

Certum S/MIME Mailbox certificate activation

Ver. 1.1

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
E-mail verification step.....	3
CSR method.....	6
Generating key pair on the cryptographic card	6
Providing e-mail address.....	9
Certificate activation step	10

1. Product description

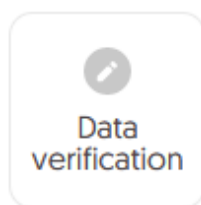
Secure your e-mail by signing and encrypting messages using Certum S/MIME certificates. Thanks to the unique signature and encryption feature, you can be sure that the e-mails you send are properly protected against their potential leakage or modification and you can assure the recipient of your identity. 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

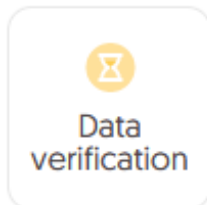
You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **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.

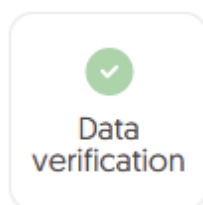
As the activation process goes, each step will go through the next statuses:



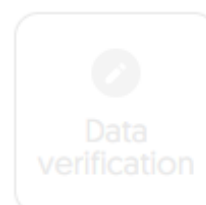
Step is awaiting to provide the data



Data is saved and waiting for verification



Verification was successful



Providing the data is not available yet

E-mail verification step

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

The screenshot displays the Certum Data Security Products dashboard. The top navigation bar includes the Certum logo, the text "Data Security Products", and a user profile icon labeled "D". The left sidebar contains three menu items: "Dashboard" (selected), "Certificates", and "Certificates search".

The main content area is divided into three sections:

- Hello:** A greeting message stating, "You have logged in to the data security products panel where you can activate, check the status and manage them." It features a Certum logo icon.
- Events:** A section with a table header containing "Events", "Product", and "Event date". Below the header is a large empty box with a box icon and the text "There is no events to display."
- Useful information:** A section with a lightbulb icon and the text: "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." Below this is a "Useful sources" section with links: "Automatic Subscriber verification", "Help, required documents", "CSR and PFX generator", and "Our products".

At the bottom of the dashboard is a detailed view for an "S/MIME" certificate. It shows the order number "ORDER/0000123456/dk" and two progress indicators: "E-mail verification" (highlighted with a red box) and "Certificate activation". Below these are the following details:

- Product: Certum S/MIME Mailbox 365 days - issue
- Status: **Waiting for activation**
- Common name: -
- Certificate expires: -

A "Show more" link is located at the bottom of this section.

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

← Back

Certificate for order ORDER/0000123456/dk

CERTIFICATE STATE
Waiting for activation

E-mail address for certificate

Waiting for data

[Provide e-mail address](#)

Details

Product category
S/MIME

Product
Certum S/MIME Mailbox 365 days - issue

Order date
2023-11-22 01:00

Certificate serial number
-

Verification details

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.

CSR

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

```
MIIMXLSHQF9Qkr2exY8DUUCUv1GNG6i40JcdV1GwRHKV+HobE9/rz2F2sdQFsa/iG
Wp5y2A6aNs06k7Mzc7oFMq2m+geTR1E1FUneG1spQqaF1KDShCCFQJLFFSI9vqDQ
2hQcR0dt+h//d7+TgzKoXaKY7ZFCnY666KHFWg/U2iRADxYb4yYEDSgQmHIX+NS
ceB4zI3b1Rm9QRKIEBqMGTgUVTSDuv2nmWJr9wZ8oS21cynWFlmTV/IvGnT1HMax
1CaERLpD9UITLy1iOzQLrdnlnhnpC61xHUBMtrvSp4EDBYMCwAAATANBgkqhkiG
9w0BAQsFAAOCAQEAb50uh6ZGqaknkbqEiekdwtYG+FR+cEqav5o9oohL4sCL6vH
BjdS8bog3E6mTe4aF07cwQhtKDQNVKvUa+VVgH9Ra2NGWQM1iInS7wBhYEPomP
yG8D2iF2e2iBG1QI9eA9/aQvKH4LwAcOR0FKR+QpYe7qQ2E2zCdFTH/+d7YX40F2
6G1IHTzbJN/M0bN0Q07DFaRCaRu4xcvH+J/ceSUGMVi.i2YBVW7D1JgXqg5ATLSLo
f7E1ybvHAjNB06EKfadCdsGyh5LTSyLN3atdhXvQK09g3f8NefopfaZ2Icx3/BRZa
FtDR7yzEynjCjZMR2Mp10qFvrxYTAyTGhaX8w==
-----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 http://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

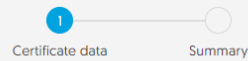
Check provided data on the summary screen. If the data is correct, complete the e-mail verification step.

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.

-  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 Mailbox 365 days - issue
- E-mail address [E]:
joedoe@yourdomain.com
- Common name:
joedoe@yourdomain.com

Next, 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.