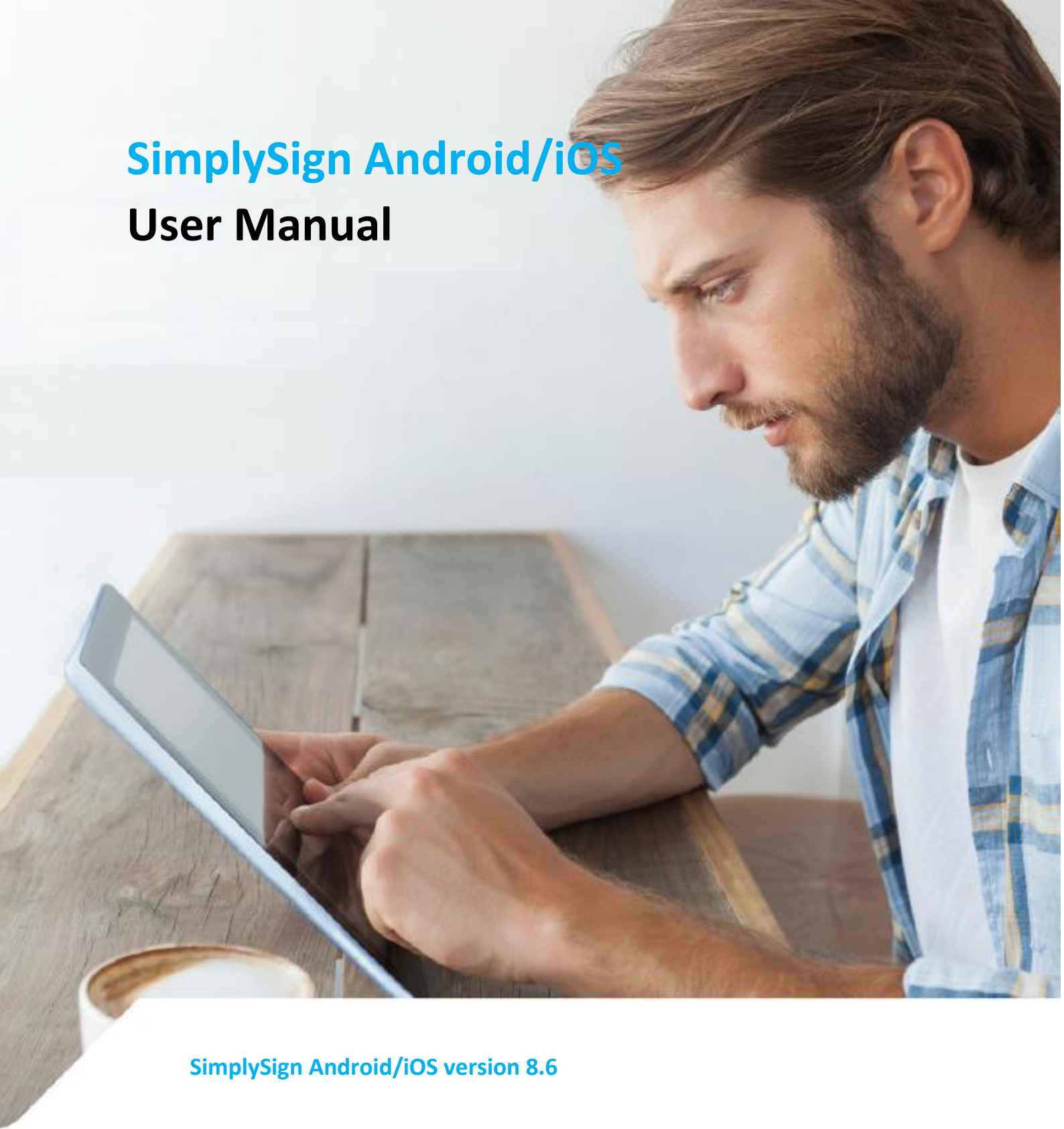


SimplySign Android/iOS

User Manual



SimplySign Android/iOS version 8.6

Table of Contents

1.	Legal Information	4
2.	Introduction	5
3.	Requirements.....	5
4.	Application Installation	6
4.1.	Application Installation on Android.....	6
4.2.	Updating the Application from Version 7.6 to 8.6 on Android	7
4.3.	Application Installation on iOS	7
4.4.	Updating the Application from Version 7.6 to 8.6 on iOS	7
5.	Biometric Security	8
6.	Starting and Activating the Application or Resetting Service Access	9
6.1.	Starting the Application	9
6.2.	Service Activation	9
6.2.1.	Activation Using Authentication (Personal) Data.....	9
6.3.	Resetting Service Access.....	17
6.3.1.	Manual Reset Using a 16-Character Activation Code	18
6.3.2.	Automatic Reset Using a QR Code	26
6.4.	Signing Without Activation	33
6.4.1.	Application Not Activated	33
6.4.2.	Application in “Signing and Generating One-Time Codes” Mode.....	37
6.5.	Application Operating Modes.....	41
6.5.1.	Operating in “Generate One-Time Codes Only” Mode.....	41
6.5.1.1.	Forcing Time Synchronization	42
6.5.2.	Operating in “Signing and Generating One-Time Codes” Mode.....	43
6.6.	Multiple Account Support	44
6.6.1.	“Signing and Generating One-Time Codes” Mode.....	44
6.6.2.	“Generate Codes Only” Mode.....	48
6.7.	Signing In to the Application.....	52
6.7.1.	“Signing and Generating One-Time Codes” Operating Mode.....	52
7.	Account Settings/Application Options.....	58
7.1.	Account and Settings	58
7.1.1.	Account Management.....	59
7.1.2.	“Certificates and Cards” Option	60
7.1.2.1.	Setting the Default Certificate.....	61
7.1.2.2.	Warning of an Approaching Certificate Expiration Date	62
7.1.3.	“Signature Settings” Option	63

7.1.4.	Visualization Options.....	65
7.1.4.1.	Font Property Options Used in the Visualization	65
7.1.4.2.	Setting a Signature with a Custom Image/Facsimile and Managing Images/Facsimiles 66	
7.1.4.3.	“Additional Text” Option.....	73
7.1.4.4.	“Reason for Signing” Option	79
7.1.4.5.	“Location” Option.....	84
7.1.4.6.	“Trusted Timestamp” Option	90
7.1.4.7.	Generating a Summary Account Usage Report for a Selected Month.....	91
7.1.4.8.	Using Default Templates and Adding the Date to the Visualization	94
7.1.5.	“Application Settings” Option	99
7.1.5.1.	Notifications	99
7.1.5.2.	Factory Settings	100
8.	Signing Files.....	102
8.1.	Adding a File to the List of Files to Be Signed	102
8.2.	Starting the File-Signing Process.....	105
8.3.	Selecting a Signing Certificate.....	106
8.4.	Entering the PIN for the Selected Signing Certificate.....	110
8.5.	Signing a File	111
9.	Signing Multiple Files at Once	113
10.	Creating a Signature with a Visualization	115
11.	Importing Files from External Applications	117
12.	Handling Errors While Signing Files	119
12.1.	Invalid PDF File.....	119
12.2.	Protected PDF File	120
12.3.	Invalid PIN for the Signing Certificate.....	121
12.4.	Blocked Card	122
13.	Managing Signed Files	122
13.1.	Sending Signed Files by Email	122
13.2.	Saving Signed Documents to Google Drive	124
14.	Deleting Files	128
15.	Integration with the e-Delivery System.....	129
15.1.	Activating an e-Delivery Mailbox	129
15.1.1.	Activating an e-Delivery Mailbox When SimplySign Is Active	129
15.2.	Signing In to an e-Delivery Mailbox.....	138

1. Legal Information

The economic copyrights to this documentation and the software it describes belong to Asseco Data Systems S.A., with its registered office in Gdańsk at ul. Jana z Kolna 11. These rights are protected by the Polish Act on Copyright and Related Rights (Journal of Laws No. 24, item 83 of 4 February 1994, as amended).

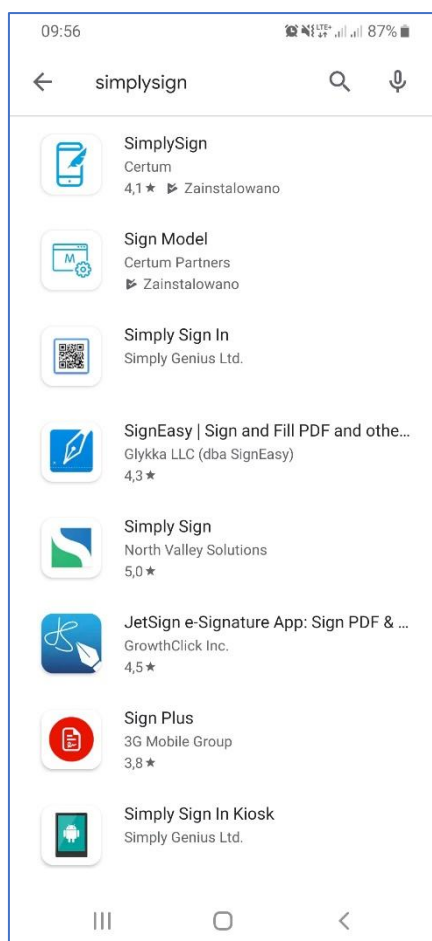
This documentation is distributed under the granted license.

2. Introduction

The SimplySign application for Android/iOS enables users to sign PDF documents using a virtual card containing a qualified or standard certificate. The application supports electronic signatures in the PAdES format (PDF Advanced Electronic Signature, ETSI TS 102 778) and uses the CAdES or PKCS#7 standards to describe data structures containing a signature.

In addition, SimplySign integrates with the e-Delivery system, enables users to view their mailbox, and generates tokens for signing in to e-Delivery.

This manual is generally applicable to both Android and iOS. Most illustrations are based on Android; however, differences in iOS, such as the file-sharing screen, are also illustrated where applicable.



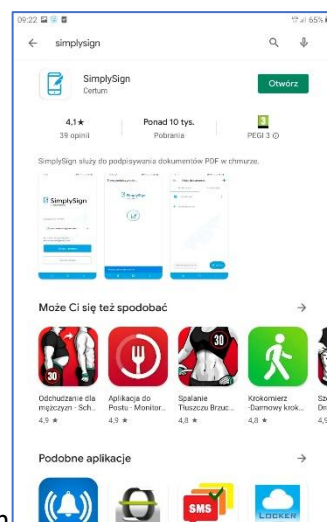
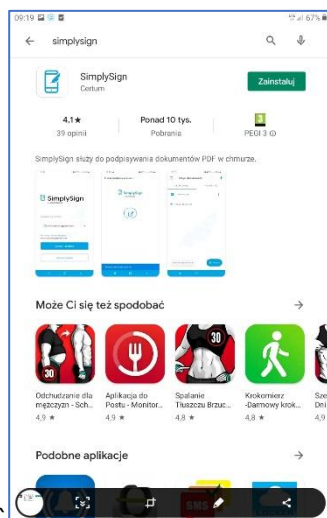
3. Requirements

SimplySign requires Android 13+ or iOS 18+, at least one registered and initialized virtual card, an active SimplySign service account, qualified or standard certificate(s), or an e-Delivery mailbox.

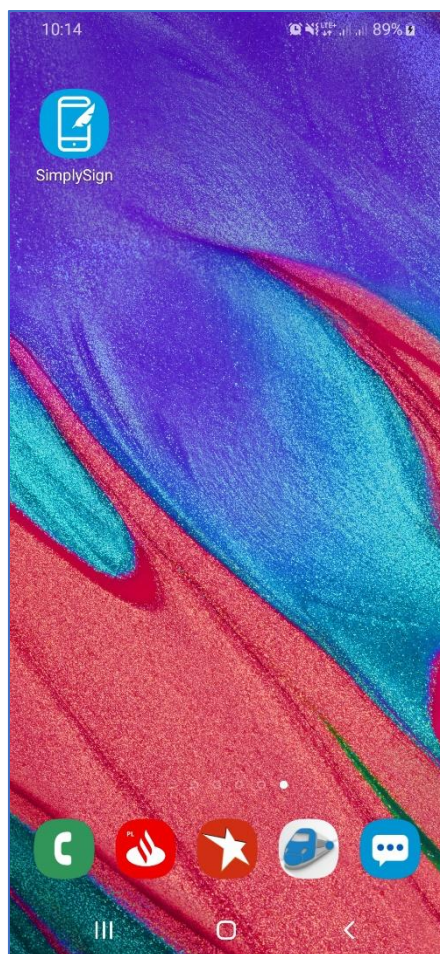
4. Application Installation

4.1. Application Installation on Android

To install the application on an Android device, open the Google Play Store, search for SimplySign, and install it.



After successful installation, the SimplySign icon appears on the device home screen.



4.2. Updating the Application from Version 7.6 to 8.6 on Android

During the update from version 7.6 to 8.6, only the following items are transferred:

- The account list and the data required to sign in or generate a one-time code
- The activated application mode

Other settings, especially signature settings, are not transferred and must be configured again.

4.3. Application Installation on iOS

4.4. Updating the Application from Version 7.6 to 8.6 on iOS

During the update from version 7.6 to 8.6, only the following items are transferred:

- The account list and the data required to sign in or generate a one-time code

- The activated application mode

Other settings, especially signature settings, are not transferred and must be configured again.

5. Biometric Security

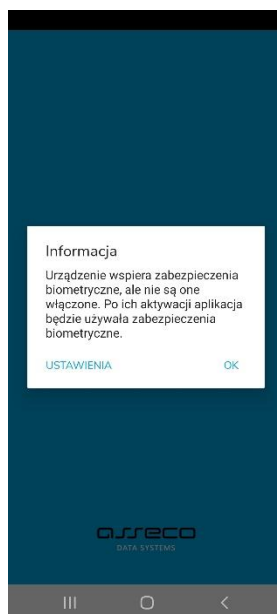
The application supports the biometric security configured on the device. If fingerprint or facial recognition is configured in the device operating system, authentication using the selected security method is required when the application starts.

WARNING!!!

Facial biometric authentication (Face ID) on Android is officially supported from Android 10 (internally named Quince Tart). Any earlier use of biometrics is based on proprietary solutions from device manufacturers. Therefore, the SimplySign developer is not responsible for errors or inconvenience resulting from the use of biometric data on older operating systems or from manufacturer-specific implementations.

Biometric security operates as follows:

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

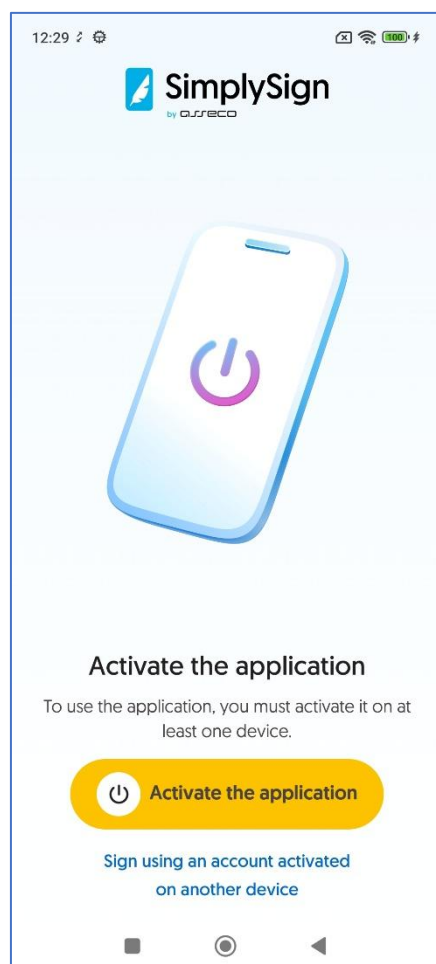


- B. If biometric security is enabled on the device, authentication using the selected biometric method appears when the application starts.

6. Starting and Activating the Application or Resetting Service Access

6.1. Starting the Application

Start SimplySign by tapping its icon on the home screen. The start screen appears when the application opens.



6.2. Service Activation

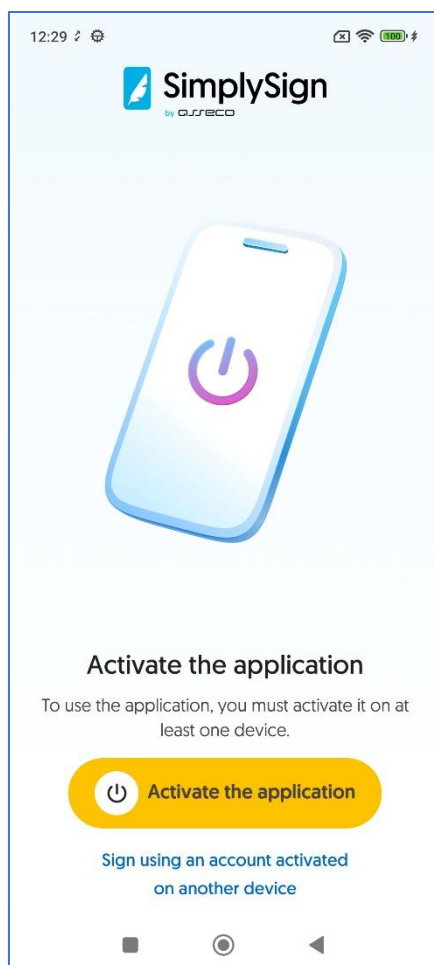
6.2.1. Activation Using Authentication (Personal) Data

Holders of a qualified certificate issued by CERTUM on a SimplySign medium, or holders of an e-Delivery mailbox, can use convenient unattended activation based on their personal data. This is activation using authentication data: information known to the user, consisting of personal data and identity-document details. The SimplySign activation process is described below.

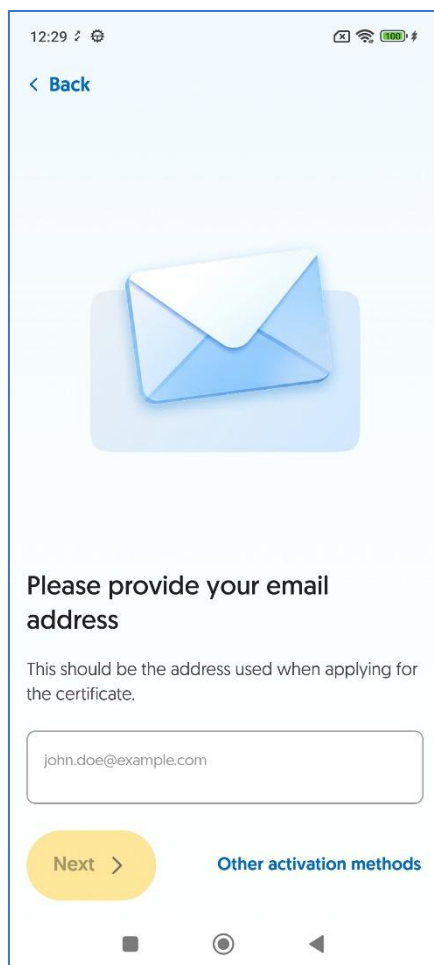
!!!WARNING

For activation using authentication data, the user must have at least one qualified certificate issued by CERTUM on a virtual card in the SimplySign service, or an e-Delivery mailbox. The certificate may be revoked or expired.

To activate the service using authentication data, start SimplySign.

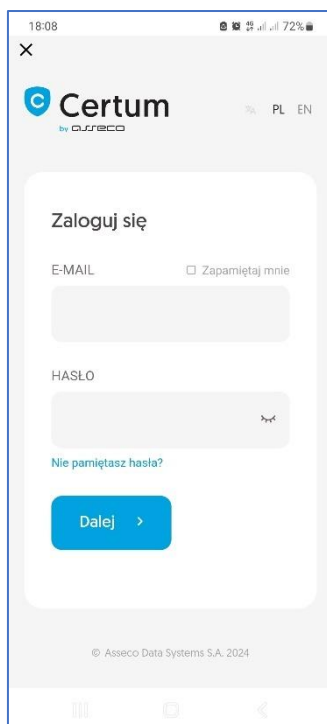


Begin activation by selecting Activate Application. A screen appears where you can enter the email address used as the user identifier.

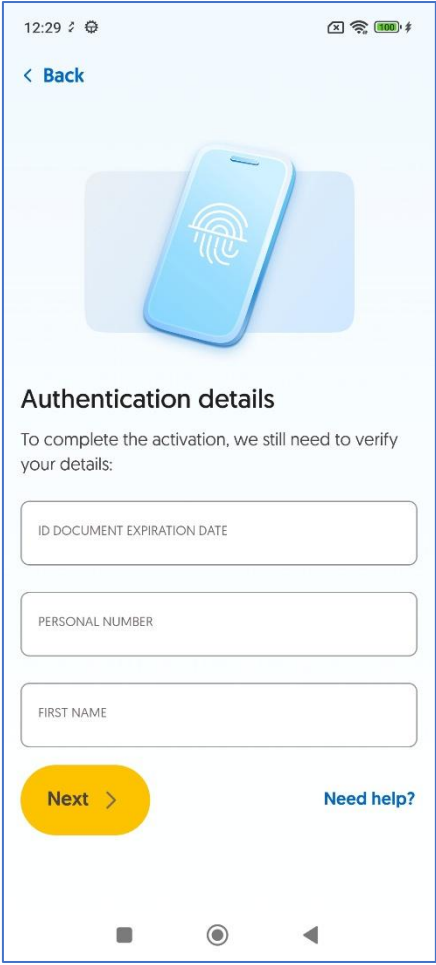
A screenshot of a mobile application interface. At the top, the status bar shows the time 12:29, signal strength, Wi-Fi, and battery level. Below the status bar is a blue header with a back arrow and the text "< Back". The main area has a light blue background with a large, stylized blue envelope icon. Below the icon, the text "Please provide your email address" is displayed in bold. Underneath, a smaller line of text reads: "This should be the address used when applying for the certificate." A text input field contains the placeholder email "john.doe@example.com". At the bottom of the form area, there is a yellow button with the text "Next >" and a blue link labeled "Other activation methods". The very bottom of the screen shows three standard Android navigation icons: a square, a circle, and a triangle.

In the E-mail field, enter the email address used as the user identifier.

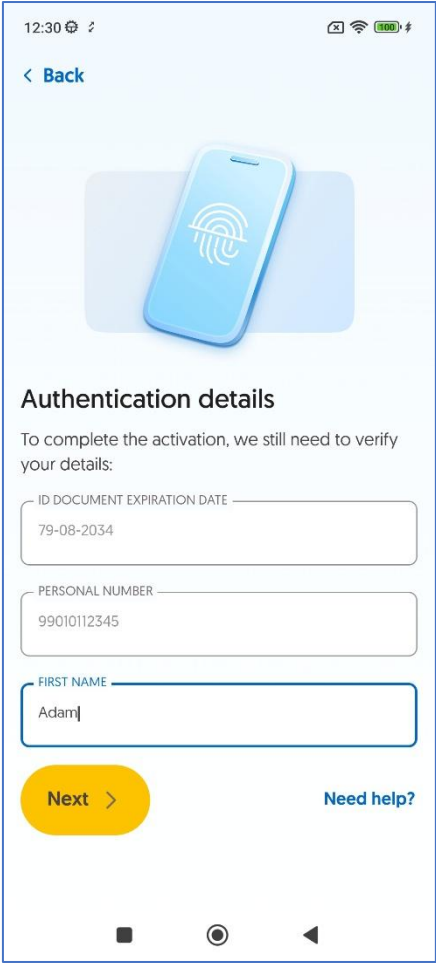
Select Next. If the identifier is correct, during first-time activation the application opens the Panel Certum sign-in screen to synchronize SimplySign with e-Delivery.



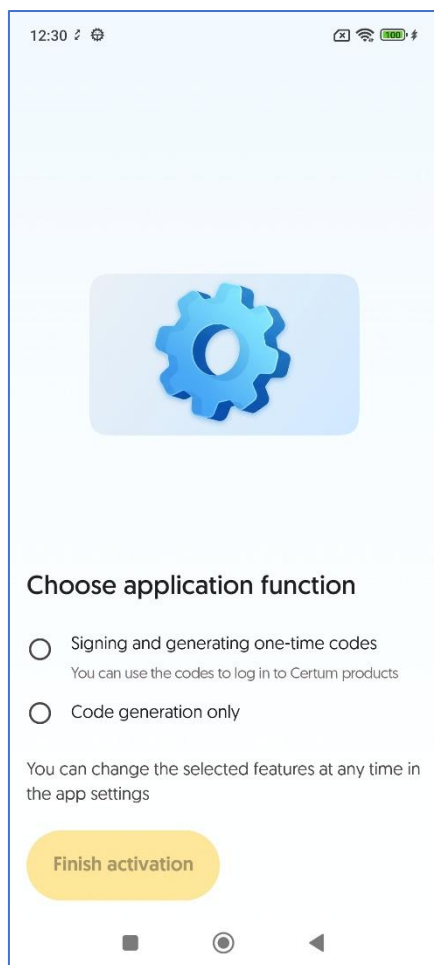
On the sign-in screen, enter the correct Panel Certum login and password, then select Next. The application then asks for three randomly selected items of the user's personal data.

A mobile application screen for authentication. At the top, the status bar shows the time 12:29, signal strength, Wi-Fi, and battery level. Below the status bar is a blue header with a back arrow and the text '< Back'. The main content area has a light blue background. In the center, there is a blue smartphone icon with a white fingerprint icon on its screen. Below the icon, the title 'Authentication details' is displayed in bold. Underneath the title, a message states: 'To complete the activation, we still need to verify your details:'. There are three input fields stacked vertically: 'ID DOCUMENT EXPIRATION DATE', 'PERSONAL NUMBER', and 'FIRST NAME'. At the bottom of the form, there is a yellow rounded button with the text 'Next >' and a blue link labeled 'Need help?'. The bottom of the screen shows the standard Android navigation bar with three icons: a square, a circle, and a triangle.

Enter the correct personal data.

A screenshot of a mobile application's activation screen. At the top, the status bar shows the time 12:30, signal strength, Wi-Fi, and battery level. Below the status bar is a blue header with a back arrow and the text '< Back'. The main content area has a light blue background. In the center, there is a blue smartphone icon with a white fingerprint icon on its screen. Below the icon, the title 'Authentication details' is displayed in bold. Underneath the title, a message states: 'To complete the activation, we still need to verify your details:'. There are three input fields: 'ID DOCUMENT EXPIRATION DATE' with the value '79-08-2034', 'PERSONAL NUMBER' with the value '99010112345', and 'FIRST NAME' with the value 'Adam'. At the bottom, there is a yellow 'Next >' button and a blue 'Need help?' link. The bottom of the screen shows the Android navigation bar with back, home, and recent apps icons.

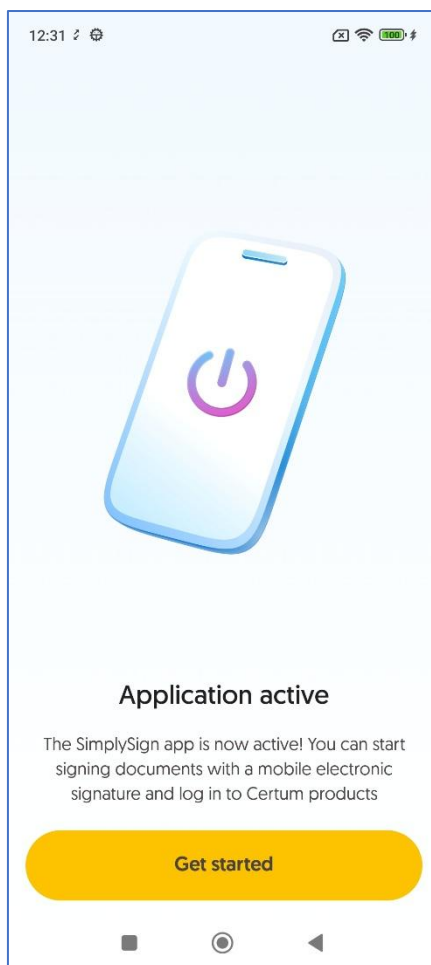
After entering the personal data, select Next. If the data is correct, the application is activated and displays the screen for selecting its operating mode.



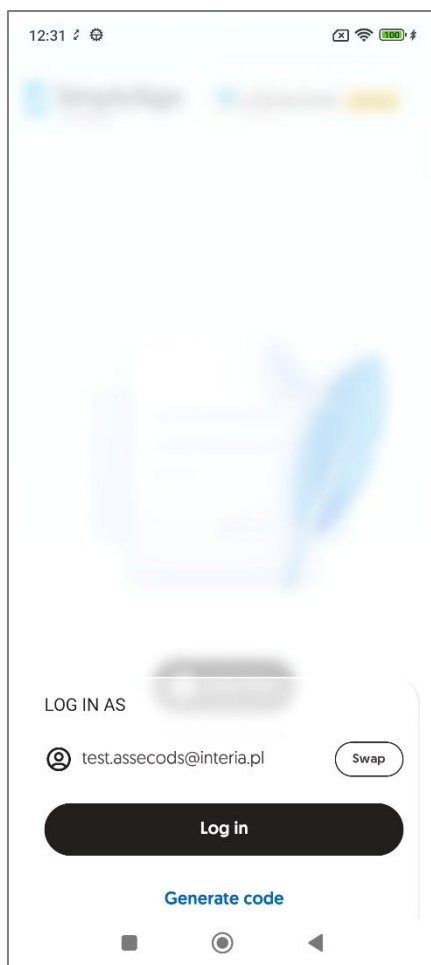
Two modes are available:

- Signing and Generating One-Time Codes – enables document signing and simultaneous generation of one-time codes;
- Generate Codes Only – generates one-time codes only; signing must then be performed on another device;

After selecting a mode, select Complete Activation. A screen confirms that the application is active.



After selecting Get Started, the application opens the start screen.



6.3. Resetting Service Access

Resetting Service Access requires contacting the Certum helpline and requesting an access reset. A Certum helpline representative resets access after verifying the personal data of the user requesting the reset.

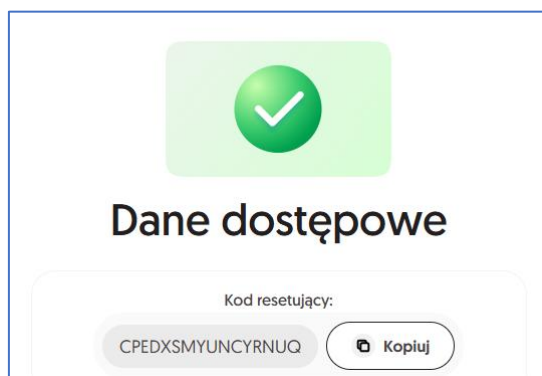
The user data from the qualified-certificate application submitted in the Certum system is verified.

After successful verification, the user receives a six-character secret code from the Certum operator.

Certum also sends a one-time service-access reset link to the email address used as the user identifier in SimplySign. The link is valid for 24 hours from the time it is generated.

The user opens the email, selects the activation link, and is taken to a Certum page where the six-character secret must be entered.

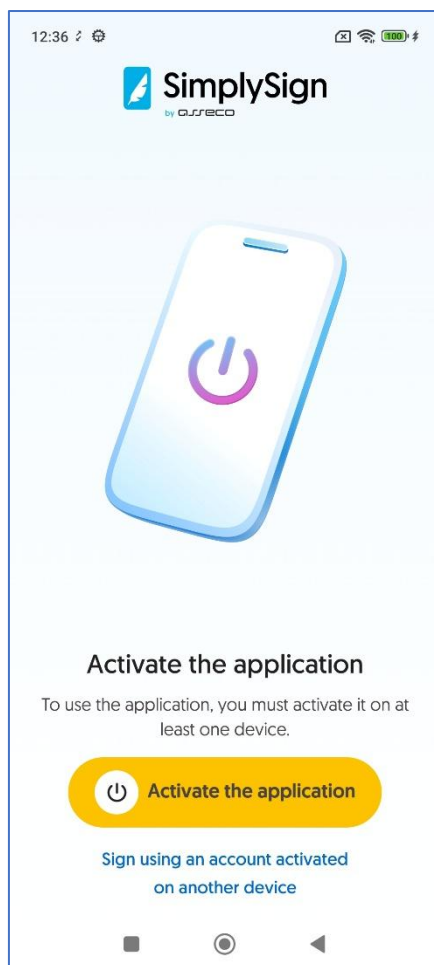
Depending on the reset method, after entering the secret and selecting Send, the user receives either a QR code (photo code) or a 16-character reset code. Do not close the browser after receiving this information; continue to the next stage of resetting service access.



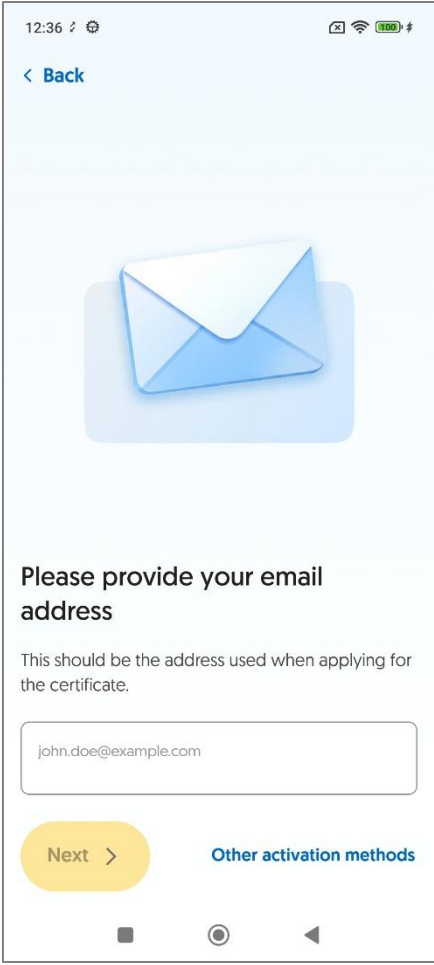
Both methods are described in the following subsections.

6.3.1. Manual Reset Using a 16-Character Activation Code

To reset access using a 16-character activation code, start SimplySign.



Select Activate Application. The application activation screen appears.



12:36

< Back



Please provide your email address

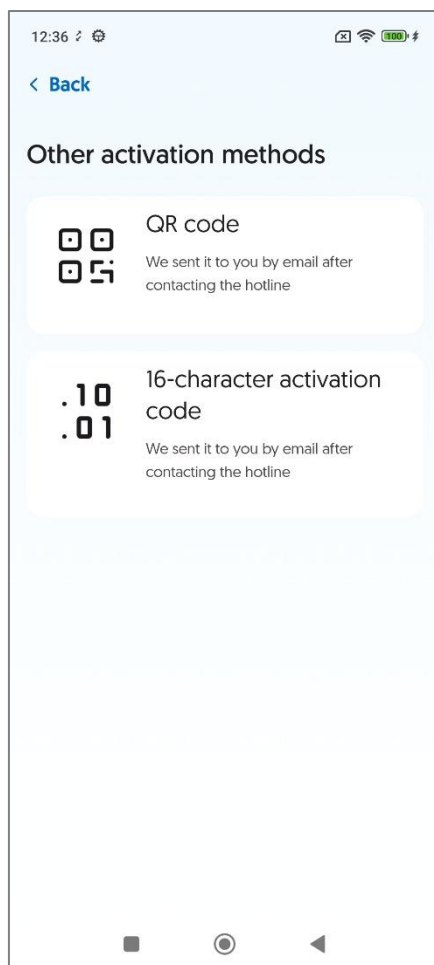
This should be the address used when applying for the certificate.

john.doe@example.com

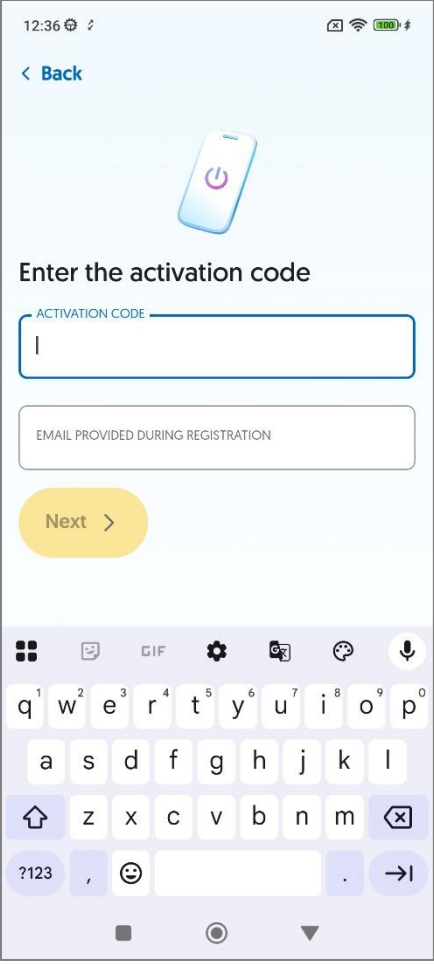
Next > [Other activation methods](#)

Navigation icons: square, circle, triangle

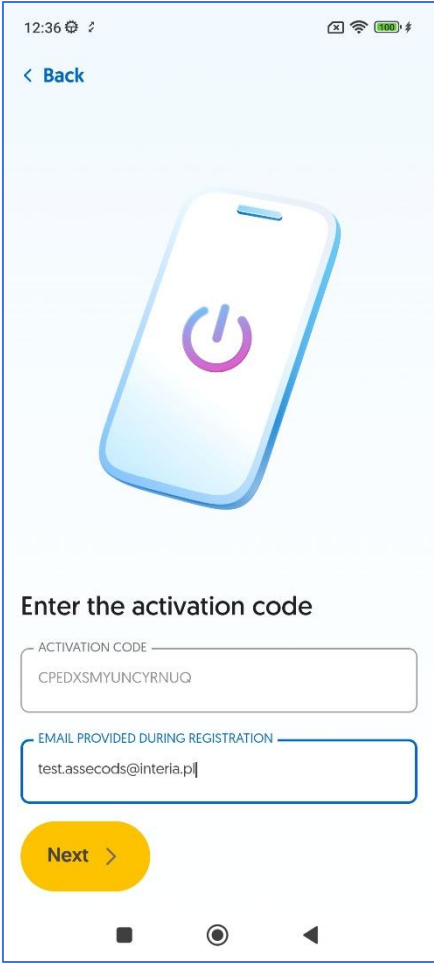
Select Other Activation Methods at the bottom of the screen. Additional options appear.



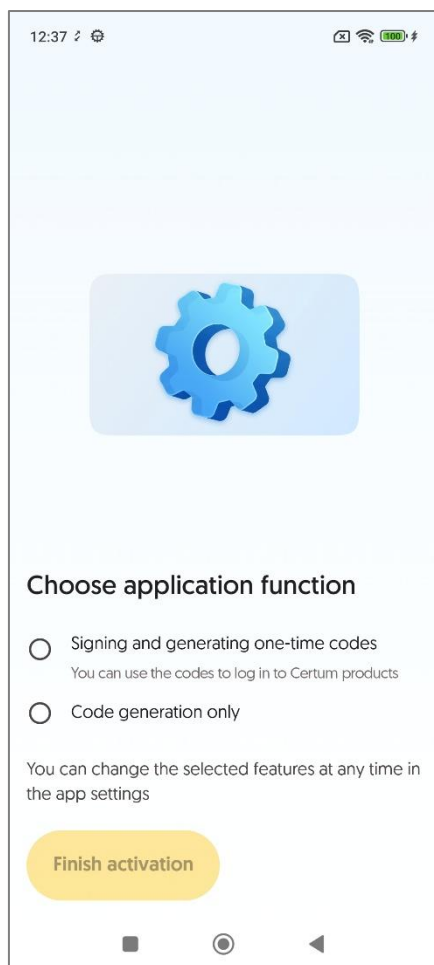
Select 16-character activation code. A screen for entering the 16-character activation code appears.

A screenshot of a mobile application's activation screen. At the top, the status bar shows the time 12:36, signal strength, Wi-Fi, and battery level. Below the status bar is a blue header with a '< Back' link. In the center, there is a blue smartphone icon with a power button. Below the icon, the text 'Enter the activation code' is displayed. Underneath is a text input field labeled 'ACTIVATION CODE' with a single character 'I' entered. Below the input field is a text box labeled 'EMAIL PROVIDED DURING REGISTRATION'. At the bottom of the form is a yellow 'Next >' button. A virtual keyboard is visible at the bottom of the screen, showing the QWERTY layout with various function keys like '?123', a smiley face, and a search icon.

Complete the activation code and E-mail fields.

A screenshot of a mobile application's activation screen. At the top, the status bar shows the time 12:36, signal strength, Wi-Fi, and battery level. Below the status bar is a blue header with a back arrow and the text '< Back'. The main area features a large illustration of a smartphone with a purple power button icon on its screen. Below the illustration, the text 'Enter the activation code' is displayed. There are two input fields: the first is labeled 'ACTIVATION CODE' and contains the text 'CPEDXSMYUNCYRNUQ'; the second is labeled 'EMAIL PROVIDED DURING REGISTRATION' and contains the text 'test.assecods@interia.pl'. At the bottom of the form is a yellow button with the text 'Next >'. The entire screen is framed by a blue border, and the Android navigation bar is visible at the very bottom.

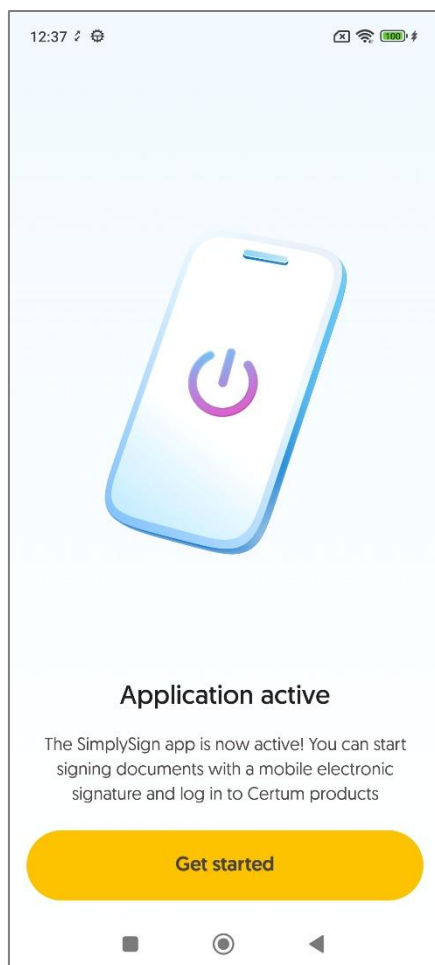
Select Next. If the entered data is correct, service access is restored and the screen for selecting the application operating mode appears.



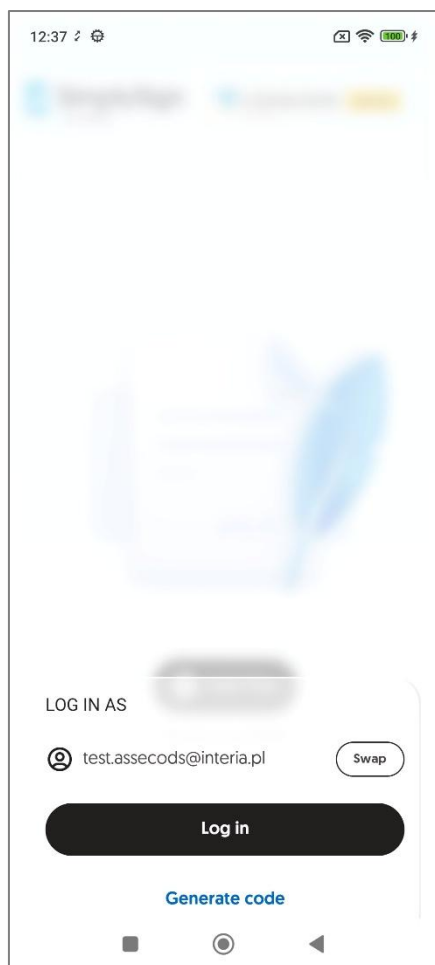
Two modes are available:

- Signing and Generating One-Time Codes – enables document signing and simultaneous token generation;
- Generate Codes Only – generates one-time codes only; signing must then be performed on another device;

After selecting a mode, select Complete Activation. A screen confirms that the application is active.

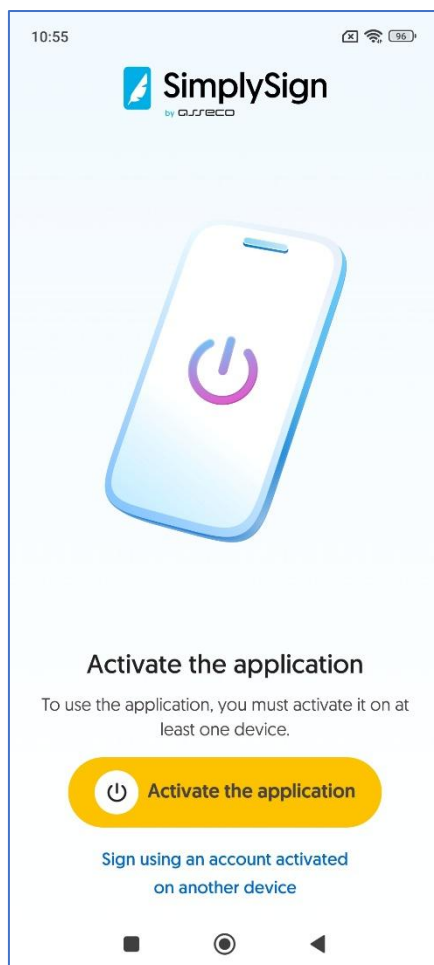


After selecting Get Started, the application opens the start screen.

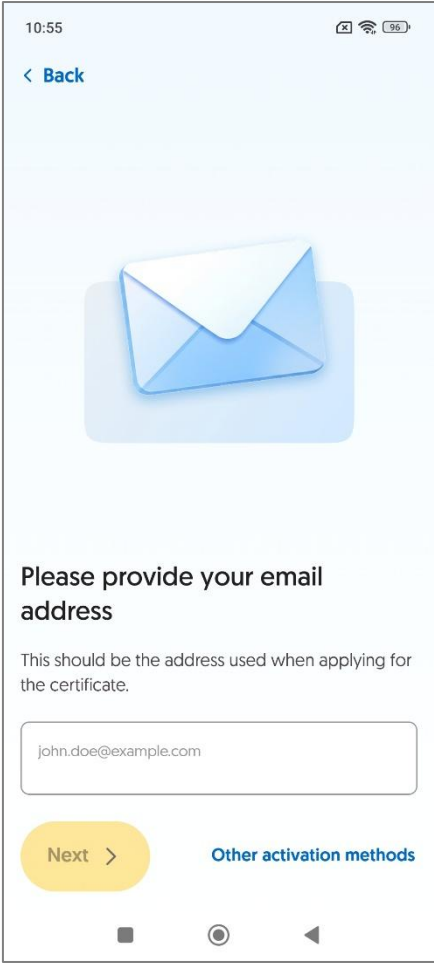


6.3.2. Automatic Reset Using a QR Code

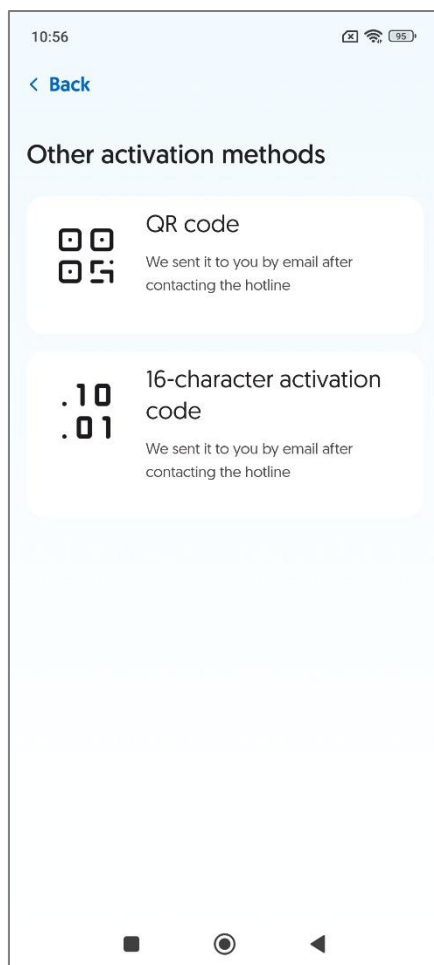
To reset service access automatically, start SimplySign.



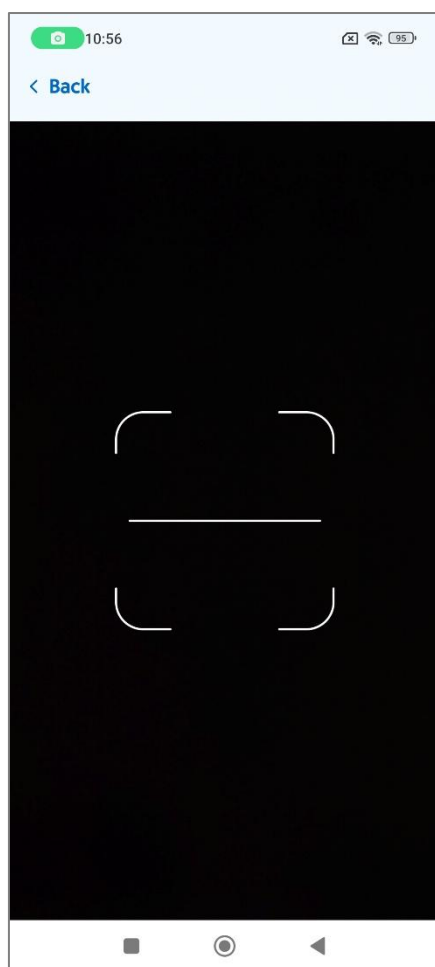
Select Activate Application. The application activation screen appears.

A mobile application screen with a light blue background. At the top, the status bar shows the time 10:55, signal strength, Wi-Fi, and battery icons. Below the status bar is a blue header with a back arrow and the text '< Back'. In the center is a large, stylized blue envelope icon. Below the icon, the text 'Please provide your email address' is displayed in bold. Underneath, a smaller line of text reads: 'This should be the address used when applying for the certificate.' A white text input field contains the placeholder text 'john.doe@example.com'. At the bottom, there is a yellow rounded button with the text 'Next >' and a blue text link 'Other activation methods'. The very bottom of the screen shows the standard Android navigation bar with three icons: a square, a circle, and a triangle.

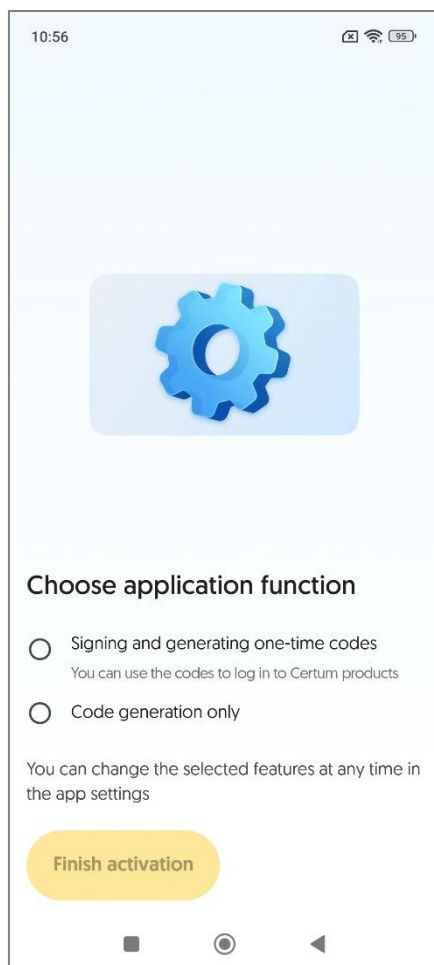
Select Other Activation Methods at the bottom of the screen. Additional options appear.



Select QR Code. A screen for scanning the QR code appears.



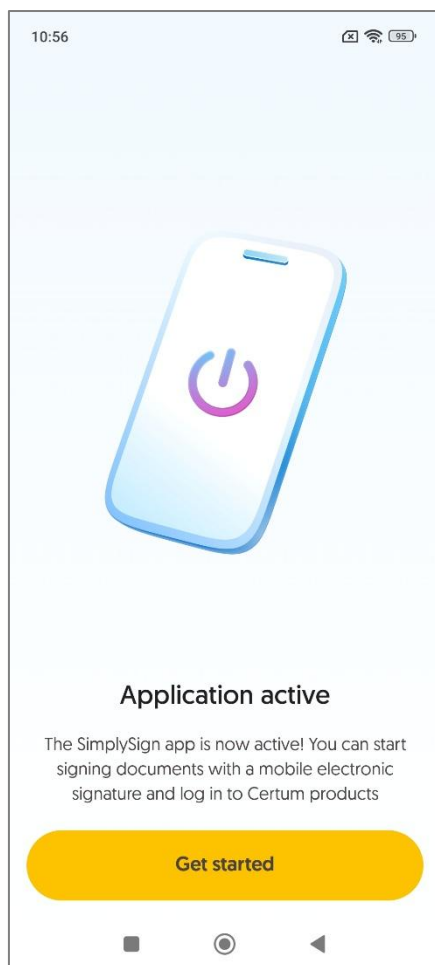
After scanning the QR code, the screen for selecting the application operating mode appears.



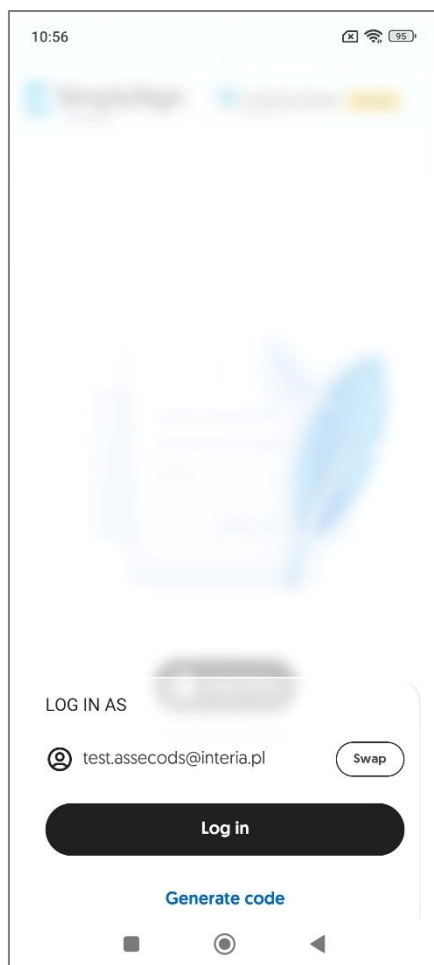
Two modes are available:

- Signing and Generating One-Time Codes – enables document signing and simultaneous generation of one-time codes;
- Generate Codes Only – generates one-time codes only; signing must then be performed on another device;

After selecting a mode, select Complete Activation. A screen confirms that the application is active.



After selecting Get Started, the application opens the start screen.

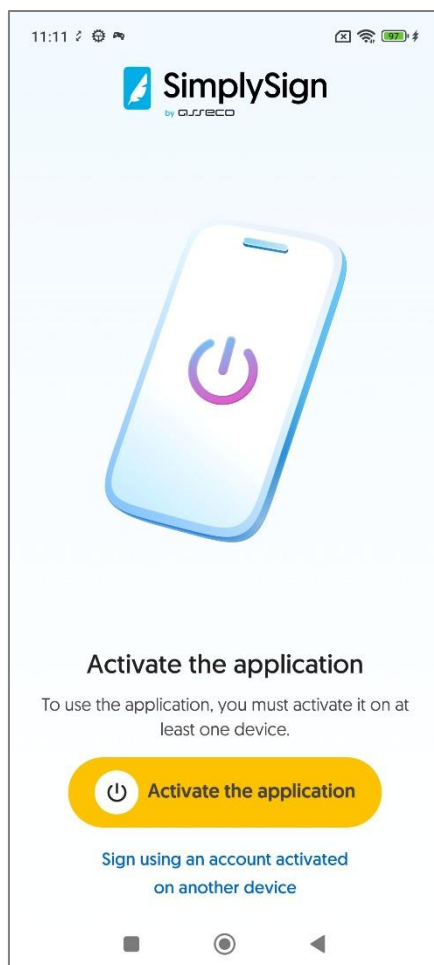


6.4. Signing Without Activation

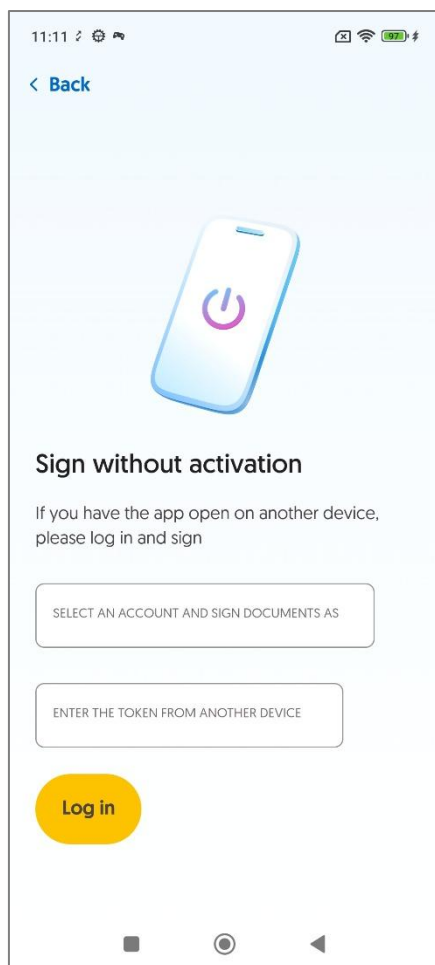
SimplySign supports signing without activation by signing in with a one-time code from another device. This option is available when the application is not activated or is activated in Signing and Generating One-Time Codes mode.

6.4.1. Application Not Activated

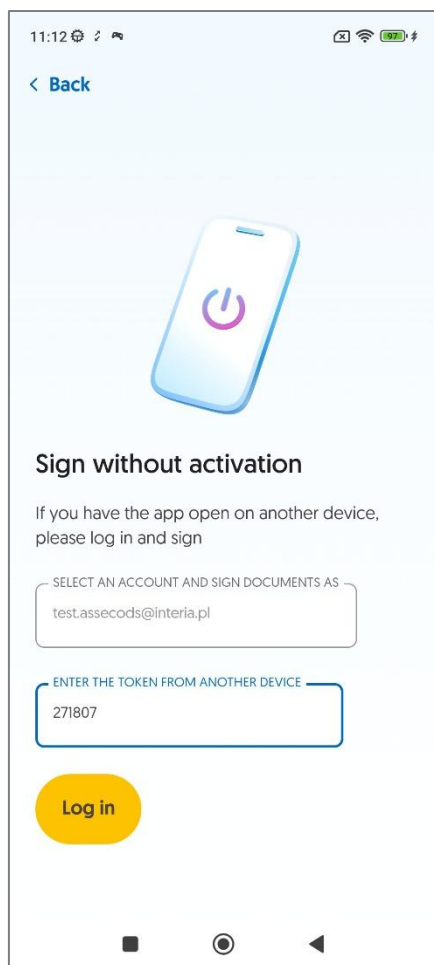
To sign in to an account activated on another device when this application is not activated, select Sign using an account activated on another device.



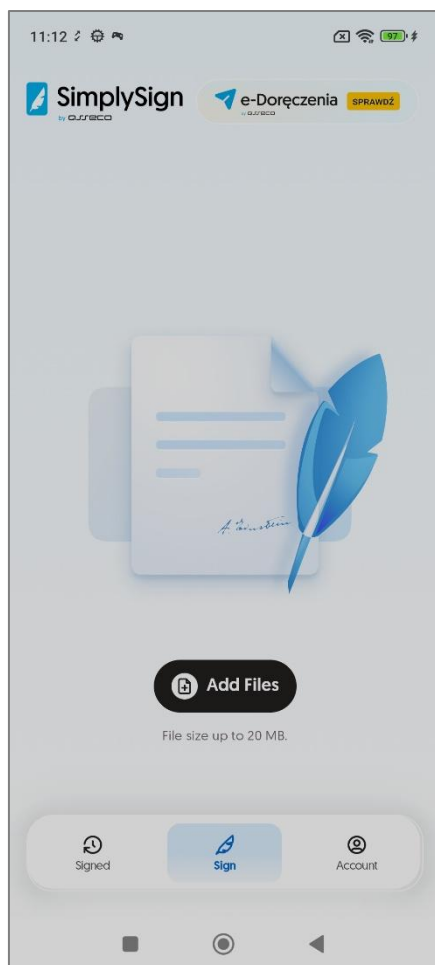
After selecting Sign using an account activated on another device, a screen appears where you can enter the login and one-time code.



Enter the login and the one-time code from the other device.

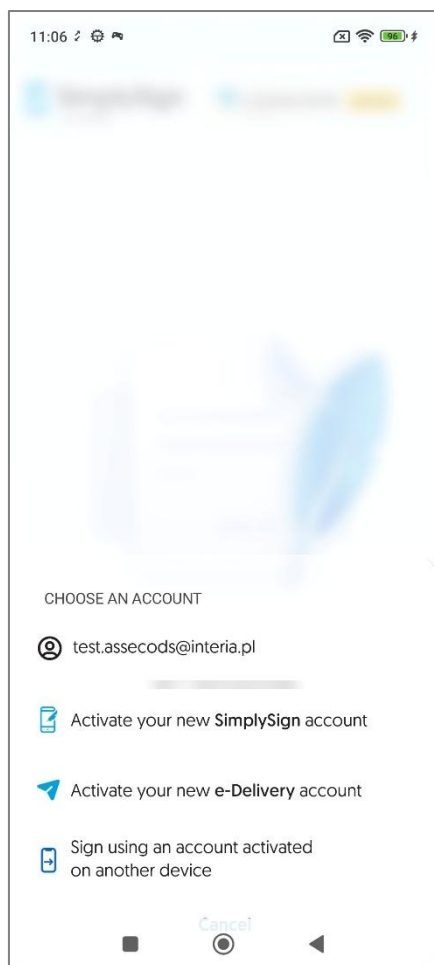


Select Sign In. If the login and one-time code are correct, you are signed in and can create a signature.

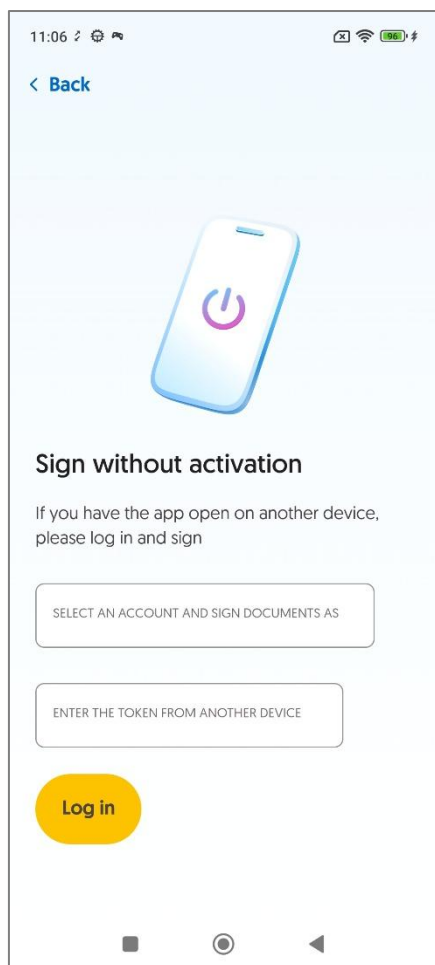


6.4.2. Application in “Signing and Generating One-Time Codes” Mode

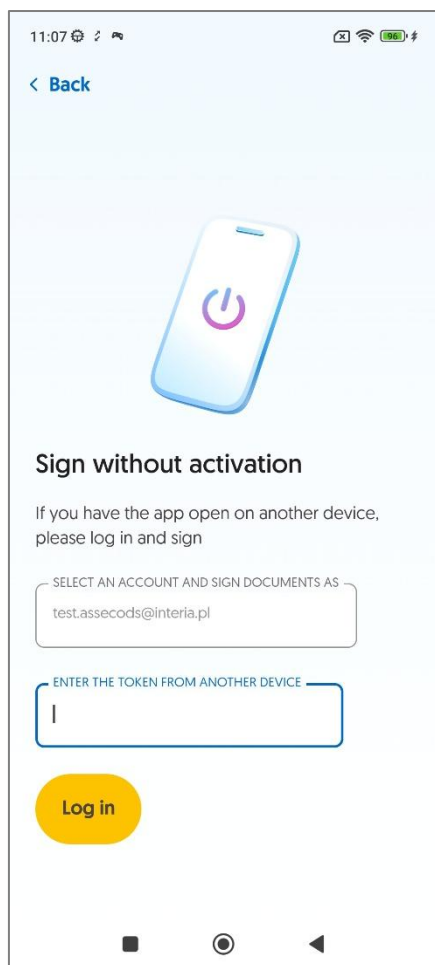
To sign in to an account activated on another device while in Signing and Generating One-Time Codes mode, select Change in the account list. The available options appear.



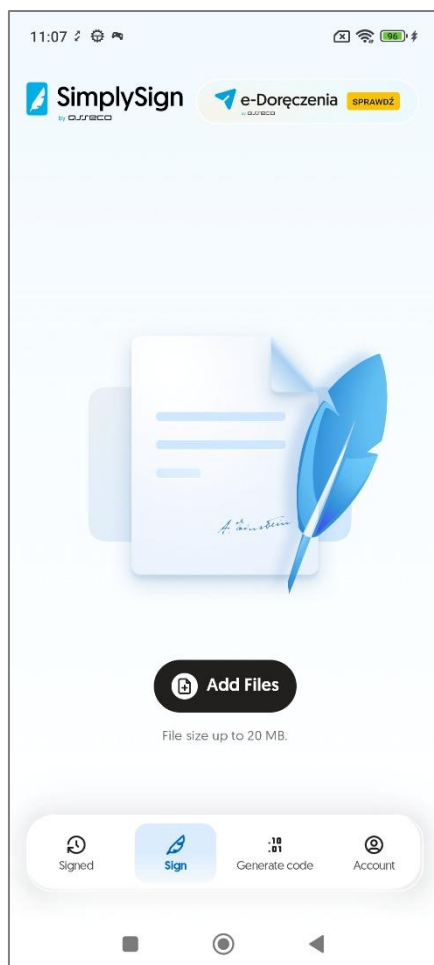
Select Sign using an account activated on another device. A screen appears where you can enter the login and one-time code.



Enter the login and one-time code.



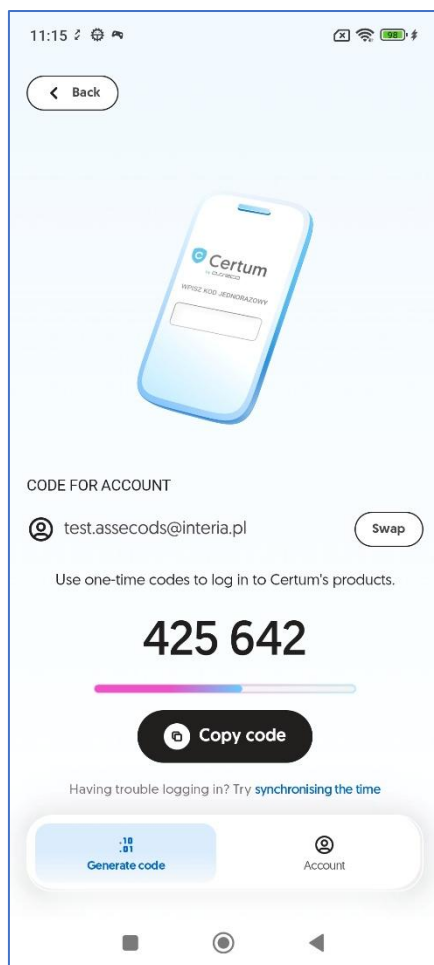
Select Sign In. If the login and one-time code are correct, you are signed in and can create a signature.



6.5. Application Operating Modes

6.5.1. Operating in “Generate One-Time Codes Only” Mode

If Generate One-Time Codes Only is selected during activation, the application only generates one-time codes. When started, it immediately displays the currently generated one-time code.



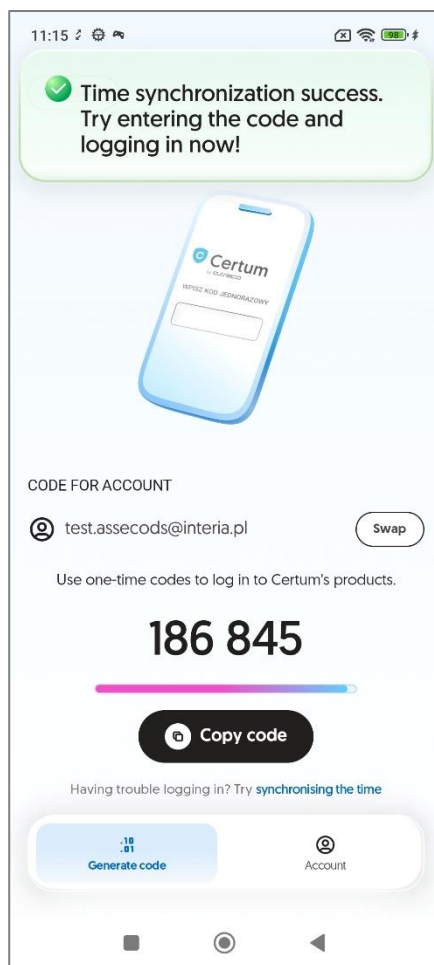
6.5.1.1. Forcing Time Synchronization

In Generate Codes Only mode, you can manually force time synchronization. This recalculates the one-time code using synchronized time.

Use this option if sign-in problems suggest that the one-time code is being generated incorrectly on the device.

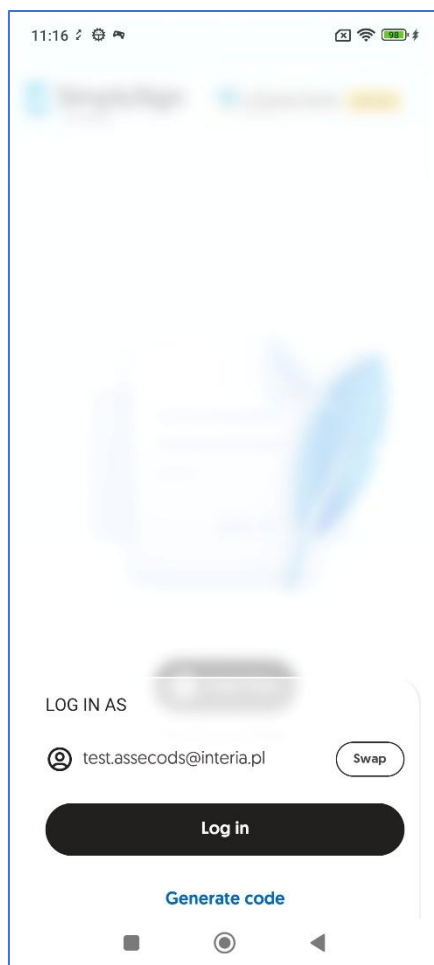
This synchronization changes time only within SimplySign and does not affect the device time settings.

To synchronize, select Try Time Synchronization. The time is synchronized.



6.5.2. Operating in “Signing and Generating One-Time Codes” Mode

If Signing and Generating One-Time Codes mode is selected during activation, the application generates one-time codes and can also sign documents. When started, it displays a screen from which you can generate one-time codes (Generate Code) or proceed to document signing (Sign In).

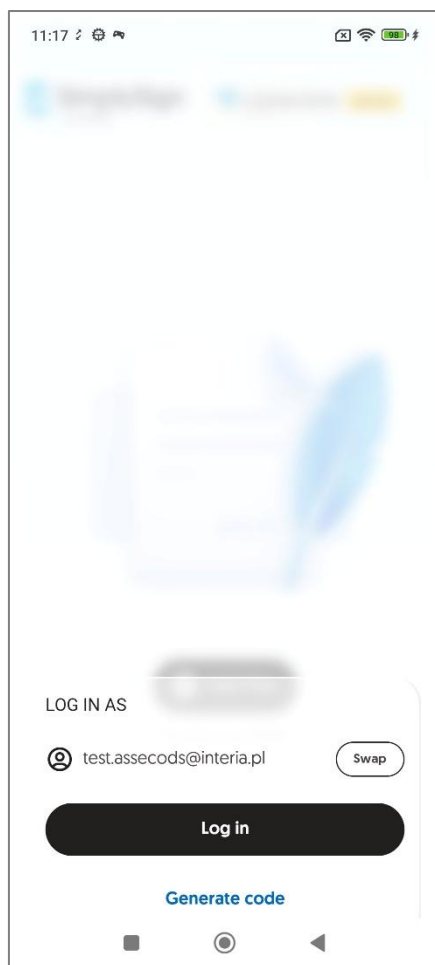


6.6. Multiple Account Support

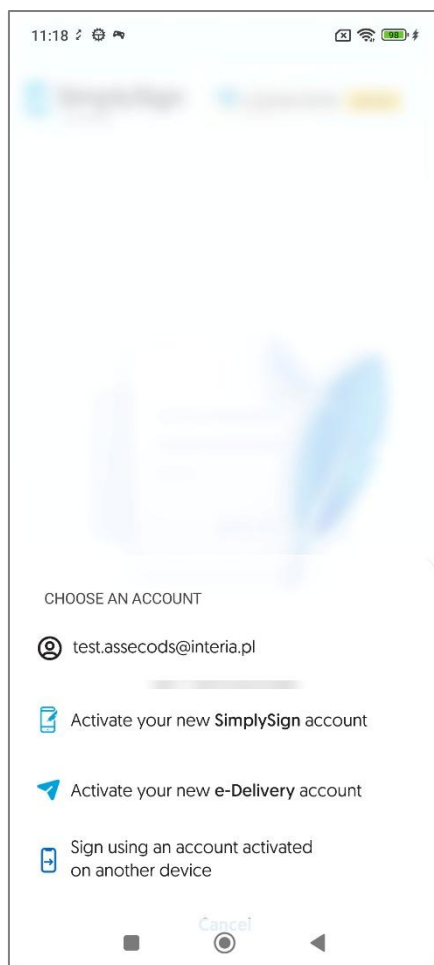
The application supports multiple accounts. The following describes how to add another account in Signing and Generating One-Time Codes mode and in Generate Codes Only mode.

6.6.1. “Signing and Generating One-Time Codes” Mode

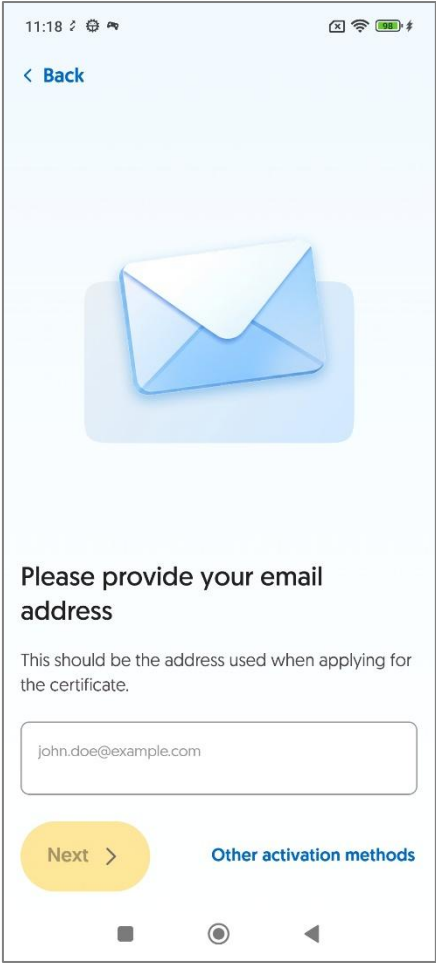
To add another account in Signing and Generating One-Time Codes mode, start the application.



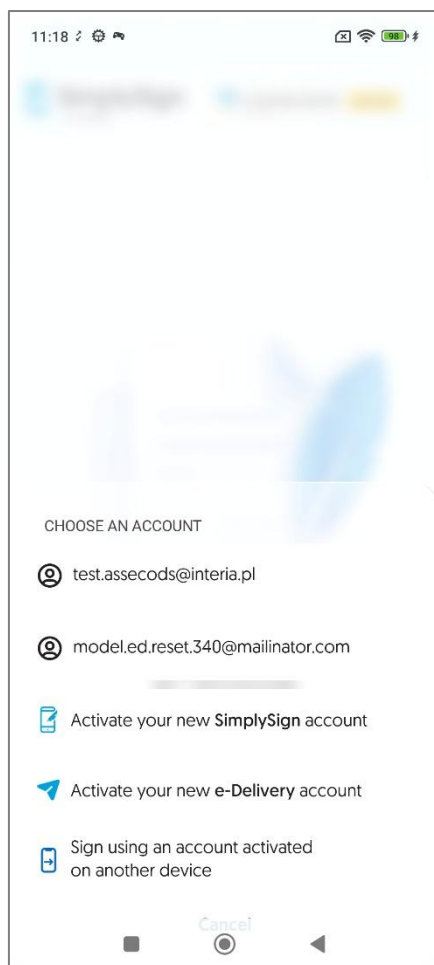
Select Change. The account list expands and displays the Activate New SimplySign Account option.



After selecting Activate New SimplySign Account, a screen appears where you can activate a new account using your preferred method.

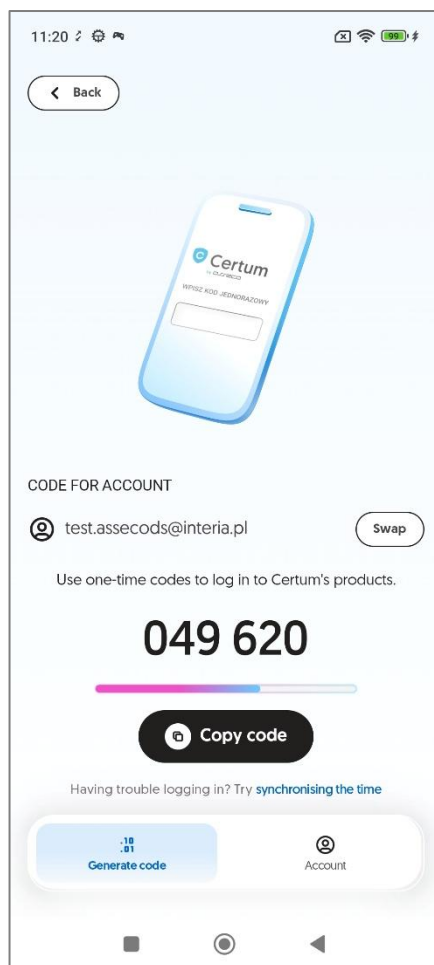
A screenshot of a mobile application interface. At the top, the status bar shows the time 11:18, signal strength, Wi-Fi, and battery icons. Below the status bar is a blue header with a back arrow and the text "< Back". The main area has a light blue background with a large, stylized blue envelope icon. Below the icon, the text "Please provide your email address" is displayed in bold. Underneath, a smaller line of text reads: "This should be the address used when applying for the certificate." A text input field contains the placeholder email "john.doe@example.com". At the bottom, there is a yellow button with the text "Next >" and a blue link labeled "Other activation methods". The very bottom of the screen shows three standard Android navigation icons: a square, a circle, and a triangle.

The activation methods were described in an earlier section. After another account is activated, it appears in the application.

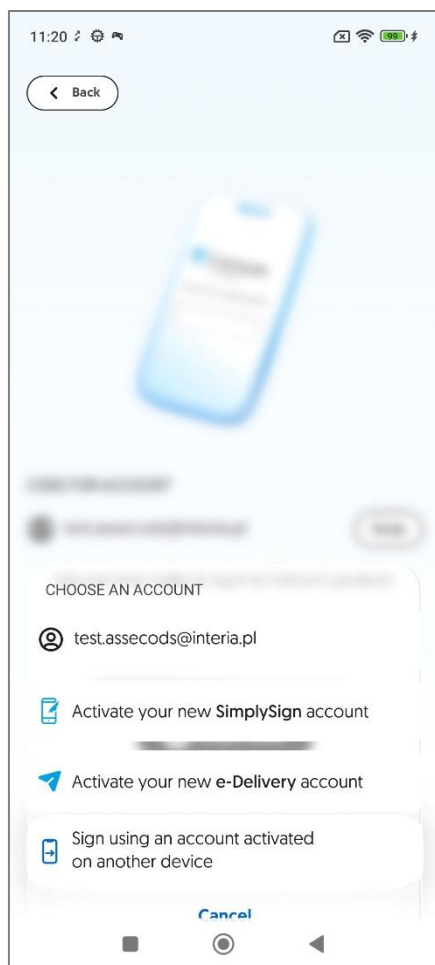


6.6.2. “Generate Codes Only” Mode

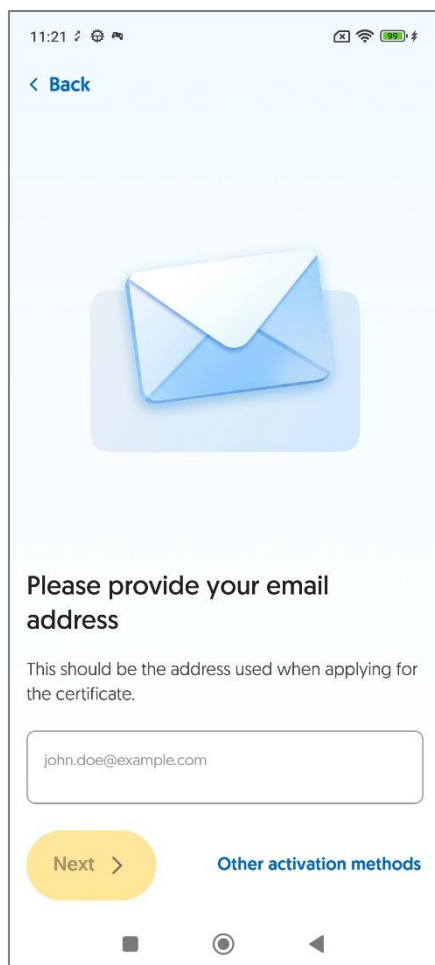
To add another account in Generate Codes Only mode, start the application.



Select Change. The account list expands and displays the Activate New SimplySign Account option.



After selecting Activate New SimplySign Account, a screen appears where you can activate a new account using your preferred method.

A screenshot of a mobile application interface. At the top, the status bar shows the time 11:21, signal strength, Wi-Fi, and battery level at 99%. Below the status bar is a blue header with a back arrow and the text "< Back". The main content area has a light blue background. In the center is a large, stylized blue envelope icon. Below the icon, the text "Please provide your email address" is displayed in bold. Underneath, a smaller line of text reads: "This should be the address used when applying for the certificate." Below this is a white text input field containing the placeholder text "john.doe@example.com". At the bottom of the form area, there is a yellow rounded button with the text "Next >" and a blue link labeled "Other activation methods". The very bottom of the screen shows the standard Android navigation bar with three icons: a square, a circle, and a triangle.

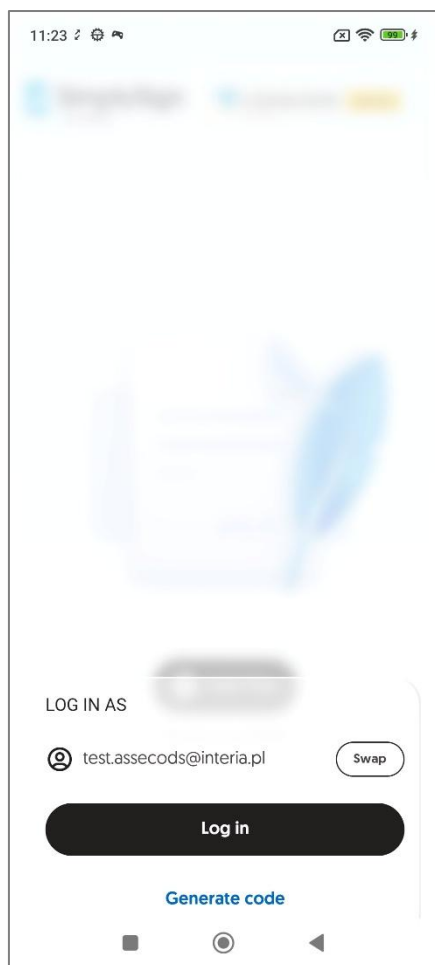
The activation methods were described in an earlier section. After another account is activated, it appears in the application.



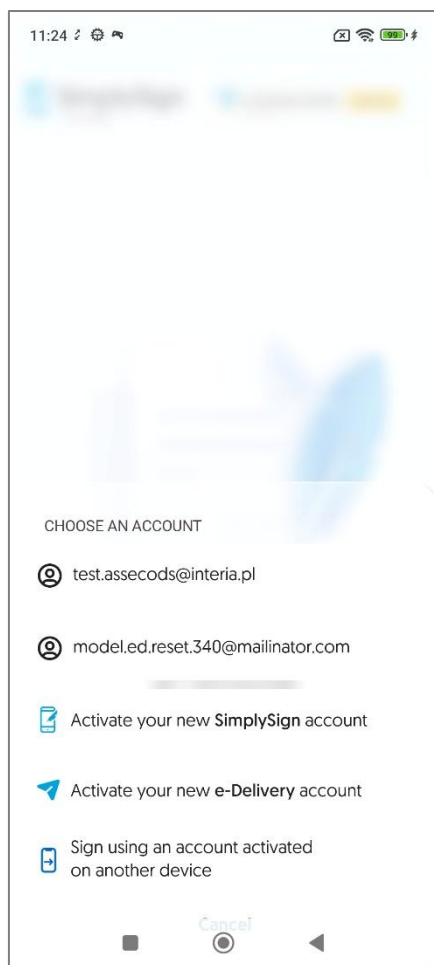
6.7. Signing In to the Application

6.7.1. “Signing and Generating One-Time Codes” Operating Mode

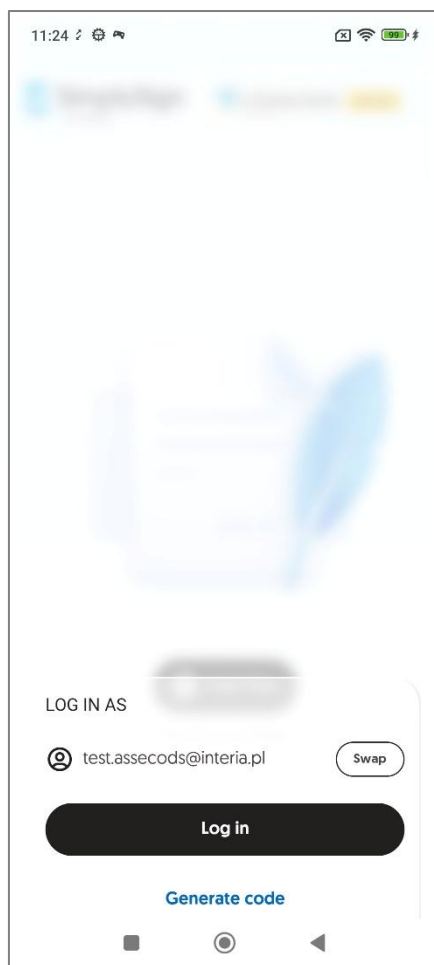
If the application is set to Signing and Generating One-Time Codes mode, its start screen appears when the application is opened.



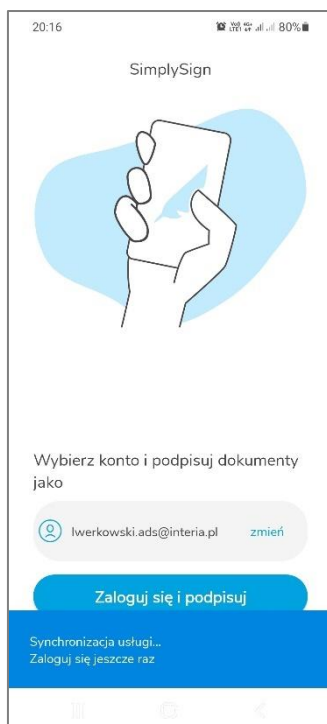
Because the application supports multiple accounts, select Change. The account list appears.



Select the appropriate account from the account list.

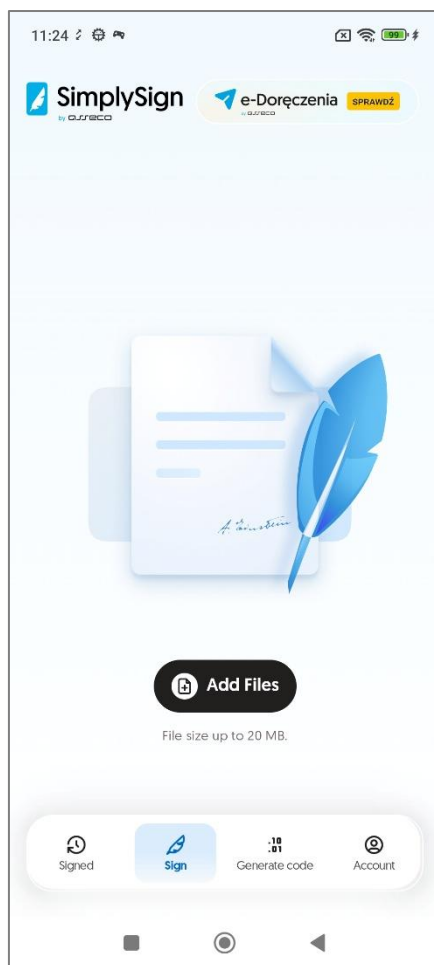


Then select Sign In. The application automatically generates a one-time code and attempts to sign the user in to the service. If a sign-in problem is caused by an invalid one-time code, the application automatically synchronizes time in SimplySign and displays a message indicating this.



This synchronization changes time only within SimplySign and does not affect the device time settings.

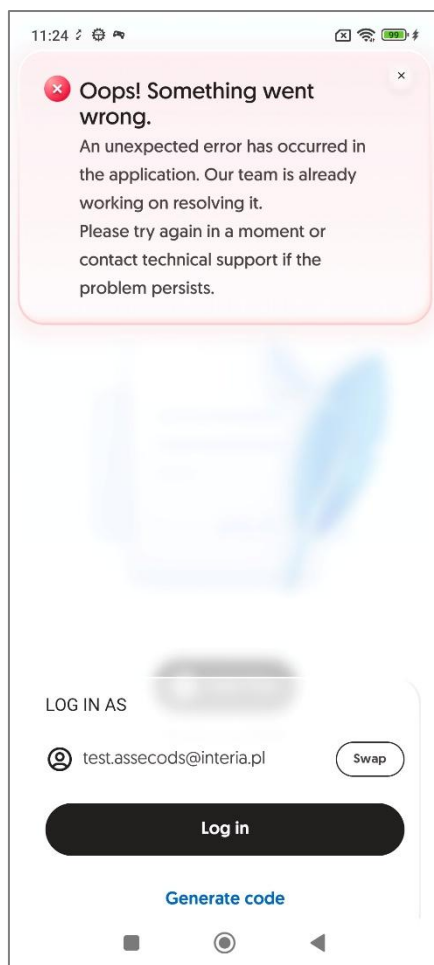
After automatic time synchronization, select Sign In again. You are signed in to the SimplySign service.



If this is the first sign-in on the device, a message asks you to allow the application to access internal device information.

After selecting Allow, you are signed in to the service and a screen appears where you can add files for signing or open the application options.

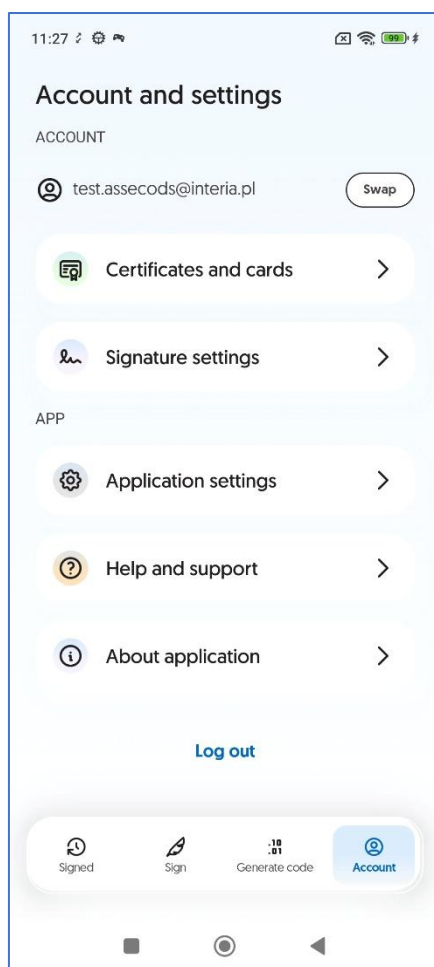
If the one-time code is invalid or another error prevents sign-in, the No access/No network connection message appears at the bottom.



7. Account Settings/Application Options

After signing in, you can change the default application options. Select the Account icon in the lower-right corner to display the available options.

7.1. Account and Settings



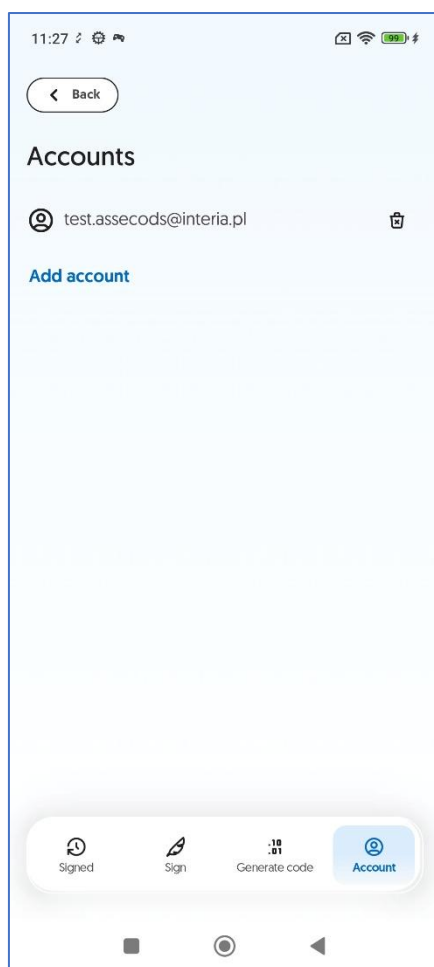
The following options are available in Account and Settings:

- Account Management
- Certificates and Cards
- Signature Settings
- Application Settings
- Help and Support
- About the Application

These options are described in detail in the following subsections.

7.1.1. Account Management

This option is used to manage accounts. Selecting it displays the account list.



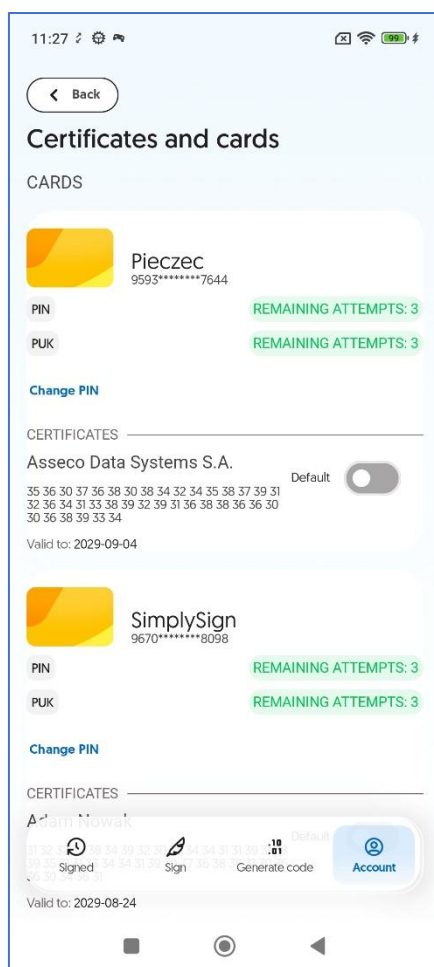
You can remove a selected account from the application. To do so, select the trash icon to the right of the account name.

7.1.2. “Certificates and Cards” Option

This option is used to manage your cards and certificates. Selecting it displays a screen with the signed-in user’s cards and basic certificate information.

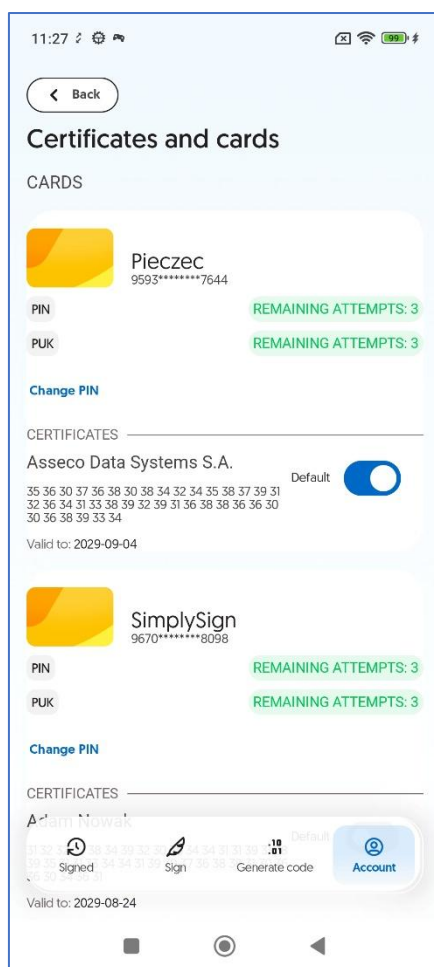
The configured default certificate is shown, followed by the card and the certificates it contains. The following data is displayed:

- The following card information:
 - Card label
 - PIN status
 - PUK status
 - The Common Name (CN) field from certificates on the card
 - Certificate serial number
 - Certificate expiration date



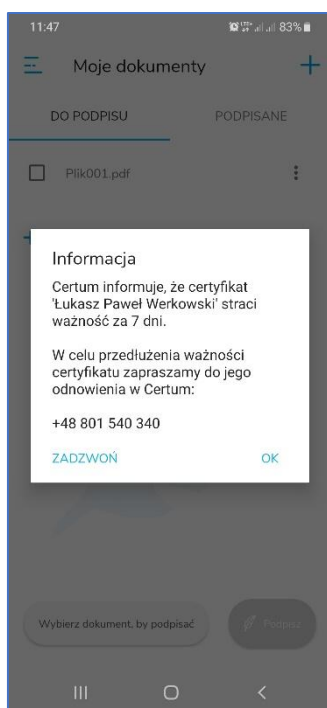
7.1.2.1. Setting the Default Certificate

To set a certificate as the default, select Default on the right side of the certificate entry in the list.



7.1.2.2. Warning of an Approaching Certificate Expiration Date

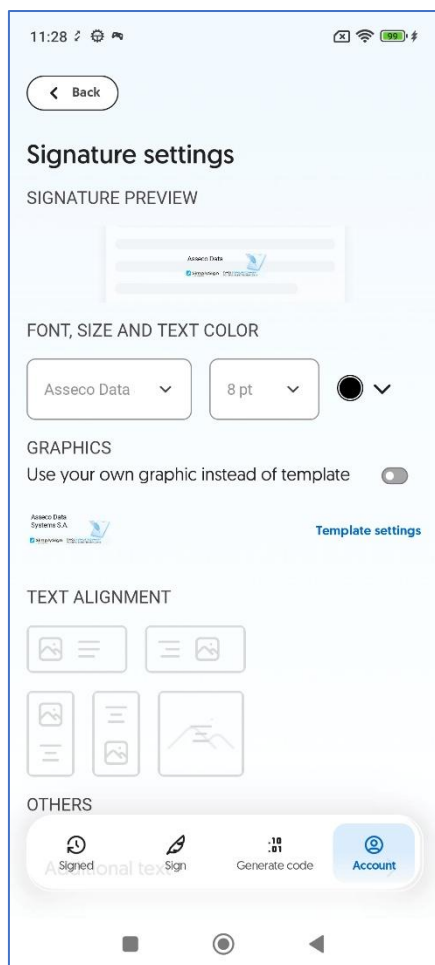
If fewer than 14 days remain before a qualified certificate expires, the application displays an appropriate warning after sign-in.

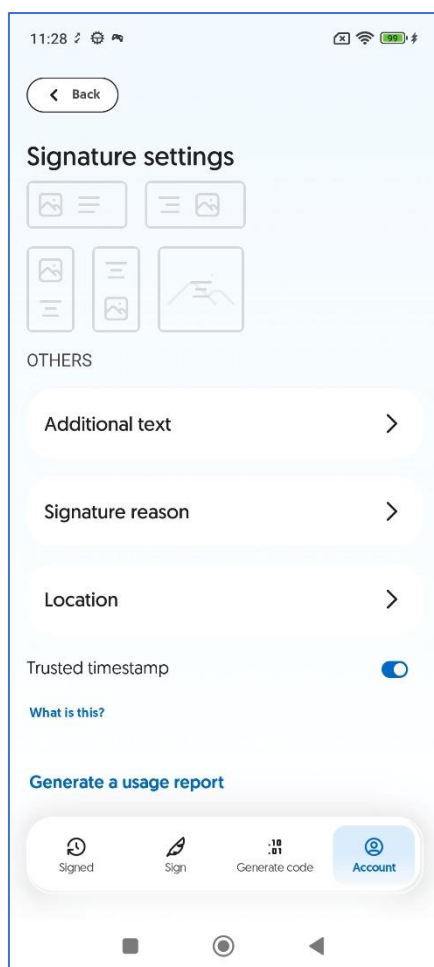


7.1.3. “Signature Settings” Option

This section lets you configure the following signature options:

- the typeface used in the visualization, as well as its size and color
- set a custom image used in the visualization
- align the text relative to the custom image in the visualization
- set custom text to appear in the visualization
- set a custom reason for signing to appear in the visualization and in the properties of the signed PDF file
- set a custom location to appear in the visualization and in the properties of the signed PDF file
- set the template used to create the visualization
- enable or disable adding a timestamp to signed files
- generate a summary account usage report for a selected month



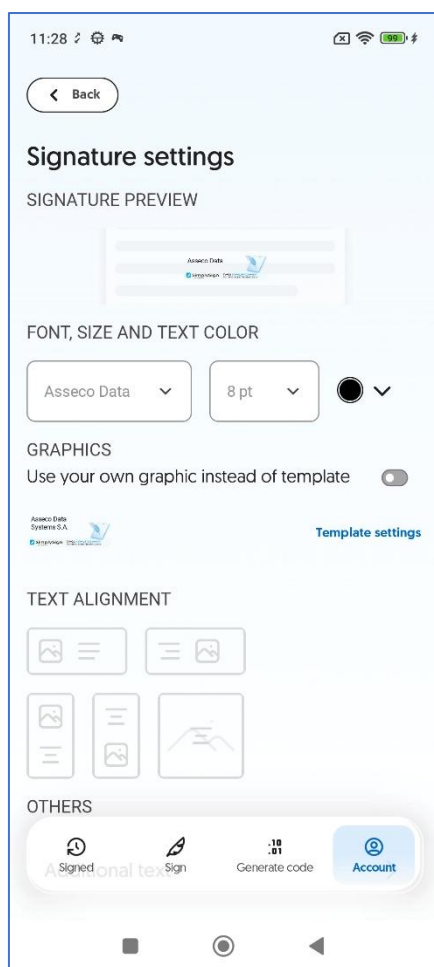


7.1.4. Visualization Options

The visualization-related settings are described in the following subsections.

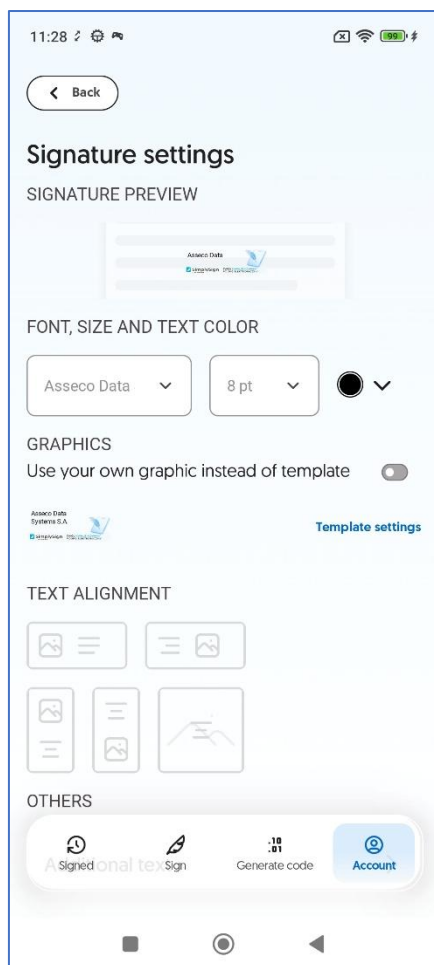
7.1.4.1. Font Property Options Used in the Visualization

In Signature Settings, you can change the font used in the visualization, including its typeface, size, and color.

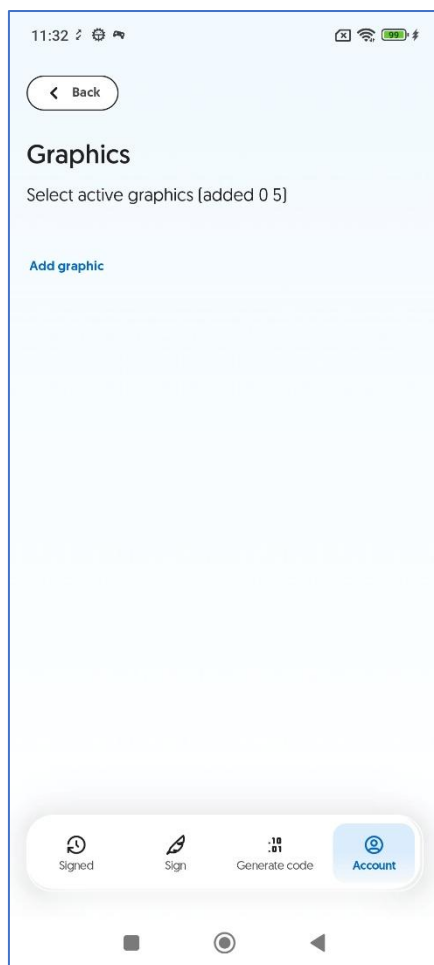


7.1.4.2. Setting a Signature with a Custom Image/Facsimile and Managing Images/Facsimiles

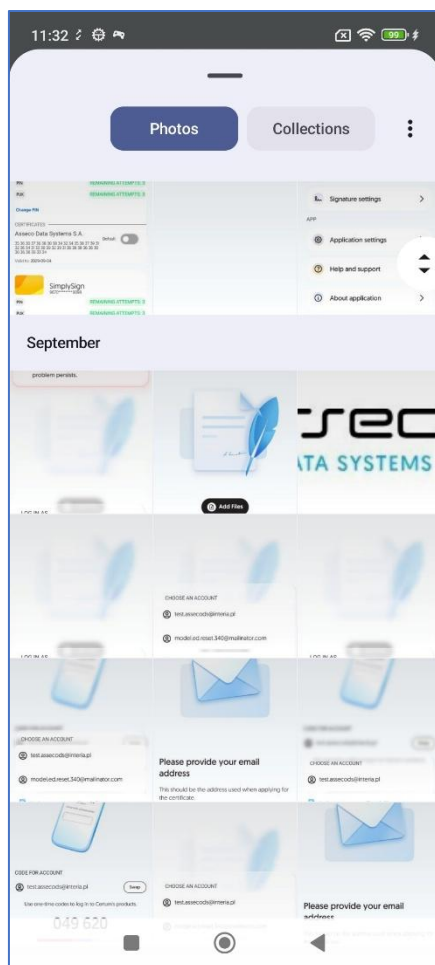
Another visualization setting is Use a Custom Image Instead of Templates.



Selecting this option enables Image Settings. Selecting Image Settings displays the available images and an option to add your own image to the list.



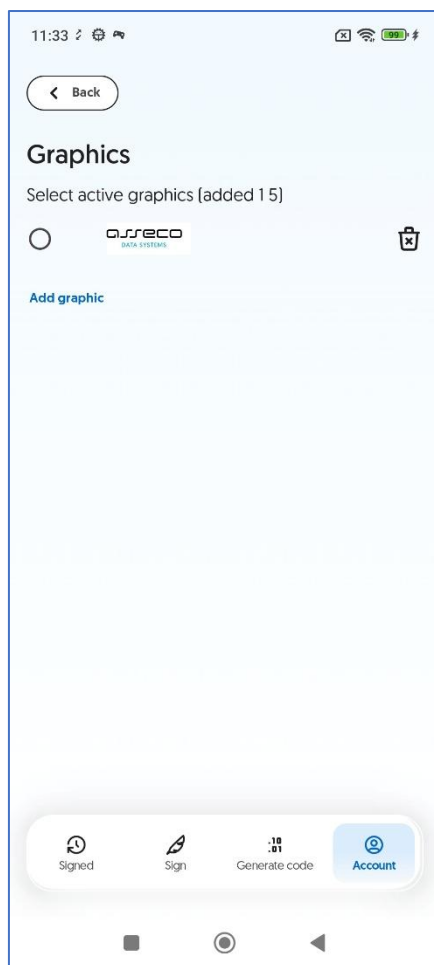
After selecting Add Image, the list of images available on the device appears.



After selecting an image, an editor opens so that you can add the image to the list.



After selecting Save Image, the selected image appears in the list of available images.

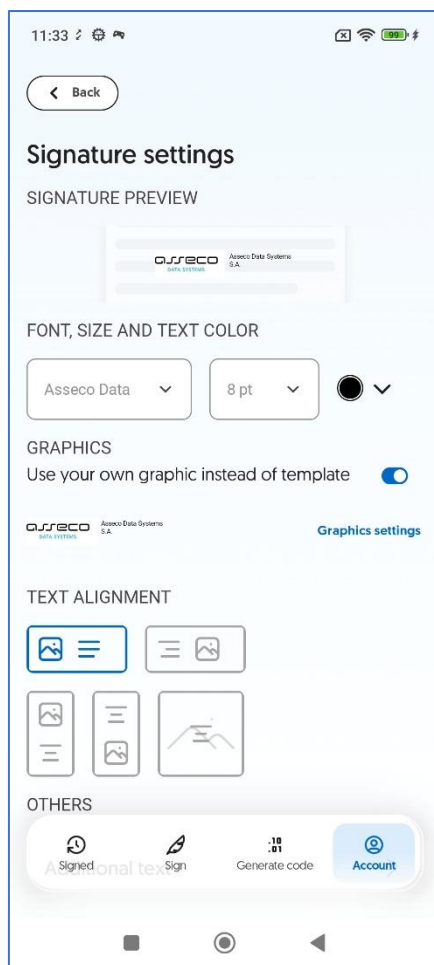


To set the selected image as the one included in the visualization, also select the option button to the left of that image.



In addition, the Text Alignment section lets you choose the position of the image relative to the text in the visualization. The following options are available:

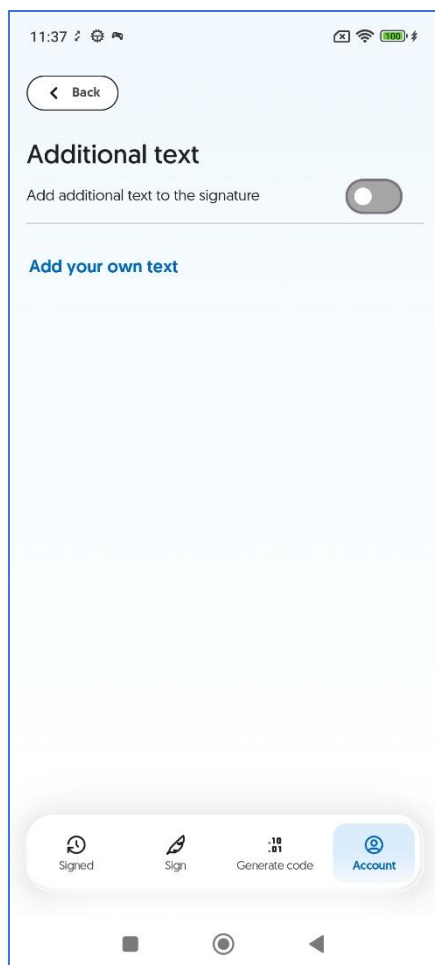
- image to the left of the text
- image to the right of the text
- image above the text
- image below the text
- text overlaid on the image



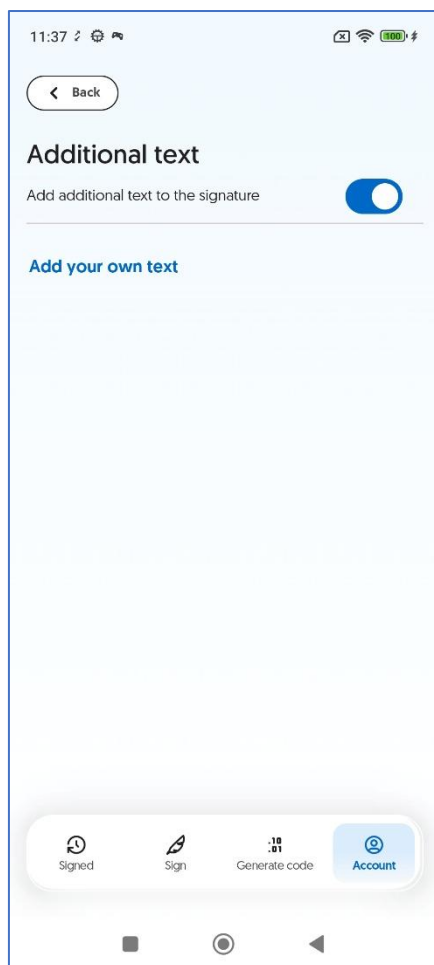
After selecting the image and text alignment in the options above, the Signature Preview section shows a preview of the visualization.

7.1.4.3. “Additional Text” Option

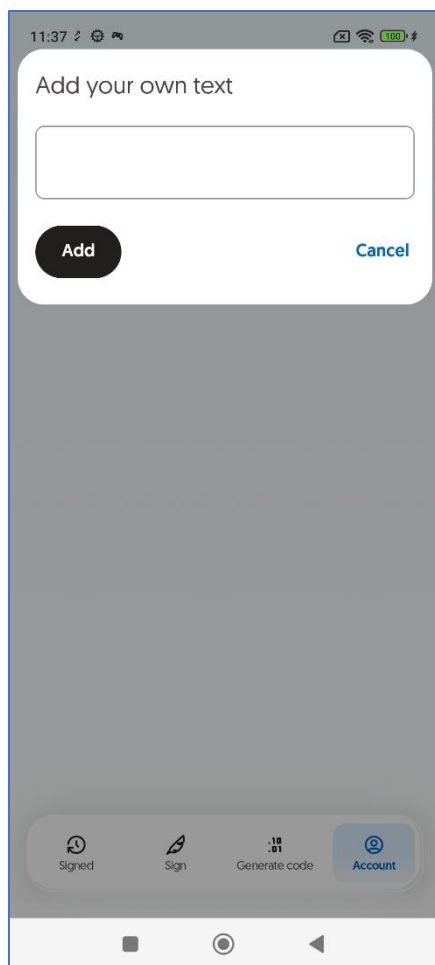
This option lets you define additional text that appears in the signature visualization.

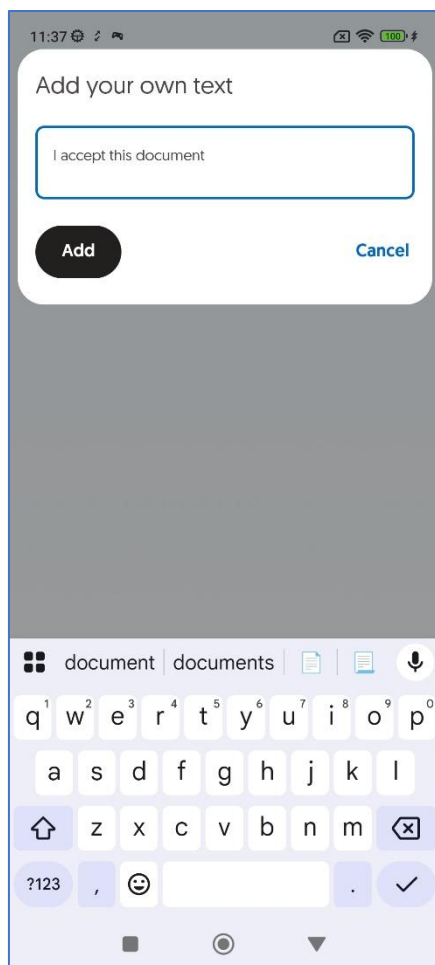


To enable this option, select the toggle on the right.

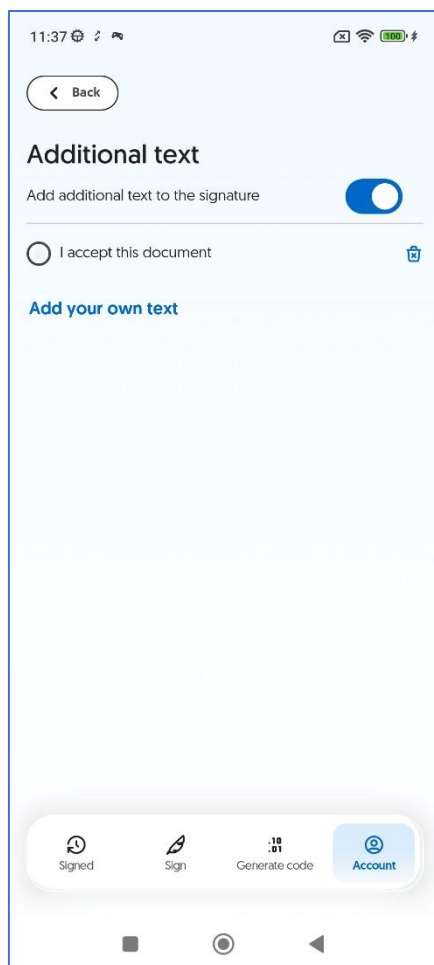


In addition to enabling this option, add text to the list and select the text that should appear in the visualization. To do so, select Add Custom Text. A form appears where you can enter your own text.

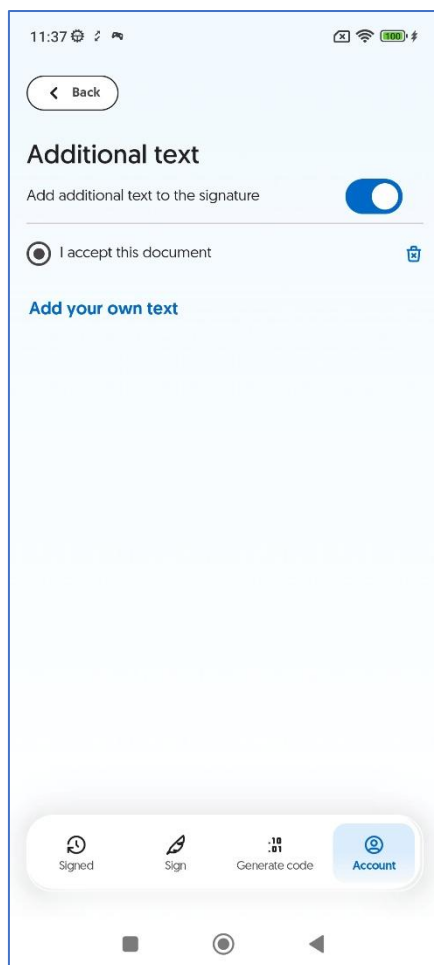




After entering your own text, select Add. The selected text appears in the list.



To set the selected text as the text included in the visualization, also select the option button to the left of that text.



7.1.4.4. “Reason for Signing” Option

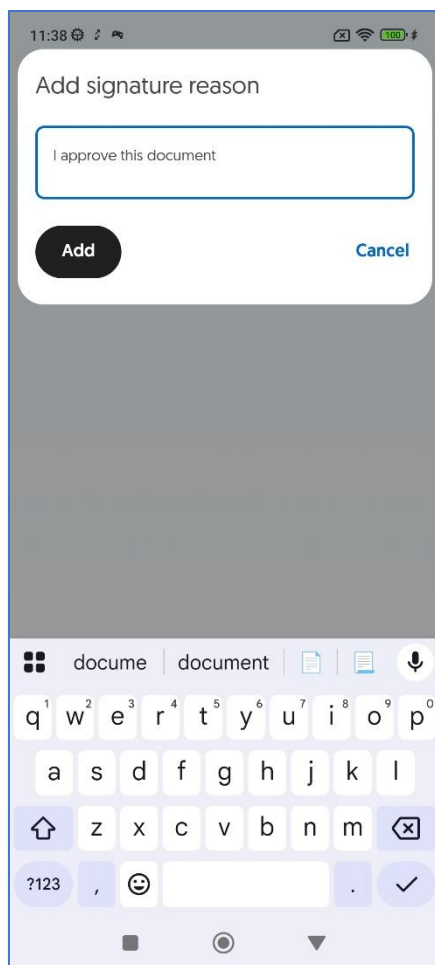
This option determines whether a Reason for Signing is added to the visualization and signature structure.



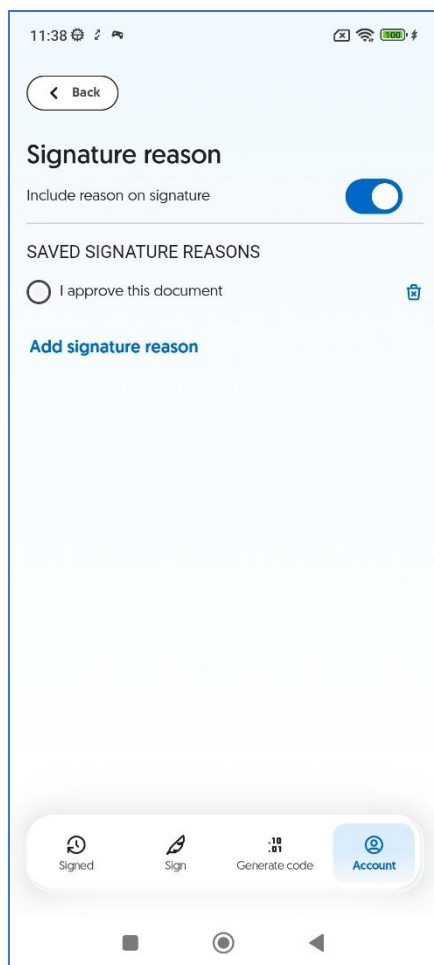
To enable this option, select the toggle on the right.



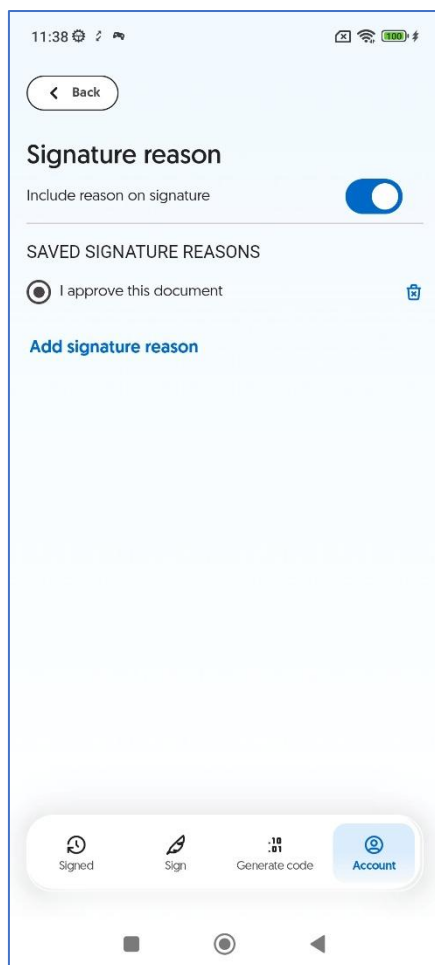
In addition to enabling this option, add a reason to the list and select the text to be inserted in the visualization and signature structure as the Reason for Signing. To do so, select Add Reason for Signing. A form appears where you can enter your own reason.



After entering your own text, select Add. The selected text appears in the list.

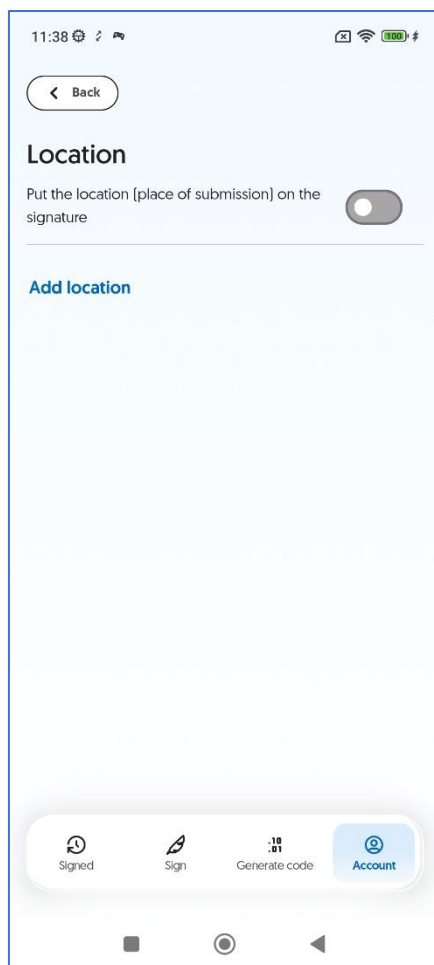


To set the selected reason as the one included in the visualization and signature structure, also select the option button to the left of that text.

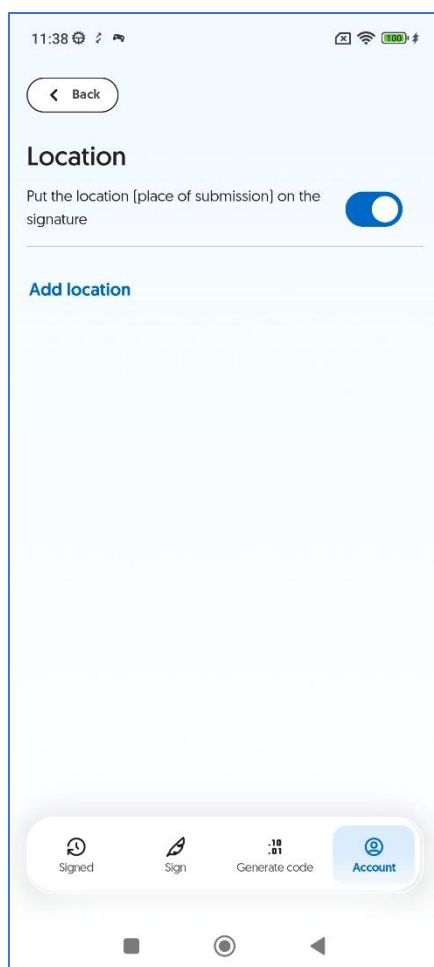


7.1.4.5. "Location" Option

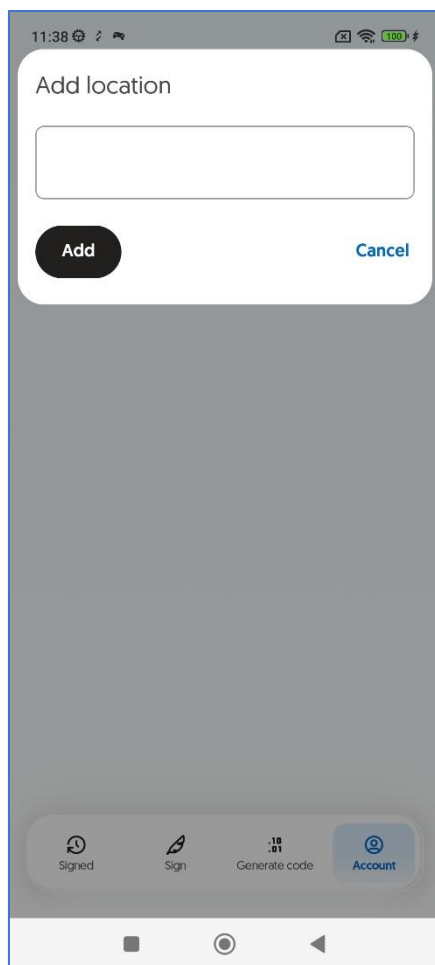
This option determines whether a Location is added to the visualization and signature structure.

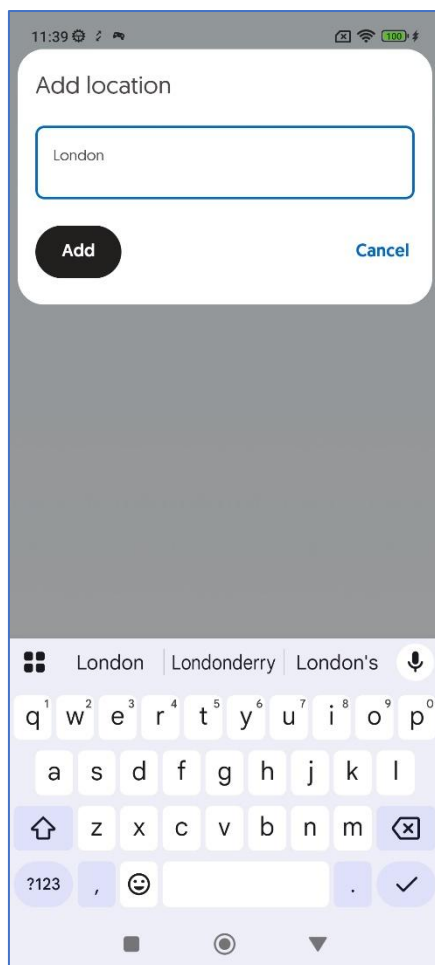


To enable this option, select the toggle on the right.

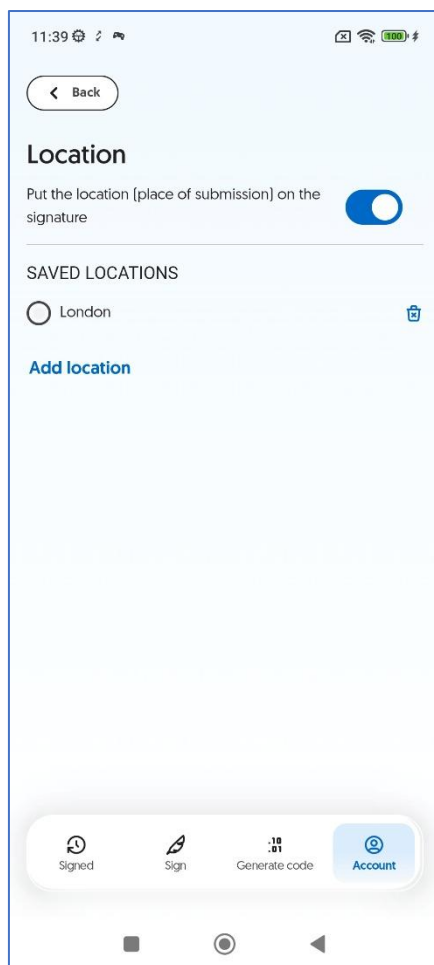


In addition to enabling this option, add a location to the list and select the location that should appear in the visualization and signature structure. To do so, select Add Location. A form appears where you can enter your own location.

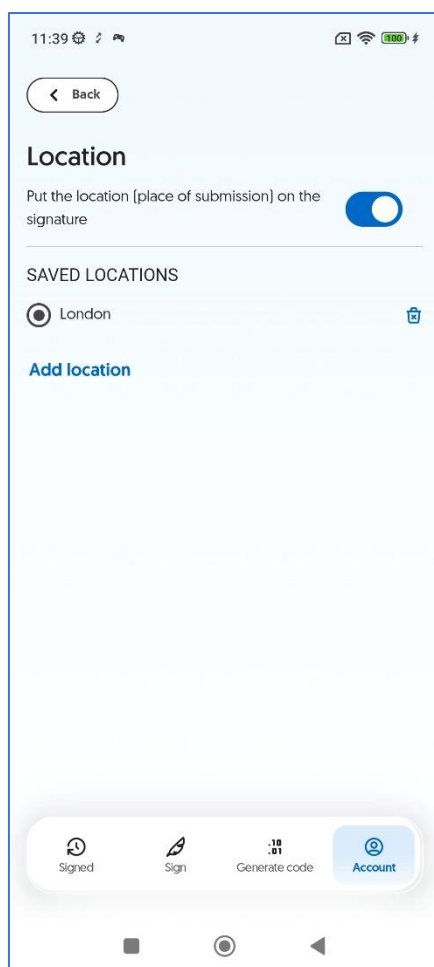




After entering your own location, select Add. The selected location appears in the list.

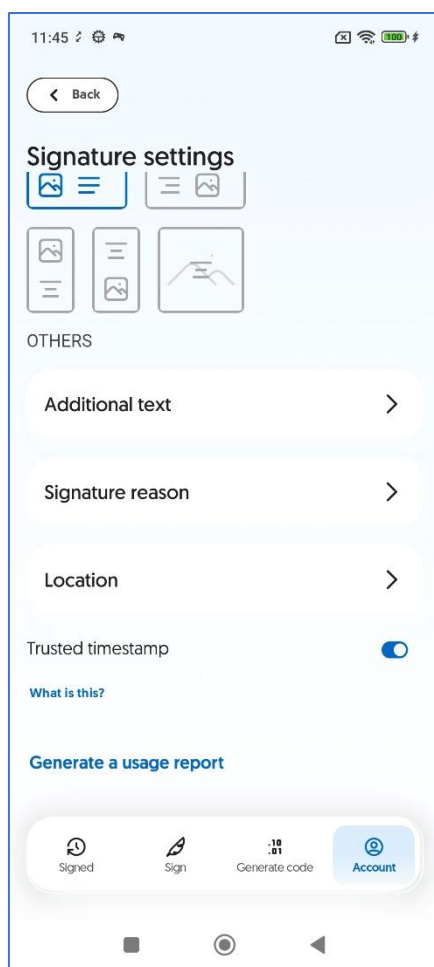


To set the selected location as the one included in the visualization and signature structure, also select the option button to the left of that location.



7.1.4.6. “Trusted Timestamp” Option

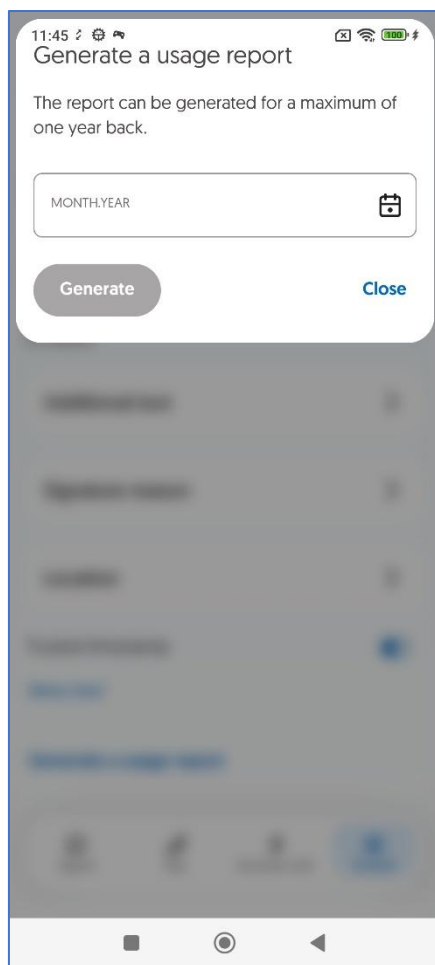
Enabling this option adds a trusted timestamp to the signature structure, indicating the date and time when the document was signed.

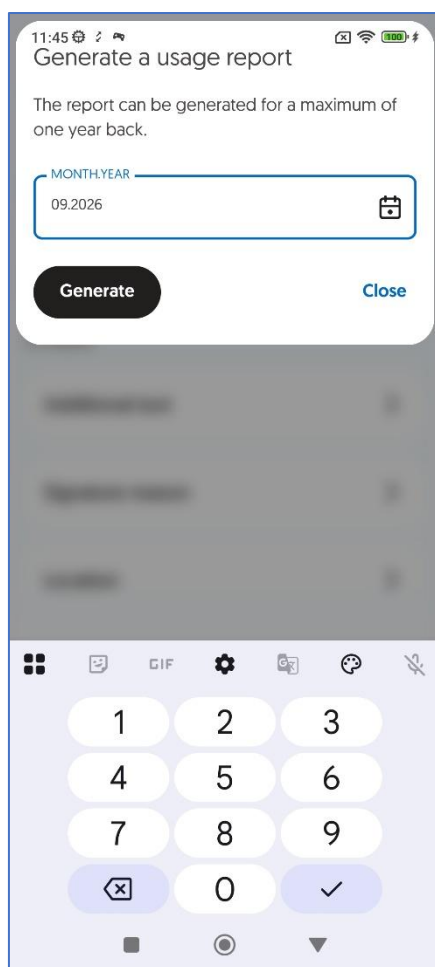


7.1.4.7. Generating a Summary Account Usage Report for a Selected Month

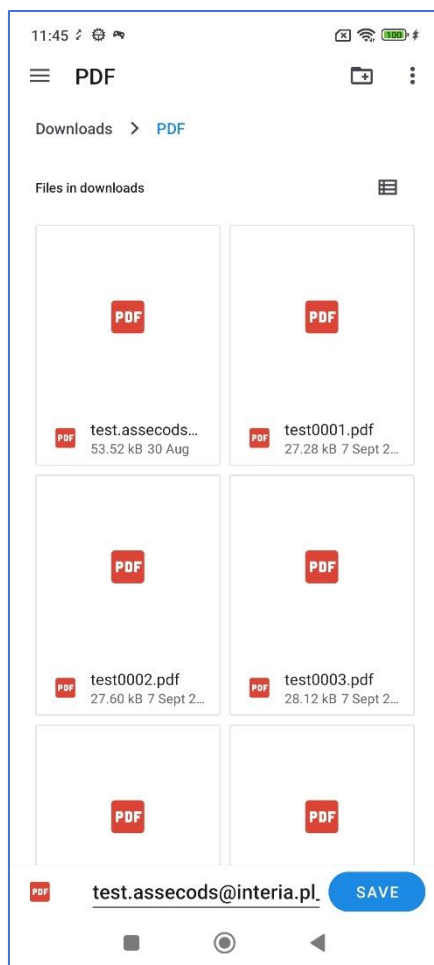
This option generates a PDF summary report of events occurring on the account during a selected month. Reports can be generated for a selected month up to one year in the past.

To generate a report, select this option. A form appears where you can select the month covered by the report.





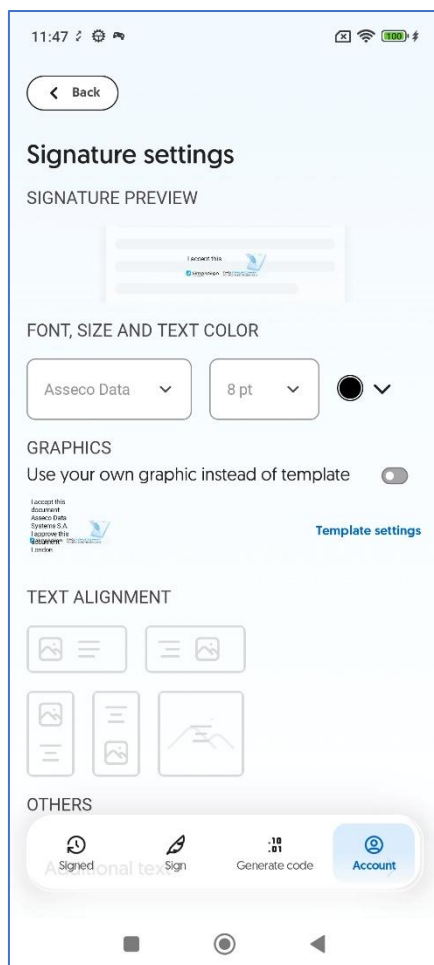
After selecting the appropriate month, select Generate. Report generation begins. After a short time, the report is generated and the system save dialog appears; select the location where the generated report should be saved.



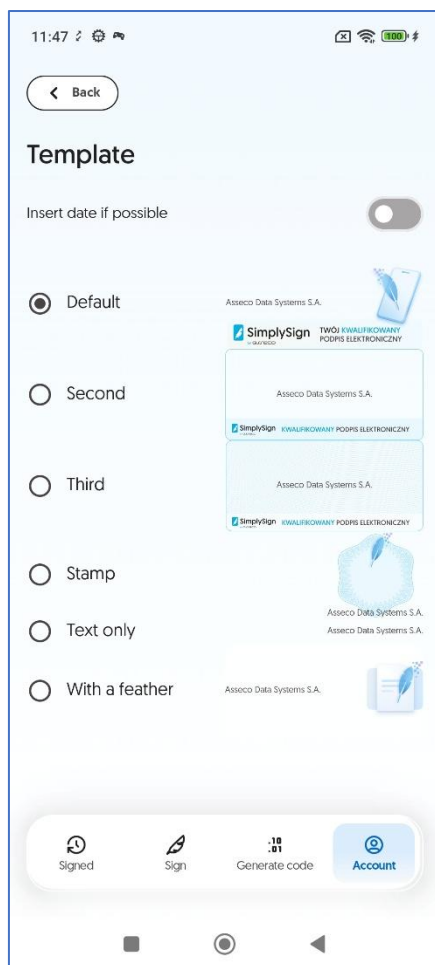
After selecting Save, the report is saved in the selected location on the device.

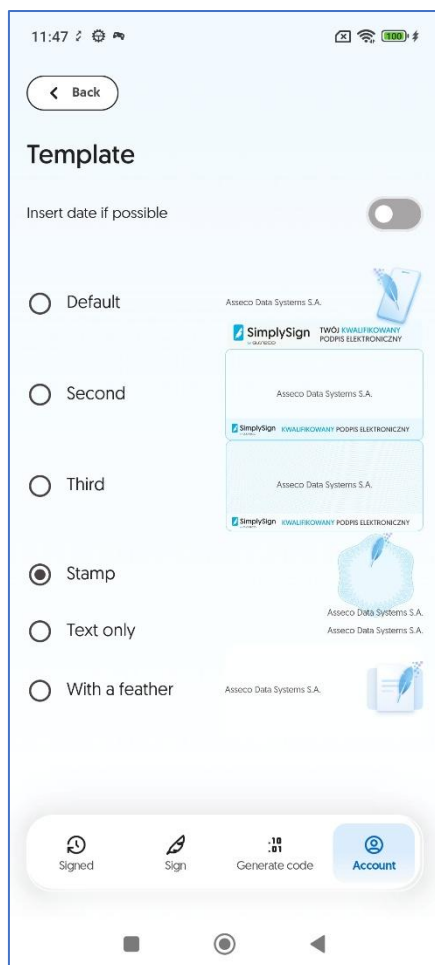
7.1.4.8. Using Default Templates and Adding the Date to the Visualization

When Use a Custom Image Instead of Templates is disabled, you can use one of several default templates built into the application for the visualization. In this case, Signature Settings displays Template Settings instead of Image Settings.

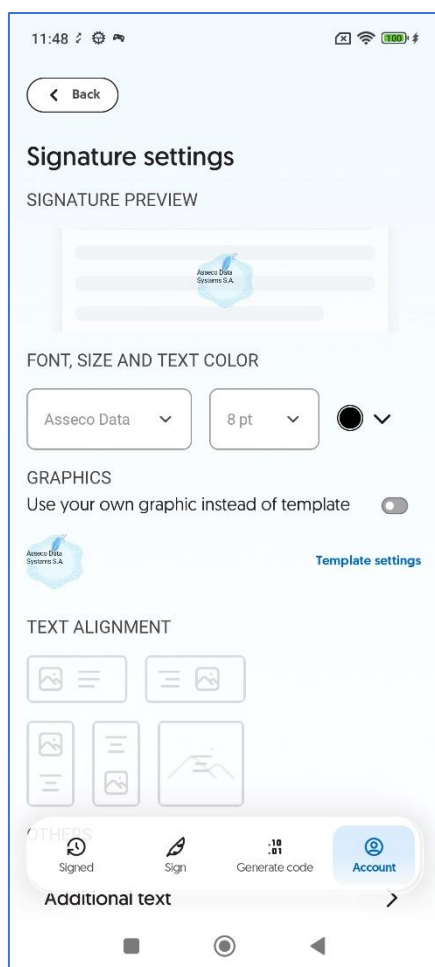


To select one of the built-in templates, select Template Settings. The list of built-in templates appears.

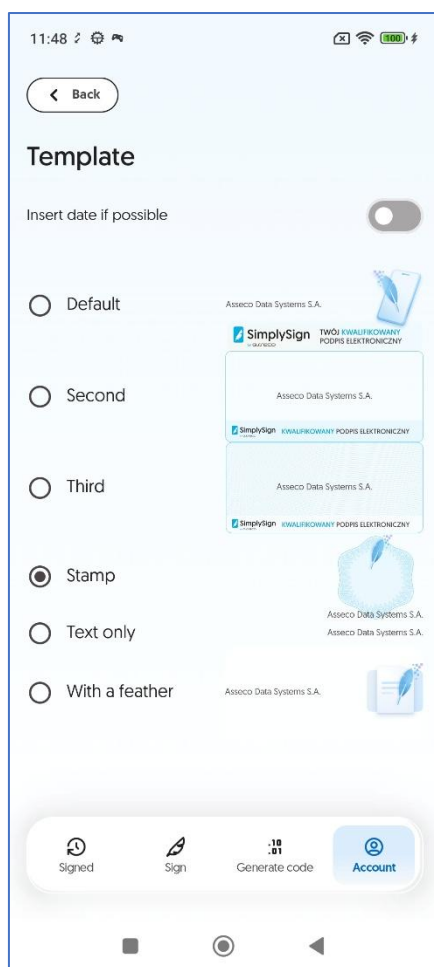




After selecting a template and returning to the settings, the selected template appears on the left side of the settings panel.



The template list also includes Insert Date If Possible. Enabling it adds the signature date to the visualization.



7.1.5. “Application Settings” Option

This option lets you perform the following actions:

- Enable push notifications for the application
- Perform a factory reset of the application

7.1.5.1. Notifications

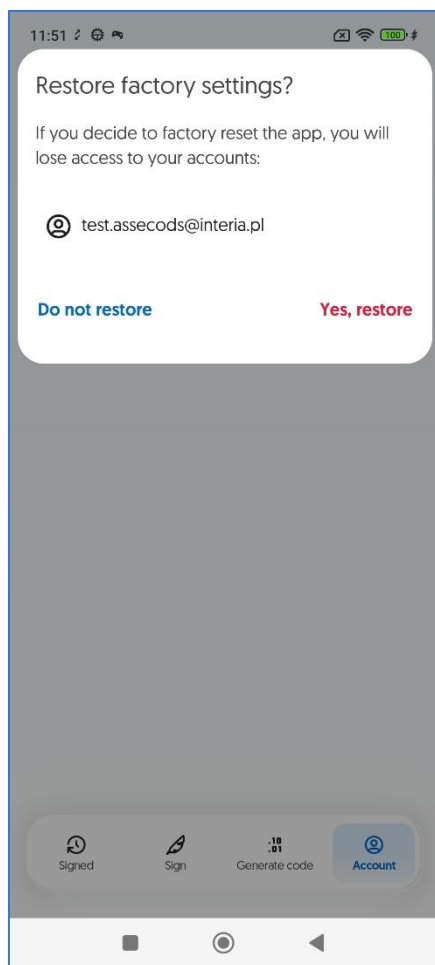
This section lets you configure push notifications for the application. When enabled, a push notification is sent to the application for the following events:

- Generation of an account event report
- Resetting Service Access
- PUK change

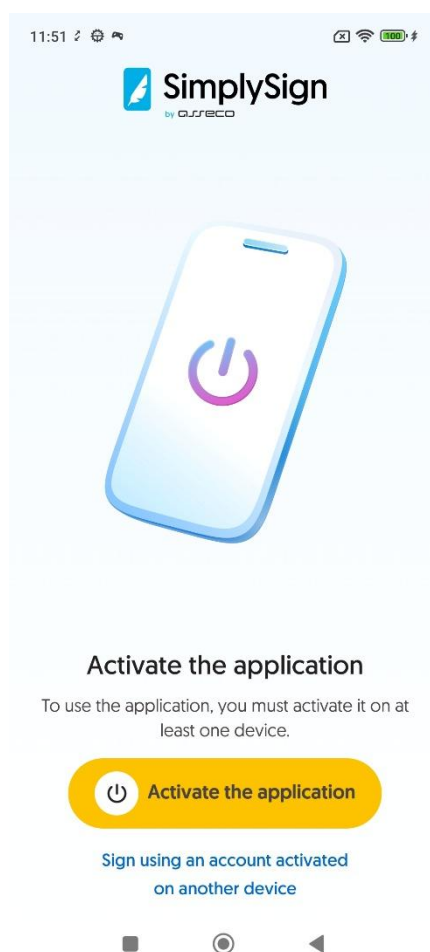


7.1.5.2. Factory Settings

Selecting this option resets the application to factory settings, including clearing active accounts from the application.



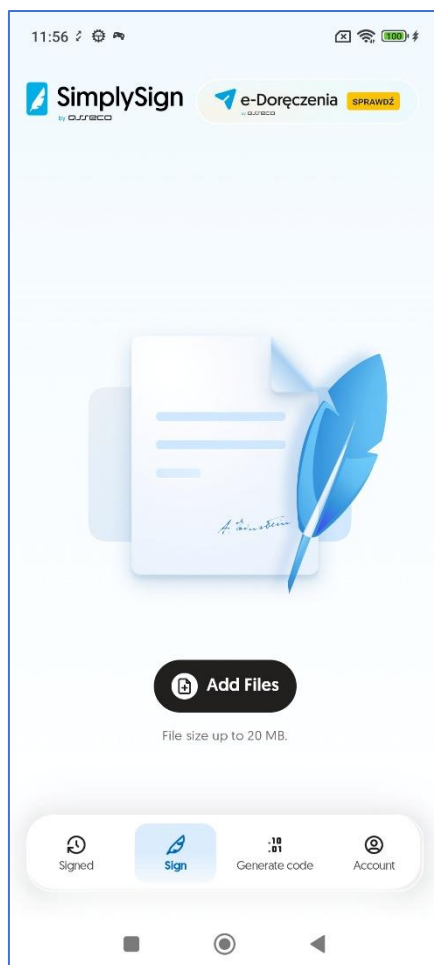
After the factory reset, the application returns to the initial screen shown after installation.



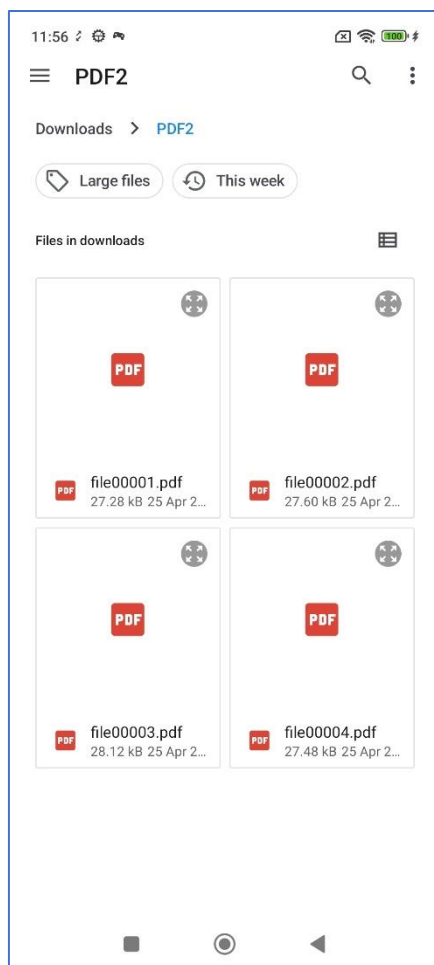
8. Signing Files

8.1. Adding a File to the List of Files to Be Signed

To add a file to the list of files to be signed, sign in to the service. After sign-in, the application opens the Sign tab.

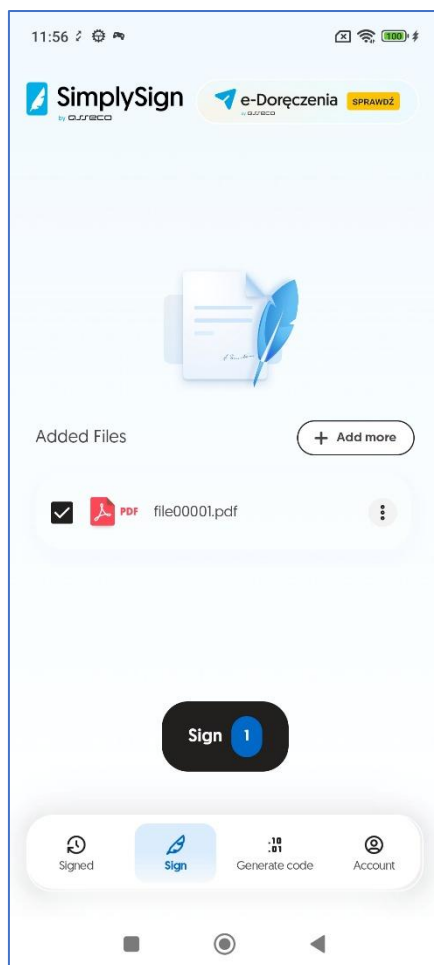


Then select Add Files in the center of the screen. The file browser appears.



In the browser, locate and select the file to be added to the list of files to be signed.

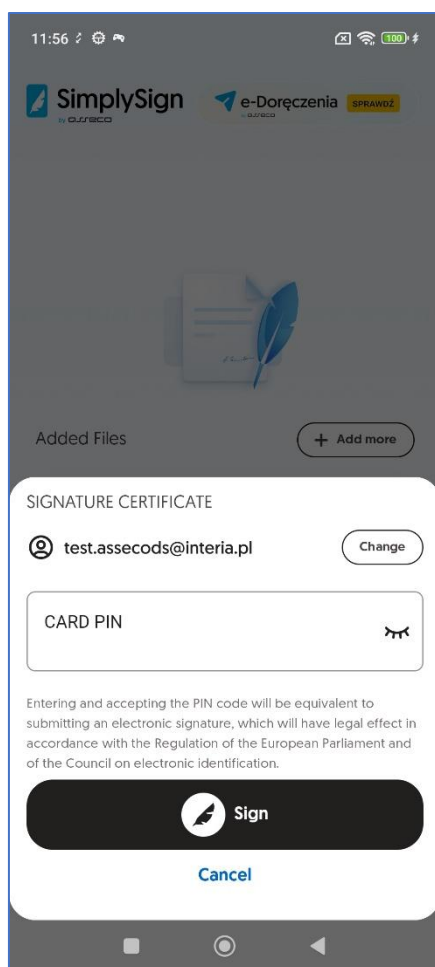
After selection, the file is added to the file list on the Sign tab.



8.2. Starting the File-Signing Process

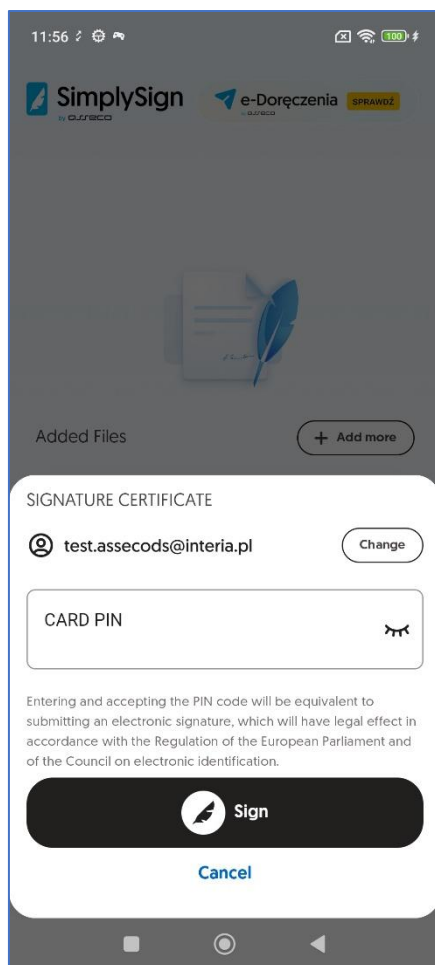
To start signing a file, select the file in the list and select Sign.

The application begins retrieving the user's cards and certificates. A PIN entry window appears. If the user's account contains several certificates, a Change button appears next to the account name, allowing the user to change or select the certificate used to sign the document.

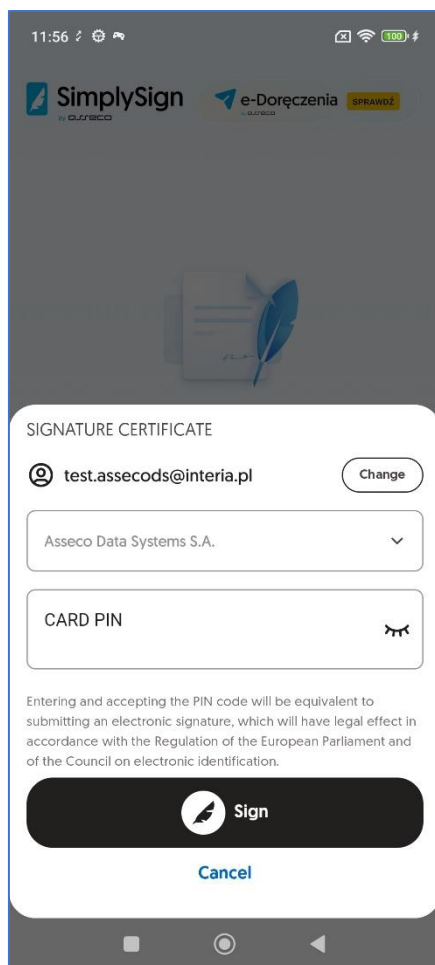


8.3. Selecting a Signing Certificate

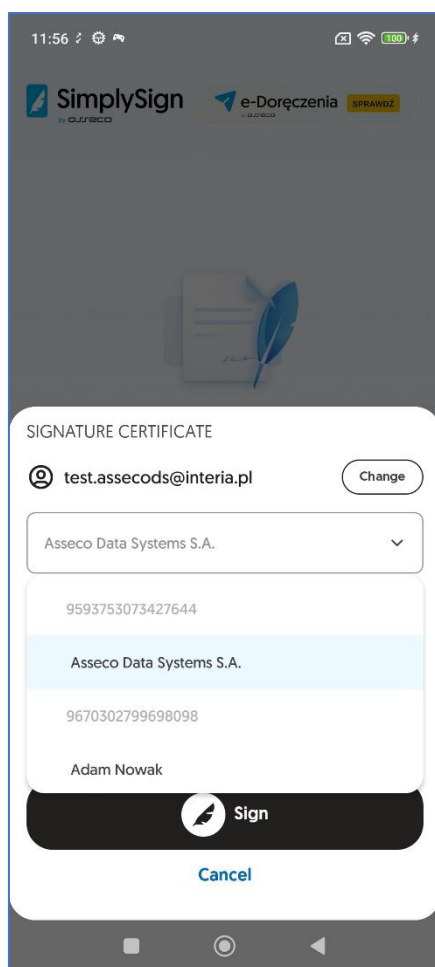
If the signed-in user's account contains several certificates, the PIN entry screen shown after the signing process starts lets the user view and change the selected certificate. The application selects the newest certificate by default. To sign with another certificate, select Change to the right of the account name.



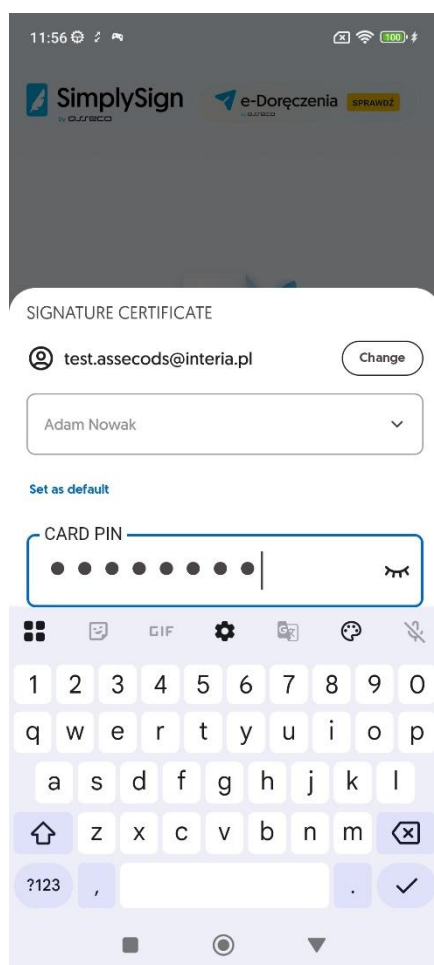
After selecting Change, the application displays the currently selected default certificate.



After selecting the down-arrow icon next to the certificate name, the application displays the available cards and the certificates on them. The user can select the specific certificate to use for signing the document.

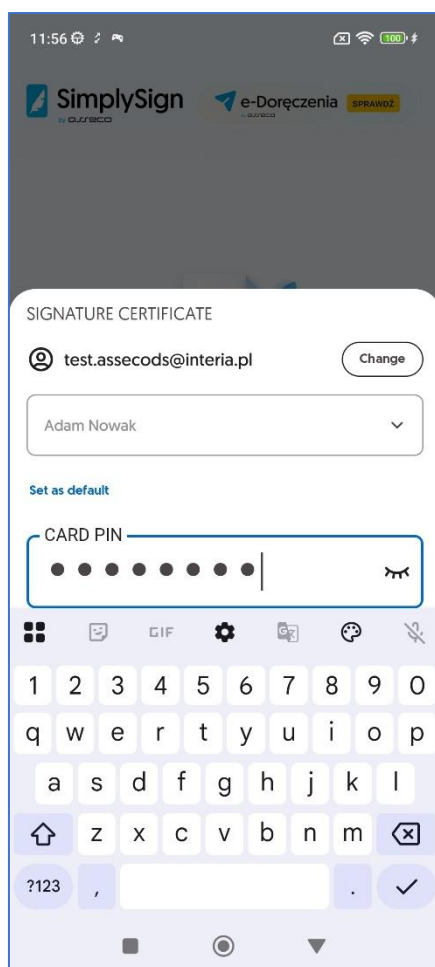


After selecting the certificate, enter its PIN.



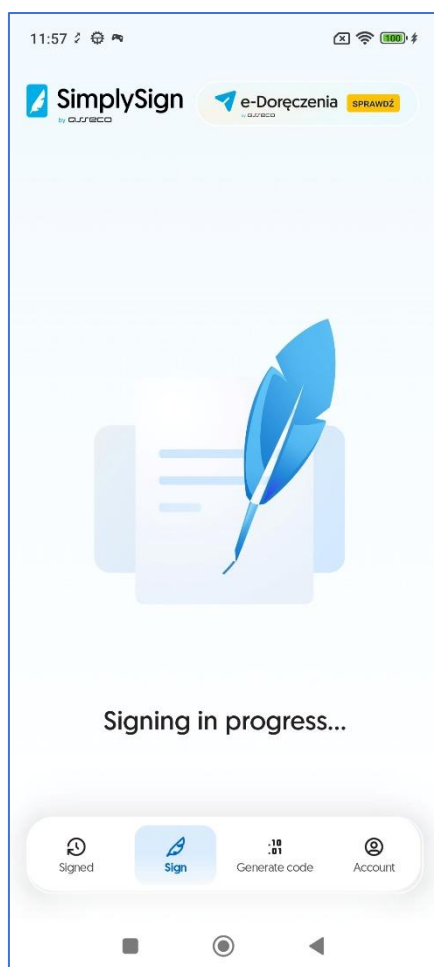
8.4. Entering the PIN for the Selected Signing Certificate

After selecting the certificate, enter the PIN for that certificate.

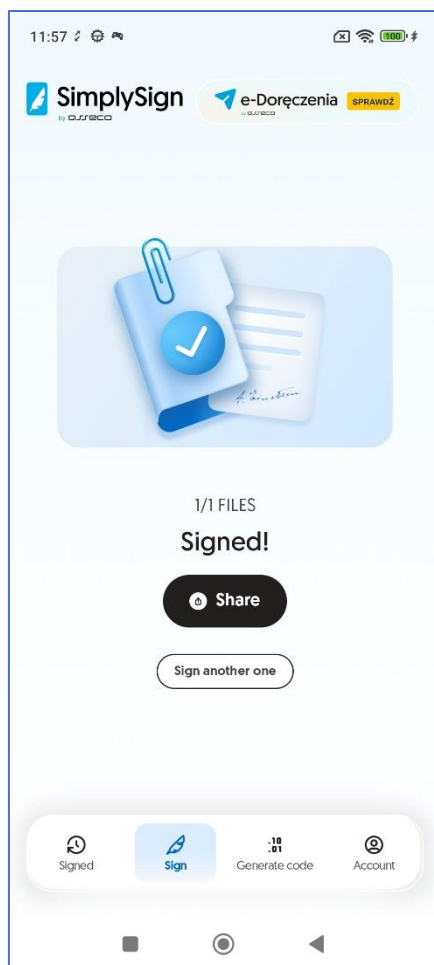


8.5. Signing a File

After entering the PIN and selecting Sign, the selected file-signing process begins. An animation on the screen represents the signing process.



When signing is complete, a summary appears.



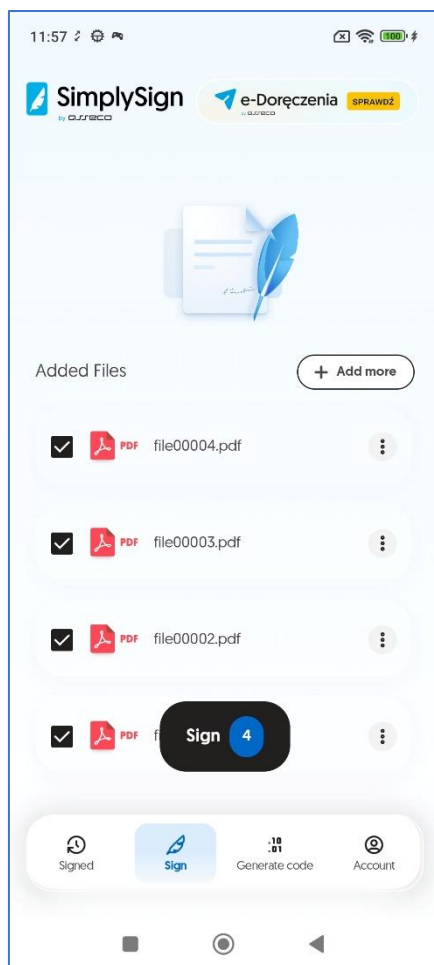
The following options are available on the summary screen:

- Share – starts sending the signed file to external applications;
- Sign More – returns to the Sign tab.

9. Signing Multiple Files at Once

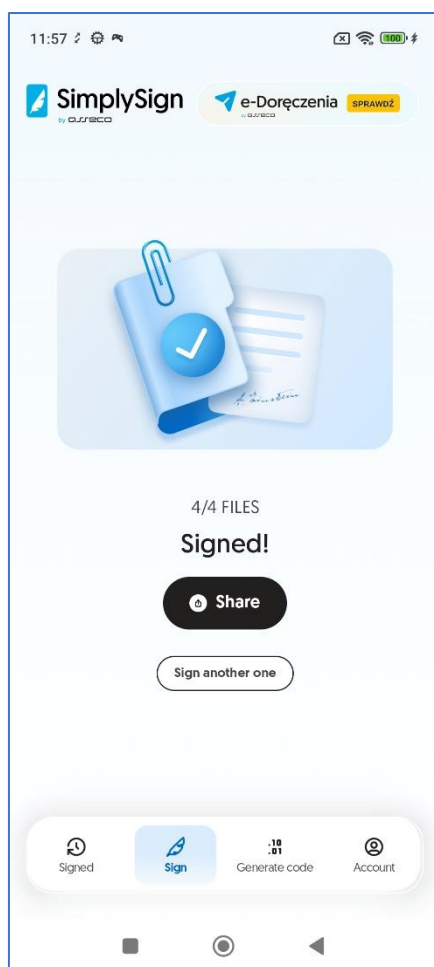
SimplySign can sign several files at once after the PIN for the signing certificate is entered only once.

To sign several files at once, add the files to the list of files to be signed.



After adding and selecting the files, start the signing process as described in the previous subsection.

All selected files are signed. After they are signed successfully, an appropriate report appears.



The summary contains the options described in the previous section.

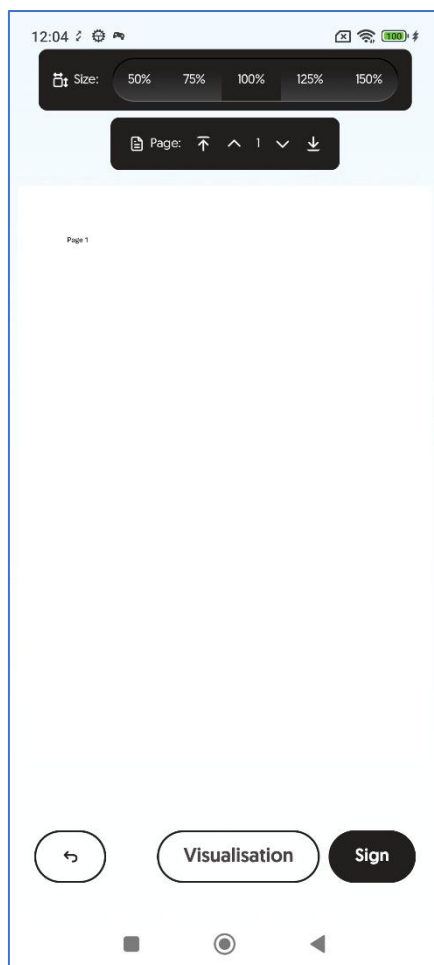
10. Creating a Signature with a Visualization

SimplySign can create a signature with a visualization.

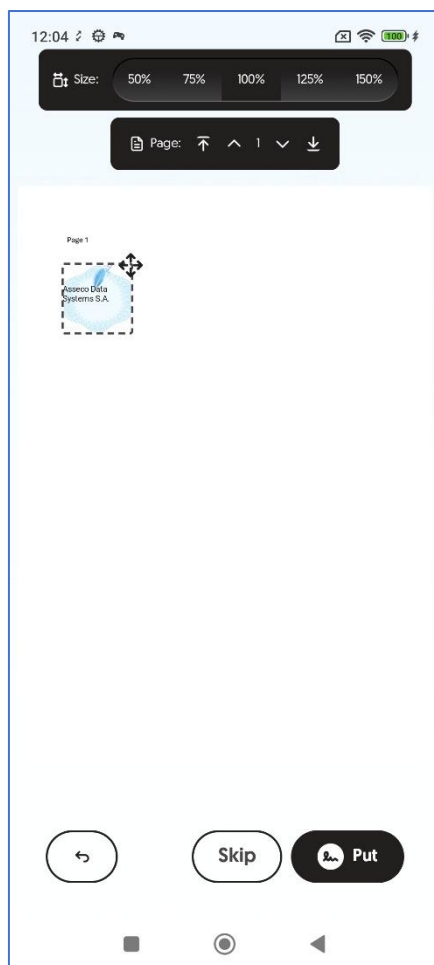
The visualization contains the image selected by the signer in the application options (Template Settings or Use a Custom Image Instead of Templates). Depending on the settings, it may also contain the current date and the reason for signing. In the settings, either configure a custom image or select a predefined template; in Template Settings, select the option to include the current signing date in the visualization.

To create a signature with a visualization, select the document name in the list of files to be signed. A preview of the selected file opens, where you can add the visualization.

At the top of the preview is a navigation bar for quickly moving through the document pages.



Then select Visualization. A movable signature sample appears in the file preview. Move it to the desired location.



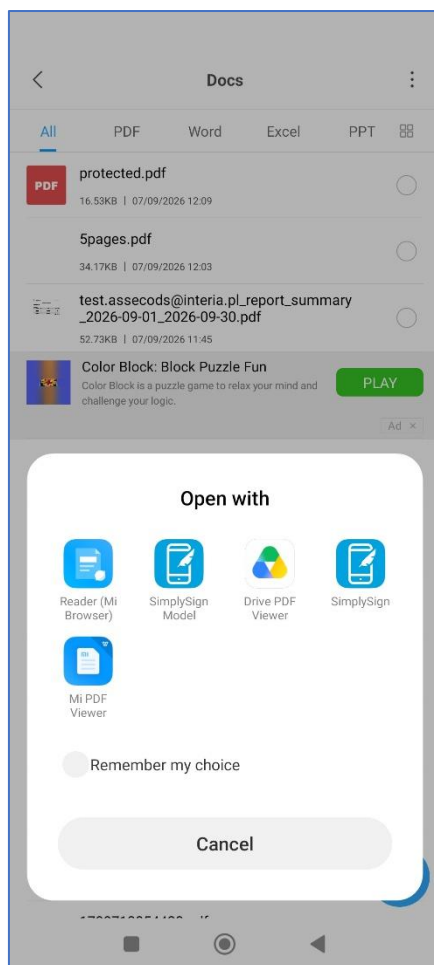
Then select Place. The standard signing process described in the previous sections begins for the selected file.

The following is an example PDF file containing a signature with a visualization.

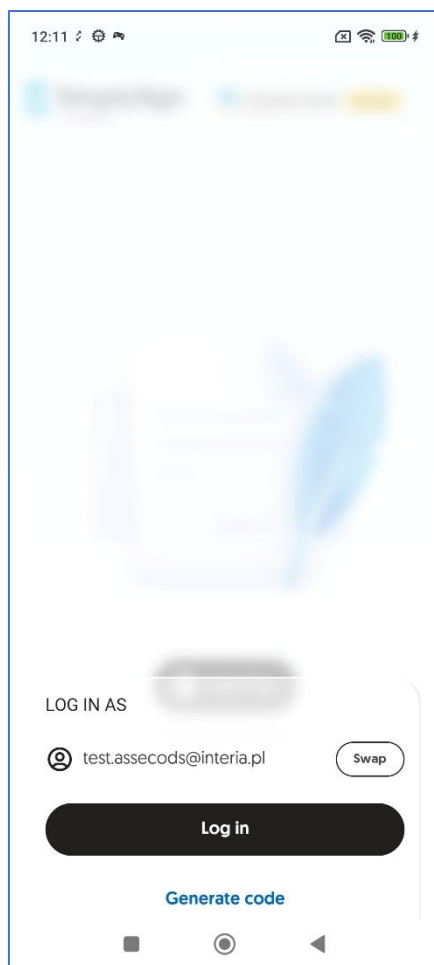
11. Importing Files from External Applications

A PDF document can be imported from an external application directly into the list of files to be signed.

Display the options for the selected file. SimplySign appears in the list of available applications.



Select SimplySign. The SimplySign application starts and immediately opens its start screen.



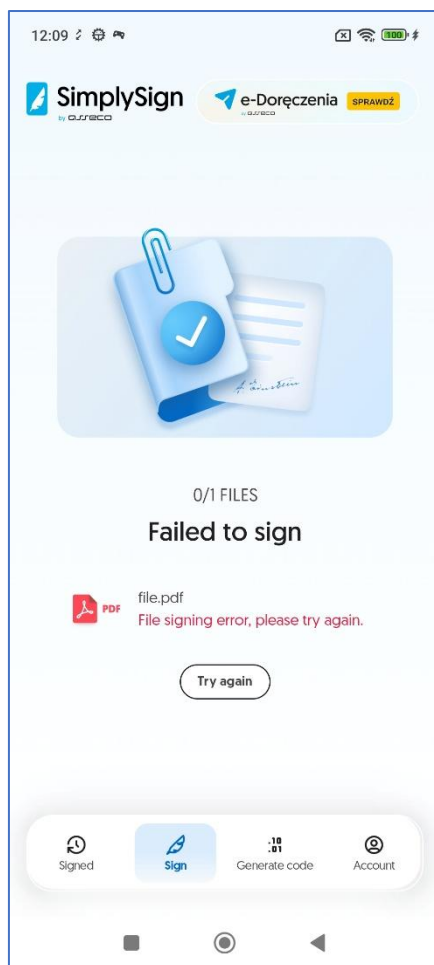
Sign in. The selected file appears in the list of files to be signed and can be signed.

12. Handling Errors While Signing Files

12.1. Invalid PDF File

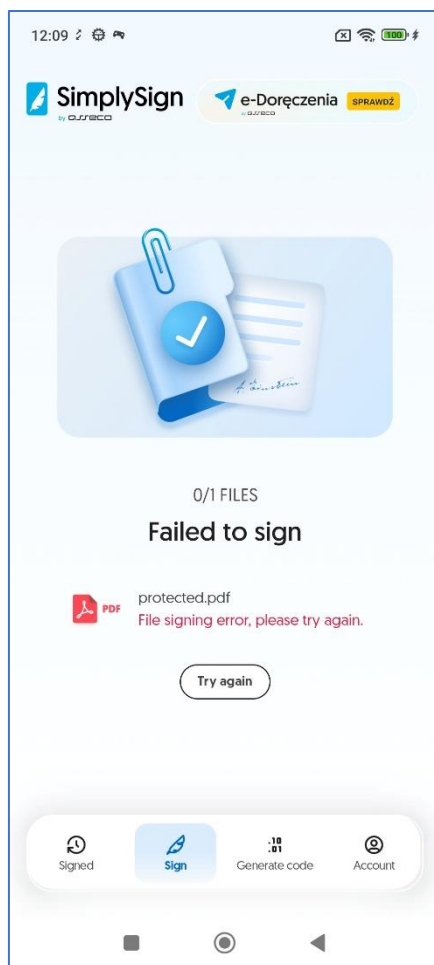
If an attempt is made to sign a structurally invalid PDF file, after the PIN is entered and confirmed an error appears stating: File signing error, try again.

.



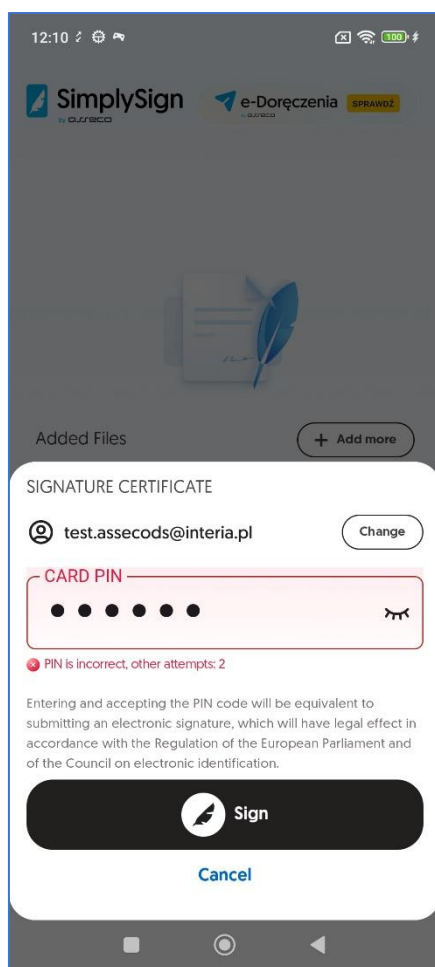
12.2. Protected PDF File

If an attempt is made to sign a PDF file protected against modification, after the PIN is entered and confirmed an error appears stating: The selected files are not valid PDF files.



12.3. Invalid PIN for the Signing Certificate

If an invalid PIN is entered and confirmed, an error appears stating that the entered PIN is invalid, together with the number of remaining PIN-entry attempts.



12.4. Blocked Card

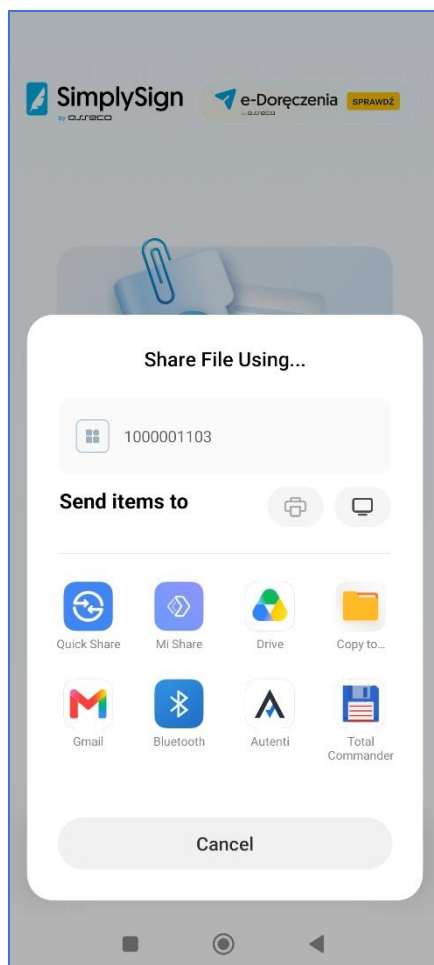
If a card is blocked (its PIN is blocked), this is indicated in the card list by a red card icon at the end of the header containing the card name.

The following example shows a blocked card.

13. Managing Signed Files

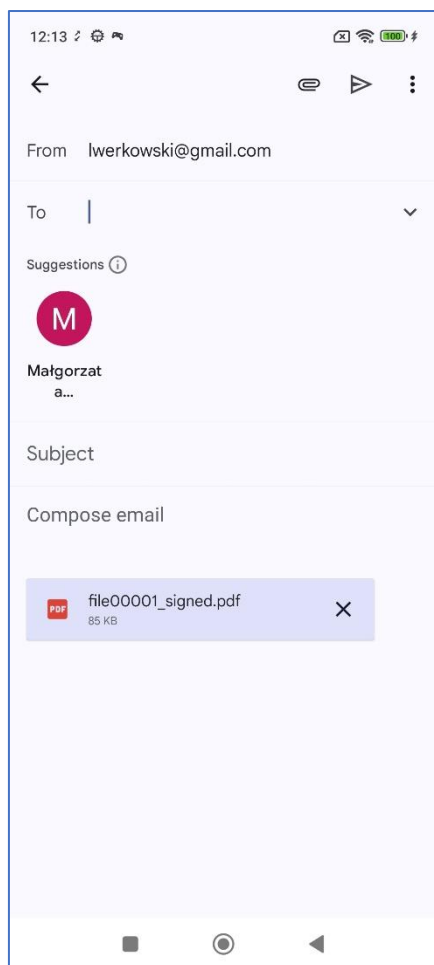
13.1. Sending Signed Files by Email

Signed files can be emailed to another user from the Signed tab. First select the files to be sent, then select Share. A list of applications to which the signed file can be transferred appears.



In this example, Gmail was selected. A window opens for preparing an email message.

The previously selected signed files appear as attachments. Enter the recipient's email address, the subject, and the message content.

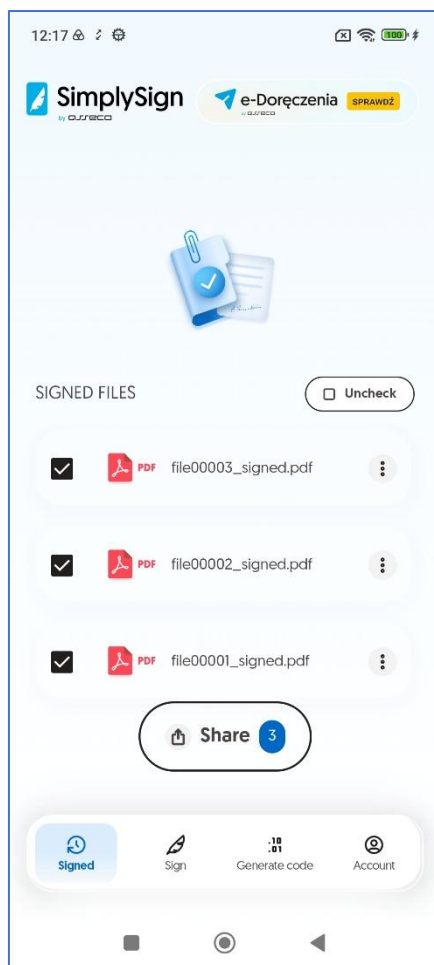


After composing the message, select the right-arrow button. The message is sent and the application returns to the Signed tab. The sent files are deselected.

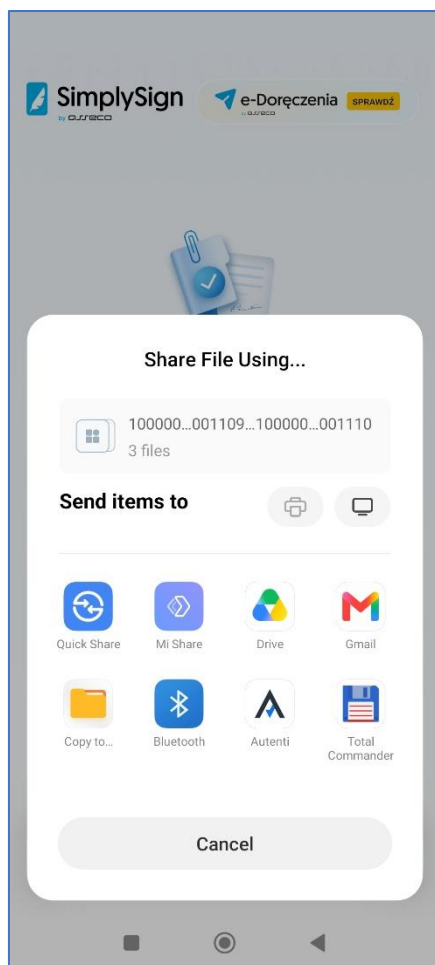
13.2. Saving Signed Documents to Google Drive

Signed files can be sent from the Signed tab to another user's virtual drive.

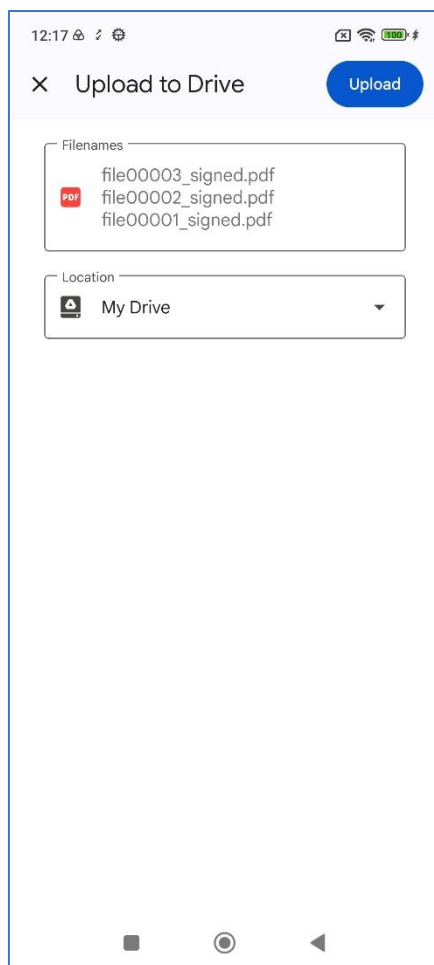
First select the files to be sent.



After selecting the files, select the cloud icon with an upward arrow. A window appears where you can specify the destination for the files.

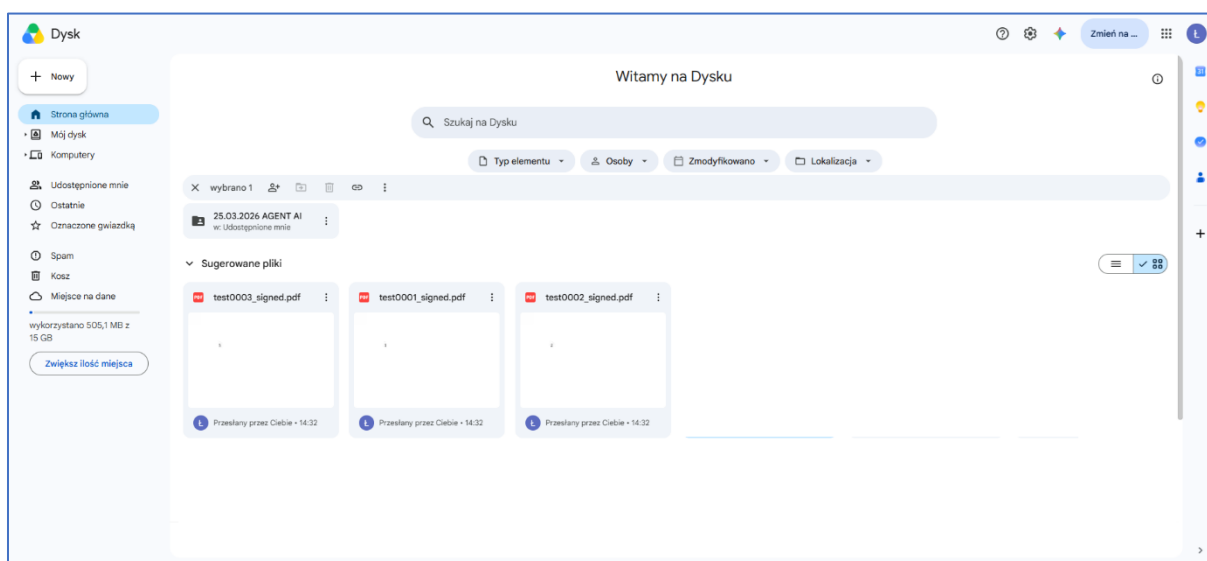


Then select Drive. A screen appears where you can configure the parameters of the user's drive to which the signed files will be sent.



After configuring the destination drive, select Upload. The files are saved to the specified drive.

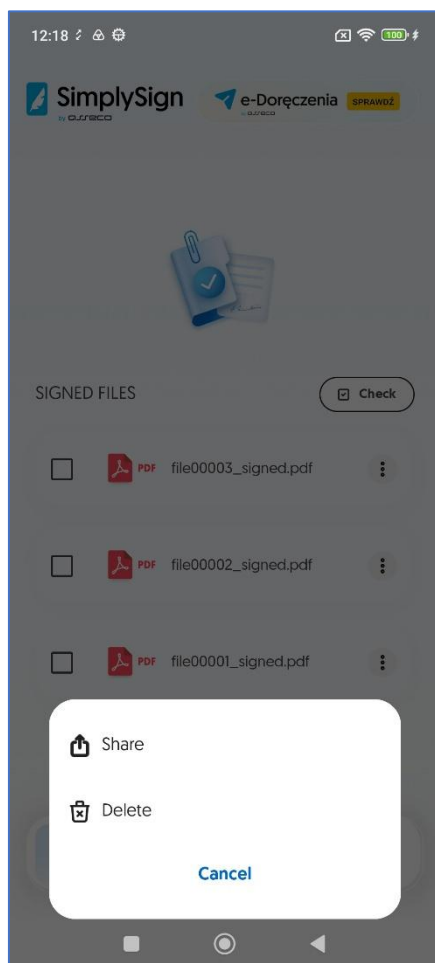
The drive owner can see them after signing in to their Google account.

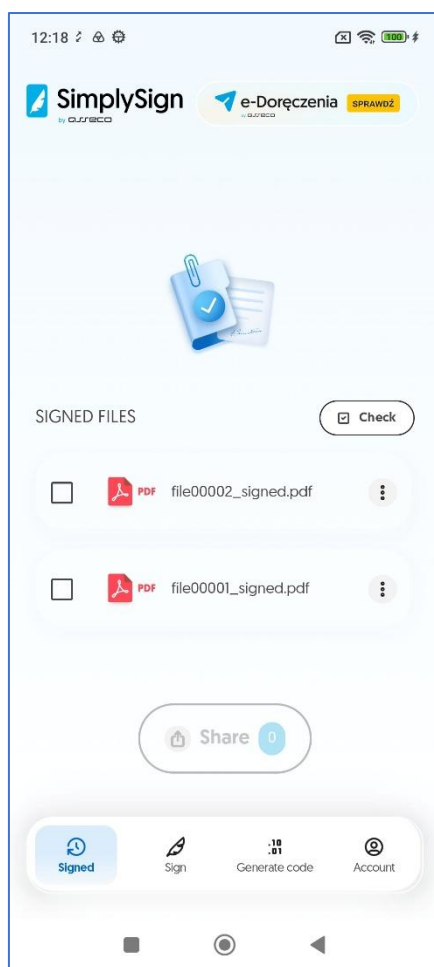


14. Deleting Files

Deleting files from the list of files to be signed and from the list of signed files works in the same way.

For the selected file, open the context menu by selecting the three vertical dots on the right side of the screen. Select Delete from the context menu; the file is removed.





15. Integration with the e-Delivery System

The application is integrated with the e-Delivery system. It can be used to activate the e-Delivery service and sign in to an e-Delivery mailbox to view its status. Mailbox activation and sign-in are described below.

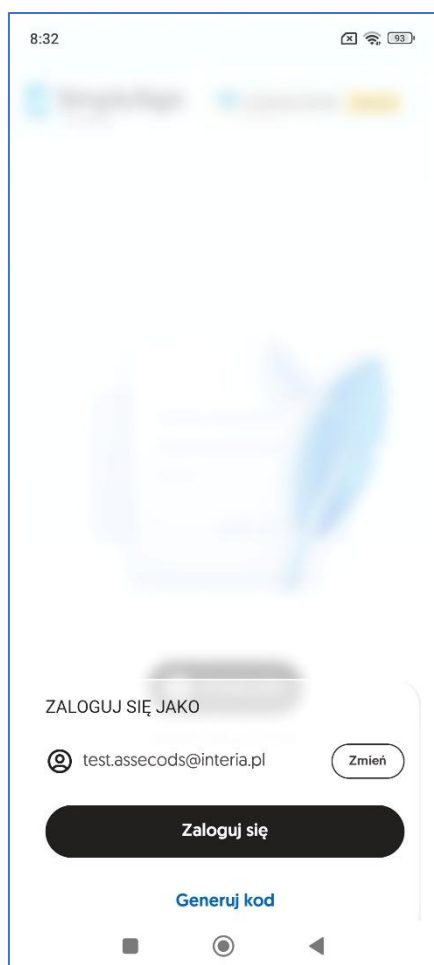
15.1. Activating an e-Delivery Mailbox

In most cases, an e-Delivery mailbox is activated by users who already have an active SimplySign application. Such users usually already have an active qualified certificate and use it to create an e-Delivery mailbox in Panel Certum, which must then be activated. The procedure for this case is described in subsection 15.1.1.

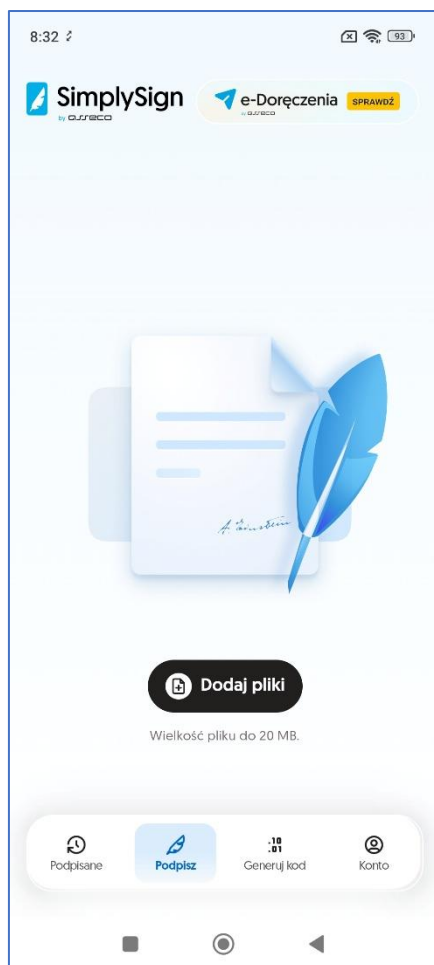
For users who do not yet have an active application, mailbox activation is the same as activating SimplySign using authentication data, as described in section 6.2.1. This activates both the SimplySign application and the e-Delivery mailbox.

15.1.1. Activating an e-Delivery Mailbox When SimplySign Is Active

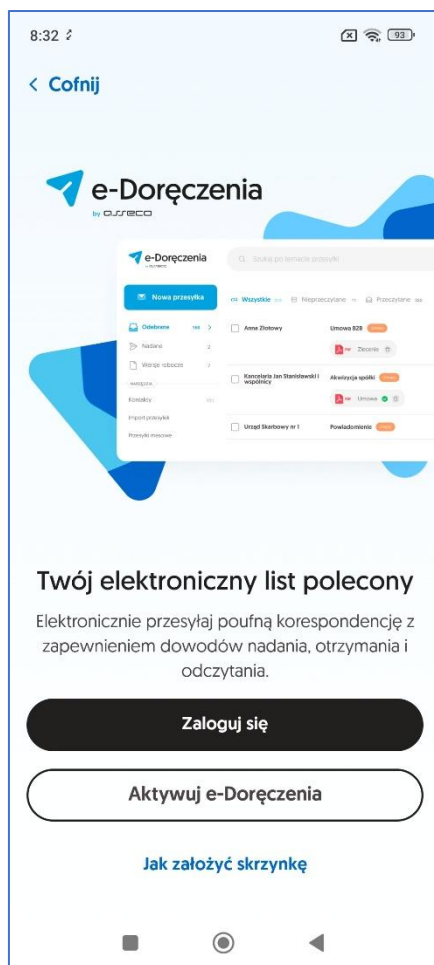
To begin activating an e-Delivery mailbox, start SimplySign.



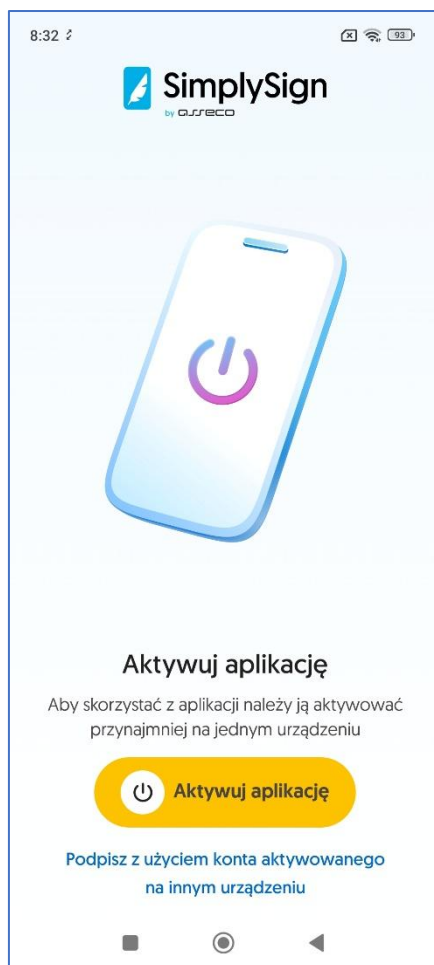
Then sign in to the application.



Then select e-Delivery in the upper-right corner of the screen. An information page about the e-Delivery service appears, with options to activate e-Delivery or sign in to an active mailbox.



Then select Activate e-Delivery. A screen appears where you can begin activating the e-Delivery service.

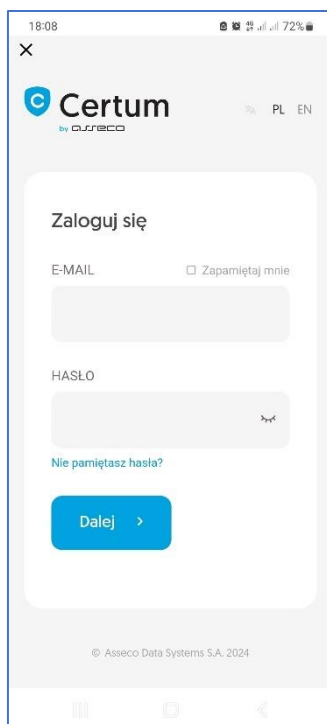


In the next step, select Activate Application. A window appears where you must enter the user's login.



The screenshot shows a mobile application interface for email verification. At the top, the status bar displays the time 8:32, signal strength, Wi-Fi, and battery level at 93%. Below the status bar is a blue header with a back arrow and the text 'Cofnij'. The main content area features a large blue envelope icon. Below the icon, the text 'Podaj adres e-mail' is displayed, followed by a subtext: 'Powinien być to adres użyty podczas składania wniosku o certyfikat'. A text input field contains the email address 'jan.kowalski@example.com'. At the bottom, there is a yellow button labeled 'Dalej >' and a blue link labeled 'Inne metody aktywacji'. The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps icons.

In the E-mail field, enter the email address used as the user identifier, then select Next. If the identifier is correct, the application opens the Panel Certum sign-in screen to synchronize SimplySign with e-Delivery.



On the sign-in screen, enter the correct Panel Certum login and password, then select Next. The application then asks for three randomly selected items of the user's personal data.



8:32   

[< Cofnij](#)

Dane uwierzytelniające

By zakończyć aktywację potrzebujemy jeszcze zweryfikować Twoje dane:

NUMER DOKUMENTU TOŻSAMOŚCI

DATA URODZENIA

IMIĘ

[Dalej >](#) [Potrzebujesz pomocy?](#)

Then enter the correct personal data.



8:32   

[< Cofnij](#)

Dane uwierzytelniające

By zakończyć aktywację potrzebujemy jeszcze zweryfikować Twoje dane:

NUMER DOKUMENTU TOŻSAMOŚCI

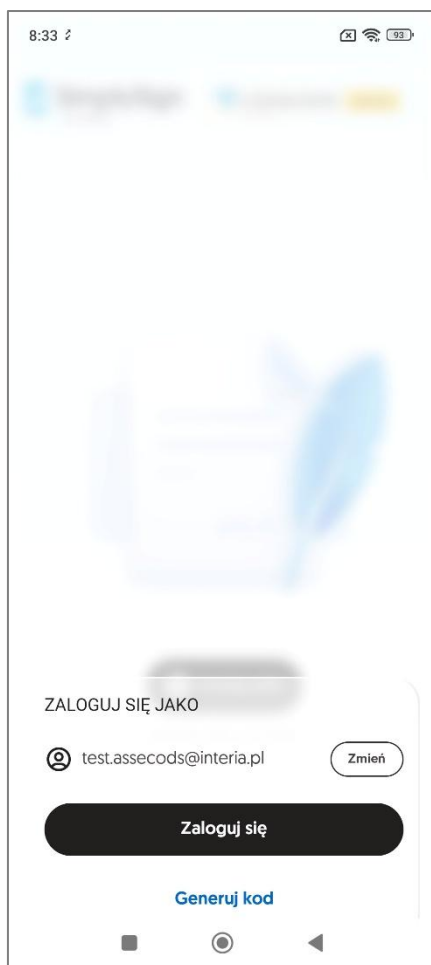
DATA URODZENIA

IMIĘ

[Dalej >](#) [Potrzebujesz pomocy?](#)

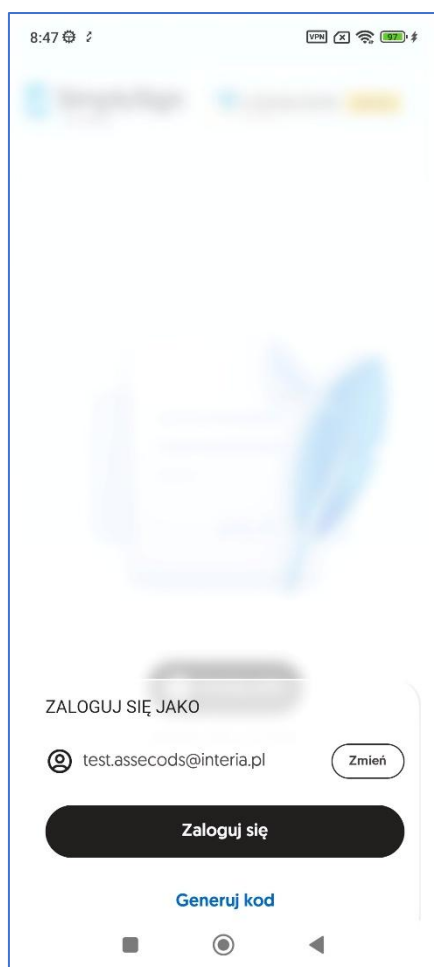
After entering the personal data, select Next. If the data is correct, the application is activated. After the successful-activation message is closed, the application returns to the start screen.



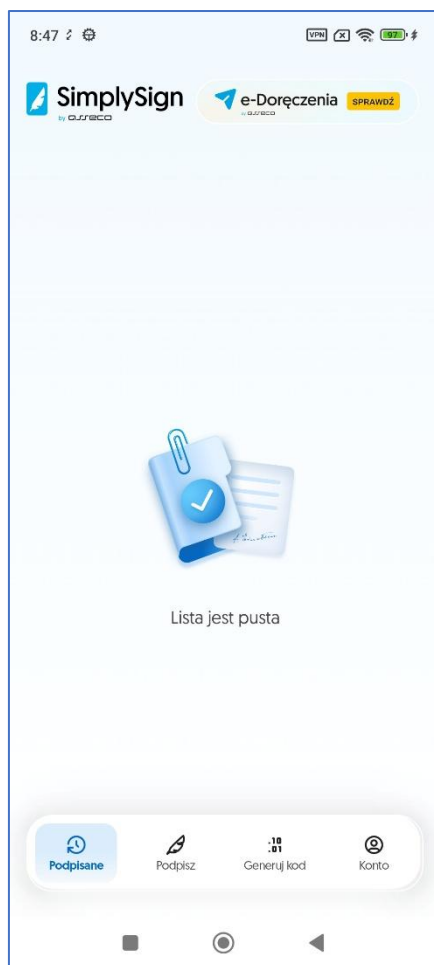
15.2. Signing In to an e-Delivery Mailbox

Signing in to an e-Delivery mailbox takes place in two stages: first with the static Panel Certum password, and then with a one-time code generated by SimplySign. The process for signing in to an active mailbox is described below.

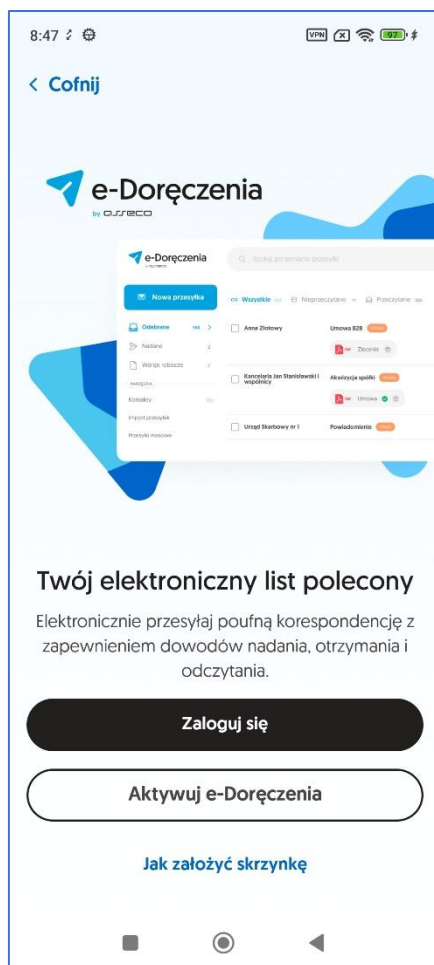
To sign in to an e-Delivery mailbox, start SimplySign.



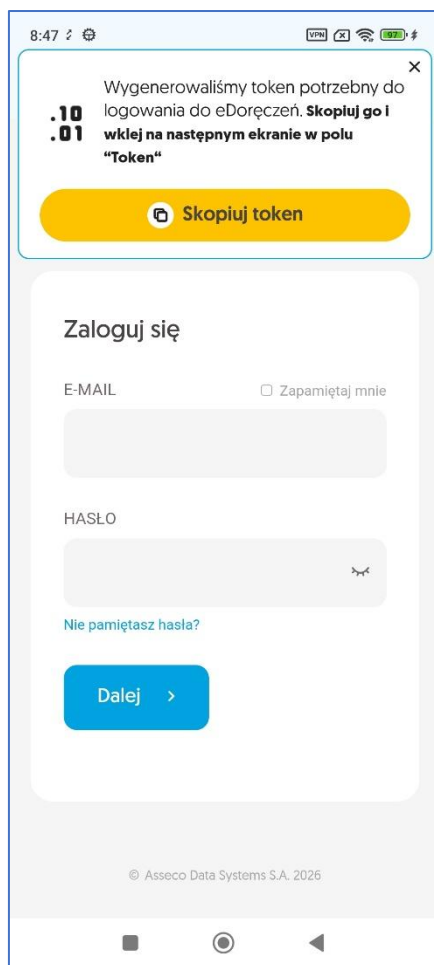
Then sign in to the SimplySign service.



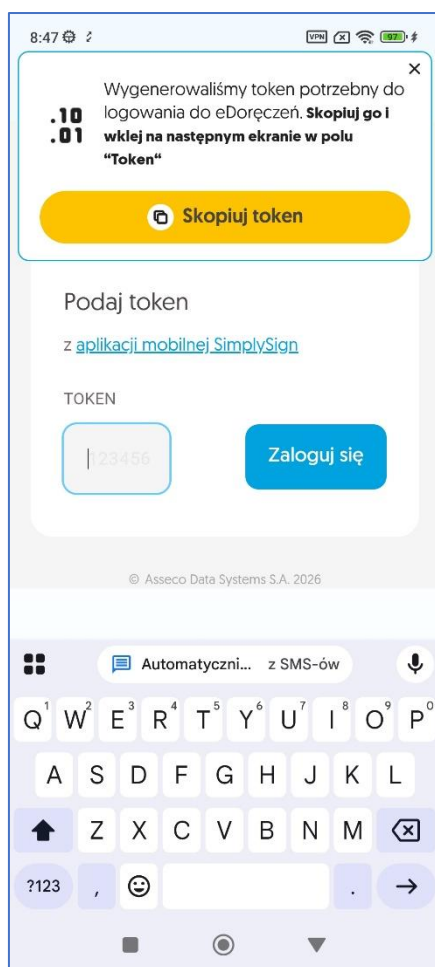
Then select e-Delivery in the upper-right corner. An information page about the e-Delivery service appears, with options to activate e-Delivery or sign in to an active mailbox.



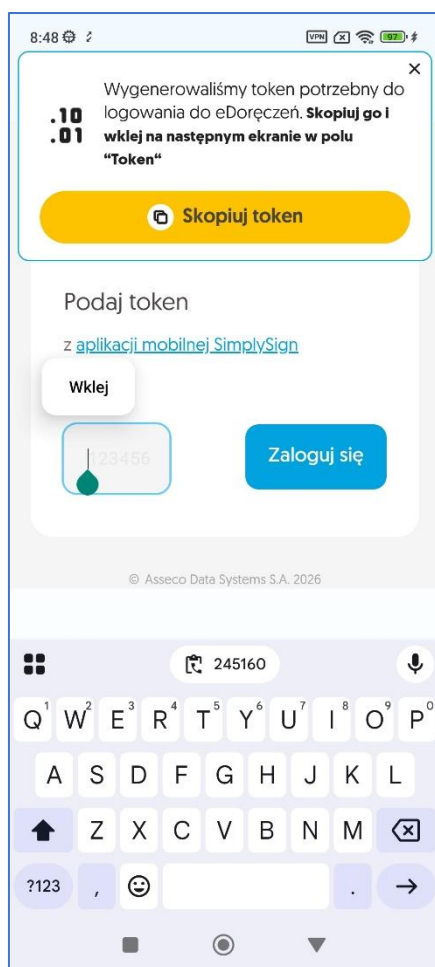
Next, select Sign In. A form appears where you must enter the user's login and static password, the same credentials used for Panel Certum.



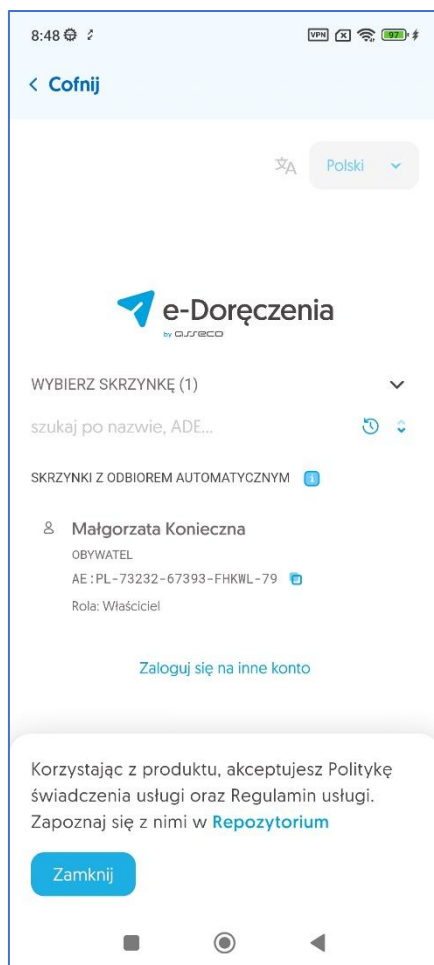
After entering the correct login and password, select Next. A form appears where you must enter the one-time code from SimplySign.



Select Copy Token. The one-time code is copied to the clipboard. Paste the copied token into the token field and select Sign In. You are signed in to the e-Delivery mailbox.



In the next step, select the mailbox.



After selecting the mailbox, its contents are loaded.

You can now close the overlay used to copy the token and begin browsing the e-Delivery mailbox.

