

Certum Premium EV SSL certificate activation

Ver. 1.6

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Data verification step	4
Domain verification step	9
Certificate activation step	11

1. Product description

An SSL (TLS) certificate is a type of certificate used in security protocols to certify the authenticity of a domain and its owner. It encrypts and secures website traffic, including the transmission of confidential data that customers enter on your website. Thanks to the SSL certificate, your customers' personal data, logins and passwords, credit card numbers and other data will be secured.

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 organization's data and the verification
- **Domain verification** – providing the domains 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 ale waiting
for verification



Verification
was successful



Providing the
data is not
available yet

Data verification step

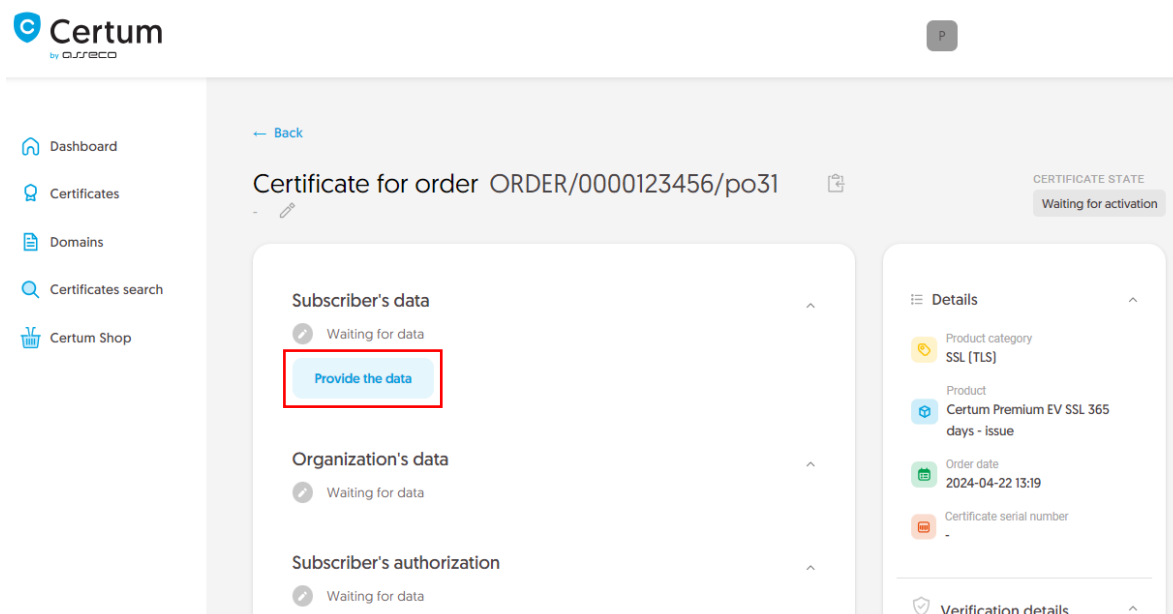
Providing data to be verified is the step in which you provide the data of the organization for which the certificate will be issued, the data of the subscriber (the person who represents the organization and will be the owner of the certificate) and the data of the subscriber's authorization to represent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

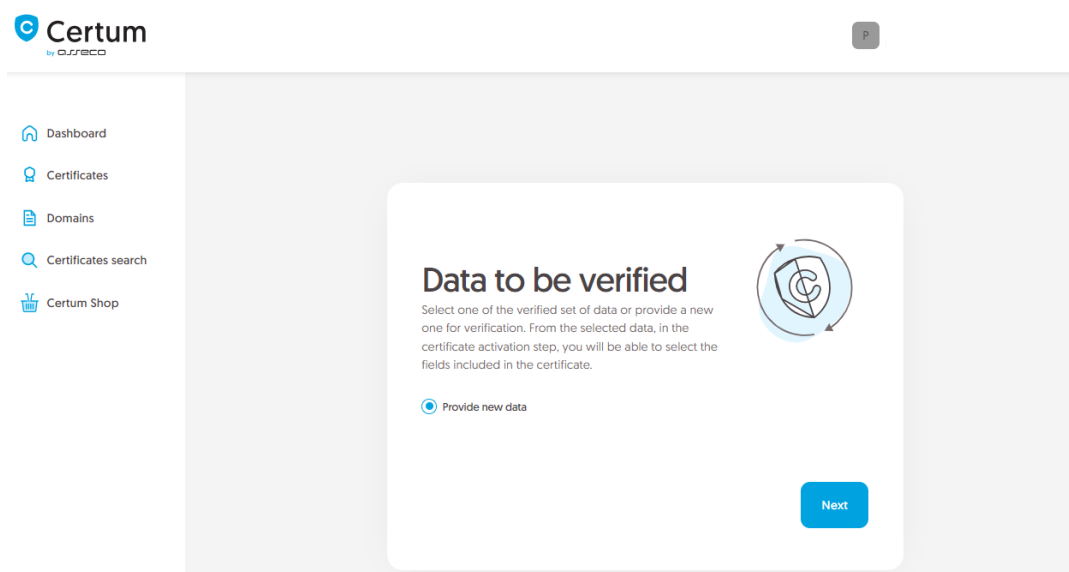
The screenshot displays the Certum dashboard interface. On the left, a navigation menu includes 'Dashboard', 'Certificates', 'Domains', 'Certificates search', and 'Certum Shop'. The main content area features a 'Hello' message, an 'Events' table, and a 'Useful information' section. A 'Useful sources' section lists links for 'Automatic subscriber verification', 'Help, required documents', 'CSR and PFX generator', and 'Our products'. The 'SSL [TLS]' section, with order number ORDER/0000123456/po31, shows three steps: 'Data verification' (highlighted with a red box), 'Domain verification', and 'Certificate activation'. Below these steps, details for the 'Certum Premium EV SSL 365 days - Issue' certificate are shown, including its status 'Waiting for activation', common name, and expiration date. A 'Show more' link is at the bottom of this section.

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.

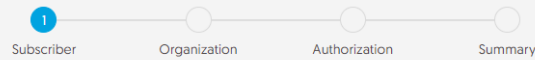
The wizard will guide you through the process of providing the data. In the first stage, choose to provide new data. In the future, it will be possible to use them to issue another certificate.



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.

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 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@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. Here, provide the organization's details, the address of its headquarters and the city, state and country of the registration authority where the organization's legal existence was established. 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

BUSINESS CATEGORY*

Private Organization

REGISTRATION NUMBER*

12345678

Headquarters of the organization

COUNTRY*

Poland

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warszawa

POSTAL CODE*

10-100

STREET AND HOUSE NUMBER*

Jana Kochanowskiego 1

Jurisdiction of incorporation

JURISDICTION OF INCORPORATION COUNTRY NAME*

Poland

JURISDICTION OF INCORPORATION STATE OR PROVINCE NAME*

mazowieckie

JURISDICTION OF INCORPORATION LOCALITY NAME*

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.

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 registry**. However, this does not prevent you from adding a document confirming the subscriber's authorization.



Certum
by *o.r.e.c.o.*

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Subscriber Organization **Authorization** 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

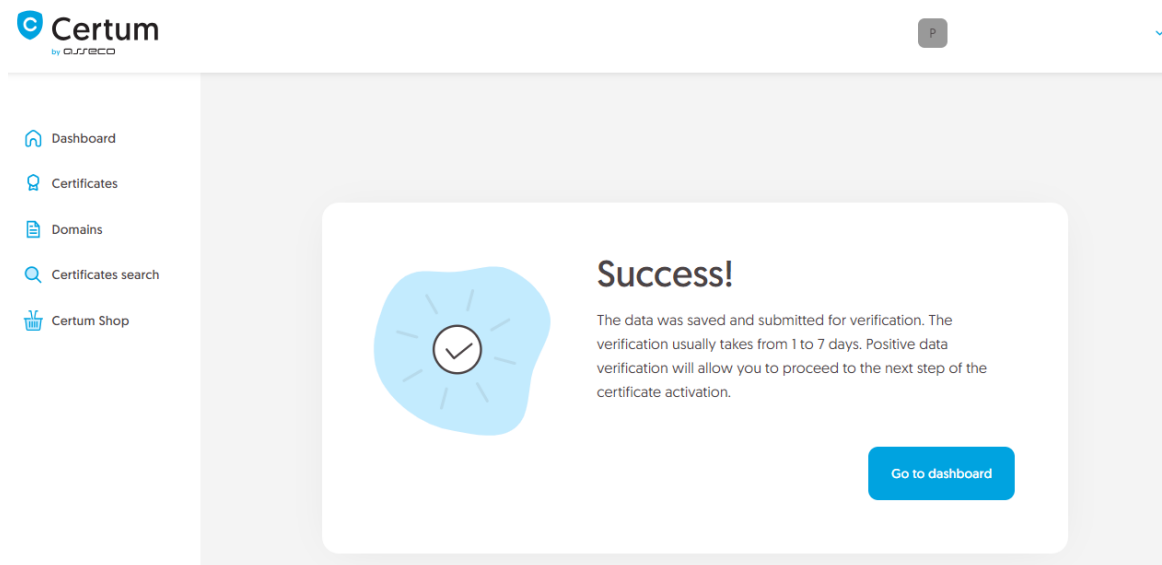
Chosen registry type

DUNS
12345678

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

After selecting the authorization verification method 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](#).



Positive verification of the provided data will allow you to proceed to the next step providing the domains.

Domain verification step

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

The screenshot shows the Certum dashboard with a sidebar on the left containing navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area is divided into several sections:

- Hello:** A greeting message stating, "You have logged in to the data security products panel where you can activate, check the status and manage them." accompanied by a Certum logo icon.
- Events:** A table with columns for Events, Product, and Notification date.
- Useful information:** A text block explaining the certificate activation process, including steps like providing organization and subscriber data, domains, and keys.
- Useful sources:** A list of links: Automatic subscriber verification, Help, required documents, CSR and PFX generator, and Our products.
- SSL [TLS]:** A detailed view for a certificate with order number ORDER/0000123456/po31. It features three status indicators: Data verification (green checkmark), Domain verification (grey circle with a slash, highlighted with a red box), and Certificate activation (grey circle with a slash). Below these are fields for Alias, Product (Certum Premium EV SSL 365 days - issue), Status (Under verification), Common name, and Certificate expires.

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

In this step, you will provide the domains to be included in the certificate.

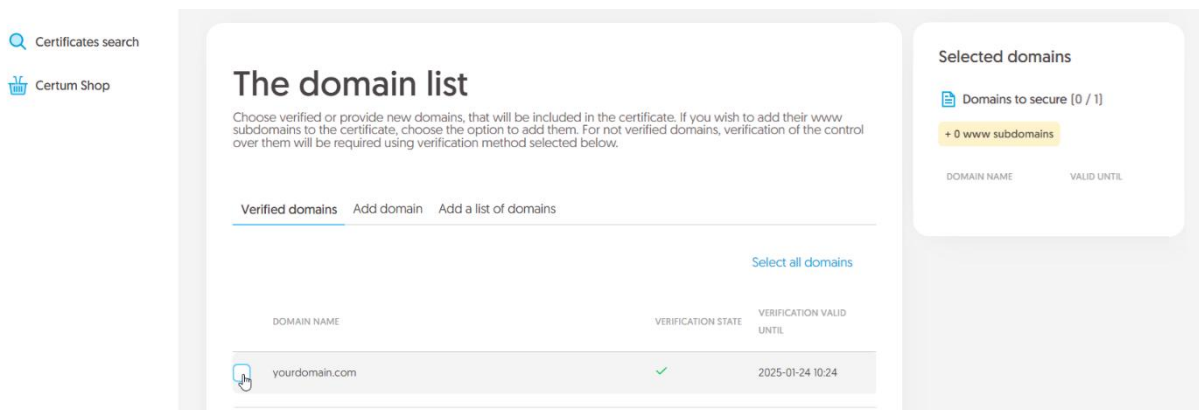
Provide the new domains to the list using **Add domain** tab:

The screenshot shows the 'The domain list' interface in the Certum dashboard. At the top, there are two tabs: 'Domain data' (active) and 'Summary'. The main content area includes:

- The domain list:** A section with a description: "Provide the domains that will be included in the certificate. If you wish to add their www subdomains to the certificate, choose the option to add them. Verification of the control over the domains will be required using verification method selected below." Below this is a text input field with the placeholder "yourdomain.cd" and a yellow "Add domain" button. The "Add domain" text in the input field is highlighted with a red box.
- Selected domains:** A section titled "Domains to secure (1 / 1)" showing a table with one domain: "yourdomain.com". The table has columns for "DOMAIN NAME" and "VALID UNTIL". The "VALID UNTIL" column shows "verification required" and a trash icon. Below the table is a toggle switch labeled "add www. subdomains to the list".

A blue arrow points from the "Add domain" button in the "Selected domains" section to the "Add domain" button in the "The domain list" section.

or choose verified earlier domains from **Verified domains** tab:



If you have a list of domains in a text file, you can paste its content on the **Add a list of domains** tab. More about domain verification before starting the certificate activation process you can check in [domain management instruction](#) (this option is currently available only for **customers**).

If you want to add a free www subdomain to a given domain in the certificate, provide it to the list or use the **add www. subdomains to the list** switch.

At this stage, if the domain requires verification, choose the method to verify that you have control over the domains and if you wish, provide the e-mail address of the person who will receive the domain verification code. If you need help with choosing a domain verification method, please check supported [verification methods](#).

After providing the domains, their verification method and proceeding, check provided data on the summary screen. If the data is correct, complete the domain verification step.

The success screen will inform you that your domains have been saved. Verify them using chosen earlier verification method or if they are already verified, proceed to the last step, which is **Certificate activation**.

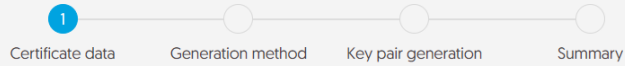
Certificate activation step

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 you will choose the Common name of the certificate and generate a key pair.


Choose which of the domains you want to set as the Common name of the certificate (if more than one domain is provided) and the fields for the certificate. Some fields are required and cannot be unmarked.

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



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 Premium EV SSL 365 days - issue

Common name:
yourdomain.com

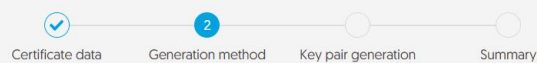
Organization [O]:
Your company

Locality [L]:
Warszawa

Once you have chosen the Common name and the fields for the certificate, go to the key pair generation.

For SSL certificates, the available key generation method is CSR which means pasting a certificate signing request generated by a generator, e.g. [Certum Tools](#), or by the application/server where the certificate will be installed.

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



Key pair generation method

CSR method requires to provide CSR generated with Certum Tools app or by your own.

Key pair generation method

CSR

[Back](#)

[Next](#)

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.



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 and proceeding will display the summary screen. 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. Certum will finally verify the data in the certificate and after positive verification, will issue it. 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.

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.