

Certum S/MIME Organization certificate activation

Ver. 1.7

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step	4
E-mail verification step.....	7
Certificate activation step	8
CSR method.....	10
Generating key pair on a cryptographic card.....	11
Summary	14

1. Product description

Certum S/MIME certificates are security certificates used in e-mails to secure electronic communication. They enable the encryption of message content, ensuring privacy and confidentiality of e-mail correspondence. Additionally, S/MIME certificates allow for the addition of digital signatures, to confirm the sender's identity and guarantee the integrity of the transmitted content.

With Certum S/MIME certificates, it is possible to enhance the security of e-mail communication by verifying the e-mail address/identity of the sender, encrypting messages and ensuring integrity.

2. Certificate activation

As the Certum **customer**, you will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab.

As the **partner**, you start the process through partner panel from the **Dashboard** by choosing the product you want to order.

The process of issuing the certificate consists of several steps:

- **Data verification** – providing organization's data and the verification
- **E-mail verification** – providing an e-mail 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:



Step is
awaiting for
the data



Data is saved
and waiting for
verification



Verification
was successful



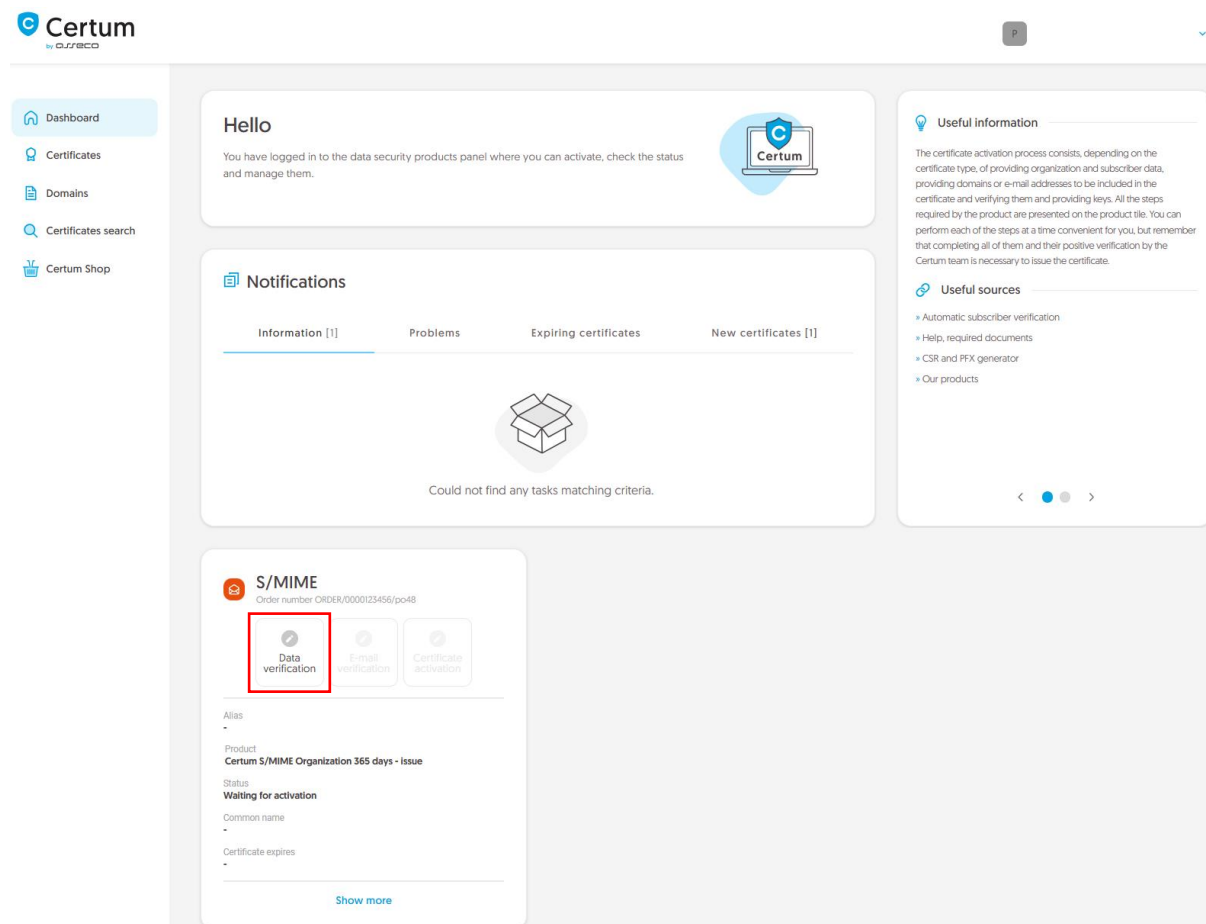
Providing the
data is not
available yet

Data verification step

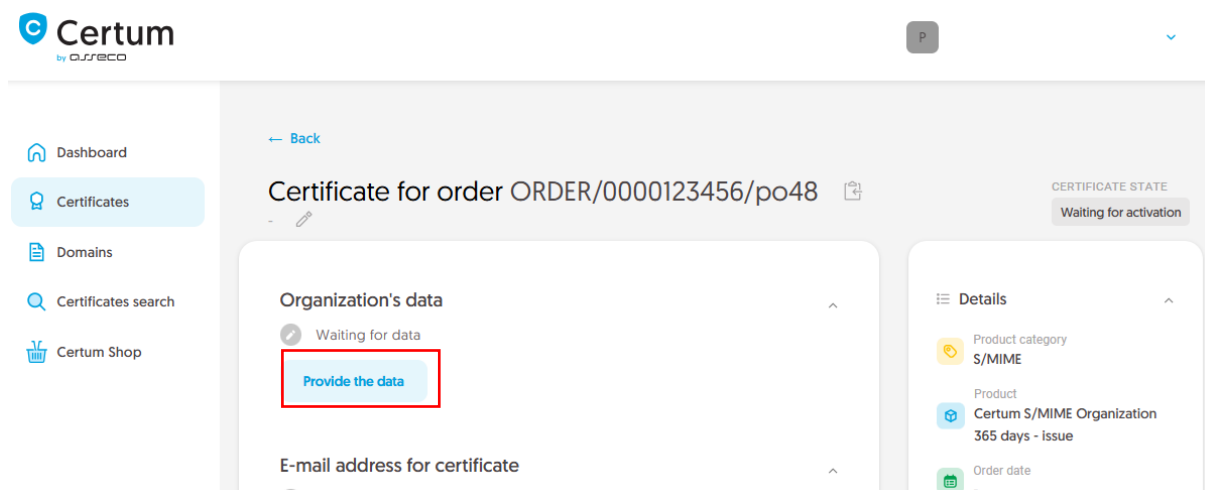
Providing data to be verified is the step in which you provide the data of the organization for which the certificate will be issued. From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

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

As the Certum **customer**, you will be able to start the data verification step from **Dashboard**, using **Data verification** option:

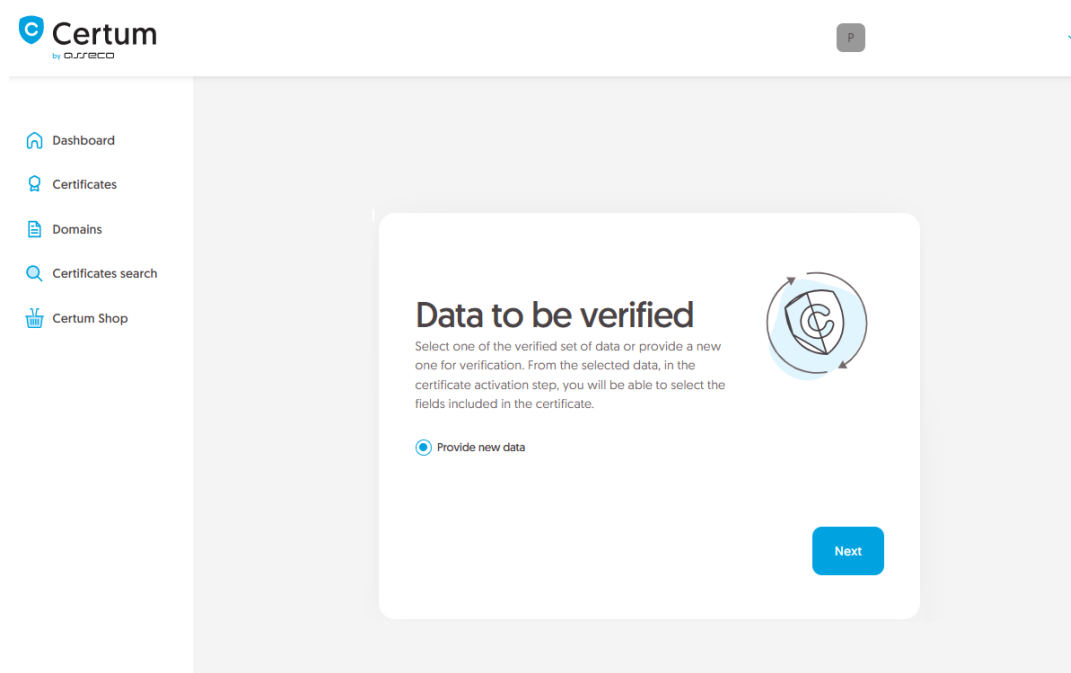


or from the **Certificates** list – choose the certificate you want to activate and use **Provide the data** option in the organization's data section:



As the **partner**, you will be able to start the data verification step from **Dashboard**, using new order option. After choosing the product type and providing the order details, you will be able to provide the data used in the first step of issuing the certificate.

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



In the next stage, provide 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.

Certum
by **QUECO**

Dashboard
Certificates
Domains
Certificates search
Certum Shop

1 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*

Your company

Headquarters of the organization

COUNTRY*

Poland [PL]

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warsaw

Verification method

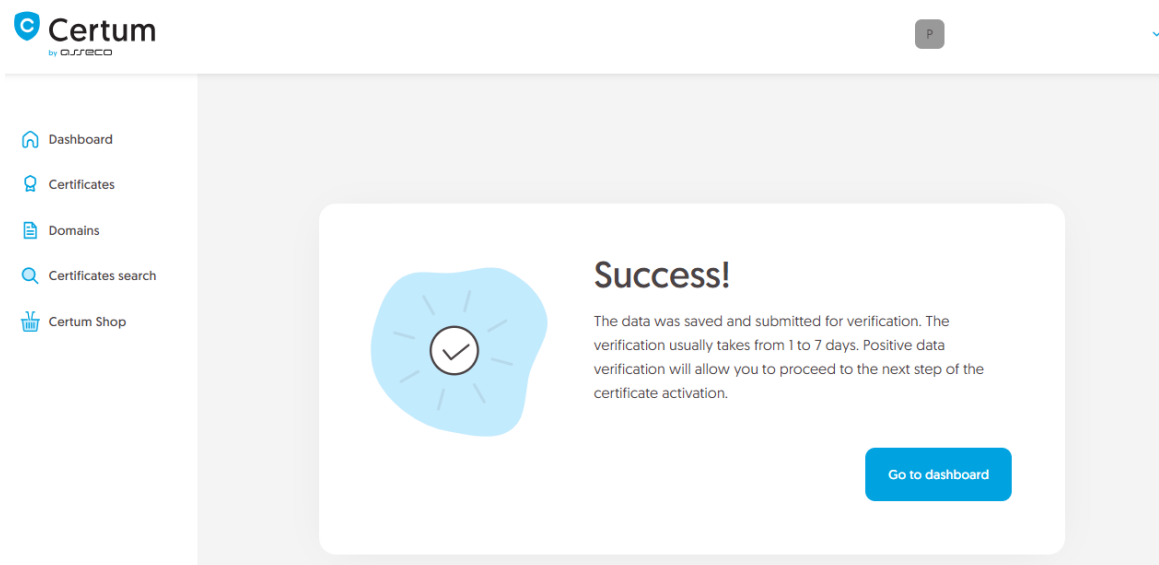
☒ Search the information about the organization by registration number ☐ Add the document to verify organization existence

REGISTRATION NUMBER TYPE*

DUNS

In the next step verify provided information on the summary screen. If the data is correct, mark the statements if required and complete the step of providing data to be verified.

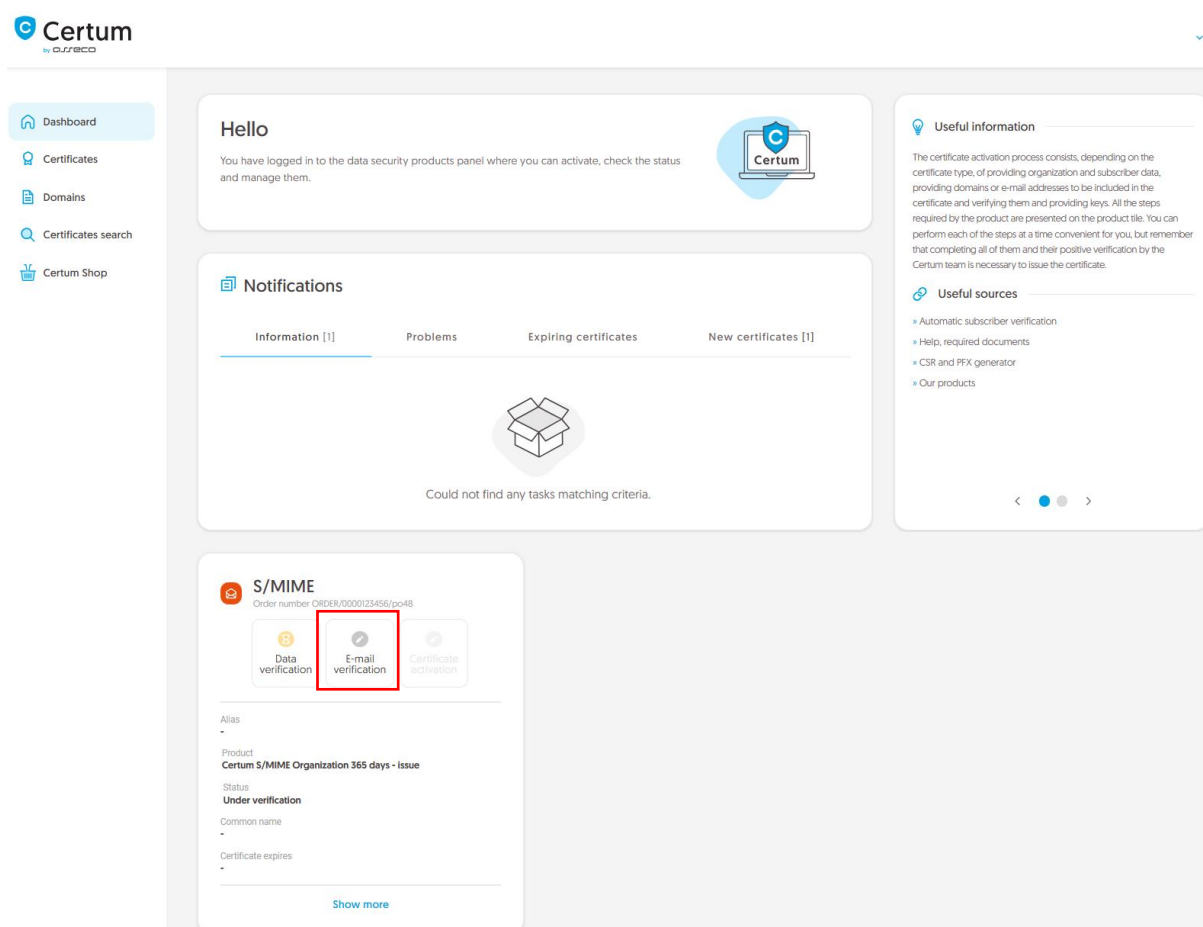
The success screen will inform you that the data have been saved for verification. Certum will verify it. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details.



When the data to be verified is saved, you can proceed to the next step which providing an e-mail.

E-mail verification step

You will be able to start the e-mail verification step from **Dashboard**, using **E-mail verification** option:



or similar to the **Data verification** step: from the **Certificates** list – choose the certificate you want to activate and use **Provide e-mail address** option.

In this step, you provide the e-mail to be included in the certificate.

Provide the e-mail address to include in the certificate and proceed.

The screenshot shows the Certum by CjSRECO web interface. On the left is a sidebar menu with icons and labels for 'Dashboard', 'Certificates', 'Domains', 'Certificates search', and 'Certum Shop'. The main content area has a header with the Certum logo and a user profile icon labeled 'P'. Below the header is a progress bar with two steps: 'E-mail data' (active, marked with a blue circle and number 1) and 'Summary' (inactive, marked with a grey circle). The main content area is titled 'Provide an e-mail address' and contains a sub-header: 'Provide an e-mail address which you want to include in the certificate. It will require a verification of the control over it.' Below this is a text input field labeled 'E-MAIL ADDRESS*' with a placeholder text 'Provide an e-mail address'. At the bottom right of the form is a blue button labeled 'Next'.

Check provided data on the summary screen. If the data is correct, complete the e-mail verification step.

The success screen will inform you that the e-mail address has been saved. Verify the access to it or if the data to be verified and the e-mail address are both verified, 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, you will choose the Common name and the fields you want to include in the certificate and generate key pair. Some fields are required and cannot be unmarked.

Choose the Common name and the fields to the certificate.

Certum
by SURECO

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.

Certum S/MIME Organization 365 days - issue

☒ E-mail address [E]:
yourcompany@yourdomain.com

☒ Common name:
Please choose Common name

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

For S/MIME certificates, the available key generation methods are:

- **CSR** – certificate signing request, generated by a generator, e.g. [Certum Tools](#) or by the application/server where the certificate will be installed
- **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.

The screenshot shows the Certum web interface. On the left is a sidebar with navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area has a progress bar at the top with four steps: Certificate data (checked), Generation method (active, marked with a '2'), Key pair generation, and Summary. Below the progress bar is a white box titled 'Key pair generation method'. Inside this box, there is a paragraph explaining that the user should choose a key generation method, noting that the CSR method requires a CSR generated with Certum Tools or by the user, and that Certum SignService allows storing keys on a cryptographic card. Below this text are two radio button options: 'CSR' (which is selected) and 'Generating key pair on card'. At the bottom of the white box are two buttons: 'Back' and 'Next'.

Certum
by aureco

Dashboard
Certificates
Domains
Certificates search
Certum Shop

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

Key pair generation method

Choose one of the key generation methods available below. CSR method requires to provide CSR generated with Certum Tools app or by your own. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card.

Key pair generation method






☒ CSR ☐ Generating key pair on card





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

CSR method

Once you have selected CSR method, you can proceed to submit your CSR. At this stage you will be able to download the [Certum Tools](#) application to generate a CSR or provide your own.

After proceeding, paste your CSR. After pasting the CSR, it will be verified whether it is correct. If a CSR error occurs, it will be indicated in the error message.

-  Dashboard
-  Certificates
-  Domains
-  Certificates search
-  Certum Shop

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

CSR

Enter Certificate Signing Request [CSR] or use the Certum Tools application to generate new CSR.

```
Ft08LL08yLqdIruyl12WjCxHIDcmM4c3/Kzuau3J4CNrMPoMCfEi4BjAaZEirBo5
oCeTFy4XK7dukV4clQn6dfn7xIOmsD1Uhbrc+tZMB1M29X1Rt3jrf802XA4g3Jhm
rOKjq0IT3yePoScwn86HKr2L6PrR8oH0UCIPnV/rYIsTyQh81bnnb5YWBBFxiU5j
3boknaXulMuHk+DL7V1L2t3PeH4QC82GmluxKi3UaltvhLaxWJW/w5bh2kFTMa8G
eo53bJvt7HFjc85xHA7jRMduu9SMggI2FkvHKQvrlXcCAwEAATANBgkqhkiG9w0B
AQsFAAOCAQEACjtc1kAhHwITVF7E41/3PQZ19D12Bnv5tkMuYD1Kzcw1LkbG4cru
gvEYXjYiUt2B9BC8OKBGeIpBCaEwWOL9rpZ6m8uq+Y2X53BpupxhGG7IG8acazdV
IyUIqo+6svL79lnr4EFX6bX2zfEIAROX8M+Xg880D+YbvcHHECETRWdlud4Sa1/A
ph7e1E5ggHYyatVyLgdL5CCWt7OK9aanPtyNKiNINvAvVsP8aYQMjptZhYXzBohe
6P8DUbQQ51XOG6Bq57EGpCf1IXjwHLGQnE#4VACwQxk70Nw0sTmPHj/HP06s4mRr
eegIXyvS9JRnlAa27o71UbFoyFASsc/zv==
-----END CERTIFICATE REQUEST-----
```

 Correct

 [Download Certum Tools app](#)

[Back](#)

[Next](#)



Remember to save the private key if you generated a CSR using the generator. You will need it to install the certificate once it is issued.

Providing the correct CSR you go to the [summary](#).

Generating key pair on a cryptographic card

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

The screenshot shows the Certum web interface. On the left is a sidebar with navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area features a progress bar at the top with four steps: Certificate data (completed), Generation method (active, step 2), Key pair generation, and Summary. Below the progress bar is a section titled 'Key pair generation method' with a sub-header 'Key pair generation method'. It contains two radio buttons: 'CSR' and 'Generating key pair on card' (selected). Below this is a dropdown menu labeled 'KEY ALGORITHM AND KEY LENGTH' with 'RSA 2048' selected.

Certum
by ORSEC

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Certificate data 2 Key pair generation Summary

Key pair generation method

Choose one of the key generation methods available below. CSR method requires to provide CSR generated with Certum Tools app or by your own. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card.

Key pair generation method

☐ CSR ☒ Generating key pair on card

KEY ALGORITHM AND KEY LENGTH

RSA 2048

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 *o.r.r.e.c.o*

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.

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

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

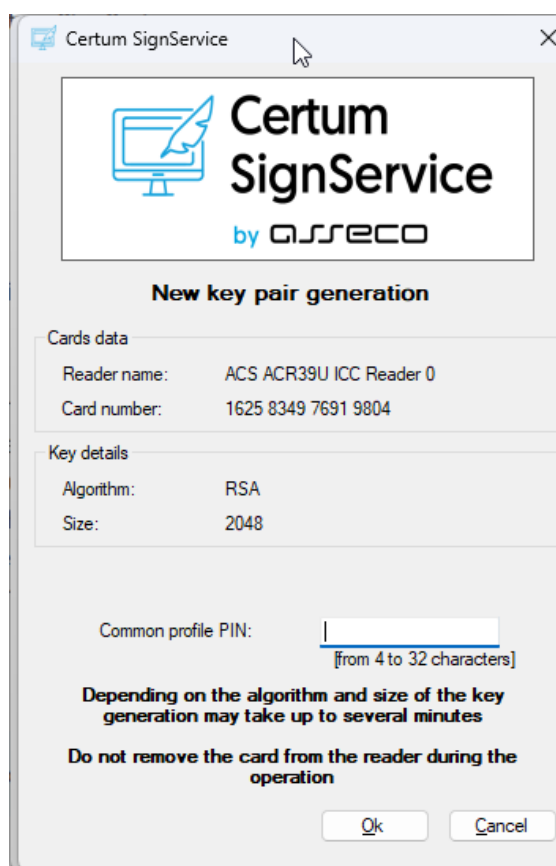
To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.

Certum
by *o.r.r.e.c.o*

Dashboard
Certificates

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

Open CertumSignService?
https://certmanager.certum.pl wants to open this application.
[Open CertumSignService](#) [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, you can proceed to the next stage of this step which is providing an e-mail.

Summary

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.

If you need a PFX file, you can use the [Certum Tools](#) generator.