Generating a request for subsequent certificate User guide for Opera

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:

- o installed and initialised operating system
 - Windows 7 ServicePack 1
 - Windows 8.1 (April 2014 update)
 - Windows 10
- o installed and used **Opera** version 33 or higher
- enabled Javascript support for scripting, enabled support for Java language and also permission for storing cookies in the internet browser
- o installed component and extension of I.CA PKI Service Host
- o 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.

| AUTHORITY | CONNECTED V | VITH TRUST | | S 🕆 🖸 |
|-----------------------|---|---|---|----------------------|
| | ≡g | CREATE A QUALIFIED | CERTIFICATE REQUEST | |
| 1. Test system | 2. Entering data | 3. Verification | 4. Saving request | 5. Completion |
| | | | or trouble-free generation of reque | |
| | ed to perform some updates softw | ets the minimum requirements f | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |
| | ed to perform some updates softw | ets the minimum requirements f rare components, in this case it i se of complications contact tech Begin analysi | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |
| aske | ed to perform some updates softw In cas | ets the minimum requirements frare components, in this case it is se of complications contact tech Begin analysi Waiting for test la Details | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |
| aske | ed to perform some updates softw In cas | ets the minimum requirements f pare components, in this case it i se of complications contact tech Begin analysi Waiting for test la Details | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |
| aske | ed to perform some updates softw In cas Description Operation system versio | ets the minimum requirements f pare components, in this case it i se of complications contact tech Begin analysi Waiting for test la Details | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |
| aske | ed to perform some updates softw In cas Description Operation system versio Browser type and versio | ets the minimum requirements f pare components, in this case it i se of complications contact tech Begin analysi Waiting for test la Details | or trouble-free generation of reque s necessary to confirm acceptance (nical support I.CA . | |

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)

| AUTHORITY | CONNECTED V | VITH TRUST | CERTIFICATE REQUEST | |
|------------------------|---|---|--|----------------------|
| 1 . Test system | 2. Entering data | 3. Verification | 4. Saving request | 5. Completion |
| | ed to perform some updates softwa | are components, in this case it is | or trouble-free generation of reque necessary to confirm acceptance (| |
| | ed to perform some updates softwa | ts the minimum requirements f | or trouble-free generation of reque necessary to confirm acceptance o ical support I.CA . | |
| | ed to perform some updates softwa | tts the minimum requirements f are components, in this case it is e of complications contact tech Begin analysi | or trouble-free generation of reque necessary to confirm acceptance o ical support I.CA . | |
| aske | ed to perform some updates softwo | tts the minimum requirements fr are components, in this case it is e of complications contact tech Begin analysi Test ended in en Details | or trouble-free generation of reque necessary to confirm acceptance o ical support I.CA . | of these updates. |
| aske Result | ed to perform some updates softwork In case | tts the minimum requirements f are components, in this case it is e of complications contact tech Begin analysi Test ended in el Details in Window | r trouble-free generation of reque necessary to confirm acceptance o iical support I.CA . | of these updates. |
| aske Result | ed to perform some updates softwork In case Description Operation system versio | tts the minimum requirements frare components, in this case it is e of complications contact tech Begin analysi Test ended in er Details in Window n Opera w | r trouble-free generation of reque necessary to confirm acceptance o iical support I.CA. | of these updates. |
| Result | ed to perform some updates softwork In case Description Operation system versio Browser type and versio | tts the minimum requirements frare components, in this case it is e of complications contact tech Begin analysi Test ended in er Details in Window n Opera vi JavaScrij | r trouble-free generation of reque necessary to confirm acceptance o sical support I.CA . TOT 10 this operation system is suppor rsion 71, this web browser is suppo | of these updates. |

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** and **Extension**.

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



| AUTHORITY | CONNECTED | WITH TRUST | | S 🕀 🛛 |
|-----------------------|--------------------------------|------------------------|--|----------------------|
| | | CREATE A QUALIFIE | D CERTIFICATE REQUEST | |
| 1. Test system | 2. Entering data | 3. Verification | 4. Saving request | 5. Completion |
| | d to perform some updates soft | | is for trouble-free generation of reque it is necessary to confirm acceptance | |
| | | Begin analy | sis | |
| | | Test completed su | ccessfully | |
| Result | Description | Deta | ils | |
| ~ | Operation system vers | ion Wind | ows 10 this operation system is supp | orted. |
| ~ | Browser type and versi | ion Oper | a version 71, this web browser is supp | ported. |
| ✓ | Support of JavaScript | JavaS | cript enabled. | |
| ✓ | Support of extensions | Exter | sions are supported | |
| ~ | Support of cookies stor | rage Stora | ge of cookies are enabled. | |
| | | Continue | | |

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

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 subsequence 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 Extension (supplement) I.CA PKIService Host

It is necessary to have all extensions in your browser installed and permitted. You will be redirected to the browser setting by click on the highlighted title Extension. There you can find extensions and install them. After all those steps reload the page.

3.1.6 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.

| | CONNECTED V | VITH TRUST | | 640 | | | |
|-----------------------|---|------------------------|-----------------------------|-----------------|--|--|--|
| | | ATE AN APPLICATION FOR | A SUBSEQUENT CERTIFICATI | | | | |
| 1. System Test | 2. Verification | 3. Recapitulation | 4. Signing a Request | 5. Finalization | | | |
| The personal certifie | Choose where is your certificate stored (registered) The personal certificate store in Windows O ther storage (eg I.CA smart card) | | | | | | |
| | Select the certificate | e for which you want t | o issue a renewal certific | ate. | | | |
| [2021-0 | 8-07][00016C6E](I.CA Test Public | : CA/RSA 11/2015) | \checkmark | | | | |
| | Continue | | | | | | |

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 | | S # |
|----------------------------|-----------------|-------------------------|--------------------------------|-----------------------|
| | CT CRE | TATE AN APPLICATION FOR | A SUBSEQUENT CERTIFIC | ATE |
| 1. System Test | 2, Verification | 3. Recapitulation | 4. Signing a Request | 5. Finalization |
| Certificate | | Allo | wed adjustments of re | enewed certificate >> |
| Commercial | | 260 | 08972 (27CF4C hex) | |
| Full name | | | | |
| Country | | CZ | | |
| Organization | | Prv | ní certifikační autorita, a.s. | |
| Given name | | | | |
| Surname | | | | |
| Identifier of legal entity | , | | | |
| E-mail in the certificate | extensions | | | |
| SN ICA | | 944 | 4270 | |

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

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



| AUTHORITY CONNECTE | D WITH TRUST | | S # (|
|--|--|-----------------------------|-----------------------------|
| J | CREATE AN APPLICATION FOR / | A SUBSEQUENT CERTIFICATE | |
| 1. System Test 2. Verification | 3. Recapitulation | 4. Signing a Request | 5. Finalization |
| Certificate | | Hide permitte | d adjustments >> |
| TWIN | | | |
| Full name | | | |
| Country | | | |
| Organization | | | |
| Given name | | | |
| Surname | | | |
| E-mail in the certificate extensions | | | |
| SN ICA | | | |
| IK MPSV | | | |
| SN ICA | | | |
| Revocation password | Revocation password | | 0 |
| Key Repository Type (CSP) | Operating System Windows | V | |
| Certificate sent in the ZIP format | \blacksquare Allow exporting the key 🕜 | ✓ Allow 1 | the strong key protection 🕐 |
| ☑ id-kp-clientAuth 0 | ☑ id-kp-emailProtection 📀 | | 🗆 ms-SmardCardLogon 📀 |
| Edit the e-mail | Delete [|] Change | |
| Add UPN (Microsoft Universal Principal Name) | | | |
| TWIN qualified | | | |
| ik mpsv 🗿 | Delete |] Change | |
| | | | |
| | 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.



| | CONNECTED | WITH TRUS | σT | | € # © | |
|----------------|--------------------------------------|----------------------------|--------------------|---------------------------------|------------------------|--|
| | | EATE AN APPLICA | TION FOR | A SUBSEQUENT CERTIFICATI | E | |
| 1. System Test | 2. Verification | 3. Recapi | tulation | 4. Signing a Request | 5. Finalization | |
| | | Data | overview | 1 | | |
| | Certifica | te sent in the ZIP forma | t Yes | | | |
| | | Period of validit | y 365 | | | |
| | K | ey Repository Type (CSI |) Operati | ng System Windows | | |
| | Algorithm | thumbnails / Key lengt | h sha2564 | lgorithm / 2048 | | |
| | | Allow exporting the ke | y Yes | | | |
| | Allow t | he strong key protectio | n Yes | Yes | | |
| E | extended usage setting k | ey of qualified certificat | e id-kp-e r | id-kp-emailProtection | | |
| Exte | ended usage setting key o | of commercial certificat | e id-kp-cli | entAuth / id-kp-emailProtection | | |
| | | certifica | ate settin | gs | | |
| | | Full nam | e | | | |
| | | Given nam | e | | | |
| | | Surnam | e | | | |
| | | Organizatio | n | | | |
| | E-mail in the certificate extensions | | | | | |
| | IK MPSV | | | | | |
| Country | | | У | | | |
| SN ICA | | | | | | |
| | | SN IC | A | | | |
| | | The dat | a are still vali | d? | | |
| | YES, the da | ita are valid | NO, f | he 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.

| CREATING A CERTIFICATE REQUEST |
|--|
| Ð |
| Please wait, key generation and creation of the certificate request. |

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

| Enter PIN | | | | | |
|-----------|-----|-----|-----|--|--|
| PIN | | ••• | • | | |
| | 1 | 2 | 3 | | |
| | 4 | 5 | 6 | | |
| | 7 | 8 | 9 | | |
| | | 0 | <<< | | |
| | · . | | | | |
| CANCEL OK | | | | | |

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 than follow next few steps to generate the request:

| 1 . System Test | 2. Verification | 3. Recapitul | | 4. Signing a Request | 5. Finalization | |
|------------------------|--|---------------------------|-----------------|------------------------------|-----------------|--|
| | | | | | | |
| | | | | | | |
| | Certifica | te sent in the ZIP format | Yes | | | |
| | CREATING A REQUEST FOR A | Period of validity | 365 | | | |
| | | | reques | t creation is in pro | gress. | |
| | | | id-kp-email | | | |
| | | of commercial certificate | id-kp-client | Auth / id-kp-emailProtection | | |
| | | | e settings | | | |
| | Creating a new RSA signature key × An application is creating a Protected item. — Crypto API Private Key — Security level set to Medium Set Security Level OK Cancel | | | | | |
| | SN ICA 951626 | | | | | |
| | | | ne still valid? | | | |
| | | | | | | |

You can change the 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).

| Create a Password | | × |
|-------------------|-------------------------------------|---|
| | Create a password to | o protect this item. |
| | Create a new passw Password for: | ord for this item. CryptoAPI Private Key |
| | Password: Confirm: | •••• |
| | < Back | Finish Cancel |

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 a 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 a request to processing**, the dialog containing your request for subsequence certificate appears. It is necessary to sign the request with previous certificate, which you are requesting the subsequent one.

| AUTHORITY | CONNECTED | WITH TRUST | | S # C |
|--|-----------------------------------|--------------------------|-----------------------------|--|
| | CT CRE | ATE AN APPLICATION FOR | A SUBSEQUENT CERTIFIC | ATE |
| 1. System Test | 2. Verification | 3. Recapitulation | 4. Signing a Request | 5. Finalization |
| signed with a currently va | alid certificate and sent for pro | ocessing. | | your request for a certificate will be |
| Follow the instructions he Please be aware that adr | 3 1 3 | te-key-backup | | private key can not be considered a |
| Save on local disk or e | external storage | | | |
| | | Send the request to be j | processed | |

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



| | CONNECTED WITH TRUST | • # • | | | | |
|---|---|-----------------------|--|--|--|--|
| | | | | | | |
| 1. System Test | 2. Verification 3. Recapitulation 4. Signing a Request 5. Fi | inalization | | | | |
| | Created request for certificate | | | | | |
| signed with a curre | IDING THE RENEWAL CERTIFICATE REQUEST | a certificate will be | | | | |
| We Advised to that Follow the instruct Please be aware th fault the services p | ۲ Please wait, sign and send the renewal certificate request. | ot be considered a | | | | |
| Save on local di | Send the request to be processed | | | | | |
| Copyright I.CA All Rights Reserved První certifikační autorita, a.s. Contacts 9.08.04 | | | | | | |
| | Signing data with your private signature key × An application is requesting access to a Protected item. Password for: Privátní klíč Crypto API | | | | | |
| | OK Cancel Details | | | | | |

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:



| | CONNECTED | WITH TRUST | | • # • | |
|---|------------------------|--------------------------|---------------------------------------|------------------------|--|
| | CR CR | EATE AN APPLICATION FOR | A SUBSEQUENT CERTIFICA | ΓE | |
| 1. System Test | 2. Verification | 3. Recapitulation | 4. Signing a Request | 5. Finalization | |
| The re | | | was successfull īcate: 57086107315 | 5 | |
| | You can track the | status of your applica | tion with ID 57086107 | 31576. | |
| | ID request for t | the commercial cer | tificate: 5708600532 | 2749 | |
| You can track the status of your application with ID 5708600532749. | | | | | |
| | Ti | ime of receipt: 25.08.20 | 20 08:54:46 | | |
| | | Exit guide | | | |

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

4. Solving problems

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

| Message | from webpage | × |
|---------|---|---|
| | Error when generating the private key. If you generate the key on a smart card, make sure that: 1.Card reader is connected and functional 2.Card is inserted and the PIN is entered 3.On card is a place to store other key | |
| | ОК | |

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 <u>technical support</u>.