

První certifikační autorita, a.s.



Online certificate issuance

User documentation

Version: v1.05

Date: 11.09.2024

Prepared by: David Hoření

Content

1	Introduction.....	3
1.1	Online Certificate Issuance – Limiting Conditions.....	3
1.2	Online certificate issuance procedure.....	4
2	Initial registration of the applicant for the certificate – entering data.....	5
3	Initiation process – start screen	7
4	Download the application for a supported platform	8
5	ZealiD application – User Verification	8
5.1	User notification and registration	9
5.2	Device registration	10
5.3	Uploading of selfie video – user verification by selfie video.....	11
5.4	Picture of the identity document	11
5.4.1	Identity document picture – verification of a personal document authenticit	12
5.4.2	Identity document picture – control of the identity document picture	12
5.4.3	Identity document picture – user registration completion.....	13
6	Online certificate issuance – generating a certificate request.....	14
6.1	Issuance of a certificate online – QR code loading.....	14
6.2	Online certificate issuance – online I.CA generator	15
6.2.1	Online certificate issuance – creating a request	15
6.2.2	Issuance of a certificate online – payment.....	17
6.3	Issuance of a certificate online – signing of the certificate issuance agreement.....	18
6.4	Issuance of a certificate online – certificate installation.....	18
6.5	Online certificate issuance – access to electronic documentation	19
7	List of document revisions.....	20

1 Introduction

The document describes the conditions and procedure for issuing a personal electronic certificate (without personal presence at the RA I.CA office) with on-line verification of the applicant's identity, based on verification of the identity of a natural person (applicant) and biometric identity verification. This verification is carried out using a special ZealiD authentication application, installed on the applicant's mobile phone or tablet.

The whole process is implemented in the form of a step menu. A description of each step is given below.

1.1 Online Certificate Issuance – Limiting Conditions

The service of issuing a personal electronic certificate with on-line verification of the applicant's identity is an additional service to the standard process of issuing personal certificates in the presence of the applicant at the office of the client registration authority and can only be provided under the restrictive conditions specified below. In the event that it is not possible for the applicant to meet the conditions specified below or to accept them, it is not possible to provide the on-line issue service to the applicant. This does not limit the applicant's ability to submit an application for an electronic certificate in the standard way – i.e. in the form of an in-person form at the office of the client's RA I.CA.

1. Technical conditions

- The user must have a functional smartphone with Android and/or iOS (iPhone) operating system and active internet access, on which he/she installs the ZealiD utility application (see below)
- The user must have a personal computer with Windows-10 (or higher version) or MacOS (the last 3 official versions of macOS), a monitor with minimal HD resolution and a working Internet connection.

2. Procedural conditions

- Within the meaning of Articles 6, 7 and 9 of the General Data Protection Regulation (GDPR), in addition to the personal data provided, when issuing an electronic certificate in the presence form (legal requirements), the applicant must also expressly consent to the provision and processing of data of a special nature (biometric data) – namely a photo of the face and the submitted identity document, and their storage on page I.CA for the same period, for which the data required for the issuance of an electronic certificate in the presence form are stored – i.e. data provided by the applicant for the certificate on the basis of legal conditions based on Regulation (EC) No. 910/2014 of the European Parliament and of the Council (eIDAS Regulation) and Act No. 297/2016 on trust services for electronic transactions. The text of the conditions under which the service can be provided can be viewed under the link: <https://www.ica.cz/userfiles/files/dokumenty/Podminky%20pro%20zadost%20o%20Ovydani%20certifikatu%20distancnim%20způsobem.pdf> .
- As part of the data processing, the applicant must confirm his/her will to sign a contract for the issuance and use of a qualified certificate with I.CA (see link: https://www.ica.cz/userfiles/files/dokumenty/online_smlouva_vzor.pdf for a sample contract) and to sign this contract electronically before the end of the entire process.

1.2 Online certificate issuance procedure

The actual process of verifying the applicant's identity and issuing the electronic certificate takes place in several successive steps:

1. Initial registration

- For initial registration, the user is asked to enter basic identification data, which will then be checked as part of the online verification process.

2. Installing the ZealiD app on a mobile device

- The ZealiD application, which is available for Apple and Android platforms in the respective markets, is used for online verification of the identity of the applicant for the certificate.



3. Online verification process in the ZealiD app on mobile devices

Within the ZealiD application, the following operations are performed:

- Biometric facial analysis. For the necessary functionality of the application, it is necessary to allow the ZealiD application to access the camera and camera during installation.
- Verification of your personal documents, where a scan of the submitted personal documents (ID card or passport) is performed, processing of the obtained data and biometric comparison of the photo with your face.

4. Generate a certificate request

- The operation takes place through the I.CA web interface, where the user is shown the application items obtained from the online verification for review and approval by the applicant.

5. Payment for the service

- The User chooses the form of payment for the service (by credit card or by means of a proforma invoice).

6. Signing a contract on the issuance and use of an electronic certificate

- The user has the option to view the electronic contract and then sign it.
 - A sample contract is available for inspection under the link:
https://www.ica.cz/userfiles/files/dokumenty/online_smlouva_vzor.pdf .

7. Obtaining an electronic certificate.

- After signing the contract, the user will receive the issued certificate to the email address specified in the certificate issuance process. At the same time, the user receives a link to download the electronic agreement on the issuance and use of the certificate.

2 Initial registration of the applicant for the certificate – entering data

For initial registration, the user is asked to enter basic identification data, which will then be checked as part of the online verification process. Therefore, it is important to properly check the registration before saving it – see Fig. 1.

Fig. 1

The screenshot shows the 'Applicant pre-registration' form on the Certification Authority website. The form is titled 'Applicant pre-registration' and includes a sub-header 'Pre-registration of the applicant for the on-line issuance of the certificate'. A note states: 'Before issuing the certificate online, you need to register first. Fill in the information below according to the relevant personal document. After successful registration, you will receive a confirmation by email and instructions to complete the process. The process of issuing the certificate can be started 24 hours after your registration.' The form is divided into three main sections: 'Personal information', 'Personal document', and 'Captcha'. The 'Personal information' section includes fields for 'First name (required)', 'Surname (required)', 'Area code' (with a dropdown menu showing '+420'), 'Phone number (required)', and 'E-mail address (required)'. The 'Personal document' section includes fields for 'Personal document type (required)' (with a dropdown menu showing 'Identity card'), 'Document's expiry date (required)', 'Document's country of issuance (required)' (with a dropdown menu showing 'Czech Republic'), 'Document's issuer', and 'Document number (required)'. The 'Captcha' section includes a 'Captcha (required)' field and a video player showing a captcha challenge. A 'Save registration' button is located at the bottom of the form.

If the certificate is not issued, the User's personal data will be deleted after 10 days from the date of pre-registration.

The user will receive information about saving the registration by e-mail. – see Fig. 2.

Fig. 2

Dear Client

thank you for completing the pre-registration for the online issuance of the I.CA certificate.

You will be notified about the possibility of starting the identity verification process and issuing the certificate online via a notification message, which you will receive within 24 hours after successful pre-registration.

Your pre-registration will be active from: **Sep 13th 2024 12:02pm to Sep 16th 2024 12:02pm**

Information provided by you to be verified:

First name	Jan
Surname	novák
Phone number	+420123456789
E-mail address	test@ica.cz
Personal document type	Identity card
Document number	1561464894165
Document's expiry date	Feb 12 2033
Document's country of issuance	Czech Republic

Thank you for using our services.

Yours sincerely

První certifikační autorita, a.s.



The online process can be started 24 hours after the successful saving of the registration for the next 3 days.

Fig. 3

Dear customer

your initial registration is already active. You can now start the identity verification and certificate issuance process.

Start identity verification and certificate issuance

Yours sincerely
První certifikační autorita, a.s.



3 Initiation process – start screen

The process for on-line processing of the application and the issuance of the electronic certificate can be launched from the website www.ica.cz in the Qualified Certificate for Electronic Signature section, or directly under the <https://www.ica.cz/on-line-ziskani-certifikatu> link, after clicking on which the introductory screen containing basic information and related links will be displayed. The applicant must agree with the procedure and conditions for the online issuance of the electronic certificate (remotely), Otherwise, it is not possible to issue the certificate remotely or to provide the service – see Figure 4.

Fig. 4

CERTIFICATION AUTHORITY EN

Verification of the applicant for the on-line issuance of the certificate

Issuance of a certificate without personal presence at the RA ICA workplace takes place in several successive steps and includes:

- 01 Installation of the ZealiD application**
Installation of the ZealiD application on a mobile device.
Allow camera and camera access during installation.
- 02 Biometric analysis of the face using the ZealiD application**
Touch ID / Face ID must be activated.
- 03 Verification of your identification documents**
A scan of the show identification documents (ID card or passport), processing of the obtained data and biometric comparison of the photo with your face is performed.
- 04 Generation a request**
Generating a request for an electronic certificate.
Takes place via the web interface.
- 05 Signing an Agreement**
Signing an Agreement on the issuance and use of the electronic certificate.
A sample of the Agreement is available for view [HERE](#).

* If you agree to this process under the conditions below, click the "I agree" button.

I agree

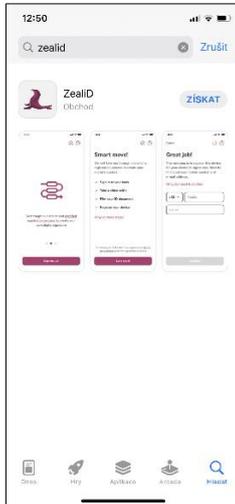
Notice:
The issuance of an electronic certificate on-line is only possible if you agree with the procedure described in the previous points and under the following conditions:

- As part of the process of verifying the applicant's identity, a scan of the face and submitted identification documents is performed, with the data obtained in this way being processed in the ICA system and stored there in accordance with the relevant [certification policies](#) and [conditions for issuing certificates in a remote manner](#).
- Before the end of the process of issuing an electronic certificate, you will be asked to sign the Agreement on the issuance and usage of an electronic certificate (see above), which will need to be signed by you.
- In the event that the online verification does not take place in the required quality or before the completion of the certificate issuance process you do not sign the Agreement on the issuance and use of the electronic certificates, the certificate issuance service will not be provided, or the generated certificate will be immediately revoked by the ICA.

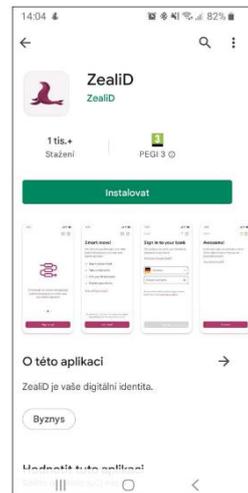
4 Download the application for a supported platform

Enter “ZealiD” into the browser, the searched application – see fig. 5.:

Fig. 5



ZealiD app for iOS



ZealiD app for Android

5 ZealiD application – User Verification

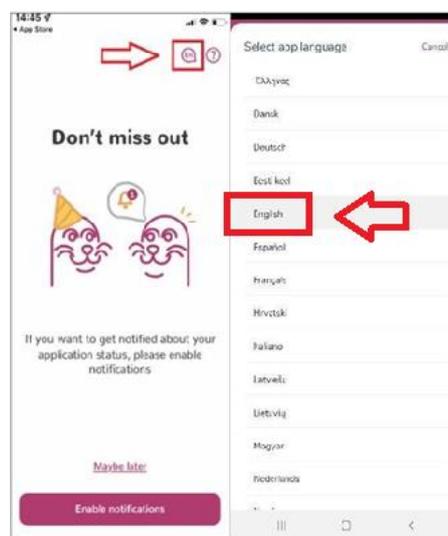
Launch the ZealiD application by the icon from the desktop of your mobile device

By default, the ZealiD app is in English.



If necessary, change the required language version – see Fig. 6.

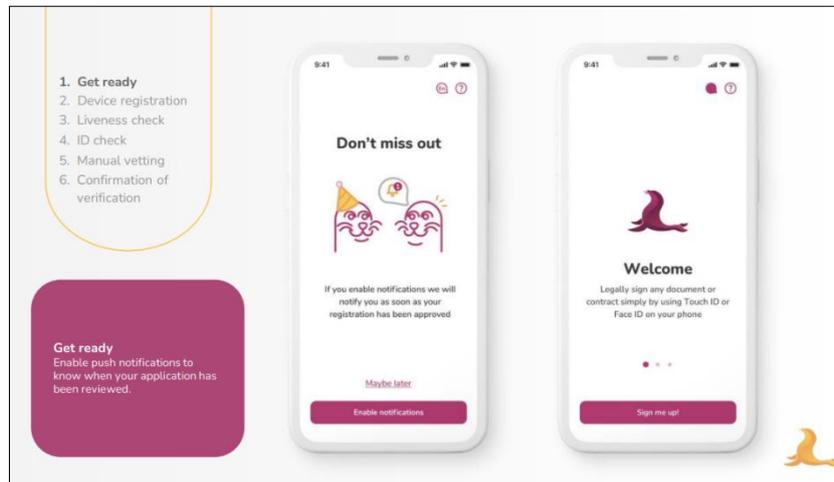
Fig. 6



5.1 User notification and registration

For registration and verification of the user/device, enable notification – see Fig. 7.

Fig. 7



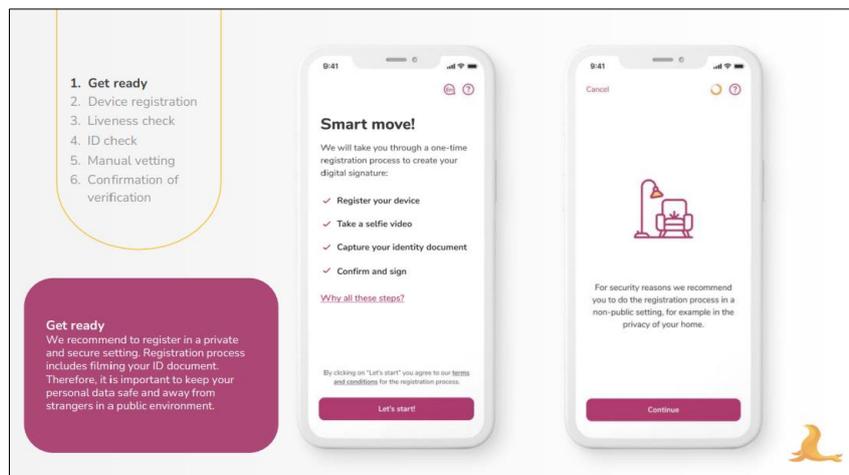
User registration consist from few steps, in following steps the application will require:

- Registration of your device
- Upload selfie video by ZealiD application and by mobile device
- Scanning your identity document

This validation process will reliably ensure the user identity verification and then the applicant for the I.CA certificate, for this reason it is necessary to go through all the steps above and provide the required information.

Before starting the verification process, you can get the information about the process see - fig.8. Then follow the guide.

Fig. 8



5.2 Device registration

insert required contact information, to which a one-time OTP code will be sent to verify/register your device to the system. See Fig. 9:

Fig. 9

Cancel

Let's start!

During this step, you will register this device for your electronic signatures. Start by filling out your mobile number and e-mail address.

Why do I need to do this?

+420 Mobile

Email

Continue

copy OTP codes that have been sent to the contact phone and e-mail. It registers the signature authorization device and, if the mobile device has "Face ID" technology, it can use this functionality to confirm transactions – see Figure 10.

Fig. 10

Cancel

Register your device

SMS code
Fill in the code we sent to +33 11* *** 333

1 2 3 - 4 5 6

E-mail code
Fill in the code we sent to sve*****men@gmail.com

Resend codes

Continue

Cancel

Register your device

Do you want to register this device for authorizing remote signatures?

Cancel OK

Continue

Cancel

Register your device

Do you want to allow "ZealID" to use Face ID?
Face ID will be used for secure transaction confirmation

Don't Allow OK

Continue

5.3 Uploading of selfie video – user verification by selfie video

To take a selfie video, the app requires permission to access the camera. The user sets the face according to the oval frame into the camera (first from a distance and then up close). It waits for the selfie video to be processed – see Fig. 11.

Fig. 11

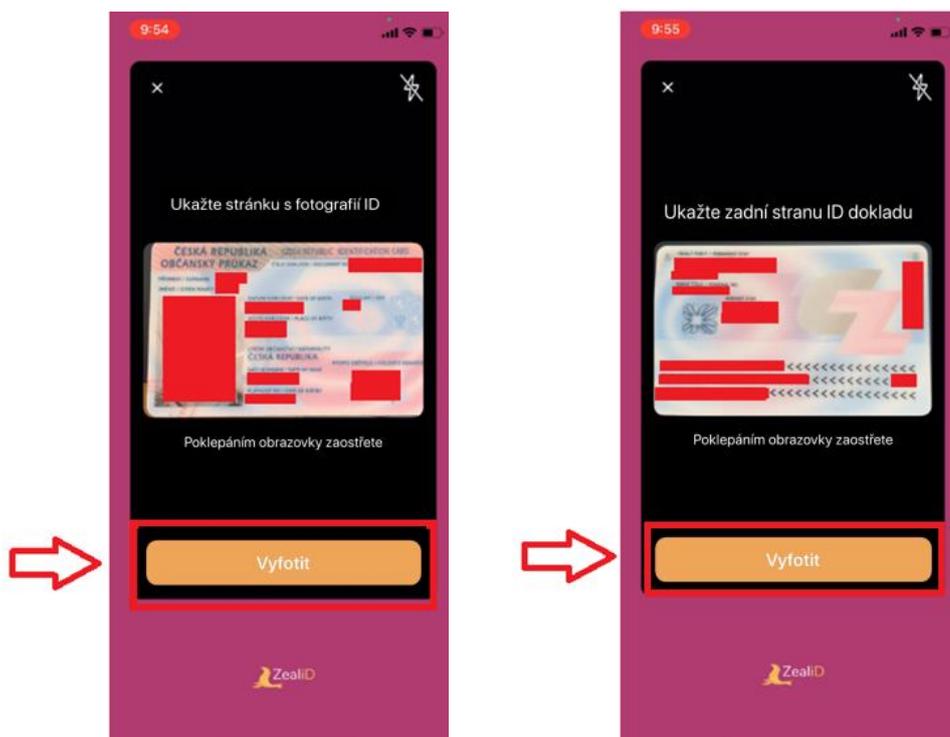


5.4 Picture of the identity document

Choose one of the accepted forms of identity document from the list. Put your identity document on the flat surface and ensure suitable light conditions.

Then arrange the front of the identity document to the frame, application will require scanning the document (green and purple dot). The back side of the document will be scanned in the same way – see fig.12.

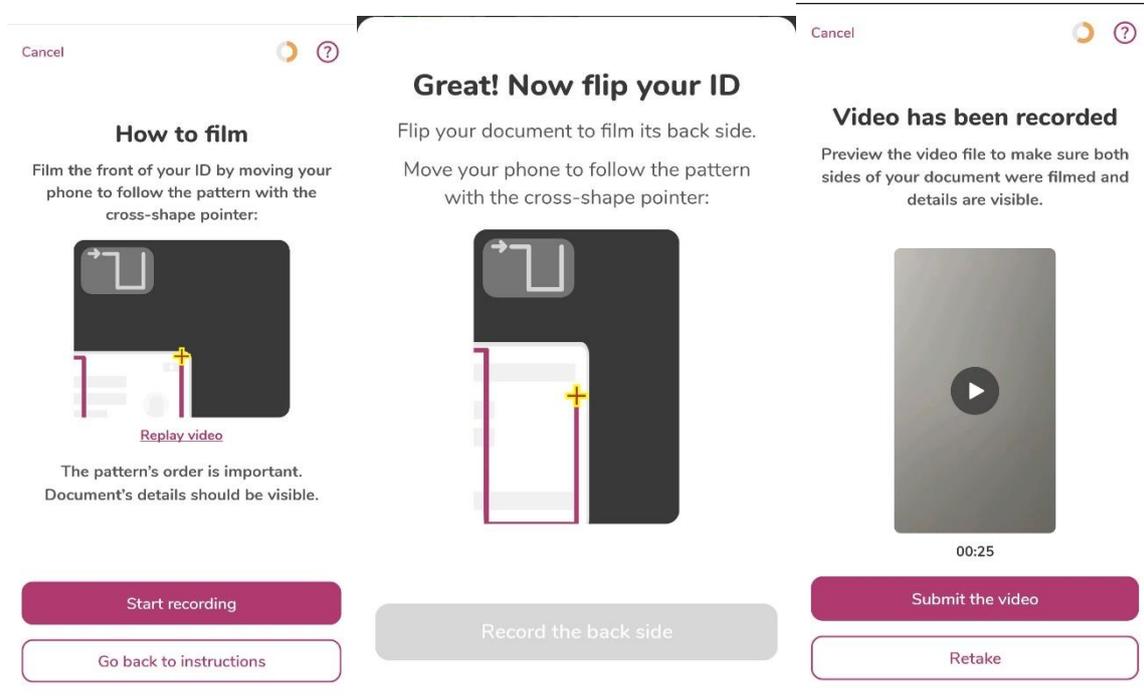
Fig. 12



5.4.1 Identity document picture – verification of a personal document authenticit

Now the user rotates the front of their ID by moving it according to the purple dot pattern. They turn the back of their identity document in the same way – see Fig. 13.

Fig. 13



5.4.2 Identity document picture – control of the identity document picture

The user checks the images of the front and back of the ID document and then agrees to the general terms and conditions – see Fig. 14.



5.4.3 Identity document picture – user registration completion

Check the information obtained from the identity document picture and then agree on the general conditions. Wait for your ID to be processed – see fig.15:

Fig. 15



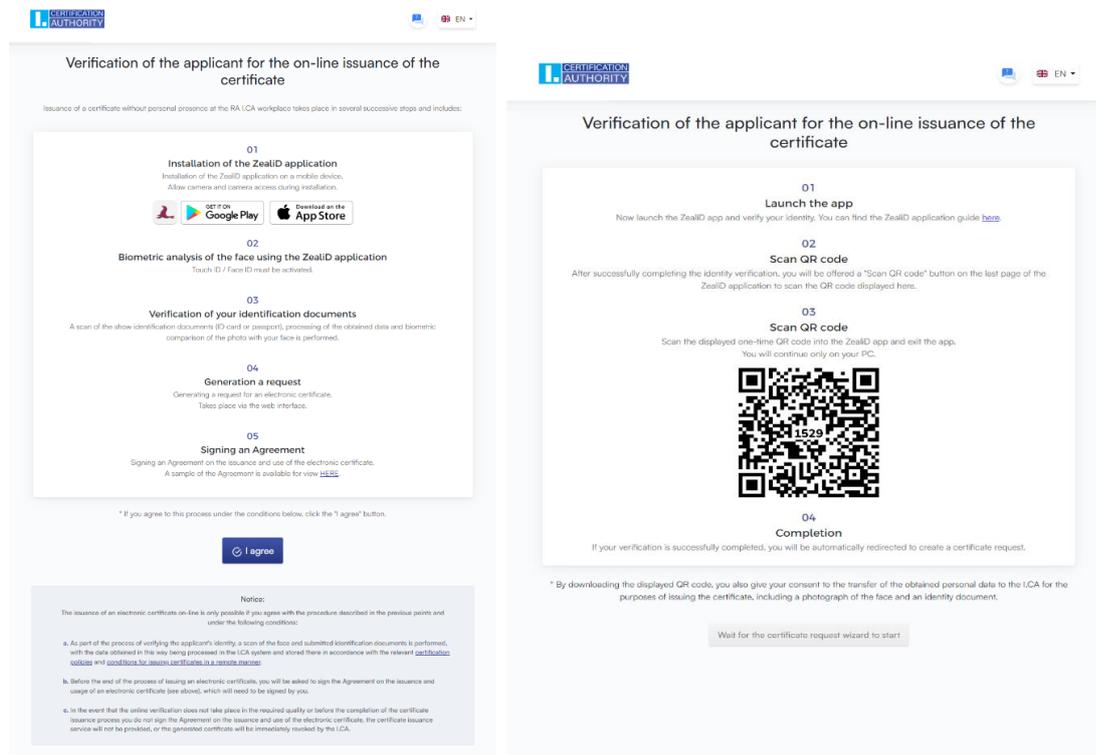
When verifying the applicant's identity in the mobile application, a technology certificate is issued to ensure secure communication within the verification process. This certificate secures the transfer of information between the user and the application.

6 Online certificate issuance – generating a certificate request

6.1 Issuance of a certificate online – QR code loading

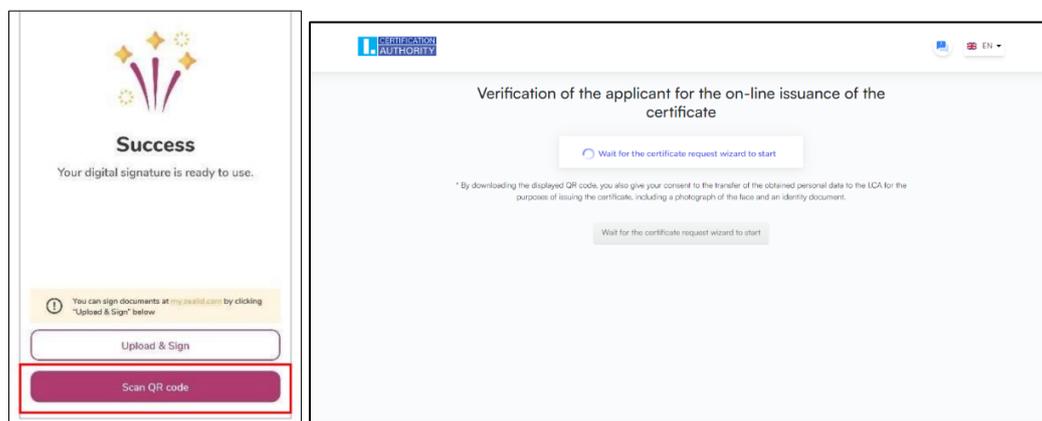
The last step in the ZealiD application is to read the generated QR code, which is displayed on the web interface I.CA after selecting the option "I agree, I want to continue" on the home screen – see Fig. 16.

The Fig.16



Follow the instruction in your mobile device to read the displayed QR code from the computer screen. After successful reading of QR code, the verification data from ZealiD will be redirected to the process of creating a certificate request – see fig.17:

Fig. 17



6.2 Online certificate issuance – online I.CA generator

6.2.1 Online certificate issuance – creating a request

Data entry – Name, surname and country is already pre-filled in the request based on the identification data from ZealiD application and it is not possible to change this data. The user

Fills in the following information:

- E-mail specified in the certificate (allows signing in e-mail)
- E-mail for communication with I.CA (documentation will be sent to this address after the certificate is issued)
- Phone number (the password for the encrypted documentation will be sent to this number)
- Password for certificate revocation

Fig. 18

CERTIFICATION AUTHORITY

EN

Create a certificate request

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

Information about the applicant

First name (mandatory) Surname (mandatory) Country (mandatory)

E-mail in the certificate E-mail for contact with I.CA (mandatory) Prefix Phone number (mandatory)

Insert optional identifier for individuals

Certificate setting

Key type (mandatory) Revocation password (mandatory) Key Repository Type (CSP) (mandatory)

Certificate sent in the ZIP format Certificate containing IC MLSA for communication with the public authorities Choose gender (mandatory)

Allow exporting the key Allow the strong key protection

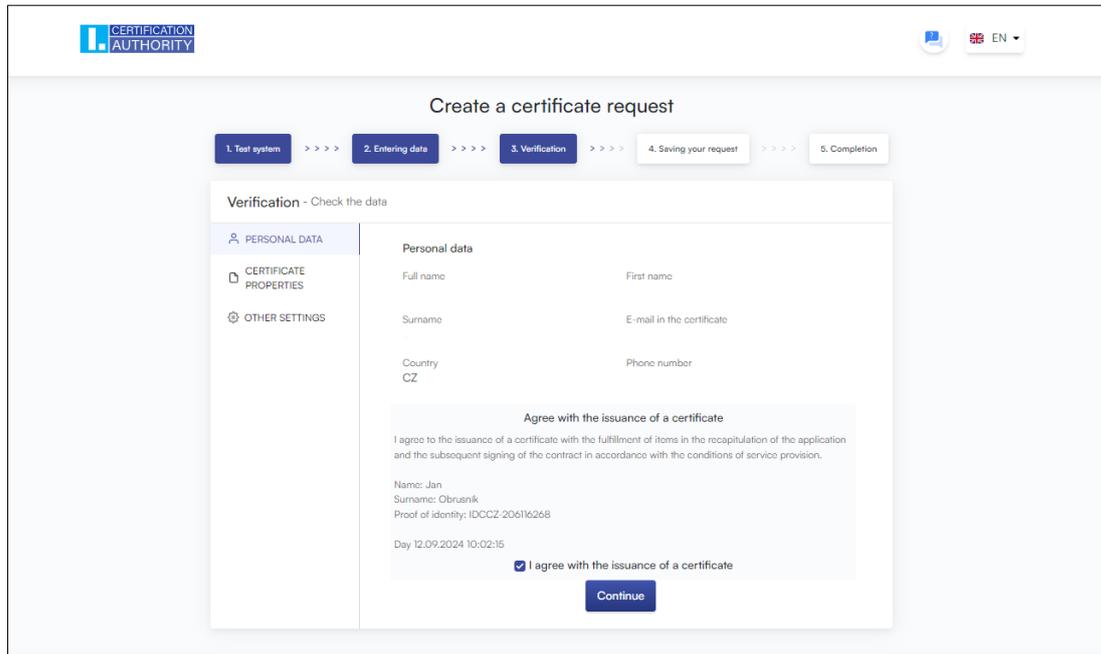
Choose gender

Advanced options

Continue

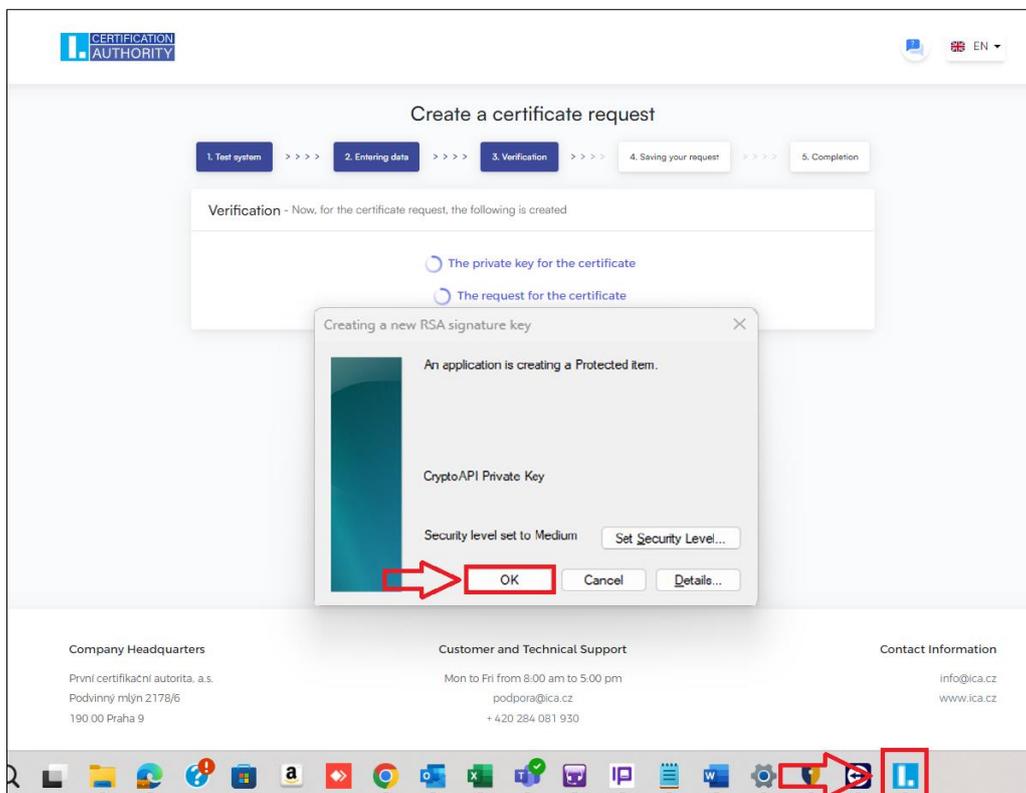
After the data control, agree with the conditions for service providing – see fig. 19:

Fig. 19



On the Windows toolbar, enable the generation of the new RSA signing key – see fig. 20

Fig. 20



6.2.2 Issuance of a certificate online – payment

To pay for the service, select one of the possible payment methods:

- Bank transfer – you will receive a proforma invoice to the contact e-mail address
- By payment card – you will be redirected to the merchant's payment gateway – pictures 21 and 22:

Fig. 21

The screenshot shows the 'Create a certificate request' form at the 'Saving your request' step. The progress bar indicates the current step is '4. Saving your request'. The form content includes:

- A message: 'Request for certificate has been successfully generated. By clicking on "Send the request to be processed" button your request for a certificate will be sent for processing.'
- Price information: 'The price of issuing certificate is 500.00 KC' with a dropdown menu.
- Payment method selection: 'Payment card' (with logos for Mastercard, Visa, and others) and 'By bank transfer' (selected).
- Tax document details: 'Including VAT' (selected) and 'Without VAT'.
- Billing address form with fields for: Company name (První certifikační autorita, a.s.), Identification number (26439395), VAT identification number, Street (Podvinný mlýn), Street number/building (2178/6), City (Praha 9), Zip code (19000), and Country (Czech Republic).
- A 'Send the request to be processed' button.

Fig. 22

The screenshot shows the 'Create a certificate request' form at the 'Completion' step. The progress bar indicates the current step is '6. Completion'. The form content includes:

- A green success message: 'Your request for the certificate has been successfully accepted and will be processed after payment.'
- Receipt information: 'Time of receipt: 12.09.2024 10:09:40'.
- Tracking information: 'You can track the status of your request with ID 6106510000410.'
- Instructions: 'We recommend that you create a backup of your private key. Follow the instructions here: <https://www.ics.cz/Private-key-backup>'.
- Invoice information: 'The advance invoice has been sent to your email address.'
- Final message: 'After payment, the certificate will be issued, which you will receive at the email address specified in the request. The tax document will be sent to you at the same time.'
- An 'Exit the wizard' button.

The user can then uninstall the application from their mobile device, it will no longer be needed for the further process of issuing the certificate.

6.3 Issuance of a certificate online – signing of the certificate issuance agreement

After paying for the service, they will receive a request to their contact e-mail address to sign a contract on the issuance and use of the certificate – see Fig. 23.

Fig. 23

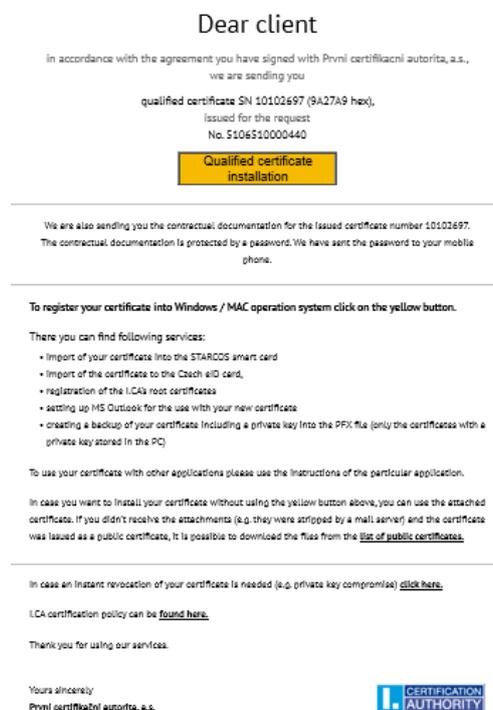


Read the agreement on the issuance and use of the certificate carefully – preview is displayed by clicking the **"Show preview of the agreement"** button, and signing is done by clicking the **"Sign contract"** button. The contract must be signed within three days of receiving the email to sign the contract.

6.4 Issuance of a certificate online – certificate installation

After signing the electronic contract, the user will be sent a link to install the issued certificate and a zipped file with documentation, which will be included in the attachment of the e-mail – see Fig. 24.

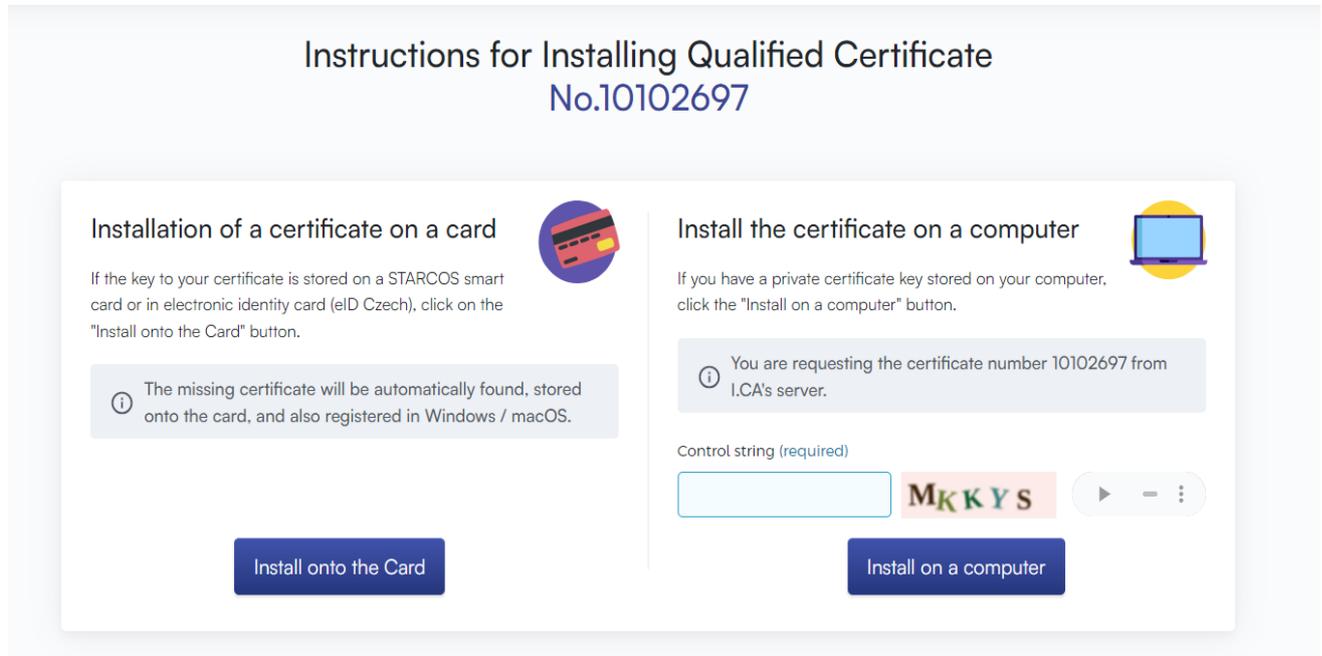
Fig. 24



If the certificate is on a smart card, the user uses the **"Install certificate on smart card"** button – the smart card must be connected to the PC during the installation.

If the certificate is for the MS Windows repository, the user copies the check string and uses the **"Install certificate to PC"** button – see Figure 25.

Fig. 25



6.5 Online certificate issuance – access to electronic documentation

In the sent e-mail for the installation of the certificate, see chapter 6.4, there is a zipped file with an electronically signed agreement on the issuance and use of the certificate. This file is encrypted and can be opened by entering the password that we sent you via SMS after signing the contract.

7 List of document revisions

The table contains a list of revisions made to this document.

Description of the revision	1.0 Create a document	
Drafted	Ing. Petr Kolpek	18.3.2022
Description of the revision	1.02 Updates in relation to the new version of ZealiD TRA Service certification and the release of a new version of the service application for mobile devices.	
Drafted	Ing. Petr Kolpek, Ing. Jan Abel	17.1.2023
Description of the revision	1.03 Update in relation to the new version of the pre-registration form and text editing in the notification email.	
Drafted	Ing. Petr Kolpek, Ing. Jan Abel	30.5.2023
Description of the revision	1.04 Updates in relation to the new version of the ZealiD application and adjustments in the way signed documentation is sent	
Drafted	David Hoření	7.11.2023
Description of the revision	1.05 Update regarding the new version of the ZealiD application, text adjustments, and the new version of online generators.	
Drafted	David Hoření	11.09.2024