

Open Source Code Signing on a card certificate activation

Ver. 1.0

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step	4
Certificate activation step	8

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.

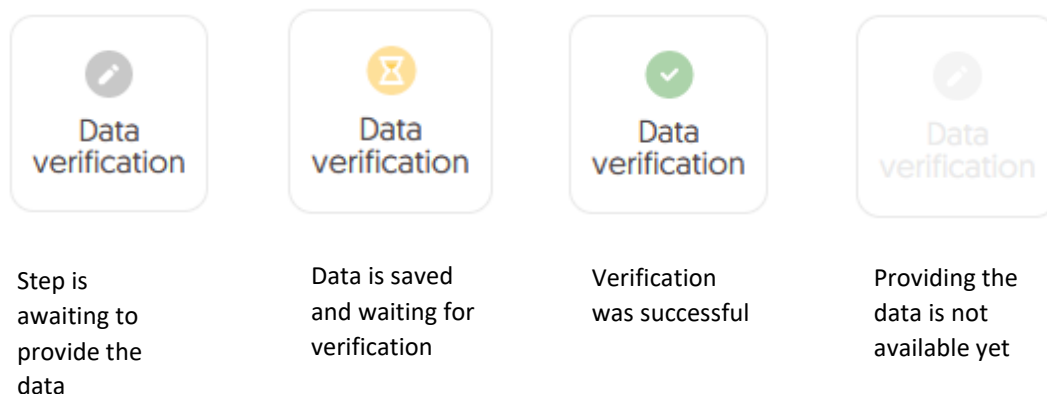
Digital code signing makes using the application safe, which translates into greater trust in your brand and an expansion of your group of users.

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's data and the verification
- **Certificate activation** – key pair generation, 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:

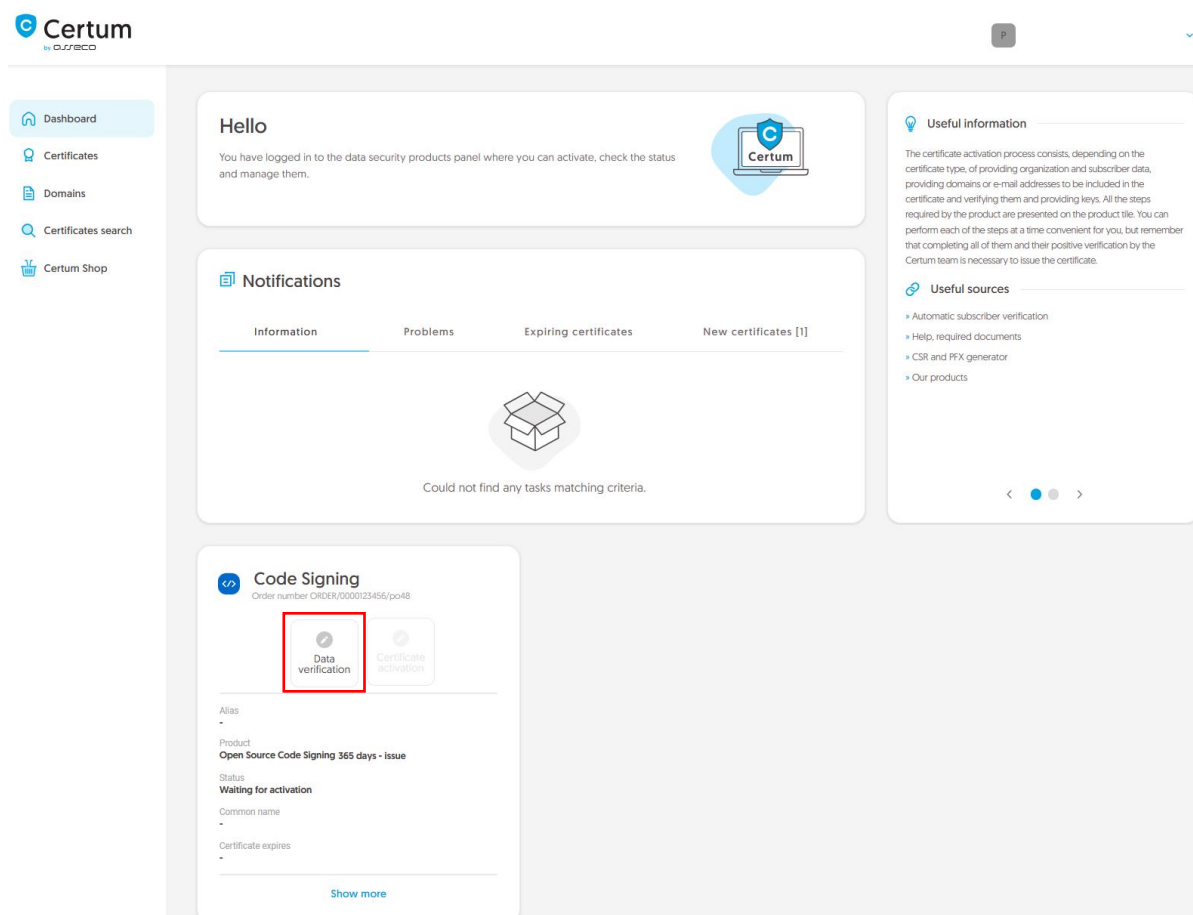


Data verification step

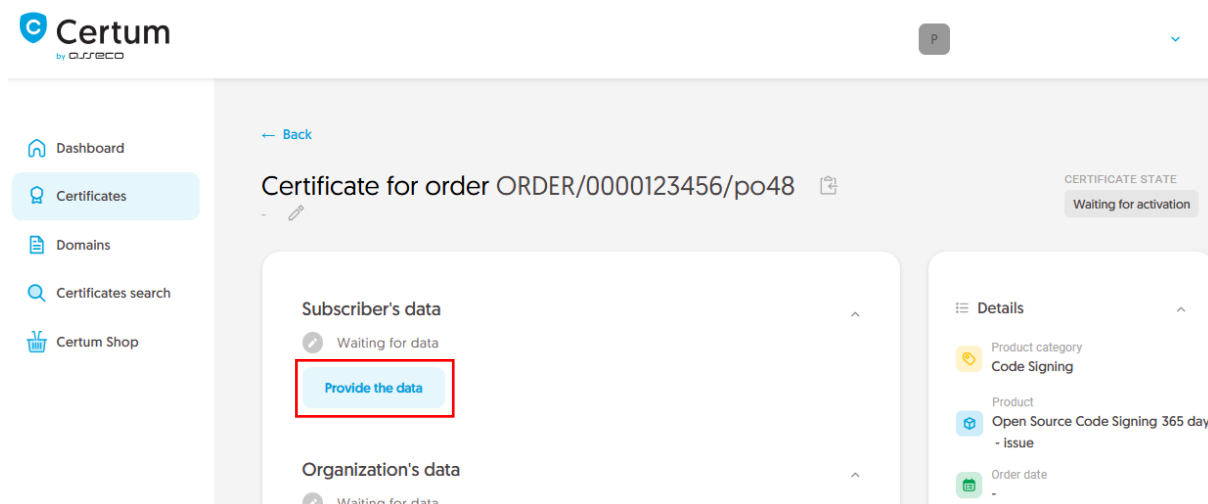
Providing data to be verified is the step in which you provide the data of the subscriber (the person who will be the owner of the certificate). From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

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

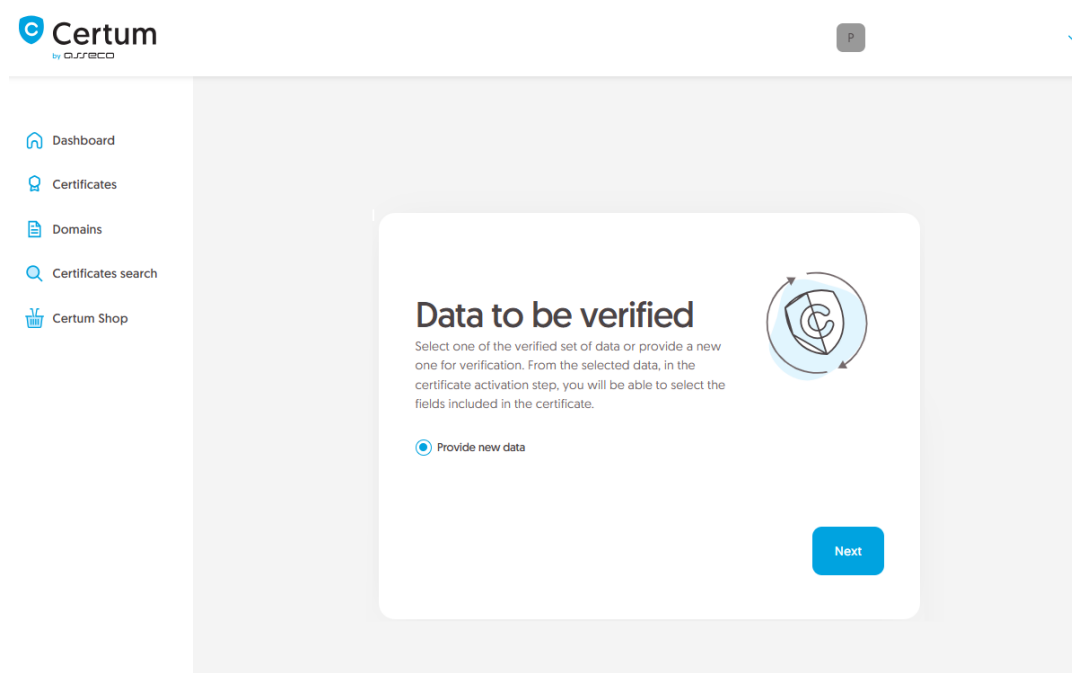
You will be able to start the data verification step from **Dashboard**, using **Data verification** option:



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 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.



P

[Dashboard](#)
[Certificates](#)
[Domains](#)
[Certificates search](#)
[Certum Shop](#)

1
Subscriber

Organization

Summary

Subscriber data

The subscriber is a person who will be the owner of the certificate: the data of him or her or organization that he or she can represent will be available to include in the certificate. After completing this step, 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. For Open Source certificate provide the subscriber's address.

Certum
by QSECO

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Subscriber Organization Summary

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*

Open Source Developer

Headquarters of the organization

COUNTRY*

Poland [PL]

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warsaw

Verification method

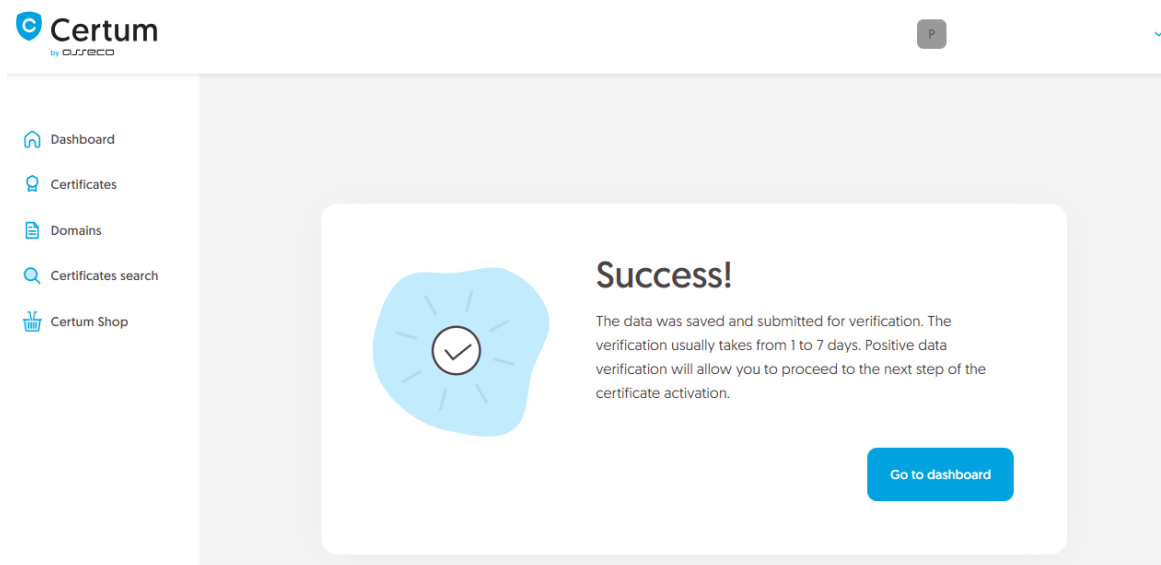
☒ Add the document to verify organization existence

Added documents [0] [Read about required documents](#)

After providing all the required data, go to the data verification step summary.

Check 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.

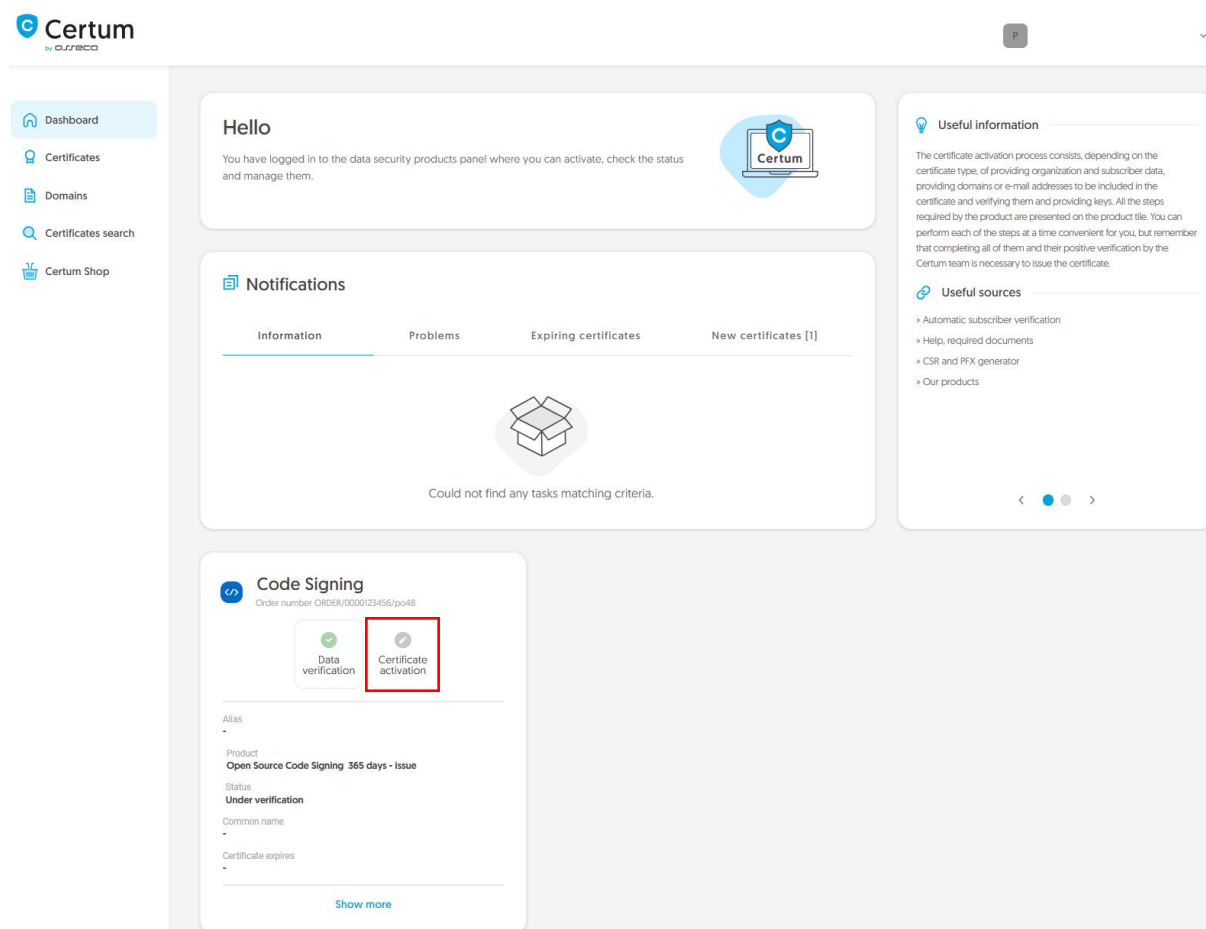
The success screen will inform you that the data have been saved for verification. Certum will verify them. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the subscriber's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



Positive verification of the provided data will allow you to go to the **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, you will choose the fields you want to include in the certificate and generate key pair.

Choose the fields you want to include in the certificate. Some fields are required and cannot be unmarked.

Certum
by CURESCO

Dashboard
Certificates
Domains
Certificates search
Certum Shop

1 Certificate data Generation method Key pair generation Summary

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
Open Source Code Signing 365 days - issue

☒ Common name:
Open Source Developer, Joe Doe

☒ Organization [O]:
Open Source Developer

☒ Locality [L]:
Warsaw

☒ State or province [SP]:
mazowieckie

Once you have chosen the fields to the certificate, go to the key pair generation.

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.

The screenshot displays the Certum SignService web application. On the left is a sidebar with navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area shows a progress bar with four steps: Certificate data (completed), Generation method (active, step 2), Key pair generation, and Summary. Below the progress bar, the title 'Key pair generation method' is followed by a subtitle: 'Generating key pair with Certum SignService application allows you to store keys on a cryptographic card.' Under the heading 'Key pair generation method', the option 'Generating key pair on card' is selected with a radio button. Below this, a dropdown menu labeled 'KEY ALGORITHM AND KEY LENGTH' is set to 'RSA 3072'. An information box explains that the CSR method allows obtaining a certificate with a key in a file format, while generating keys on a card requires the certificate to be installed on the card and connected to the computer. At the bottom, there are 'Back' and 'Next' buttons.

Certum
by *ORFECO*

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Certificate data **2** Generation method Key pair generation Summary

Key pair generation method

Generating key pair with Certum SignService application allows you to store keys on a cryptographic card.

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.

[Back](#) [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](#).

Certum
by **ojsreco**

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Certificate data Generation method **Key pair generation** Summary

Key pair generation

Follow the instruction below to generate key pair.

[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.

When the key pair is generated, next window of the wizard will appear.

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

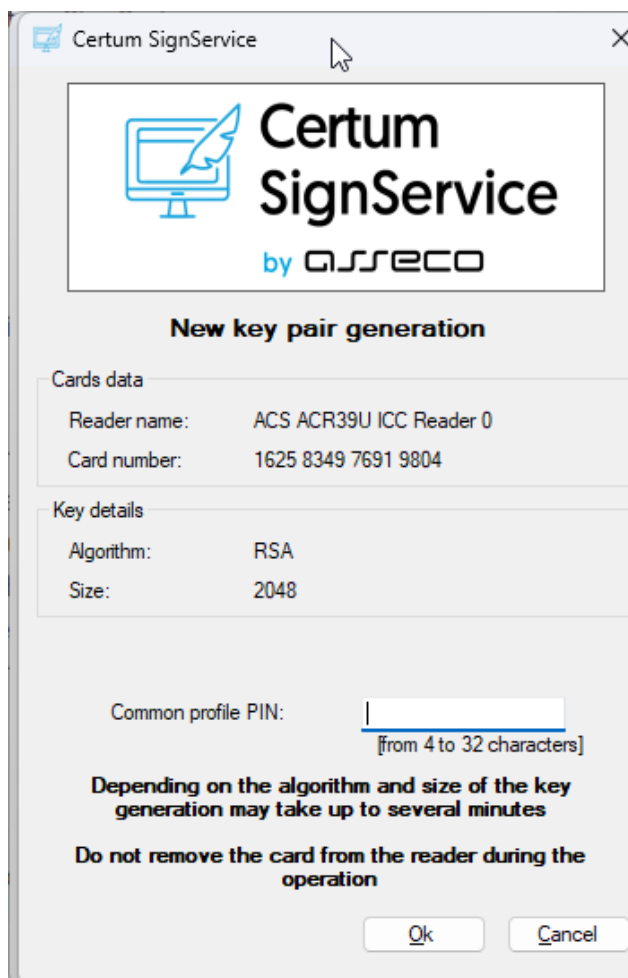
To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.

Certum
by **ojsreco**

Dashboard
Certificates

Certificate data Generation method **Key pair generation** Summary

Open CertumSignService?
https://certmanager.certum.pl wants to open this application.
[Open CertumSignService](#) [Cancel](#)



The image shows a Windows-style dialog box titled "Certum SignService" with a close button (X) in the top right corner. The dialog features the Certum SignService logo, which includes a stylized blue icon of a computer monitor with a pen writing on it, followed by the text "Certum SignService by GSECO". Below the logo, the title "New key pair generation" is centered. The dialog is divided into two main sections: "Cards data" and "Key details". The "Cards data" section contains two fields: "Reader name:" with the value "ACS ACR39U ICC Reader 0" and "Card number:" with the value "1625 8349 7691 9804". The "Key details" section contains two fields: "Algorithm:" with the value "RSA" and "Size:" with the value "2048". Below these sections, there is a label "Common profile PIN:" followed by a text input field. A hint "[from 4 to 32 characters]" is displayed below the input field. A warning message is centered: "Depending on the algorithm and size of the key generation may take up to several minutes". Below the warning, another centered message reads: "Do not remove the card from the reader during the operation". At the bottom right, there are two buttons: "Ok" and "Cancel".

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 summary.

Check all of provided data. Mark the required statements if needed and complete certificate activation.

The success screen will inform you that the certificate has been submitted for issuance. 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 the certificate.