

Certum S/MIME Organization certificate activation

Ver. 1.1

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step	4
E-mail verification step.....	7
CSR method.....	9
Generating key pair on the cryptographic card	10
Providing e-mail address.....	13
Certificate activation step	14

1. Product description

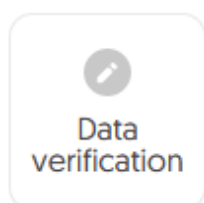
Secure your e-mail by signing and encrypting messages using Certum S/MIME certificates. Thanks to the unique signature and encryption feature, you can be sure that the e-mails you send are properly protected against their potential leakage or modification and you can assure the recipient of your identity. The Certum S/MIME certificate has a wide range of use. You can also use it to secure your Windows station using the user authentication feature on systems or applications.

2. Certificate activation

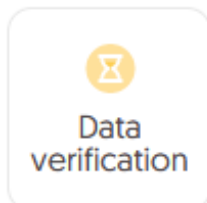
You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **Data verification** – providing organization's data and the verification
- **E-mail verification** – key pair generation, providing an e-mail and the verification
- **Certificate activation** – choosing the fields to include in the certificate and submit to issue.

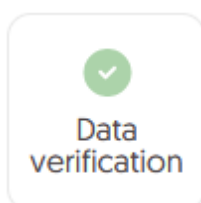
As the activation process goes, each step will go through the next statuses:



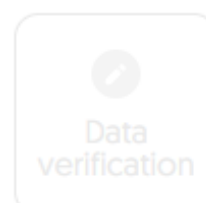
Step is awaiting to provide the data



Data is saved and waiting for verification



Verification was successful



Providing the data is not available yet

Data verification step

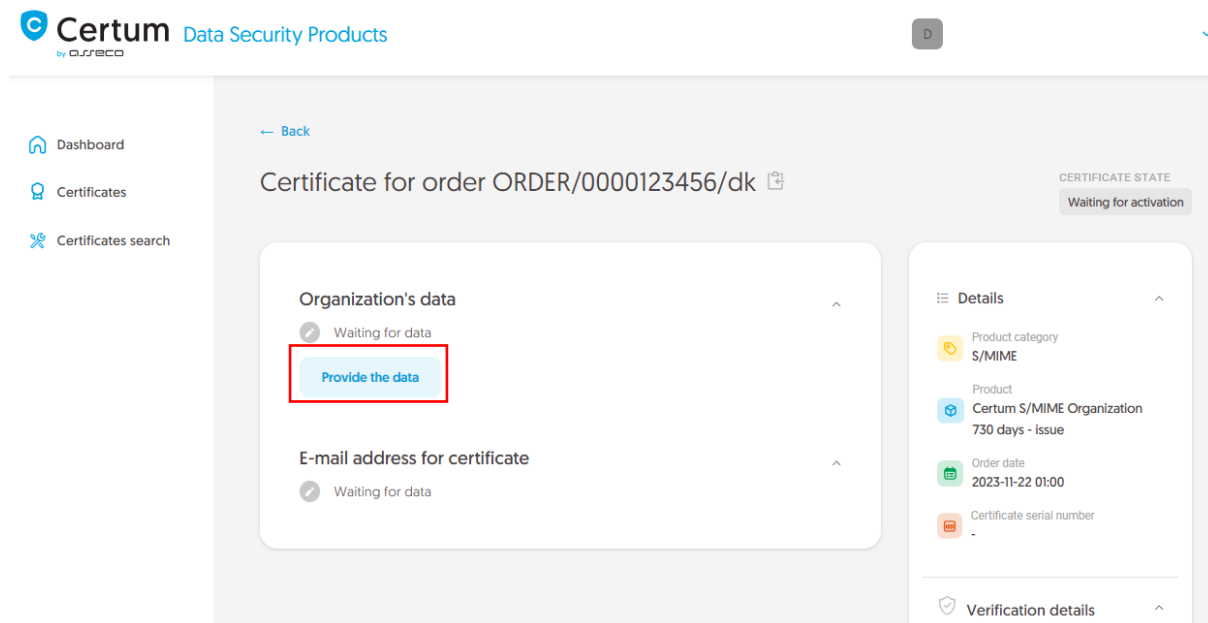
Providing data to be verified is the step in which you provide the data of the organization for which the certificate will be issued. From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

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

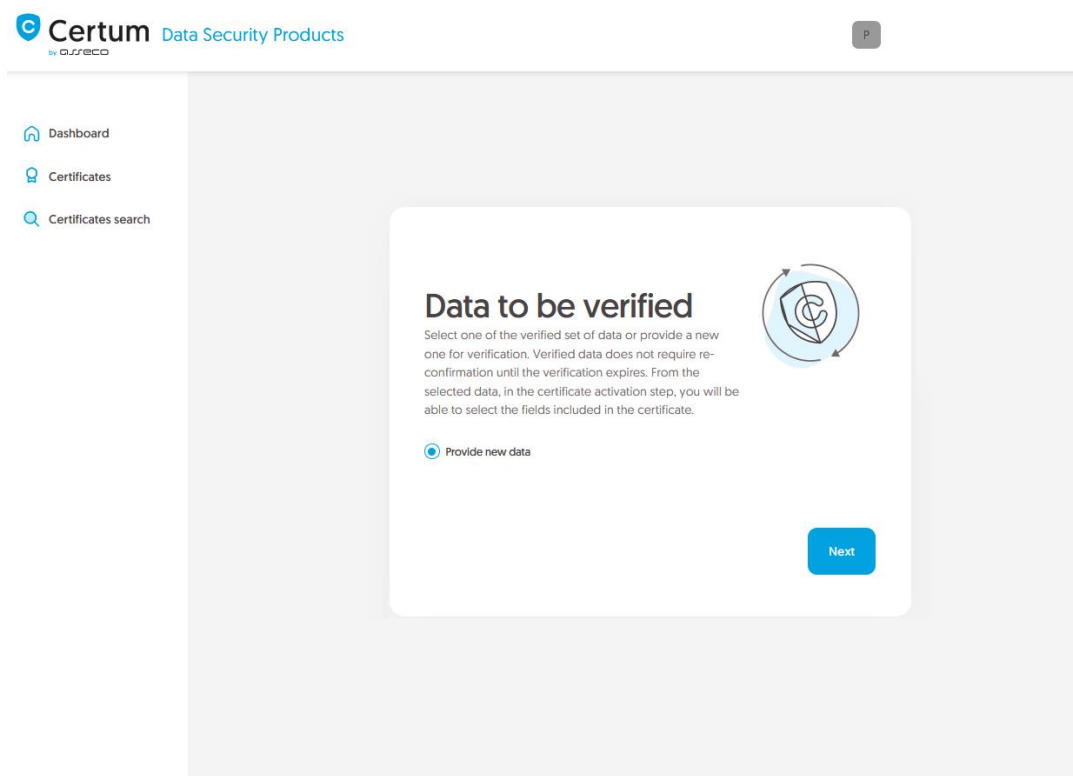
You will be able to start the data verification step from **Dashboard**, using **Data verification** option:

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' section (currently empty), and a 'Useful information' section. A 'Useful sources' section provides links to 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'. A 'S/MIME' certificate card is shown with the 'Data verification' step highlighted in red. The certificate details include the product name 'Certum S/MIME Organization 730 days - issue' and the status 'Waiting for activation'.

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



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 Data Security Products
by CEFECO

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

Headquarters of the organization

COUNTRY*

Poland

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warszawa

Verification method

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

REGISTRATION NUMBER TYPE*

KRS




REGISTRATION NUMBER IN THE REGISTRY*

12345678

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

In the next step 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.

-  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 and providing 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 will generate a key pair and provide the e-mail to be included in the certificate.

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.

- Dashboard
- Certificates
- Certificates search

Key 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 for certificates stored in the cloud will be generated automatically.

Key pair generation method

CSR Generating key pair on card

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



CSR

Enter Certificate Signing Request (CSR) or use the Certum Tools application to generate new CSR.

```
MIImLShQF9Qkr2exY8DUUCLw1GMG6140JcdDviGhRHKV+HobE9/rz2F2s0QFse/1g
Wp5y2A6eM5o6k7Mzc7oFMg2m+geTR1E1FUneG1spQaE1KDShCCFQJLFSI9vqDQ
2hQcR0d+H//d7+TgzKcXaXY7ZFCnYM66GkHPvg/U2iRADxYb4cYEESgOMhIK+NS
ceB4eI3b1Rm9QRKIEbqMGTgUVTSduv2hmWJc9wZ8oS2LcynWFMmTV/IvGnT1Hhax
1CaERLpD9UTIIsy1i0zQLrdrnNnypC561xHUBMrv9p4EDBVM3wEAATANBgkqhkiG
9w0BAQsFAAOCAQEAb50uh62GqaknkbqeIekdwtYG+FR+cEqcav5o9oohL4sCL6vH
BJdS8bog3E6mTe4aF07cwQhtKQWVEKvUA+VWgeH9Rse2NGWQM1i1nS7wBhYEPomP
y98D2iF2e2iB61QI9tA9/sQvHdLwAcORFR+QPye7qQ2E2tCdffIH/+d7YK40f2
6G1IHTzbJN/MDbnMQ07DFaRCxRu4xcvH+J/cSUGMVi12YBVk7D1JgxqgSATLSLo
f7E1ybvHAjNB06EKfAdCd8Gyh5LT8yLN3atdKvQK09g3f8NeFopfe2Icx3/BR2a
FtDSR7yzEynjCj2MA2Np10qFvrxYTAyTGhzX8v==
-----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 and proceeding will allow you to provide e-mail to include in the certificate.

Generating key pair on a cryptographic card

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. 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 for certificates stored in the cloud will be generated automatically.

Key pair generation method

CSR Generating key pair on card

KEY ALGORITHM AND KEY LENGTH

RSA 2048

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](#).

Certum Data Security Products
by GJRECO

Dashboard
Certificates
Certificates search

1 Key pair generation E-mail data 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.
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.

Certum Data Security Products
by GJRECO

Dashboard
Certificates
Certificates search

Allow this site to open the certumkoalaservice link with CertumSignService?

[Choose a different application.](#)

Always allow https://100.101.10.90:4300 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, you can proceed to the next stage of this step which is providing an e-mail.

Providing e-mail address

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

Provide an e-mail address

Provide an e-mail address which you want to include in the certificate. It will require a verification of the control over it.

E-MAIL ADDRESS*

Provide an e-mail address

Next




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

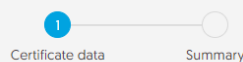
The success screen will inform you that the e-mail address has been saved. Verify the access to it. After completing e-mail verification its status should change to "verified", which will allow you to proceed to the last step, which is **Certificate activation**.

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 Common name of the and 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.

 **S/MIME**
Certum S/MIME Organization 730 days - issue

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

Common name:

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. 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.

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