

Certum S/MIME Mailbox certificate activation

Ver. 1.6

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
E-mail verification step.....	4
Certificate activation step	6
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



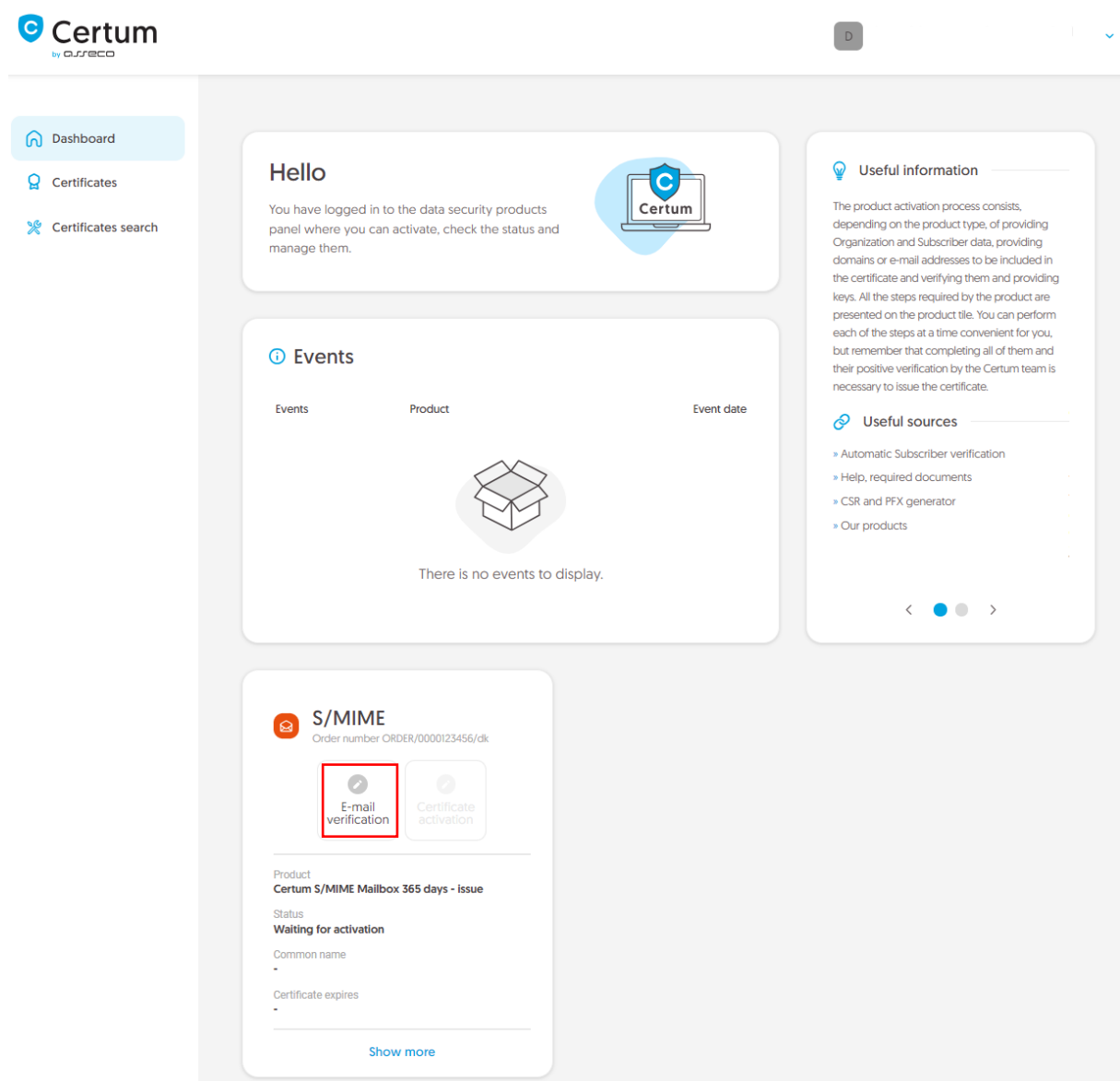
Verification
was successful



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:



The screenshot displays the Certum dashboard interface. On the left, a navigation menu includes 'Dashboard', 'Certificates', and 'Certificates search'. The main content area is divided into several 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 providing details about the product activation process, including steps like providing Organization and Subscriber data, and verifying domains or e-mail addresses. It also lists 'Useful sources' such as 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'.
- S/MIME:** A section for a specific certificate with the order number 'ORDER/0000123456/dk'. It contains two buttons: 'E-mail verification' (highlighted with a red box) and 'Certificate activation'. Below the buttons, the product is identified as 'Certum S/MIME Mailbox 365 days - issue', and the status is 'Waiting for activation'. Other fields like 'Common name' and 'Certificate expires' are currently empty.

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

The screenshot shows the Certum dashboard interface. On the left is a navigation menu with 'Dashboard', 'Certificates', and 'Certificates search'. The main content area is titled 'Certificate for order ORDER/0000123456/dk' and has a 'CERTIFICATE STATE' of 'Waiting for activation'. A section titled 'E-mail address for certificate' contains a 'Waiting for data' indicator and a blue button labeled 'Provide e-mail address' which is highlighted with a red rectangular box. To the right, a 'Details' panel lists: Product category S/MIME, Product Certum S/MIME Mailbox 365 days - issue, Order date 2023-11-22 01:00, and Certificate serial number. A 'Verification details' section is partially visible at the bottom.

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 'Key pair generation method' screen in the Certum dashboard. At the top, a progress bar shows four steps: 'Certificate data' (completed), 'Generation method' (current step, marked with a '2'), 'Key pair generation', and 'Summary'. The main content area has the heading 'Key pair generation method' and a sub-heading 'Key pair generation method'. Below this, there are two radio button options: 'CSR' (which is selected) and 'Generating key pair on card'. At the bottom left is a 'Back' link, and at the bottom right is a blue 'Next' button.

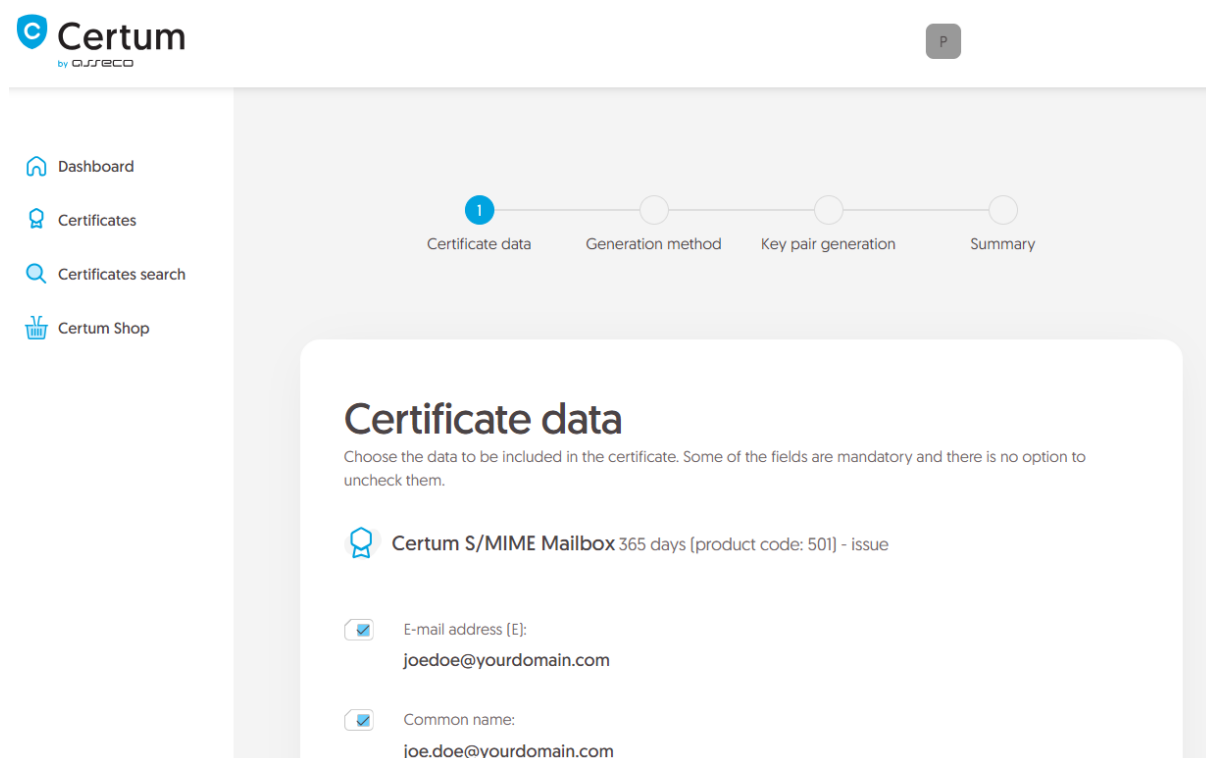
Check provided data on the summary screen. If the data is correct, complete the e-mail verification step.

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.



The screenshot shows the Certum dashboard interface. On the left is a navigation menu with 'Dashboard', 'Certificates', 'Certificates search', and 'Certum Shop'. The main content area features a progress bar with four steps: 'Certificate data' (active, marked with a '1'), 'Generation method', 'Key pair generation', and 'Summary'. Below the progress bar is a 'Certificate data' form. The form title is 'Certificate data' and includes a note: 'Choose the data to be included in the certificate. Some of the fields are mandatory and there is no option to uncheck them.' The form shows a selected certificate: 'Certum S/MIME Mailbox 365 days [product code: 501] - issue'. Two fields are checked: 'E-mail address [E]: joedoe@yourdomain.com' and 'Common name: joe.doe@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 shows the Certum web interface. At the top left is the Certum logo with 'by GISECO' underneath. A navigation menu on the left includes 'Dashboard', 'Certificates', 'Certificates search', and 'Certum Shop'. The main content area features a progress bar with four steps: 'Certificate data' (checked), 'Generation method' (active, highlighted with a '2'), 'Key pair generation', and 'Summary'. Below the progress bar is a white card titled 'Key pair generation method'. The card contains the following text: '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.' Below this text are two radio button options: 'CSR' (selected) and 'Generating key pair on card'. At the bottom of the card are 'Back' and 'Next' buttons.

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.

Certum
by QSR&CO

Dashboard
Certificates
Certificates search
Certum Shop

Certificate data Generation method **3** Key pair generation Summary

CSR

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

```
L19mygaEXrhonuK65zr3emh3CC5e2bivMFPeE+2wMdhgovg4TBNR3iRNt-9voB1+D
7GhYUekaIgt/pVtckenierFTmogCh8VjtNhjDrumG4Z4c3wURb8WnN57Zei1ORa
QwuOaQxIQD1lyT3WnAasEQuHgSfgHw72jgYdeofF1P6gIYHoj8BCxsT4fbaJUV
UxRtmHgG63sDe9PcegVzf9j2h6v0MM6huc2JWwFlni7BTH+gouhjj5uFxxn1Vn
B38oeuI66jzoeHqGwA8yVqHArvzhfjccyLoYEtdD29LfdAgMBhAEmDQYUkoZI
hvoNAQELBQADggEBAK3tFnYSElmo/9LEvSDuzcK0rbu+fQxPHG/Ow76GXpFMrzT2
L41YoXhf9bJC1KUyihpUaP9hrja1hgSnj5PQ3i7Z5Cn1DY+170F9dmkFX3Bh3j
/AJOnFO5CaaVprUwFy13B04IeSvf20qPnUKYIqY8K0wRwUvL0wa3T1eSQDatzj
J/yoeE+VoV3lyCoocYly+Yh1zPrHWtun1wFVvfCgICXj1lap5fj/FTJ501Wdm
342L14KCZ15NodJbQ00gSUDhhaovL6++14foH8whsFb3cHaNVd5XrHhph2BHDIVY
FdUmTF+K2FN164PIehg2WNI650zrtTI+26RQznM=
-----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 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.

Certum
by *ORSEC*

Dashboard
Certyfikaty
Wyszukiwarka certyfikatów
Sklep Certum

Wybór danych do certyfikatu Metoda generacji Generacja kluczy Podsumowanie

Wybór metody generowania kluczy

Wybierz jedną z dostępnych metod generacji pary kluczy. Metoda CSR wymaga podania CSR wygenerowanego w aplikacji Certum Tools lub samodzielnie. Generacja za pomocą aplikacji Certum SignService pozwoli zapisać klucze na karcie kryptograficznej.

Metoda generacji pary kluczy

CSR Generowanie pary kluczy na karcie

ALGORYTM KLUCZA I DŁUGOŚĆ KLUCZA

RSA 2048

Metoda CSR pozwoli uzyskać certyfikat wraz z kluczem w formie do przenoszenia i instalacji z pliku. Pamiętaj, by zapisać klucz prywatny, który wygenerowałeś wraz z CSR.

Wygenerowanie kluczy na karcie spowoduje, że wydany certyfikat zostanie zainstalowany na karcie kryptograficznej i jej podłączenie do komputera będzie wymagane zawsze, gdy certyfikat jest używany. Wspierane są tylko karty Certum.

Cofnij Kontynuuj

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 **QSR**

Dashboard
Certificates
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**

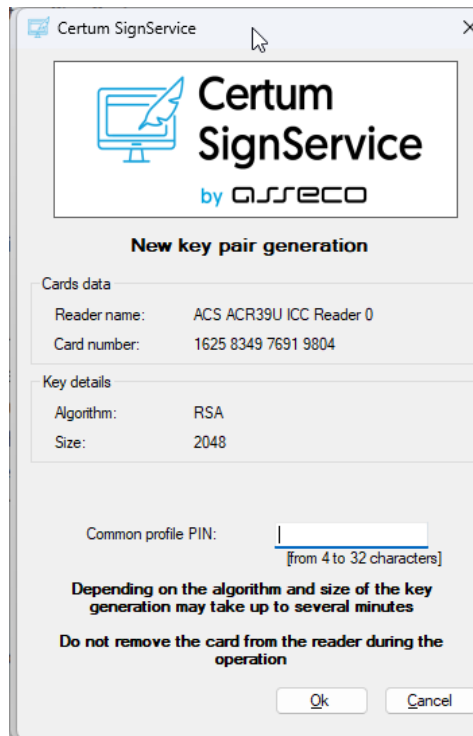
To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.

Certum
by **QSR**

Dashboard
Certificates
Certificates search

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

Choose a different application.
 Always allow <https://certmanager.test.certum.pl> to open certumkoalaservice links
Open Link **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.