

Generating a request for a subsequent certificate User Guide

Contents

Contents	1
1. Introduction.....	2
2. Software requirements	2
3. The Process of Generating a Request for a Subsequent Certificate	2
1.1. Software Test.....	3
1.2. Selecting a Certificate to Create a Subsequent Certificate Request	5
1.3. Recapitulation.....	6
1.4. Additions and Changes to Certain Data.....	7
1.5. Generating a Certificate Request	9
1.6. Signing and sending a request for a subsequent certificate	12
4. Problem Solving.....	14

1. Introduction

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

2. Software requirements

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

2.1. installed and running operating system:

- Windows 7 ServicePack 1
- Windows 8.1 (April 2014 update)
- Windows 10
- Windows 11

2.2. The 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 when generating a request for a smart card)

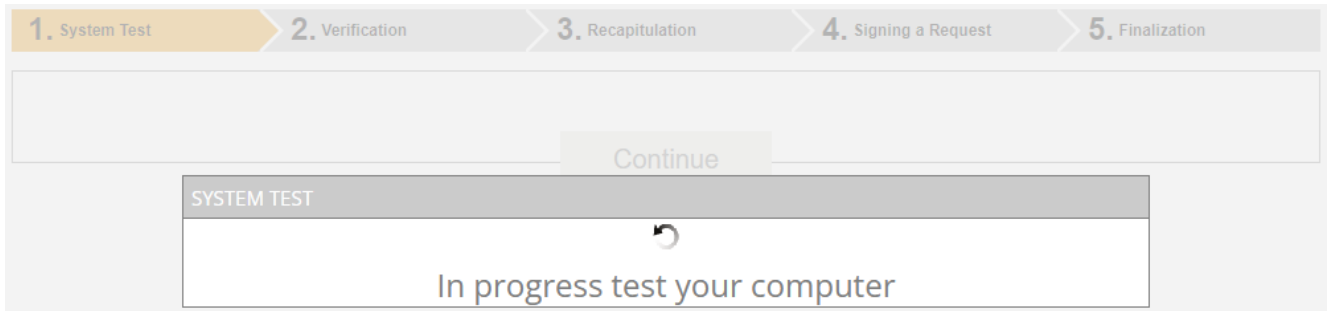
3. The Process of Generating a Request for a Subsequent Certificate

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

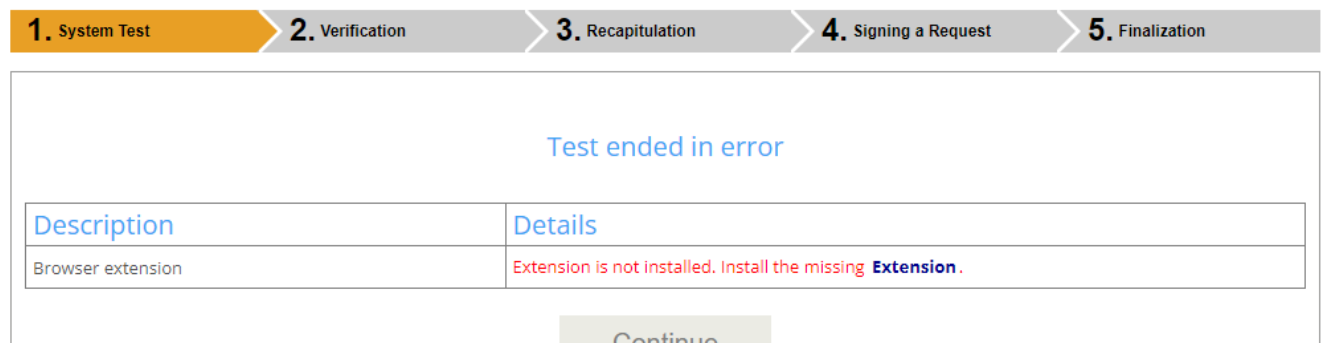
1. **System Test**
2. **Verification**
3. **Recapitulation**
4. **Signing a Request**
5. **Finalization**

1.1. Software Test

To make it easier to check if your computer is ready to generate a request, a check page is displayed when you start generating the request to verify that key software components are present.



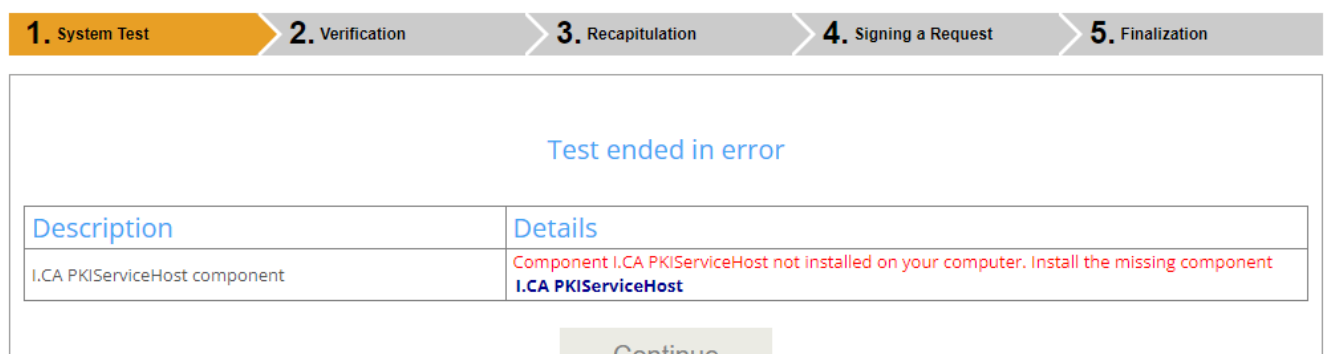
In the absence of the component and the **I.CA PKIService Host** extension, an error message appears, see below.



Description	Details
Browser extension	Extension is not installed. Install the missing Extension .

[Continue](#)

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00



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

[Continue](#)

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

Click on the highlighted "**I.CA PKIServiceHost**" and "**Extension**" to install the necessary components to generate the request on the PC. After successful installation, restart the browser.

If you have a certificate stored on your smart card, you may receive an error for the **SecureStore** application you download and install.

The page will test the computer, if no problems are detected, it will automatically proceed to the actual creation of the subsequent certificate request.

If an error occurs during the check, you cannot proceed with the creation of the subsequent certificate request. First, you must resolve the error that prevents the certificate request from being created. The meaning of the error messages is given in the following sections.

3.1.1. Unsupported Operating System

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

3.1.2. Unsupported Internet Browser

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

3.1.3. Javascript Support

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

3.1.4. I.CA PKIService Host

The site requires the **I.CA PKIService Host** component installed for its functionality. Make sure you have it installed. If you don't have the component installed on your computer, use the highlighted name I.CA PKIService Host to download it, after installation it is necessary to restart the browser.

3.1.5. Extension (Add-on) I.CA PKIService Host

It is also necessary to have a browser extension installed and enabled. Clicking on the highlighted name of the Extension will redirect you to the settings where you can find and install the extension, after installation it is necessary to refresh the page.

3.1.6. Storing Cookies

In order for the request generation pages to work properly, your browser must allow the site to store cookies. If you have disabled the storage of cookies, please enable it.

1.2. Selecting a Certificate to Create a Subsequent Certificate Request

If the checking process is error-free, the page displays a form where you select a valid certificate for which you want to issue a subsequent certificate.

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Choose where is your certificate stored (registered)

The personal certificate store in Windows Other storage (eg I.CA smart card)

Select the certificate for which you want to issue a renewal certificate.

[2023-05-26] I.CA Qualified 2 CA/RSA 02/2016

Continue

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

If your certificate is stored in the **Windows certificate storage**, leave "**The personal certificate store in windows**" selected. If your certificate is on an I.CA smart card, select "**Other storage**" (e.g. I.CA smart card).

Depending on your previous selection, you are presented with a list of certificates for which a subsequent certificate can be issued. If you have selected **Other storage**, you must have a card reader connected and a smart card inserted.

A subsequent certificate can only be issued for certificates that have not expired and are not placed on the CRL!

If you receive an email notifying you that your certificate is about to expire, the email contains a URL where you can create a request for a subsequent certificate. The URL also includes the serial number of the certificate.

If you enter this URL in your browser, the certificate is selected automatically.

1.3. Recapitulation

1. System Test > 2. Verification > **3. Recapitulation** > 4. Signing a Request > 5. Finalization

Data overview	
Certificate sent in the ZIP format	Yes
Period of validity	365
Key Repository Type (CSP)	Operating System Windows
Algorithm thumbnails / Key length	sha256Algorithm / 2048
Allow exporting the key	Yes
Allow the strong key protection	Yes
Extended usage setting key of qualified certificate	id-kp-emailProtection
Extended usage setting key of commercial certificate	id-kp-clientAuth / id-kp-emailProtection
certificate settings	
Full name	Full name
Given name	Given name
Surname	Surname
Organization	Organization
E-mail in the certificate extensions	E-mail in the certificate extensions
IK MPSV	IK MPSV
Country	Country
SN ICA	SN ICA
SN ICA	SN ICA
The data are still valid?	
<input type="button" value="YES, the data are valid"/> <input type="button" value="NO, the data have changed"/>	

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

If the entries in the certificate are up to date, continue by clicking "**YES, the data are valid**" to start generating the certificate request.

If an item in the certificate has changed, continue by clicking "**NO, the data have changed**" and proceed to section 3.4 Adding and changing some data.

1.4. Additions and Changes to Certain Data

In this step, you can modify some of the information that your subsequent certificate will contain.

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Revocation password ?

Key Repository Type (CSP)

Certificate sent in the ZIP format Allow exporting the key ? Allow the strong key protection ?

id-kp-clientAuth ? id-kp-emailProtection ? ms-SmartCardLogon ?

Edit the e-mail Delete Change

TWIN qualified

IK MPSV ? Delete Change

For issuance of a certificate with correct data, please contact **I.CA's technical support**.

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

Password for invalidation:

If during the use of the certificate the private key is compromised, data is changed (change of name, residence...) or there are other reasons why the certificate should no longer be used, it is necessary to invalidate the certificate.

The certificate can be invalidated via the web interface. When you invalidate the certificate, you will be prompted to enter a password for invalidation.

If you do not enter a password, the password set for the current certificate will be used as the password to invalidate the certificate.

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

Key Storage Type (CSP):

For **Key Storage Type (CSP)**, select the Cryptographic Service Provider (CSP) module from the menu that generates your private key. All CSPs displayed here are installed on your computer.

Send certificate in ZIP format

If you want to send the public part of the new certificates in ZIP format, leave the box checked.

Private Key Export:

If your chosen key store type (CSP) supports private key exporting, you are offered the option to enable private key exporting. This option allows you to export the certificate including the private key. This will allow you to transfer the private key between storages. Key management requires extra care in this case due to the higher risk of key theft/misuse.

Strong private key protection:

If your chosen key store type (CSP) supports strong private key protection, you are offered the option to enable strong private key protection. Before each use of your key, you will be notified that your key is being used.

You then have the option to choose between:

Medium - you will only ever be notified by an informative message

Strong - you will be required to enter a password before each use

Editing your email:

If an email is included in an existing certificate, you have the option to remove it from subsequent certificates here. In this case please request a new certificate with corrected data.

After pressing the "**Continue**" button, you will see a recap of the data and the settings for the subsequent certificate.

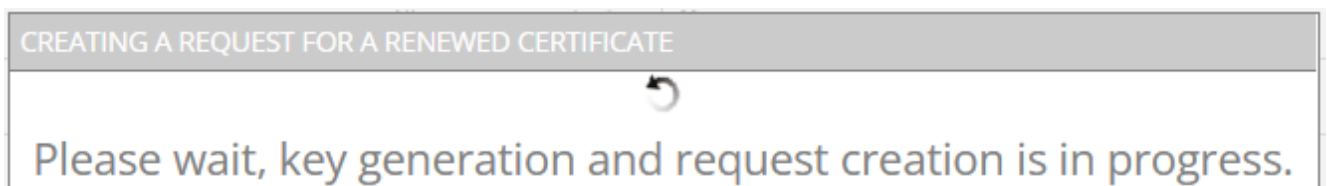
1.5. Generating a Certificate Request

The following procedure varies slightly for each type of key storage system (CSP):

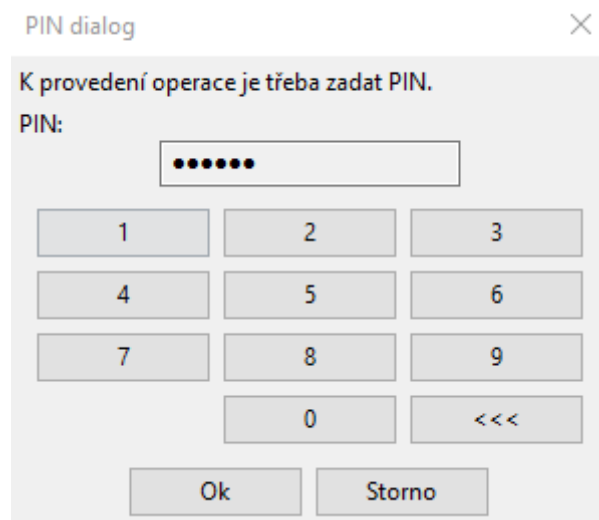
3.5.1. SecureStoreCSP – Smart Card I.CA

If you select SecureStoreCSP as the key storage type when filling in the requestor information, the procedure for generating the request is as follows:

You will first see the following dialog. At this point, your private key is generated. It may take a few tens of seconds to generate the private key.

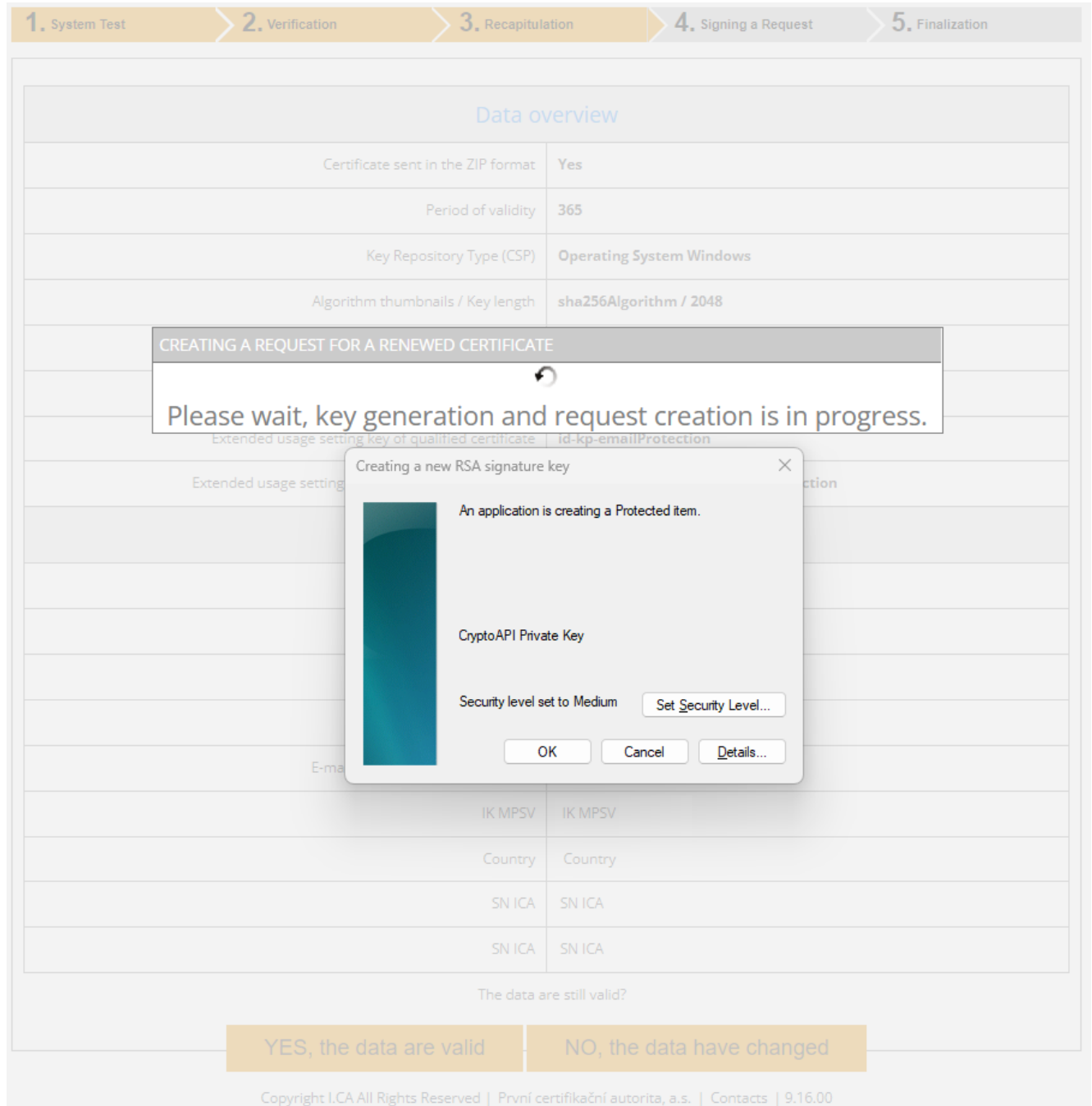


Once the private key is created, you are prompted to enter the PIN for your card.



3.5.2. Microsoft Enhanced RSA and AES Cryptographic Provider With Strong Private Key Protection

If you select 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 application generation process is as follows:



The screenshot shows a multi-step process with the following steps: 1. System Test, 2. Verification, 3. Recapitulation, 4. Signing a Request, and 5. Finalization. The current step is 4. Signing a Request.

Data overview

Certificate sent in the ZIP format	Yes
Period of validity	365
Key Repository Type (CSP)	Operating System Windows
Algorithm thumbnails / Key length	sha256Algorithm / 2048

CREATING A REQUEST FOR A RENEWED CERTIFICATE

Please wait, key generation and request creation is in progress.

Creating a new RSA signature key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium [Set Security Level...](#)

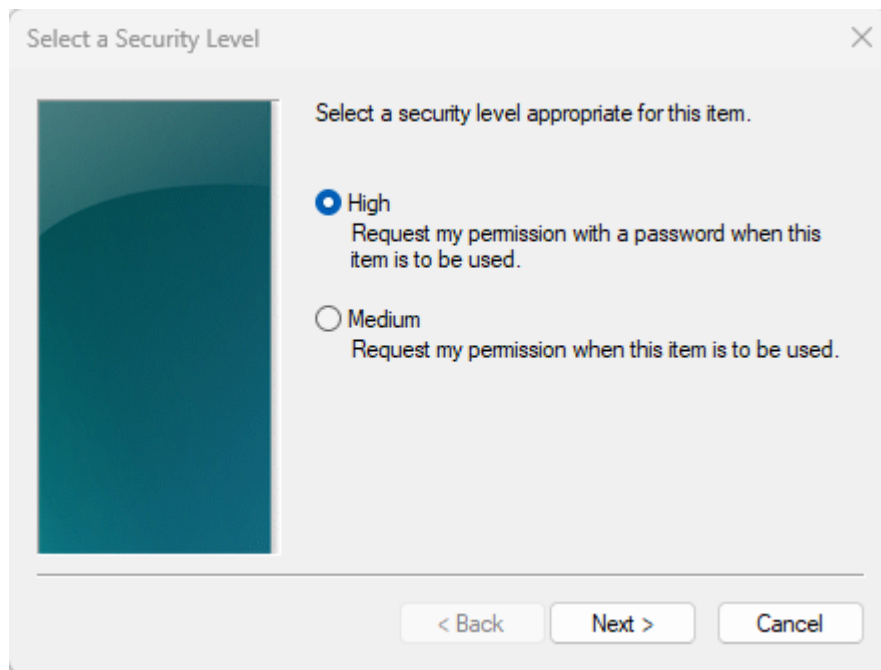
OK Cancel [Details...](#)

The data are still valid?

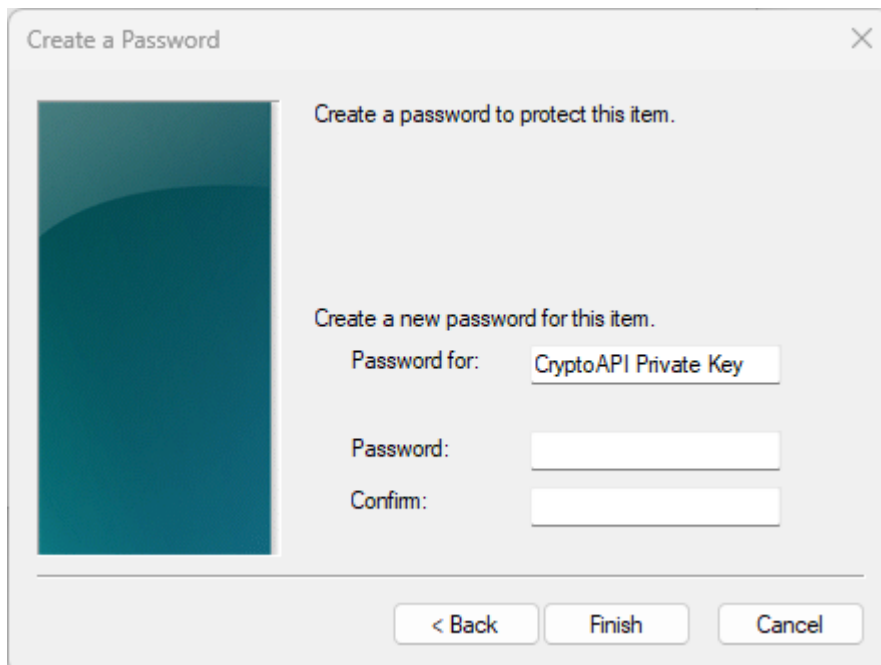
YES, the data are valid NO, the data have changed

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

If you click on "**Select a Security Level**", you will be able to change the security level.

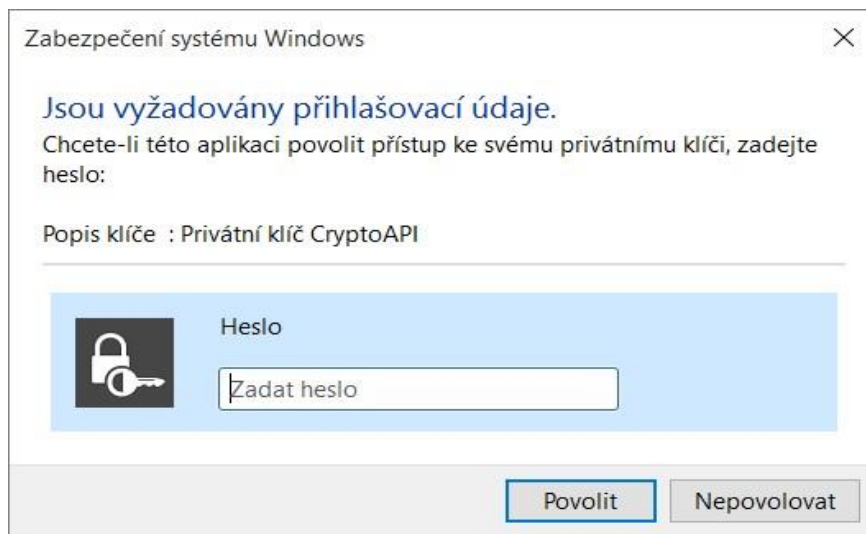


If you select the "**High**" security level, you will be prompted for a password. (You will need to enter this password whenever you use your issued certificate).



Clicking the "**Finish**" button will change the security level. Now click "**OK**".

In the next dialog, grant permissions by clicking **"Allow"**. If you have chosen a **"high"** security level, you must also enter a password.



1.6. Signing and sending a request for a subsequent certificate

If no error occurred while generating the request, the page will display the generated request in PKCS10 format.

When you click the **"Submit Request for Processing"** button, a dialog will appear containing your request for a follow-up certificate. This request must be signed with the certificate for which you are requesting a subsequent.

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Created request for certificate

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.

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.

Save on local disk or external storage

The price of issuing renewal certificate is 725.00 CZK

Choose the payment method

By bank transfer (you will receive an advance invoice by e-mail)

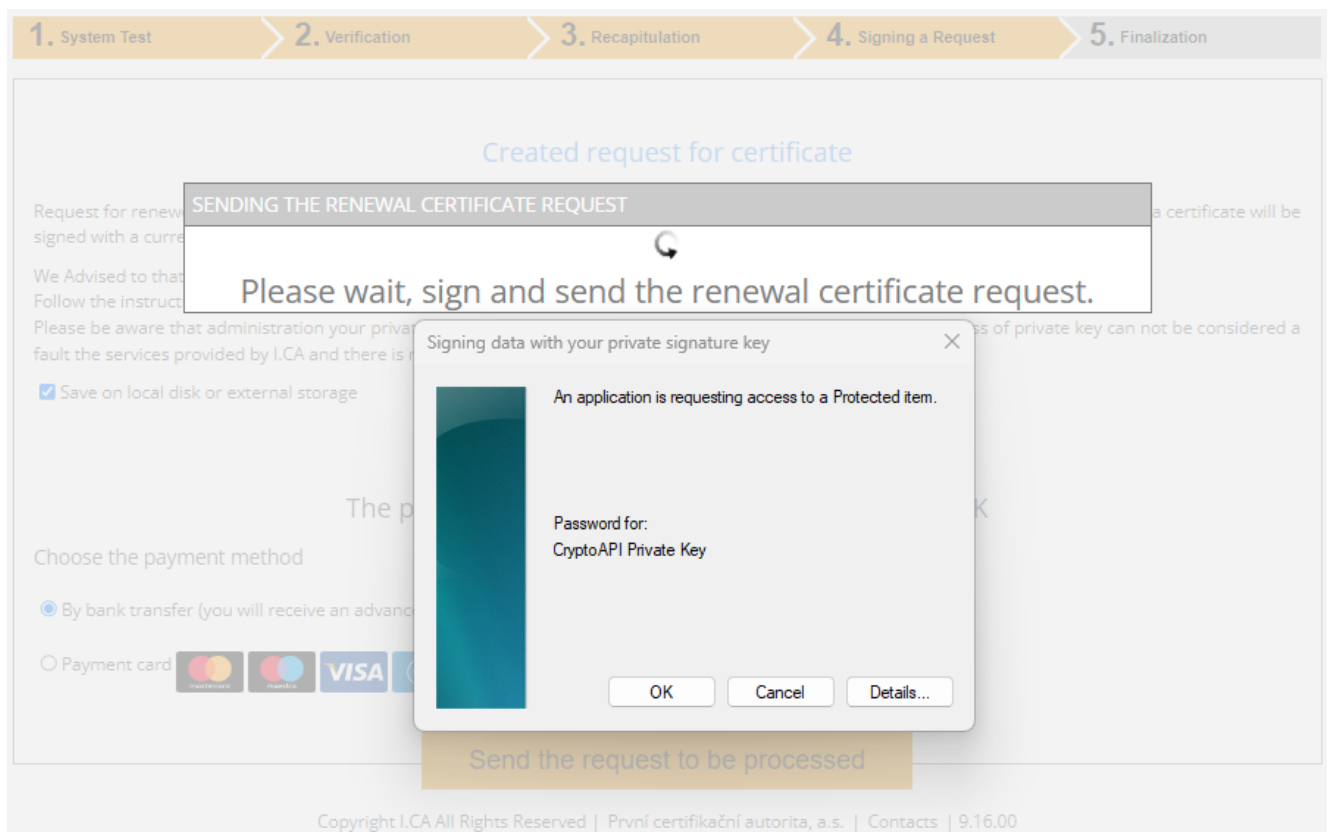
Payment card 

Send the request to be processed

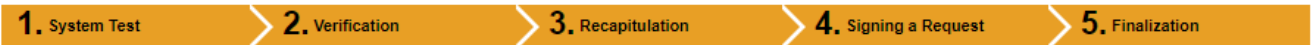
The application needs to be signed by clicking on the "OK" button

If the request is generated to a smart card, it needs to be signed by entering the **PIN code** of the smart card.

If you are requesting a TWINS subsequent certificate, you must sign both the subsequent qualified certificate request and the commercial certificate request.



If your application is successful, you will see the following page:



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

ID request for the qualified certificate: 5708611016745

You can track the status of your application with ID 5708611016745.

ID request for the commercial certificate: 5708600766504

You can track the status of your application with ID 5708600766504.

Time of receipt: 27.04.2023 09:33:38

If the download does not start automatically, click the file to download [here](#)

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 application. The tax document will be sent to you at the same time.

[Exit guide](#)

Copyright I.C.A. All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9:16:00

4. Problem Solving

If an error occurs 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 state of your computer's hardware or software. In this case, we recommend contacting [I.C.A. | Contacts \(ica.cz\)](#)