



Document Signing in the Cloud certificate activation

Ver. 3.0

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.....	13

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

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
- **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, 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:

The screenshot shows the Certum customer dashboard. The top left features the Certum logo and a navigation menu with 'Dashboard', 'Certificates', and 'Certificates search'. The main content area is divided into several sections:

- Hello**: A greeting message stating the user is logged in to the data security products panel.
- Events**: A table with columns for 'Events', 'Product', and 'Event date'.
- Document Signing**: A section for a specific product with order number ORDER/0000123456/pol3. It contains three buttons: 'Data verification' (highlighted with a red box), 'E-mail verification', and 'Certificate activation'. Below the buttons, the product name is 'Document Signing in the cloud 365 days - Issue', and the status is 'Waiting for activation'. Other fields like 'Common name' and 'Certificate expires' are currently empty.
- Useful information**: A section providing details about the product activation process.
- Useful sources**: A list of links for 'Automatic Subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'.

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

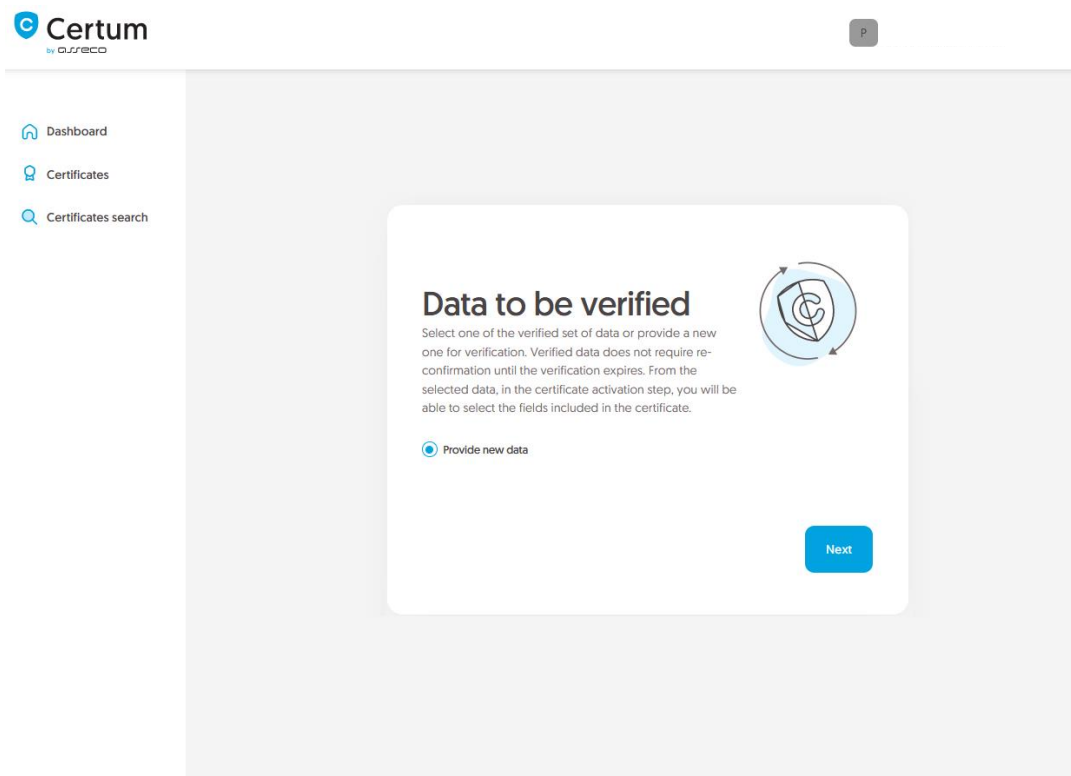
As the **partner**, you will be able to start the data verification step from **Dashboard**, using new order option. After choosing the product type and providing the order details, you will be able to provide the data used in the first step of issuing the certificate.

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.



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
by eSSECO

Dashboard
Certificates
Certificates search

Chose data to be verified **2** Subscriber Organization Authorization Summary

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

E-MAIL ADDRESS OF THE SUBSCRIBER*

joedoe@yourcompany.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 **individual** certificate variant, provide address details of subscriber's residence. Next, go to the data verification step [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*

Joe Doe

Headquarters of the organization

COUNTRY*

Poland

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warszawa



As a natural person you do not represent any organization. Provide the Subscriber's address data, which will be included in the certificate.

Back

Next

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.

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*

DUNS

REGISTRATION NUMBER IN THE REGISTRY*

12345678

[Back](#)

[Next](#)

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.



Certum
by *csreco*

Dashboard
Certificates
Certificates search

Chose data to be verified ✓ Subscriber ✓ Organization ✓ Authorization 4 Summary

Authorization data

Choose the verification method to confirm the Subscriber's relationship with the organization.

Subscriber data

Name Surname
Joe Doe

Verification method

Subscriber is visible in DUNS, LEI or other registry as organization's representative Add the document to verify Subscriber's relationship with the organization

Chosen registry type

DUNS
12345678




Back Next

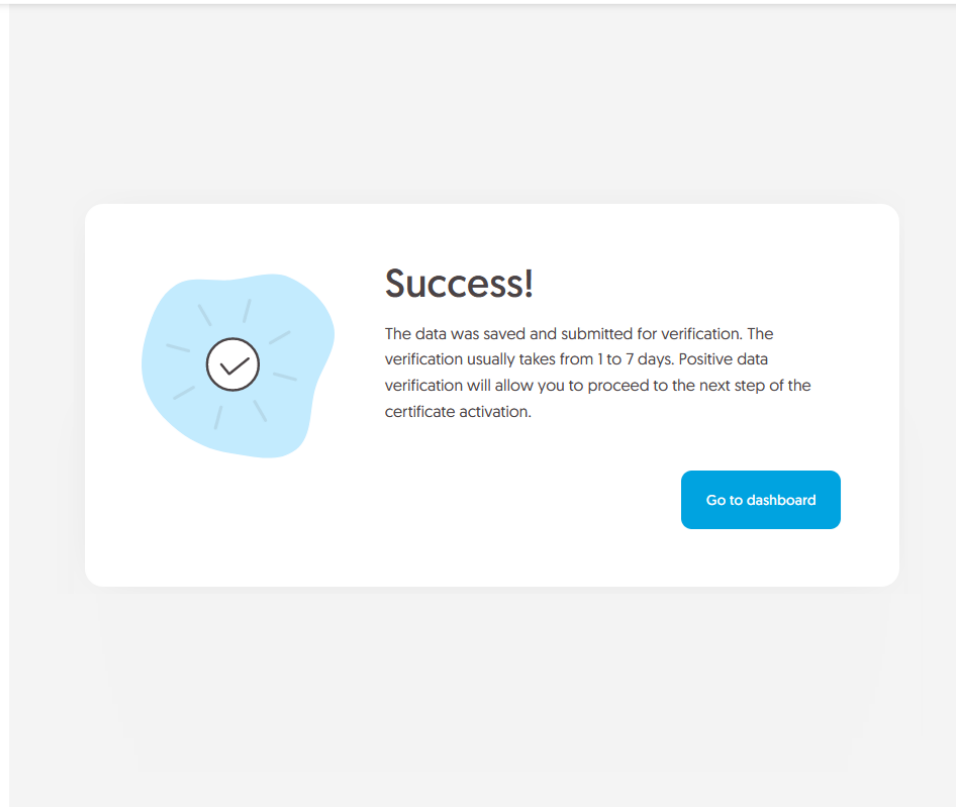
After selecting the authorization verification method go to the next stage.

Data verification step summary

Check provided information on the summary screen. If the data is correct, mark the 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. You may check the [instruction for automatic identity verification](#).

-  Dashboard
-  Certificates
-  Certificates search



The screenshot shows a success message in a web application. On the left, there is a blue circular icon with a white checkmark inside. To the right of the icon, the word "Success!" is displayed in a bold, dark font. Below this, a paragraph of text explains that the data has been saved and submitted for verification, and that the process usually takes 1 to 7 days. A blue button with the text "Go to dashboard" is located at the bottom right of the message box. The background of the page is light gray, and a sidebar with navigation options is visible on the left.

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:

- [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

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](#)

Document Signing


Order number ORDER/0000123456/po13



Data verification



E-mail verification



Certificate activation

Product
Document Signing in the cloud 365 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 will provide the e-mail to be included in the certificate.

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 fields you want to include in the certificate. 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.

 **Document Signing**
Document Signing in the cloud 365 days - issue

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

Common name:
Joe Doe

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 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.

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

Certificate data **2** Generation method Key pair generation Summary

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.

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.



[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. 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 [application installation instruction](#) and [how to activate SimplySign application](#)

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