User manual

SECUREDOC v 2.0

Version 1.3

Table of contents

1. Program information

SecureDoc v2.0 is an application designed to create and verify electronic signatures with the option of issuing a signature with a time stamp.

In the SecureDoc v2.0 application, an electronic signature may be submitted with the use of certificates issued by: EuroCert, CenCert (Enigma), KIR, PWPW, and Certum (Asseco).

Signature formats available in SecureDoc are PAdES-BES, PAdES-T, XAdES-BES, XAdES-T in internal and external types (Detached / Enveloping / Enveloped).

Cryptographic hash function (Digest algorithm): SHA-256

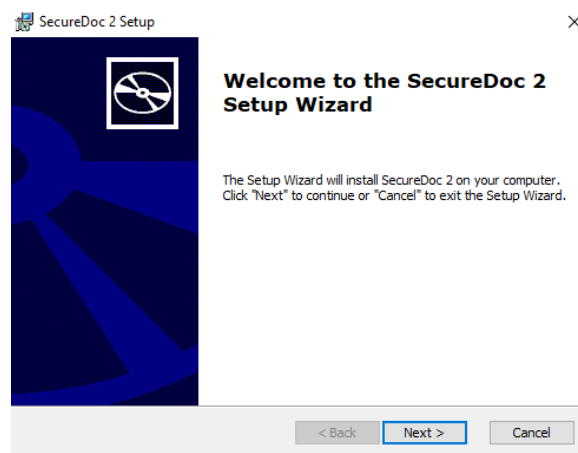# 2. Minimum system requirements

- Windows 10 (or newer) operating system
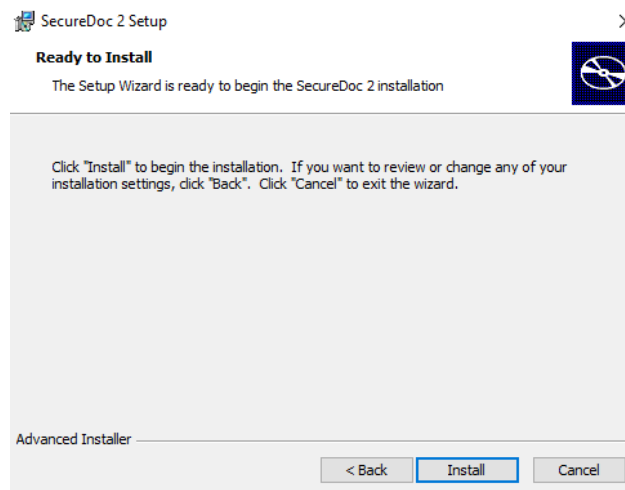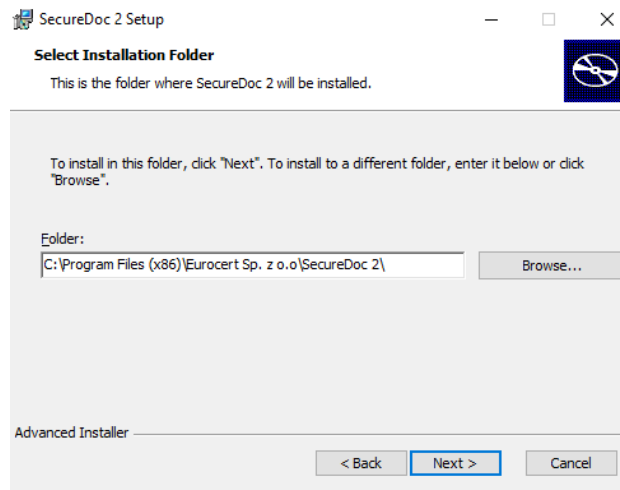- Internet connection (required for using file verification and for using ECSigner cloud signature)

To use your qualified electronic signature issued by EuroCert in SecureDoc, second application must be installed:

- Cryptographic card management application - Charismathics Smart Security Interface – in case of electronic signature on a device
- ECSigner – in case of ECSigner cloud signature

3. Installation

To install the application, go to https://eurocert.pl/index.php/oprogramowanie and download "*SecureDoc 2 - application to create and verify an electronic signature* ". After running the downloaded installer, follow the dialogue boxes below:

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy: Dział techniczny: +48 22 390 59 95
+48 22 490 36 45   +48 22 490 49 86   biuro@eurocert.pl
handlowy@eurocert.pl   wsparcie@eurocert.pl   www.eurocert.pl
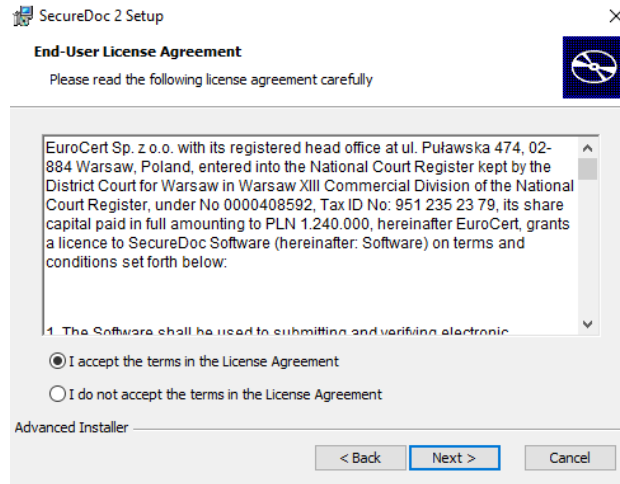
After completing this step, the application is ready to use.

4. Signing

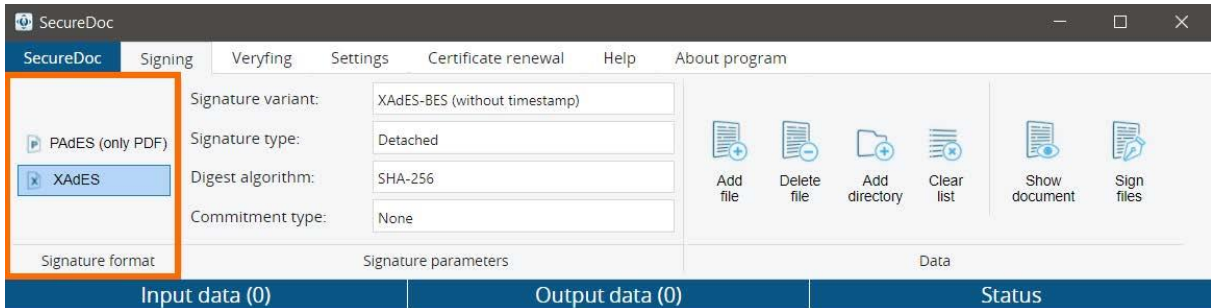The „Signing" tab is dedicated to documents signing using electronic signatures. In the „Signature format" section there are two available signature formats:

- PAdES
- XAdES

PAdES signature format is dedicated and exclusive for PDF files.

XAdES signature format can be used to sign any file format (.xml, .docx, .jpeg, .odt etc.). PDF files also can be signed using XAdES signature format, however it's always recommended to use PAdES.

4.1 „Signature parameters" section

This section contains all of the main parameters of the performed signature.
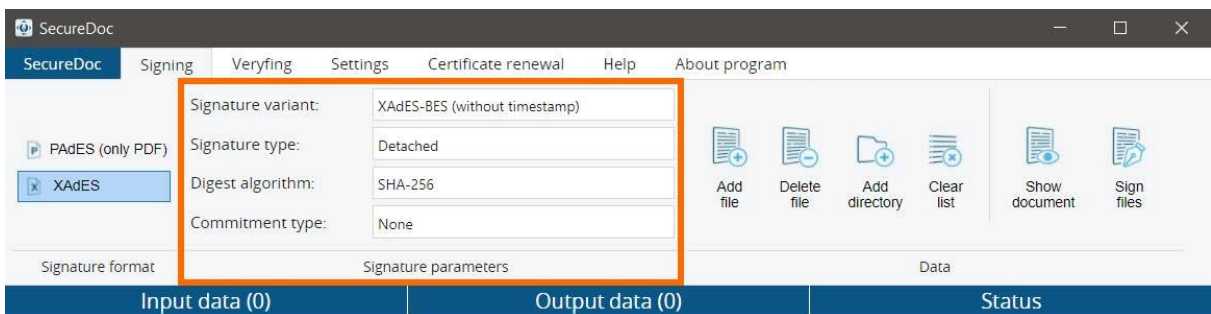
4.1.1 Signature variant

Depending on the chosen signature format, the following options are available: PAdES-BES / PAdES-T or XAdES-BES / XAdES-T.

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

Variant -T means that during the signing process, electronic signature will be placed with a timestamp.

The Qualified Timestamp Service ("timestamp" mentioned above) is an additional service that allows to precisely determine the date and time of activities carried out in the electronic environment.
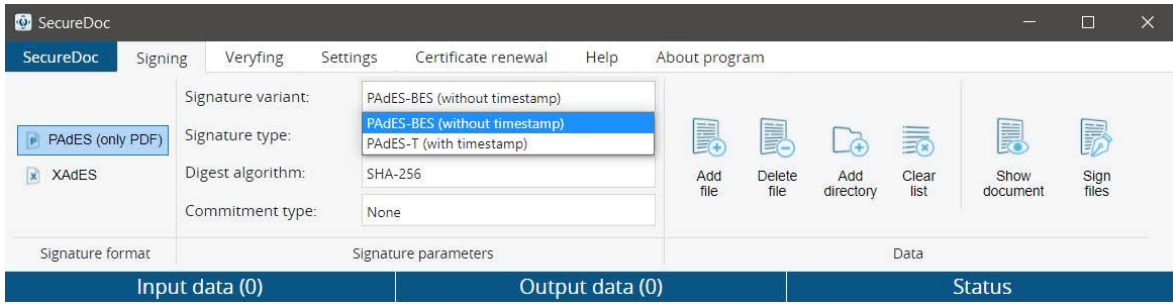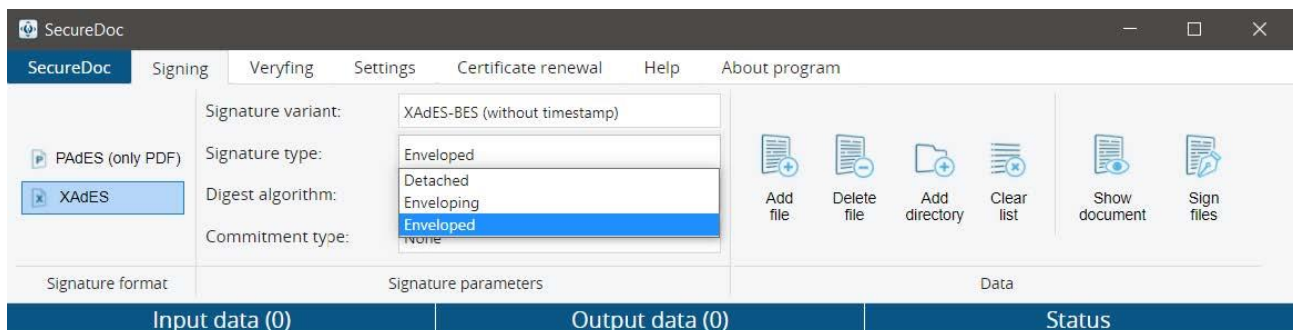
Timestamping makes it possible to confirm the time and date when the electronic signature was placed on the file or to determine if a given document existed at a specific time and has not been changed since. Under the provisions of applicable law, this has effects of a *date certain*.

By using a timestamp issued by a qualified entity, you get a guarantee that the deadline for signing the document will not be challenged in relation to courts, institutions, companies, individual clients, etc.

It is also worth noting that the timestamp does not retrieve the current time from the computer on which the signature is issued, but asks a dedicated server to obtain information about the time.

4.1.2   Signature type

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

4.1.2.1 Detached

When signing a document with a detached signature type, the signature itself will be created in a separate file and saved in the same folder as the original file. The file which is being created after signing the document with a detached signature type, has a XAdES format.

Detached signature type can be used to sign files of any format or size.

It should be noted, that when verifying a file signed with a detached signature - you must have access to a source file (original file, which contains contents of a document) + file with a signature (file created during the signing process, which contains only the signature). Also, when sending a file signed using a detached signature type - it is necessary to send both files (the original one and the one containing the signature).

It is important not to change in any way (including the name of the files) the original file or the file which was created, as any changes will result in negative verification of the signature.

4.1.2.2 Enveloping

Enveloping signature type should be used for any files being signed in XAdES format, where we need the signature to be included in the signed file. So the signature issued using Enveloping signature type will contain both – the content of the document and the signature itself (2 in 1).

It is worth remembering that the file signed using the Enveloping signature type will be saved in XAdES format.

So, if for example, we sign a file „document.txt", the resulting file (containing the signature) will be named „document.txt.XAdES".

4.1.2.3 Enveloped

This signature type is equivalent to the Enveloping signature type and is used only for XML files. File signed using this signature type will contain both the contents of a document as well as signature.

So if we want to sign an XML file so it contains the signature with the content of the document – Enveloped signature type should be selected. This signature type applies only to XML files.

4.1.3 Digest algorithm
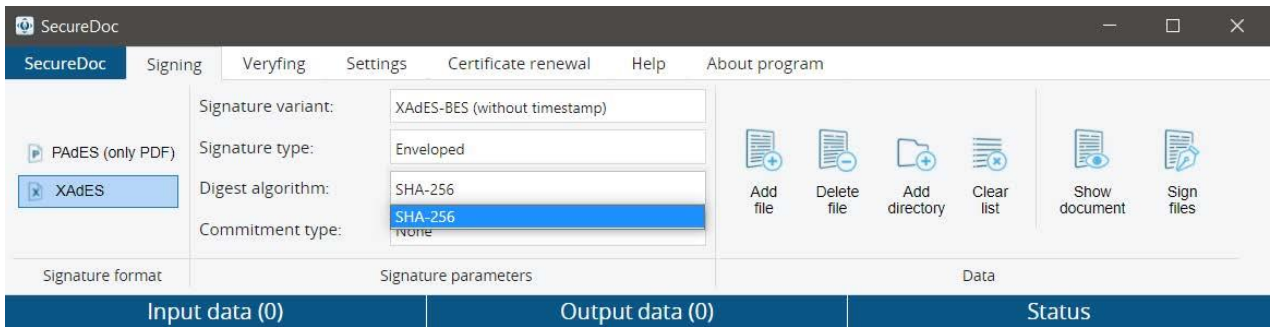
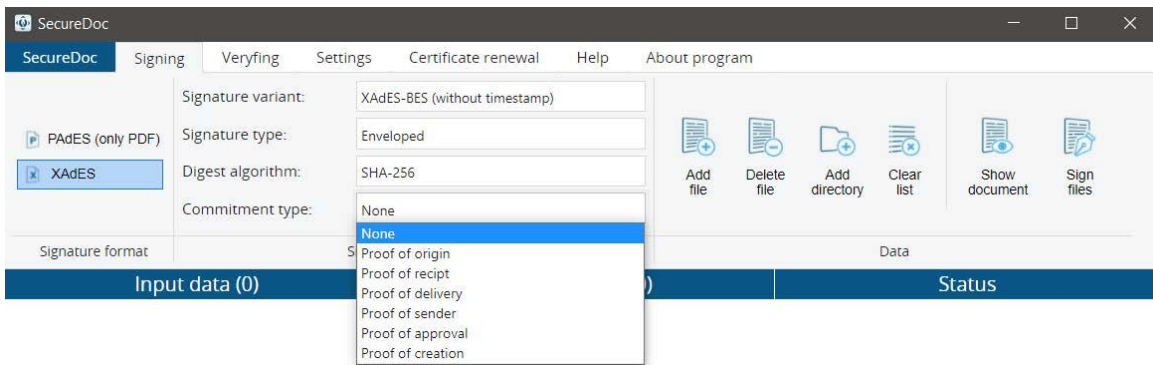SHA-256 is a type of cryptographic hash function. Higher hash value provides higher security.
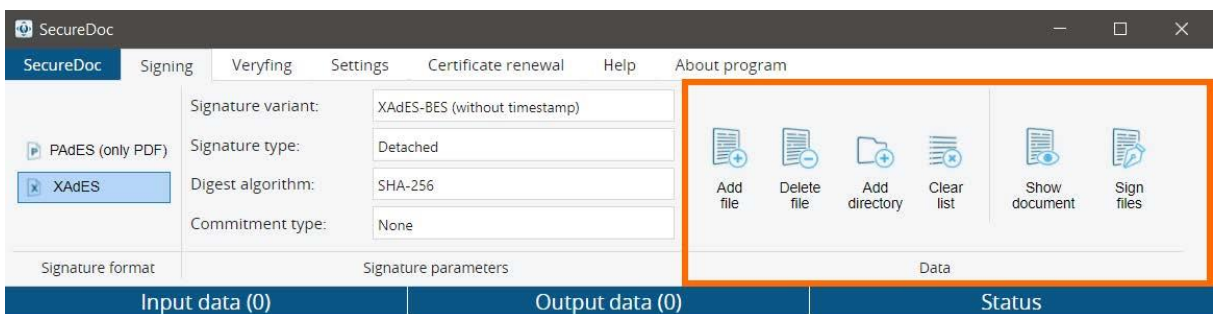
4.1.4 Commitment type

This field is optional and contains additional information about the signing reason. There are 6 types of commitments to choose from:

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

4.2 „Data" section

After clicking „Add file" button, the file explorer window will appear, from which user can indicate files for signing. Alternatively, files can be added to the list by drag&drop feature.

„Add directory" – with this button, from the selected folder we can add all files that meet the criteria in the signature settings, e.g. if we have chosen the PAdES signature format - all PDF files will be uploaded from the chosen catalog, and with the selected XAdES signature format all file formats will be uploaded.

We can also delete files that we have selected for signing using the „Delete file" button – for single file delete (the selected file (the highlighted one) will be deleted from the signing list), or „Clear list" – to delete all files from the list.

After clicking „Show document" button, file preview will be displayed in a new window.

„Sign files" – after pressing this button, all files from the list will be queued to the process of signing.

4.3 Signing process

To sign a file using a qualified signature, the device with a cryptographic card must be plugged into your PC. In case of using the ECSigner cloud signature, ECSigner application must be running in the background with your account logged in.

1. Specify the signature format with which the document should be signed (in the „Signature format" section).
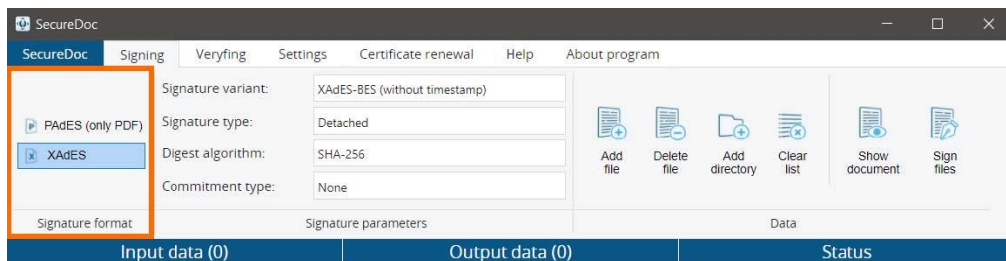
2. Select the required signature parameters in the „Signature parameters" section.
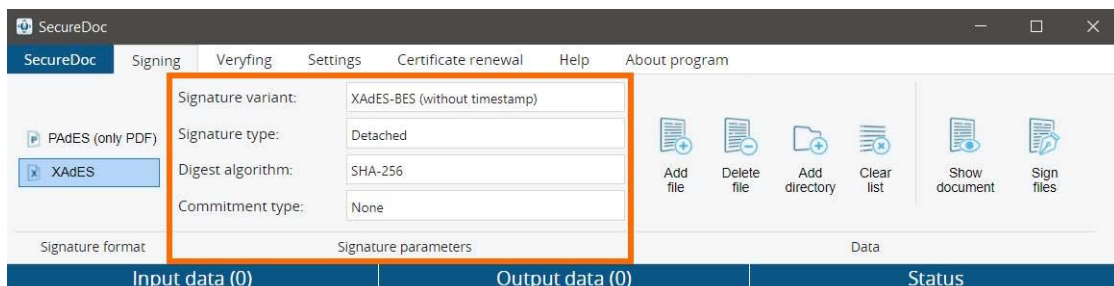
3. Add files you would like to sign.

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

4. Click „Sign files". It is worth noting that all of the documents from the selected files list will be signed using the same signature parameters.

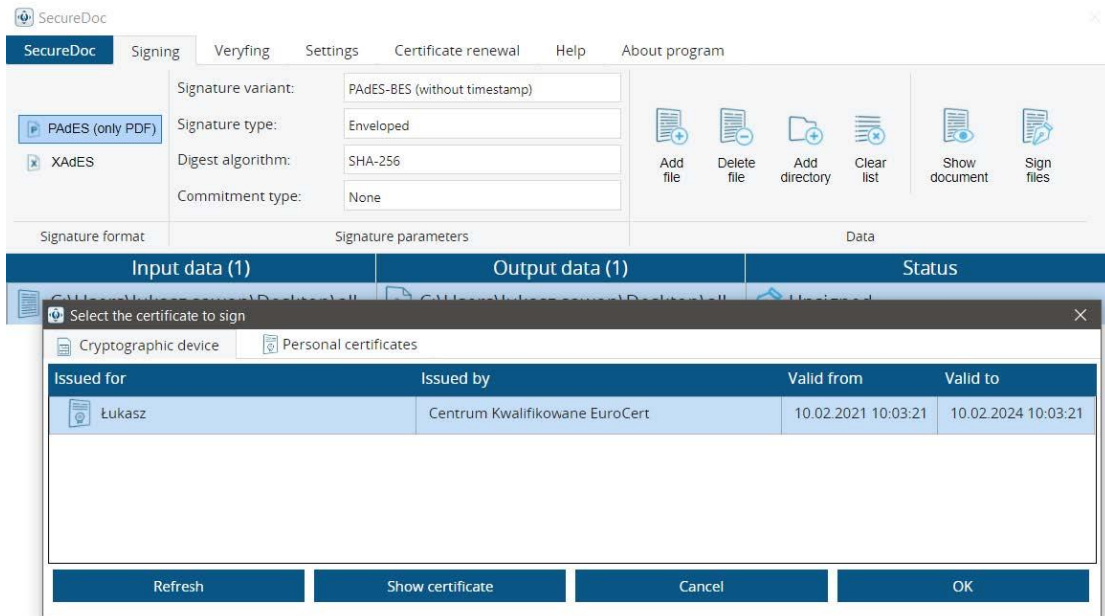5. After clicking on „Sign files", the certificate selection window will appear. Select the „Cryptographic device" tab, and select a particular certificate from the list. Then click „OK". Certificates from the currently connected device and ECSigner cloud signature certificates are displayed in this tab.

In the „Personal Certificates" tab all of the registered in Windows certificates are displayed (including non-qualified certificates which are not placed on the cryptographic device).

It is recommended to use the „Cryptographic device" tab, as in such a case the application refers directly to the certificate from the connected cryptographic device.

6. After selecting the certificate and clicking „OK", a pop-up window with relevant information will appear. After reading the message click „OK".

7. In case of electronic signature on a USB device, PIN code has to be entered. If the PIN is correct, signature will be made.
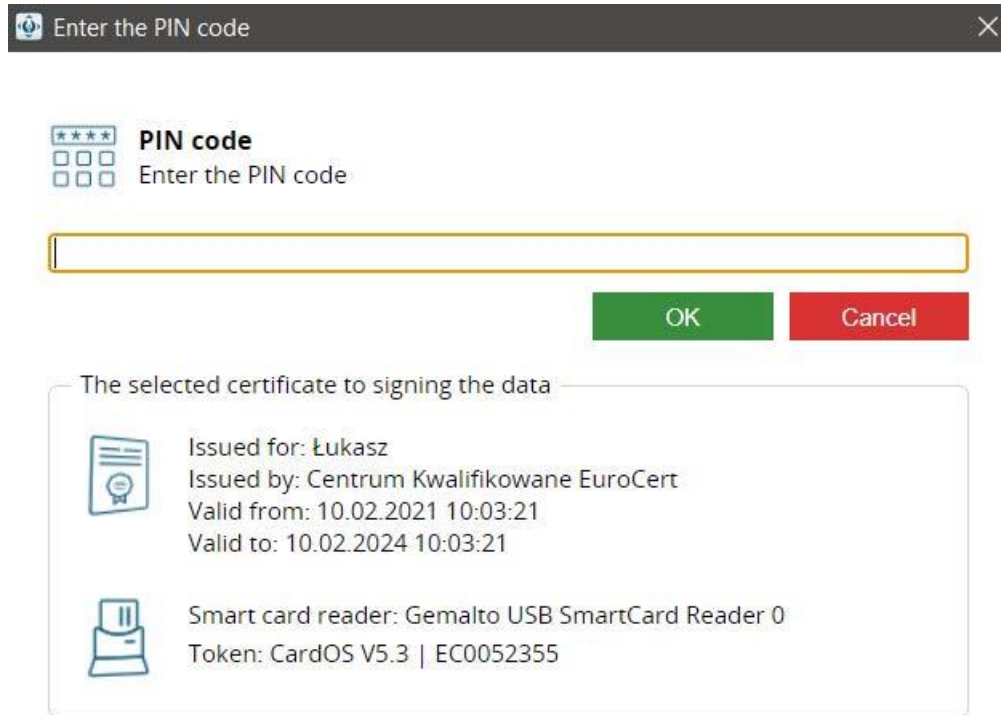
In case of ECSigner cloud signature, user has to log in using his email address and password and then enter the authorization code (OTP code) from the mobile ECSigner application.

8. The last step is to check the signature status. If the document has been successfully signed – the status in the window next to the signed file will be „Signed". If an error has occurred during the process – the status will be „Unsigned".
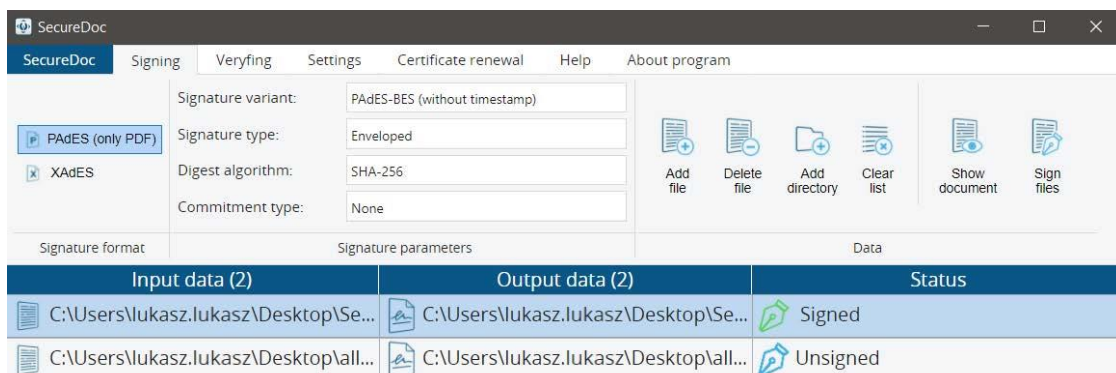
4.4 Signing a PDF file with graphical representation

To sign PDF files with graphical representation, "Perform graphic signature when creating a signature in PAdES format" option must be enabled in „Settings" tab. Then the signature process will contain an additional step, in which the PDF file preview is displayed.

After clicking the rubberstamp icon and clicking on a particular place in the file, the graphical representation will be placed.
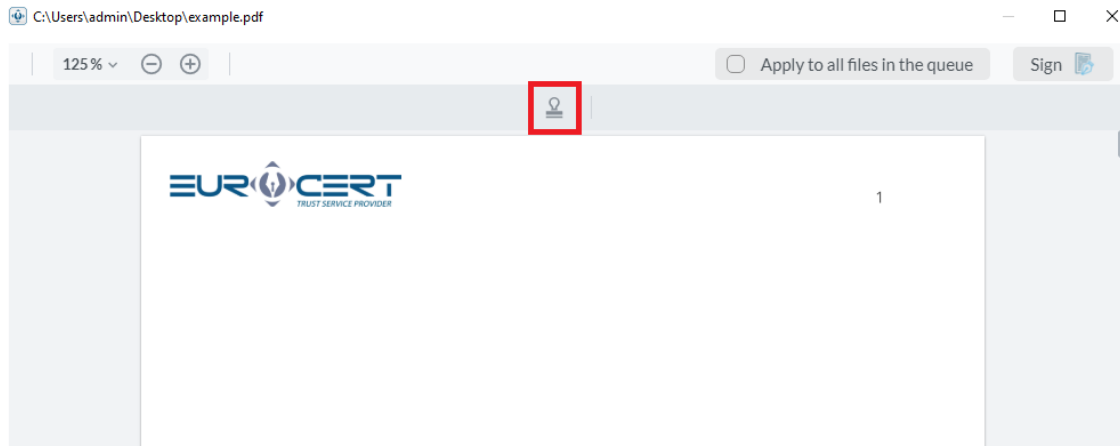
After clicking „Sign" button, the signature will be created. If there are more files in the queue for signing, these steps must be repeated. During the signature process only one graphical representation can be added on a given file.

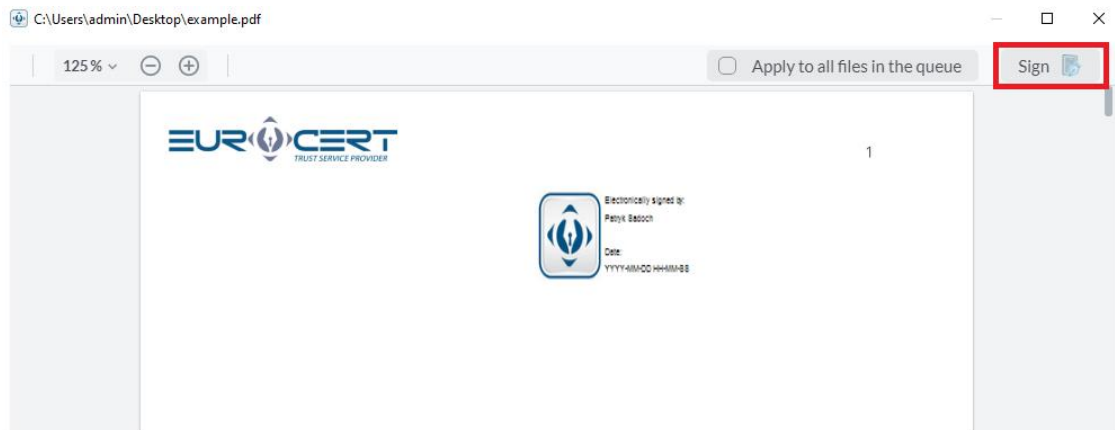When signing a lot of PDF files, user can add a graphical representation on the first file, then enable the „Apply to all files in the que" option and then click "Sign" button. This way all files will be signed with the graphical representation in the same place.

4.5 Adding signatures to a previously signed file

To add a signature to a file that was previously signed – add the file and proceed in the same way as you would normally sign any file. When the „Choose an action" window will appear – click the „Add signature" button.

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

Choose an action

Signature fileC:\Users\lukasz.sawon\Desktop\SecureDoc manual Windows - ENG.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. Veryfing

In this tab user can verify already signed files and generate a verification report.

The functionality of the „Add file", „Delete file", „Add directory", „Clear list" and „Show document" is exactly the same as the functionality of the corresponding buttons in the „Signing" tab. Files signed using different signature configuration can be added to the list at the same time.

If file was signed using the „Detached" signature type – only the file containing the signature should be added to the list (without the original file). Remember that both the signature file and the signed file should be in the same folder. Otherwise, the application will not be able to refer to the source file (signed with detached signature type).

In the case of an internal signature (Enveloping / Enveloped), signed file has to be added to the list.

5.1 Signed file verification process

1. Add files that you want to verify by clicking „Add file" button or by using drag&drop.
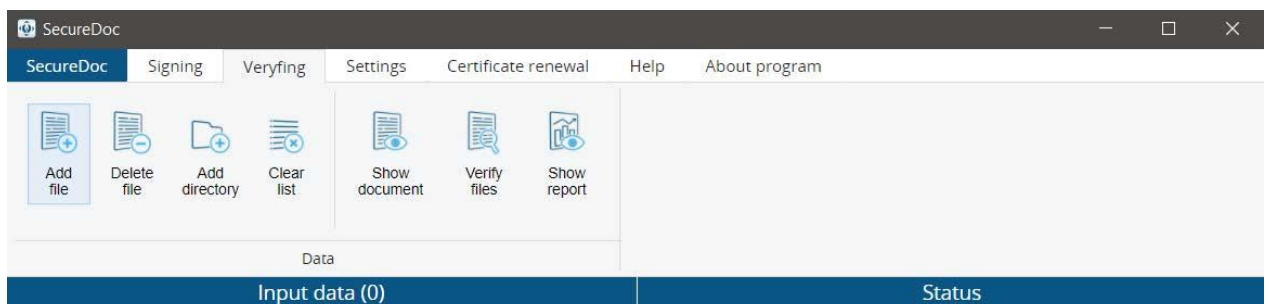
2. Click „Verify files" (Internet connection is required).
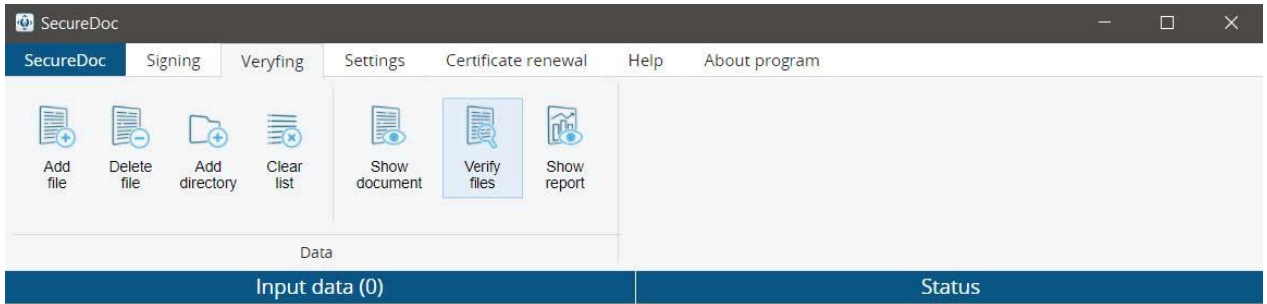
3. Wait for the verification process to finish.
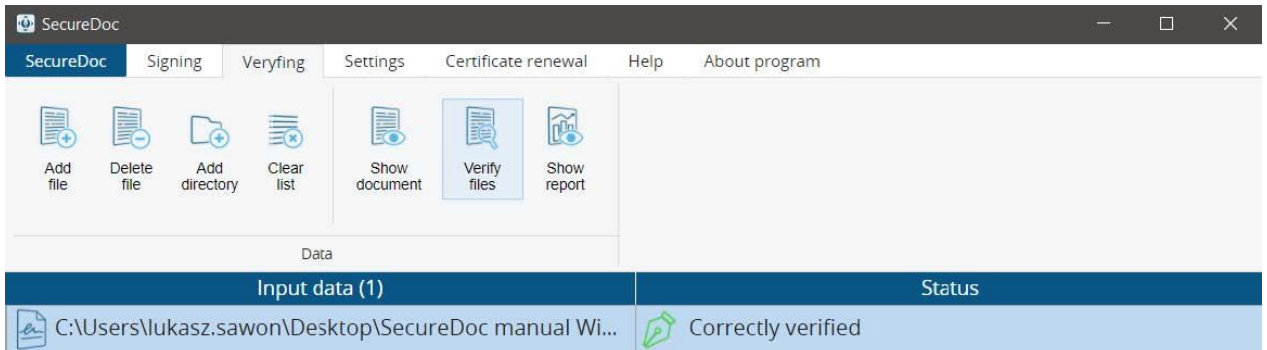
Depending on the result of the verification „Correctly verified" or „Negatively verified" status will appear.

For more information about the verification result click „Show report".

There is also an option to open a verified document by clicking on „Show document".

6. Settings

6.1 Application settings

6.1.1 General settings

6.1.1.1 Language

In order to change the language in General settings, select one of the available languages from the drop-down list in the „Language" section.

6.1.1.2 Updates

During application startup, SecureDoc 2.0 will search for available updates and will display a notification upon finding a newer version. In order to install the newest update, accept the notification and proceed with the installation.

You may also find information about the installed and available versions of the application in this section.
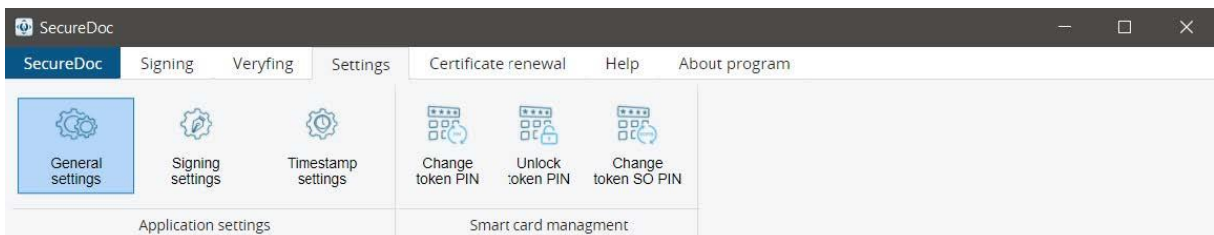
6.1.1.3 Proxy

In this section proxy server can be configured for SecureDoc. In order to configure a proxy, the "Turn on proxy" option has to be enabled. Fill in all the necessary information and click "Save".

Alternatively, system settings can be used for the proxy configuration. To do that, enable both options „Turn on proxy" and „Use system credentials".

Before signing files, it's advised to test the connection by clicking „Check connection to proxy server".

6.1.2 Signing settings

In the Signing settings tab, we can adjust the default settings at the application start-up. Newly set default settings of the signature parameters will be available after application restart.

The following default setting options are available in the application (Each of the available options is explained shortly within SecureDoc v2.0):

- Default signature format
- Default signature variant
- Default signature type
- Default digest algorithm
- Default type of commitment

6.1.2.1 Additional signing options

In this section, we can configure the following options:

"Overwrite a PDF document when a PAdES format signature is created" – Unchecking this option will result in the creation of a signed copy of the file with -sig suffix within the source directory.

With this option checked, the signature will be created within the source file and will overwrite the original document.

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl

"Perform graphic signature when creating a signature in PAdES format" - Selecting this option will allow to add a **graphic signature** when signing with the PAdES signature format (on .pdf documents).

"Do not encode XML data to Base64 when using the Enveloping type in XAdES signature format" – Unchecking this option will allow us to sign the XML files encoded as Base64. Checking this option will allow us to sign XML files normally, using the standard UTF-8 encoding.

"Overwrite the XML document when using the Enveloping type in XAdES signature format" – If the signed file is in XML format, and we need to sign it keeping the original file extension - **check** this option.

If we need to create the XAdES file out of XML file - **uncheck** this option.

"Create the Enveloped signature type in standard version" – A signature created with this option checked will disallow adding next signatures to the document.

6.1.3   Timestamp settings

To sign files using timestamps, the timestamp configuration has to be done beforehand. The client will obtain the required configuration data via email upon purchasing the optional Timestamp service product. This data has to be entered here and saved.

- Timestamp server address – personalized access link to the timestamp server
- Username – personalized login
- Password – personalized password (cannot be changed)

After saving the data, it's advised to test the connection to the server by clicking „Check timestamp configuration" button.

6.2 Smart card management

Warning! If the PIN was entered incorrectly three times, it will get locked. In order to unlock the PIN code, follow the instructions in the "Unlock token PIN" section.

6.2.1   Change token PIN

To change your PIN code, click „Change token PIN" button. The following window will appear:

First enter your current PIN code in the "Old PIN" field, then enter the new PIN code twice.

The minimal PIN length is 4 characters. The maximum PIN length is 8-10 characters. New PIN can contain any characters: numbers, letters (lowercase, uppercase), symbols, and other.

6.2.2 Unlock token PIN

Entering the incorrect PIN code three times will lock it. In order to unlock the PIN code, press "Unlock token PIN", then the following window will appear:

Enter your SO PIN code, then enter new PIN code twice.

WARNING! If incorrect SO PIN was entered three times, the cryptographic card will be irreversibly locked. In such a case, a new cryptographic card with a new certificate will have to be purchased.

6.2.3   Change token SO PIN

To change your SOPIN code, click „Change token SO PIN" button. The following window will appear:

Enter your current SO PIN, then enter new SO PIN twice.

New SO PIN can contain any characters: numbers, letters (lowercase, uppercase), symbols, and other characters. Minimal SO PIN length is 4 characters, the maximum length depends on cryptographic card modes, and normally is 8-10 characters.

WARNING! If incorrect SO PIN was entered three times, the cryptographic card will be irreversibly locked. In such a case, a new cryptographic card with a new certificate will have to be purchased.

Additional information:

During the PIN / SO PIN code change procedure, only one cryptographic card can be connected. Connecting more devices can cause locking the card. EuroCert does not take responsibility for the causes of not following the aforementioned procedure.

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy: Dział techniczny: +48 22 390 59 95
+48 22 490 36 45   +48 22 490 49 86   biuro@eurocert.pl
handlowy@eurocert.pl   wsparcie@eurocert.pl   www.eurocert.pl

7. Certificate renewal

Purchase renewal

To buy the certificate renewal, go to our website (sklep.eurocert.pl) or contact with our sales department (sales@eurocert.pl).

Certificate renewal

We suggest starting the renewal procedure at least 7 days before the expiration date of the current certificate. If the procedure had been started less than 72 hours prior to the expiration date, we do not guarantee a successful renewal.

After purchasing the renewal code, go to the "Certificate renewal" tab in SecureDoc and click the "Certificate renewal" button.

Enter your renewal code in the new window. Fill in the form and sign the newly generated agreement with your valid signature.

Please notice that purchasing the renewal code does not result in renewing the certificate. The Certificate will be renewed only after finishing the Certificate renewal procedure.

After the agreement had been accepted by EuroCert, enter the renewal code in SecureDoc application in the Certificate renewal tab again. Entering the renewal code after the agreement acceptation will result in activating the renewed certificate.

8. Help

This tab contains our Technical Department's contact details along with a download link leading to AnyDesk remote access application.

9. About program

This tab contains SecureDoc 2 licence terms.

EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
KRS: 0000408592
NIP: 9512352379

Dział handlowy:
+48 22 490 36 45
handlowy@eurocert.pl

Dział techniczny:
+48 22 490 49 86
wsparcie@eurocert.pl

+48 22 390 59 95
biuro@eurocert.pl
www.eurocert.pl