

První certifikační autorita, a.s.



Issuance of a certificate online

User documentation

Version: v1.03

Date: 30.05.2023

Worked out by: Petr Kolpek

Contents

1	Introduction.....	3
1.1	Issuance of certificate online – restrictive conditions	3
1.2	Issuance of a certificate online – process.....	4
2	Initial registration of the certificate applicant – data entry	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 authenticity.....	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	Issuance of a certificate online – generating a certificaterequest.....	14
6.1	Issuance of a certificate online – QR code loading.....	14
6.2	Issuance of a certificate online – online I.CA generator.....	15
6.2.1	Issuance of a certificate online– 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	Issuance of a certificate online – access to the electronic documentation repository.....	20

1 Introduction

This document determines terms and issuance procedure of personal electronic certificate (without personal presence at the RA I.CA workplace) with online verification of the applicant's identity, based on verification of the natural person (applicant) identity against the bank and biometric identity verification. This verification is running with usage of the special ZealiD verification application, installed on the applicant's mobile phone or tablet.

Whole process is realized by the form of a step menu. The description of single steps is given below.

1.1 Issuance of certificate online – restrictive conditions

The personal electronic certificate issuance service with online applicant's identity verification is an additional service to the standard process of the personal certificate issuance in presence of the applicant at the working place of public registration authority and can only be provided under the restrictive conditions written below. If it is not possible to accept or fulfil conditions below by the applicant's certificate, it is not possible to provide online certificate issuance service to the applicant. This does not limit the applicant to request electronic certificate issuance in standard way – i.e. a full - time form at the public I.CA RA workplace.

1. Technical conditions

- The user must have functional smartphone with Android or iOS (iPhone) operating system and active internet access, on which he will install the ZealiD utility application (see the procedure below).
- The user must have personal computer with Windows 10 (or higher version) operating system, display with minimum HD resolution and functional internet access.

2. Procedural conditions

- In terms of articles 6, 7 and 9 of the General data protection regulation (GDPR) must applicant, beyond the personal data, provided while issuing the electronic certificate by the presence form (legal requirements), explicitly agreed also with providing and processing the special nature data (biometric data) – concretely photographs of the face and the presented identity document, and their storage on I.CA side for the same period as the data required for the issuance of an electronic certificate by presence form - i.e. data provided by the certificate applicant on the bases of the legal conditions in accordance with European Parliament and Council Regulation (EU) no. 910/2014 (eIDAS regulation) and Act no. 297/2016 about the services creating confidence for electronic transactions. Text for conditions, for which the service can be provided, can be viewed under the link: https://www.ica.cz/userfiles/files/dokumenty/Podminky%20pro%20zadost%20o%20vydani%20certifikatu%20distancnim%20způsobem_AJ.pdf
- Within the frame of data processing, the applicant must confirm his will to sign contracts about issuing and using qualified certificate (see the agreement sample in the link: https://www.ica.cz/userfiles/files/dokumenty/online_smlouva_vzor_EN.pdf with I.CA and electronically sign this agreement before the process is completed.

1.2 Issuance of a certificate online – process

Actual process of applicant's identity verification and issuing of the electronic certificate takes place in several successive steps:

1. Initial registration

- For the initial registration is user asked to enter basic identification data, which will be then checked within the frame of on-line verification process.

2. Install the ZealiD application on a mobile device

- The ZealiD application, which is in relevant markets available for Apple and Android platforms, is used to verify applicant's identity online.



3. Process of online verification in the ZealiD application on mobile device

Within the frame of ZealiD application, the following operations are performed:

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

4. Generating a certificate request

- Operation takes place through the I.CA web interface, where the user is shown the request items obtained from online verification to be controlled and confirmed by the applicant.

5. Service payment

- The user will choose the payment form for the service (by credit card or pro forma invoice).

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

- The user has the opportunity to view an electronic contract and then sign it.
 - contract sample is available to view in the link:
https://www.ica.cz/userfiles/files/dokumenty/online_smlouva_vzor_EN.pdf


7. Obtaining an electronic certificate

- After signing the contract, user will receive issued certificate to the e-mail address mentioned in the frame of the certificate issuance. At the same time, user will receive a link to download an electronic contract for the issuance and use of the certificate.

2 Initial registration of the certificate applicant – data entry

For the initial registration, the user is asked to enter basic identification data, which will be then checked in the frame of on-line verification process. Therefore, it is important to properly check before saving the registration – see fig. 1.

Fig. 1.




PRE-REGISTRATION OF THE APPLICANT FOR THE ON-LINE ISSUANCE OF THE CERTIFICATE

Before issuing the certificate online, a pre-registration of the applicant is required. Please fill in the information below.
After completing the pre-registration, you will receive a registration confirmation and instructions for issuing the certificate online to the e-mail address you provided.

The process of issuing the certificate can be started **24 hours after your registration**.

First name	<input type="text"/>	Surname	<input type="text"/>
Phone number	<div>+ 420 <input type="text"/></div>	E-mail address	<input type="text"/>
Personal document type	<div>Identity card ▼</div>	Document's expiry date	<input type="text"/>
Document's country of issuance	<div>Czech Republic ▼</div>	Document's issuer (optional)	<input type="text"/>
Document number	<input type="text"/>		



If no certificate is 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 ICA certificate.

Before the certificate is issued, your identity will be verified through the ZealiD application, install it on your mobile device. More info [here](#).

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: **Jun 1st 2023 2:23pm to Jun 4th 2023 2:23pm**

Information provided by you to be verified:

First name	<input type="text"/>
Surname	<input type="text"/>
Phone number	<input type="text"/>
E-mail address	<input type="text"/>
Personal document type	<input type="text"/>
Document number	<input type="text"/>
Document's expiry date	<input type="text"/>
Document's country of issuance	<input type="text"/>

Thank you for using our services.

Yours sincerely
První certifikační autorita, a.s.




The on-line process can be started 24 hours after successful registration saving for the next 3 days. see fig. 3.
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

Starting the process for online processing of the request for an electronic certificate is possible on <https://www.ica.cz/english> website in the part Qualified certificate for electronic signature or right under the link <https://www.ica.cz/qualified-certificate-for-esign>, after its opening the start screen containing basic information and related links will be displayed. Applicant must agree with the procedure and conditions for online issuance of the electronic certificate (remotely) or it is not possible to issue a certificate remotely, i.e. provide the service – see fig. 4.

Fig. 4.

ICERTIFICATION AUTHORITY CONNECTED WITH TRUST

 VERIFICATION OF THE APPLICANT FOR THE ON-LINE ISSUANCE OF THE CERTIFICATE

For remote issuance of an electronic certificate (without personal presence at the Registration authority I.CA), online verification of your identity is required, using identity verification with the bank and biometric identity verification. This verification is carried out using a special ZealID verification application, installed on the applicant's mobile phone or tablet.

The process of verification the identity of the applicant and issuing an electronic certificate takes place in several successive steps and includes:

- 1. Installation of the ZealID application on a mobile device**
 - Supported platforms are Apple and Android
- 2. Verification of your identity towards the bank** (takes place within the ZealID application)
 - Verification through these banks is currently supported <https://www.zealid.com/en/coverage>
- 3. Biometric analysis of the face** (takes place within the application ZealID)
 - for the required functionality of the application, it is necessary to allow the ZealID application to access the camera during installation
- 4. Verification of your identification documents** (takes place within the ZealID application)
 - 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
- 5. Generation a request for a certificate** (takes place via the web interface)
- 6. Signing an Agreement on the issuance and usage of an 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, I want to continue" button. If not, click the "I disagree, I don't want to continue" button.

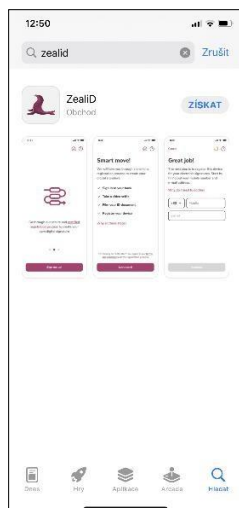
Please note that the issuance of an electronic certificate on-line is only possible if you agree with the procedure described in the previous points and under the following conditions:

- 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 I.CA 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,
- if the online verification does not take place in the required quality or you do not sign an Agreement on the issuance and usage of the certificate before the end of the certificate issuance process, the certificate issuance will not be provided, resp. the generated certificate will be immediately revoked by I.CA.

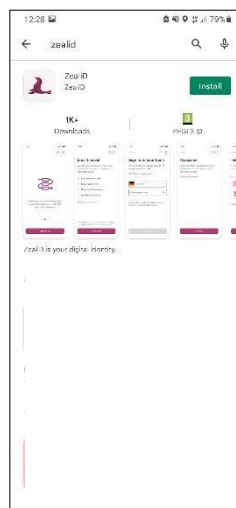
4 Download the application for a supported platform

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

Fig. 5.



ZealiD application for iOS

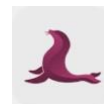


ZealiD application for Android

5 ZealiD application – user verification

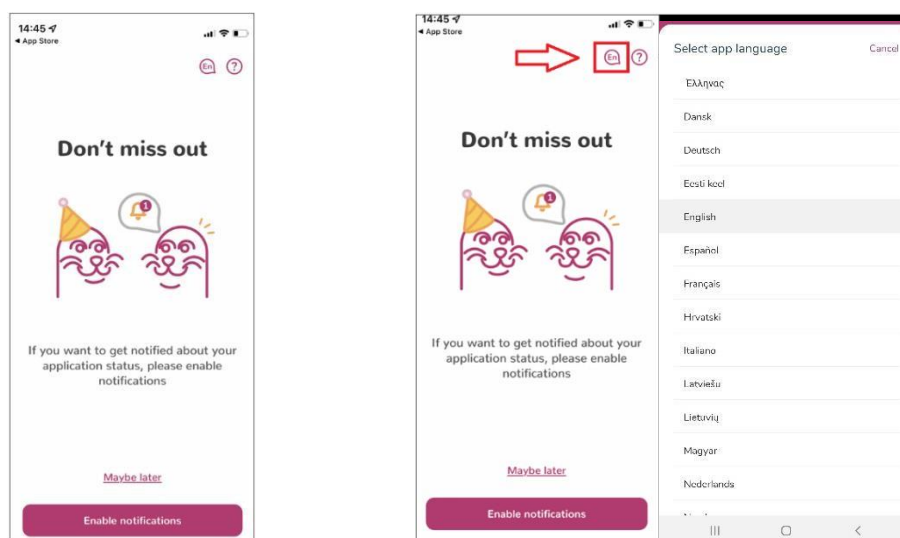
Launch the ZealiD application by the icon from the desktop of your mobile device.

By default, the ZealiD is in English.



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

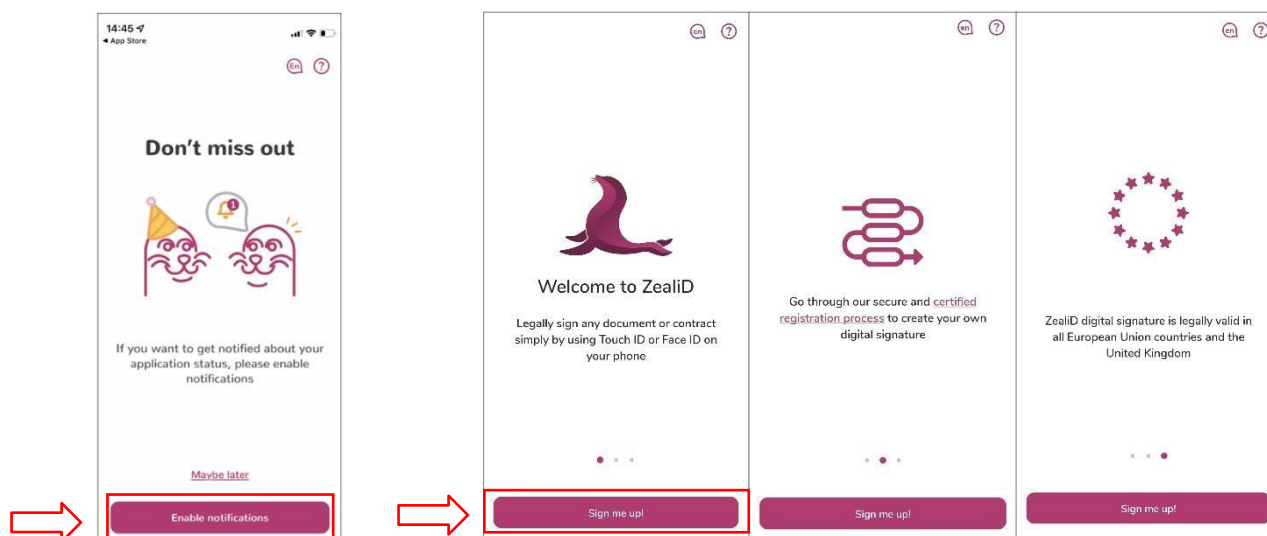
Fig. 6.



5.1 User notification and registration

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

Fig. 7.



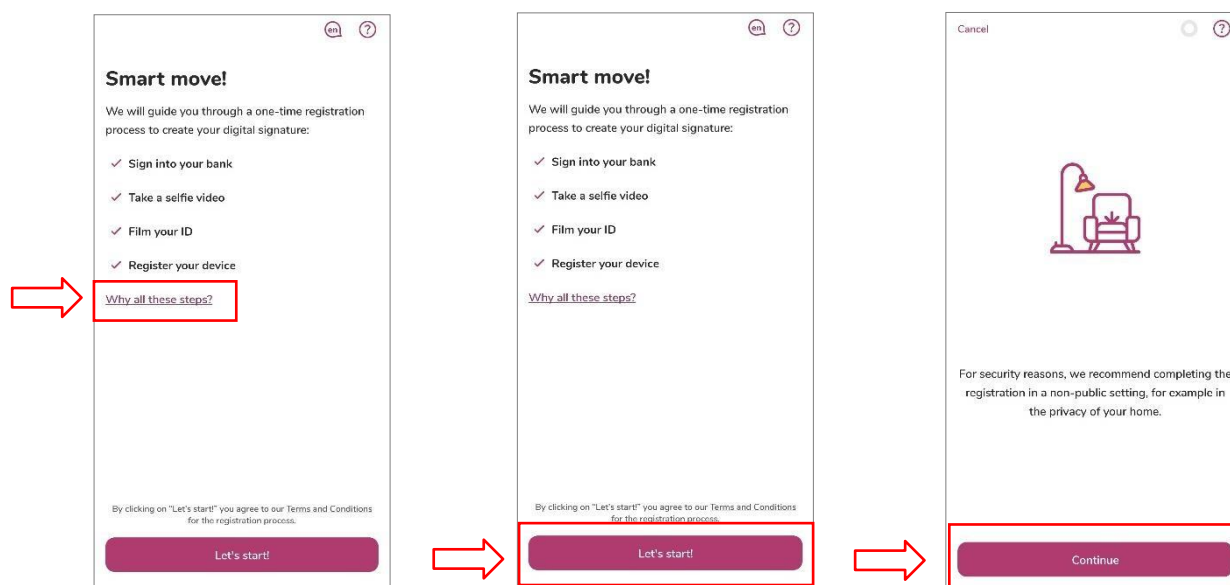
User registration consist from few steps, in following steps the application will require:

- 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 the OTP codes which were sent to your contact phone number or e-mail. Register your device for remote signature authorization and if your mobile device has “Face ID”, you can use it to confirm transaction – see fig. 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

1 0 0 0 - 0 0 0 0

[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

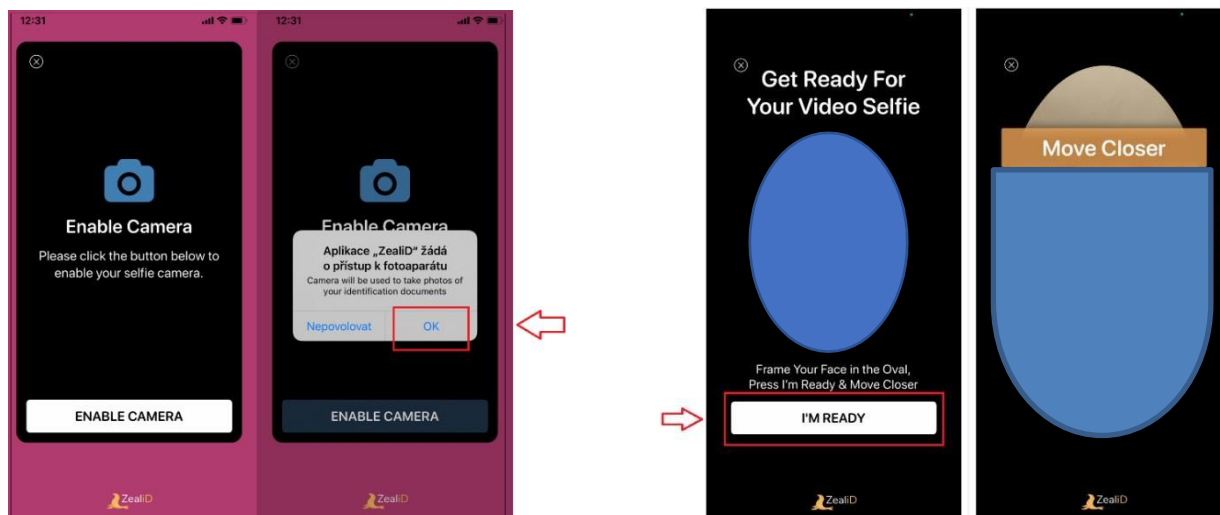
Don't Allow OK

Continue

5.3 Uploading of selfie video – user verification by selfie video

To take a selfie video, application requires permission for access to the camera. Adjust the face to the oval frame of the camera (first from distance and then up close). Wait for the selfie video to be processed – see fig. 11.

Fig. 11.

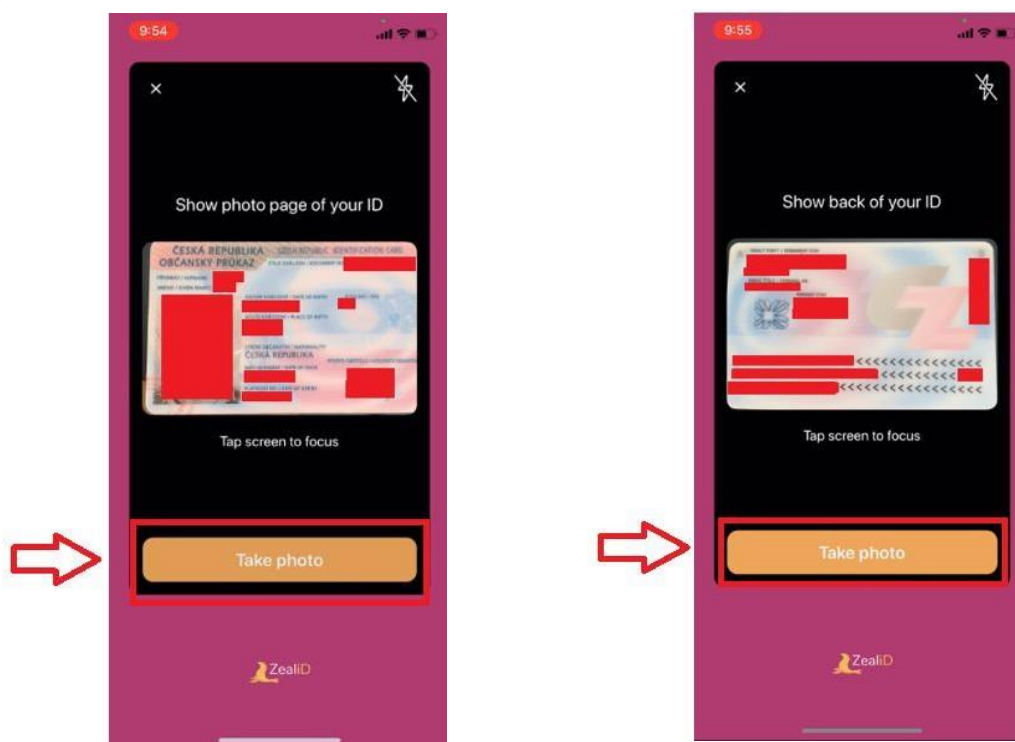


5.4 Picture of the identity document

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.

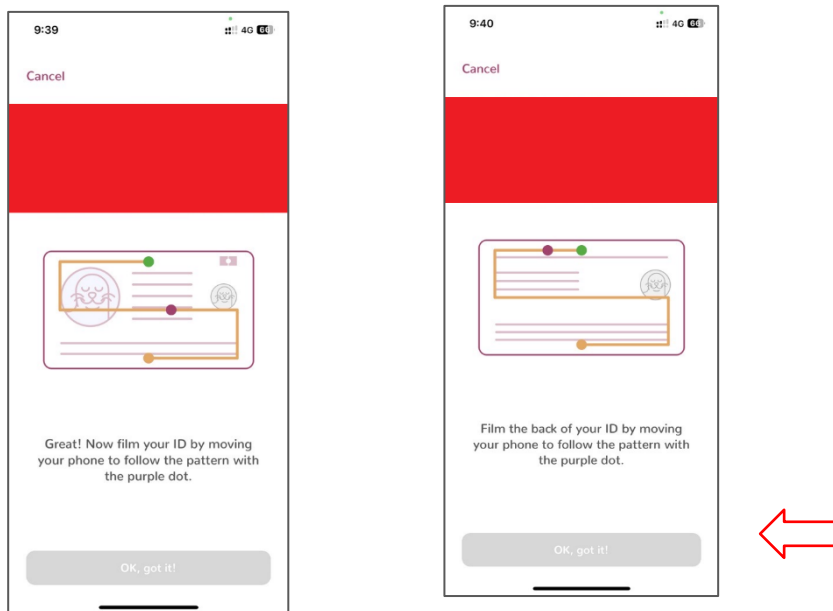
Fig. 12



5.4.1 Identity document picture – verification of a personal document authenticity

Now scan the front of your ID by following the example with the purple dot. Scan the back of you ID in the same way see fig. 13.

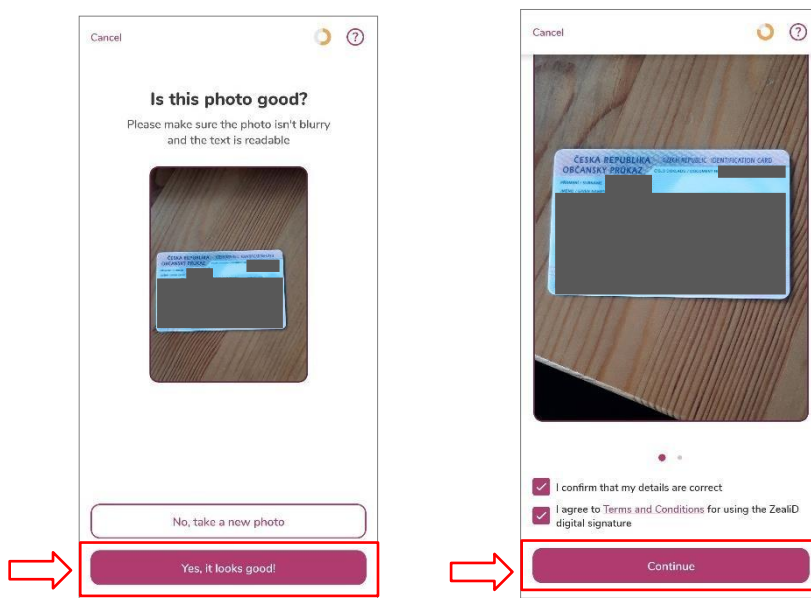
Fig.13



5.4.2 Identity document picture – control of the identity document picture

Control the picture in the front of identity document, in case of illegibility make another picture. Then check the picture in the back of your identity document and in case of illegibility also make new picture – see fig. 14.

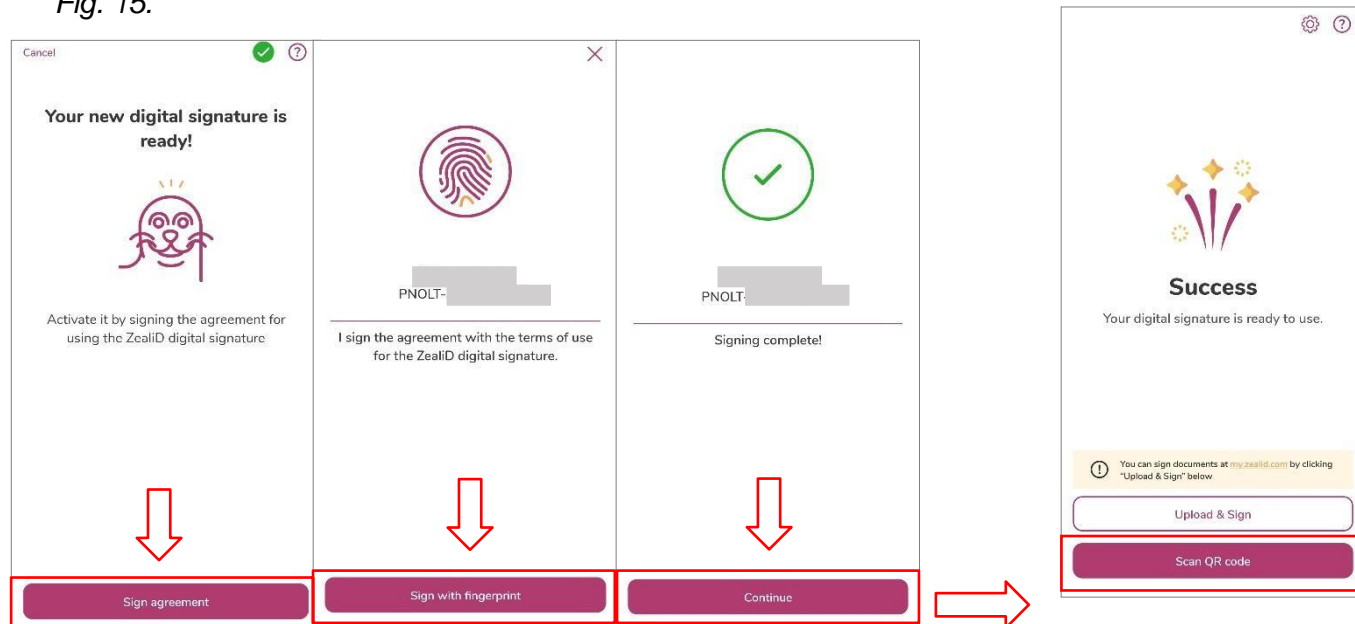
Fig. 14.



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.



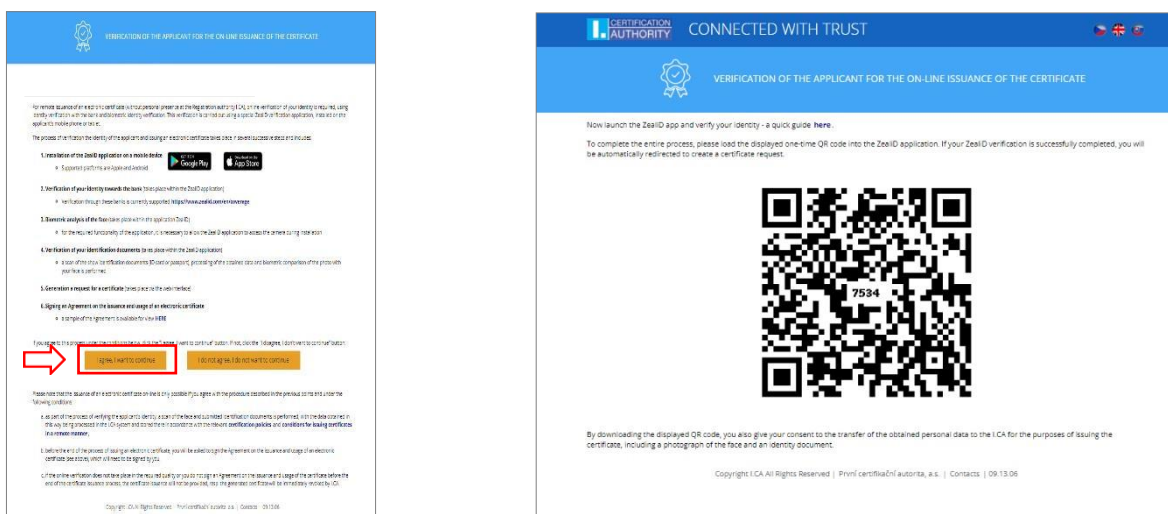
When the applicant's identity is verified in the mobile application, a technology certificate is issued to ensure secure communication during the verification process. This certificate secures the transfer of information between the user and the application.

6 Issuance of a certificate online – generating a certificate request

6.1 Issuance of a certificate online – QR code loading

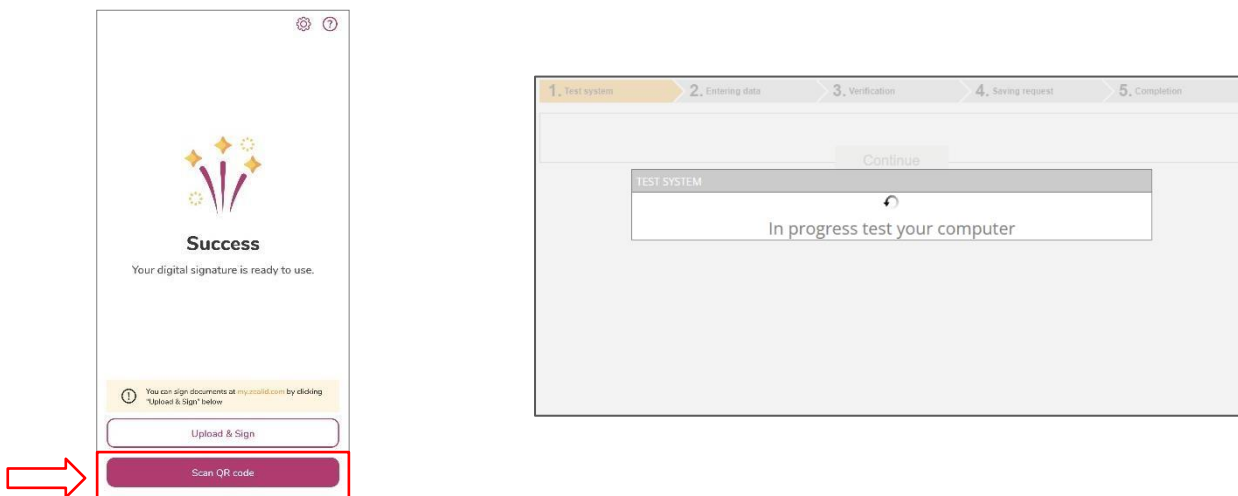
The last step in the ZealiD application is to load the generated QR code, which will be displayed in the I.CA web interface after selecting the “**I agree, I want to continue**” option on the start screen – see fig. 16:

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 Issuance of a certificate online – online I.CA generator

6.2.1 Issuance of a certificate online– 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.

Fill in the following information:

- E-mail mentioned in the certificate
- E-mail for communication with I.CA (documentation for certificate issuance will be sent on this e-mail address)
- Certificate revocation password

Fig. 18.

The screenshot shows the 'CREATE A QUALIFIED CERTIFICATE REQUEST' interface. At the top, the 'CERTIFICATION AUTHORITY' logo and 'CONNECTED WITH TRUST' text are visible, along with flags for the Czech Republic, UK, and Lithuania. A progress bar indicates five steps: 1. Test system, 2. Entering data (current step), 3. Verification, 4. Saving request, and 5. Completion. The main form is titled 'Information about the applicant' and contains several input fields: 'Name' (pre-filled with 'Žošuą'), 'Surname' (pre-filled with 'Kūnpala'), 'Country' (pre-filled with 'Lithuania'), 'E-mail' (pre-filled with 'test@ica.cz'), 'Key type' (set to 'RSA 2048'), 'Revocation password' (set to '1111'), and 'Key Repository Type (CSP)' (set to 'Operating System Windows'). There are three checkboxes: 'Certificate sent in the ZIP format' (checked), 'Allow exporting the key' (checked), and 'Allow the strong key protection' (checked). A link 'Advanced Certificate Options >>' is located at the bottom right of the form. A red arrow points to a 'Continue' button at the bottom center. The footer contains the text 'Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.13.06'.

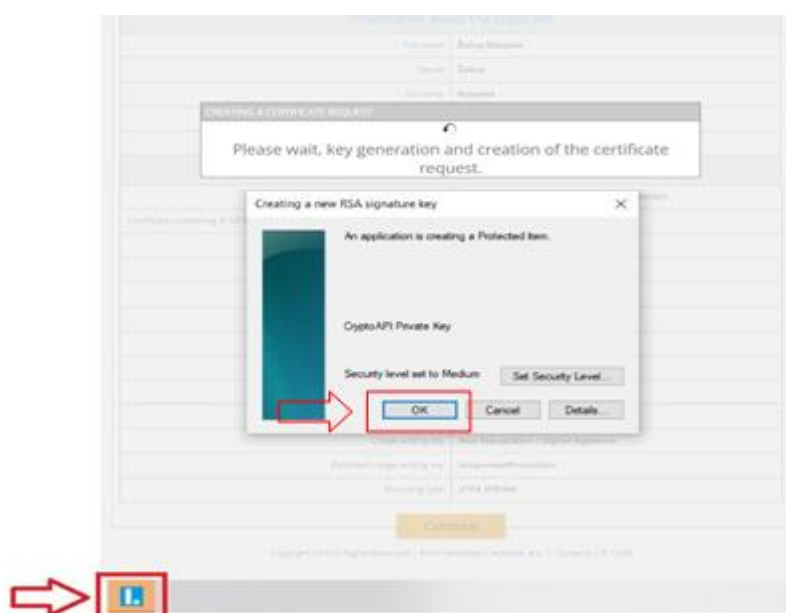
After the data control, agree with the conditions for service providing – see fig. 19:

Fig. 19.

1. Test system		2. Entering data		3. Verification		4. Saving request		5. Completion	
Information about the applicant									
Full name	Žošuq Kūnpala								
Name	Žošuq								
Surname	Kūnpala								
E-mail in the certificate	test@ica.cz								
Country	Lithuania								
Certificate setting									
Type of the certificate	Qualified certificate								
Type of applicant	Current user (individual - non-entrepreneurial)								
Revocation password	1111								
E-mail for contact with ICA	test@ica.cz								
Certificate sent in the ZIP format	Yes								
Period of validity	30 days								
Algortmus podpisu certifikátu	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	Non Repudiation / Digital Signature								
Extended usage setting key	id-kp-emailProtection								
Encoding type	UTF8_STRING								
Agree with the issuance of a certificate									
<p>I agree to the issuance of a certificate with the fulfillment of items in the recapitulation of the application and the subsequent signing of the contract in accordance with the conditions of service provision.</p> <p>Name: Žošuq Surname: Kūnpala Proof of identity: PNOIT-39010101111 Day 25.04.2022 10:18:10</p> <p><input checked="" type="checkbox"/> I agree with the issuance of a certificate</p>									
<div style="display: inline-block; border: 2px solid red; padding: 5px;"> <div style="display: inline-block; border: 2px solid orange; padding: 5px;">Continue</div> </div>									

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

Choose one of the possible ways of the payment to pay for the service:

- Bank transfer – you will receive proforma invoice on the contact e-mail address
- Card payment – you will be redirected to the merchant's payment gateway – fig. 21 and 22:

Fig. 21.

CERTIFICATION AUTHORITY CONNECTED WITH TRUST

CREATE A QUALIFIED CERTIFICATE REQUEST

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

Created request for certificate

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.

The price of issuing certificate is 500.00 CZK

Select currency

☒ CZK
☐ EUR

Billing address

Street Street number / building ide
City / town Zip code
Lithuania

Send the request to be processed

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.13.06

Fig. 22.

CERTIFICATION AUTHORITY CONNECTED WITH TRUST

CREATE A QUALIFIED CERTIFICATE REQUEST

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

Your request for the certificate has been successfully accepted and will be processed after payment.

Request ID for the qualified Certificate : 5106510000071
You can track the status of your application with ID 5106510000071.

Time of receipt : 26.04.2022 12:06:56

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.

Pay

Exit guide

Copyright I.CA All Rights Reserved | První certifikační autorita, a.s. | Contacts | 9.13.06

You can then uninstall the app from your mobile device, it will no longer be needed for further certificate issuance.

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

After paying for the service, you will receive a request to sign the agreement about issuance and use of the certificate, on your contact e-mail address – see fig. 23.:

Fig. 23.



Read the agreement on the issuance and use of the certificate carefully – preview can be displayed by “**Display agreement preview**” button and sign it using the “**Sign agreement**” button.

6.4 Issuance of a certificate online – certificate installation

After signing the electronic agreement, the link for issued certificate installation will be sent on your contact e-mail address – see fig. 24:

Fig. 24.



If it is a certificate on the smart card, use the “**Install the certificate onto the card**” button – smart card must be inserted in the reader connected to the PC.

If it is a certificate in MS Windows storage, copy the control chain and use “**Install the certificate to PC**” button – see fig. 25:


Fig. 25.

**Instructions for Installing Qualified
Certificate No10096119**

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.

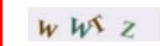
The missing certificate will be automatically found, stored onto the card, and also registered in Windows / MAC.

 **Install the Certificate onto the Card**

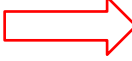
Install the certificate on a personal computer

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 10096119 from I.CA's server.

Control string: 

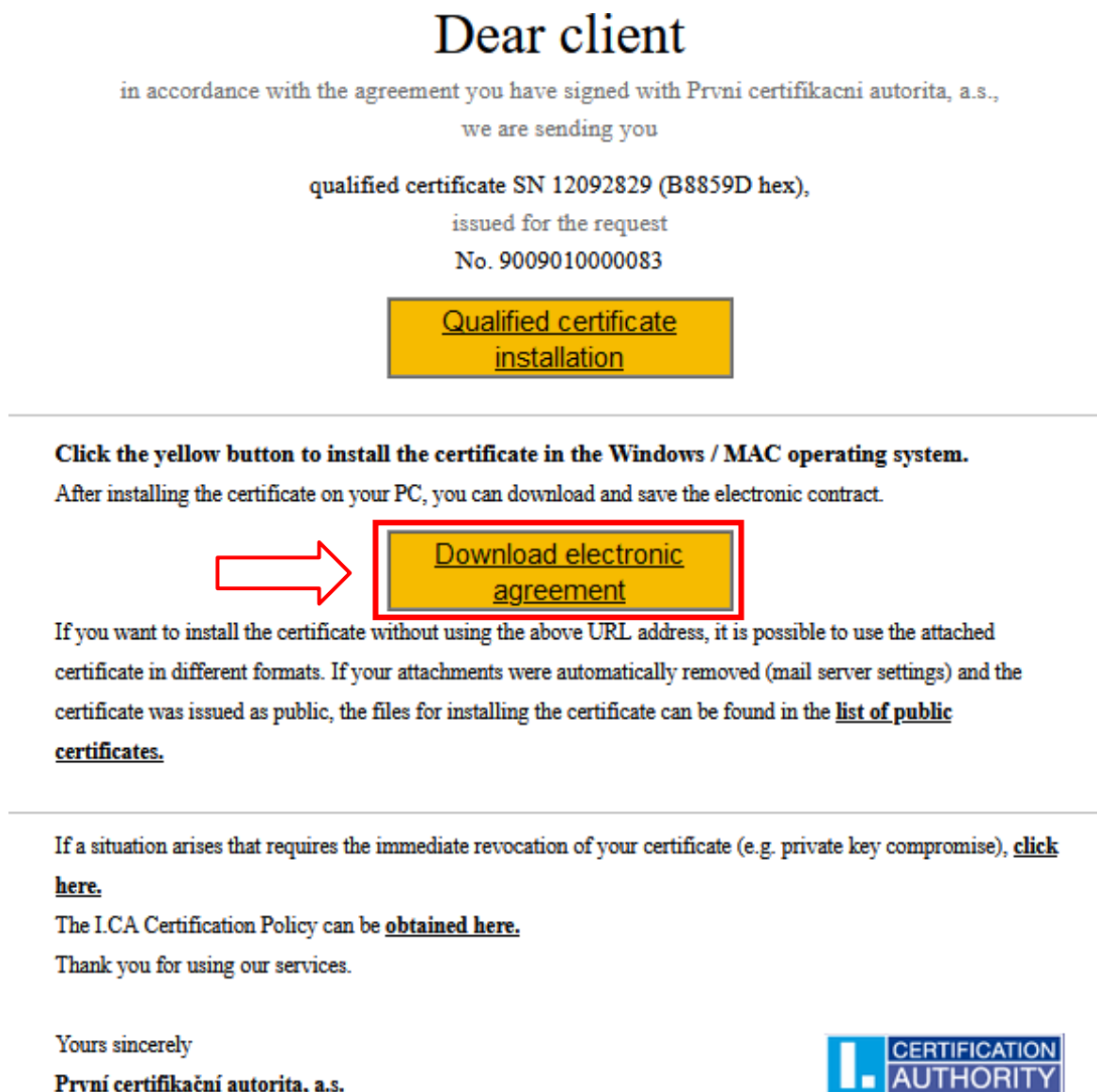
Enter the security code from the picture and click on the "Install the Certificate to PC" button.

 **Install the Certificate to PC**

6.5 Issuance of a certificate online – access to the electronic documentation repository

In the e-mail sent for the installation of the certificate, see chapter 6.2.4., it is possible to download electronically signed agreement about issuance and use of the certificate – see fig. 26:


Fig. 26.



From the list, choose the certificate that **just has been issued** and confirm by the “OK” button.

Write the control chain here at the bottom of the screen and download the signed agreement for issuing and using the certificate – see fig. 27:

Fig. 27.

 CERTIFICATION
AUTHORITY

Úložiště dokumentů

Žošua Kūnpala

VYHLEDAT

Detail dokumentů

ID žádosti	5106510000070
Certifikační autorita	Kvalifikovaná
Typ certifikátu	Q-PE-CZ
Prvotní/Následný	Prvotní
ID plátce	26984
SN vydaného certifikátu	10096119
AKID vydaného certifikátu	FE114B1F9C25D52D16DC930DF4B6A842159E5CA7
ID majitele certifikátu	10072606
Obecné jméno	Žošua Kūnpala
SN žadatele	10096119
AKID žadatele	FE114B1F9C25D52D16DC930DF4B6A842159E5CA7
ID žadatele	10072606
Čas vložení dokumentu	26.04.2022 11:09:15

Dokumenty

Typ dokumentu	Čas poslední změny	Formát dokumentu	
Smlouva o vydání a používání certifikátu	26.04.2022 11:56:32	.pdf	<div>Stáhnout</div>

Kontrolní řetězec:

PE

PEN