



Certum Commercial SSL certificate activation

Ver. 1.4

assecO

 **Certum**
by assecO

Table of contents

1. Product description	3
2. Certificate activation	3
Domain verification step.....	3
Certificate activation step.....	7

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.

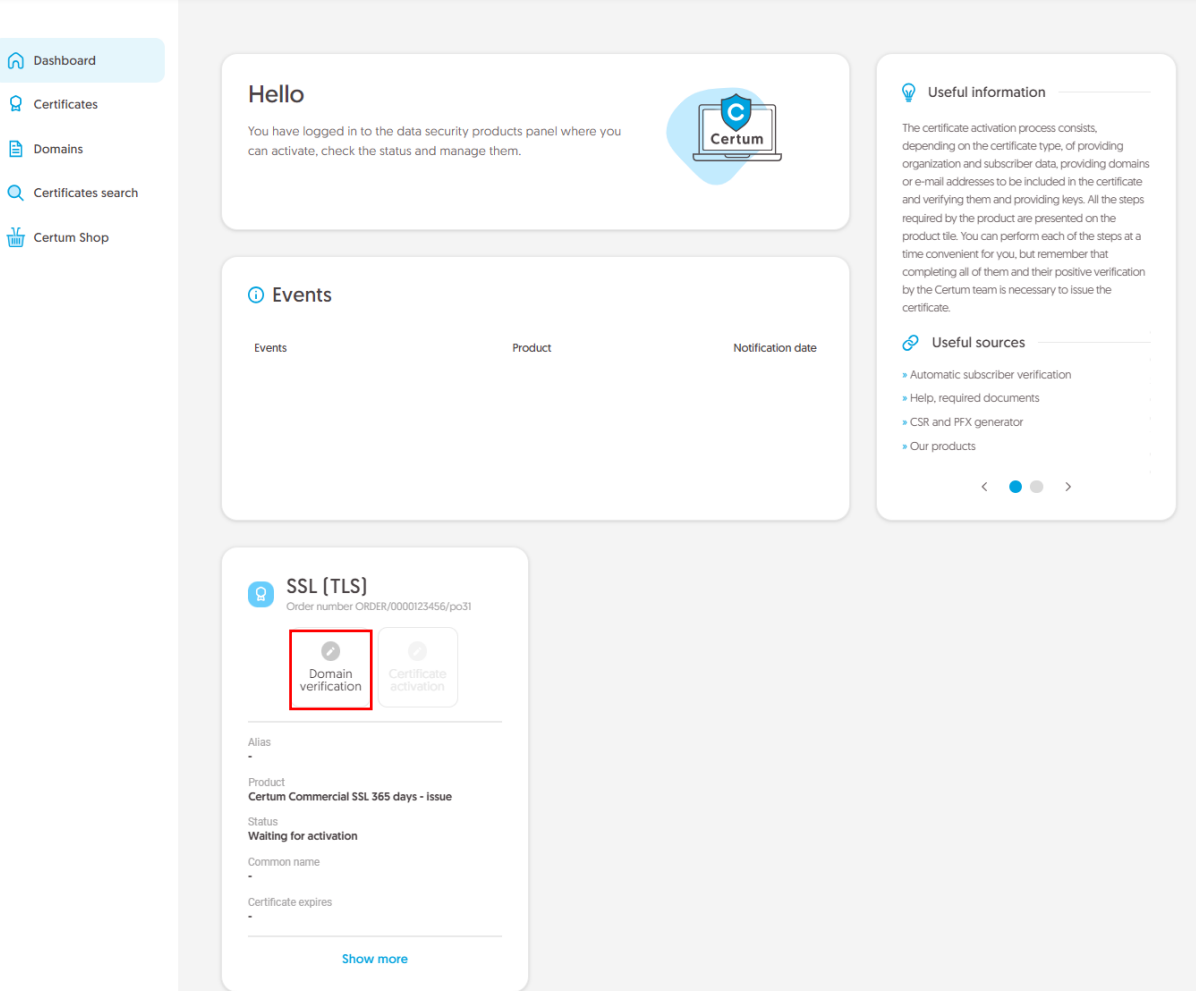
2. Certificate activation

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:

- **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.

[Domain verification step](#)

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



Hello

You have logged in to the data security products panel where you can activate, check the status and manage them.

Events

Events	Product	Notification date

Useful information

The certificate activation process consists, depending on the certificate 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

SSL [TLS]
Order number ORDER/0000123456/po31

Domain verification

Certificate activation

Alias
-

Product
Certum Commercial SSL 365 days - Issue

Status
Waiting for activation

Common name
-

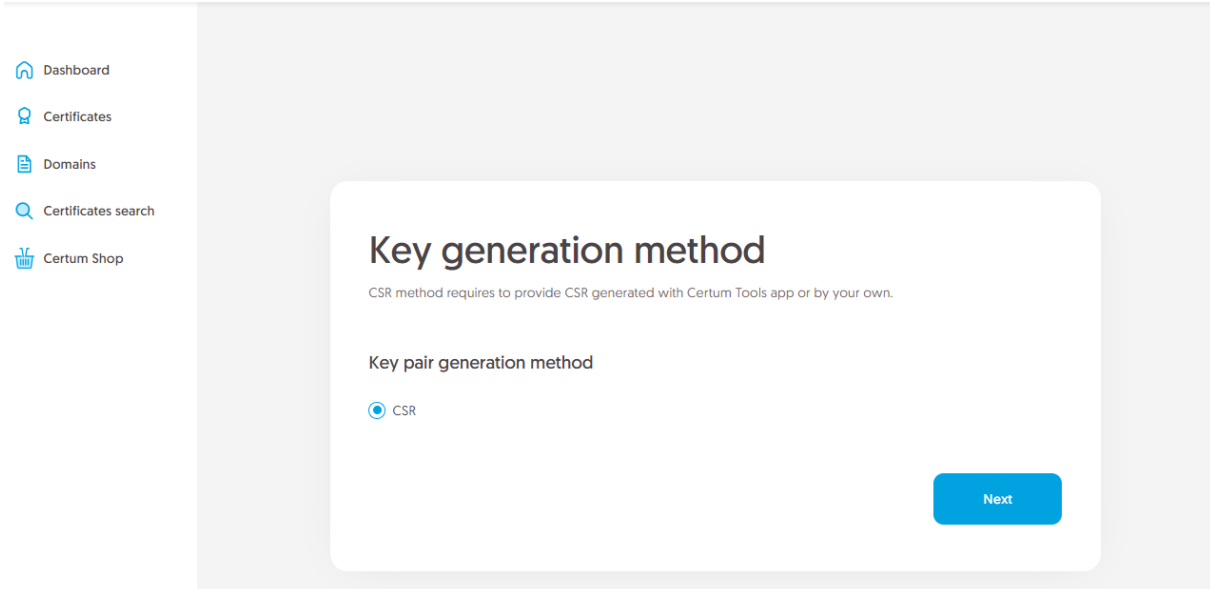
Certificate expires
-

[Show more](#)

or 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.



Key generation method

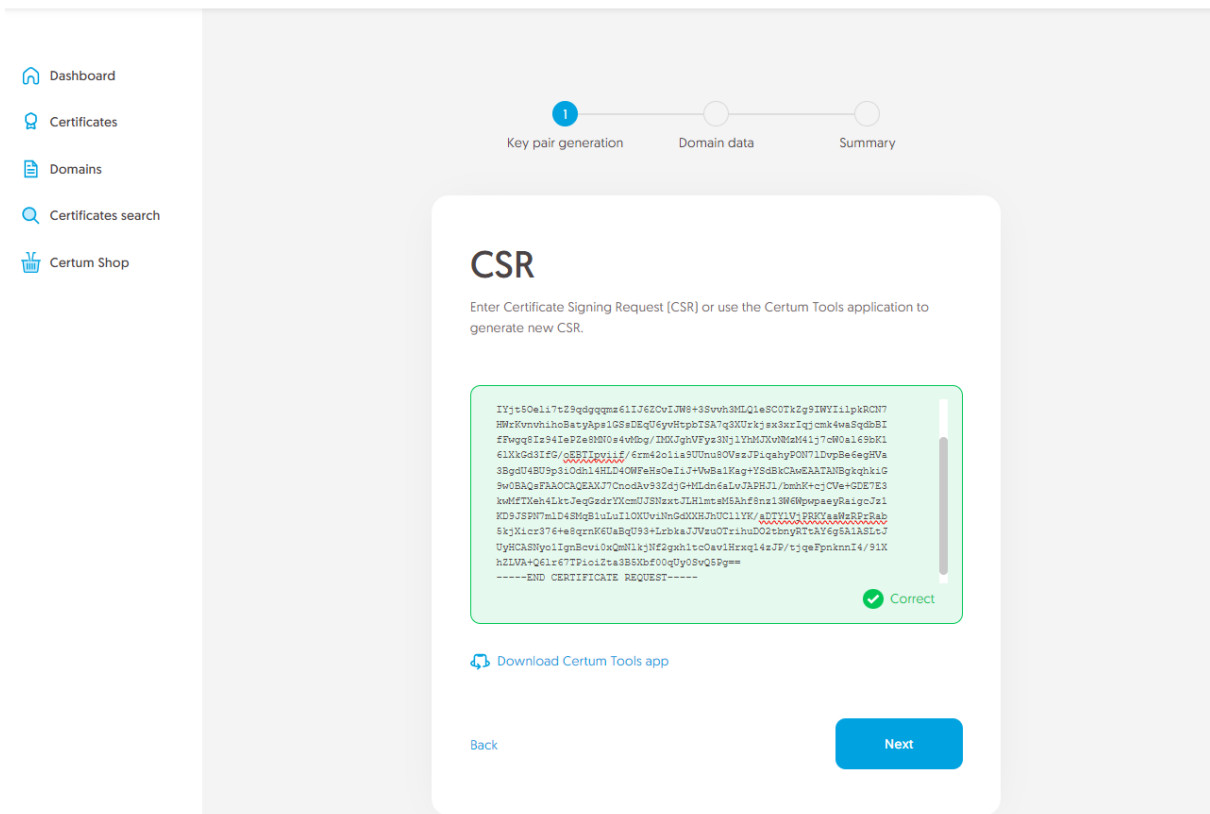
CSR method requires to provide CSR generated with Certum Tools app or by your own.

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.



CSR

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

```

IYjt5Oe117t29qdgqqms611J62CvLJW8+3Svvh3MLQ1eSCOTk2g9IMWI11pkrCN7
HwzKvvh1h0BatyApe1GSsDEqU6yvhTpbTSA7q3XU7k7ex3xz1qjcmk4waSgdbBI
fFwgq8IeP4TeP2e8M0e4Wdq/IXKJghVfys3Nj1YmJXvM41j7cW0a1.69bK1
6LXkG3IFG/cBET7py1f/6rm42o1ia9UUnu8OVaz7PiqahyPON71DvpBe6egHVa
3BgdU48U9p3iOdh14HLD4OWFeHe0eIiJ+VwBslKag+Ys4bkCmEATANBgtqkxIG
9w0BAQeFAAOCAQEAJ7CnodAv932dJG+HLdneLwJAPHJ1/bmhK+cjCVe+QDE7E3
kwMfTeh4LktJeqGedrYXcmUJSNaxtJLHlmtaM5Ahf8na13W6WpvpaeYRaigoJz1
KD9JSPH7m1D48Hg81uLuILOUv1NnGdXKH7hDC1LYK/a7YV1UvPRR7easWdR5r8ab
SkjYicr376+e8qenK6UaBqU93+LzkaJUVauOTrihuDO2tbmyRTtAYegSAlASL7J
UyHCA8Myc01ZgnBcvi0xQmN1kjN2gkx1tcOav1Hrxq14a7P/tjgeFpnknn14/91X
h2LVA+Q61z67TPi0i2ta3B5XbF00qUy08vQ5P9==
-----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 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](#).

The screenshot shows the 'The domain list' step in the Certum Data Security Products interface. The progress indicator at the top shows three steps: 'Key pair generation' (completed), 'Domain data' (current step), and 'Summary'. The main content area is titled 'The domain list' and includes instructions: '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.' Below this, there are three tabs: 'Verified domains', 'Add domain', and 'Add a list of domains'. A table lists domains with columns for 'DOMAIN NAME', 'VERIFICATION STATE', and 'VERIFICATION VALID UNTIL'. One domain, 'yourdomain.com', is listed with a green checkmark and a valid until date of '2024-07-18 08:47'. A 'Next' button is visible at the bottom right of the table. On the right side, there is a 'Selected domains' sidebar showing 'Domains to secure (0 / 1)' and '+ 0 free www subdomains'.

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).

The screenshot shows the Certum Data Security Products interface. On the left is a navigation menu with icons and labels for Dashboard, Certificates, Domains, Certificates search, and Certum Shop. The main content area has a progress indicator at the top with two steps: 'Certificate data' (active, marked with a blue circle and '1') and 'Summary'. Below this is a white card titled 'Certificate data' with the instruction: 'Choose the data to be included in the certificate. Some of the fields are mandatory and there is no option to uncheck them.' The card lists three fields, each with a blue square checkbox and a document icon: 'Common name: yourdomain.com', 'Organization (O): Your company', and 'Locality (L): Warszawa'.

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.