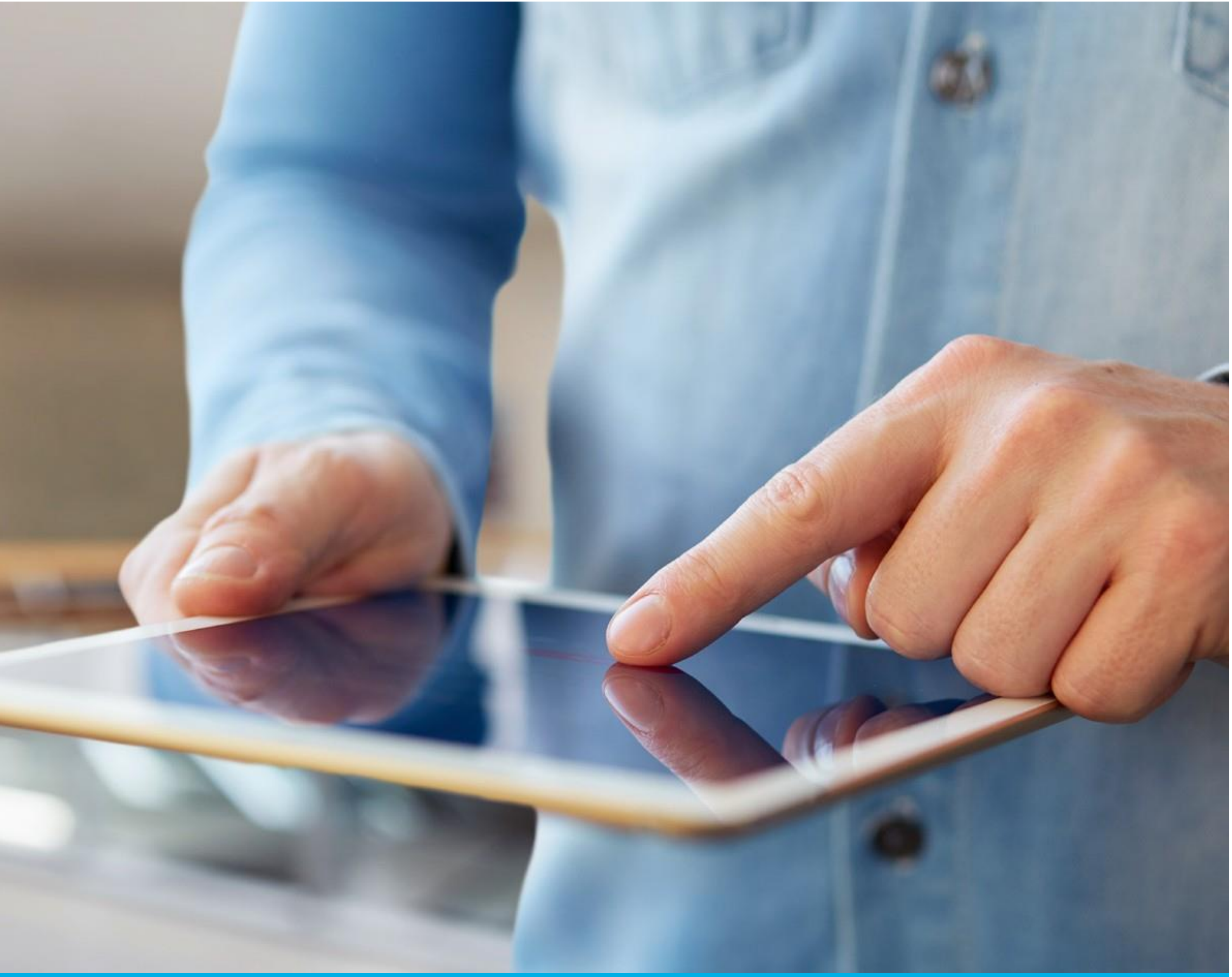


Certum S/MIME Individual certificate activation

Ver. 1.6

Table of contents

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:

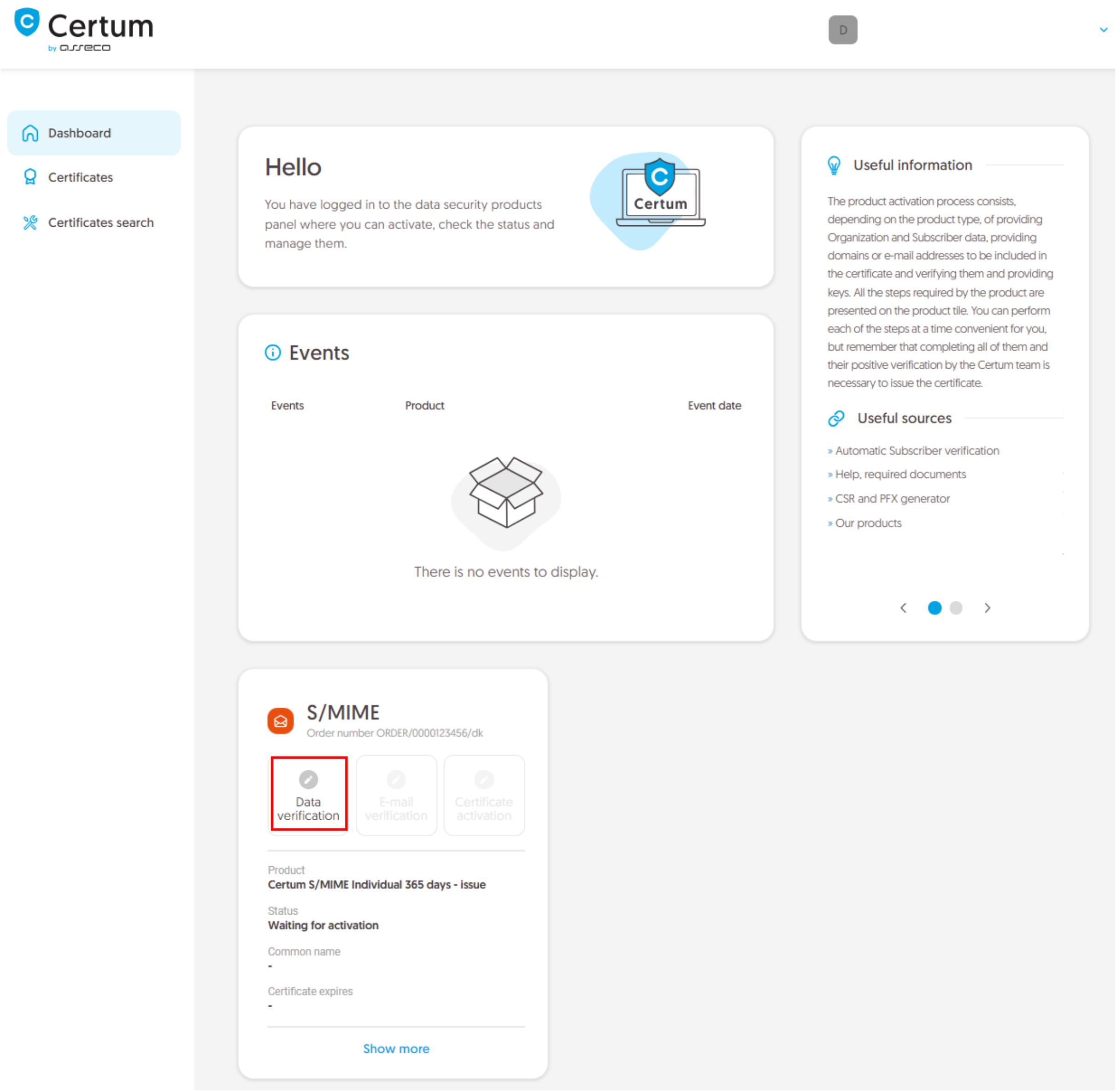
✎	⧗	✓	✎
Step is awaiting to provide the data	Data is saved and waiting for verification	Verification was successful	Providing the data is not available yet

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.

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



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

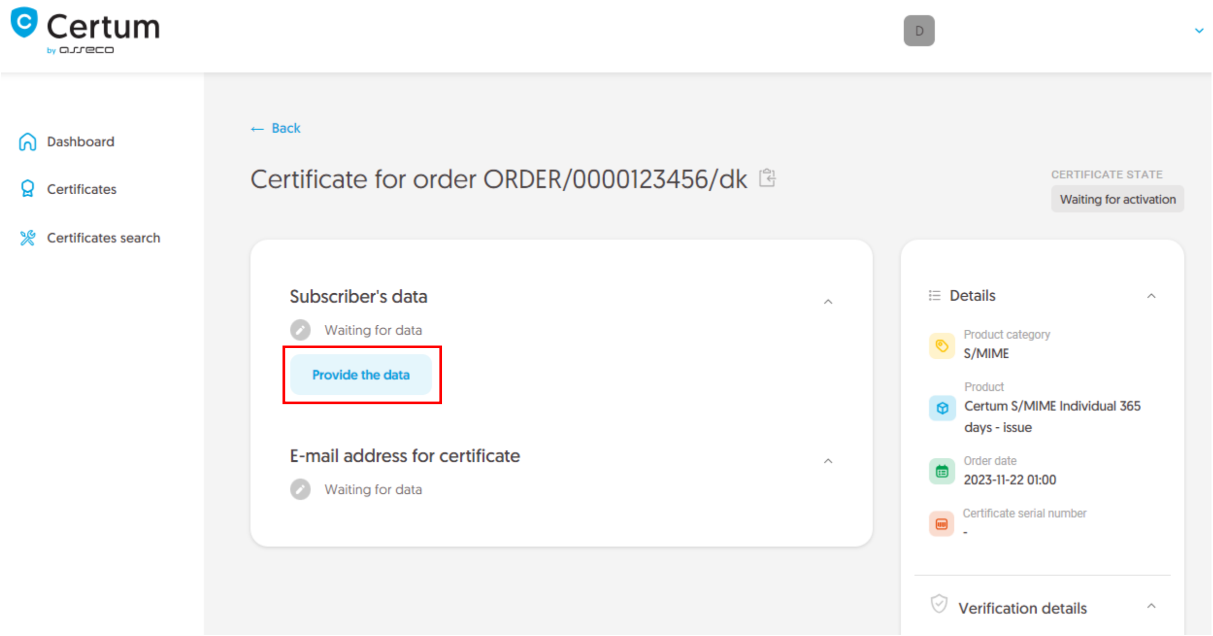
Product
Certum S/MIME Individual 365 days - issue

Status
Waiting for activation

Common name
-

Certificate expires
-

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



Certum by asseco

D

Dashboard

Certificates

Certificates search

← 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

Details

Product category

S/MIME

Product

Certum S/MIME Individual 365 days - issue

Order date

2023-11-22 01:00

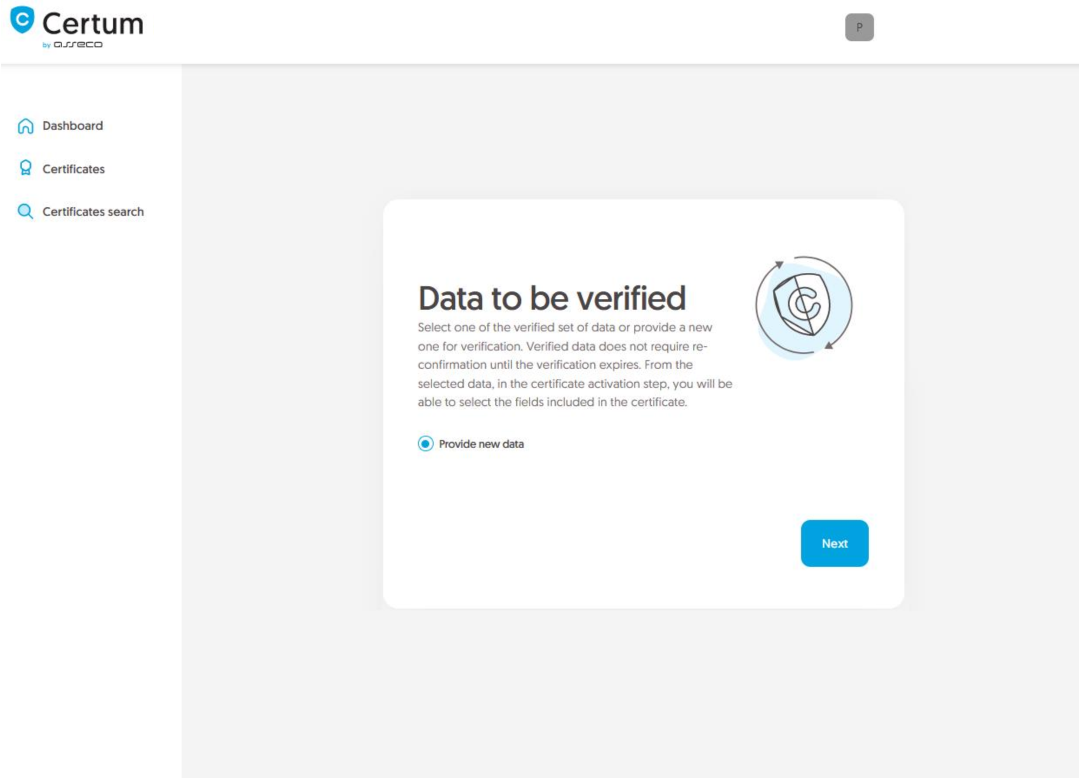
Certificate serial number

-

Verification details

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.



Certum by asseco

P

Dashboard

Certificates

Certificates search

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.

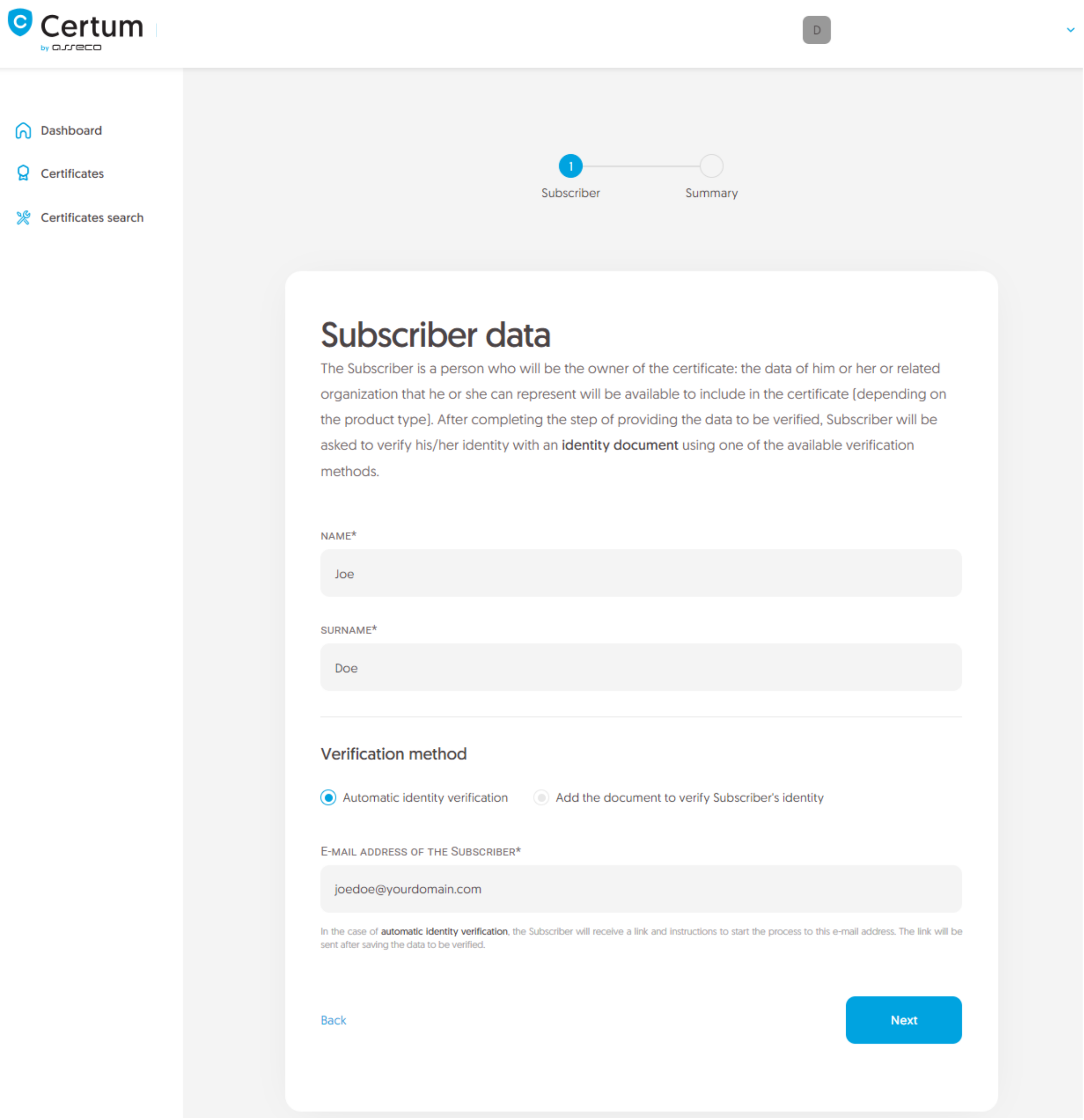
● Provide new data

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.



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

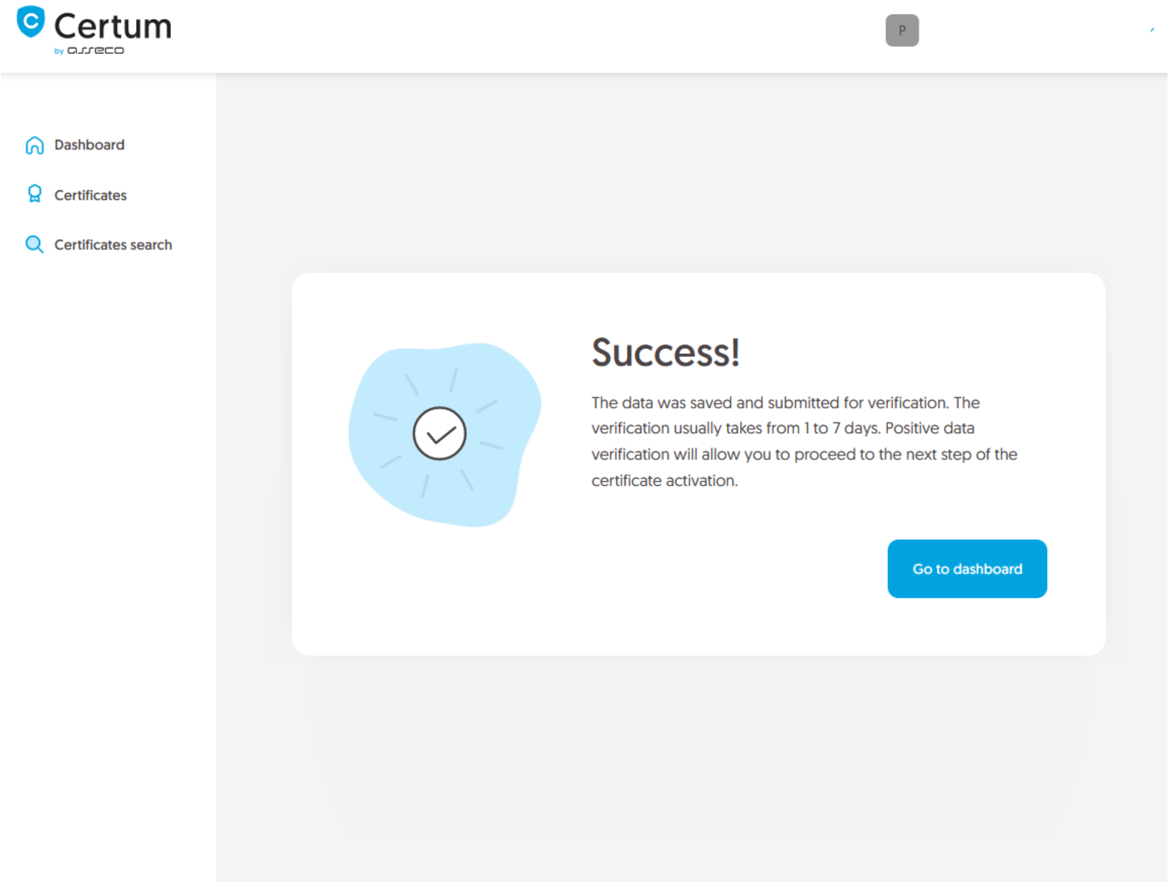
E-MAIL ADDRESS OF THE SUBSCRIBER*

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.

After selecting the verification method and proceeding, 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. 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].



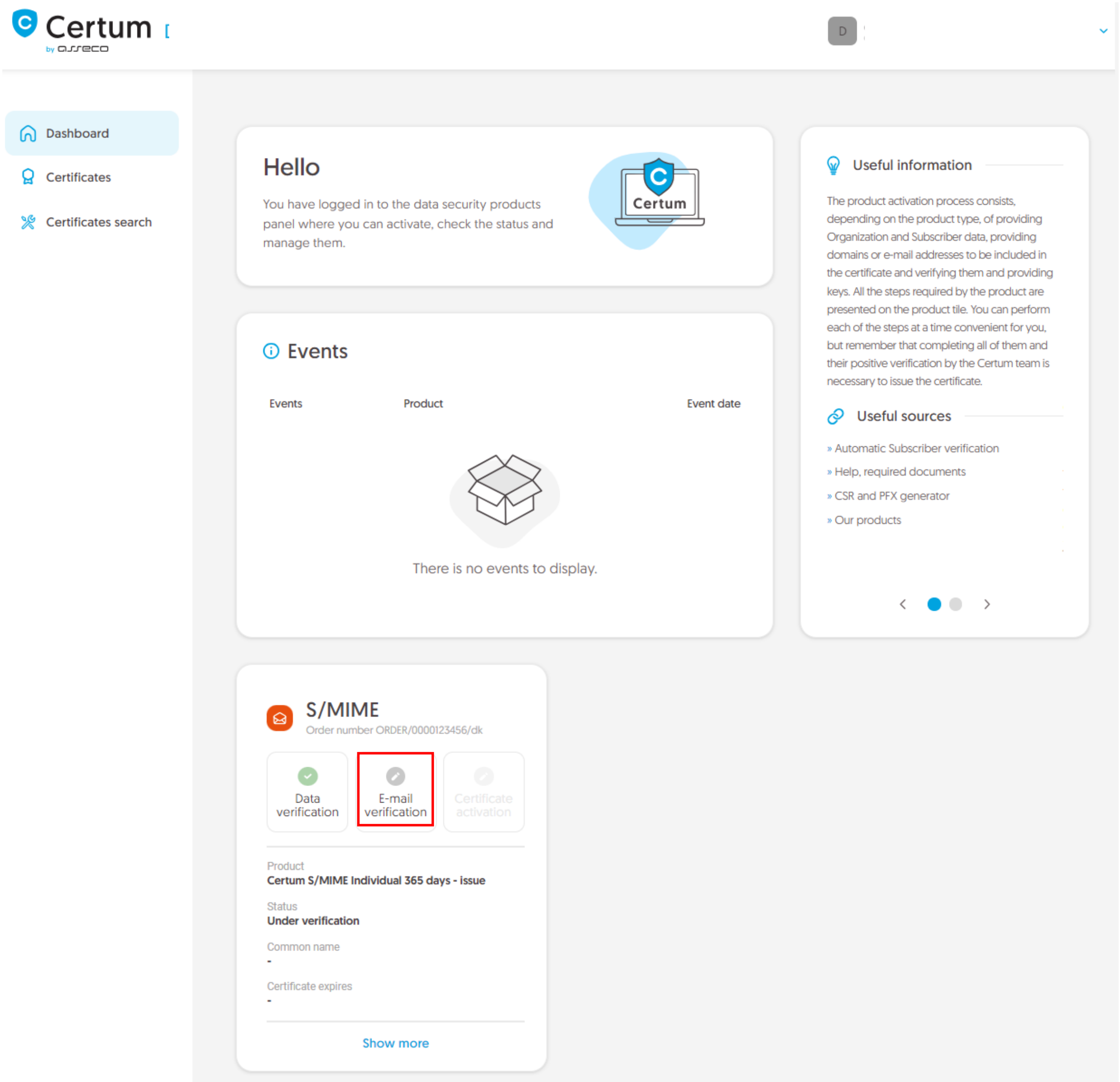
Success!

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.

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



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

Product
Certum S/MIME Individual 365 days - issue

Status
Under verification

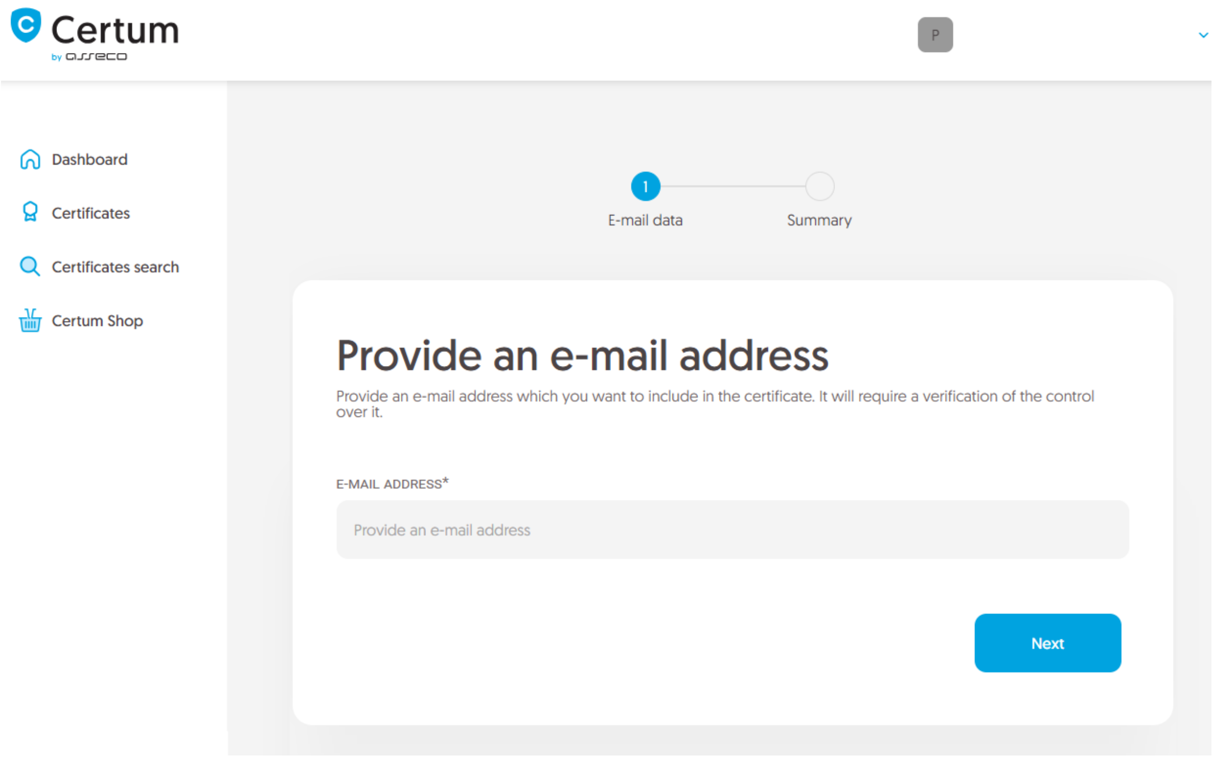
Common name
-

Certificate expires
-

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.



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

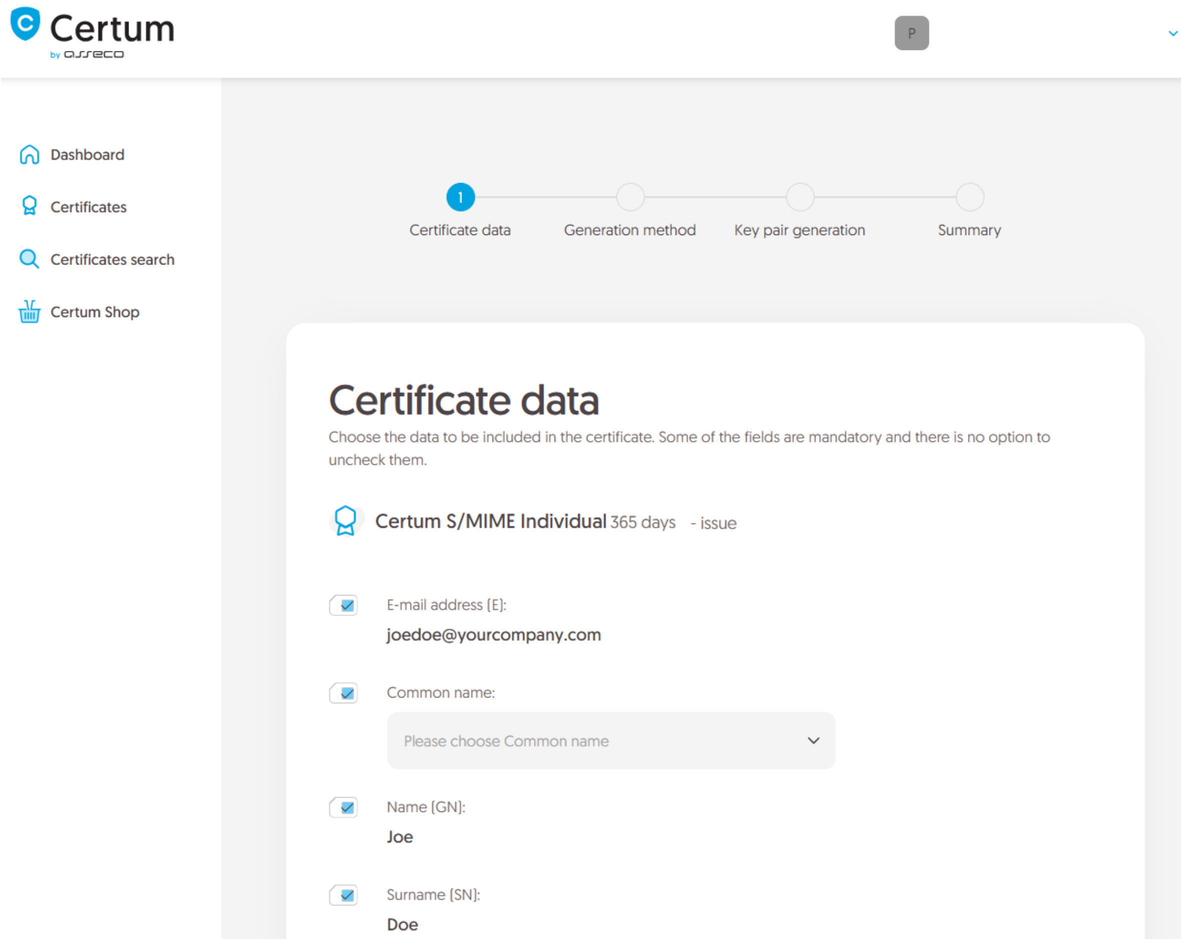
Check provided data on the summary screen. If the data is correct, complete the e-mail verification step.

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 and generate a key pair.



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 Individual 365 days - issue

☑ E-mail address [E]:
joedoe@yourcompany.com

☑ Common name:
Please choose Common name

☑ Name [GN]:
Joe

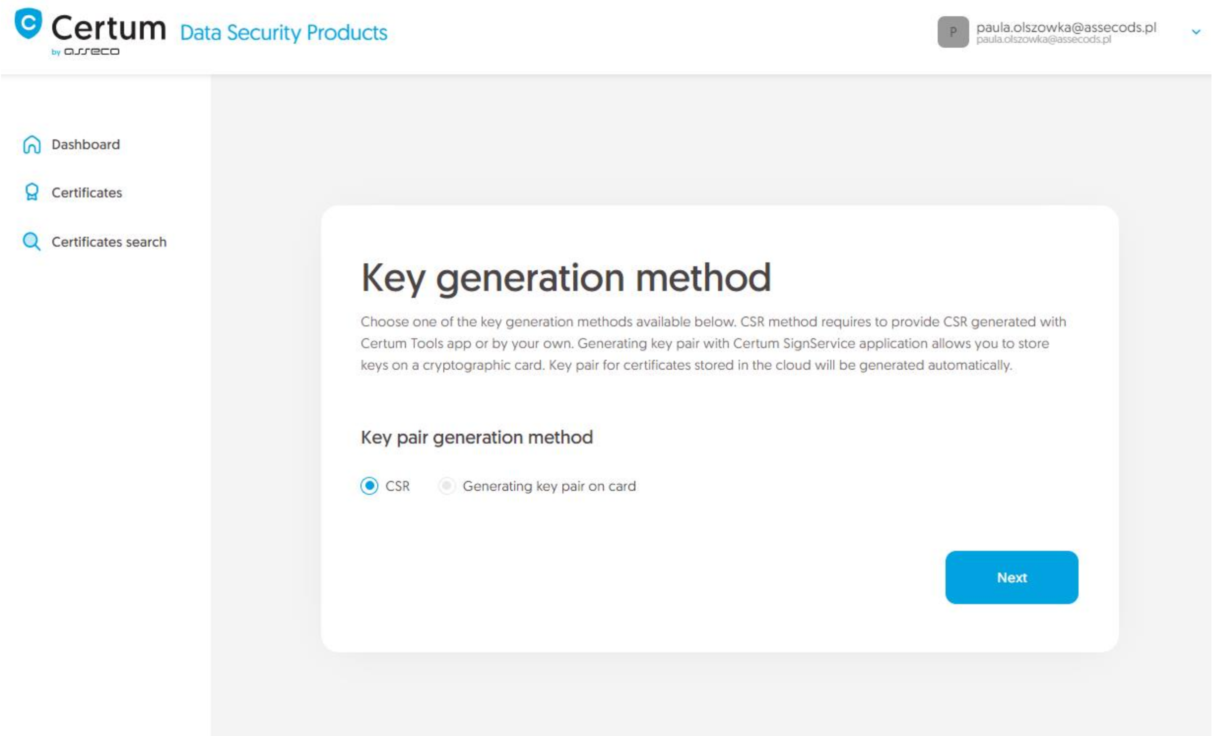
☑ Surname [SN]:
Doe

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



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.

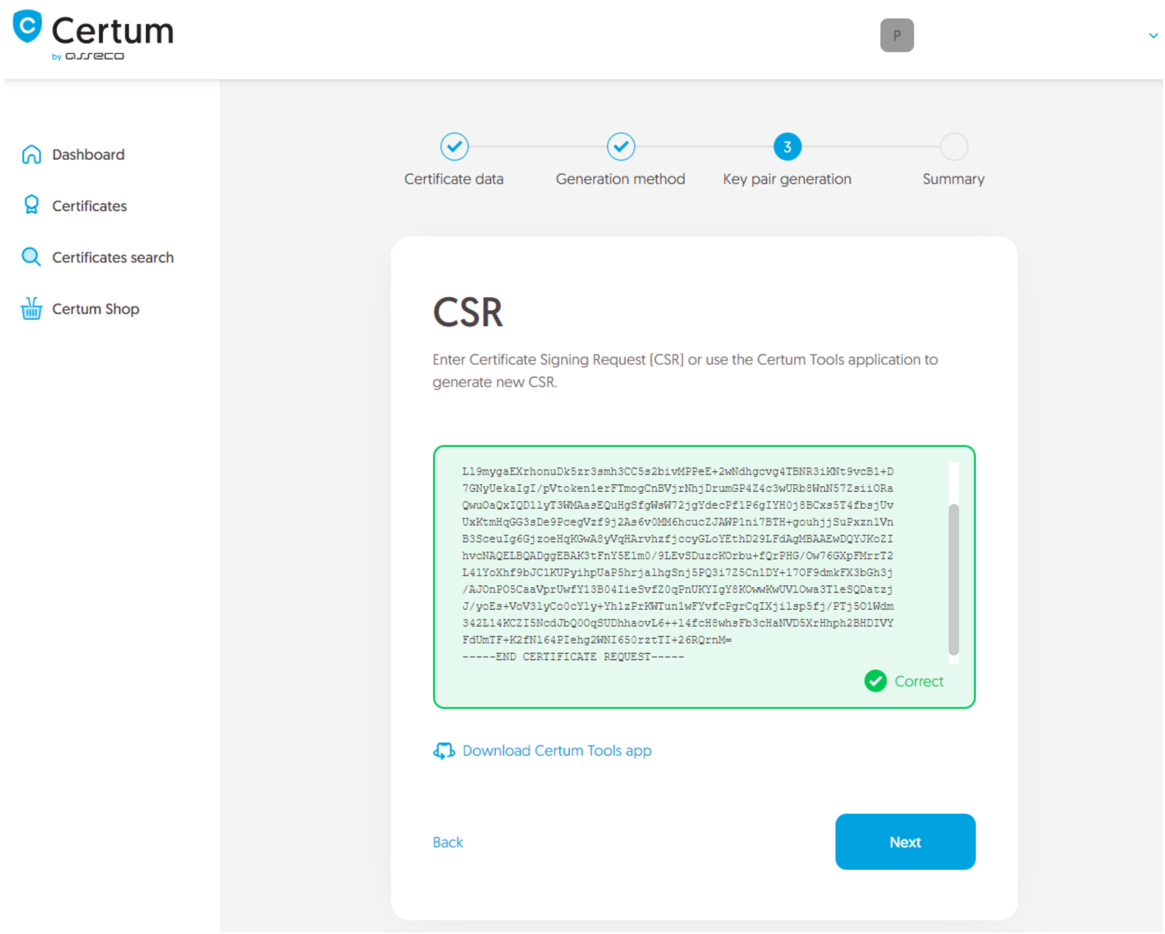
Key pair generation method

● CSR ○ Generating key pair on card

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.



CSR

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

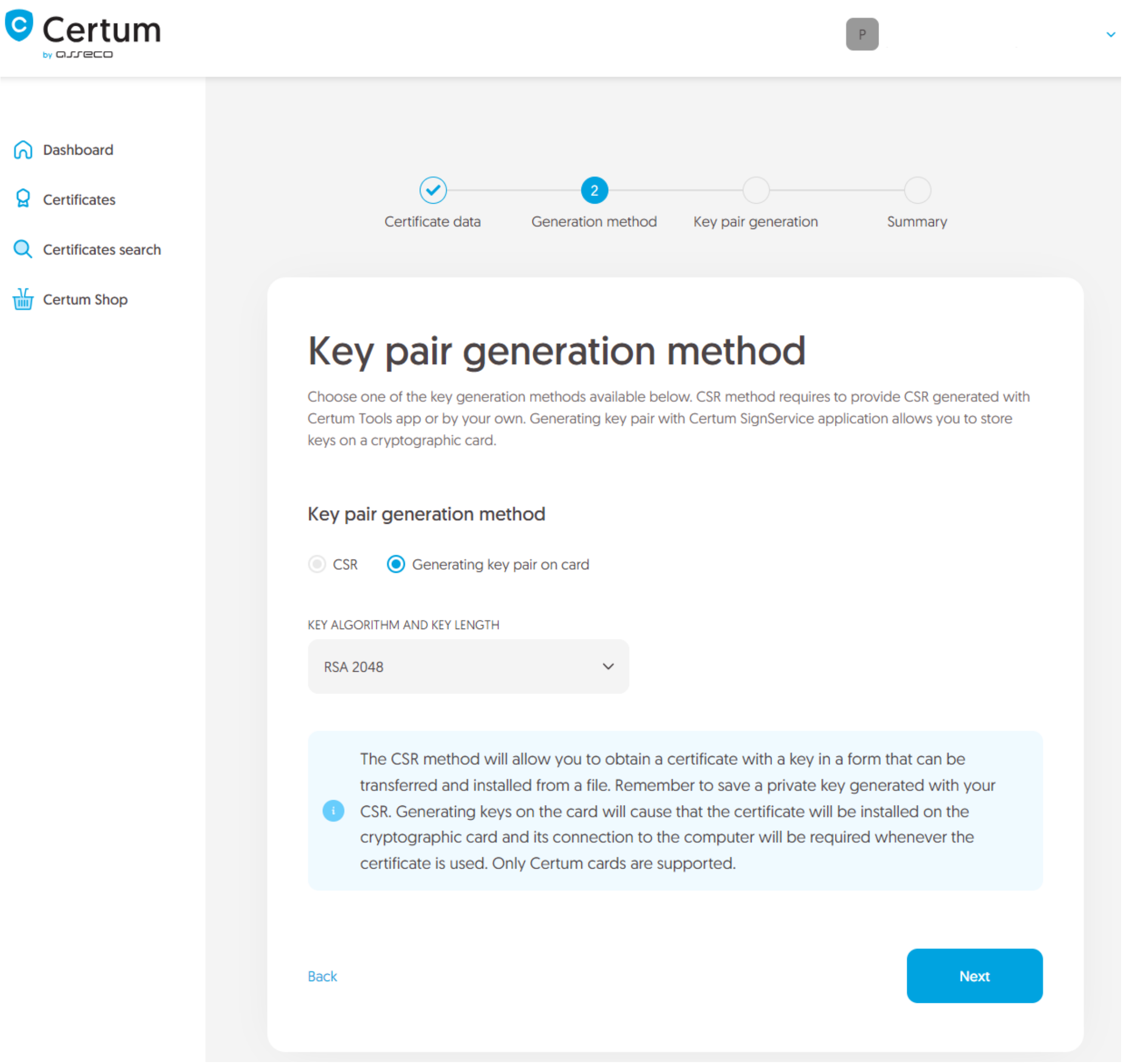
```
L19mygaEXrhonuDk5zr3smh3CC5s2bivMPPeE+2wNdhgcvg4TBNR3iKNt9vcB1+D
7GNyUekaIgI/pVtoken1erFTmogCnBVjrNhjDrumGP4Z4c3wURb8WnN57ZsiiORa
QwuOaQxIQD1lyT3WMAasEQuHgSfgWsW72jgYdecPf1P6gIYH0j8BCxs5T4fbsjUv
UxKtmHqGG3sDe9PcegVzf9j2As6v0MM6hcucZJAWP1ni7BTH+gouhjjSuPxzn1Vn
B3SceuIg6GjzoeHqKGwA8yVqHArvhzfjccyGLoYEthD29LFdAgMBAAEwDQYJKoZI
hvcNAQELBQADggEBAK3tFnY5E1m0/9LEvSDuzcKOrbu+fQrPHG/Ow76GXpFMrrT2
L41YoXhf9bJC1KUPyihpUaP5hrjalhgSnj5PQ3i7Z5Cn1DY+17OF9dmkFX3bGh3j
/AJOnPO5CaaVprUwfY13B04IieSvfZ0qPnUKYIgY8KOwwKwUVlOwa3TleSQDatzj
J/yoEs+VoV3lyCo0cYly+Yh1zPrKWTun1wFYvfcPgrCqIXjilsp5fj/PTj5O1Wdm
342L14KCZI5NcdJbQ0OqSUDhhaovL6++14fcH8whsFb3cHaNVD5XrHhph2BHDIVY
FdUmTF+K2fN164PIehg2WNI650rztTI+26RQrnM=
-----END CERTIFICATE REQUEST-----
```

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.



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

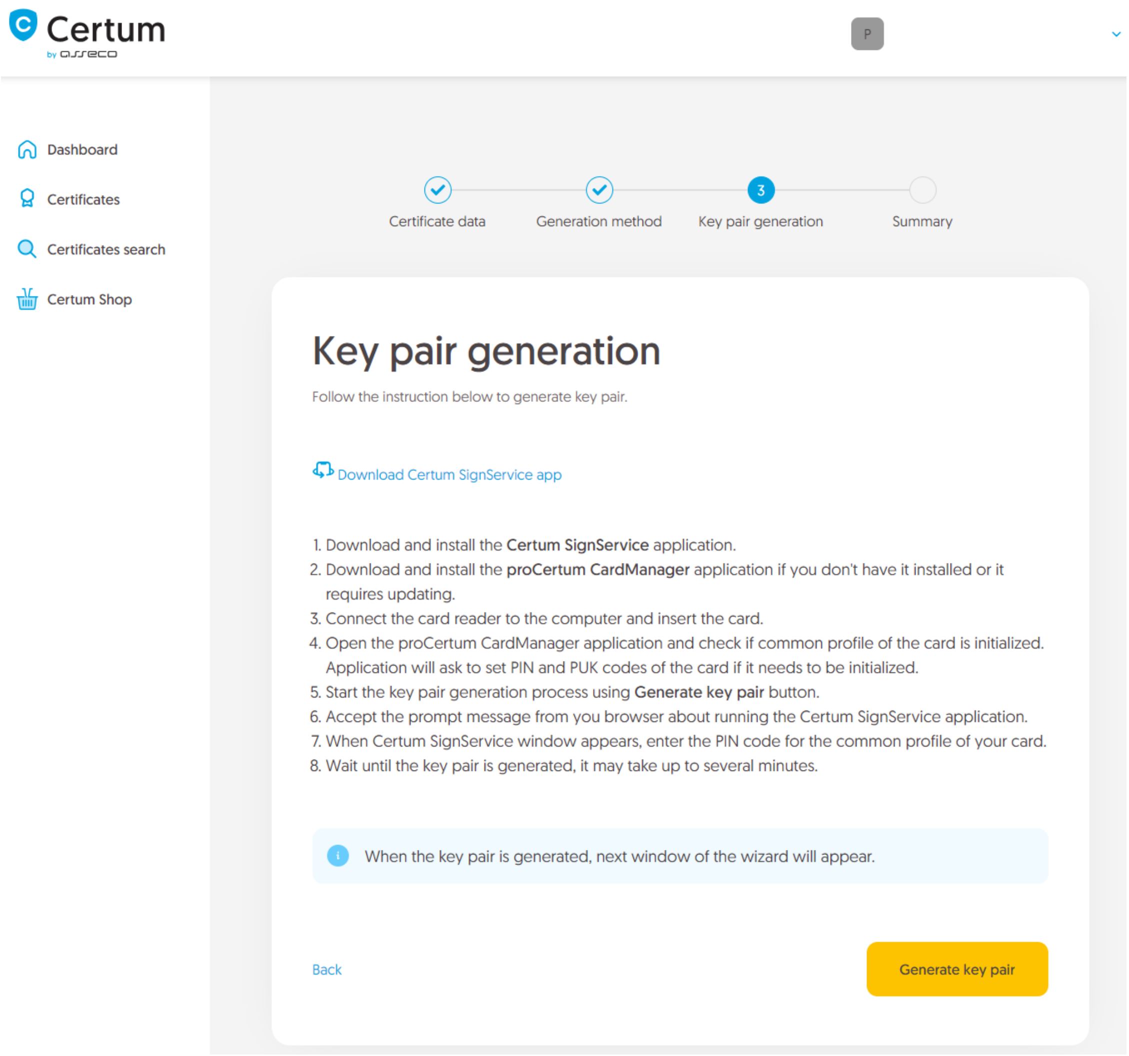
KEY ALGORITHM AND KEY LENGTH

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.

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.



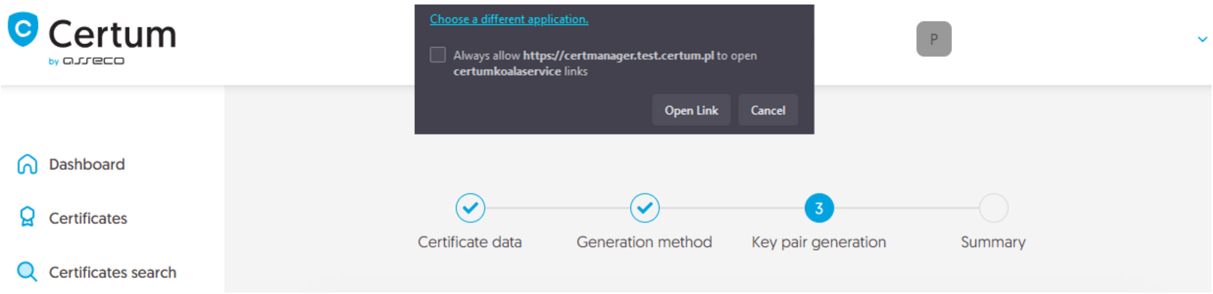
Key pair generation

Follow the instruction below to generate key pair.

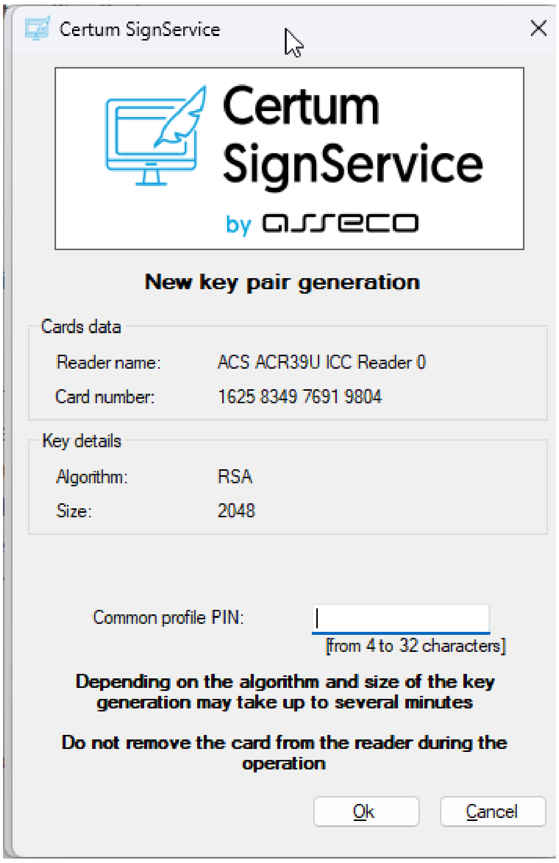
1. Download and install the **Certum SignService** application.
2. Download and install the **proCertum CardManager** application if you don't have it installed or it requires updating.
3. Connect the card reader to the computer and insert the card.
4. Open the proCertum CardManager application and check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

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

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.



□ Always allow **https://certmanager.test.certum.pl** to open **certumkoalaservice** links



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

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.