

Issuance of the subsequent certificate from the smart card Starcos 3.0 to the new smart card Starcos 3.7


- 1) Insert the new smart card Starcos 3.7 to the card reader. To initialize the smart card, set up PUK and PIN.
- 2) Click on I.CA SecureStore icon to start initialization of your smart card



- actual version of I.CA SecureStore: <https://www.ica.cz/download-application>

- 3) To set up the card click on "YES"

Card initialization



PIN or PUK have not been set up on card, do you want to set it up now?

NO YES

- 4) Choose your PUK and PIN (min. 6 max. 8 numbers) and click on "OK" button

PIN/PUK initialization

choose your PUK

PUK verification

choose your PIN

PIN verification

CANCEL OK

- 5) In e-mail with notification about your certificate expiration, choose the option “Issuance of subsequent certificate”

Dear client

Your qualified
certificate no. 10083378
issued by První certifikační autorita, a.s.
will expire on 10.08.2021 12:31:57

Issuance of subsequent certificate

certificate items:


common name	████████████████████
given name	████████████████████
surname	████████████████████
country	CZ
organization	████████████████████
e-mail (SAN.rfc822Name)	████████████████████
serial number	IDCCZ-██████████
serial number	ICA - ██████████

Please note that the new certificate will be valid for 365 days. The validity period starts when the certificate is issued. Therefore please consider whether you want to apply for the subsequent certificate now or later. You should apply for the subsequent certificate no later than 1 working day before the end of validity of your current certificate. It is impossible to apply for a subsequent certificate after the expiration of your current certificate.

PAYMENT FOR THE SERVICE

After submitting a request for the subsequent certificates you will be sent by e-mail a pro forma invoice for the certificates.

6) It is necessary to test your computer by click on “Start test” button


CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

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

Is your computer ready?

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

Start Test


Waiting for test launch

Result	Description	Details
	Operation system version	
	Browser type and version	
	Support of JavaScript	
	Support of extensions	
	Support of I.CA smart card / I.CA SecureStore application	
	Support of cookies storage	

Continue

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

7) After successful completion of the test press “Continue”


CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

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

Is your computer ready?

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

Start Test

Test completed successfully

Result	Description	Details
✓	Operation system version	Windows 10 this operation system is supported.
✓	Browser type and version	Chrome version 85.0, this web browser is supported.
✓	Support of JavaScript	JavaScript enabled.
✓	Support of extensions	Extensions are supported
✓	Support of I.CA smart card / I.CA SecureStore application	I.CA smartcards are supported applications I.CA SecureStore is installed.
✓	Support of cookies storage	Storage of cookies are enabled.

Continue

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

8) After the first control of personal data press “Continue”

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

Certificate		Allowed adjustments of renewed certificate >>
Qualified		[REDACTED]
Full name		[REDACTED]
Given name		Kateřina
Surname		[REDACTED]
Country		CZ
Organization		[REDACTED]
Identifier of legal entity		NTRCZ [REDACTED]
Serial Number		IDCCZ [REDACTED]
E-mail in the certificate extensions		[REDACTED]
SN ICA		[REDACTED]

Continue

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

9) After second control of personal data click on “YES, the data are valid”

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)	SecureStore CSP / Smart card I.CA
Algorithm thumbnails / Key length	sha256Algorithm / 2048

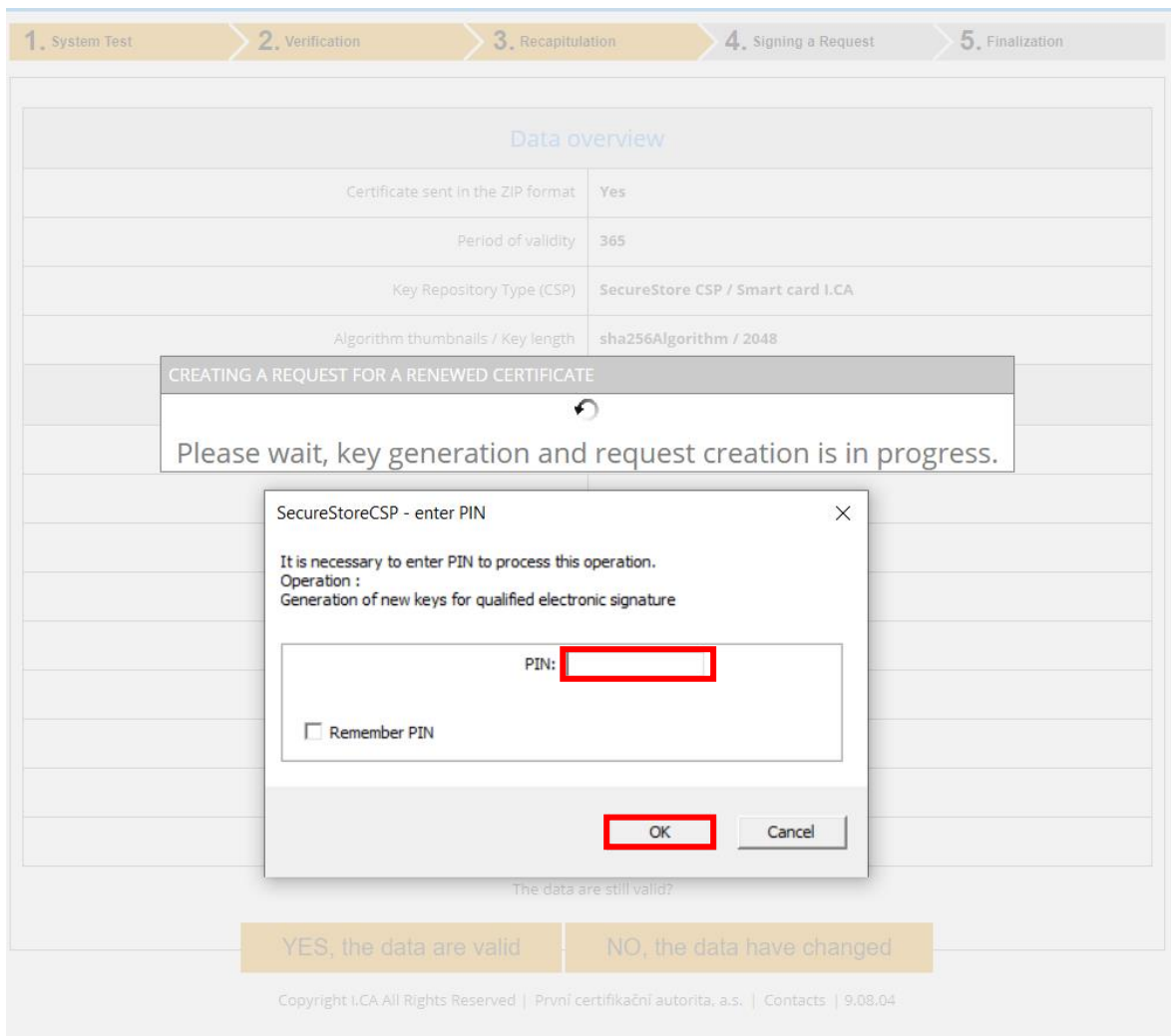
certificate settings	
Full name	[REDACTED]
Serial Number	IDCCZ [REDACTED]
Given name	Kateřina
Surname	[REDACTED]
Organization	[REDACTED]
E-mail in the certificate extensions	[REDACTED]
Country	CZ
Identifier of legal entity	NTRCZ [REDACTED]
SN ICA	[REDACTED]

The data are still valid?

YES, the data are valid NO, the data have changed

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

10) After generating the private key on the new smart card, enter PIN for the new card again



The screenshot displays a web application interface with a progress bar at the top containing five steps: 1. System Test, 2. Verification, 3. Recapitulation, 4. Signing a Request, and 5. Finalization. Below the progress bar is a 'Data overview' table with the following data:

Property	Value
Certificate sent in the ZIP format	Yes
Period of validity	365
Key Repository Type (CSP)	SecureStore CSP / Smart card I.CA
Algorithm thumbnails / Key length	sha256Algorithm / 2048

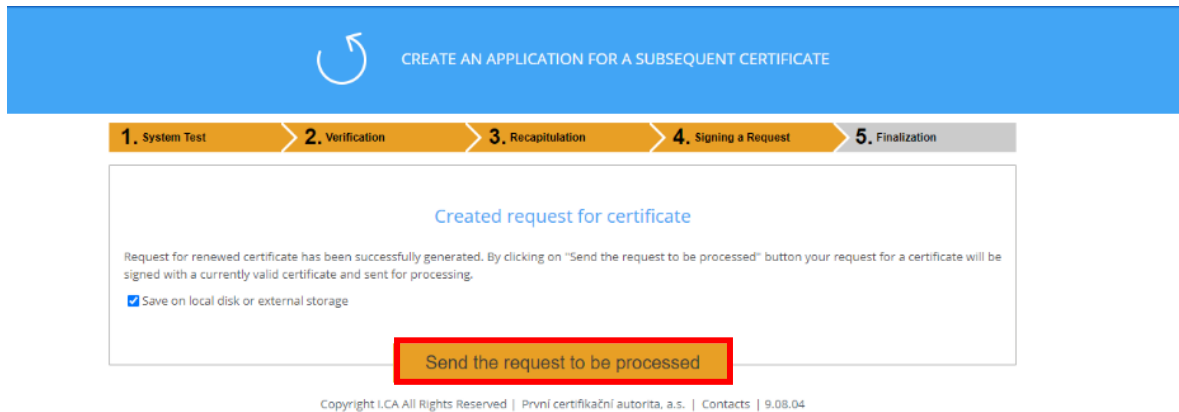
Overlaid on the table is a dialog box titled 'CREATING A REQUEST FOR A RENEWED CERTIFICATE' with a circular arrow icon and the text: 'Please wait, key generation and request creation is in progress.'

Below this is another dialog box titled 'SecureStoreCSP - enter PIN' with a close button (X). The text inside reads: 'It is necessary to enter PIN to process this operation. Operation : Generation of new keys for qualified electronic signature'. There is a text input field labeled 'PIN:' with a red rectangular highlight around it. Below the input field is a checkbox labeled 'Remember PIN' which is currently unchecked. At the bottom of the dialog are two buttons: 'OK' (highlighted with a red rectangle) and 'Cancel'.

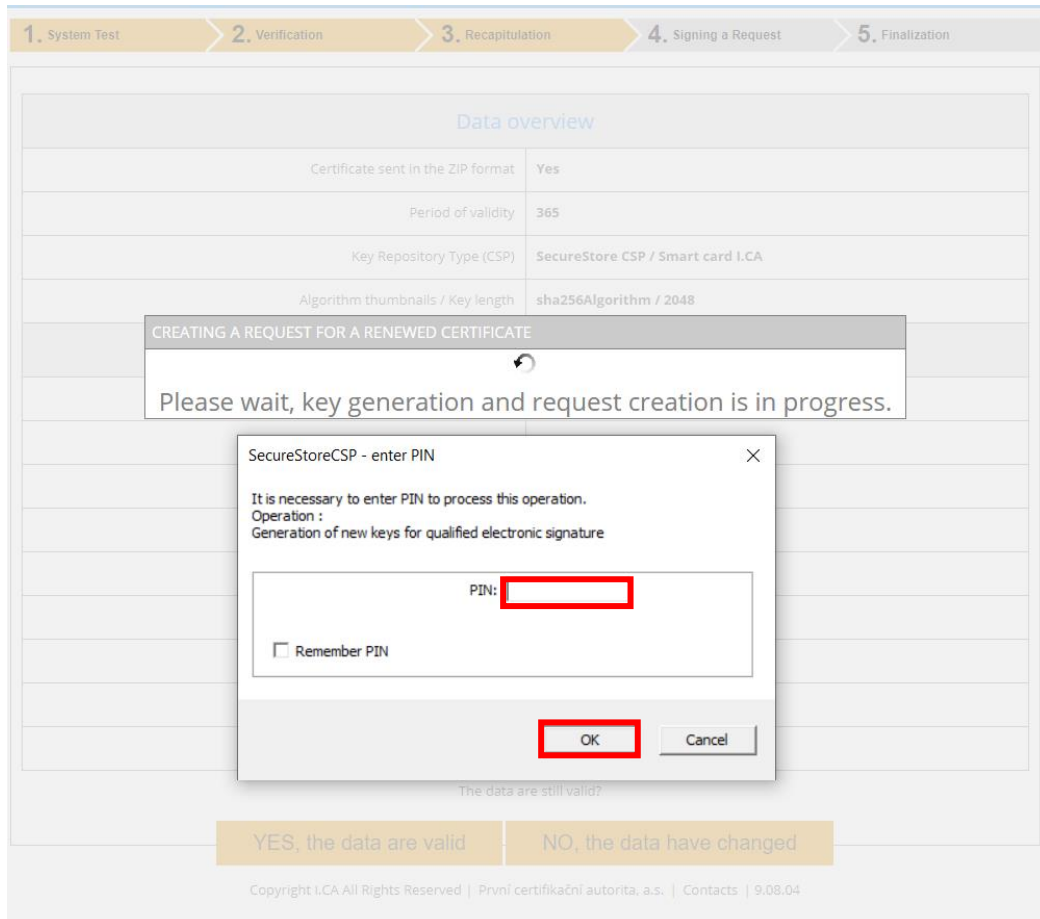
Below the PIN dialog, the text 'The data are still valid?' is visible. At the bottom of the interface are two buttons: 'YES, the data are valid' and 'NO, the data have changed'. The footer contains the text: 'Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.04'.

11) After successful generating of the key, insert the previous smart card Starcos 3.0 to the smart card reader


12) Click on “Send the request to be processed”



13) Enter the PIN for previous smart card Starcos 3.0 (generally four-digit) due to directions



- 14) Now the private key for subsequent certificate is generated on the new smart card Starcos
3.7. Wait for e-mail with issued certificate.

 CREATE AN APPLICATION FOR A SUBSEQUENT CERTIFICATE

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: 7607910003905
You can track the status of your application with ID 7607910003905.
Time of receipt: 08.09.2020 13:30:25
If the download does not start automatically, click the file to download [here](#)

Exit guide

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

Certificate installation on the smart card

- 1) Insert smart card Starcos 3.7 (where the private key was generated) into the card reader
- 2) In the e-mail with issued subsequent certificate click on the “Qualified certificate installation” button

Dear client

in accordance with the agreement you have signed with První certifikační autorita, a.s.,
we are sending you

subsequent qualified certificate SN [REDACTED]
issued for the request
No. [REDACTED]

**Qualified certificate
installation**

To register your certificate into Windows / MAC operation system click on the yellow button.

There you can find following services:

- import of your certificate into the STARCOS smart card
- import of the certificate to the Czech eID card,
- registration of the I.CA's root certificates
- setting up MS Outlook for the use with your new certificate
- creating a backup of your certificate including a private key into the PFX file (only the certificates with a private key stored in the PC)

To use your certificate with other applications please use the instructions of the particular application.

In case you want to install your certificate without using the yellow button above, you can use the attached certificate. If you didn't receive the attachments (e.g. they were stripped by a mail server) and the certificate was issued as a public certificate, it is possible to download the files from the [list of public certificates](#).


In case an instant revocation of your certificate is needed (e.g. private key compromise) [click here](#).

I.CA certification policy can be [found here](#).

Thank you for using our services.

Yours sincerely
První certifikační autorita, a.s.

3) On the web browser, where you will be redirected, click on yellow button “Install the Certificate onto the Card”


INSTALLATION INSTRUCTIONS

Instructions for Installing Qualified Certificate No. [REDACTED]

Installation of a certificate on a Starcos smart card

If the key to your certificate is stored on a STARCOS smart card or in electronic identity card (eID Czech), click on the "Install the Certificate onto the Card" button.

The missing certificate will be automatically found, stored onto the card, and also registered in Windows / MAC.

Install the Certificate onto the Card

Install the certificate on a personal computer

If you have a private certificate key stored on your personal computer (Windows OS), click the "Install the Certificate to PC" button

You are requesting the certificate number [REDACTED] server.

Control string: Q Y Z 7

Enter the security code from the picture and click on the "Install the Certificate to PC" button.

Install the Certificate to PC

Registering root certificates I.CA

Registration of Root Certificates I.CA

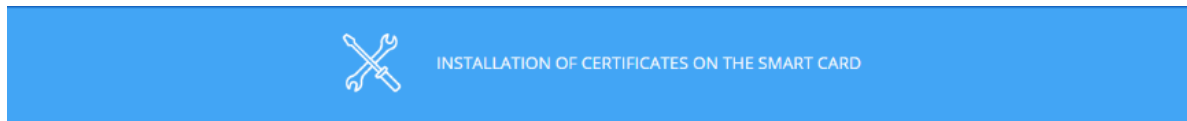
Setting mail client

Set up an email client

Private key and Certificate Backup

Make a Backup of the Certificate

4) For installation click on the button “Install”



Installation of certificates on the smart card

This is where you can install certificates issued by I.CA on your smart card.

Press install to begin installing certificates on your smart card. Before starting the installation, insert the card into the reader and enter your PIN when prompted. After pressing install wait for the installation to complete.

Register certificates to MS Windows

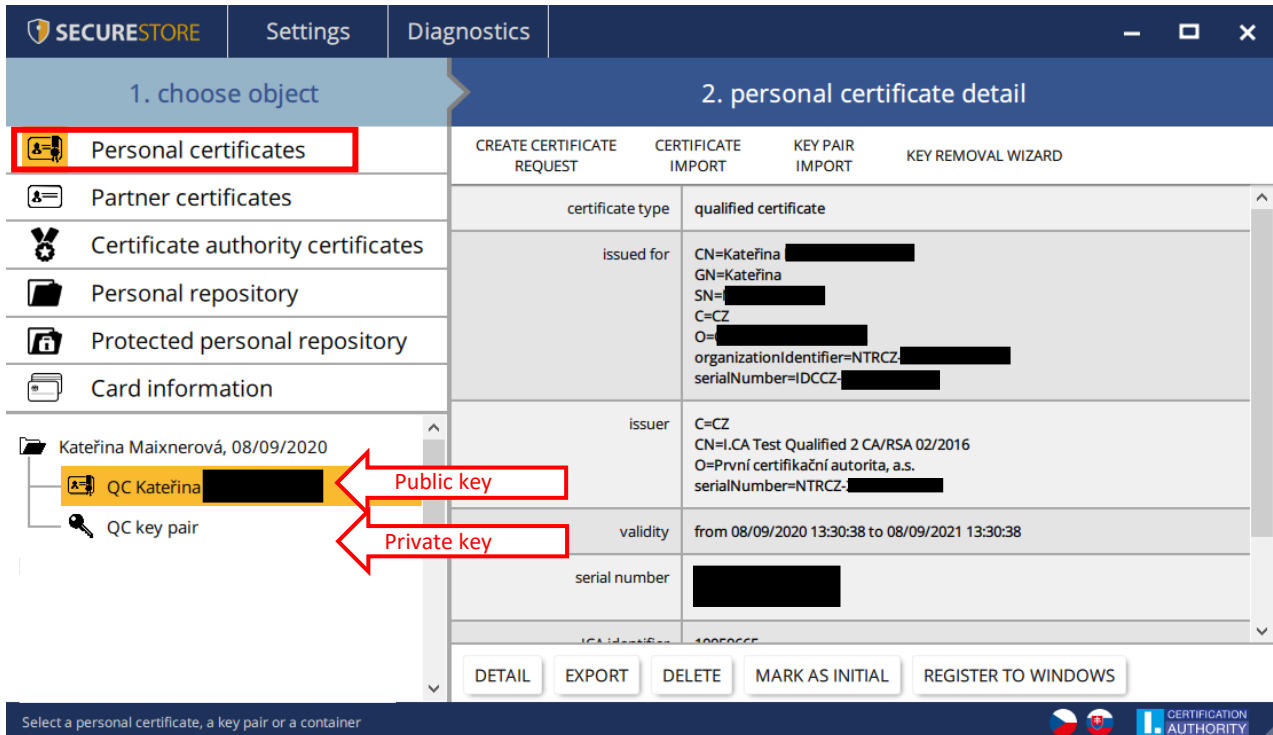
Install

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.08.07

5) Wait until installation is not finished. After installation close the web browser window



6) Control if the certificates were successfully installed in I.CA SecureStore application



The screenshot shows the I.CA SecureStore application interface. The left sidebar is titled '1. choose object' and lists several categories: Personal certificates (highlighted with a red box), Partner certificates, Certificate authority certificates, Personal repository, Protected personal repository, and Card information. Under 'Personal certificates', a folder 'Kateřina Maixnerová, 08/09/2020' is expanded, showing 'QC Kateřina' (highlighted with a yellow box) and 'QC key pair'. Red arrows point from the 'QC key pair' to the 'Public key' and 'Private key' labels.

The main area is titled '2. personal certificate detail' and contains a table with the following data:

certificate type	qualified certificate
issued for	CN=Kateřina GN=Kateřina SN= C=CZ O= organizationIdentifier=NTRCZ- serialNumber=IDCCZ-
issuer	C=CZ CN=I.CA Test Qualified 2 CA/RSA 02/2016 O=První certifikační autorita, a.s. serialNumber=NTRCZ-
validity	from 08/09/2020 13:30:38 to 08/09/2021 13:30:38
serial number	

At the bottom of the main area, there are buttons: DETAIL, EXPORT, DELETE, MARK AS INITIAL, and REGISTER TO WINDOWS. The status bar at the bottom left says 'Select a personal certificate, a key pair or a container' and the bottom right shows the CERTIFICATION AUTHORITY logo.

Rem: In case of TWINS certificates 2x private and 2 public keys will be displayed

We are ready to answer all your questions on e-mail address podpora@ica.cz