



Certum S/MIME Organization certificate activation

Ver. 1.6

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step.....	4
E-mail verification step	7
Certificate activation step.....	9
CSR method	11
Generating key pair on a cryptographic card	12
Summary.....	15

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 organization's 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:



Step is
awaiting for
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 organization for which the certificate will be issued. 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 Data Security Products dashboard. The top navigation bar includes the Certum logo, the text 'Data Security Products by asreco', a user profile icon with the letter 'D', and a dropdown arrow. The left sidebar contains three menu items: 'Dashboard' (selected), 'Certificates', and 'Certificates search'. 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 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 text explaining the product activation process, including providing organization and subscriber data, domains, and email addresses, and verifying them.
- Useful sources:** A section with a link icon and a list of links: 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'.
- S/MIME:** A section for a specific certificate with the title 'S/MIME' and order number 'ORDER/0000123456/dk'. It contains three buttons: 'Data verification' (highlighted with a red box), 'E-mail verification', and 'Certificate activation'. Below the buttons, the product name is 'Certum S/MIME Organization 730 days - issue', the status is 'Waiting for activation', and there are fields for 'Common name' and 'Certificate expires', both currently empty.

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

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 **Provide the data**. In the future, it will be possible to use them to issue another certificate.

In the next stage, provide the organization's data. Here, provide the organization's details and the address of its headquarters. The data will be used to verify the existence of the organization.

Choose also how Certum will verify the existence of the organization:

- **By registration number** – Certum will search for information about the organization in the public register using the provided number
- **Attaching a document** – you will add a document confirming the establishment of the organization.

Certum Data Security Products
by QURECO

Dashboard
Certificates
Certificates search

Organization data

Provide the data to let us verify your organization existence. From this data you will be able to choose the fields to include in the certificate.

The data of the organization

ORGANIZATION*

Your company

Headquarters of the organization

COUNTRY*

Poland

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warszawa

Verification method

Search the information about the organization by registration number

Add the document to verify organization existence

REGISTRATION NUMBER TYPE*

KRS




REGISTRATION NUMBER IN THE REGISTRY*

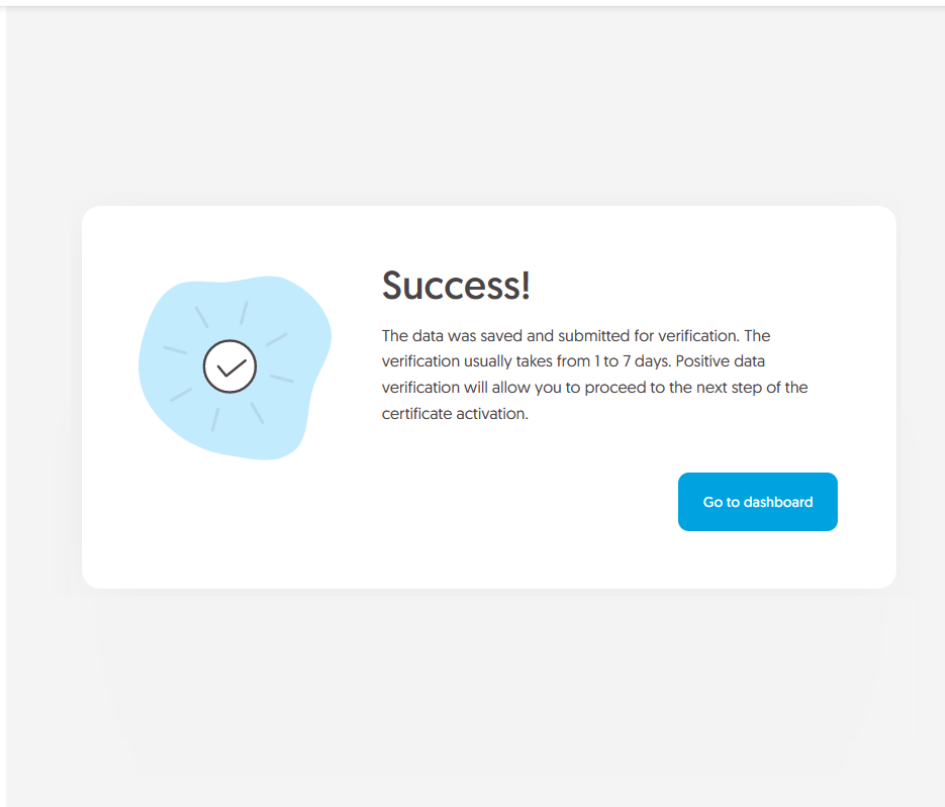
12345678

[Back](#) [Next](#)

In the next step verify 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.

-  Dashboard
-  Certificates
-  Certificates search

A screenshot of a web application interface showing a success message. The message is contained within a white rounded rectangle on a light gray background. On the left side of the message box is a blue circular icon with a white checkmark inside. To the right of the icon, the word "Success!" is written in a bold, dark font. Below this, a paragraph of text explains that the data was saved and submitted for verification, and that the verification process typically takes 1 to 7 days. It states that positive verification will allow the user to proceed to the next step of certificate activation. At the bottom right of the message box is a blue button with the text "Go to dashboard" in white.

Success!

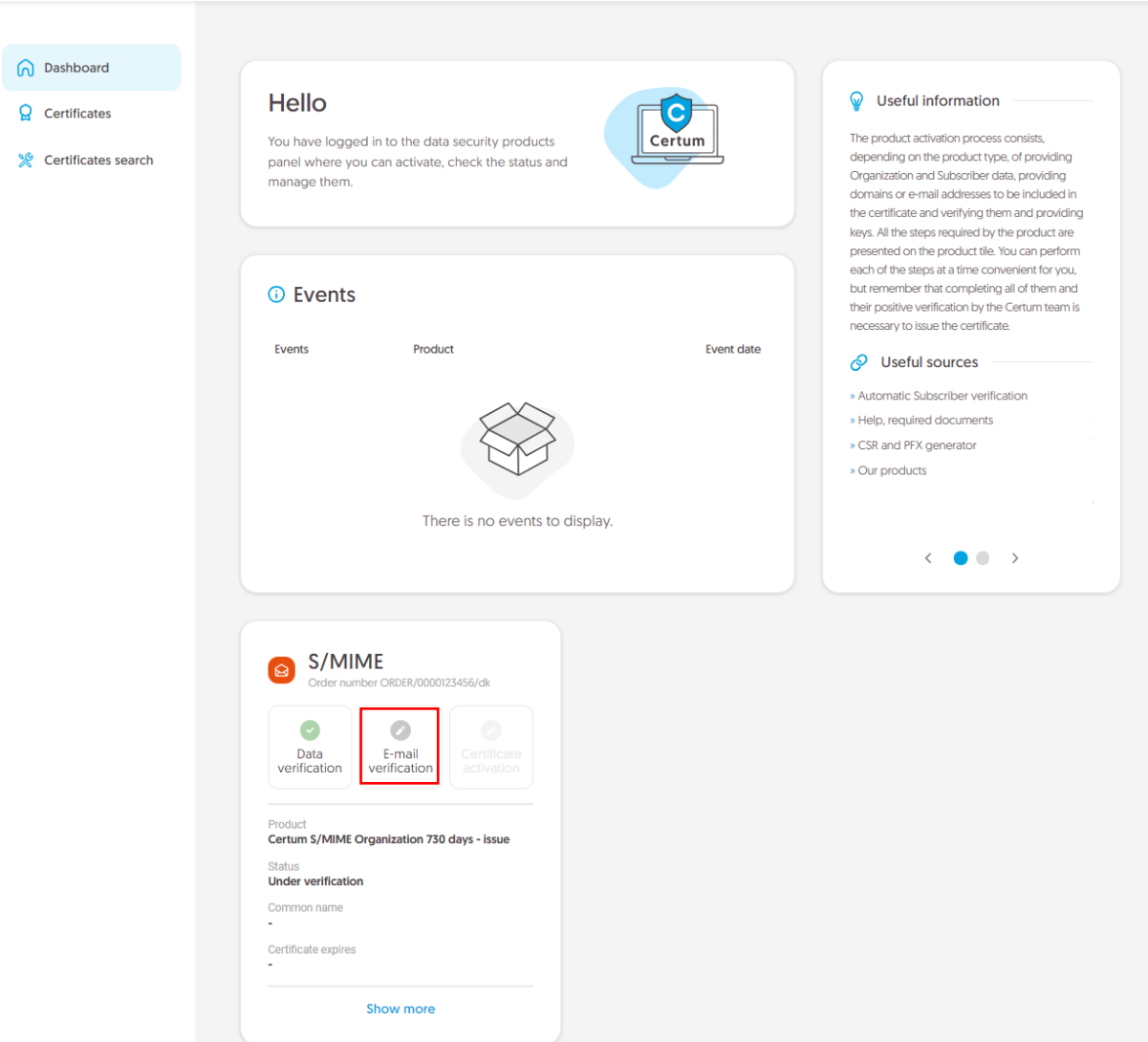
The data was saved and submitted for verification. The verification usually takes from 1 to 7 days. Positive data verification will allow you to proceed to the next step of the certificate activation.

[Go to dashboard](#)

Positive verification of the provided data will allow you to proceed to the step which 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:



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 Organization 730 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 provide the e-mail to be included in the certificate and generate a key pair.

Provide the e-mail address to include in the certificate and proceed.

Dashboard

Certificates

Certificates search

Certum Shop

1 E-mail data Summary

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.

In this step, choose the Common name the fields you want to include in the certificate and generate key pair. Some fields are required and cannot be unmarked.

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.

 Certum S/MIME Organization 365 days - issue

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

Common name:
Please choose Common name ▼

Organization [O]:
Your company

Locality [L]:
Warszawa

State or province [SP]:
mazowieckie

Once you have chosen the fields to the certificate, 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. 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' (completed), 'Generation method' (current step, marked with a '2'), 'Key pair generation', and 'Summary'. Below the progress bar, the heading 'Key pair generation method' is followed by a paragraph: '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.' Two radio button options are shown: 'CSR' (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.

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.

```
L19mygaEXrhonuDK5zr3emh3CC5e2bivMFPeE+2wMdhgovg4TBNR3iRNt-9voB1+D
7GhYUekaIgt/pVtckenierFTmogChBVjtNhjDrumGf4Z4c3wURb8WnN57zei1ORa
QwuOaQxIQD1lyT3WMAaEQHhSfgHw72jgYdeofF1P6gIYHoj8BCxsT4fbaJUV
UxRtmHgG3sDe9PcegVzF9j2h86v0M6huc2JWAFlni7BTH+gouhjj5uFxxn1Vn
B3SoeuIge6jzoeHqGwA8yVqHArvzrfjccyGloYEtD29LfdAgMBhAEwDQYUkoZI
hvoNAQELBQADggEBAK3tFnYSElmo/9LEvSDuzcKOrbu+fQxPHG/Ow76GXpFMrzT2
L41YoXhf9bJC1KUyPyhUaP9hrja1hgSnj5PQ3i7Z5Cn1DY+170F9dmkFX3Bh3j
/AJOnPO5CaaVprUwFy13B04IeSvf20qPnUKYIqY8K0wRwUvL0wa3T1eSQDatzj
J/yoEe+VoV3lyCoocYly+Yh1zPrHWtun1wFVvfCgICXj1lap5fj/FTJ501Wdm
342L14KCZ15NodJbQ00qSUdhhaovL6++14fo8WshPb3cHaNVd5XrHhph2BHDIVY
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 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 web interface for key pair generation. The top left features the Certum logo and a navigation menu with links to Dashboard, Certificates, Certificates search, and Certum Shop. The top right has a user profile icon labeled 'P'. A progress bar at the top indicates four steps: Certificate data, Generation method, Key pair generation (the current step, marked with a '3'), and Summary. The main content area is titled 'Key pair generation' and includes instructions to follow the steps below. A link to 'Download Certum SignService app' is provided. An 8-step list details the process: 1. Download and install the Certum SignService application. 2. Download and install the proCertum CardManager application if not installed or needs updating. 3. Connect the card reader to the computer and insert the card. 4. Open the proCertum CardManager application and check if the common profile of the card is initialized. The application will ask to set PIN and PUK codes if needed. 5. Start the key pair generation process using the 'Generate key pair' button. 6. Accept the browser prompt about running the Certum SignService application. 7. When the Certum SignService window appears, enter the PIN code for the common profile of your card. 8. Wait until the key pair is generated, which may take several minutes. A light blue information box states: 'When the key pair is generated, next window of the wizard will appear.' At the bottom left is a 'Back' link, and at the bottom right is a yellow 'Generate key pair' button.

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](#)

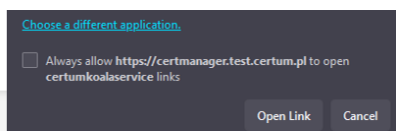
1. Download and install the **Certum SignService** application.
2. Download and install the **proCertum CardManager** application if you don't have it installed or it requires updating.
3. Connect the card reader to the computer and insert the card.
4. Open the proCertum CardManager application and check 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.

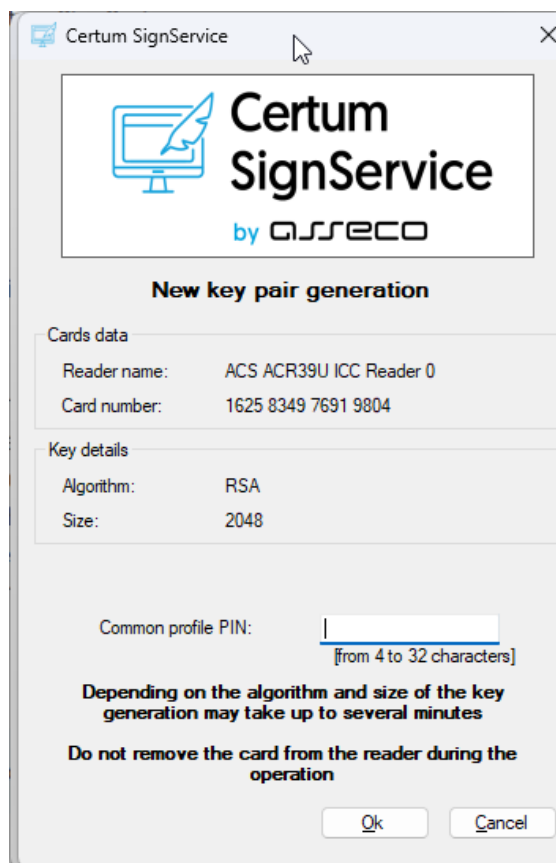
i When the key pair is generated, next window of the wizard will appear.

[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.





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.

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.