

# Certum S/MIME Mailbox certificate activation

Ver. 1.7

assecO

 **Certum**  
by assecO

## Table of contents

1. Product description .....	3
2. Certificate activation .....	3
E-mail verification step.....	4
Certificate activation step .....	5
CSR method.....	7
Generating key pair on a cryptographic card.....	8

## 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:

- **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



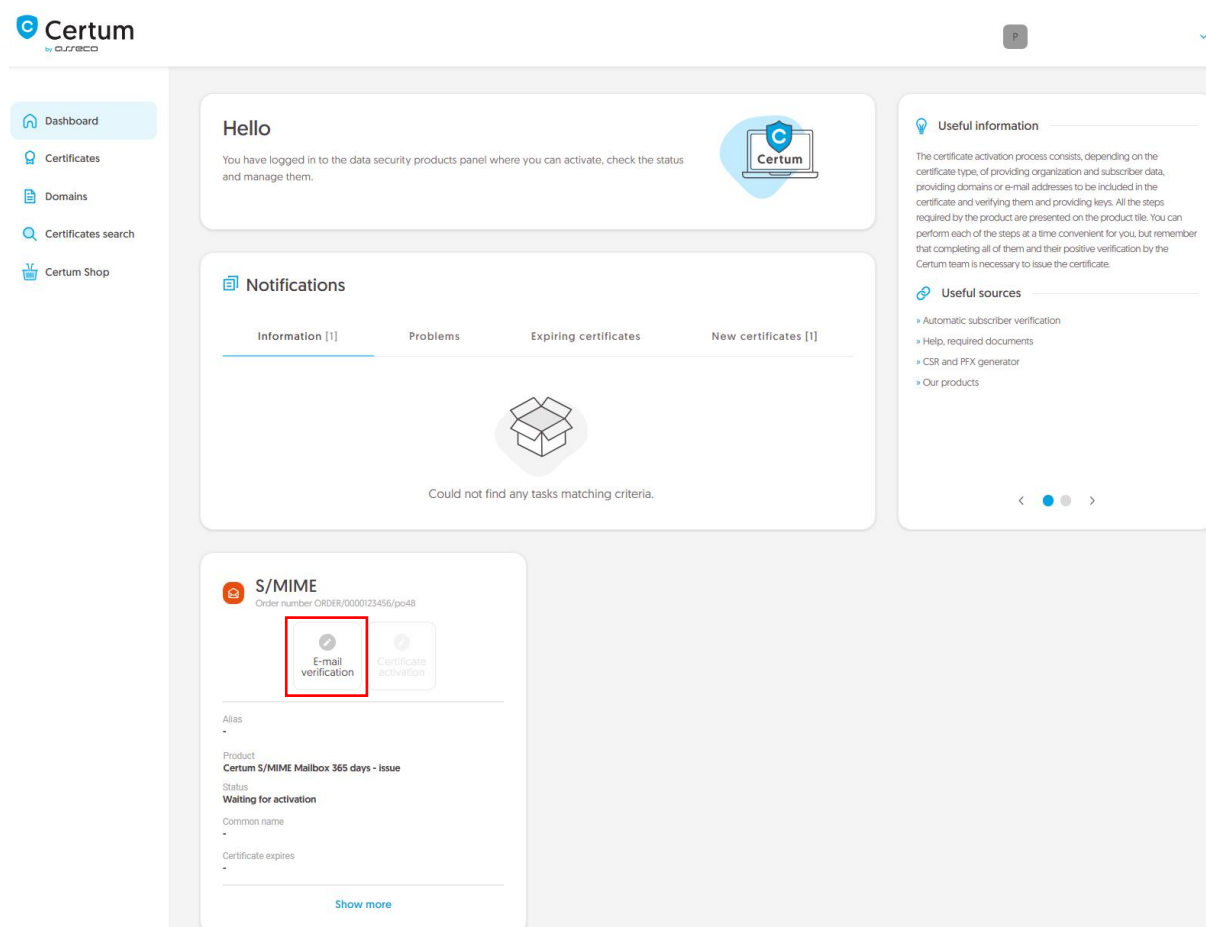
Verification  
was successful



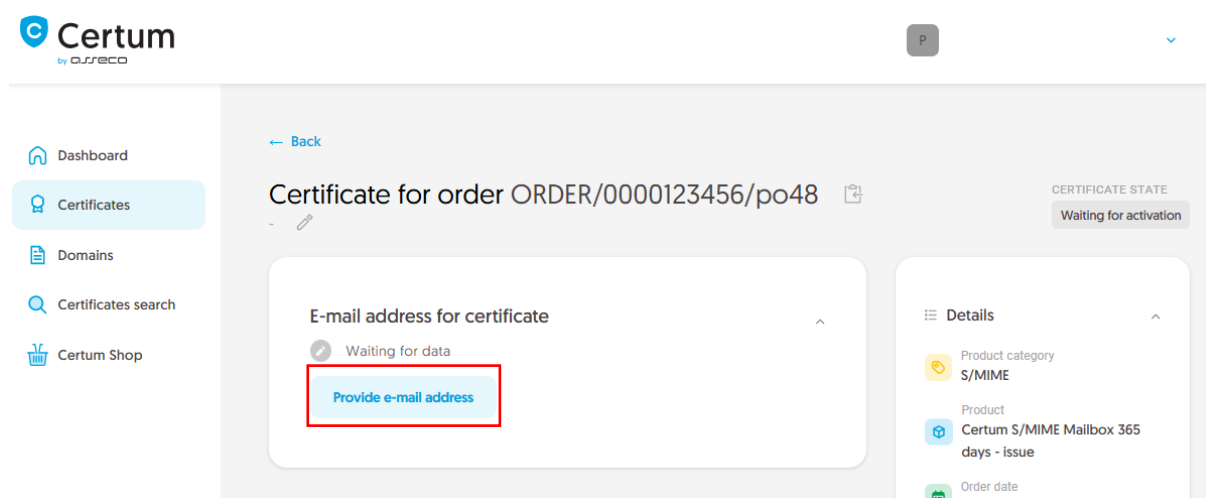
Providing the  
data is not  
available yet

## E-mail verification step

As the Certum **customer**, you will be able to start the e-mail verification step from **Dashboard**, using **E-mail verification** option:



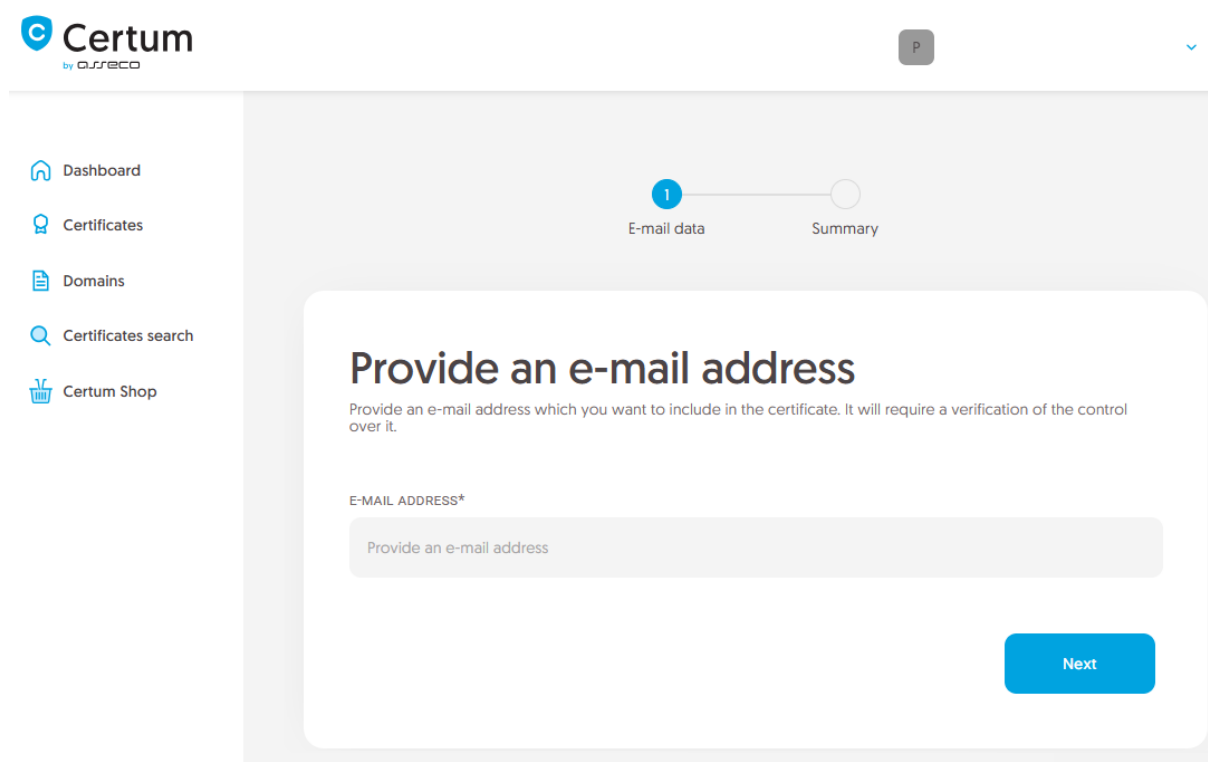
or from the **Certificates** list – choose the certificate you want to activate and use **Provide e-mail address** option.



As the **partner**, you will be able to start the e-mail 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.

In this step, you will 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 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 header with the Certum logo and a user profile icon. Below the header is a progress bar with two steps: 'E-mail data' (active, marked with a blue circle and the number 1) and 'Summary'. The main form is titled 'Provide an e-mail address' and includes a subtext: 'Provide an e-mail address which you want to include in the certificate. It will require a verification of the control over it.' There is a label 'E-MAIL ADDRESS\*' above a text input field with the placeholder 'Provide an e-mail address'. A blue 'Next' button is located at the bottom right of the form.

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 you will check the fields to be included in the certificate and generate key pair.

**Certum**  
byjureco

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.

**S/MIME**  
Certum S/MIME Mailbox 365 days - issue

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

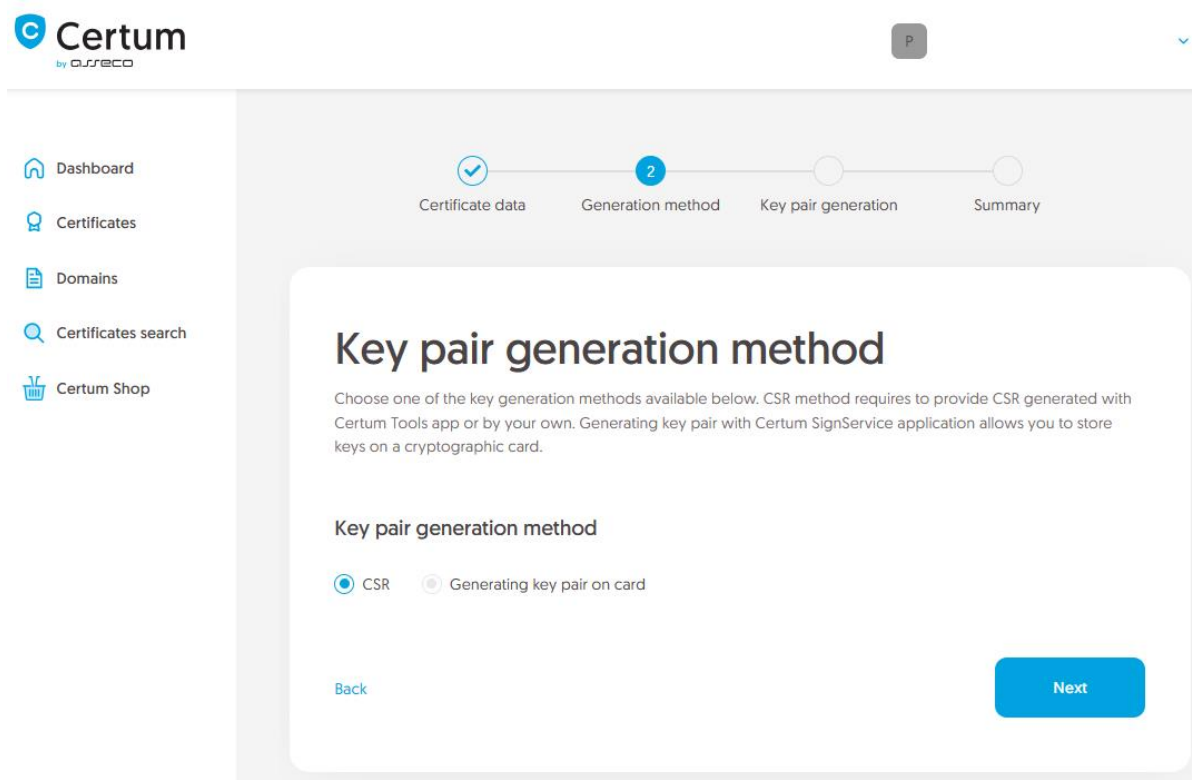
☒ Common name:  
joedoe@yourdomain.com

Once you have checked the chosen data, 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 displays 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 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 paragraph explaining the choice of generation methods. Two radio buttons are present: 'CSR' (selected) and 'Generating key pair on card'. At the bottom of the form are 'Back' and 'Next' buttons.

**Certum**  
by *ujfeco*

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.

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, Generation method, Key pair generation (highlighted with a blue circle and the number 3), and Summary. Below the progress bar, the 'CSR' section is active. It contains the text: 'Enter Certificate Signing Request [CSR] or use the Certum Tools application to generate new CSR.' Below this text is a green box containing a long, multi-line base64-encoded string representing a CSR. At the bottom right of the green box is a green checkmark icon and the word 'Correct'.



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 will allow you to 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 by DRSKO 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, the title 'Key pair generation method' is displayed. A text block explains that users should choose a key generation method, noting that the CSR method requires a CSR generated with Certum Tools or manually, while the Certum SignService application allows storing keys on a cryptographic card. Two radio buttons are present: 'CSR' (unselected) and 'Generating key pair on card' (selected). Below this, a dropdown menu labeled 'KEY ALGORITHM AND KEY LENGTH' is set to '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](#).

## 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.

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 summary.

### 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.