Certum Trusted SSL certificate activation

Ver. 1.6

asseco

Certum
by asseco

## Table of contents

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

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 organization's data and the verification
- **Domain verification** – key pair generation, providing the domains and the verification
- **Certificate activation** – choosing the fields to include in the certificate and submit to issue.
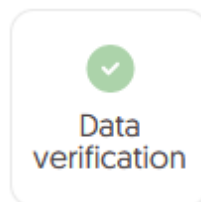
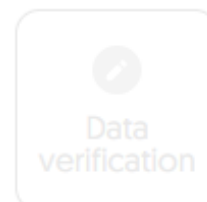As the activation process goes, each step will go through the next statuses:
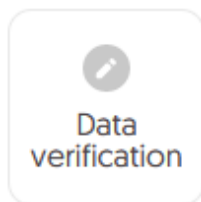
Step is awaiting to provide the data
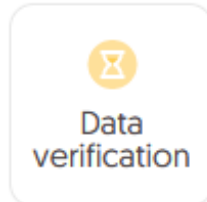
Data is saved and ale waiting for verification

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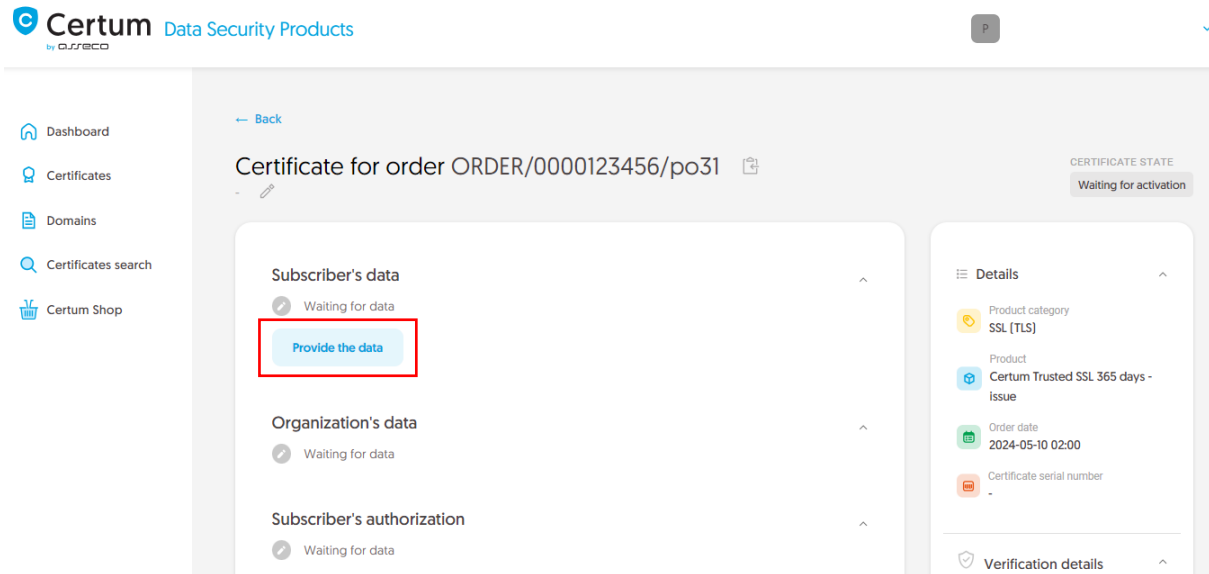
The list of supported verification documents you can check at Information about required documents.

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 to provide new data. In the future, it will be possible to use them to issue another certificate.
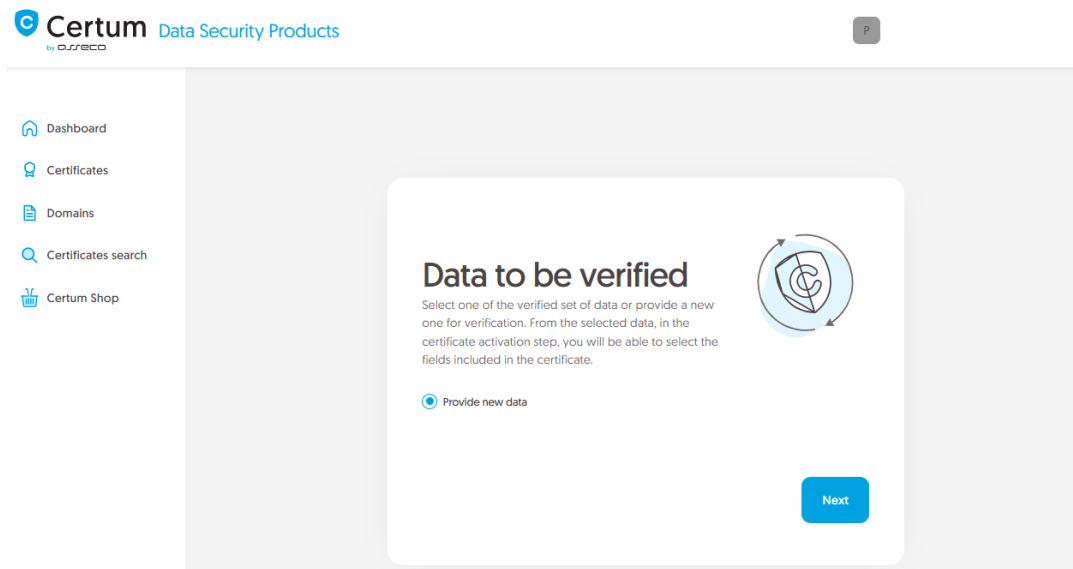
In the next stage, provide the details of the subscriber, which means the person who represents the organization and will be the owner of the certificate. Please write the names and surnames in the form as they appear on the subscriber's identity document.

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.
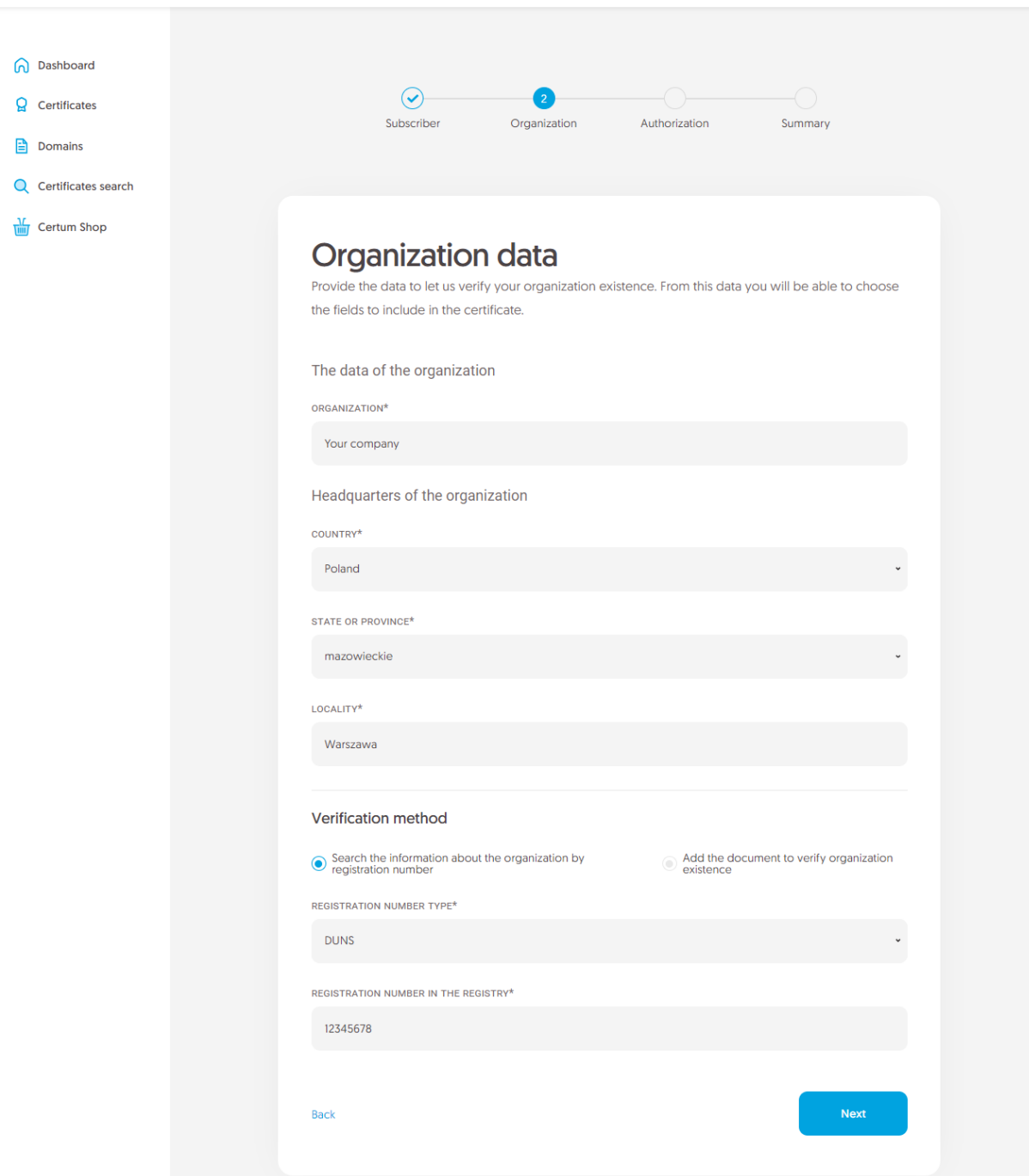
After providing the subscriber's data, go to the next stage: providing the organization's data. Here, provide the organization's details, the address of its headquarters and the city, state and country of the registration authority where the organization's legal existence was established. The data will 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.

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.

After selecting the authorization verification method and proceeding, verify 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.

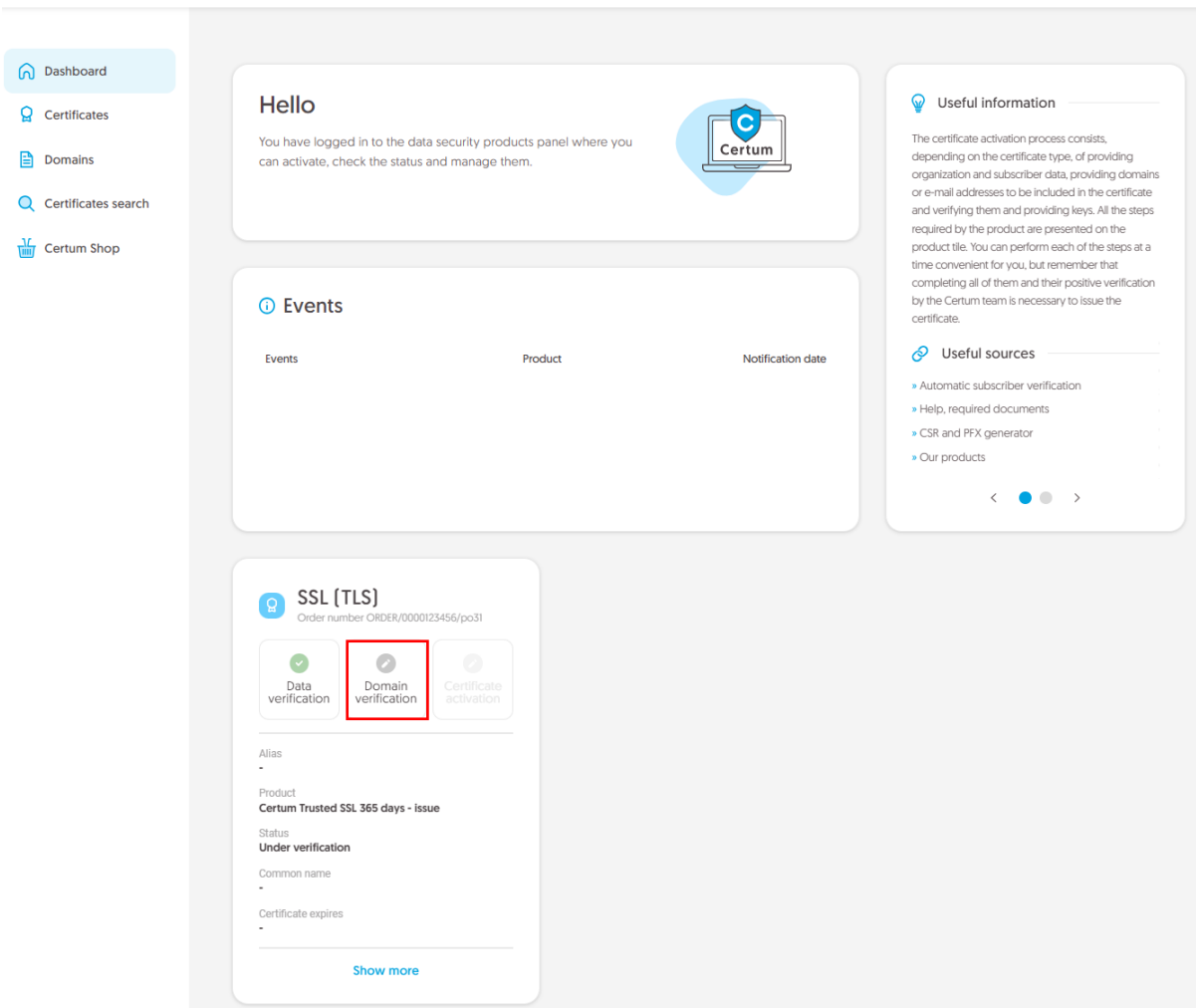The success screen will inform you that the data have been saved for verification. Certum will verify them. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the subscriber's identity, if such verification method has been chosen. You may check the instruction for automatic identity verification.
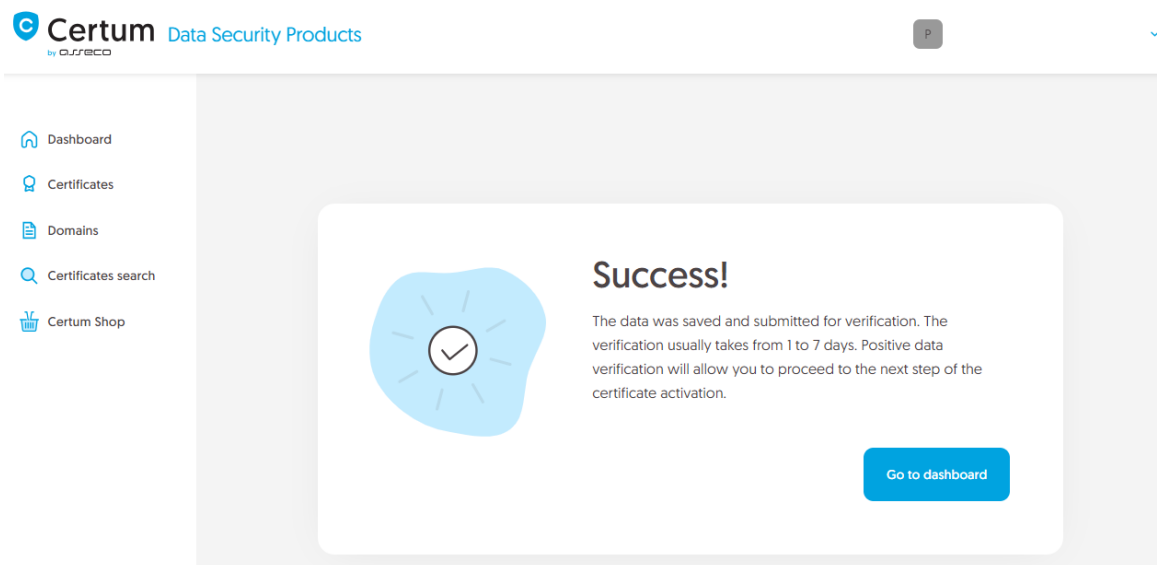
Positive verification of the provided data will allow you to proceed to the step which is generating keys and providing domains.

Domain verification step

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

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 generate a key pair and provide the domains to be included in the certificate.

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.

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 allow you to provide domains to include in the certificate and choose the verification method of the control over them.

Choose verified earlier domains from **Verified domains** tab or provide the new domains to the list using **Add domain** 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.

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 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 your chosen verification method or if they are already verified, proceed to the last step, which is **Certificate activation**.

Certificate activation step

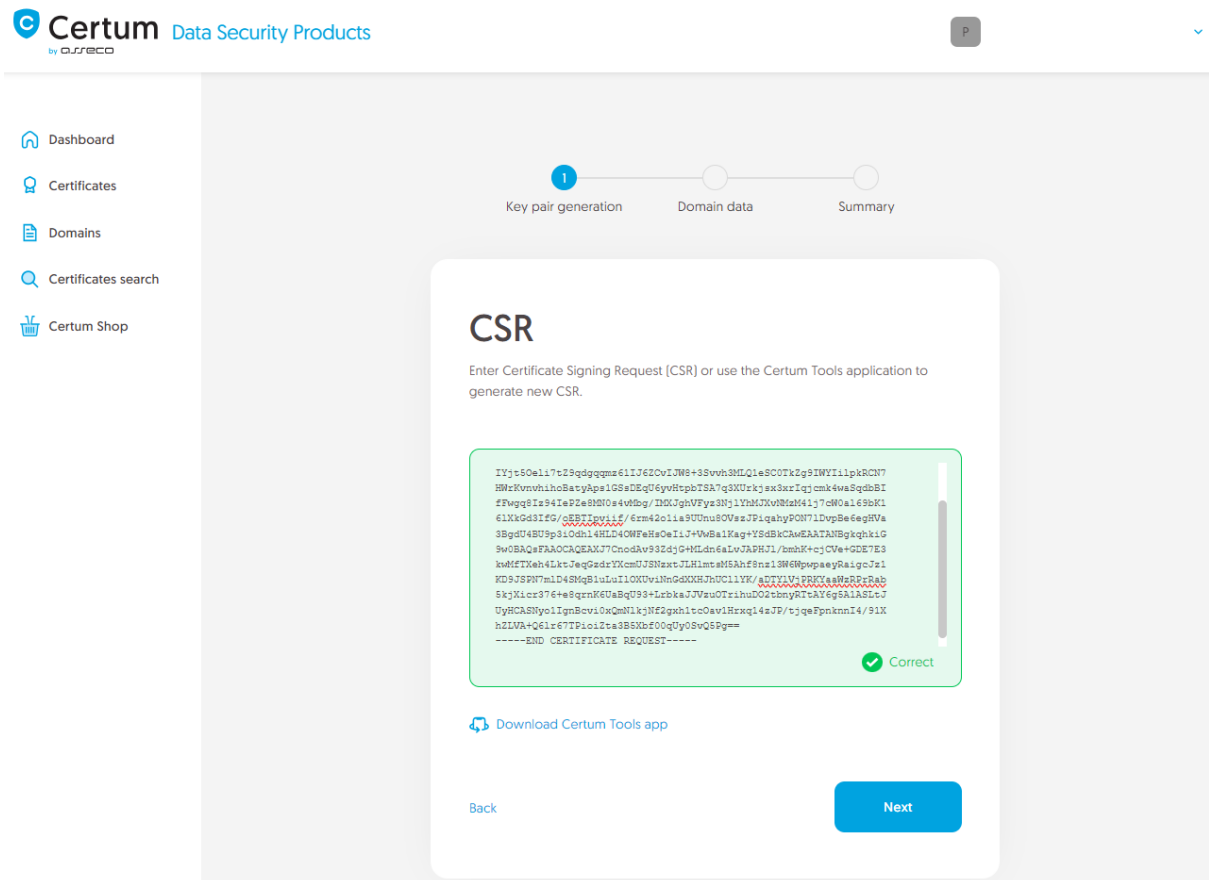You will be able to start certificate activation step from **Dashboard**, using **Certificate activation** option or similar to the previous step: from the **Certificates** list – choose the certificate you want to activate and use **Activate certificate** option.

In this step, choose which of the domains you want to set as the Common name of the certificate (if more than one domain is provided) and choose the fields you want to include in the certificate. Some fields are required and cannot be unmarked.
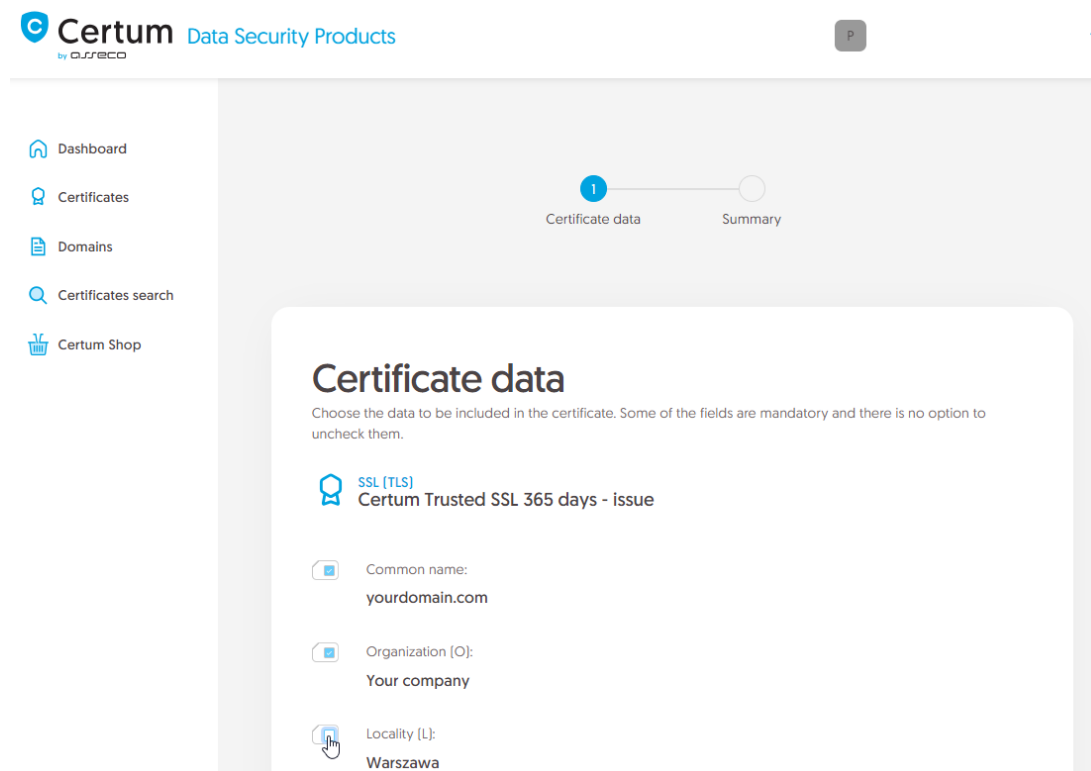
Once you have chosen the fields to the certificate, go to the summary screen and check all of provided data. Mark the required statements and complete certificate activation.

The success screen will inform you that the certificate has been submitted for issuance. 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 your certificate.

If you need a PFX file, you can use the Certum Tools generator.