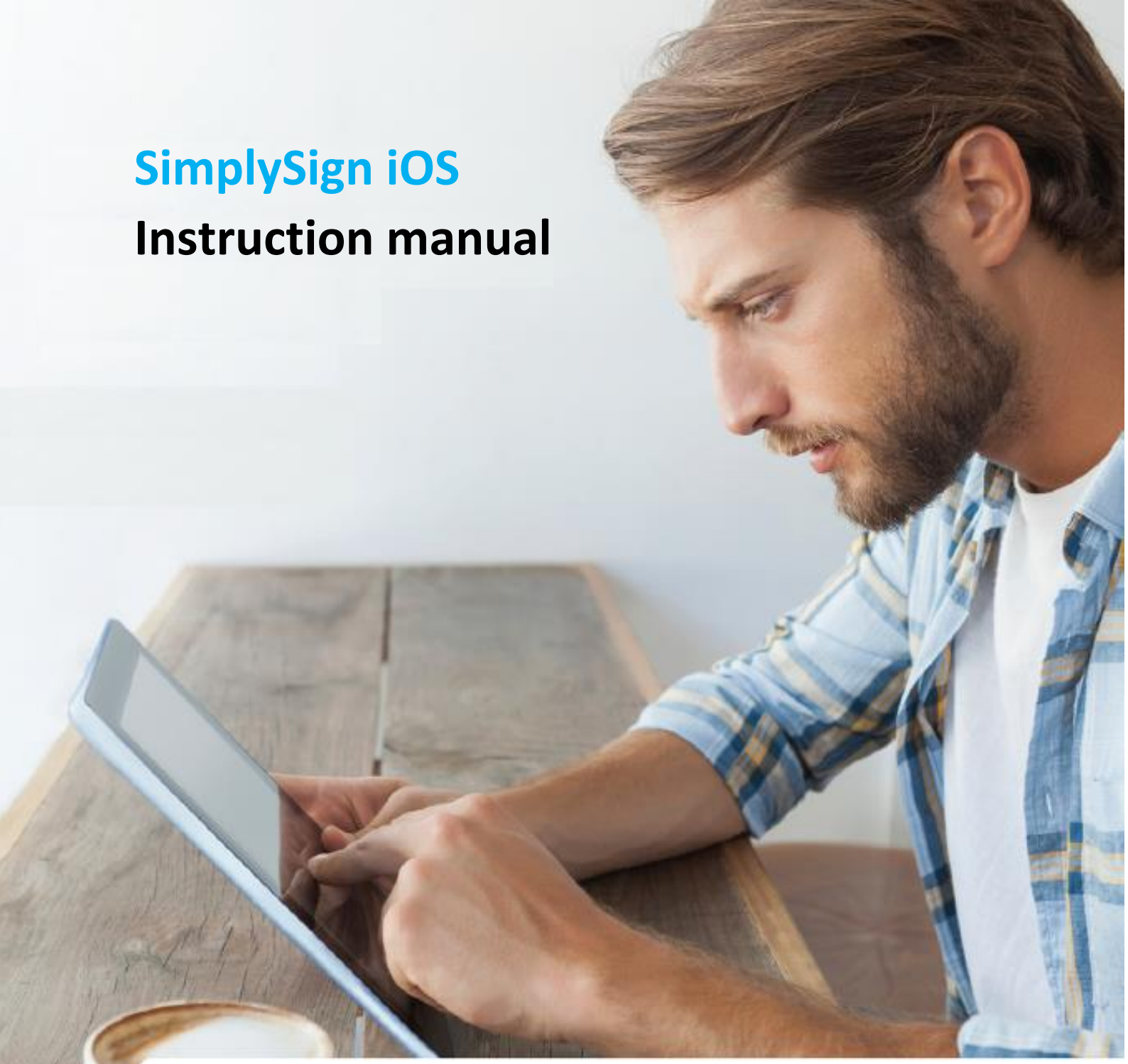
SimplySign iOS

Instruction manual



SimplySign iOS **version 4.1**

certum.pl

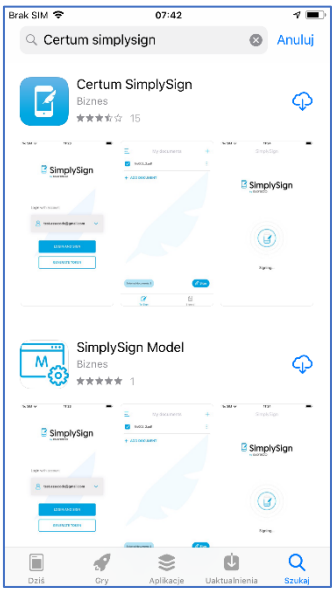
Certum by asseco

Table of Contents

1. Legal information

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.

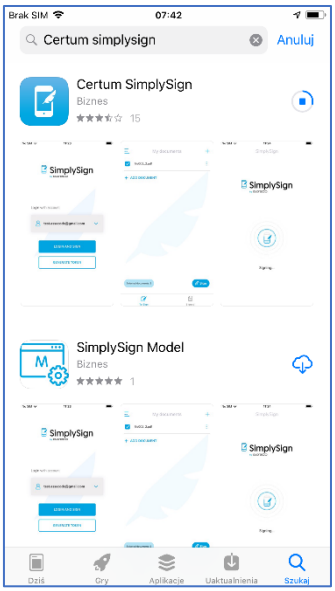


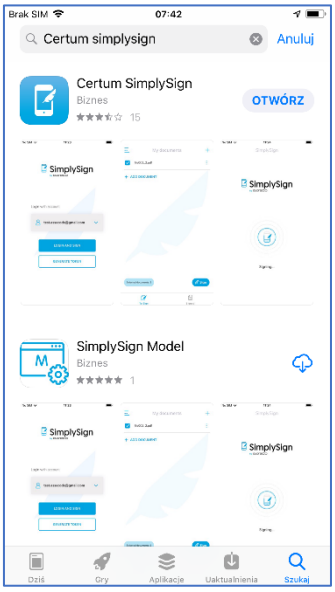
3. Requirements

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.



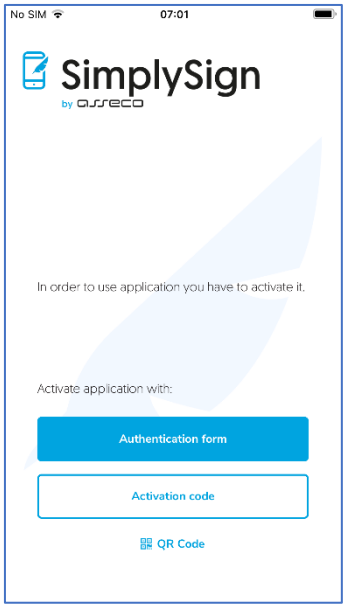


After correct installation, the **SimplySign** application icon will appear on the device Desktop.

5. Launching, activation of the application or reseting access to the service

5.1. Launching the application

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



5.2. Service activation

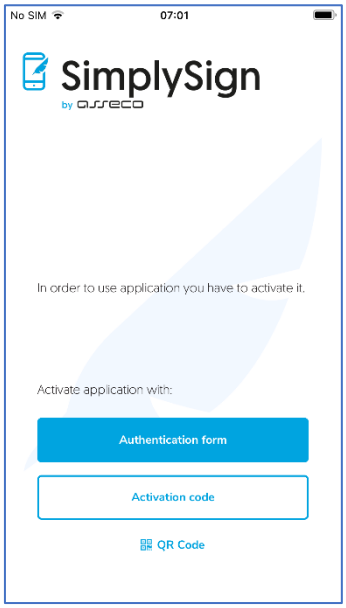
5.2.1. Activation using (personal) authentication data

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.

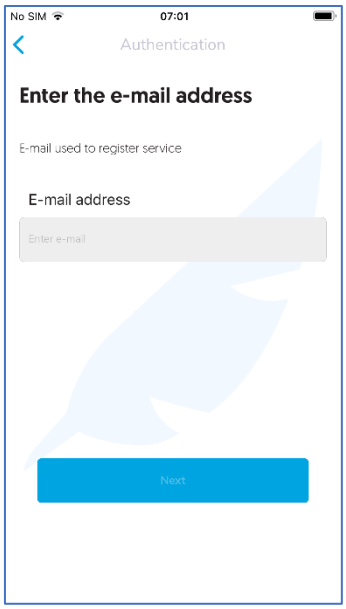
!!!ATTENTION

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.

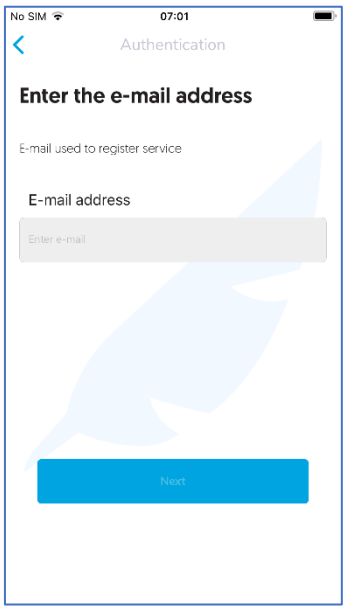


The **activation** is started by pressing the **Authentication Data** button. After pressing this button, a screen allowing for entering the e-mail address, which is the User's ID appears.

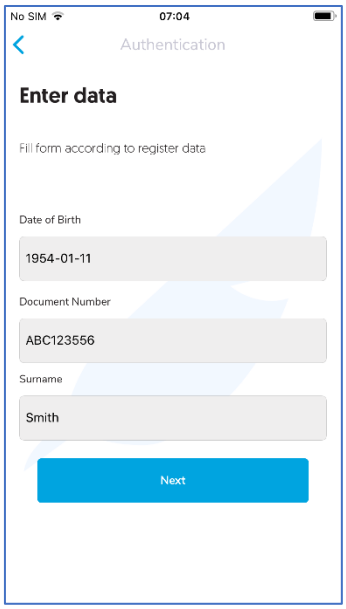


Then, in the field **E-mail address provided during registration**, you must enter an email, which is the User's ID.

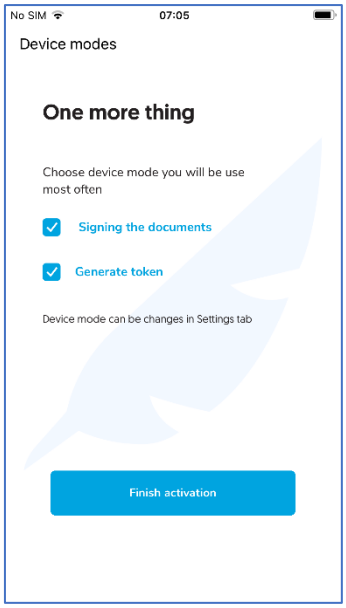
Then, press the **Next** button. If the ID is correct, the application will ask you to enter 3 randomly selected personal data of the User.



Then you must enter the correct personal data.



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

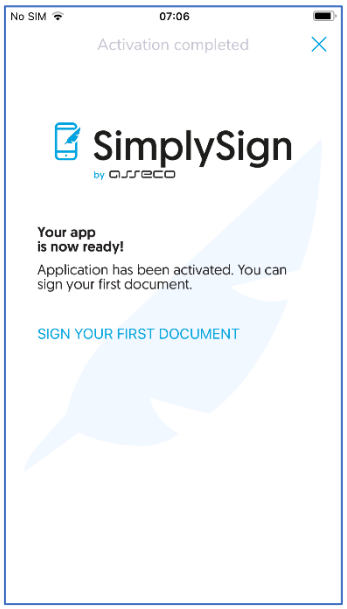


Two modes are available:

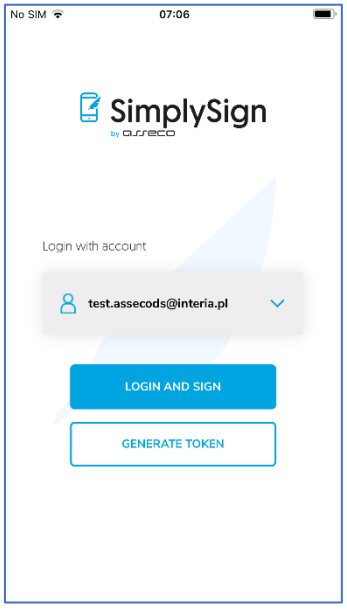
- Sign documents – it only allows you to sign documents – in such a case the login token will be downloaded from another device;
- Generate token code– it only allows you to generate a token – in such a case you will have to place a signature using another device;

The modes can be combined in order to obtain a possibility to generate a token and sign documents on the same device.

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



After pressing the **Sign your first document** button, the application will go to the start screen.



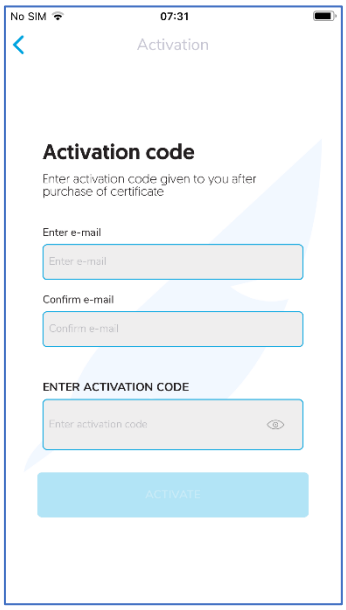
5.2.2. Activation using the activating code

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

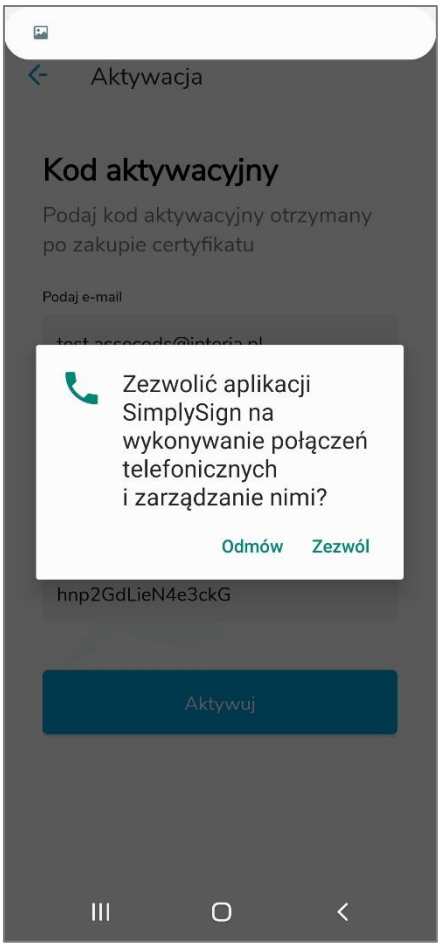
In the case of activation using the Activating Code, press the **Activating Code** button. After pressing this button, a screen allowing for activation of the application with the use of this activating code appears.

NOTE!!!

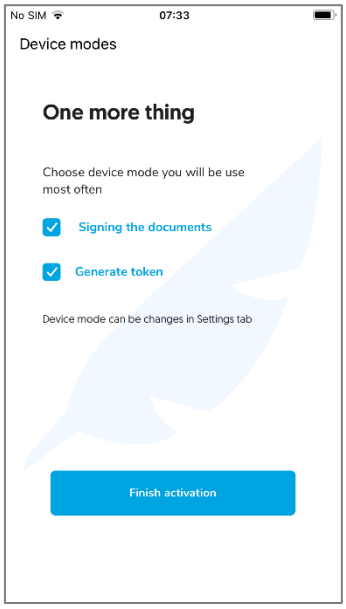
The e-mail address entered will be used also as the User's ID. It is recommended to use a real e-mail address to which the user has access – it is related to the fact that the e-mail messages (e.g. resetting a PIN code for a virtual card) sent from the SimplySign System to the User will be sent to that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



Then fill in the fields **Enter e-mail address**, **Enter e-mail address again** and **Enter activating code**. After these data are entered, press the **Activate** button. The application will ask for permission to access the internal information of the phone to register the device in the **SimplySign** system.



After agreeing, if the data is correct, the application will be activated and it will go to the screen, where you must select the application operating mode.



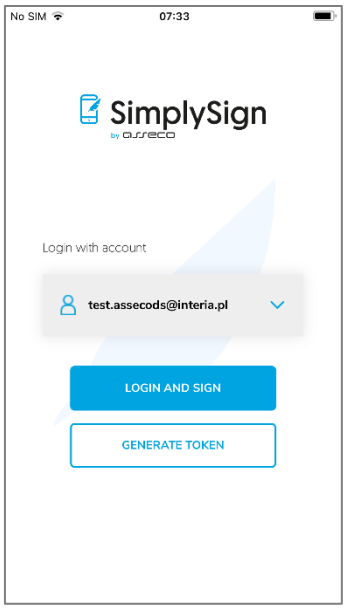
Two modes are available:

- Sign documents – it only allows you to sign documents – in such a case the login token will be downloaded from another device;
- Generate token code – it only allows you to generate a token – in such a case you will have to place a signature using another device;

The modes can be combined in order to obtain a possibility to generate a token and sign documents on the same device.

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

After pressing the **Sign your first document** button, the application will go to the start screen.



5.3. 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.

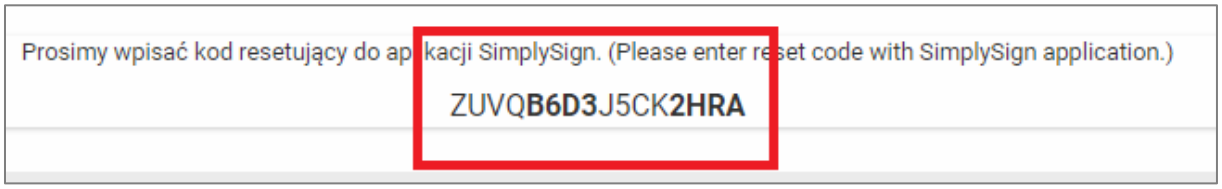
The User's data contained in their Application for qualified certificate submitted in the Certum system are verified.

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**.

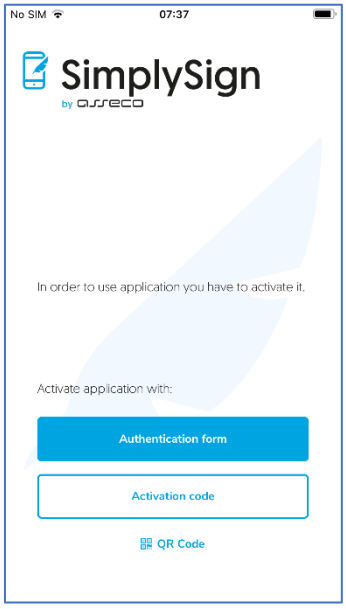
Depending on the reset method, when a secret is entered and the **Send** button is pressed, the User obtains either the so-called **QR Code** called a photocode or the so-called **16-character resetting code**. After receiving this data, do not close the browser but proceed to the next step of resetting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



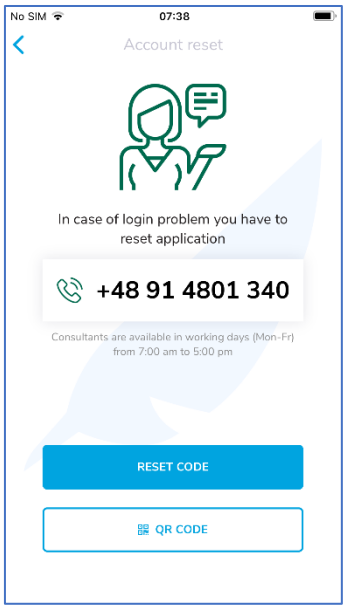
Both methods are described in the following sections.

5.3.1. Manual reset using the 16-character resetting code

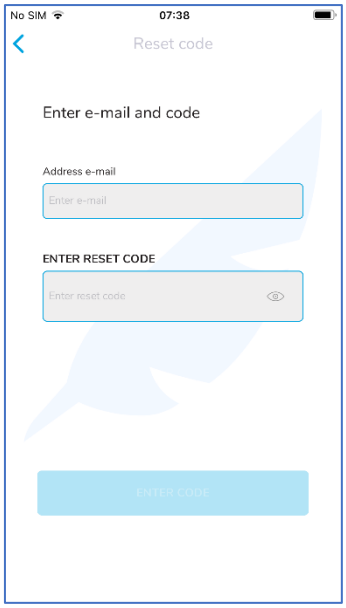
To reset access with the **16 character reset code**, start the **SimplySign** Application.



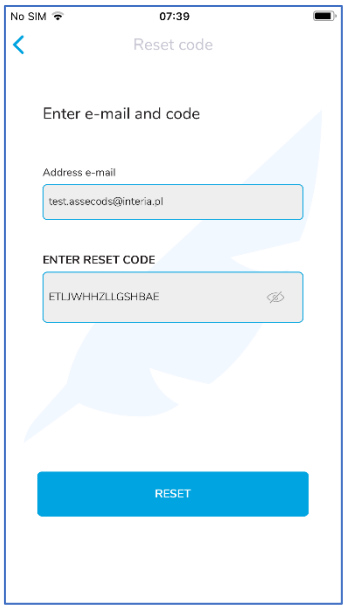
Next, press the **QR CODE** button located at the bottom of the screen. Further options will be displayed.



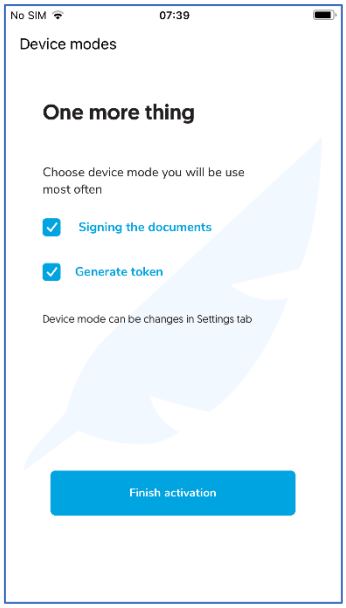
Then, press the **Reset code** button. A screen allowing you to enter the 16-character resetting code will appear.



Fill in the **Enter e-mail** and **Enter reset code** fields.



Then, press the **Reset** button. If the entered data is correct, access to the service is restored and the application will go to the screen where the application operating mode is to be selected.

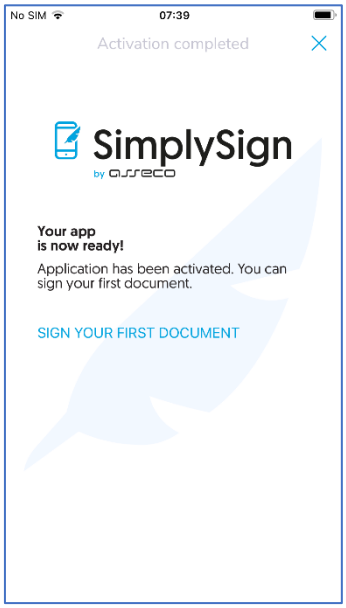


Two modes are available:

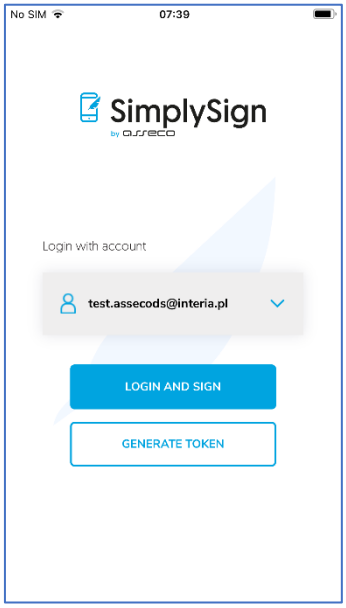
- Sign documents – it only allows you to sign documents – in such a case the login token will be downloaded from another device;
- Generate token code – it only allows you to generate a token – in such a case you will have to place a signature using another device;

The modes can be combined in order to obtain a possibility to generate a token and sign documents on the same device.

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

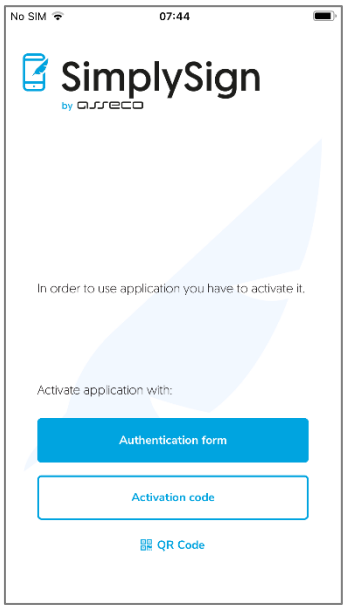


After pressing the **Sign your first document** button, the application will go to the start screen.

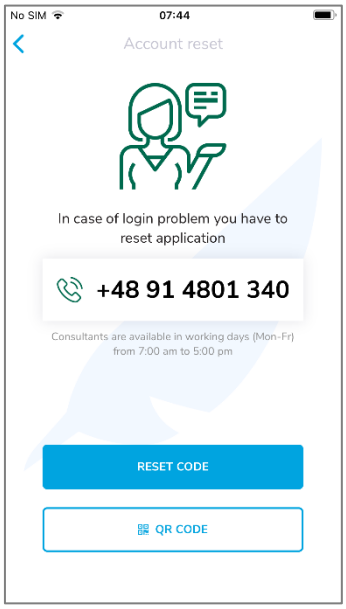


5.3.2. Automatic resetting with the use of QR Code

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

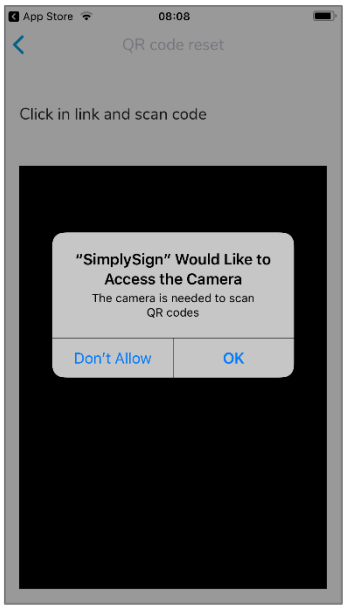


Next, press the **QR CODE** button located at the bottom of the screen. Further options will be displayed.

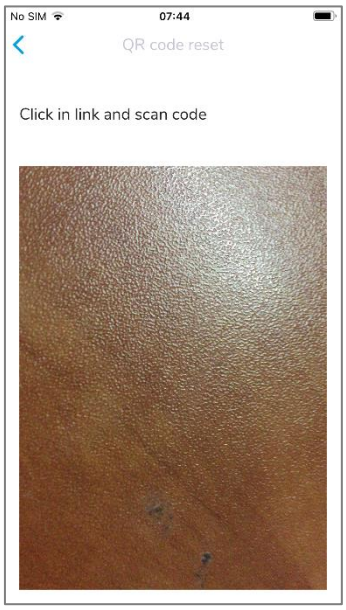


Then, press the **QR code** button. A screen allowing to scan the QR Code will appear.

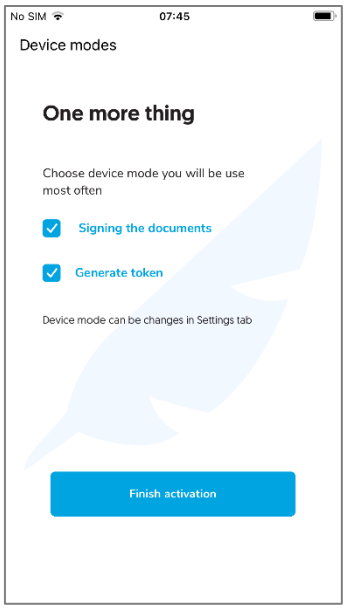
The application will ask for permission to access the internal information of the phone to register the device in the **SimplySign** system.



After allowing the access, you will be able to **scan the QR Code**.



After scanning the **QR Code**, the application will go to the screen where the application operating mode is to be selected.



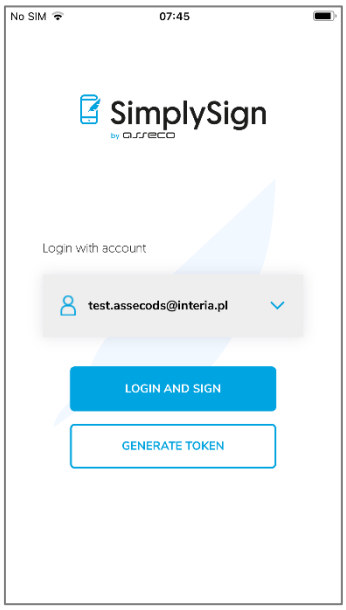
Two modes are available:

- Sign documents – it only allows you to sign documents – in such a case the login token will be downloaded from another device;
- Generate token code – it only allows you to generate a token – in such a case you will have to place a signature using another device;

The modes can be combined in order to obtain a possibility to generate a token and sign documents on the same device.

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

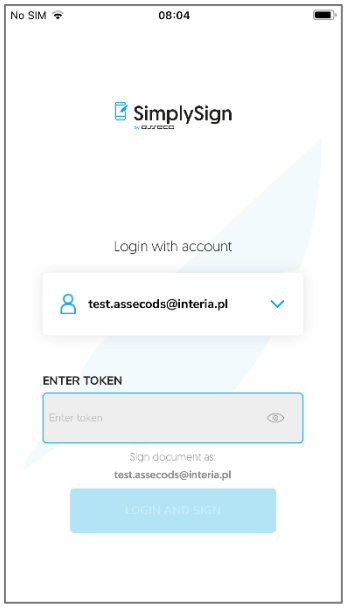
After pressing the **Sign your first document** button, the application will go to the start screen.



5.4. Application operating modes

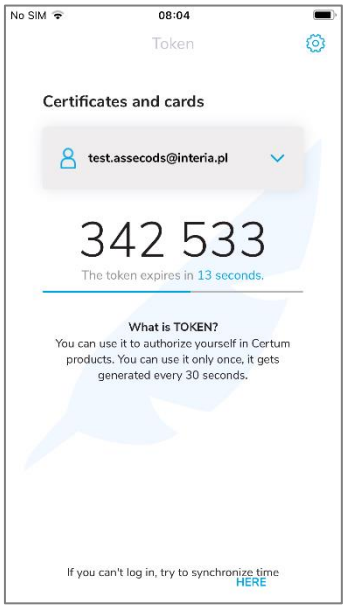
5.4.1. Operation in "Sign documents"

If during activation of the application it is set that the application should work in the “Document signing” mode, this will cause that the application will not generate OTP Tokens and only signing of documents will be possible. In such a case, after launching the application, a screen allowing logging into the service will be immediately displayed.



5.4.2. 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.



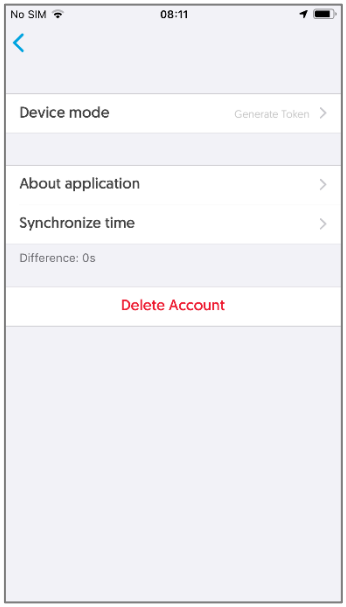
5.4.2.1. Force time synchronization

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.

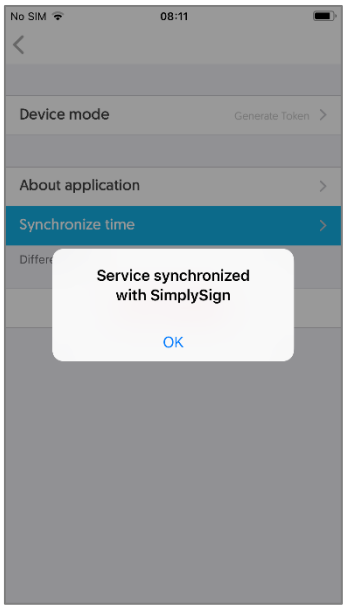
This is used in case of problems with logging when there is a suspicion that the **OTP Token** is generated incorrectly on the device.

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.

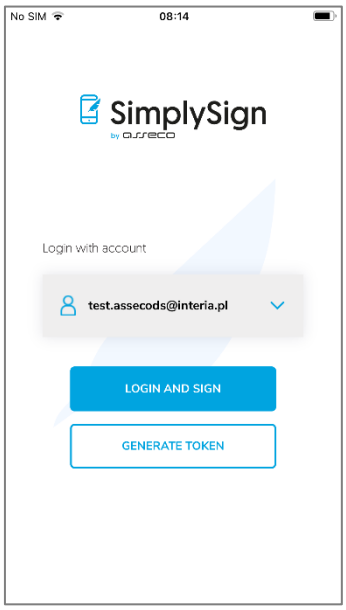


Then, press **Time Synchronization** button in the Settings. The time will be synchronized and the difference between the time in the SimplySign application and the time on the device will be shown in the Settings.



5.4.3. Operation in "All in one" 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.



5.4.4. 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:

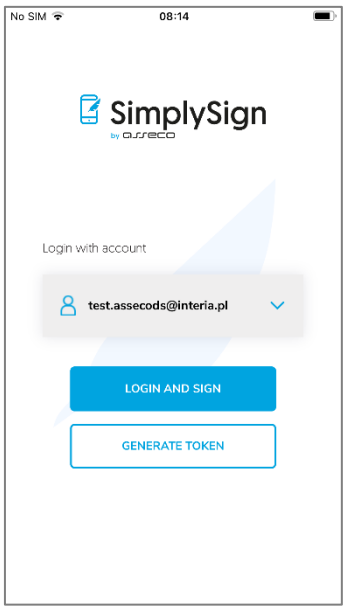
- from “All in one” mode to “Generate token code” mode
- from “All in one” mode to “Sign documents” mode
- from “Generate token code” mode to “All in one” mode
- from “Generate token code” mode to “Sign documents” mode

5.5. Multiple accounts support

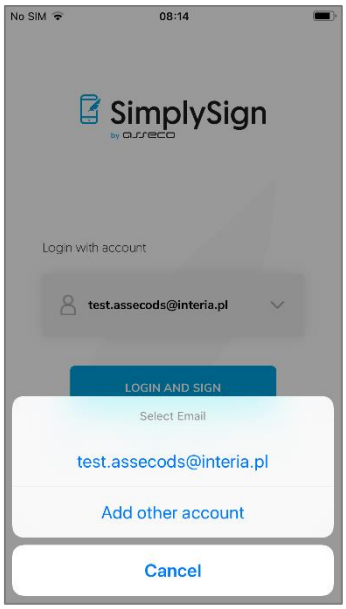
The application allows the use of multiple accounts. Below is a description of adding another account in the **All in One** mode and the **Token code generating** mode.

5.5.1. "All in one" mode

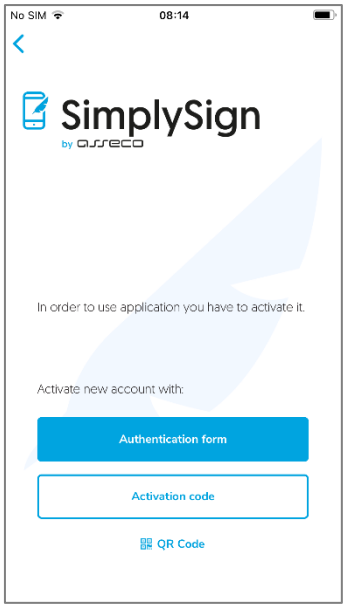
To add another account in the All in One mode, start the application.



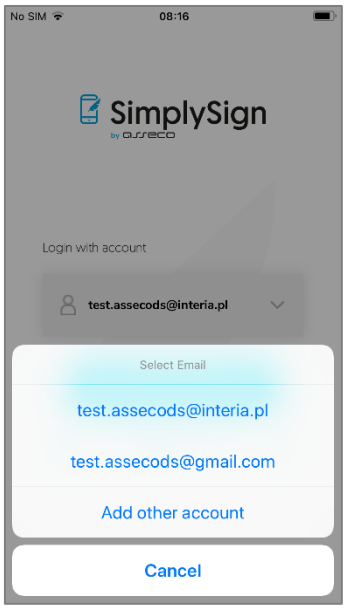
Press the area within the account name. A list of accounts with the option **+ Other account** will be expanded.



After pressing **+ Other account** button, a window allowing you to activate the new account in the way you choose will appear.

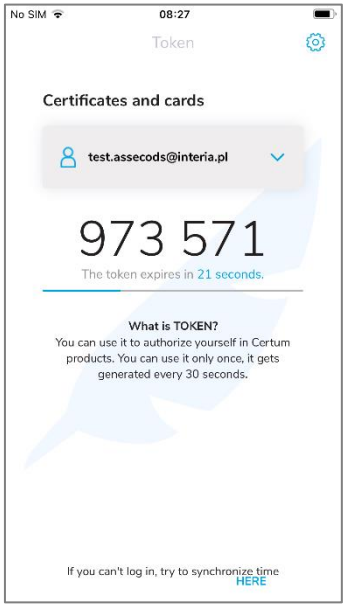


Methods of activation are presented in the previous chapter. After activation of another account, it will be visible in the application.

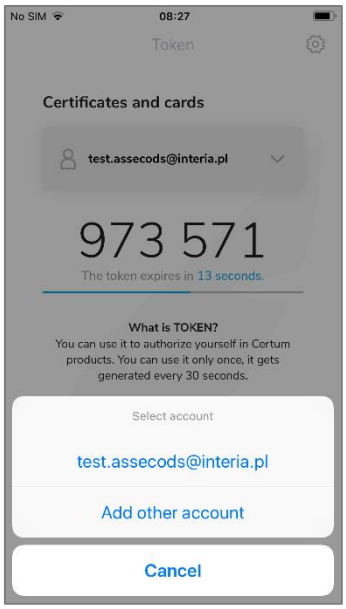


5.5.2. "Generate token code" mode

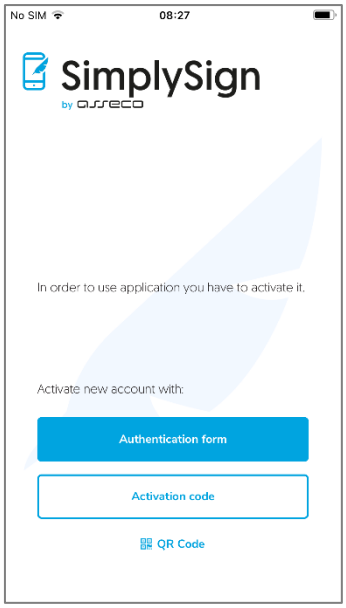
To add another account in the **Generate token code** mode, start the application.



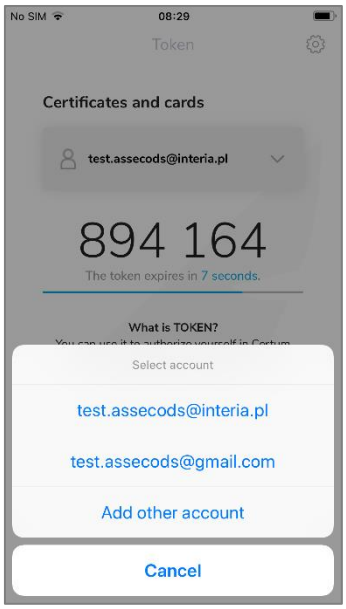
Press the area within the account name. A list of accounts with the option **+ Other account** will be expanded.



After pressing **+ Other account** 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.



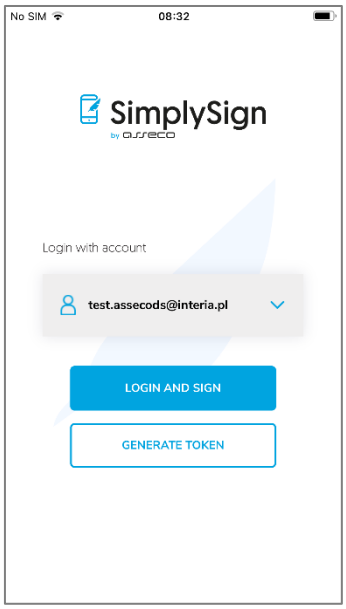
5.6. Logging into the application

5.6.1. "Sign documents" operating mode

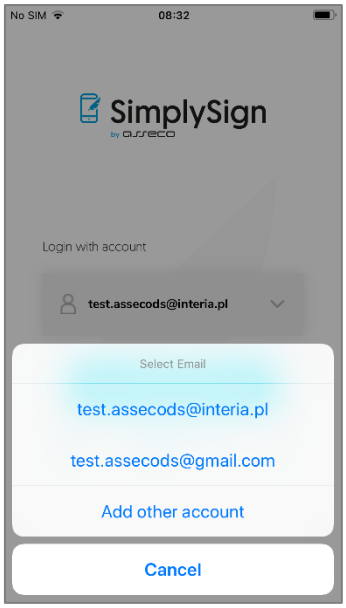
If the application is set to “Sign documents” operating mode, after activating the application, a log-in screen, where you have to enter OTP Token to the account to which you want to log in, will appear.

5.6.2. "All in one" operating moge

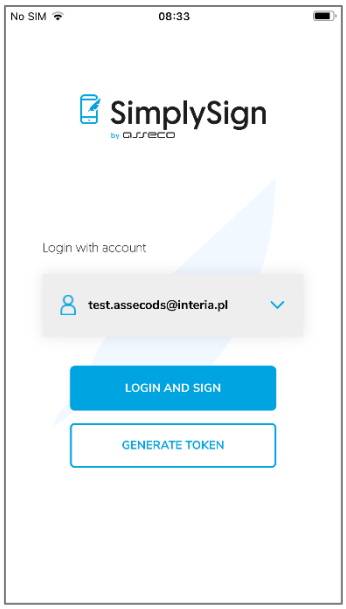
If the application was set to “All in one” operating mode, then after activating the application, a start screen of the application will appear.



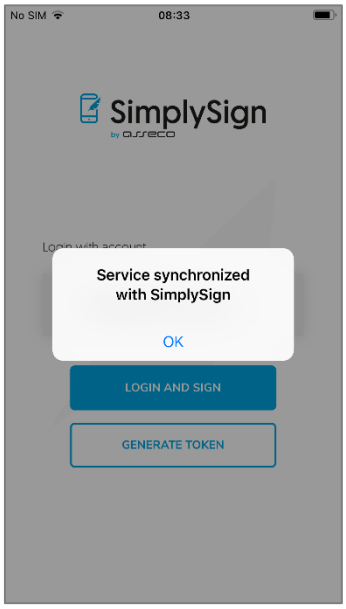
Since the application allows the use of several accounts, you must press the area within the user name. A list of accounts will appear.



Select the appropriate account from the list.

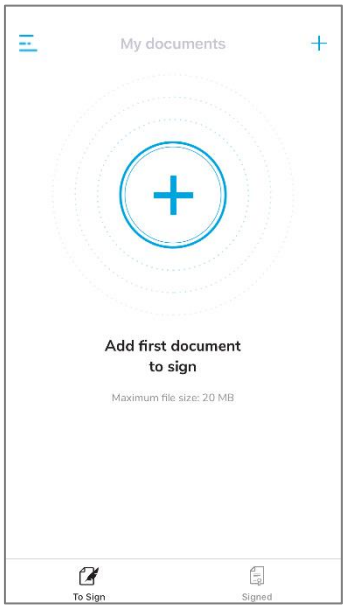


Then press the **Login and sign** button. The application will automatically generate the OTP Token and will make an attempt to log the user in to the service. If you experience problems during login resulting from an incorrect OTP Token, an automatic synchronization of the time in the **SimplySign** application will occur and a message concerning this fact will be displayed.



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

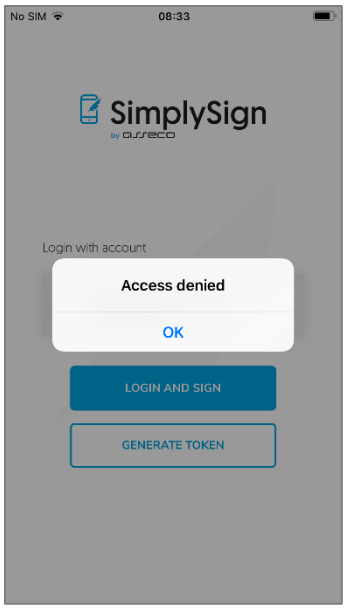
After automatic time synchronization, press the **Login and sign** button again. You will be logged into the **SimplySign** service.



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 appear.

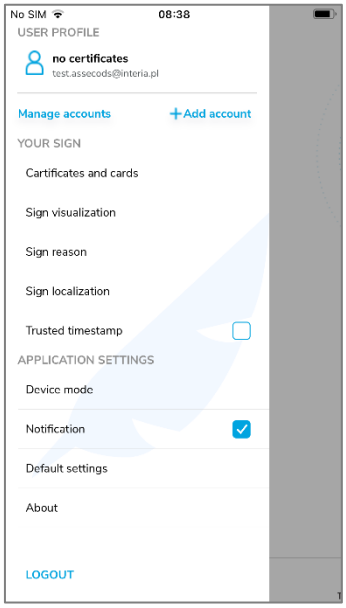
After pressing the Allow button you will be logged into the service and a screen where you can add files to be signed or go to application options will appear.

If the OTP token entered is incorrect or some other error preventing from logging in occurs, an Access denied message will appear on the bottom.



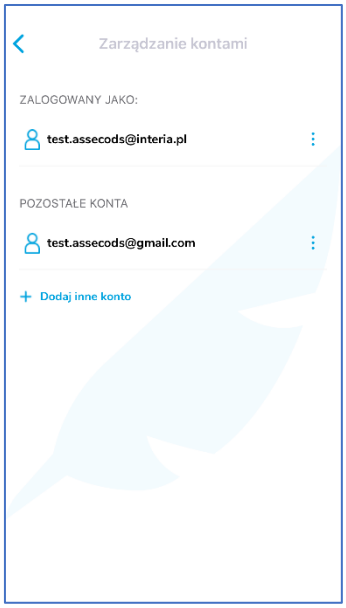
6. Application Settings/Options

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".



6.1. „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.

6.2. 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.

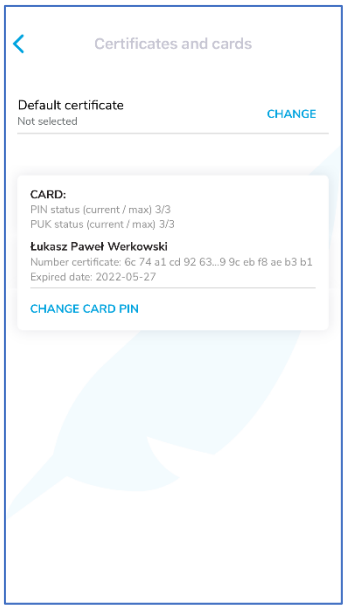
6.2.1. „Certificate and cards" option

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:

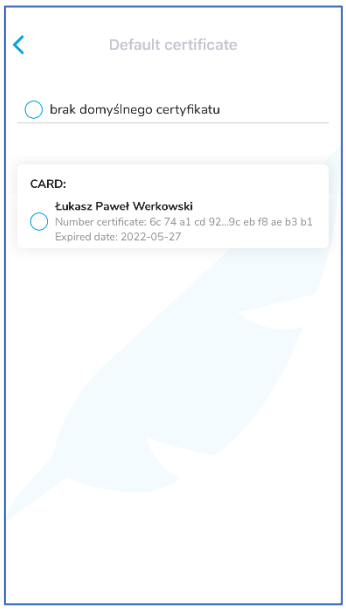
- Default certificate name
- The following information about the cards:

- 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

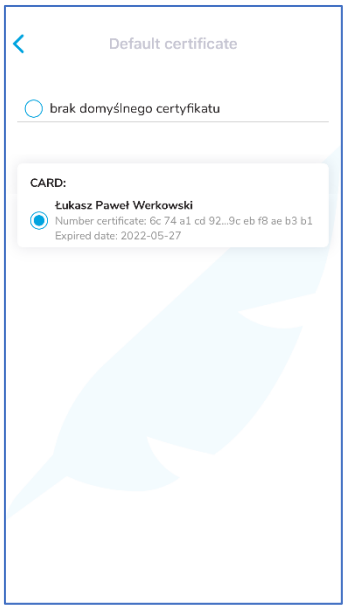


6.2.1.1. Setting the default certificate

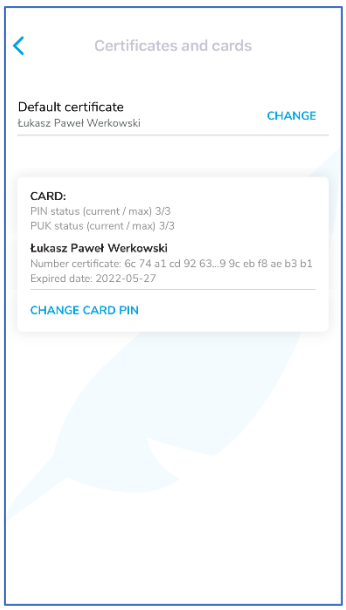
To set the default certificate, press the **Set** button. The available certificates will be displayed.



Then indicate the certificate to be set as default.

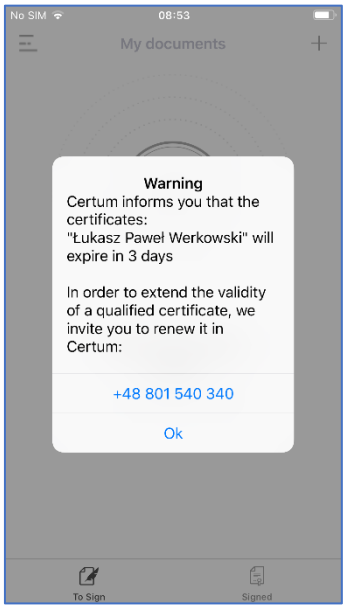


After selecting the default certificate, return to the settings – the selected default certificate will appear on the list.



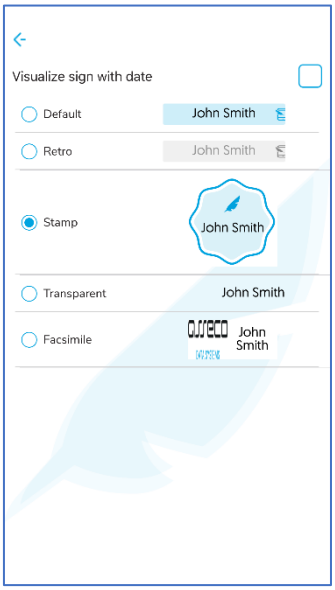
6.2.1.2. Warning of impending expiry of the certificate

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



6.2.2. „Visualize sign" option

This option allows you to set the pattern of the so-called facsimile that will be in the **signature visualization** and allows you to enable the option of adding the current date to the visualization (the option of **visualize signs with date**).



Six default patterns are available. It is possible to add your Facsimile – this is described in the next section.

6.2.2.1. Adding your own Facsimile

In the signature visualization, you can set your own facsimile image as a graphic sign.

To do so, log into the User's Panel located at the address below and add your own image file there in the Settings.

https://cloudsign.webnotarius.pl/ccm/welcome

During logging in, enter the **User ID** and the **token** generated on the device. After logging in, select **My Account → My Facsimiles** and use the **Add New Facsimile** button to add your own image file, which will be used as a facsimile.

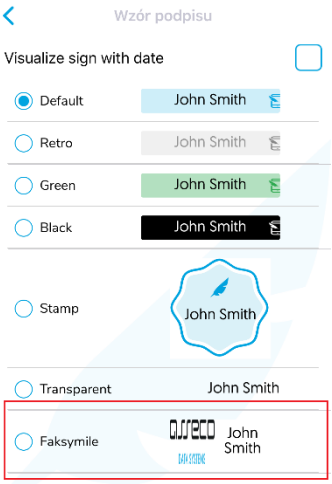
After adding the facsimile, log into the application on your mobile device, go to the settings and set the facsimile added in the Signature pattern section.

Below are the screenshots:

- the first and the second from the User Control Panel, where facsimile is added and set as default;
- the second from the mobile application, in which the added facsimile is set for use in visualization;


Certum
by asseco
Witaj, test.assecods@gmail.com
Wyloguj
Moje karty
Moje konto
Moje konto > Moje faksymile
Moje dane
Moje faksymile
Moje raporty
Moje preferencje
Zarządzanie faksymiliami
Moje faksymile
Odśwież
+
Certum
by asseco
asseco
DATA SYSTEMS
Dodaj nową faksymile
Menu faksymile
Ustaw jako domyślny
Usuń
Menu faksymile
asseco
DATA SYSTEMS


Certum
by asseco
Witaj, test.assecods@gmail.com
Wyloguj
Moje karty
Moje konto
Moje konto > Moje faksymile
Moje dane
Moje faksymile
Moje raporty
Moje preferencje
Zarządzanie faksymiliami
Moje faksymile
Odśwież
+
Certum
by asseco
asseco
DATA SYSTEMS
Dodaj nową faksymile
Menu faksymile
Ustaw jako domyślny
Usuń
Menu faksymile
asseco
DATA SYSTEMS

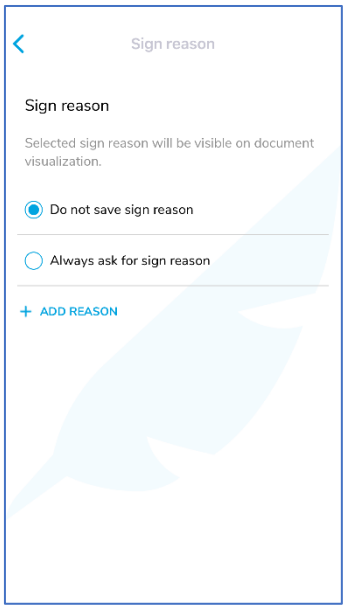


6.2.3. „Sign reason" option

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:

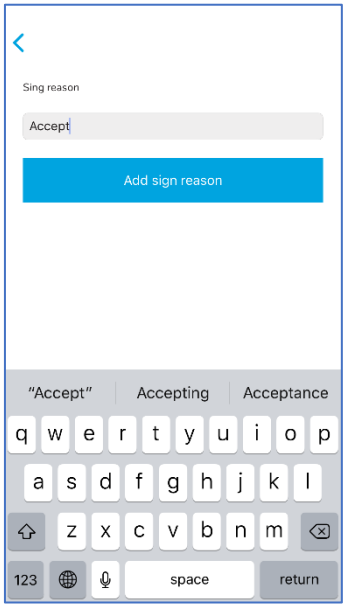
- Do not save sign reason - if you choose this option, a Signature reason will not be added to the signature structure.
- Always ask for a Sign reason - if you choose this option the application, every time before signing, will ask for a Signature reason which will be added to the signature structure.



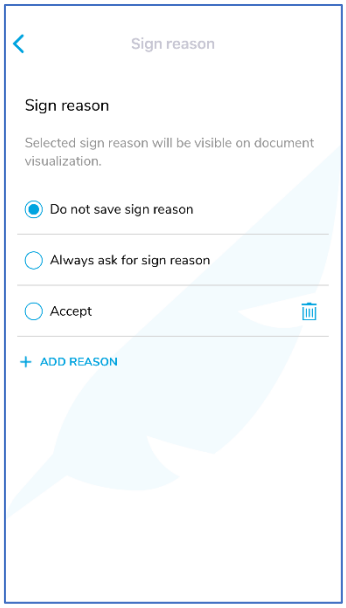
The application allows you to add your own signature to the list. This reason will be selectable in the future while signing a document if the option of adding a Signature reason is enabled.

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.

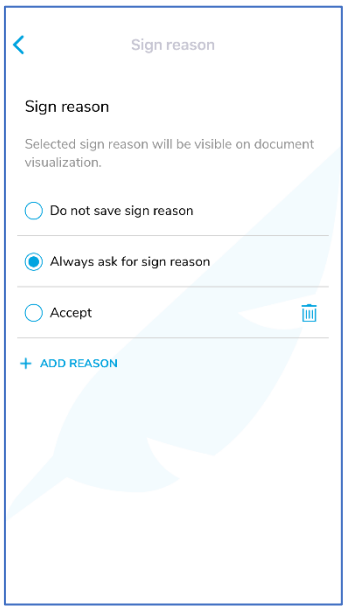
Enter your own Signature reason.



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.



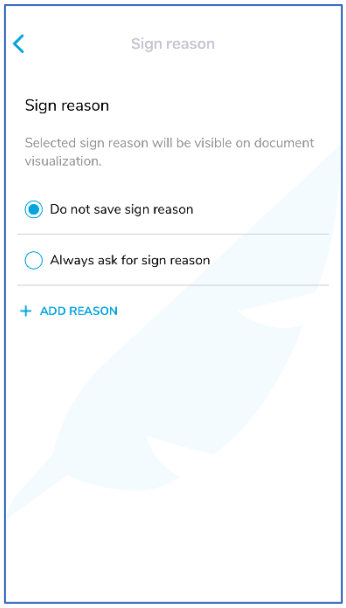
If you choose the added Sign reason this reason will be always, without asking, added to the signature structure.

The Sign reasons entered by the User can be deleted.

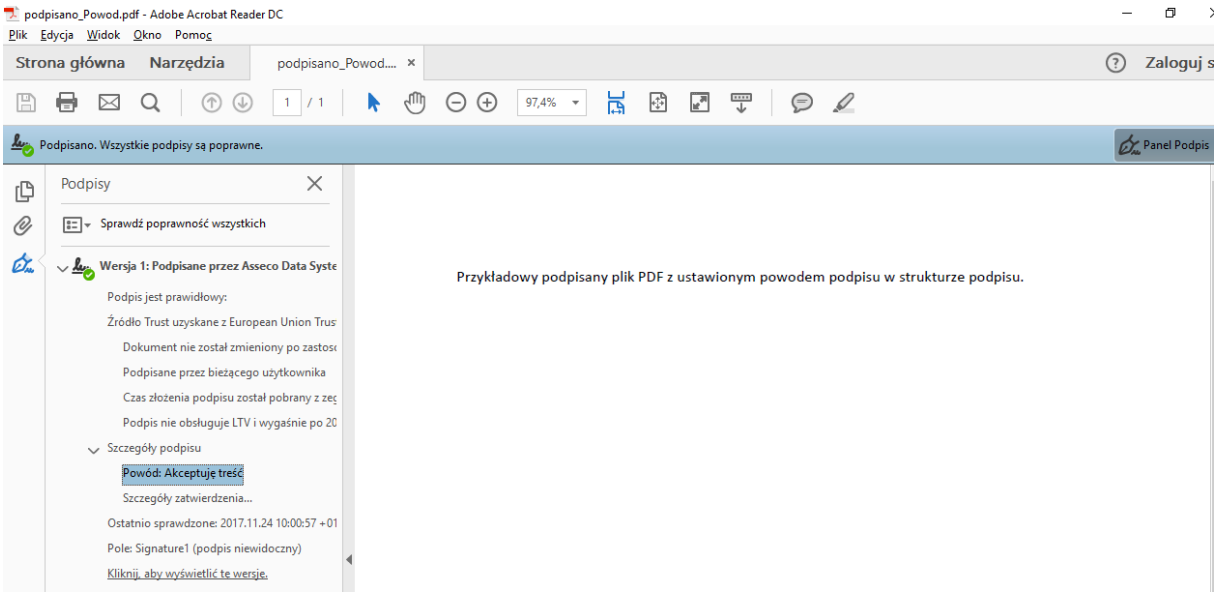
Then you have to press the cross icon located within the area of the Sign reason.

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.

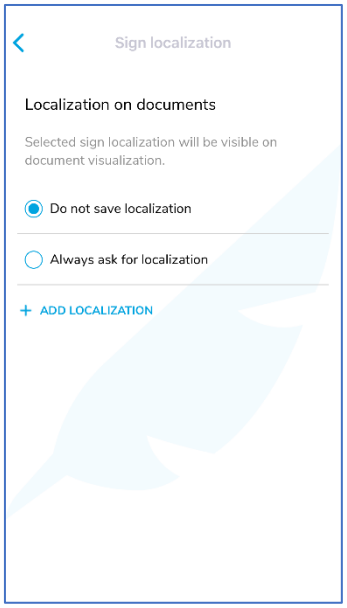


6.2.4. „Localization" option

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

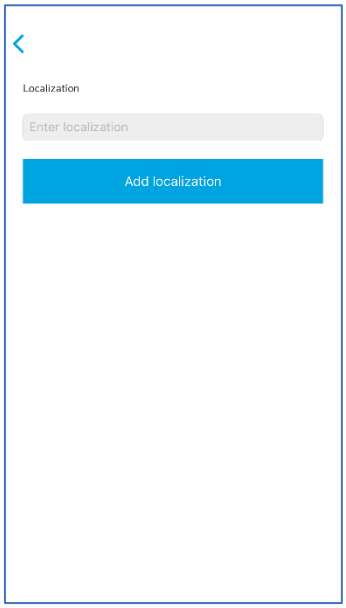
By default there are two options:

- 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.

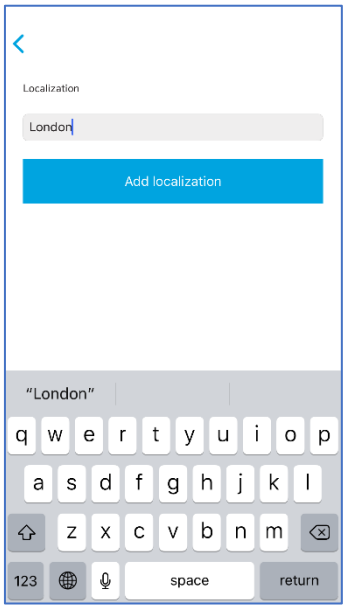


The application allows you to add your own localization to the list. This localization will be selectable in future while signing a document if the option of adding a localization is **enabled**.

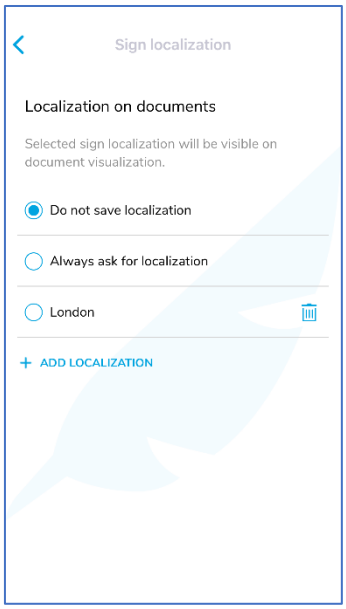
To add your own location to the list, press the **Add location** button. A screen where you can enter your own localization will be displayed.



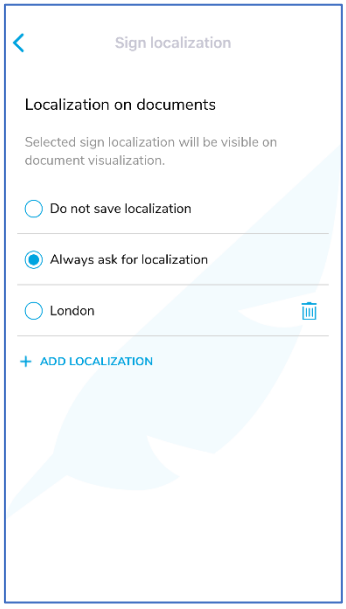
You have to enter your own localization.



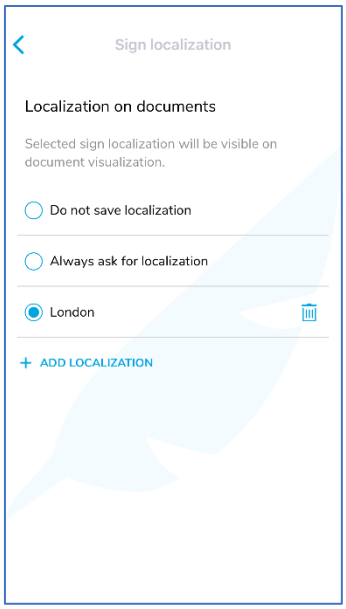
After entering your own localization, press the **Add location** button located on the virtual keyboard. The entered localization will be added to the list of reasons.



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.

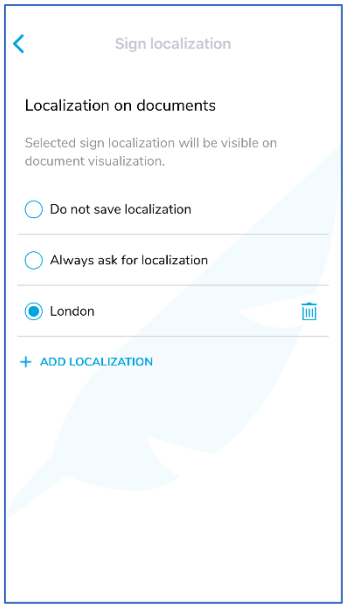


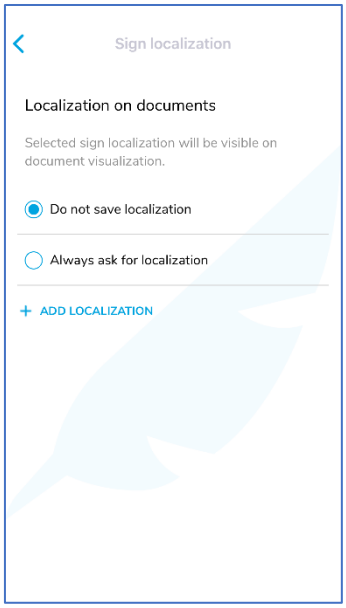
Localizations entered by the User can be deleted.

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

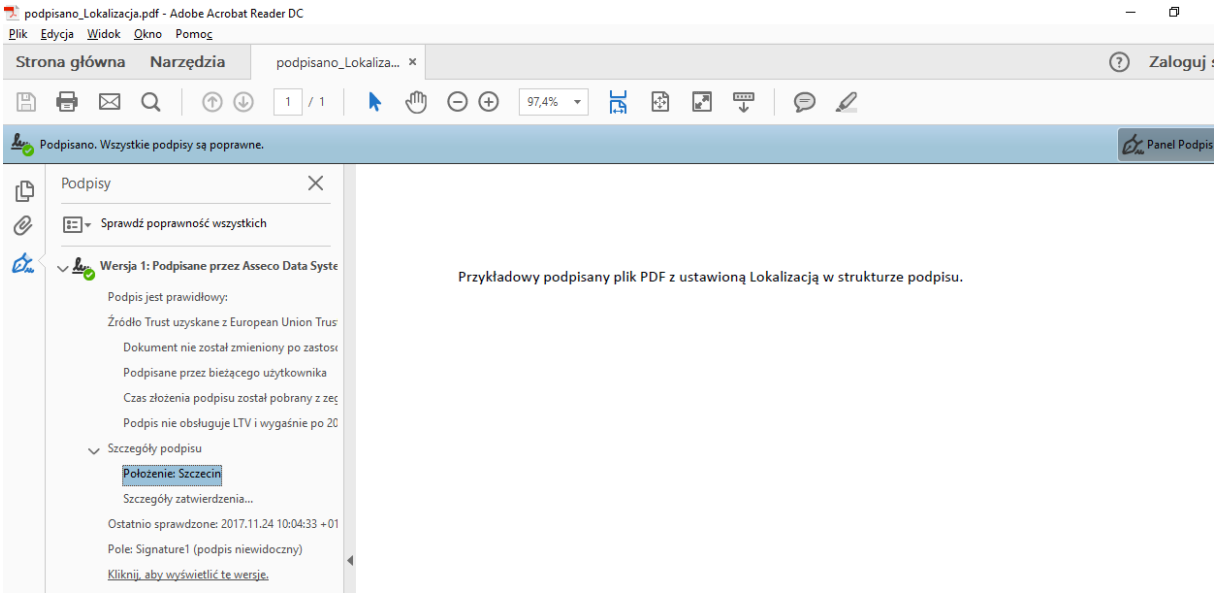
On the following two images a situation where the localization has been selected and later it has been deleted using the cross icon is presented.

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.



6.2.5. „Trusted time stamp” option

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

6.3. 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.

6.3.1. „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.

6.3.2. „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:

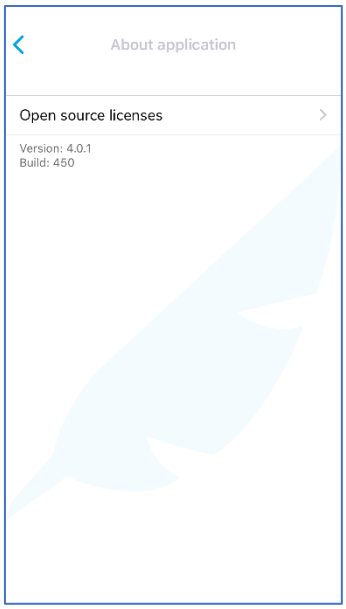
7. Resetting the access to the service
8. Changing the PUK code
9. Generating the event report in the CCM module by the User

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 appication" option

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

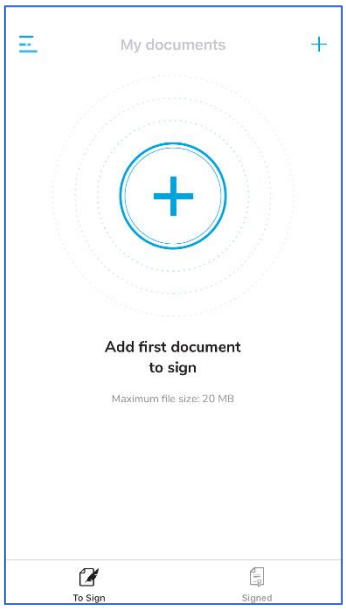


7. Signing files

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.

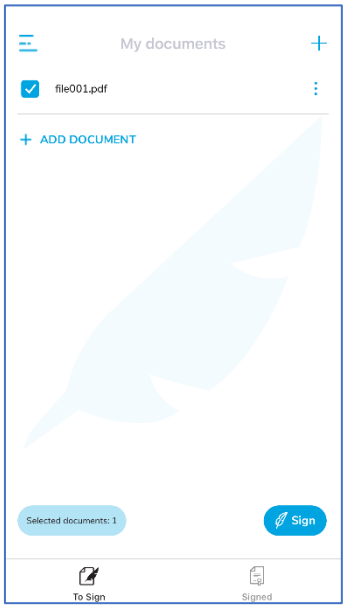
After logging in, the application goes to the **To sign** tab.



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.

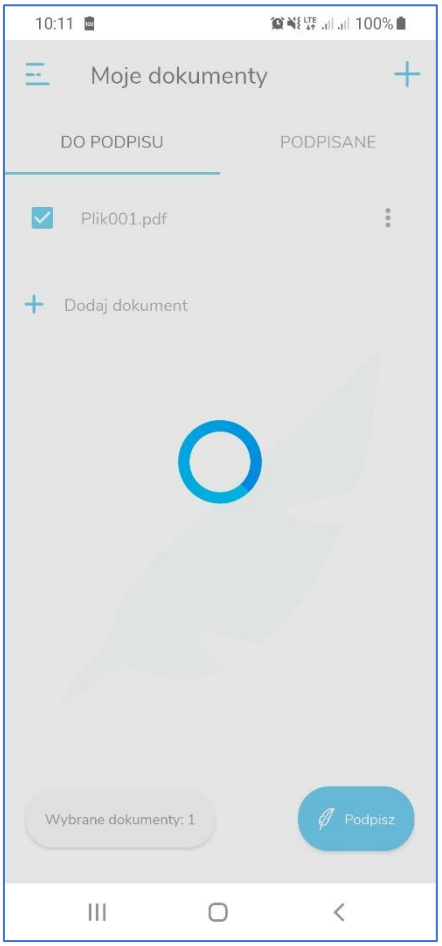
After choosing a file it is placed on the list of files in the **To sign** tab.



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.

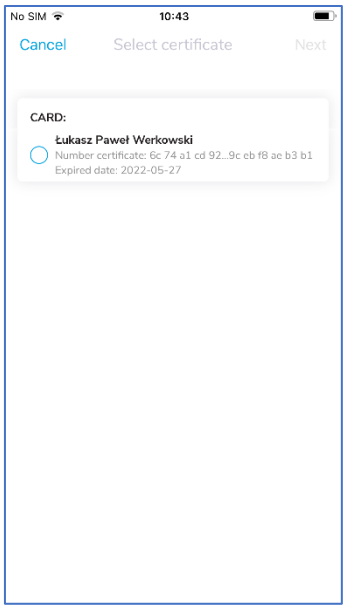
A process of downloading cards and certificates of the User will start - it is signaled by a circle icon symbolizing the passage of time.



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.

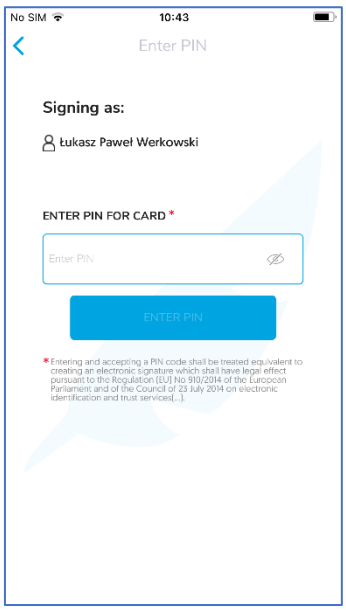
The situation in which the certificate (third in the order) issued for the Subscriber **Łukasz Paweł Werkowski** has been chosen is presented below.



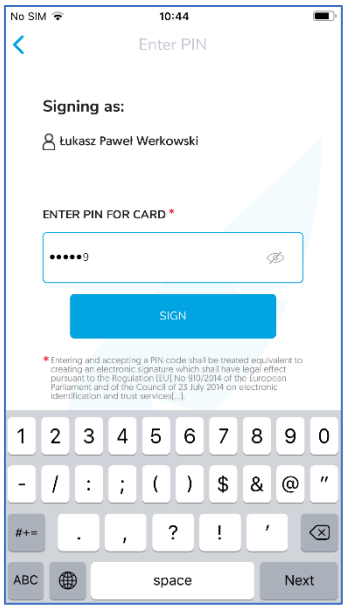
7.4. Entering the PIN code to the selected Signing certificate

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.

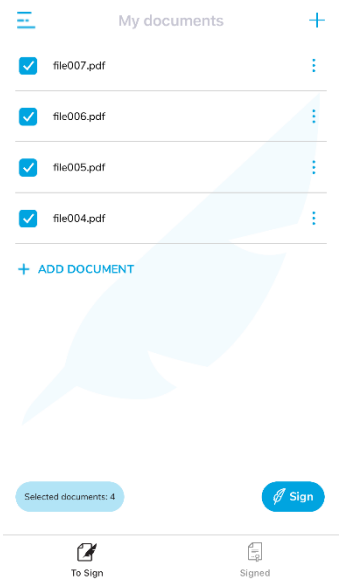
The following options are available on the summary screen:

- 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.

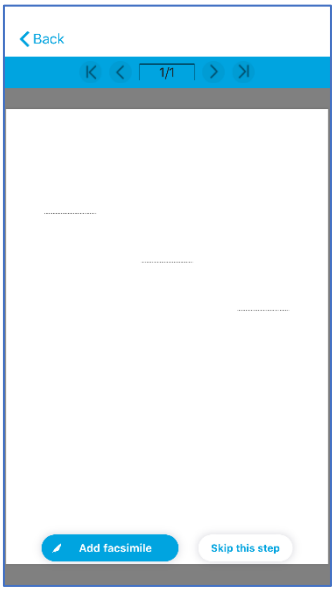
9. Making a signature with visualization

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

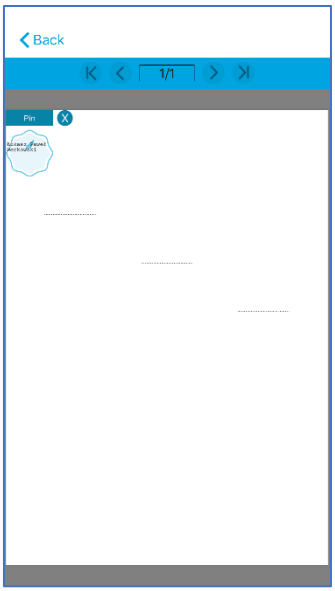
The visualization contains a graphic sign selected by the signatory in the options of the application (the option of **Visualize sign)**. Additionally, depending on the settings, it may also contain the current date and the Signature reason. Then, in the settings you should set the signature pattern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

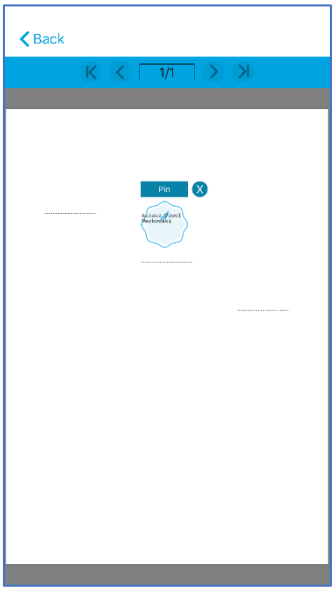
In order to make a signature with the visualization, click within the area of the document name on the list of files to be signed. A preview of the selected file where you can add the visualization will be activated.

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

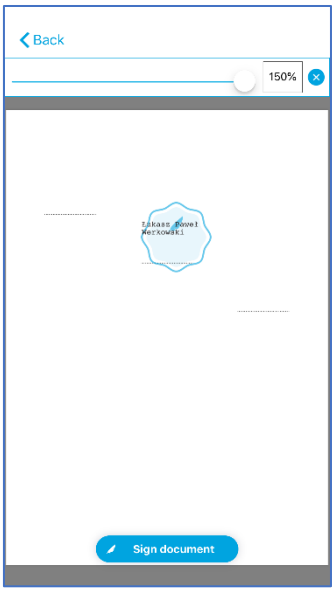


Then, press the **Add facsimile** button. The file preview will show a signature pattern that can be moved. The pattern should be moved to the desired place.



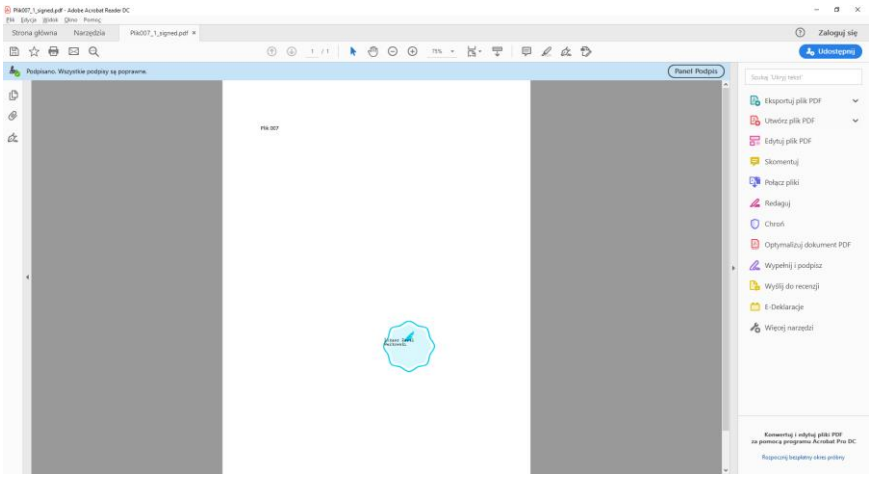


Then, press the **PIN** button. The visualization will be added to the file. Dodatkowo, na górze ekranu, pojawi się suwak pozwalający na skalowanie podpisu. Poniżej przedstawiono efekt przeskalowania wizualizacji podpisu do 150%.



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.

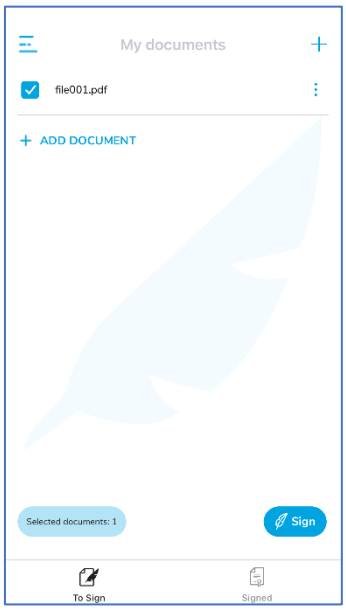


10. Changing the default certificate while Signing files

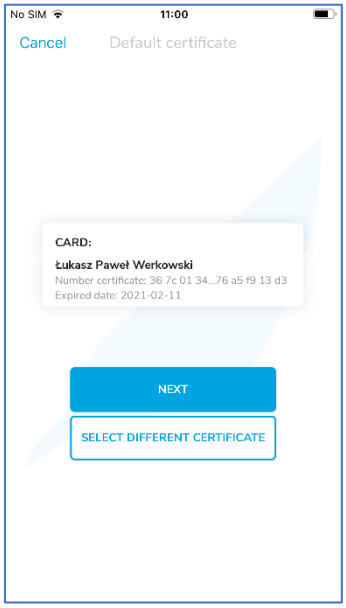
In case when a default certificate is set in the application Settings, when signing files it is suggested by default as a certificated which will be used for signing files. However, during the signing process you can temporarily change it to a different one and make a signature with that other certificate. 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.

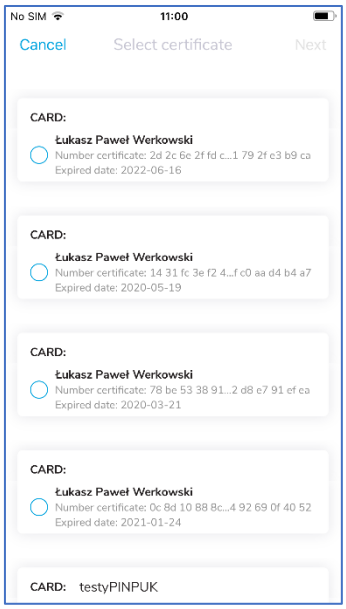
A process of signing during which a default signing certificate was temporarily changed to a different temporary one is presented below.

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

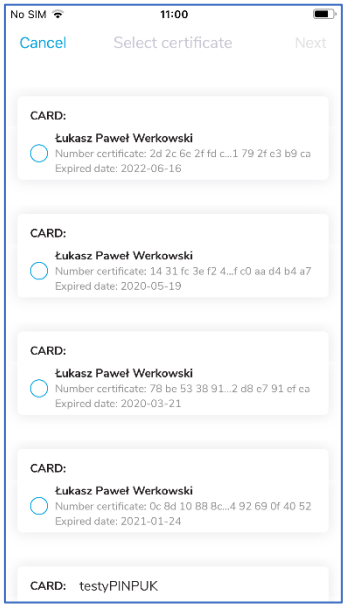


After selecting files which are to be signed and pressing the **Sign** button, the process of signing starts. A certificate set in the application Settings as a default will be indicated for signing.

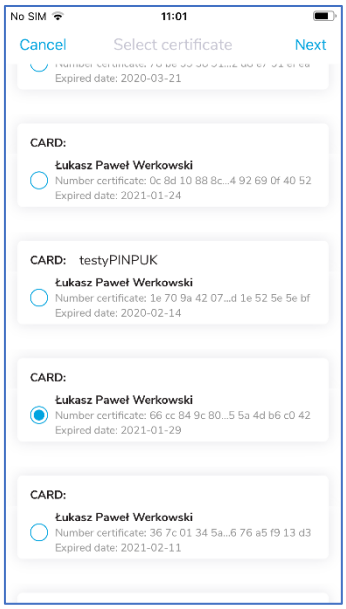




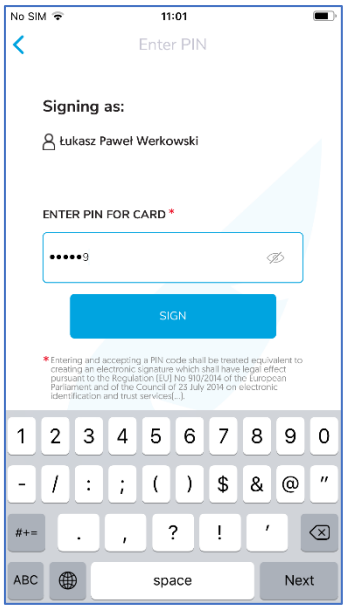
To temporarily change a signing certificate to a different one, press the **Choose different certificate** button. A list of cards and certificates will be displayed, where the certificate that is currently set as default is indicated (below in the picture a sample certificate with serial number 36 7c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



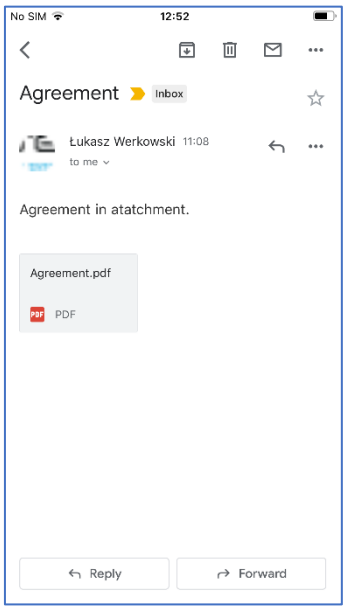
The signing process continues as described in the previous chapters. After the signature is made, the original default certificate is set.

11. Importing files from external applications

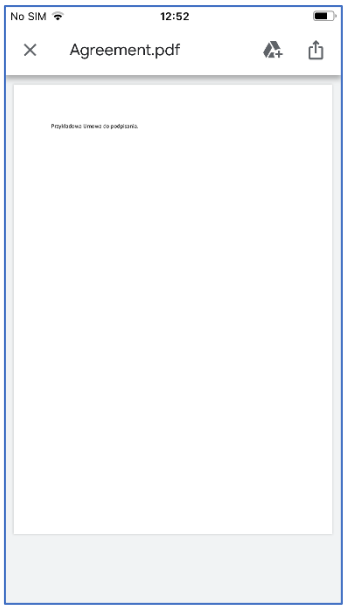
It is possible to import a PDF document from the external application directly to the list of files to be signed.

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

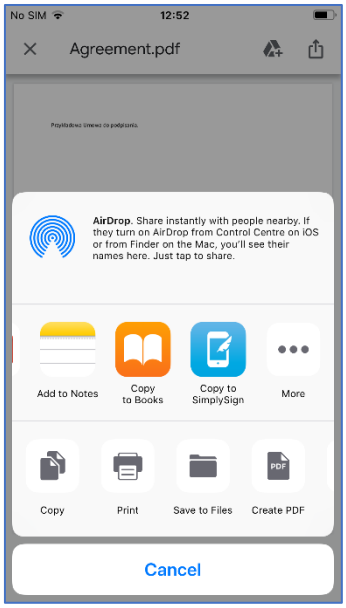
In order to import a PDF document, open a message containing that file.



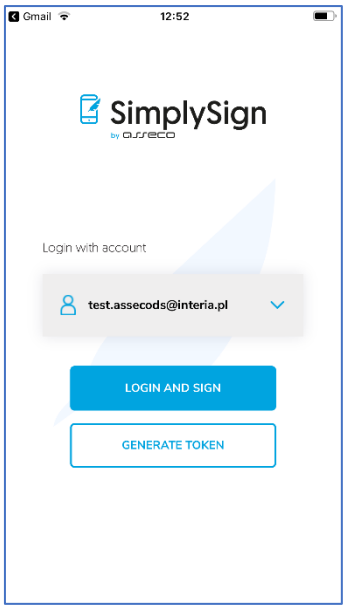
Then, display the contents of the file.



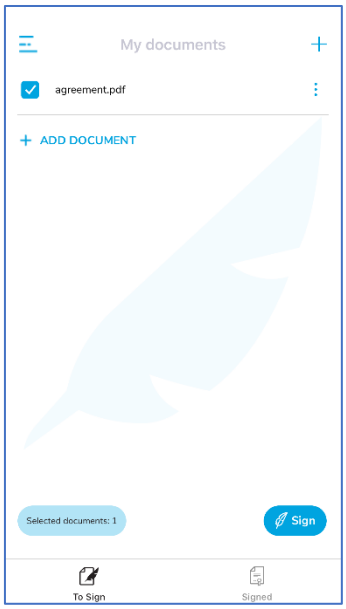
Then press the Share icon, located in the top right of the screen – the **SimplySign** application will appear in the list of options.



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**.

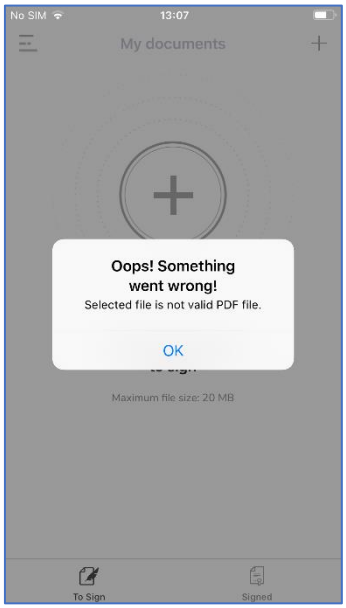


The next step is to sign a file in line with a description presented in previous sections.

12. Handling errors when Signing files

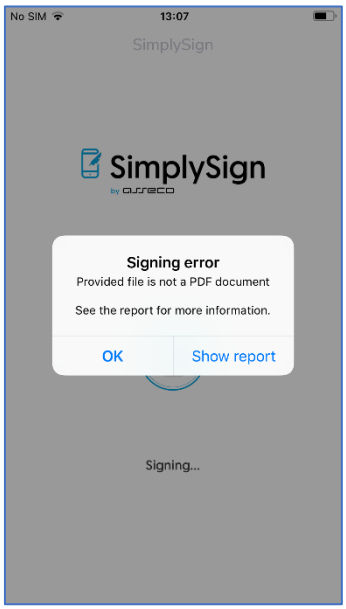
12.1. Incorrect PDF file

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.



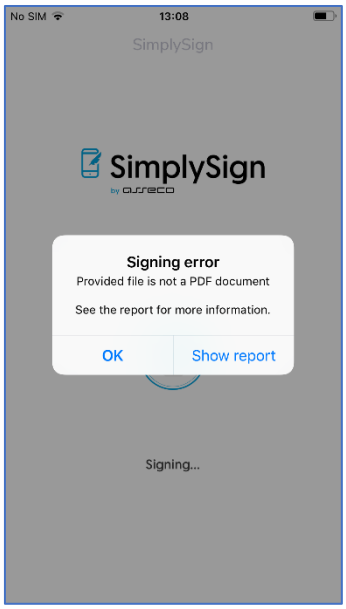
12.2. Secured PDF file

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

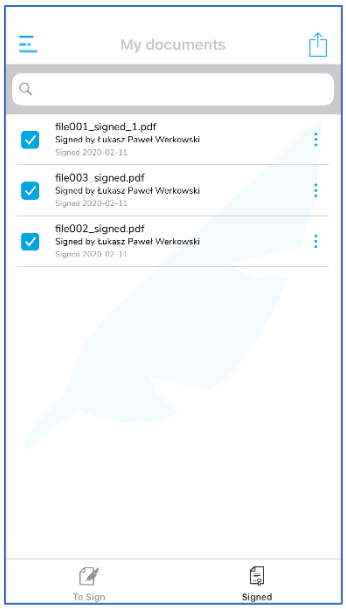
If the card is blocked (blocked PIN code), the following message will appear when you try to sign a file with a certificate from this card: **The document has not been signed. Blocked** PIN.

13. Handling the signed files

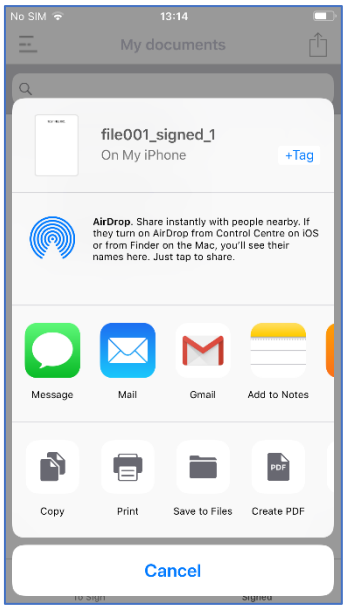
13.1. Sending of signed files by e-mail

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.

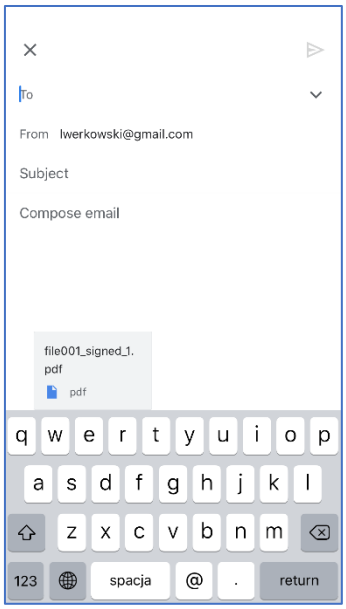


Then select the files to be sent and press the file sharing button. A screen allowing the selection of the e-mail program through which these files are to be sent will appear.



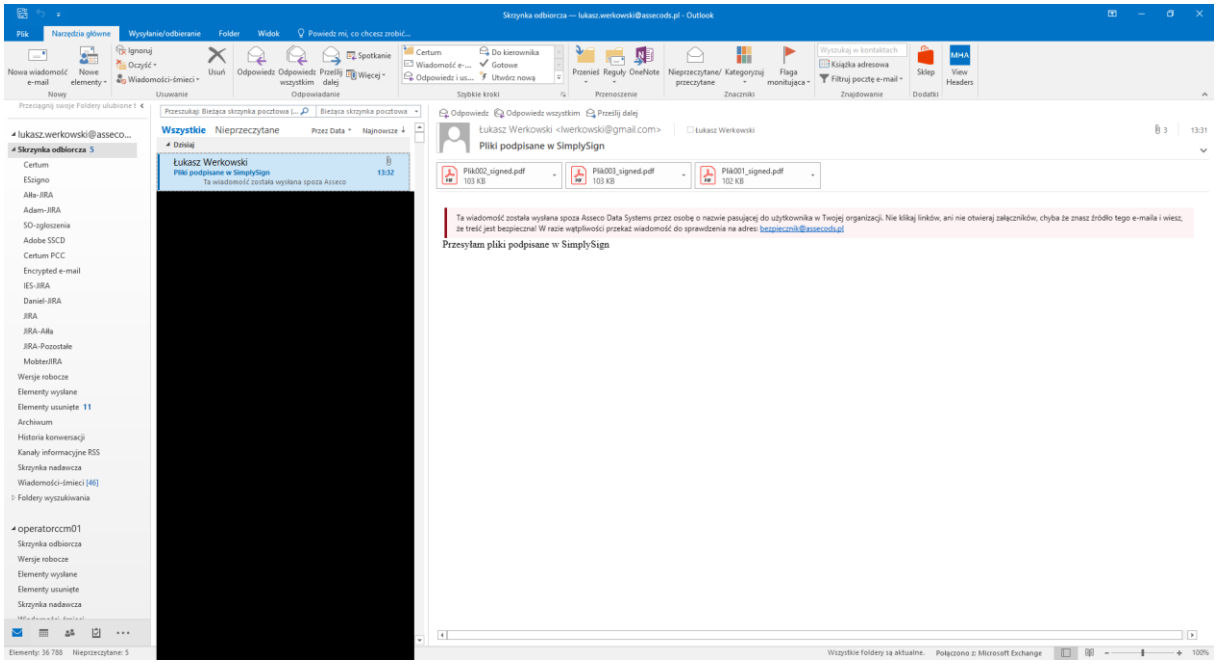
In the presented example the **Gmail** option was selected. A window allowing for preparation of an e-mail message was opened.

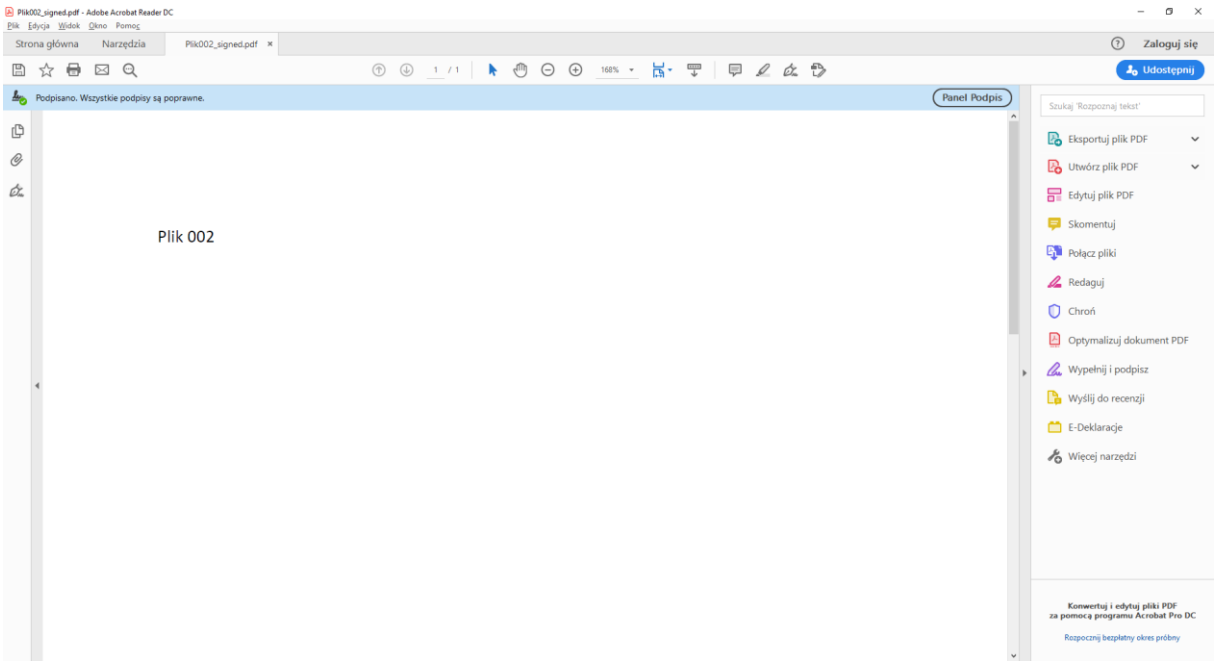
The selected files which have been previously signed are visible as the attachments. Later you have to enter a recipient's e-mail address, subject and content of the message.



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.

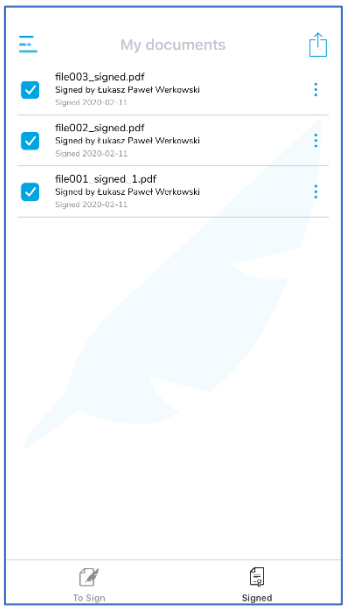




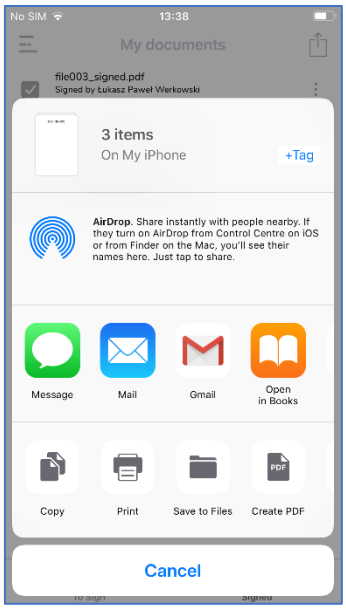
13.2. Save signed documents to iCloud Drive

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

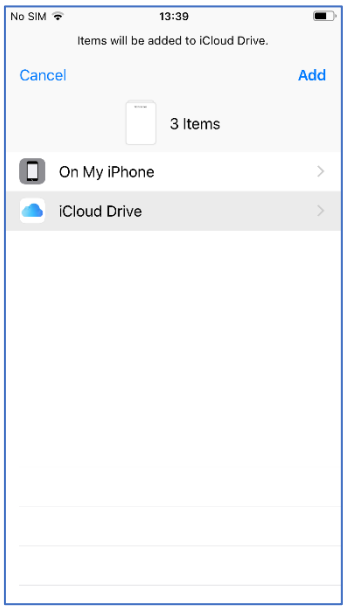
To do this, firstly you have to select files which are to be sent.



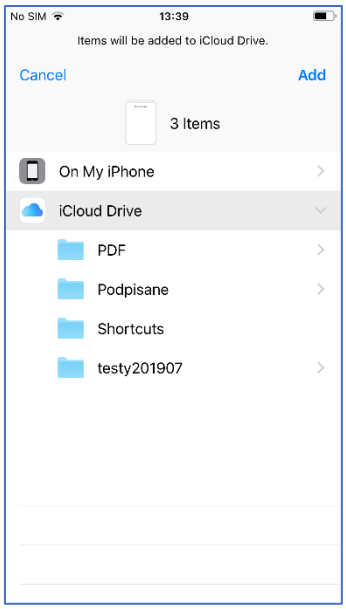
After selecting the files, press the file sharing icon. A screen allowing for indication of a destination of the sent files will be displayed.



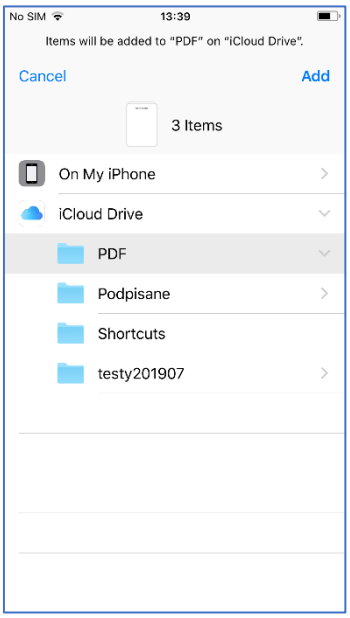
Then you have to choose the service to which you want to send the selected files.



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

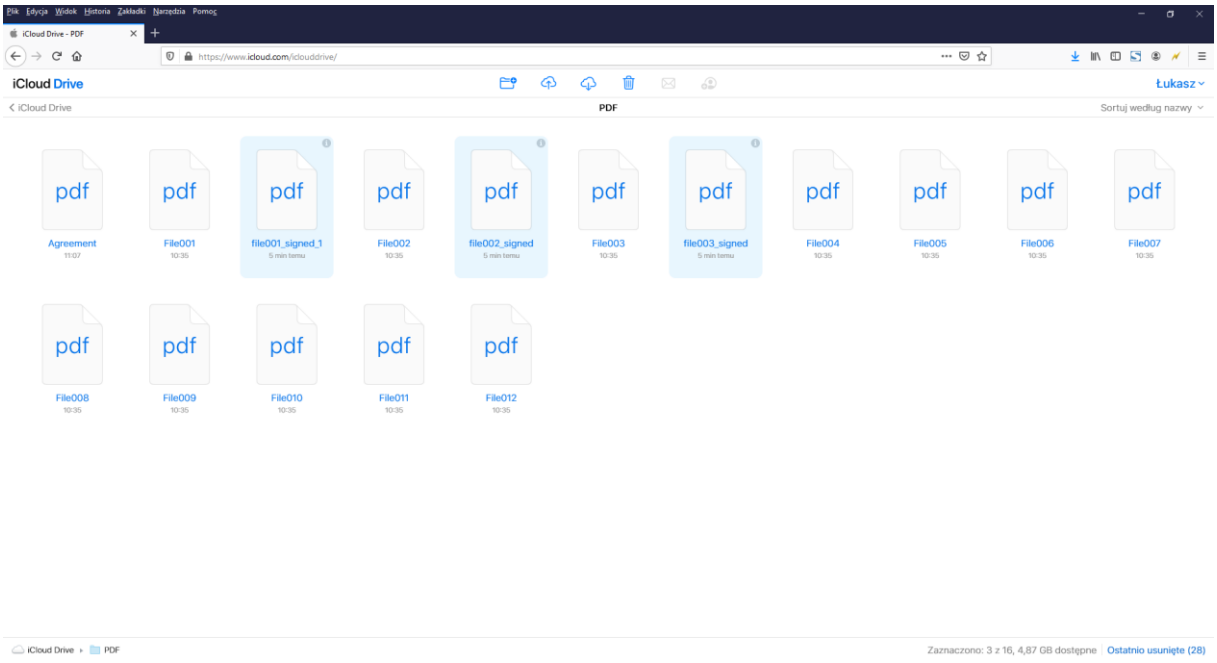


A situation in which a directory named **PDF** was selected as the target directory is presented below.



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

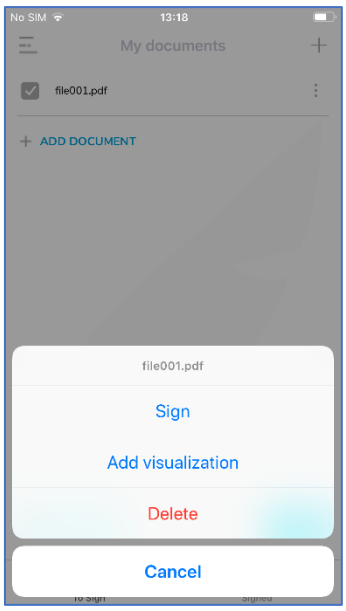
They will be visible for the drive owner after logging into their iCloud account.

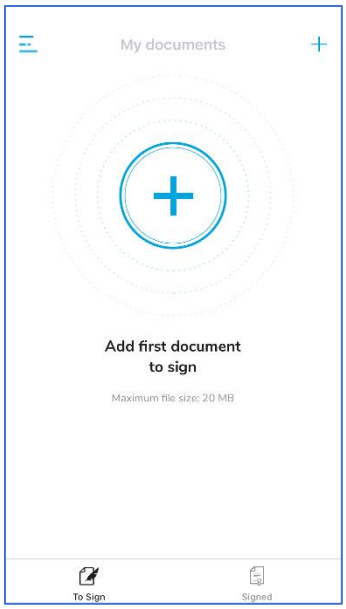


14. Deleting files

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.




My documents
Add first document
to sign
Maximum file size: 20 MB
To Sign
Signed