

Certum Trusted SSL certificate activation

Ver. 1.3

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	14

1. Product description

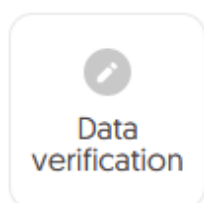
An SSL (TLS) certificate is a type of certificate used in security protocols to certify the authenticity of a domain and its owner. It encrypts and secures website traffic, including the transmission of confidential data that customers enter on your website. Thanks to the SSL certificate, your customers'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

2. Certificate activation

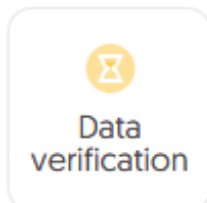
You will be able to start the activation process of your certificate in the store at **My account** in the **Data security products** tab. The process consists of several steps:

- **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.

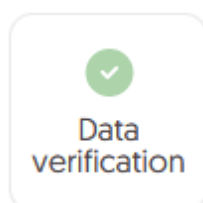
As the activation process goes, each step will go through the next statuses:



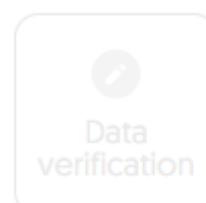
Step is
awaiting to
provide the
data



Data is saved
and ale waiting
for verification



Verification
was successful



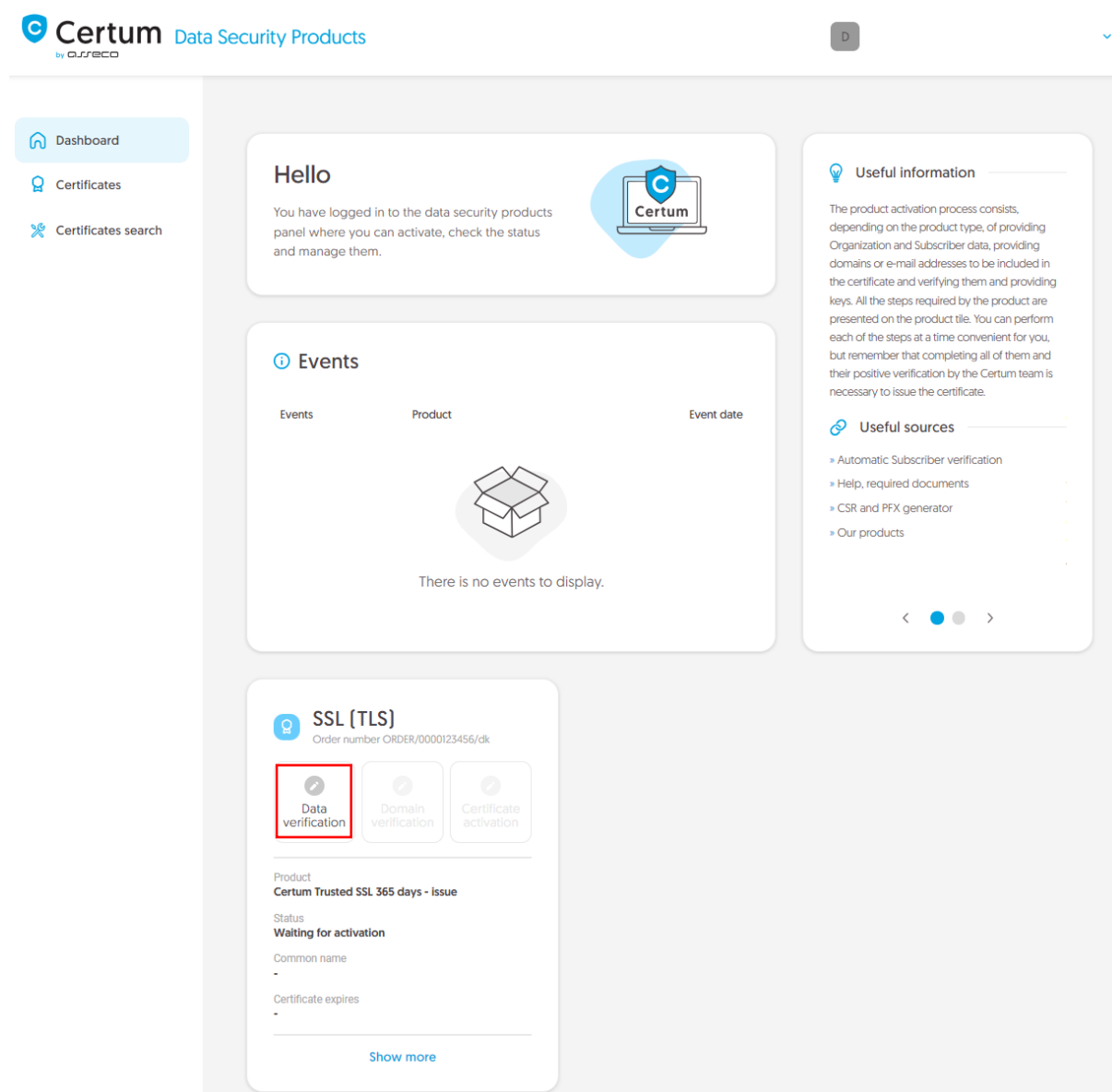
Providing the
data is not
available yet

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.

Certum Data Security Products
by GURECO

Dashboard
Certificates
Certificates search

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 ☐ 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.

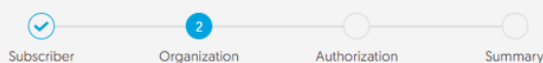
[Back](#) [Next](#)

After providing the Subscriber's data, go to the next stage: providing the organization's data. 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.

-  Dashboard
-  Certificates
-  Certificates search



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*

KRS

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 register". However, this does not prevent you from adding a document confirming the Subscriber's authorization.



Certum Data Security Products

Dashboard
Certificates
Certificates search

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

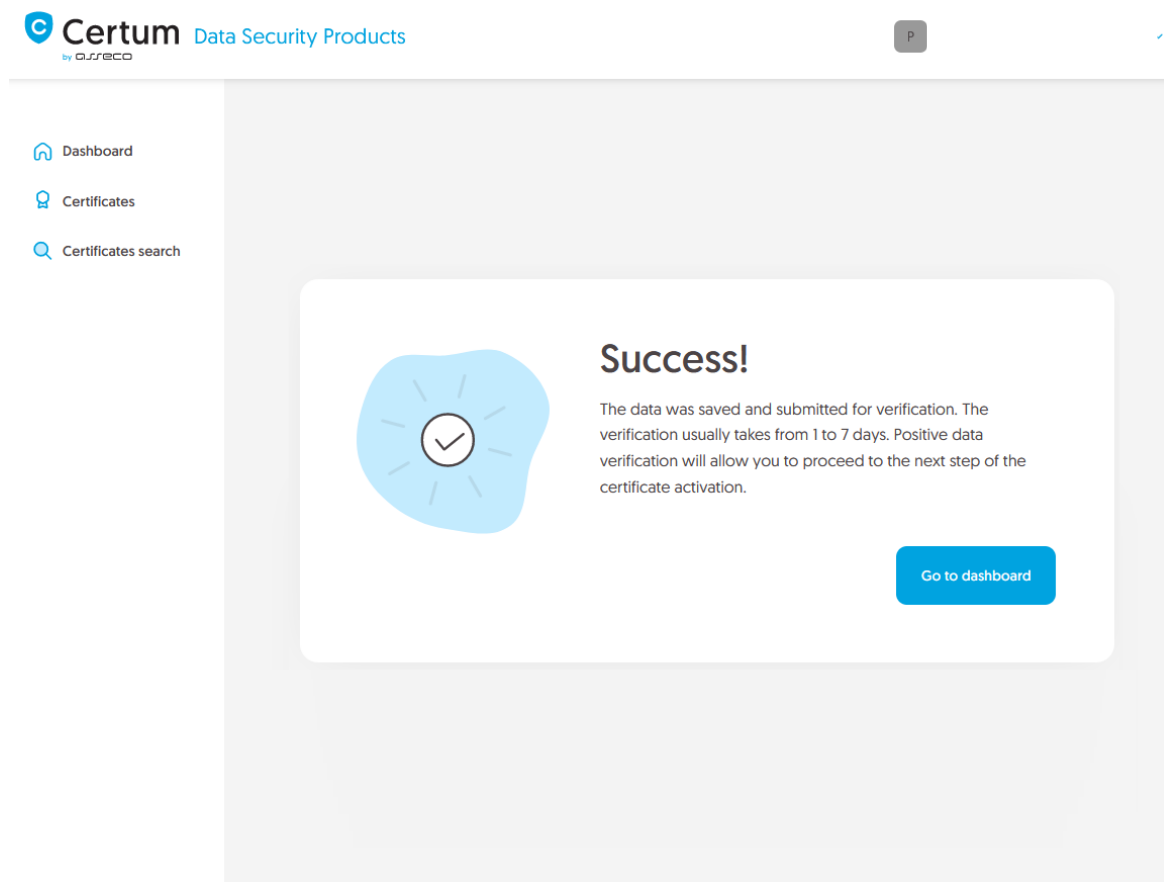
DUNS
12345678

Back Next

After selecting the authorization verification method and proceeding, verify provided information on the summary screen. If the data is correct, mark the 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:

Certum Data Security Products

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

There is no events to display.

SSL (TLS)

Order number ORDER/0000123456/dk

Data verification Domain verification Certificate activation

Product
Certum Trusted SSL 365 days - issue

Status
Under verification

Common name
-

Certificate expires
-

Show more

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


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.

 **Certum** Data Security Products
by sseco

P

 Dashboard

 Certificates

 Certificates search

Key generation method

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

Key pair generation method

☒ CSR

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](#)
- [Certificates search](#)

1 Key pair generation Chose domains Domain data Summary

CSR

Enter Certificate Signing Request (CSR) or use the Certum Tools application to generate new CSR.

```

unvjv2U6Yo1HX7Fm250Sesee1ATUHmy6NL8PT0VhQ/N2JGHeGsEB09HvWDcYfOgp
iw/zjVSD08KpXqW6vWx19OGs9h4PuoL18G1g25zvC1u8ELPmBxvpWQMck3FTh90
EtvauWJkHdYqgv79T9Q+gOvjFv+Am11YMUOYU/ODps3cSrnU5b8nc56ZYKz21i8
Io4TLvENkkHne271jUtiPKUTvD+tzKjyRHwFeF08165qUp5fJqr/oB6/viIyseo6
1WVuNIEN4mrDptOX24CtUcCipJ2QMvGvHz1Gep+AgHBAAEvOOYJKoZInvcNAQEL
BQADggEBACcPchW5LrmWdNb1cRq9PnPFapdNHavF2MSqC6D8uFPHTysq2/UzA8n
JWdGHaK6F2Usec3acz8GtgHgUK8tYKkzde2MqG5CJV60vi4Fo+mcWEJu08488Op
nTOP1JS+xZfj8Ho9aVJPrLcEAJP3ivzN83W1Tyzv4urOQMeVuaTUJQD8sPG19Lx
3K61RcThjE4ku/6cZ/XL4iGrn3b2jAIA8sbbs2oT1Csm1APbLZMavUzgw4xznX3Z
6vQp2bnt/jW9nyGLnGD00cHgDMcpHpppPf2cbdrBwQBSjEFC1cq7LIaJy8NtLLE
zsAhY/oG7EUH94zoFimMRwKYG2aD0=
-----END CERTIFICATE REQUEST-----

```

✓ Correct

[Download Certum Tools app](#)

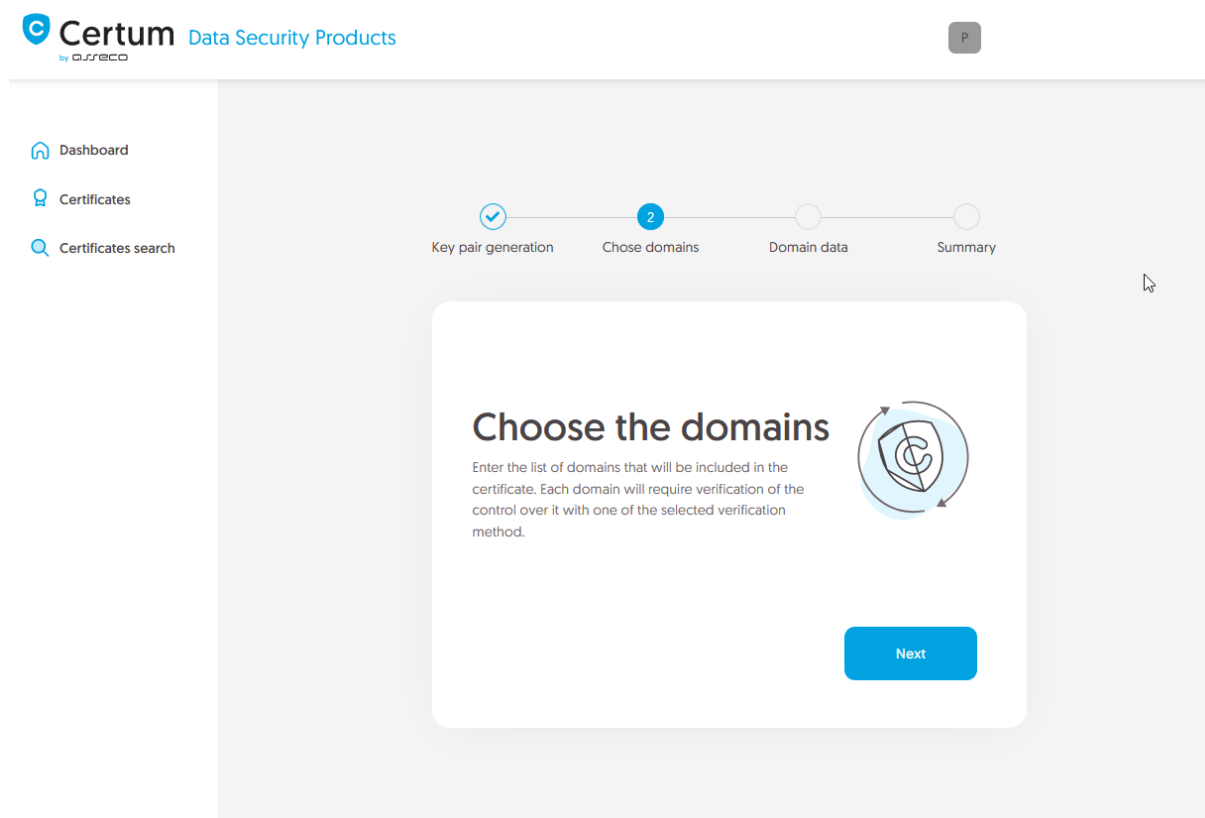
[Back](#)

[Next](#)



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.

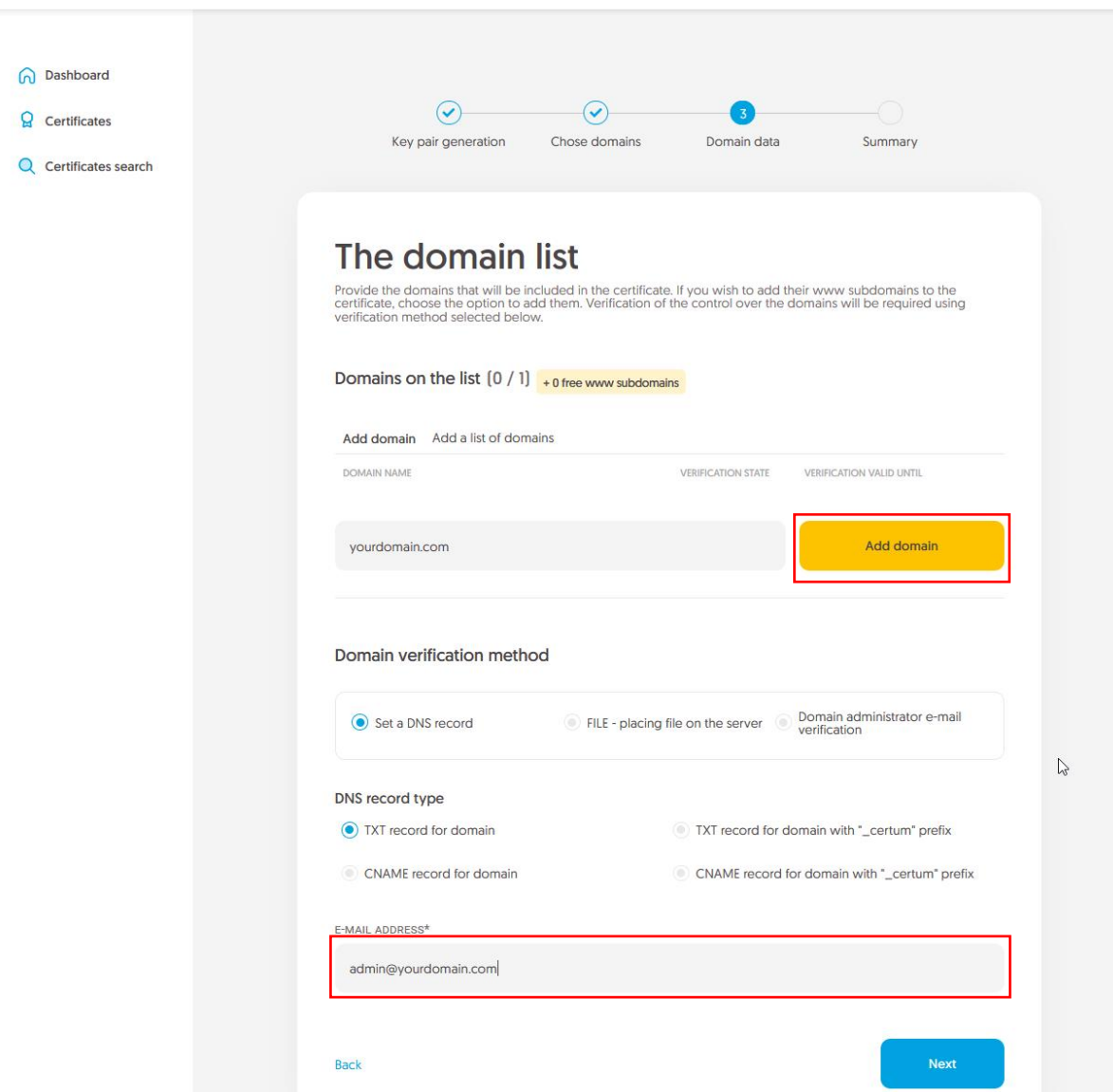
Providing the correct CSR and proceeding will allow you to provide domains to include in the certificate and choose the method of the verification of the control over them. The stage of providing domains begins with an information screen, after which you should proceed further.



Now provide the domains to the list. Confirm each of them with the **Add domain** button. If you have a list of domains in a text file, you can paste its content on the **Add a list of domains** tab.

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 choose also a 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](#).



The domain list

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.

Domains on the list (0 / 1) + 0 free www subdomains

Add domain Add a list of domains

DOMAIN NAME	VERIFICATION STATE	VERIFICATION VALID UNTIL
yourdomain.com		

Domain verification method

☒ Set a DNS record
 ☐ FILE - placing file on the server
 ☐ Domain administrator e-mail verification

DNS record type

☒ TXT record for domain
 ☐ TXT record for domain with "_certum" prefix
 ☐ CNAME record for domain
 ☐ CNAME record for domain with "_certum" prefix

E-MAIL ADDRESS*

admin@yourdomain.com

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

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. After completing domain verification, their 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 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.

The screenshot shows the 'Certificate data' form in the Certum Data Security Products interface. The top navigation bar includes the Certum logo and 'Data Security Products' text. A sidebar on the left contains links to 'Dashboard', 'Certificates', and 'Certificates search'. The main content area features a progress indicator with two steps: 'Certificate data' (active, marked with a blue circle and '1') and 'Summary'. Below the progress indicator, the 'Certificate data' form is displayed. It has a title 'Certificate data' and a subtitle '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 includes a section for 'SSL (TLS)' with the text 'Certum Trusted SSL 365 days - issue'. Below this, there are three fields: 'Common name:' with the value 'yourdomain.com', 'Organization (O):' with the value 'Your company', and 'Locality (L):' with the value 'Warszawa'. Each field has a small icon to its left.

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.