

SimplySign iOS

Instruction manual



SimplySign iOS version 6.1

Table of Contents

1. Legal information	4
2. Introduction.....	5
3. Requirements	5
4. Application installation.....	5
5. Biometric Security	7
6. Launching, activation of the application or resetting access to the service.....	11
6.1. Launching the application	11
6.2. Service activation	12
6.2.1. Activation using (personal) authentication data	12
6.2.2. Activation using the activating code	16
6.3. Resetting the access to the service	21
6.3.1. Manual reset using the 16-character resetting code	23
6.3.2. Automatic resetting with the use of QR Code.....	27
6.4. Signature without activation	32
6.4.1. Application not activated	32
6.4.2. Application in the „Signing and Generate token” mode	34
6.5. Application operating modes	37
6.5.1. Operation in "Generate token code"	37
6.5.1.1. Force time synchronization	37
6.5.2. Working in the „Signing and Generate token” mode.....	39
6.5.3. Changing the application operating mode	39
6.6. Multiple accounts support	39
6.6.1. „Signing and Generate token” mode	40
6.6.2. "Generate token code" mode	42
6.7. Logging into the application	45
6.7.1. „Signing and Generate token” mode	45
7. Application Settings/Options	48
7.1. „Account management” option	49
7.2. Signature section	50
7.2.1. „Certificate and cards” option.....	50
7.2.1.1. Setting the default certificate.....	51
7.2.1.2. Warning of impending expiry of the certificate	52
7.2.2. „Additional text” option	53
7.2.3. „Sign reason” option	56

7.2.4.	„Localization” option	60
7.2.5.	“Visualize signature” option	65
7.2.5.1.	Font style	66
7.2.5.2.	Font color	67
7.2.5.3.	Alignment	69
7.2.5.4.	Template.....	69
7.2.6.	„Facsimile management” option.....	71
7.2.6.1.	Adding your own facsimile	71
7.2.6.2.	Changing the default facsimile	76
7.2.6.3.	Removal of facsimiles	79
7.2.7.	„Trusted time stamp” option	82
7.2.8.	“Generate report” Option	82
7.3.	Application Settings Section.....	87
7.3.1.	„Device function” option.....	87
7.3.2.	„Notification” option	87
6.3.3.	„Factory reset” option.....	87
6.3.4	„About appication” option	87
7.	Signing files.....	88
7.1.	Adding a file to the list of files to be signed	88
7.2.	Starting the proces of file signing	90
7.3.	Selection of the Signing certificate.....	90
7.4.	Entering the PIN code to the selected Signing certificate.....	91
7.5.	Signing a file.....	92
8.	Signing multiple files at a time	93
9.	Making a signature with visualization	95
10.	Changing the default certificate while Signing files	97
11.	Importing files from external applications	100
12.	Handling errors when Signing files	103
12.1.	Incorrect PDF file	103
12.2.	Secured PDF file.....	104
12.3.	Incorrect PIN to the Signing certificate	104
12.4.	Blocked card	105
13.	Handling the signed files	105
13.1.	Sending of signed files by e-mail	105
13.2.	Save signed documents to iCloud Drive	108
14.	Deleting files.....	111

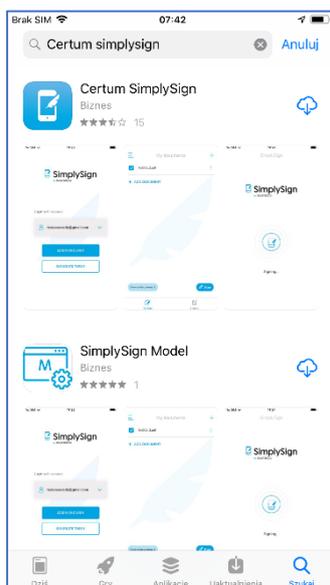
1. Legal information

Proprietary copyrights to this documentation and the software described hereto are vested in **Asseco Data Systems S.A.** with its seat in Gdańsk, ul. Jana z Kolna 11. The above rights are protected by the Act on Copyrights and Related Rights (Journal of Laws No. 24, item 83 dated February 4, 1994, as amended).

The below documentation is distributed based on the granted license.

2. Introduction

The **SimplySign** application for iOS system allows the users to sign PDF documents based on the virtual card with qualified certificate or common certificate. The application supports electronic signature in PAdES format (PDF Advanced Electronic Signature ETSI TS 102 778) and uses CAdES or PKCS#7 standards to describe data structures containing a signature.

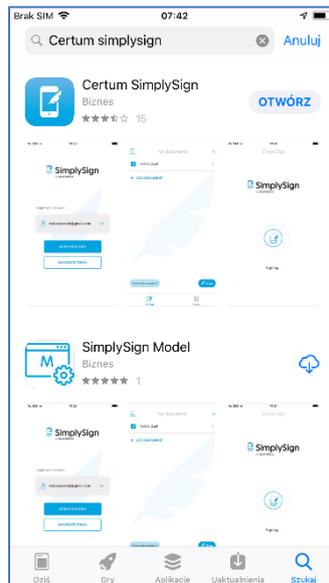
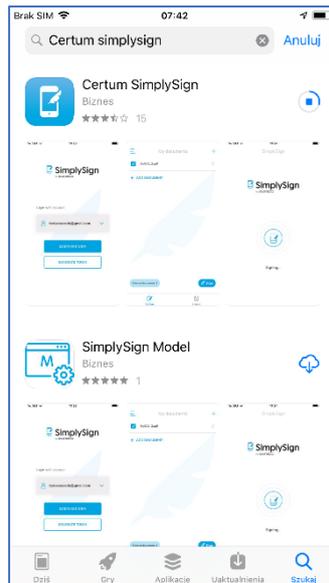


3. Requirements

The **SimplySign** application requires the **iOS** system in version 11+, at least one registered and initialized virtual card, active account in the **SimplySign** service and qualified/common certificate(s).

4. Application installation

In order to install the application on devices with **iOS** system, you have to open **App Store**, find **Certum SimplySign** application and then install it. Please pay special attention to install **Certum SimplySign** application and not **SimplySign Model** application. The **Certum SimplySign** application should be installed.



After correct installation, the **SimplySign** application icon will appear on the device Desktop.

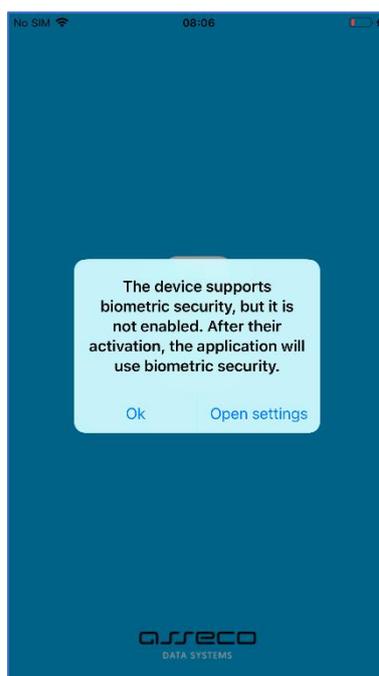


5. Biometric Security

The app supports the use of biometric security set on the device. If the device's operating system is set to use fingerprint or facial image biometric security, it will force authentication with the selected security method when the app is launched.

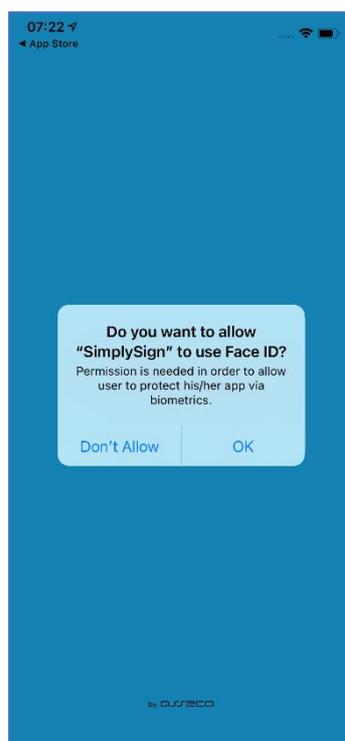
Biometric security works according to the following logic:

- A. If the device supports biometric security but it is not enabled then the following message appears when the application is launched:

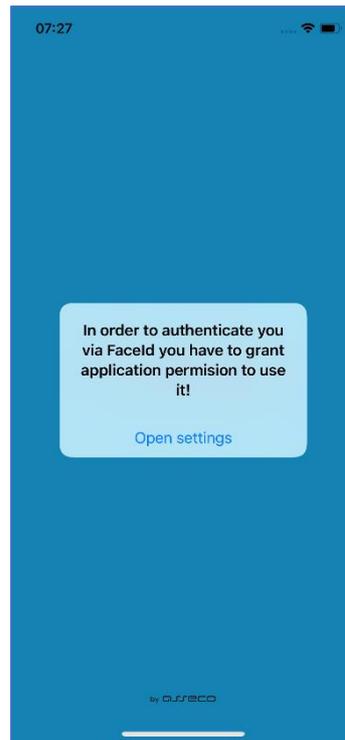


Pressing **Open settings** takes you to Settings, where you can set Touch ID/Face ID

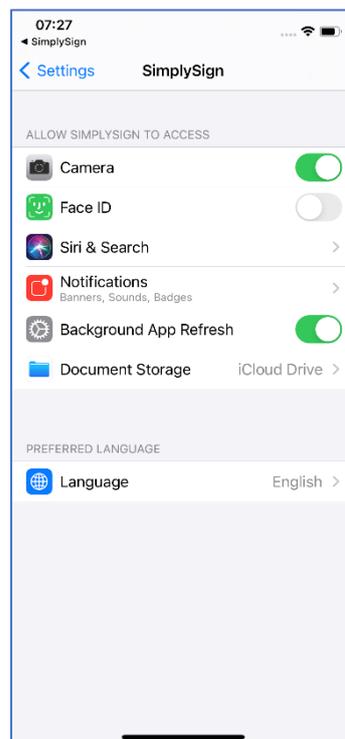
- B. If your device has Face ID enabled, the following message appears when you launch the application for the first time. There is no such message for Touch ID.



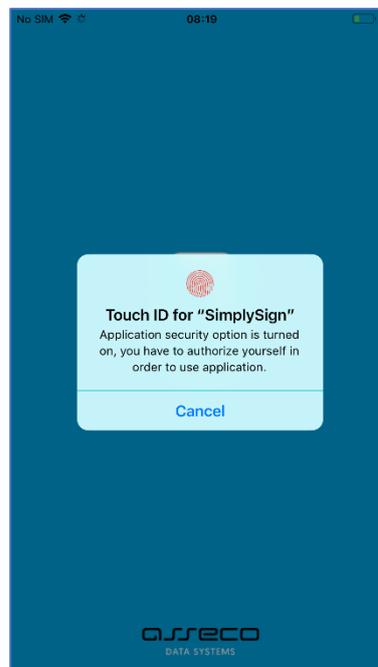
If you select **Do not allow**, the following message will be displayed, allowing you to move to the settings.



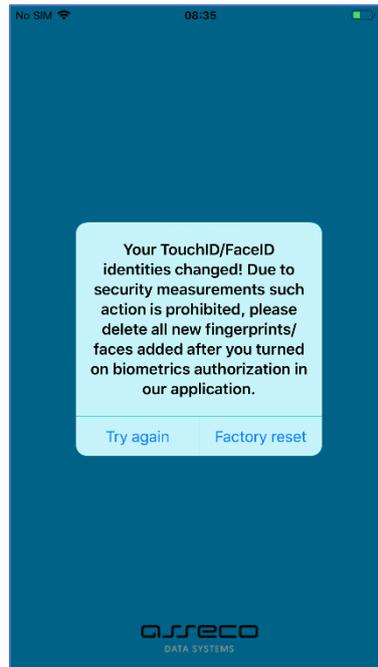
Pressing **Open settings** will take you to Settings, where you need to allow Face ID for the SimplySign application. Until you grant this permission, the application will not allow you to work – it will keep displaying the message "**To use FaceID you must grant the application permission to use this feature**"



- C. If biometric security is enabled on the device, the authentication with the selected security will appear the next time you launch the application.



- D. If the biometric security settings are changed in the Operating System of the device (for example, another fingerprint is added), the following message will appear when the application is launched:

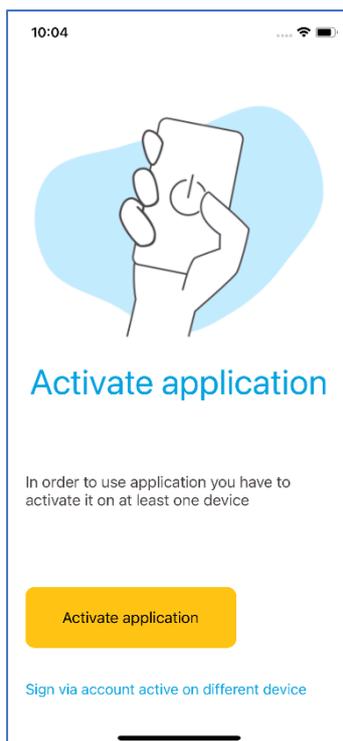


In this case, you need to perform a factory reset and activate the application again.

6. Launching, activation of the application or resetting access to the service

6.1. Launching the application

The **SimplySign** application is launched using a button located on the Desktop. After launching the application a start screen appears.



6.2. Service activation

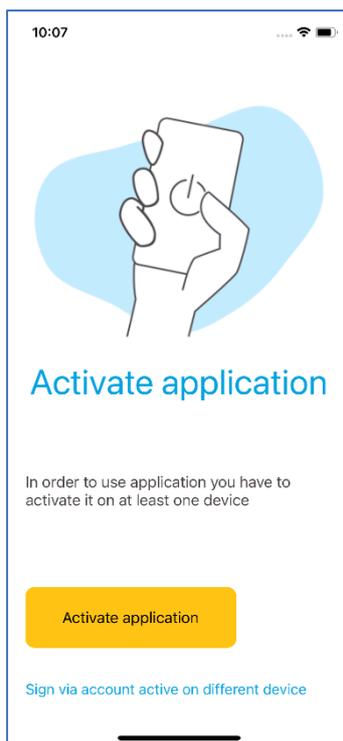
6.2.1. Activation using (personal) authentication data

Holders of a qualified certificate issued by **CERTUM** and contained on the SimplySign medium have the opportunity to benefit from a very **convenient, maintenance-free** activation of the application based on their personal data. This is the activation through the so-called authentication data. In practice, these are the data known to the User (personal data plus the data of their identity document). The following is the description of the process of performing such activation of the **SimplySign** application.

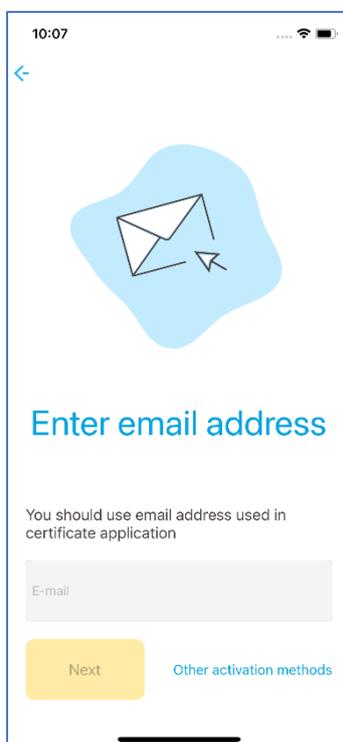
!!!ATTENTION

The condition for correct activation through authentication data is that the User must have at **least one qualified certificate** issued by **CERTUM** and contained on a virtual card in the **SimplySign** service. The certificate can even be canceled or overdue.

In order to perform the activation using the authentication data, the **SimplySign** application should be launched.

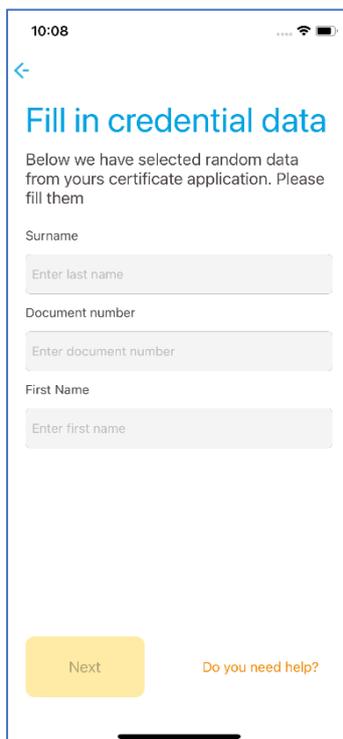


The activation is started by pressing the **Activate application** button. After pressing this button, a screen allowing for entering the e-mail address, which is the User's ID appears.



Then, in the field **Enter email address**, you must enter an email, which is the User's ID.

Then, press the **Next** button. If the ID is correct, the application will ask you to enter 3 randomly selected credential data of the User.



10:08

<

Fill in credential data

Below we have selected random data from yours certificate application. Please fill them

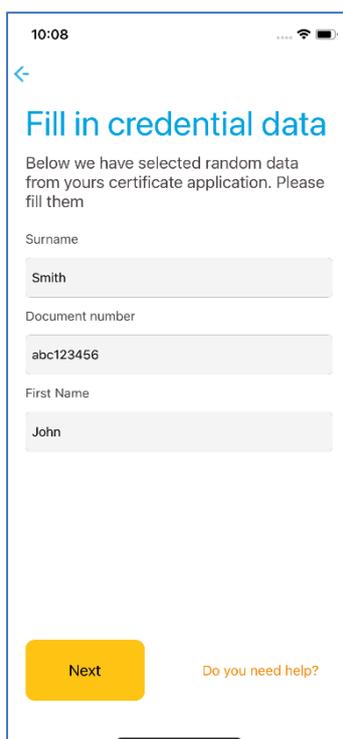
Surname

Document number

First Name

Next Do you need help?

Then you must enter the correct credential data.



10:08

<

Fill in credential data

Below we have selected random data from yours certificate application. Please fill them

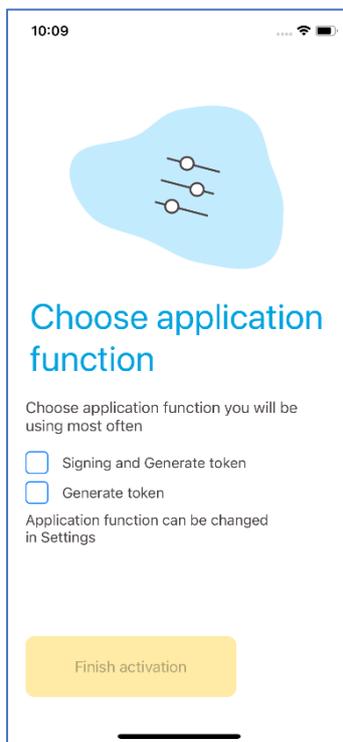
Surname

Document number

First Name

Next Do you need help?

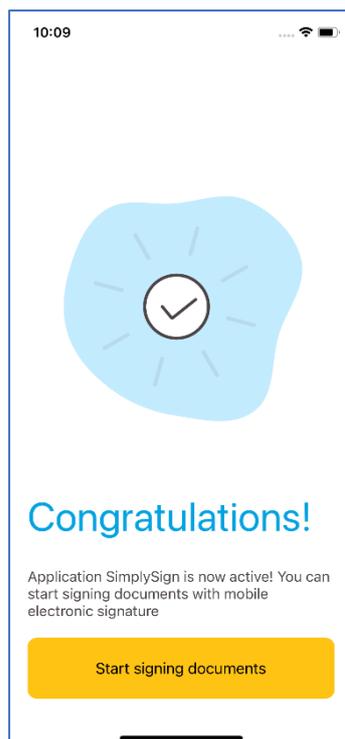
After entering personal data, press the **Next** button. If the credential data is correct, the application will be activated and it will take you to the screen, where you must select the operation mode.



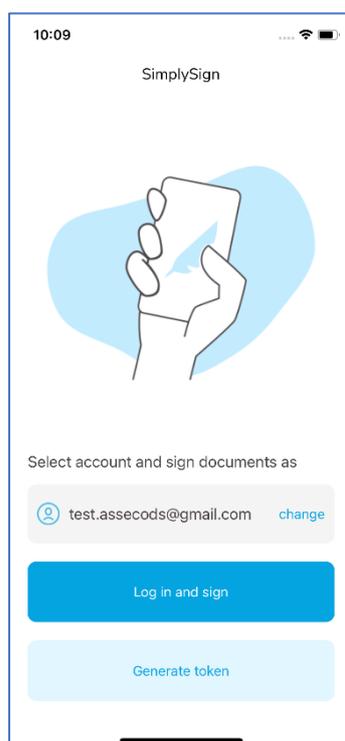
Two modes are available:

- Signing and Generate token – allows you to sign documents and generate tokens at the same time;
- Generate token – it only allows you to generate a token – in such a case signing will have to be done on another device;

After selecting the appropriate mode, press the **Finish activation** button. A screen indicating that the application is active will be displayed.



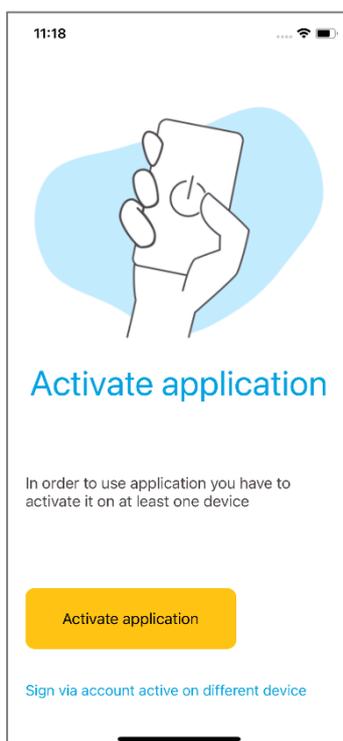
After pressing the **Start signing documents** button, the application will take you to the start screen.



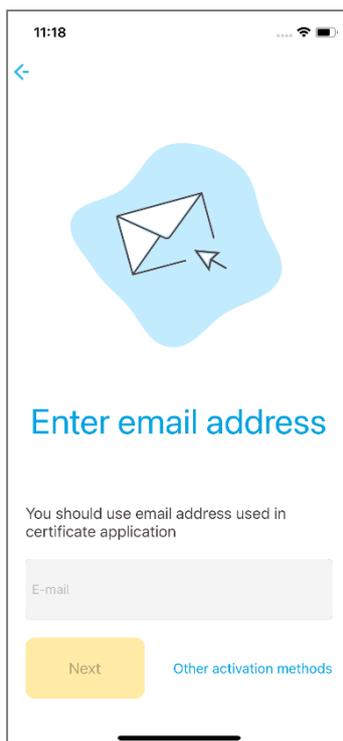
6.2.2. Activation using the activating code

The application can be activated also using an **activating code** which is received by email during the purchase of **SimplySign** – mobile electronic signature in **Certum Store**.

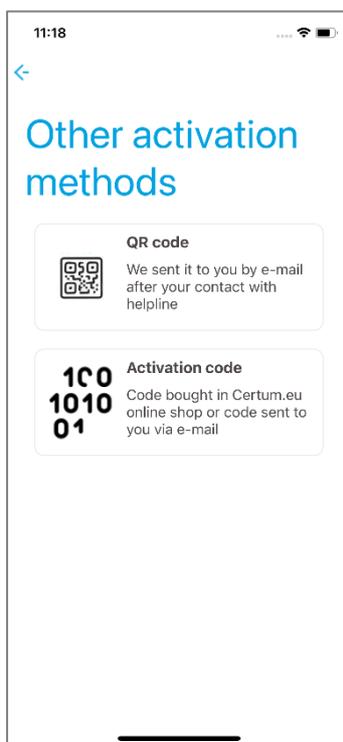
In order to perform activation with an activation code, run the application.



Then, press the **Activate application** button. A screen with various activation options will appear.



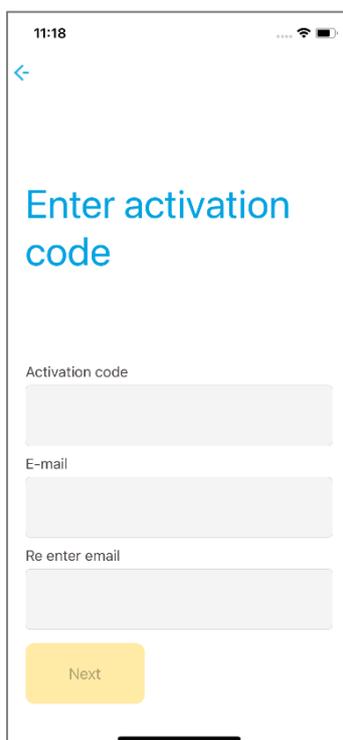
Then select the **Other activation methods** button. Other activation options will appear.



In the case of activation using the Activation code, press the **Activation code** button. After pressing this button, a screen allowing for activation of the application with the use of this activation code appears.

NOTE!!!

The email address entered will be used also as the User's ID. It is recommended to use a real email address to which the user has access – this is due to the fact the email messages (e.g. resetting a PIN code for a virtual card) sent from the SimplySign System to the User will be sent to that address.



11:18

<

Enter activation code

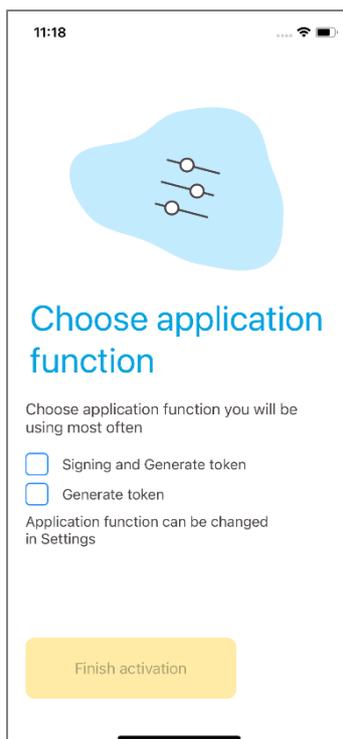
Activation code

E-mail

Re enter email

Next

Then fill in the **Activation code**, **E-mail** and **Re enter email** fields. After these data are entered, press the **Next** button. The application will be activated and will take you to the screen where you can select the application operation mode.

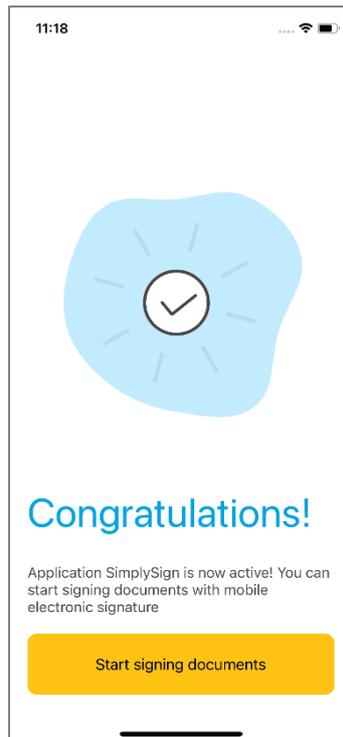


Two modes are available:

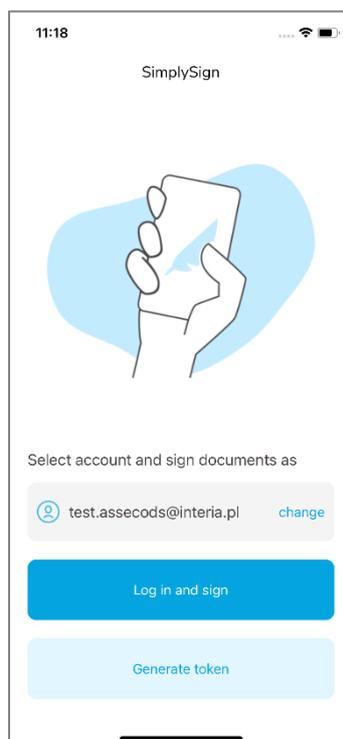
- Signing and Generate token – allows you to sign documents and generate tokens at the same time;
- Generate token – it only allows you to generate a token – in such a case signing will have to be done on another device;

After selecting the appropriate mode, press the **Finish activation** button. A screen indicating that the application is active will be displayed.

After selecting the appropriate modes, press the **Finish Activation** button. A screen indicating that the application is active will be displayed.



After pressing the **Start signing documents** button, the application will take you to the start screen.



6.3. Resetting the access to the service

Resetting the access to the service consists in contacting the **Certum** Help line in order to submit a request for service access reset. The employee of the Certum Help line performs the access resetting process by verification of personal details of the User requesting the reset of the access to the service.

The User's data contained in their Application for qualified certificate submitted in the Certum system are verified.

After correct verification, the User receives a 6-digit code, the so-called secret, from the Certum Operator.

Certum sends a one time link for resetting the service access to the e-mail address, which is the User's ID in the **SimplySign** System – the link is valid for 24 hours from the moment of its generation in the SimplySign system.

The User receives the e-mail message, clicks on the activation link and is directed to Certum website, where they are asked to enter the **6-digit secret**.

Depending on the reset method, when a secret is entered and the **Send** button is pressed, the User obtains either the so-called **QR Code** called a photocode or the so-called **16-character resetting code**. After receiving this data, do not close the browser but proceed to the next step of resetting the access to the service.



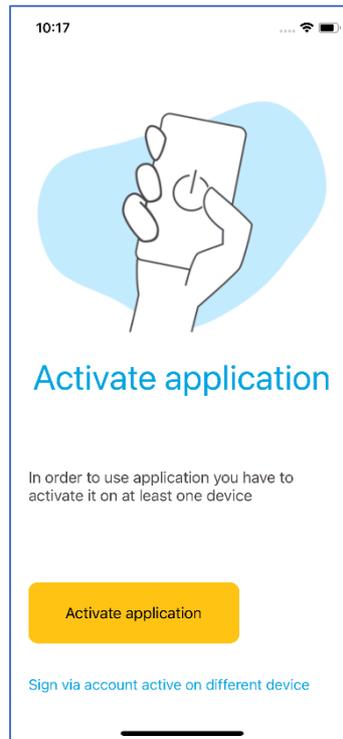
Prosimy wpisać kod resetujący do aplikacji SimplySign. (Please enter reset code with SimplySign application.)

ZUVQB6D3J5CK2HRA

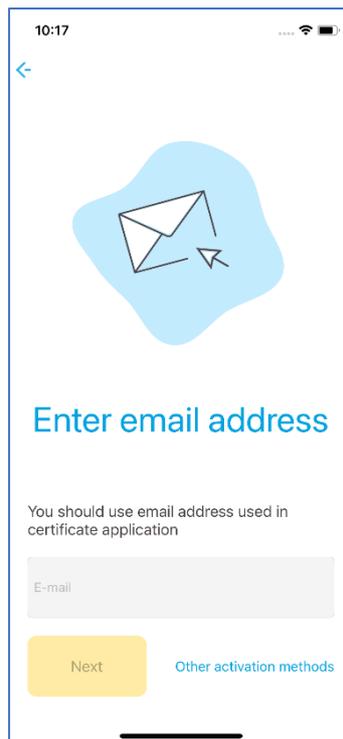
Both methods are described in the following sections.

6.3.1. Manual reset using the 16-character resetting code

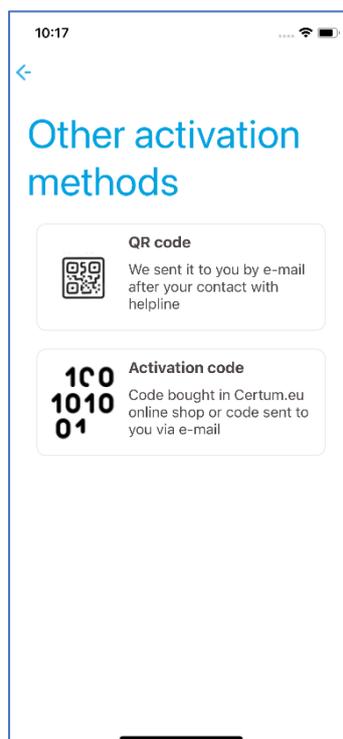
To reset access with the **16 character reset code**, start the **SimplySign** Application.



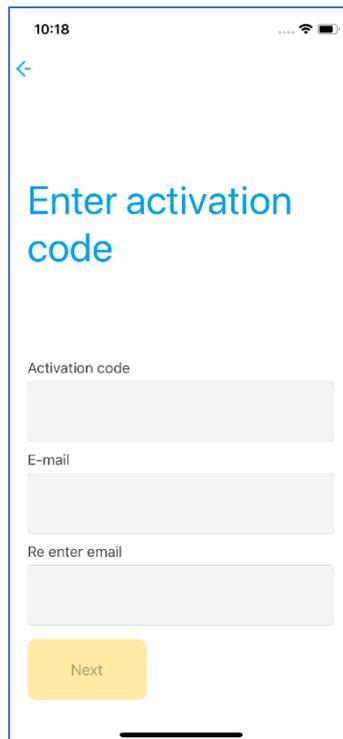
Then, press the **Activate application** button. A screen with various activation options will appear.



Then select the **Other activation methods** button. Other activation options will appear.



Select **Activation code**.



10:18

<

Enter activation code

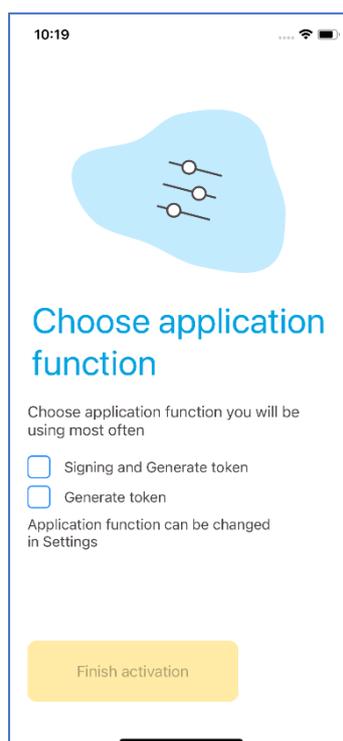
Activation code

E-mail

Re enter email

Next

Then fill in the **Activation code** (where you must enter a 16-character resetting code), **E-mail**, and **Re enter email** fields and press **Next**. If the entered data is correct, access to the service is restored and the application will take you to the screen where the application operating mode is to be selected.



10:19

<

Choose application function

Choose application function you will be using most often

Signing and Generate token

Generate token

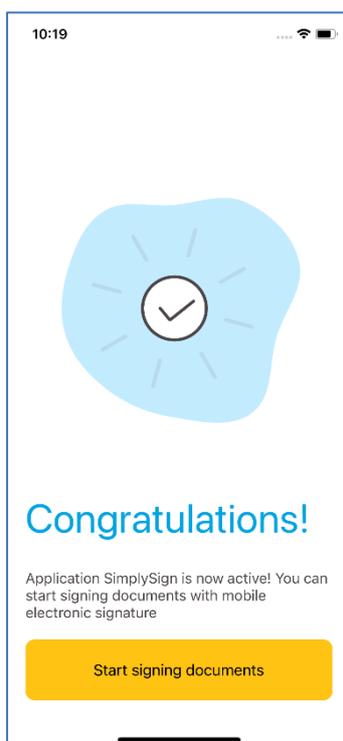
Application function can be changed in Settings

Finish activation

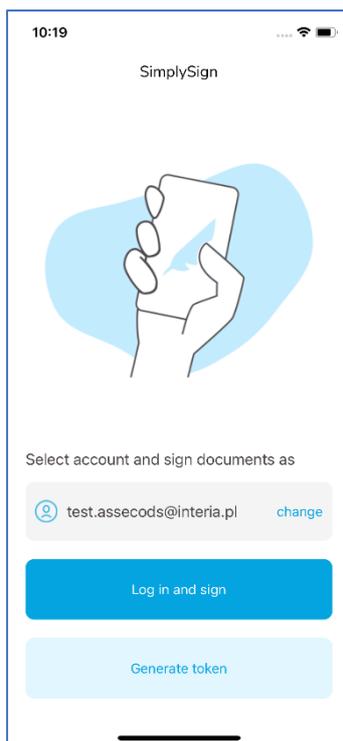
Two modes are available:

- Signing and Generate token – allows you to sign documents and generate tokens at the same time;
- Generate token – it only allows you to generate a token – in such a case signing will have to be done on another device;

After selecting the appropriate mode, press the **Finish activation** button. A screen indicating that the application is active will be displayed.

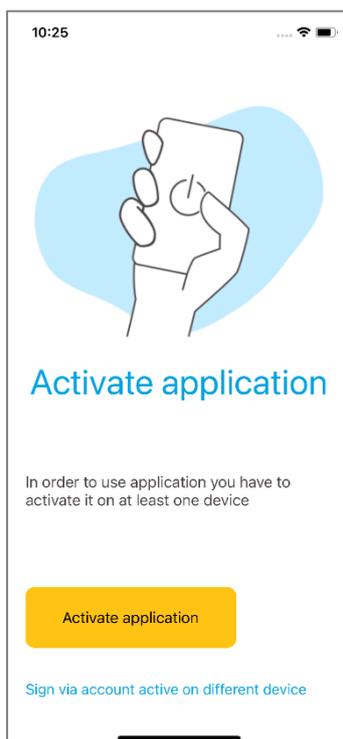


After pressing the **Start signing documents** button, the application will take you to the start screen.

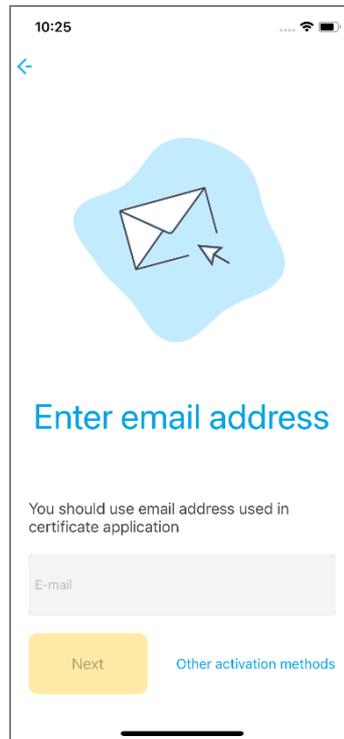


6.3.2. Automatic resetting with the use of QR Code

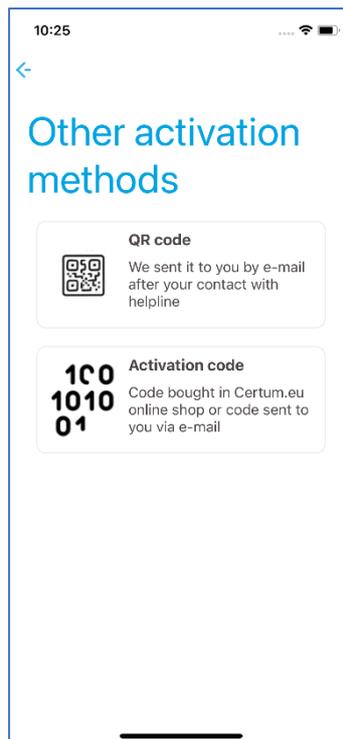
In order to reset the access to the service by automatic reset, run the **SimplySign** application,



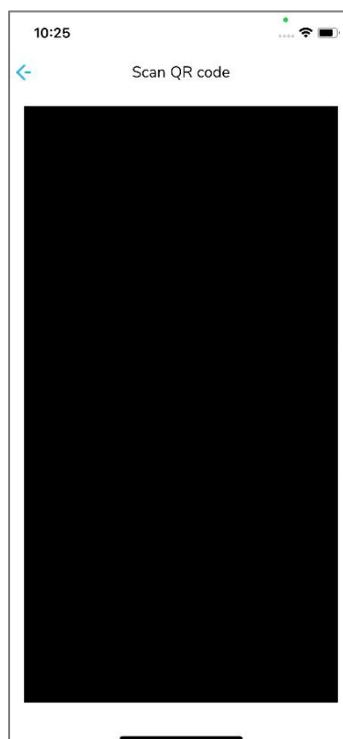
Then, press the **Activate application** button. Further options will be displayed.



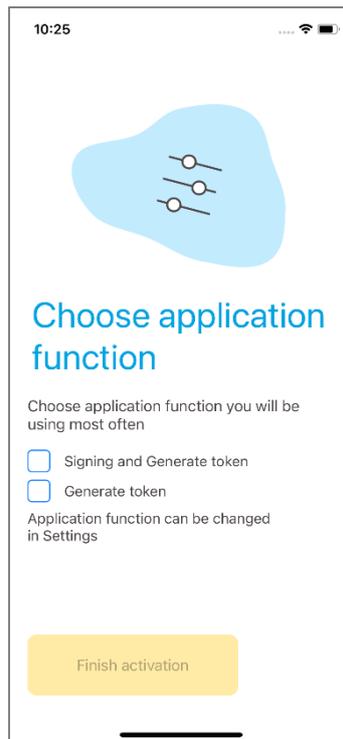
Then select the **Other activation methods** button. A screen will appear where you can select other activation methods.



Then select the **QR code** option and you will be able to **scan** the **QR code**.



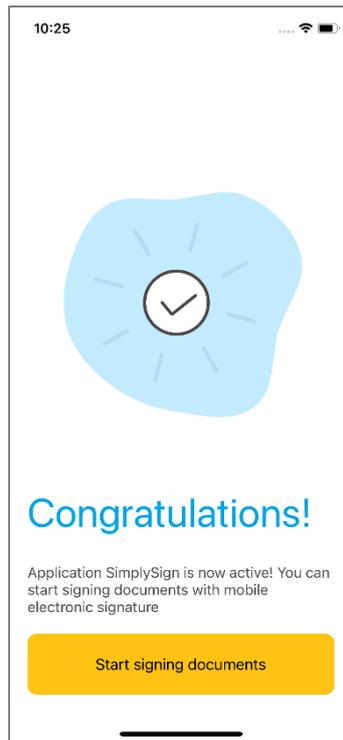
After scanning the **QR Code**, the application will take you to the screen where you can select the application operating mode.



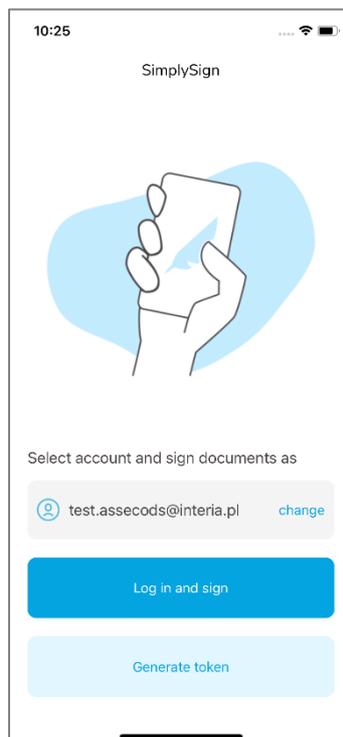
Two modes are available:

- Signing and Generate token – allows you to sign documents and generate tokens at the same time;
- Generate token – it only allows you to generate a token – in such a case signing will have to be done on another device;

After selecting the appropriate mode, press the **Finish activation** button. A screen indicating that the application is active will be displayed.



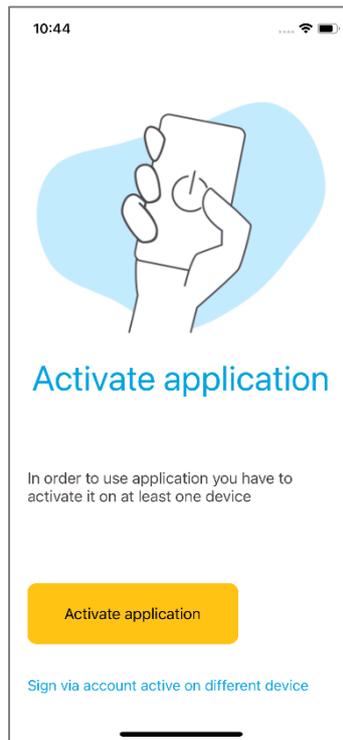
After pressing the **Start signing documents** button, the application will take you to the start screen.



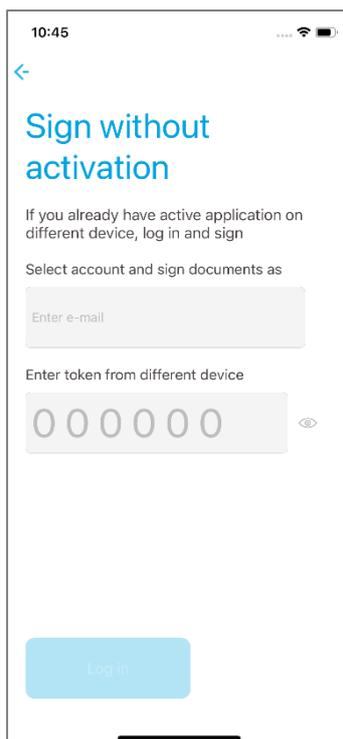
6.4. Signature without activation

6.4.1. Application not activated

To log in into an application that is not activated using an account activated on another device, select the option **Sign via account active on different device**.



When you select **Sign via account active on different device**, a screen will appear allowing you to enter your login and OTP token.



10:45

<

Sign without activation

If you already have active application on different device, log in and sign

Select account and sign documents as

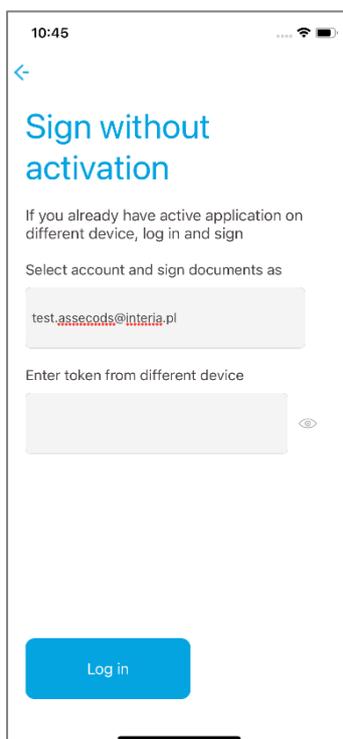
Enter e-mail

Enter token from different device

0 0 0 0 0 0

Log in

The login and OTP token must be filled in.



10:45

<

Sign without activation

If you already have active application on different device, log in and sign

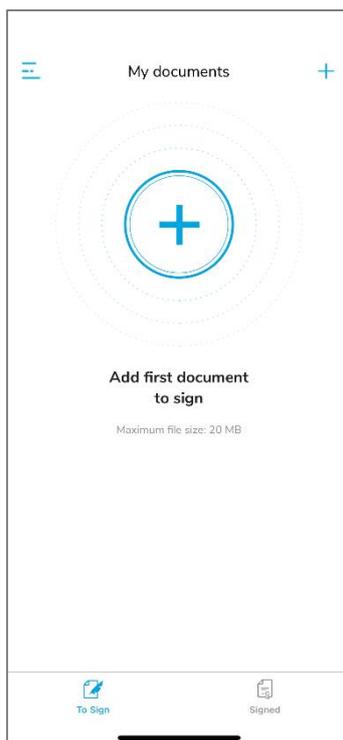
Select account and sign documents as

test.assecods@interia.pl

Enter token from different device

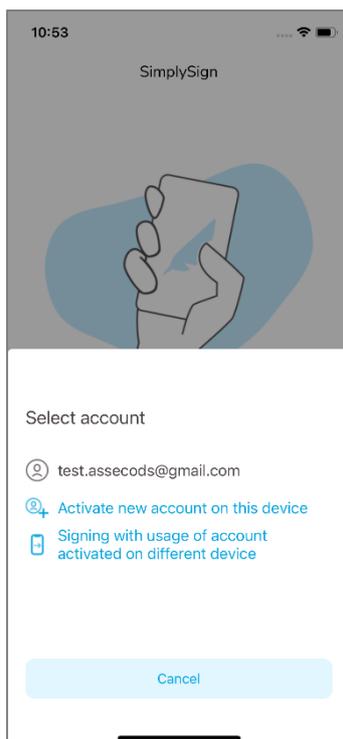
Log in

Then press the **Log in** button. If the login and OTP are correct then you will be logged in and able to sign a document.

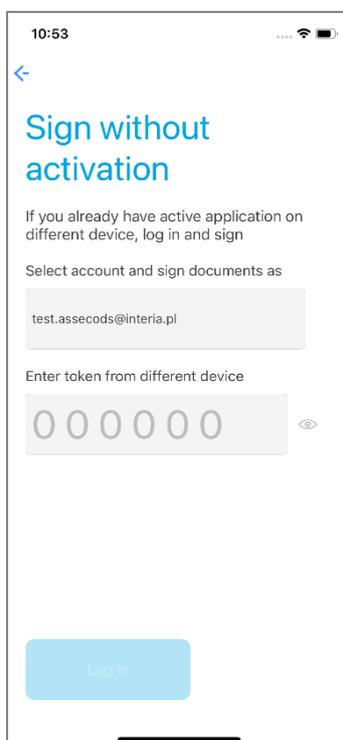


6.4.2. Application in the „Signing and Generate token” mode

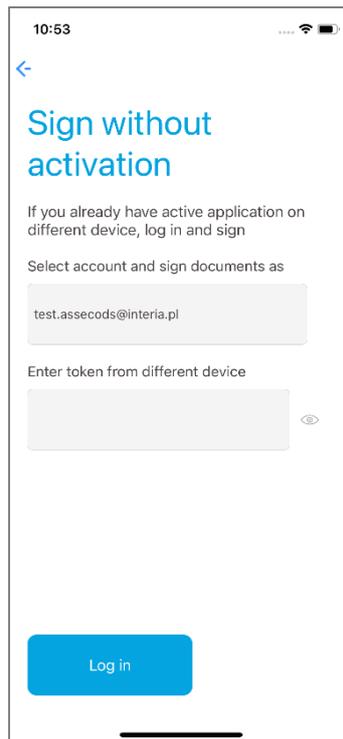
To log in into an account activated on another device in the "**Signing and Generate token**" mode, press **Change** in the list of accounts. Options will appear.



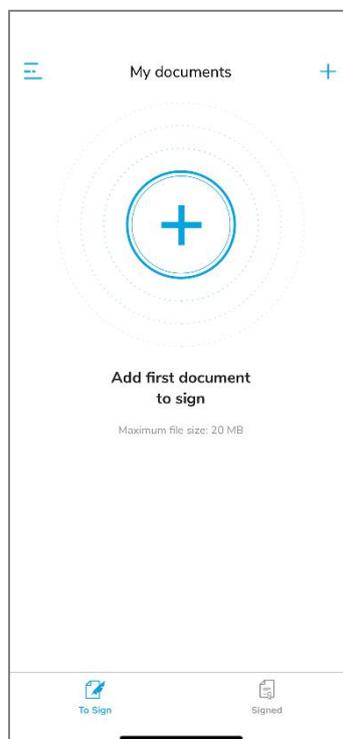
Then select the option **Sign with the usage of account activated on different device**. A screen will appear that allows you to enter your login and OTP token.



The login and OTP token must be filled in.



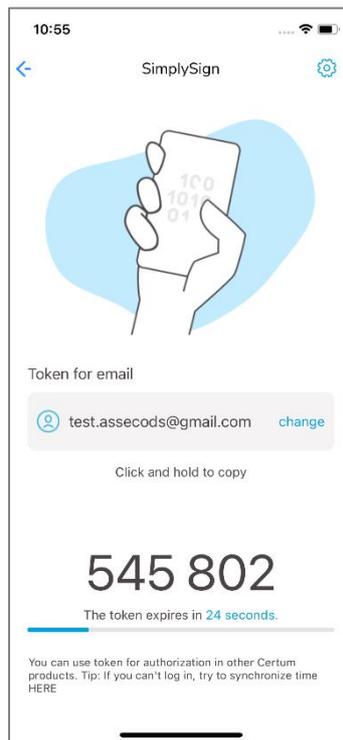
Then press the **Log in** button. If the login and OTP are correct then you will be logged in and able to sign a document.



6.5. Application operating modes

6.5.1. Operation in "Generate token code"

If during activation of the application it is set that the application should work in the "Token code generating" mode, this will cause that the application will only generate OTP Tokens and in this case, after starting the application, the screen displaying the currently generated OTP Token will be activated immediately.



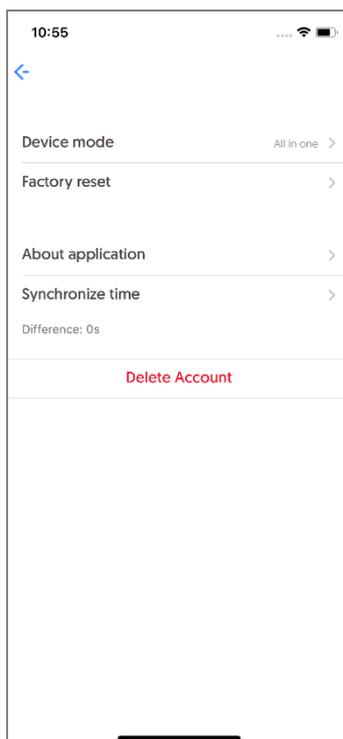
6.5.1.1. Force time synchronization

In the "Generate token code" mode, it is possible to manually force time synchronization, which will cause the **OTP Token** value to be converted based on the synchronized time.

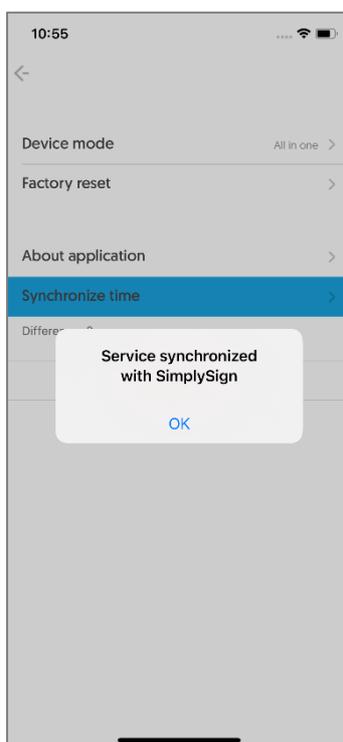
This is used in case of problems with logging when there is a suspicion that the **OTP Token** is generated incorrectly on the device.

Such synchronization changes the time only within the **SimplySign** application and does not affect the time settings on the device.

To force time synchronization manually, go to the Settings. The settings are activated with the use of the gear icon at the top right of the screen.

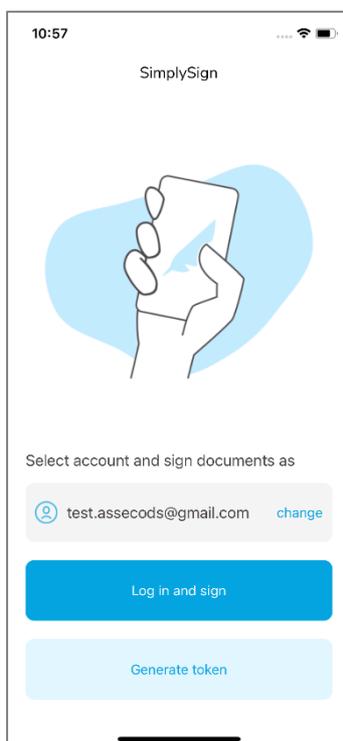


Then, press **Time Synchronization** button in the Settings. The time will be synchronized and the difference between the time in the SimplySign application and the time on the device will be shown in the Settings.



6.5.2. Working in the „Signing and Generate token” mode

If during activation of the application it is set that the application should work in both modes, this will cause that the application will generate OTP Tokens and signing of documents will also be possible. In such a case, after launching of the application, a screen allowing you to start generating OTP Tokens (Generate Token button) or signing of documents (Sign document button) will be activated.



6.5.3. Changing the application operating mode

It is possible to change the application operating mode.

Change of the operating mode is made in the Settings.

Only the following changes of the application operating mode are possible:

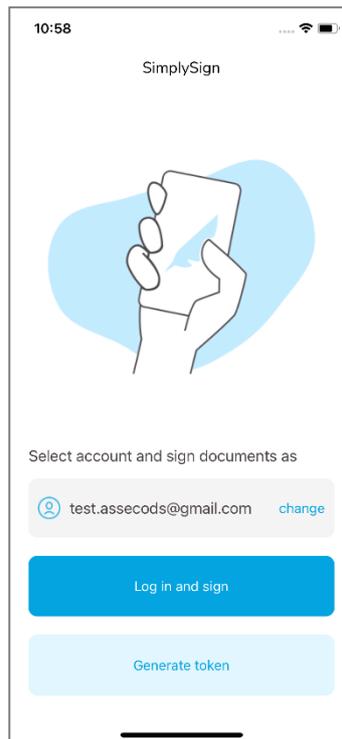
- From the "Signing and Generate token" mode to the "Generate token" mode
- From the "Generate token" mode to the "Signing and Generate token" mode

6.6. Multiple accounts support

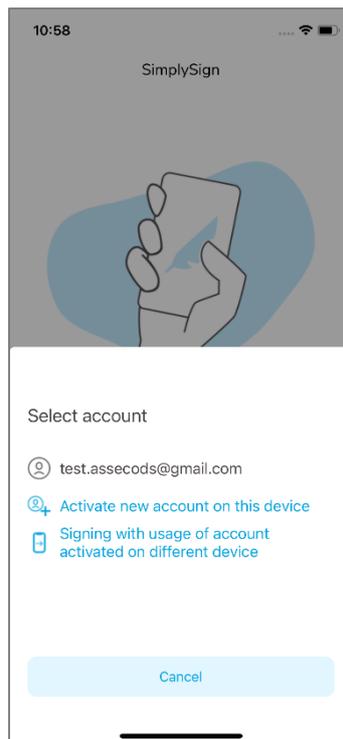
The application allows the use of multiple accounts. Below is a description of adding another account in the **All in One** mode and the **Token code generating** mode.

6.6.1. „Signing and Generate token” mode

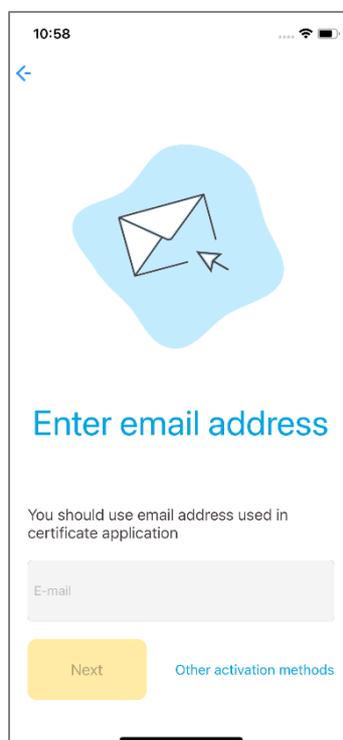
To add another account in the **“Signing and Generate token”** mode, run the application.



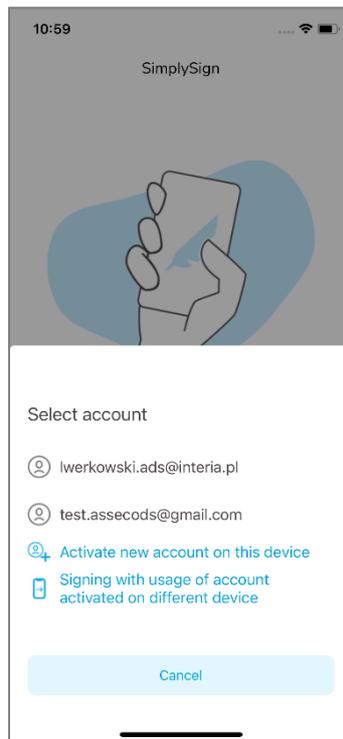
Press the **Change** button. A list of accounts will expand with the option **Activate new account on this device**.



After pressing the **Activate new account on this device** button, a window allowing you to activate the new account in the selected method will appear.

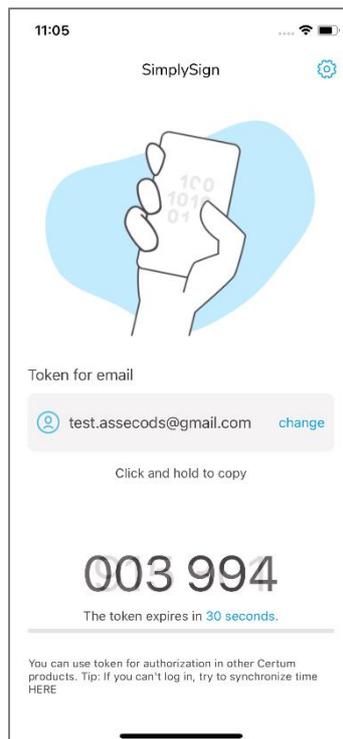


Methods of activation are presented in the previous chapter. After activation of another account, it will be visible in the application.

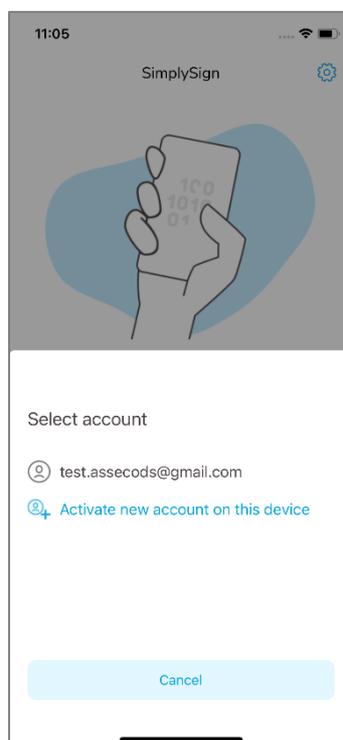


6.6.2. "Generate token code" mode

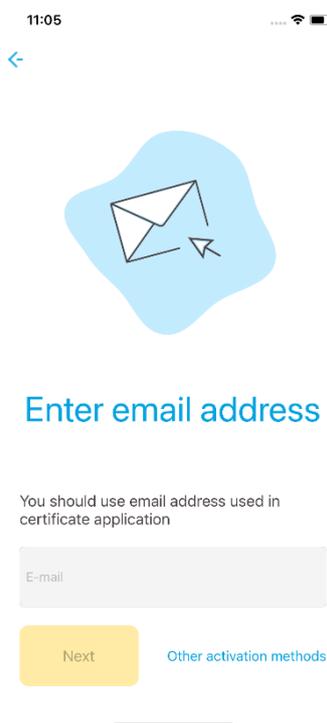
To add another account in the **Generate token code** mode, run the application.



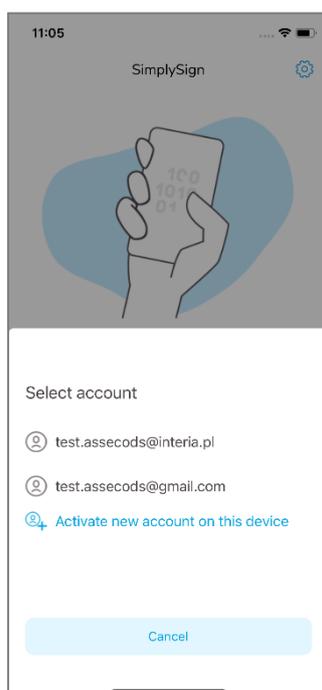
Press the area of the account name. A list of accounts will expand with the option **Activate new account on this device**.



After pressing the **Activate new account on this device** button, a window allowing you to activate the new account in the way you choose will appear.



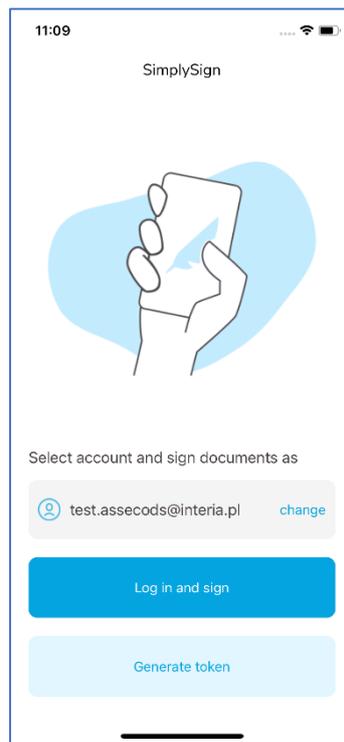
Methods of activation are presented in the previous chapter. After activation of another account, it will be visible in the application.



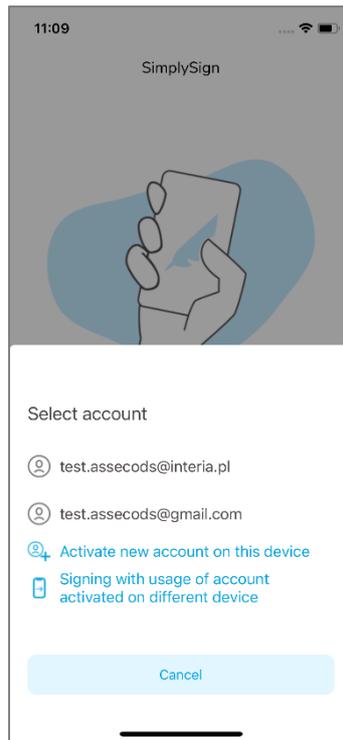
6.7. Logging into the application

6.7.1. „Signing and Generate token” mode

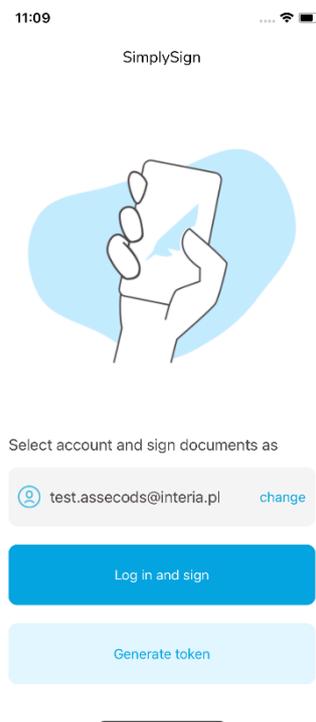
If the application has been set to the “Signing and Generate token” mode, then the start screen will be displayed upon running the application



Since the application allows the use of several accounts, you must press the area of the user name. A list of accounts will appear.



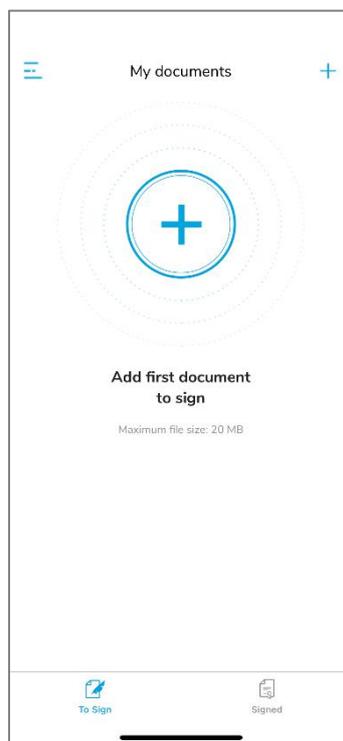
Select the appropriate account from the list.



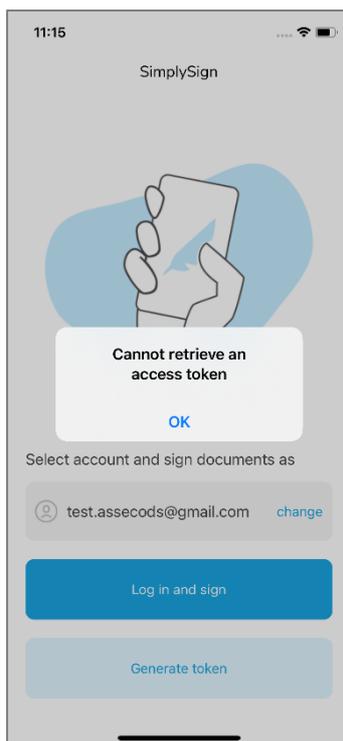
Then press the **Log in and sign** button. The application will automatically generate the OTP Token and will make an attempt to log the user in to the service. If the token is correct, you will be logged into the **SimplySign** service.

If you log in on this device for the first time, a message about the necessity to allow the application to access the internal information of the device will be displayed.

After pressing the **Allow** button you will be logged into the service and a screen where you can add files to be signed or go to application options will appear.

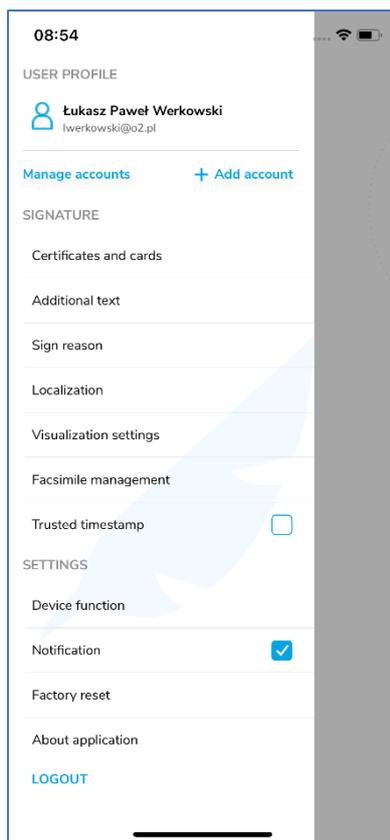


If the OTP token entered is incorrect or another error preventing from logging in occurs, the message **Cannot retrieve an access token** will be displayed at the bottom.



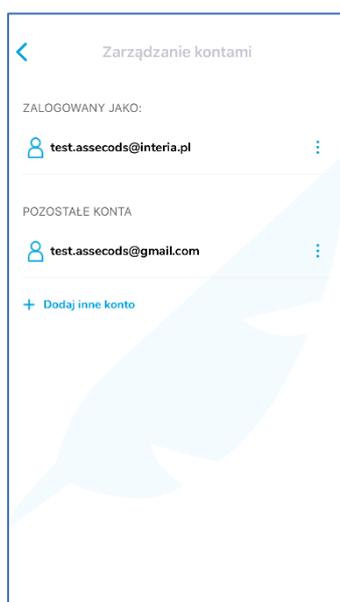
7. Application Settings/Options

After logging in to the application, you can change the default application options. After logging in and pressing the icon at the top left of the screen, the options menu will be "expanded".



7.1. „Account managment” option

This option allows you to manage your accounts. When selected, a list of accounts is displayed with indication of the account to which the User is currently logged in.



It is possible to remove the selected account from the application. To do this, press the bin button located to the right of the account name.

7.2. Signature section

In **Signature** section, the following options are available:

- Certificates and cards
- Visualize sign
- Sign reason
- Localization
- Trusted timestamp

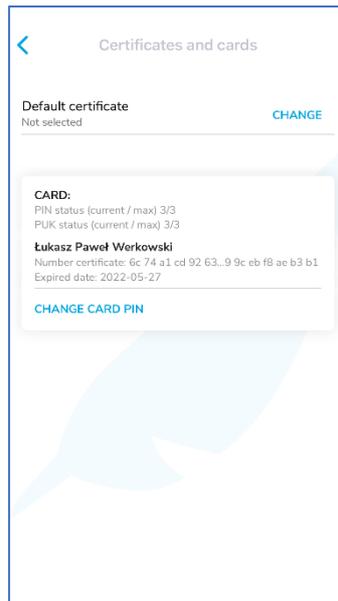
The above options are described in detail in next sections.

7.2.1. „Certificate and cards” option

This option allows you to manage your cards and certificates. After selecting it, a window with displayed tabs and basic data about the certificates of the logged User will appear.

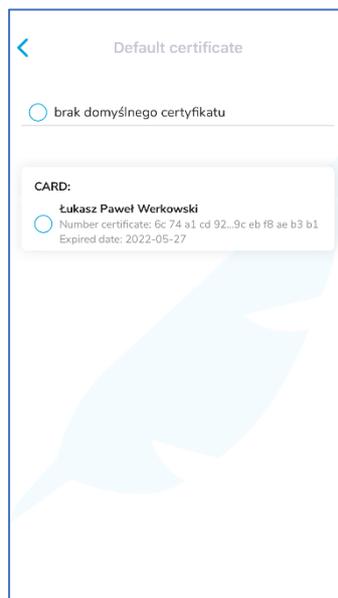
The default certificate set is presented and the card and certificates contained therein are displayed below. The following data are presented:

- Default certificate name
- The following information about the cards:
 - Card label
 - PIN code status
 - PUK code status
 - Common Name (CN) field of the certificates contained in the card
 - Serial number of the certificate
 - Expiry date of the certificate

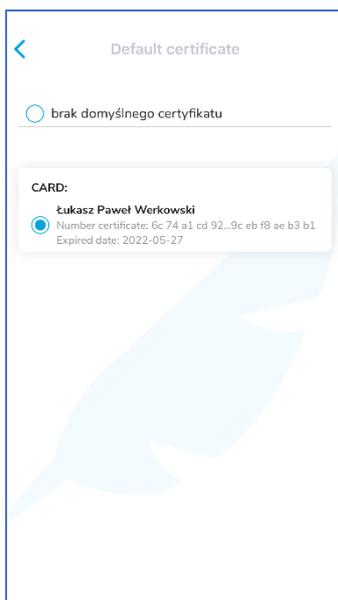


7.2.1.1. Setting the default certificate

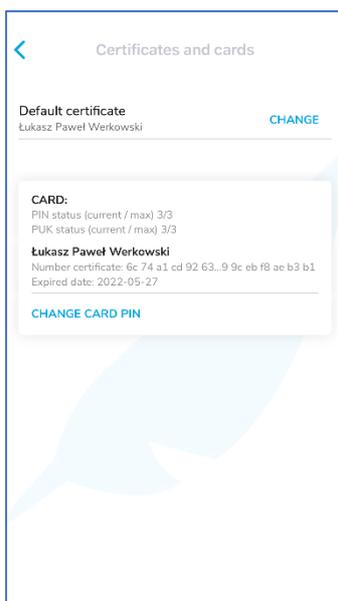
To set the default certificate, press the **Set** button. The available certificates will be displayed.



Then indicate the certificate to be set as default.

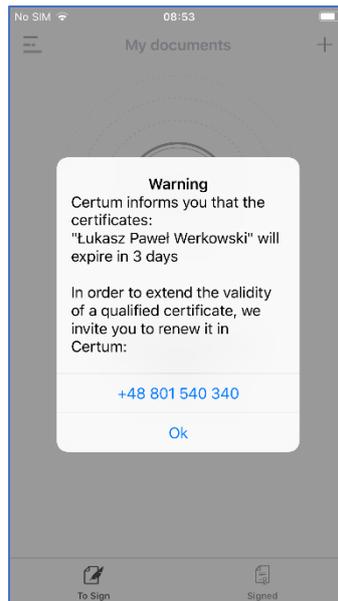


After selecting the default certificate, return to the settings – the selected default certificate will appear on the list.

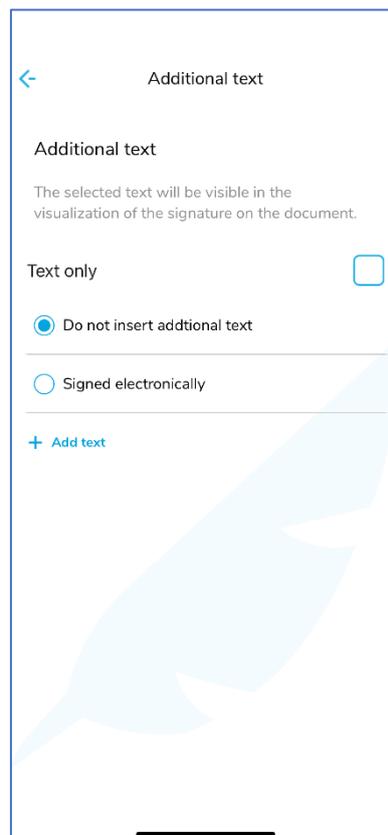


7.2.1.2. Warning of impending expiry of the certificate

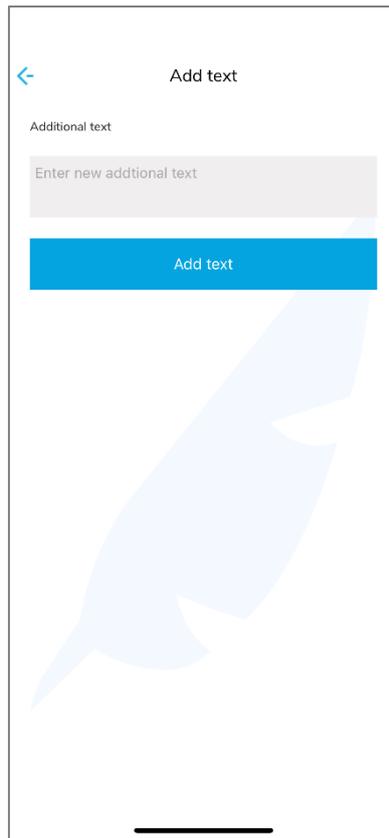
If a qualified certificate will expire in less than 14 days, the application displays an appropriate warning after logging in.



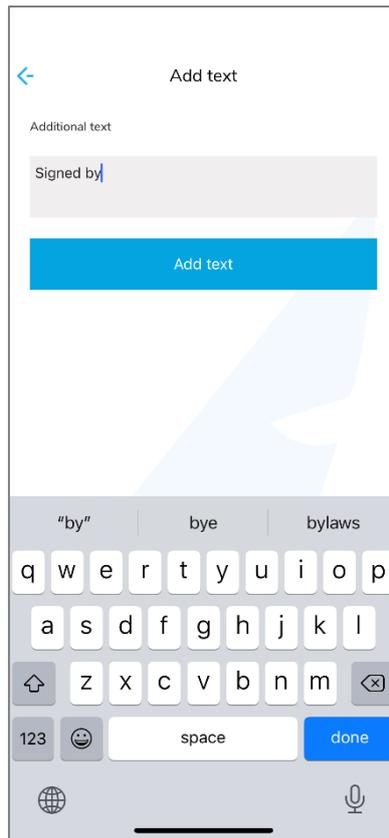
7.2.2. „Additional text” option



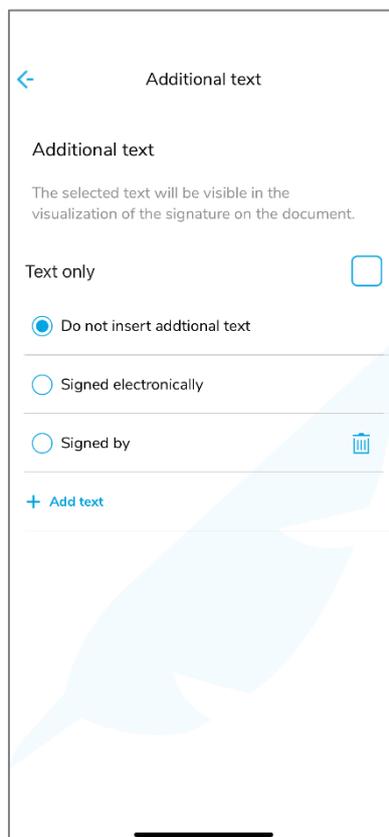
In order to add your own text, press the **+Add text** button. A window will appear in which you can enter your own additional text.



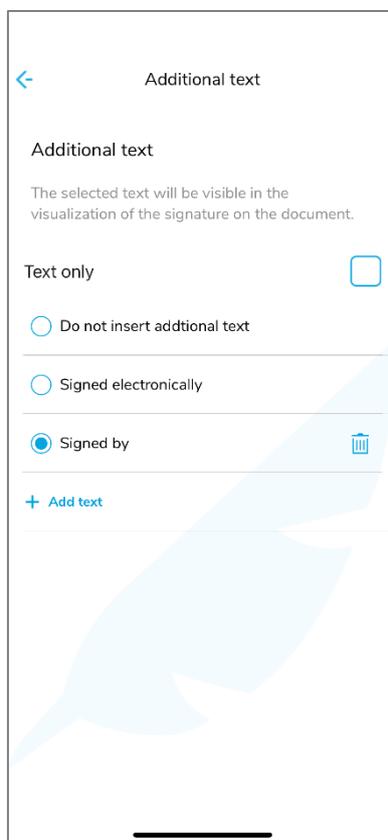
Enter your own text.



After entering your own text, press the **Add text** button. The text entered will appear in the list.



In order for the added text to be visible in the visualization, it must be selected.



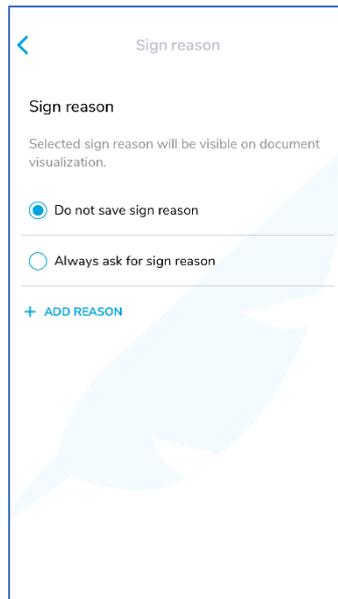
In the settings, in the upper right corner, there is the **Text only** option. If you select it, only this text will appear in the visualization. All other elements (CN, date, reason, location) will not be included in the visualization.

7.2.3. „Sign reason” option

Choosing this option allows for specification whether the so-called Sign reason will be added to the signature structure.

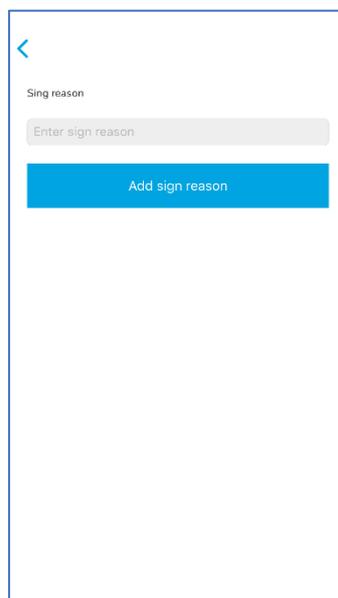
By default there are two options:

- Do not save sign reason - if you choose this option, a Signature reason will not be added to the signature structure.
- Always ask for a Sign reason - if you choose this option the application, every time before signing, will ask for a Signature reason which will be added to the signature structure.

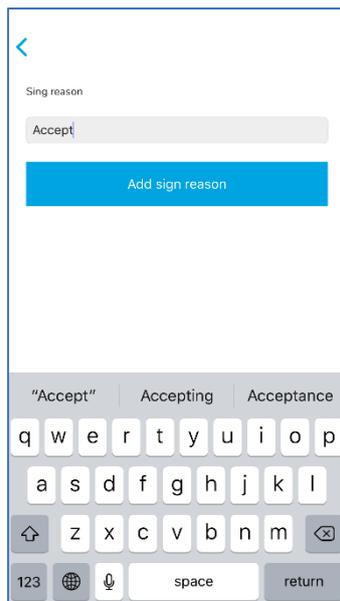


The application allows you to add your own signature to the list. This reason will be selectable in the future while signing a document if the option of adding a Signature reason is enabled.

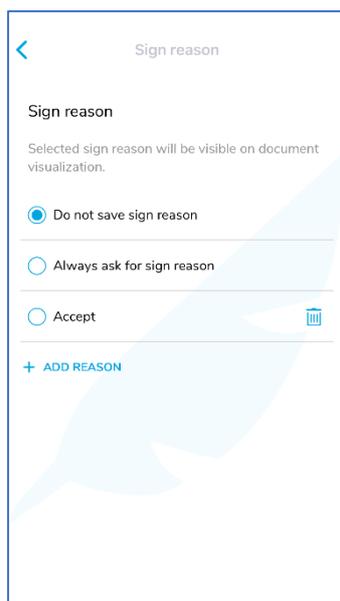
To add your own Signature reason to the list, press the “+” button located in the bottom right corner of the screen. A screen where you can enter your own Signature reason will be displayed.



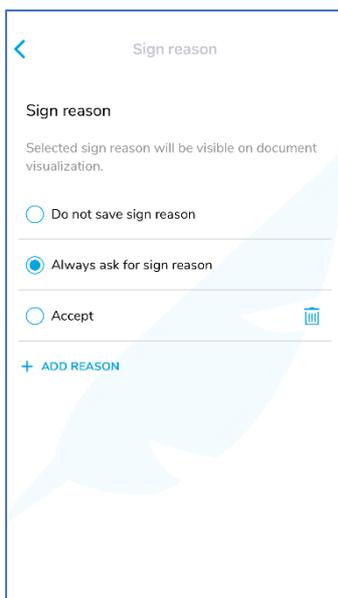
Enter your own Signature reason.



After entering your own Signature reason, press **Enter** button located on the virtual keyboard. The entered Signature reason will be added to the list of reasons.



A situation when the option **Always ask for Sign reason** is **enabled** is presented below. As a result, the application, every time before signing, will ask for a Signature reason which will be added to the signature structure.

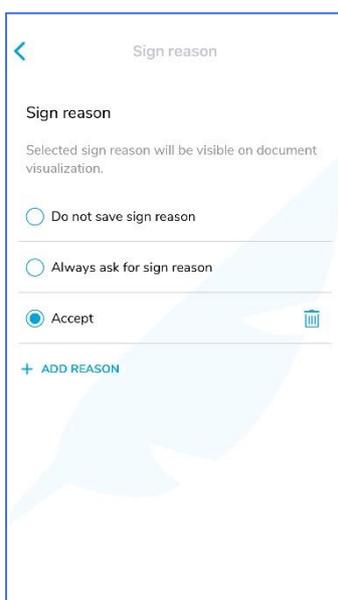


If you choose the added Sign reason this reason will be always, without asking, added to the signature structure.

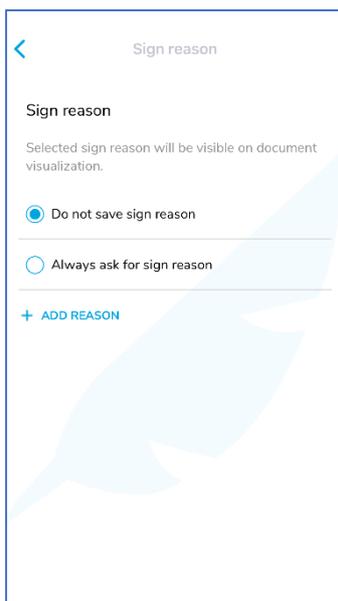
The Sign reasons entered by the User can be deleted.

Then you have to press the cross icon located within the area of the Sign reason.

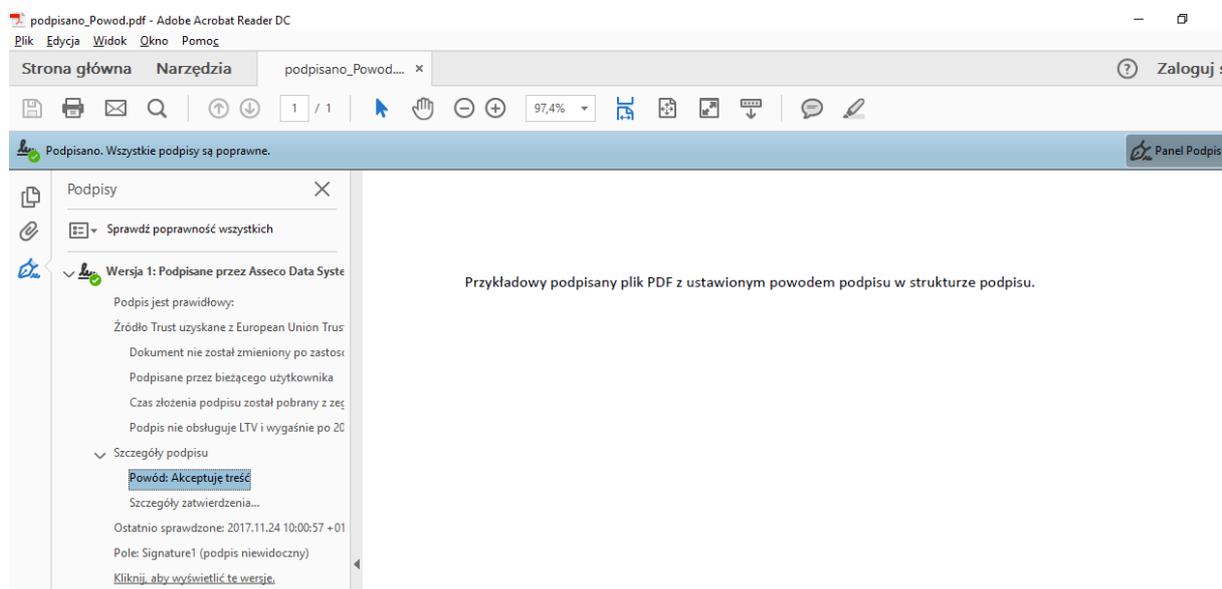
On the following two images a situation where the Sign reason has been selected and later it has been deleted using the cross icon is presented.



The selected Signature reason is removed from the list of Signature reasons.



Below, you can see a view of signature properties in PDF file in Desktop application. While signing, the Signature reason with a content **I accept the content** was set.

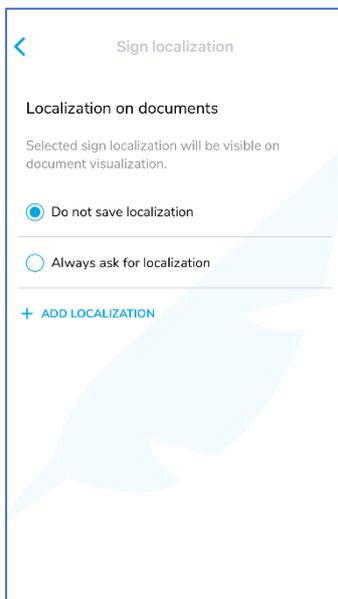


7.2.4. „Localization” option

Choosing this option allows for specification whether the so-called Localization will be added to the signature structure.

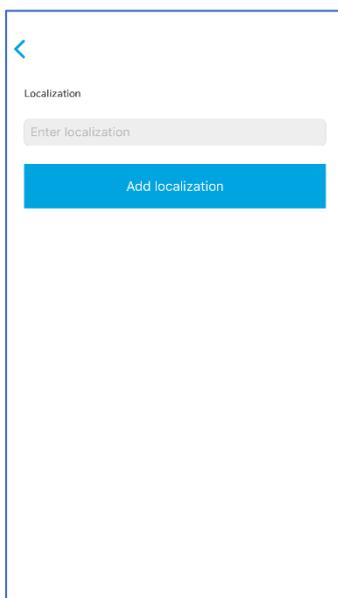
By default there are two options:

- Do not save localization - if you choose this option, a localization will not be added to the signature structure.
- Always ask for localization - if you choose this option, the application will ask, every time before signing, for localization which will be added to the signature structure.

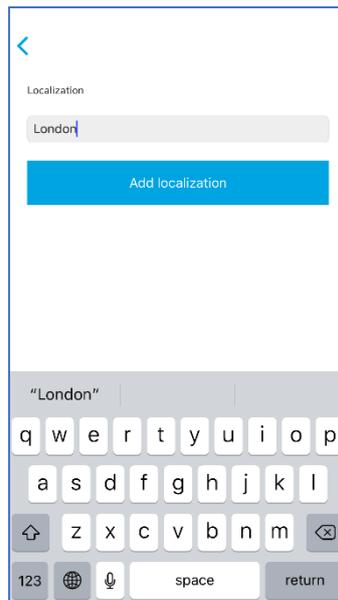


The application allows you to add your own localization to the list. This localization will be selectable in future while signing a document if the option of adding a localization is **enabled**.

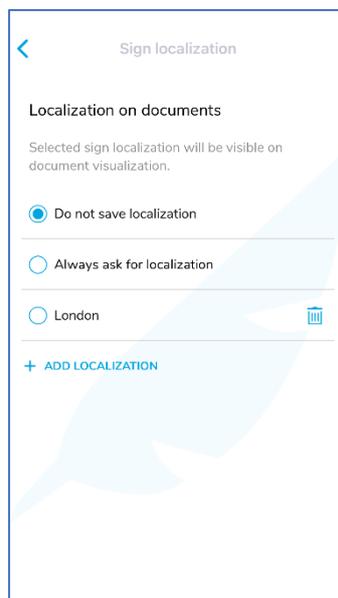
To add your own location to the list, press the **Add location** button. A screen where you can enter your own localization will be displayed.



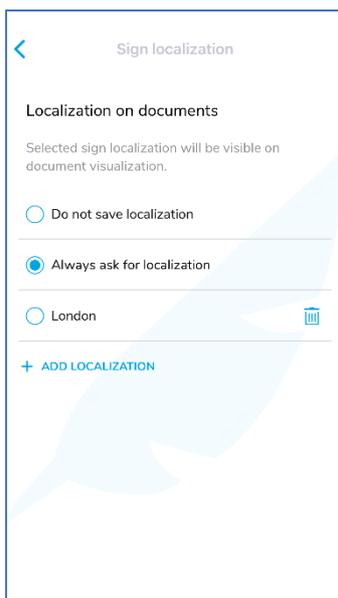
You have to enter your own localization.



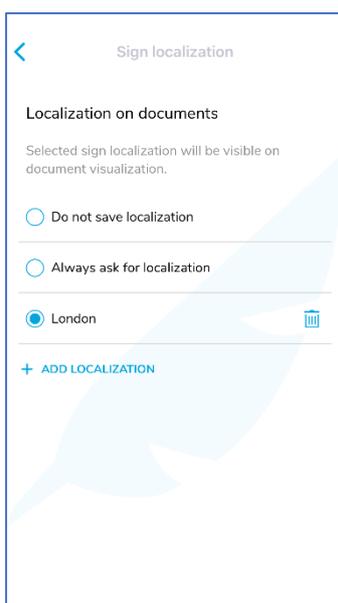
After entering your own localization, press the **Add location** button located on the virtual keyboard. The entered localization will be added to the list of reasons.



A situation when the option "Always ask for localization" is **enabled** is presented below. As a result, the application will ask, every time before signing, for a localization which will be added to the signature structure.



If you choose an added localization this localization will be always, without asking, added to the signature structure.

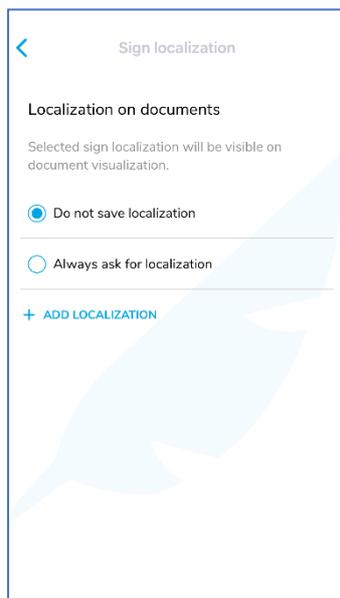
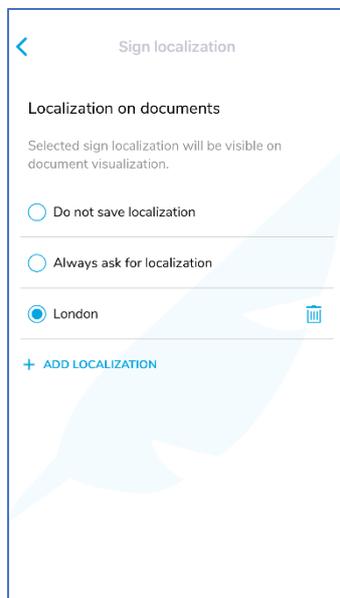


Localizations entered by the User can be deleted.

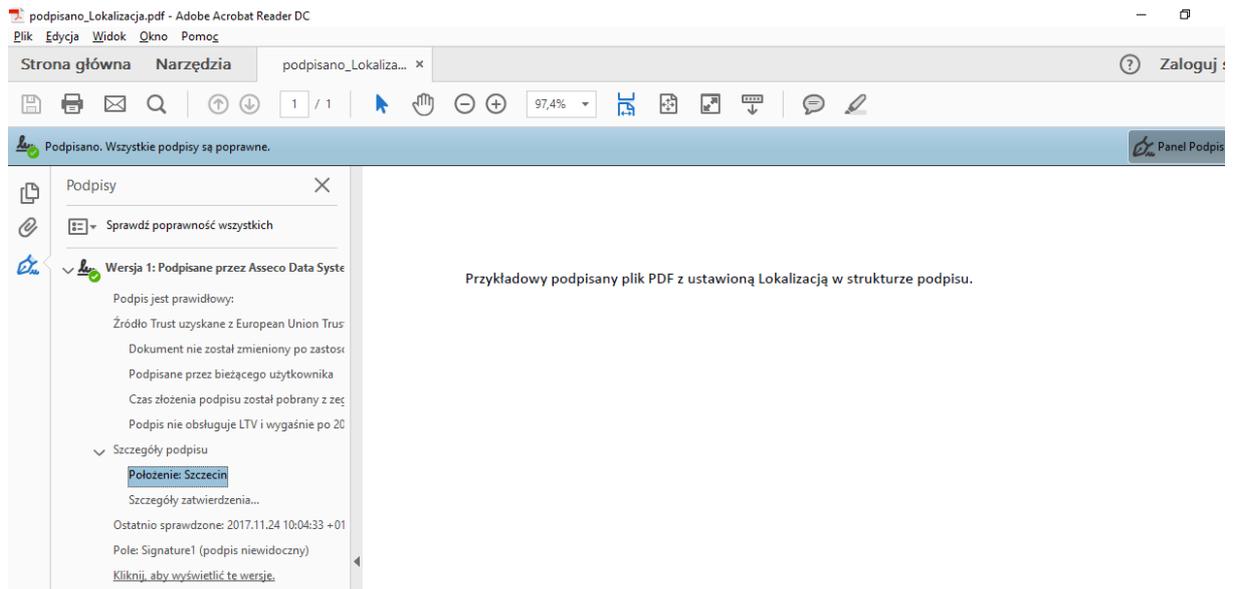
Then you have to press the cross icon located on the right within the area of the localization.

On the following two images a situation where the localization has been selected and later it has been deleted using the cross icon is presented.

The selected localization is removed from the list of localizations,



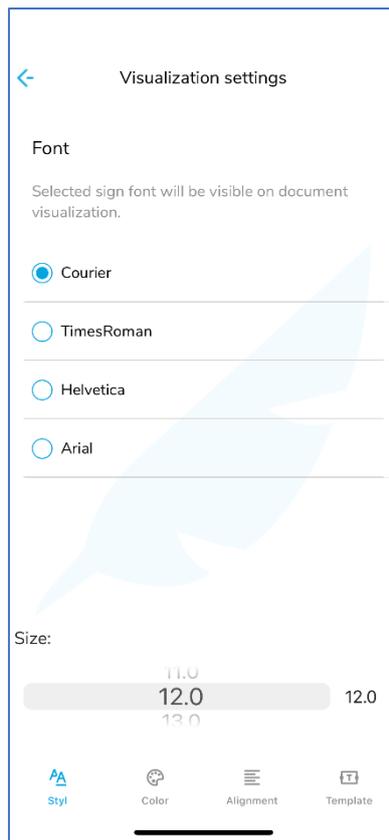
Below, you can see a view of signature properties in PDF file in Desktop application. While signing, a Localization **Szczecin** was set.



7.2.5. “Visualize signature” option

This option allows you to manage the visualization settings. The following options are available:

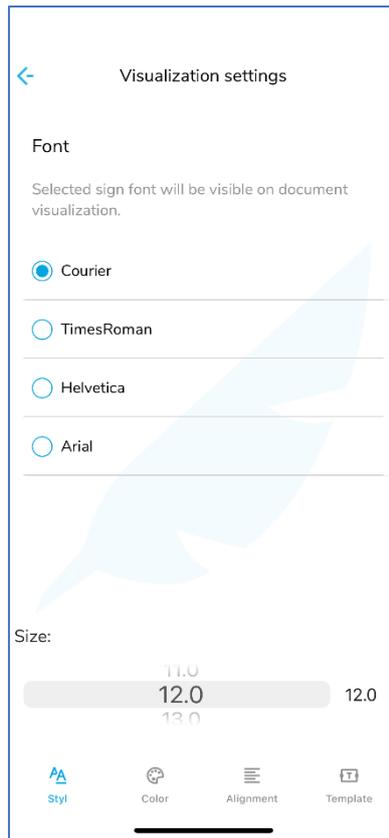
- Font style options
- Font color options
- Alignment options
- Template



7.2.5.1. Font style

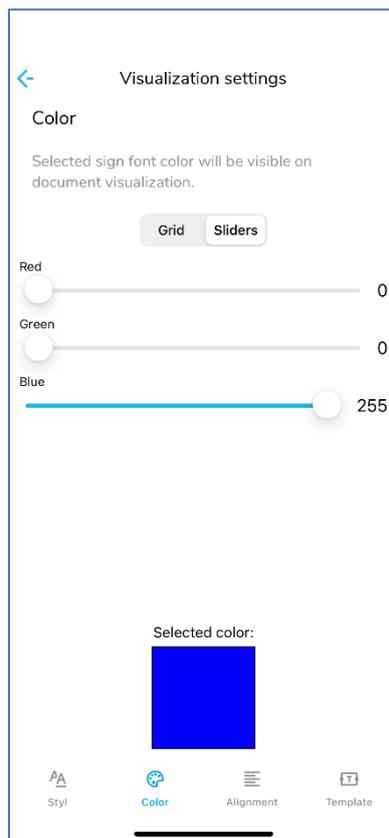
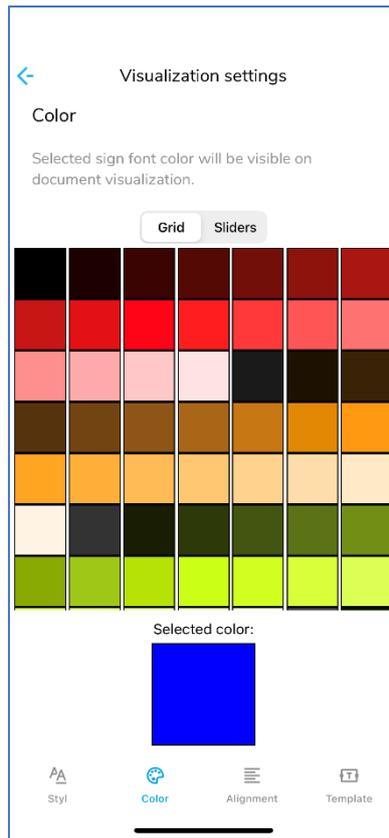
The following font options can be defined in the **Style** tab:

- Font typeface
- Font size



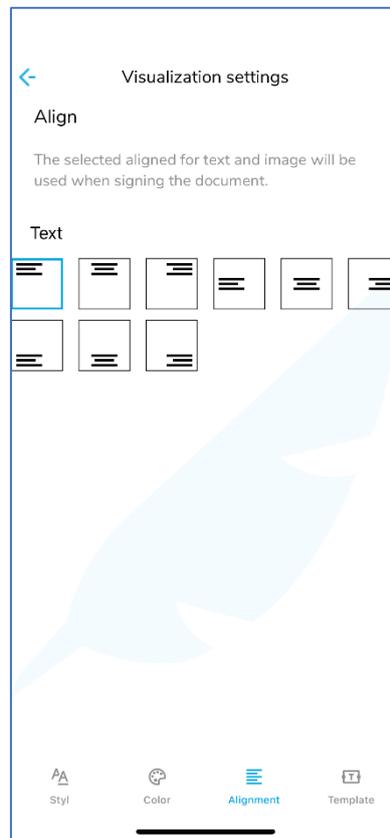
7.2.5.2. Font color

The following font color options can be defined in the **Color** tab. You can select a color from the pallet (**Grid** option) or using the sliders (**Slider** option) in **RGB mode**.



7.2.5.3. Alignment

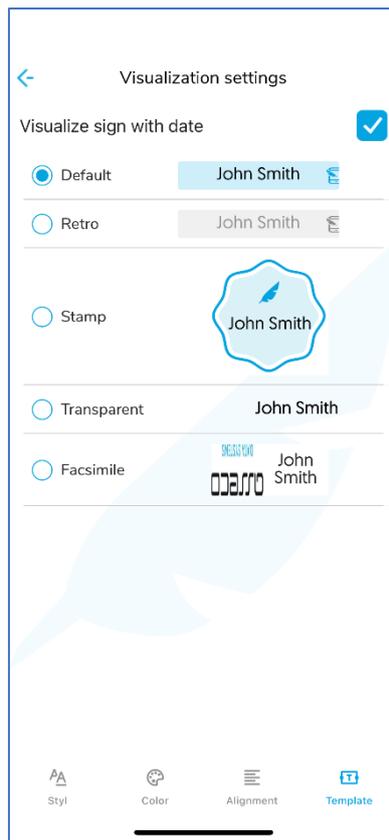
In the **Alignment** tab you can define options for alignment of the text and facsimile in the visualization.



To define the alignment, select the appropriate icon.

7.2.5.4. Template

In the **Template** tab you can choose a template according to which the visualization will be performed.



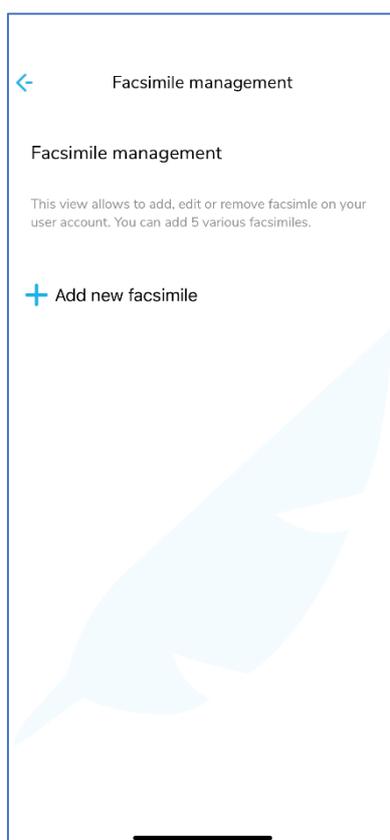
If you select facsimile, the visualization alignment option will also appear in the **Alignment** tab.



7.2.6. „Facsimile management” option

The **Facsimile management** option allows you to manage your own facsimiles. You can add and remove your own facsimiles. You can add facsimiles only from the files saved on your device. A maximum of five various facsimiles can be added.

7.2.6.1. Adding your own facsimile



To add your own facsimile, press the **Add new facsimile** button. The system's file explorer will be launched, in which the graphic file representing the facsimile must be selected.



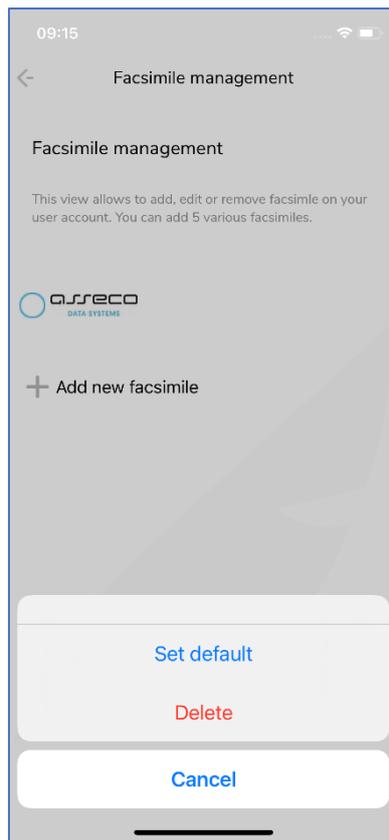
After selecting the graphic file, the image editor will be launched.



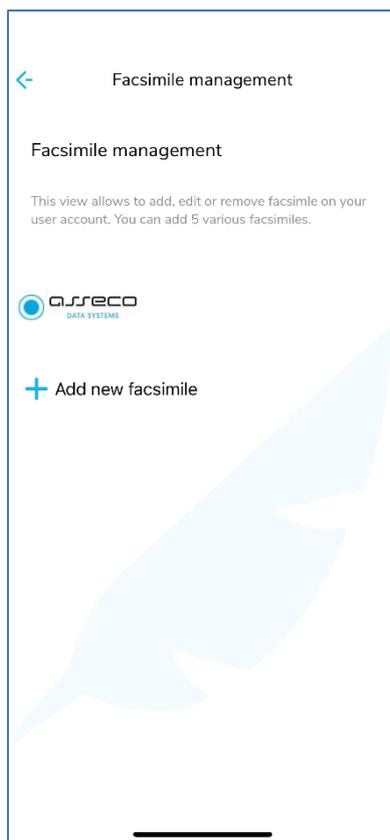
Confirm the selected facsimile by pressing the Choose button. After confirmation, the selected pattern will appear on the list.



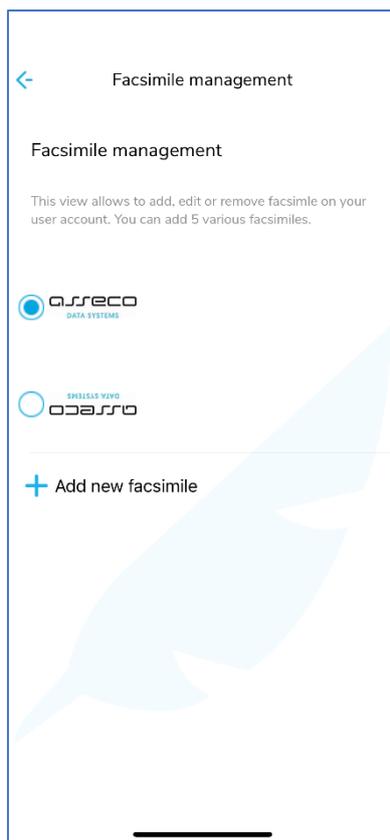
In the next step, set the default facsimile. To do this, press the selected facsimile. Options will appear, including **Set default**.



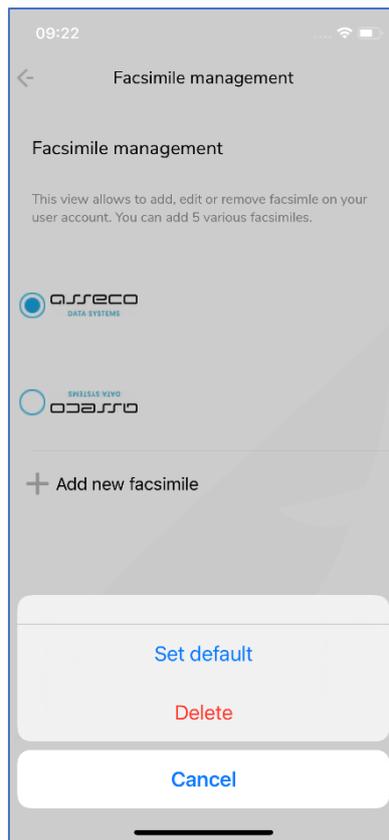
When you select the **Set default** option, the selected facsimile will be marked on the list and set as default.



7.2.6.2. Changing the default facsimile



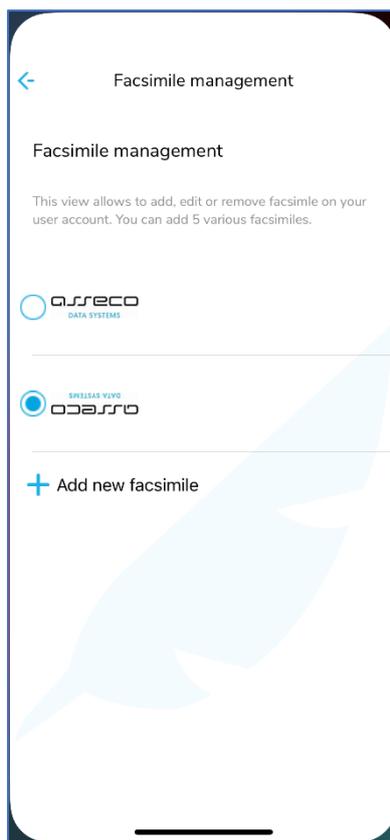
To change the default facsimile, click on the facsimile to be set as a default. You will be asked to confirm the change of the default facsimile.



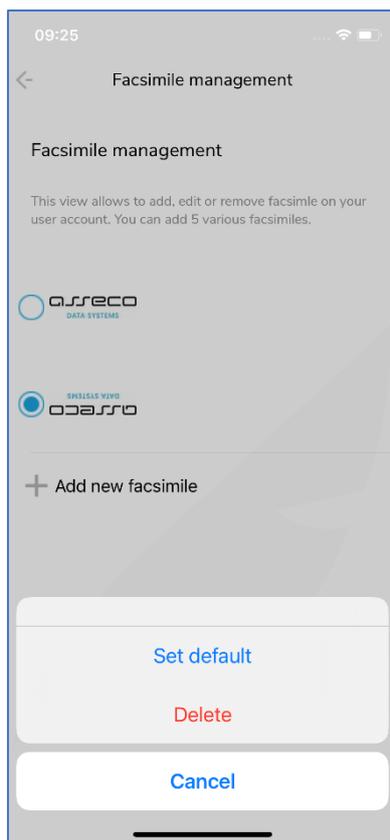
When you select the **Set default** option, the default facsimile will be changed.



7.2.6.3. Removal of facsimiles



To remove the selected facsimile from the list, click on it. You will be asked to confirm the removal of the selected facsimile.



After confirmation, the selected facsimile will be removed from the list.



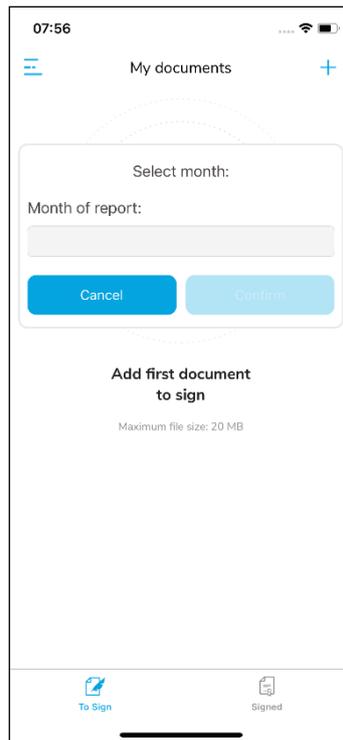
7.2.7. „Trusted time stamp” option

Enabling this option will result in adding a time stamp to the signature.

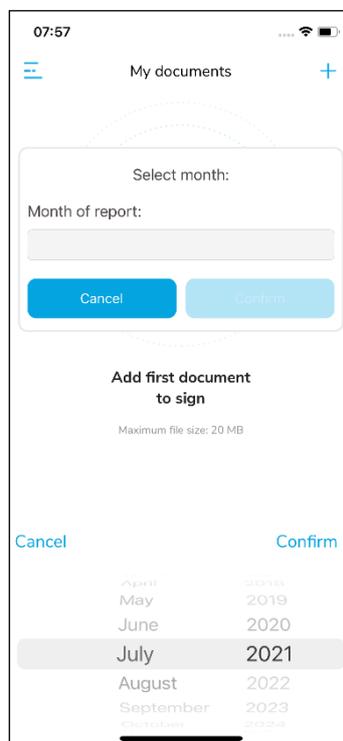
7.2.8. “Generate report” Option

This option allows you to generate a summarized report of events in PDF form. Reports can be generated for the period of the selected month up to one year back.

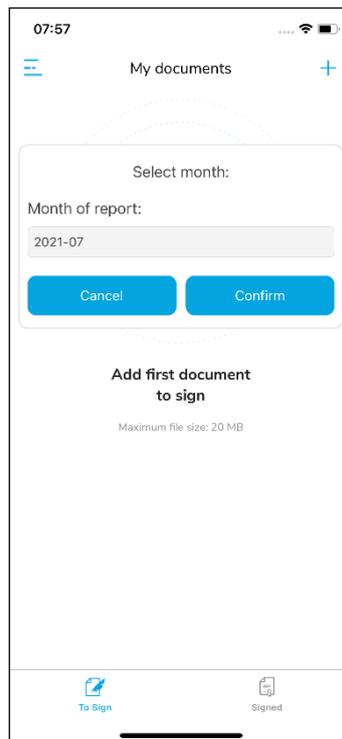
In order to generate a report, select this option – a form will appear where you can select the month to which the report will relate.



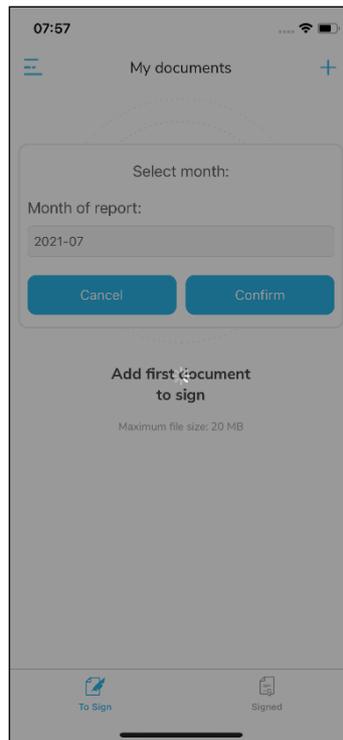
Then click in the empty edit box – a form will appear allowing you to select the month.



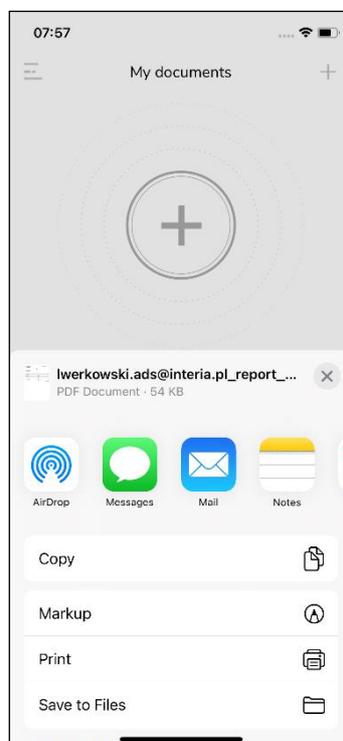
After selecting the appropriate month, press the **Confirm** button. You will return to the form allowing for report generation and the selected month will be entered into the form.



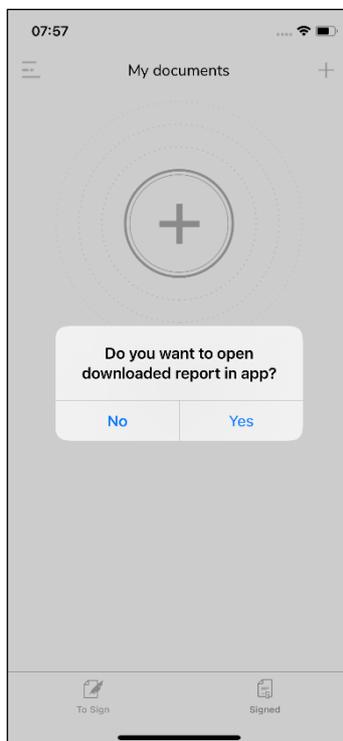
Then, press the **Confirm** button. The report generation will begin.



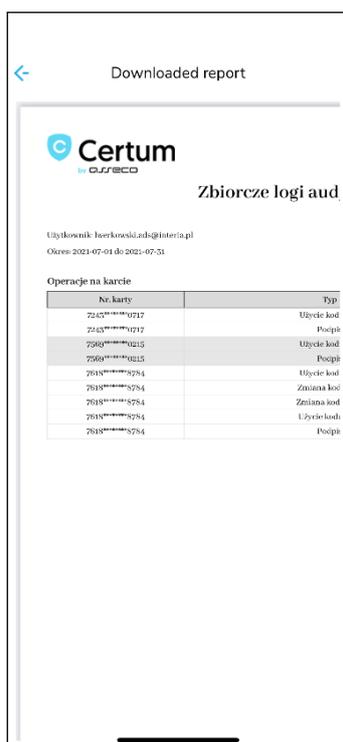
After a moment, the report will be generated and a system save window will be displayed where you must indicate the location where the generated report will be saved.



After pressing Save, you will be asked if you want to view the report on the device.



After pressing Yes, the report will be displayed on the device.



7.3. Application Settings Section

In the **Application Settings** section, the following options are available:

- Functions of the application
- Language of the application
- Notifications

The above options are described in detail in next sections.

7.3.1. „Device function” option

This option allows you to set the application operating modes. You can set the modes:

- Signing – setting this mode will allow the application to be used to sign files and will not generate OTP tokens
- Generate token codes – setting this mode will allow the application to be used to generate OTP tokens only without the possibility of executing a signature

Both modes can be enabled at the same time – then the application will work in the mode called “All in One”, i.e. the application will generate OTP tokens and will allow to execute the signature.

7.3.2. „Notification” option

Enabling this option will cause the application to present notifications about events that occurred on the User’s account. If this option is enabled, the application notifies the following events:

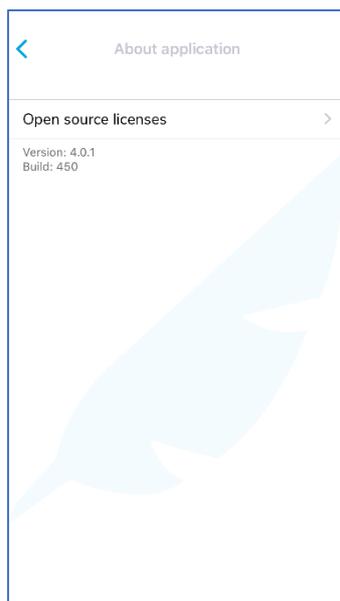
8. Resetting the access to the service
9. Changing the PUK code
10. Generating the event report in the CCM module by the User

6.3.3. „Factory reset” option

This option allows you to reset the entire application and return to the condition it was in after installation.

6.3.4 „About application” option

Selecting this option will cause displaying detailed information about the application.

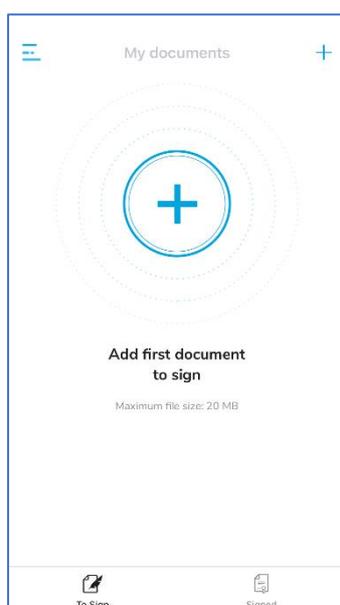


7. Signing files

7.1. Adding a file to the list of files to be signed

In order to add a file to the list of files to be signed, log into the service.

After logging in, the application goes to the **To sign** tab.



Then, press the **Plus** button located in the middle of the screen. A browser of files will be shown.



Using the file browser, find and select a file, which should be included on the list of files to be signed.

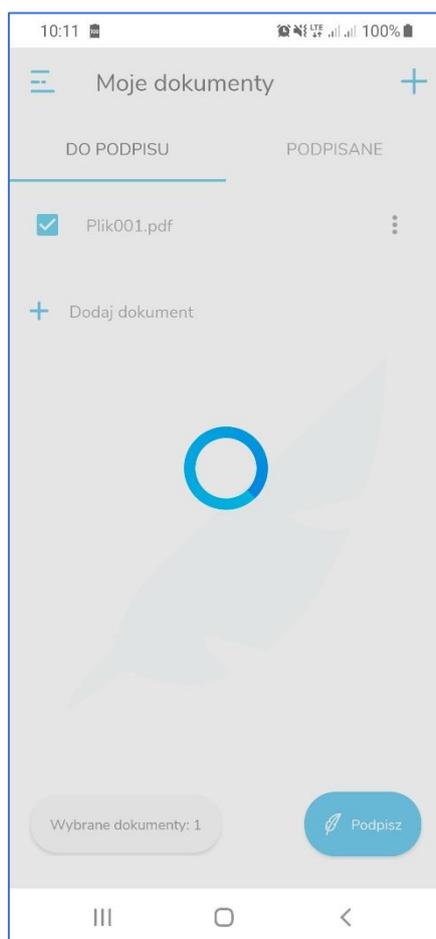
After choosing a file it is placed on the list of files in the **To sign** tab.



7.2. Starting the proces of file signing

In order to start the process of signing files, choose this file on the list and press the **Sign** button located in the bottom right corner of the screen.

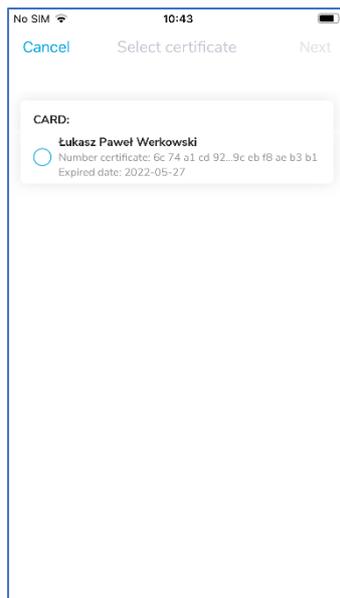
A process of downloading cards and certificates of the User will start - it is signaled by a circle icon symbolizing the passage of time.



7.3. Selection of the Signing certificate

After reading the cards and certificates of the User, choose a certificate from the list with which a signature will be performed.

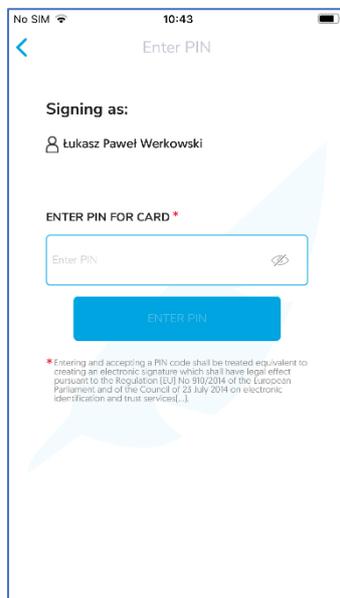
The situation in which the certificate (third in the order) issued for the Subscriber **Łukasz Paweł Werkowski** has been chosen is presented below.



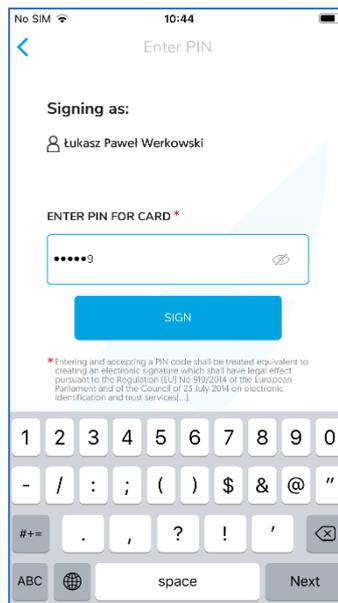
7.4. Entering the PIN code to the selected Signing certificate

After indicating a certificate, start the process of entering the PIN code to the selected certificate.

To do this, press the arrow directed right, located in the upper right corner of the screen. A screen where you have to enter the PIN code will appear.



Enter the PIN code for the card.



7.5. Signing a file

After entering the PIN code and pressing the **Sign document** button the process of signing the selected file will start. An animation symbolizing the signing process will be visible on the screen.



After finishing the signing process a summary will be displayed.



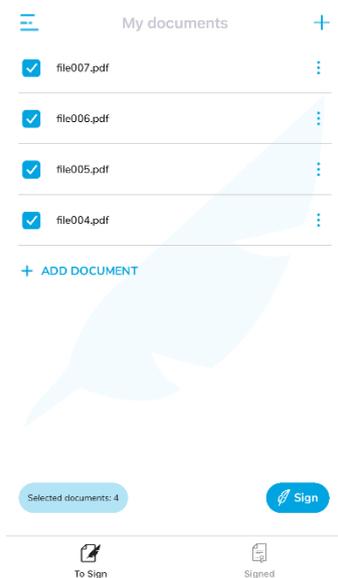
The following options are available on the summary screen:

- Sign next file – selecting this option will take you to the **To sign** tab
- Send document – selecting this option will start the process of sending the signed file to external applications;
- Back to folder – selecting this option will take you to the **Signed** tab;

8. Signing multiple files at a time

SimplySign application allows for signing multiple files at a time, with a single PIN code entered to the certificate with which the signature is made.

To sign multiple files at a time, enter these files to the list of files to be signed.



After entering files to the list and selecting them, start the signing process, as described in the previous section.

As a result, all selected files will be signed. After correct signing of files, a relevant report will be displayed.



The summary contains options described in the previous chapter.

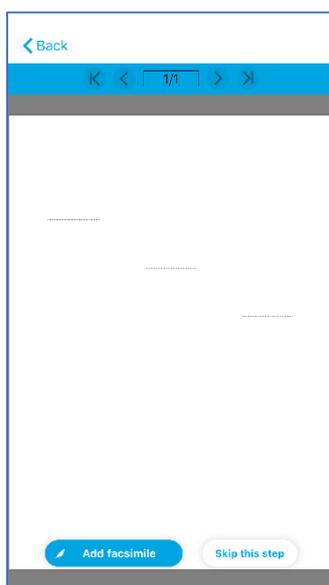
9. Making a signature with visualization

SimplySign application allows for making a signature with the so-called visualization.

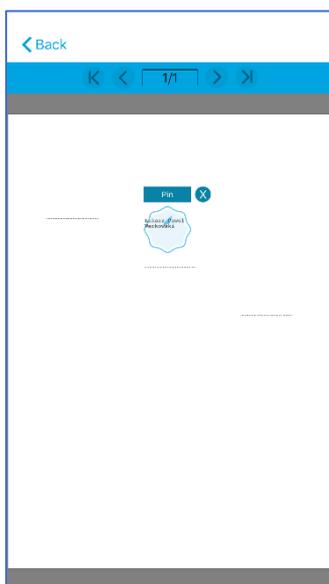
The visualization contains a graphic sign selected by the signatory in the options of the application (the option of **Visualize sign**). Additionally, depending on the settings, it may also contain the current date and the Signature reason. Then, in the settings you should set the signature pattern and mark in the **Visualize sign** option the desire to attach the current date of the signature to the visualization.

In order to make a signature with the visualization, click within the area of the document name on the list of files to be signed. A preview of the selected file where you can add the visualization will be activated.

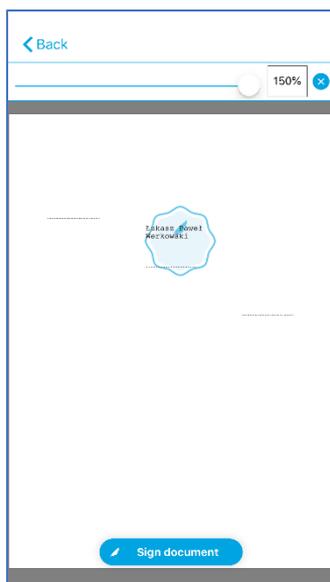
Na podglądzie, u góry strony znajduje się pasek nawigacyjny pozwalający na szybkie przechodzenie po stronach dokumentu.



Then, press the **Add facsimile** button. The file preview will show a signature pattern that can be moved. The pattern should be moved to the desired place.

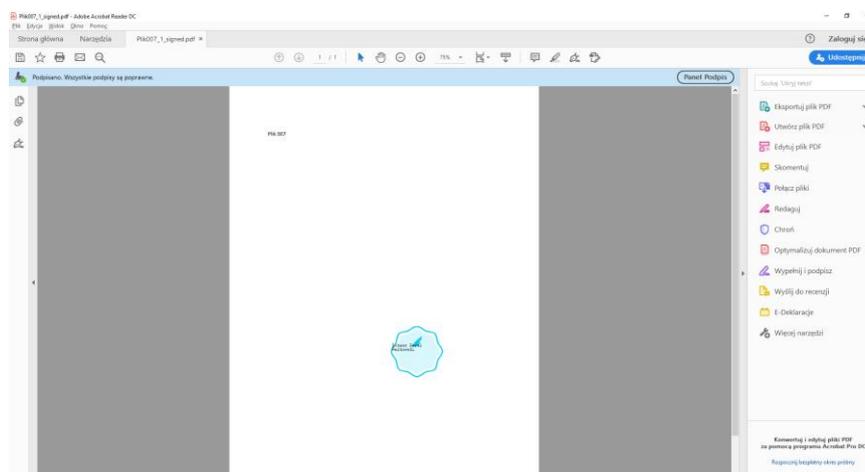


Then, press the **PIN** button. The visualization will be added to the file. Dodatkowo, na górze ekranu, pojawi się suwak pozwalający na skalowanie podpisu. Poniżej przedstawiono efekt przeskalowania wizualizacji podpisu do 150%.



Then, press the **Sign document** button. The standard process, described in the previous chapters, of signing the indicated file will be started.

Below is an example of a PDF file signed with the visualization.

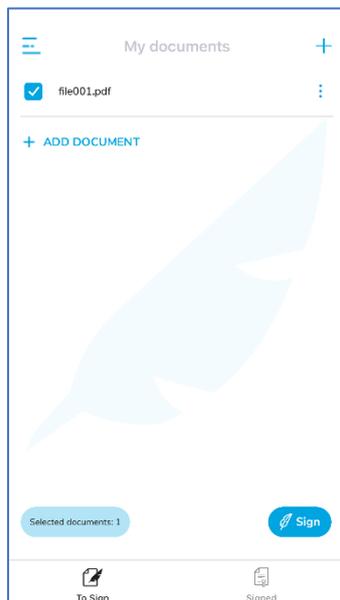


10. Changing the default certificate while Signing files

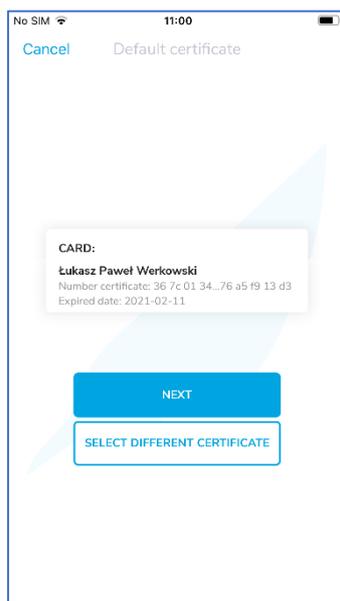
In case when a default certificate is set in the application Settings, when signing files it is suggested by default as a certificated which will be used for signing files. However, during the signing process you can temporarily change it to a different one and make a signature with that other certificate. As it was previously highlighted, such a change is temporary and concerns only this one action of signing files, at the next action of signing files, the same initially set default certificate will be suggested again.

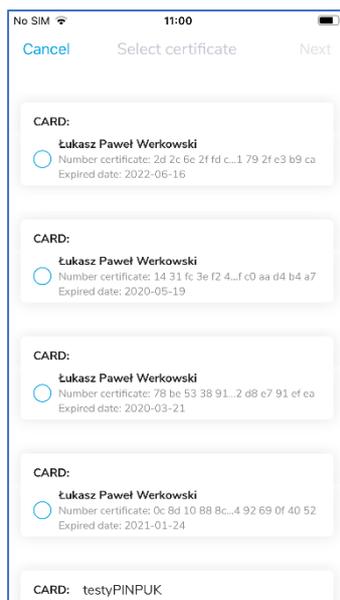
A process of signing during which a default signing certificate was temporarily changed to a different temporary one is presented below.

The process starts as standard in the **To sign** tab where you have to choose files which will be signed.

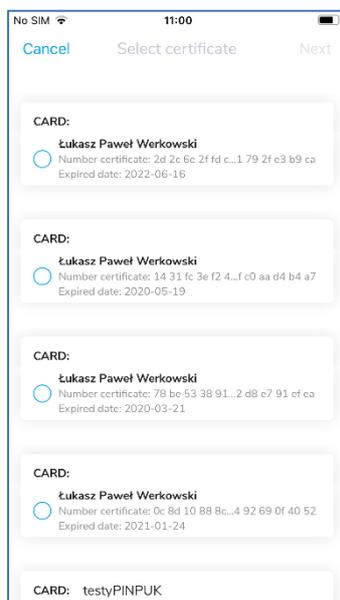


After selecting files which are to be signed and pressing the **Sign** button, the process of signing starts. A certificate set in the application Settings as a default will be indicated for signing.

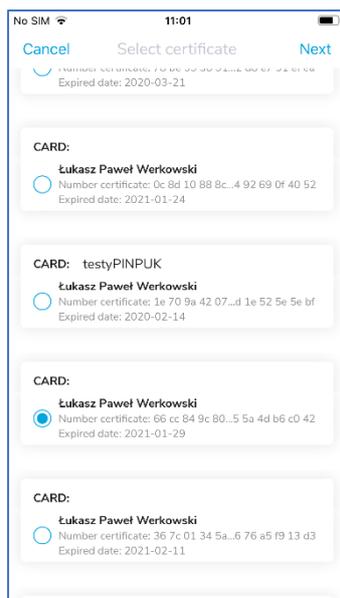




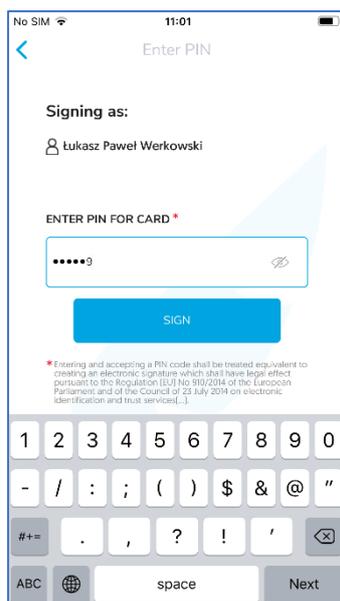
To temporarily change a signing certificate to a different one, press the **Choose different certificate** button. A list of cards and certificates will be displayed, where the certificate that is currently set as default is indicated (below in the picture a sample certificate with serial number 36 7c 01 ...).



Then, choose a temporary certificate. (below in the picture there is a sample certificate with serial number 66 cc 84 ...).



After indicating the temporary certificate, go to the next step. A screen where you have to enter PIN code to the card with the selected certificate will be displayed.



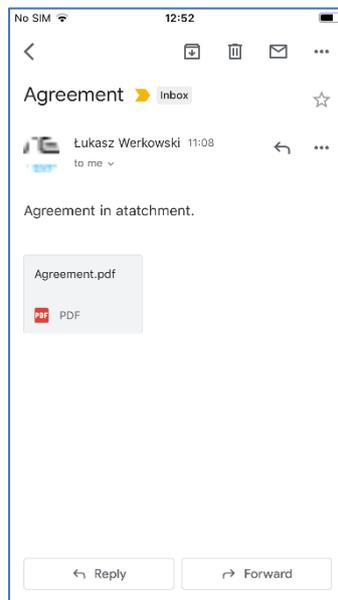
The signing process continues as described in the previous chapters. After the signature is made, the original default certificate is set.

11. Importing files from external applications

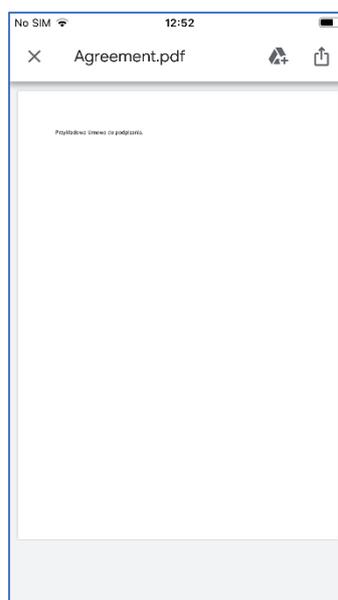
It is possible to import a PDF document from the external application directly to the list of files to be signed.

An example of PDF document import from the Microsoft Outlook application is presented below.

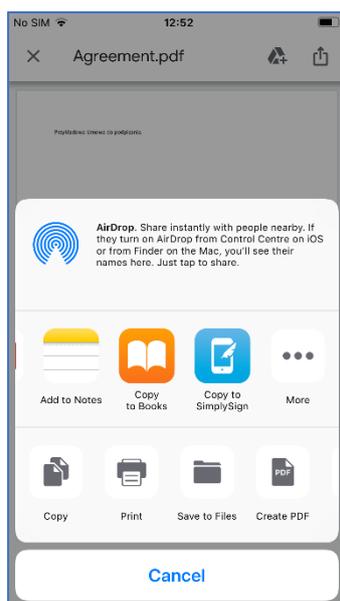
In order to import a PDF document, open a message containing that file.



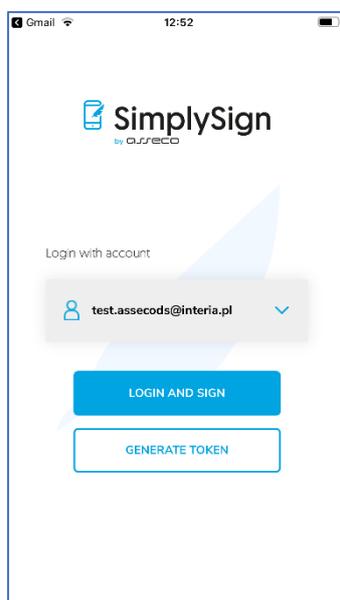
Then, display the contents of the file.



Then press the Share icon, located in the top right of the screen – the **SimplySign** application will appear in the list of options.



Then select the **SimplySign** application icon – the SimplySign application will be launched – the application will go straight to the login screen.



You have to log into the application – the imported file will be included in the list of files **To sign**.

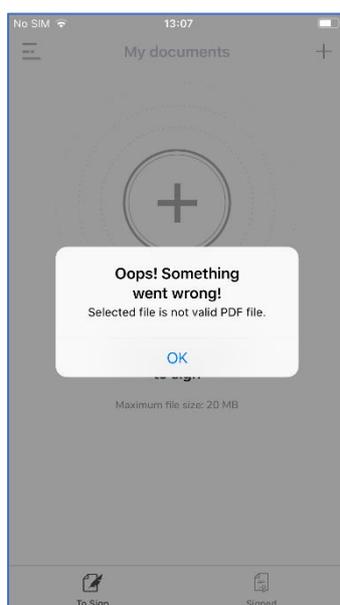


The next step is to sign a file in line with a description presented in previous sections.

12. Handling errors when Signing files

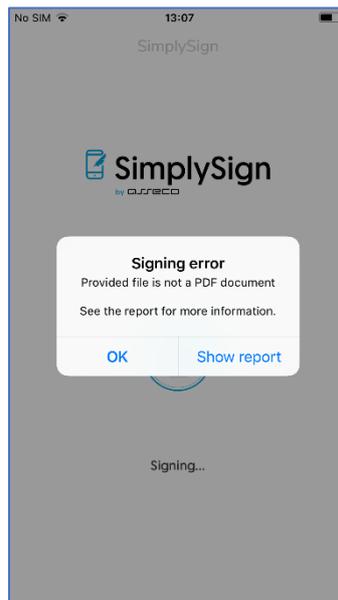
12.1. Incorrect PDF file

If an attempt is made to add a PDF file that is structurally incorrect to the list of files, a message with a content **The selected file is not a valid PDF file** will be displayed and the file will not be added to the list.



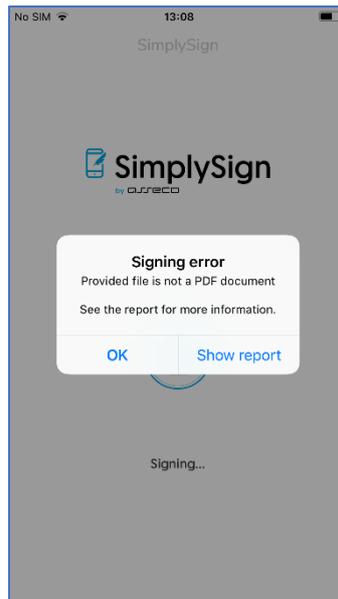
12.2. Secured PDF file

When you try to sign a PDF file secured against modification, then after entering and confirming the PIN code an error with a content **The document has not been signed** will appear. **Document secured against modification.**



12.3. Incorrect PIN to the Signing certificate

When you enter and confirm an incorrect PIN code, an error message saying "The document has not been signed" will appear. **An incorrect PIN code was entered...**



12.4. Blocked card

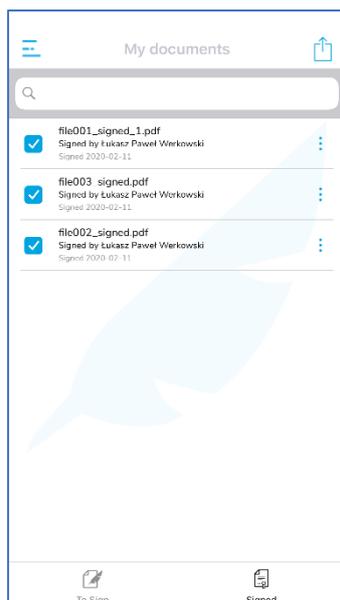
If the card is blocked (blocked PIN code), the following message will appear when you try to sign a file with a certificate from this card: **The document has not been signed. Blocked PIN.**

13. Handling the signed files

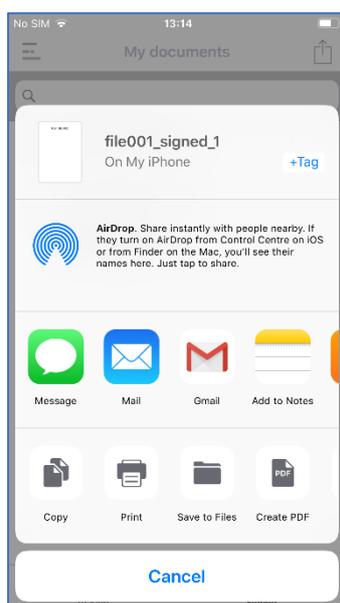
13.1. Sending of signed files by e-mail

Signed files can be sent from the level of the Signed tab by e-mail to another user.

To do this, firstly you have to select files which are to be sent.

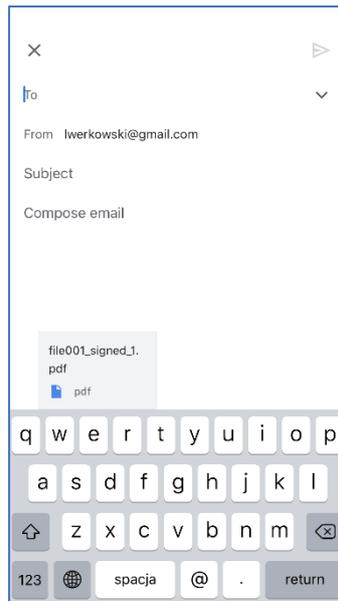


Then select the files to be sent and press the file sharing button. A screen allowing the selection of the e-mail program through which these files are to be sent will appear.



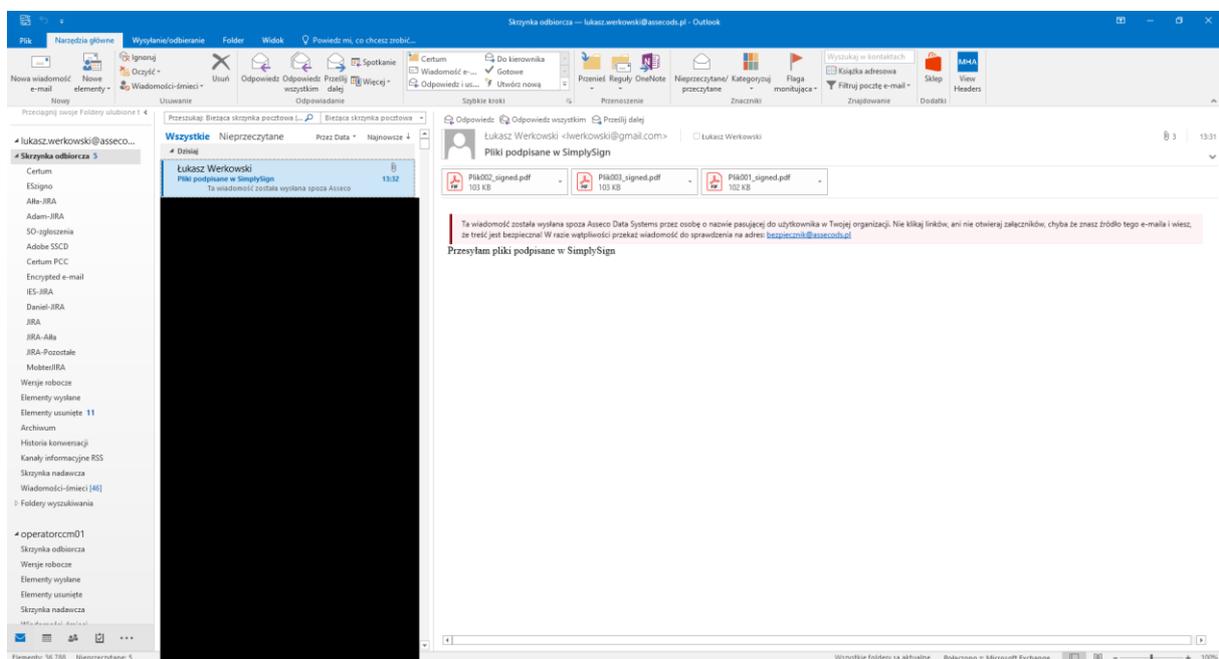
In the presented example the **Gmail** option was selected. A window allowing for preparation of an e-mail message was opened.

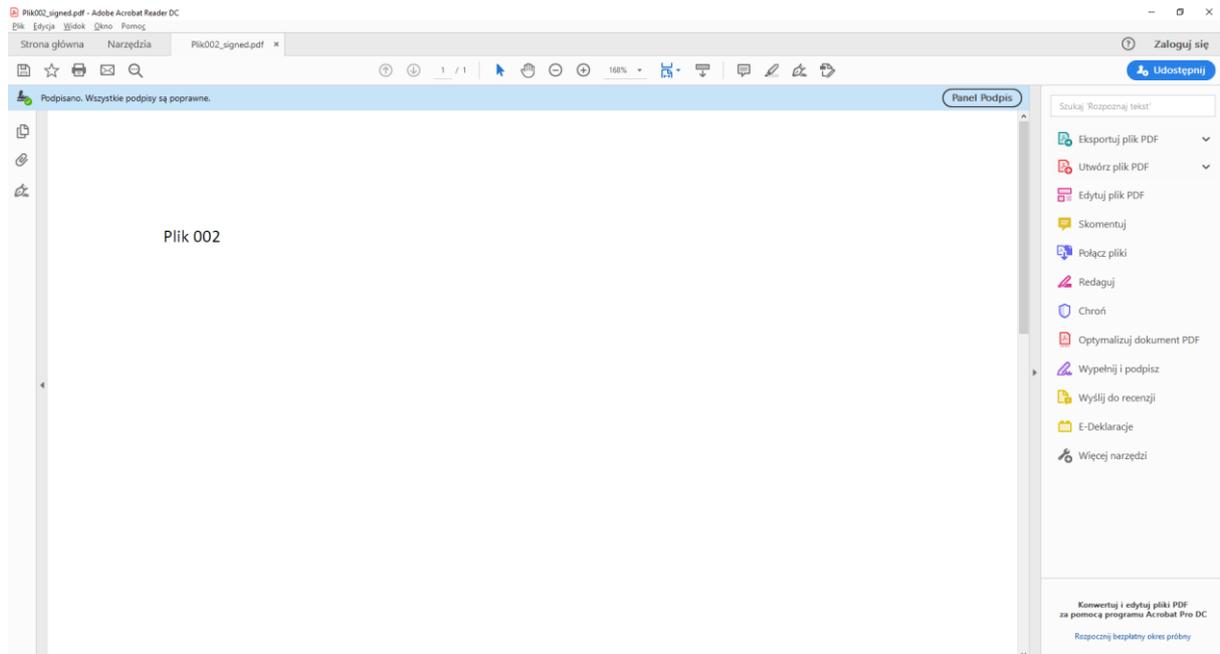
The selected files which have been previously signed are visible as the attachments. Later you have to enter a recipient's e-mail address, subject and content of the message.



After creating a message, you have to press the button of a right arrow. The process of sending messages will start and the application will return to the **Signed** tab.

The recipient will see a message in their mail box. It can be opened, for example, in a desktop application as presented in a figure below.

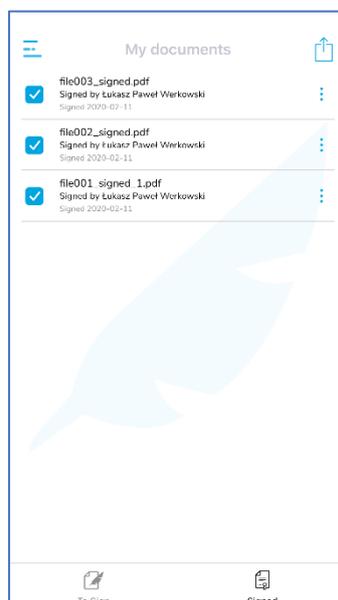




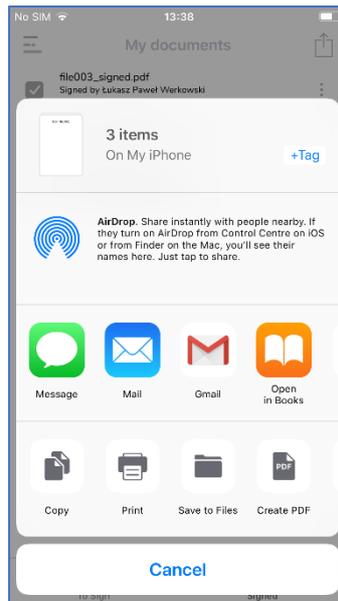
13.2. Save signed documents to iCloud Drive

Signed files can be sent from the level of the **Signed** tab to **iCloud Drive**.

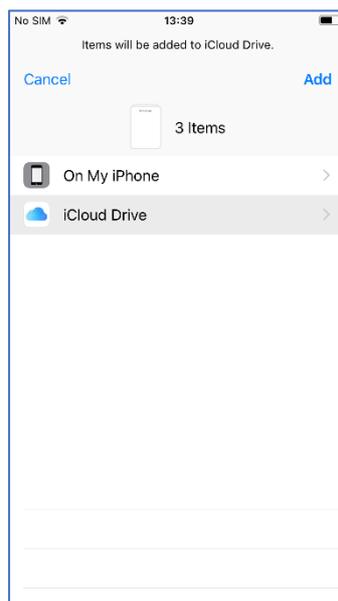
To do this, firstly you have to select files which are to be sent.



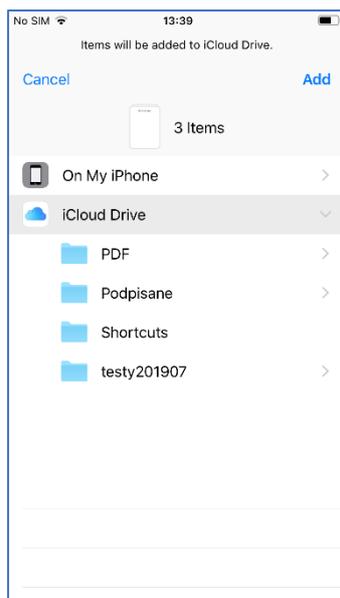
After selecting the files, press the file sharing icon. A screen allowing for indication of a destination of the sent files will be displayed.



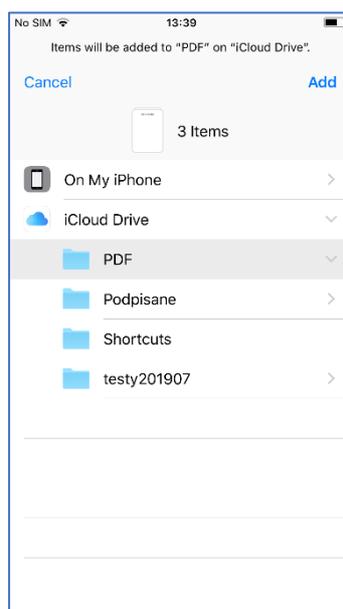
Then you have to choose the service to which you want to send the selected files.



Then select **iCloud Drive** service. A screen allowing the selection of the appropriate directory for the files to be selected will appear.

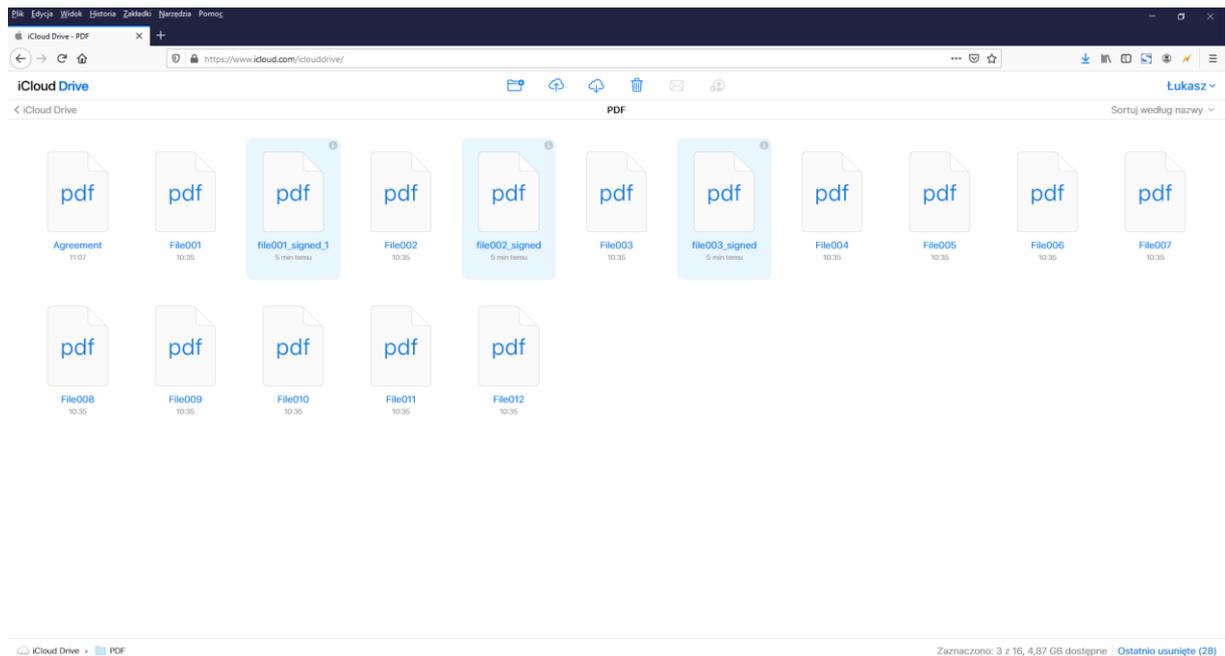


A situation in which a directory named **PDF** was selected as the target directory is presented below.



Then, press the **Add** button. The files will be sent to iCloud Drive.

They will be visible for the drive owner after logging into their iCloud account.



14. Deleting files

Deleting files on the list of files to be signed and on the list of signed files is performed in the same way.

First, select the file to be deleted. Then press the context menu button (three vertical dots on the right side of the screen) for the selected file. In the context menu there is an option **Delete** – use it and the file will be deleted.

