Generating a request for a certificate
User Guide for browser Internet Explorer

První certifikační autorita, a.s.

Version 8.15

Contents

1. Introduction

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

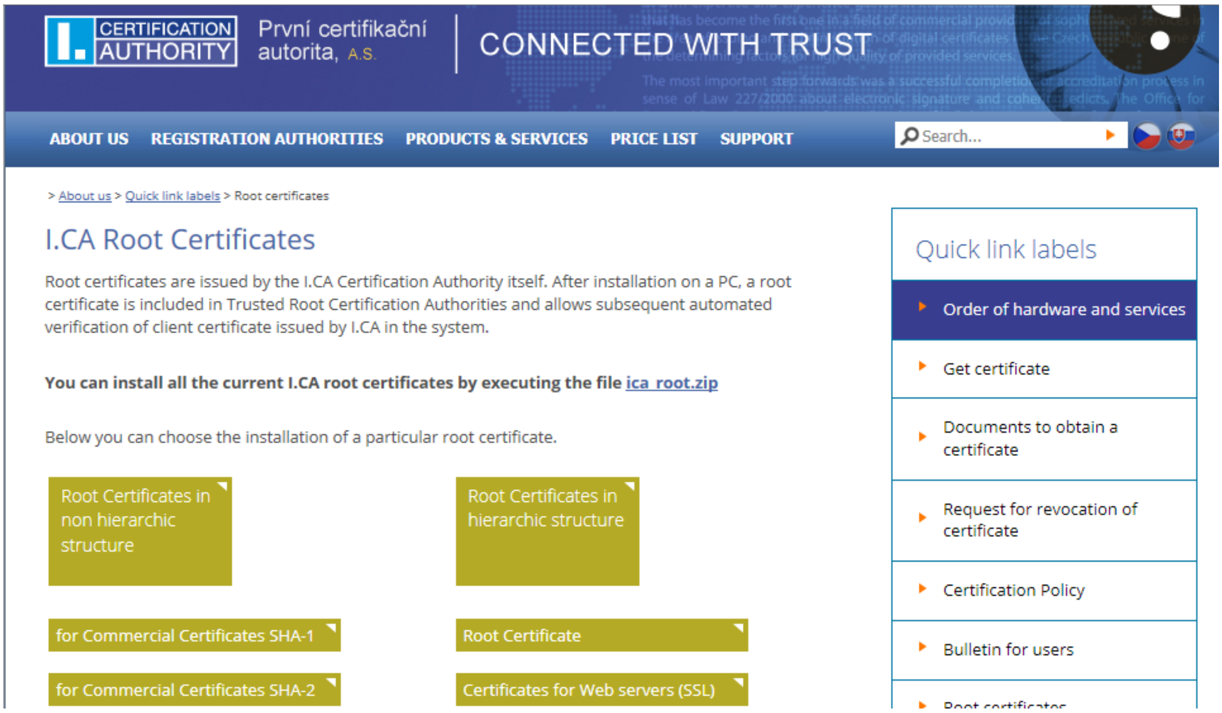
2. Software Requirements

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 **Internet Explorer** version 8.0 – 11.0
- 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: http://www.ica.cz/Root-certificate



> About us > Quick link labels > Root certificates

I.CA Root Certificates

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.

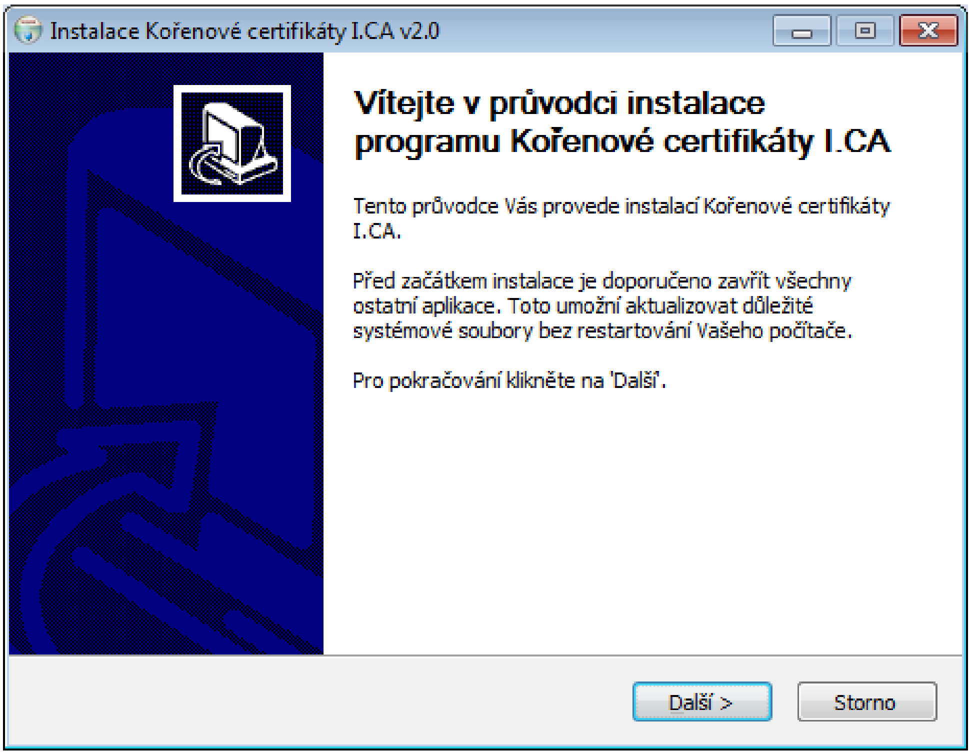
You can install all the current I.CA root certificates by executing the file ica_root.zip

Below you can choose the installation of a particular root certificate.

Root Certificates in non hierarchic structure
Root Certificates in hierarchic structure
for Commercial Certificates SHA-1
Root Certificate
for Commercial Certificates SHA-2
Certificates for Web servers (SSL)
Quick link labels
Order of hardware and services
Get certificate
Documents to obtain a certificate
Request for revocation of certificate
Certification Policy
Bulletin for users
Root certificates

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.



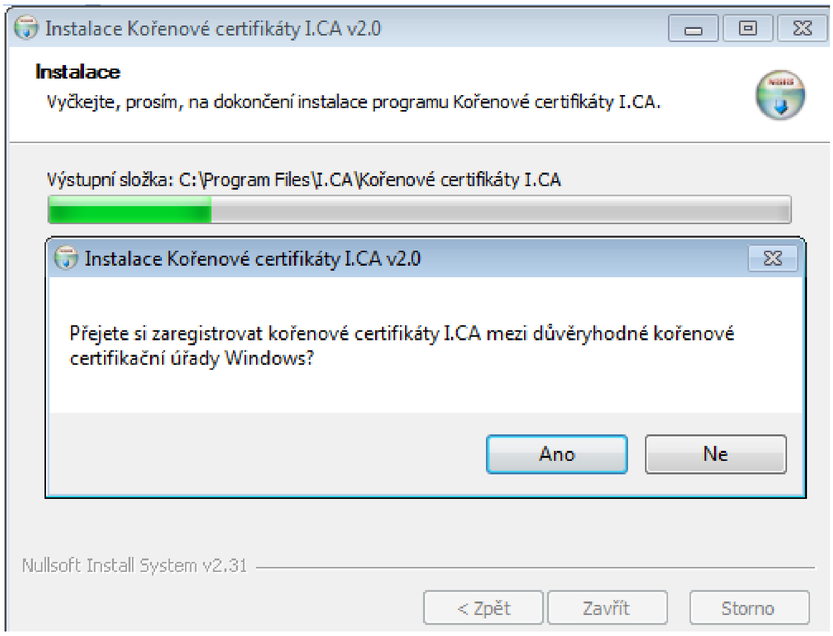
Vítejte v průvodci instalace programu Kořenové certifikáty I.CA

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'.

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



Instalace Kořenové certifikáty I.CA v2.0

Instalace

Vyčkejte, prosím, na dokončení instalace programu Kořenové certifikáty I.CA.

Výstupní složka: C:\Program Files\I.CA\Kořenové certifikáty I.CA

Instalace Kořenové certifikáty I.CA v2.0

Přejete si zaregistrovat kořenové certifikáty I.CA mezi důvěryhodné kořenové certifikační úřady Windows?

4. The process of generating a request for a certificate

Creating the request choose after selecting the type of certificate here http://www.ica.cz/Certificate

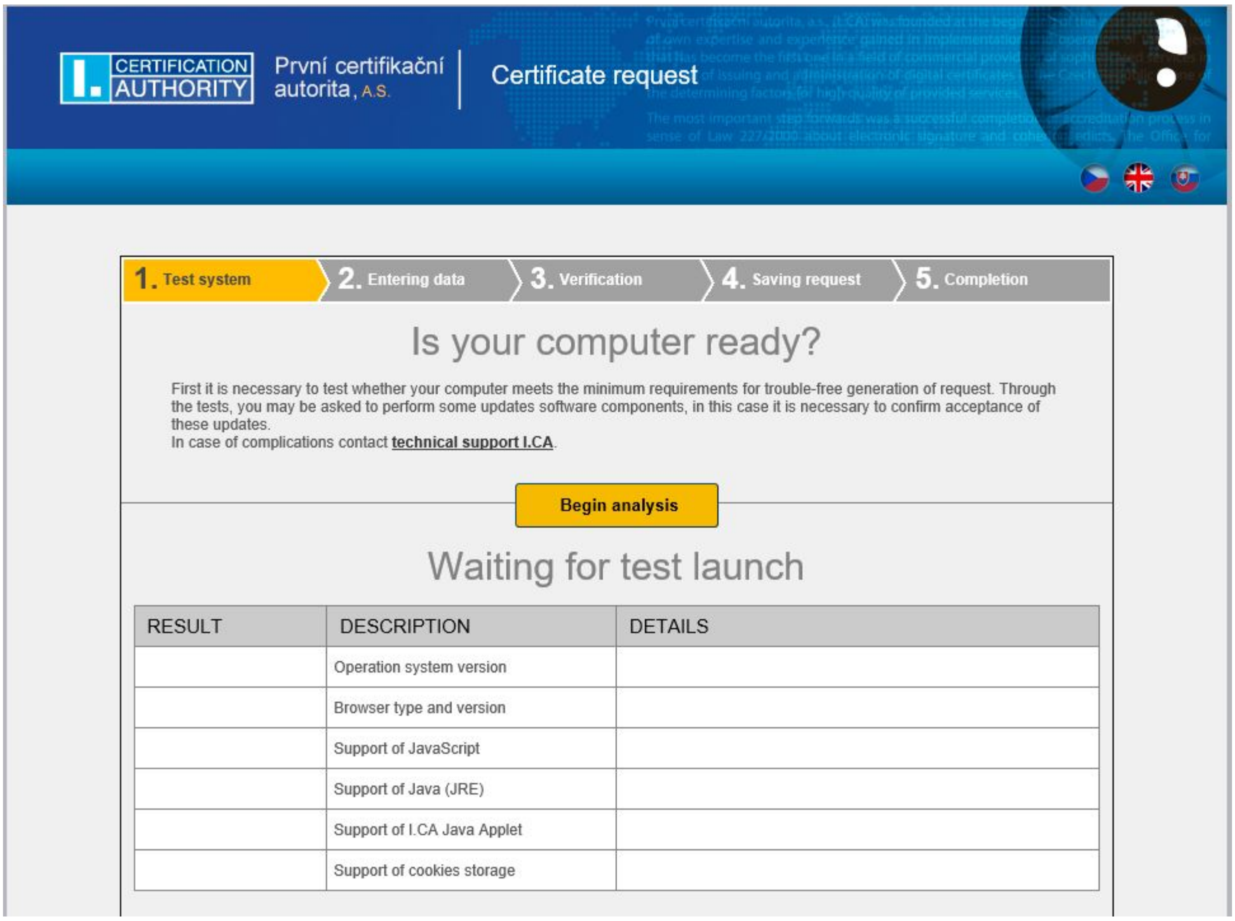
Process generace a request for initial certificate:

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

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.



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

Is your computer ready?

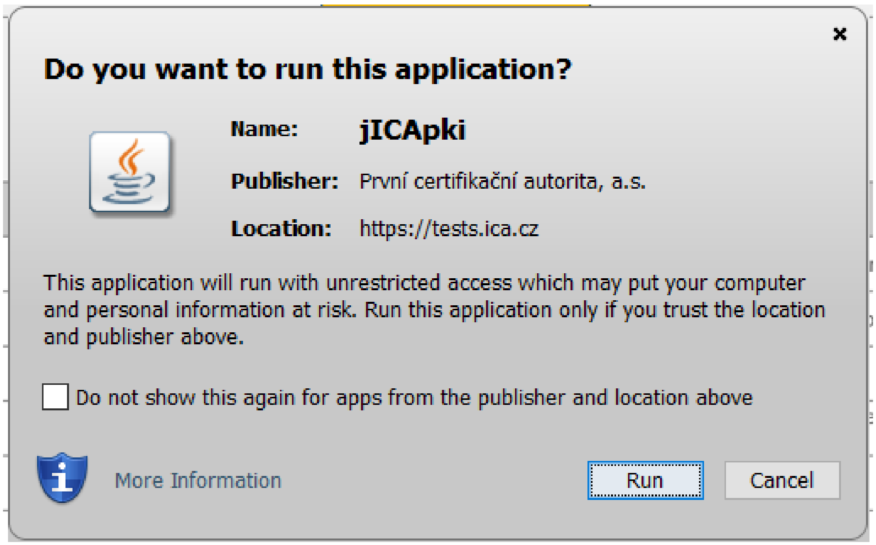
First it is necessary to test whether your computer meets the minimum requirements for trouble-free generation of request. Through the tests, you may be asked to perform some updates software components, in this case it is necessary to confirm acceptance of these updates.
In case of complications contact **technical support I.CA**.

Begin analysis

Waiting for 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	

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 you want to run this application?

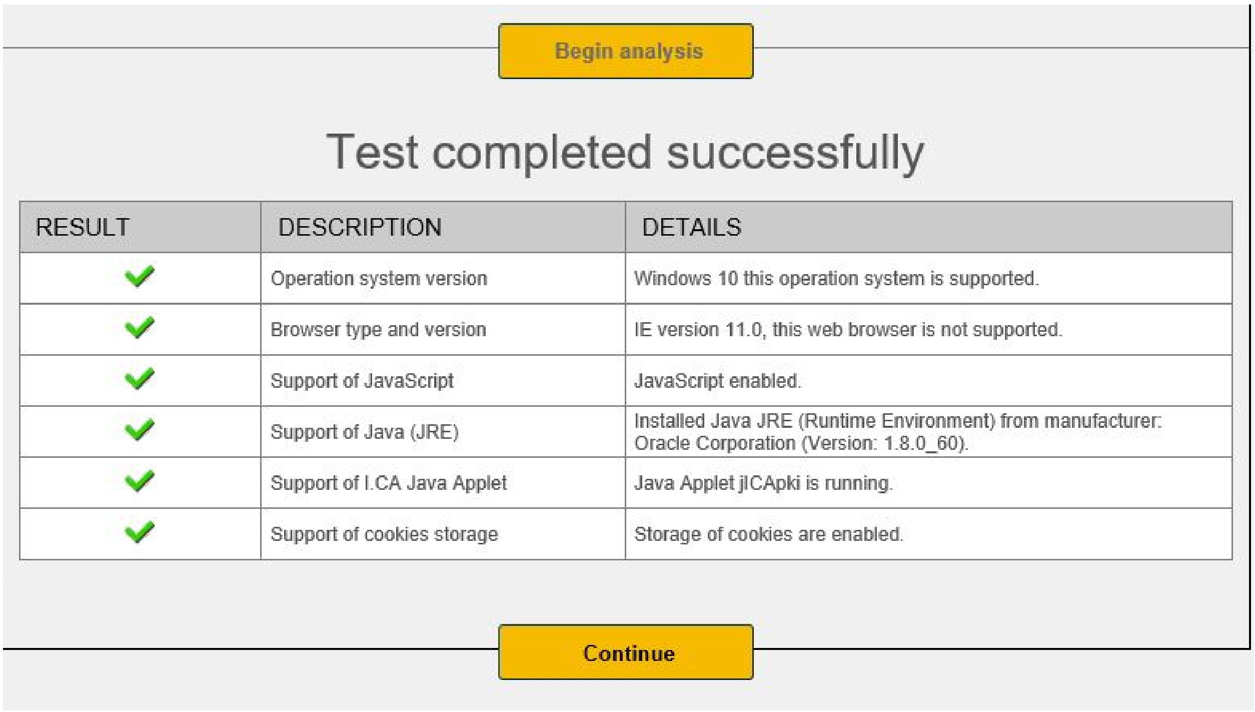
Name: jICApki

Publisher: První certifikační autorita, a.s.

Location: https://tests.ica.cz

This application will run with unrestricted access which may put your computer and personal information at risk. Run this application only if you trust the location and publisher above.

□ Do not show this again for apps from the publisher and location above



Test completed successfully

RESULT	DESCRIPTION	DETAILS
✓	Operation system version	Windows 10 this operation system is supported.
✓	Browser type and version	IE version 11.0, 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_60).
✓	Support of I.CA Java Applet	Java Applet jICApki 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.

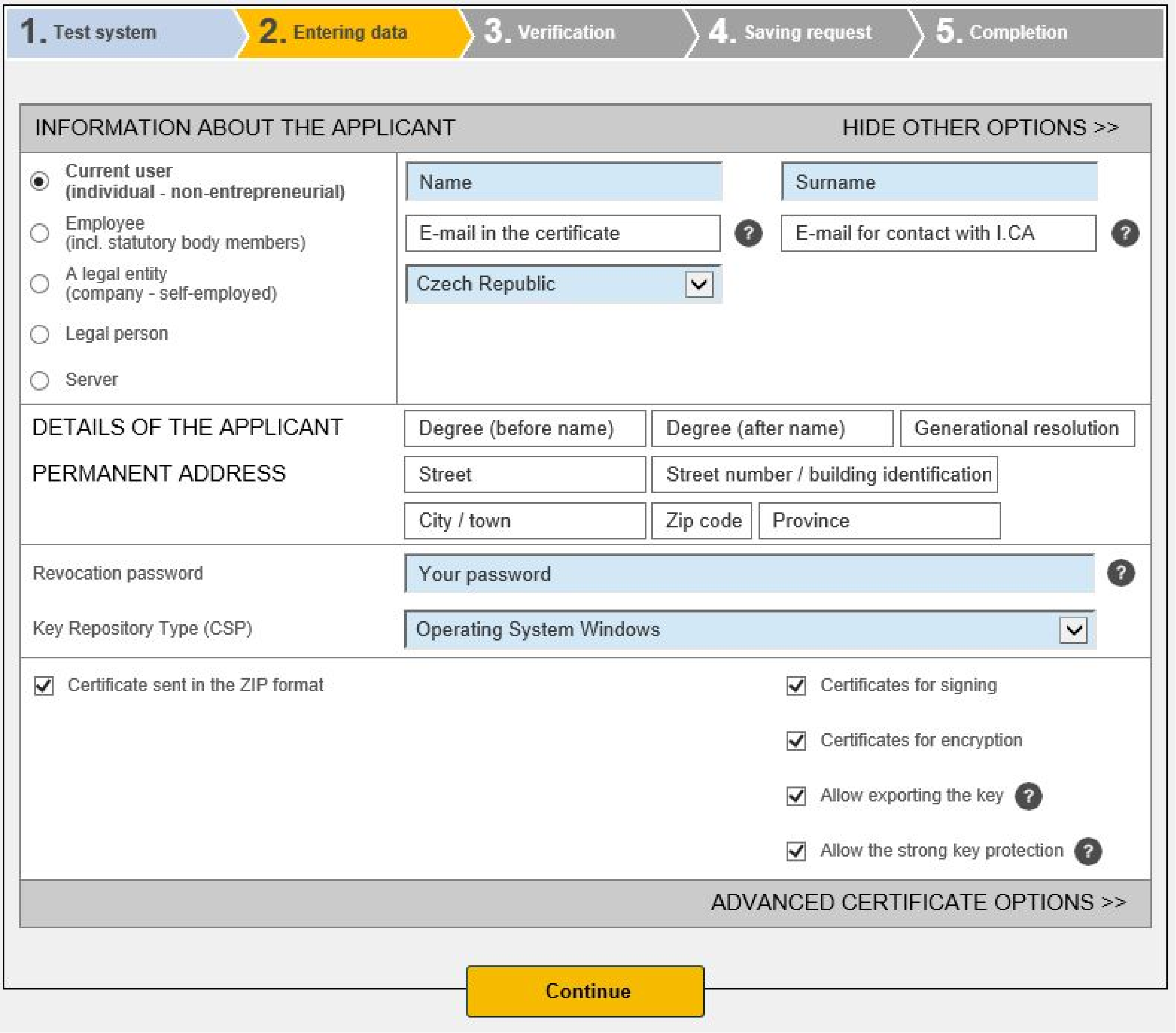
Installing the JRE is described in Chapter 6.

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.



INFORMATION ABOUT THE APPLICANT HIDE OTHER OPTIONS >>

● Current user (individual - non-entrepreneurial)
○ Employee (incl. statutory body members)
○ A legal entity (company - self-employed)
○ Legal person
○ Server

Name | Surname
E-mail in the certificate ? | E-mail for contact with I.CA ?
Czech Republic

DETAILS OF THE APPLICANT: Degree (before name) | Degree (after name) | Generational resolution

PERMANENT ADDRESS: Street | Street number / building identification | City / town | Zip code | Province

Revocation password: Your password ?

Key Repository Type (CSP): Operating System Windows

☑ Certificate sent in the ZIP format

☑ Certificates for signing
☑ Certificates for encryption
☑ Allow exporting the key ?
☑ Allow the strong key protection ?

ADVANCED CERTIFICATE OPTIONS >>

Continue

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:

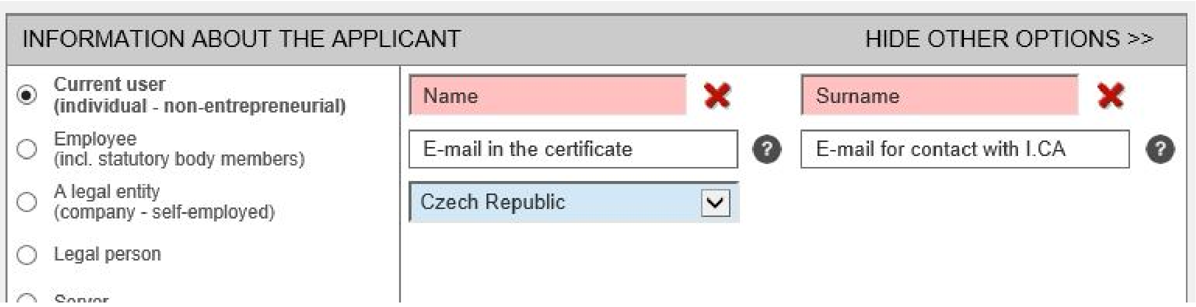
If the selected storage type keys (CSP) supports export the private key, you are given the option to enable export the private key. This option allows to export the certificate including private key. The private key so you will be able to transfer between storage. Key management requires in this case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

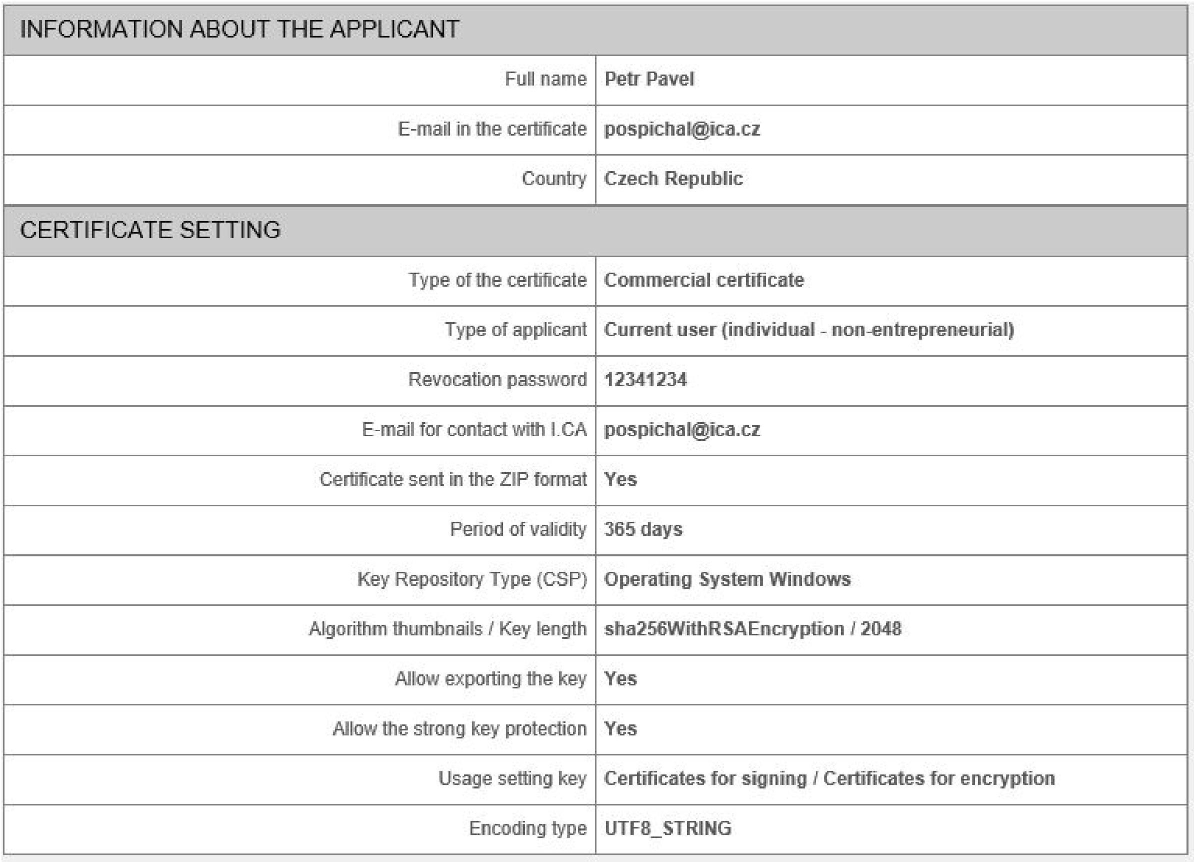


● Current user (individual - non-entrepreneurial)
○ Employee (incl. statutory body members)
○ A legal entity (company - self-employed)
○ Legal person
○ Server

Name ✖
Surname ✖
E-mail in the certificate ?
E-mail for contact with I.CA ?
Czech Republic

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

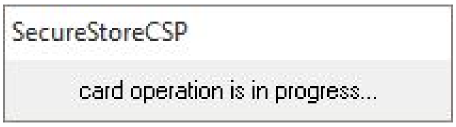
To the repair it is possible to go one step back. Click the **Continue** button to begin the creation of the private key

4.4. Generating a certificate request

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

4.4.1. SecureStoreCSP – smart card I.CA

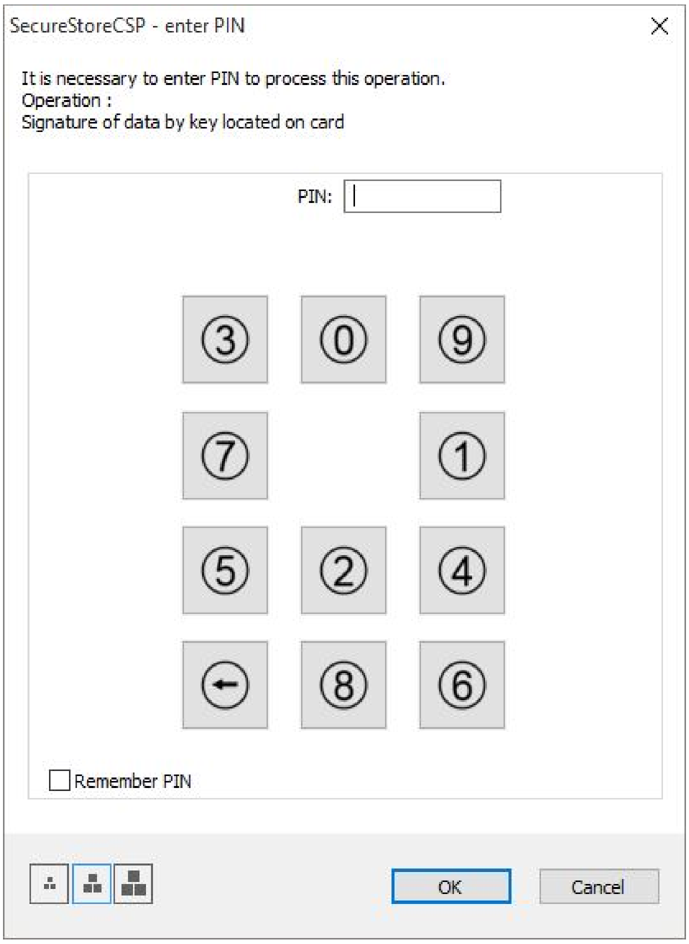
Displayed you will the following dialog, now generating your private key. Creating a private key may take several tens of seconds.



SecureStoreCSP

card operation is in progress...

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



SecureStoreCSP - enter PIN

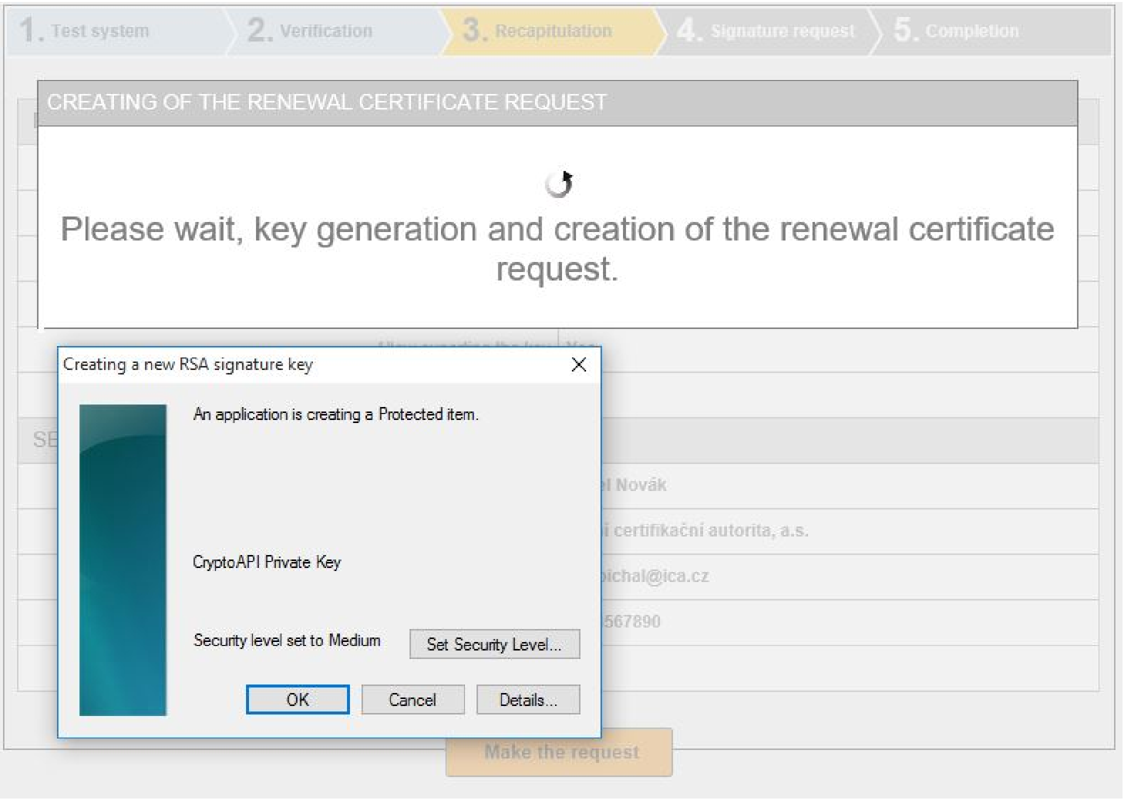
It is necessary to enter PIN to process this operation.
Operation :
Signature of data by key located on card

PIN:

□ Remember PIN

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:



CREATING OF THE RENEWAL CERTIFICATE REQUEST

Please wait, key generation and creation of the renewal certificate request.

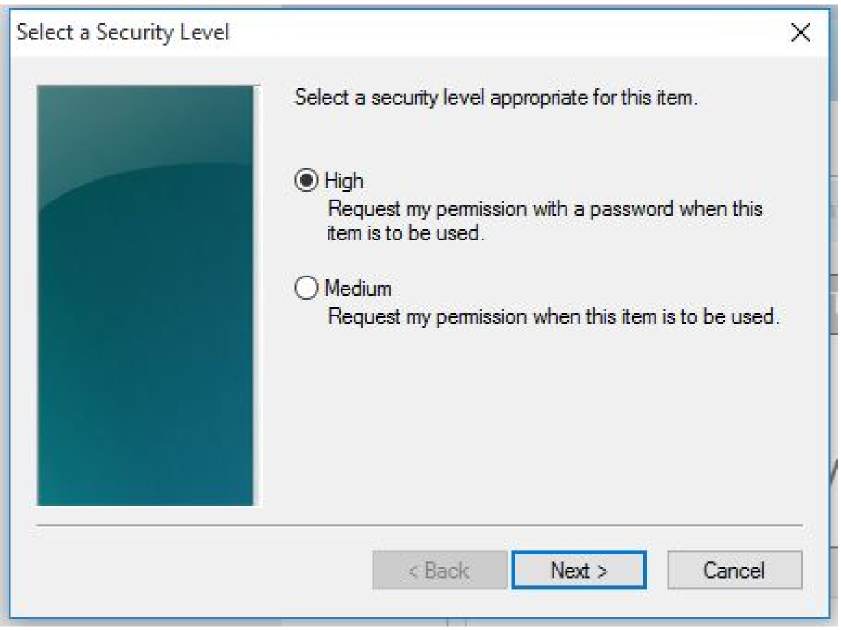
Creating a new RSA signature key

An application is creating a Protected item.

CryptoAPI Private Key

Security level set to Medium

Choose Select a security level appropriate for this item:



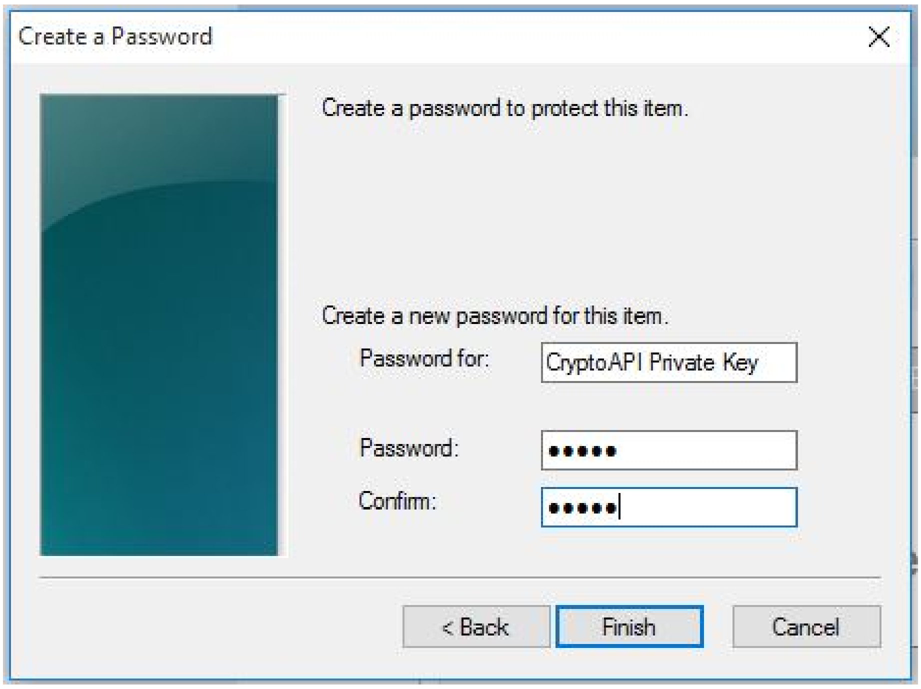
Select a Security Level

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.

High = It must enter the password.



Create a Password

Create a password to protect this item.

Create a new password for this item.

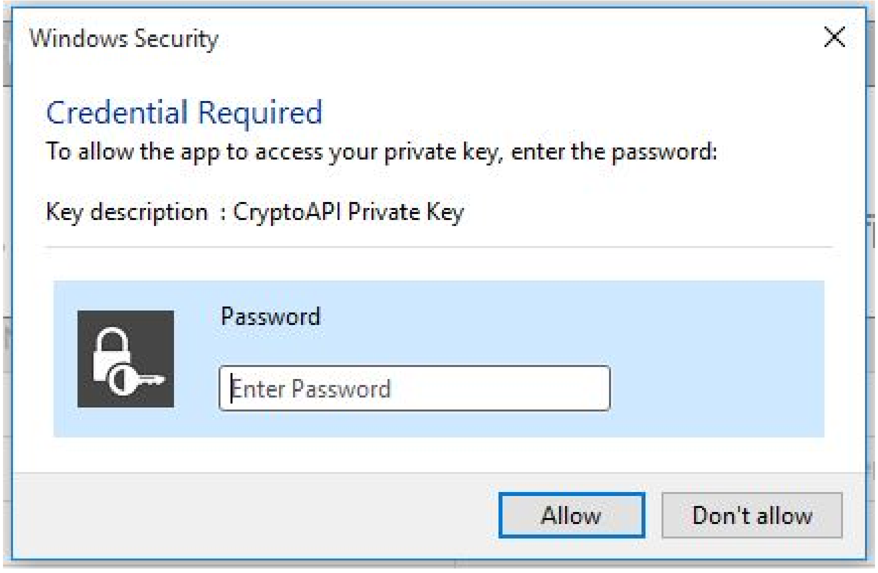
Password for: CryptoAPI Private Key

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.



Windows Security

Credential Required

To allow the app to access your private key, enter the password:

Key description : CryptoAPI Private Key

Password

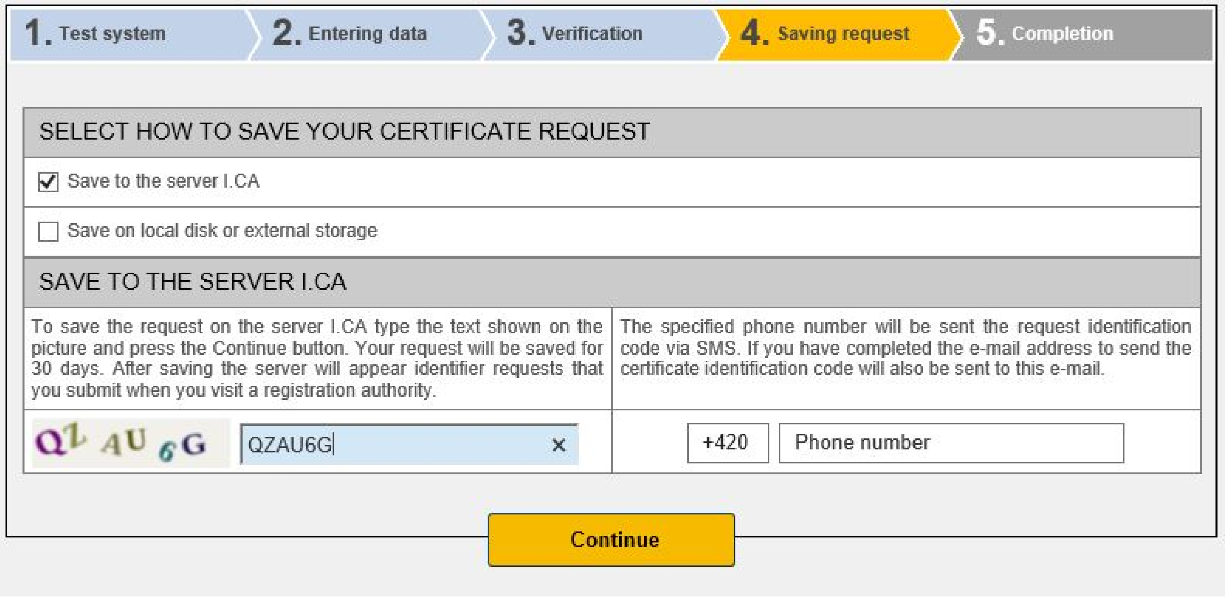
Enter Password

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.



SELECT HOW TO SAVE YOUR CERTIFICATE REQUEST

☑ Save to the server I.CA

□ Save on local disk or external storage

SAVE TO THE SERVER I.CA

To save the request on the server I.CA 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 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.

QZAU6G

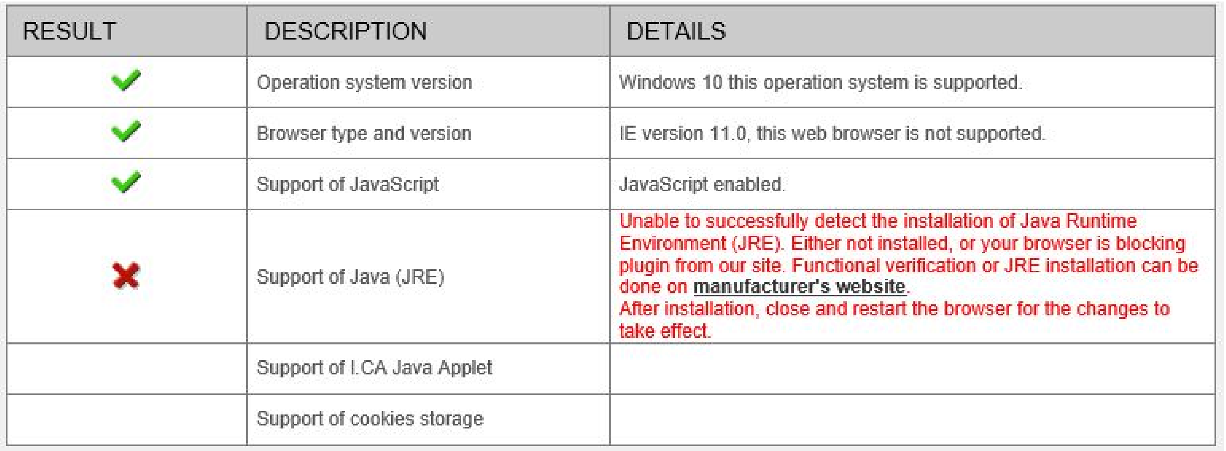
+420 Phone number

5. Issuance certificate

After creating the certificate request, you must personally visit the registration authority I.CA - list here http://www.ica.cz/Registration-Authorities-HQ. 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 http://www.ica.cz/Documents-qualified-certificate.

6. Installation Java Runtime Environment (JRE)

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

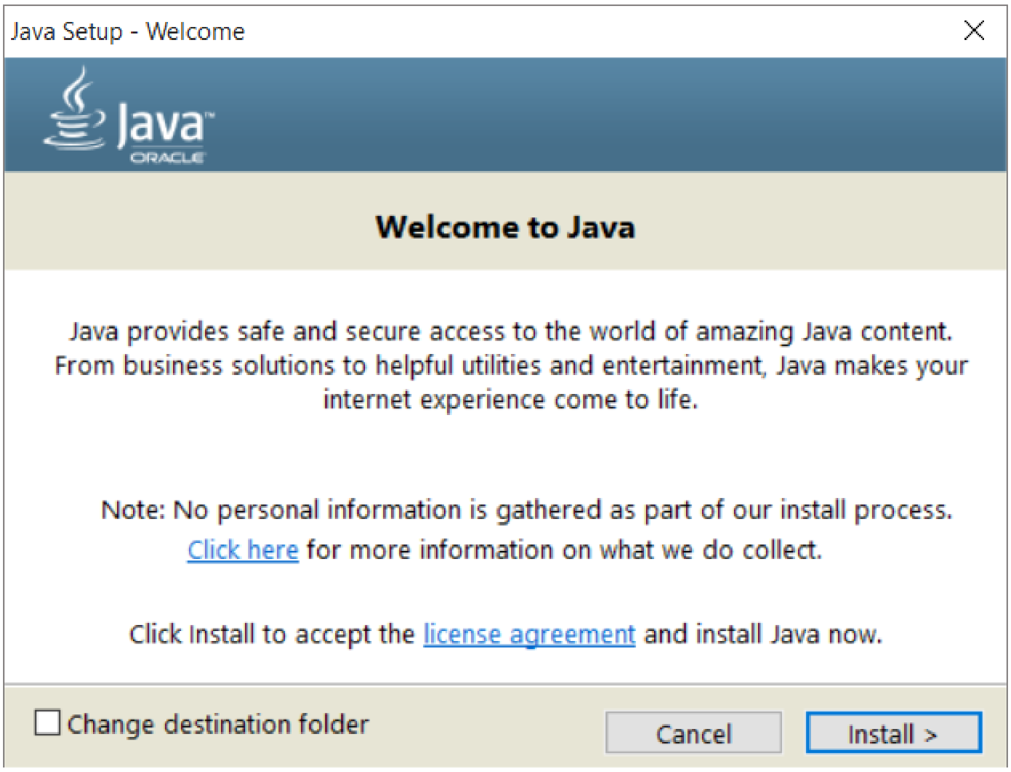


RESULT	DESCRIPTION	DETAILS
✓	Operation system version	Windows 10 this operation system is supported.
✓	Browser type and version	IE version 11.0, this web browser is not supported.
✓	Support of JavaScript	JavaScript enabled.
✗	Support of Java (JRE)	Unable to successfully detect the installation of Java Runtime Environment (JRE). Either not installed, or your browser is blocking plugin from our site. Functional verification or JRE installation can be done on manufacturer's website. 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: https://java.com/en/download/index.jsp. 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

Welcome to Java

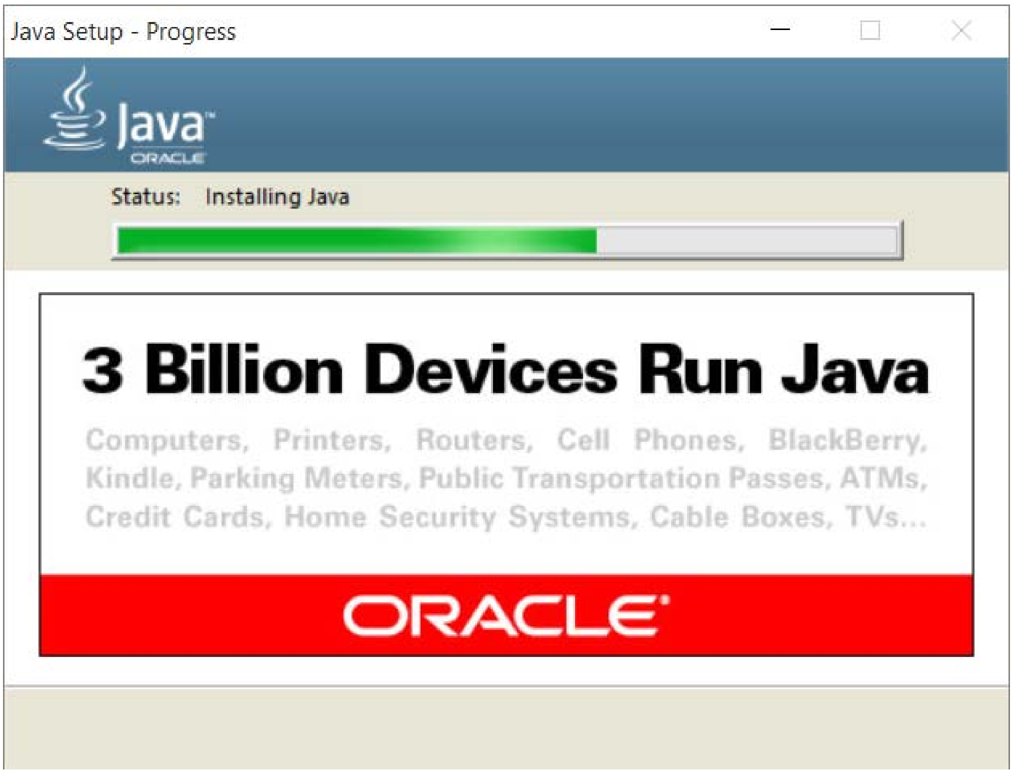
Java provides safe and secure access to the world of amazing Java content. From business solutions to helpful utilities and entertainment, Java makes your internet experience come to life.

Note: No personal information is gathered as part of our install process. Click here for more information on what we do collect.

Click Install to accept the license agreement and install Java now.

□ Change destination folder

Java
ORACLE
Cancel
Install >

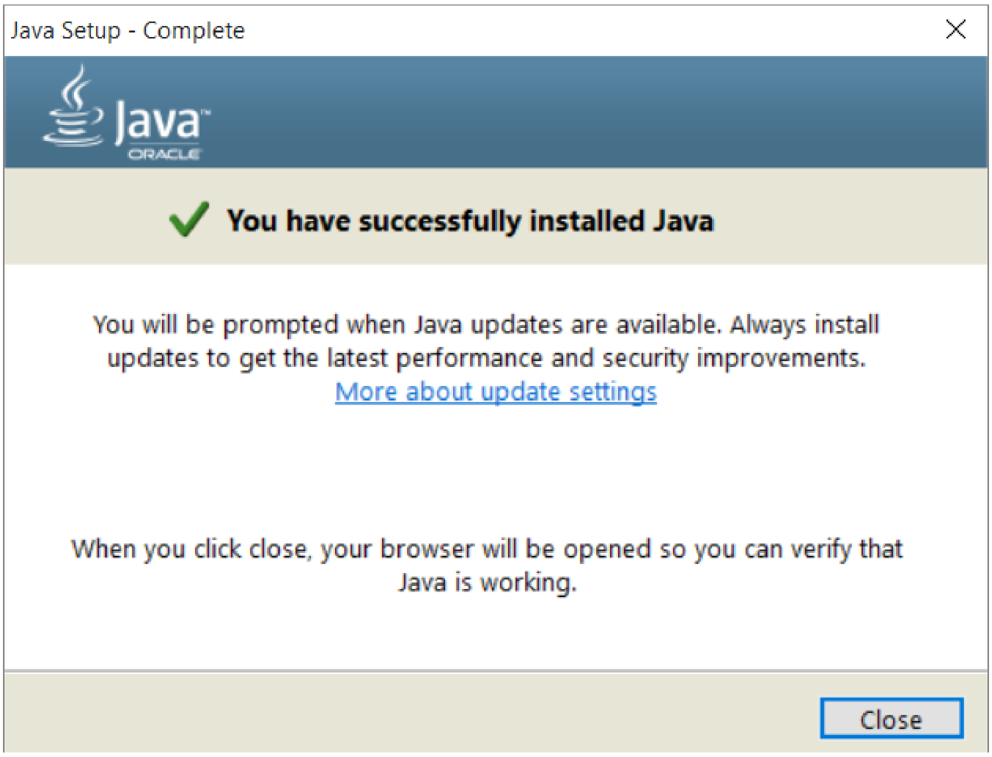


Java Setup - Progress

Status: Installing Java

Java
ORACLE
3 Billion Devices Run Java
Computers, Printers, Routers, Cell Phones, BlackBerry, Kindle, Parking Meters, Public Transportation Passes, ATMs, Credit Cards, Home Security Systems, Cable Boxes, TVs...
ORACLE

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



Java Setup - Complete

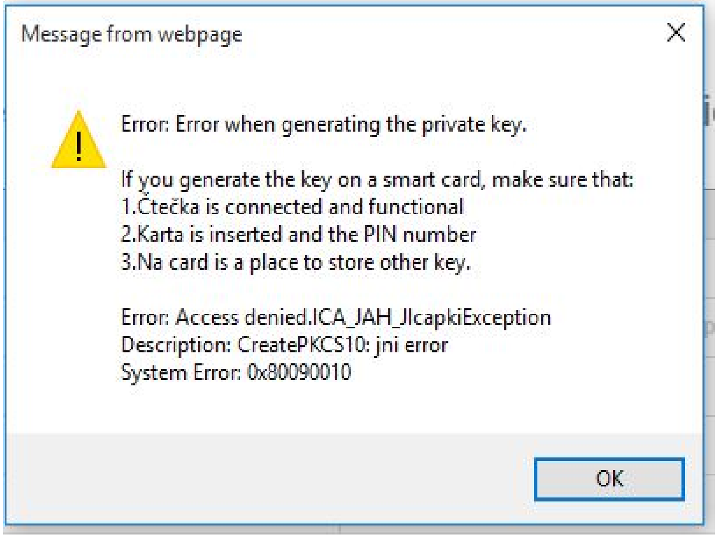
✓ You have successfully installed Java

You will be prompted when Java updates are available. Always install updates to get the latest performance and security improvements.
More about update settings

When you click close, your browser will be opened so you can verify that Java is working.

7. Troubleshooting

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



Message from webpage

Error: Error when generating the private key.

If you generate the key on a smart card, make sure that:
1.Čtečka is connected and functional
2.Karta is inserted and the PIN number
3.Na card is a place to store other key.

Error: Access denied.ICA_JAH_JIcapkiException
Description: CreatePKCS10: jni error
System Error: 0x80090010

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 technical support I.CA.