Positive verification of the provided data will allow you to proceed to the step which is generating keys.

### Key generation step

You will be able to start the key pair generation step from **Dashboard**, using **Key generation** option:



**Dashboard**

- Dashboard
- Certificates
- Certificates search

**Hello**

You have logged in to the data security products panel where you can activate, check the status and manage them.

**Events**

Events	Product	Event date

**Useful information**

The product activation process consists, depending on the product type, of providing Organization and Subscriber data, providing domains or e-mail addresses to be included in the certificate and verifying them and providing keys. All the steps required by the product are presented on the product tile. You can perform each of the steps at a time convenient for you, but remember that completing all of them and their positive verification by the Certum team is necessary to issue the certificate.

**Useful sources**

- Automatic Subscriber verification
- Help, required documents
- CSR and PFX generator
- Our products

**Code Signing**  
Order number ORDER/0000123456/pol4

Data verification **Key generation** Certificate activation

Product  
EV Code Signing 365 days - issue

Status  
**Under verification**

Common name  
-

Certificate expires  
-

[Show more](#)

or similar to the **Data verification** step: from the **Certificates** list – choose the certificate you want to activate and use **Generate key pair** option.

In this step, you will generate a key pair for the certificate.

For Code Signing certificates, the available key generation method is **Generating key pair on card** – the keys will be saved on the cryptographic card.

When choosing a method for generating key pair on card, also choose the algorithm and key length. Your choice should depend on the algorithm and key length supported by the application in which you use the certificate or the recommendation of e.g. your IT department.

After selecting the method for generating key pair on card, choose the algorithm and key length.

- [Dashboard](#)
- [Certificates](#)
- [Certificates search](#)

## Key generation method

Choose one of the key generation methods available below. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card. Key pair for certificates stored in the cloud will be generated automatically.

### Key pair generation method

- Generating key pair on card

#### KEY ALGORITHM AND KEY LENGTH

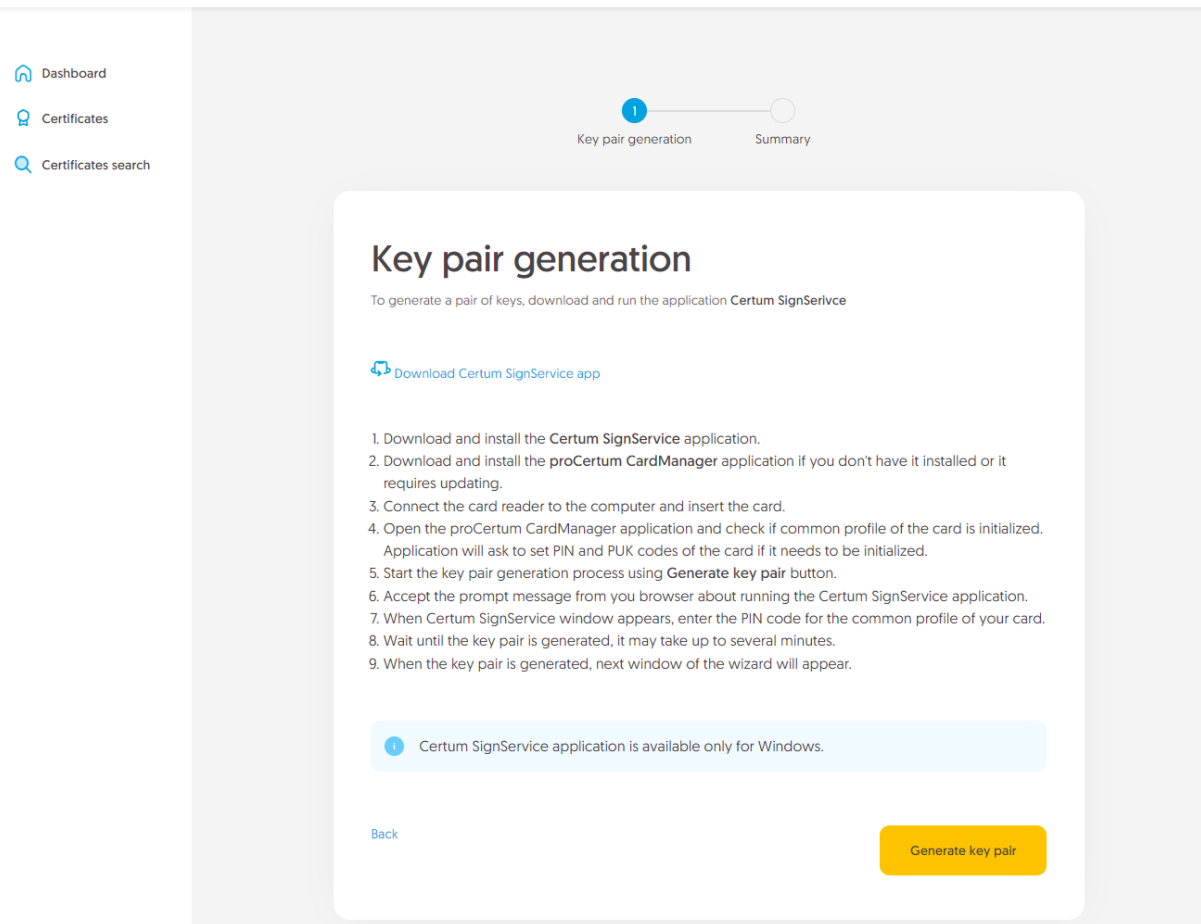
RSA 3072

The CSR method will allow you to obtain a certificate with a key in a form that can be transferred and installed from a file. Remember to save a private key generated with your CSR. Generating keys on the card will cause that the certificate will be installed on the cryptographic card and its connection to the computer will be required whenever the certificate is used. Only Certum cards are supported.

Next

In the next stage, make sure that you have the card inserted into the reader, the reader connected to the computer and the card itself has an initialized common profile with a PIN code set for it. The process also requires having the proCertum CardManager application installed on your computer, where you can also check the status of the card and the status of PIN and PUK codes.

You may check the instruction of [how to assign PUK and PIN codes for the first time](#).



Dashboard

Certificates

Certificates search

Key pair generation Summary

## Key pair generation

To generate a pair of keys, download and run the application **Certum SignService**

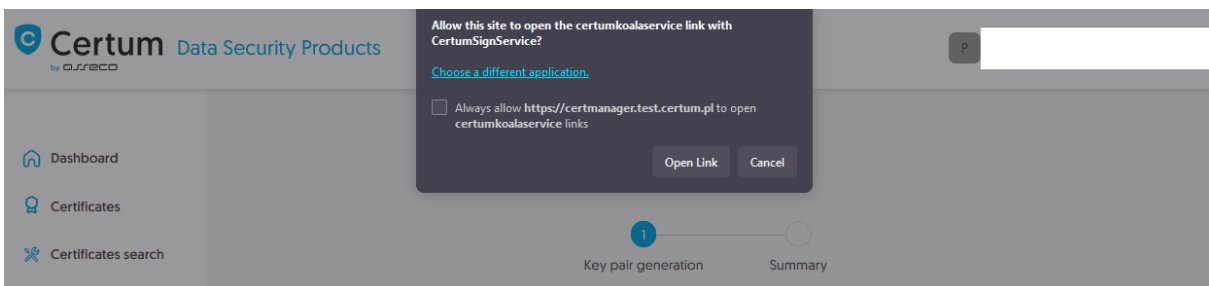
[Download Certum SignService app](#)

1. Download and install the **Certum SignService** application.
2. Download and install the **proCertum CardManager** application if you don't have it installed or it requires updating.
3. Connect the card reader to the computer and insert the card.
4. Open the **proCertum CardManager** application and check if common profile of the card is initialized. Application will ask to set PIN and PUK codes of the card if it needs to be initialized.
5. Start the key pair generation process using **Generate key pair** button.
6. Accept the prompt message from you browser about running the **Certum SignService** application.
7. When **Certum SignService** window appears, enter the PIN code for the common profile of your card.
8. Wait until the key pair is generated, it may take up to several minutes.
9. When the key pair is generated, next window of the wizard will appear.

**1** Certum SignService application is available only for Windows.

[Back](#) [Generate key pair](#)

To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.



Dashboard

Certificates

Certificates search

Key pair generation Summary

Allow this site to open the certumkoalaservice link with CertumSignService?

[Choose a different application.](#)

Always allow <https://certmanager.test.certum.pl> to open certumkoalaservice links

[Open Link](#) [Cancel](#)

Certum SignService

**Certum SignService**  
by GISECO

**New key pair generation**

Cards data

Reader name: ACS ACR39U ICC Reader 0  
Card number: 1625 8349 7691 9804

Key details

Algorithm: RSA  
Size: 2048

Common profile PIN:   
[from 4 to 32 characters]

**Depending on the algorithm and size of the key generation may take up to several minutes**

**Do not remove the card from the reader during the operation**

Ok Cancel

After providing the PIN code, the key generation process will begin on the card. This may take up to a few minutes. Once the key is generated, the process will proceed to the next stage.




Check provided data on the summary screen. If the data is correct, complete the key pair generation step.

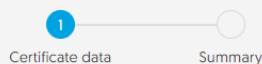
The success screen will inform you that the key pair generation step is completed. You can proceed to the last step, which is **Certificate activation**.

### Certificate activation step

You will be able to start certificate activation step from **Dashboard**, using **Certificate activation** option or similar to the previous step: from the **Certificates** list – choose the certificate you want to activate and use **Activate certificate** option.


In this step, choose the fields you want to include in the certificate. Some fields are required and cannot be unmarked.

-  Dashboard
-  Certificates
-  Certificates search



## Certificate data

Choose the data to be included in the certificate. Some of the fields are mandatory and there is no option to uncheck them.

 **Code Signing**  
EV Code Signing 365 days - issue

- Common name:  
Your company
- Organization [O]:  
Your company
- Locality [L]:  
Warszawa
- State or province [SP]:  
mazowieckie

Once you have chosen the fields to the certificate, go to the summary screen and check all of provided data. Mark the required statements and complete certificate activation.

The success screen will inform you that the certificate has been submitted for issuance. Certum will finally verify the data in the certificate and after positive verification, will issue it. The issued certificate can be downloaded from the certificate creation e-mail or from the certificate details view: in a convenient **PEM** or **DER** encoding. You can install your certificate on the cryptographic card from the certificate details view.

From the certificate details view you can also download subordinate certificates for your certificate.