

Generating a request for subsequent certificate

User guide for Internet Explorer

První certifikační autorita, a. s.

Verze 8.16

1. Introduction

This document serves like a guide for generating the request for subsequent certificate through the web site.

2. Software requirements

Computer intended for generating the request must fulfil the following certificate requirements:

- installed and initialised operating system
 - **Windows 7 ServicePack 1**
 - **Windows 8.1 (April 2014 update)**
 - **Windows 10**
- installed and used **Internet Explorer** version 10 - 11
- enabled Javascript support for scripting, enabled support for Java language and also permission for storing cookies in the internet browser
- installed component and extension of **I.CA PKI Service Host**
- **I.CA SecureStore Card Manager** (just in case of generating request on the smart card)

3. The process of generating a request for a subsequent certificate

Process of generating the request for subsequent certificate is divided into few steps:

Test of systems

Personal data control

Recapitulation



Request signing


Completion

3.1 Control of software equipment

Easy way how to control presence of key software components in your computer is by control page. This page will be displayed when you start with generating.

Click on the button **Begin analysis**.

 **CERTIFICATION AUTHORITY** CONNECTED WITH TRUST 

 **CREATE A QUALIFIED CERTIFICATE REQUEST**

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 extensions	
	Support of cookies storage	

Continue

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.03

In case of missing component and extension of **I.CA PKIService Host**, an error notification appears (see below)

CERTIFICATION AUTHORITY CONNECTED WITH TRUST 

 CREATE A QUALIFIED CERTIFICATE REQUEST

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

Test ended in error

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 supported.
✓	Support of JavaScript	JavaScript enabled.
✗	Support of extensions	Extensions are not installed. Install the missing components I.CA PKIServiceHost
	Support of cookies storage	Waiting for test ...

Continue

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.03

Install necessary components for generating request to the PC by click on the highlighted text **I.CA PKIServiceHost**.

Restart your browser after installation and click on the yellow field **Begin analysis**.



- 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

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 supported.
✓	Support of JavaScript	JavaScript enabled.
✓	Support of extensions	Extensions are supported
✓	Support of cookies storage	Storage of cookies are enabled.

Continue

If everything is alright with the computer, you can click on **Continue** button and start to create a request for subsequent certificate.

If some error appeared meanwhile the control, it is not possible to continue with making request for subsequent certificate. First eliminate mistakes which are blocking the creation of request for subsequent certificate. Meaning of potential error reports is explained in following chapters.

3.1.1 Unsupported operating system

For generating a request is necessary to use one of the operating system mentioned in chapter 2.

3.1.2 Unsupported web browser

For generating a request is necessary to use one of the web browser type mentioned in chapter 2.

3.1.3 JavaScript support

Websites for generating a request for subsequent certificate requires a support in JavaScript language. If the control failed it means that the support of scripting is probably turned off in the website settings. Allow the support of scripting in JavaScript language in your browser.

3.1.4 I.CA PKIServiceHost

Component I.CA PKIServiceHost needs to be installed for the right website functionality. Make sure this component was installed. If the component is not installed in your computer, use the highlight title I.CA PKIServiceHost to download it. After all those steps you have to restart your computer.

3.1.5 Cookies Storage

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

3.2 Certificate selection for creating a request for subsequent certificate

If the process of control goes well, you can select the valid certificate for which you want to issue a renewal certificate.

The screenshot shows the I.CA web interface for creating a subsequent certificate. The header includes the I.CA logo and the text "CONNECTED WITH TRUST". The main heading is "CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE". Below this is a progress bar with five steps: 1. System Test, 2. Verification, 3. Recapitulation, 4. Signing a Request, and 5. Finalization. The current step is 2. Verification. The main content area has two sections. The first section is titled "Choose where is your certificate stored (registered)" and has two radio button options: "The personal certificate store in Windows" (selected) and "Other storage (eg I.CA smart card)". The second section is titled "Select the certificate for which you want to issue a renewal certificate." and has a dropdown menu with the selected certificate: "[2021-08-07][00016C6E][I.CA Test Public CA/RSA 11/2015]". A "Continue" button is at the bottom of the form. The footer contains the text: "Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.04".

If your certificate is stored in the Windows storage system, select the first option **The personal certificate store in Windows**. If your certificate is storage on the I.CA smart card, choose the second option **Other storage (eg I.CA smart card)**.

Based on your selection of the storage is offered the list of available certificates which are usefull for your subsequent certificate. If you selected **Other storage**, you must connect smart card reader with inserted smart card.

Issue a subsequent certificate is possible only with certificate that is valid and is not placed on the CRL (Certificate revocation list)!



If you receive an e-mail notification of your certificate expiration, part of the e-mail contains 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 the Certificate part, there are some displayed data from current certificate, like serial number, validity of certificate and separated subject items.

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

CONNECTED WITH TRUST

CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

1. System Test > **2. Verification** > **3. Recapitulation** > **4. Signing a Request** > **5. Finalization**

Certificate	Allowed adjustments of renewed certificate >>
Commercial	2608972 (27CF4C hex)
Full name	██████████
Country	CZ
Organization	První certifikační autorita, a.s.
Given name	██████████
Surname	██████████
Identifier of legal entity	██████████
E-mail in the certificate extensions	██████████
SN ICA	944270

Continue

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.04

After clicking on Allowed adjustments of renewed certificate in the upper corner the following options are displayed:

CERTIFICATION AUTHORITY CONNECTED WITH TRUST

CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Certificate Hide permitted adjustments >>

TWIN	[REDACTED]
Full name	[REDACTED]
Country	[REDACTED]
Organization	[REDACTED]
Given name	[REDACTED]
Surname	[REDACTED]
E-mail in the certificate extensions	[REDACTED]
SN ICA	[REDACTED]
IK MPSV	[REDACTED]
SN ICA	[REDACTED]

Revocation password: ?

Key Repository Type (CSP): Operating System Windows ▾

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

id-kp-clientAuth ? id-kp-emailProtection ? ms-SmardCardLogon ?

Edit the e-mail: Delete Change [REDACTED]

Add UPN (Microsoft Universal Principal Name):

TWIN qualified

IK MPSV ? Delete Change [REDACTED]

Continue

Revocation password:

If the private key is somehow compromised, some personal data changed (name, address...) or there are some other reasons to stop using certificate it is necessary to revoke the certificate.

It is possible to revoke certificate through the web site. In the case of revocation, you will be asked for revocation password.

If you do not know the password, the existing password set in the current certificate will be used.

If you decided to use another different password it should be 4 to 32 characters long. Only capital and small letters without diacritics and numbers are allowed.

Key repository type (CSP):

From the option in **Key repository type (CSP)** select the module providing Cryptographic service provider (CSP), which will generate your private key.

Export of private key:

If your selected key repository type (CSP) supporting export of the private key, you have the option to allowed export of the private key. This option allowed you to export the certificate including private key. Then the private key will be portable between storage. In this case, key management requires caution because of the higher risk of theft / misuse.

Strong security of the private key:

If your selected key repository type (CSP) supporting strong security of the private key, you have the option to allowed strong security of the private key. This option allowed you to export the certificate including private key. Before each use of your keys, you will be notified that your key is used.

Afterwards you have those options:

Medium- you will get the informative report

Strong - before every use you will be required to enter your password

E-mail edit:

If the current certificate includes e-mail address, here you can delete it to the subsequent certificate. Change is not possible in the most cases so you have to apply for the new certificate with the correct data.

Certificate restrictive content:

Your certificate may include extended use keys and alternative subject names, which are not allowed in certificate due to certification policy. In this case the warning is displayed it is necessary to remove extensions before you continue.

After clicking **Continue** button you will see recapitulation of the personal data and settings of subsequent certificate.



CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Data overview	
Certificate sent in the ZIP format	Yes
Period of validity	365
Key Repository Type (CSP)	Operating System Windows
Algorithm thumbnails / Key length	sha256Algorithm / 2048
Allow exporting the key	Yes
Allow the strong key protection	Yes
Extended usage setting key of qualified certificate	id-kp-emailProtection
Extended usage setting key of commercial certificate	id-kp-clientAuth / id-kp-emailProtection
certificate settings	
Full name	[REDACTED]
Given name	[REDACTED]
Surname	[REDACTED]
Organization	[REDACTED]
E-mail in the certificate extensions	[REDACTED]
IK MPSV	[REDACTED]
Country	[REDACTED]
SN ICA	[REDACTED]
SN ICA	[REDACTED]
The data are still valid?	
<input type="button" value="YES, the data are valid"/> <input type="button" value="NO, the data have changed"/>	

In case that all the data in certificate are actual, continue on the button „**YES, the data are valid**“ and start to generate the private key.

3.4 Generating a certificate request

Next steps depend on type of private key storage (CSP):

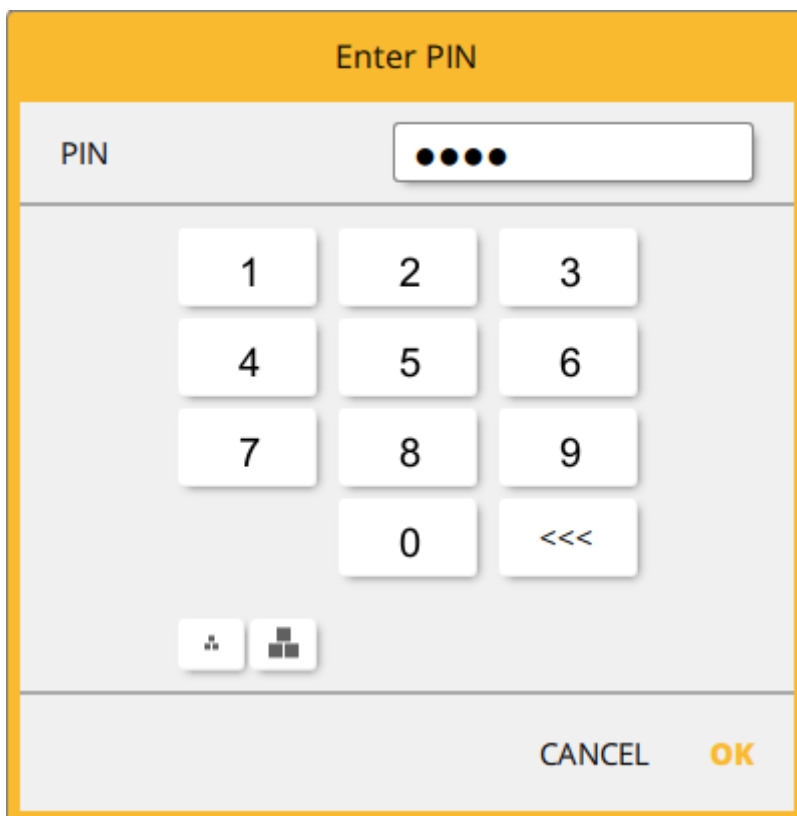
3.4.1 Secure Store CSP – I.CA smart card

If you choose Secure Store CSP as a storage for private key than follow next few steps to generate the request:

First the following dialog displayed. That time your private key is generating. Creating a private key may take several tens of seconds.



After the private key is create you are prompted to enter PIN to your smart card.



3.4.2 Microsoft Enhanced RSA and AES Cryptographic Provider with strong security of the private key

If you choose Microsoft Enhanced RSA and AES Cryptographic Provider (or Microsoft Enhance RSA and AES Cryptographic Provider /prototype/) as a storage and you permit the Strong private key then follow next few steps to generate the request:

CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Data overview

Certificate sent in the ZIP format	Yes
Period of validity	365

CREATING A REQUEST FOR A RENEWED CERTIFICATE

Please wait, key generation and request creation is in progress.

Extended usage setting key of qualified certificate	id-kp-emailProtection
Extended usage setting key of commercial certificate	id-kp-clientAuth / id-kp-emailProtection

certificate settings

Creating a new RSA signature key

An application is creating a Protected item.

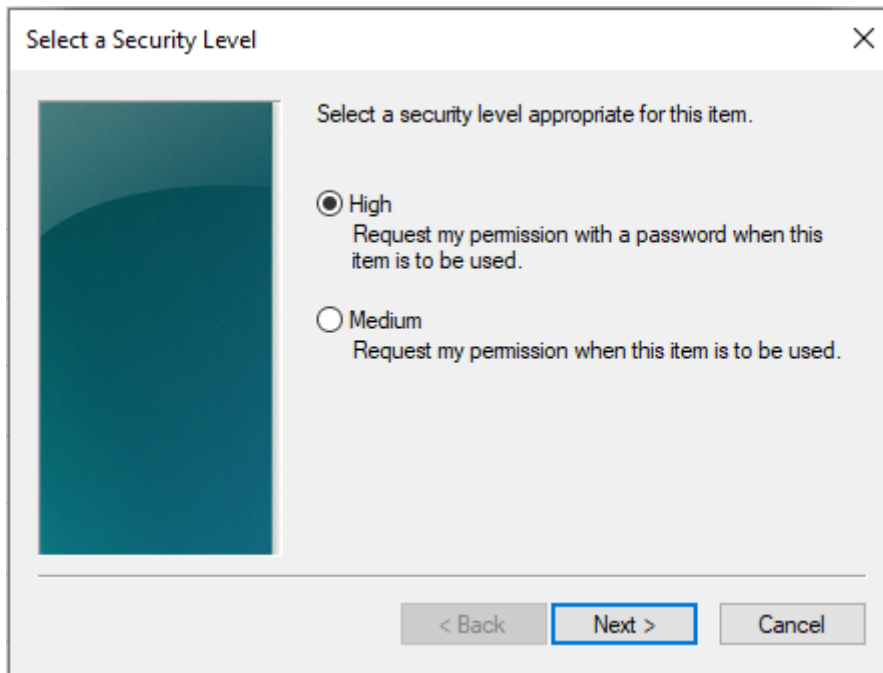
CryptoAPI Private Key

Security level set to Medium

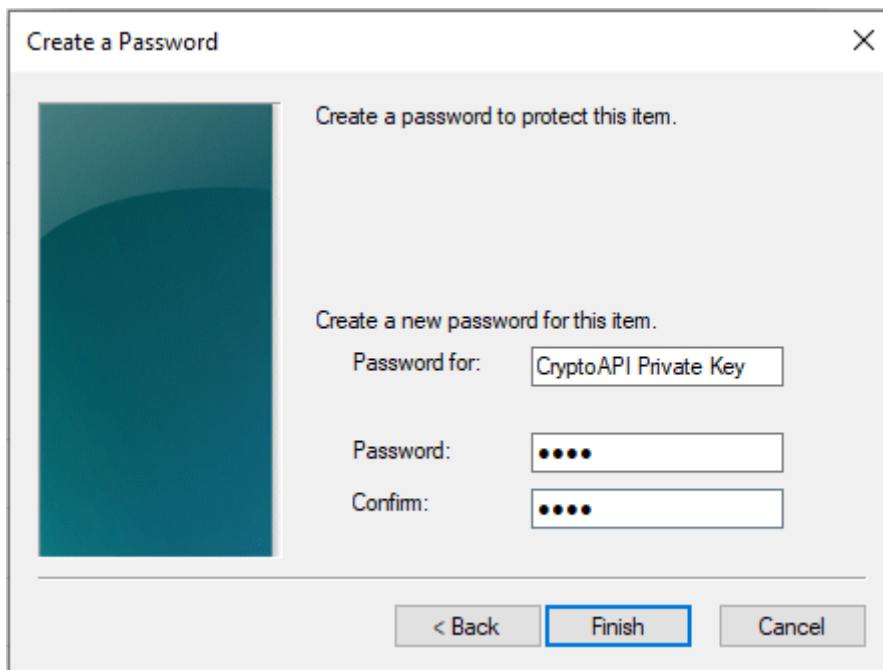
SN ICA 951626

The data are still valid?

You can change security level by clicking on **Set Security Level** button:

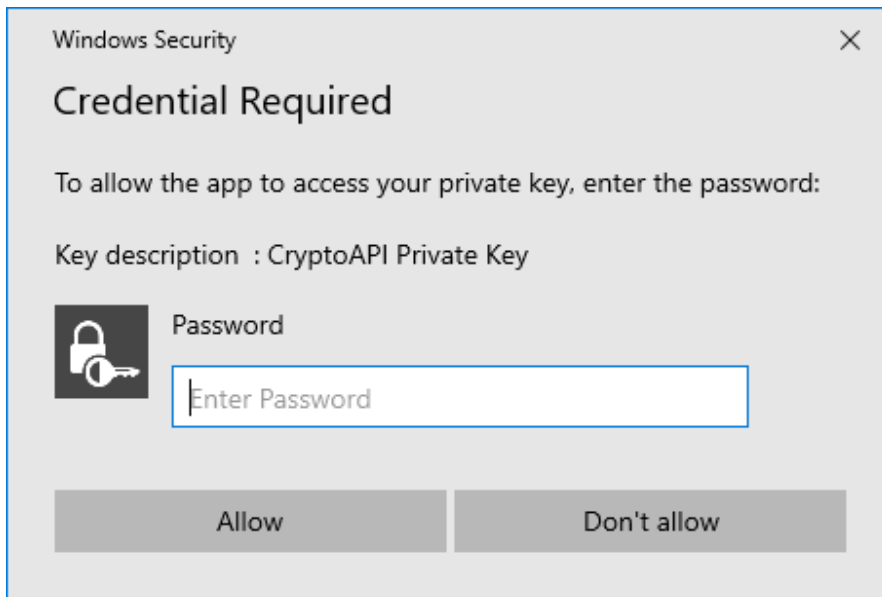


When you choose high security level, you will be asked for enter the password (you will need this password every time while using your certificate).



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

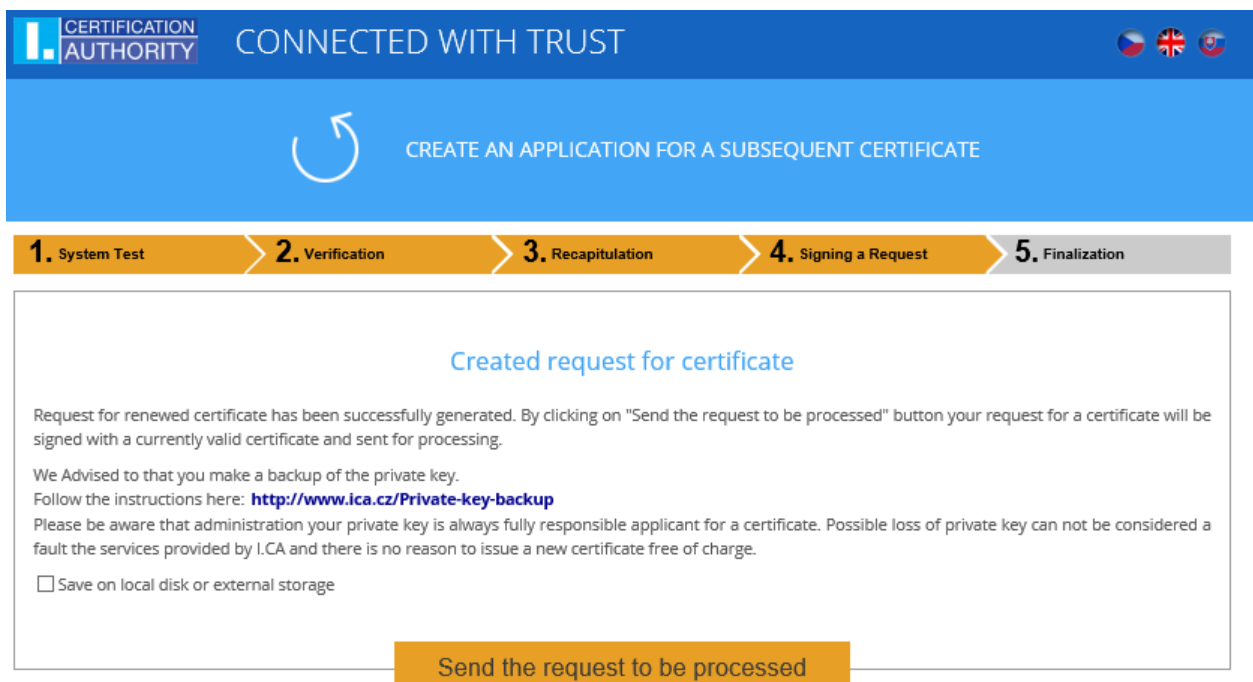
In the next dialog window click **Allow** to permit access to the private key. If you have chosen a **high level** of security, you must enter the password.



3.5 Signing and sending the request for subsequent certificate

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

After click on the button **Send the request to be processed**, the dialog containing your request for subsequent certificate appears. It is necessary to sign the request with previous certificate, which you are requesting the subsequent one.



CERTIFICATION AUTHORITY CONNECTED WITH TRUST

CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

1. System Test > 2. Verification > 3. Recapitulation > 4. Signing a Request > 5. Finalization

Created request for certificate

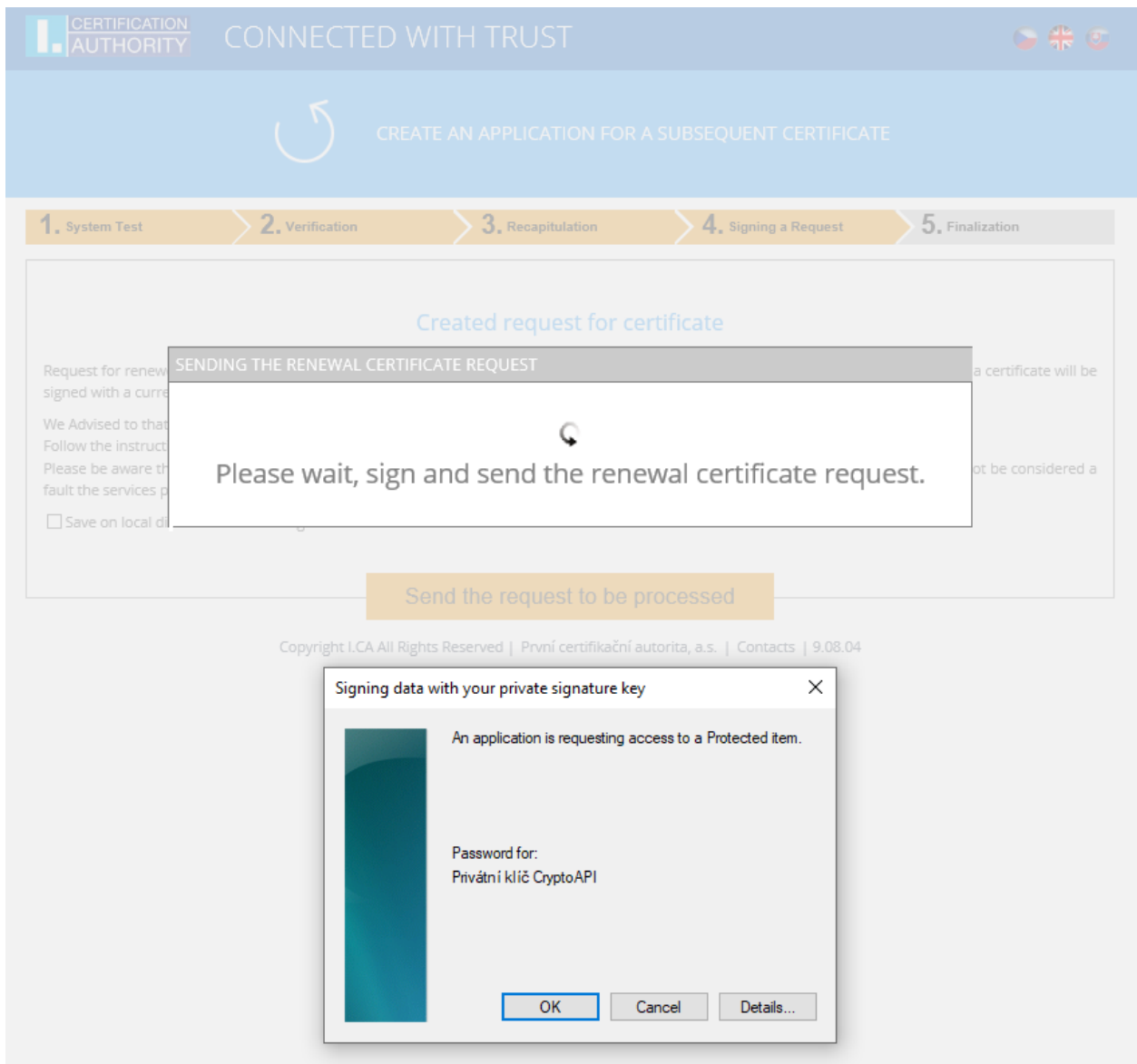
Request for renewed certificate has been successfully generated. By clicking on "Send the request to be processed" button your request for a certificate will be signed with a currently valid certificate and sent for processing.

We Advised to that you make a backup of the private key.
Follow the instructions here: <http://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.

Save on local disk or external storage

Send the request to be processed



Sign the request by click on the button **OK**.

When the request is generating on the smart card it is necessary to sign it with the **PIN code** relevant to this card.

When the request is for TWINS certificate, it is necessary to sign the both request (qualified and commercial certificate).

In case off correct sending of the request, following page will be displayed:

- 1. System Test
- 2. Verification
- 3. Recapitulation
- 4. Signing a Request
- 5. Finalization

The request for renewal certificate was successfully received.

ID request for the qualified certificate: 5708610731576
You can track the status of your application with ID 5708610731576.

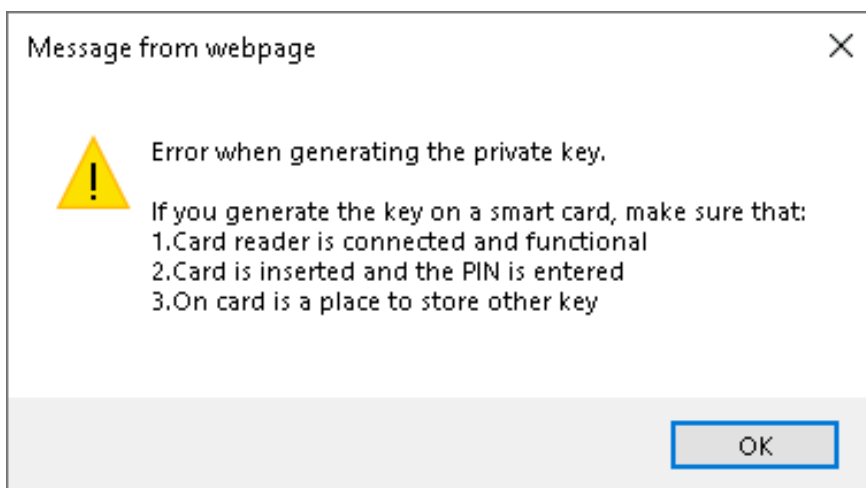
ID request for the commercial certificate: 5708600532749
You can track the status of your application with ID 5708600532749.

Time of receipt: 25.08.2020 08:54:46

Exit guide

4. Solving problems

When an error occurs in the process of generating the request you will be informed by an error message.



Some errors can be in serious technical way, related with the state of the hardware or software of your computer. In this case, we recommend to contact [technical support](#).