User manual

SECUREDOC
v 2.0

Version 1.4

Table of contents

1. Program Information

SecureDoc 2.0 is an application designed to create and verify electronic signatures with an option of signing with a timestamp. Additionally, you can use the SecureDoc 2.0 application to perform the Certificate Renewal process (only for physical signatures).

Application offers the following electronic signature formats: PAdES-BES, PAdES-T, XAdES-BES, XAdES-T in Detached, Enveloping and Enveloped types.

2. Minimal requirements

- MacOS Catalina (10.15) or newer.
- Internet connection (required for ECSigner cloud signature, timestamping, verification and certificate renewal)

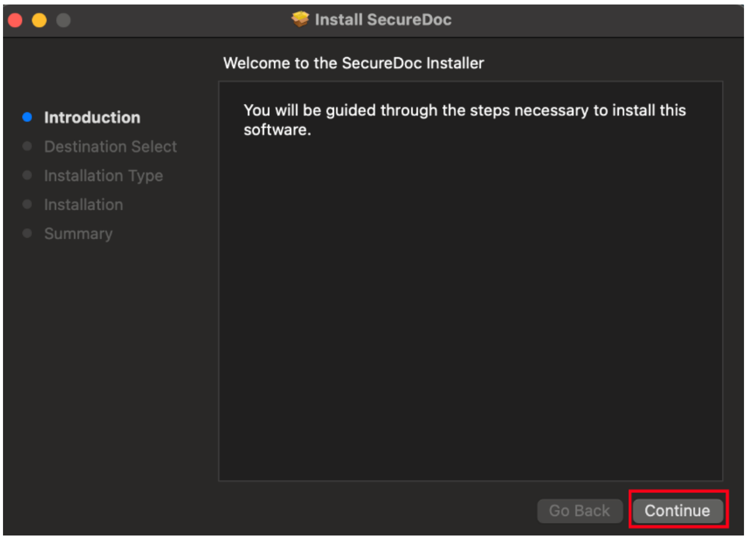
In order to use the electronic signature in SecureDoc app, you must also install:

- Cryptographic card management application - **Charismathics Smart Security Interface** – if using a physical card (USB reader + card).
- **ECSigner** application – if using the ECSigner cloud signature.

3. Installation process

Proceed to the eurocert.pl website and download ***SecureDoc 2 - application to create and verify an electronic signature***.

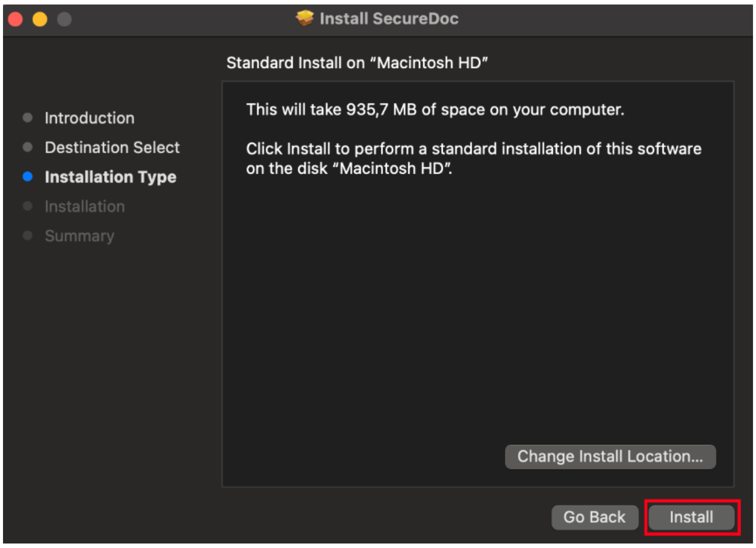
After downloading and running the installer proceed with the following steps:



Install SecureDoc

Welcome to the SecureDoc Installer

You will be guided through the steps necessary to install this software.

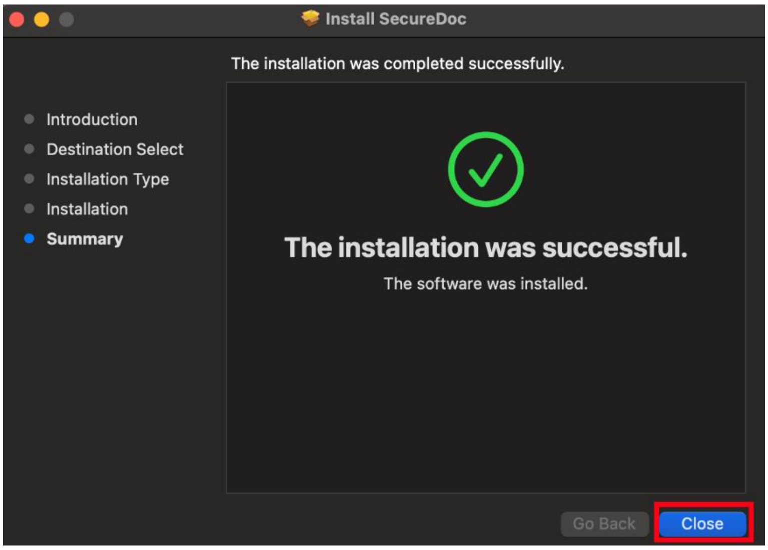


Install SecureDoc

Standard Install on "Macintosh HD"

This will take 935,7 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".



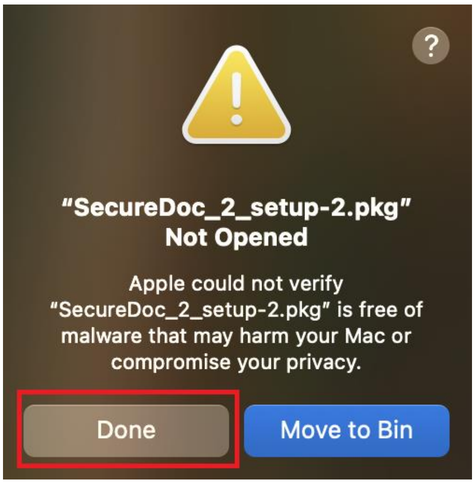
Install SecureDoc

The installation was completed successfully.

The installation was successful.

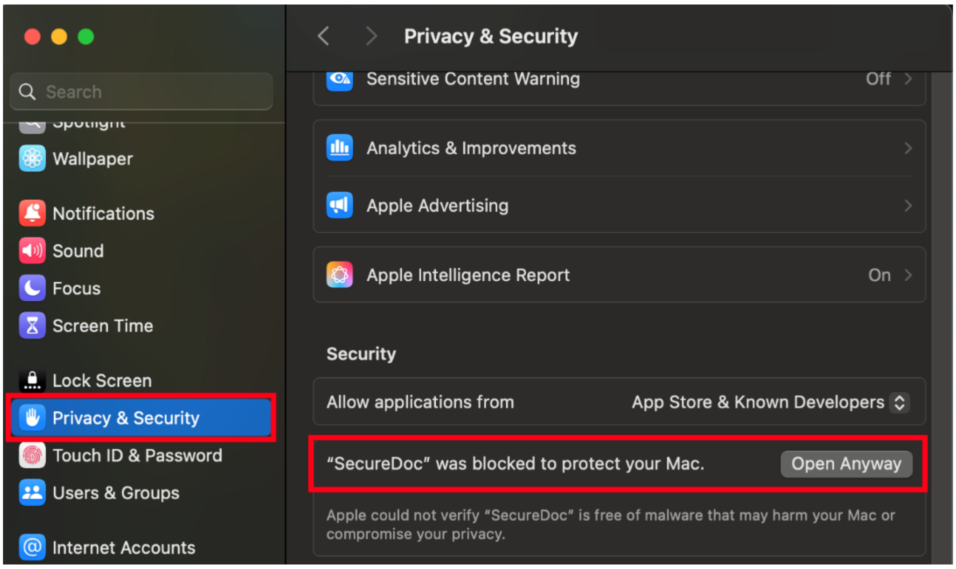
The software was installed.

After completing this step, the application will be ready to use. If, however, the following message appears when launching the installer, indicating that it has been blocked by Apple, click **Done**, then go to **System Settings** → **Privacy & Security**, and click **Open Anyway** in the **Security** section.



"SecureDoc_2_setup-2.pkg" Not Opened

Apple could not verify "SecureDoc_2_setup-2.pkg" is free of malware that may harm your Mac or compromise your privacy.



Privacy & Security

Sensitive Content Warning Off

Analytics & Improvements

Apple Advertising

Apple Intelligence Report On

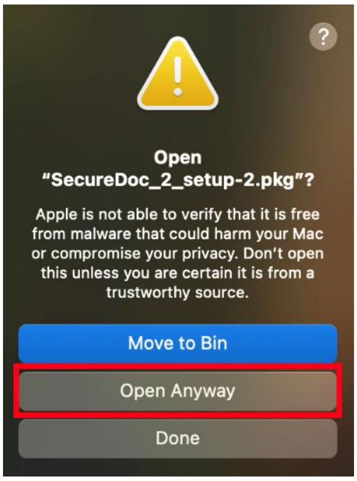
Security

Allow applications from: App Store & Known Developers

"SecureDoc" was blocked to protect your Mac. Open Anyway

Apple could not verify "SecureDoc" is free of malware that may harm your Mac or compromise your privacy.

Another window will then appear, in which you should select **Open Anyway**.



Open "SecureDoc_2_setup-2.pkg"?

Apple is not able to verify that it is free from malware that could harm your Mac or compromise your privacy. Don't open this unless you are certain it is from a trustworthy source.

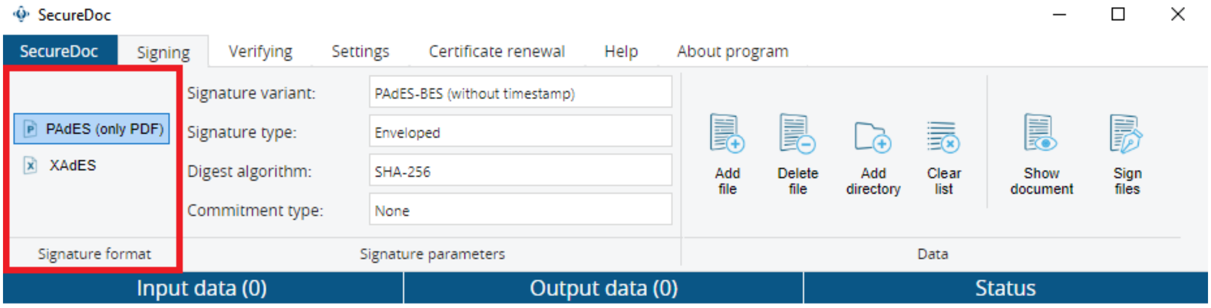
After that, the installation proces should begin. If a similar message appears when launching the SecureDoc application for the first time after installation, you will need to add an exception in the same way via **System Settings**.

4. Signing

The **Signing** tab is dedicated for signing using electronic signatures. The signing process is composed of selecting the correct signature format ad parameters, adding the file(s) to the list, selecting the appropriate certificate and authorization. The entire process is fully described in the next steps.

4.1 **Signature format** section

There are two electronic signature formats available in the **Signature format** section:



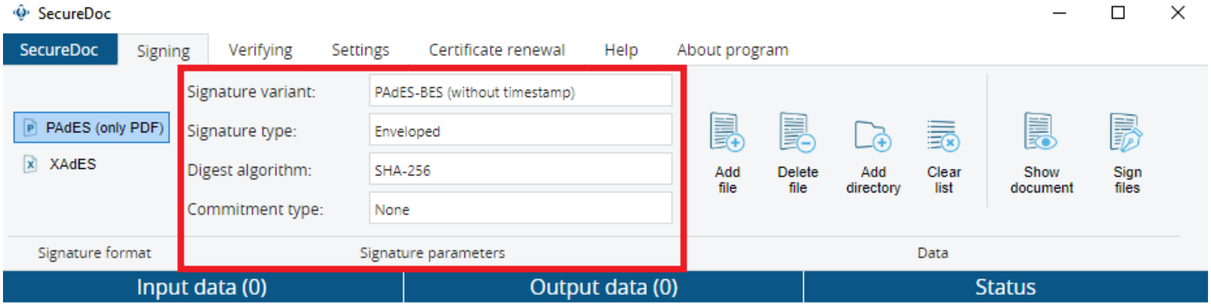
Signature variant: PAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

PAdES format is dedicated for signing PDF files. Graphic representation of the signature can only be added using this format.

XAdES format can be used for signing files of any extension (.xml, .docx, .odt etc.). Despite that being technically possible, we don't recommend using the XAdES format for signing PDF files.

4.2 **Signature parameters** section

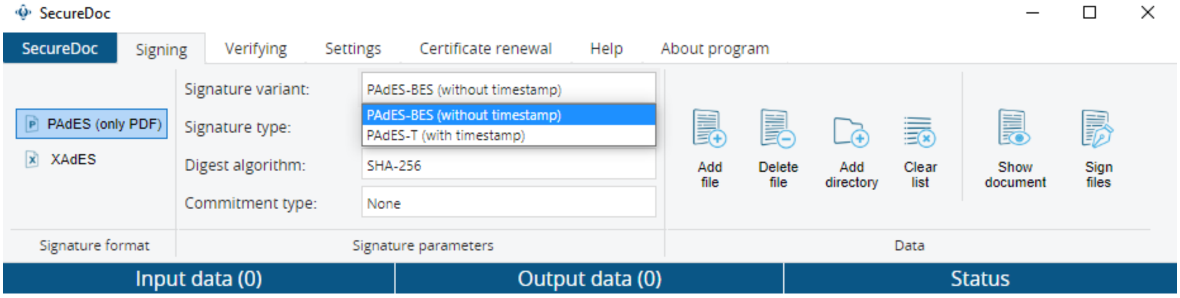
In this section we will find the most important parameters, which will be applied to the current file list after clicking **Sign files**. Specific parameters influence which files we will be able to add to this list and the effect after signing the files. As a user of the SecureDoc application, we have some flexibility in choosing how we sign a given file – usually, there is more than one method. However, we must be aware of how certain parameters will affect the file being signed. Often, we need to adjust to the requirements of an external system to which we will ultimately upload the signed files.



Signature variant: PAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

4.2.1 Signature variant

Depending on the chosen Signature Format, the following Signature Variants are available: PAdES-BES / PAdES-T lub XAdES-BES / XAdES-T.



Signature variant: PAdES-BES (without timestamp)
Signature type:
Digest algorithm: SHA-256
Commitment type: None

BES variant means that during the signing process electronic signature will be placed without a timestamp.

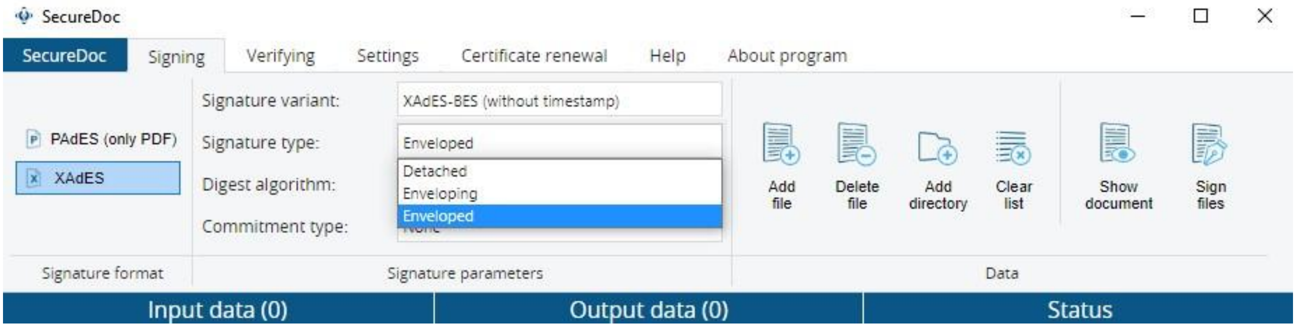
T variant means that the signature will be placed with a timestamp. Qualified timestamp service is an additional service that allows accurate depiction of the date and time of the performed actions in the electronic signature environment.

The Timestamp allows for the confirmation of the time at which the electronic signature was applied, or to establish that a given document existed at a specific time and has not been altered. Under the provision of applicable law, this results in a certain date effect.

By using a timestamp issued by a qualified entity, you are guaranteed the inviolability of the document's signing date in relation to: courts, institutions, companies, individual clients, etc.

The timestamp does not take the current time from the computer on which the signature is applied, instead, it queries a dedicated server to obtain the time information.

4.2.2 Signature type



Signature variant: XAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm:
Commitment type: None

4.2.2.1 Detached

The *Detached* signature type allows files with any extension to be signed. When applying a detached signature, the signature itself will be created in a separate file and saved in the same folder as the file being signed. The detached signature file is saved in the .XAdES format.

It is important to remember that when verifying such a signature, both the source file (containing the document's content) and the signature file (containing the certificate of the signature) are required. Additionally, when sending the detached signature, it is necessary to attach the signed file (the one containing the document's content).

Once the detached signature is applied, no modifications should be made to either the source file or the newly created file. Altering the content of either file will compromise data integrity, and the signature will no longer be verifiable. In the case of SecureDoc, it is also important not to modify the names of these files.

4.2.2.2 Enveloping

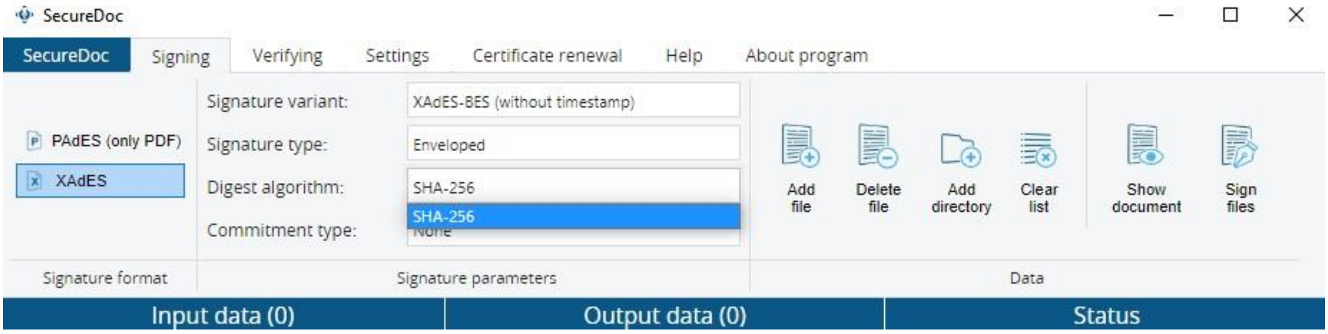
The Enveloping signature type should be used for any files signed in the XAdES format, where we want the signature to be contained within the signed file itself. In other words, the signature file, signed with the Enveloping type, will contain both the source document's content and the certificate of the signature (2-in-1). The file signed with the Enveloping type will be saved in the XAdES format. The file created in this way is sufficient for correct signature verification.

4.2.2.3 Enveloped

For the PAdES signature format, the only available signature type is *Enveloped* – it is automatically selected when this format is chosen. For the XAdES format, the *Enveloped* signature type is intended for XML files.

With the default settings of the SecureDoc application, signing a file using the *Enveloped* type will result in the modification of the original file. This means that the file selected for signing will be overwritten – its extension, name, and location will remain unchanged.

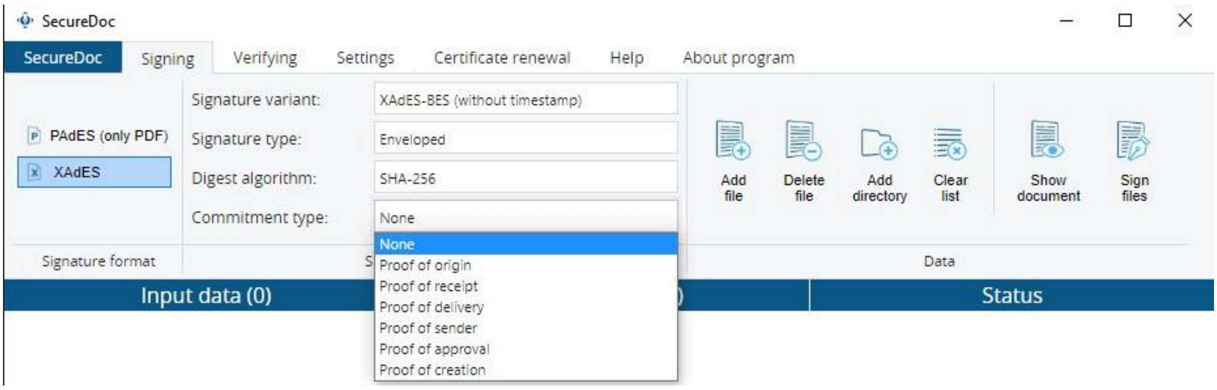
4.2.3 Digest algorithm



Signature variant: XAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

This parameter indicates the specific algorithm that will be used to calculate the so-called file hash (a digest of the file) which is to be signed.

4.2.4 Commitment type



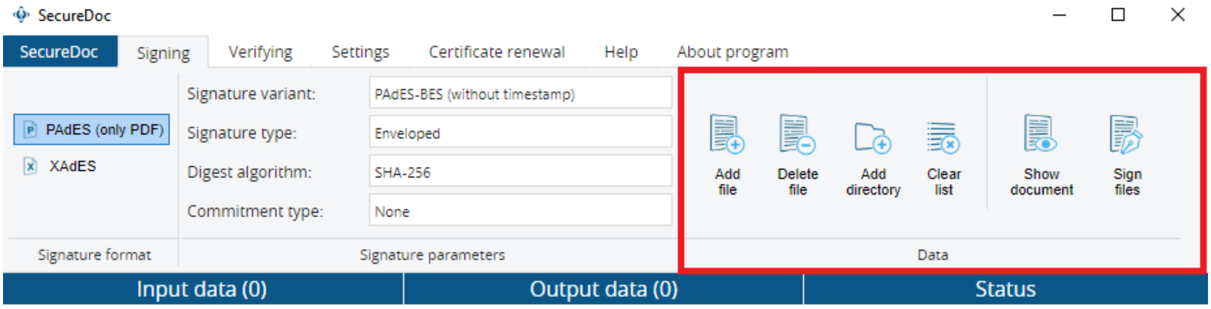
Signature variant: XAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

None
Proof of origin
Proof of receipt
Proof of delivery
Proof of sender
Proof of approval
Proof of creation

This optional parameter adds information to the signature about the reason it was applied. Apart from the default value “None”, six types of commitments are available for selection:

- Proof of origin
- Proof of receipt
- Proof of delivery
- Proof of sender
- Proof of approval
- Proof of creation

4.3 **Data** section



Signature variant: PAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

When you click **"Add File"**, a window will open where you can select the files to be signed. The files will be added to the list. Alternatively, you can drag and drop selected files into the application window.

"Add Folder" – this button allows you to add all files from the selected folder that meet the criteria set in the signature settings. For example, if the PAdES signature format is selected, all PDF files from the chosen folder will be imported. If the XAdES format is selected with either the *Detached*, *Enveloping*, or *Enveloped* type, then all available files from the selected folder will be imported accordingly.

You can also remove files selected for signing using the **"Remove File"** button – to remove files individually (the currently selected, highlighted file will be deleted), or the **"Clear List"** button – to remove all files from the list.

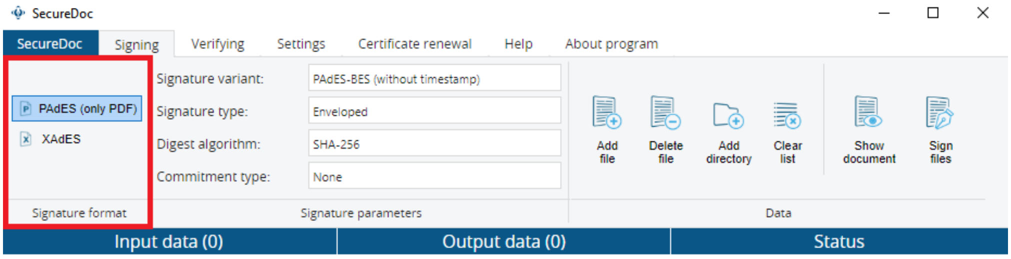
Clicking the **"Show Document"** button will display the content of the selected document in a new window.

"Sign Files" – clicking this button will start the process of signing all files on the list.

4.4 Adding signatures to a previously signed file

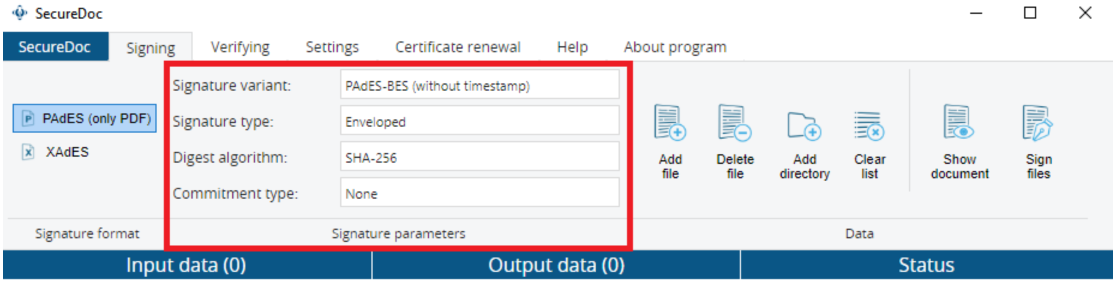
Please note that in order to sign a file with a qualified electronic signature, a device with a cryptographic card must be connected to the computer. If you are using the ECSigner cloud signature, the ECSigner application must be running in the background with a logged-in account.

1. Select the **PAdES signature format** (PDF only).



Signature variant: PAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

2. Select other desired **signature parameters**.



Signature variant: PAdES-BES (without timestamp)

Signature type: Enveloped

Digest algorithm: SHA-256

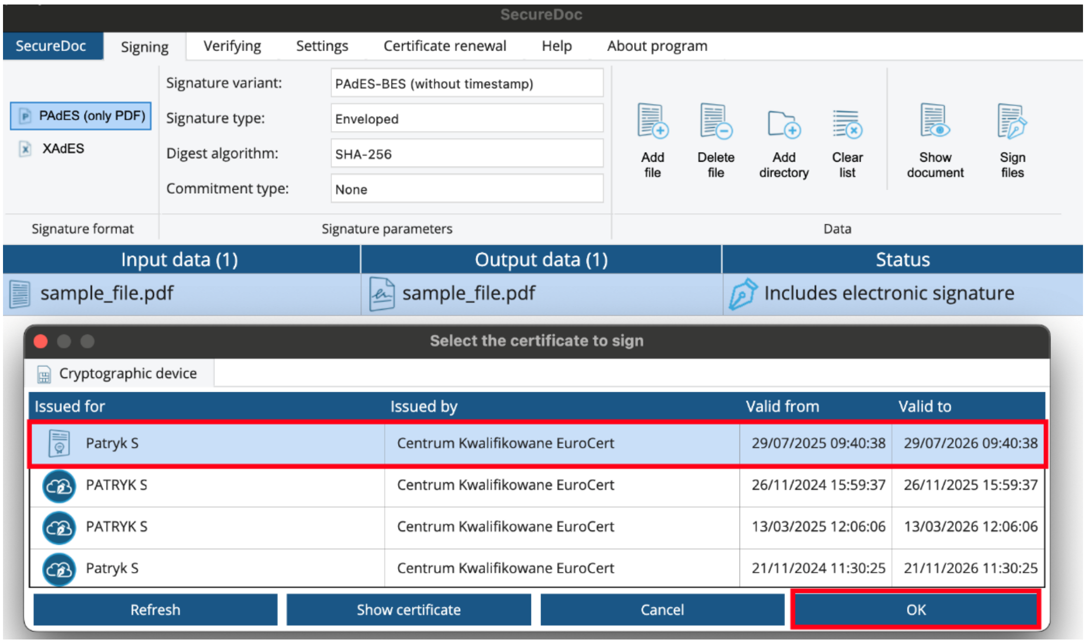
Commitment type: None

3. Add the files you wish to sign using the **"Add file"** button, or drag and drop them directly from a folder into the SecureDoc application window.

4. Click "**Sign files**". Please note that all documents selected for signing will be signed using the same signature parameters.

   After clicking "**Sign files**", a certificate selection window will appear. Select the certificate you want to use for signing and click **"OK**”. It is recommended to use the **Cryptographic devices** tab. This tab displays certificates stored on the currently connected device, as well as any available ECSigner cloud certificates. You can distinguish the type of signature by the icon next to the certificate holder’s name.

   Note: The **Personal certificates** tab allows you to view certificates stored in the Windows certificate store. This often includes non-qualified certificates unrelated to EuroCert.



Signature variant: PAdES-BES (without timestamp)

Signature type: Enveloped

Digest algorithm: SHA-256

Commitment type: None

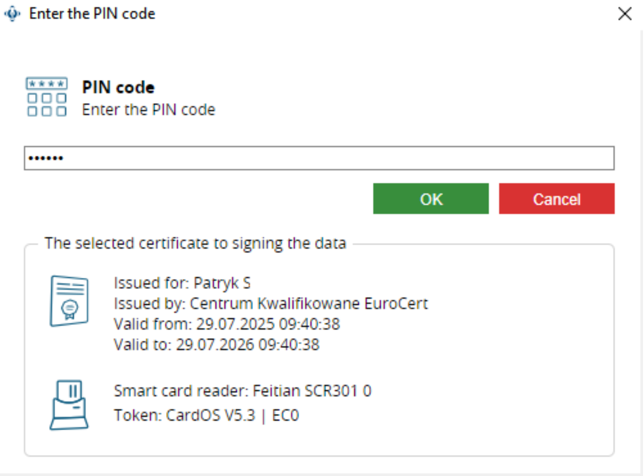
Input data (1)	Output data (1)	Status
sample_file.pdf	sample_file.pdf	Includes electronic signature

Issued for	Issued by	Valid from	Valid to
Patryk S	Centrum Kwalifikowane EuroCert	29/07/2025 09:40:38	29/07/2026 09:40:38
PATRYK S	Centrum Kwalifikowane EuroCert	26/11/2024 15:59:37	26/11/2025 15:59:37
PATRYK S	Centrum Kwalifikowane EuroCert	13/03/2025 12:06:06	13/03/2026 12:06:06
Patryk S	Centrum Kwalifikowane EuroCert	21/11/2024 11:30:25	21/11/2026 11:30:25

5. After selecting the certificate and clicking **"OK"**, a message regarding the signature will be displayed. After reviewing the message, click **"OK**”.

6. When using a physical card for signing, enter your PIN and click **"OK**”.

When using the ECSigner cloud signature, log in to your account and then enter the authorisation code (OTP) from the ECSigner mobile app.



Enter the PIN code

PIN code
Enter the PIN code

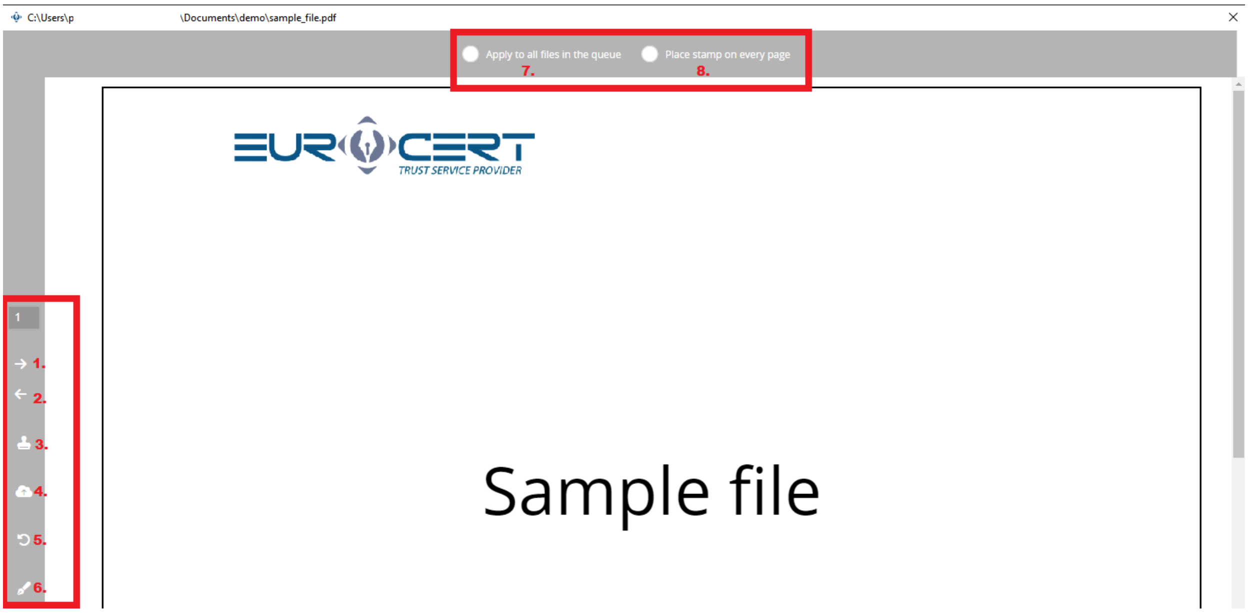
••••••

The selected certificate to signing the data

Issued for: Patryk S
Issued by: Centrum Kwalifikowane EuroCert
Valid from: 29.07.2025 09:40:38
Valid to: 29.07.2026 09:40:38

Smart card reader: Feitian SCR301 0
Token: CardOS V5.3 | EC0

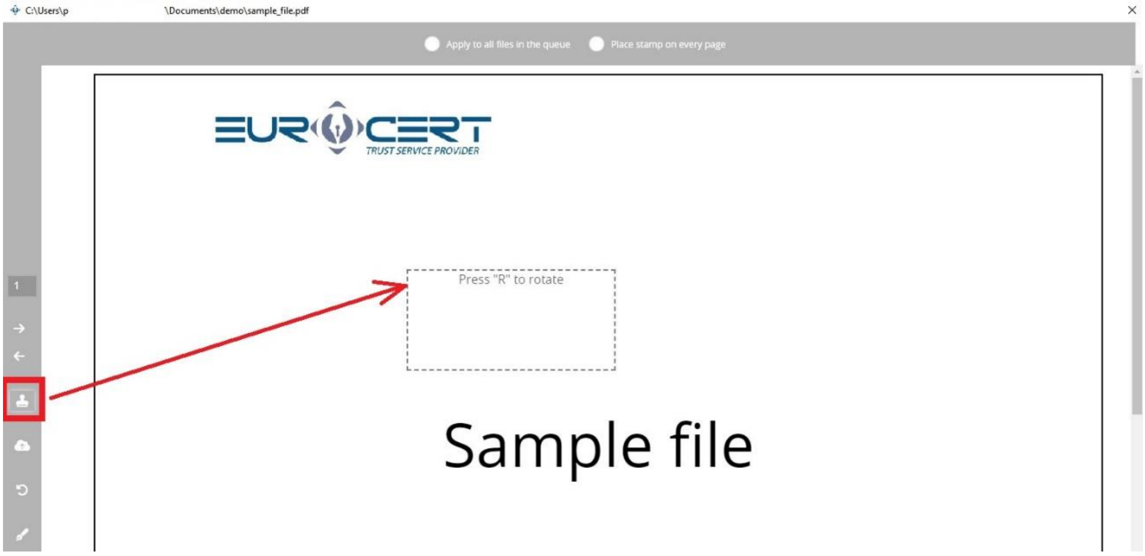
7. With the default application settings, during the signing of a PDF file using the PAdES format, a preview of the file will be displayed at this stage. Here, the user can add a graphical representation of the signature in the chosen location on the document. This has no effect on the legal validity of the signature — it is purely cosmetic. A detailed description of the buttons shown in the image below can be found in the following steps.



C:\Users\p \Documents\demo\sample_file.pdf

○ Apply to all files in the queue
7.
○ Place stamp on every page
8.
1
1.
2.
3.
4.
5.
6.
EUROCERT TRUST SERVICE PROVIDER
Sample file

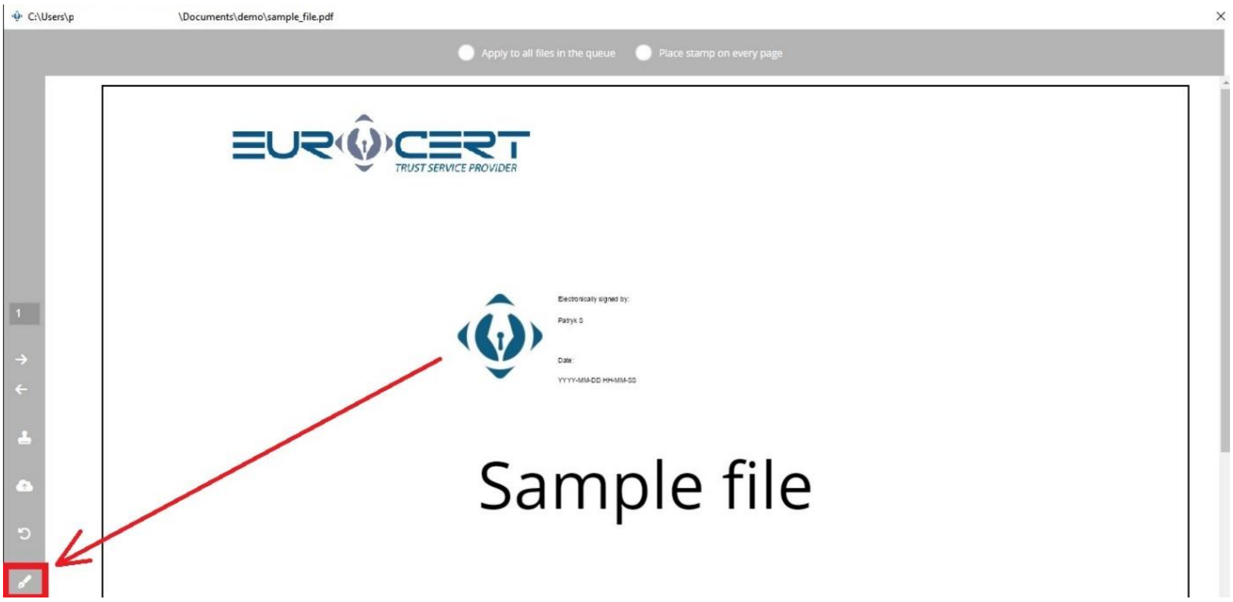
8. Click the „Stamp" button (3), then move the cursor to the chosen location and click the left mouse button to place the graphic representation. To navigate to a different page, use the arrow buttons (1) and (2) or manually enter the page number in the field above the arrows.



C:\Users\p \Documents\demo\sample_file.pdf

×
○ Apply to all files in the queue
○ Place stamp on every page
1
→
←
TRUST SERVICE PROVIDER
Press "R" to rotate
Sample file

After placing the graphic representation, click the „Sign" button (6) with the pen icon to finalize the process.



C:\Users\p \Documents\demo\sample_file.pdf

Electronically signed by:

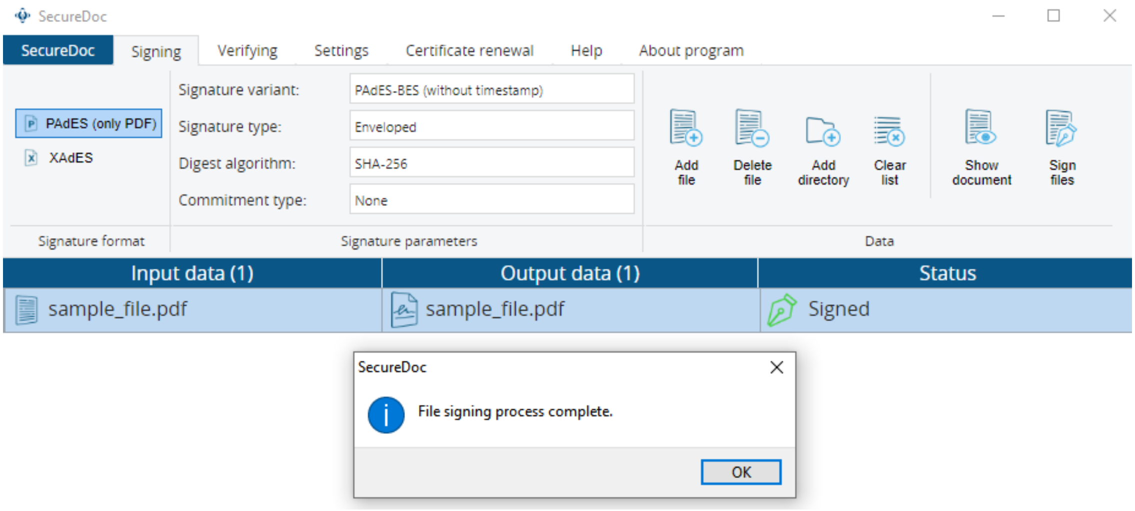
Patryk S

Date:

YYYY-MM-DD HH-MM-SS

×
○ Apply to all files in the queue
○ Place stamp on every page
1
→
←
TRUST SERVICE PROVIDER
Sample file

9. Check the document signing status. If the operation was successfull, the status window will display „Signed" state. If there was an error, it will show the „Unsigned" status.



Signature variant: PAdES-BES (without timestamp)
Signature type: Enveloped
Digest algorithm: SHA-256
Commitment type: None

Input data (1)	Output data (1)	Status
sample_file.pdf	sample_file.pdf	Signed

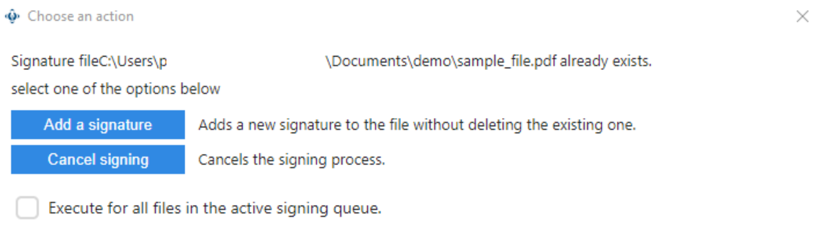
SecureDoc

File signing process complete.

10. (optional)
The SecureDoc app allows you to change the default logo to your own. In order to do that, use the „**Load logo**" (4) and select the file prepared earlier. Logo must have equal width and height, and must be saved in the **.jpg** format – if needed, you can revert to the default logo using the ,,**Restore default logo**" button (5). When signing multiple PDF files at the same time, the „Apply to all files in queue" function may be useful (7) – this way settings chosen for the selected file will be applied to the other files in queue, without viewing them separately. To apply the graphical representation in the same spot on every page of the document, use the „Place signature on all pages" function (8). Regardless of the selected graphical representation settings, click „**Sign**" buton to finalize the signing process (6).

4.5 Adding Additional Signatures to a File

If a file already contains at least one electronic signature, the signing process will include an additional window. To add another signature to the document, select the „Add signature" button.



Signature fileC:\Users\p \Documents\demo\sample_file.pdf already exists.

select one of the options below

Add a signature – Adds a new signature to the file without deleting the existing one.

Cancel signing – Cancels the signing process.

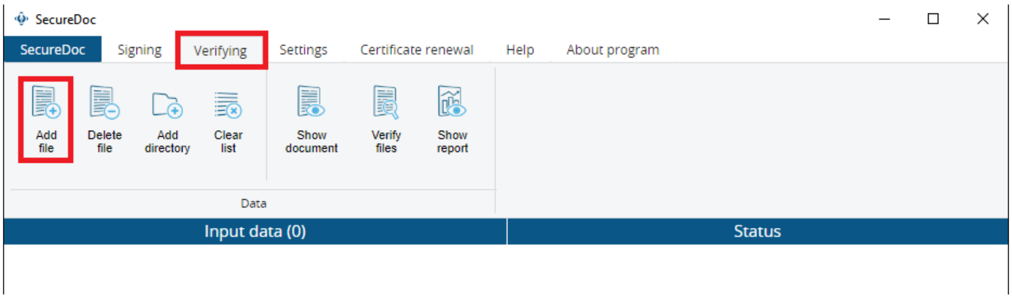
□ Execute for all files in the active signing queue.

5. Verifying

In this tab, you can verify signed files and generate verification reports. You can add multiple files at once, even if they were signed using different formats and signature parameters. For files signed with **XadES Detached**, both the **original file** and the newly generated **.XAdES file** must be located in the same folder — otherwise, verification will not be possible.

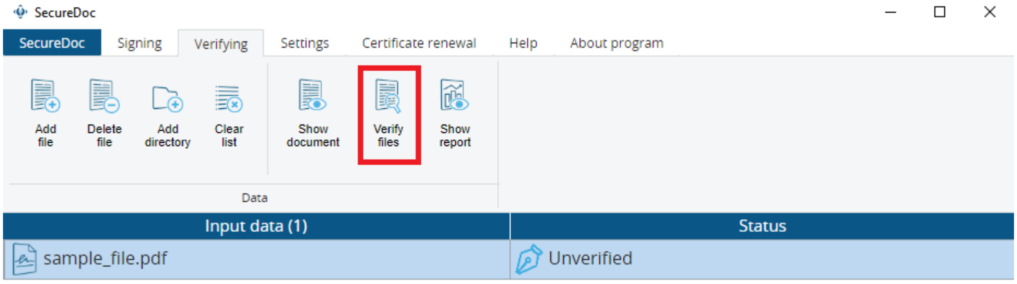
5.1 File verification process

1. Add the files you want to verify using the „Add files" button or by dragging and dropping them into the application window.



Input data (0)	Status

2. Click „Verify files" (Note: internet connection is required for the verification process).



Input data (1)	Status
sample_file.pdf	Unverified

3. We await the verification status notification. Possible outcomes:

- **Positively verified** – All signatures found have been verified positively.
- **Negatively verified** – At least one signature has been verified negatively.
- **Unspecified** – The verification outcome of at least one of the signatures is unclear.

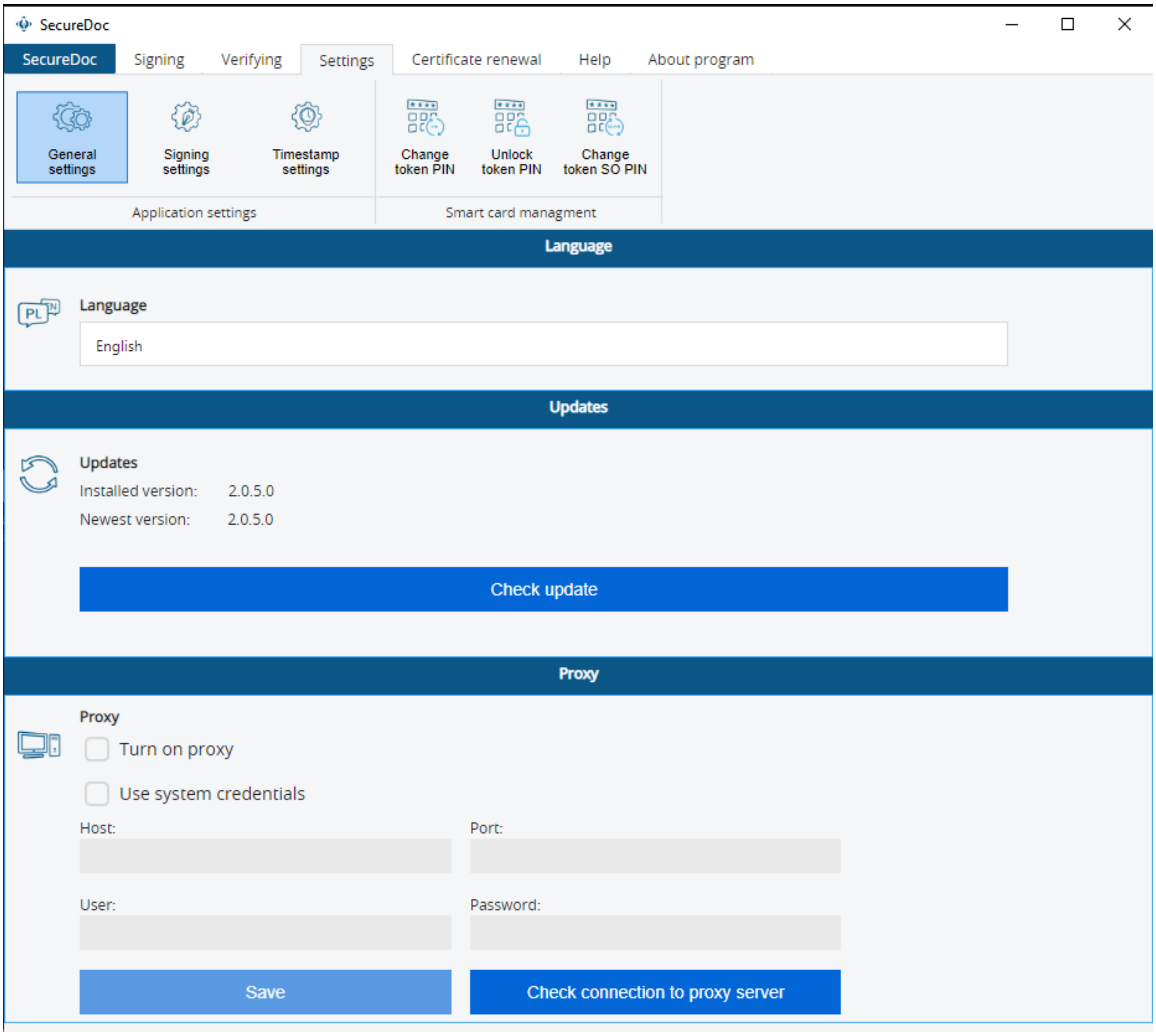
To view the details of the detected signatures, click on the name of the file you are interested in and then click „**Show report**". Each report page is dedicated to a separate signature. You can change the pages using the arrows in the left side of the menu after viewing the report.

6. Settings

This tab contains all the settings related to the operation of the SecureDoc application and the way files are signed. Additionally, it includes functions related to the cryptographic card. All features are described below.

6.1 **General settings** section

6.1.1 General settings



Language

Language: English

Updates

Updates
Installed version: 2.0.5.0
Newest version: 2.0.5.0

Proxy

Proxy
☐ Turn on proxy
☐ Use system credentials
Host:
Port:
User:
Password:

6.1.1.1 Language

To change the language in the general settings, go to the **Language** section and select one of the available languages from the list. Currently, Polish, English, and German are supported.

6.1.1.2 Updates

At launch, the SecureDoc 2.0 application checks for available updates. If an outdated version is detected, the application will display a message indicating that an update is available. To install the new version, the user must accept the displayed message and proceed with the installation.

In the **Updates** section, you can check the installed version number and manually initiate an update.

6.1.1.3 Proxy

In this section, it is possible to configure a proxy server to be used by the SecureDoc application. To do this, tick the "Enable proxy" option, enter all the necessary information in the available fields, and click the "Save" button.

Alternatively, system credentials can be used. To do this, tick both the "Enable proxy" and "Use system credentials" options, and leave the fields empty.

Before signing files, we recommend testing the connection using the "Check proxy server connection" button.

6.1.2 Signing settings

6.1.2.1 Default format and signature parameters

In this section, you can select the default format, variant and type of signature, the hash function, and the type of commitment. This way, your default parameters will be automatically selected in the **Signing** tab as soon as the application is launched. The newly selected default settings will only take effect after closing and restarting the application.

6.1.2.2 Additional signing parameters

In this section, you can configure the following options:

„Overwrite PDF document when a PAdES signature is created" - disabling this option means that the signed PDF file will be saved as a separate file in the same folder as the original, with "-sig" added to the file name.

When this option is enabled, the signed file will overwrite the original without changing its name. No new file is created during signing in this case.

„Apply graphical signature when a PAdES signature is created" – this option allows you to add a graphical representation of the signature to the PDF document. This step can also be skipped during signing.

Disabling this option completely skips the PDF preview stage during the signing process, shortening the entire procedure.

„Do not encode XML data to Base64 when creating an XAdES signature of the enveloping type" - disabling this option will cause the signed XML file to be saved encoded in Base64. Enabling it allows the XML files to be saved using standard UTF-8 encoding.

„Overwrite XML document when creating an XAdES signature of the enveloped type” – when this option is enabled, the document format (.XML) will remain unchanged after signing..

If you need the XML file to be saved in the .XAdES format after signing, this option should be disabled.

„Create an XAdES signature of the enveloped type in standard version” – signature created with this configuration prevents additional signatures from being added to the same document.

6.1.3 Timestamp Settings

To be able to use timestamps in the SecureDoc application, you need to configure access to the timestamp server.

After purchasing a timestamp package and receiving the necessary configuration data from EuroCert, you should fill in the required fields and click the "**Save**" button.

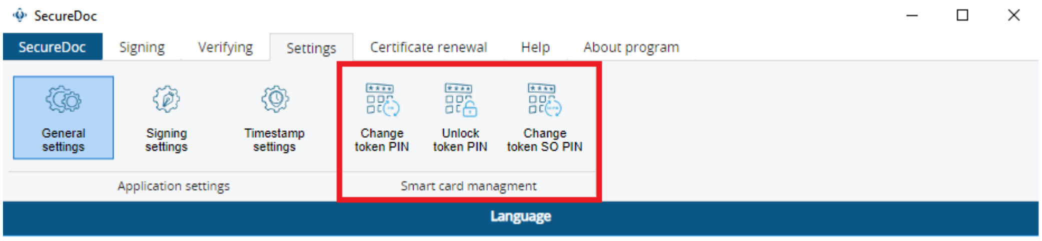
- Timestamp server address
- Username – personalised login
- Password – password for the timestamping service

The server address and username can be found in your account at https://portal.eurocert.pl. The password for the timestamping service is set by the user, also from their account. Before signing documents, it is recommended to test the timestamp configuration by clicking the **"Check timestamp configuration"** button.

6.2 **Card Management** section

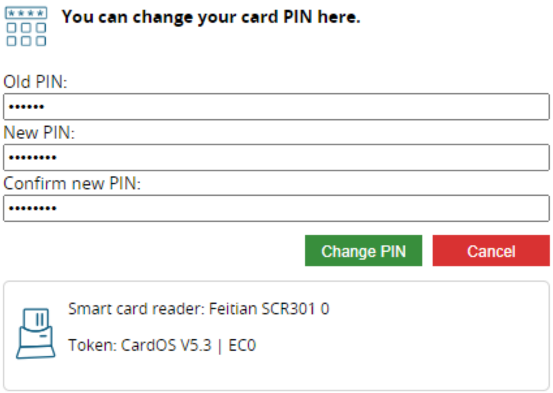
The application allows you to manage the PIN and SO PIN codes of a cryptographic card issued by EuroCert.

The user can change the PIN and SO PIN codes (as long as they are not yet blocked), and can also unblock the PIN code if it has already been blocked.



6.2.1 Change token PIN

To change the PIN code, click on **"Change token PIN"**, after which the following window will appear:



You can change your card PIN here.

Old PIN: ••••••

New PIN: ••••••••

Confirm new PIN: ••••••••

Smart card reader: Feitian SCR301 0

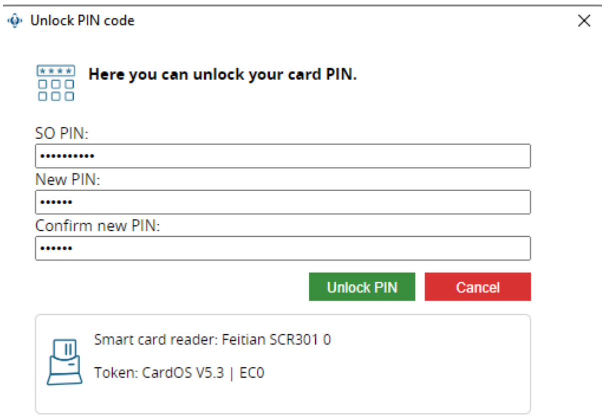
Token: CardOS V5.3 | EC0

In the **"<u>Old PIN</u>"** field, enter your current PIN. In the next two fields, enter the new PIN, then click **"<u>Change PIN</u>**”. If the operation is successful, the new PIN will be used for authentication from that point onward.

6.2.2 Unlock token PIN

Entering the wrong PIN three times while signing an electronic document or attempting to change the PIN will result in the PIN being blocked. Once the PIN is blocked, the user is unable to sign any documents.

To unblock the PIN, click **"<u>Unblock token PIN</u>"**, after which the following window will appear:



Here you can unlock your card PIN.

SO PIN: ••••••••••

New PIN: ••••••

Confirm new PIN: ••••••

Smart card reader: Feitian SCR301 0

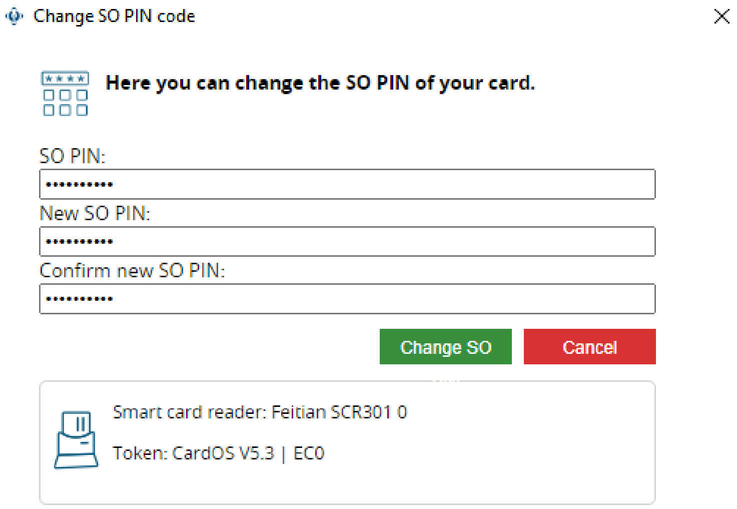
Token: CardOS V5.3 | EC0

First you will need to input the SO PIN, then the new PIN twice and press „<u>Unlock PIN</u>”.

WARNING! Entering the incorrect SO PIN three times will permanently block the cryptographic card. In such a case, a new certificate on a new card must be purchased.

6.2.3 Change token SO PIN

To change the SO PIN code, click **"<u>Change token SO PIN</u>"**, after which the following window will appear:



Change SO PIN code

Here you can change the SO PIN of your card.

SO PIN: ••••••••••

New SO PIN: ••••••••••

Confirm new SO PIN: ••••••••••

Smart card reader: Feitian SCR301 0

Token: CardOS V5.3 | EC0

In the **"<u>SO PIN</u>"** field, enter the current SO PIN. In the next two fields, enter the new SO PIN.

The new SO PIN can consist of any characters: numbers, letters (uppercase and lowercase), symbols, and other characters. The minimum length is 4 characters; the maximum depends on the model of the cryptographic card (usually 8-10 characters).

WARNING! Entering the incorrect SO PIN three times will permanently block the cryptographic card. In such a case, a new certificate on a new card must be purchased.

Additional information:

When changing the PIN or SO PIN codes, only one cryptographic card should be connected to the computer. Connecting more than one may result in some of them becoming blocked. EuroCert takes no responsibility for any consequences resulting from ignoring this recommendation.

7. Certificate renewal

Purchase renewal

The product *Electronic Signature Renewal on EuroCert Card* can be purchased via our online shop HERE or by contacting our sales department: handlowy@eurocert.pl

Certificate renewal

We recommend starting the renewal procedure at least 7 days before the current certificate expires. If you begin the process later than 72 hours before the expiry date, we cannot guarantee successful completion of the renewal.

To begin the renewal procedure (after purchasing the product and receiving the renewal code), go to the **Certificate Renewal** tab in the SecureDoc application and click **"Renew Certificate"**. After entering the renewal code, complete the application and sign the generated agreement using your current qualified electronic signature.

Warning: Purchasing the product alone does not automatically extend the validity of your qualified signature. The new certificate will only be generated once the procedure described in the instructions (provided with the renewal code) has been completed.

8. Help

The **Help** tab includes a button to download the latest version of the SecureDoc user manual, provides contact information for the technical support team, and offers the ability to download the **AnyDesk** remote support application.

9. About program

This tab contains the license terms & conditions.