

# Reissue – issue a new copy of your certificate

Ver. 1.2

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 .....	8

## 1. Introduction

Reissue can be used to get the new copy of the certificate with new pair of keys but with the same expiration date as the original certificate.

The example reasons for certificate reissue

- the private key for the certificate was lost
- other key algorithm or length is needed
- error appears during installation or certificate and private key mismatch
- web server/hosting provider was changed



Reissue will automatically invalidate the previous certificate 14 days after issuing a new copy of the certificate. This is the time to replace the certificate in the application or on the server. Due to this, we encourage all users who reissue the certificate to immediately install a new copy of the certificate to ensure that the website or a signing application still uses valid certificate.

## 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 valid certificate you want to reissue, open its details and use the **Reissue** option.

**Certum**  
by **ASSECO**

← Back

Certificate for order ORDER/0000123456/po

CN: abcabcabc11.pl

CERTIFICATE STATE **Valid**

**Subscriber's data**

Name	Last name	E-mail address
Paula	Chlebicka	paula.chlebicka@assecodata.pl

Verification method  
Automatic identity verification

**Organization's data**

Organization	Verification method
Asseco Data Systems S.A.	KRS 0000421310

Country	State or province	Locality
Poland	pomorskie	Gdańsk

**Subscriber's authorization**

Verification method  
KRS 0000421310

**Domain list [2]**

Domain
assecodata.pl
www.assecodata.pl

**Subordinate certificates**

**Details**

- Product category: SSL (TLS)
- Product: Trusted MultiDomain SSL 4 domains 365 days - issue
- Activation date: 2023-11-02 14:30
- Valid to: 2024-11-01 14:30
- Certificate serial number: 6a5d7ffef2f6c2ac3b0b4a43c2cb773

**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

The screenshot shows the Certum web interface. On the left is a navigation menu with 'Dashboard', 'Certificates', and 'Certificates search'. The main content area has a progress bar with two steps: 'Choose generation method' (active) and 'Key generation'. Below the progress bar is a white card titled 'Reissue certificate'. The card contains the following text: '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.' Under the heading 'Key pair generation method', the 'CSR' option is selected with a radio button. A light blue information box contains the text: 'The reissue can be used to get the new copy of the certificate with new pair of keys but with the same expiration date as the original certificate. The reasons for certificate reissue: - the private key for the certificate was lost, - other key algorithm or length is needed, - error appears during installation or certificate and private key mismatch, - web server/hosting provider was changed. Issuing a reissue certificate will automatically revoke the previous certificate after 14 days.' At the bottom of the card are 'Cancel' and 'Next' buttons.

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.

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

✓
2

Choose generation method    Key generation

## Reissue - CSR data

Enter Certificate Signing Request [CSR] or use the Certum Tools application to generate new CSR.

```

LcZNBbFKx9i:fenLdvM3zB4zdevuiw6s9+So4k/G4IsWH/V6hFOqqgE1sGnekksP
2F0pFWLsE2AB7lcV82dtvvVT8k/v1mH0h4vTLRii6i+qbmSoc4FrvjHPolreBYI
ummkF80IqVTUGD2fS8j5mkQDUKOYAQA2wgop4tsT+S8IGB/zwHvRB22cKWA4iV
-----BEGIN-----
-----END CERTIFICATE REQUEST-----

```

✓ Correct

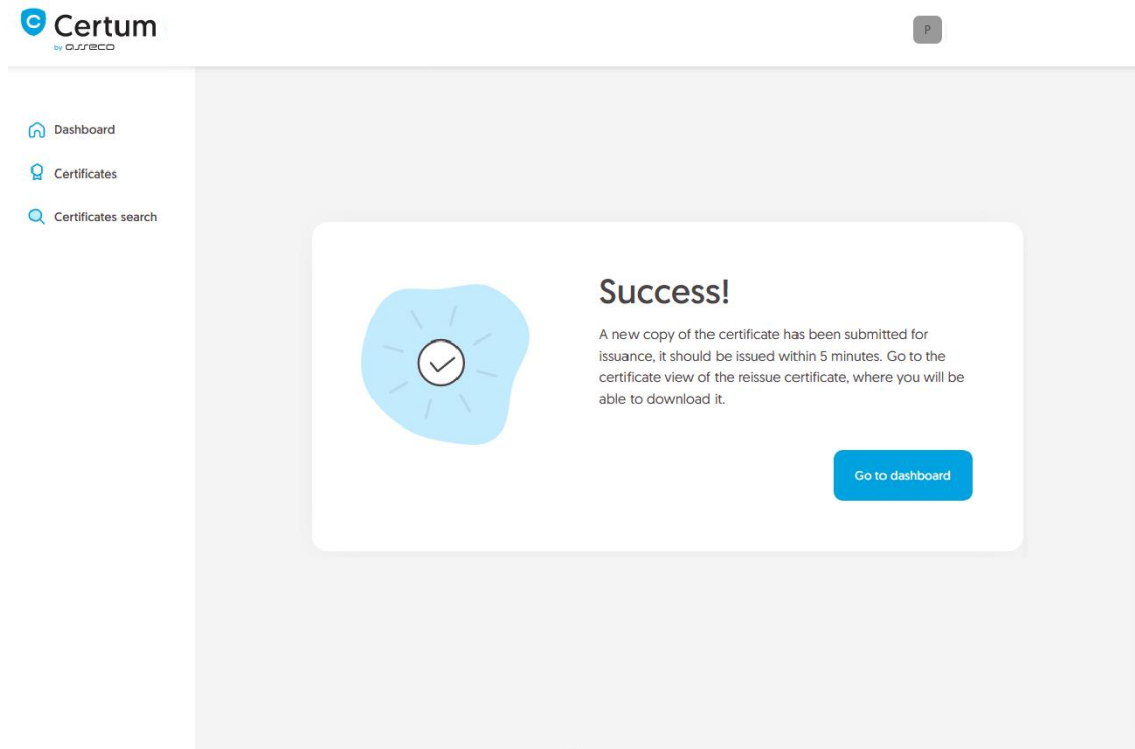
[Download Certum Tools app](#)

[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.



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.

Therefore, the previous certificate will be submitted for revocation within 14 days. Reminder:



Reissue will automatically invalidate the previous certificate 14 days after issuing a new copy of the certificate. This is the time to replace the certificate in the application or on the server. Due to this, we encourage all users who reissue the certificate to immediately install a new copy of the certificate to ensure that the website or a signing application still uses valid certificate.

## Generating key pair on a cryptographic card

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

**Certum**  
by GRSPEC

Dashboard  
Certificates  
Certificates search

Choose generation method | Key generation

### 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

Choose key algorithm and key length

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.

The reissue can be used to get the new copy of the certificate with new pair of keys but with the same expiration date as the original certificate. The reasons for certificate reissue:

- the private key for the certificate was lost,
- other key algorithm or length is needed,
- error appears during installation or certificate and private key mismatch,
- web server/hosting provider was changed.

Issuing a reissue certificate will automatically revoke the previous certificate after 14 days.

Cancel Next

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 the Certum web interface. On the left, there is a navigation menu with 'Dashboard', 'Certificates', and 'Certificates search'. The main content area is titled 'Reissue certificate' and includes a progress indicator with two steps: 'Choose generation method' (completed) and 'Key generation' (current). Below the title, there is a link to 'Download Certum SignService app' and a list of 9 numbered instructions for generating keys on a card. A blue information box states: 'Certum SignService application is available only for Windows.' At the bottom right, there is a yellow 'Generate key pair' button and a 'Back' link.

**Reissue certificate**

To generate a pair of keys, download and run the application **Certum SignService**

[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.
9. When the key pair is generated, next window of the wizard will appear.

**i** Certum SignService application is available only for Windows.

[Back](#) [Generate key pair](#)

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 the same Certum web interface as above, but with a browser security warning dialog box overlaid. The dialog box title is 'Allow this site to open the certumkoalaservice link with CertumSignService?'. It contains a link 'Choose a different application.' and a checkbox 'Always allow http://100.101.10.90:4300 to open certumkoalaservice links'. At the bottom of the dialog are 'Open Link' and 'Cancel' buttons. The background interface is dimmed.

**Allow this site to open the certumkoalaservice link with CertumSignService?**

[Choose a different application.](#)

Always allow <http://100.101.10.90:4300> to open certumkoalaservice links

[Open Link](#) [Cancel](#)



The image shows a Windows-style dialog box titled "Certum SignService". At the top left is a small icon of a computer monitor with a pen writing on it. To its right is the text "Certum SignService" in a large, bold, black font, with "by GISECO" in a smaller, blue font below it. Below the logo is the heading "New key pair generation" in bold black text. The dialog is divided into two main sections: "Cards data" and "Key details".

**Cards data**

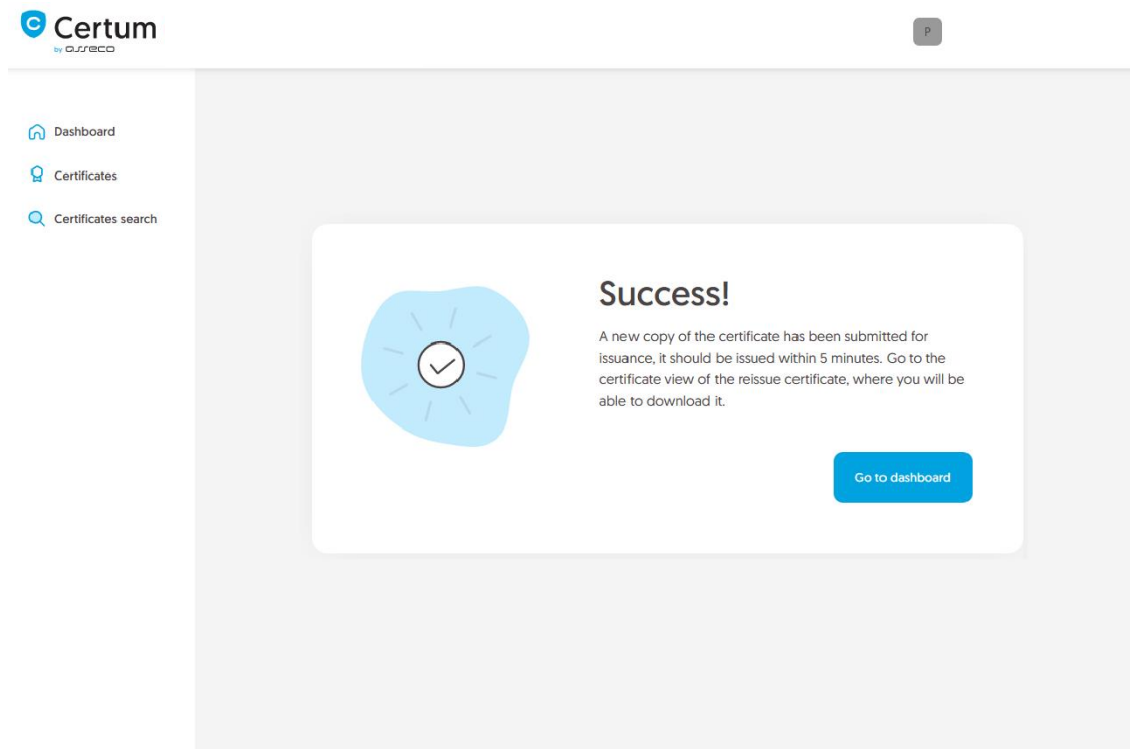
Reader name:	ACS ACR39U ICC Reader 0
Card number:	1625 8349 7691 9804

**Key details**

Algorithm:	RSA
Size:	2048

Below these sections is a text label "Common profile PIN:" followed by a text input field. Below the input field is the text "[from 4 to 32 characters]". Below this is a bold warning: "Depending on the algorithm and size of the key generation may take up to several minutes". Below that is another bold warning: "Do not remove the card from the reader during the operation". At the bottom right are two buttons: "Ok" and "Cancel".

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.



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.

Therefore, the previous certificate will be submitted for revocation within 14 days. Reminder:



Reissue will automatically invalidate the previous certificate 14 days after issuing a new copy of the certificate. This is the time to replace the certificate in the application or on the server. Due to this, we encourage all users who reissue the certificate to immediately install a new copy of the certificate to ensure that the website or a signing application still uses valid certificate.