



User guide

proCertum SmartSign

Version 1.10
(valid from version 9.4.4.0)

Copyrights of this documentation and software described belong to **Asseco Data Systems S.A.** seated in Gdańsk, Poland, ul. Jana z Kolna 11. The above rights are secured by act on copyright and derivate laws (Dz. U. No. 24, item 83, of 4th February 1994 with its following changes).

The following documentation is spread on the basis of granted license.

Table of Contents

1. INTRODUCTION	4
2. HARDWARE AND SOFTWARE REQUIREMENTS	5
3. APPLICATION UPDATE.....	6
3.1 EXE packet update	6
3.2 MSI packet update	7
4. APPLICATION INSTALLATION	9
5. APPLICATION OPERATION	13
Help	15
Settings.....	17
5.1.1. Settings – General	18
5.1.2. Settings – Signature	20
5.1.3. Settings – Verification.....	26
5.1.3.1. Basic options of verification.....	26
5.1.3.2. Additional options of verification.....	27
5.1.4. Settings – Timestamp.....	27
File signing.....	29
5.1.5. Adding elements to the list	29
5.1.6. Signature operation	30
5.1.7. Multiple signature	34
5.1.8. Countersignature	36
5.1.9. Signing PDF files.....	38
5.1.9.1. Adding graphic symbol of signature	38
5.1.10. Context menu.....	41
Signature verification	42
5.1.11. Adding elements to the list.....	43
5.1.12. Information about signature and document, which is being verified.....	43
5.1.13. Verification operation	45
5.1.14. Verification status	47
5.1.15. Context menu.....	49
System context menu	50
Update reporting.....	51
6. TABLE OF WINDOWS.....	53

1. Introduction

proCertum SmartSign is an application designed for signing documents with electronic signature.

Note: It is recommended to use the current version of the **proCertum SmartSign** software, which can be downloaded from:

<https://support.certum.eu/en/software/procertum-smartsign/>

proCertum SmartSign application:

- supports qualified certificates issued by Asseco Data Systems S.A. as well as KIR, PWPW, Enigma, and Eurocert. KIR Graphite, PWPW Dark, PWPW Blue, Enigma, and Eurocert cards are supported exclusively via the CSP interface.
- supports non-qualified certificates issued by Asseco Data Systems S.A.
- creates e-signatures in **XAdES**, **CAAdES/ETSI** or **PAAdES** formats. Created signature can be an **internal signature** (signature file will contain document's content) or an **external signature** (signature file will include only information about signature);
- marks documents with **qualified** or **non-qualified timestamp**, when reference to reliable time as well as confirmation is required, that the document or signature was existing at that moment;

2. Hardware and software requirements

Please find minimal hardware and software requirements enabling correct operation of **proCertum SmartSign** application below:

- PC/Laptop class computer;
- operating system (64-bit architecture) Windows 11;
- configured Internet connection;
- cryptographic card reader*;
- cryptographic card*;
- software driving operation of card readers*.

Attention!

Cryptographic card reader, cryptographic card as well as software managing operation of readers are required only in case of signing process with qualified signature.

Additionally, for the application to work correctly, it is required that the application has access to the following addresses:

213.222.201.0 - 213.222.201.255

213.222.198.0 - 213.222.198.255

<http://time.certum.pl>

<http://public-qlts.certum.pl>

<http://public-qlts.certum.pl/qts-17>

<http://qts10.clide.certum.pl>

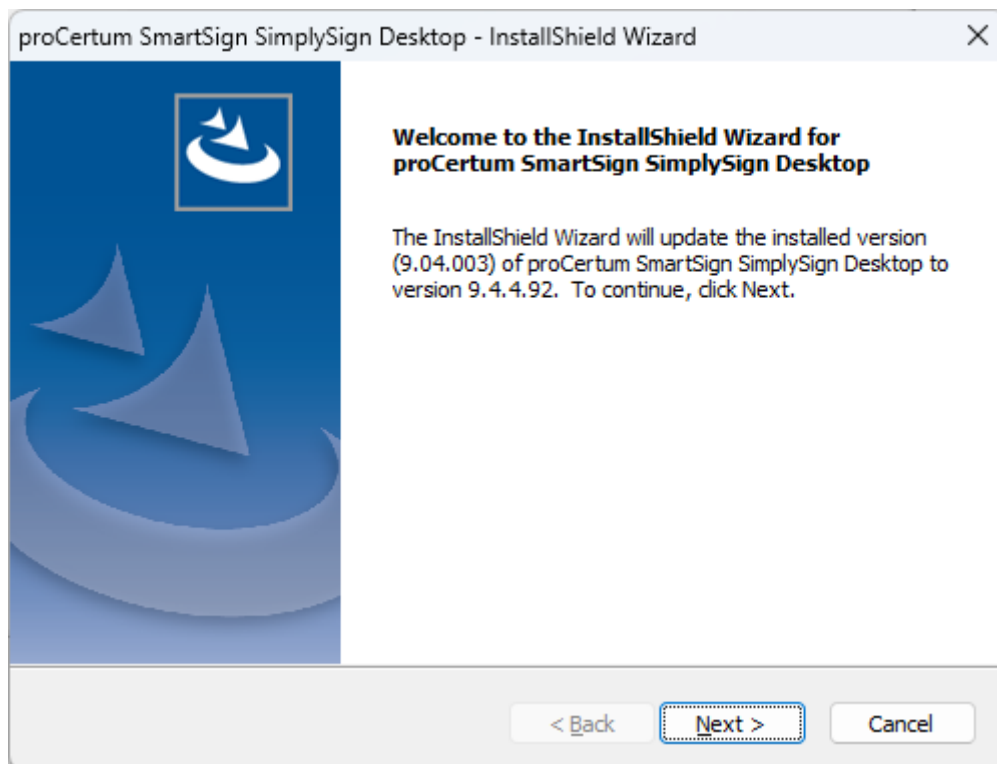
<http://qts.certum.pl/default/clide>

<http://ocsp.certum.pl/>

3. Application update

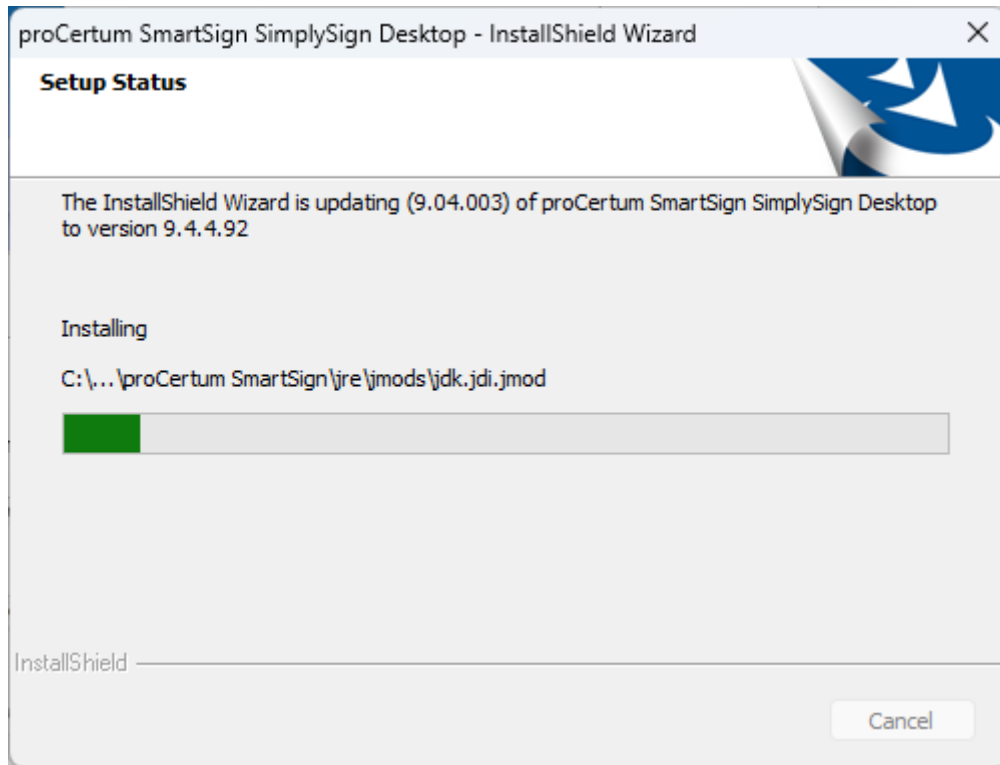
3.1 EXE packet update

To update an application installed from an EXE package, download the appropriate new EXE package, **close** the **proCertum SmartSign** and **SimplySign Desktop** applications, and then run the downloaded EXE package. An installer window will appear informing you that an update will be performed.



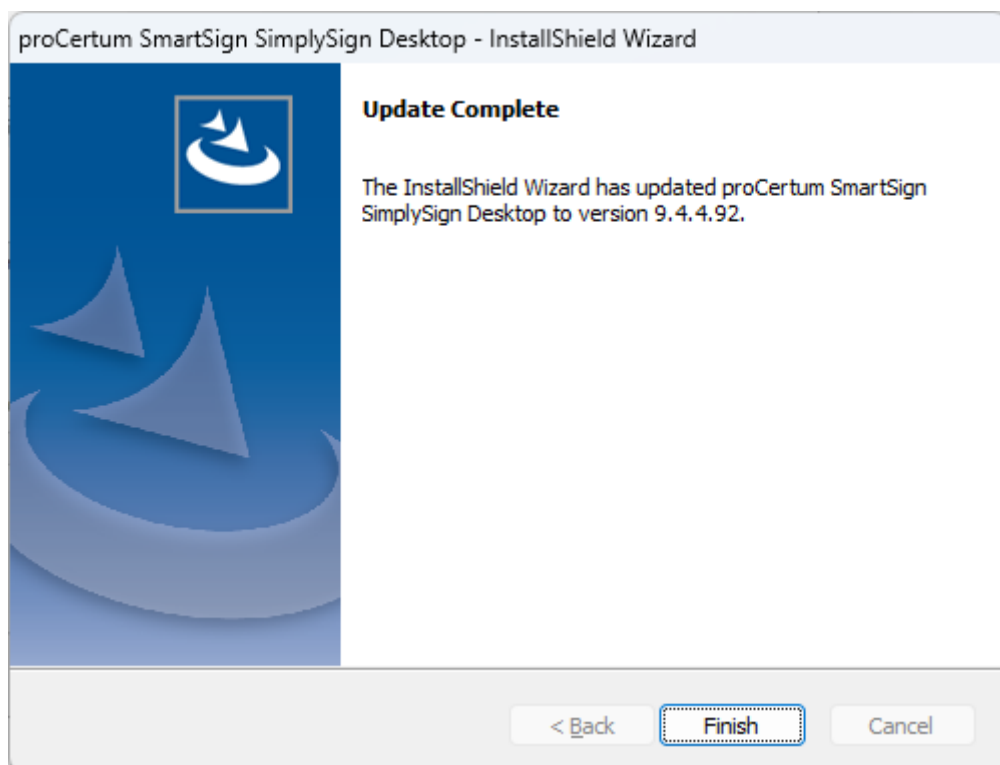
Window 1: Update information

After pressing the **Next** button, the application update will begin.



Window 2: Update progress

After the update is completed, the installer will display a window informing you that the update has been completed.



Window 3: Information about the end of the update

3.2 MSI packet update

To update an application installed from an MSI package, download the appropriate new MSI package, disable the proCertum SmartSign and SimplySign Desktop applications, and then run the downloaded MSI package using the command:

```
msiexec /i downloaded_package.msi
```

and follow the installation wizard.

You can also update application In **silent mode** by issuing the command:

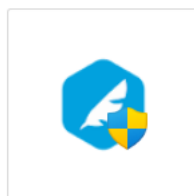
```
msiexec /i downloaded_package.msi /q
```

The update will then be performed without displaying the installer windows.

4. Application installation

To get the **proCertum SmartSign** application started, it should be installed correctly in the system. For this purpose double click **proCertum SmartSign.exe** file icon.

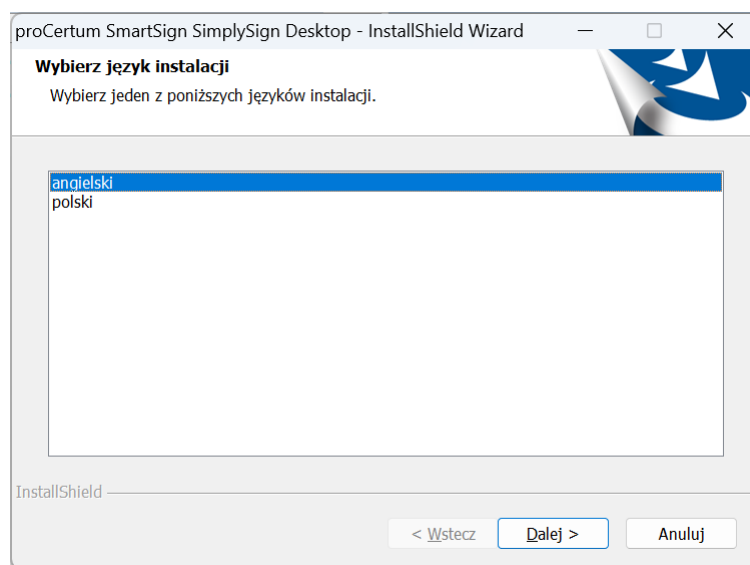
Note: If you have an earlier version of the software installed on your system, it is recommended to uninstall it first.



SimplySignDeskt
op-9.4.4.92-win-
64-bit.exe

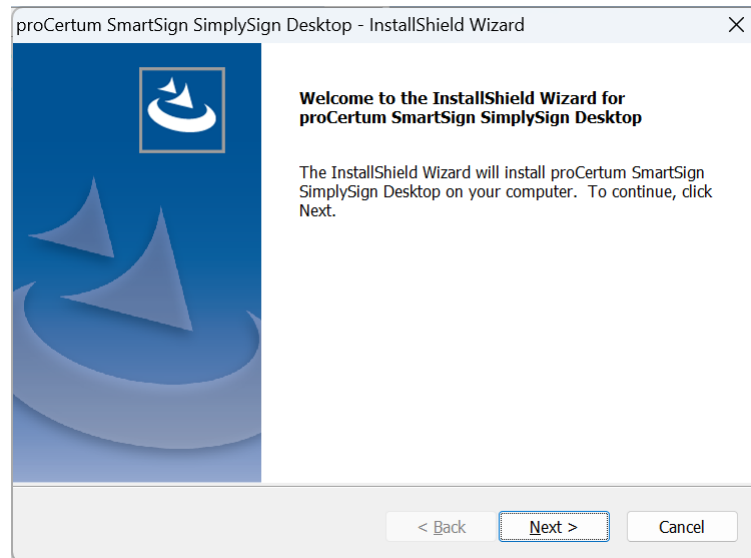
Window 4: Installer Icon

After the installation has been run, the following window will be displayed:



Window 5: Setup language choice

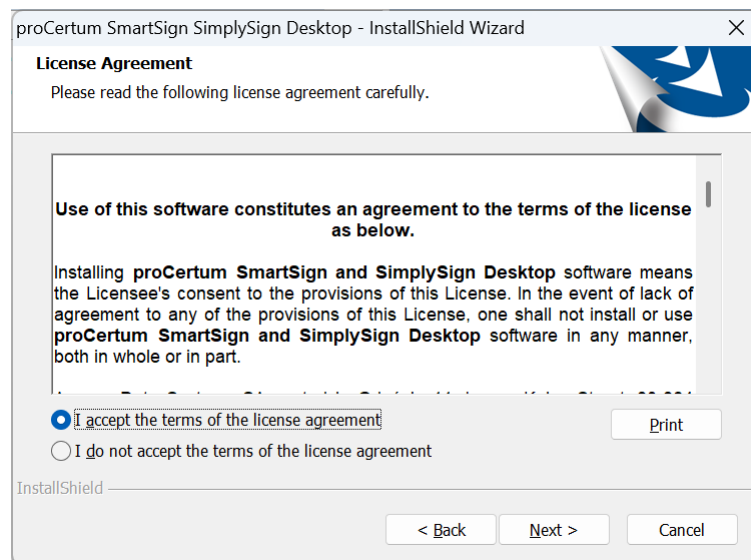
After the language is selected, click **Next >**. The application installation starts. Welcoming window of installation wizard will be displayed then.



Window 6: Welcoming window of installation wizard

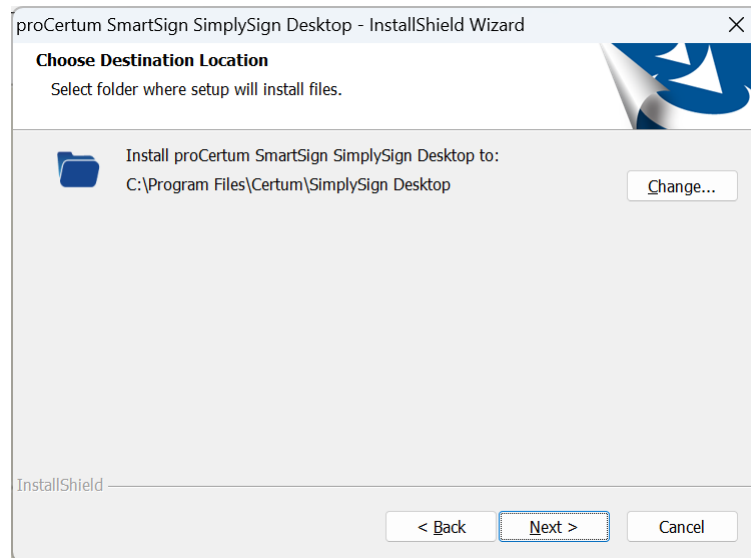
After you have clicked Next > read the license agreement in the installers window.

After you have read the conditions, you must click on **I accept the terms of the license agreement** and then click **Next >**. Otherwise (after choosing an option **I do not accept the terms of the license agreement**) license terms and conditions will be refused and further installation will not be possible.



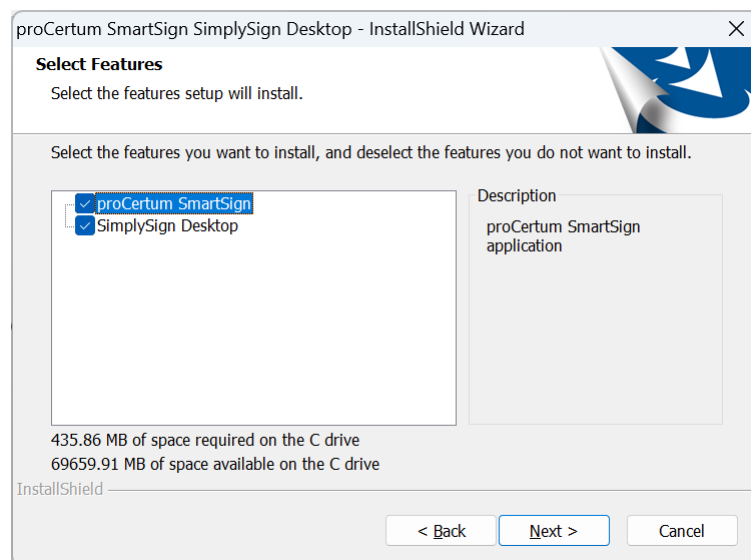
Window 7: License agreement

The next step will be the selection of the location, where the files of **proCertum SmartSign** application should be installed. Defaults to: **C:\Program Files\Certum\SimplySign Desktop**. If we would like to change final destination click Change... and set new final location. After choosing final location click **Next >**.



Window 8: Choose Destination application

You will be presented with the components that can be installed.



Window 9: Selecting the components to be installed

The components that can be installed are:

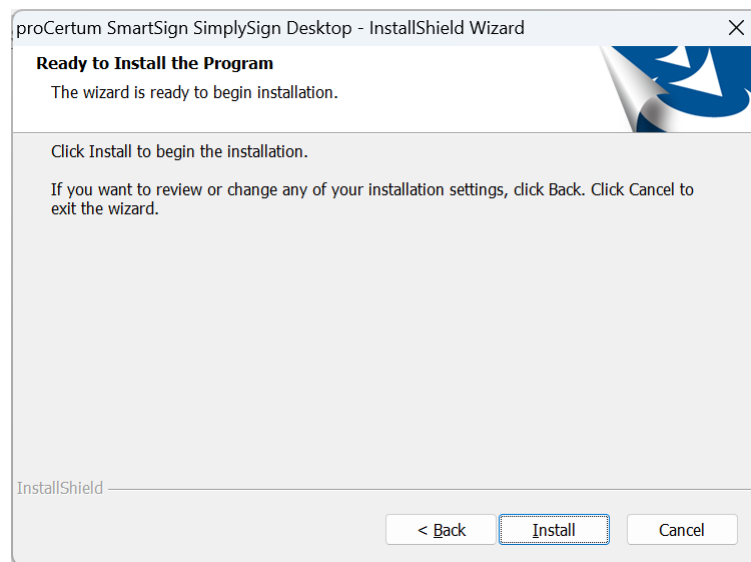
- **proCertum SmartSign** – the proCertum SmartSign application;
- **SimplySign Desktop** – the SimplySign Desktop application;

Those with a physical cryptographic card should deselect the SimplySign component and leave only the proCertum SmartSign component selected.

Those with a certificate on a virtual SimplySign card should leave both components selected.

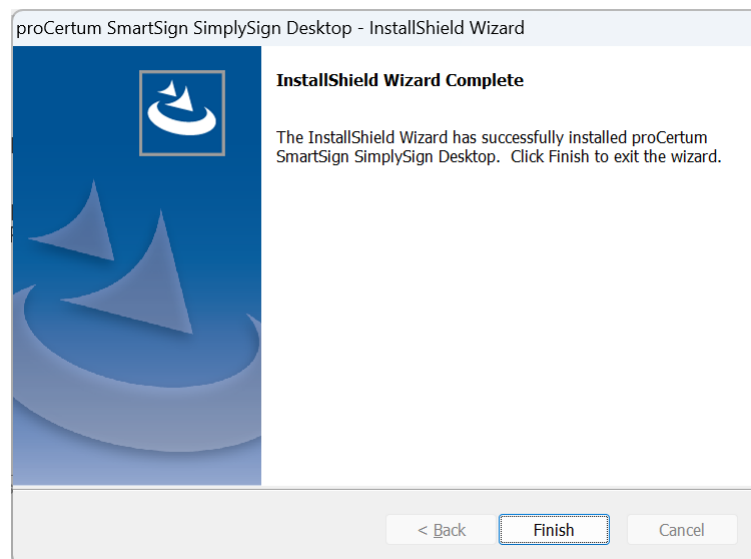
After selecting the appropriate components, click Next. A window will appear informing you that

installation is ready.



Window 10: Installer is ready to start the installation process

After you have clicked **Install** the installation process of **proCertum SmartSign** will be started. If application is installed correctly, the following message will appear:



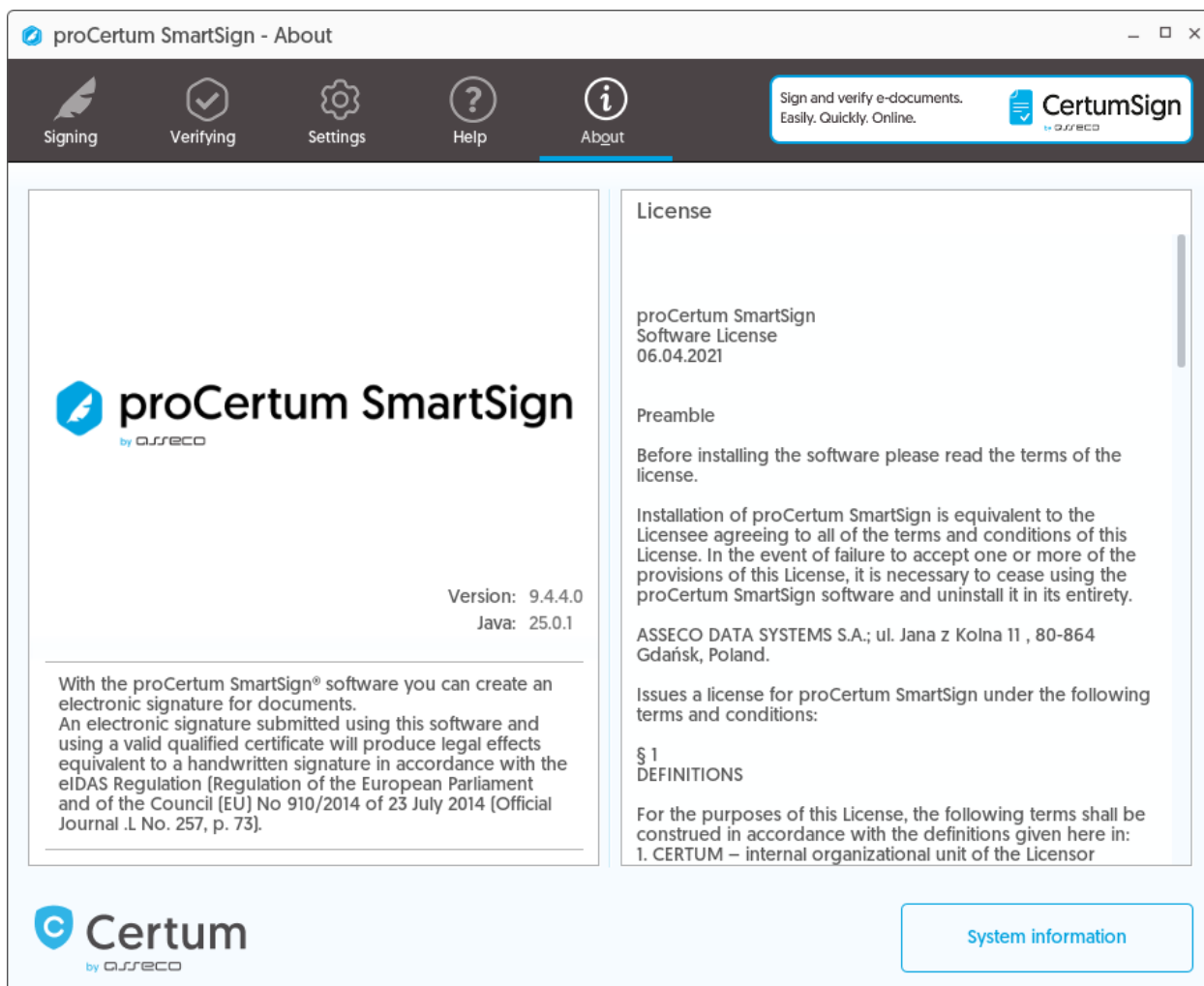
Window 11: The installation process has been successfully completed.

Clicking **Finish** closes **proCertum SmartSign** application installation wizard.

To get the application started, click **proCertum SmartSign** icon, which is available on desktop or in the menu Start > Programs > Certum > proCertum SmartSign.

5. Application operation

proCertum SmartSign is an application designed for signing documents with electronic signature and signature verification. **proCertum SmartSign** can be an element of **secure device for signing with electronic signature** in accordance with the Polish Act on Electronic Signature from 18 September 2001.

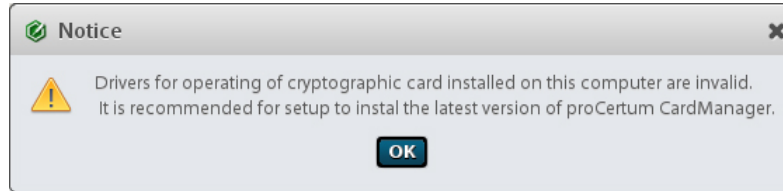


Window 12: Main window of proCertum SmartSign application

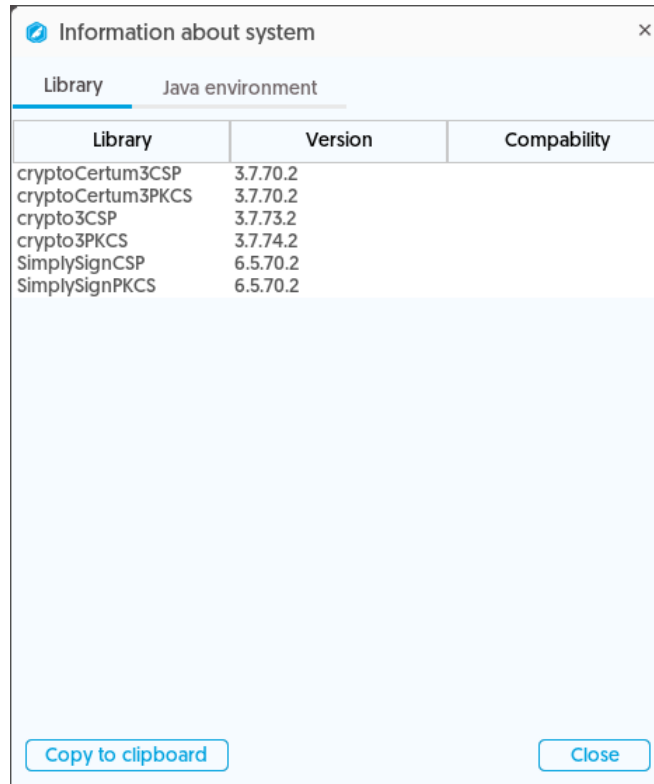
In **proCertum SmartSign** application we can list five tabs:

- **Signing** – realizes electronic signature operation, enables multiple signing and countersignature under already existing signature;
- **Verifying** – realizes electronic signature verification process;
- **Settings** – configuration of signing and verification service;
- **Help** – user's documentation;
- **About Program** – information about version of software and user's license.

There is a **System information** button in welcoming window and **About Program** window. Clicking this button causes displaying window, which contains information about environment, in which the application has been started. The list of libraries designed for cryptographic card operation is being presented in **Libraries** tab of this window. Application possesses embedded verification mechanism of these libraries and in case of incompatibility, the information about that will be displayed in **Compatibility** column. Verification takes place during every start of application. In case of incompatibility of any of libraries, the user will be informed about that.



Window 13: Information about library incompatibility



Window 14: Information about system – Library

The window containing information about Java environment, in which the application works, is presented in **Java Environment** tab.



Window 15: Information about system – Java Environment tab

Help

For assistance in the use of the application, click the **Help** button.

proCertum SmartSign - Help

Signing Verifying Settings **Help** About

Sign and verify e-documents. Easily, Quickly, Online. **CertumSign**

Online support

Use technical support:

We are available on working days from 8:00 a.m. to 4:00 p.m. at the following telephone number:

+48 914 801 340 - mobile calls

801 540 340 - landline calls*

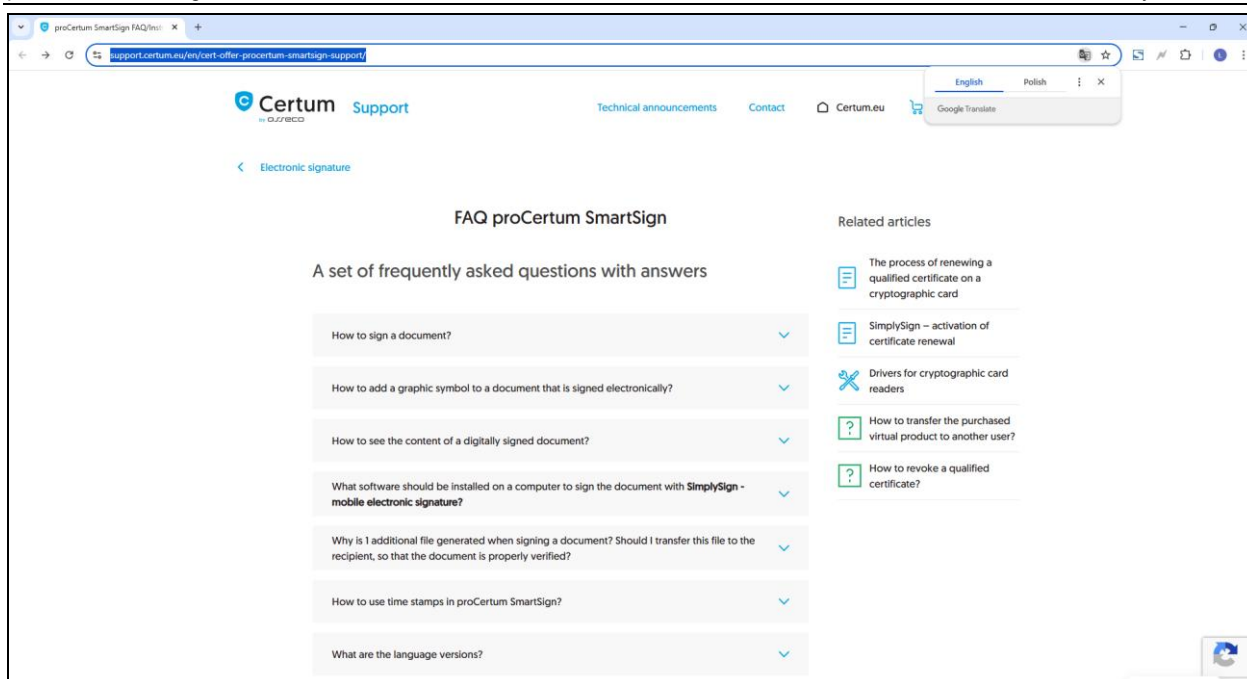
infolinia@certum.pl - our email

* - calls charged according to the mobile operator price list

[Visit](#)

Window 16: Bookmark Help

After pressing the **Visit** button, the user will be redirected to a website with frequently asked questions and their answers.



Window 17: Bookmark Help on the website WWW

Settings

Settings tab is designed for configuration of settings:

- general;
- operation of signing with e-signature;
- e-signature verification operation;
- timestamp,

proCertum SmartSign - Settings

Signing Verifying **Settings** Help About

Sign and verify e-documents. Easily, Quickly, Online. **CertumSign**

General **Signature** Verification Timestamp

UPDATES

Checking available updates: once a day [Recently checked: 2026-04-15 09:01:51] **Check now**

PROXY SETTINGS

Use pro... Use automatic proxy

Host Port

Disable proxy f...
Divide individual hosts with "|" si...

Required authorization

Userna...

Passwo...

FILE SYSTEM VIEW

Change the file selection window view to a simple, system-independent view.

Restore default settings

Window 18: Settings – General tab

5.1.1. Settings – General

General tab enables configuration of Proxy settings as well as turning on and off automatic update check.

- Update – after selecting an option **Check update automatically**, the mechanism enabling application updates reporting will be started. The mechanism will be invoked while starting of application. Additionally there will be a possibility manual check, if there are any updates available, by clicking **Check now**.
- Proxy – after selecting an option **Use Proxy** additional fields for Proxy settings configuration will be unblocked:
 - **Host** – Proxy server address. (compulsory field)
 - **Port** – communication port with Proxy server. (compulsory field)
 - **Disable proxy for** – turns off the communication with Proxy server for host mentioned in the field for example **192.168.0.2 | 192.168.0.3**. (optional field)

If proxy server requires authentication, please select an option **Required authorization**. Additional fields will be unblocked then:

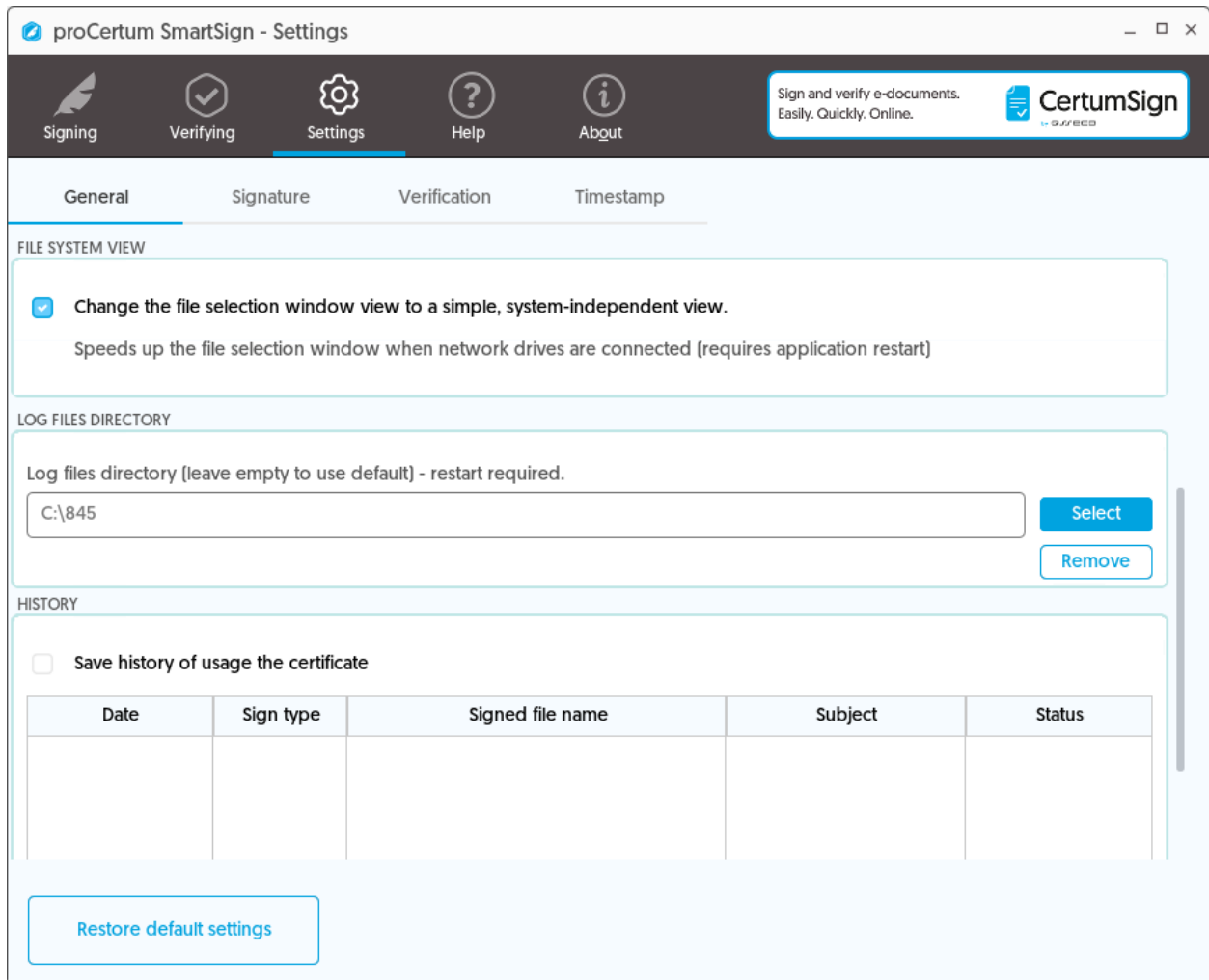
- **User** – ID of Proxy user. (compulsory field)
- **Password** – user's password. (optional field)
- File system view – section allows you to switch the file system view:
 - **Change the file selection window view to a simple, system-independent view** – selecting this option will change the view of the system windows regarding file selection

to simple – this speeds up the application's interaction with network drives – NOTE!!! – changing this option requires restarting the application

- Log files directory – this section allows you to specify the directory where the application will save logs – NOTE!!! – changing this option requires restarting the application
- History – after selecting this option, the option to save logs will be available. The application generates a separate log file that records the time, signature type and file name, certificate CN, and operation status. The log file is saved in the user's home directory. The contents of the log file are presented in the application as a table in the Configuration Panel.

The screenshot shows the 'proCertum SmartSign - Settings' window. The 'Settings' tab is active, and the 'General' sub-tab is selected. The interface includes a navigation bar with icons for Signing, Verifying, Settings, Help, and About. A banner at the top right reads 'Sign and verify e-documents. Easily. Quickly. Online.' with the CertumSign logo. The main content area is divided into sections: 'UPDATES' with a dropdown for 'Checking available updates' set to 'once a day' and a 'Check now' button; 'PROXY SETTINGS' with checkboxes for 'Use proxy' and 'Use automatic proxy', and input fields for 'Host', 'Port', and 'Disable proxy f...'; and 'FILE SYSTEM VIEW' with a checked checkbox for 'Change the file selection window view to a simple, system-independent view.' and a 'Restore default settings' button.

Window 19: Settings – General tab – part I



Window 20: Settings – General tab – part II

5.1.2. Settings – Signature

Signature tab enables settings configuration for signing process, which is being realized in **Signing** tab.

The screenshot shows the 'proCertum SmartSign - Settings' window. The top navigation bar includes 'Signing', 'Verifying', 'Settings' (active), 'Help', and 'About'. A banner on the right says 'Sign and verify e-documents. Easily, Quickly, Online.' with the 'CertumSign' logo. Below the navigation bar are tabs for 'General', 'Signature' (active), 'Verification', and 'Timestamp'.

SIGNATURE FORMAT

- XAdES**
XAdES signature - Electronic signature in XAdES format is in accordance with act on electronic signature. Format is compatible with requirements of the act on electronic signature. Format is compatible with the latest standards based on XML language and recommended for general usage.
- CADES/ETSI**
CADES/ETSI signature - Electronic signature in CADES/ETSI format is in accordance with act on electronic signature. Older signature format.

SIGNATURE TYPE

- External signature**
Signature file will contain only information about the signature. Please remember to deliver the document with the signature while signature's verification.
- Internal signature**
Signature file will also contain document's content

DIGEST FUNCTION

Digest function: SHA-256

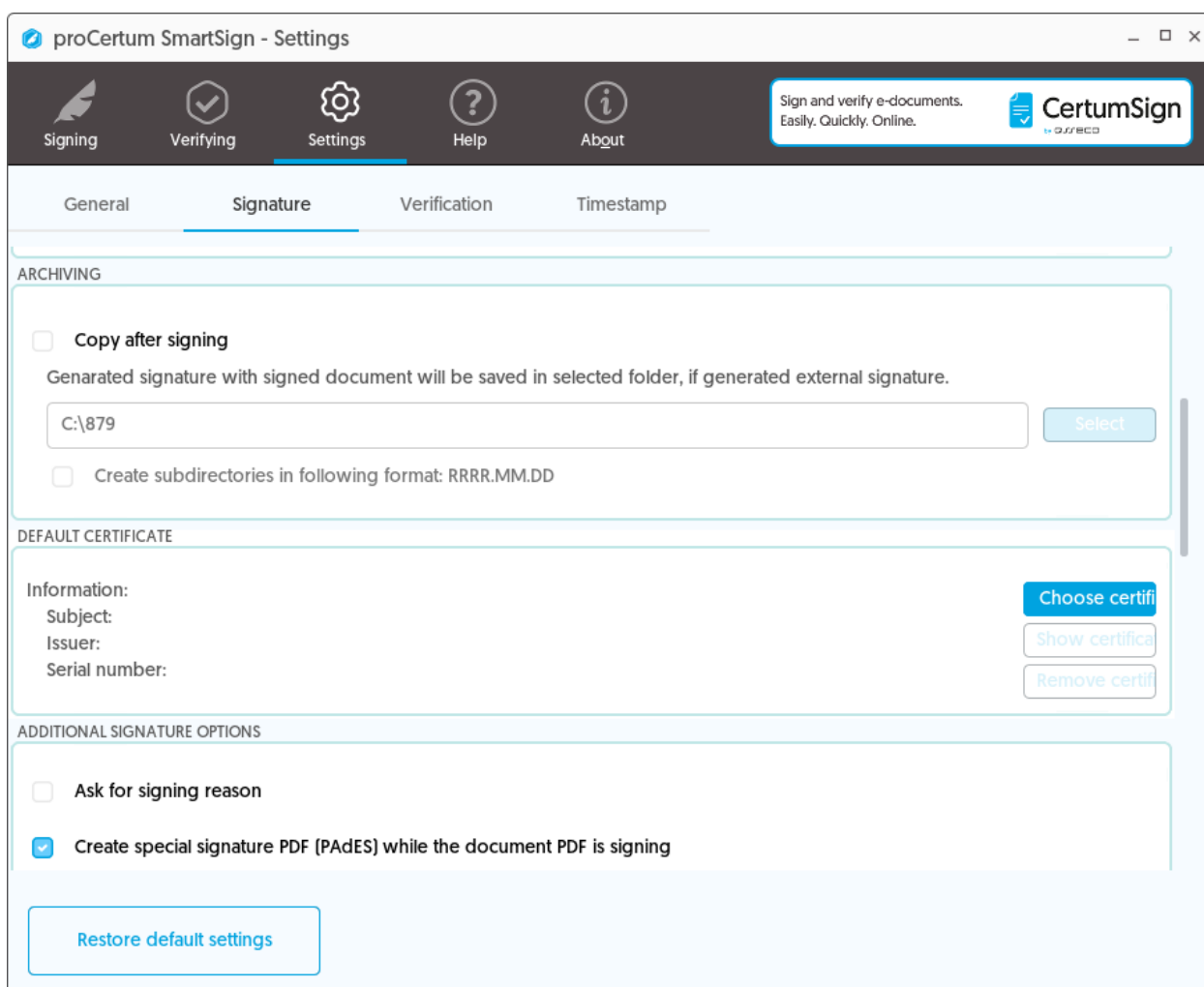
ARCHIVING

[Restore default settings](#)

Window 21: Signature - Settings tab

We can define following parameters:

- **Signature format:**
 - **XAdES** – Electronic signature in **XAdES** format;
 - **CAAdES/ETSI** – Electronic signature in **CAAdES/ETSI** format.
- **Signature type:**
 - **External signature** – signature file will contain only information about signature. Please remember to deliver the document with the signature while the signature's verification;
 - **Internal signature** – signature file will contain document's content.
- **Digest function** – the parameter denotes the name of the hash function used when creating the signature. Currently, only SHA-256 is possible.

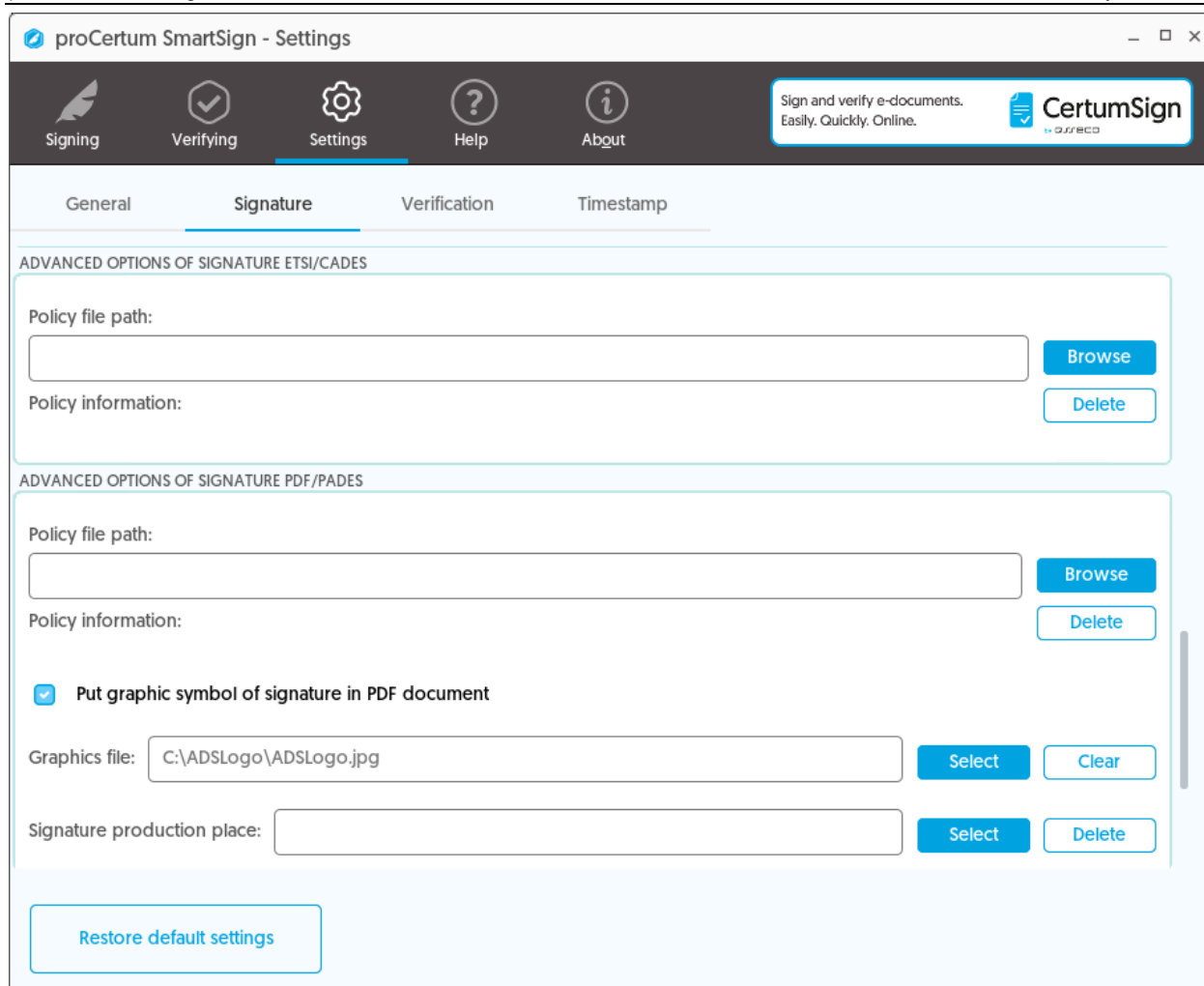


Window 22: Signature - Settings tab

- **Archiving:**
 - **Copy after signing** - selecting this option will cause selection the folder where the files of signature will be copied which will be generated after completed operation of signing;
 - **Create subfolders in YYYY.MM.DD format** - selecting this option that in the folder which is set to create subfolders for signed files in the format YEAR.MONTH.DAY created on the basis of the current date.

Default certificate - this option allows you to select which will be the default certificate used to sign the certificate.

- **Select the certificate** - after pressing the button on the list will be loaded all available certificates. To set the default certificate you should choose one of certificate and click **OK**;
 - **View certificate** - after pressing the button the details of the certificate will be displayed;
 - **Remove certificate** - by pressing the button the certificate will be removed from the configuration.
-
- **Additional options of the signature**
 - **Before signing the signature ask for a reason** - selecting this option, before signing the application will present a window for selecting reason of signature, which will be located in the structure of signature and will be presented later in the properties of the signature.
 - **Create a special signature PDF (PAdES while signing of PDF document** - selecting this option will cause if signed file will be PDF file this signature will be placed in the internal structure of the PDF and will be visible after opening PDF file in the PDF file editor;
 - **Select the type of commitment (XAdES signature only)** - Select the type of commitment for which a signature is created. Select from the following types of commitments:
 - The formal approval;
 - Confirmation of creation;
 - Delivery confirmation;
 - Confirmation of origin;
 - Confirmation of receipt;
 - Confirmation of posting.
 - **Signature variant** - allows you to select one of the following options for signature:
 - **Do not include the additional information (BES)** - selecting this option will cause that signature will be created in a basic format (no time stamp);
 - **Include a time stamp (T)** - selecting this option will cause that signature will be created with the time stamp proving the date of signature - is then required to define the settings tab of the time stamp in time stamp tab;
 - **Include a time stamp, certificates and CRL (XL/LTV)** - selecting this option will cause that signature will be created in the so-called. enhanced format that contains a time stamp proving the date of signature and contains CRL list as evidence of the validity of the signature at the time of submission - is then required to define the settings tab of the time stamp in time stamp tab;



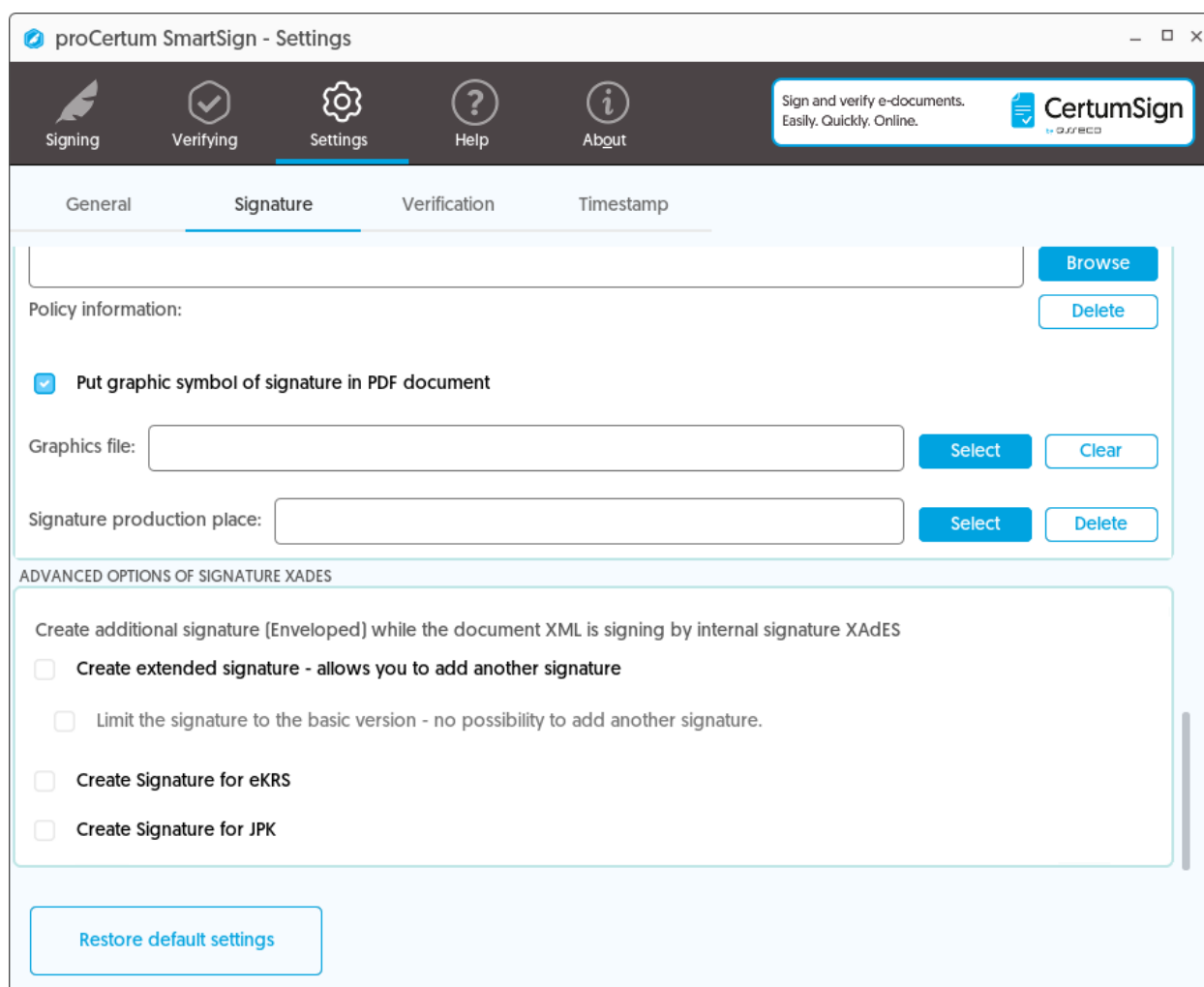
Window 23: The Settings tab - Signature - the part relating to Advanced options of signature

- Advanced options of signature ETSI / Cades
 - **The path to the file signature policy** - indicates the path to the signature policy defining the criteria for submitting and verifying the signature. Selection of the appropriate signature policy is made by pressing the button Browse. The Remove button allows you to remove the selected policy and return to the default setting.
- Advanced options of signature PDF/PAdES
 - **The path to the file signature policy** - indicates the path to the signature policy defines the criteria for submitting and verifying the signature. Selection of the appropriate signature policy is made by pressing Browse. The Remove button allows you to remove the selected policy and return to the default setting;
 - **Include a graphic symbol of the signature in the PDF document** - selecting this option, during the signing of PDF files for each file will be possible to an indication of an image file to use as a graphic symbol of the signature;
 - **Symbol File** – this option allows you to define the default signature symbol file placed in PDF files;
 - **Signer location** - this option allows you to specify the signer's location for the PDF signature in the configuration;



A dialog box titled "Signature production place" with a close button (X) in the top right corner. It contains four text input fields labeled "Postal Code:", "City:", "State/Province:", and "Country:". At the bottom right, there are two buttons: "OK" and "Cancel".

Window 24: Settings – Signature–Signer location



The main settings window for proCertum SmartSign. The title bar reads "proCertum SmartSign - Settings". The navigation bar includes icons for Signing, Verifying, Settings (active), Help, and About. A banner on the right says "Sign and verify e-documents. Easily, Quickly, Online." with the CertumSign logo. The "Signature" tab is selected, showing a "Policy information" section with a "Browse" button and a "Delete" button. Below that, a checkbox "Put graphic symbol of signature in PDF document" is checked. There are two "Graphics file:" input fields, each with "Select" and "Clear" buttons. The "Signature production place:" input field has "Select" and "Delete" buttons. A section titled "ADVANCED OPTIONS OF SIGNATURE XAdES" contains several options: "Create additional signature [Enveloped] while the document XML is signing by internal signature XAdES" (checked), "Create extended signature - allows you to add another signature" (unchecked), "Limit the signature to the basic version - no possibility to add another signature." (unchecked), "Create Signature for eKRS" (unchecked), and "Create Signature for JPK" (unchecked). A "Restore default settings" button is at the bottom left.

Window 25: Settings – Signature – XAdES advanced options

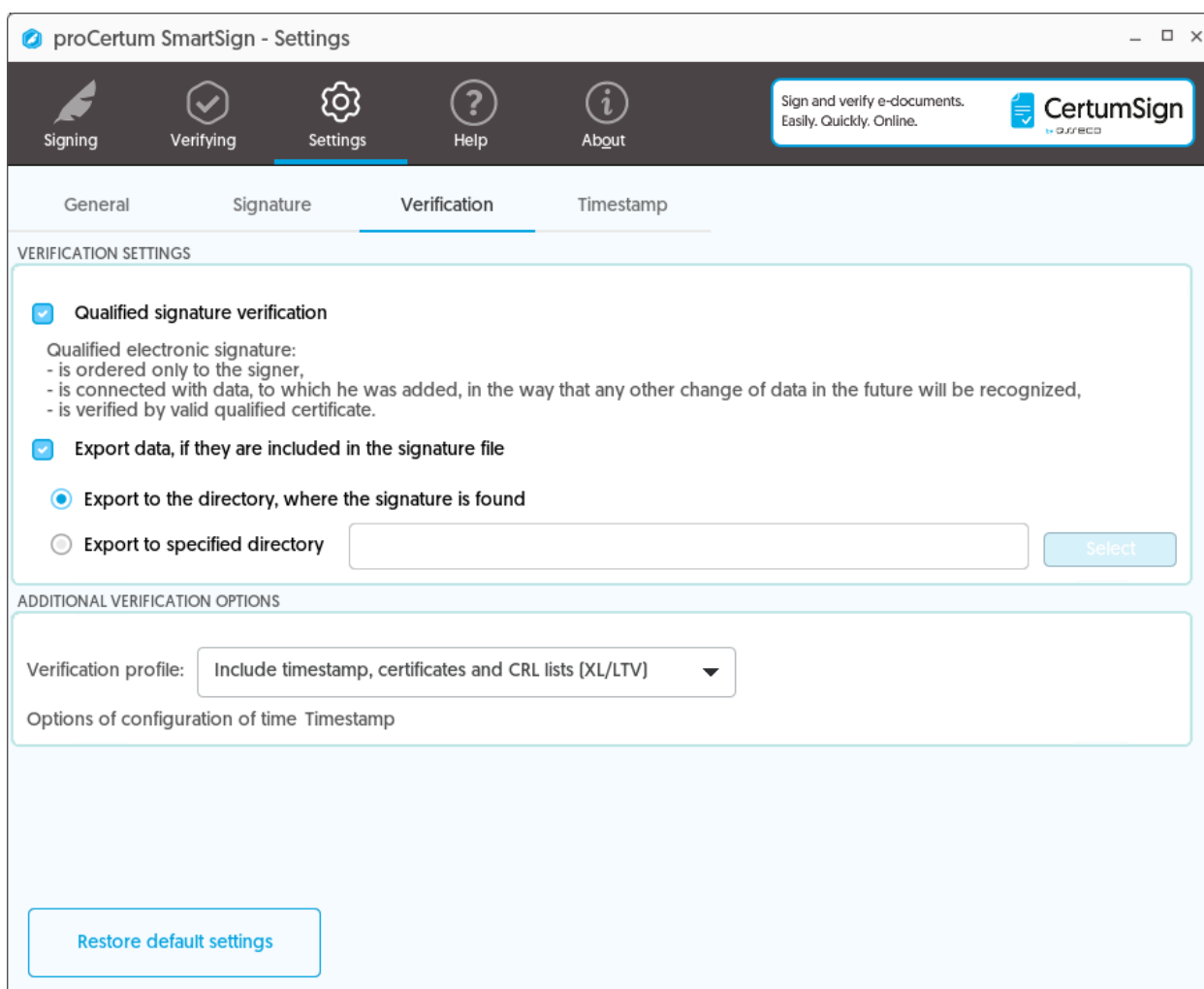
- Advanced options of signature XAdES
 - **Create extended signature** – selecting this option will result in the signature being created in standard enveloped mode if the signed file is a properly structured XML file –

this mode is required by the European Commission;

- **Limit signature to the basic version** – selecting this option will prevent additional signatures from being added to the signature.
- **Create signature for eKRS** – selecting this option will ensure signatures comply with eKRS requirements.
- **Create signature for JPK** – selecting this option will ensure signatures comply with JPK requirements.

5.1.3. Settings – Verification

Verification tab enables settings configuration for the verification process realized in **Verifying** tab.



Window 26: Settings - Verification

5.1.3.1. Basic options of verification

Selecting **Qualified signature verification** will cause setting proper runtime mode of **proCertum SmartSign** application, which consists in verifying, if the signature operation has been completed with the usage of qualified signature in accordance with the act on electronic signature.

Note!

If you have selected **Qualified signature verification**, the application will check if signing certificate is

qualified certificate. If it appears that the certificate is not qualified certificate, error message will appear.

If data are enclosed in signature file and the user will select an option **Export data, if they are included in the signature file**, it will cause data separation and data saving in the chosen place.

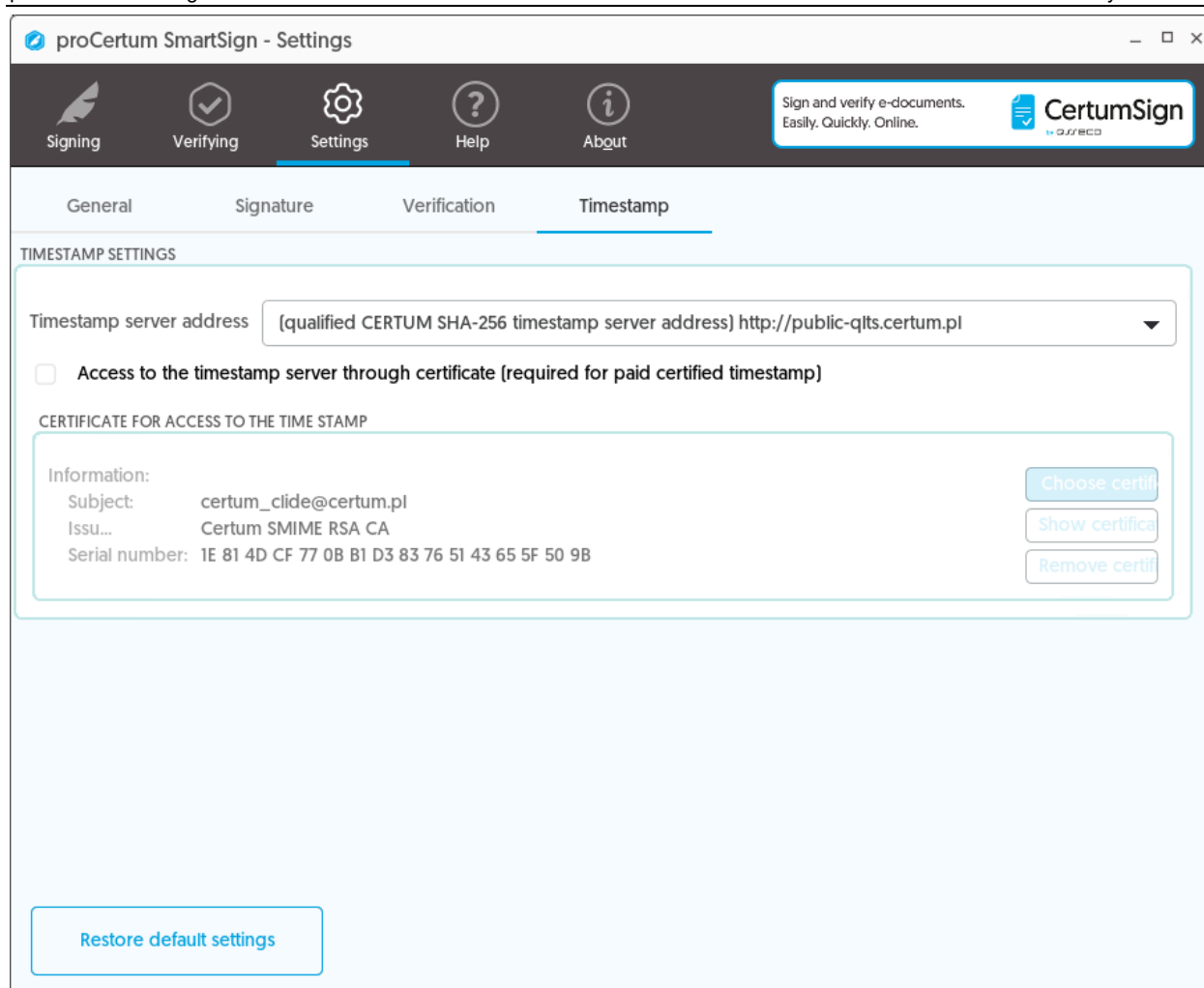
5.1.3.2. Additional options of verification

An additional option is so called **verification variant** specifying the details of the verification process. Choose from the following variants of verification:

- **Do not include the additional information (BES)** - selecting this will cause the subject to verify will only be the integrity of the signature;
- **Include a time stamp (T)** – selecting this will cause the subject to verify will only be the integrity of the signature, after positive verification of the signature will be attached to the time stamp of the time providing a positive verification of the signature - is then required to define the settings tab of the time stamp in time stamp tab;
- **Include the time stamp, certificates and CRL lists (XL/LTV)** - selecting this option will cause the will be carried out full of verification of signature, after verification of sued signature will be accompanied by the time stamp proving a positive verification time and signature CRL lists, which were used for verification - is then required to define the settings tab of the time stamp in time stamp tab;

5.1.4. Settings – Timestamp

Timestamp tab allows you to configure settings for time-stamping operations undertaken during the submission or verification of electronic signature.



Window 27: The Settings tab - Timestamp

We can define the following parameters:

- **Address timestamp server** enables marking the signature files of the timestamp which are available in the following predefined settings:
 - qualified CERTUM SHA-256 timestamp server address (<http://public-qts.certum.pl>) – a public qualified timestamp that does not require an access certificate, a free service for holders of qualified certificates issued by Certum PCC.

Additionally, the following items can be added manually:

- <http://qts.certum.pl/default/clide> – CERTUM's qualified timestamp server address – a qualified timestamp that requires an access certificate;
- <http://time.certum.pl> – CERTUM's non-qualified timestamp server address;

WARNING!!!

Access to a qualified time stamp CERTUM can also be using of access certificate. Therefore, if you choose a qualified time stamp CERTUM you can select **Access to the server by the time stamp through certificate**. After selecting the options settings will be unlocked certificate:

- **Choose Certificate** - after pressing the button the list will be loaded all the certificates. Select the certificate authorizing access to a qualified time stamp CERTUM and press **OK**;

- **View the certificate** - after pressing the button will display the details of the certificate;
- **Remove certificate** - by pressing the button the certificate will be removed from the configuration.

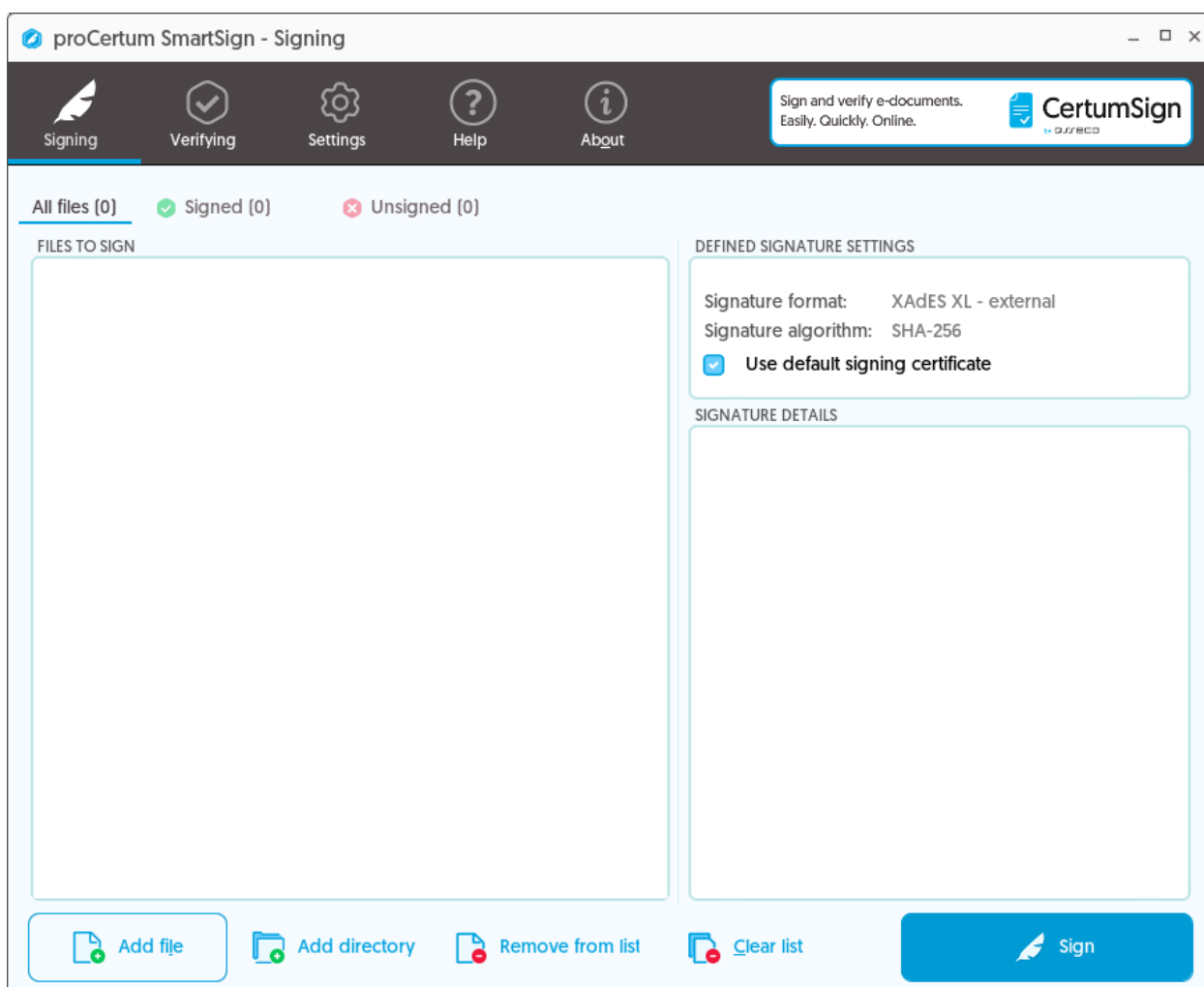
File signing

Signing tab enables signing file with an electronic signature.

It consists of 4 sections:

- **List of elements to sign** – file names, modification dates, size and status of signature (To sign/Signed/File has been skipped) are listed here;
- **Defined signature settings** – information about signature format (ETSI/XAdES as well as about signature type: internal/external).
- **Signature details** – information about signature.
- **Information** – Statistic information about the quantity of selected files with the division to files designed for files to sign, already signed files as well as files, which haven't been signed yet.

WARNING! It is recommended that the single signature file does not exceed 10 000 files of size about 50 KB



Window 28: Signing

5.1.5. Adding elements to the list

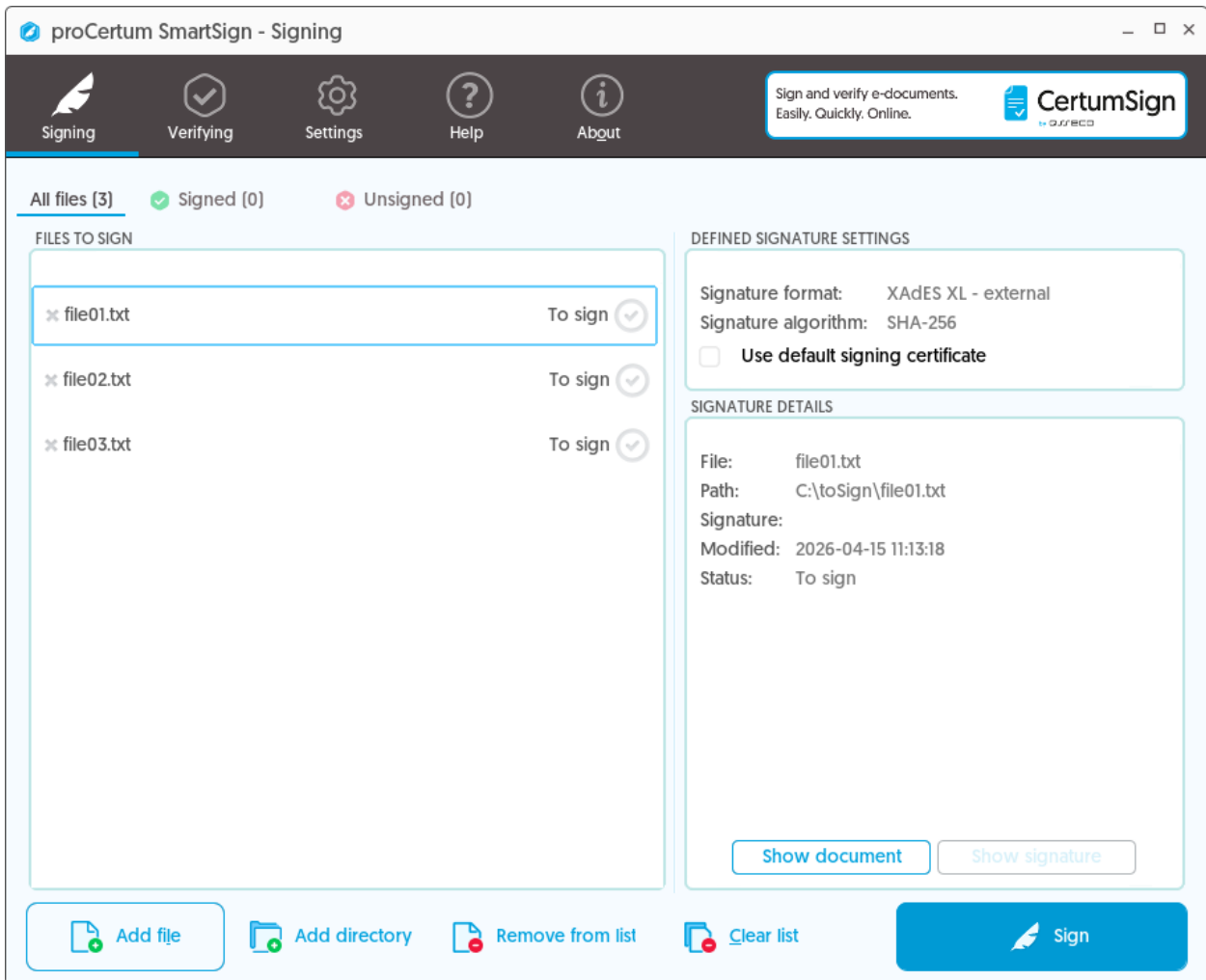
Electronic signature operation can be executed in two ways:

- on single file – by indication with the usage of the **Add file** button,
- on group of files – by multiple file selection with the usage of **Add directory**.

Indicated files will be added to the list of elements to sign. To remove file(s) selective from the list to sign please show chosen file(s) and click **Remove file(s) from the list**. To remove all files from the list of elements to sign please click **Clear list**.

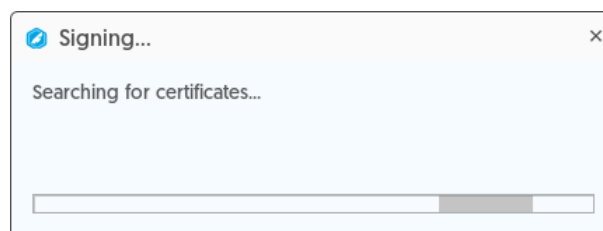
5.1.6. Signature operation

If all elements to sign are on the list, please click **Sign**.



Window 29: Signing – List of elements to sign

proCertum SmartSign application will find certificates enabling signing documents with an e-signature.



Window 30: Searching for certificates

After searching has been completed, the certificates will be displayed.



Window 31: List of qualified certificates

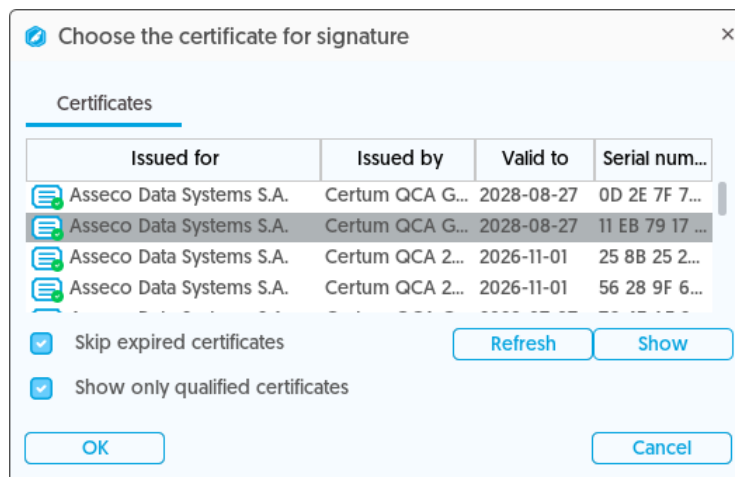
Note!

Qualified certificates will be displayed in dialogue window. To display all certificates available on given computer, please select an option **Show only qualified certificates**.



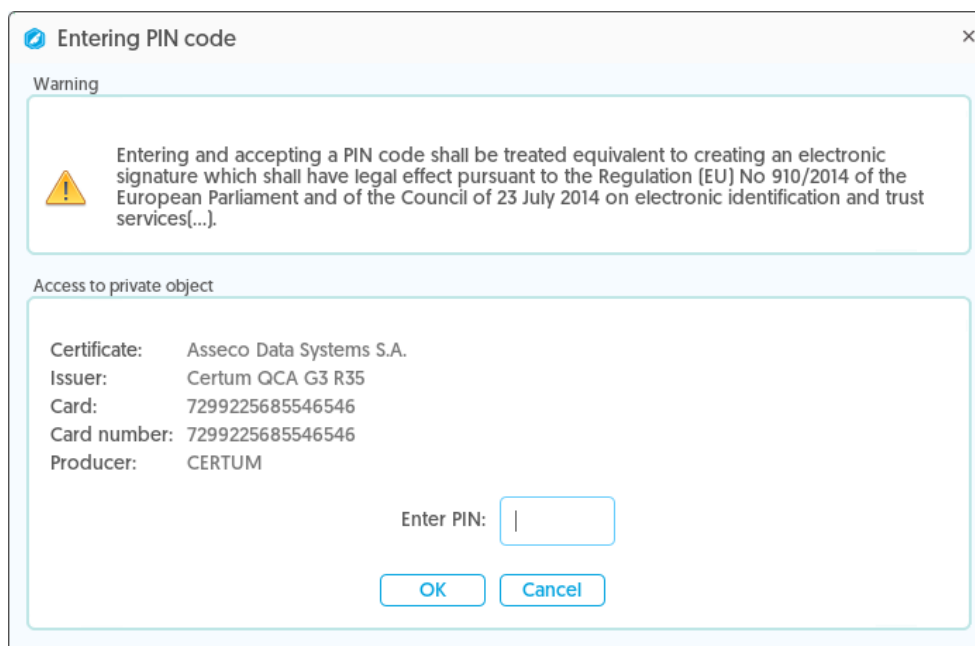
Window 32: List of qualified certificates and non-qualified certificates

To execute signature operation, please show certificate and click **OK**.



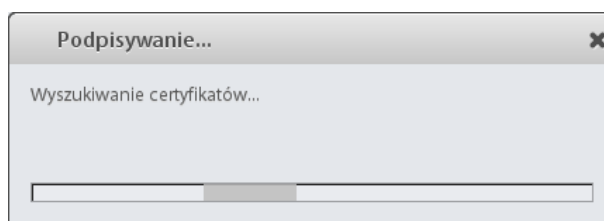
Window 33: Certificate selection for signature operation

If the user has selected qualified certificate for signature operation, reminder, referring to insertion of authentication PIN code will be displayed. Please enter the PIN then and click **OK**.

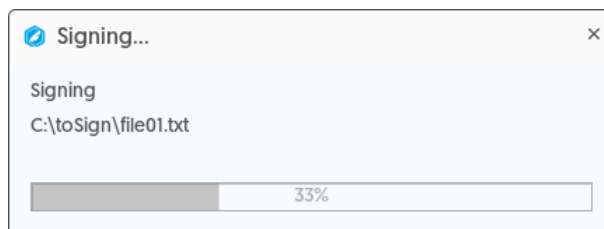


Window 34: Reminder referring to PIN insertion

If entered PIN is invalid, **proCertum SmartSign** application will search for keys associated with the certificate. After that the signing process will be started.

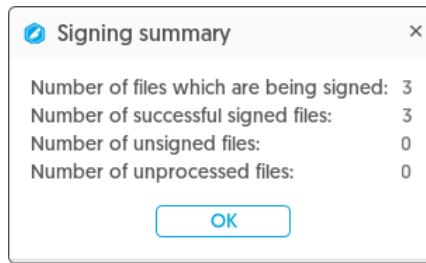


Window 35: Signing... - Searching certificates



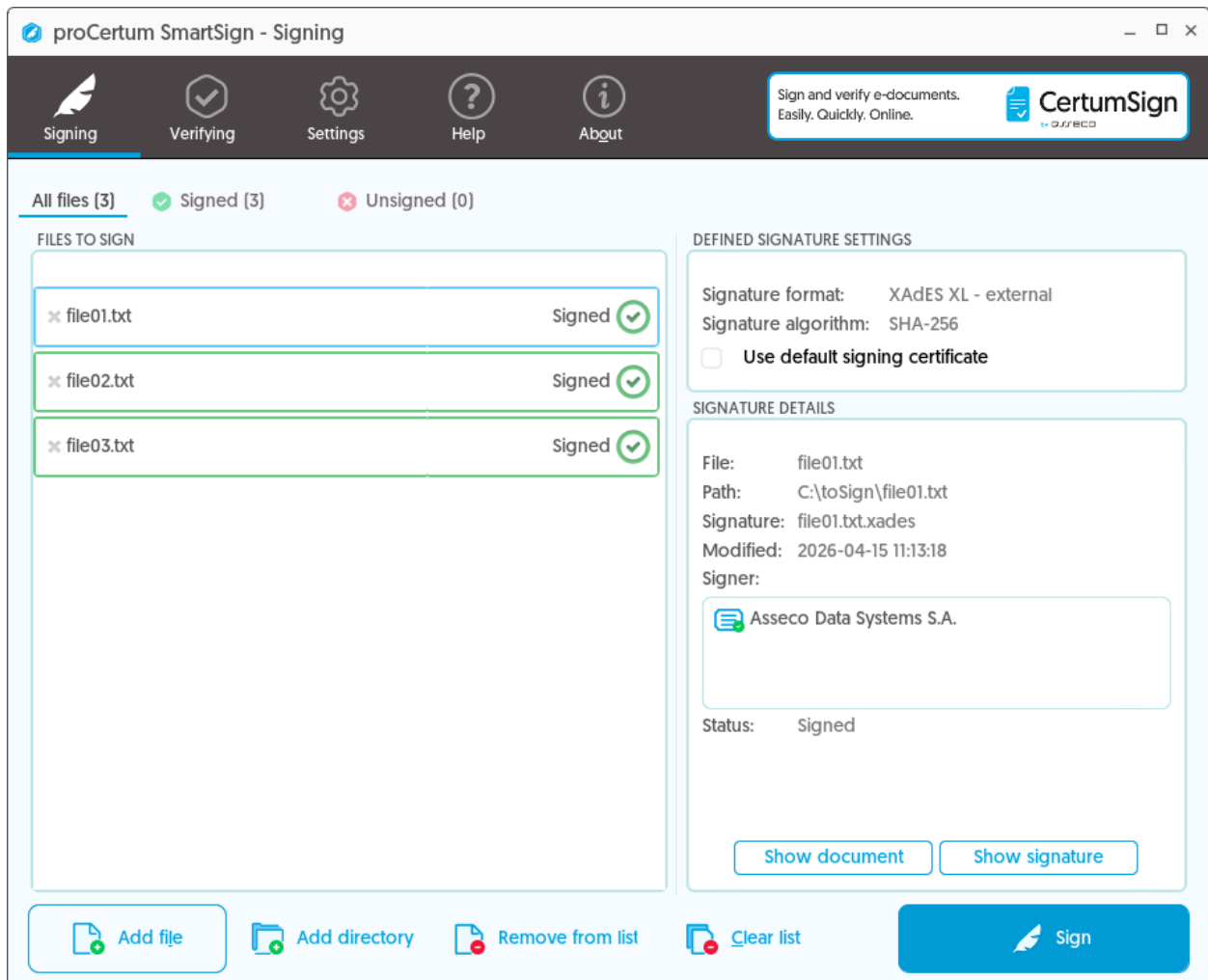
Window 36: Signing... - Performing signature

After the signing process has been successfully completed, the summary will be displayed.



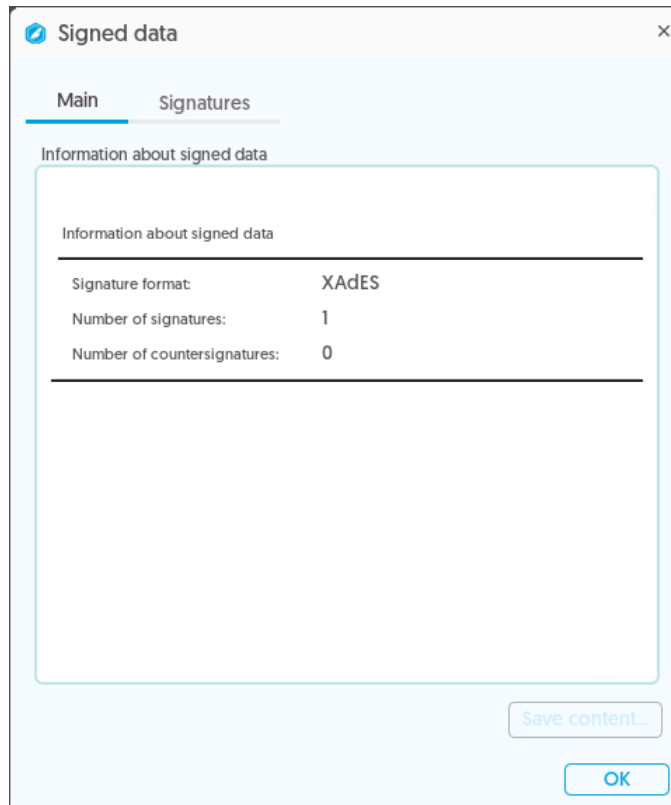
Window 37: Signing summary

Signature details section on the tab **Signing** will be updated with the information concerning signature file (field **Signature**) as well as signing file (field **Signer**).

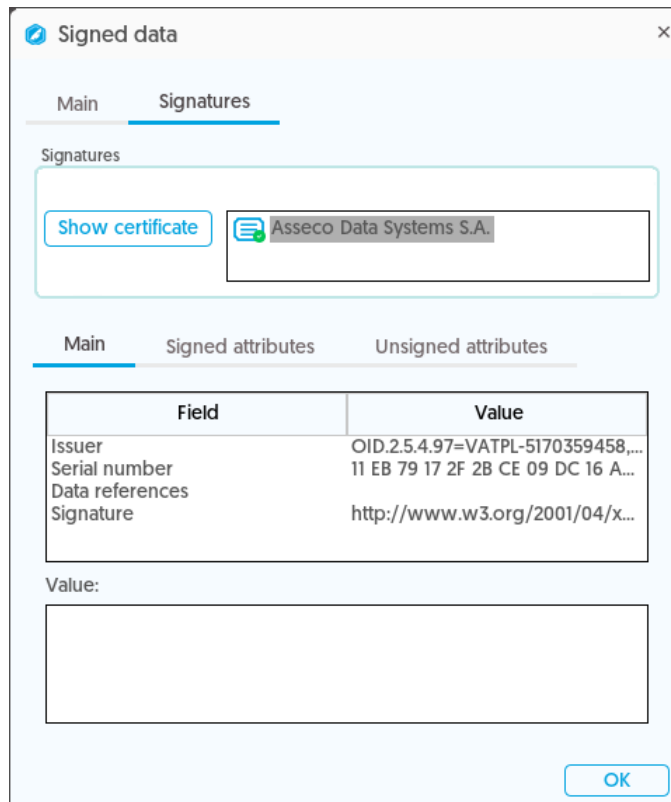


Window 38: Signing – executed signature

Data can be browsed by clicking **Show signature** button:



Window 39: Signed data – Main tab

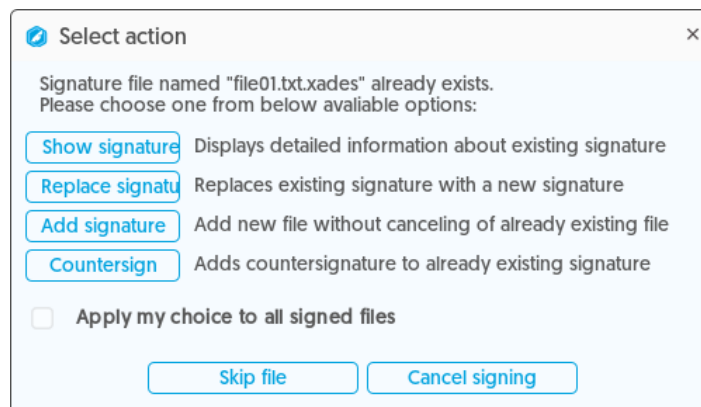


Window 40: Signed data – Signatures tab

5.1.7. Multiple signature

To perform **multiple signature**, please select file (original, signature file should not be selected), which

was signed at least once. Please click **Sign** button then. Certificate selection and entering PIN code is similar like by single signing. After the proper PIN code has been entered, the following window will appear:

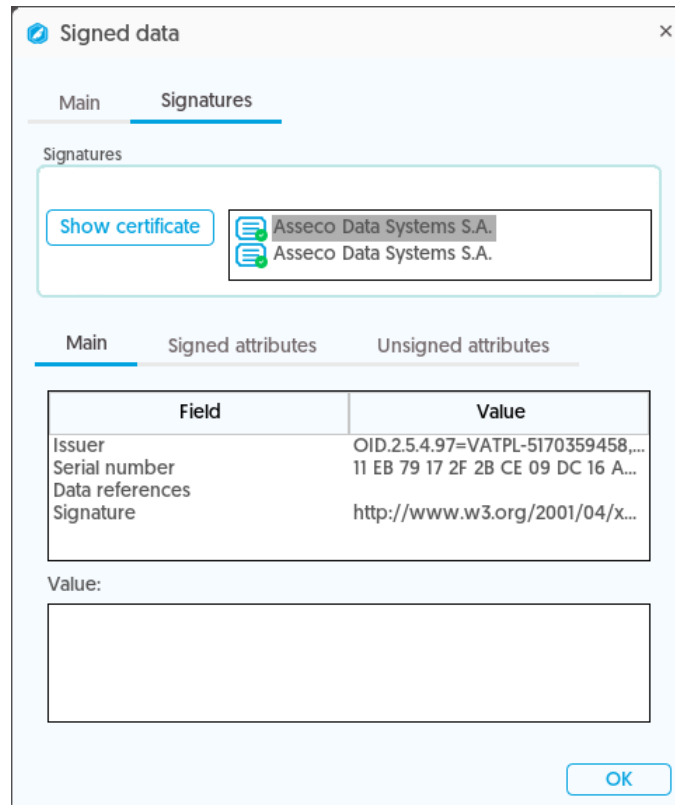


Window 41: Window enabling selection of an action performed by at least one already existing signature

For **multiple signature**, please click **Add signature** button. In case of selecting an option **Replace signature**, all already existing signatures will be replaced with one. Data informing about already existing signature can be displayed by clicking **Show signature**. After the signature has been performed, you can check all signatures of the given file by clicking **Show signature**.



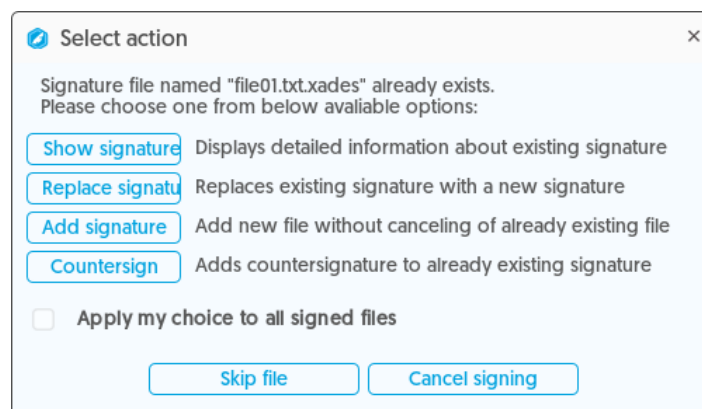
Window 42: Signed data – Main tab for multiple signature



Window 43: Signed data – signature for multiple signature tab

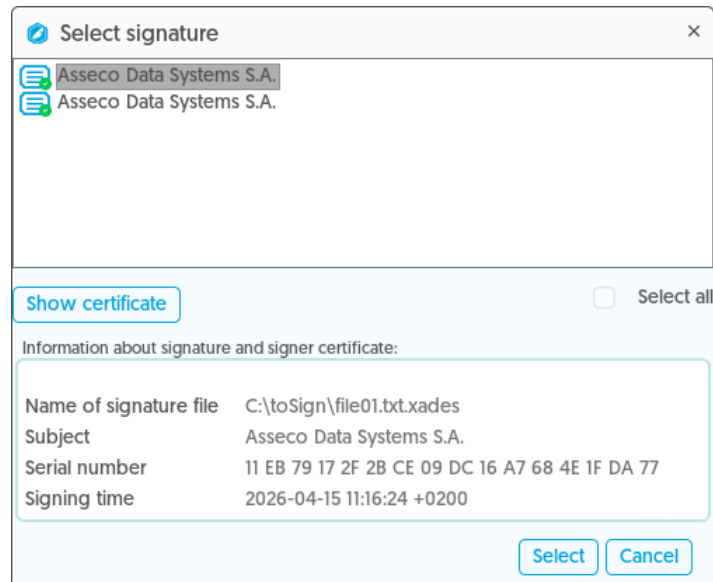
5.1.8. Countersignature

To perform **countersignature** please select file (original, signature file should not be selected), which was signed at least once. Please click **Sign** button then. Certificate selection and entering PIN code is similar like by single signing. After the proper PIN code has been entered, the following window will appear.



Window 44: Window enabling selection of action by at least one signature

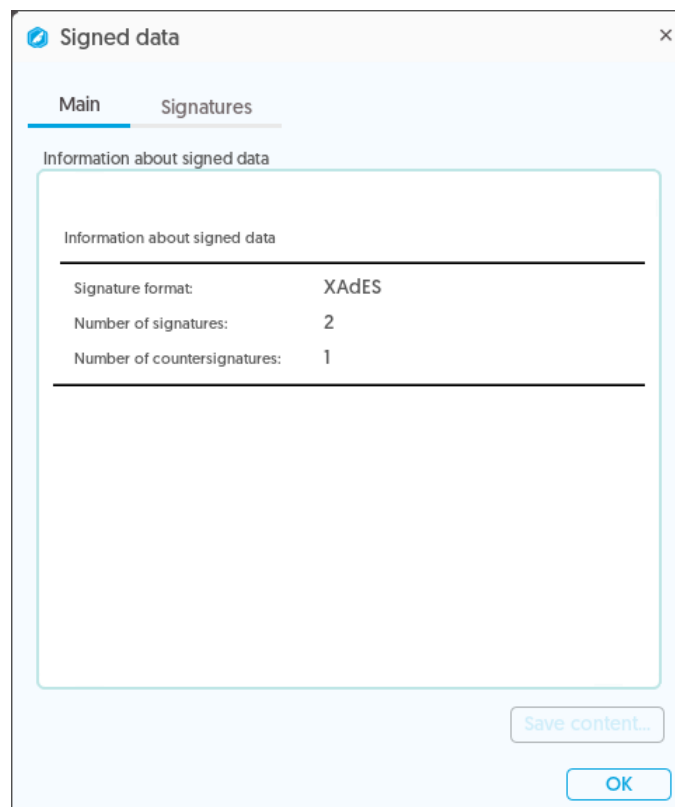
For **countersignature**, please click **Countersign** button. In case of selecting an option **Replace signature**, all already existing signatures will be replaced with one. Data informing about already existing signature can be displayed by clicking **Show signature**. After the **Countersign** button has been clicked, there will be a window displayed. Please select the certificate from this window, which you would like to countersign:



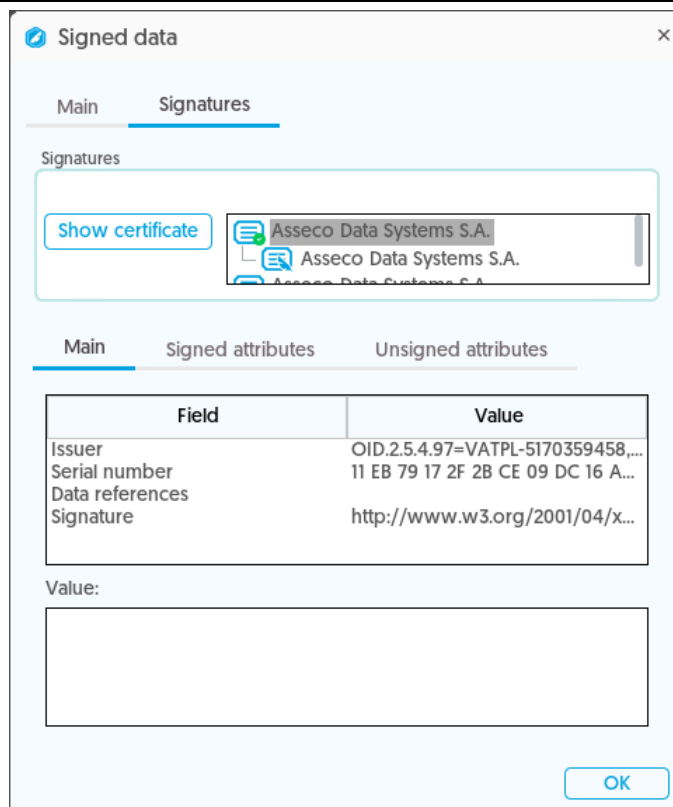
Window 45: Window enabling signature selection for countersignature

After the certificate has been selected, please click **Select**. After the signature has been performed, all signatures of given data can be checked by clicking **Show signature**.

Window 46: Signature selection window when all signatures for countersigning are selected



Window 47: Signed data – main tab for countersignature



Window 48: Signed data – signatures for countersignature tab

Countersignatures of signatures are marked by **C** letter

5.1.9. Signing PDF files

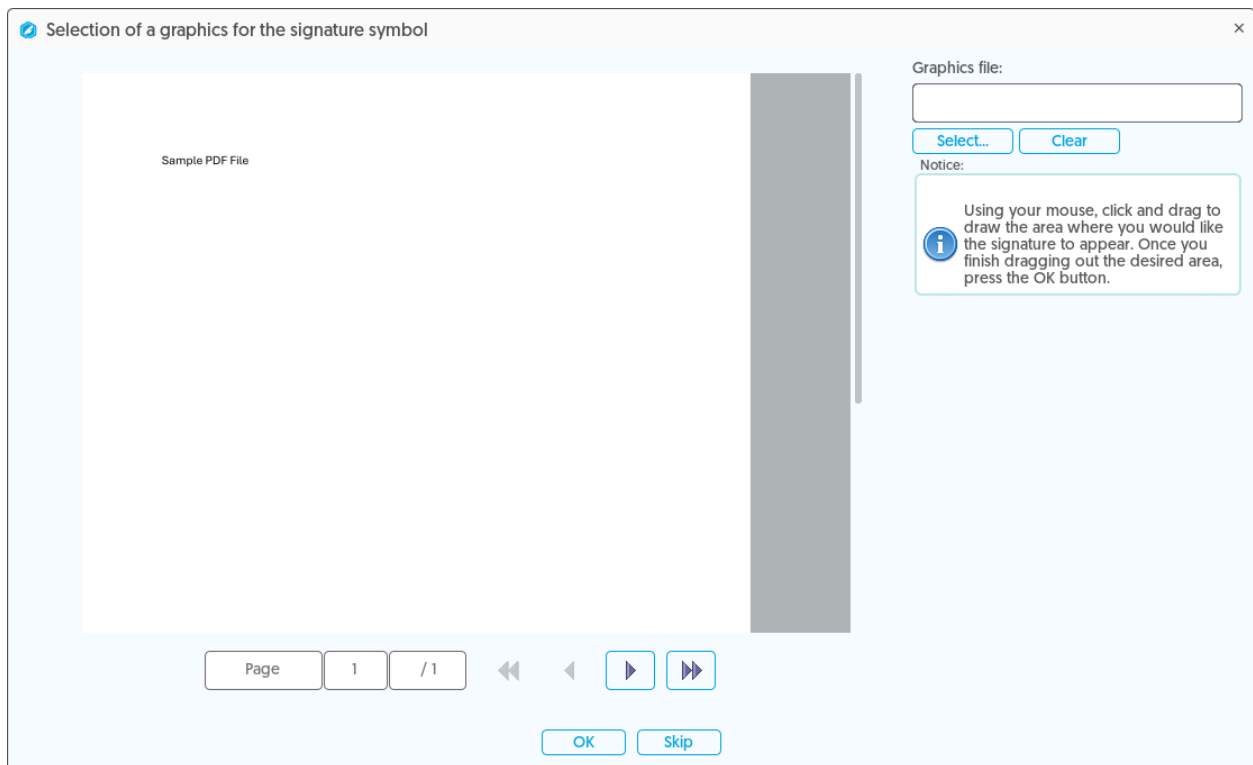
If enabled signature is set Create a special PDF (PAdES) when the signed document is PDF document, application for an ensemble is made of the signature of the PDF file in a PDF file so called PAdES format. The process of signing is no different essentially from the process described above. The signature is placed directly in the PDF.

WARNING!

For the correct interpretation of signatures in PDF files is required Adobe ® Reader ® at least version 10.0.

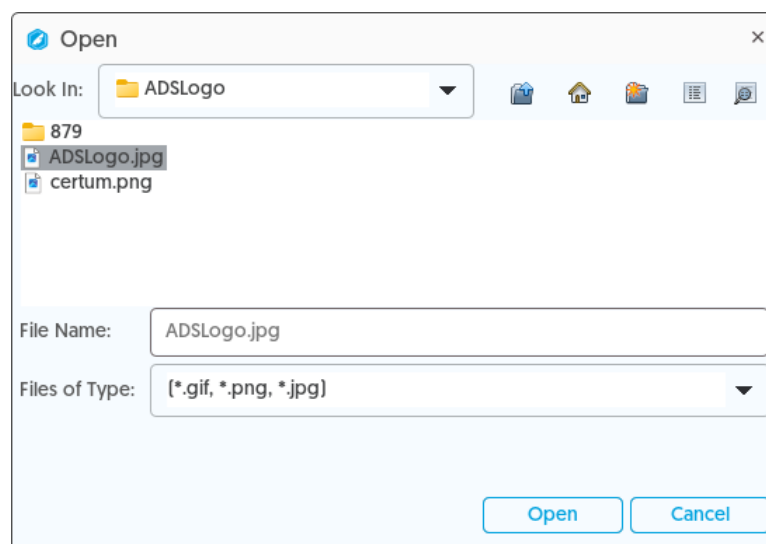
5.1.9.1. Adding graphic symbol of signature

If in advanced options, of signature PDF / PAdES option **Place graphic symbol of signature in PDF document** is selected when signing a PDF file, after selecting the signing certificate it will be made possible to select the graphic file signature symbol In the case of serial signing of PDF files for each of signing a PDF file application allows you to define a specific symbol.



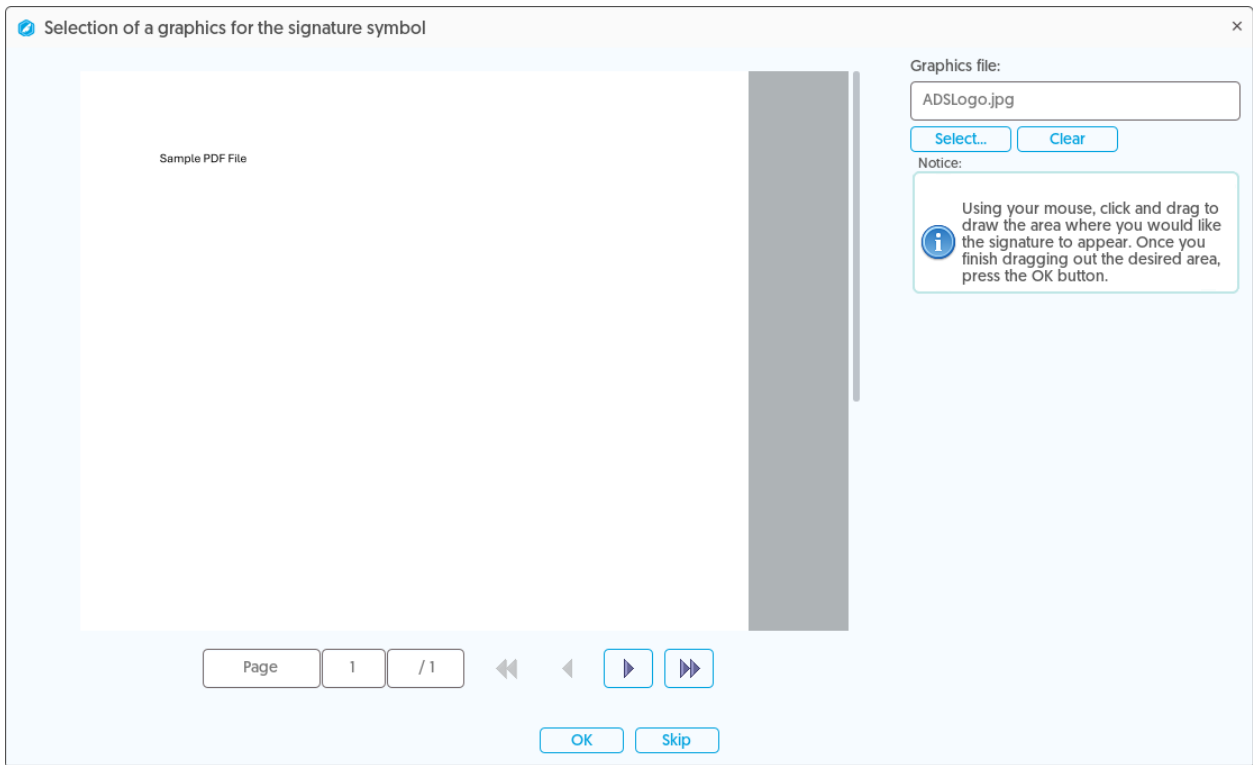
Window 49 Adding a signature graphic symbol - The main window

After pressing the **Choose** button it will be enabled to display a graphic file used as a graphic symbol of signature (acceptable formats are jpg, gif and png).



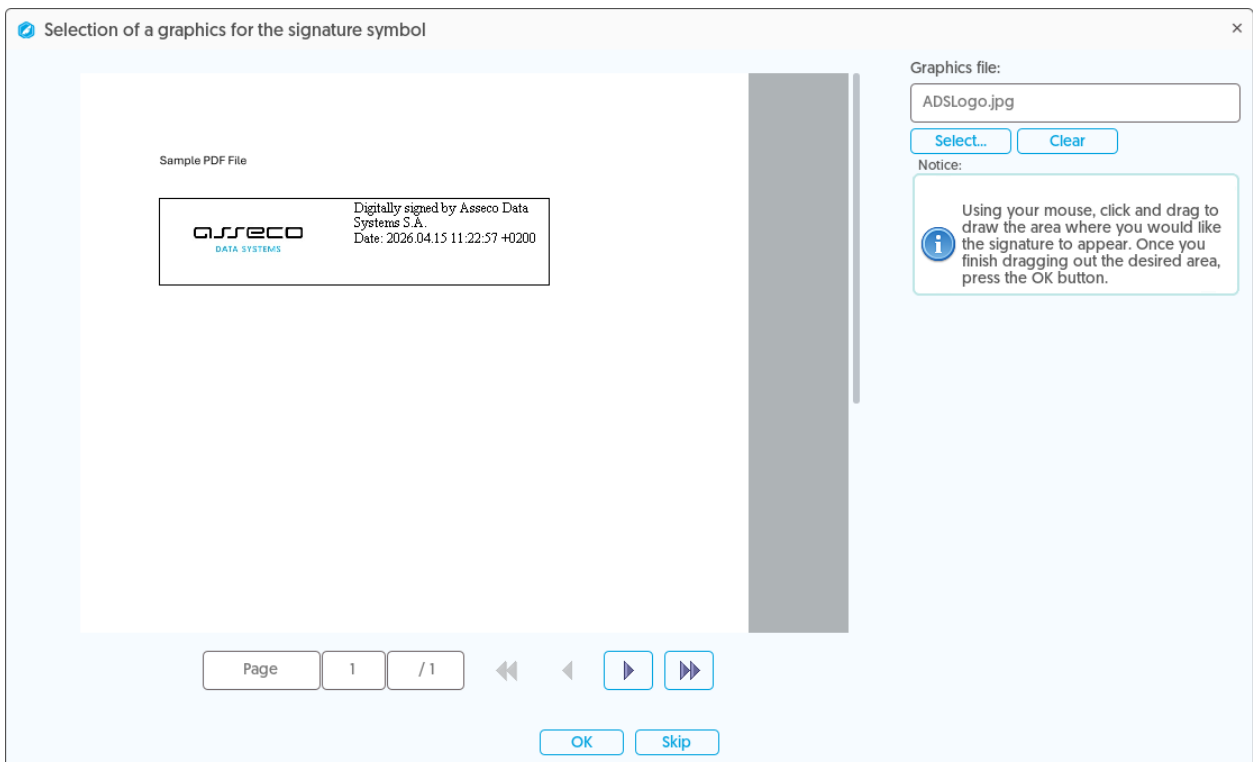
Window 50 Adding a graphic symbol of the signature - Indication of the graphic file

After selecting the file, the main window will be updated with the selected file.



Window 51 a signature graphic symbol - The chosen graphic file

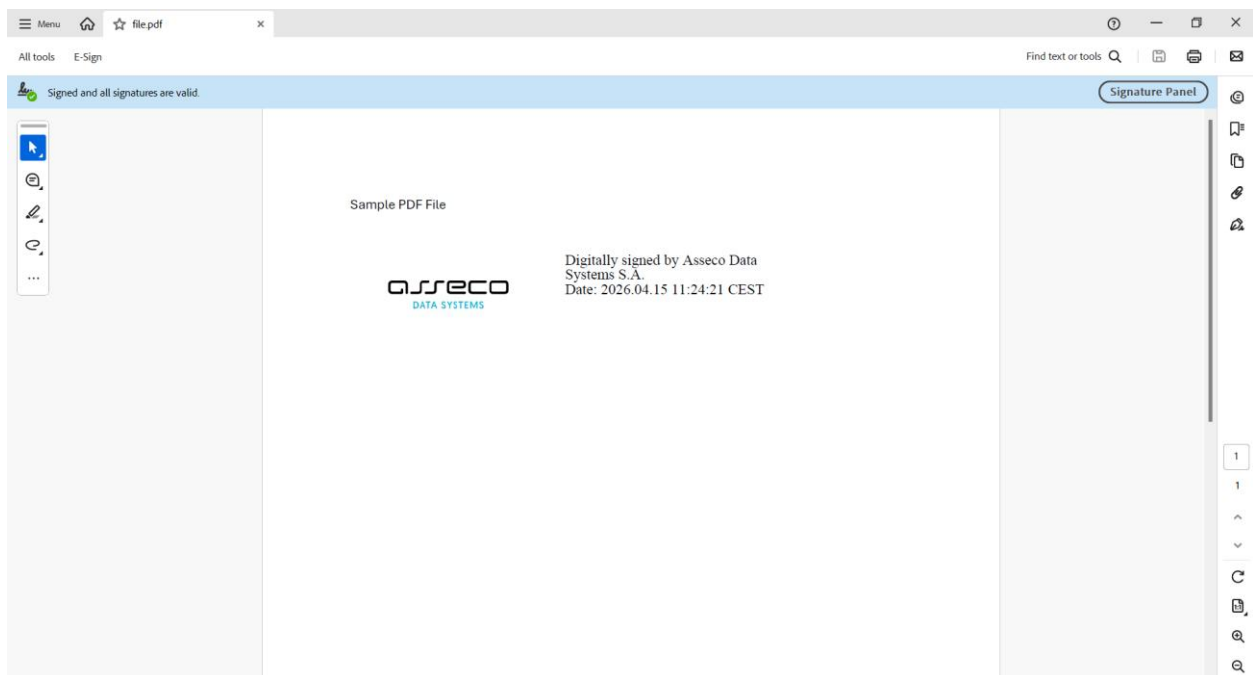
The field in which the graphic symbol is to be placed on the document indicates the mouse while holding the left mouse key. After defining symbol of this field with information on signing will appear in the document.



Window 52 a signature graphic symbol - graphical symbol added to the document

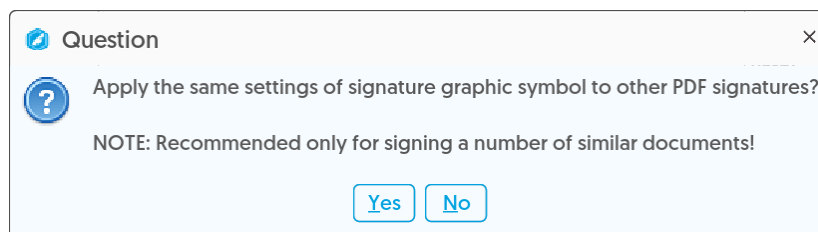
After confirmation with **OK** the signature is made. After opening the PDF document with a signature

graphic symbol will be immediately visible.



Window 53 Adding a graphic symbol of a placed signature - signed file with a placed graphic symbol of signature

If you sign multiple PDF documents at the same time, a message will appear on the screen.

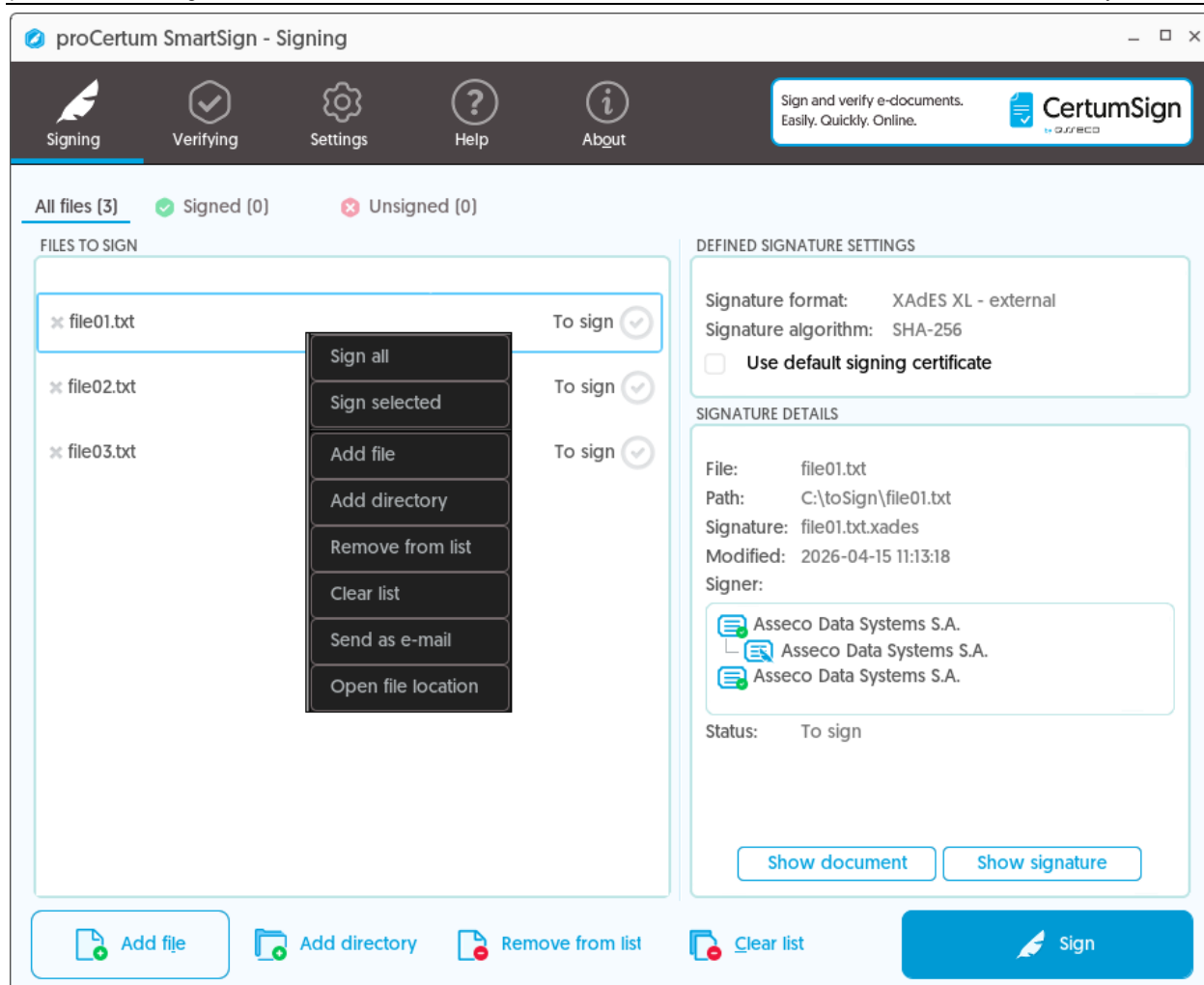


Window 54 Adding a graphic symbol of a placed signature – multiple signature

5.1.10.Context menu

To get the context menu started, please click right mouse button on any place on the list. There are 8 available options in the menu:

- **Sign all** – after this option has been selected, the signature will be performed on all files available in the list.
- **Sign selected** – after this option has been selected, the signature will be performed only on selected files. To select more than one file, please hold left Ctrl button and by clicking left mouse button select next file(s).
- **Add file** – this option works in the same way as Add file button.
- **Add directory** – this option works in the same way as Add directory button.
- **Remove from list** – this option works in the same way as Remove file(s) from list button.
- **Clear list** – this option works in the same way as Clear list button.
- **Send as e-mail** - This option starts the mail program to the operating system as the default, and generates an email attaching to it signatures of the created files and the files signed (in the case of external signatures).
- **Open file location** - this option allows you to display folder of the file.



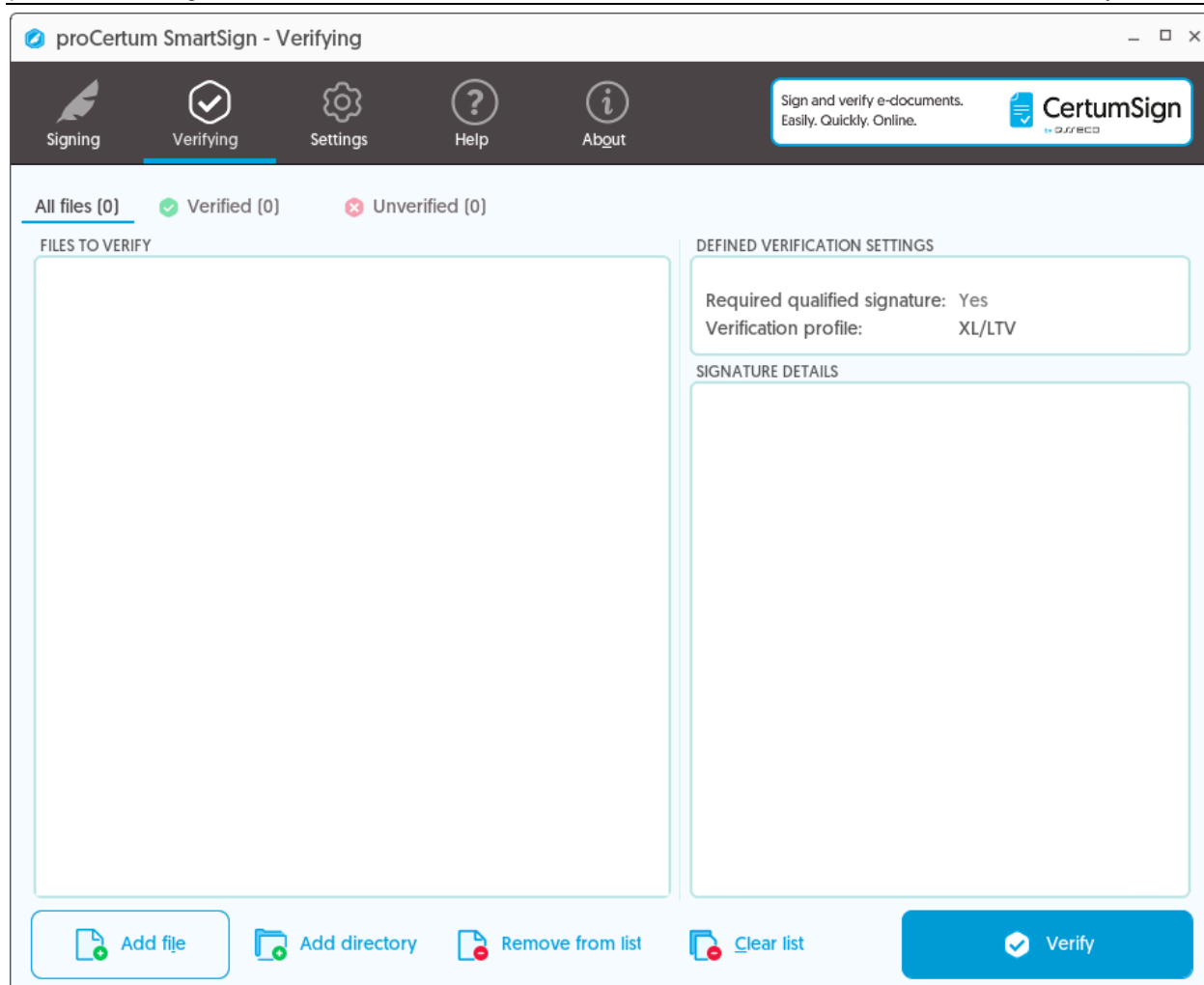
Window 55: Signing tab – context menu

Signature verification

Verifying tab enables electronic signature verification.

It consists of 4 sections:

- **List of elements to verify** – file names are displayed on the list, modification date, size and status of signature (To verify/Verified successfully/Verified unsuccessfully).
- **Defined signature settings** – information about verification settings referring to qualified signature verification (See: point 4.1.3).
- **Signature details** – information referring to signature on selected file.
- **Information** – statistic information about the number of selected files with the division to files designed for files to verify, already verified files as well as files, which haven't been verified successfully.



Window 56: Verifying tab

5.1.11. Adding elements to the list

If we want to perform electronic signature verification operation, we can perform it:

- on single file – by selecting file with the usage of **Add file** button,
- on group of files – by multiple selection of file with the usage of **Add file** button or by adding directory with the usage of **Add directory** button.

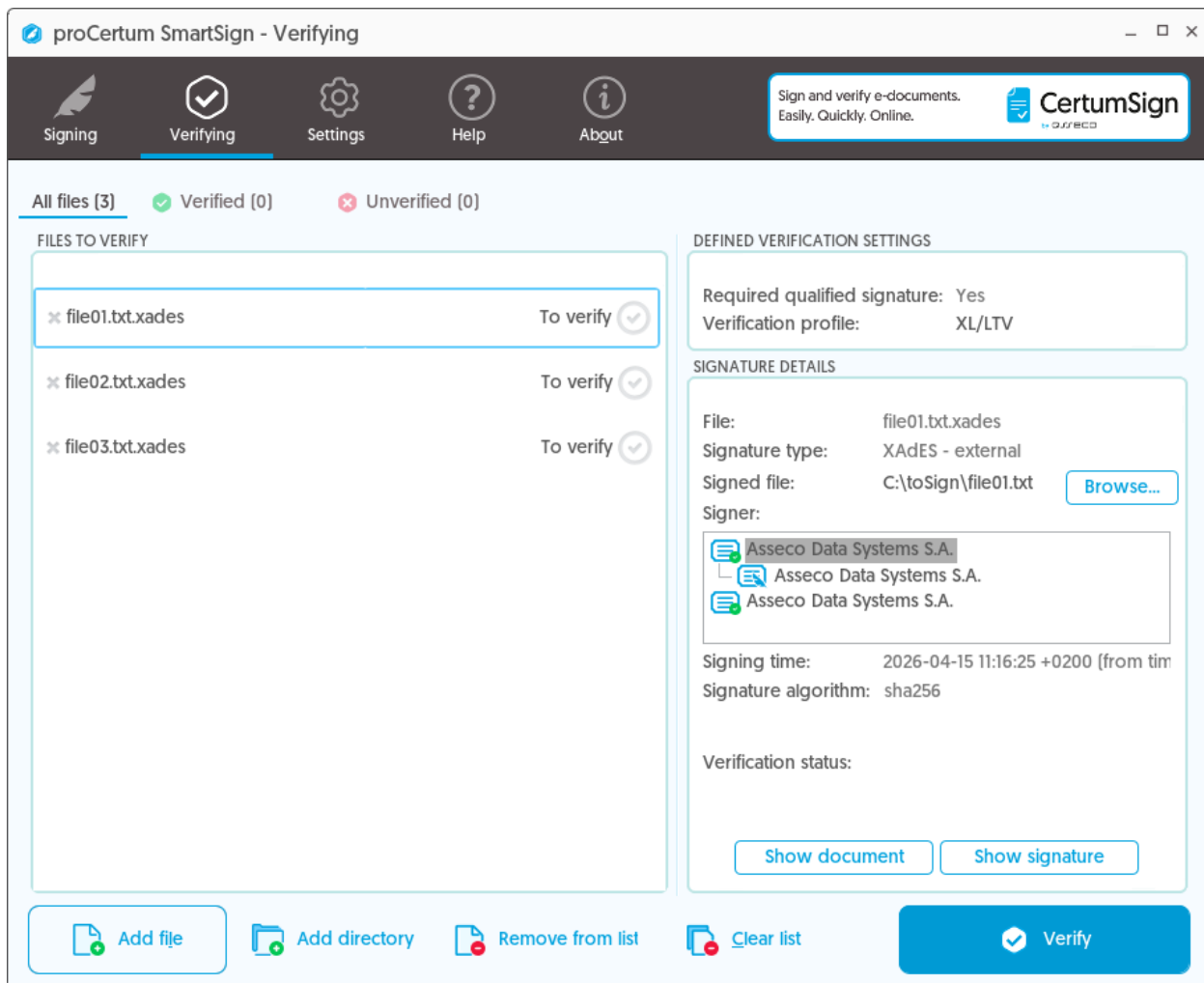
Selected files will be added to the list of documents to verify. To remove file(s) selective from the list to verify, please indicate selected file(s) and click **Remove file(s) from list**. To remove all files from verification list, please click **Clear list**.

Indicated files will be added to the list of elements to verify. To remove file(s) selective from the verification list, please indicate selected file(s) and click **Remove file(s) from list**. To remove all files from verification list, please click **Clear list**.

Attention!

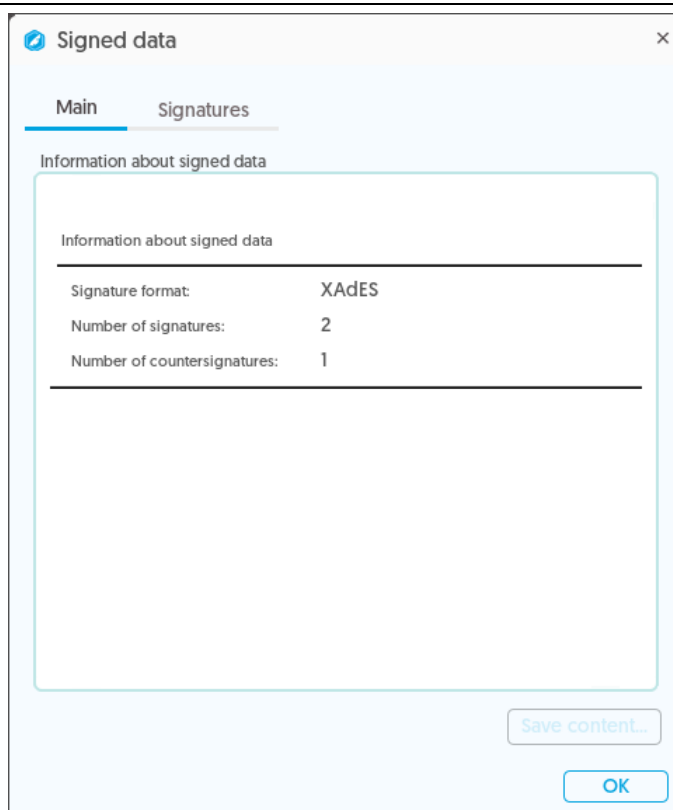
Files with internal or **external signature** (information about signature is found in the **Signature information** section) can be found in the list of elements for verification. If selected element is an external signature, please select source file in the **Signature information** section, on which the signature operation has been performed. It should be done by clicking button.

5.1.12. Information about signature and document, which is being verified



Window 57: Verifying tab – List of elements to verify

Detailed information can be inquired by clicking **Show signature** button. **Signed data** window will be displayed then.



Window 58: Signed data

There are two tabs in the **Signed data** window:

- **Main** – contains information about signature type as well as number of signatures, countersignatures and certificates;
- **Signatures** – contains information about signature and signer certificate, signed and no-signed attributes etc.

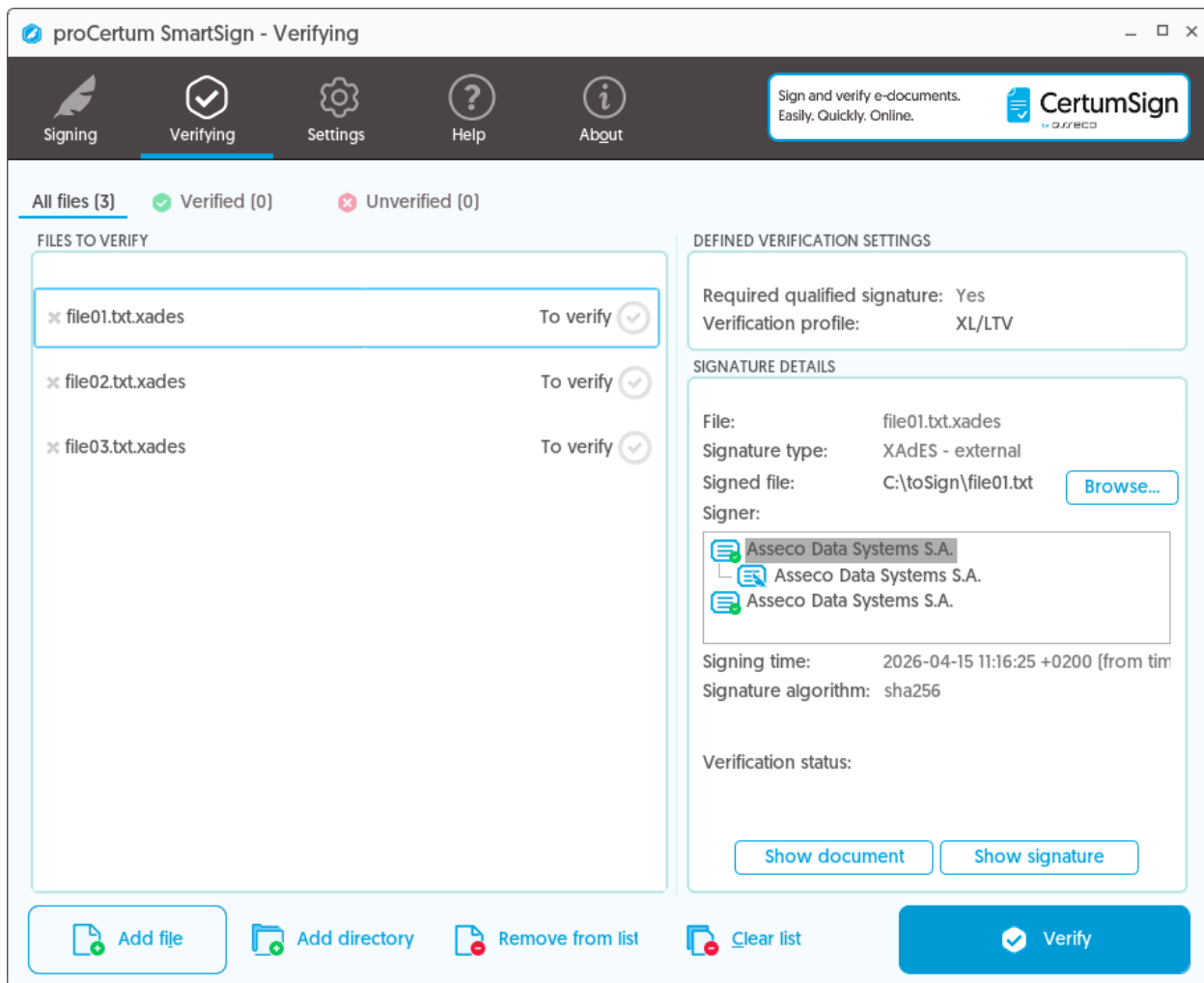
To display the document, which is being verified, please click Show document button.

Note!

Document is being displayed out of control of **proCertum SmartSign** application, with the usage of external application, which is proper for this document type.

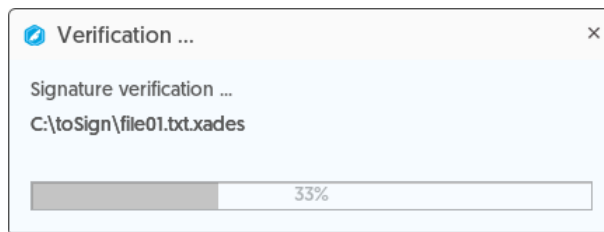
5.1.13.Verification operation

If all the elements for verification are found on the list, please click **Verify**.



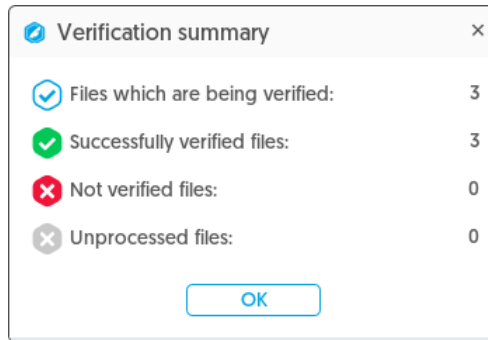
Window 59: Verifying tab – List of elements to verify

The signature verification process starts.



Window 60: Verification...

After the e-signature verification process has been completed, the summary will be displayed.



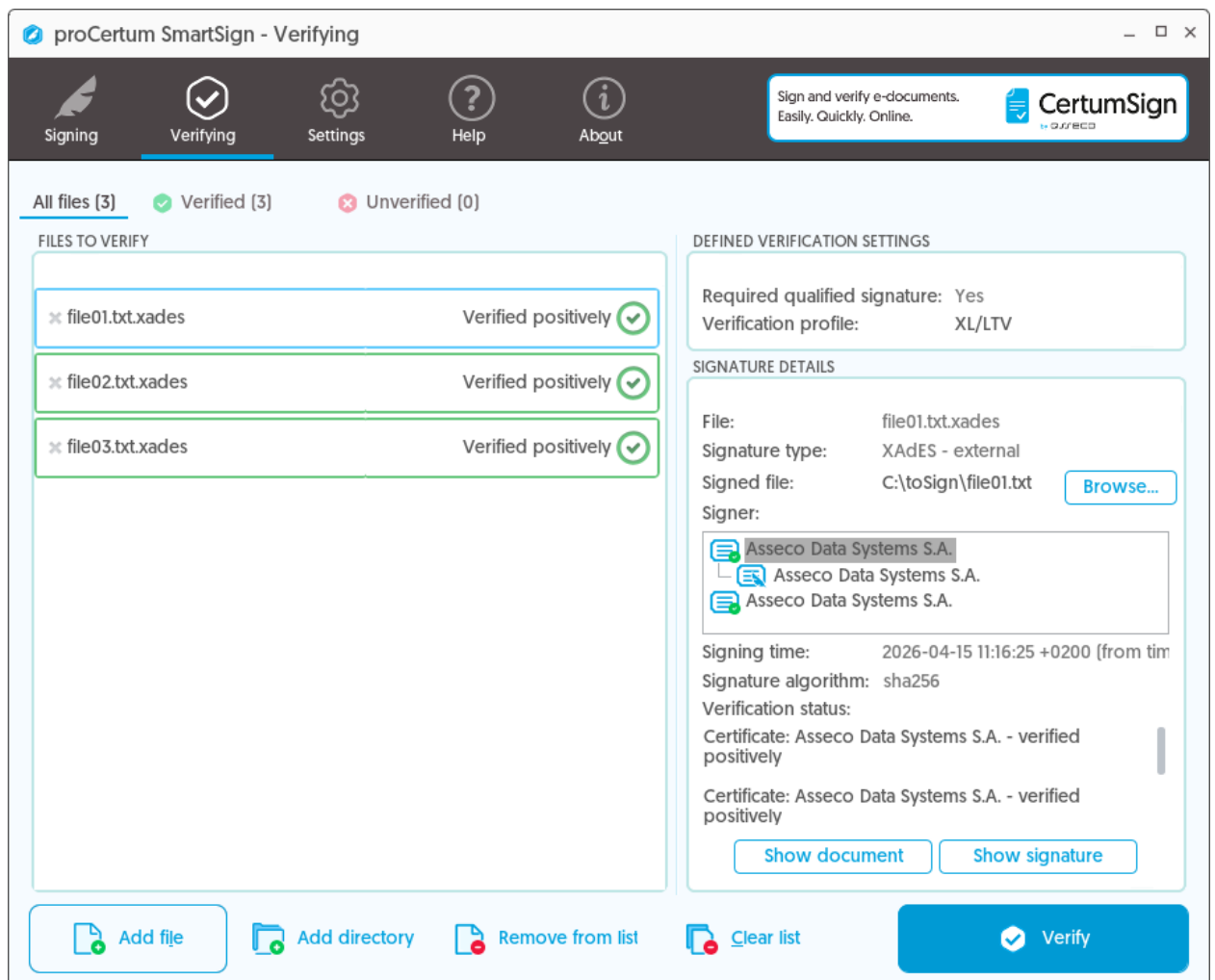
Window 61: Verification summary

5.1.14.Verification status

Verification operation can result as successful and unsuccessful. Depending on operation result, its status will be defined as:

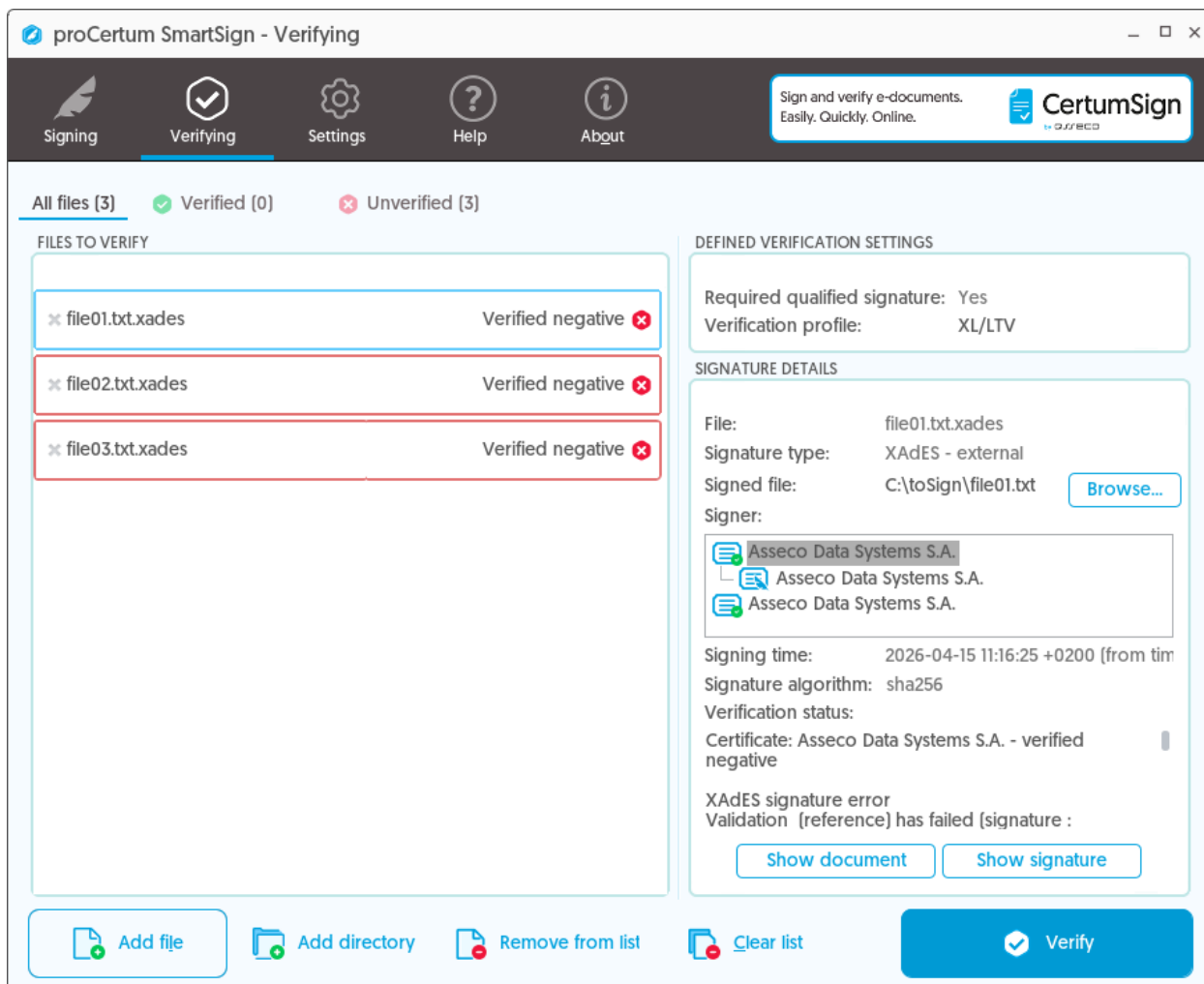
- Verified positively;
- Verified negative.

If the verification process is defined as **successful**, the entry *Certificate: Asseco Data Systems S.A. – verified positively* will be shown in **Verification status** field in section **Signature information**.



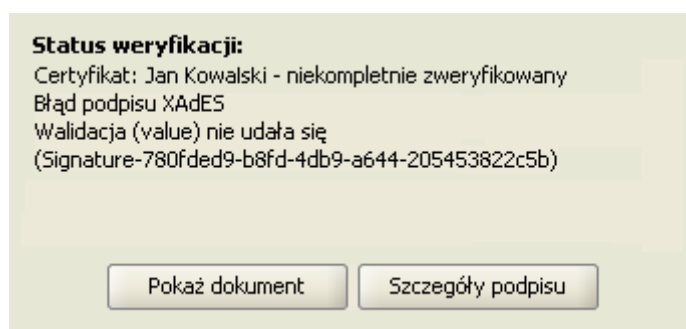
Window 62: Verification status: Verified positively

If the status of verification process is defined as **unsuccessful**, the element will be marked with red and there will be an entry Certificate: Jan Kowalski – verified incomplete, displayed in **Signature information** section in **Verification status** field.

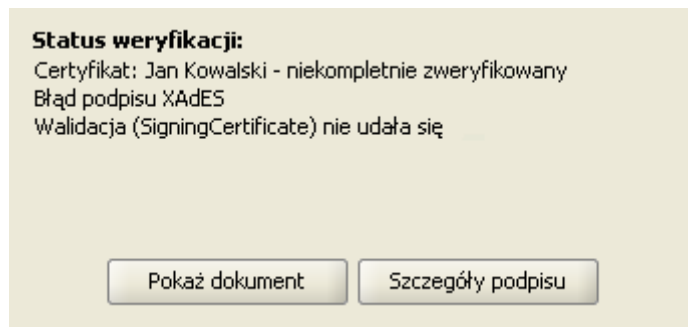


Window 63: Verification status: Verified negative

Error reason for the signature file will be also given in the **Verification status** field. Find error examples below.



Window 64: Signature value invalid



Window 65: Certificate invalid

NOTE:

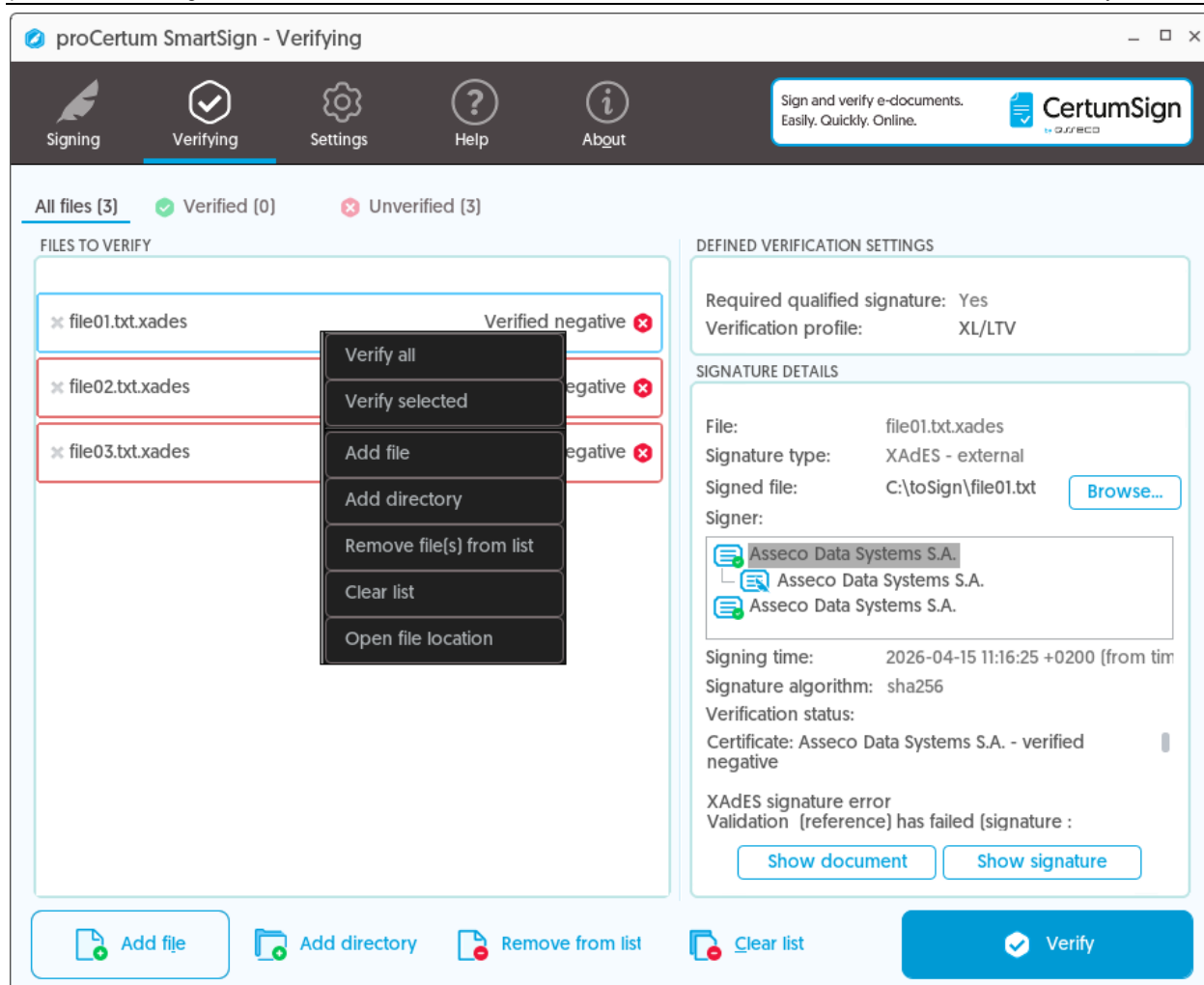
Full qualified signature validation and a validation report are provided by the **Certum Sign** (formerly **WebNotarius**) platform, available at:

<https://sign.certum.pl>

5.1.15.Context menu

To get the context menu started, please click right mouse button on any place on the list. There are 7 available options in the menu:

- **Verify all** – after this option has been selected, signature of all files found on the list will be verified.
- **Verify selected** – after this option has been selected, the signature will be verified only for selected files. To select more than one file, please hold left **Ctrl** button and by clicking left mouse button select next file(s).
- **Add file** – this option works in the same way as **Add file** button.
- **Add directory** – this option works in the same way as **Add directory** button.
- **Remove file(s) from list** – this option works in the same way as **Remove file(s) from list** button.
- **Clear list** – this option works in the same way as **Clear list** button.
- **Open file location** – option allows you to display folder of the file.



Window 66: Verifying tab – context menu

System context menu

After the **proCertum SmartSign** application has been installed, there will be a new position added in the context menu. To get the menu started, click **right mouse** button on **any file**. There will be a new position available in the menu under the name **proCertum SmartSign**. After selecting it with the mouse cursor, there will be three options displayed:

- **Sign** – after this option has been selected, **proCertum SmartSign** application with selected **Signing** tab will be started and marked file will be loaded to the list of files designed for signing. Further signing procedure is described in **4.3** point.
- **Verify** – after selecting this option, **proCertum SmartSign** application with selected **Verifying** tab will be started and marked file will be loaded to the list of files designed for verification. Further verification procedure is described in point **4.4**.
- **Show signature** – after selecting this option, **Signed data** will be displayed with the usage of mechanisms included in **proCertum SmartSign** application. This option is available only for signature file.

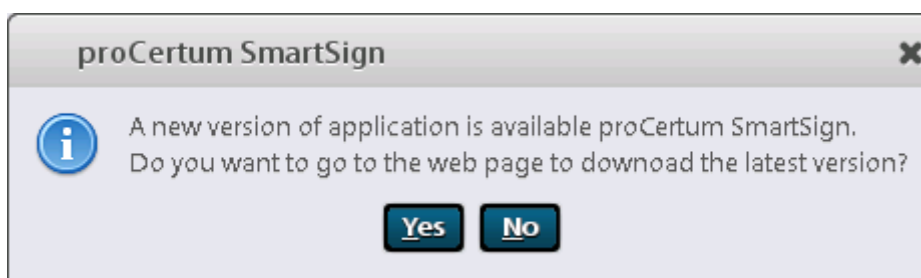


Window 67: System context menu

Update reporting.

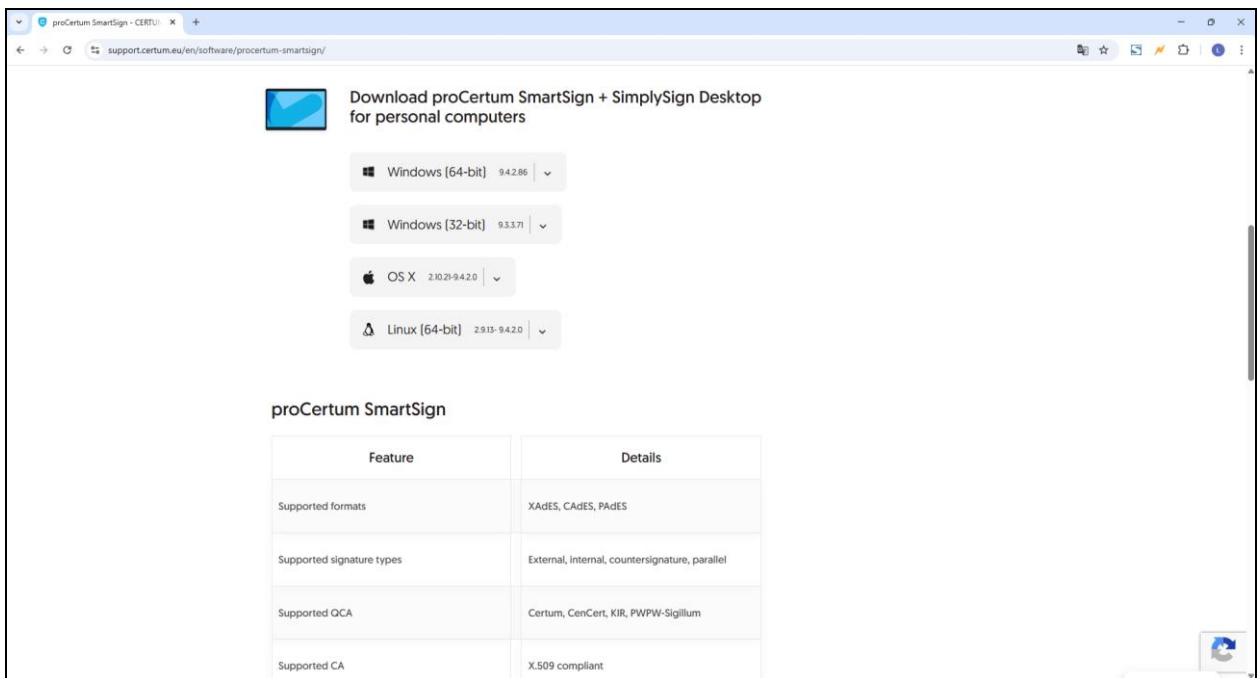
There is an **update reporting mechanism** included in **proCertum SmartSign** application, which will be activated by marking proper option in application general settings. The mechanism starts while getting the application started.

When the latest software will be available, following message will appear:



Window 68: Update message

After clicking button **Yes**, the **www page** window will be opened, where you can download the latest version of application. **To make the mechanism work, the computer has to be connected to the Internet.**



Window 69: WWW page with the latest proCertum SmartSign version

6. Table of windows

Window 1: Update information	6
Window 2: Update progress	7
Window 3: Information about the end of the update	7
Window 4: Installer Icon	9
Window 5: Setup language choice	9
Window 6: Welcoming window of installation wizard	10
Window 7: License agreement	10
Window 8: Choose Destination application	11
Window 9: Selecting the components to be installed	11
Window 10: Installer is ready to start the installation process	12
Window 11: The installation process has been successfully completed	12
Window 12: Main window of proCertum SmartSign application	13
Window 13: Information about library incompatibility	14
Window 14: Information about system – Library	14
Window 15: Information about system – Java Environment tab	15
Window 16: Bookmark Help	16
Window 17: Bookmark Help on the website WWW	17
Window 18: Settings – General tab	18
Window 19: Settings – General tab – part I	19
Window 20: Settings – General tab – part II	20
Window 21: Signature - Settings tab	21
Window 22: Signature - Settings tab	22
Window 23: The Settings tab - Signature - the part relating to Advanced options of signature	24
Window 24: Settings – Signature–Signer location	25
Window 25: Settings – Signature – XAdES advanced options	25
Window 26: Settings - Verification	26
Window 27: The Settings tab - Timestamp	28
Window 28: Signing	29
Window 29: Signing – List of elements to sign	30
Window 30: Searching for certificates	30
Window 31: List of qualified certificates	31
Window 32: List of qualified certificates and non-qualified certificates	31
Window 33: Certificate selection for signature operation	31
Window 34: Reminder referring to PIN insertion	32
Window 35: Signing... - Searching certificates	32
Window 36: Signing... - Performing signature	32
Window 37: Signing summary	33
Window 38: Signing – executed signature	33
Window 39: Signed data – Main tab	34
Window 40: Signed data – Signatures tab	34
Window 41: Window enabling selection of an action performed by at least one already existing signature	35
Window 42: Signed data – Main tab for multiple signature	35
Window 43: Signed data – signature for multiple signature tab	36
Window 44: Window enabling selection of action by at least one signature	36
Window 45: Window enabling signature selection for countersignature	37

Window 46: Signature selection window when all signatures for countersigning are selected	37
Window 47: Signed data – main tab for countersignature	37
Window 48: Signed data – signatures for countersignature tab	38
Window 49 Adding a signature graphic symbol - The main window	39
Window 50 Adding a graphic symbol of the signature - Indication of the graphic file	39
Window 51 a signature graphic symbol - The chosen graphic file	40
Window 52 a signature graphic symbol - graphical symbol added to the document	40
Window 53 Adding a graphic symbol of a placed signature - signed file with a placed graphic symbol of signature	41
Window 54 Adding a graphic symbol of a placed signature – multiple signature	41
Window 55: Signing tab – context menu	42
Window 56: Verifying tab	43
Window 57: Verifying tab – List of elements to verify	44
Window 58: Signed data	45
Window 59: Verifying tab – List of elements to verify	46
Window 60: Verification...	46
Window 61: Verification summary	47
Window 62: Verification status: Verified positively	47
Window 63: Verification status: Verified negative	48
Window 64: Signature value invalid	48
Window 65: Certificate invalid	49
Window 66: Verifying tab – context menu	50
Window 67: System context menu	51
Window 68: Update message	51
Window 69: WWW page with the latest proCertum SmartSign version	52