

Open Source Code Signing in the cloud certificate activation

Ver. 1.0

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step	4
Certificate activation step	8

1. Product description

A Standard Code Signing in the cloud certificate is a certificate stored in the SimplySign cloud service.

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.

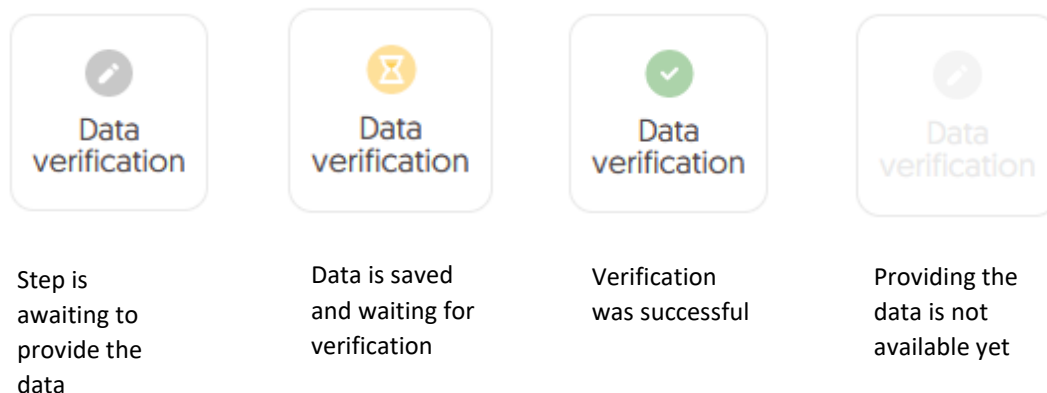
Digital code signing makes using the application safe, which translates into greater trust in your brand and an expansion of your group of users.

2. Certificate activation

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'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:

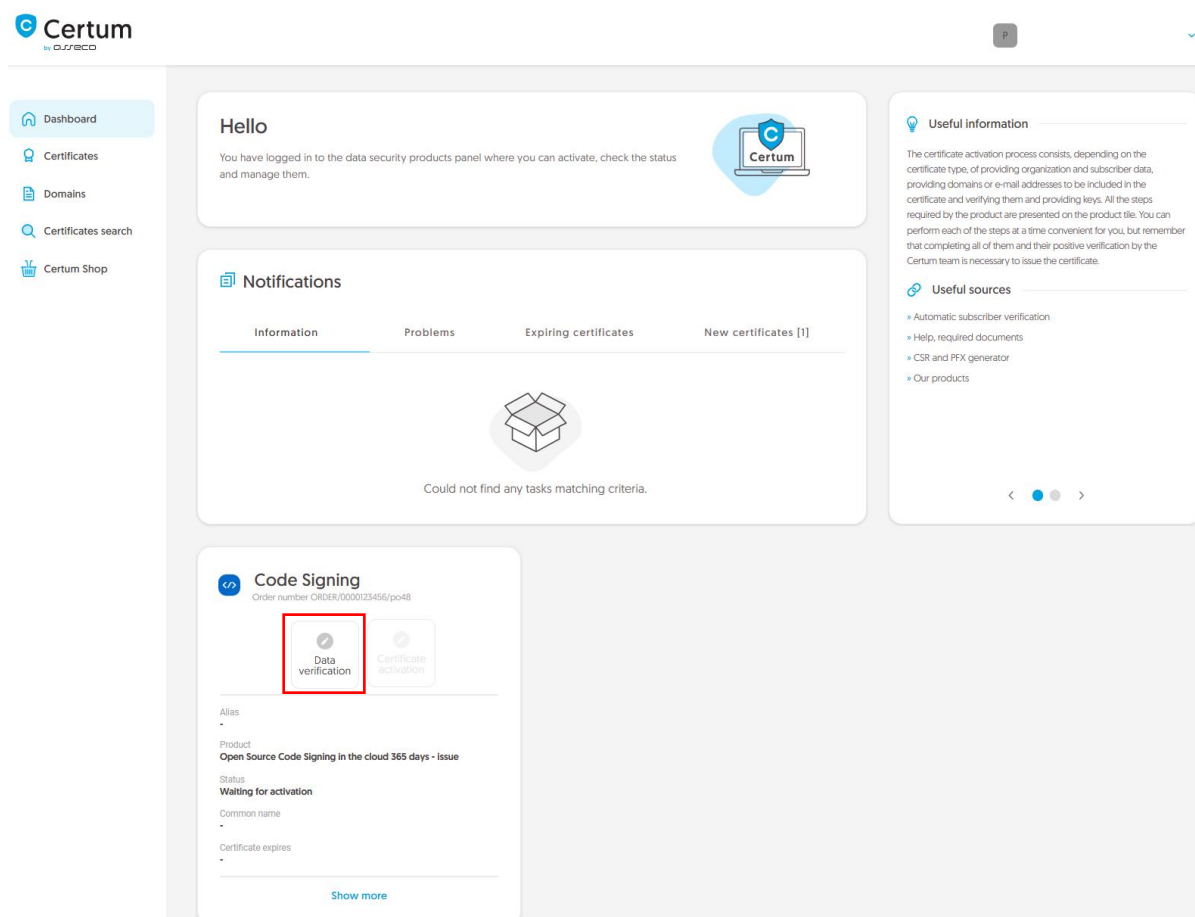


Data verification step

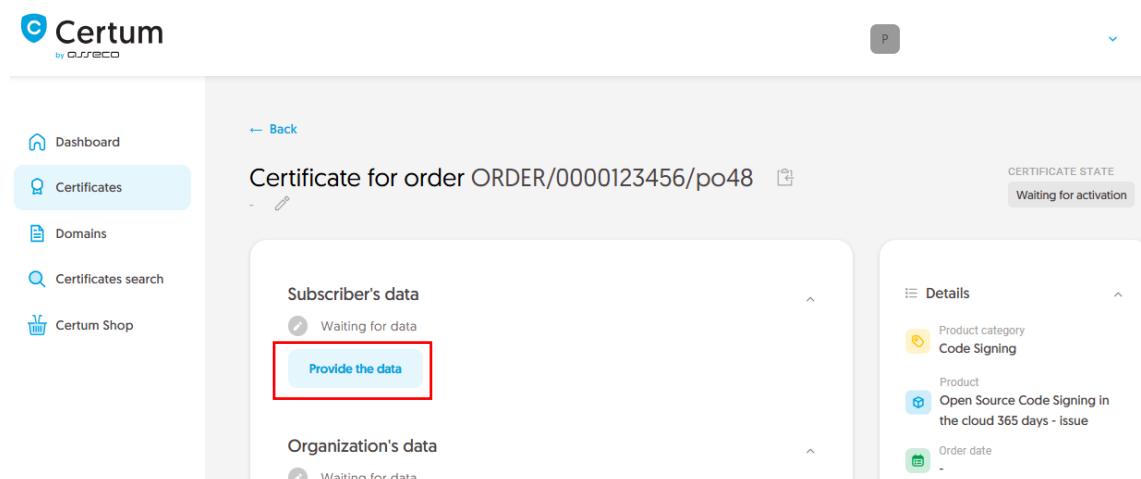
Providing data to be verified is the step in which you provide the data of the subscriber (the person who will be the owner of the certificate). From the data provided here, it will be possible to select data for the certificate in the last step of certificate activation.

The list of supported verification documents you can check at [Information about required documents](#).

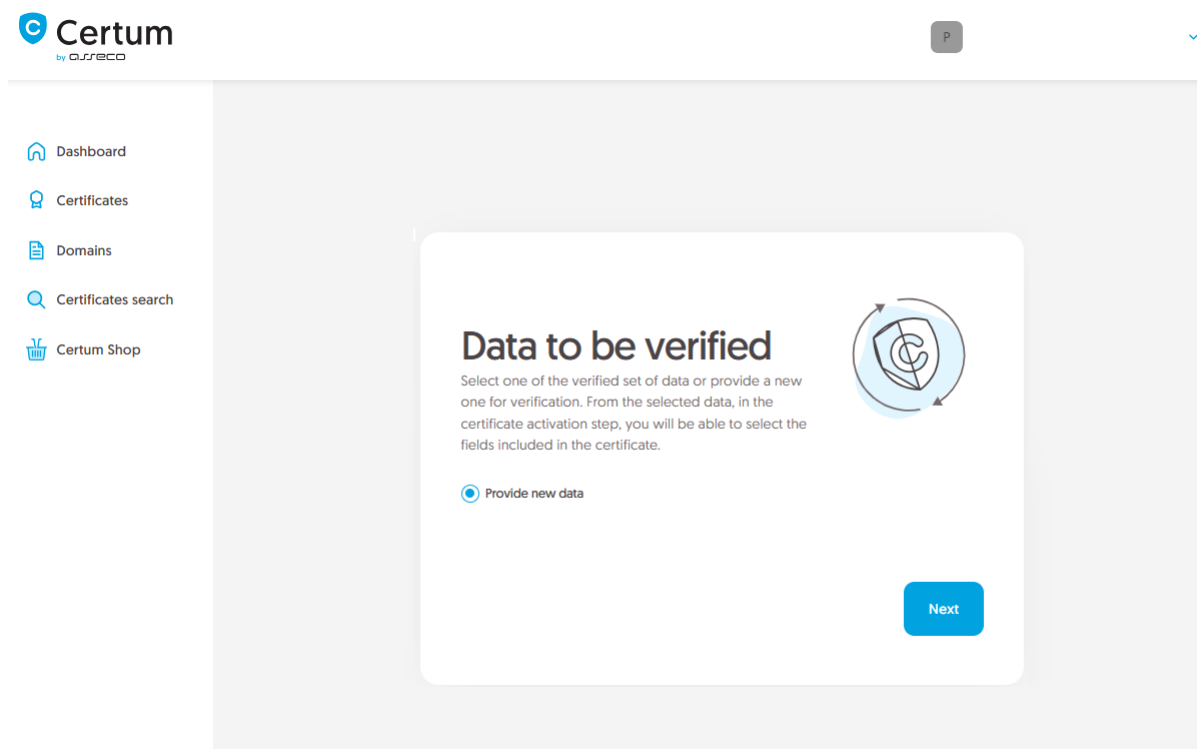
You will be able to start the data verification step from **Dashboard**, using **Data verification** option:



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



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.




The screenshot shows the Certum by OURSEC portal interface. On the left is a sidebar menu with links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area displays a wizard step titled "Data to be verified". Below the title, it says: "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." There is a circular icon with a dollar sign and arrows. Below this, the option "Provide new data" is selected with a radio button. A blue "Next" button is at the bottom right of the wizard box.

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.



P

[Dashboard](#)
[Certificates](#)
[Domains](#)
[Certificates search](#)
[Certum Shop](#)

1

Subscriber

Organization

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@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.

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

After providing the subscriber's data, go to the next stage: providing the organization's data. For Open Source certificate provide the subscriber's address.



P

Dashboard

Certificates

Domains

Certificates search

Certum Shop

Subscriber

2

Organization

Summary

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*

Open Source Developer

Headquarters of the organization

COUNTRY*

Poland [PL]

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warsaw

Verification method

☒ Add the document to verify organization existence

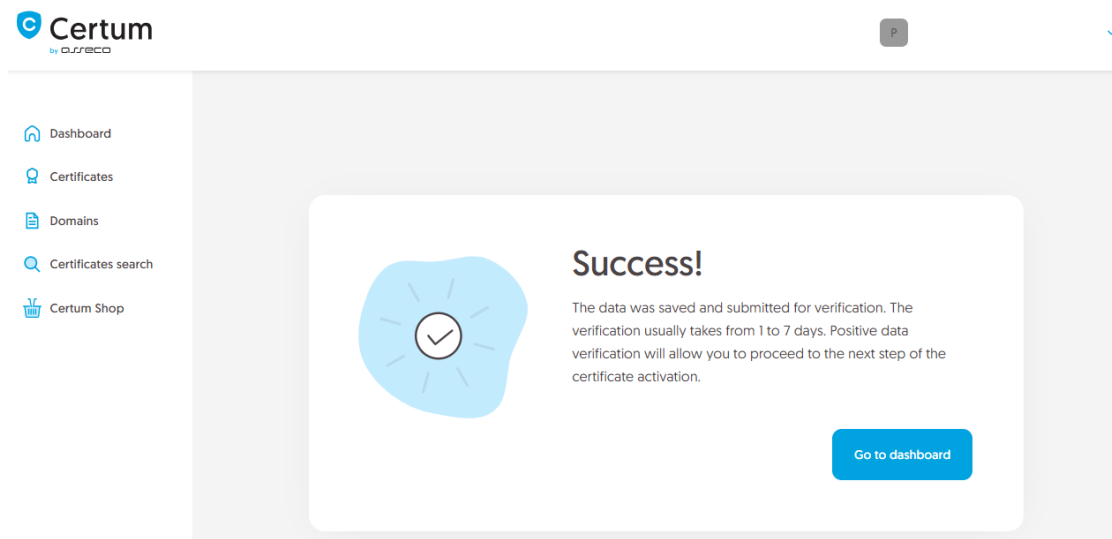
Added documents [0]

[Read about required documents](#)

After providing all the required data, go to the 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.

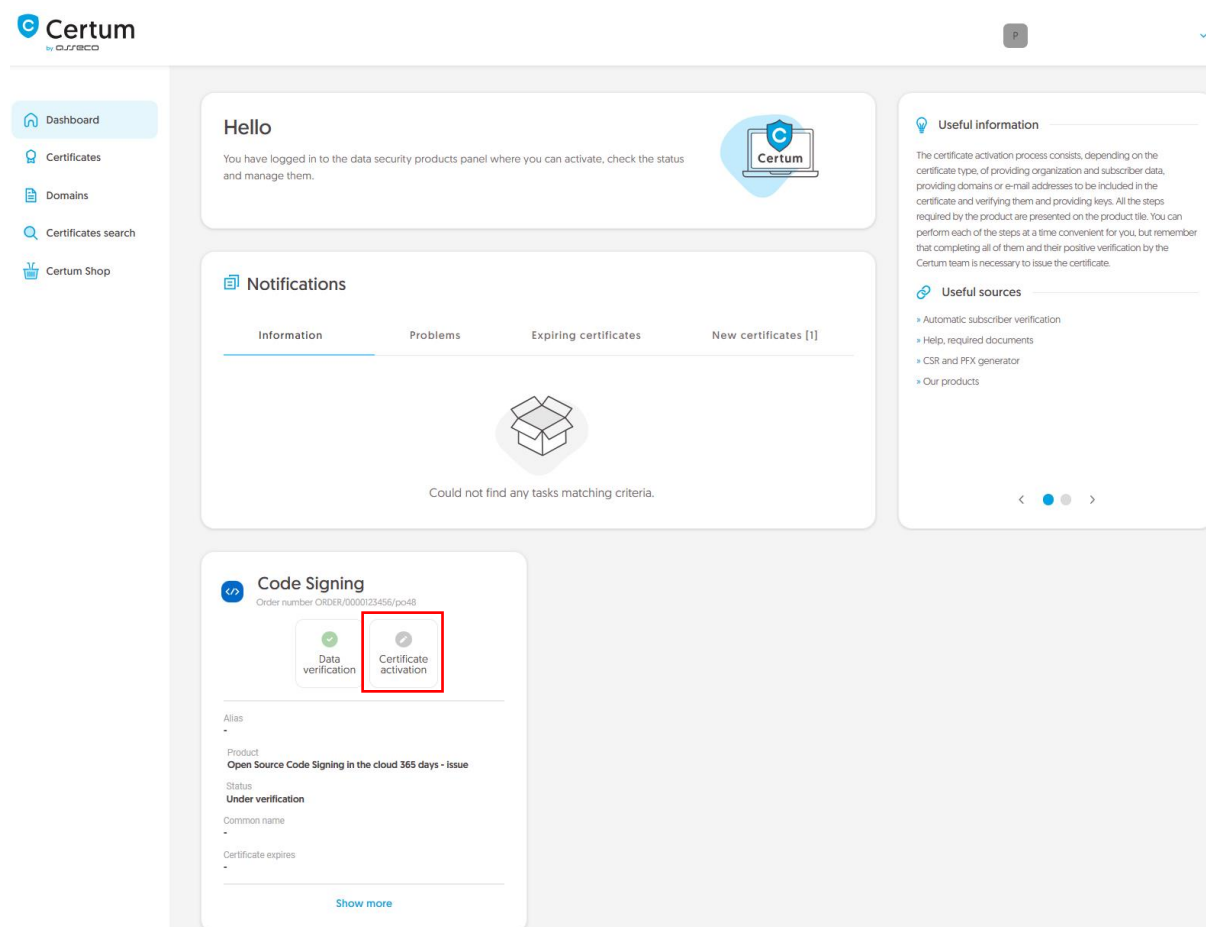
The success screen will inform you that the data have been saved for verification. Certum will verify it. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the subscriber's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



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

Certificate activation step

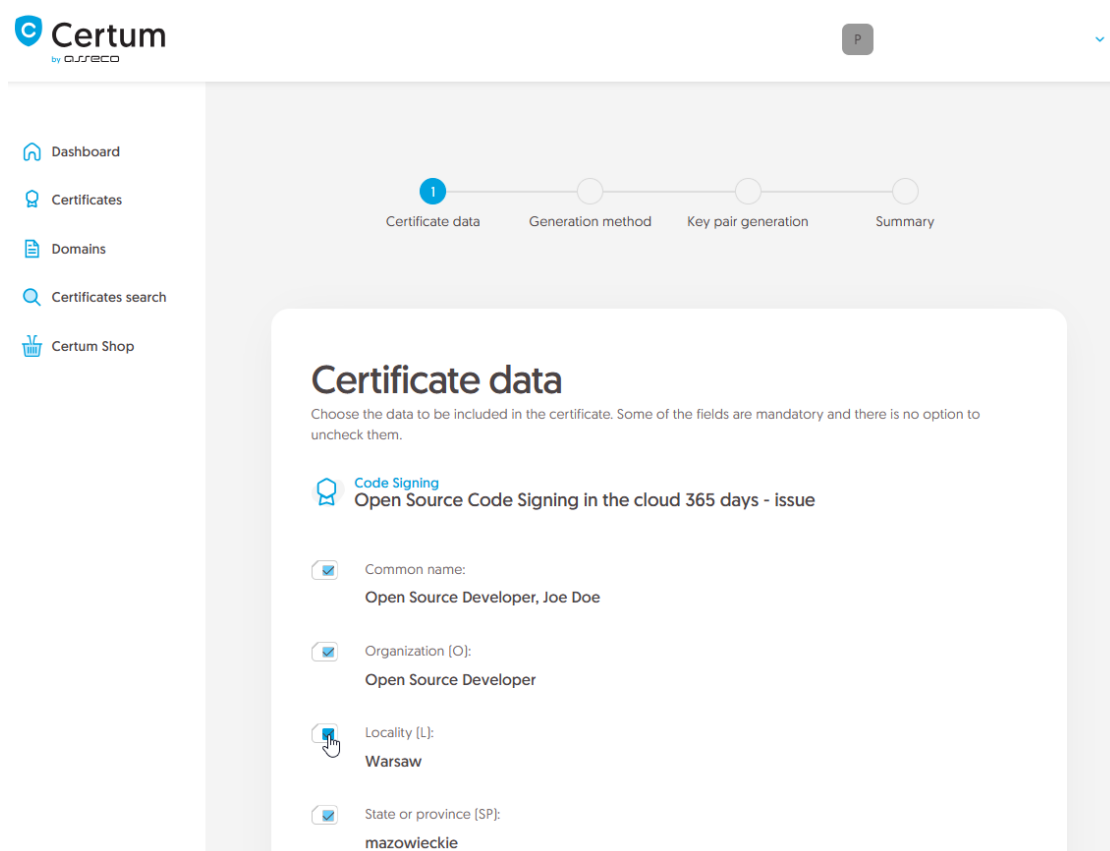
You will be able to start certificate activation step from **Dashboard**, using **Certificate activation** option:



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.



Certum
by CURESCO

Dashboard
Certificates
Domains
Certificates search
Certum Shop

1 Certificate data Generation method Key pair generation Summary

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.

Code Signing
Open Source Code Signing in the cloud 365 days - issue

☒ Common name:
Open Source Developer, Joe Doe

☒ Organization [O]:
Open Source Developer


☒ Locality [L]:
Warsaw

☒ State or province [SP]:
mazowieckie

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

For Code Signing in the cloud 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.



P

[Dashboard](#)
[Certificates](#)
[Domains](#)
[Certificates search](#)
[Certum Shop](#)

✓

2

Certificate dataGeneration methodKey pair generationSummary

Key pair generation method

Key pair for certificates stored in the cloud will be generated automatically.

Key pair generation method

☒ Certificate stored in the cloud






KEY ALGORITHM AND KEY LENGTH





RSA 3072

In the next step, you will provide or declare to create an account in the SimplySign service, which is used to store Certum certificates in the cloud.

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

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.

-  Dashboard
-  Certificates
-  Domains
-  Certificates search
-  Certum Shop


-  Certificate data
-  Generation method
-  Key pair generation
-  Summary

SimplySign account

SimplySign certificates [certificates stored in the cloud] require providing a SimplySign e-mail address account which will be used to access the certificate. Provide a SimplySign account on which issued certificate will be automatically installed.

SIMPLYSIGN ACCOUNT*

Provide a SimplySign account e-mail address

 If the SimplySign account does not exist, it will be created for you. Issued certificate will be installed automatically on SimplySign account.

 **SimplySign**
by ORFECO

[Back](#)

[Next](#)

After providing the SimplySign account e-mail, proceed to the summary and check provided data on the summary screen. If the data is correct, complete the certificate activation step.

The success screen will inform you that the certificate has been submitted for issuance. The issued certificate will be installed on the SimplySign account provided in previous step. Now you may check the [application installation instruction](#) and [how to activate SimplySign application](#).

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