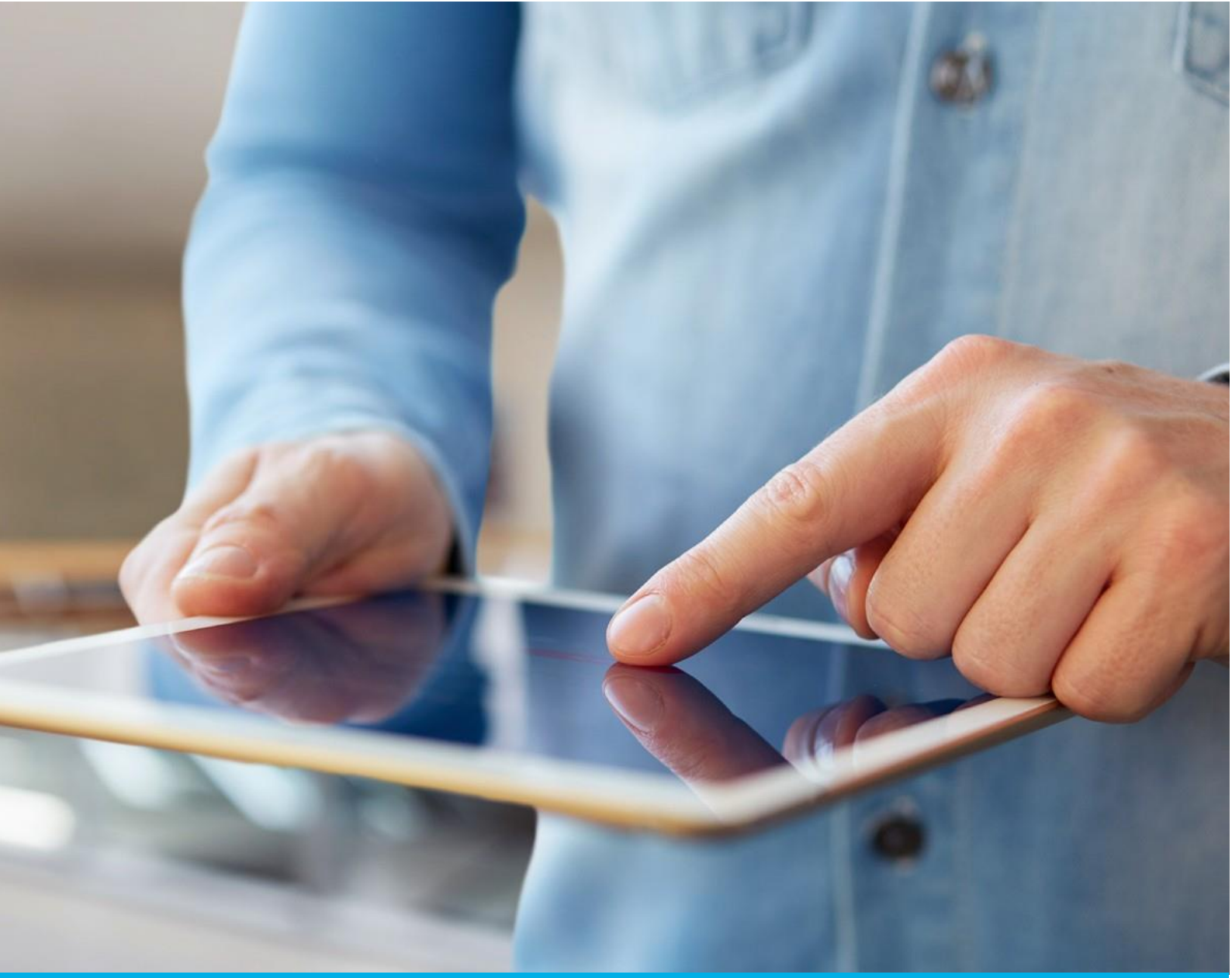


Reissue – issue a new copy of your certificate

Ver. 1.2

asseco

Certum by asseco

Table of contents

certum.pl
infolinia@certum.pl

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.

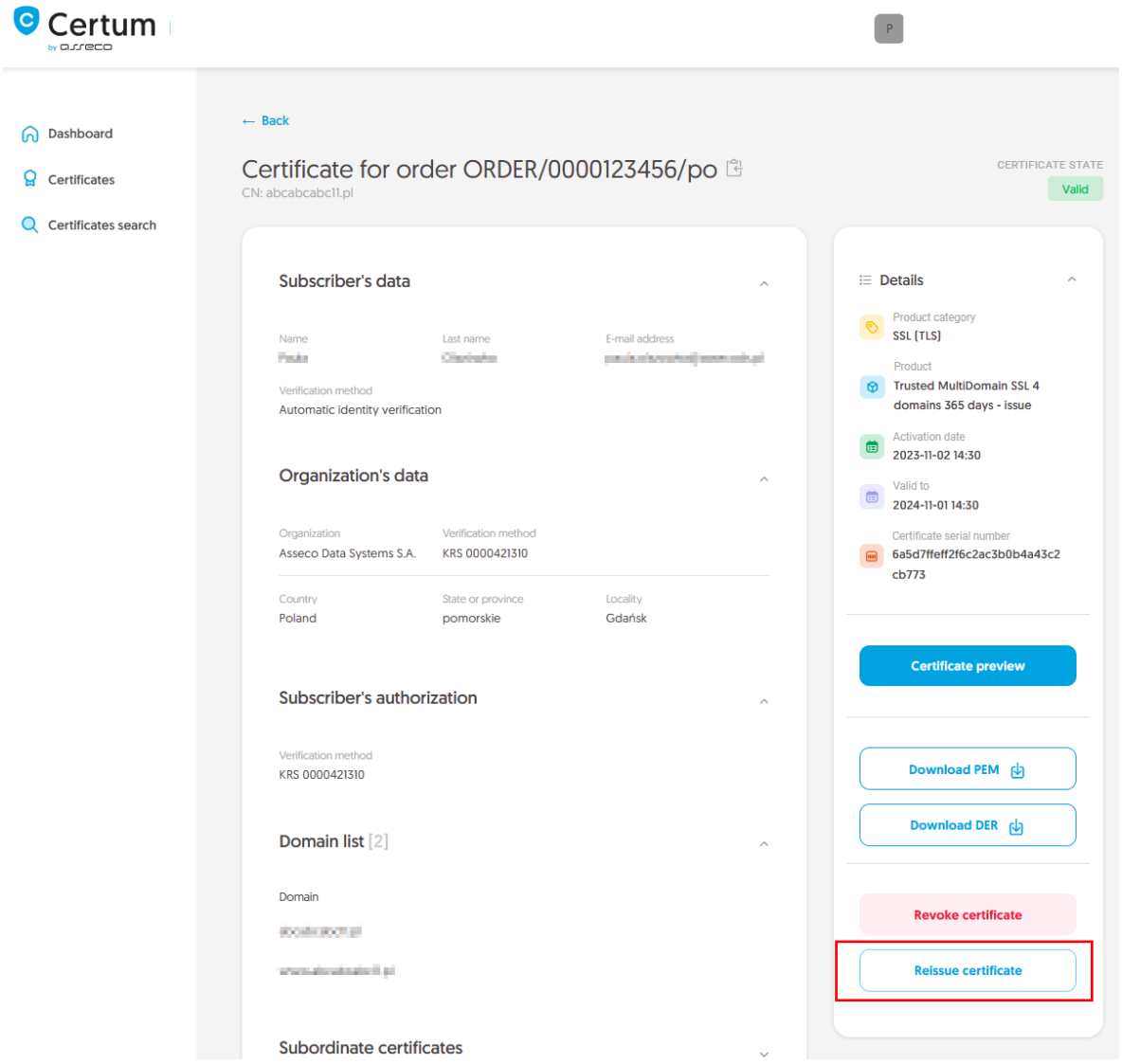
2. How to reissue certificate?

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.pl
infolinia@certum.pl



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:

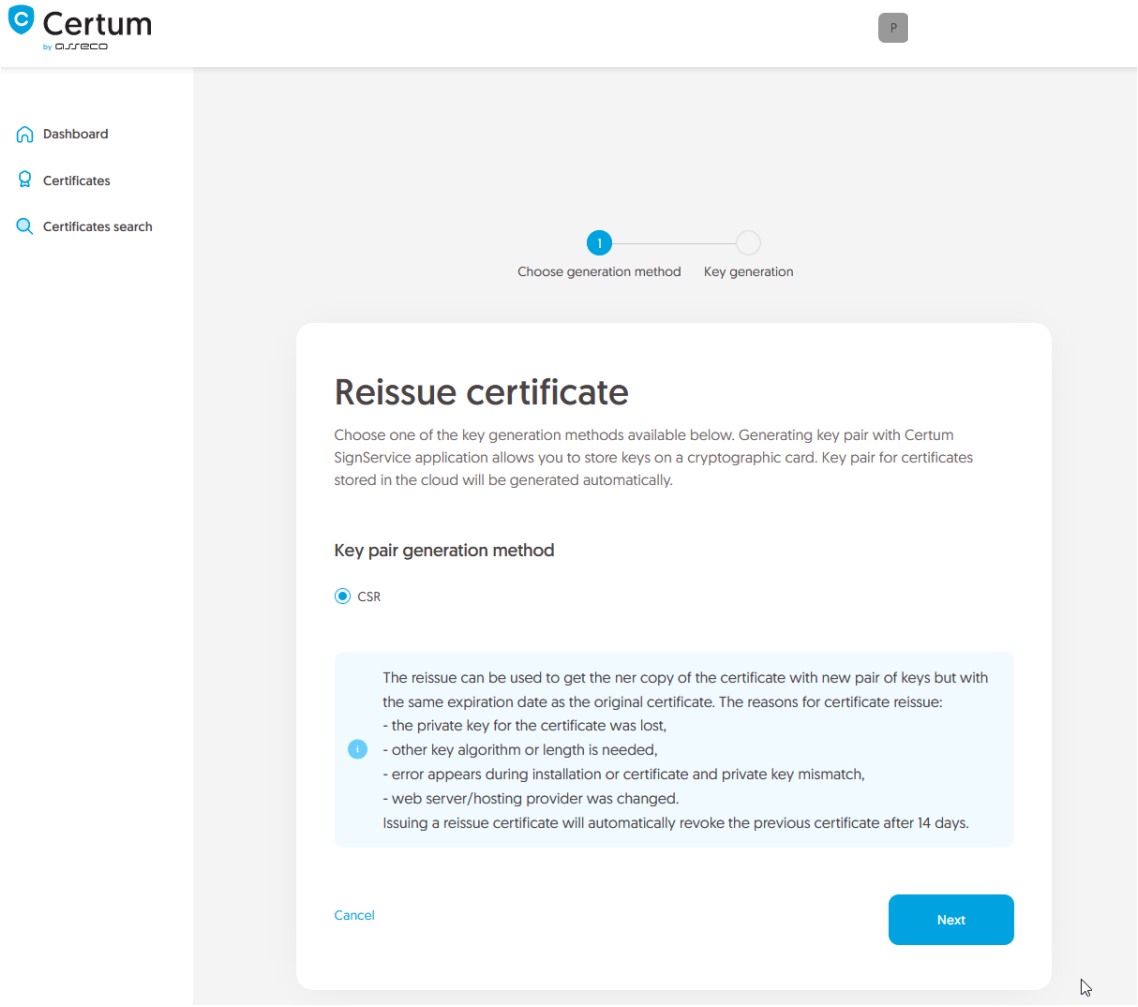
• **CSR** – certificate signing request, generated by a generator, e.g. Certum Tools or by the application/server where the certificate will be installed

• **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.

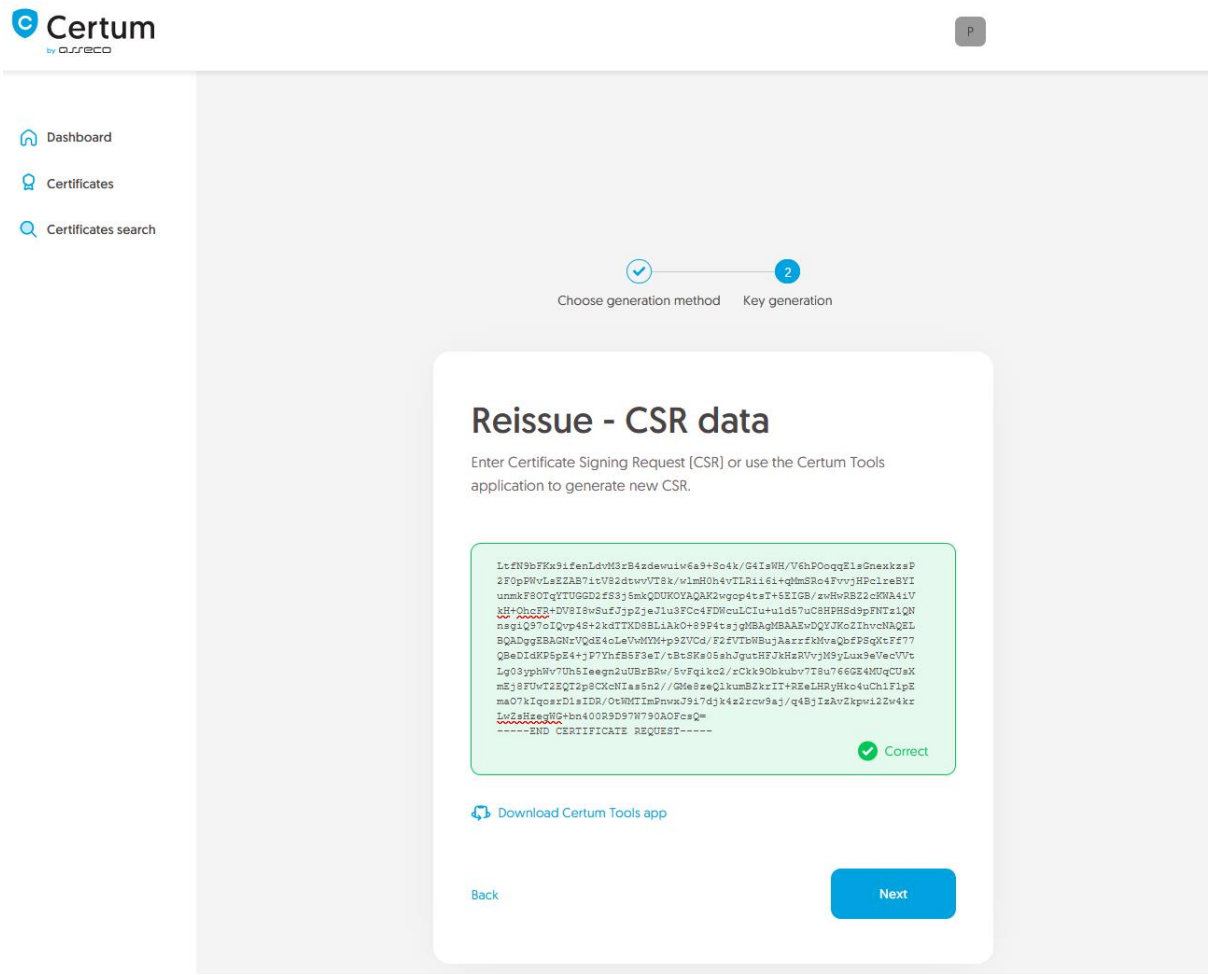
certum.pl
infolinia@certum.pl

CSR method



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.

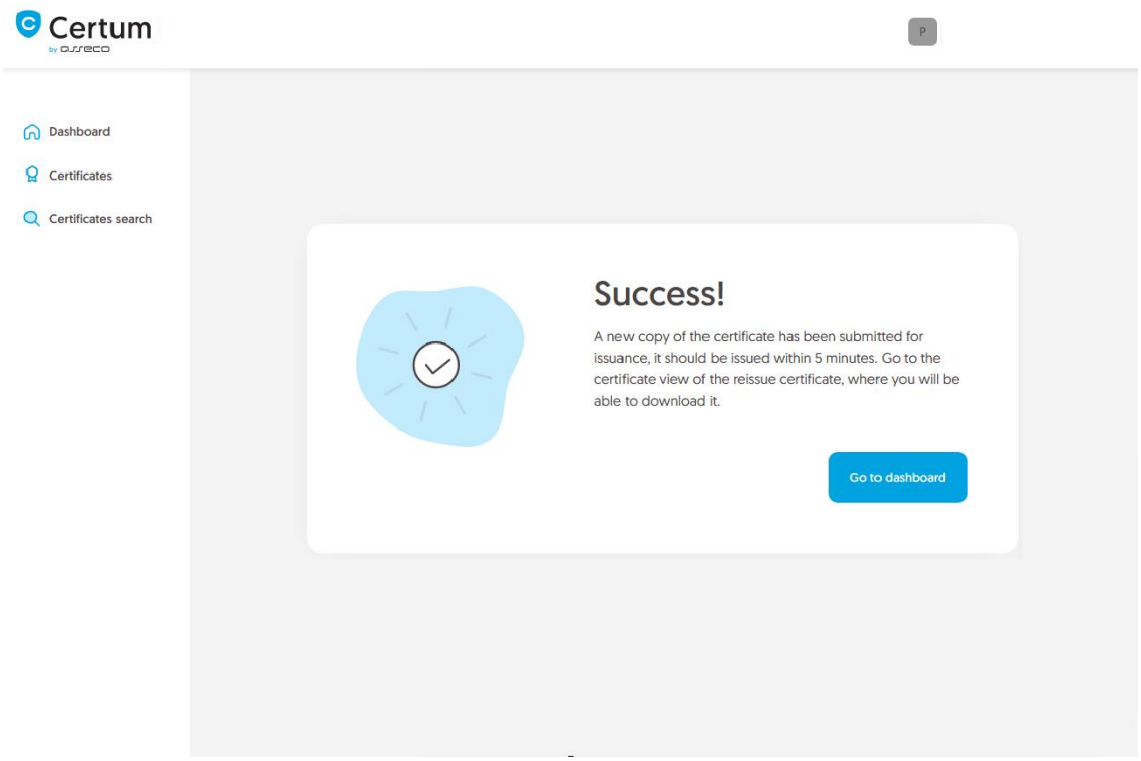
certum.pl
infolinia@certum.pl



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.

certum.pl
infolinia@certum.pl



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.

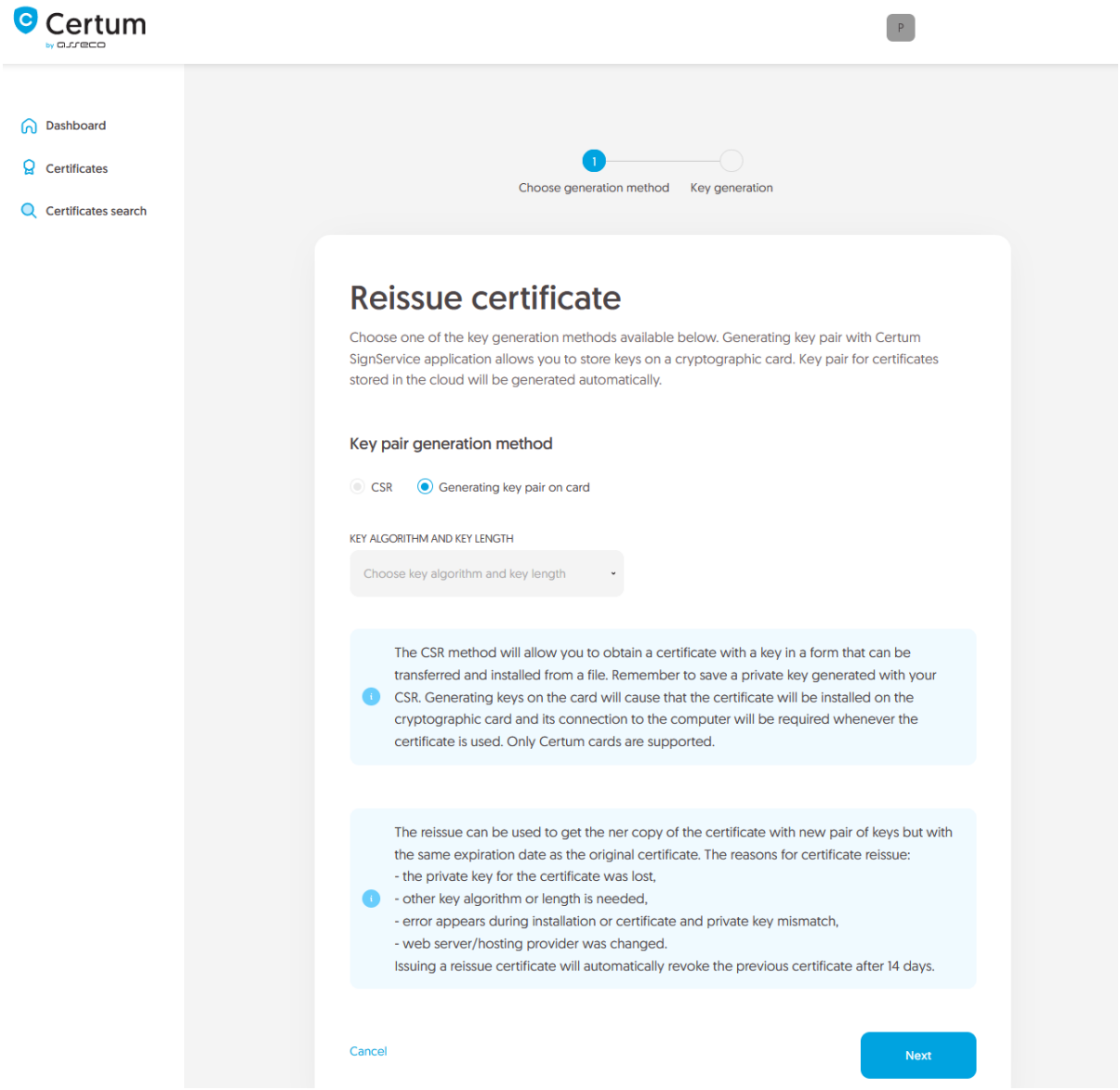
Therefore, the previous certificate will be submitted for revocation within 14 days. Reminder:

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.

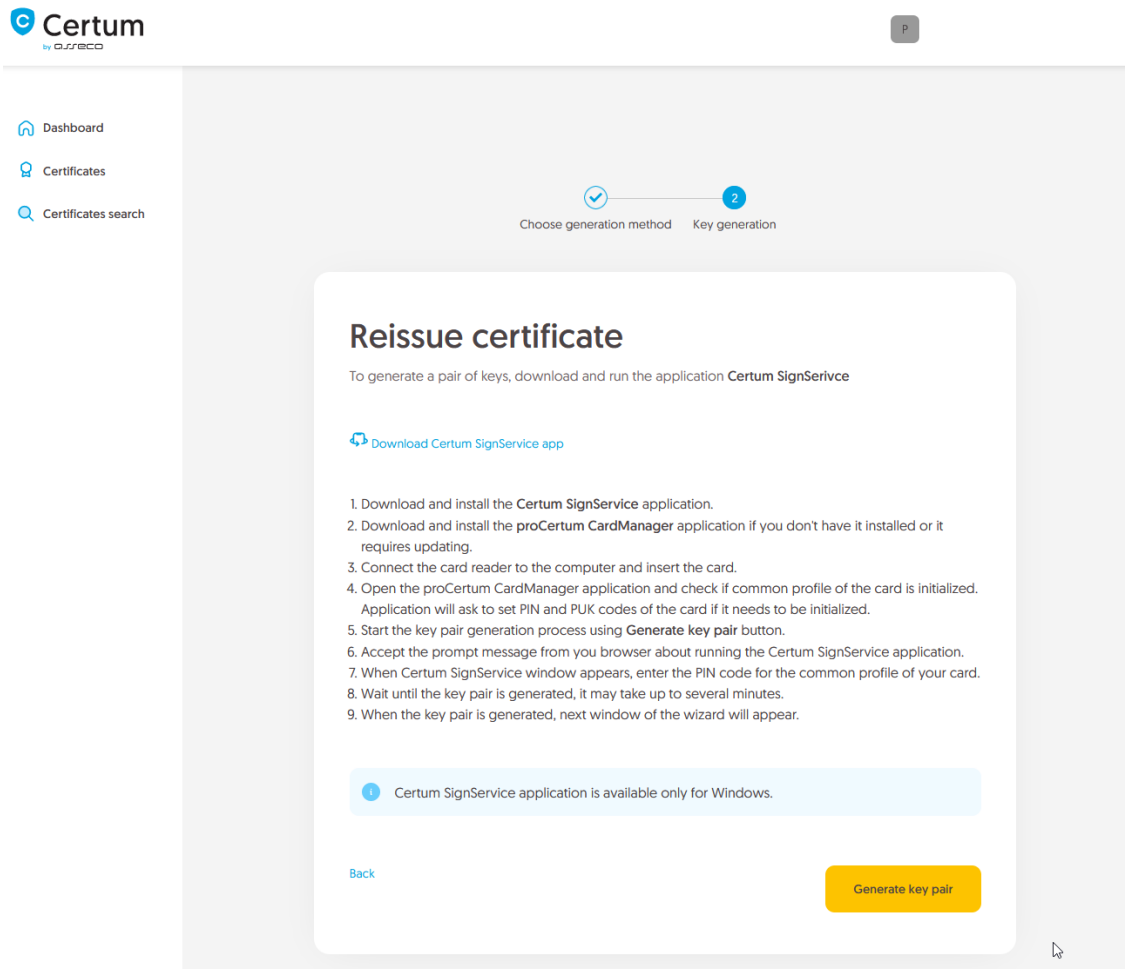
certum.pl
infolinia@certum.pl

Generating key pair on a cryptographic card

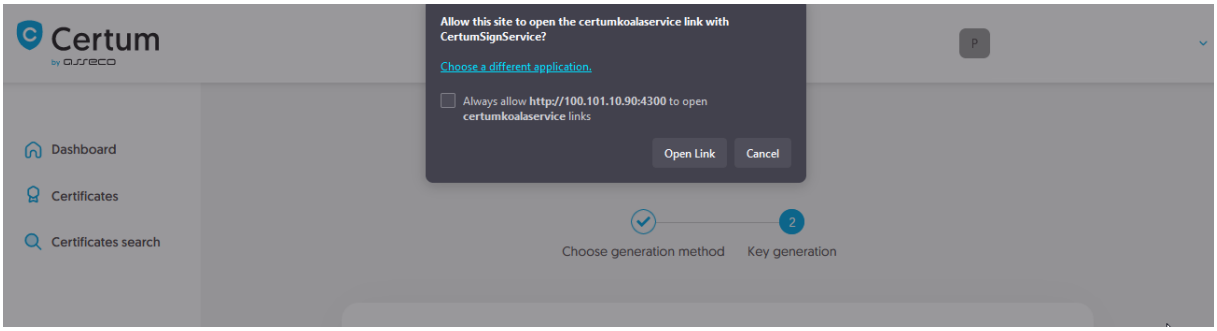
After selecting the method for generating key pair on card, choose the algorithm and key length.



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.

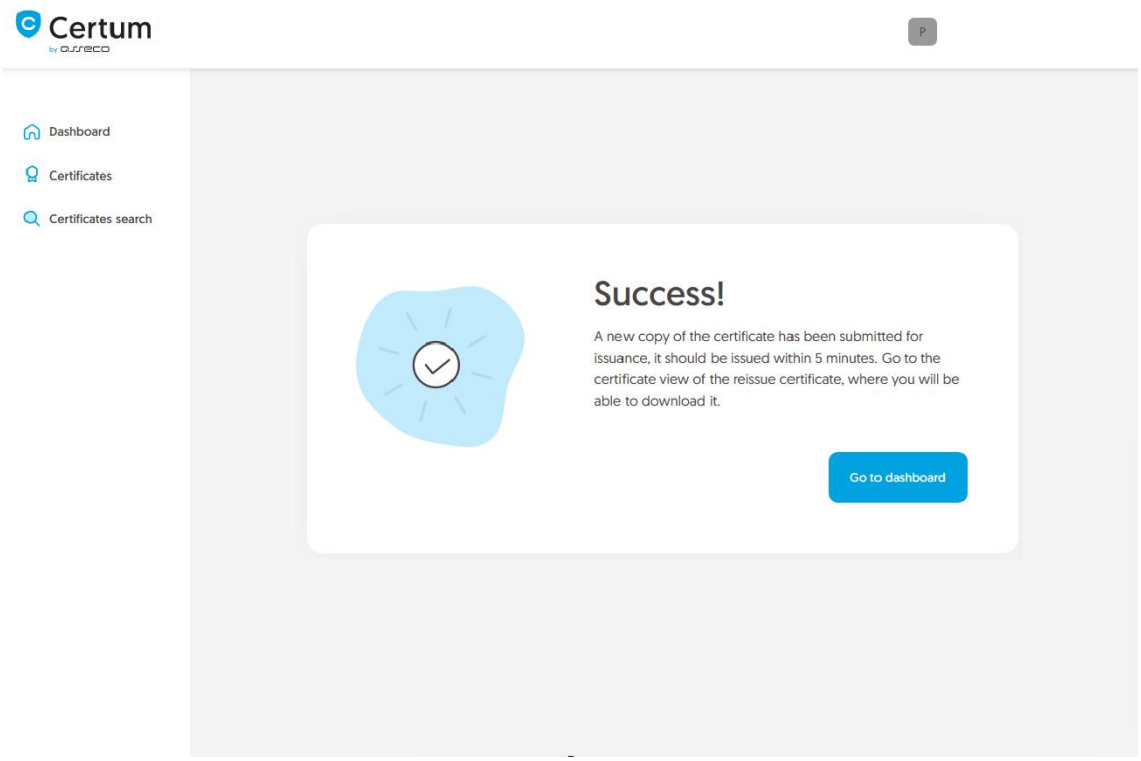


To generate keys on the card, you will also need the Certum SignService application installed on your computer. After starting key generation, the Certum SignService application can ask for permission to run and then to provide the PIN code of the card's common profile in order to generate keys on it.



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.

certum.pl
infolinia@certum.pl



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.

certum.pl
infolinia@certum.pl