



Certum S/MIME Individual 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

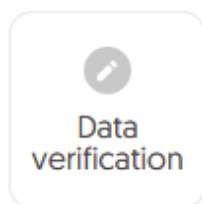
Secure your e-mail by signing and encrypting messages using Certum S/MIME certificates. Thanks to the unique signature and encryption feature, you can be sure that the e-mails you send are properly protected against their potential leakage or modification and you can assure the recipient of your identity.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

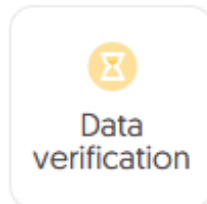
You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **Data verification** – providing the Subscriber 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.

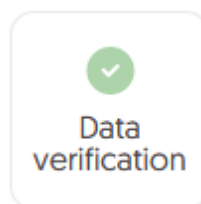
As the activation process goes, each step will go through the next statuses:



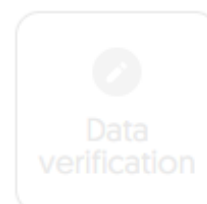
Step is awaiting to provide the data



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 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:

The screenshot displays the Certum Data Security Products dashboard. The top navigation bar includes the Certum logo and 'Data Security Products'. The main content area is divided into several sections:

- Dashboard** (selected): A sidebar menu with options for 'Dashboard', 'Certificates', and 'Certificates search'.
- 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.' accompanied by a Certum logo icon.
- Events**: A section with a table header containing 'Events', 'Product', and 'Event date'. Below the header is an empty box with the text 'There is no events to display.' and a box icon.
- Useful information**: A section providing details about the product activation process, including steps like providing organization and subscriber data, and verifying domains or email addresses.
- Useful sources**: A section with links to 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'.
- S/MIME**: A product card for 'Certum S/MIME Individual 365 days - issue'. It shows the order number 'ORDER/0000123456/dk' and three steps in a sequence: 'Data verification' (highlighted with a red box), 'E-mail verification', and 'Certificate activation'. Below the steps, it lists the product name, status 'Waiting for activation', common name, and certificate expiration date.

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

[← Back](#)Certificate for order ORDER/0000123456/dk 

CERTIFICATE STATE

Waiting for activation

Subscriber's data

Waiting for data

[Provide the data](#)**E-mail address for certificate**

Waiting for data

DetailsProduct category
S/MIMEProduct
Certum S/MIME Individual 365 days - issueOrder date
2023-11-22 01:00Certificate serial number
-

Verification details

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.

Data to be verified

Select one of the verified set of data or provide a new one for verification. Verified data does not require re-confirmation until the verification expires. From the selected data, in the certificate activation step, you will be able to select the fields included in the certificate.

 Provide new data
[Next](#)

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.

Certum Data Security Products
by **ORFECO**

Dashboard
Certificates
Certificates search

Subscriber Summary

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 selecting the 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 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:

Certum Data Security Products

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

There is no events to display.

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

S/MIME
Order number ORDER/0000123456/dk

Data verification E-mail verification Certificate activation

Product
Certum S/MIME Individual 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 **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.

```
MIImLShQF9Qkr2exY8DUUCLw1GMG6140JcdDviGwRHKV+HobE9/rz2F2s0Qfse/1g
Wp5y2A6eM5o6k7Mzc7oFMg2m+geTR1E1FUneG1spQaE1KDShOCfQJLFSI9wqDQ
2hQcR0d+H//d7+TgzKcXaXY7ZFCnYM66GkHPvg/U2iRADxYb4cYEESgOMhIK+NS
ceB4eI3b1Rm9QRKIEbqGTgUVTSduv2hmWJc9wZ8oS2LcynWFMmTV/IvGnT1Hwax
1CaERLpD9UTIy1i0zQLrdrnNnypC561xHUBMrv9p4EDBVM3wEAATANBkqhkIG
9w0B8QeFAAOCaQeAb50uh62GqaknkbqeIekdvtYG+FR+cEgcav5o9oohL4sCL6vH
BJdS8bog3E6mTe4aF07cwQhtKQWVEKvUA+VWgeH9Rse2NGWQM1i1n87wBhYEPomP
y98D2iF2e21B61QI9tA9/sQvKhGLvAcORFR+QPye7qQ2E2tCdffIH/+d7YK40f2
6G1IHTzbJN/MDbnMQ07DFaRCxRu4xcvH+J/cSUGMVi12YBVkW7D1JgxqgSATLSLo
f7E1ybvHAjNB06EKfAdCd8Gyh5LT8yLN3atdhKvQK09g3f8NeFopfze2Icx3/8R2a
FtDSR7yzEymjCj2MA2Np10qFvrxYTAyTGhzX8w==
-----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

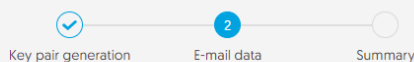
Ok Cancel

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.

- Dashboard
- Certificates
- Certificates search



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*

Next




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

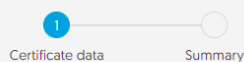
The success screen will inform you that the e-mail address has been saved. Verify the access to it. After completing e-mail verification its status should change to "verified", which will allow you to proceed to the last step, which is **Certificate activation**.

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 of the certificate.

-  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 Individual 365 days - issue

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

Common name:
Please choose Common name

Name [GN]:
Joe

Surname [SN]:
Doe

Once you have chosen the Common name of 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.