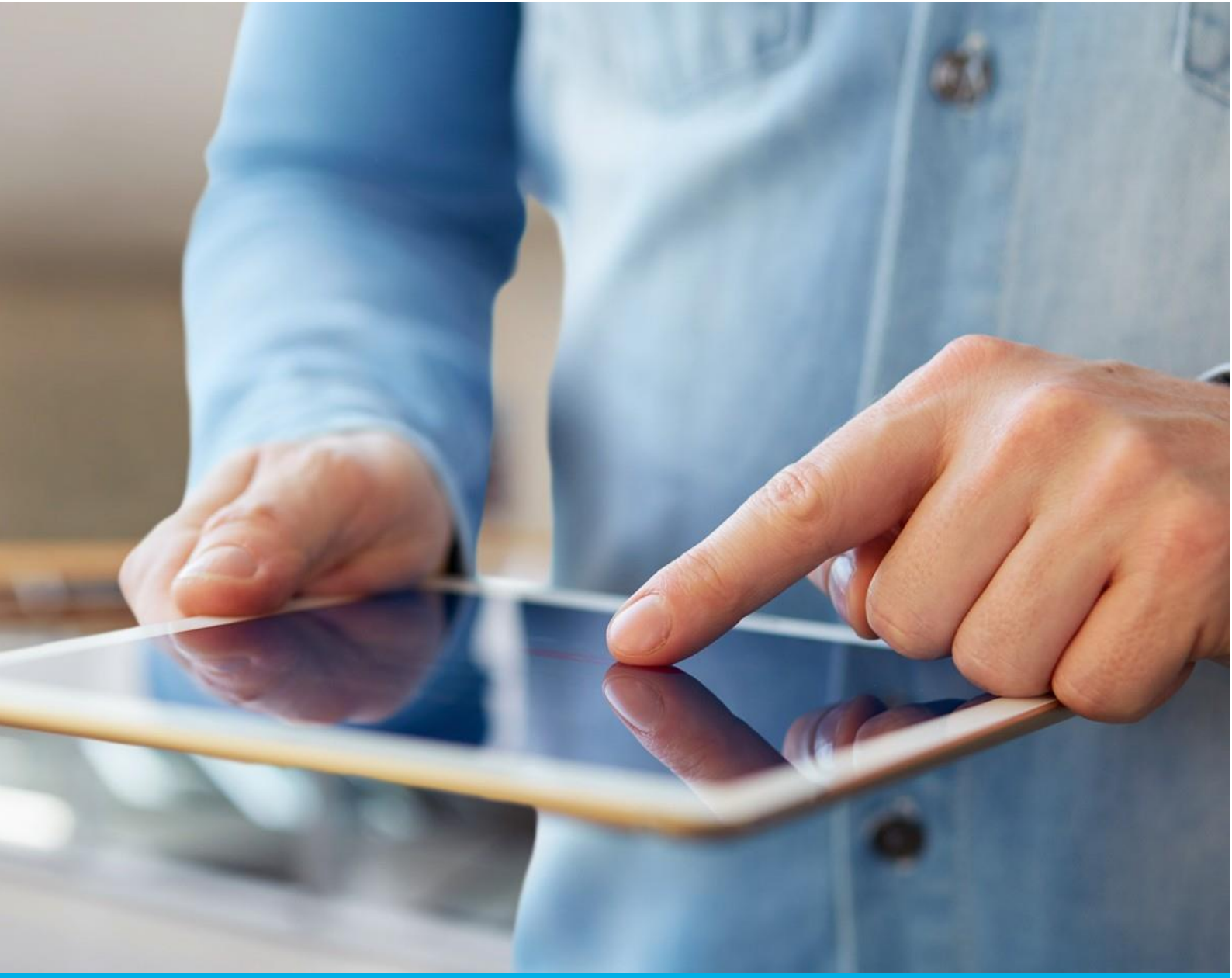


Document Signing certificate activation

Ver. 2.8

asseco

Certum by asseco

Table of contents

1. Product description 3
2. Certificate activation 3
Data verification step 4
Choosing a variant of the data to be verified 5
Data verification step summary 10
E-mail verification step 11
Certificate activation step 15

certum.pl
infolinia@certum.pl

1. Product description

A Document Signing certificate is a certificate stored in the SimplySign cloud service, designed for signing documents. It enables automatic and secure signing of documents and significantly accelerates their exchange both within a company and with its business partners.

The certificate meets the highest security standards. It also guarantees Adobe Approved Trust List (AATL) compliance and enables you to sign Adobe documents using trusted digital identifier.

Choose a solution that your customers and business partners will trust.

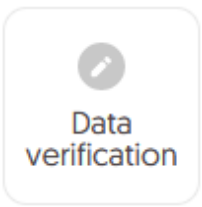
With the Certum Document Signing certificate, you can be confident that the document has not been altered and the data contained therein are protected.

2. Certificate activation

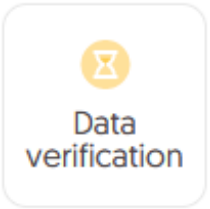
You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **Data verification** – providing the Subscriber and/or organization's data and the verification
- **E-mail verification** – key pair generation, providing an e-mail and the verification
- **Certificate activation** – choosing the fields to include in the certificate and submit to issue.

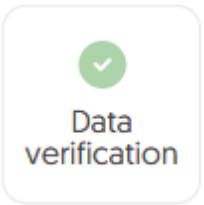
As the activation process goes, each step will go through the next statuses:



Step is awaiting to provide the data



Data is saved and waiting for verification



Verification was successful

Providing the data is not available yet

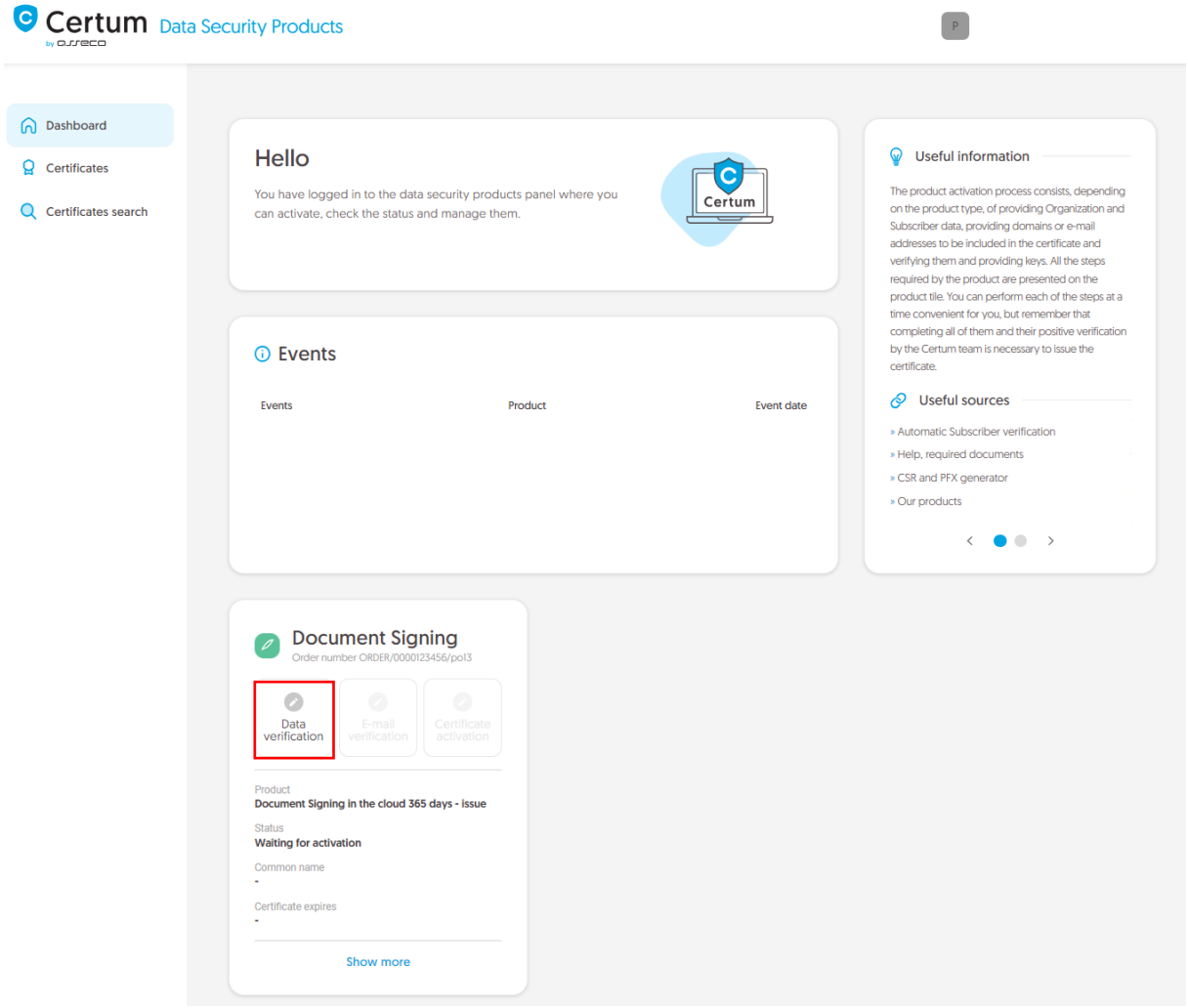
certum.pl
infolinia@certum.pl

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.

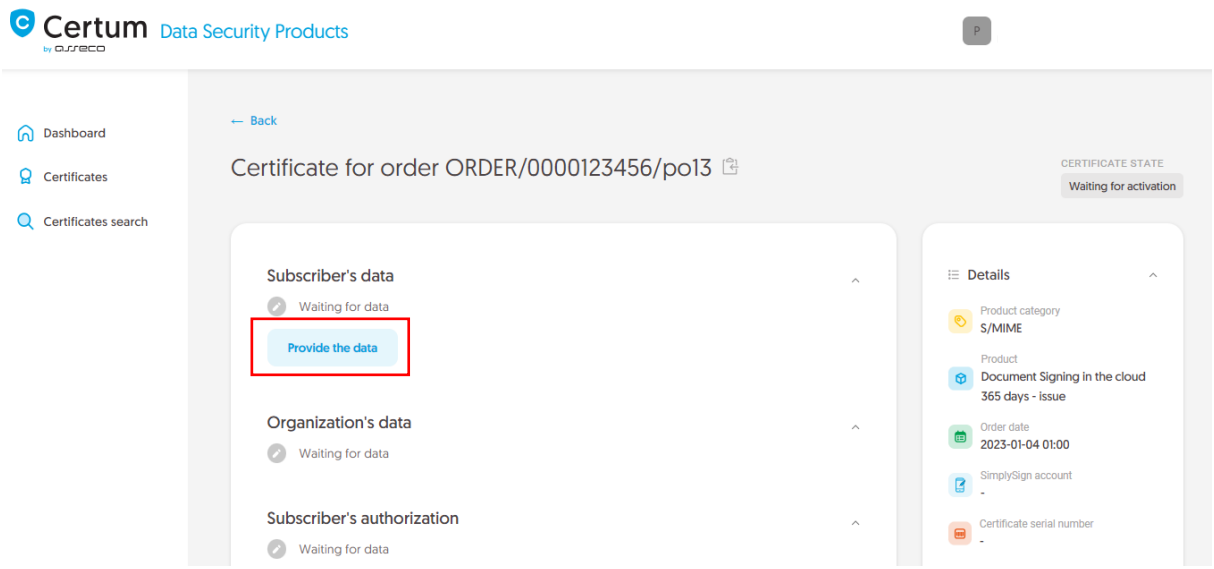
The list of supported verification documents you can check at Information about required documents.

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:

certum.pl
infolinia@certum.pl

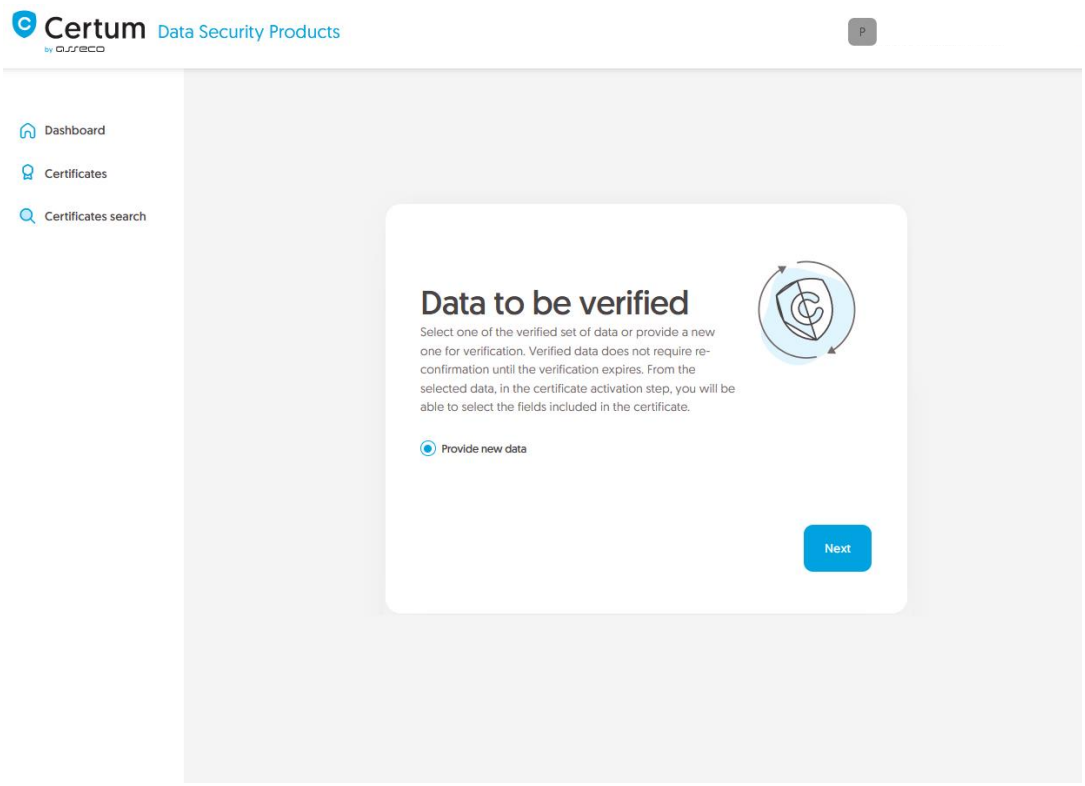


Choosing a variant of the data to be verified

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.

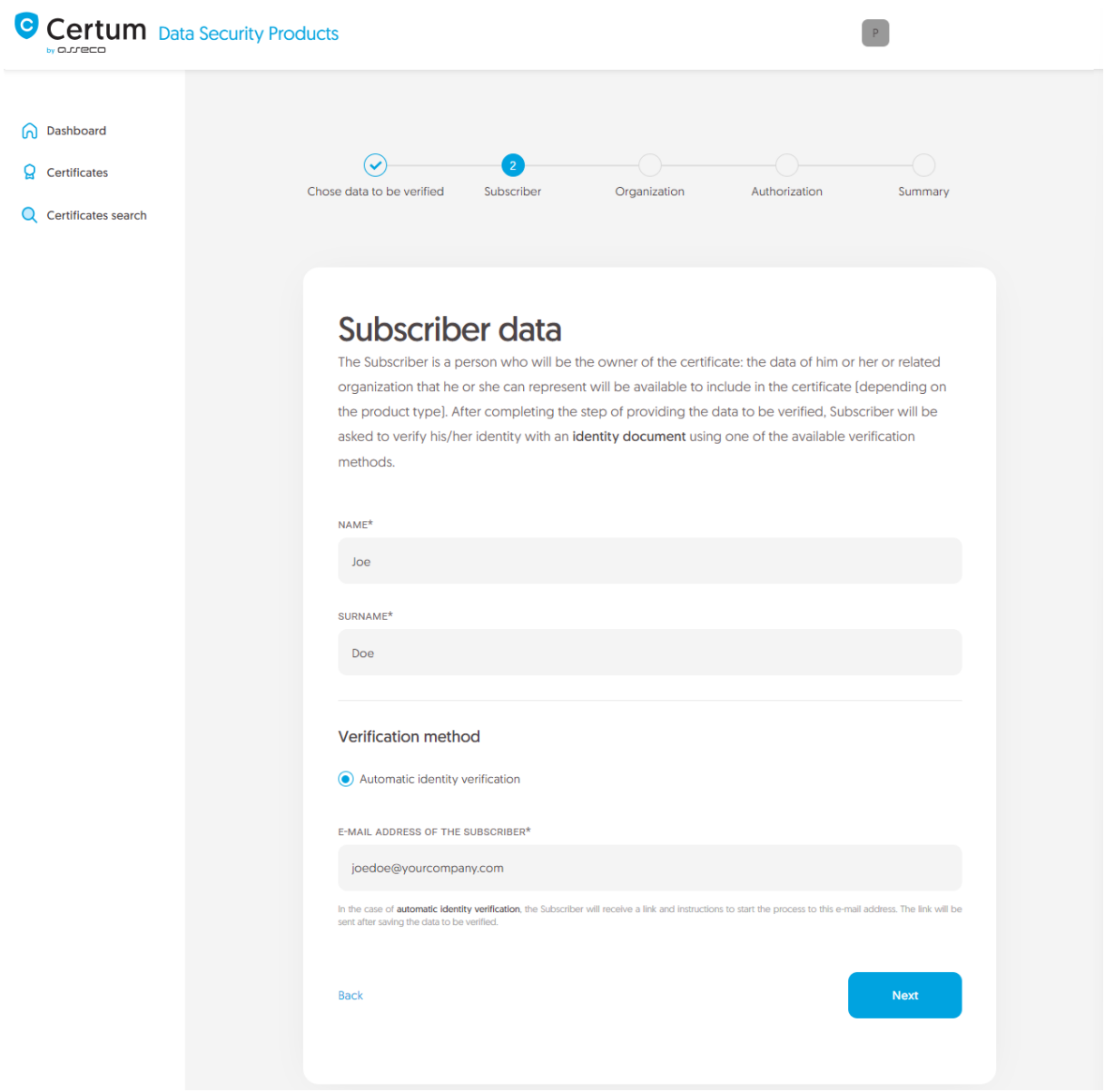
The wizard will guide you through the process of providing the data. In the first stage, choose **Provide new data**. In the future, it will be possible to use them to issue another certificate.



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.

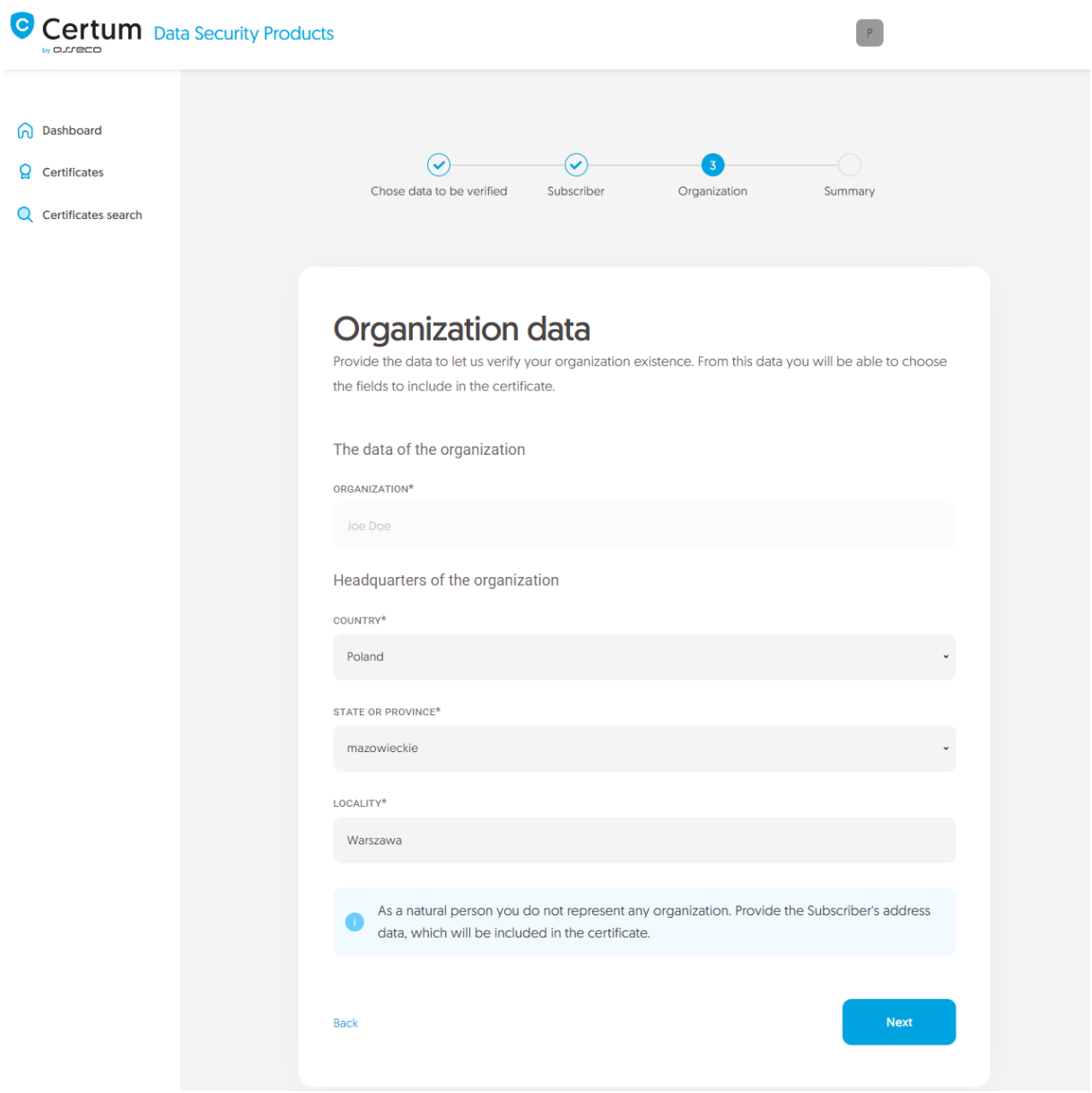
For verifying the Subscriber's identity there is one of the verification methods available: **Automatic identity verification** – the Subscriber will receive an e-mail with a link to the identity verification service to use with a computer or phone camera and an ID document.

certum.pl
infolinia@certum.pl



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

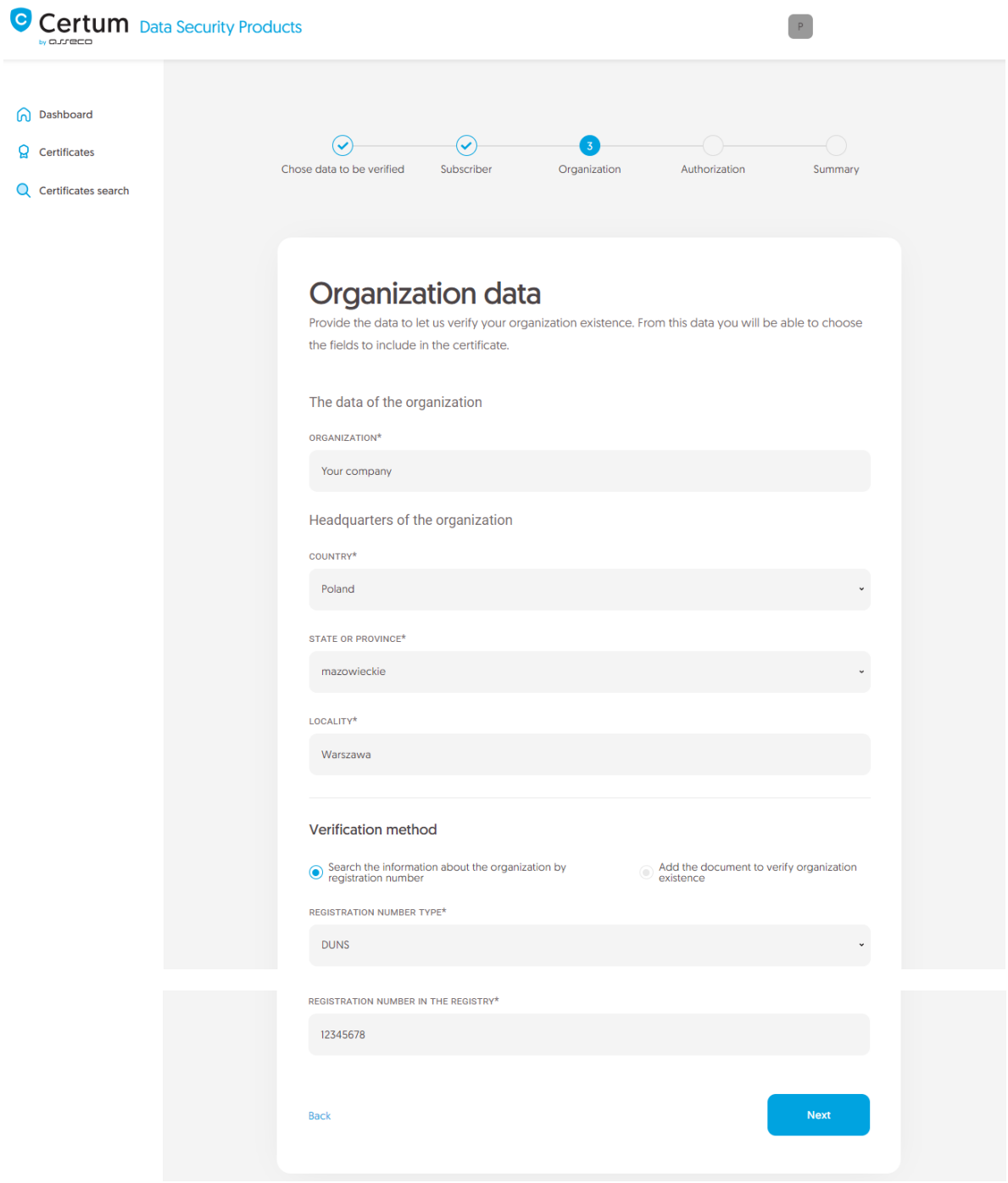
For **individual** certificate variant, provide address details of Subscriber's residence. Next, go to the data verification step summary.



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.

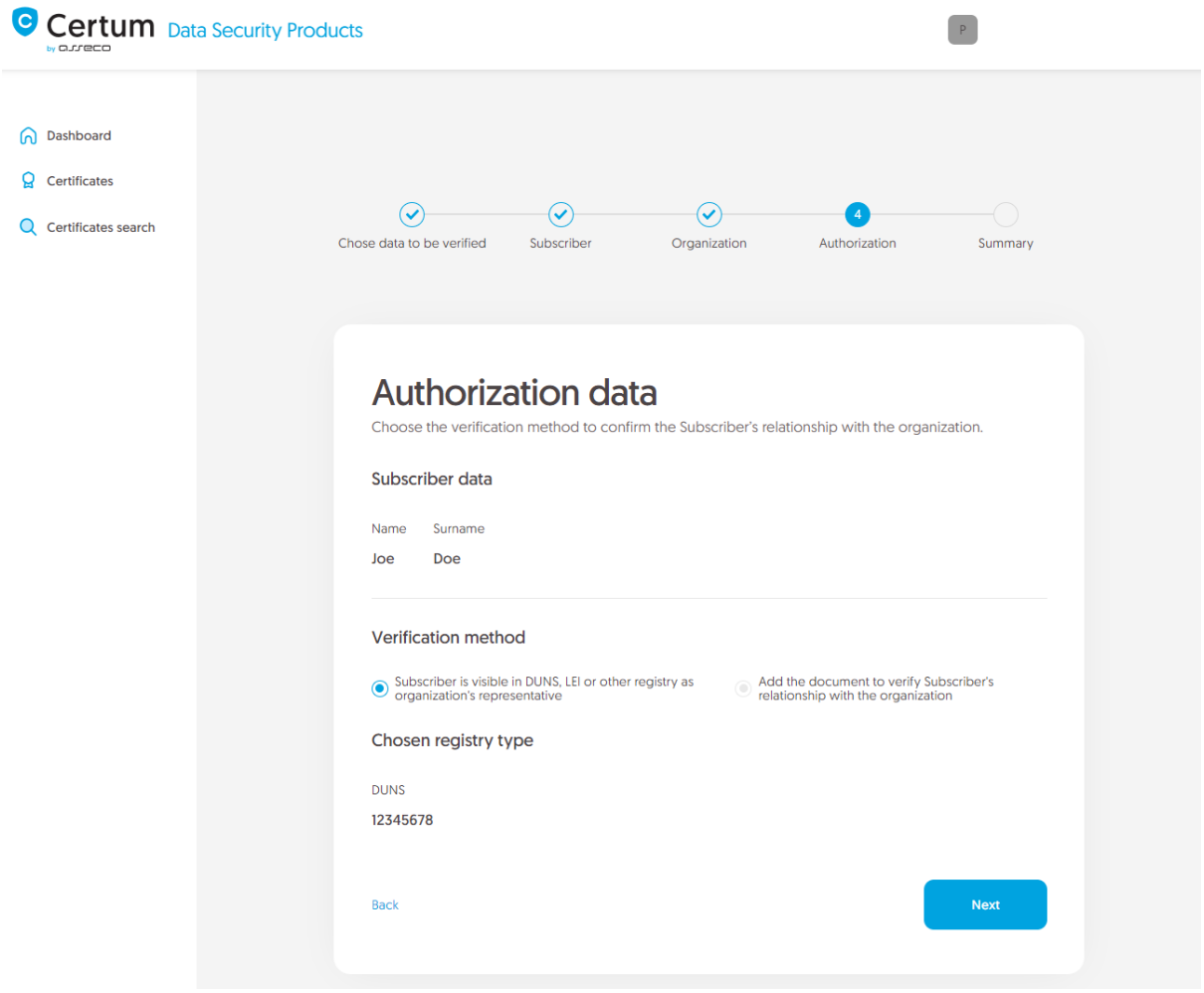


After providing all the required organization's data, proceed to the last stage of providing data for verification step, which is choosing the method of verifying the Subscriber's authorization to represent the organization. This stage is required for **organization** and **sponsor** variants of certificate.

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.

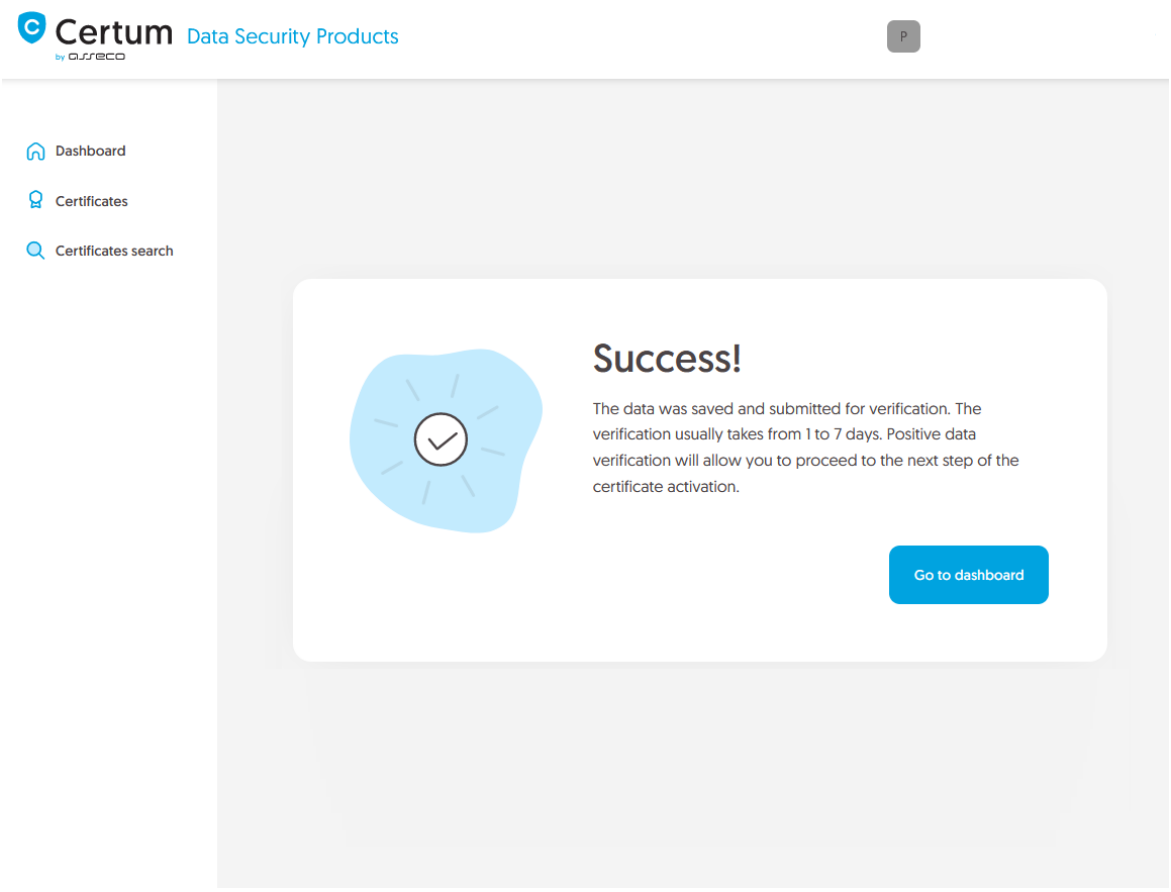


After selecting the authorization verification method go to the next stage.

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. You may check the instruction for automatic identity verification.

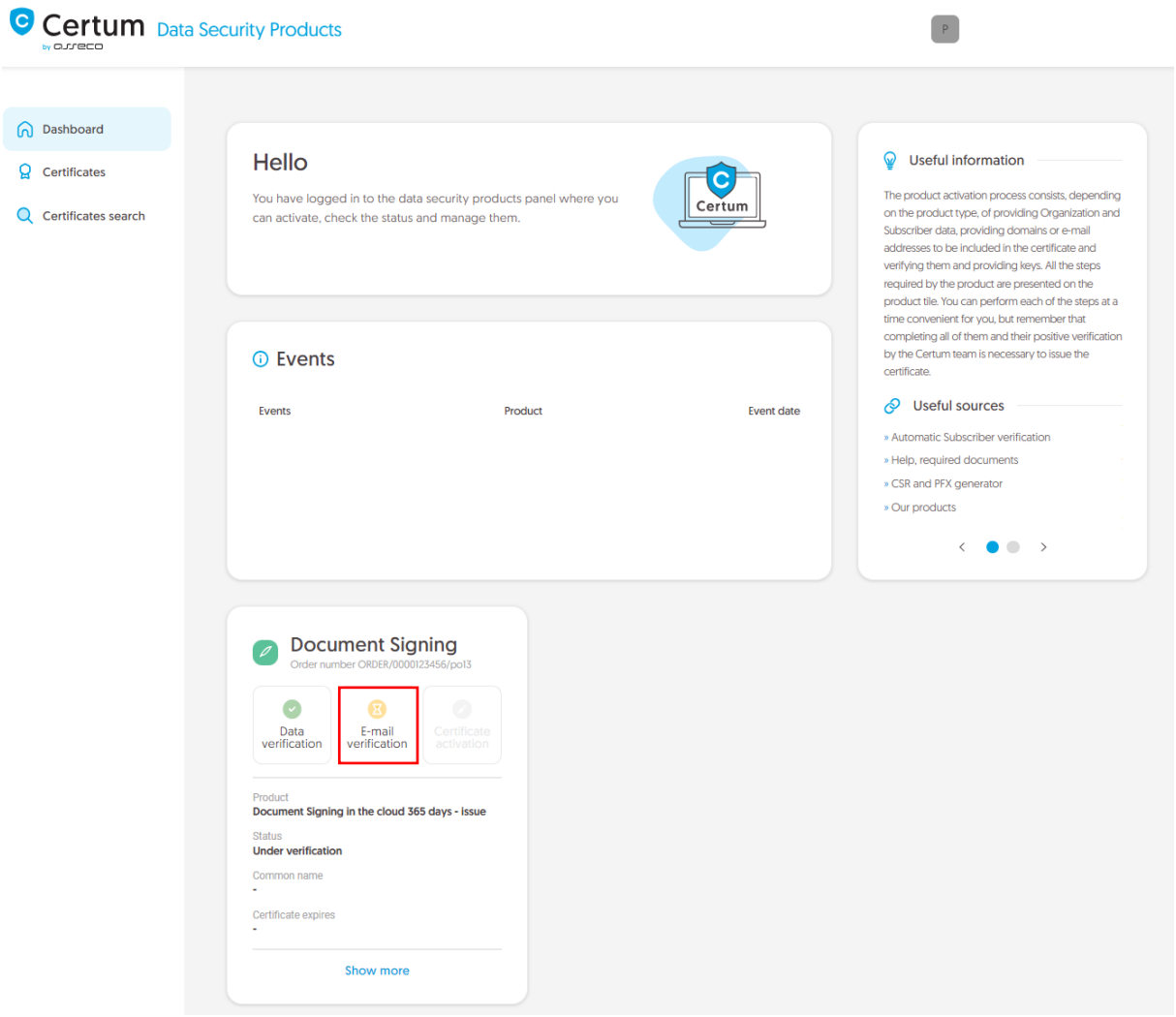


Positive verification of the provided data will allow you to proceed to the step which is generating keys.

E-mail verification step

You will be able to start the e-mail verification step from **Dashboard**, using **E-mail verification** option:

certum.pl
infolinia@certum.pl

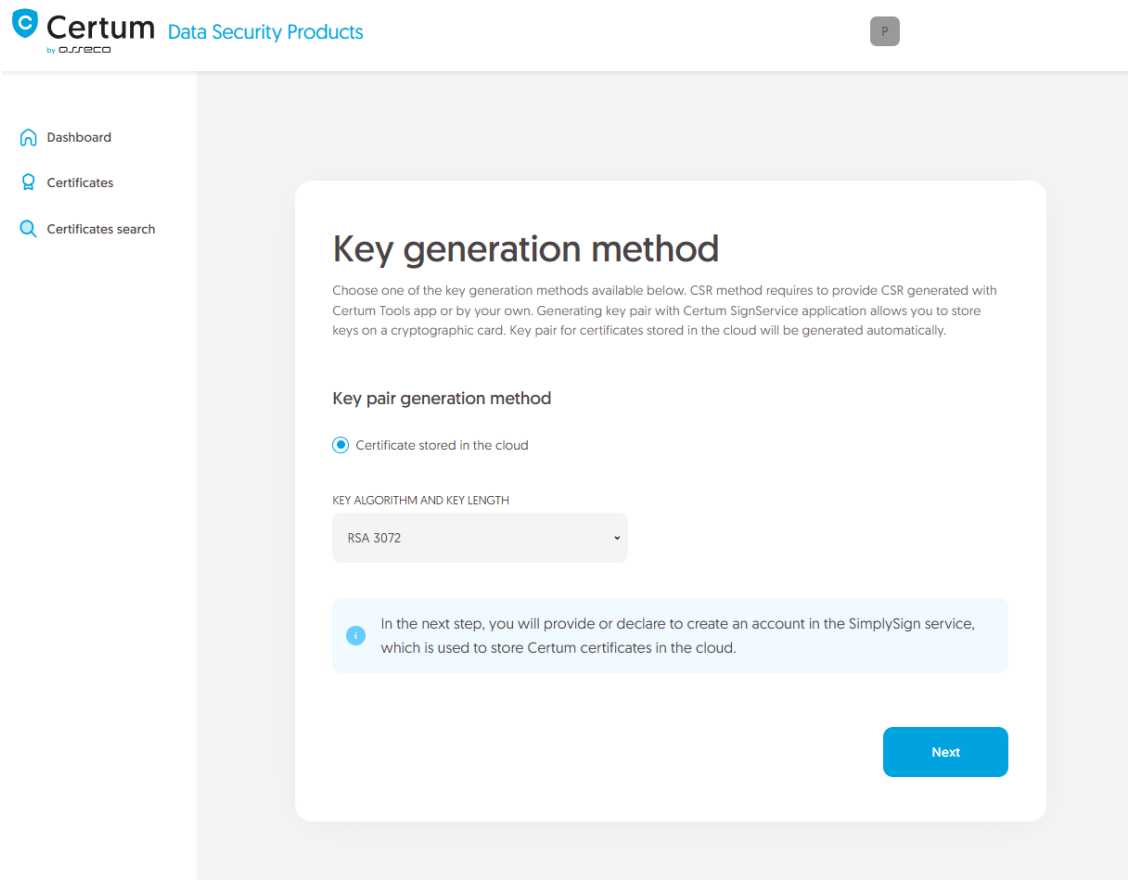


or similar to the **Data verification** step: from the **Certificates** list – choose the certificate you want to activate and use **Provide e-mail address** option.

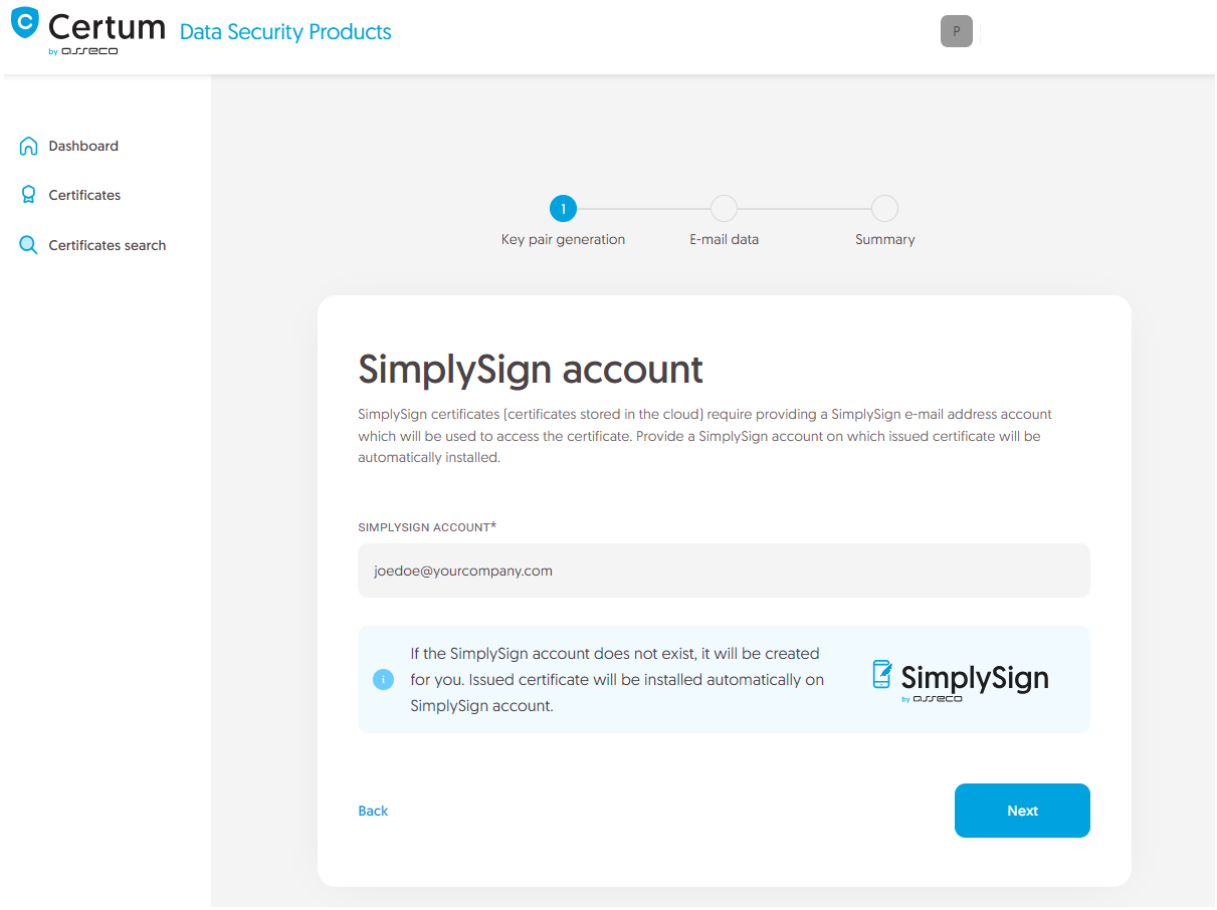
In this step, you will generate a key pair and provide the e-mail to be included in the certificate.

For Document Signing certificates, the available key generation method is **Certificate stored in the cloud** – the keys will be saved on the virtual cryptographic card in the SimplySign cloud.

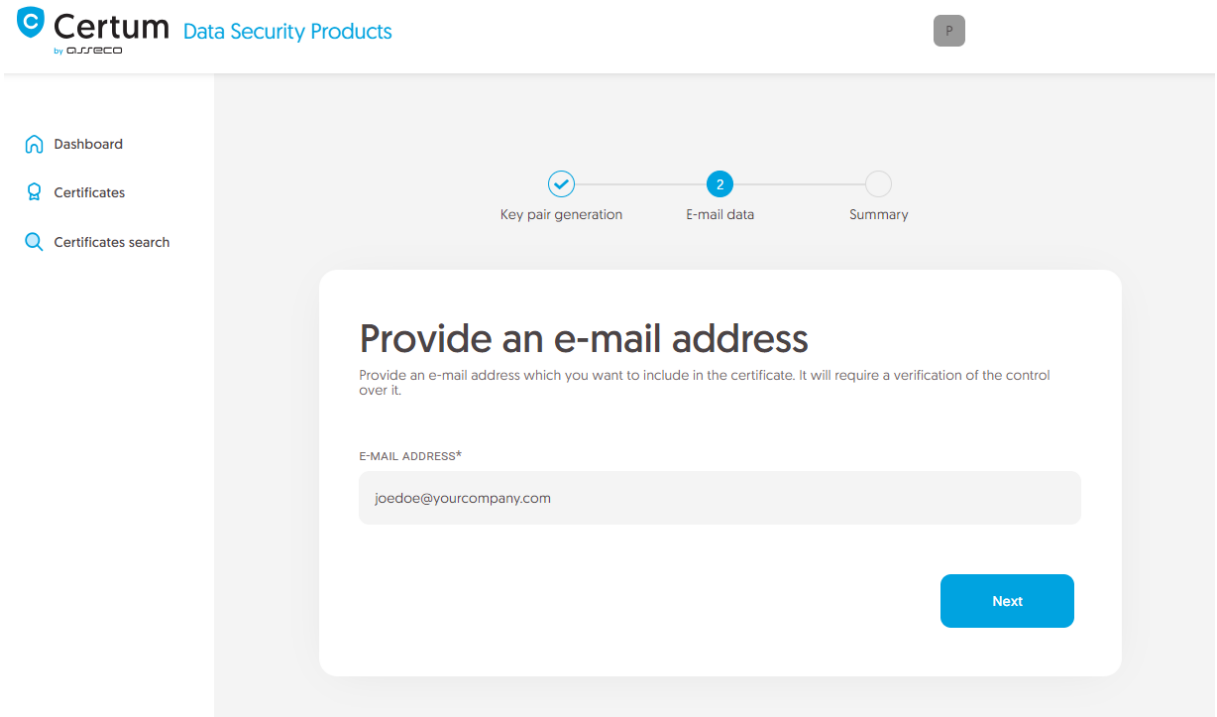
For certificate stored in the cloud, also choose the algorithm and key length. Your choice should depend on the algorithm and key length supported by the application in which you use the certificate or the recommendation of e.g. your IT department.



In the next stage, decide if you have an existing SimplySign account on which certificate will be installed or if you want to provide a new SimplySign account to be automatically created. In both cases provide an e-mail address which will be used as login to the SimplySign service and will allow to access the issued certificate.



After providing the SimplySign account e-mail, provide the e-mail address to include in the certificate and proceed.



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

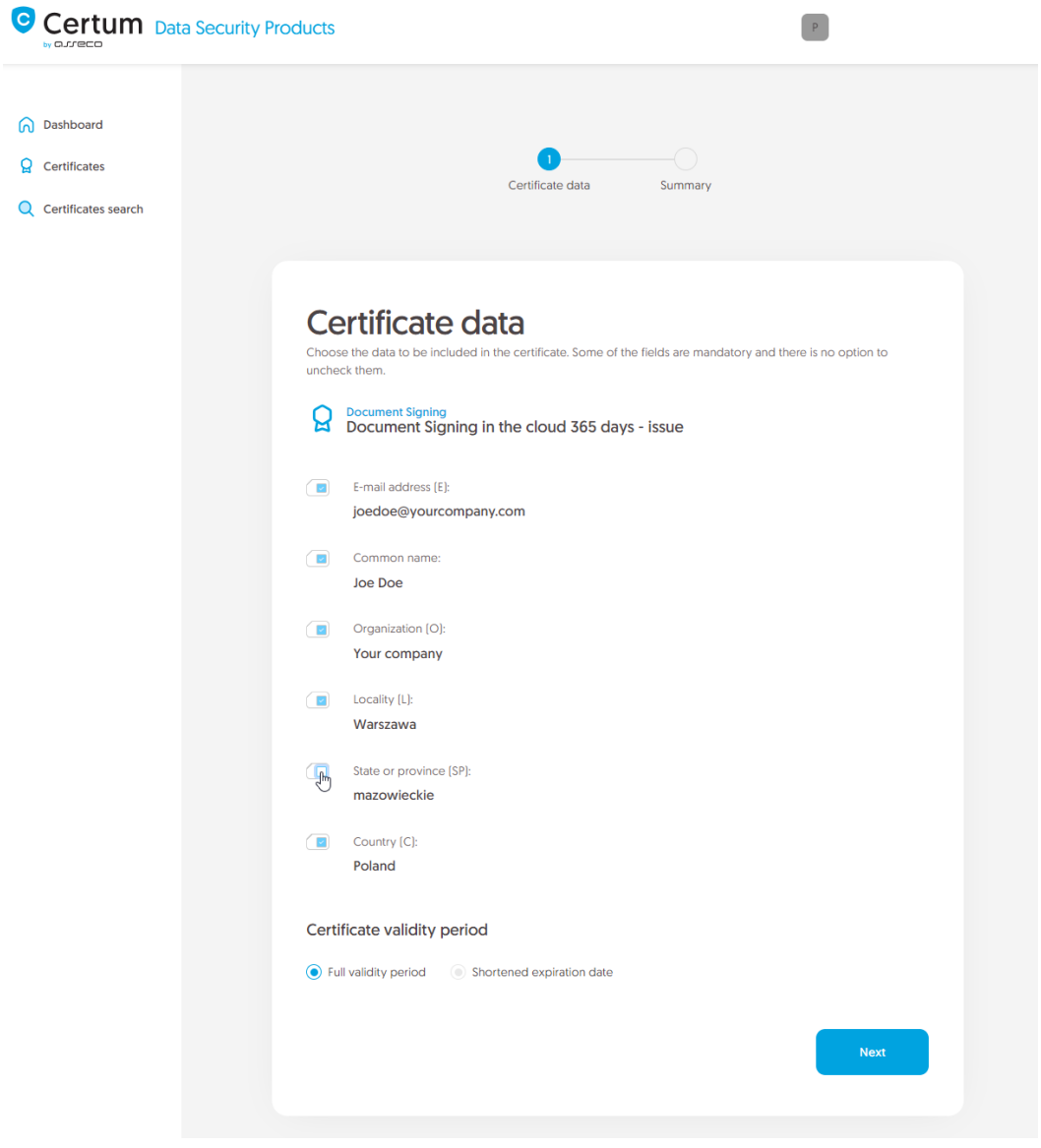
The success screen will inform you that the e-mail address has been saved. Verify the access to it. The SimplySign account e-mail address also was saved. Once certificate is issued, it will be used to access the certificate.

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 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 summary screen and check all of provided data. Mark the required statements and complete certificate activation.

The success screen will inform you that the certificate has been submitted for issuance. Certum will finally verify the data in the certificate and after positive verification, will issue it. The issued certificate will be automatically installed on the SimplySign account provided in previous step. Now you may check the instruction of how to access certificate stored in the cloud and information about required applications to use certificate stored in the cloud.

From the certificate details view you can also download subordinate certificates for your certificate.

certum.pl
infolinia@certum.pl