

Reissue – issue a new copy of the certificate

Ver. 1.3

assecO

 **Certum**
by assecO

Table of contents

1. Introduction.....	3
2. How to reissue certificate?.....	3
CSR method.....	5
Generating key pair on a cryptographic card.....	7

1. Introduction

Reissue can be used to get the new copy of the certificate with new pair of keys.

The reasons for certificate reissue:

- issuing the certificate for the next period within the product's validity period,
- private key is lost or it needs to be changed,
- other key algorithm or length is needed,
- error appears during installation or certificate and private key mismatch,
- web server/hosting provider was changed.

After the new certificate is issued, revoke previous certificate if it will not be used anymore.

2. How to reissue certificate?

As the **Certum customer**, you will be able to start the reissue process in the store at **My account** in the **Data security products** tab.

As the **partner**, you will be able to start the reissue process from **Dashboard**, from where you can go to the certificates list.

Find the last issued certificate for the product you want to do reissue for, open its details and use the **Reissue** option.

← Back

Certificate for order 6989e3d4ad202 CN: yourdomain.com

CERTIFICATE STATE: Active

Domain list [2]

Domain: yourdomain.com

Subordinate certificates

Product details

- Product category: SSL (TLS)
- Product: Certum Commercial SSL 365 days - issue
- Order date: 2026-02-09 14:40
- Customer Identifier: a564f131a2a6bfd69041eeb7573b490
- Product's validity period: 2026-08-27 15:41

Certificate details

Buttons: Certificate preview, Download PEM, Download DER, Revoke certificate, Reissue certificate

In the next step, choose how you will provide the keys for the new copy of the certificate. Depending on the product, there are the methods to choose from:

- **CSR** – certificate signing request, generated by a generator, e.g. [Certum Tools](#) or by the application/server where the certificate will be installed
- **Generating key pair on card** – the keys will be saved on the cryptographic card.

When choosing a method for generating key pair on card, also choose the algorithm and key length. Your choice should depend on the algorithm and key length supported by the application in which you use the certificate or the recommendation of e.g. your IT department.

CSR method

1 Choose generation method Key generation Summary

Reissue certificate

Choose one of the key generation methods available below. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card. Key pair for certificates stored in the cloud will be generated automatically.

Key pair generation method

CSR

Reissue can be used to get the new certificate file with new pair of keys.
The reasons for certificate reissue:

- issuing the certificate for the next period within the product's validity period,
- private key is lost or it needs to be changed,
- other key algorithm or length is needed,
- error appears during installation or certificate and private key mismatch,
- web server/hosting provider was changed.

After the new certificate is issued, revoke previous certificate if it will not be used anymore.

Cancel Next

Once you have selected CSR method, you can proceed to submit your CSR. At this stage you will be able to download the [Certum Tools](#) application to generate a CSR or provide your own.

Reissue - CSR data

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

```

B04hIKOUUrczNKNS9A28887X+kqr+Q5EzdDvx8wCSnyohzXx11R7hUCt8mxJV9PE
h3dEqKrG8bvJqK/Qat3s28kSa7VVyVMV/n/u1st4scZzM1CyGmLOTkCAFeSCDKb3
uoIj8qeINwfePQVW6ae0XtekIgo+rc84Sngc8VLnDgGY+rZgc02pvPn6NLNwR0w
9/bDsp814+NZ/aSs3Bqbs9L9wvupIxY0QYyRvrtOyAC4195SMkXFtFhzCnSxV2a6
IedCzmhr9aPN/t5rSICk09DHqPz0LEkMoxpEgJkkyqeew+/Woc0CAwEAATANBgkq
hkiG9w0BAQsFAAOCAQEAhYNsKAJ1WJtvXeZgEHwJS6wz63/su3p5FjaqWNCpxz6R
CqGBBpcuIv/gz30EL8yuCvWEE4y3Jxn/mHef4CnGMmDadyK6BwdhB1K2WS09eqpG
Viv38DHyesHnEHRPLN534/iXUOUYcG4ctqR6BfXALJgIAE0lwSjFbxn91zolncNX
46fCbI8EQcJxaJmBIF3imUVTjua0Mrqg8tfgR1fFc6jvsC+QRpD4r+e2s6P5oOC5
NDJTbvPrK2OS2AVk/JMryF7bnZRzXJFrNOSaQIq4rBWN37jnJYpEreYff+MgMEK6
CYRFRSNUGrMaoqDcA3ViCb2jLwWGx9448N/dJSsS+w==
-----END CERTIFICATE REQUEST-----

```

Correct

Back
Next

After pasting the CSR, it will be verified whether it is correct. If CSR is invalid, you will be notified with an error message.

Positive verification of the CSR and moving forward in the process will submit a new copy of the certificate to be issued. If verification of the domain or e-mail is required, after positive verification, certificate will be issued.

Once the new certificate is issued, you will find it as a new certificate on the Dashboard or in the certificate list. 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.

After the new certificate is issued, revoke previous certificate if it will not be used anymore.

Generating key pair on a cryptographic card

After selecting the method for generating key pair on card, choose the algorithm and key length.

1 Choose generation method Key generation Summary

Reissue certificate

Choose one of the key generation methods available below. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card. Key pair for certificates stored in the cloud will be generated automatically.

Key pair generation method

CSR Generating key pair on card

KEY ALGORITHM AND KEY LENGTH

RSA 2048

The CSR method will allow you to obtain a certificate with a key in a form that can be transferred and installed from a file. Remember to save a private key generated with your CSR. Generating keys on the card will cause that the certificate will be installed on the cryptographic card and its connection to the computer will be required whenever the certificate is used. Only Certum cards are supported.

Reissue can be used to get the new certificate file with new pair of keys.
The reasons for certificate reissue:

- issuing the certificate for the next period within the product's validity period,
- private key is lost or it needs to be changed,
- other key algorithm or length is needed,
- error appears during installation or certificate and private key mismatch,
- web server/hosting provider was changed.

After the new certificate is issued, revoke previous certificate if it will not be used anymore.

In the next step, make sure that you have the card inserted into the reader, the reader connected to the computer and the card itself has an initialized common profile with a PIN code set for it. If it is a new cryptographic card, you may check the instruction of [how to assign PUK and PIN codes for the first time](#).

The screenshot shows a three-step progress bar at the top: 'Choose generation method' (checked), 'Key generation' (active, step 2), and 'Summary'. The main content area is titled 'Reissue certificate' and contains the following text:

Follow the instruction below to generate key pair.

[Download Certum SignService app](#)

1. Download and install the **Certum SignService** application.
2. Download and install the **proCertum CardManager** application if you don't have it installed or it requires updating.
3. Connect the card reader to the computer and insert the card.
4. Open the proCertum CardManager application and check if common profile of the card is initialized. Application will ask to set PIN and PUK codes of the card if it needs to be initialized.
5. Start the key pair generation process using **Generate key pair** button.
6. Accept the prompt message from you browser about running the Certum SignService application.
7. When Certum SignService window appears, enter the PIN code for the common profile of your card.
8. Wait until the key pair is generated, it may take up to several minutes.

An information box states: "When the key pair is generated, next window of the wizard will appear." At the bottom, there is a 'Back' link and a yellow 'Generate key pair' button.

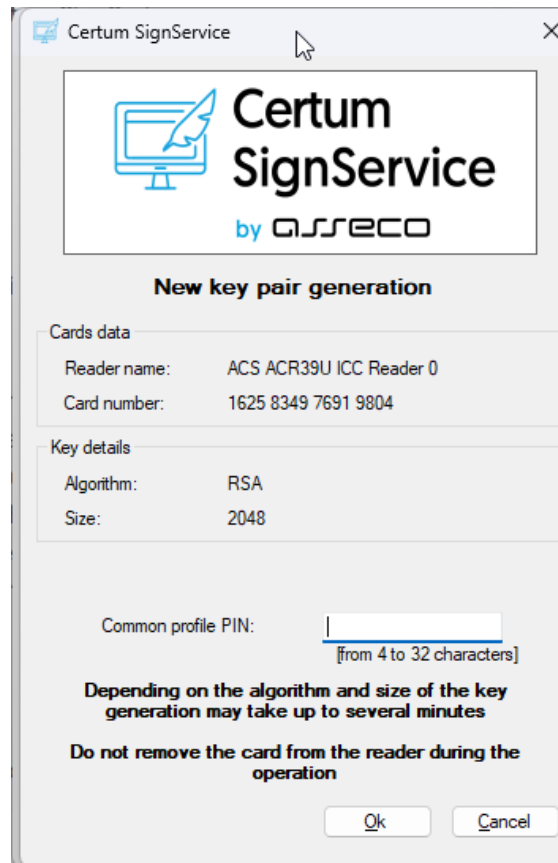
To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.

The screenshot shows a browser window with the Certum logo (by CEFECO) on the left. A dark modal dialog box is open in the center with the following text:

Open CertumSignService?
 https://certmanager.certum.pl wants to open this application.

Buttons: 'Open CertumSignService' and 'Cancel'. A small 'P' icon is visible in the top right corner of the browser window.

At the bottom, a progress bar shows the same three steps as the previous screenshot: 'Choose generation method' (checked), 'Key generation' (active, step 2), and 'Summary'.



After providing the PIN code, the key generation process will begin on the card. This may take up to a few minutes. Once the key is generated, a new copy of the certificate will be submitted to issue. If verification of the domain or e-mail is required, after positive verification, certificate will be issued.

Once the new certificate is issued, you will find it as a new certificate on the Dashboard or in the certificate list. You can install your certificate on the cryptographic card from the certificate details view.

After the new certificate is issued, revoke previous certificate if it will not be used anymore.