



Instructions for activation and installation of Certum

Document Signing certificates

version 1.2

Table of contents

1. Product description	3
2. Initiation of certificate activation	3
3. Completion of the form during activation	4
4. Verification of identity.....	6
5. Access emails to the SimplySign service	8
6. Installation of the Simply Sign app.....	9
7. Activation of access to SimplySign service	9
8. Reading the QR code	10
9. Import the certificate from the Simply Sign Desktop level	11

1. Product description

A Document Signing certificate is a certificate designed for signing documents in accordance with the AATL policy. It allows to make a digital signature that is positively verified by Adobe.

In order to obtain a certificate, follow a few simple steps:

- Apply for the certificate
- Install the Simply Sign Mobile and Simply Sign Desktop apps
- Verify your identity and association with the company for which you are submitting the certificate request
- Activate your access to Simply Sign with the QR method
- Start signing documents using your computer or mobile device
-

Note: Document Signing Certificate uses a cloud-based mechanism in SimplySign system that uploads the certificate automatically to a virtual account. The virtual account is created during the activation process, to the email address provided in the application. If you have an account, you can reuse it by providing the email address for your existing account.

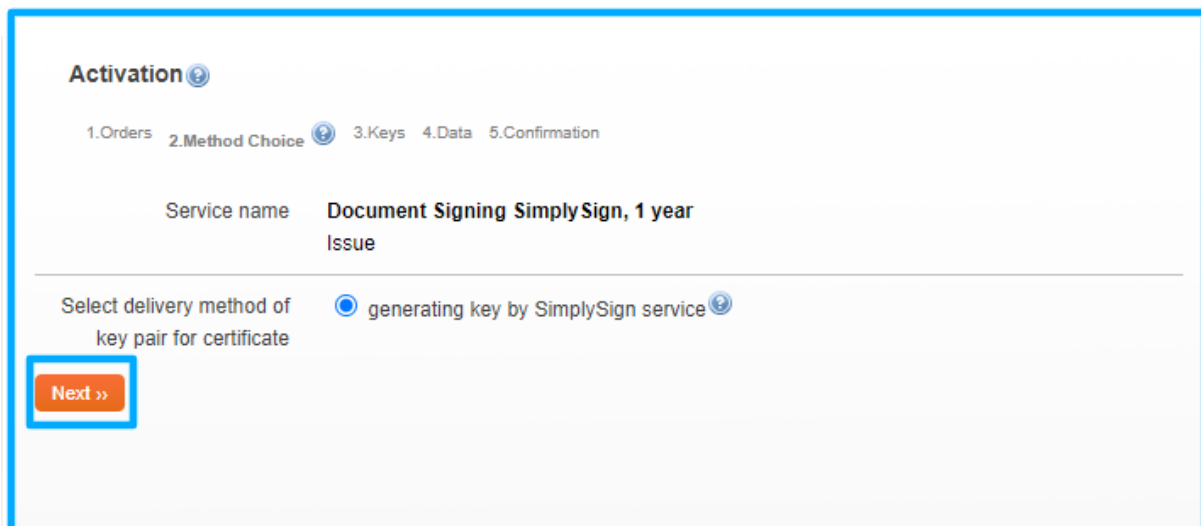
2. Initiation of certificate activation

Once you have placed your order, initiate the activation of your certificate from the [Certificate Activation](#) tab.



In order to do so, locate the appropriate certificate on the list, in this case - Document Signing Simply Sign, and then click the [Activate](#) icon.

The Service Activation window will appear, where you should select the [Key generation via the SimplySign service](#) option, and then click [Next](#).



This step will enable your certificate keys to be automatically generated.

3. Completion of the form during activation

The next step is to complete the certification request form with the data that will be contained in the certificate. Please note that the fields with an asterisk * are mandatory. Remember that the Applicant data should be the same as the certificate data.

NOTE: In the "Simply Sign account" field, enter the email address that you would like to use to create your account in Simply Sign system. You can also use existing account. If you already have an account and want to upload the certificate to an existing account, enter the e-mail used in this account.

Activation

1.Orders 2.Method Choice 3.Keys 4.Data 5.Confirmation

Service name **Document Signing SimplySign, 1 year Issue**

Applicant data:

Name *

Surname *

Phone *

Email *

Simply Sign

Emailapplicant.taxIdentificationNumber=Registration Number *

applicant.taxIdentificationNumber

Certificate Data:

Common name *

Hash function RSA-SHA256

Shortened validity period

Organization *

Organizational unit

Locality

Country *

State

Email *

In accordance with Article 13 sec. 1 and 2 of the General Data Protection Regulation (GDPR) of 27 April 2016 (hereinafter referred to as the "Regulation") I hereby inform that:

1. The Administrator of your personal data is Asseco Data Systems S.A. seated in Gdańsk, Jana z Kolna 11, 80-864 Gdańsk;
2. The Data Protection Officer of Asseco Data Systems S.A. can be reached at the email address: IOD@assecods.pl, or phone number +48 42 675 63 60.
3. Your personal data will be processed for the purpose necessary for the performance of the non-qualified certificate agreement pursuant to Article 6 sec. 1 letter b of the Regulation.
4. Your personal data will be stored for a period of: 7 years from the date of revocation or expiration of the last certificate issued on the basis of this data, in accordance with the CA/Browser Forum Baseline Requirements for the Issuance and Management of

<< Previous Next >>

Then verify that the data is correct.

NOTE: Note that when activating the Document Signing certificate, there is no option to select identity verification. The certificate is always verified using the Automatic Verification method.

Certificate Structure:

Subject E=anna.sikorska@assecods.pl, CN=Anna Sikorska, O=Asseco Data Systems, OU=Security&Trust Division, L=Szczecin, C=PL

Subject Alt. Name rfc822Name=anna.sikorska@assecods.pl

Verification method * automated identity verification (recommended)

The automated identity verification will only start after the verification of the organisation's details is completed. Verification instructions will come in a separate email. If verification fails, documents will be required.

Terms of Use

BEFORE SENDING TO CERTUM A REQUEST TO ISSUE CERTIFICATE, OR ACCEPTING CERTIFICATE OR THE FIRST USE OF IT, PLEASE READ THE TEXT OF THESE „TERMS OF USE FOR NON-QUALIFIED CERTIFICATES” REFERRED TO AS „TERMS OF USE”. IF YOU DO NOT ACCEPT THESE TERMS OF USE, DO NOT SEND THE REQUEST TO ISSUE CERTIFICATE, DO NOT ACCEPT IT AND DO NOT USE IT.

THESE TERMS OF USE BECOMES EFFECTIVE FROM THE MOMENT OF SUBMITTING THE CERTIFICATE REQUEST TO „CERTUM - Certification Authority” (HEREINAFTER „CERTUM”) AND ARE VALID UNTIL THE END OF CERTIFICATE VALIDITY PERIOD OR UNTIL THE CERTIFICATE REVOCATION. SENDING THE CERTIFICATE REQUEST MEANS THAT YOU WANT CERTUM TO REVIEW THE APPLICATION AND ISSUE THE CERTIFICATE, AND

I agree to Terms of Use *

I declare and confirm that I am aware of the fact that the certificate may expose my personal data to the extent it has been indicated for inclusion in the certificate. I also confirm that all activities carried out using this certificate may, at my discretion, be available without restriction, in particular with regard to location. The use of the certificate is not affected by Asseco Data Systems S.A., provider of security services. *

I confirm that I am of age *

I hereby confirm the accuracy of my personal data included in the application for the certificate. *

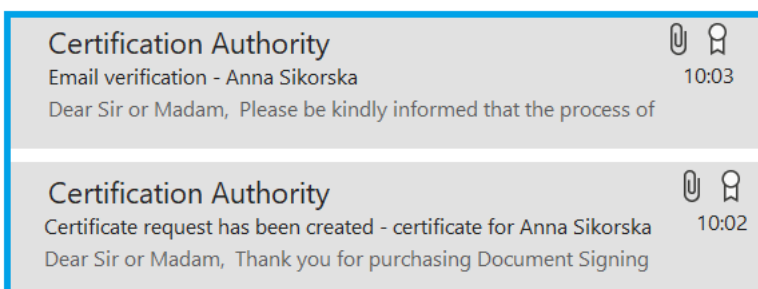
*Required

Tick the required consents and confirmations and click [Activate](#).

Correct submission of the certificate request results in the receipt of an email: Certificate request has been created

After the certificate request is successfully submitted, the email address needs to be verified. Email verification is only required when an email address has been provided in the request.

In order to verify the address go to the email and click on the link. Once you have clicked on the link, you will be taken to the Certum screen where you can click on the icon: Verify



4. Verification of identity

Automatic identity verification is necessary to issue a Document Signing certificate. The entire process is performed using a computer or other device with access to a camera, from a maintenance-free interface. During scanning, the document Data are automatically extracted and analyzed as well as compared to the Owner's face. The process is based on comparison of a facial image with a photo extracted from an identity document. The biometric solution ensures that the User is present during the identity confirmation. The entire process is live, in real time, and does not require sending documents, they are only scanned during the process to extract the data needed for verification and

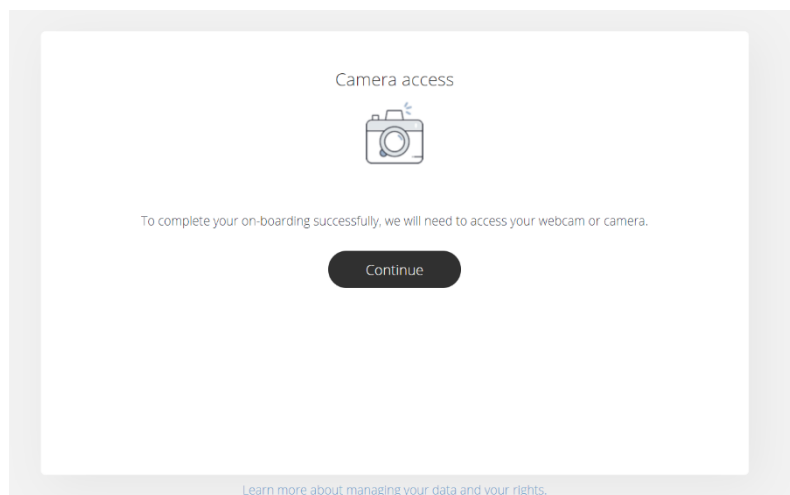
What does the process during certificate activation look like?

- In the certificate activation process, when selecting an identity verification method, select the method: **Automatic identity verification**
- After submitting the application, the User receives a unique link to the indicated email address
- After clicking on the link, the User is taken to the Certum screen on which the Automatic Verification process can be started. The User will then receive a link that initiates verification.
- Depending on the device on which the verification is performed, the process is different.

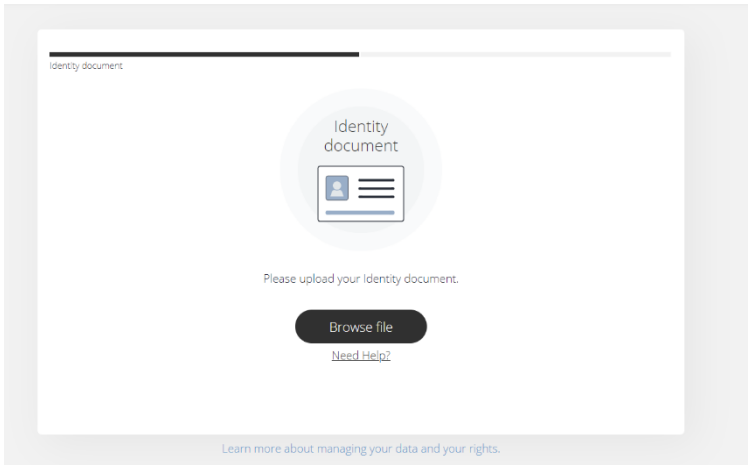
Verification using a computer

Step 1 — Document verification

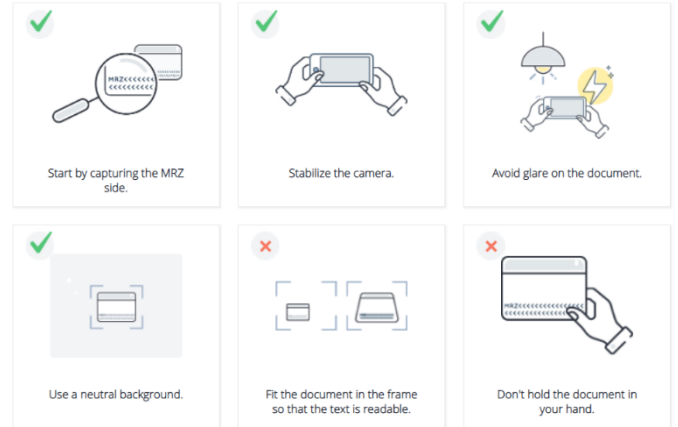
After clicking the link to initiate verification, you will be prompted to turn on your camera, so your identity can be verified. Click "Continue" and proceed to the next step.



You will then be asked to upload a photo of your identification document. The photo provided should be taken according to the guidelines provided during the process.



How to take a good picture of a document.

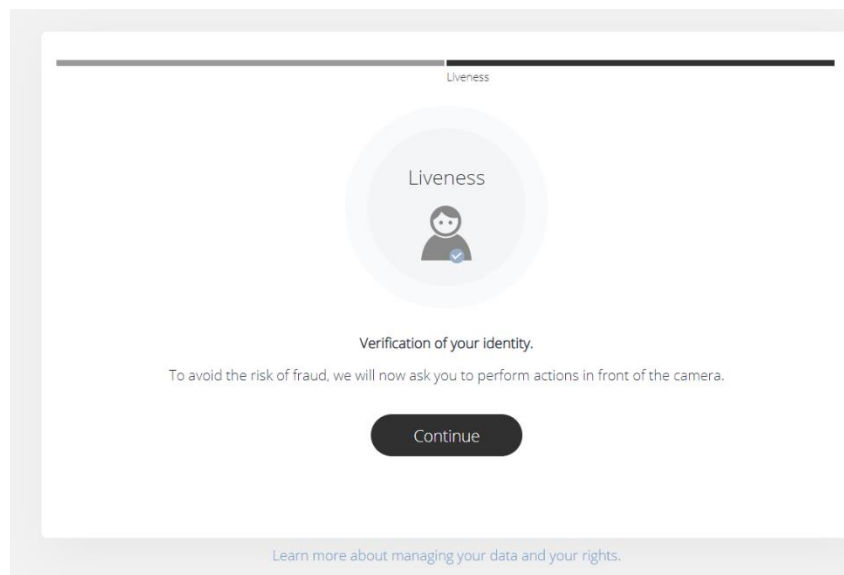


I understand

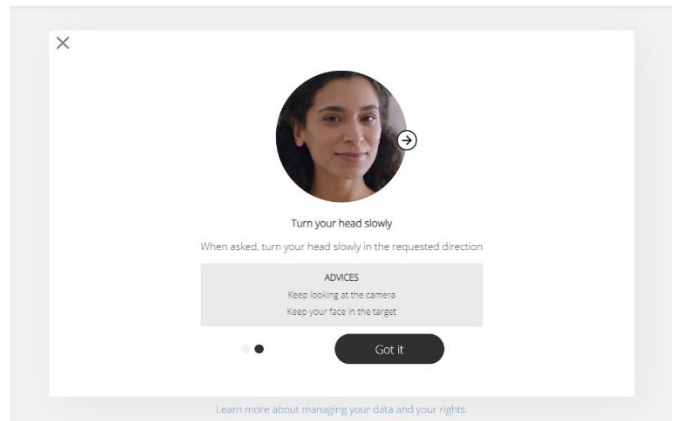
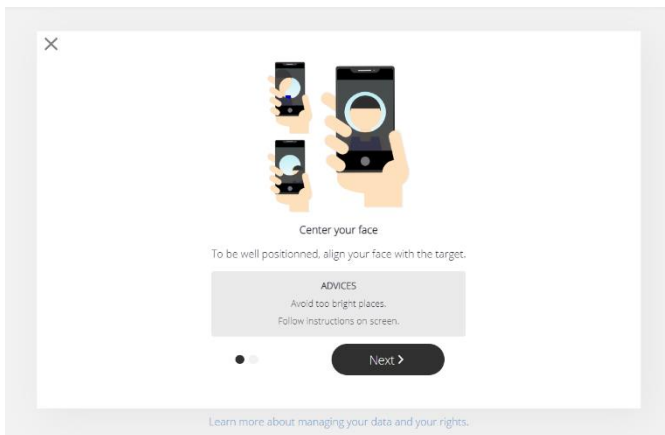
Once the data are submitted, the system will process it for approximately 12 seconds to extract the data from the document. After this process, the document image will be deleted.

Step 2 — Facial comparison

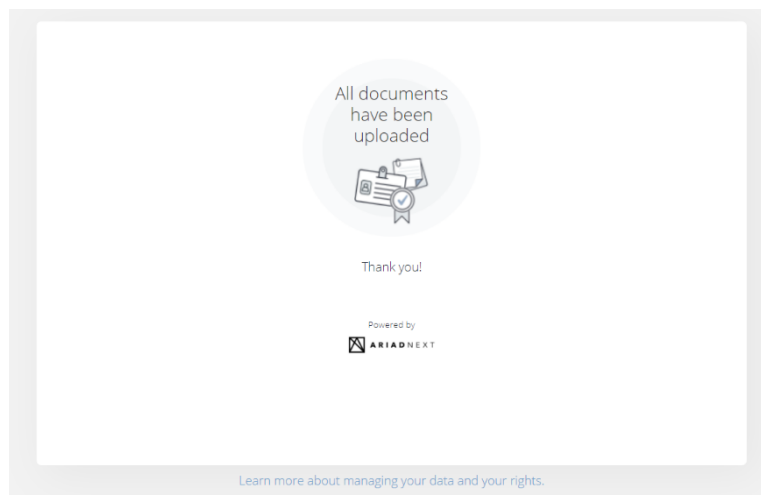
During this step you will be asked to move your face in front of the camera. This biometric solution will ensure that the User is present during the identity confirmation and is the holder of the document.



Performing this step requires you to point your face toward the center of the camera and then move your head toward the right side, looking at the camera the entire time.



After completing this step, a screen indicating that the verification was successful will be displayed. Your certificate will be issued shortly.



Mobile phone verification

The verification process is similar, but in step one, the user does not provide a pre-made photo but takes one live during the process.

5. Access emails to the SimplySign service

Once the certificate has been issued, the Certum system sends the following email messages to the user. At the same time, an account is automatically created for the user who does not have an account in the Simply Sign app. The account will be created using the email in the application.

- a) Confirmation of creating the certificate:

Certificate request has been created

- b) Secret code (activation code) needed to recover access to the service

Secret for regaining access to the SimplySign service

c) Recovering access to the service

Regaining access to the SimplySign service

6. Installation of the Simply Sign app

Note: This process is dedicated to users who do not have a Simply Sign account or app. If you have an account with an email address linked to the Certum shop and have the app installed go to the section [Certificate Import](#)

In order to fully activate the service, you will need both the mobile app and the Desktop app:

To download the mobile app use the links below:

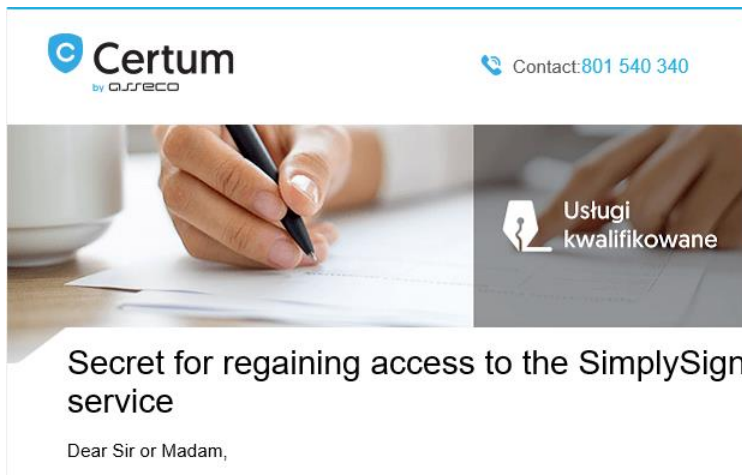
- App for Android phones: Google Play Store: [download](#)
- App for iOS phones: App Store: [download](#)

To download the PC app, use this link: <https://simplysign.certum.pl/pobierz/>

Make sure you have selected the correct version for your operating system.

7. Activation of access to SimplySign service

In the first step, open the email [Secret for recovering access to the SimplySign service](#). Copy the Secret activation code it contains. It will be required to run the Simply Sign mobile app.



Then open the email titled [Recovering access to the SimplySign service](#). Click on the link [Certum Service](#). Next, a window will open in which you should enter the Secret activation code you copied earlier. Then click the [Send](#) button

Certum
w uzasadnieniu

Contact: 801 540 340

Usługi kwalifikowane

Regaining access to the SimplySign service

Dear Sir or Madam,

In order to regain your access to the SimplySign service and the generator of one-time authorization passwords Token, required for logging in / authorization in the Certum service, please follow the instructions below:

- 1. Launch the SimplySign app on your mobile device**
(using this app you should scan the QR code necessary for the authorization of unlocking of the SimplySign service and the generator of one-time authorization passwords Token)
- 2. Prepare the 6 character activation code, which you obtained via the Certum Technical Support.**
- 3. Begin the procedure of recovering access to the SimplySign service by clicking on the link:**

Certum service: <https://model.simplysign.webnotariusz.pl/arc/app/resetseed?token=8786d294ac486823556e95b23988333d02ba6ec9e5d3966d5c51e8c474ac70fb>
(Click or copy the link to the web browser and regain access to SimplySign)

Odzyskiwanie dostępu do usługi SimplySign (Recovering access to the SimplySign service)

* Podaj sekret podany przez operatora (Enter secret provided by operator)

Wyślij (Send)

A QR code will be displayed, which must be read using the Simply Sign mobile app.

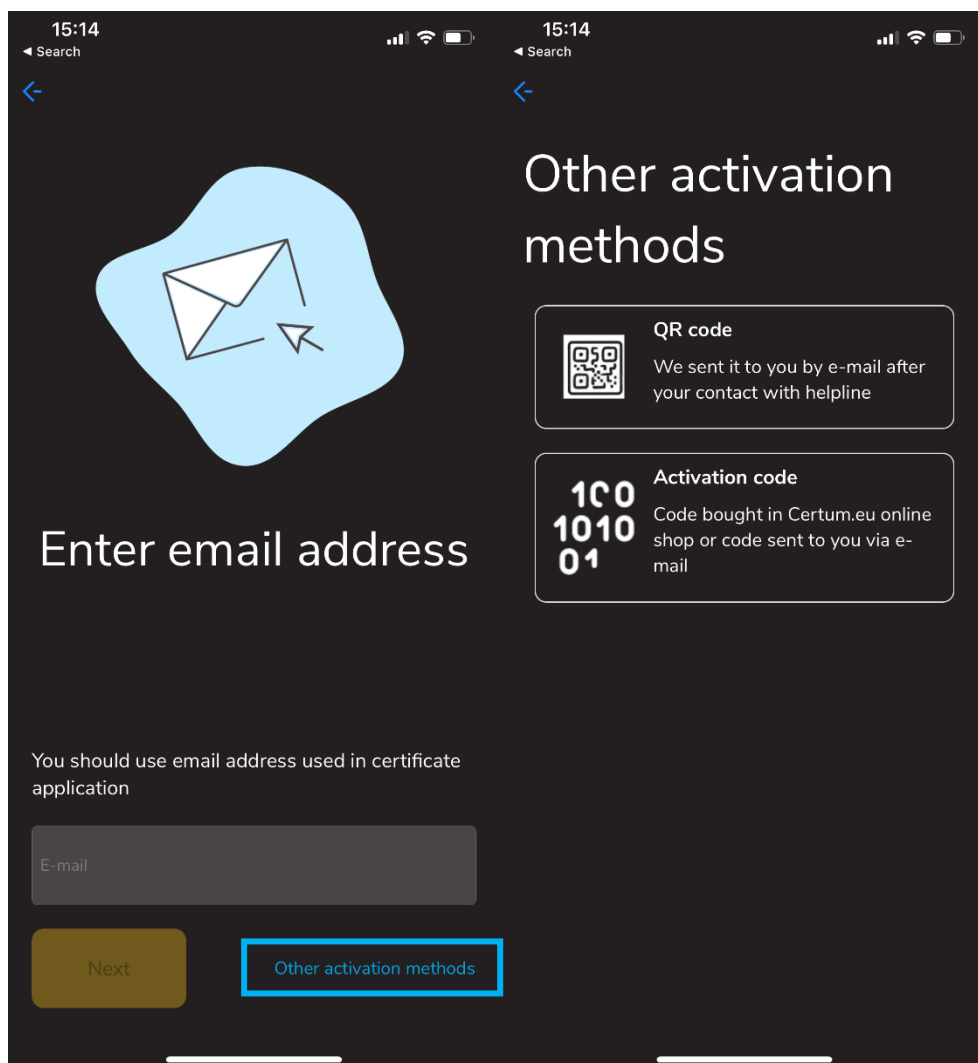


8. Reading the QR code

To read the QR code, follow these steps:

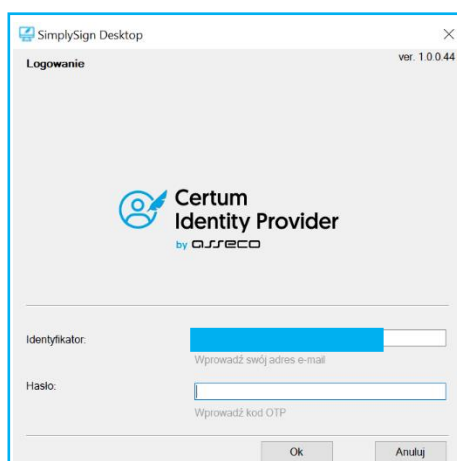
- Run the previously installed SimplySign mobile app
- Click on Other activation methods
- Click on the QR CODE button
- Allow access to the camera and read the QR CODE value from the browser screen

Once you have completed these steps, the app is ready to run



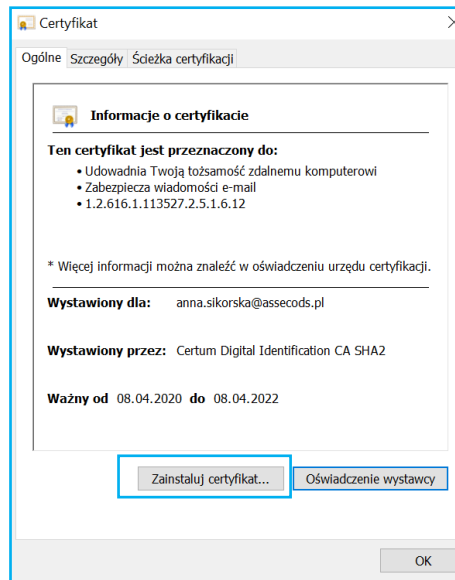
9. Import the certificate from the Simply Sign Desktop level

To import the certificate you need to open the SimplySign app on your computer. To log in, generate an OTP code (token) in the SimplySign Desktop app, then type it in the Password field. Proceed in this way each time to start the app.

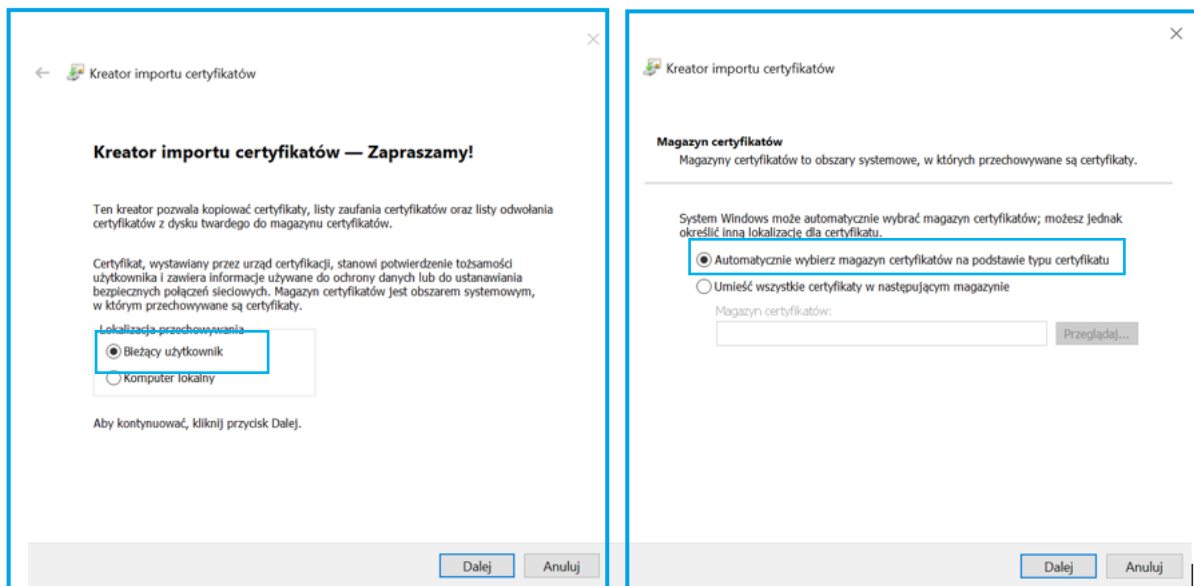


In order to import the certificate, right-click the SimplySign icon in the right-hand corner of the taskbar and then select: [Managing certificates -> List of certificates](#). Once this command is completed, a window with a list of available certificates will open.

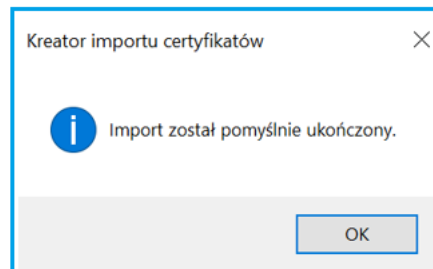
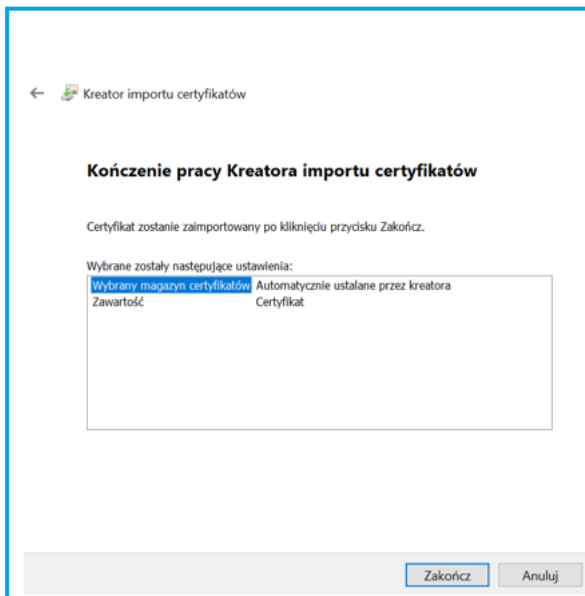
Right-click the certificate you wish to export and choose [Show certificate](#). The details of the certificate will be displayed and the [Install certificate](#) command will be available. Select this command.



The Import Wizard window will then open. Perform the import as the [Current User](#) and Continue. In the next window, select [Automatically select a certificate store](#) and continue.



The final step will be to close the Import Wizard. A confirmation of successful completion of all steps will be a pop-up window stating that the import was successful.



Once you have completed these steps you can start signing the Documents!