

Certum Commercial SSL certificate activation

Ver. 1.7

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Domain verification step	3
Certificate activation step	6

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:

- **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 waiting for
verification



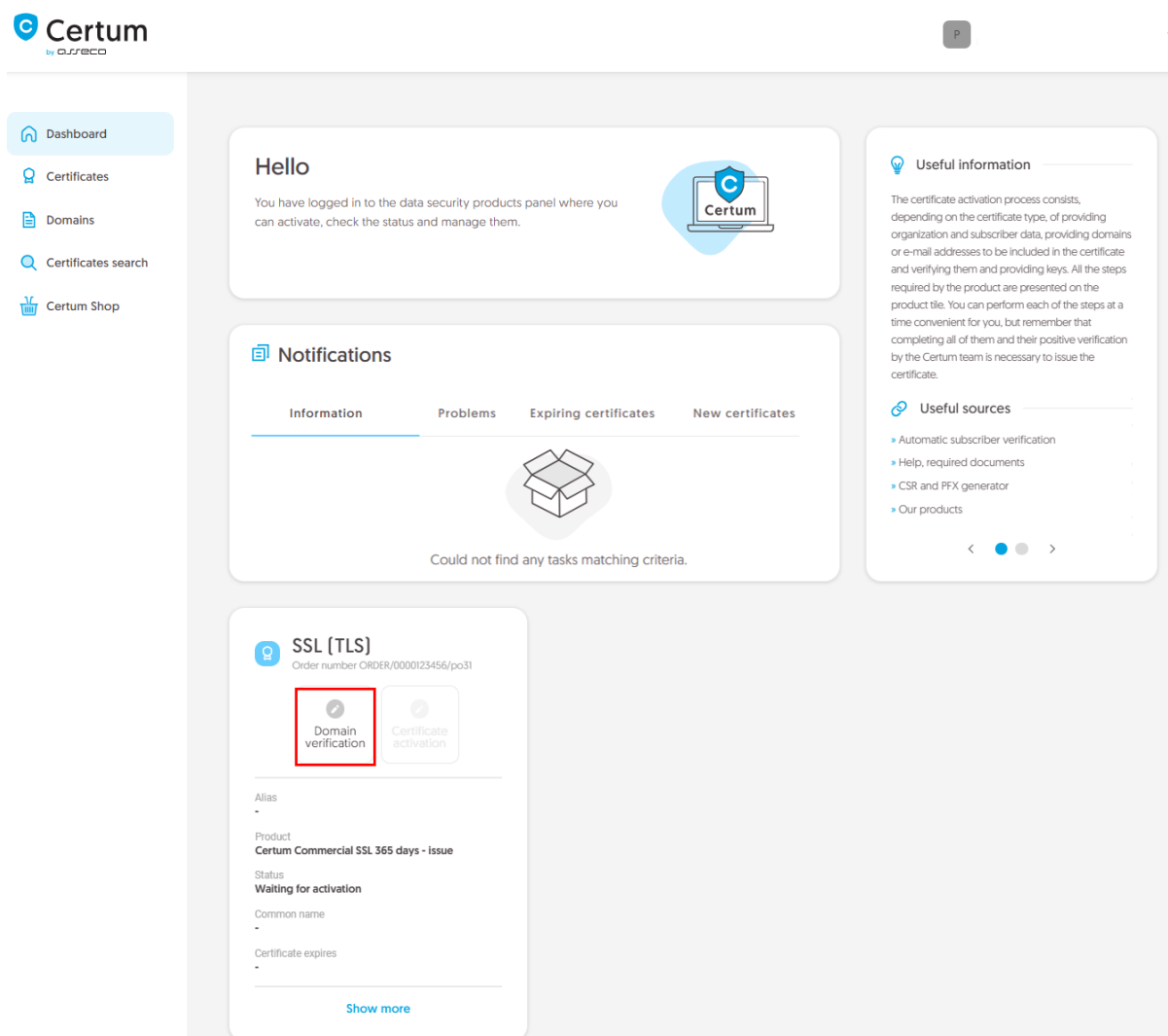
Verification
was successful



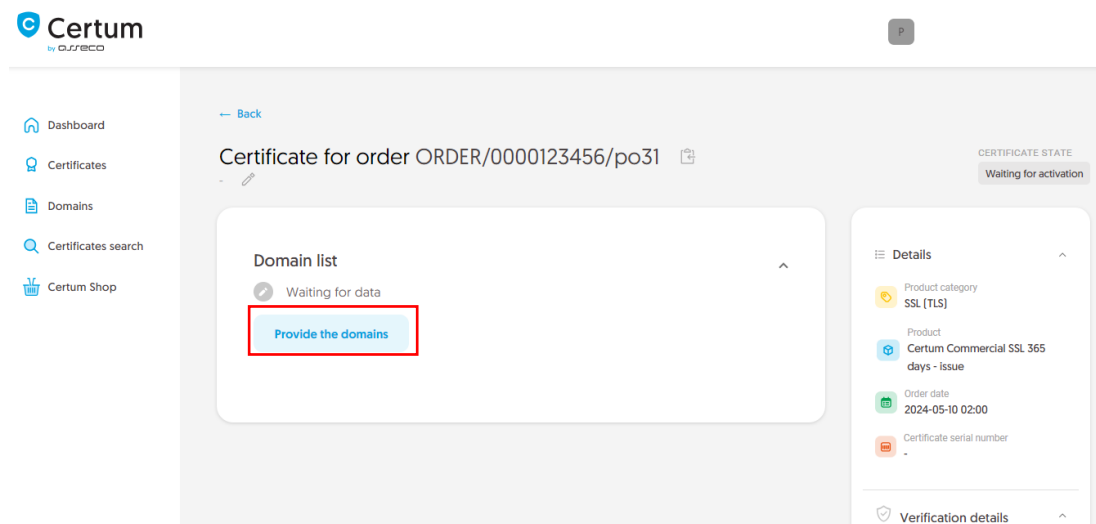
Providing the
data is not
available yet

Domain verification step

As the Certum **customer**, you will be able to start the domain verification step from **Dashboard**, using **Domain verification** option:



or from the **Certificates** list – choose the certificate you want to activate and use **Provide domains** option.



As the **partner**, you will be able to start the domain 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.

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:

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

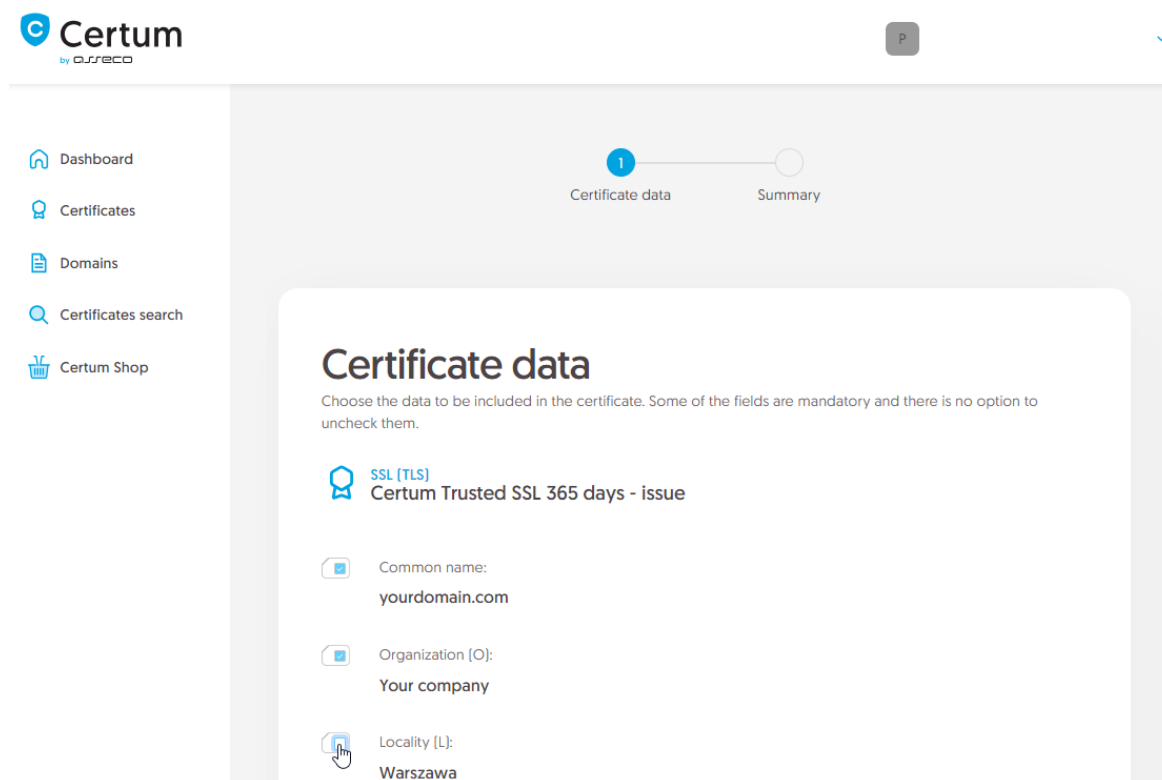
The success screen will inform you that your domains have been saved. Verify them using chosen earlier verification method or if they are already verified, proceed to the last step, which is **Certificate activation**.

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).




The screenshot shows the Certum dashboard interface. On the left is a sidebar with navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area is titled 'Certificate data' and includes a progress indicator with two steps: 'Certificate data' (active) and 'Summary'. Below the title, a message states: 'Choose the data to be included in the certificate. Some of the fields are mandatory and there is no option to uncheck them.' The form displays three fields, each with a checkbox icon:

- SSL [TLS]**
Certum Trusted SSL 365 days - issue
- Common name:**
yourdomain.com
- Organization [O]:**
Your company
- Locality [L]:**
Warszawa

Once you have chosen the Common name, 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

Certificate data

Generation method

Key pair generation

Summary

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.



Dashboard

Certificates

Domains

Certificates search

Certum Shop

Certificate data

Generation method

Key pair generation

Summary

CSR

Enter Certificate Signing Request [CSR] or use the Certum Tools application to generate new CSR.

```

19Rh02s4ESCW9nUrX2VR/qVnX3g5dG0epH+Hn75QsRpd3Xb7dnThbkPctu0LWtcWc
tuiAv5SuF9g4eIxLBu6YD0M6PZv6081wUmGIkCIcHQqMeaamZAnY8VvtDmG0uICp
1KYOpA4JC4+AesquMI/DPluzwWkHp0/1+5nYkWt6yWFqvX0RH0ueD8tfamBVVzHj
mEbAJPkCWzLCRhsa/LH1/NW1JFYZSibd3ZWtWbW3PAL/#7FNBwyAF0kEYREuSgGU
ZdV6BLUZfuF6HIExd7+cWS01fU4ypFe/GuoEI0avyOxfQIDAQABMA0GCSqGSIb3
DQEBChUAA4IBAQAjImSCNzjhTXr8uZ7j3f8uCPRAyExSEder4sH3qIO//hnZdd+/
W7yKVPYyliflMfRjXTP+SenZa3HXmMseSuhtcrkkKdWY5Fyy0P+1BEBWOW+ZpnmuxKg
9hFXTG0NMiB5SubsIyHSzaQPnnIqKuOHJ2WA8hkcP17Q0zUpW4yHnBzZTgBHFv/X
eGEIMdM7/C37MH6ipzJkz9D+1URtaT+uDwg8stDES1/aW6kQj6NZ6nJ3wXXzRI
1Q0k2Lt/SK0LxiZ+25EX3/adbi7D8wZPbxcsFmTBD5XGeHJ6SeRiCFUFvxmc6L
wU05nwbmko/BK+VYJ016BdBKBo+1vtH/c11s
-----END CERTIFICATE REQUEST-----

```

Correct



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. 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.