Generating a request for a subsequent certificate User Guide for browser Opera

První certifikační autorita, a.s.

Version 8.15



Contents

1.	Intr	oduct	ion	.3
2.	Soft	ware	Requirements	.3
3.	The	proce	ess of generating a request for a subsequent certificate	. 3
	3.1.	Cont	trol software	. 3
	3.1.	1.	Unsupported operating system	. 5
	3.1.	2.	Unsupported Web Browser	. 5
	3.1.	3.	Support for JavaScript	. 5
	3.1.	4.	Support for Java Runtime Environment (JRE)	. 5
	3.1.	5.	Storage cookies	. 5
	3.2.	Cert	ificate selection for to create request for subsequent	. 5
3	3.3.	Addi	itions and changes to some data	. 7
	3.4.	Gen	erating a certificate request	. 9
	3.4.	1.	SecureStoreCSP – smart card I.CA	. 9
	3.4.	2.	Microsoft Enhanced RSA and AES Cryptographic Provider with strong protection private keep	∋у
	3.5.	Sign	ing and sending an a request for subsequent certificate	۱1
4.	Inst	allatio	on Java Runtime Environment (JRE)	L3
5.	Tro	ublesł	hooting	15



1. Introduction

This document is a guide on how to proceed hen generating a request for a subsequent 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 **Opera** version 10.0 31.0
- o 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. The process of generating a request for a subsequent certificate

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

3.1. 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.

CERTIFICATION FAUTHORITY 2	První certifikační Ssue of autorita, A.S.	renewal certificate
		6
1. Test system	2. Verification 3. Re	capitulation \4. Signature request \5. Completion
	ls your co	mputer ready?
First it is necess issuance of a re it is necessary to In case of comp	ary to test whether your computer meets the newal certificate. Through the tests, you may o confirm acceptance of these updates. lications contact <u>technical support I.CA</u> .	minimum requirements for trouble-free generation of request for the be asked to perform some updates software components, in this case
	Be	gin analysis
	Waiting f	or test launch
RESULT	DESCRIPTION	DETAILS
	Operation system version	
	Browser type and version	
	Support of JavaScript	
	Support of Java (JRE)	
	Support of I.CA Java Applet	
	Support of cookies storage	
		Continue

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	ou wan	t to run t	his application?		×
ſ	4	Name:	jICApki		
	e l	Publisher:	První certifikační autori	ta, a.s.	
	_	Location:	https://tests.ica.cz		
This ap and pe and pu	oplication w rsonal info blisher abo	vill run with un rmation at risk ve.	restricted access which k. Run this application or	may put your c Ily if you trust t	he location
Do	not show th	nis again for a	pps from the publisher a	and location ab	ove
Û	More Infor	mation		Run	Cancel

	Test comple	eted successfully
RESULT	DESCRIPTION	DETAILS
~	Operation system version	Windows 10 this operation system is supported.
~	Browser type and version	Chrome version 44.0, 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.

3.1.1. Unsupported operating system

For generating request must use the recommended operating system.

3.1.2. Unsupported Web Browser

For generating request must use the recommended Web Browser.

3.1.3. Support for JavaScript

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

3.1.4. Support for Java Runtime Environment (JRE)

It is required to install JAVA support.

Installing the JRE is described in Chapter 6.

3.1.5. Storage cookies

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

3.2. Certificate selection for to create request for subsequent

After completing the testing computer select in the a valid certificate to which you want to make request for subsequent.



Lest system		3. Recapitulation	4. Signature request 3. Completion
CHOOSE WHER	E IS YOUR CERTIFICATE	STORED (REGIST	ERED)
The personal certific	cate store in Windows	⊖ Other	storage (eg I.CA smart card)
SELECT THE CE	RTIFICATE FOR WHICH	YOU WANT TO ISS	UE A RENEWAL CERTIFICATE.
Aleš Pospíchal [201	16-07-07][1FBF47](I.CA - Stan	dard Certification Auth	nority, 09/2009) 🔽
		Continue	

If your certificate is stored in the repository Windows, select **The personal certificate store in Windows**. If there is, for example, your certificate on a smart card I.CA, select **Other storage**.

Of one's own choice your previous choice is presented with a list of certificates which may be issued subsequent certificate. If you selected **Other storage**, you must connected in smart card reader and insert a smart card (or token).

Issue a subsequent certificate can only certificate that is valid and is not placed on the CRL!

If you receive an e-mail notification at the end of your certificate, part of the e-mail specified URL link where you can create an application for a subsequent certificate. Part of the URL is the serial number of the certificate. If you enter this URL into your browser, the certificate is automatically selected.



3.3. Additions and changes to some data

In this step, you can change some data that will contain your subsequent certificate.

CERTIFICATE	HIDE PERMITTED AD.IUSTMENTS >>
oenni lonne	
Commercial	2080583 (1FBF47 hex)
Not after	7. 7. 2016 13:20:56
Country	cz
Full name	Aleš Pospíchal
Organization	První certifikační autorita, a.s.
E-mail in the certificate	pospichal@ica.cz
Revocation password	Revocation password
Key Repository Type (CSP)	SecureStore CSP / Smart card I.CA
Certificate sent in the ZIP format	
Edit the e-mail	Delete Change pospichal@ica.cz

In the "Certificate" are displayed some details of the existing certificate. Displayed the serial number, and the validity of each item subject.

After clicking on the Permitted modifications subsequent certificate in the upper part, following options appear:

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

Modification e-mailu

Restricred content certificate

Your certificate may include extended use keys and subject alternative names that may already be present in the certification policy certificate.

Is displayed warning that the extension is necessary before proceeding to remove.

When you click the **Continue** button is displayed recapitulation data and setting subsequent certificate.

1. Test system	2. Verification 3. Rec	pitulation 4 . Signature request 5 . Completion
DATA OVERVIEW	V	
	Certificate sent in the ZIP form	Yes
	Period of valid	ity 365
	Key Repository Type (CS	P) Operating System Windows
	Algorithm thumbnails / Key len	th sha256WithRSAEncryption / 2048
	Allow exporting the I	ey Yes
	Allow the strong key protect	on Yes
SETTINGS THE	CERTIFICATE	
	Full na	ne Pavel Novák
	Organizat	on První certifikační autorita, a.s.
	E-mail in the certific	te pospichal@ica.cz
	IK MP	V 1234567890
	Cour	ry CZ

By clicking on Make the request to star creating a private key.

3.4. Generating a certificate request

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

3.4.1. 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.

	PIN:		
3	0	9	
\overline{O}		1	
(5)	2	4	
(-)	8	6	

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

High = It must enter the password.

Create a password to	o protect this item.
Create a new passw Password for:	ord for this item. CryptoAPI Private Key
Password:	••••
Confirm:	••••
	Create a new passw Password for: Password: Confirm:

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.

Credentia	I Required
To allow the	app to access your private key, enter the password:
Key descripti	on : CryptoAPI Private Key
	Password
6-	Foter Password
	Enter Hassword

3.5. Signing and sending an a request for subsequent certificate

If the process of creating the request they were correct, you will see the generated a request in PKCS10 format.



Once you click "Send a request processing" dialog is displayed, containing your request for subsequent certificate. This a request must be to signed a certificate to which you are requesting subsequent.

Confirmation	×
Message:	
<pre><?xml version="1.0" encoding="UTF-8"?> <ica> <ica> <request product_name="Certification Authority" product_version="8.01"> <header> <imple: client="">icaweb RENEWAL 8.01"/product_name="Certification Authority"> <imple: client="">icaweb RENEWAL 8.01</imple:> </imple:>icaweb RENEWAL 8.01</imple:> </imple:> </imple:> </imple:> </imple:> </header></request></ica></ica></pre>	~
The sha1 hash result:	
86E7 1FC5 157C 01BD 18F6 DBCB BA12 00A4 7A41 C458	
Sign by the certificate: C=CZ, CN=Pavel Novák, O="První certifikační autorita, a.s.", SERIALNUMBER=ICA - 10015368	
Do you wish to perform this action? Yes No Canc	el

Please sign the a request.

When a request for subsequent certificate type TWINS, it is necessary to sign the both the request - for qualified and commercial certificate.

This view is correct sending your request:



4. 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	Chrome version 44.0, 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	\times			
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 you internet experience come to life.	ır			
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 >				





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





5. 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>