Generate a certificate renewal request User Guide

Content

1. Introduction

This document serves as a guide on how to proceed when generating a subsequent certificate request via the website.

2. Software requirements

The computer on which the certificate request will be generated must meet the following requirements:

2.1. Operating system

- Windows 10
- Windows 11
- MacOS

2.2. Supported browsers are:

- Microsoft Edge
- Chrome
- Firefox
- Opera

2.3. Javascript scripting support enabled in the internet browser, support for storing cookies.

2.4. **I.CA PKIService host** component and extension installed

2.5. **I.CA SecureStore Card Manager** (only in case of generating a request for a smart card)

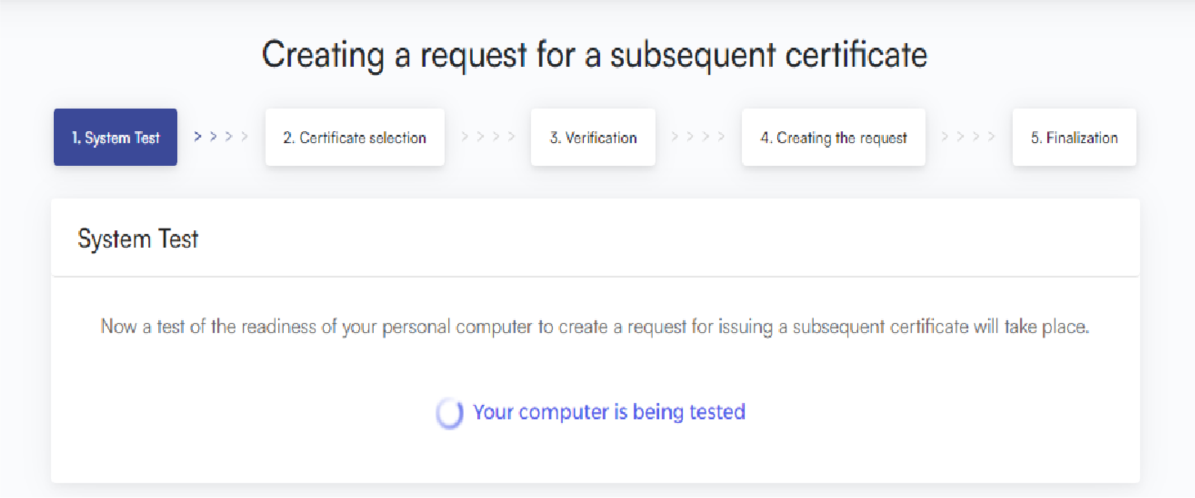
3. Process for generating a subsequent certificate request

The procedure for generating a subsequent certificate request is divided into several steps:

1. **System Test**
2. **Certificate selection**
3. **Verification**
4. **Creating the request**
5. **Finalization**

3.1. Software Inspection

To facilitate the check of your computer's readiness to generate a request, a control page is displayed when the request generation begins, which verifies the presence of key software components.



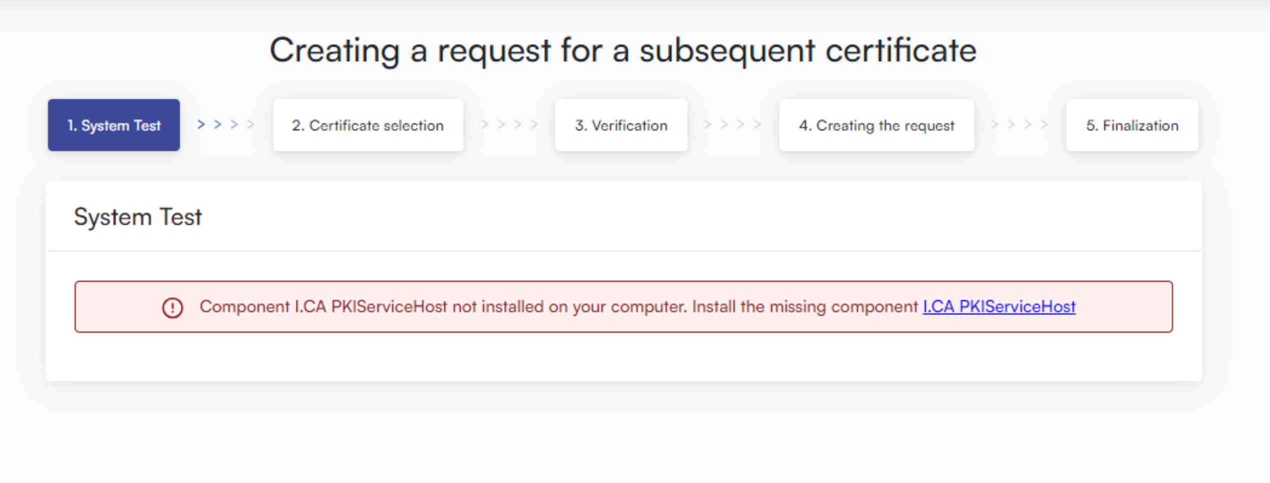
Creating a request for a subsequent certificate

System Test

Now a test of the readiness of your personal computer to create a request for issuing a subsequent certificate will take place.

Your computer is being tested

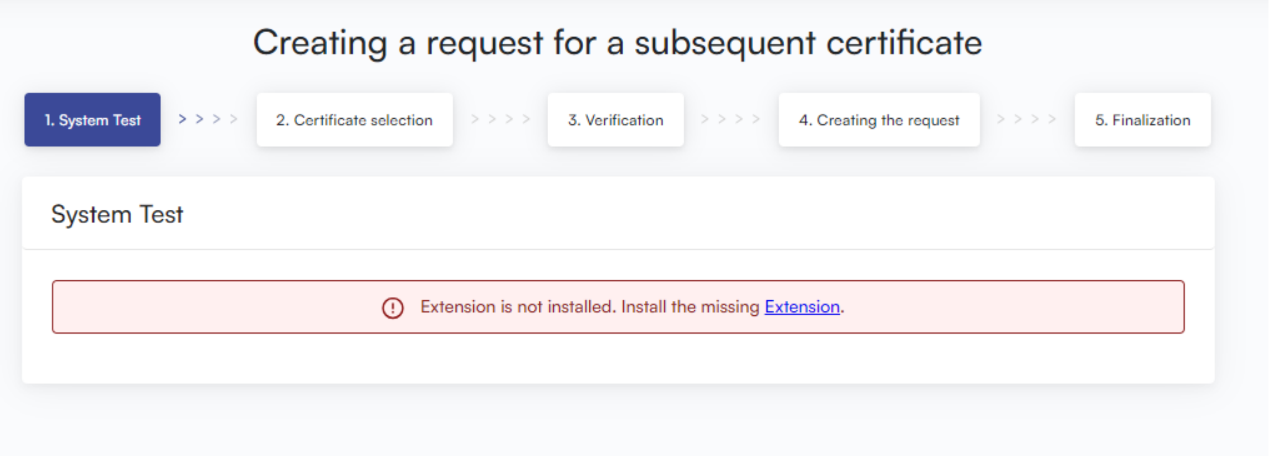
In case of absence of the component and extension **I.CA PKIService Host** , an error message appears, see below.



Creating a request for a subsequent certificate

System Test

ⓘ Component I.CA PKIServiceHost not installed on your computer. Install the missing component I.CA PKIServiceHost



Creating a request for a subsequent certificate

System Test

ⓘ Extension is not installed. Install the missing Extension.

Click on the highlighted **PKIServiceHost** and **Extension I.CA** to download and then install the necessary components to generate the request. After successful installation, restart your browser. The page will test the computer, if no problems are detected, you will proceed to the actual creation of the subsequent certificate request.

If an error occurs during the check, you cannot continue the creation a subsequent certificate request. First, you need to fix the error that prevents you from creating a certificate request. The meaning of error messages is given in the following chapters.

3.1.1. Unsupported Operating System

To generate the request, you must use one of the operating systems listed in Chapter 2.

3.1.2. Unsupported Internet Browser

To generate the request, you must use one of the browser versions listed in Chapter 2.

3.1.3. JavaScript Support

The certificate request generation pages require JavaScript scripting support. If this check fails, it most likely means that scripting support is disabled in your browser settings. Enable JavaScript scripting support in your browser.

3.1.4. I.CA PKIServiceHost

The site requires the I.CA PKIService Host component installed for its functionality. Make sure you have it installed. If you do not have the component installed on your computer, use the highlighted name I.CA PKIService Host to download it, after installation you need to restart the browser.

3.1.5. Extensions (add-on) I.CA PKIServiceHost

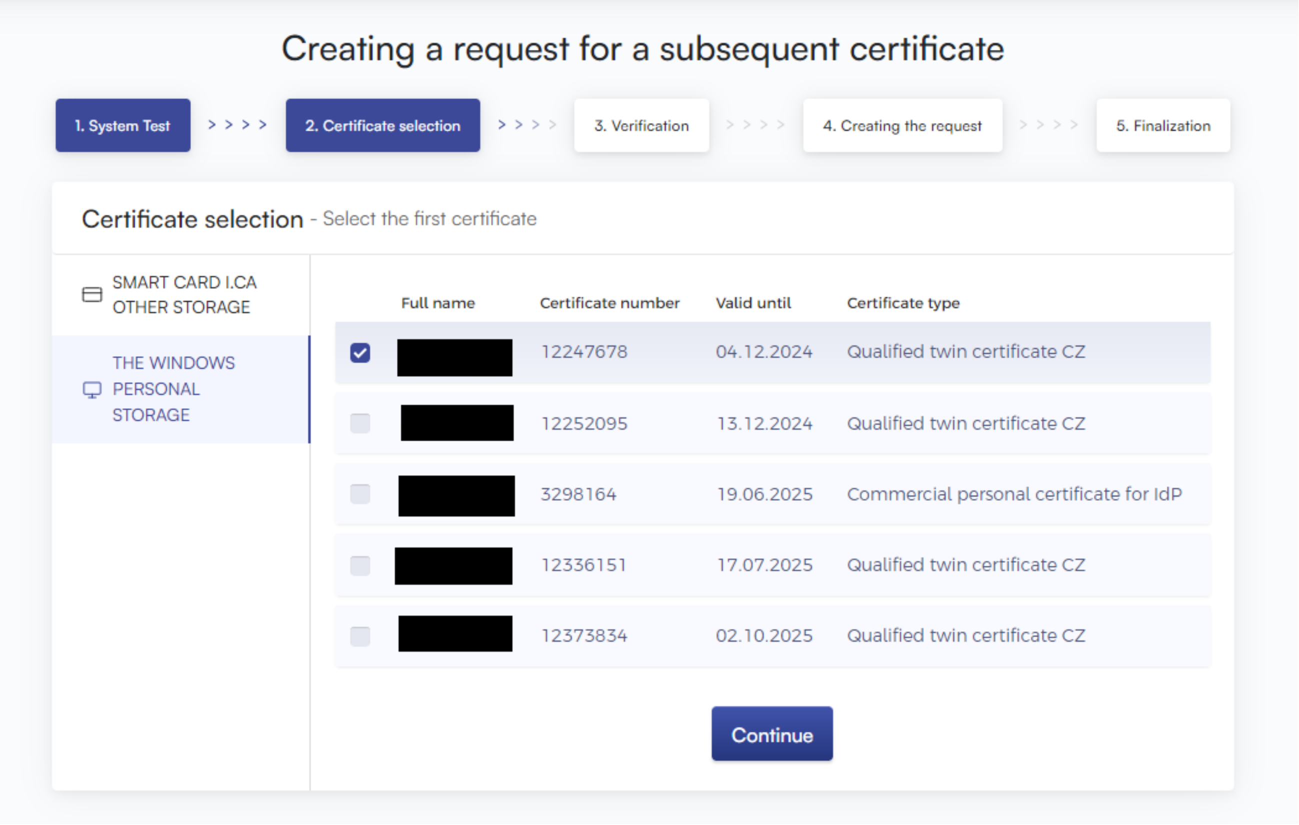
Next, you need to have the extension installed and enabled in your browser. By clicking on the highlighted name Extension, the browser will redirect you to the settings, where you can find and install the extension, after installation you need to refresh the page.

3.1.6. Storage of cookies

For the request generation site to work properly, it is necessary that your browser allows the site to store cookies. If you have cookies disabled, enable them.

3.2. Selecting a certificate to create a subsequent certificate request

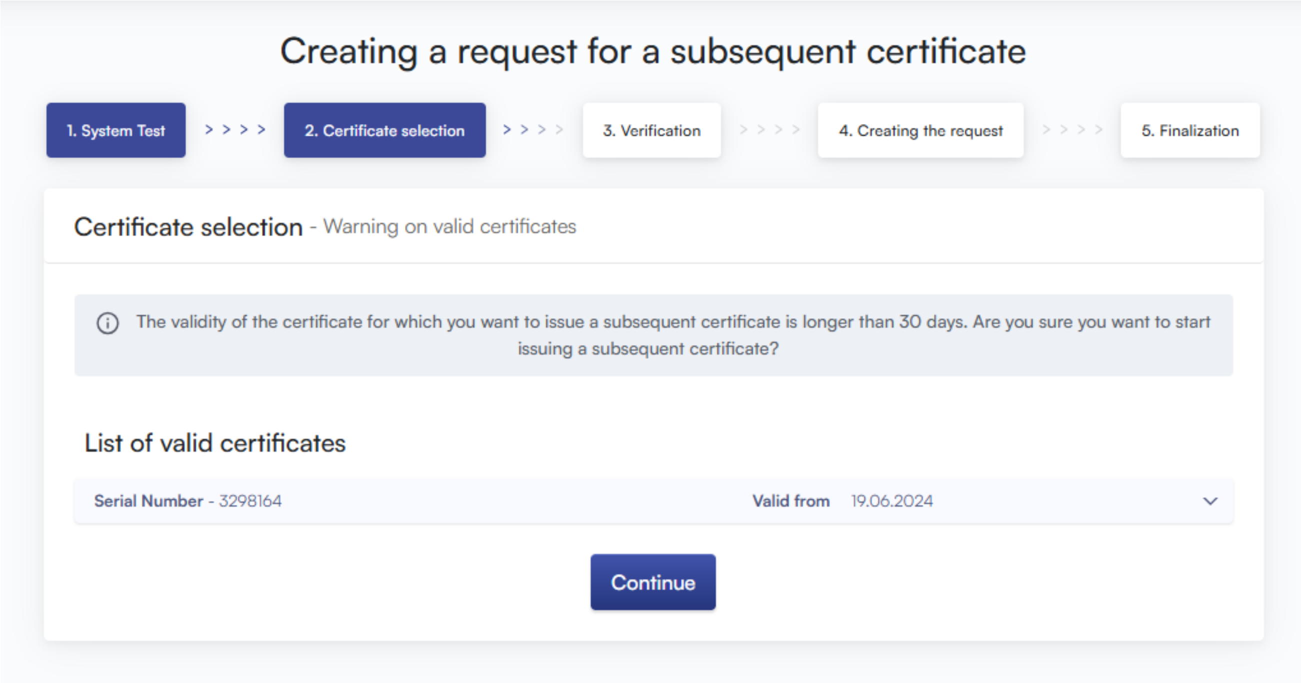
If the scan process went smoothly, the page will display a form where you select a valid certificate to issue a follow-up certificate for.



Creating a request for a subsequent certificate

Certificate selection - Select the first certificate

	Full name	Certificate number	Valid until	Certificate type
☑	[redacted]	12247678	04.12.2024	Qualified twin certificate CZ
☐	[redacted]	12252095	13.12.2024	Qualified twin certificate CZ
☐	[redacted]	3298164	19.06.2025	Commercial personal certificate for IdP
☐	[redacted]	12336151	17.07.2025	Qualified twin certificate CZ
☐	[redacted]	12373834	02.10.2025	Qualified twin certificate CZ



Creating a request for a subsequent certificate

Certificate selection - Warning on valid certificates

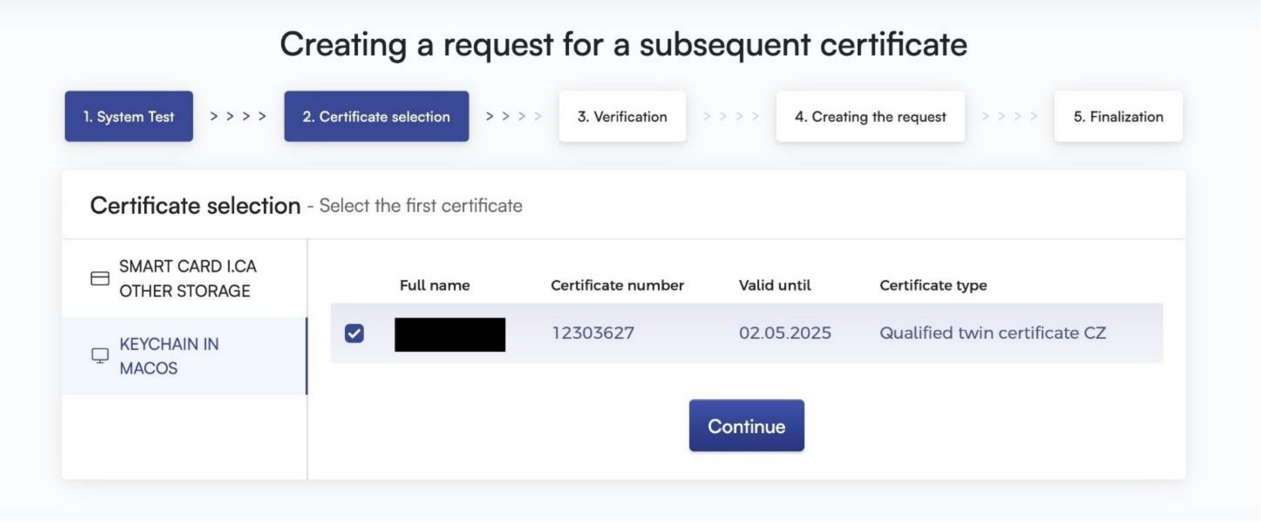
ⓘ The validity of the certificate for which you want to issue a subsequent certificate is longer than 30 days. Are you sure you want to start issuing a subsequent certificate?

List of valid certificates

Serial Number - 3298164 Valid from 19.06.2024

If your certificate is stored in the Windows store, leave the **Windows Personal certificate store** selected. If your certificate is on a I.CA smart card, select **Smart Card I.CA (Other storage).**

For a certificate stored in the MacOS repository**,** select **Keychain Access in MACOS**.



Creating a request for a subsequent certificate

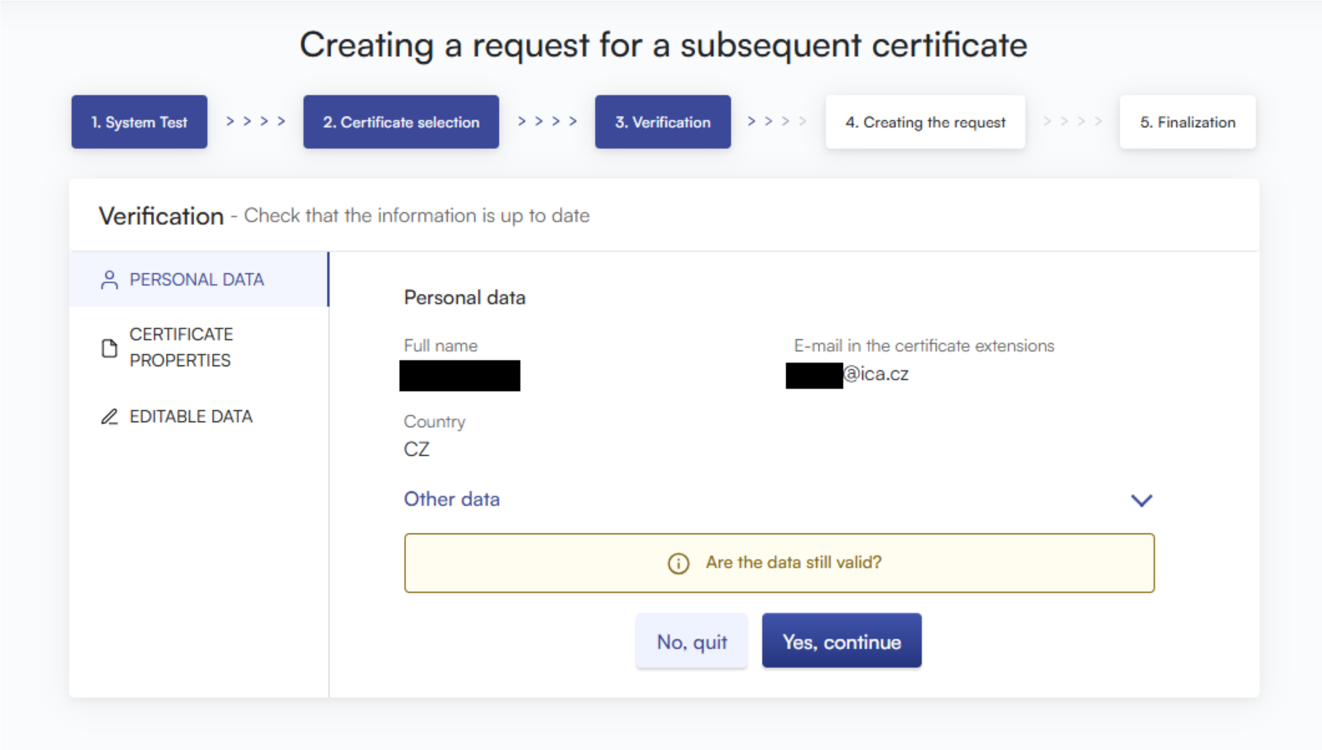
Certificate selection - Select the first certificate

	Full name	Certificate number	Valid until	Certificate type
☑	[redacted]	12303627	02.05.2025	Qualified twin certificate CZ

Depending on your previous choice, a list of certificates for which a subsequent certificate can be issued is offered. If you selected **Smart Card I.CA**, you must have a reader connected and a smart card inserted.
A subsequent certificate can only be issued for such certificates that have not yet expired and that are not placed on the CRL (list of revoked certificates)!

If you receive an email notifying you that your certificate is about to expire, the email contains a URL where you can create a follow-up certificate request. The URL also includes the serial number of the certificate.
If you enter this URL into your browser, the certificate is selected automatically.

3.3. Data control



Creating a request for a subsequent certificate

Verification - Check that the information is up to date

Personal data

Full name
[redacted]

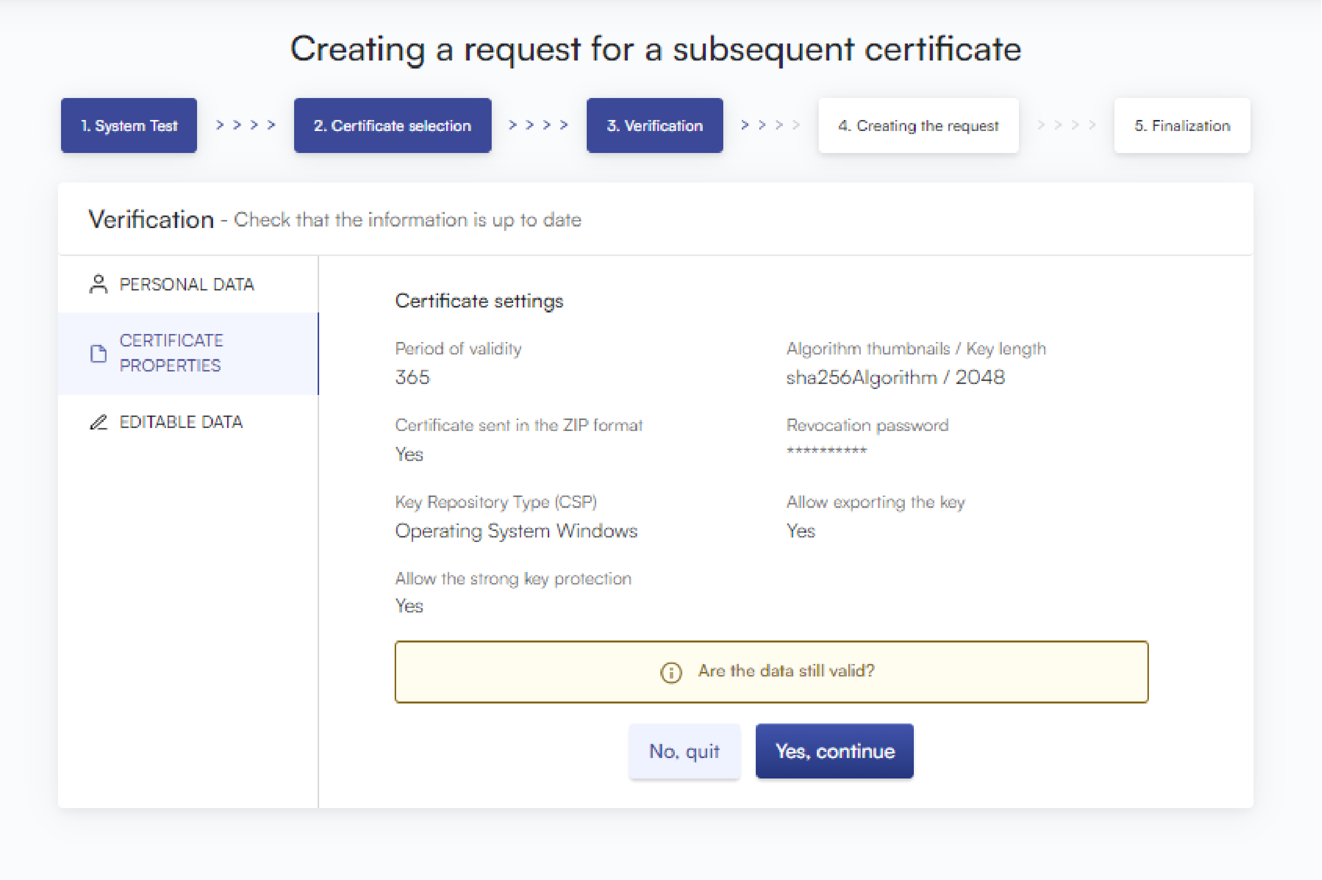
E-mail in the certificate extensions
[redacted]@ica.cz

Country
CZ

Other data

Are the data still valid?

If the items in the certificate are up-to-date, click "**YES, continue"** to start generating the certificate request. For more detailed information, expand the **"Other information"** option.



Creating a request for a subsequent certificate

Verification - Check that the information is up to date

Certificate settings

Period of validity
365

Algorithm thumbnails / Key length
sha256Algorithm / 2048

Certificate sent in the ZIP format
Yes

Revocation password
****

Key Repository Type (CSP)
Operating System Windows

Allow exporting the key
Yes

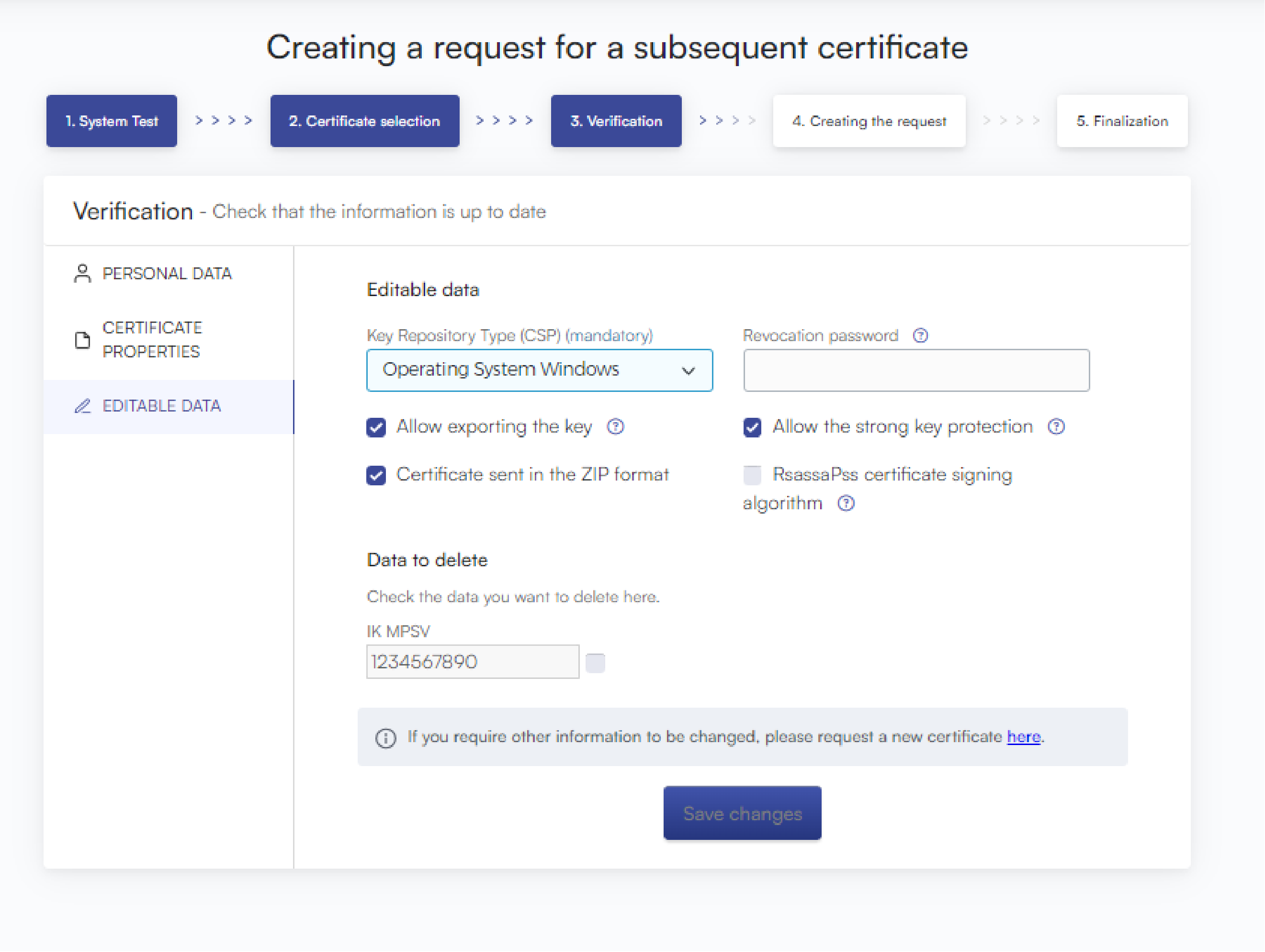
Allow the strong key protection
Yes

Are the data still valid?

The **"CERTIFICATE PROPERTIES"** section displays the settings of the existing certificate, such as the certificate serial number or storage type.
If any item in the certificate has changed, continue by clicking on **"Editable data"** and continue in the manual to point 3.4 Addition and change of certain data.

3.4. Addition and amendment of some data

In the **"EDITABLE DATA" section**, you can influence some of the data that will be contained in your subsequent certificate.



Creating a request for a subsequent certificate

1. System Test > > > > 2. Certificate selection > > > > 3. Verification > > > > 4. Creating the request > > > > 5. Finalization

Verification - Check that the information is up to date

Editable data

Key Repository Type (CSP) (mandatory): Operating System Windows

Revocation password:

☑ Allow exporting the key

☑ Allow the strong key protection

☑ Certificate sent in the ZIP format

□ RsassaPss certificate signing algorithm

Data to delete

Check the data you want to delete here.

IK MPSV: 1234567890 □

If you require other information to be changed, please request a new certificate here.

Password for invalidation:

If the private key is compromised, the data changes (name change, address...) or there are other reasons why the certificate should not be used anymore, the certificate must be revoked.

The certificate can be revoked via the web interface. When a certificate is revoked, you will be prompted to enter the password for revocation.

If you do not enter a password, the password set for the existing certificate will be used as the certificate revocation password.

If you choose to enter a different password, it must be between 4 and 32 characters long. Only uppercase and lowercase letters without diacritics and numbers are allowed.

Key Store Type (CSP):

For **Key Store Type (CSP),** choose the cryptographic module (CSP) that will generate your private key. All CSPs shown here are installed on your computer.

To export the private key:

If the key storage type (CSP) you choose supports private key export, you are offered the option to enable private key export. This option allows you to export the certificate including the private key. This will allow you to transfer the private key between storages. In such a case, key management requires increased caution due to the higher risk of theft/misuse.

Strong private key protection:

If the key storage type (CSP) you choose supports strong private key protection, you are given the option to enable strong private key protection. Each time you use your key, you will be notified that your key is in use.

You then have the option to choose between:
Medium - you will always be notified by an informative message
Strong - You will be required to enter a password before each use

To edit an email:

If an e-mail address is included in an existing certificate, you have the option to remove it from the subsequent certificate. In most cases, a change is not possible, in this case please ask for a new certificate with corrected data.

Unauthorized certificate content

In some rare cases, your certificate may contain extended key uses and subject alternative names that may not already be present in the certificate according to the certification policy.
In this case, you will see a warning and you must remove these extensions before continuing.

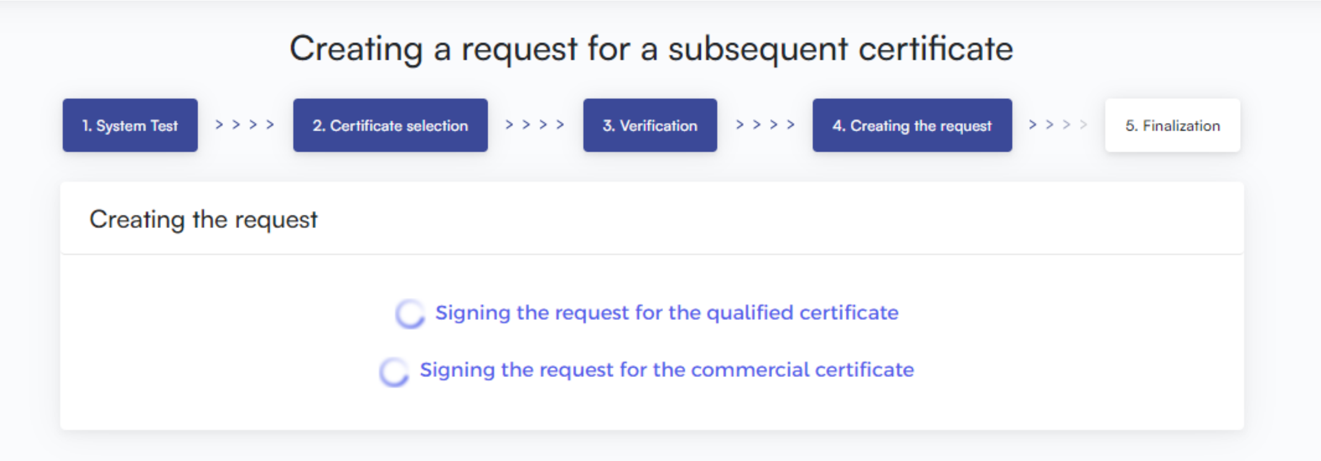
3.5. Generate a certificate request

The following steps are slightly different for each type of key store (CSP):

3.5.1. Smart Card I.CA - Microsoft Smart Card Key Storage\ I.CA SecureStore PKCS11# Library

If you choose Microsoft Smart Card Key Storage as the key storage type when filling out the requestor information, the procedure for generating the request is as follows:

First, you will see the following dialog. At this point, your private key is generated. Creating a private key can take several tens of seconds.



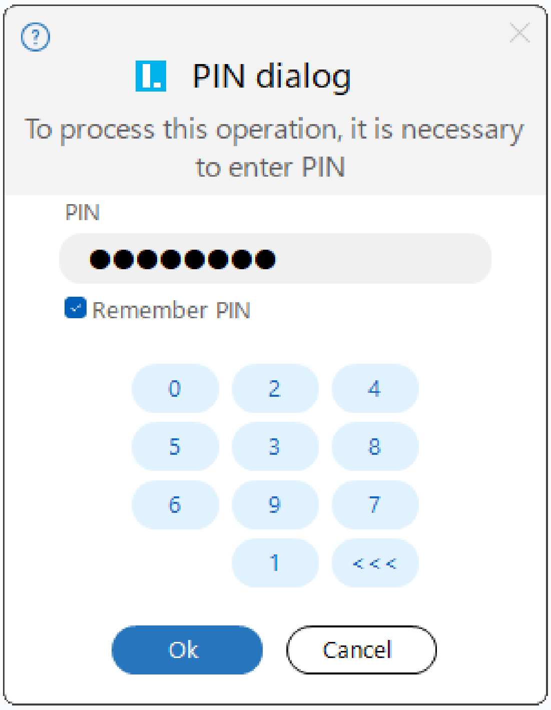
Creating a request for a subsequent certificate

Creating the request

Signing the request for the qualified certificate

Signing the request for the commercial certificate

After the private key is created, you are asked to enter your card PIN.



PIN dialog

To process this operation, it is necessary to enter PIN

PIN

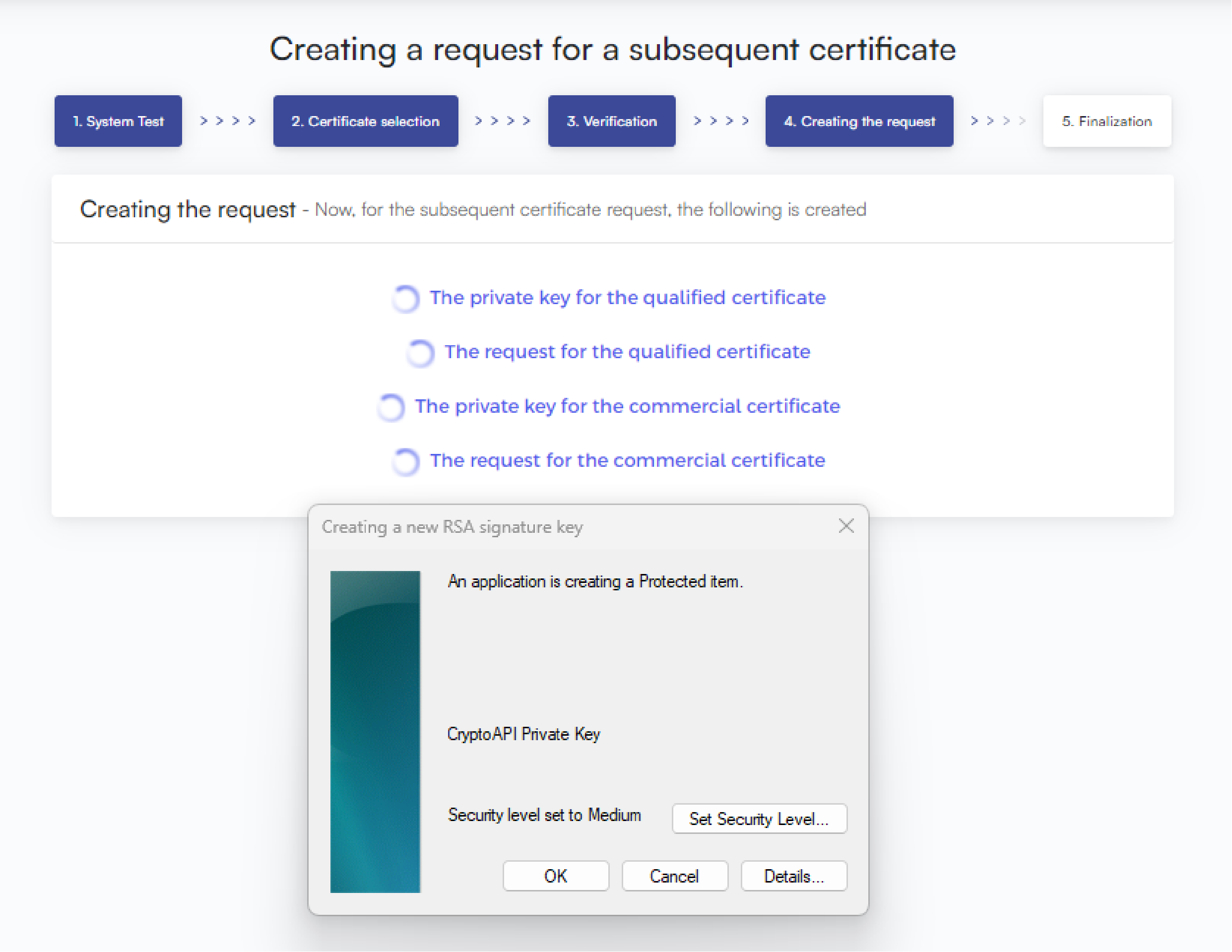
●●●●●●●●●

☑ Remember PIN

For a smart card, I.CA can also use the Microsoft Base Smart Card Crypto Provider storage type.
In the case of creating a request on MacOS, the selected storage is I.CA SecureStore PKCS11# Library.

3.5.2. Microsoft Enhanced RSA and AES Cryptographic Provider (Windows Operating System) with Strong Private Key Protection

If you choose Microsoft Enhanced RSA and
AES Cryptographic Provider (or Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) and check the Enable strong key protection option, the procedure for generating the request is as follows:



Creating a request for a subsequent certificate

Creating the request - Now, for the subsequent certificate request, the following is created

The private key for the qualified certificate

The request for the qualified certificate

The private key for the commercial certificate

The request for the commercial certificate

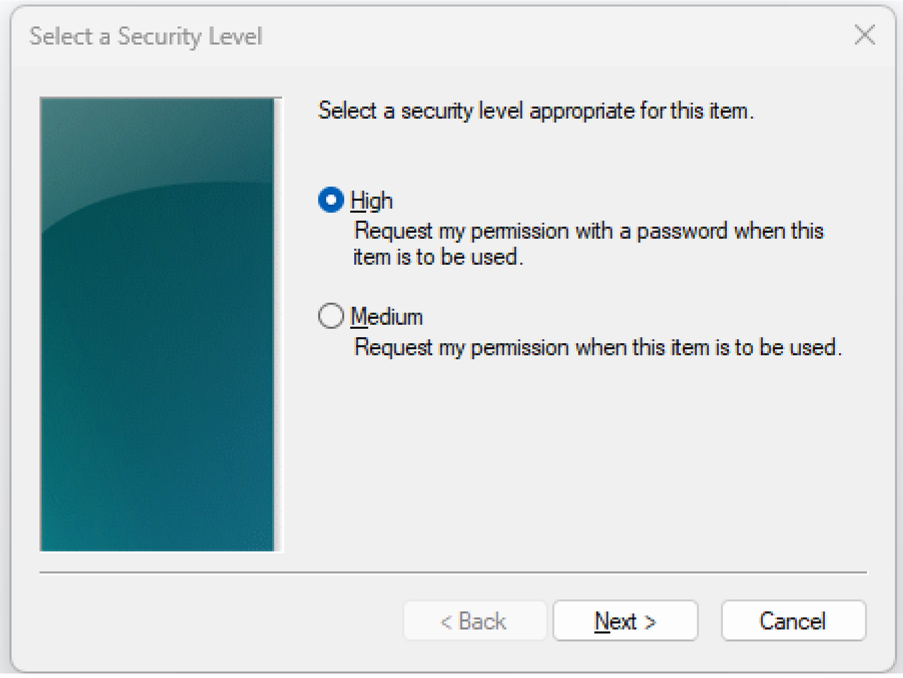
Creating a new RSA signature key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

If you click Set **Security Level**, you will be able to change the security level.



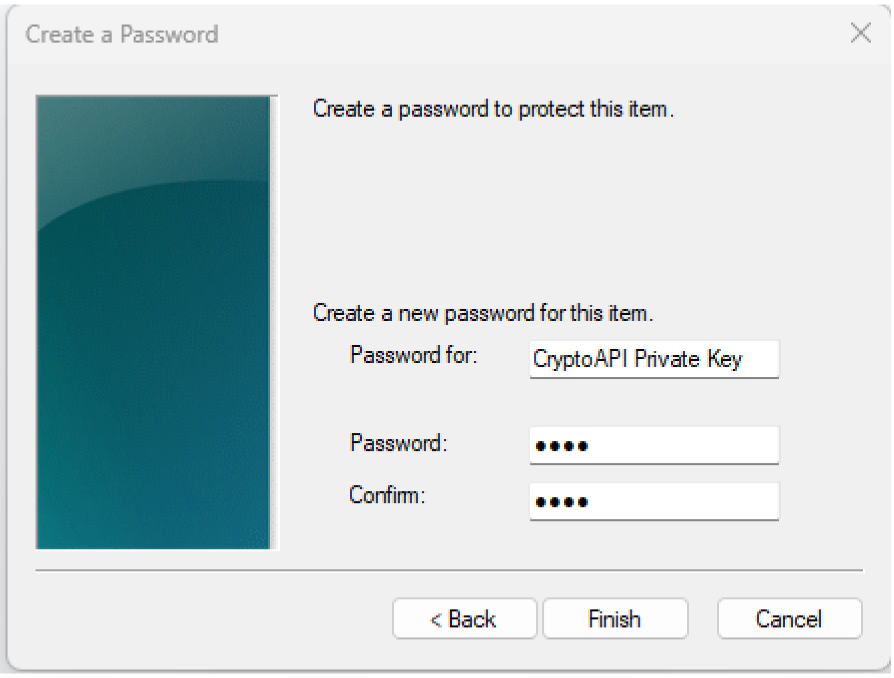
Select a Security Level

Select a security level appropriate for this item.

● High
Request my permission with a password when this item is to be used.

○ Medium
Request my permission when this item is to be used.

If you choose **High** security, you will be prompted to enter your password. (You will need to enter this password every time you use your issued certificate).



Create a Password

Create a password to protect this item.

Create a new password for this item.

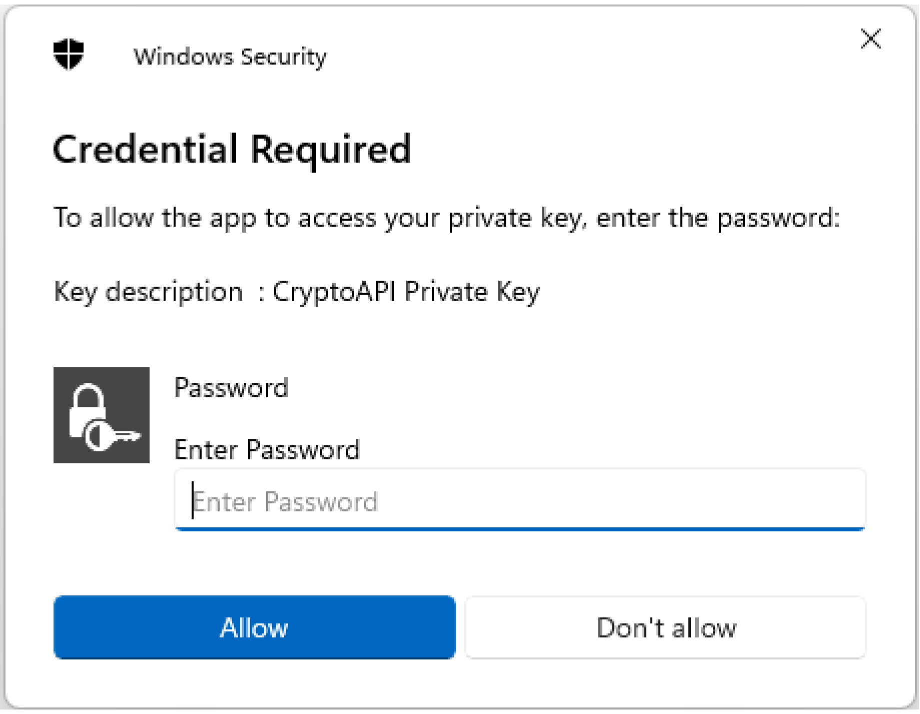
Password for: CryptoAPI Private Key

Password: ●●●●

Confirm: ●●●●

When you click **Finish**, the security level changes. Now click OK.

In the next dialog box, click **Allow to grant** permissions. If you have selected **a high** security level, you must also enter a password.



Windows Security

Credential Required

To allow the app to access your private key, enter the password:

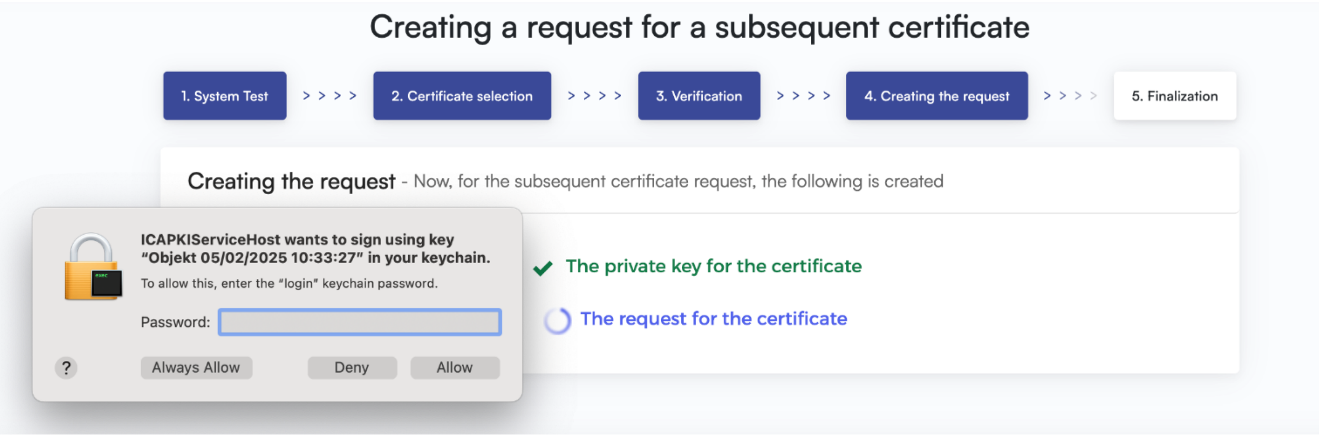
Key description : CryptoAPI Private Key

Password

Enter Password

3.5.3. MacOS File-Based Keychain

If we are making a request to MacOS for a certificate that is stored on the computer, the selected storage type will be MacOS File-Based Keychain. When generating a key for the keychain, you will be required to enter the keychain password. If you do not want a password to be required every time a certificate is used, you can choose to allow always.



Creating a request for a subsequent certificate

Creating the request - Now, for the subsequent certificate request, the following is created

✓ The private key for the certificate

The request for the certificate

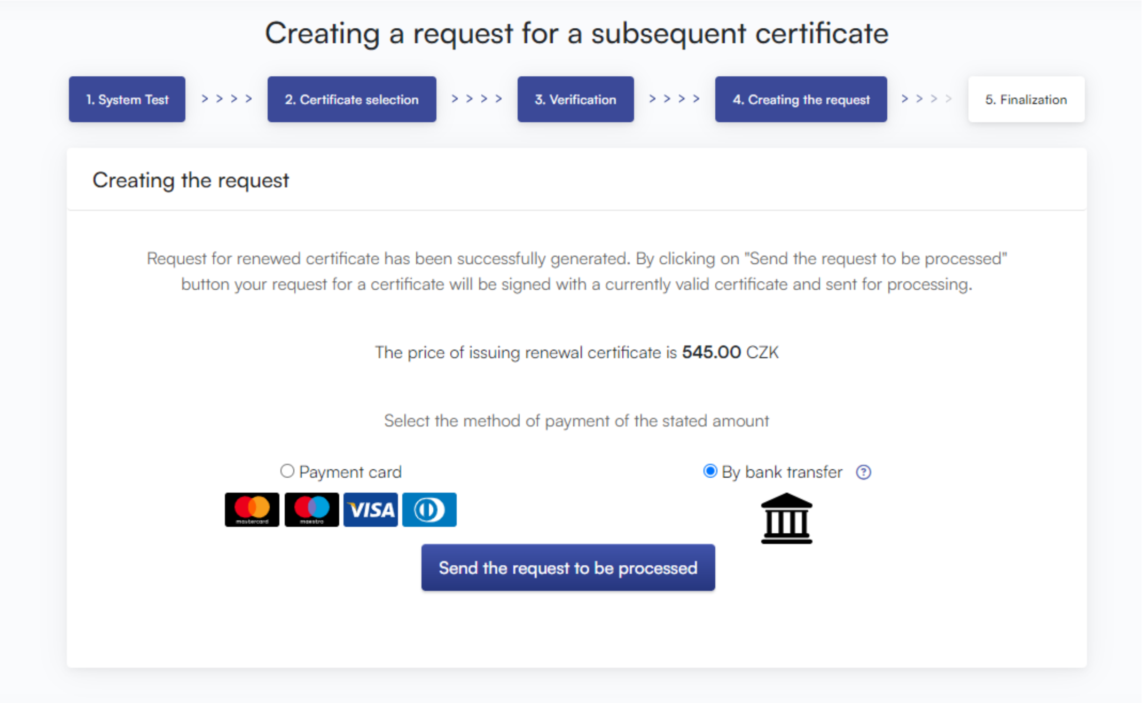
ICAPKIServiceHost wants to sign using key "Objekt 05/02/2025 10:33:27" in your keychain.

To allow this, enter the "login" keychain password.

Password:

3.6. Signing and sending a follow-up certificate request

After clicking on the **Send request for processing button**, a dialog will appear containing your request for a subsequent certificate. This request must be signed with the certificate for which you are requesting a subsequent certificate.



Creating a request for a subsequent certificate

Creating the request

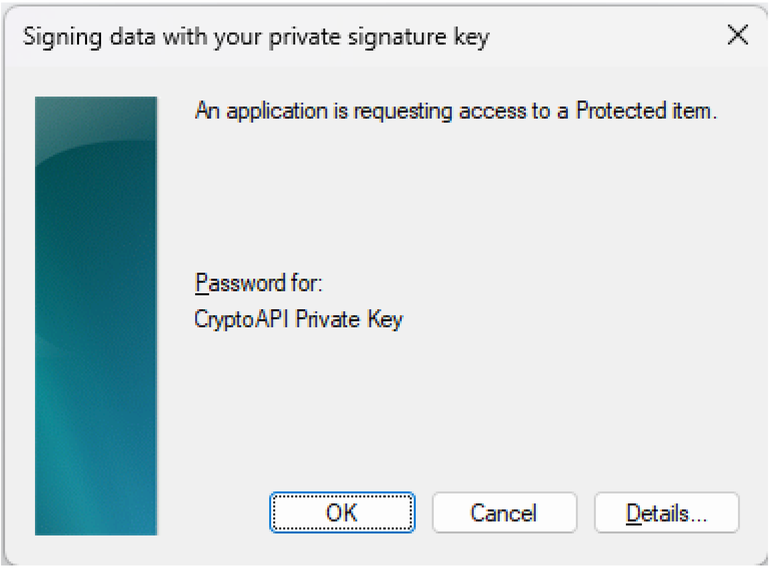
Request for renewed certificate has been successfully generated. By clicking on "Send the request to be processed" button your request for a certificate will be signed with a currently valid certificate and sent for processing.

The price of issuing renewal certificate is **545.00** CZK

Select the method of payment of the stated amount

○ Payment card ● By bank transfer

The application must be signed by clicking on the **"OK" button**.
If the application is generated on a smart card, it is necessary to sign by entering **the PIN code** for the smart card. In case you are applying for a subsequent TWINS certificate, it is necessary to sign both the application for a subsequent qualified certificate and the application for a commercial certificate.

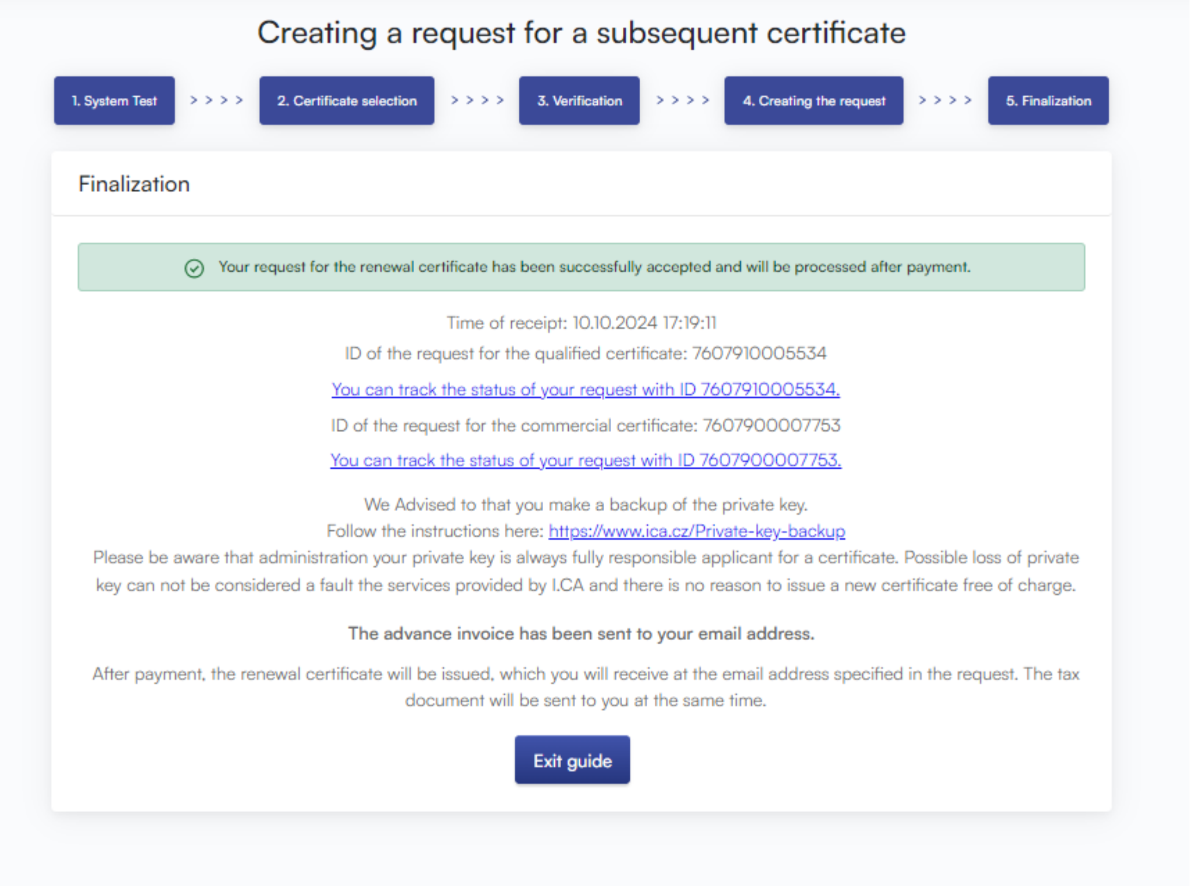


Signing data with your private signature key

An application is requesting access to a Protected item.

Password for:
CryptoAPI Private Key

After successfully submitting your application, you will see the following page:



Creating a request for a subsequent certificate

Finalization

✓ Your request for the renewal certificate has been successfully accepted and will be processed after payment.

Time of receipt: 10.10.2024 17:19:11

ID of the request for the qualified certificate: 7607910005534

You can track the status of your request with ID 7607910005534.

ID of the request for the commercial certificate: 7607900007753

You can track the status of your request with ID 7607900007753.

We Advised to that you make a backup of the private key.
Follow the instructions here: https://www.ica.cz/Private-key-backup
Please be aware that administration your private key is always fully responsible applicant for a certificate. Possible loss of private key can not be considered a fault the services provided by I.CA and there is no reason to issue a new certificate free of charge.

The advance invoice has been sent to your email address.

After payment, the renewal certificate will be issued, which you will receive at the email address specified in the request. The tax document will be sent to you at the same time.

4. Troubleshooting

In case of an error during the application generation process, you will be informed by an error message.

Some errors may be of a more serious technical nature. They may be related to the condition of your computer's hardware or software. In this case, we recommend contacting technical support I.CA.