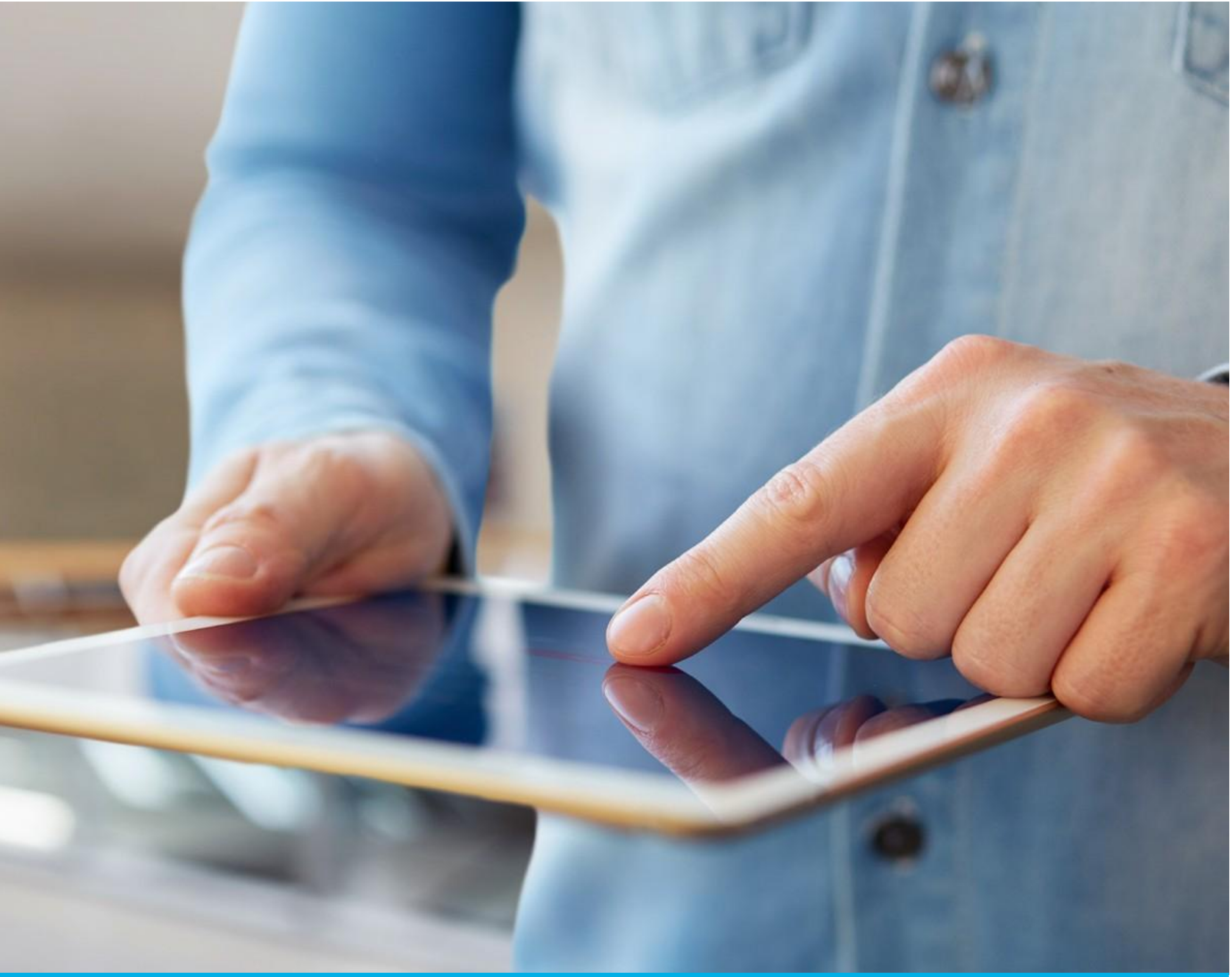


# Reissue – issue a new copy of your certificate

Ver. 1.1

## 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

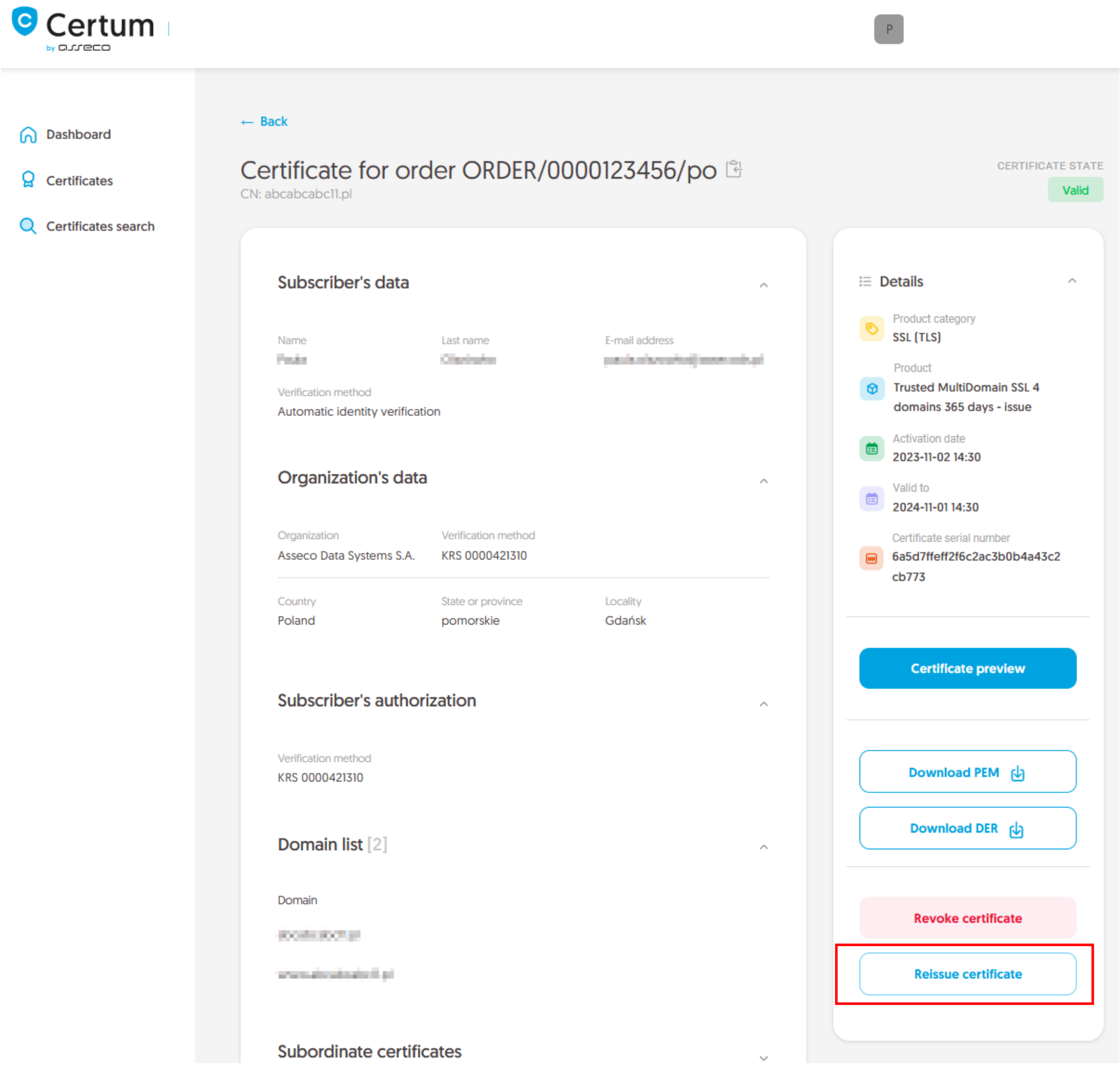
Reissue will automatically invalidate the previous certificate 14 days after issuing a new copy of the certificate. This is the time to replace the certificate in the application or on the server. Due to this, we encourage all users who reissue the certificate to immediately install a new copy of the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

P

Dashboard

Certificates

Certificates search

← Back

Certificate for order ORDER/0000123456/po

CN: abcabcabc11.pl

CERTIFICATE STATE

Valid

Subscriber's data

Name: [redacted]

Last name: [redacted]

E-mail address: [redacted]

Verification method: Automatic identity verification

Organization's data

Organization: Asseco Data Systems S.A.

Verification method: KRS 0000421310

Country: Poland

State or province: pomorskie

Locality: Gdańsk

Subscriber's authorization

Verification method: KRS 0000421310

Domain list [2]

Domain

[redacted]

[redacted]

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: 6a5d7ffeff2f6c2ac3b0b4a43c2cb773

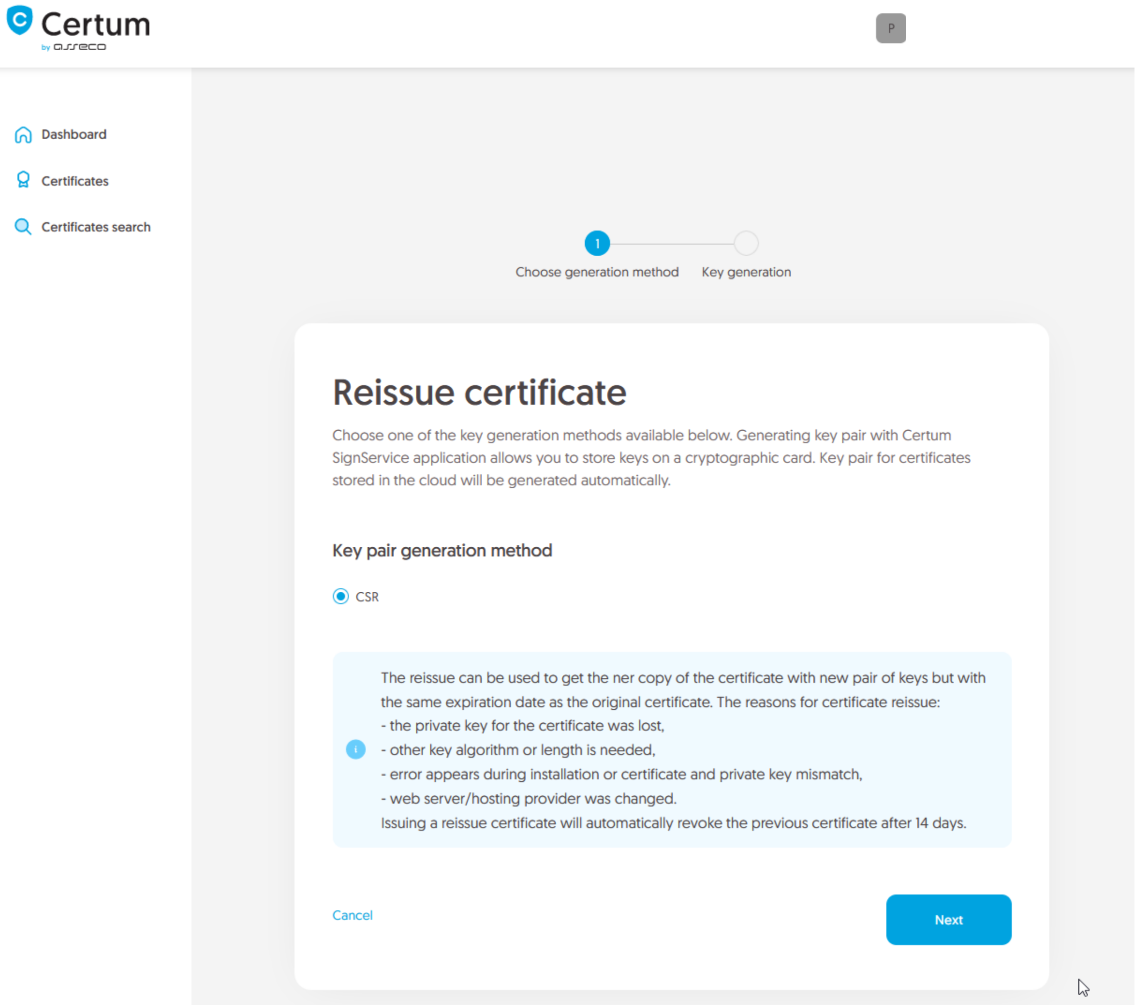
In the next step, choose how you will provide the keys for the new copy of the certificate. Depending on the product, there are the methods to choose from:

• **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



# Reissue certificate

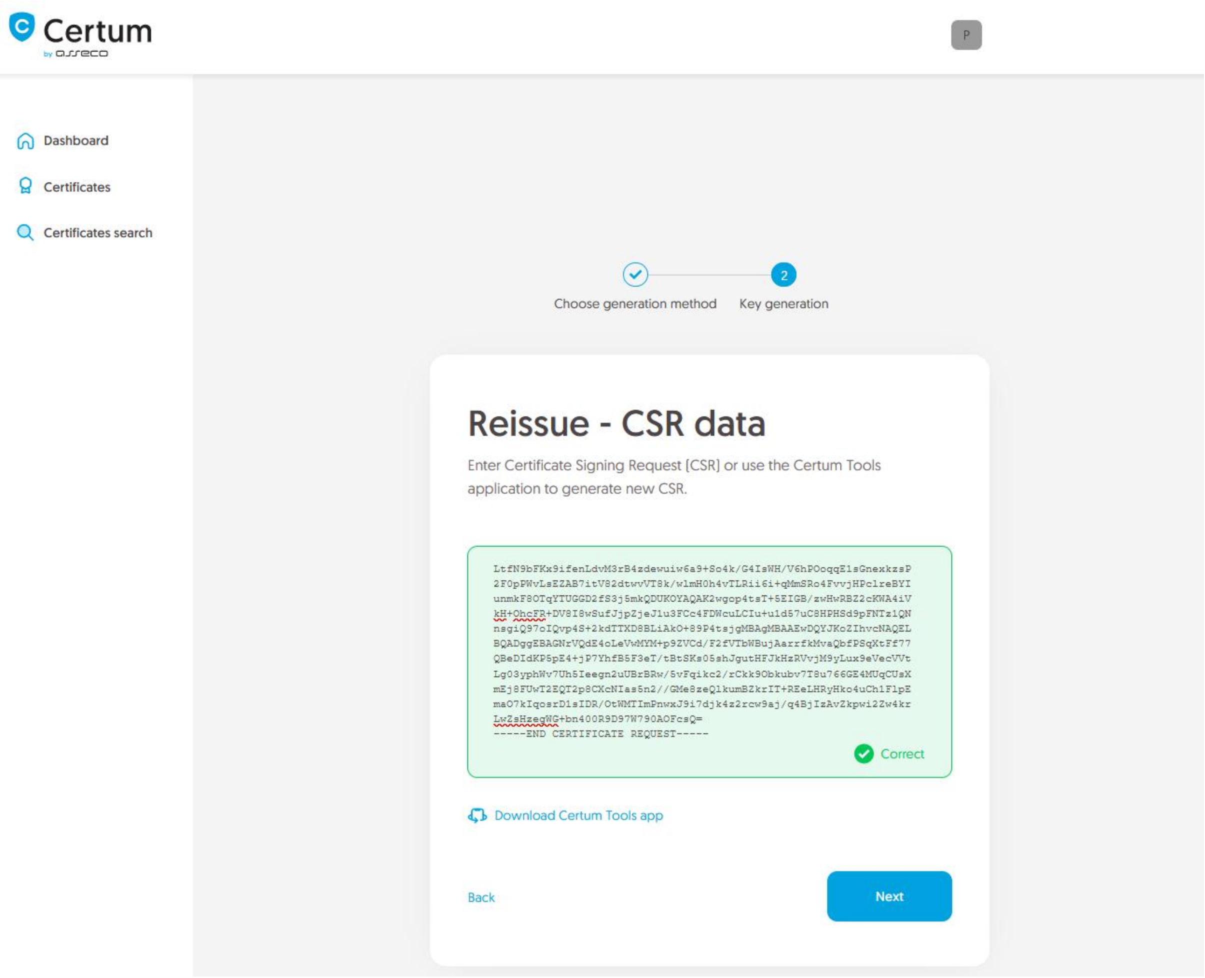
Choose one of the key generation methods available below. Generating key pair with Certum SignService application allows you to store keys on a cryptographic card. Key pair for certificates stored in the cloud will be generated automatically.

Key pair generation method

● CSR

The reissue can be used to get the ner 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.

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.

```
LtfN9bFKx9ifenLdvM3rB4zdewuiw6a9+So4k/G4IsWH/V6hPOoqqE1sGnexkzsP
2F0pPWvLsEZAB7itV82dtwvVT8k/wlmH0h4vTLRii6i+qMmSRo4FvvjHPclreBYI
unmkF8OTqYTUGGD2fS3j5mkQDUKOYAQAK2wgop4tsT+5EIGB/zwHwRBZ2cKWA4iV
kH+QhcFR+DV8I8wSufJjpZjeJ1u3FCc4FDWcuLCIu+u1d57uC8HPHSd9pFNTz1QN
nsgiQ97oIQvp4S+2kdTTXD8BLiAkO+89P4tsjgMBAgMBAAEwDQYJKoZIhvcNAQEL
BQADggEBAGNrVQdE4oLeVwMYM+p9ZVCd/F2fVTbWBujAarrfkMvaQbfPSqXtFf77
QBeDIdKP5pE4+jP7YhfB5F3eT/tBtSKs05shJgutHFJkHzRVvjM9yLux9eVecVVt
Lg03yphWv7Uh5Ieegn2uUBrBRw/5vFqikc2/rCkk9Obkubv7T8u766GE4MUqCUsX
mEj8FUwT2EQT2p8CXcNIas5n2//GMe8zeQlkumBZkrIT+REeLHRyHko4uCh1FlpE
maO7kIqosrD1sIDR/OtWMTImPnwxJ9i7djk4z2rcw9aj/q4BjIzAvZkpwi2Zw4kr
LwZsHzegWG+bn400R9D97W790AOFcsQ=
-----END CERTIFICATE REQUEST-----
```

✓ Correct

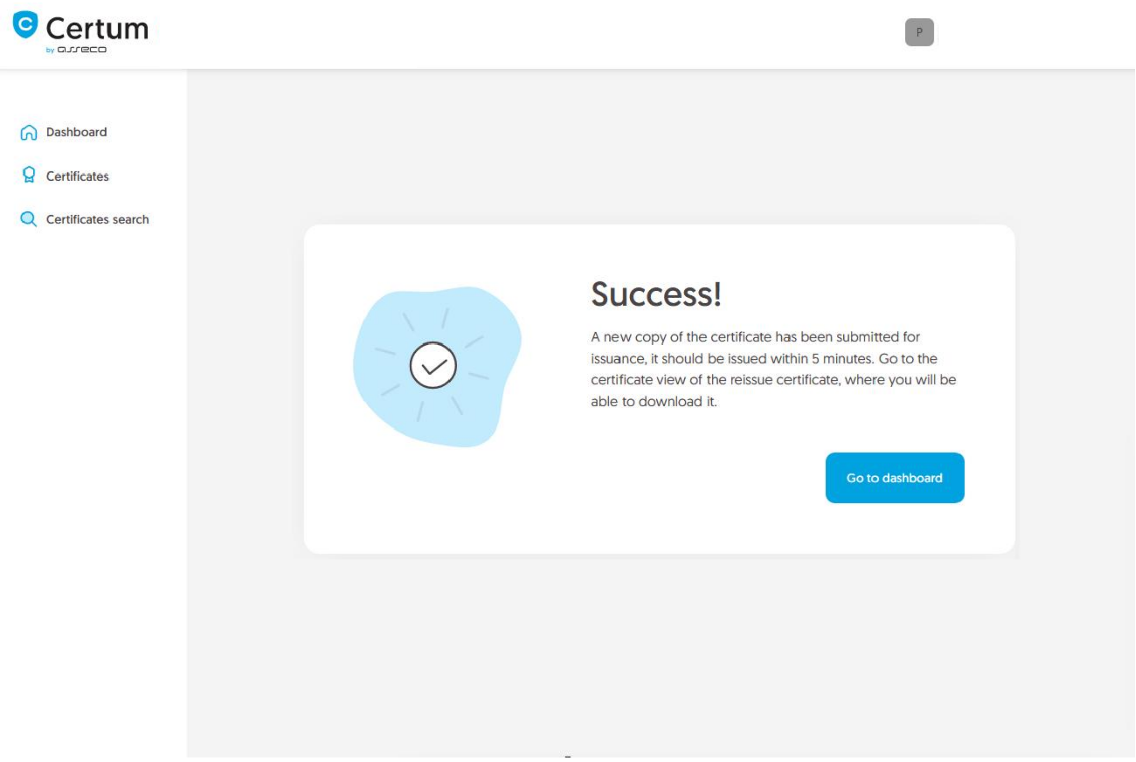
Download Certum Tools app

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.



Success!

A new copy of the certificate has been submitted for issuance, it should be issued within 5 minutes. Go to the certificate view of the reissue certificate, where you will be able to download it.

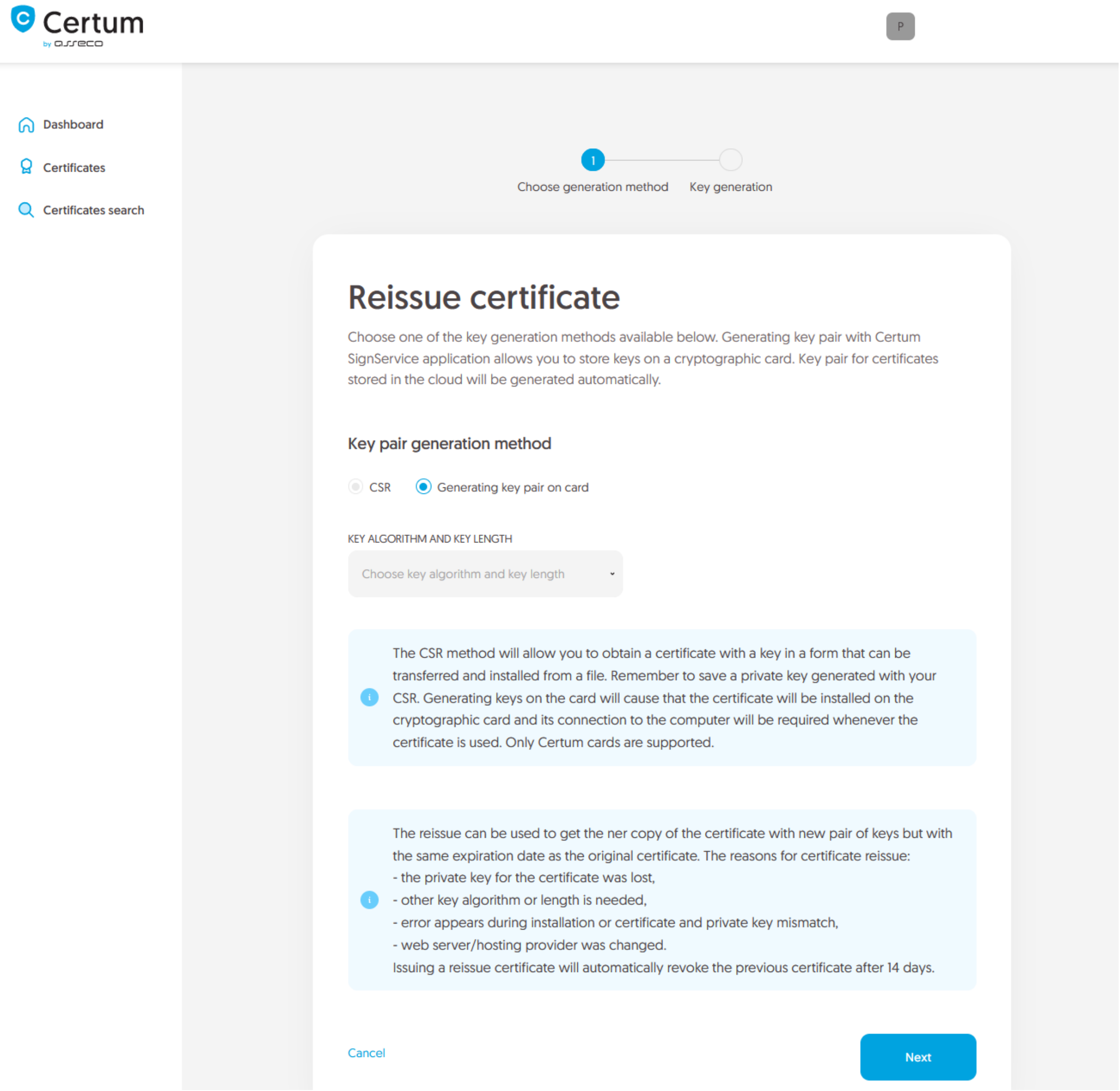
Once the new certificate is issued, you will find it as a new certificate on the Dashboard or in the certificate list. The issued certificate can be downloaded from the certificate creation e-mail or from the certificate details view: in a convenient **PEM** or **DER** encoding.

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.



### 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

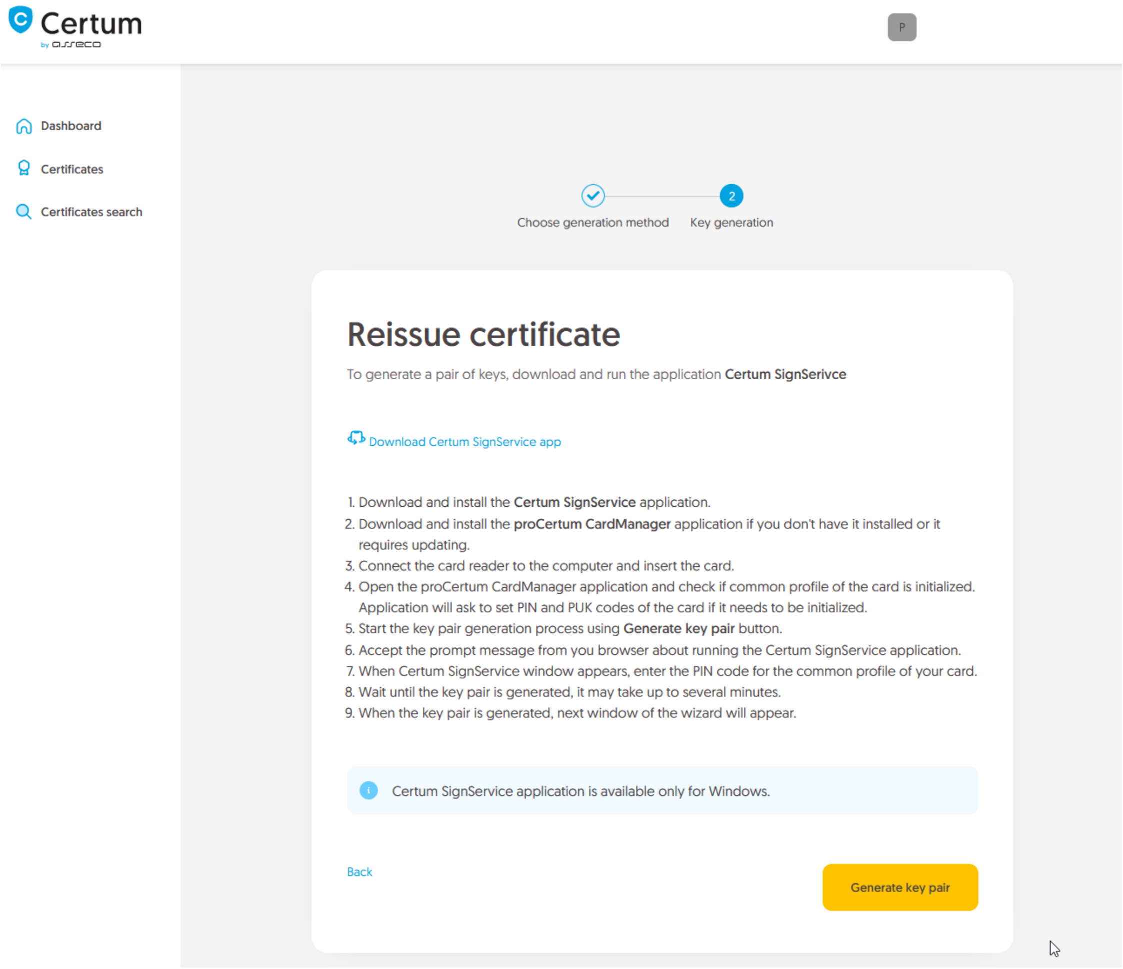
KEY ALGORITHM AND KEY LENGTH

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 ner 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.

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.



## Reissue certificate

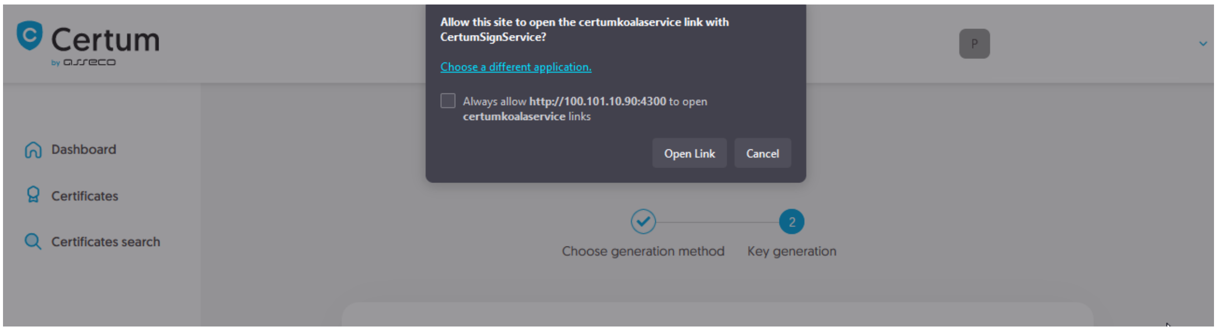
To generate a pair of keys, download and run the application **Certum SignSerivce**

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.

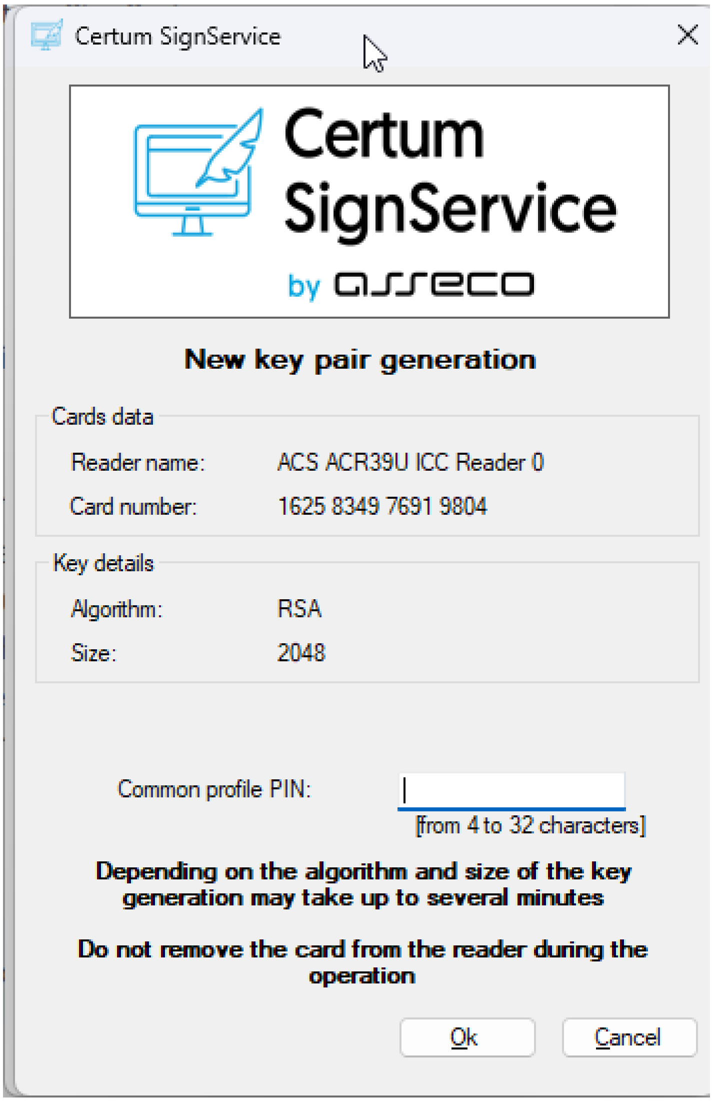
Certum SignService application is available only for Windows.

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.


**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



New key pair generation

Cards data

Reader name: ACS ACR39U ICC Reader 0

Card number: 1625 8349 7691 9804

Key details

Algorithm: RSA

Size: 2048

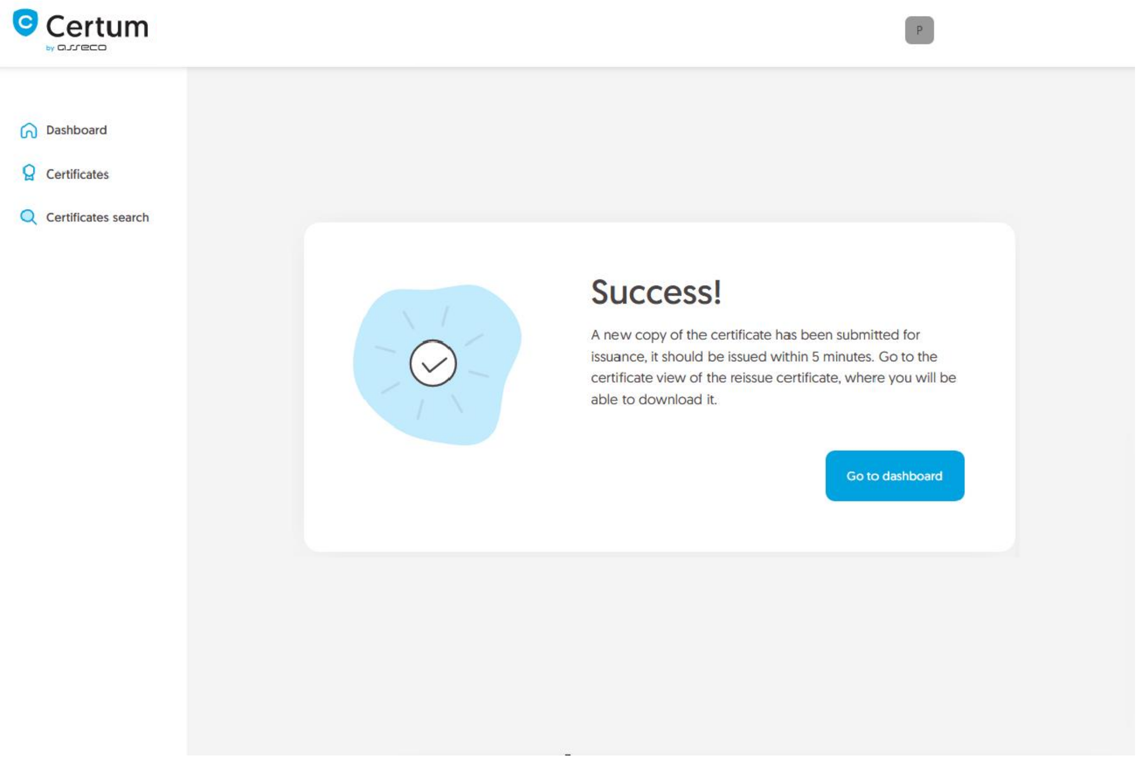
Common profile PIN:

[from 4 to 32 characters]

Depending on the algorithm and size of the key generation may take up to several minutes

Do not remove the card from the reader during the operation

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.



Success!

A new copy of the certificate has been submitted for issuance, it should be issued within 5 minutes. Go to the certificate view of the reissue certificate, where you will be able to download it.

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.