

# Generating a request for an initial certificate

## Contents

1.	Introduction.....	2
2.	Software Requirements.....	2
3.	The process of generating a request for an initial certificate .....	2
2.1	Selecting a certificate .....	3
2.2	System Test .....	4
2.3	Entering Data.....	5
2.4	Verification .....	6
2.5	Saving Request .....	7
2.6	Completion .....	7

## 1. Introduction

This document serves as a guide on how to proceed when generating an initial certificate request through the website.

## 2. Software Requirements

The computer on which the certificate request will be generated must meet the following requirements:

### 2.1. installed and running operating system

- Windows 7 ServicePack 1
- Windows 8.1 (April 2014 update)
- Windows 10
- Windows 11

### 2.2. The 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 PKIService host component and extension installed

### 2.5. I.CA SecureStore Card Manager (only when generating a request for a smart card)

### 2.6. eObčanka - Card Manager (only in the case of generating an application for an ID card)

## 3. The process of generating a request for an initial certificate

The procedure for generating a request for an initial certificate is divided into several steps:

1. **Selecting a certificate**
2. **System Test**
3. **Entering Data**
4. **Verification**
5. **Saving Request**

## 2.1 Selecting a certificate

To create an application, select the certificate type here: [I.CA | Commercial and qualified certificates](#) or choose your certificate here: [I.CA | Products \(ica.cz\)](#).

### Obtaining a request for a certificate

Step 1: For whom the certificate is intended? Select the option you are interested in:

personal	employee or self-employed person	company or government institution
----------	----------------------------------	-----------------------------------

Natural person (Personal) - if you choose this option, your certificate will contain your name and surname, optionally it is also possible to state your residence and e-mail address.

Employee or self-employed person - it is intended for those who, in addition to their name and surname, also need to state the name of company/trade or employer in the certificate. You can also use it if you are a company executive.

Company or government institution - if you need a certificate for your company, government institution, or other legal entity, select this option. The certificate will contain the name of the subject and optionally also its registered office.

- Personal – only the applicant's **first and last name** will appear on the certificate. Not the organisation.
- Employee or self-employed person - the certificate will include the **name, surname and the organisation** for which the applicant is acting.
- legal entity or authority - this is mainly an electronic seal or commercial technology certificate. The certificate does not contain the name of the applicant. Only the **organisation** is mentioned.

In the next step, select the certificate you are requesting (for example, a Qualified Certificate for Electronic Signature) and check the box: "will be stored on your computer". Then press the "**Get**" button at the bottom.

If you are requesting a certificate that is **stored on a smart card**, you must have a smart card connected to your computer. If you don't 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 you a certificate.

If you apply for a certificate with **saving on your ID card**, you need to have the eObčanka - Card Manager application installed and your ID card connected to a computer that has a PIN and QPIN set.

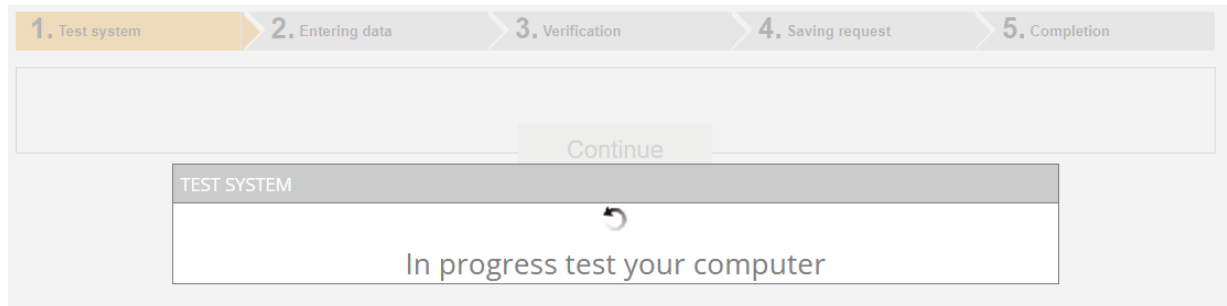
Step 2: select the option you are interested in ([Back to step 1](#))

**Qualified certificate for electronic signature**  
used to sign documents. It is used where a recognized electronic signature is required.

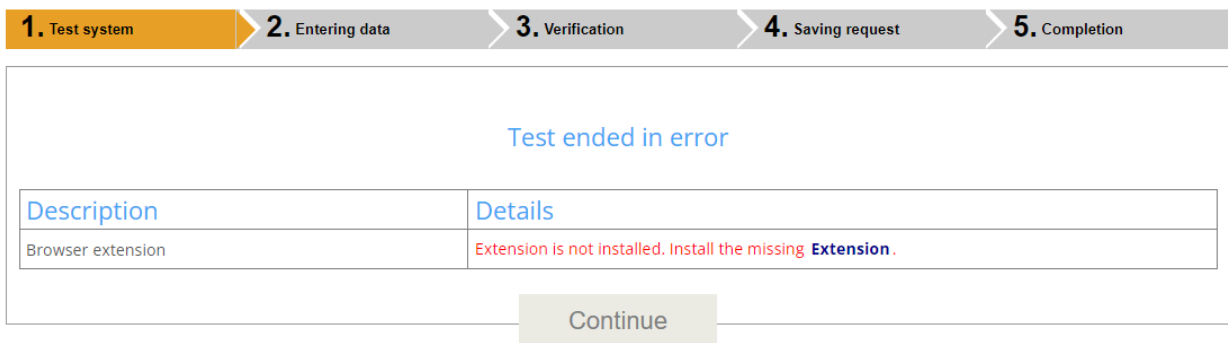
- will be stored on your computer
- will be stored on the smart card
- will be stored in the ID card

## 2.2 System Test

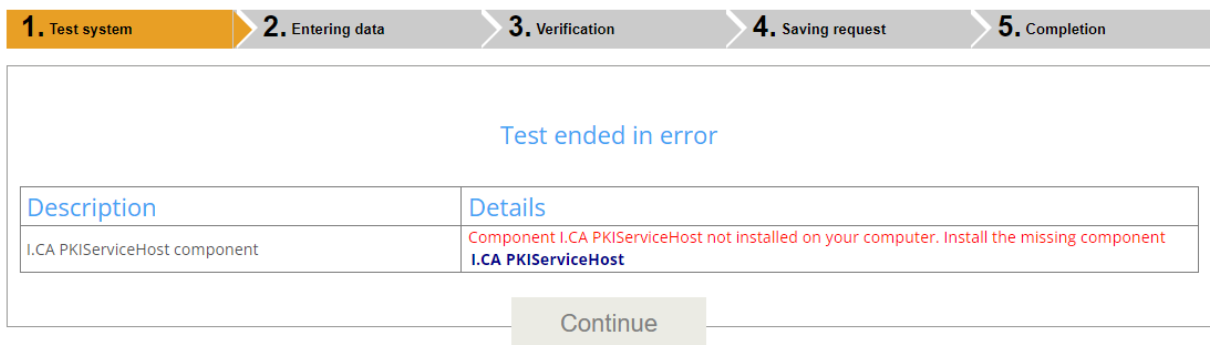
To make it easier to check if your computer is ready to generate a request, a check page is displayed when you start generating the request to verify that key software components are present.



If the component and the **I.CA PKIService Host** extension are absent, an error message appears, see below.



Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00



Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

Click on the highlighted **I.CA PKIServiceHost** and **Extension** to install the necessary components on the PC to generate the request. After successful installation, restart the browser.

If you have a certificate stored on your smart card, you may receive an error for the **SecureStore** application you download and install.

The page will test the computer, if no problems are detected, it will automatically proceed to the actual creation of the certificate request.

## 2.3 Entering Data

Fill in the details here. We recommend leaving the checkbox settings here as they are set by default. Then press the "Continue" button.

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

Information about the applicant Show other options >>

Degree (before name)  Degree (after name)

First name  Surname  Czech Republic  ?

E-mail in the certificate  ? E-mail for contact with I.C.A.  ?

Insert optional identifier for individuals

Information about the organization Show other options >>

Organization  ? [Find organization >>](#)

Insert optional identifier for organization

Key type

Revocation password  ?

Key Repository Type (CSP)

Certificate containing IC MLSA for communication with the public authorities ?  Allow exporting the key ?

Certificate sent in the ZIP format  Allow the strong key protection ?

Save the request to the card

Advanced Certificate Options >>

Continue


## 2.4 Verification

On the verification tab, you need to check that the data you have entered is correct. You can then press the "Continue" button.

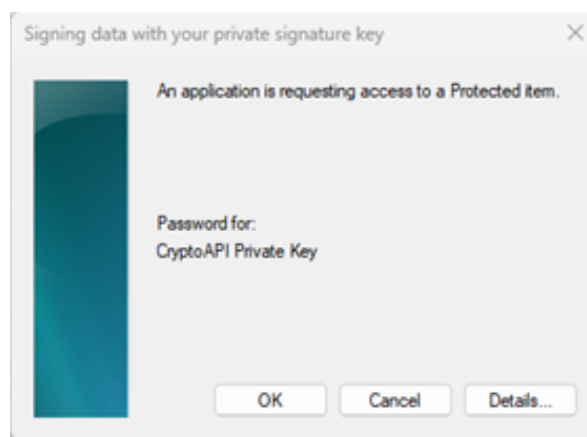
1. Test system   2. Entering data   3. Verification   4. Saving request   5. Completion

Information about the applicant	
Full name	First Name Surname
First name	First Name
Surname	Surname
Organization	I.CA
Country	Czech Republic
Certificate setting	
Type of the certificate	TWINS
Type of applicant	Employee (incl. statutory body members) or self-employed person
Certificate containing IC MLSA for communication with the public authorities	Yes
Revocation password	Revocation123
Certificate sent in the ZIP format	Yes
Period of validity	365 days
Certificate signing algorithm	pkcs#1 1v5
Key Repository Type (CSP)	Operating System Windows
Key type / Algorithm thumbnails / Key length	RSA / sha256Algorithm / 2048
Allow exporting the key	Yes
Allow the strong key protection	Yes
Usage setting key of qualified certificate	Non Repudiation / Digital Signature
Usage setting key of commercial certificate	Digital Signature / Key Encipherment
Extended usage setting key of qualified certificate	id-kp-emailProtection
Extended usage setting key of commercial certificate	id-kp-clientAuth / id-kp-emailProtection
Encoding type	UTF8_STRING

**Continue**

After pressing the "Continue" button, the private key will be generated on the computer. A new icon will appear  on the Windows tray and after clicking on this icon a window will appear, which needs to be confirmed by clicking "OK".

In the case of generating a certificate for a smart card or ID card, a PIN will be requested.



## 2.5 Saving Request

Here you leave the checkbox "Save to I.CA server" checked, type in the control string and fill in the phone number (the phone number is filled in here only to receive the SMS message with the request number that you will need at the registration authority). Then press the "Continue" button.

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

Select how to save your certificate request

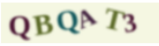
Save to the I.CA server

Save on local disk or external storage

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.

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.



Copy the text from the image on the

Continue

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00

## 2.6 Completion


At this point, the request is complete and all you have to do is visit the registration authority to verify and issue the certificate.

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

Your request has been successfully stored on the I.CA server.

Identification code of your request is

980357



With this identification code visit selected registration authority which completes the issuance of your certificate.

We advised to that you make a backup of the private key.  
Follow the instructions here: <https://www.ica.cz/Private-key-backup>

Please be aware that administration your private key is always fully responsible applicant for a certificate. Possible loss of private key can not be considered a fault the services provided by I.CA and there is no reason to issue a new certificate free of charge.

Find the registration authority

Exit guide

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.16.00