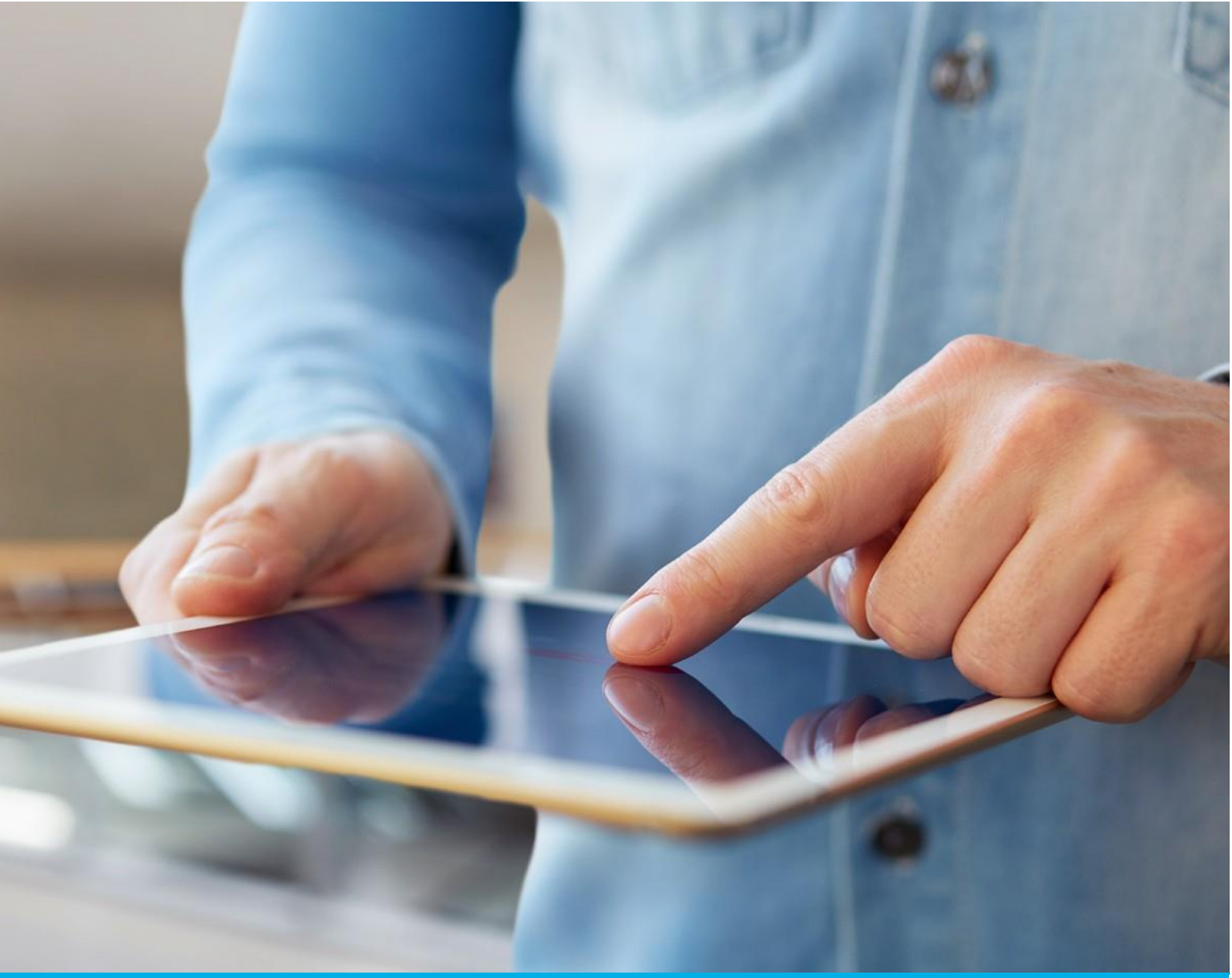


Standard Code Signing on a card certificate activation

Ver. 3.1

asseco

Certum by asseco

Table of contents

certum.pl
infolinia@certum.pl

1. Product description

The Code Signing certificate allows you to digitally sign applications and drivers, certifying their authenticity and security. Thanks to this, users of your software can be sure that it has not been modified, infected or damaged by third parties.

Signing the application with Code Signing eliminates the problem of code anonymity on the internet. With a digital signature you can be sure that users will not see an "unknown publisher" warning when installing or running your program and they will be ensured about its security. Signing your app helps protect both: your users and your brand's reputation.

Digital code signing makes using the application safe, which translates into greater trust in your brand and an expansion of your group of users.

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 and/or organization's data 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

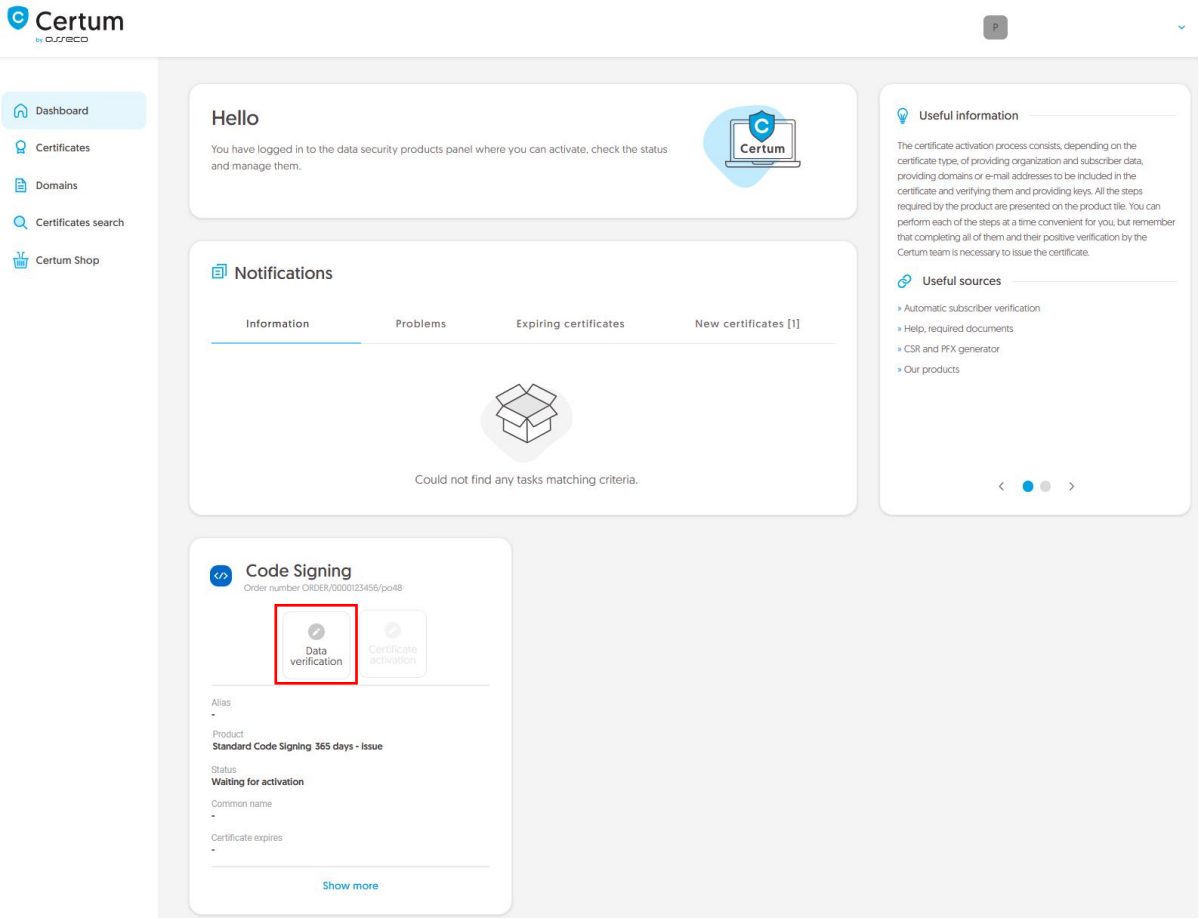
certum.pl
infolinia@certum.pl

Data verification step

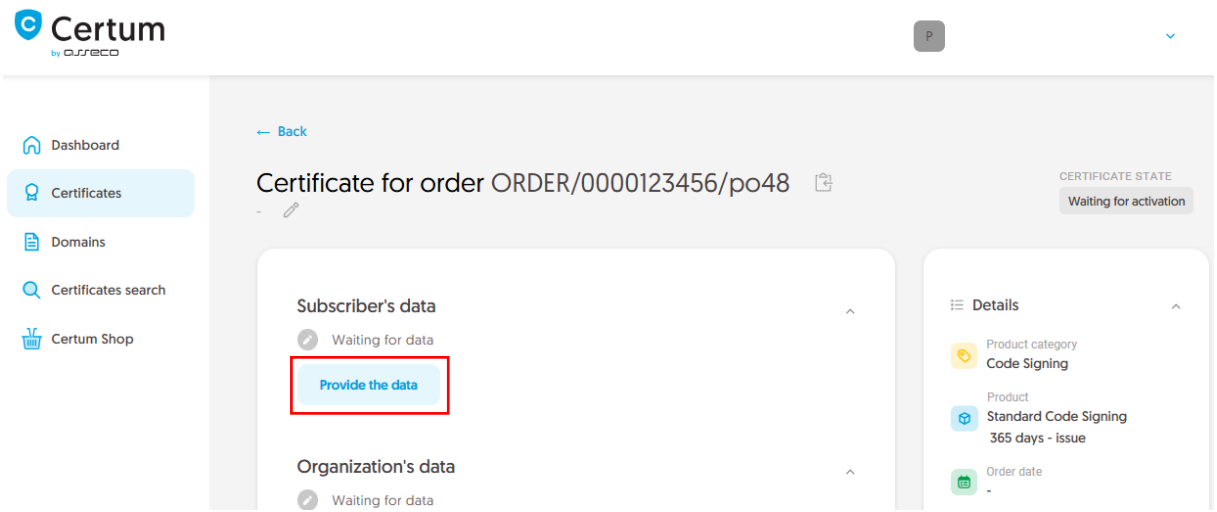
Providing data to be verified is the step in which you provide, depending on the chosen variant, the data of the organization for which the certificate will be issued, the data of the subscriber (the person who represents the organization and will be the owner of the certificate) and the data of the subscriber's authorization to represent the organization. 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:



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

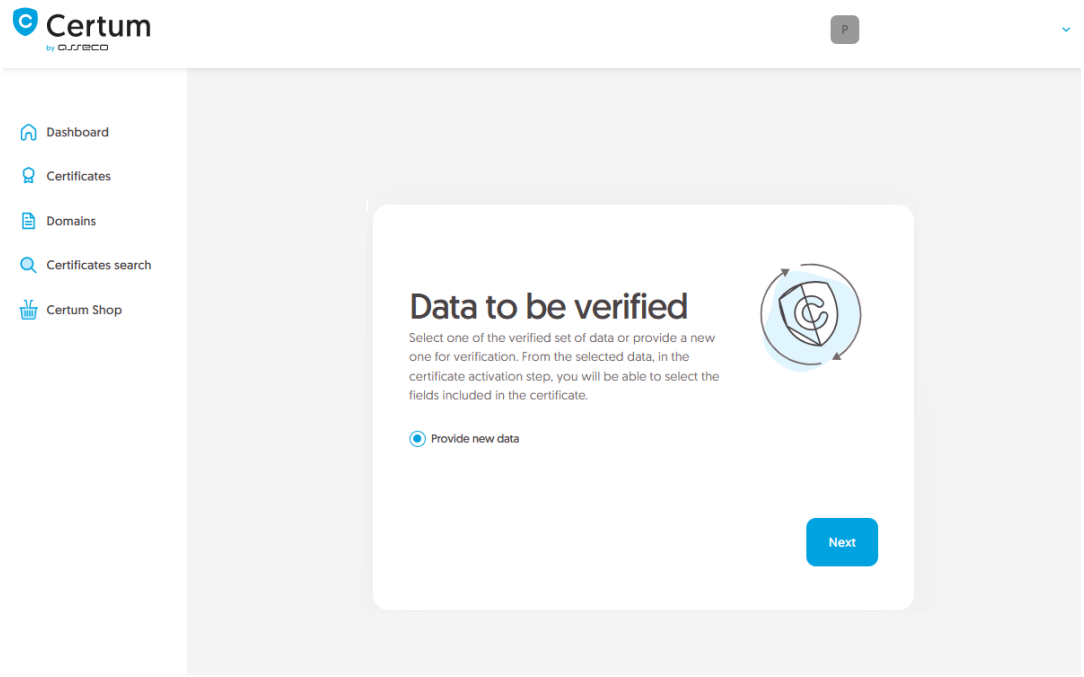
Choosing a variant of the data to be verified

Choose one of three options for providing data to be verified:

- **Individual** – the certificate contains the subscriber's data, the subscriber's identity will be verified and his address details are provided in the fields for organization data. The Common name of the certificate contains the name and surname of the subscriber
- **Organization** – the certificate contains the organization's data, the subscriber's data, organization existence and the subscriber's authorization to represent the organization are verified. The Common name of the certificate contains the organization name
- **Sponsor** – the certificate contains the subscriber and organization's data, the subscriber's identity, organization existence and the subscriber's authorization to represent the organization are verified. The Common name of the certificate contains the name and surname of the subscriber.

The wizard will guide you through the process of providing the data. In the first stage, choose **Provide new data**. In the future, it will be possible to use them to issue another certificate.

certum.pl
infolinia@certum.pl

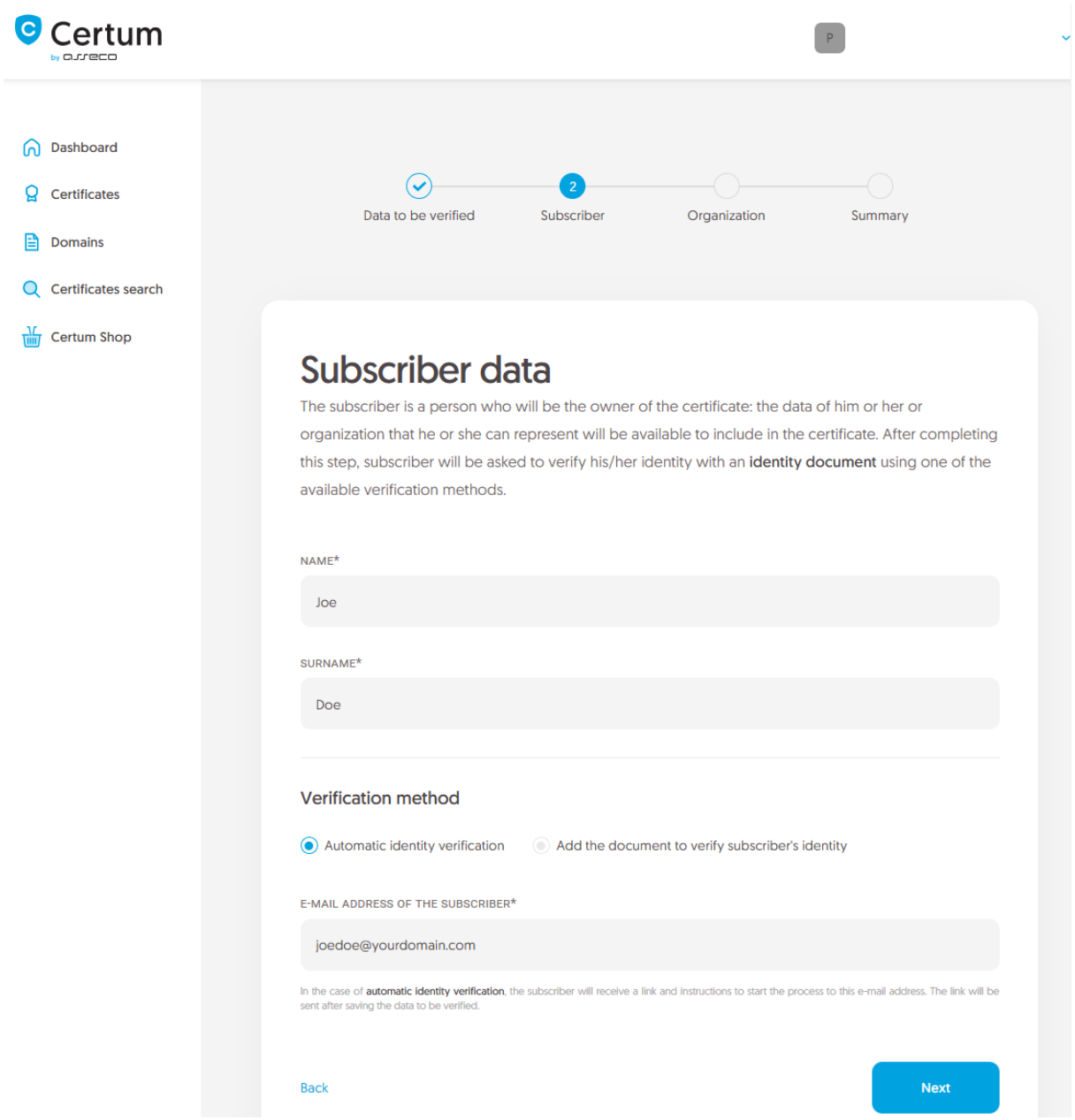


In the next stage, provide the details of the subscriber, which means the person who represents the organization and will be the owner of the certificate. Please write the names and surnames in the form as they appear on the subscriber's identity document.

Also choose a method for verifying the subscriber's identity from the available ones:

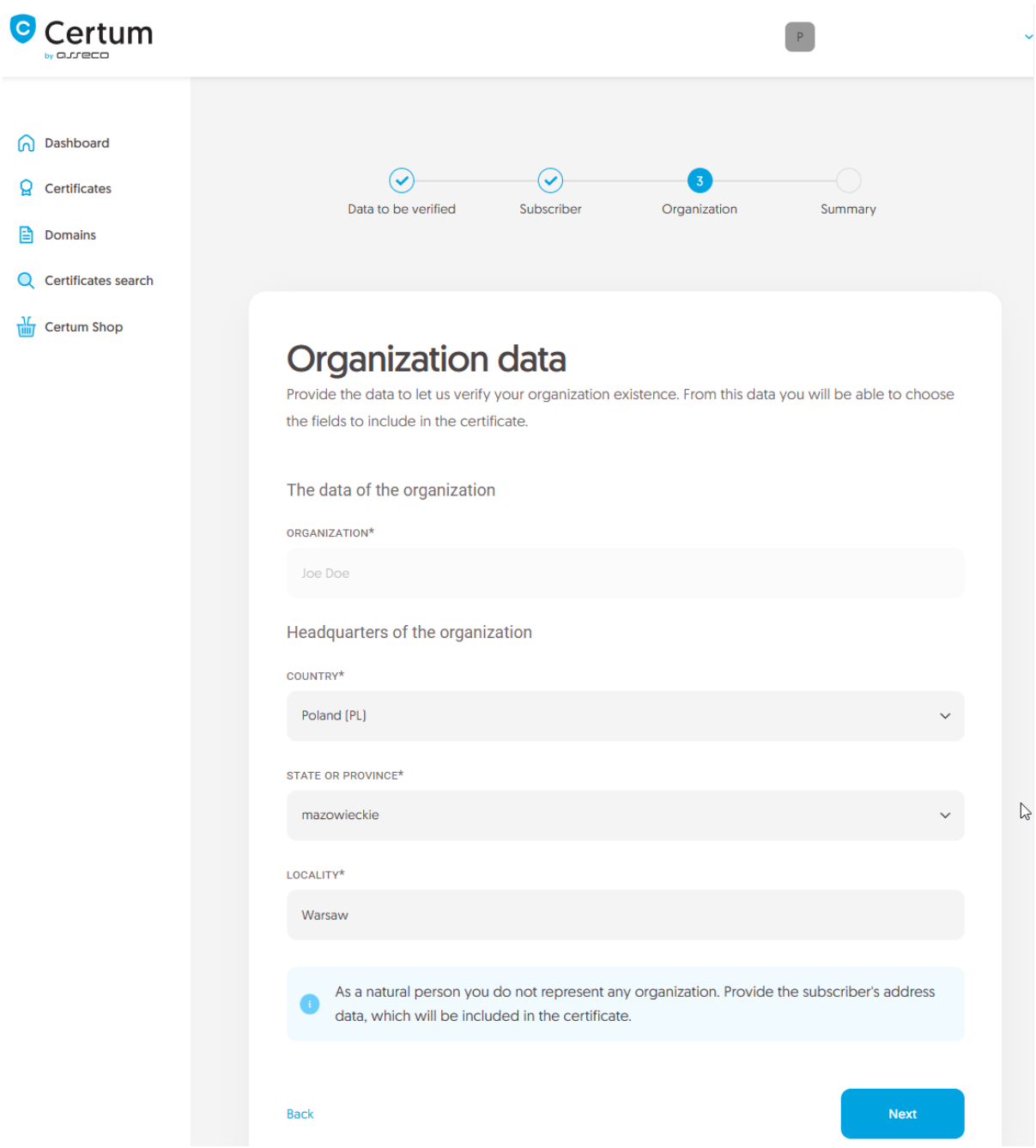
- **Automatic identity verification** – the subscriber will receive an e-mail with a link to the identity verification service to use with a computer or phone camera and an ID document
- **Attaching a document** – you will add a scan of the subscriber's identity document or an identity confirmation.

certum.pl
infolinia@certum.pl



After providing the subscriber's data, go to the next stage: providing the organization's data.

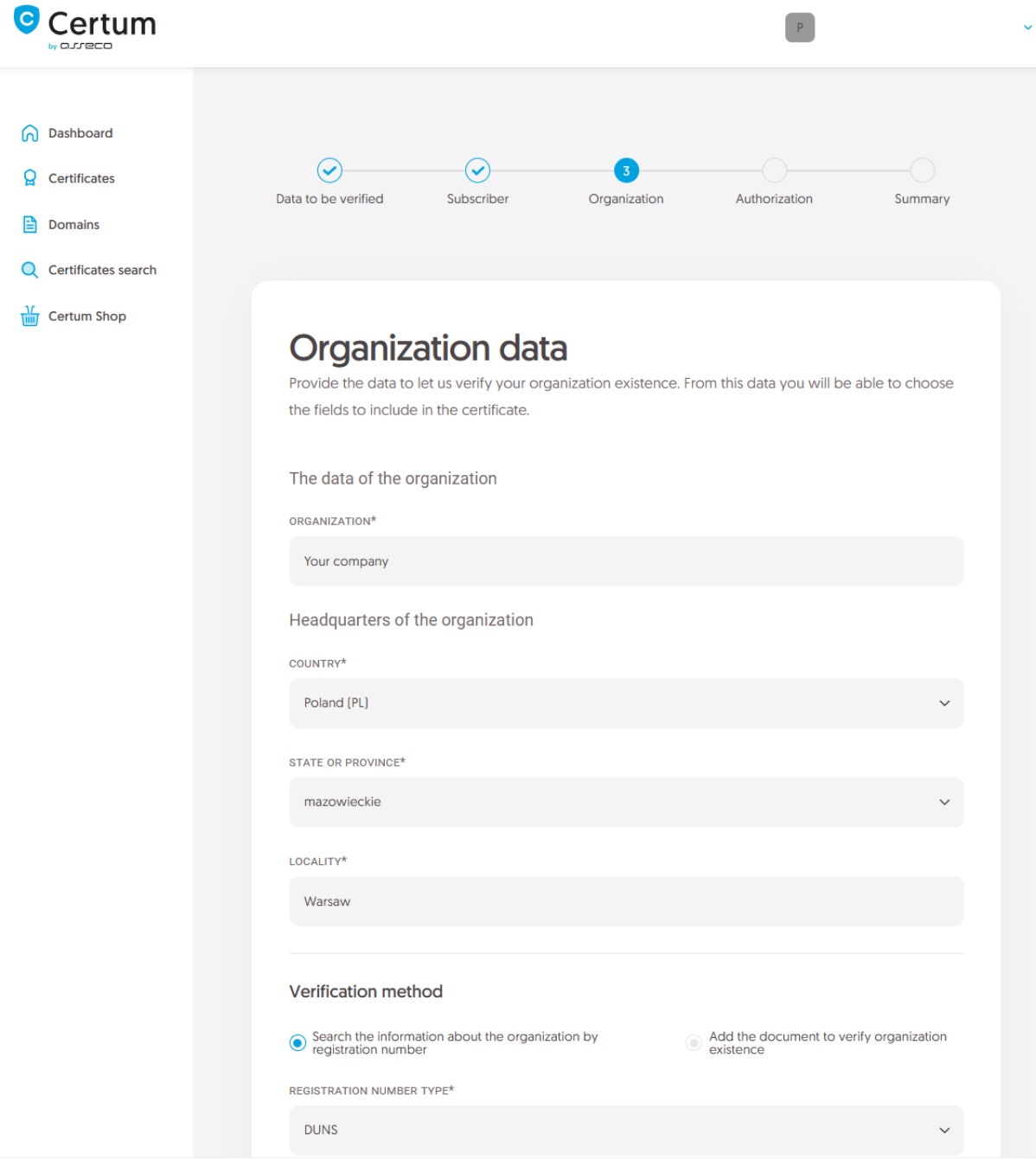
For **individual** certificate variant, provide address details of subscriber's residence. Next, go to the data verification step summary.



For **organization** and **sponsor** certificate variant 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.

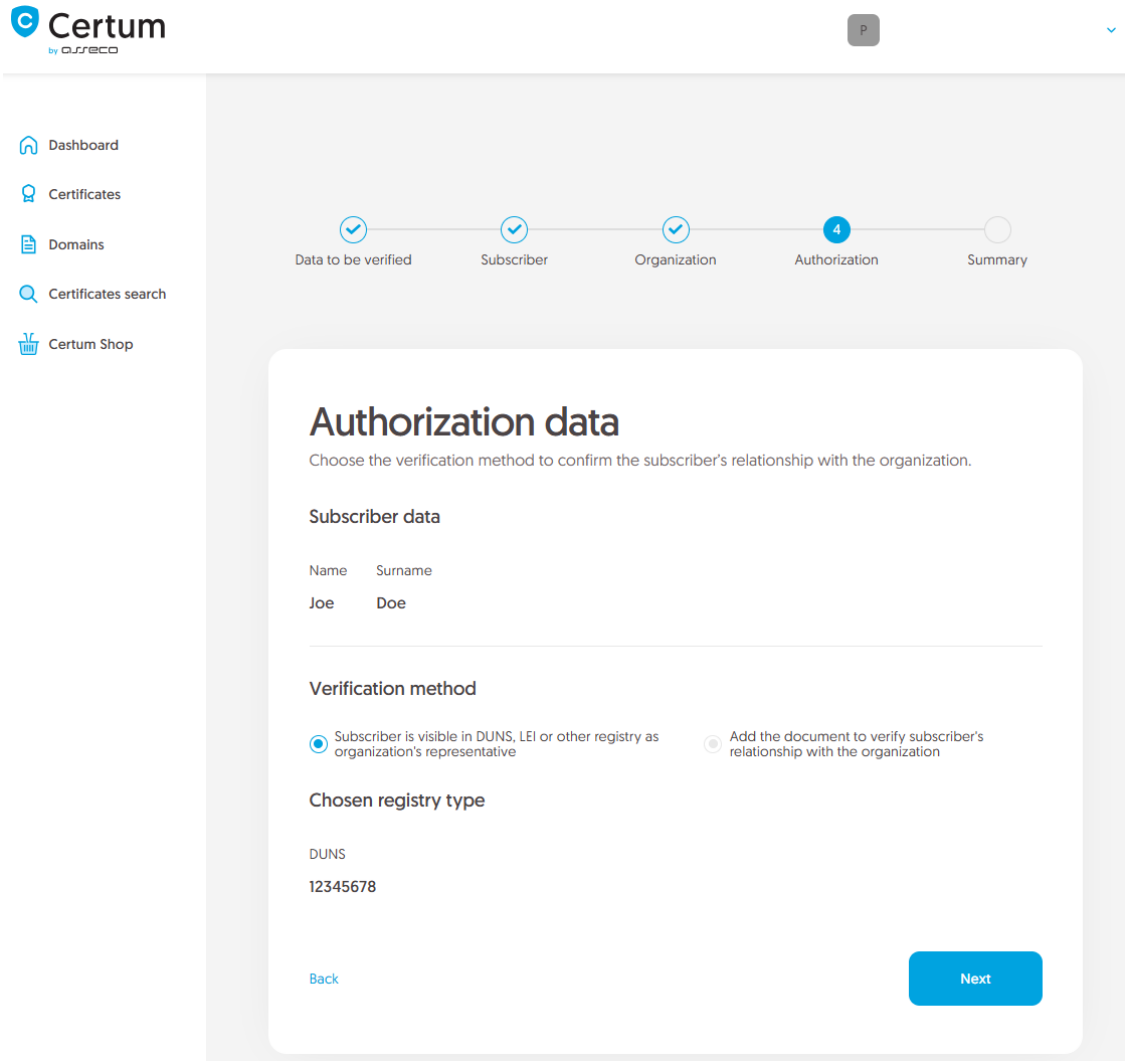


After providing all the required organization's data, proceed to the last stage of providing data for verification step, which is choosing the method of verifying the subscriber's authorization to represent the organization. This stage is required for **organization** and **sponsor** variants of certificate.

There are two methods to choose from:

- **The subscriber is visible in the registry** – the person given as the subscriber appears in one of the given registers as a representative of the organization
- **Attaching a document** – you will add a document confirming authorization. You can download an example of such document by the **Download ready to sign authorization document** link.

The method of verifying the subscriber's authorization is also influenced by the organization's chosen verification method. If the registration number and its type have been provided there, Certum will first check whether the subscriber is listed in the register and the system will automatically mark the method of verifying the subscriber's authorization as **The subscriber is visible in the register**. However, this does not prevent you from adding a document confirming the subscriber's authorization.

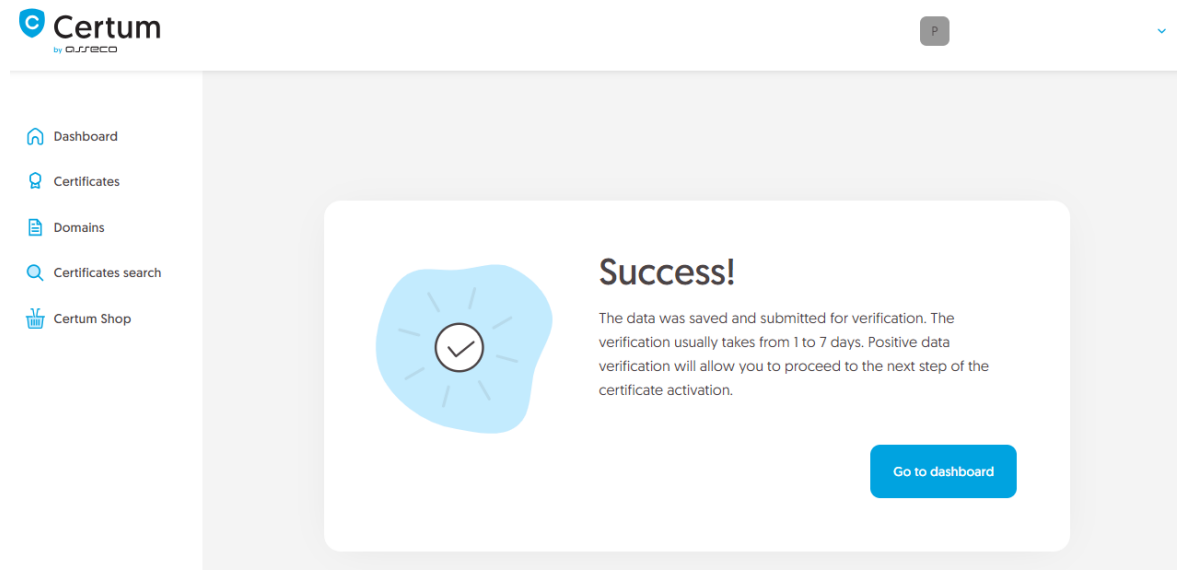


After selecting the authorization verification method go to the next stage.

Data verification step summary

Check provided information on the summary screen. If the data is correct, mark the required statements and complete the step of providing data to be verified.

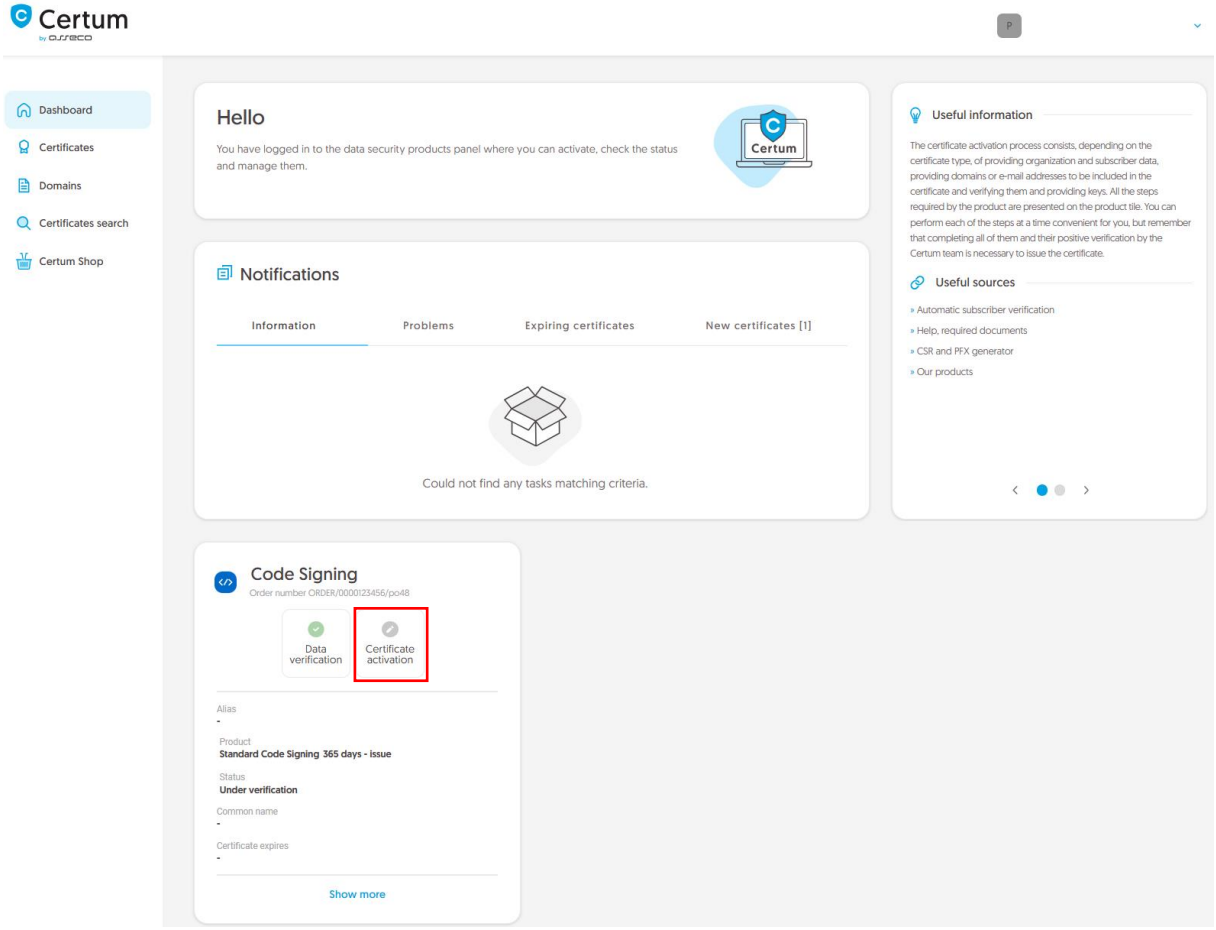
The success screen will inform you that the data have been saved for verification. Certum will verify them. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the subscriber's identity, if such verification method has been chosen. You may check the instruction for automatic identity verification.



Positive verification of the provided data will allow you to go to the **Certificate activation**.

Certificate activation step

You will be able to start certificate activation step from **Dashboard**, using **Certificate activation** option:

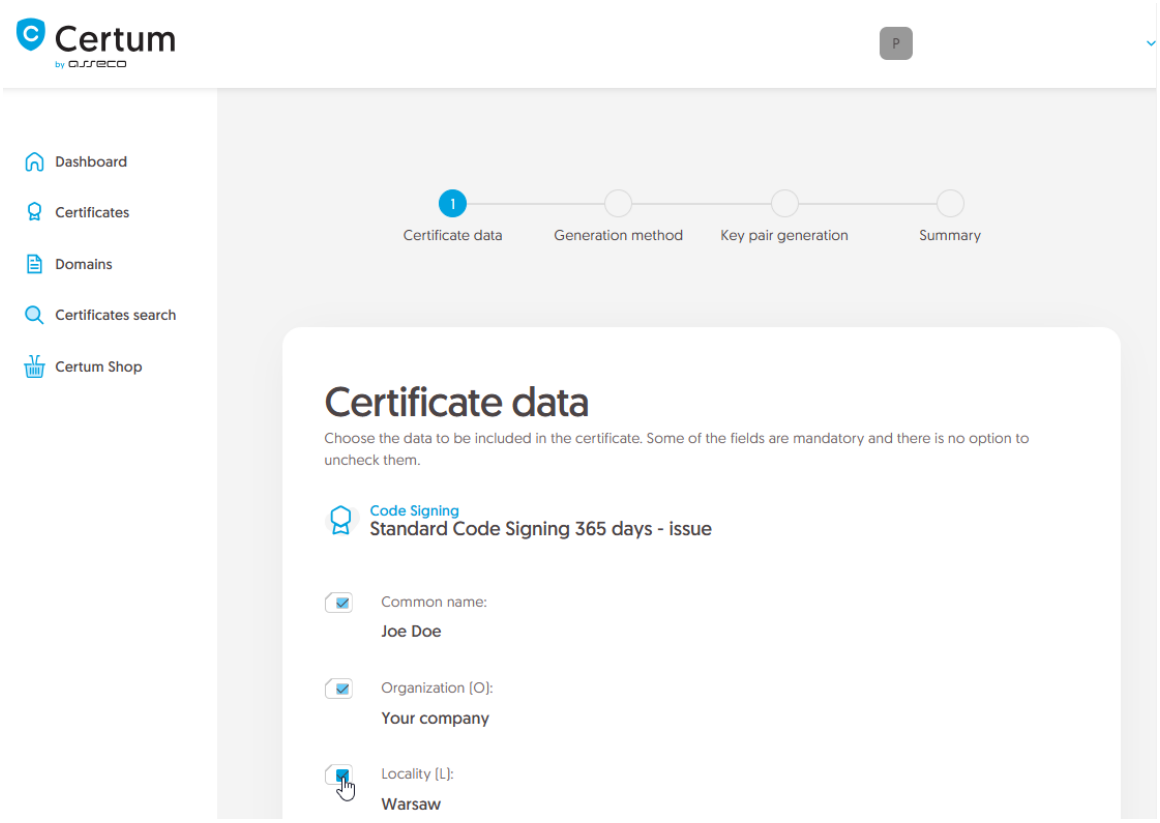


certum.pl
infolinia@certum.pl

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 fields you want to include in the certificate and generate key pair.

Choose the fields you want to include in the certificate. Some fields are required and cannot be unmarked.



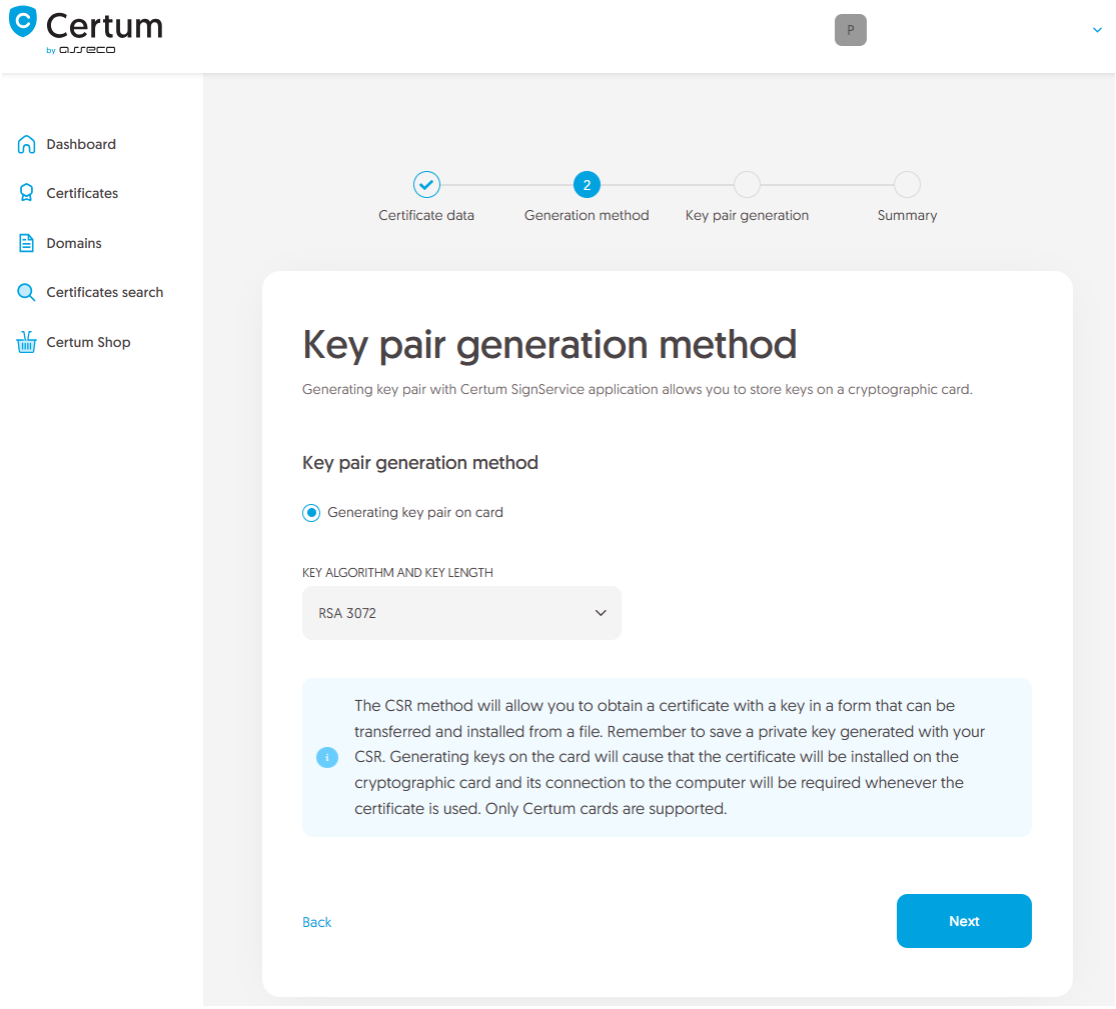
Once you have chosen the fields to the certificate, go to the key pair generation.

For Code Signing certificates, the available key generation method is **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.

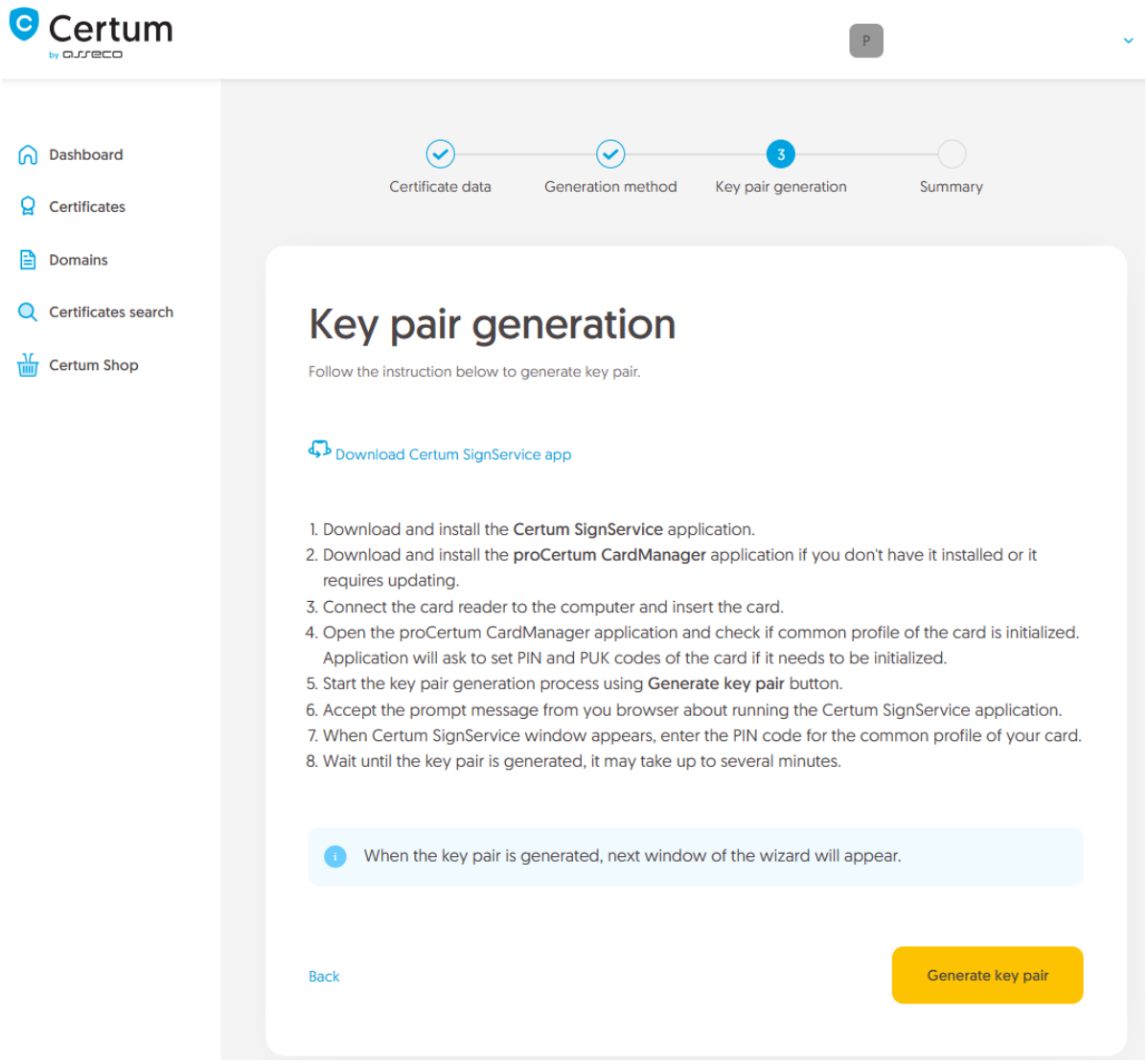
After selecting the method for generating key pair on card, choose the algorithm and key length.

certum.pl
infolinia@certum.pl

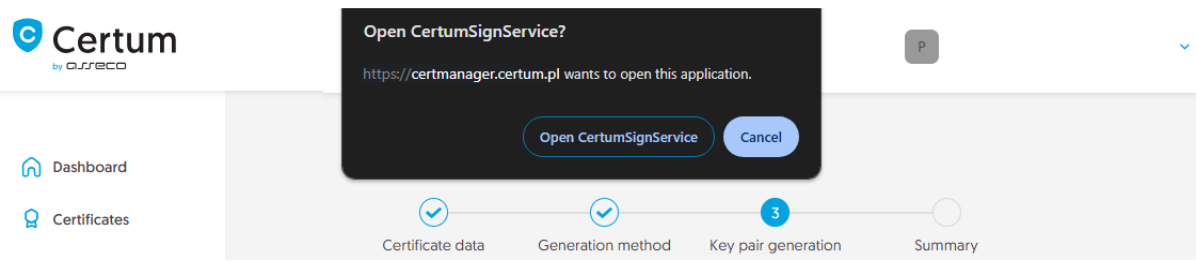


In the next stage, make sure that you have the card inserted into the reader, the reader connected to the computer and the card itself has an initialized common profile with a PIN code set for it. The process also requires having the proCertum CardManager application installed on your computer, where 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.



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.pl
infolinia@certum.pl

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, the process will proceed to the summary.

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. 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.