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: <u>https://www.ica.cz/certificate</u> or choose a certificate here: <u>https://www.ica.cz/products</u>.

C	Obtaining a request f	or a certificate ——
Step 1: For who	m the certificate is intended? Select the option	n you are interested in:
personal	employee or self-employed person	company or government institution
Natural person optionally it is a Employee or se also need to sta company execu Company or go	(Personal) - if you choose this option, your certi lso possible to state your residence and e-mail lf-employed person - it is intended for those wi ite the name of company/trade or employer in itive. wernment institution - if you need a certificate	ificate will contain your name and surname, address. ho, in addition to their name and surname, the certificate. You can also use it if you are a for your company, government institution, or
other legal enti its registered of	ty, select this option. The certificate will contair fice.	n the name of the subject and optionally also

- <u>personal</u> only the name and surname of the applicant will be stated in the certificate. Not
 organizations.
- <u>employee or self-employed</u> person the certificate will state **the name, surname and also the organization** for which the applicant is acting.
- <u>company or government institution</u> 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.

		C	Create	a certific	ate req	luest		
1. Test system	>>>>	2. Entering data		3. Verification		4. Saving your request		5. Completion
Test syster	n							
Now	a test of the	e readiness of yo	ur personal o	computer to cre	ate a reques	st for issuing a certificat	e will take p	lace.
			🔾 You	r computer is	being teste	ed		

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

Test system • Extension is not installed. Install the missing Extension. • Create a certificate request • Ext system • Create a certification • Create a certificate request • Create a certification • Create a certificate request • Create a certificate request • Create a certificate request • Create a certificate request • Create a certificate request	1. Test system > >	> > 2. Entering data		3. Verification		4. Saving your requ	est >>>	> 5. Compl
① Extension is not installed. Install the missing Extension. Create a certificate request . Test system 2. Entering data 3. Verification 4. Saving your request 5. Completion Test system ③ Component LCA PKIServiceHost not installed on your computer. Install the missing component LCA PKIServiceHost	Test system							
Extension is not installed. Install the missing Extension.	-							
Create a certificate request 1. Text system 2. Entering data 3. Verification >>>> 4. Saving your request >>>> 5. Completion Test system Component LCA PKIServiceHost not installed on your computer. Install the missing component LCA PKIServiceHost 6. Completion		!	Extension is	not installed. In	stall the missir	ng <u>Extension</u> .		
Create a certificate request 1. Test system 2. Entering data 3. Verification 2. Entering data 5. Completion Test system 3. Verification 2 5. Completion Test system Component I.CA PKIServiceHost not installed on your computer. Install the missing component I.CA PKIServiceHost								
Create a certificate request I. Test system 2. Entering data 3. Verification 4. Saving your request 5. Completion								
Create a certificate request 1. Test system 2. Entering data 3. Verification 4. Saving your request 5. Completion			•					
1. Test system >>>> 2. Entering data >>>> 3. Verification >>>> 4. Saving your request >>>> 5. Completion Test system () Component I.CA PKIServiceHost not installed on your computer. Install the missing component I.CA PKIServiceHost		(Create	a certific	ate req	uest		
Test system Component I.CA PKIServiceHost not installed on your computer. Install the missing component <u>I.CA PKIServiceHost</u>	1. Test system > >	>>> 2. Entering data		3. Verification		4. Saving your request		5. Completion
Component I.CA PKIServiceHost not installed on your computer. Install the missing component <u>I.CA PKIServiceHost</u>								
Component I.CA PKIServiceHost not installed on your computer. Install the missing component I.CA PKIServiceHost	Test system							
	() Cor	mponent I.CA PKIService+	ost not installe	ed on vour compu	ter. Install the	missing component I.C		ost

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**.

I. Test system >>>>> 2. Entering data	>>>> 3. Verification >>>> 4.	Saving your request >>>> 5. Completion
Information about the applicant		+ Show other option
Degree (before name)	Degree (after name)	
First name (mandatory)	Surname (mandatory)	Country (mandatory) ③ Czech Republic ~
z-mail in the certificate ③	E-mail for contact with I.CA ③	Prefix Phone number
Insert optional identifier for individuals		+420 🗸
Insert optional identifier for individuals	S	+420 ~
Insert optional identifier for individuals Certificate setting Key type (mandatory)	Revocation password (mandatory) ③	(+420 ✓)
Insert optional identifier for individuals Certificate setting Key type (mandatory) RSA 2048	Revocation password (mandatory) ①	+420 Key Repository Type (CSP) (mandatory) Operating System Windows
Insert optional identifier for individuals Certificate setting key type (mandatory) RSA 2048 key type (mandatory)	Revocation password (mandatory) ③ Certificate containing IC MLSA for communication with the public authorities ①	+420 Key Repository Type (CSP) (mandatory) Operating System Windows
Insert optional identifier for individuals Certificate setting Key type (mandatory) RSA 2048 Certificate sent in the ZIP format Allow exporting the key ③	Revocation password (mandatory) ③ Certificate containing IC MLSA for communication with the public authorities ③ Allow the strong key protection ③	+420 Key Repository Type (CSP) (mandatory) Operating System Windows

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**.



1. Test system >>>>>	2. Entering data >>>> 3. Verification >>	>>> 4. Saving your request >>>>	5. Completio
Verification - Check th	ne data		
A 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	Create a certificate 2. Entering data >>>> 3. Verification >>>	request >> 4. Saving your request >>>> 5	5. Completior
1. Test system >>>> Verification - Check the	Create a certificate 2. Entering date >>>> 3. Verification >> a data	request >> 4. Saving your request >>>> 5	5. Completion
1. Test system >>>> Verification - Check the A PERSONAL DATA	Create a certificate 2. Entering data 3. Verification 3. Verification 3. data Certificate setting	request >>> 4. Saving your request >>>> 5	5. Completion
1. Test system >>>>> Verification - Check the % PERSONAL DATA CERTIFICATE PROPERTIES	Create a certificate 2. Entering data >>>> 2. Entering data	request >>>> 5 4. Saving your request >>>>> 5 Type of applicant Personal - (non-entrepreneurial)	5. Completion
1. Test system >>>> Verification - Check the A PERSONAL DATA CERTIFICATE PROPERTIES Image: Contract of the settings	Create a certificate 2. Entering data >>>>> 3. Verification >>> e data certificate setting Type of the certificate Qualified certificate Certificate containing IC MLSA for communication with the public authorities Yes	request >>> E >> 4. Saving your request >>>> E Type of applicant Personal - (non-entrepreneurial) Revocation password Revocation password revocation E	5. Completion
1. Test system >>>>> Verification - Check the A PERSONAL DATA CERTIFICATE PROPERTIES OTHER SETTINGS	Create a certificate 2. Entering data >>>> 3. Verification >>> e data Certificate setting Type of the certificate Qualified certificate Certificate containing IC MLSA for communication with the public authorities Yes E-mail for contact with LCA podpora@ica.cz	request >> 4. Saving your request >>>>> E Type of applicant Personal - (non-entrepreneurial) Revocation password revocation E Certificate sent in the ZIP format Yes Yes E	5. Completion
1. Test system >>>>> Verification - Check the A PERSONAL DATA CERTIFICATE PROPERTIES Image: CERTIFICATE PROPERTIES Image: OTHER SETTINGS	2. Entering data >>>> 3. Verification >>> 2. Entering data >>>>> 3. Verification >>> 2. data Certificate setting >>>> >> Type of the certificate Cualified certificate > Certificate setting Type of the certificate Certificate containing IC MLSA for communication with the public authorities Yes E-mail for contact with LCA podpora@ica.cz Period of validity 365 days Set the set th	request >> 4. Saving your request >>>>> E Type of applicant Personal - (non-entrepreneurial) Revocation password revocation E Certificate sent in the ZIP format Yes Yes E	5. Completion



Verification - Check the	data	
A PERSONAL DATA	Other settings	
CERTIFICATE PROPERTIES	Certificate signing algorithm pkcs#1 1v5	Key Repository Type (CSP) Operating System Windows
OTHER SETTINGS	Key type / Algorithm thumbnails / Key length RSA / sha256Algorithm / 2048	Allow exporting the key Yes
	Allow the strong key protection Yes	Usage setting key Non Repudiation / Digital Signature
	Extended usage setting key id-kp-emailProtection	Encoding type UTF8_STRING
	Co	ntinue

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.

Verification - Now, for the certi	ficate request, the following is created	
	C The private key for the certificate	
Program vy	tváří nový klíč RSA pro podpis.	×
	Privátní klíč CryptoAPI	
	Je nastavena střední úroveň Nastavit úroveň zabezpečer zabezpečení.	ení
	OK Zavěž Podrohosti	ti



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.

 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. 	aving your request			
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. The specified phone number will be sent the re- identification code via SMS. If you have comp the e-mail address to send the certii identification code will also be sent to this e-mail	Save to the I.CA server			
Control string (mandatory) Prefix Phone number UHQ79Q +420	save the request on the I.CA server type the text e picture and press the Continue button. Your requived for 30 days. After saving the server will appear quests that you submit when you visit a registration a entrol string (mandatory) JHQ79G	shown on The spe uest will be identific ar identifier the e- authority. identific Prefix +420	Actified phone number will be s ation code via SMS. If you h mail address to send ation code will also be sent to Phone number	sent the request have completed the certificate this e-mail.

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 cer	tificate request
1. Test system >>>> 2. Entering data >>>> 3. Verif	ication >>>> 4. Saving your request >>>> 5. Completion
Saving your request	
 Your request has been su 	ccessfully 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: <u>https://www.ica.cz/Private-key-backup</u>
Find the registration authority	Exit the wizard