Generate an initial certificate request

Content

1. Introduction 2
2. Software requirements 2
3. Initial certificate request generation process 2
   1.1 Certificate selection 3
   1.2 Test system 4
   1.3 Entering data 6
   1.4 Verification 7
   1.5 Saving your request 9
   1.6 Completion 9

1. Introduction

This document serves as a guide to how to proceed when generating an initial 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 installed and running

- 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 PKIServiceHost component and extension** installed

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

2.6. **eObčanka – Card Manager** (only in case of generating an application for an ID card)

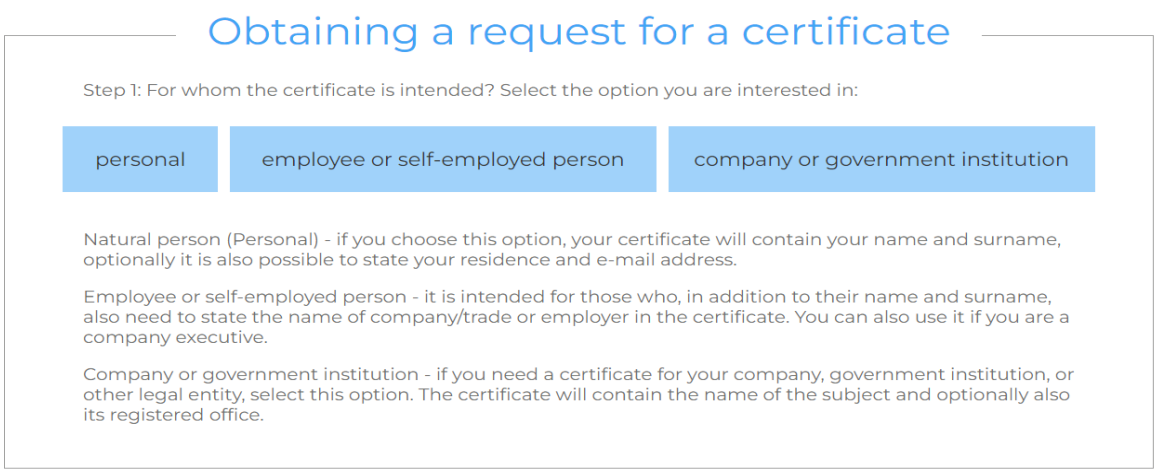
3. Initial certificate request generation process

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

1. **Test system**
2. **Entering data**
3. **Verification**
4. **Saving your request**
5. **Completion**

1.1 Certificate selection

Choose to create an application by selecting the type of certificate here: https://www.ica.cz/certificate or choose a certificate here: https://www.ica.cz/products.

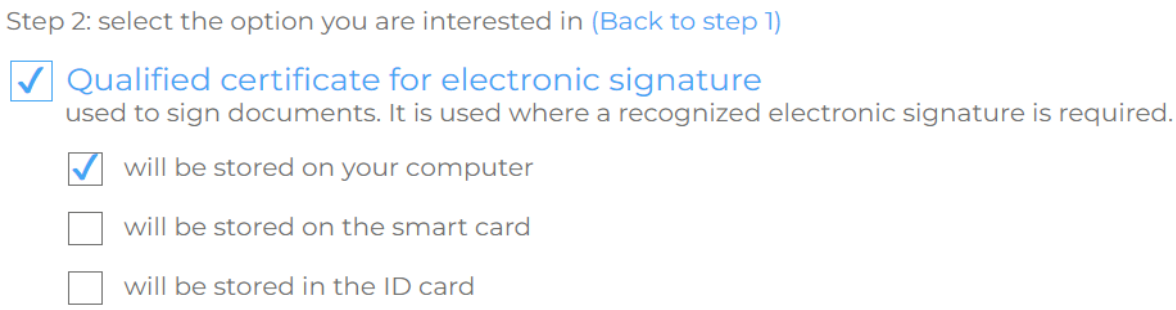


- personal – only the name and surname of the applicant **will be stated in the certificate**. Not organizations.
- employee or self-employed person – the certificate will state **the name, surname and also the organization** for which the applicant is acting.
- company or government institution – this is primarily an electronic seal or a commercial technology certificate. The certificate does not state the name and surname of the applicant. Only **the organization is listed in the certificate**.

In the next step, select the certificate you are requesting (e.g. Qualified Certificate for Electronic Signature) and check the "will be stored on your computer" box. Then, press the **"Get" button at the bottom**.

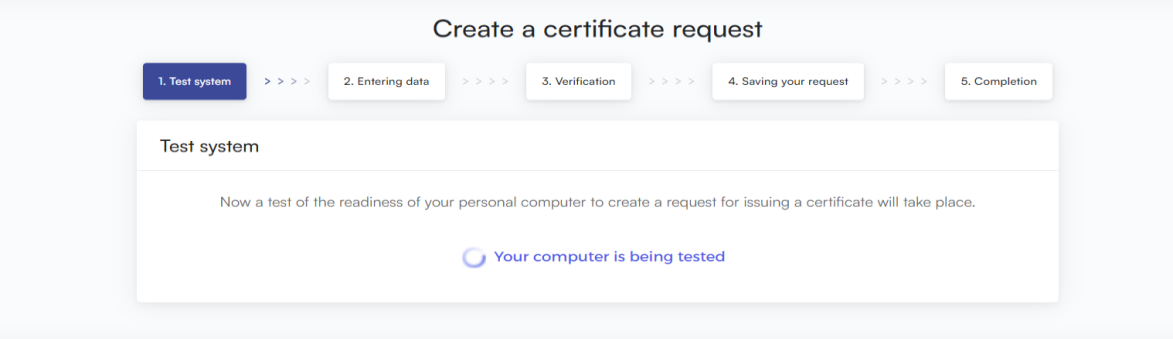
If you are requesting a certificate stored **on a smart card**, you must have the smart card connected to your computer. If you do not have a smart card, you can visit a branch of the registration authority that offers hardware, where they will then create an application and issue a certificate for you.

If you are applying for a certificate **stored on your ID card**, it is necessary to have the eObčanka – Card Manager application installed and your ID card connected to a computer that has set up a PIN and QPIN.

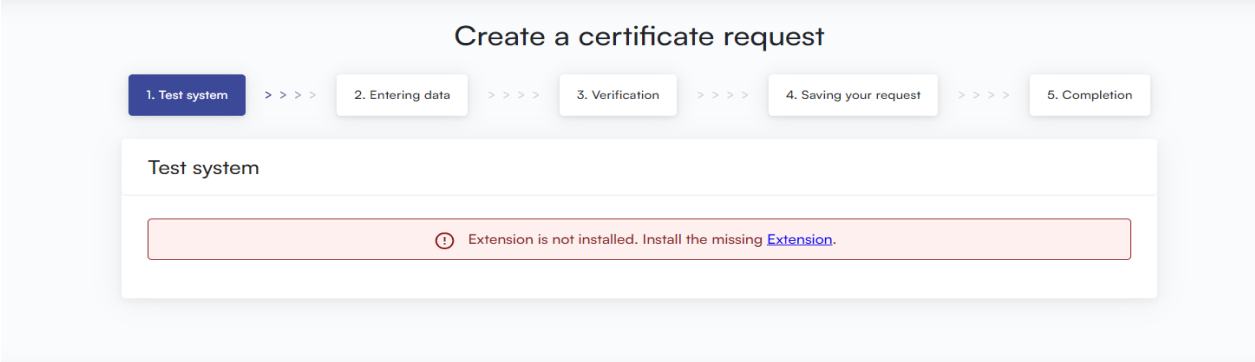


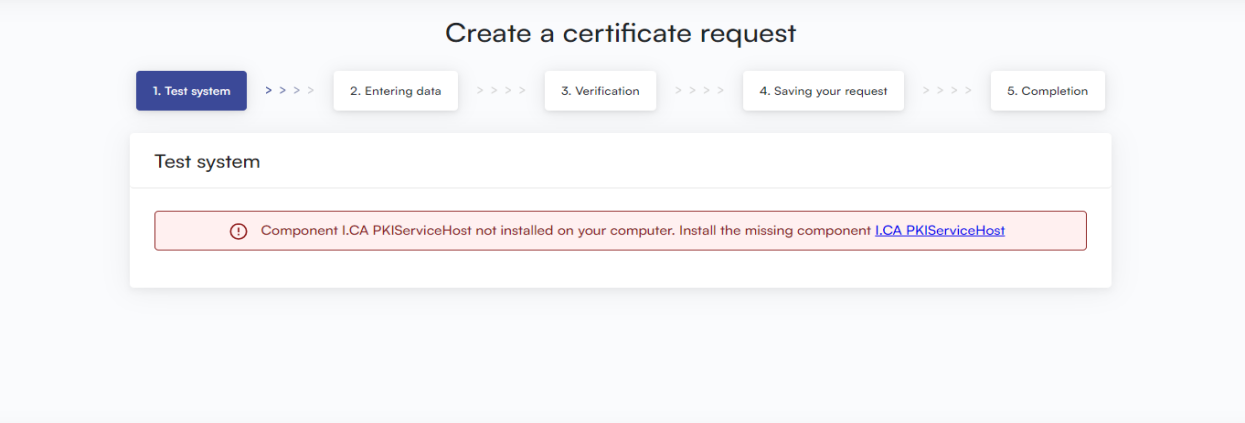
1.2 Test system

To facilitate the check of your computer's readiness to generate a request, a control page is displayed when you start generating a request to verify the presence of key software components.



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





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

The page will scan the computer, if no problems are detected, you will automatically proceed to the creation of the certificate request.

If an error occurs during the check, you cannot continue to create 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 PKIervice Guest**

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 PKIService Host**

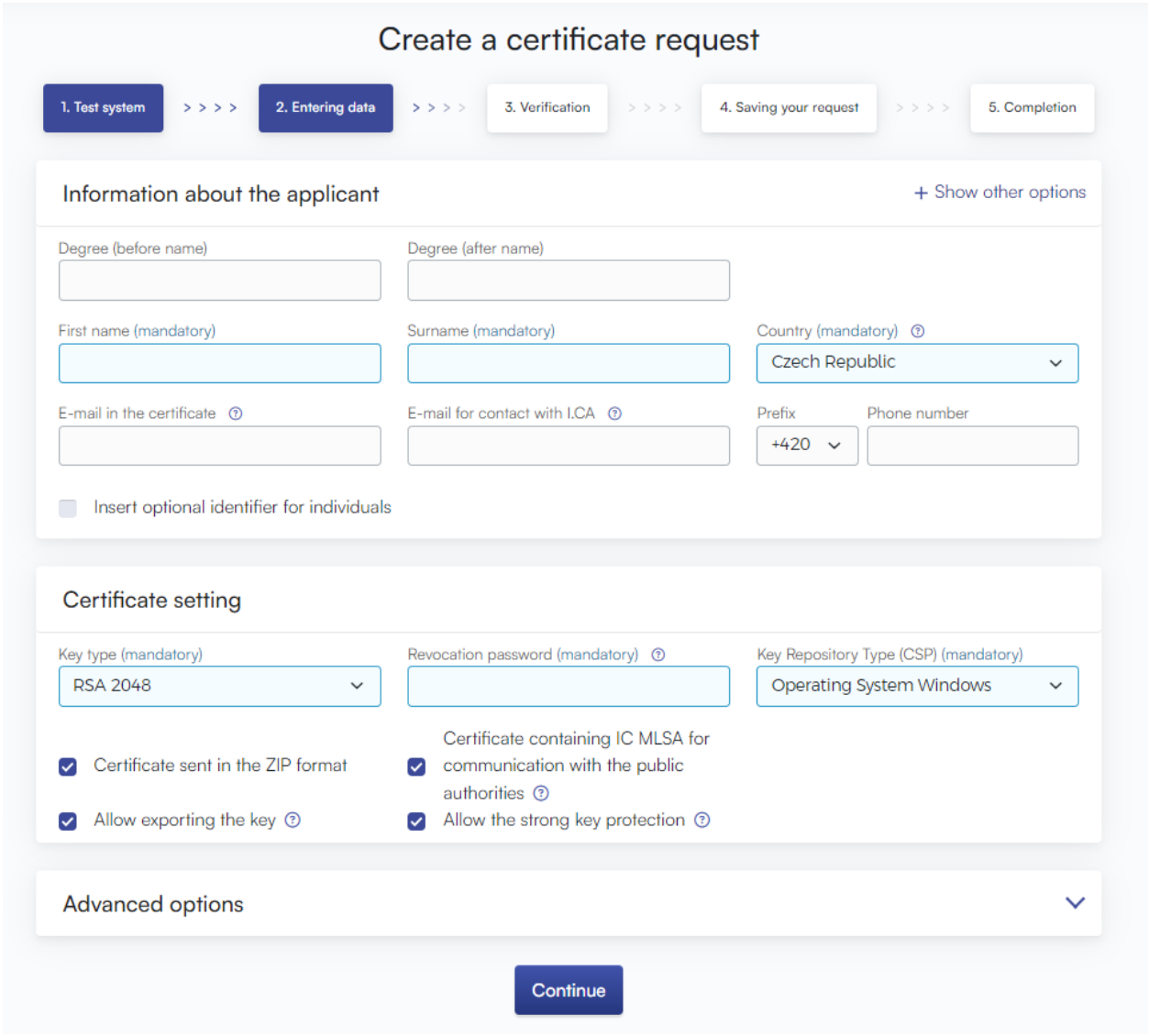
Next, you need to have the extension installed and enabled in your browser. By clicking on the highlighted name Extension, the browser will redirect you to the settings, where you can find and install the extension, after installation you need to refresh the page.

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.

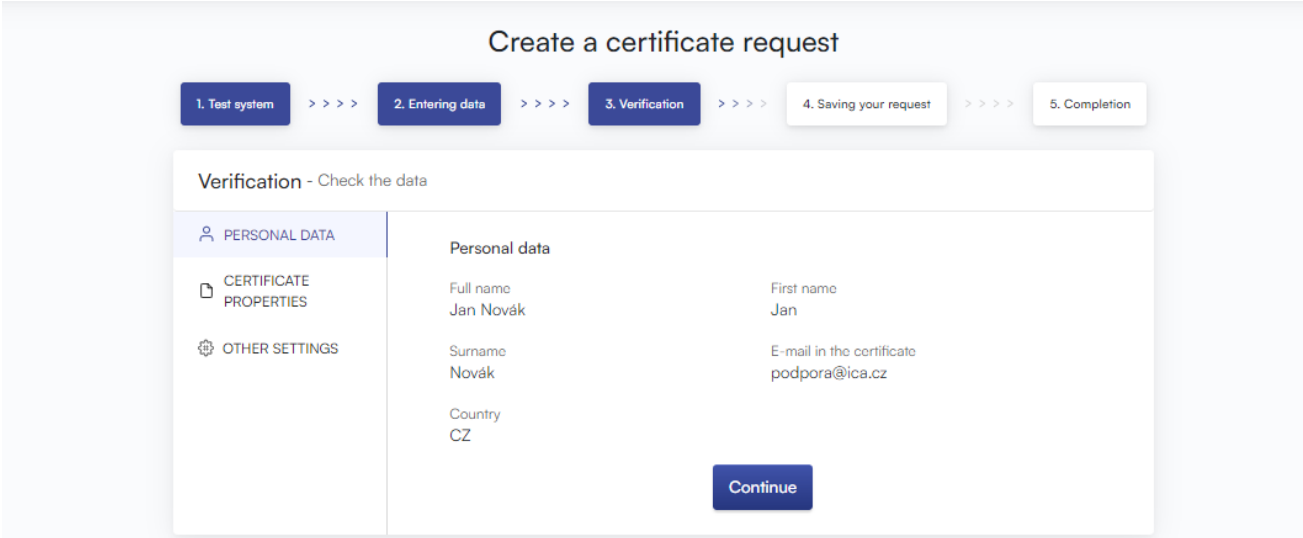
1.3 Entering data

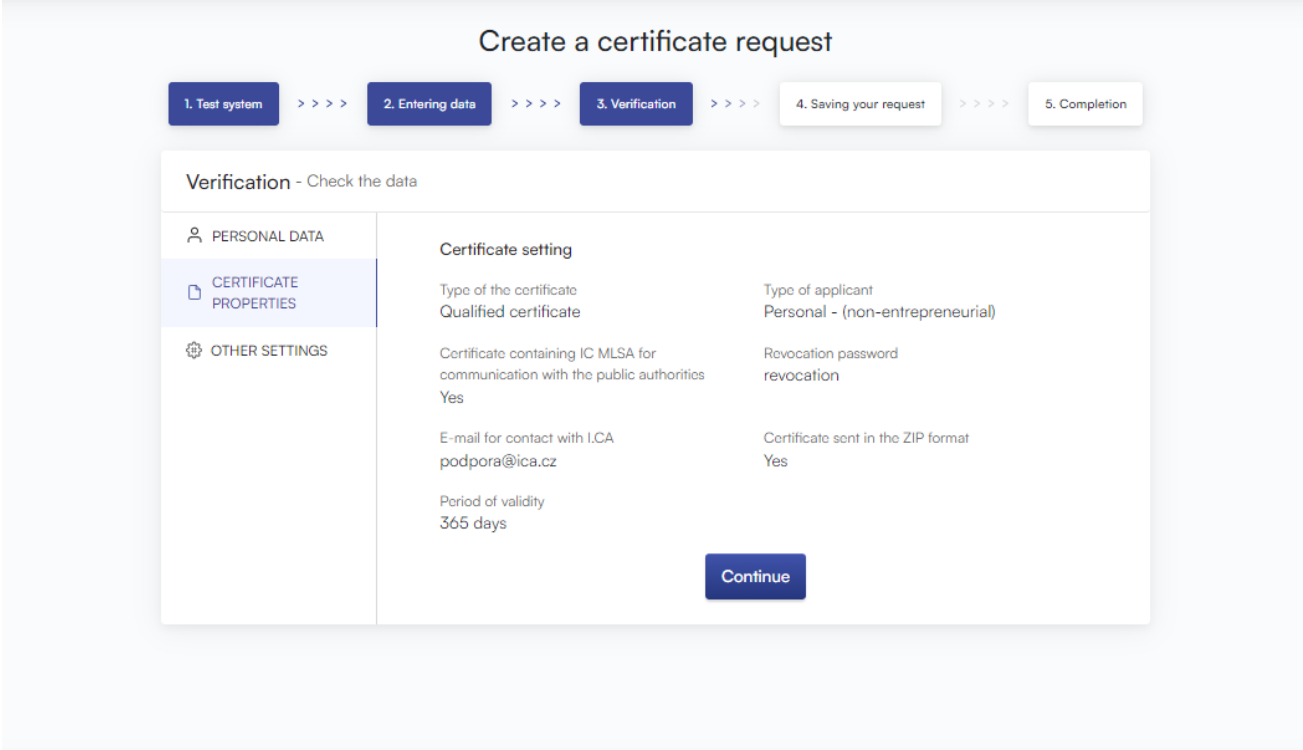
Here you will fill in the data. We recommend that you leave the checkbox settings at their default settings. Then press **the "Continue" button**.

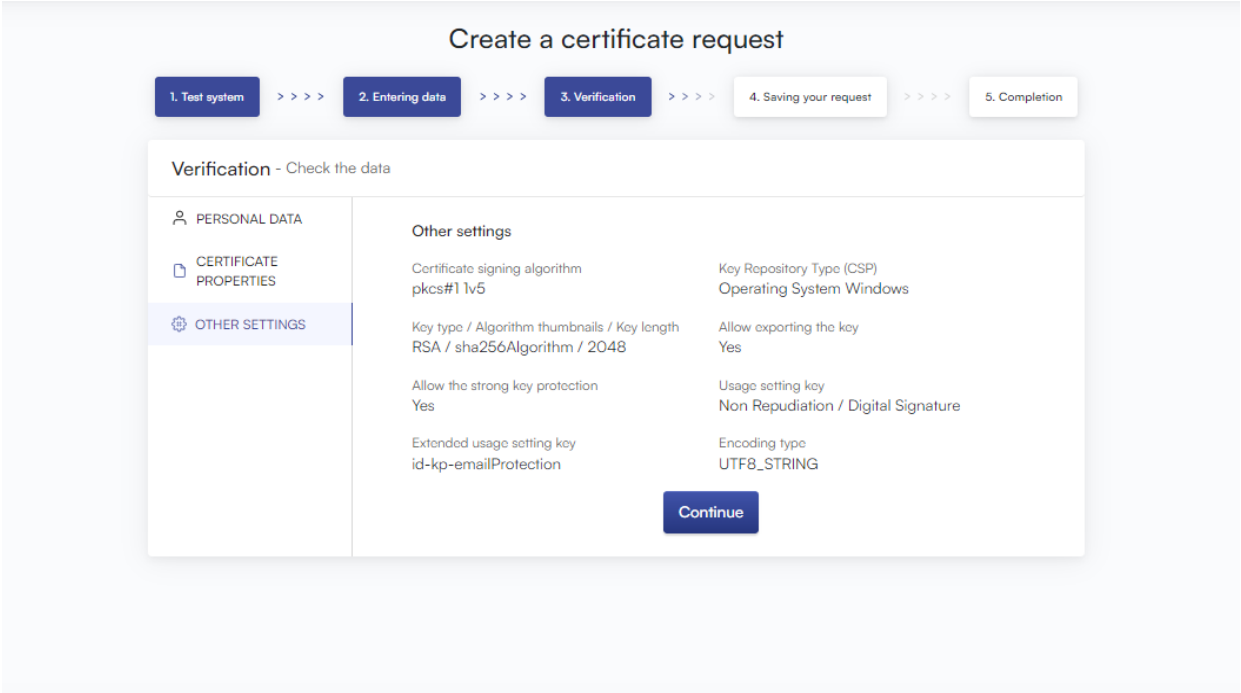


1.4 Verification

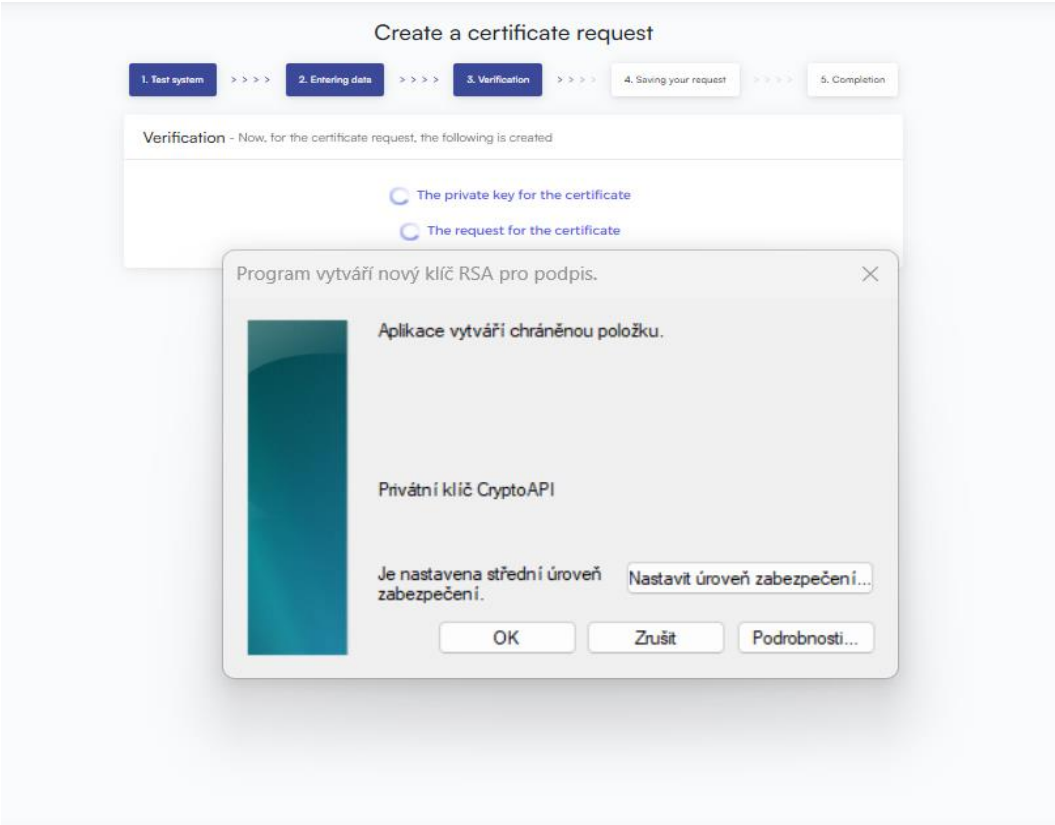
On the Data Check tab, you need to check the correctness of the data you have entered. You can then press the **"Continue" button**.


Create a certificate request
1. Test system
2. Entering data
3. Verification
4. Saving your request
5. Completion
Verification - Check the data
PERSONAL DATA
CERTIFICATE PROPERTIES
OTHER SETTINGS
Personal data
Full name
Jan Novák
First name
Jan
Surname
Novák
E-mail in the certificate
podpora@ica.cz
Country
CZ
Continue


Create a certificate request
1. Test system
2. Entering data
3. Verification
4. Saving your request
5. Completion
Verification - Check the data
PERSONAL DATA
CERTIFICATE PROPERTIES
OTHER SETTINGS
Certificate setting
Type of the certificate
Qualified certificate
Type of applicant
Personal - (non-entrepreneurial)
Certificate containing IC MLSA for communication with the public authorities
Yes
Revocation password
revocation
E-mail for contact with I.CA
podpora@ica.cz
Certificate sent in the ZIP format
Yes
Period of validity
365 days
Continue

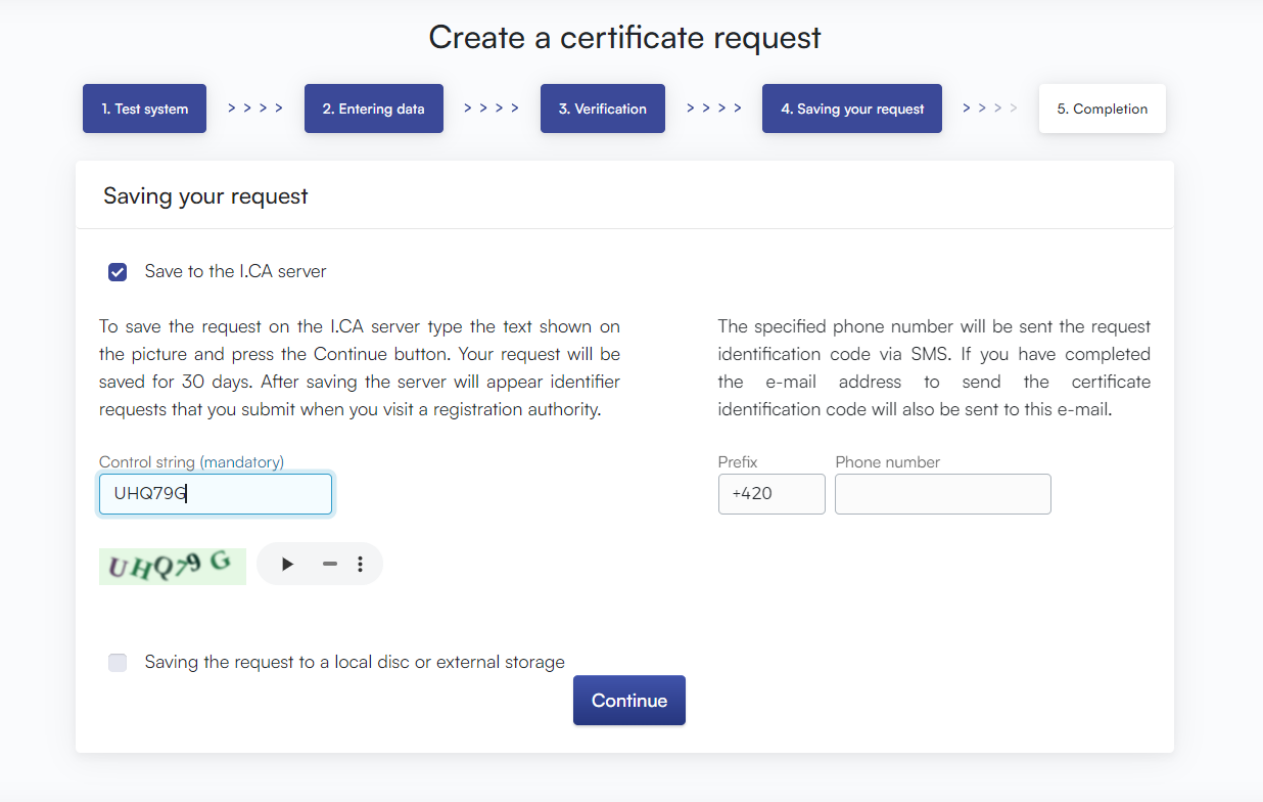


After pressing the "Continue" button, the private key will be generated to the computer. A new icon will appear on the Windows bar and after clicking on this icon, a window will appear, which needs to be confirmed by the **"OK"** button. If a certificate is generated for a chip card or ID card, a PIN will be requested.



1.5 Saving your request

Here you leave **the "Save to server I.CA" checked,** copy the control string and fill in the phone number (the phone number is filled in here only for receiving an SMS message with the application number, which you will need at the registration authority). Then press **the "Continue"** button.



1.6 Completion

In this step, the application is completed and all you have to do is visit the registration authority to verify and issue the certificate.

