

User manual



Version 1.2



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

Table of Contents

1. Program information.....	3
2. Minimum system requirements.....	3
3. Application installation.....	3
4. Signing.....	5
4.1 "Signature parameters" section.....	6
4.1.1 Signature variant.....	6
4.1.2 Signature type.....	7
4.1.2.1 Detached.....	7
4.1.2.2 Enveloping.....	7
4.1.2.3 Enveloped.....	8
4.1.3 Digest algorithm.....	8
4.1.4 Commitment type.....	8
4.2 „Data” section.....	9
4.3 Signing process.....	9
4.4 Adding signatures to a previously signed file.....	12
5. Verifying.....	12
5.1 Signed file verification process.....	12
6. Settings:.....	13
6.1 Application Settings.....	13
6.1.1 General settings.....	13
6.1.2 Signing settings.....	14
6.1.3 Timestamp settings.....	15
6.2 Smart card management.....	15
6.2.1 Change token PIN.....	15
6.2.2 Unlock token PIN.....	16
6.2.3 Change token SO PIN.....	17
7. Certificate renewal.....	17
8. Help.....	18
9. About program.....	18



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

- Mac OS High Sierra or newer,
- card management software - Charismathics Smart Security Interface,
- internet connection (necessary during the verification process).

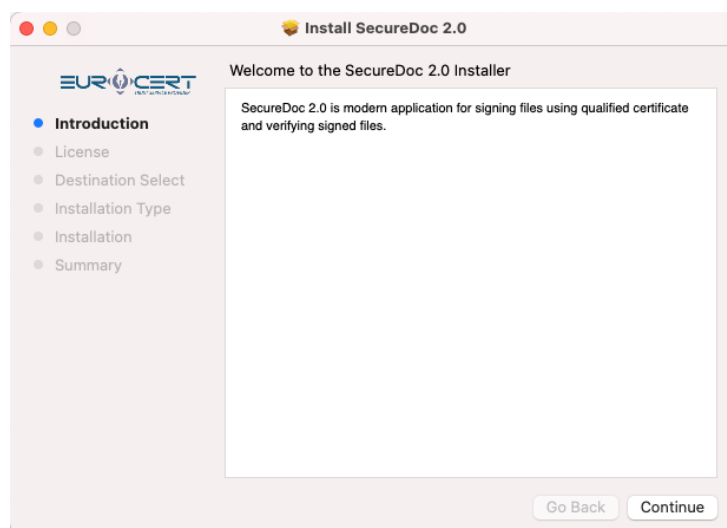
3. Application installation

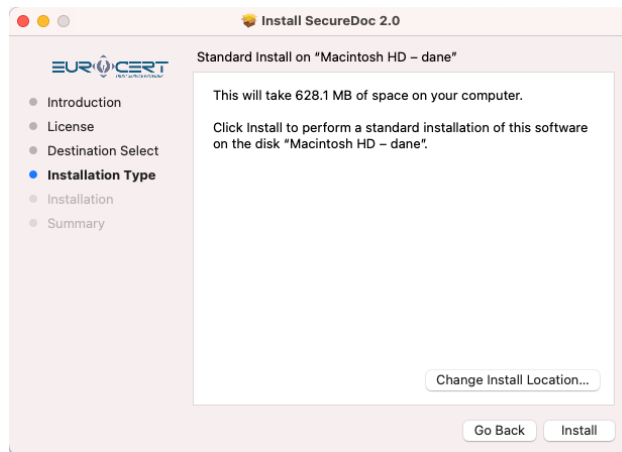
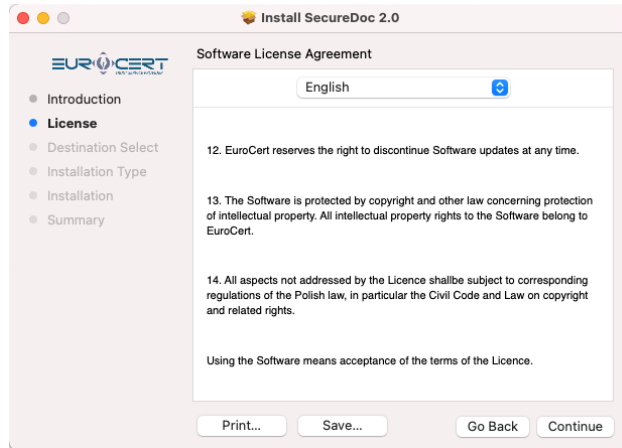
To start installing the application, go to

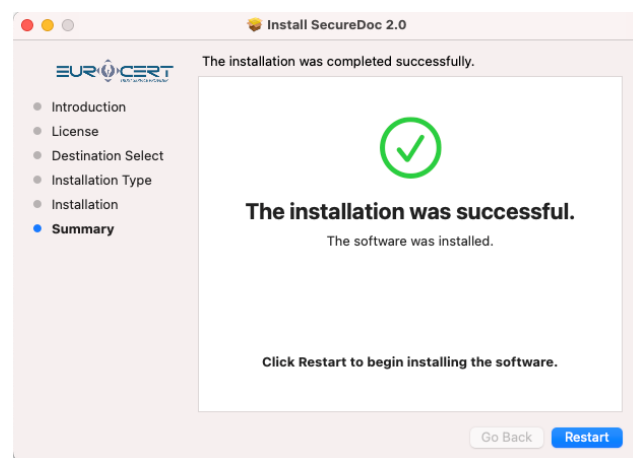
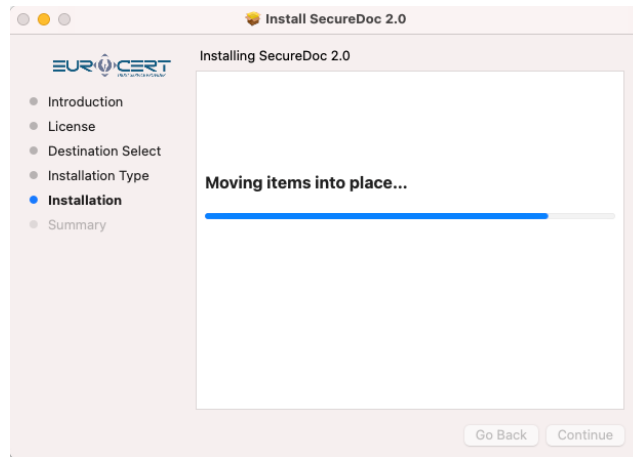
<https://eurocert.pl/index.php/oprogramowanie>

and download "*SecureDoc 2 - application for signing and verification of qualified signatures*".

After running the downloaded installer, follow the dialogue boxes below:





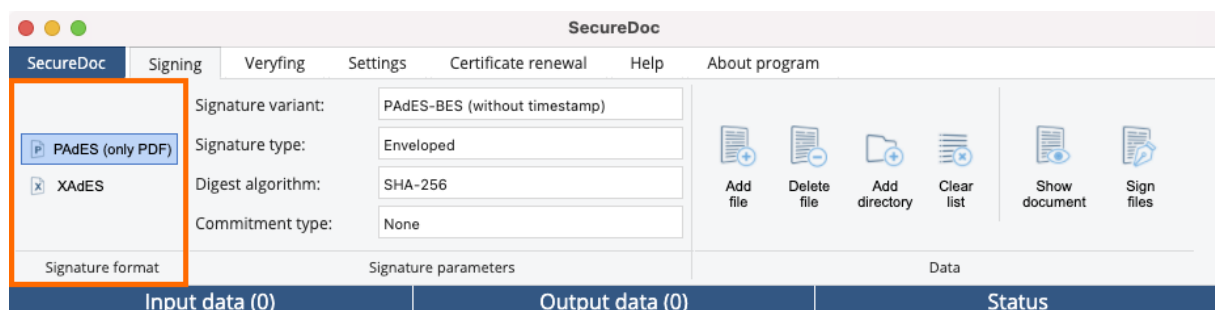


After completing this step, the application is ready for use.

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 and XAdES.

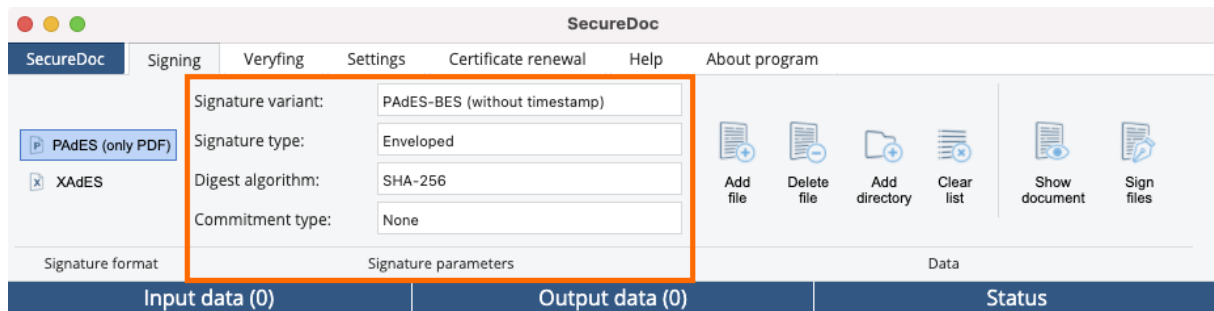


PAdES signature format is dedicated and exclusive for PDF files and is a recommended option when signing any document with the PDF extension.

XAdES signature format can be used to sign any file format (.xml, .docs, .docx, .xmls, .jpeg, .odt etc.). PDF files also can be signed using XAdES signature format, however, as mentioned above – for PDF it's recommended to use PAdES.

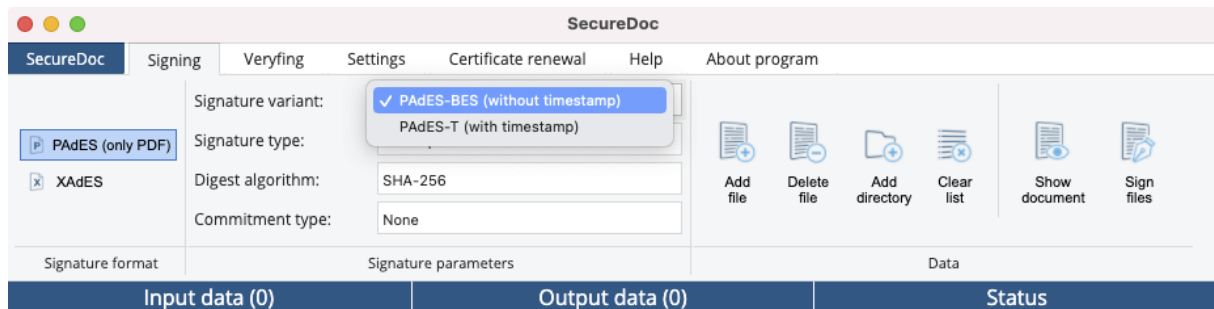
4.1 "Signature parameters" section

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 *Signature Variants* 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, however, indicates that the performed signature will be created 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.

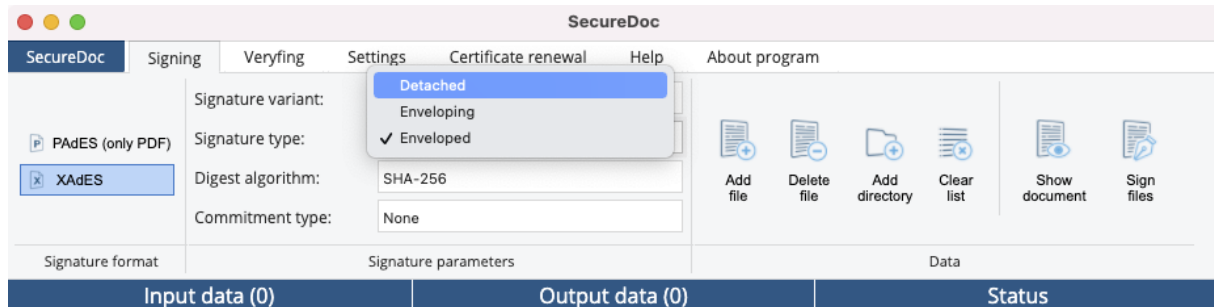
Timestamping makes it possible to confirm the time and date when the electronic signature was placed on the file or to determine if a given document existed at a specific time and has not been changed since. Under the provisions of applicable law, this has effects of a *date certain*.



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



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.

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.

The file which is being created after signing the document with a detached signature type has a XAdES format.

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.

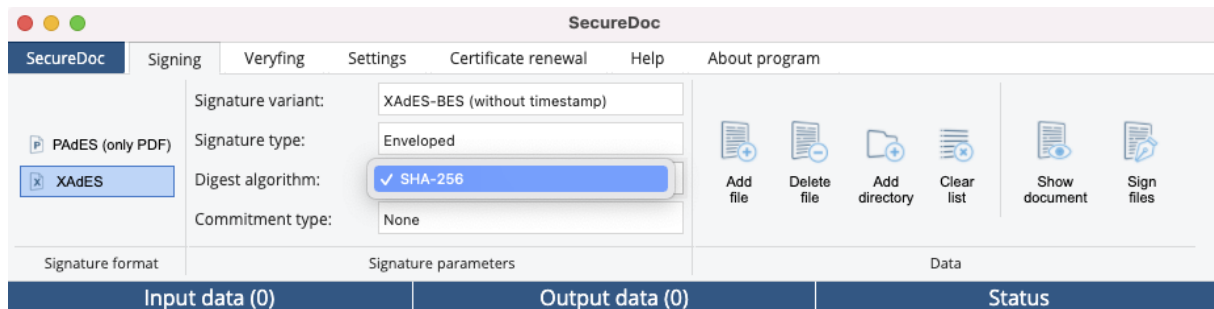
So, if for example, we sign a file „document.txt”, the resulting file (containing the signature) will be named „document.txt.XAdES”.

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 a signature as well.

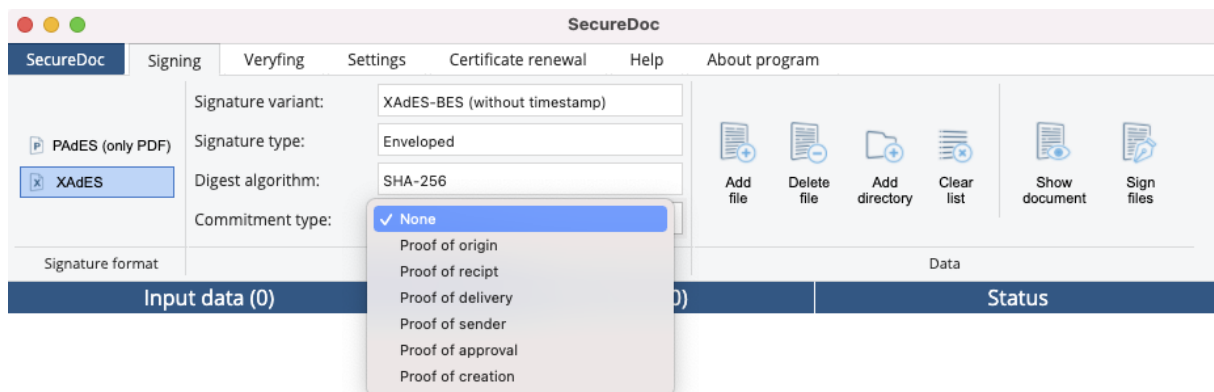
So if we want to sign an XML file so it contains the signature with the content of the document – Enveloped signature type should be selected. This signature type applies only to XML file formats.

4.1.3 Digest algorithm



- SHA-256 is a type of cryptographic security option, the higher value provides higher security.

4.1.4 Commitment type

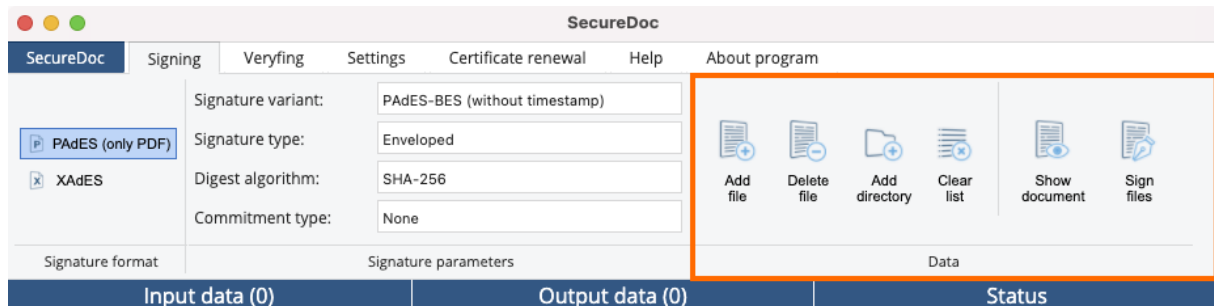


This field is optional and contains additional information about the signing reason. There are 6 types of commitments to choose from:



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

4.2 „Data” section



After clicking on „Add file” in the appeared window signing files should be selected.

„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 the entire list of selected files.

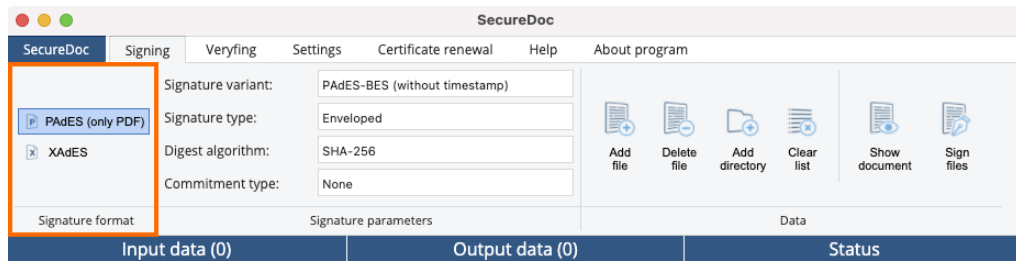
Pressing the „Show document” button will cause the content of the selected document to be displayed in a new window.

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

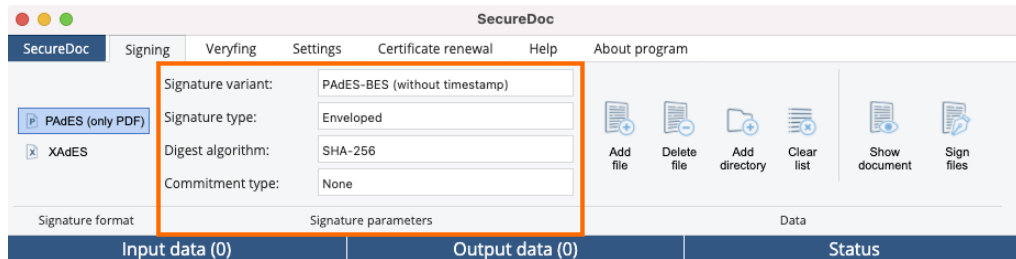
4.3 Signing process

Please remember that in order to sign a file using a qualified signature, the device with a cryptographic card must be inserted into a PC.

1. Specify the signature format with which the document should be signed (in the „Signature format” section)

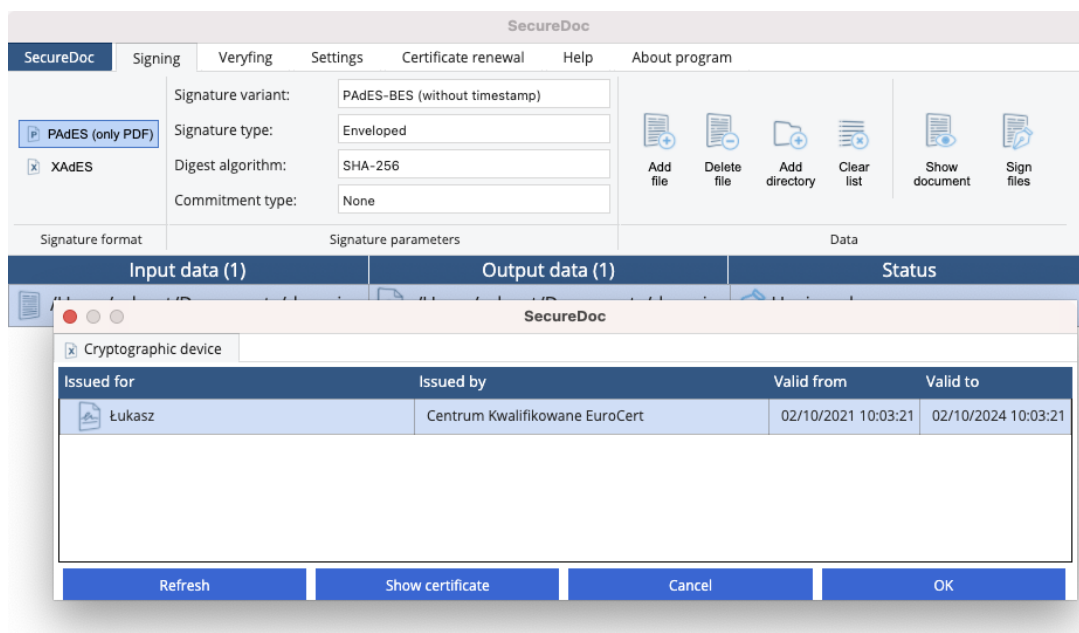


2. Select the required signature parameters in the „Signature parameters” field



3. Add files you would like to sign
4. Click „Sign files”. It is worth noting that all of the documents from the selected files list will be signed with the same signature parameter settings.
5. After clicking on „Sign files”, the certificate selection window will appear. Select the „Cryptographic device” tab, and from the list select a certificate with which you want to sign selected files. Then click „OK”. In this tab certificates from the currently connected device are displayed. In the „Personal Certificates” tab all of the registered in Windows certificates are displayed (including non-qualified certificates which are not placed in the cryptographic device).

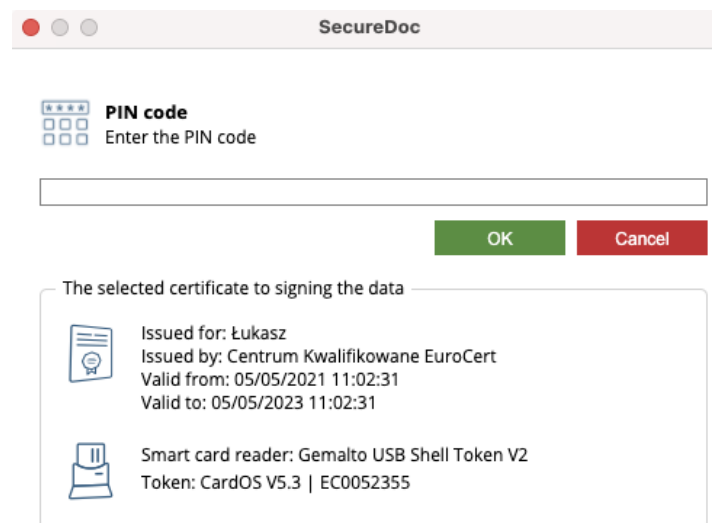
It is recommended to use the „Cryptographic device” tab, as in such a case the application refers directly to the certificate from the connected cryptographic device.



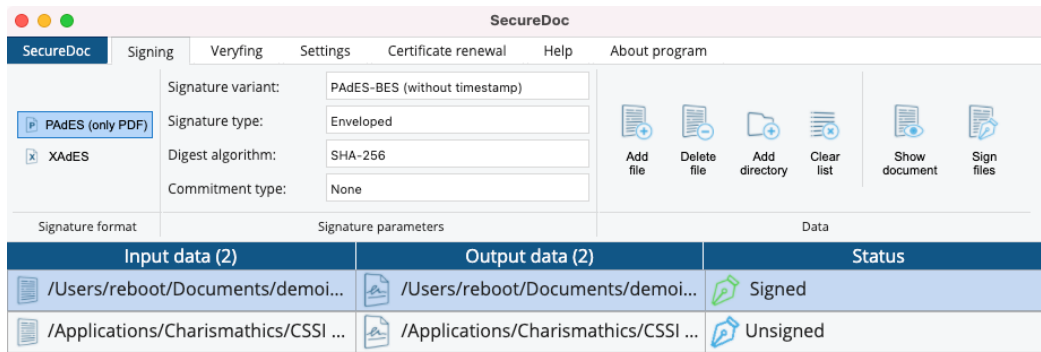
6. After selecting the certificate and clicking „OK”, a pop-up window with relevant information will appear. After reading the message click „OK”.



7. Next, we have to enter the PIN code in the appeared window and click „OK”. If the provided PIN is correct – the application will start the signing process.

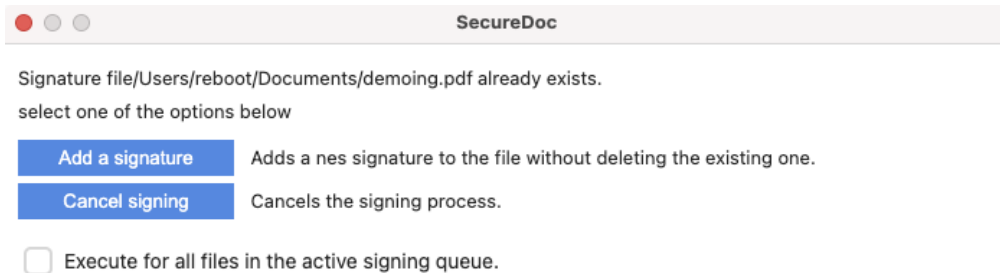


8. The last step is to check the signature status. If the document has been successfully signed – the status in the window next to the signed file will be „Signed”
If an error has occurred during the process – the status will be „Unsigned”.



4.4 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 „Add signature” window will appear – select the „Add signature” option.



5. Verifying

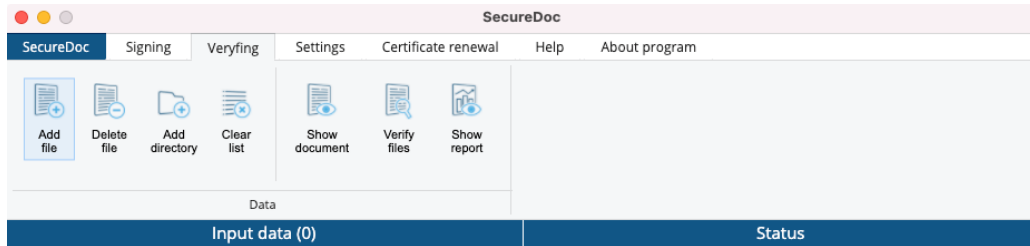
This tab provides functionality for signed files verification as well as displaying a verification report.

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.

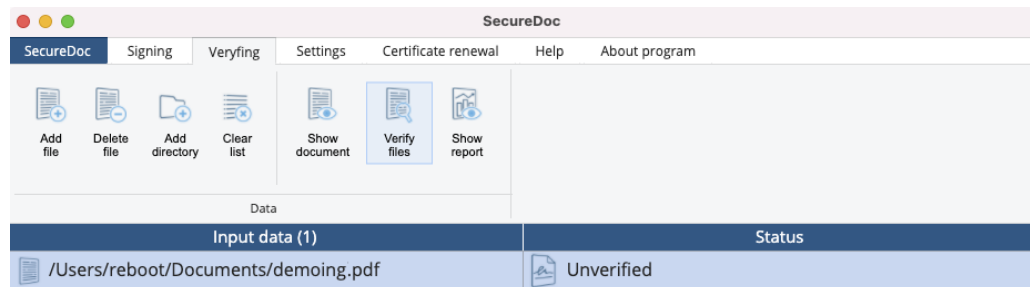
It is worth mentioning that files of different signature types can be added to the verification list at the same time. If a file is signed using the „Detached” signature type – only the file containing the signature should be added to the list (without the original file). Additionally, remember that 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), it is enough to indicate just the signed file alone.

5.1 Signed file verification process

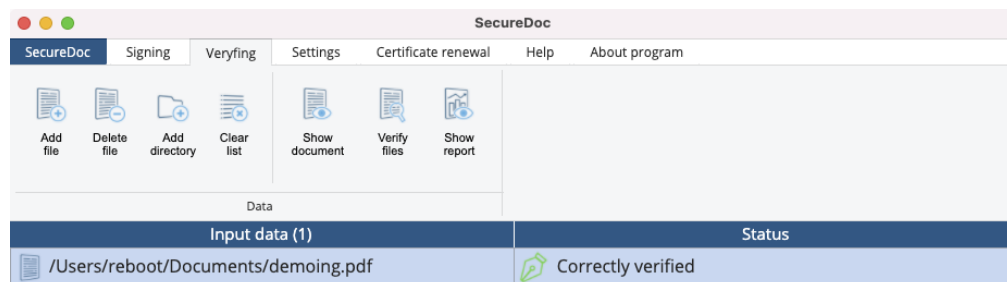
1. Add files to be verified



2. Click „Verify files” (remember that to perform verification, the internet connection is required)



3. Wait for the verification process to finish



Depending on the result of the verification, the following statuses could appear:

„Correctly Verified” or „Negatively Verified”

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

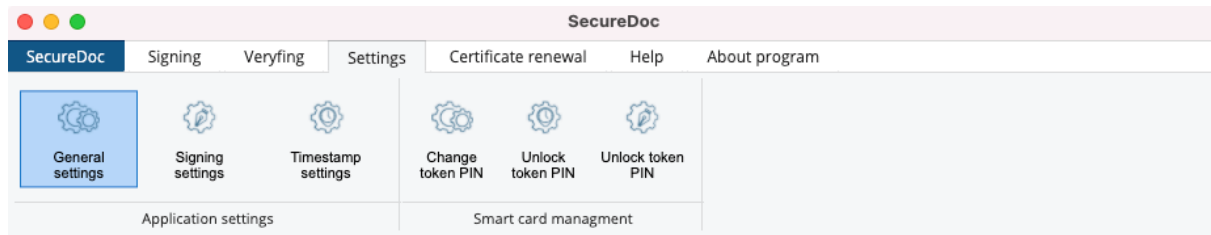
There is also an option to open a verified document by clicking on „Show document”

6. Settings:

6.1 Application Settings

6.1.1 General settings





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.

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.

Proxy

Proxy configuration settings for SecureDoc will be available in the Proxy section within the General Settings tab. In order to configure a proxy, the “Turn on proxy” option has to be checked, with all the necessary information filled in.

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

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.

“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 further signatures to the document.

6.1.3 Timestamp settings

To be able to sign files using the timestamp, the configuration will be required beforehand.

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

The client will obtain the required configuration data upon purchasing the optional Timestamp service product.

6.2 Smart card management

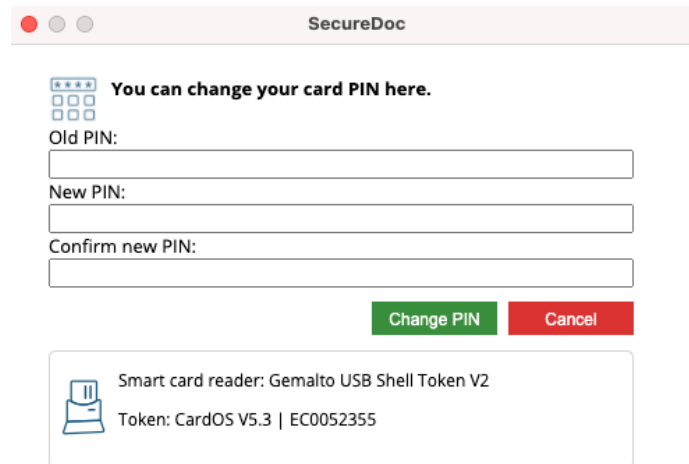
Warning! If the PIN was entered incorrectly three times, it will get locked.

In order to unlock the PIN code, follow the instructions in the “Unlock token PIN” section.

6.2.1 Change token PIN

In order to change the PIN code, click “Change token PIN”. Afterward, the following window will show up:





SecureDoc

You can change your card PIN here.

Old PIN:

New PIN:

Confirm new PIN:

Smart card reader: Gemalto USB Shell Token V2
Token: CardOS V5.3 | EC0052355

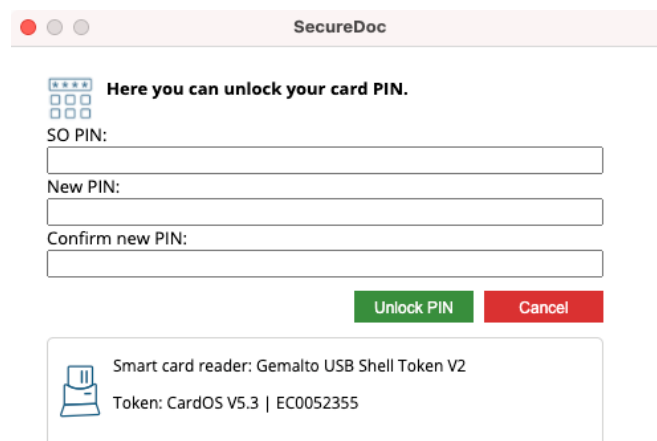
Next, enter the „Old PIN” and enter the „New PIN” twice.

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 characters.

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”, afterward the following window will appear:



SecureDoc

Here you can unlock your card PIN.

SO PIN:

New PIN:

Confirm new PIN:

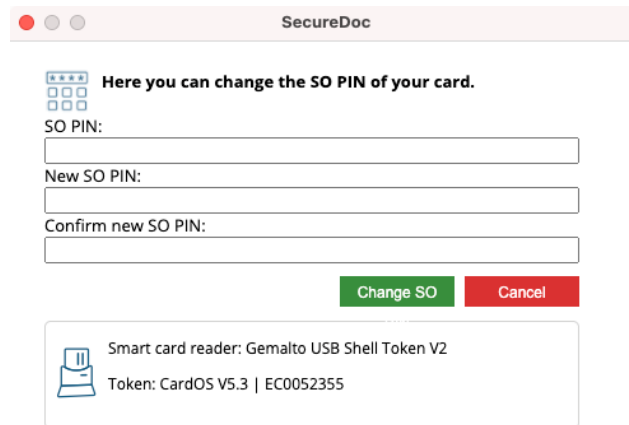
Smart card reader: Gemalto USB Shell Token V2
Token: CardOS V5.3 | EC0052355

Next, enter “SO PIN” and provide a “New PIN” 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

In order to change the SO PIN code, click “Change token SO PIN”. Afterward, the following window will appear:



The screenshot shows a window titled "SecureDoc" with a light pink header. Below the header, there is a section with a blue icon of a card and the text "Here you can change the SO PIN of your card." followed by a 2x2 grid of small squares. Below this are three input fields labeled "SO PIN:", "New SO PIN:", and "Confirm new SO PIN:". At the bottom right of this section are two buttons: a green "Change SO" button and a red "Cancel" button. Below the input fields is a box containing a smart card reader icon and the text "Smart card reader: Gemalto USB Shell Token V2" and "Token: CardOS V5.3 | EC0052355".

Next, enter the “Old SO PIN” and provide the “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 info:

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

7. Certificate renewal

Purchase renewal

Clicking this button will redirect us to the store page (sklep.eurocert.pl) in the „Online renewal – for current EuroCert customers” product.

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, proceed to the "Certificate renewal" tab and click the Certificate renewal button.

We'll have to input the renewal code in the prompted window. Afterward, fill the form and sign the generated agreement with a 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 acceptance 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 connection application.

9. About program

This tab contains SecureDoc 2 licence terms.

