# Generating a request for a certificate User Guide for browser Mozilla Firefox

První certifikační autorita, a.s.

Version 8.15

# Contents

1.	I	Intro	duct	ion3
2.		Requirements		
3.	Installation root certificate I. CA			on root certificate I. CA
4.	•	The p	proce	ess of generating a request for a certificate5
4	1.1	1.	Cont	rol software5
	4	4.1.1		Unsupported operating system7
	4	4.1.2		Unsupported Web Browser7
		4.1.3	•	Support for JavaScript7
		4.1.4	•	Support for Java Runtime Environment (JRE)7
	4	4.1.5		Storage cookies7
4	1.2	2.	Fillin	g in data about the applicant8
4	1.3	3.	Chec	king the entered data10
4	1.4	1.	Gene	erating a certificate request10
		4.4.1	•	SecureStoreCSP – smart card I.CA10
		4.4.2	•	Microsoft Enhanced RSA and AES Cryptographic Provider with strong protection private key 11
4	1.5	5.	Savir	ng certificate
5.		Issua	nce	certificate14
6.		Insta	llatic	on Java Runtime Environment (JRE)14
7.	-	Troul	blesh	nooting16



## 1. Introduction

This document is a guide on how to proceed hen generating a request for a certificate through the website.

# 2. Software Requirements

The computer where will you generate a certificate request must fulfill the following requirements:

- Operating system vision:
  - Microsoft Windows XP Service Pack 3
  - Windows Vista
  - Windows 7
  - Windows 8 / 8.1
  - Windows 10
- Browser **Mozilla Firefox** version 13.0 39.0
- The current software Java Runtime Environment (JRE).
  - This software is detected a test page automatically if it detects that the software is not present, it prompts user to download / install.
- In the web browser must be enabled scripting support Javascript, Java enabled, support storing cookies.

# 3. Installation root certificate I. CA

When you start the page for generating request a certificate, browser can inform you that you are entering on untrusted sites. This problem is caused by the fact that you have not stored in the repository root certificates I.CA, you can download here: <u>http://www.ica.cz/Root-certificate</u>



<b>CERTIFICATION</b> AUTHORITY autorita, A.S.	CONNECTED WITH TRUST	t of commercial provid an at south of digital certificates that are Creck 9 of provided services a successful completioner accreditation process in concic signature and cobia of sectors, the Office for					
ABOUT US REGISTRATION AUTHORITIES PI	RODUCTS & SERVICES PRICE LIST SUPPORT	🔎 Search 🕨 🍃 🕑					
> <u>About us</u> > <u>Quick link labels</u> > Root certificates							
I.CA Root Certificates		Quick link labels					
Root certificates are issued by the I.CA Certificatio certificate is included in Trusted Root Certification verification of client certificate issued by I.CA in the	Root certificates are issued by the I.CA Certification Authority itself. After installation on a PC, a root certificate is included in Trusted Root Certification Authorities and allows subsequent automated verification of client certificate issued by I.CA in the system.						
You can install all the current I.CA root certific	You can install all the current I.CA root certificates by executing the file ica root.zip						
Below you can choose the installation of a particu	lar root certificate.	<ul> <li>Documents to obtain a certificate</li> </ul>					
Root Certificates in non hierarchic structure	Root Certificates in Thierarchic structure	Request for revocation of certificate					
		<ul> <li>Certification Policy</li> </ul>					
for Commercial Certificates SHA-1	Root Certificate	<ul> <li>Bulletin for users</li> </ul>					
for Commercial Certificates SHA-2	Certificates for Web servers (SSL)	<ul> <li>Poot cortificatos</li> </ul>					

Click on **ica\_root.zip**, you will see a dialog to download the file. Save the file to your hard disk, unzip and run extended ica\_root\_v200.exe.

This starts on installation wizard Root certificates I.CA.

🕞 Instalace Kořenové certifikát	y I.CA v2.0
	Vítejte v průvodci instalace programu Kořenové certifikáty I.CA Tento průvodce Vás provede instalací Kořenové certifikáty I.CA. Před začátkem instalace je doporučeno zavřít všechny ostatní aplikace. Toto umožní aktualizovat důležité systémové soubory bez restartování Vašeho počítače. Pro pokračování klikněte na 'Další'.
	Další > Storno

During installation, you can register all root certificates among trusted, confirm ANO (Yes).

闭 Instalace Kořenové certifikáty I.C	CA v2.0	
<b>Instalace</b> Vyčkejte, prosím, na dokončení inst	alace programu Kořenové certifikáty I.O	CA.
Výstupní složka: C: \Program Files \I	.CA\Kořenové certifikáty I.CA	
🕞 Instalace Kořenové certifiká	ty I.CA v2.0	23
Přejete si zaregistrovat kořeno certifikační úřady Windows?	vé certifikáty I.CA mezi důvěryhodn	ié kořenové
	Ano	Ne
Nullsoft Install System v2.31 ———	< 7nět Zavřít	Storm

# 4. The process of generating a request for a certificate

Creating the request choose after selecting the type of certificate here <a href="http://www.ica.cz/Certificate">http://www.ica.cz/Certificate</a>

Process generace a request for initial certificate:

- 1) Control software
- 2) Filling in the applicant's data
- 3) Checking the data filled
- 4) Generating a certificate request
- 5) Saving the certificate request

## 4.1. Control software

Before you start generating request must run the kontrol software components.

Click on the **Begin analysis** button to start the test your computer.



AUTHORITY	První certifikační Certifica autorita, A.s.	ate request
<b>1.</b> Test system First it is necess the tests, you m	2. Entering data 3. Ver Is your con ary to test whether your computer meets the av be asked to perform some undates softwa	iffication 4. Saving request 5. Completion          mputer ready?         minimum requirements for trouble-free generation of request. Through this case it is necessary to confirm accentance of
these updates. In case of comp	ications contact <u>technical support I.CA</u> . Be Waiting fe	<sup>gin analysis</sup> or test launch
RESULT	DESCRIPTION	DETAILS
	CALLS TO THE STATE OF A DOMESTIC STATE FOR THE ACCURATE	
	Operation system version	
	Operation system version Browser type and version	
	Operation system version Browser type and version Support of JavaScript	
	Operation system version           Browser type and version           Support of JavaScript           Support of Java (JRE)	
	Operation system version         Browser type and version         Support of JavaScript         Support of Java (JRE)         Support of I.CA Java Applet	

During the test screen appeal with a warning of the JRE, select **Run**. Will be instar and run the applet ICApki, which is necessary for the functionality of the site to generace the certificate request. This installation can take a while.

Do y	vou wan	t to run tl	his application?		×
ſ	4	Name:	jICApki		
	E	Publisher:	První certifikační autori	ita, a.s.	
	_	Location:	https://tests.ica.cz		
This a and pe and pu	pplication w ersonal info ublisher abo	vill run with un rmation at risk ve.	restricted access which . Run this application or	may put your c nly if you trust tl	omputer he location
Do	not show th	nis again for a	pps from the publisher a	and location abo	ove
Û	More Infor	mation		Run	Cancel



Test completed successfully						
RESULT	DESCRIPTION	DETAILS				
~	Operation system version	Windows 10 this operation system is supported.				
~	Browser type and version	Firefox version 40.0, this web browser is not supported.				
~	Support of JavaScript	JavaScript enabled.				
~	Support of Java (JRE)	Installed Java JRE (Runtime Environment) from manufacturer: Oracle Corporation (Version: 1.8.0 51).				
~	Support of I.CA Java Applet	Java Applet jlCApki is running.				
~	Support of cookies storage	Storage of cookies are enabled.				

After completing the test computer click the **Continue** button.

If checks error occurs you can not continue making request.

#### 4.1.1. Unsupported operating system

For generating request must use the recommended operating system.

#### 4.1.2. Unsupported Web Browser

For generating request must use the recommended Web Browser.

#### 4.1.3. Support for JavaScript

When generating request support is required scripting in JavaScript. This support must enable in your browser.

#### 4.1.4. Support for Java Runtime Environment (JRE)

It is required to install JAVA support.

Installing the JRE is described in Chapter 6.

#### 4.1.5. Storage cookies

It is necessary to allow your browser to store the cookies. If you are disabled from storing cookies, you must enable it.



## 4.2. Filling in data about the applicant

After completing the testing computer you can continue filling out obligatory čems.

1. Test system <b>2.</b> Entering d	ata 3. Verification	angle <b>4</b> . sav	ing request	angle <b>5.</b> Completion
INFORMATION ABOUT THE APP	LICANT		HIDE	OTHER OPTIONS >>
Current user (individual - non-entrepreneurial)     Employee (incl. statutory body members)     A legal entity (company - self-employed)     Legal person     Sonver	Name E-mail in the certificate Czech Republic		Surname E-mail for c	contact with I.CA
DETAILS OF THE APPLICANT PERMANENT ADDRESS	Degree (before name) Street City / town	Degree (afte Street numb Zip code	er name) er / building ic Province	Generational resolution
Revocation password Key Repository Type (CSP)	Your password Operating System Window	/S		<ul><li><b>⊘</b></li></ul>
Certificate sent in the ZIP format			<ul> <li>Certificate</li> <li>Certificate</li> <li>Allow exp</li> <li>Allow the</li> </ul>	es for signing es for encryption porting the key ? strong key protection ?
		ADVA	NCED CER	TIFICATE OPTIONS >>

Blue-tinged entries are required. Other items can be found by clicking on Hide others options.

#### E-mail in the certificate:

Fill in when you use electronic signatures for signing e-mail messages (eg. MS Outlook). E-mail address listed in the certificate must match the e-mail sender.

#### E-mail for contact with I. CA:

This e-mail address may be different compared with the above, will be used for sending information e-mails.

#### **Revocation password:**

The certificate can be revoke through a web interface. When certificate revocation will be prompted to enter the password for revocation.

If you do not enter a new password will be used existing password.



## Key repository Type (CSP):

Here you can select from a menu module providing cryptographic service provider (CSP), which will generate your private key. All CSP displayed here are installed on your computer.

#### Export private key:

If the selected storage type keys (CSP) supports export the private key, you are given the option to enable export the private key. This option allows to export the certificate including private key. The private key so you will be able to transfer between storage. Key management requires in this case caution because of the higher risk of theft / misuse.

#### Strong private key:

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

You can choose:

**Middle** - you always notice only informative report **Strong** - before every use you will be required to enter your password

After clicking a button to **Continue**, take place checking the completed data. If any of the entered data do not meet, you must be repaired. These data are tinged with red.

IN	FORMATION ABOUT THE APP	LICANT			HIDE OTHER OPTIC	)NS :	>>
۲	Current user (individual - non-entrepreneurial)	Name	×		Surname	×	
0	Employee (incl. statutory body members)	E-mail in the certificate		0	E-mail for contact with I.CA		0
0	A legal entity (company - self-employed)	Czech Republic	~				
0	Legal person						
$\cap$	Conjor						



## 4.3. Checking the entered data

#### In step Recapitulation Check the entered dat.

INFORMATION ABOUT THE APPLICANT				
Full name	Petr Pavel			
E-mail in the certificate	pospichal@ica.cz			
Country	Czech Republic			
CERTIFICATE SETTING				
Type of the certificate	Commercial certificate			
Type of applicant	Current user (individual - non-entrepreneurial)			
Revocation password	12341234			
E-mail for contact with I.CA	pospichal@ica.cz			
Certificate sent in the ZIP format	Yes			
Period of validity	365 days			
Key Repository Type (CSP)	Operating System Windows			
Algorithm thumbnails / Key length	sha256WithRSAEncryption / 2048			
Allow exporting the key	Yes			
Allow the strong key protection	Yes			
Usage setting key	Certificates for signing / Certificates for encryption			
Encoding type	UTF8_STRING			

To the repair it is possible to go one step back. Click the **Continue** button to begin the creation of the private key

#### 4.4. Generating a certificate request

The procedures for different types of private key storage (CSP).

#### 4.4.1. SecureStoreCSP – smart card I.CA

Displayed you will the following dialog, now generating your private key. Creating a private key may take several tens of seconds.

SecureStoreCSP card operation is in progress...

After creating the private key you're prompted to enter a PIN on your card.





4.4.2. Microsoft Enhanced RSA and AES Cryptographic Provider with strong protection private key

If you choose the type of storage key Microsoft Enhanced RSA and AES Cryptographic Provider (eventualy Microsoft Enhanced RSA and AES Cryptographic Provider /prototype/) and enter the option enable strong key protection, follow these steps:



Test system	2. Verification	3. Recapitulation	
CREATING C	OF THE RENEWAL CERT	FIFICATE REQUEST	
		Ċ	
Please	wait, key genera	ation and creat	ion of the renewal certificate
		request.	
Creating a new	/ RSA signature key	×	
	An application is creating a Prote	ected item.	
		el N	ovák
		i c	ertifikační autorita, a.s.
	CryptoAPI Private Key	pict	al@ica.cz
	Security level set to Medium	Set Security Level	
	OK Car	ncel Details	
		Make the reque	st

Choose Select a security level appropriate for this item:

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.	
	O Medium Request my permission when this item is to be used.	
	< Back Next > Cancel	

High = It must enter the password.

Create a password t	o protect this item.
Create a new passw	ord for this item.
Password for:	CryptoAPI Private Key
Password:	••••
Confirm:	••••
 - C Pack	Enide

After click on the button **Finish** will change the security level. Now click on the button **OK**.

In the next dialog click Allow to grant permissions. If you have chosen a high level of security, you must enter the password.

windows sect	inty
Credentia	I Required
To allow the	app to access your private key, enter the password:
Key descripti	on : CryptoAPI Private Key
	Password
Ω	
<b>•</b> 0=•	Enter Password

## 4.5. Saving certificate

By selecting **Save on local disk or external storage** request will be stored on your hard drive or other selected media.

If you want to save the a request to the server I.CA you rewrite code (captcha) referred to in the box Control string and press **Continue**. If your request is successfully stored on the server I.CA, you will receive an identifier, that must be submitted by visiting the registration authority.



The identifier will be sent to the email address specified in the request or sms in mobile phone number.

1 Test system	<b>2.</b> Entering data	3. Verification	<b>4</b> . Saving reques	st 5. Completion
SELECT HOW TO	SAVE YOUR CERTIF	ICATE REQUEST		
Save to the server I	.CA			
Save on local disk of	or external storage			
SAVE TO THE SE	RVER I.CA			
To save the request or picture and press the C 30 days. After saving t you submit when you vis	the server I.CA type the te ontinue button. Your request he server will appear identit it a registration authority.	ext shown on the will be saved for code certifier requests that	specified phone number will via SMS. If you have comple icate identification code will a	be sent the request identification eted the e-mail address to send the lso be sent to this e-mail.
Q1 40 6G	QZAU6G	×	+420 Phone num	ber
		-		
		Continue		

## 5. Issuance certificate

After creating the certificate request, you must personally visit the registration authority I.CA - list here <u>http://www.ica.cz/Registration-Authorities-HQ</u>. Bring with them a request you generated (such as in a USB flash drive, stored on a smart card) or the request identifier stored on the server I.CA. Further, the documents requested by the type certificate - information here <u>http://www.ica.cz/Documents-qualified-certificate</u>.

# 6. Installation Java Runtime Environment (JRE)

If the support for "Java Runtime Environment" not installed, you will be prompted to install.

RESULT	DESCRIPTION	DETAILS
~	Operation system version	Windows 10 this operation system is supported.
~	Browser type and version	Firefox version 40.0, this web browser is not supported.
~	Support of JavaScript	JavaScript enabled.
×	Support of Java (JRE)	Unable to successfully detect the installation of Java Runtime Environment (JRE). Either not installed, or your browser is blocking plugin from our site. Functional verification or JRE installation can be done on <u>manufacturer's website</u> . After installation, close and restart the browser for the changes to take effect.
	Support of I.CA Java Applet	
	Support of cookies storage	



Installation is available here: <u>https://java.com/en/download/index.jsp</u>. On the page producer JAVA select button **Free Java Download** and then **Agree and Start Free Download**.

Choose to run or save the installation file to disk and then run the installation.

Select button Install follow the installation wizard.

Java Setup - Welcome X					
Welcome to Java					
Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life.					
Note: No personal information is gathered as part of our install process. <u>Click here</u> for more information on what we do collect.					
Click Install to accept the license agreement and install Java now.					
Change destination folder Cancel Install >					
Java Setup - Progress — 🗆 🗙					
Status: Installing Java					
<b>3 Billion Devices Run Java</b> Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security, Systems, Cable Power, TVS					
ORACLE'					



At the end of the wizard, select the **Close** button. I recommend a browser restore to save the changes.

Java Setup - Complete	$\times$
Vou have successfully installed Java	
You will be prompted when Java updates are available. Always install updates to get the latest performance and security improvements. <u>More about update settings</u>	
When you click close, your browser will be opened so you can verify that Java is working.	
Close	

# 7. Troubleshooting

When an error occurs in the proces of generating the request will be informed error message.



Some errors can be serious technical. Can be related with the state of the hardware or software of your computer. In this case, we recommend contacting <u>technical support I.CA.</u>