

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	5
1.4	Verification	6
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>.

Obtaining a request for a certificate

Step 1: For whom the certificate is intended? Select the option you are interested in:

personal

employee or self-employed person

company or government institution

Natural person (Personal) - if you choose this option, your certificate will contain your name and surname, optionally it is also possible to state your residence and e-mail address.

Employee or self-employed person - it is intended for those who, in addition to their name and surname, also need to state the name of company/trade or employer in the certificate. You can also use it if you are a company executive.

Company or government institution - if you need a certificate for your company, government institution, or other legal entity, select this option. The certificate will contain the name of the subject and optionally also its registered office.

- 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.

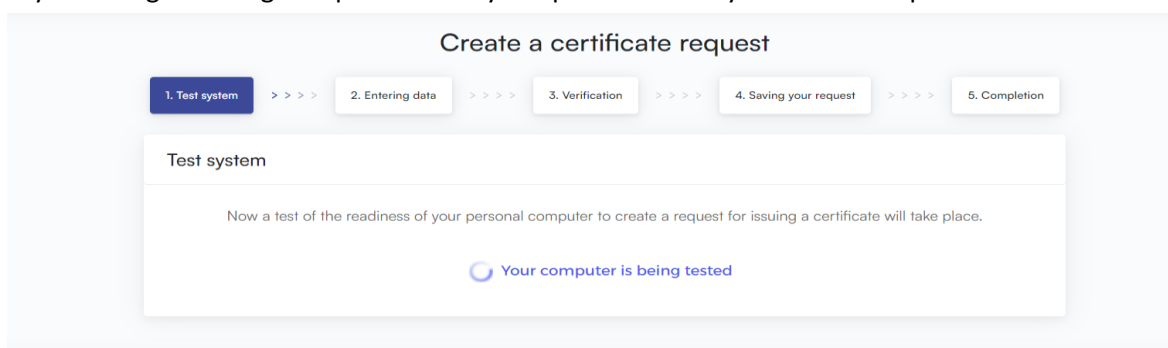
If you are applying for a certificate **stored on your ID card**, it is necessary to have the eObčanka – Card Manager application installed and your ID card connected to a computer that has set up a PIN and QPIN.

Step 2: select the option you are interested in ([Back to step 1](#))

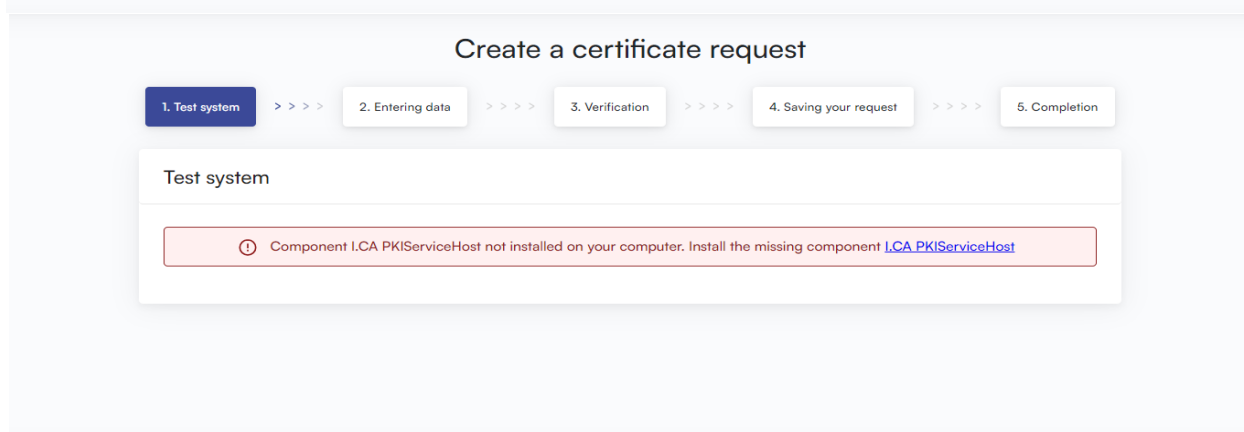
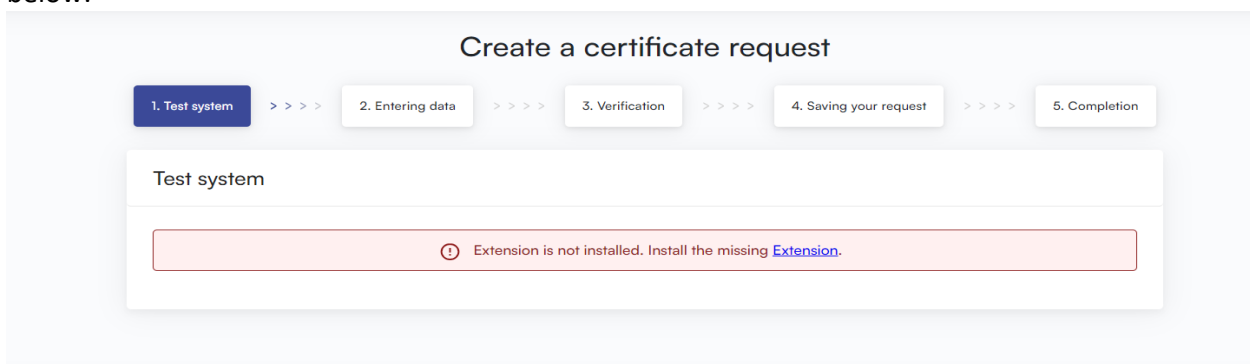
- Qualified certificate for electronic signature**
used to sign documents. It is used where a recognized electronic signature is required.
 - will be stored on your computer
 - will be stored on the smart card
 - will be stored in the ID card

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 PKIService 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**.

Create a certificate request

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

Information about the applicant + Show other options

Degree (before name)	Degree (after name)	
<input type="text"/>	<input type="text"/>	
First name (mandatory)	Surname (mandatory)	Country (mandatory) ⓘ
<input type="text"/>	<input type="text"/>	Czech Republic ▼
E-mail in the certificate ⓘ	E-mail for contact with I.C.A. ⓘ	Prefix Phone number
<input type="text"/>	<input type="text"/>	+420 ▼ <input type="text"/>

Insert optional identifier for individuals

Certificate setting

Key type (mandatory)	Revocation password (mandatory) ⓘ	Key Repository Type (CSP) (mandatory)
RSA 2048 ▼	<input type="text"/>	Operating System Windows ▼

- Certificate sent in the ZIP format
- Certificate containing IC MLSA for communication with the public authorities ⓘ
- Allow exporting the key ⓘ
- Allow the strong key protection ⓘ

Advanced options ▼

Continue

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

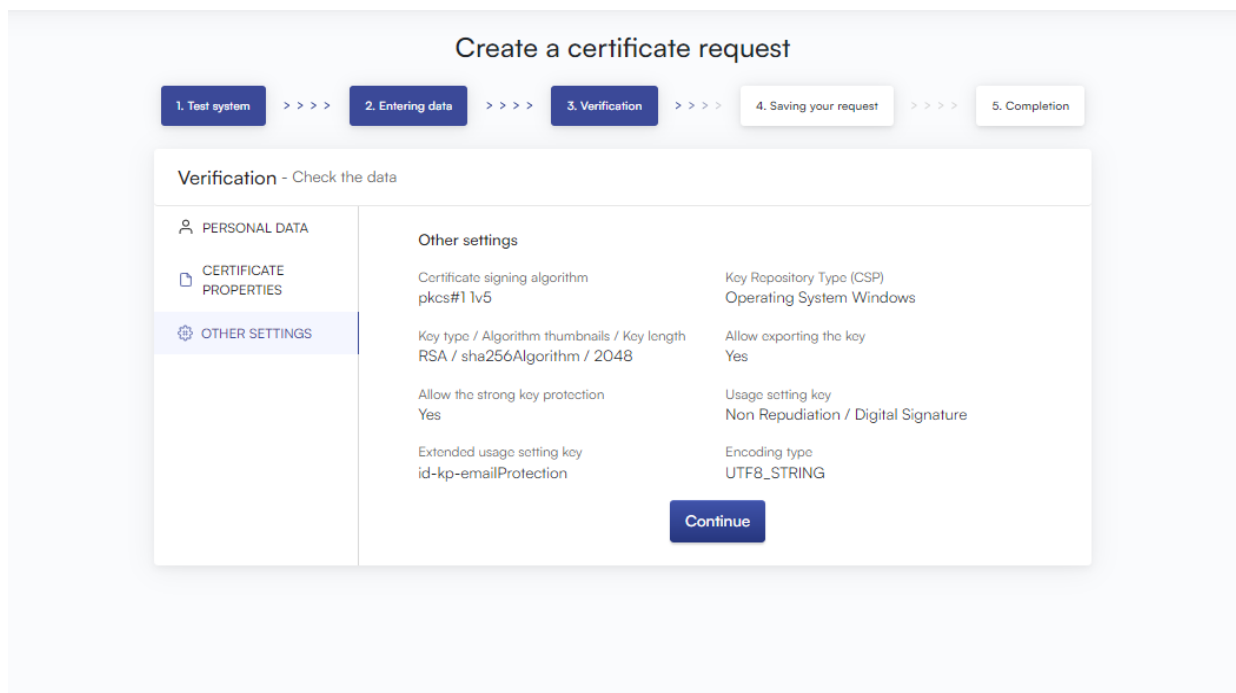
PERSONAL DATA	Personal data	
CERTIFICATE PROPERTIES	Full name Jan Novák	First name Jan
OTHER SETTINGS	Surname Novák	E-mail in the certificate podpora@ica.cz
	Country CZ	
	Continue	


Create a certificate request

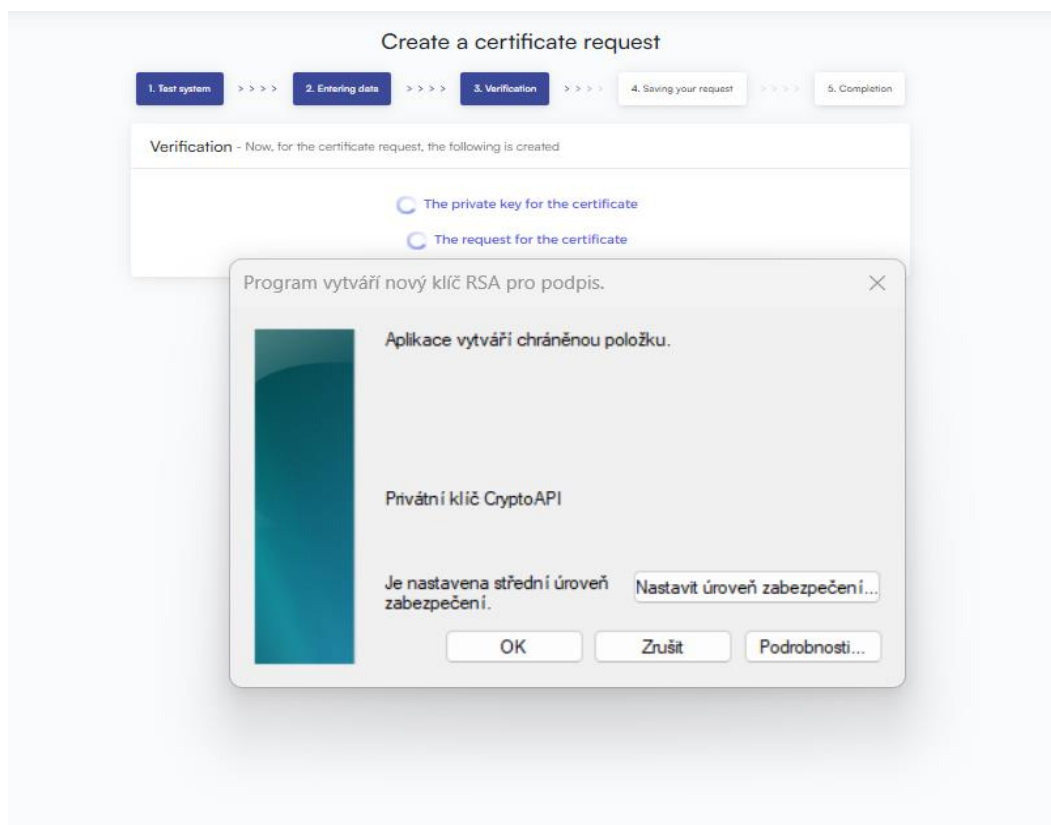
1. Test system >>>> 2. Entering data >>>> 3. Verification >>>> 4. Saving your request >>>> 5. Completion

Verification - Check the data

PERSONAL DATA	Certificate setting	
CERTIFICATE PROPERTIES	Type of the certificate Qualified certificate	Type of applicant Personal - (non-entrepreneurial)
OTHER SETTINGS	Certificate containing IC MLSA for communication with the public authorities Yes	Revocation password revocation
	E-mail for contact with ICA 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.

Create a certificate request

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

Saving your request

Save to the I.CA server

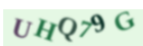
To save the request on the I.CA server type the text shown on the picture and press the Continue button. Your request will be saved for 30 days. After saving the server will appear identifier requests that you submit when you visit a registration authority.

Control string (mandatory)

UHQ79d

The specified phone number will be sent the request identification code via SMS. If you have completed the e-mail address to send the certificate identification code will also be sent to this e-mail.

Prefix Phone number

 ▶ - ⋮

Saving the request to a local disc or external storage

Continue

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.

Create a certificate request

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

Saving your request

✔ Your request has been successfully stored on the I.CA server.

Identification code of your request has been sent to the email address indicated in the certificate request.

Identifier has been successfully sent to your e-mail podpora@ica.cz
We recommend that you create a backup of your private key.
Follow the instructions here: <https://www.ica.cz/Private-key-backup>

Find the registration authority

Exit the wizard