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

První certifikační autorita, a.s.

Version 8.15

Contents

1. Introduction 3
2. Software Requirements 3
3. The process of generating a request for a subsequent certificate 3
   3.1. Control 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. Certificate selection for to create request for subsequent 5
   3.3. Additions and changes to some data 7
   3.4. Generating 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 key 9
   3.5. Signing and sending an a request for subsequent certificate 11
4. Installation Java Runtime Environment (JRE) 13
5. Troubleshooting 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
- 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

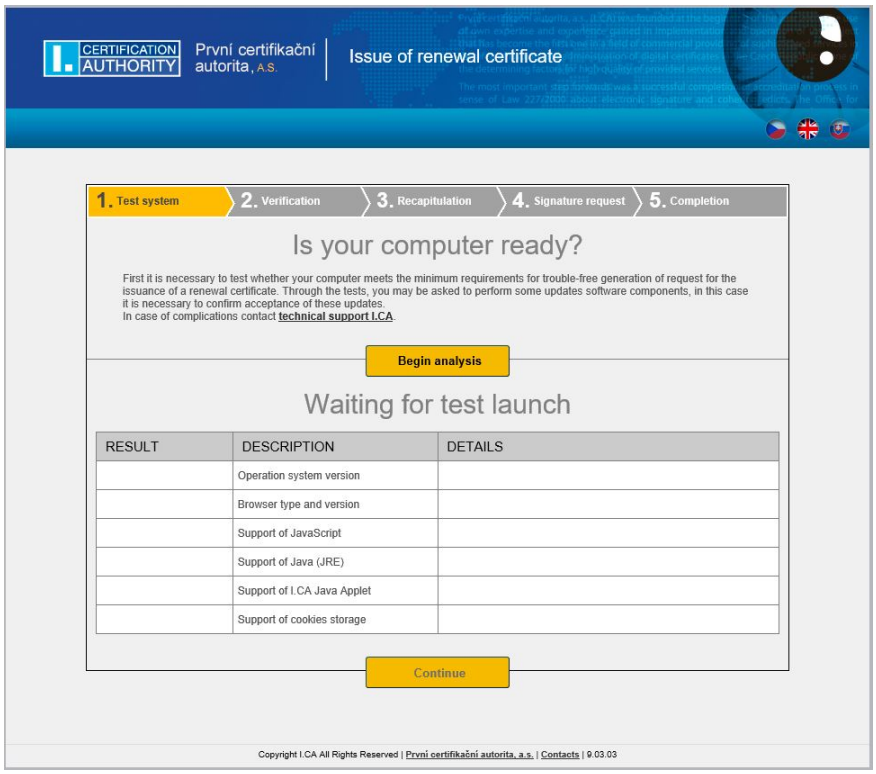
Process generace a request for initial certificate:

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

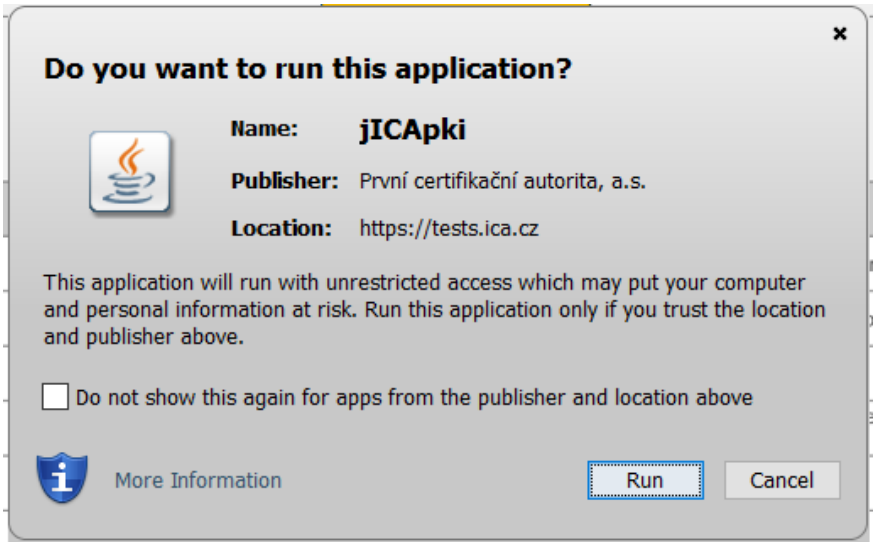
3.1. Control software

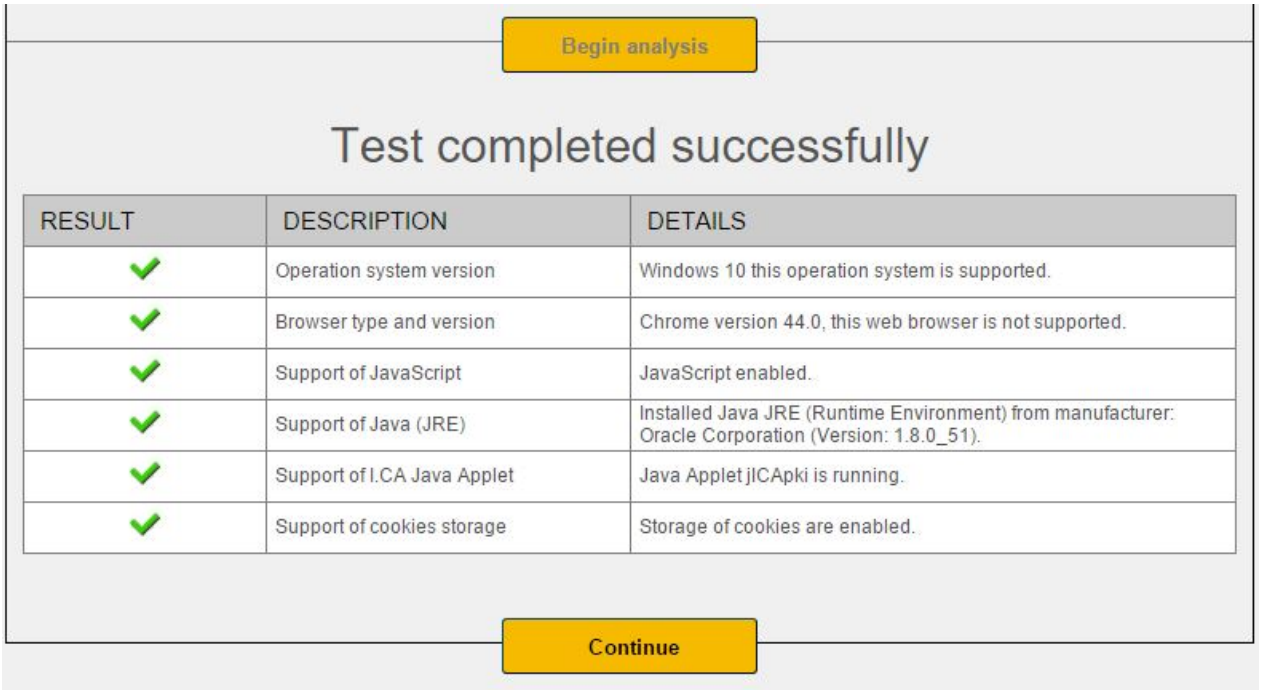
Before you start generating request must run the kontrol software components.

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



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.





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.

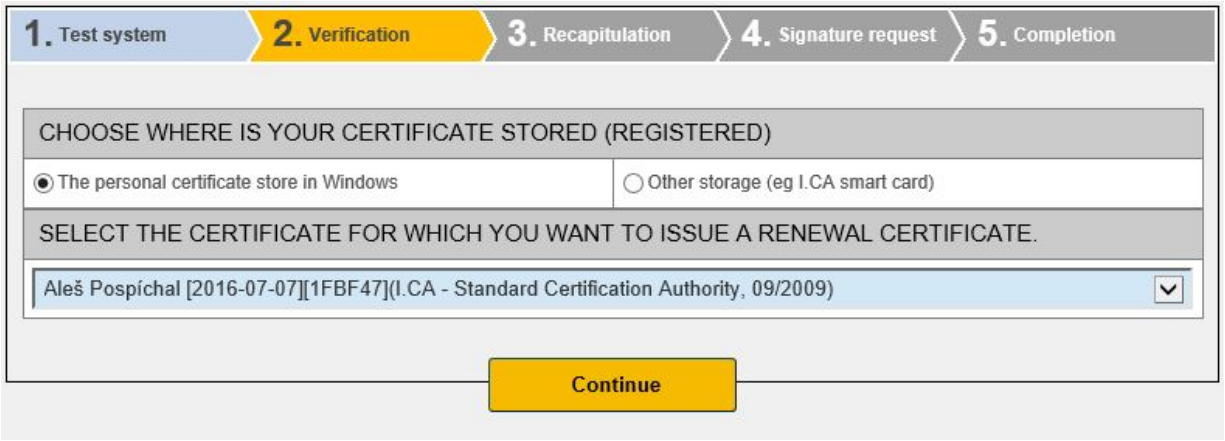
Installing the JRE is described in Chapter 6.

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.



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**.

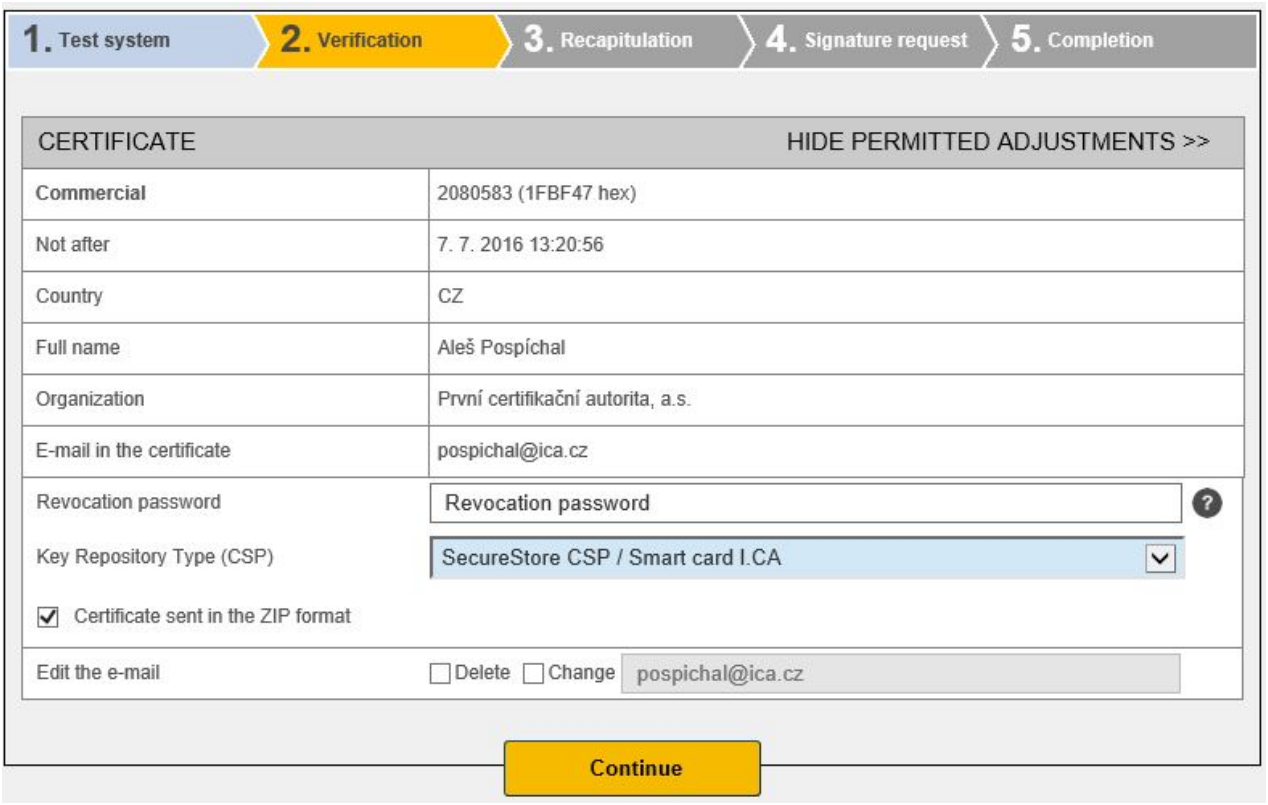
Of one's own choice your previous choice is presented with a list of certificates which may be issued subsequent certificate. If you selected **Other storage**, you must connected in smart card reader and insert a smart card (or token).

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.



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.

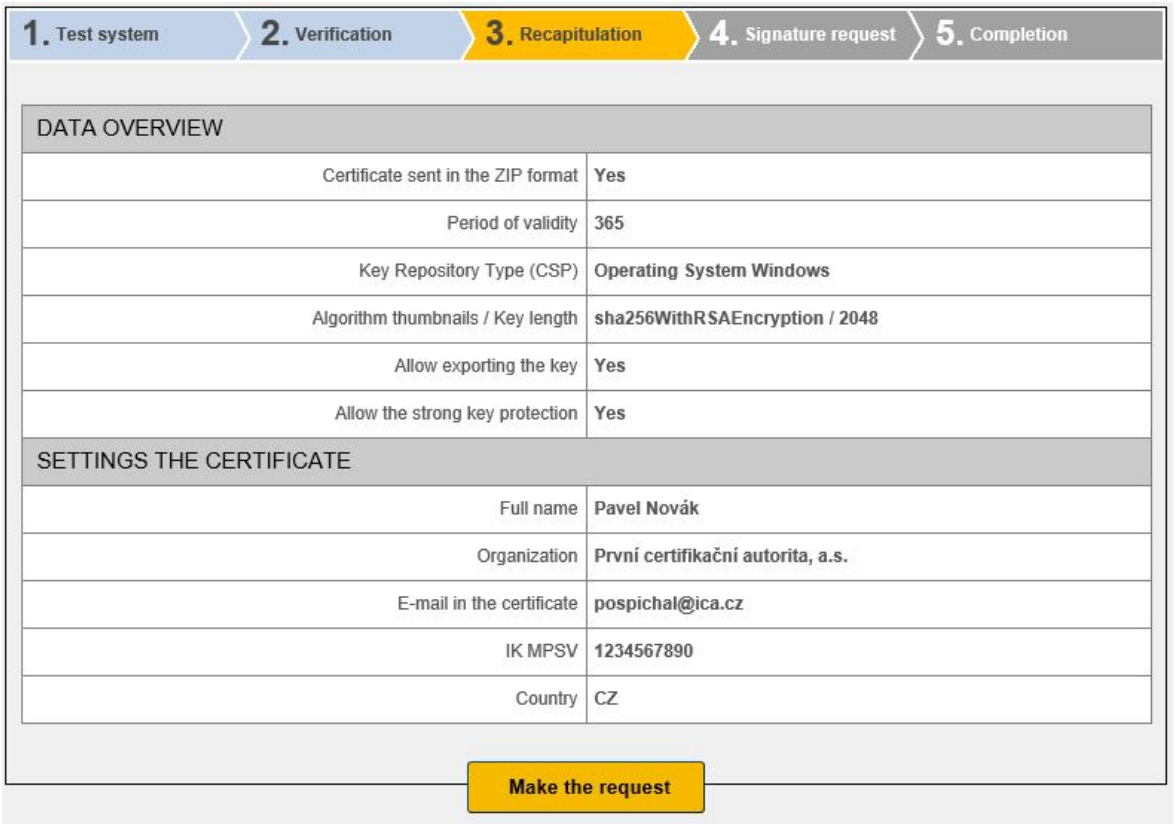
You can choose:
Middle - you always notice only informative report
Strong - before every use you will be required to enter your password

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.



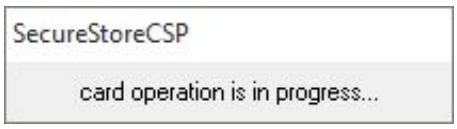
By clicking on **Make the request** to star creating a private key.

3.4. Generating a certificate request

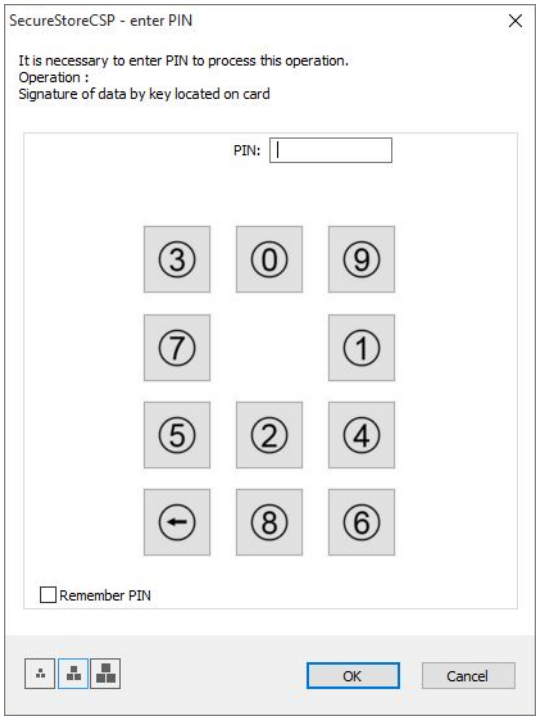
The procedures for different types of private key storage (CSP).

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.

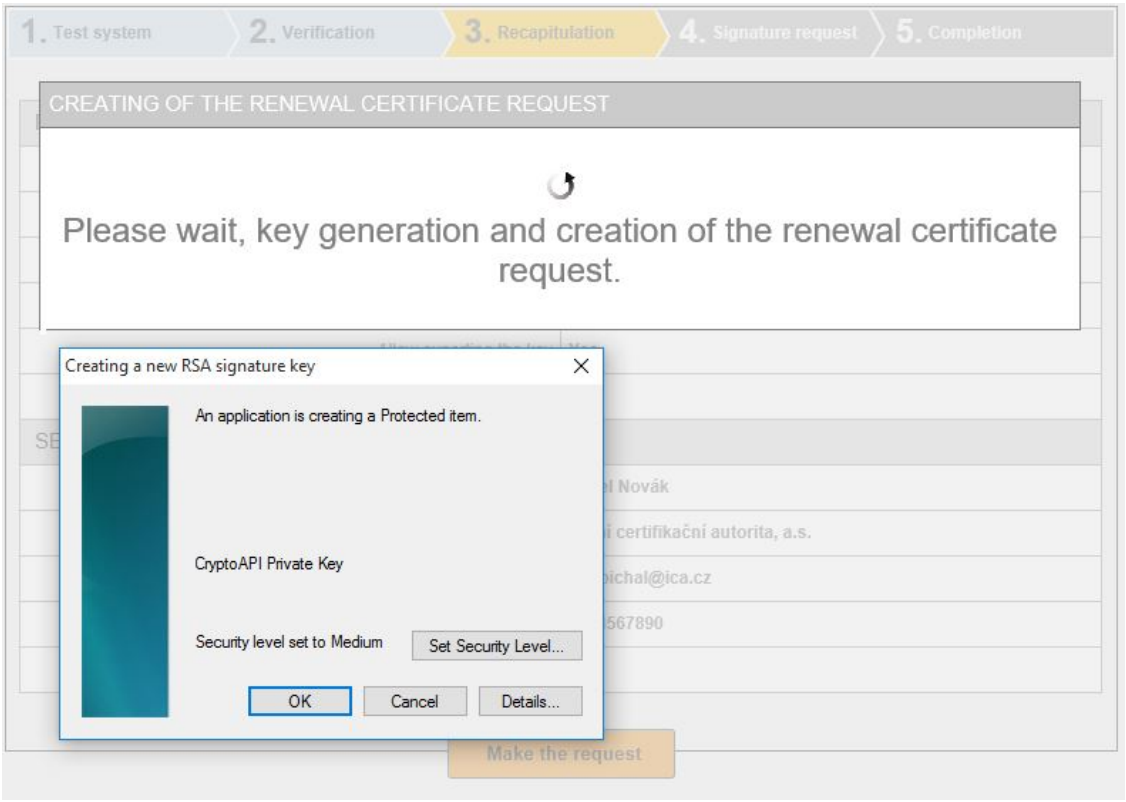


After creating the private key you're prompted to enter a PIN on your card.



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:



Choose Select a security level appropriate for this item:

High = It must enter the password.

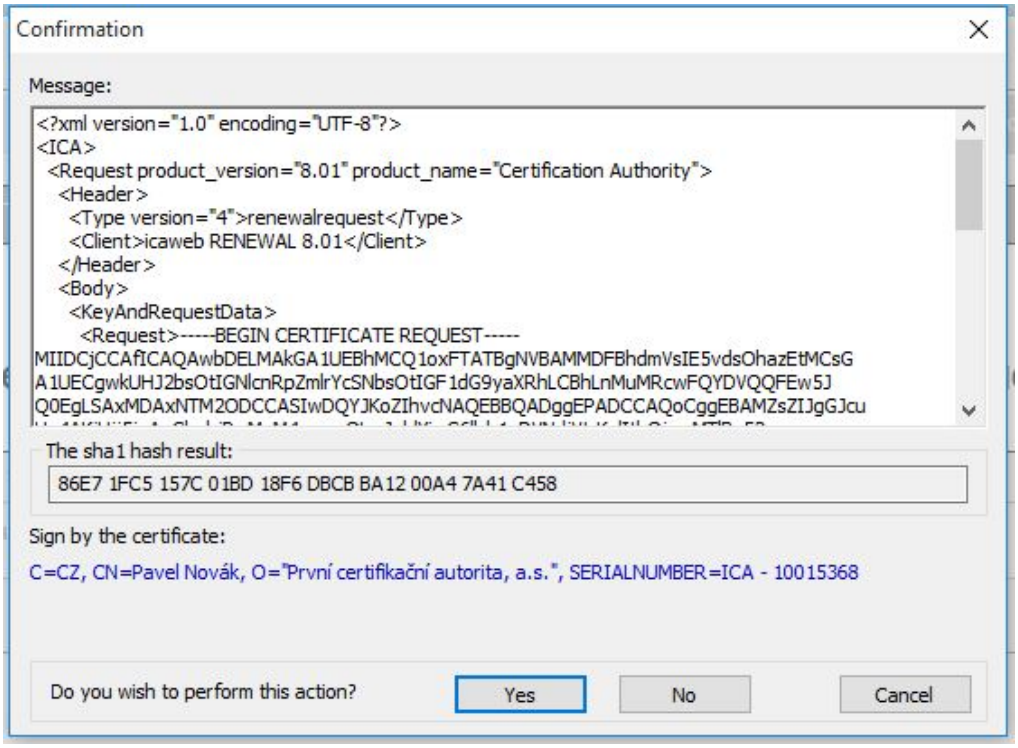
After click on the button **Finish** will change the security level. Now click on the button **OK**.

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

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.

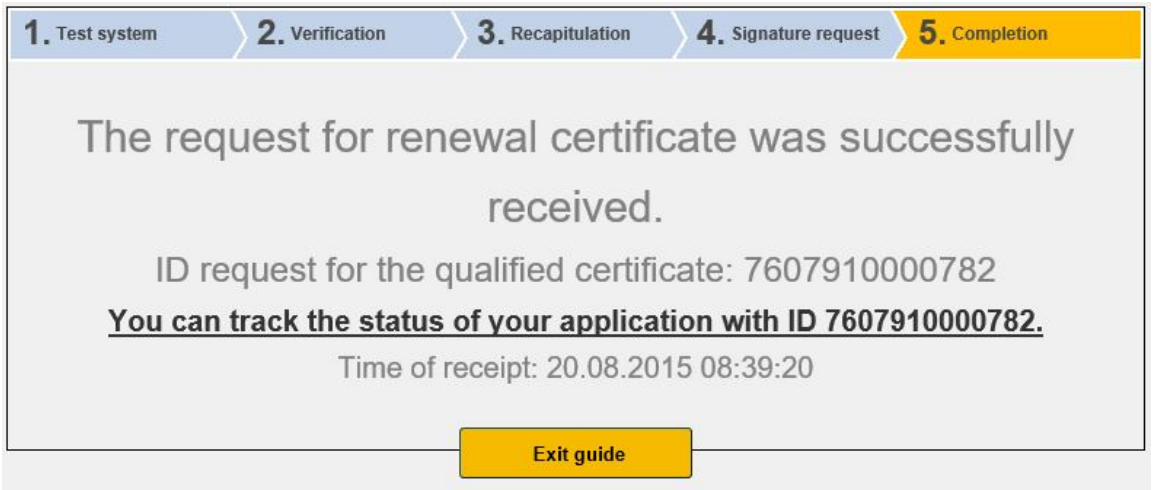
Once you click "Send a request processing" dialog is displayed, containing your request for subsequent certificate. This a request must be to signed a certificate to which you are requesting subsequent.



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)

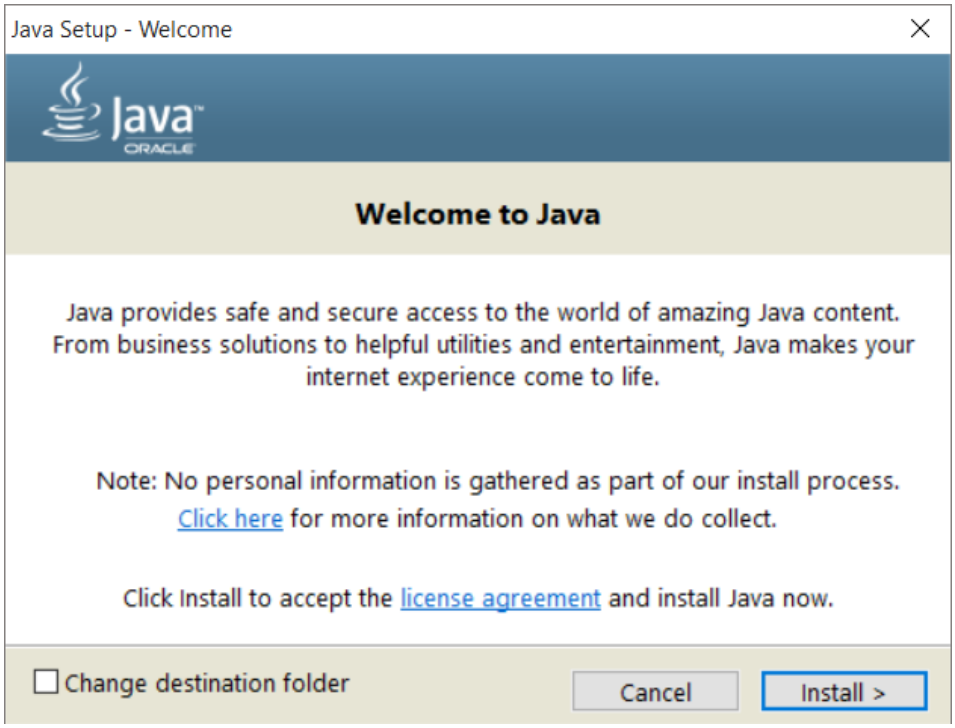
If the support for "Java Runtime Environment" not installed, you will be prompted to install.

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 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.

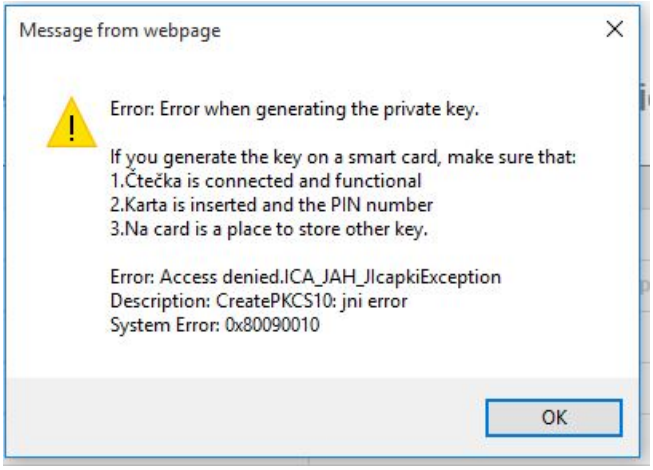
Select button **Install** follow the installation wizard.



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 technical support I.CA.