Guide –

Certum Commercial SSL

Certum Commercial SSL Certificate Activation Guide

version 1.2

Table of Contents

1. Product description

An SSL certificate (TLS) is a security protocol certifying the authenticity of a domain and its owner. It encrypts and secures traffic on websites, including the transmission of confidential data that customers enter on your site. Thanks to an SSL certificate all personal data, logins and passwords, credit card numbers and other data of your customers will be secured.

2. Product activation

The guide is prepared using the example of Google Chrome browser and concerns the process of activating the Certum Commercial SSL certificate.

After placing an order in the Certum shop, activation will be available in the Certificate Activation tab (see section 2.2).

2.1. Adding the activation code

If you want to activate the product from an electronic code received e.g. on your e-mail address - before you begin the activation, add the code in the Electronic Codes tab. To do so, log in to your account on https://sklep.certum.pl
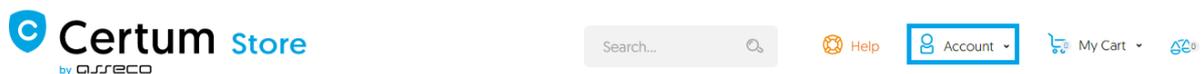
In case you do not have an account, click on the Create an Account button to create one. If you already have an account, select Log in.

After logging in, click on the customer panel - Your Account.

To add a code select the Electronic Codes tab. Enter the code in the Electronic code field and click Add button. Note! Remember that the activation code consists of 16 characters. After entering or copying the code make sure that the number of characters is correct.

If you enter the code correctly, the product will appear on the list in the Your codes/Entered manually section. After processing the code, go to the Activate Certificates tab (see next point 2.2).

2.2. Start of certificate activation

After placing an order or adding a code to your account, start activation in the Activate Certificates tab.

Find the correct certificate in the list and click Activate.

Important! You can select between two methods of certificate activation. We recommend using the CSR method, which will provide you with a certificate file (public part) and a private key. For this method, a CSR request must first be generated:

- either by the server administrator
  or
- via the CSR generator, available in the Certum shop user account.

If you need the pfx/p12 file, you can choose the method of key pair generation.

2.2.1. Activation method – key pair generation

If you want to perform the activation using the key pair generation method, click on the Next button.

In order to generate the keys, download and run the Certum CryptoAgent app (to run the app you need a Java environment installed on your computer https://www.java.com/pl/).

A warning communicate will appear in the bottom bar of your browser, where you can click Save to download the Certum app.

When the Certum CryptoAgent window appears, run the app by clicking Run.
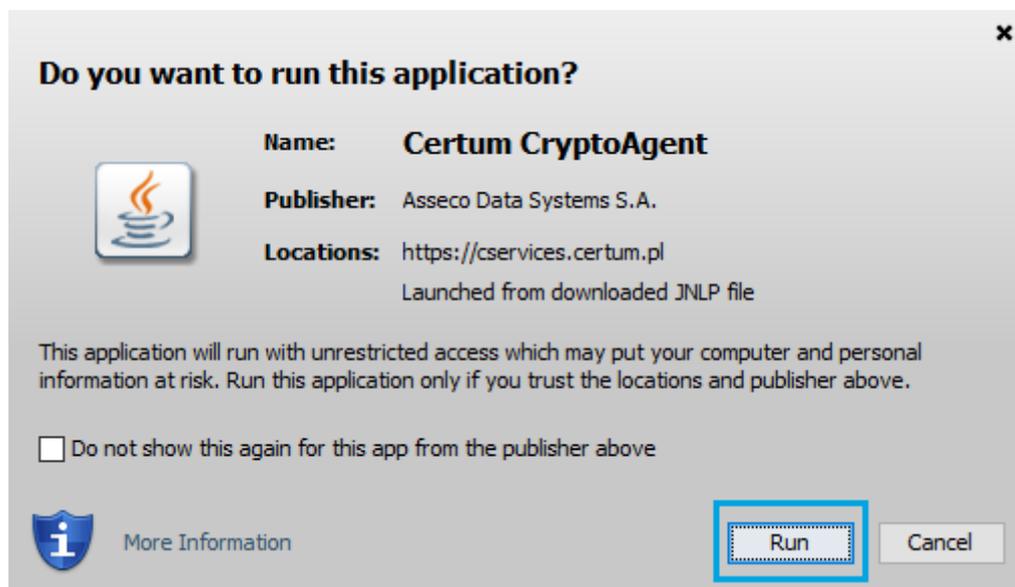
After a short while, the app will run in the background and during the activation process there will be a possibility to save the keys in the Certum app. The default settings, i.e. RSA key algorithm (change to EC possible) and 2048 key length are correct for SSL certificate operation.

After clicking on the Generate Keys button, a message will appear that the certificate keys have been generated. Clicking the Next button will take you to the next activation step (see chapter 3 - Filling in the form during activation).

2.2.2. Activation method - CSR request

If you want to issue a certificate using the CSR method, use any CSR generator that meets your needs or the Open SSL tool recommended by Certum. Read more: https://www.support.certum.eu/en/what-is-csr/.

3. Filling in the form during activation

In this stage, fill in the form with the applicant's details and the certificate data. In case of using the CSR method, the data entered in the request will automatically be entered as certificate data. Fields with an asterisk (*) are mandatory.

Note! If you want the certificate to secure two variants of the domain (yourdomain.eu and www.yourdomain.eu) enter the name of the website alone in the Domain 1 field and tick the checkbox add variant with www on the right.

Applicant data:

Name

Surname

Phone

Email

Specified end of certificate validity - this date will be entered as the valid to date when issuing the certificate. Setting this field will shorten the validity period, but guarantee its expiry on the indicated date. To use the maximum validity period, the field should be left blank.

If you want to keep the maximum validity period of the certificate, leave this field blank.

Certificate Data:

Hash function   RSA-SHA256

Shortened validity period

DNS Domain 1 *   certum.pl   ☐ add variant with www

Applicant data:

Name

Surname

Phone

Email

Enter a domain name for which a certificate is to be issued . If you enter a domain name with the www prefix, eg www.certum.pl - issued certificate will secure both the domain certum.pl and www.certum.pl. In the case of Wildcard SSL certificate, issued for a group of sub-domains under the main domain such as *.certum.pl, it will secure both certum.pl and www.certum.pl domains, as well as subdomains within the certum.pl domain.

Certificate Data:

Hash function   RSA-SHA256

Shortened validity period

DNS Domain 1 *   certum.pl   ☐ add variant with www

Note: As of October 2021, the FILE verification method is only available for certificates containing only one domain in the order. This method is not available for Wildcard certificates and for single domain certificates with the "www" checkbox checked. If you checked the checkbox next to the "Add www variant" box, the email or DNS method will be available.
Read more: https://www.support.certum.eu/en/technical-news/domain-verification-changes/

In the case of the wildcard SSL certificate issued for a group of subdomains within the main domain, e.g. *.certum.pl, it will secure both the certum.pl and www.certum.pl domains (without selecting the checkbox) and subdomains within the certum.pl domain. Remember to start your domain name with *.yourdomain.eu. After filling in the data, click the Next button.

In the last step (Confirmation), verify that the entered data is correct and select the required approvals and declarations, and then click Activate.

4. Verification of access to the domain

In order for Certum to issue the SSL certificate, the user should prove that they have access to the domain to be secured. The verification of the access to the domain should be performed in ONE of THREE ways:

- verification of the e-mail address by confirming the verification link, which will be sent by Certum to the administrator's address (e.g.: admin@yourdomain.eu, administrator@yourdomain.eu, webmaster@ yourdomain.eu, postmaster@ yourdomain.eu, hostmaster@ yourdomain.eu),
- verification of the access to the domain by placing on the server a file with a name that the user receives from Certum,
- verification of the access to the domain by creating an appropriate TXT record in the DNS with a name that the user receives from Certum

You can select the method of verification of access to the domain in the Activate Certificates tab. Select the certificate you are interested in from the list and click on the Verify Domain button.

Note! The option to verify the access to the domain will be possible only after the activation of the product. The verification code is valid for 72 hours from the moment of sending, in case the link is no longer valid you can send the code again in the same way as the first code.

In the next step you will see a list of domains to verify. Click on the domain name you want to verify.

When you click on the domain, the verification methods to choose from will appear.

4.1. Verification of the administrator's email address

Using this method, select one from the list of available addresses and send a verification link there. After selecting the address to which we have access, click the Send button. In the email you receive there will be a verification link which you can click on to verify the access to the domain.

4.2. Verification of the access to the domain by placing a file on the server

The method consists in placing a special web page on a server supporting the certified domain, and then confirming the change by clicking the link in the message sent to the given email address.
In the DNS Domain section, select verification by placing a file on the server (FILE), enter any email address to which instructions will be sent along with the file.

Place the file (received by email) on your website in the area /.well-known/pki-validation/
After performing the above action, in order to verify the correct placement of the file, click on the verification link from the e-mail - Verify the domain.

4.3. Verification of the access to the domain by creating an appropriate TXT record in the DNS

The method consists in placing an appropriate entry in the TXT record in the DNS for the certified domain, and then confirming the change by clicking the link in the email sent.
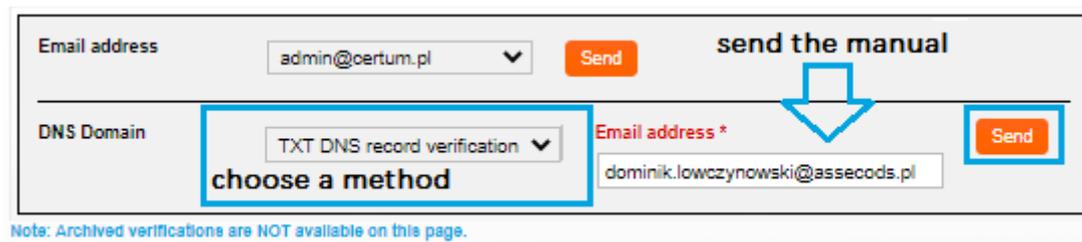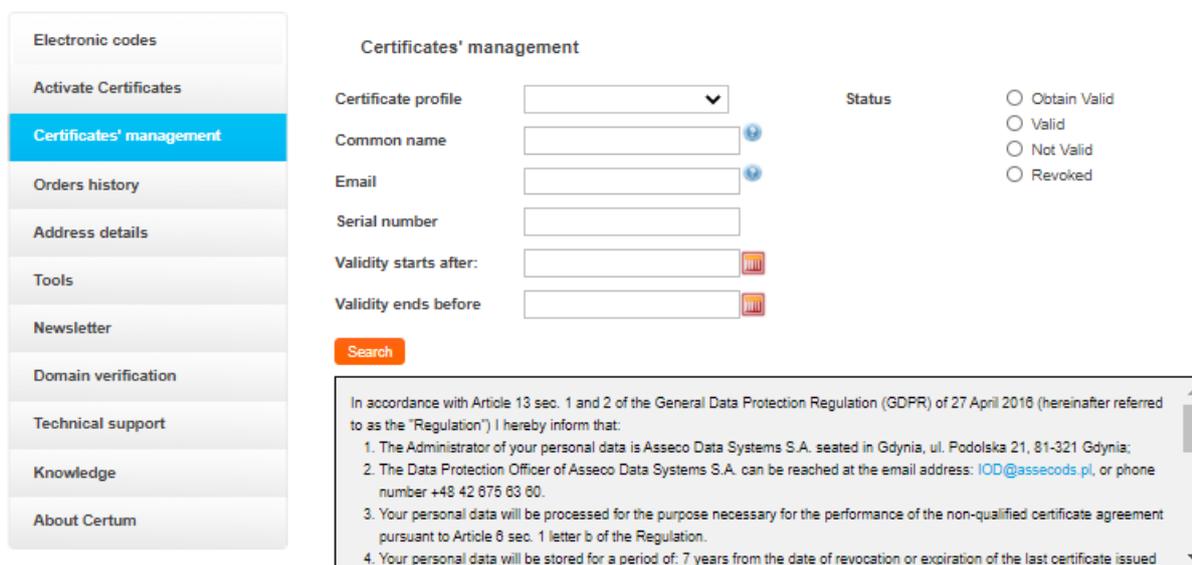
The received email will contain an instruction for placing the relevant entry in the TXT record in the DNS for the certified domain and confirming the change by clicking the link given in the email.
Please note that it can take up to 24 hours to refresh/update the DNS entries.

5. Certificate downloading

After correct verification, wait for the certificate to be issued.
Important! In the case of an order placed by a traditional transfer, it is also necessary to register the payment in order to issue the certificate.

To download the certificate file, log in to https://certum.store/. Issued certificates can be found in the Certificates Management tab.


At the bottom of the page there is a list of issued certificates. After clicking on the selected certificate, the available options for the certificate will expand.

5.1. Downloading the pfx/p12 file after activation via key pair generation

If you have activated the certificate by generating a key pair, after selecting the certificate in Certificate Management click on the Download PFX file button.
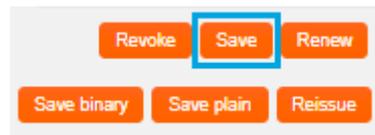
In the next step, run the CryptoAgent app.
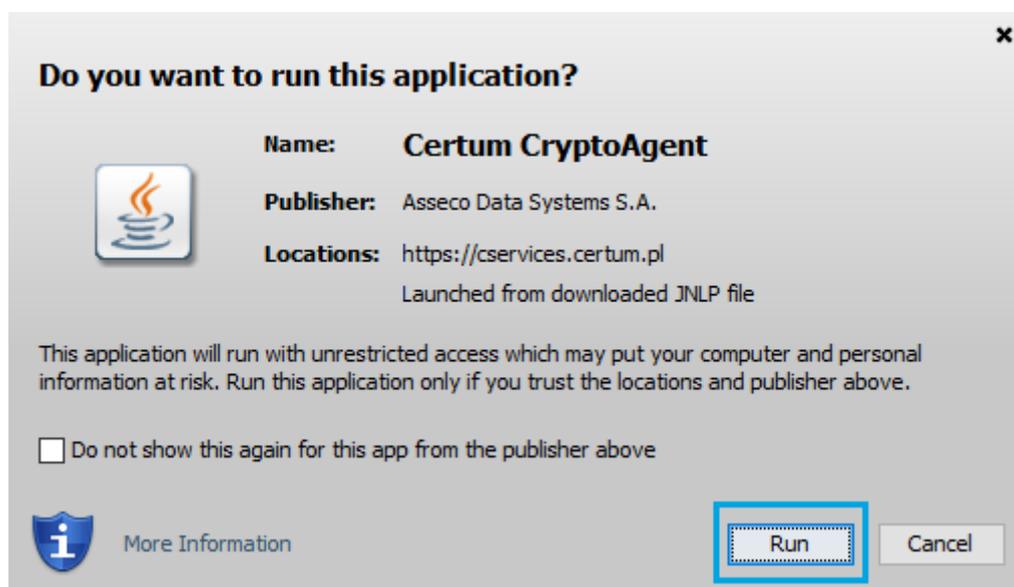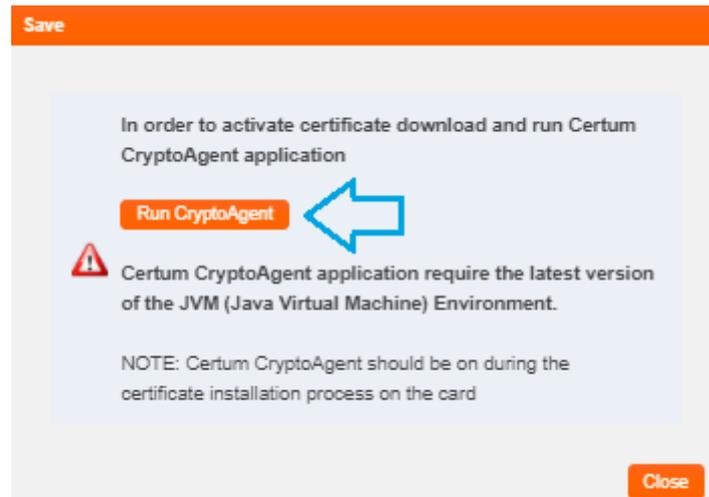
The application will run in the background, and on the website it will be possible to download the certificate. A password will also be generated to the file, which must be saved for it to be possible to access the file. The certificate will be downloaded after clicking on the Get binary button.

5.2. Downloading the certificate and private key files (CSR method)

If you have activated the certificate using the CSR method, the certificate file (the public part) is downloaded directly from the Certificate Management tab in a binary (.cer - Save binary button) or text form (.pem - Save plain button).
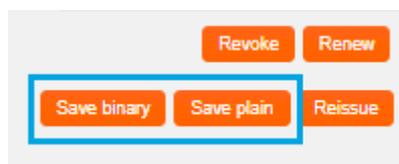
To implement the certificate on the server you also need a private key file (privateKey.pem), which was generated earlier together with the CSR. In case the key is lost, use the Reissue option. This is a reissue of the certificate.