

Certum Trusted SSL certificate activation

Ver. 2.0

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	10

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 to
provide the
data



Data is saved
and ale waiting
for verification



Verification
was successful



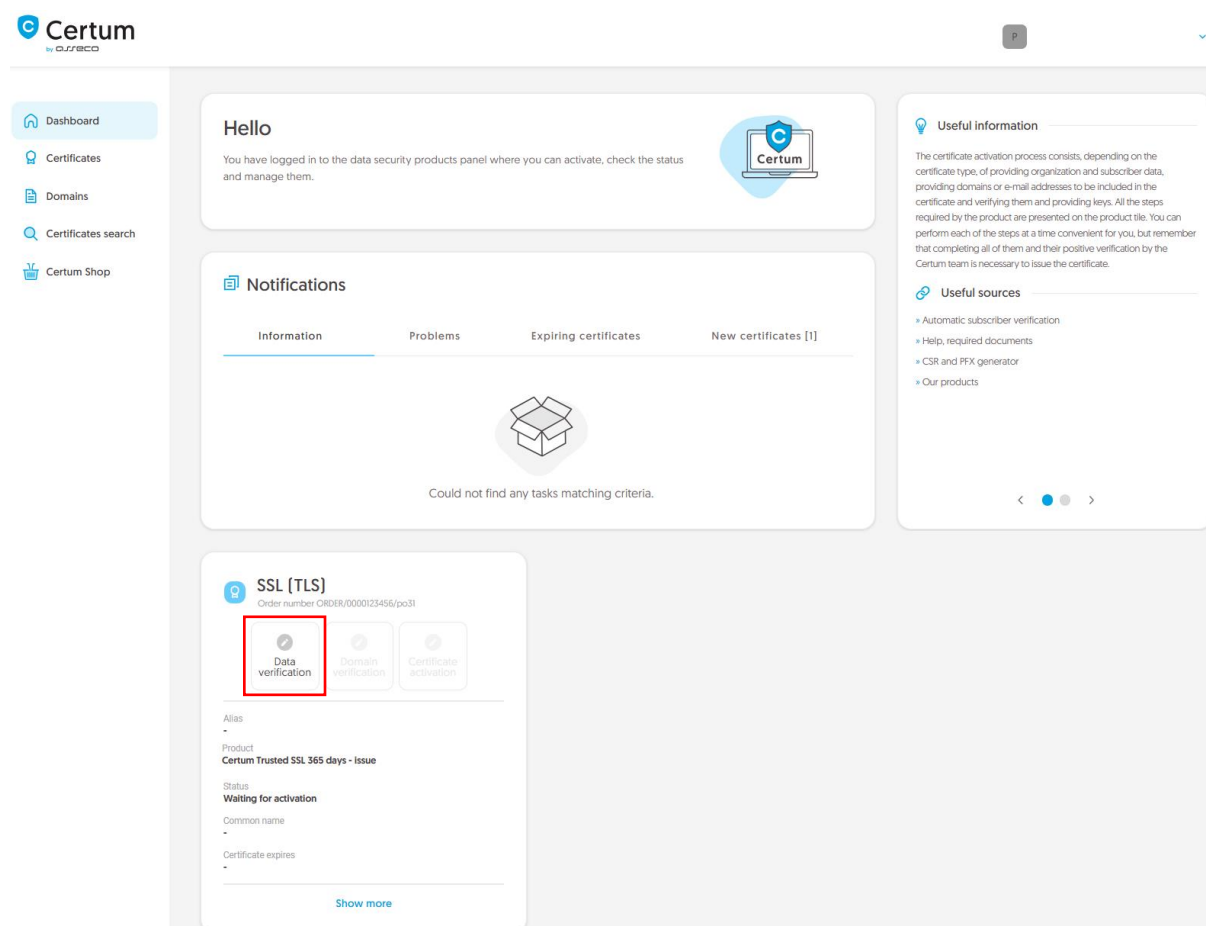
Providing the
data is not
available yet

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](#).

As the Certum **customer**, 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:

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.

Certum
by DJR&CO

Dashboard
Certificates
Domains
Certificates search
Certum Shop

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 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.

Certum
by DJFECO

Dashboard
Certificates
Domains
Certificates search
Certum Shop

Subscriber Organization Authorization 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*

Your company

Headquarters of the organization

COUNTRY*

Poland [PL]

STATE OR PROVINCE*

mazowieckie

LOCALITY*

Warsaw

Verification method

☒ Search the information about the organization by registration number ☐ Add the document to verify organization existence

REGISTRATION NUMBER TYPE*

DUNS

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.



The screenshot shows the Certum by DUNECA website interface. On the left is a sidebar with navigation links: Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area features a progress bar at the top with four steps: Subscriber (checked), Organization (checked), Authorization (active, marked with a '3'), and Summary. Below the progress bar is a white card titled 'Authorization data' with the instruction: 'Choose the verification method to confirm the subscriber's relationship with the organization.' The card contains three sections: 'Subscriber data' with fields for Name (Joe) and Surname (Doe); 'Verification method' with two radio button options, the first of which is selected; and 'Chosen registry type' with the text 'DUNS' and '12345678'. At the bottom of the card are 'Back' and 'Next' buttons.

Certum
by DUNECA

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

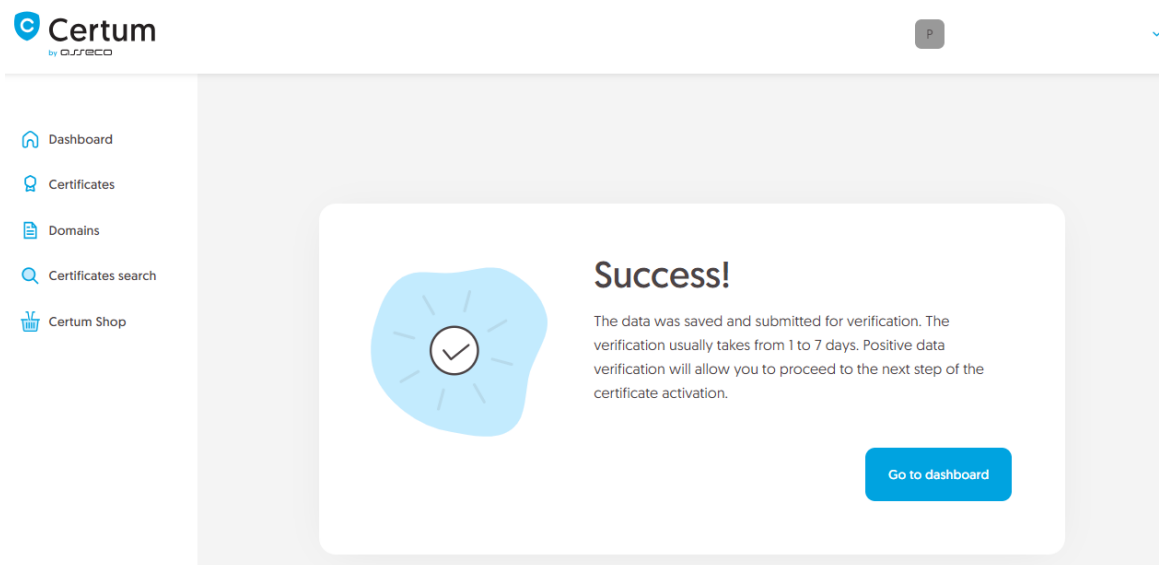
Chosen registry type

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.

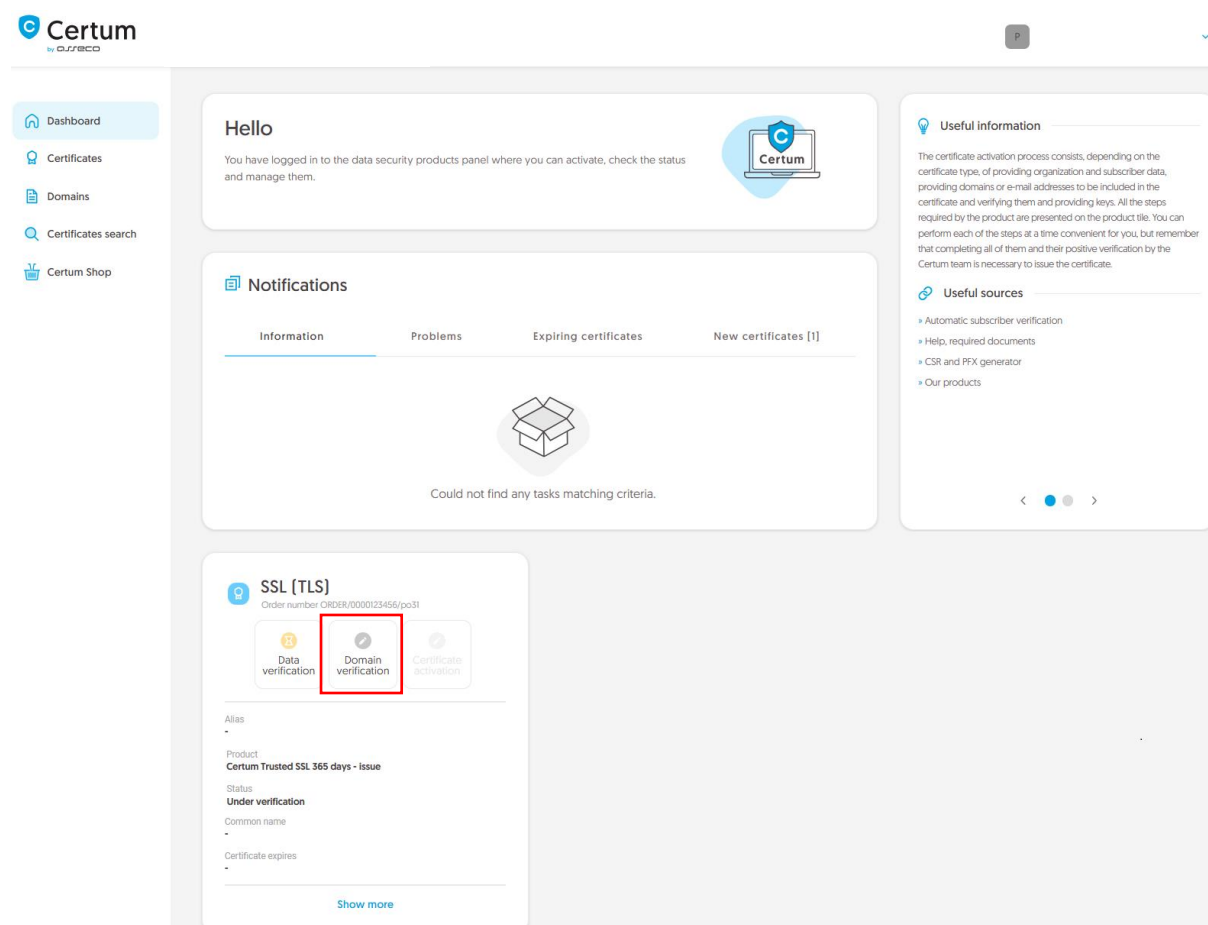
The success screen will inform you that the data have been saved for verification. Certum will verify it. During this time, if you want to add another document confirming the provided data, you can add it in the certificate details. This is also the time to perform automatic verification of the subscriber's identity, if such verification method has been chosen. You may check the [instruction for automatic identity verification](#).



When the data to be verified is saved, you can proceed to the next step which is providing the 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 provide the domains to be included in the certificate.

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

The screenshot shows the Certum 'The domain list' interface. The left sidebar contains links for Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main area has a progress bar with 'Domain data' (active) and 'Summary'. Below the title 'The domain list', there is 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.' There are three tabs: 'Verified domains', 'Add domain' (highlighted with a red box), and 'Add a list of domains'. Under 'Add domain', there is a text input field containing 'yourdomain.cc' and a yellow 'Add domain' button. A blue arrow points from the button to the 'Selected domains' panel on the right. This panel shows 'Domains to secure (1 / 1)' with a '+ 0 www subdomains' button. Below is a table with columns 'DOMAIN NAME' and 'VALID UNTIL'. The first row shows 'yourdomain.com' with 'verification required' and a trash icon. At the bottom, there is a toggle switch for 'add www. subdomains to the list'.

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

The screenshot shows the Certum 'The domain list' interface with the 'Verified domains' tab selected. The left sidebar is the same. The main area has the same progress bar. Below the title 'The domain list', there is a description: 'Choose verified or provide new 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. For not verified domains, verification of the control over them will be required using verification method selected below.' There are three tabs: 'Verified domains' (active), 'Add domain', and 'Add a list of domains'. Under 'Verified domains', there is a 'Select all domains' link. Below is a table with columns 'DOMAIN NAME', 'VERIFICATION STATE', and 'VERIFICATION VALID UNTIL'. The first row shows 'yourdomain.com' with a green checkmark and the date '2025-01-24 10:24'. The right sidebar is the same as in the previous screenshot.

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.

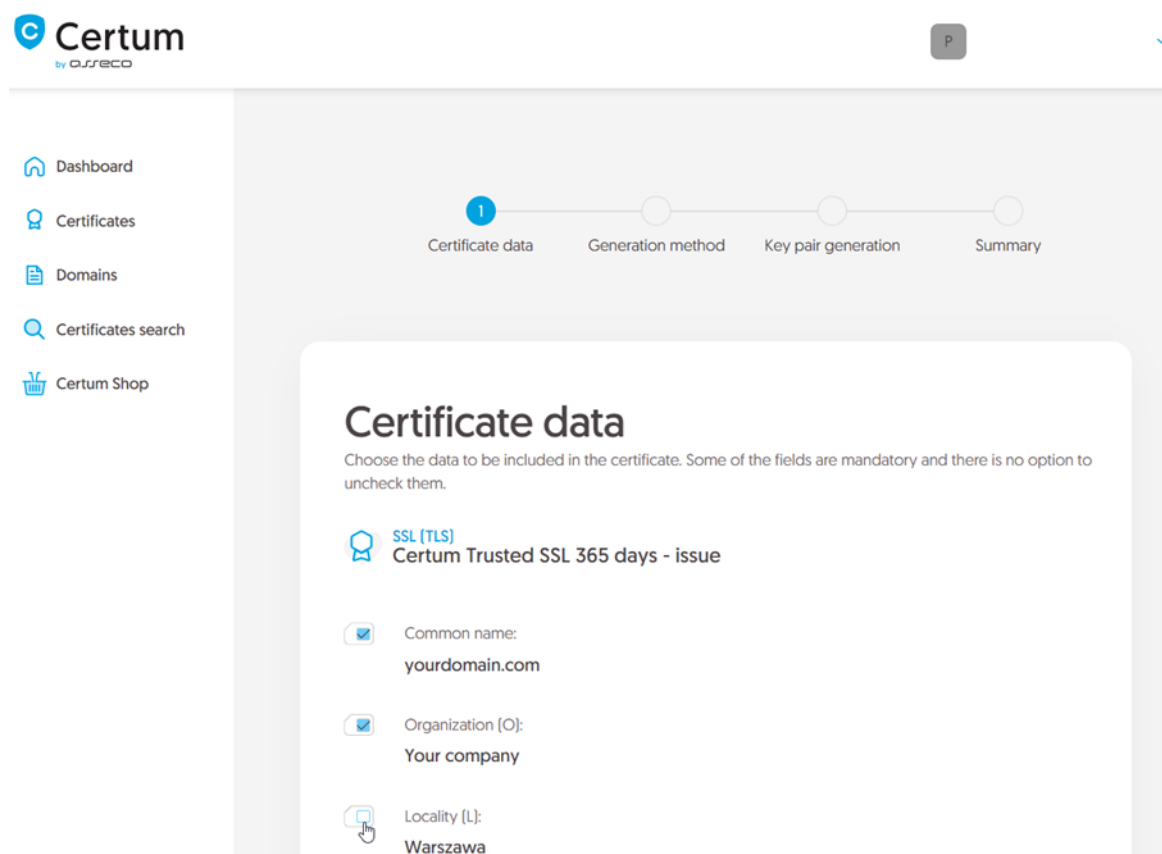
The success screen will inform you that your domains have been saved. Verify them using chosen earlier verification method or if the data to be verified and the domains are both verified, proceed to the last step, which is **Certificate activation**.

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 and fields 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.



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 displays a progress bar with four steps: Certificate data (active, marked with a blue '1'), Generation method, Key pair generation, and Summary. Below the progress bar, the 'Certificate data' section is highlighted. It contains a sub-header 'SSL (TLS) Certum Trusted SSL 365 days - issue'. Underneath, there are three fields with checkboxes: '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 checkbox that is currently checked.

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

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.

```

Pc08LL08yLqdIruyl12WjCkHIDcmM4c3/KzuuSj4CNrMPCFF14BjAaZEirBoS
oCetPy4XX7duKv4c1Qn6dfn7x1OmaDIUhbzro+tcZMB1M29X1Rt3jrf80ZKA4g3Oam
r0Kjg01T3yePoScwn86HRzZ16PrR8oH0UCIPnV/rY1sTyQ81bnnb5W588Fk1U5j
3oooknaXuNhuHk+D17VLL2t3P8H4QC82GmluxF13Ua1cvhLexWJW/w5bhh2kFTMa8G
eo53bJVt7HFj3c85xHA7jRMduu9SMgg1ZFkvHQvz1XoCawEAATANBgkqhkiG9w0B
AQIFAACCAQEACjctclKAhrWITVF7E41/3PQZ19D1Z8nv5tdhuYD1Kzcm1LkbG4cru
gvEYXjY1UtzB9B8C8OKBeIpBcaZwWOL9zrpZ6m8uq+Y2X53BpupxhG97IG8caardV
IyUIqo+6svL79lnr4EzX6bXZzEiAROX8M+xq880D+YdyoRHECETRMdlud45a1/A
phTe1E5ggRiYatVyLgdLSCCw70R9aanPtyNkiNINvAvsP8aYQMjptZhyXzBohe
6P8D0bQ5sLXOG8Bg57E0pCf1IXjwHLGQnEz4VA0wQxk70Nw0eTMpHj/HF06e4mRt
eeqIXyvS9rRn1AeA27o71UbFoyFA5so/zw==
-----END CERTIFICATE REQUEST-----

```

[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 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.