

Certum S/MIME Individual certificate activation

Ver. 1.8

assecO

 **Certum**
by assecO

Table of Contents

- 1. Product description 2
- 2. Certificate activation 3
 - Data verification step 3
 - E-mail verification step..... 7
 - Certificate activation step 9
 - Summary 12

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

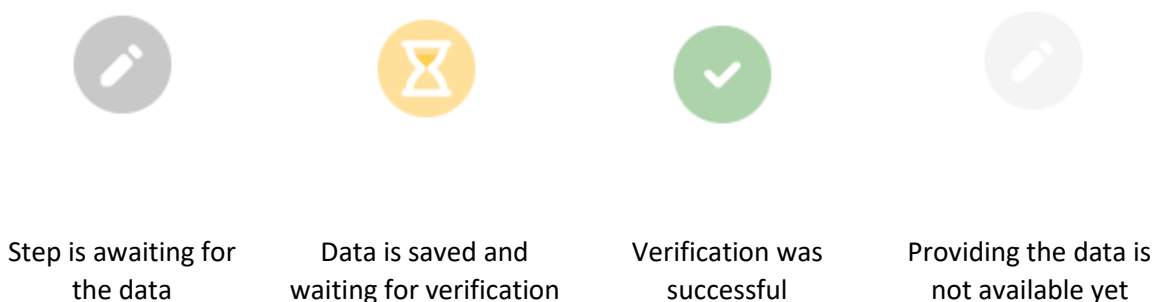
As the Certum **customer**, you will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab.

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:

- **Data verification** – providing the subscriber data and the verification
- **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:



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](#).

As the Certum **customer**, you will be able to start the data verification step from **Dashboard**, using **Data verification** option:

The screenshot shows the Certum dashboard interface. At the top, there is a navigation bar with a logo, language options (PL, EN), a notification bell, and a user profile (TT Customer). The main content area is divided into several sections:

- Dashboard:** A sidebar on the left with links to Dashboard, Certificates, Domains, Transfers, Certificate Discovery, and Certum Shop.
- Hello:** A welcome message stating, "You have logged in to the data security products panel where you can activate, check the status and manage them." It includes a Certum logo.
- Notifications:** A section with tabs for Information, Problems, Expiration, and New certificates. It displays a message: "Could not find any tasks matching criteria." with an icon of an open box.
- Useful information:** A section explaining the certificate activation process, mentioning the need for organization and subscriber data, domains or e-mail addresses, and keys. It notes that all steps are presented on the product tile and can be completed at a convenient time, but full verification by the Certum team is necessary for issuance.
- Useful sources:** A section with links to "Automatic subscriber verification", "Help, required documents", "CSR and PFX generator", and "Our products".
- S/MIME Certificate Details:** A card showing details for an S/MIME certificate. It includes the order number "ORDER/0000123456/b01" and three steps: "Data verification" (highlighted with a red box), "E-mail verification", and "Certificate activation". Below this, it lists "Alias: -", "Product: Certum S/MIME Individual 365 days - issue", and "Status: Waiting for activation".

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

The screenshot shows the detailed view of a certificate for order "ORDER/0000123456/b01". The page title is "Certificate for order ORDER/0000123456/b01" and the "CERTIFICATE STATE" is "Waiting for activation".

The main content area is divided into two sections:

- Subscriber's data:** A section with a status "Waiting for data" and a blue button labeled "Provide the data" (highlighted with a red box).
- Details:** A section showing certificate information:
 - Product category: S/MIME
 - Product: Certum S/MIME Individual 365 days - issue
 - Order date: 2025-11-27 13:35

As the **partner**, you will be able to start the data 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.

The wizard will guide you through the process of providing the data. In the first stage, choose to **Provide new 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. From the selected data, in the certificate activation step, you will be able to select the fields included in the certificate.



Provide new data

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.

1
Subscriber Summary

Subscriber data

The subscriber is a person who will be the owner of the certificate: the data of him or her or organization that he or she can represent will be available to include in the certificate. After completing this step, 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@subscriberemail.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](#)

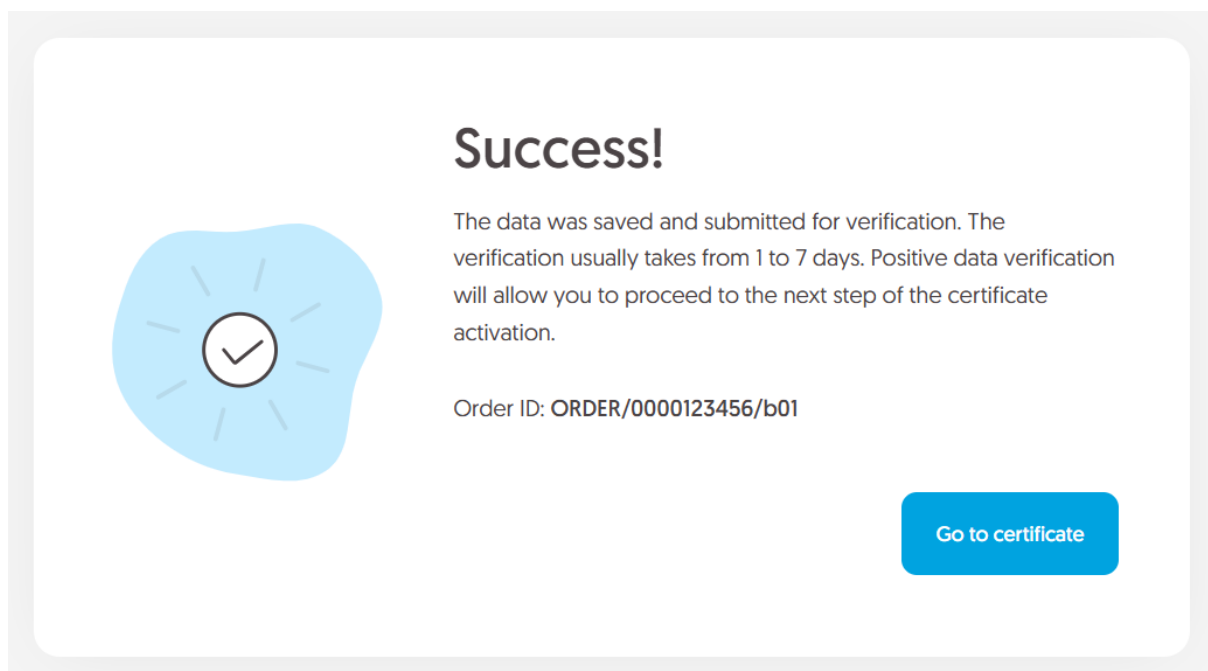
After selecting the verification method go next.

Data verification step summary

Check provided information on the summary screen. If the data is correct, mark the statements if required 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 it. 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](#).



When the data to be verified is saved, you can proceed to the next step which is providing an e-mail.

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 dashboard interface. On the left is a navigation menu with items: Dashboard, Certificates, Domains, Transfers, Certificate Discovery, and Certum Shop. The main content area is divided into several sections:

- Hello:** A welcome message stating, "You have logged in to the data security products panel where you can activate, check the status and manage them." It includes a Certum logo icon.
- Notifications:** A section with tabs for Information, Problems, Expiration, and New certificates. The Information tab is active, showing an empty state with a box icon and the text: "Could not find any tasks matching criteria."
- Useful information:** A section explaining the certificate activation process, noting that steps vary by certificate type and subscriber data. It lists steps like providing domains or e-mail addresses and keys.
- Useful sources:** A section with links to "Automatic subscriber verification", "Help, required documents", "CSR and PFX generator", and "Our products".
- S/MIME Certificate Detail:** A card for an S/MIME certificate with order number ORDER/0000123456/b01. It features three steps: "Data verification", "E-mail verification" (highlighted with a red box), and "Certificate activation". Below the steps, the status is shown as "Under verification".

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 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 a two-step process. Step 1, 'E-mail data', is active and highlighted with a blue circle containing the number '1'. Step 2, 'Summary', is shown as a grey circle. The main content area has a white background with a rounded border. It features a large heading 'Provide an e-mail address', a sub-heading 'Provide an e-mail address which you want to include in the certificate. It will require a verification of the control over it.', a label 'E-MAIL ADDRESS*', and a text input field containing 'joedoe@youremail.com'. A blue 'Next' button is positioned at the bottom right of the form area.

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 or if the data to be verified and the e-mail address are both verified, 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 choose the Common name of the certificate and generate key pair.

Choose the Common name of certificate.

The screenshot shows a progress bar at the top with four steps: 'Certificate data' (highlighted with a blue circle and the number 1), 'Generation method', 'Key pair generation', and 'Summary'. Below the progress bar, the main content area is titled 'Certificate data'. Underneath the title, there is a sub-header 'S/MIME' with a small icon, followed by the text 'Certum S/MIME Individual 365 days - issue'. Below this, there are two checked checkboxes. The first is labeled 'E-mail address (E):' and has the value 'joedoe@youremail.com' entered. The second is labeled 'Common name:' and has a dropdown menu with 'Joe Doe' selected and a hand cursor icon pointing to it.

Once you have chosen the Common name of the certificate, go to the key pair generation.

For this type of certificates, the available key generation method is CSR which means providing a certificate signing request generated by a generator, e.g. [Certum Tools](#), or by the application/server where the certificate will be installed.

The screenshot shows a four-step progress bar at the top: 'Certificate data' (checked), 'Generation method' (active, step 2), 'Key pair generation', and 'Summary'. Below the progress bar, the main heading is 'Key pair generation method'. A sub-heading reads: 'CSR method requires to provide CSR generated with Certum Tools app or by your own.' Underneath, the section is titled 'Key pair generation method' and contains a radio button labeled 'CSR' which is selected. At the bottom left is a 'Back' link, and at the bottom right is a blue 'Next' button.

CSR method

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.

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.

```
d86KieYDxTLhnO/3JNuVFv6xuW9pT38zTLVCYvjm5pA22QZhxOUqHDJKAsbu/zvC
96D0aF/wvYloff3i3C9y4FyWgajUC2Sw0WjAYzT6bFhKTM/lPOy8hqaBOoB3MsnW
CH2w2vBMYNm+1WP7r/WvzvwyD5b9EjU4ThRbz3GX5rzMqq7JgCfOdnfOC4G4iFO0
vXSKCWA64vg75/8/1plrLYI/8J82rk+PRKqgb7hRYtqWfAGPHZkJw5/itX9cQfp
gCDEix1VCVBKnIolE8KY1mWMycByGVIfy/d8AN7xxar/w7/k1eE50ExAgMBAAEw
DQYJKoZIhvcNAQELBQADggEBAJqP2fTUfXUnoHcLJiEZvT1zBTqYxyr5hRK+i54J
FfbxWWOLua0YEB70ZD1ZV+03NtF0tmzEveLtmJtdaot1uQlaTmopkQ04SnLetMHi
2hTQSJdizIB3w7wbci7PDzG/ZtnWTO3UfcM0wD7t3FwgUJXYBEvL/Z/Y3YttYrsA
NHYA7qpkNF9X1WUEsJ7LLzUVU2vRpfXIZfJVHyWjW5zDTxMqoQYk3/1ZyM/nzON7
dBCGp0CmEM8GS9wa2Cdc3a6yHmT//BykKZfU1a2MIw0+BDcxwCgZLzHmHnw640YBw
li+gfp4M9npcHi8BZ31u9jpQW/v0s1Sj3DQn0PnILKkDeHY=
-----END CERTIFICATE REQUEST-----
```

Correct

[Download Certum Tools app](#)

Remember to save the private key if you generated a CSR using the generator (e.g. Certum Tools app). You will need it to install the certificate once it is issued.

Providing the correct CSR and proceeding will display the summary screen. Check all of provided data. Mark the required statements if needed and complete certificate activation.

Summary

Go to the summary screen and check all of provided data. Mark the required statements if needed 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.

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.