

---

# ***PEM-HEART Signature***

## **User's Guide**



ul. Jutrzenki 116, 02-230 Warsaw

Tel .: (+48) 22 570 57 10; Fax: (+48) 22 570 57 15

<http://www.enigma.com.pl> , [biuro@enigma.com.pl](mailto:biuro@enigma.com.pl)

---

## Table of Contents

0	Setting the English language .....	3
1	Introduction .....	5
2	Product safety .....	5
3	Signing.....	6
3.1	Signing - if you use smartcard or USB token .....	6
3.2	Signing - if you use rSign (cloud signing).....	8
4	Signature verification .....	13
5	Work in the main program window .....	16
5.1	Starting the program .....	16
5.2	Signing from the main program window .....	17
5.2.1	Signing from the main program window – if you use the smartcard or USB token.....	17
5.2.2	Signing from the main program window - if you use rSign (cloud signing).....	18
5.3	Signature verification .....	21
5.4	Signing a file that has been already signed.....	23
5.5	Countersignature.....	24
5.6	Time stamping .....	26
5.7	Placing the XML document signature in specified position.....	27
6	Smart card support.....	29
6.1	Changing the PIN .....	29
6.2	Unlocking the card .....	30
6.3	Diagnostics .....	31
7	Signing with rSign (cloud signing).....	33
7.1	The configuration on your desktop.....	33
7.2	Installing the certificate that was renewed online on another computer.....	36
7.3	Removing the certificate configuration (or one of the rSign certificates) from the computer .....	38
7.4	rSign application on your mobile phone.....	40
7.4.1	Main windows .....	40
7.4.2	Reading the key ID .....	40
7.4.3	Backup of mobile application data .....	40
7.4.4	Changing the application PIN.....	41
7.4.5	Authorized mobile telephone number .....	41
7.4.6	Signature PIN timeout (remembering the signature PIN) .....	42
7.4.7	Transferring activation data from another phone .....	43
7.4.8	Deactivating the signature data on the phone .....	45
8	Program options, working without Internet.....	46
8.1	Options of signatures .....	46
8.2	Files .....	47
8.3	Proxy.....	48
8.4	PIN.....	48
8.5	Certificates.....	48
8.6	TSL lists.....	49
8.7	General .....	50
8.8	Updates .....	50
8.9	Import Data.....	51
9	Troubleshooting.....	52

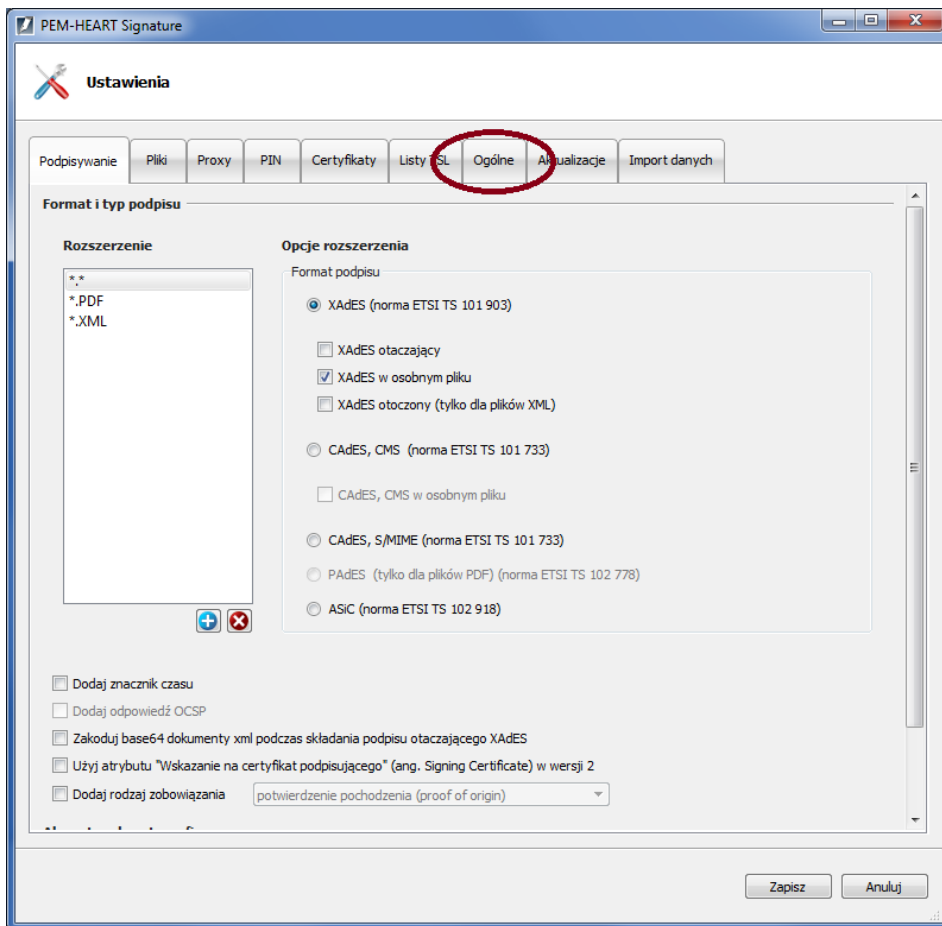
## 0 Setting the English language

To change the language to English, launch the PEM-HEART Signature program.

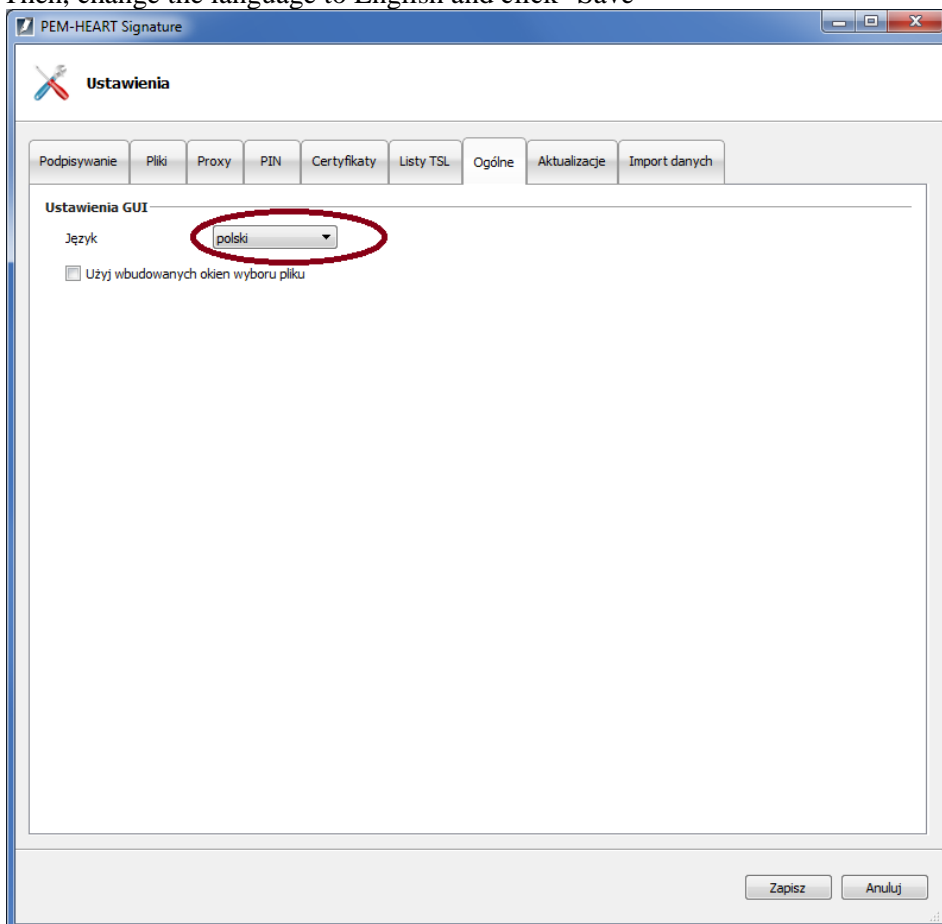
Then click "Ustawienia" button.



Then choose "Ogólne" tab



Then, change the language to English and click "Save"



# 1 Introduction

**PEM-HEART Signature** software is designated to:

- 1) create qualified signatures or electronic seals based on certificates issued by CenCert,
- 2) validate qualified electronic signatures or seals (also based on certificates issued in other EU countries), when the certificate is valid (not outside the validity period).

It is also possible to:

- validate electronic signatures/seals outside the certificate validity period, if the signature is in the archival form (see description of the archival form in the Notes in Chapter 4), or
- validate signatures/seals based on commercial (non-qualified) certificates issued by CenCert.

## 2 Product safety

The program should be used on a computer which is under control of the certificate owner. The computer should be protected from access by unauthorized persons, have installed anti-virus software up to date and current operating system updates.

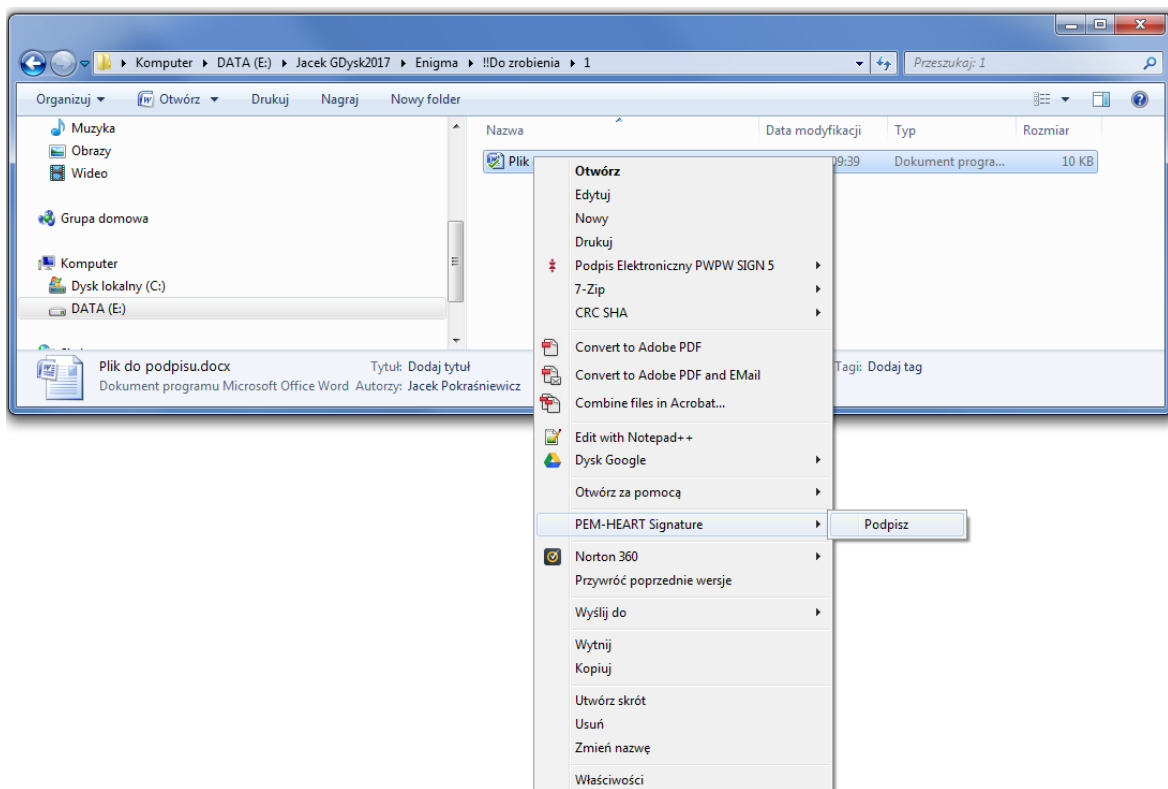
Electronic signatures must not be made on a computer which safety is unknown (e.g. computer available to the public or to untrusted people, etc.).

## 3 Signing

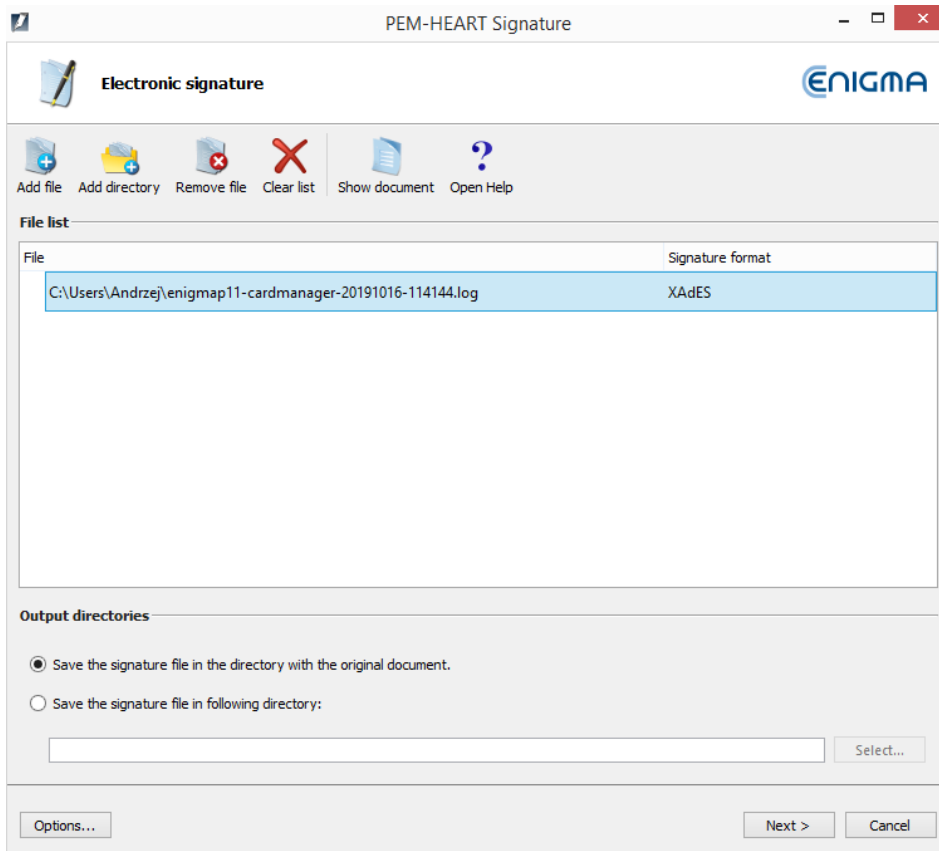
### 3.1 Signing - if you use smartcard or USB token

If you work on *Mac OS* or *Linux* - go to chapter 5.2.

For sign a file on a disk, insert your CenCert card into a card reader (or insert USB token to the USB port), then **Right** click on the file name. Then select the menu command **PEM-HEART Signature** -> **Podpisz**.

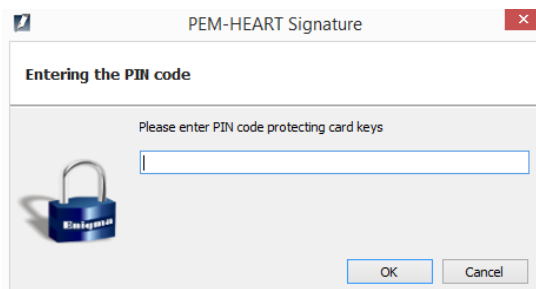


The signature window is displayed:

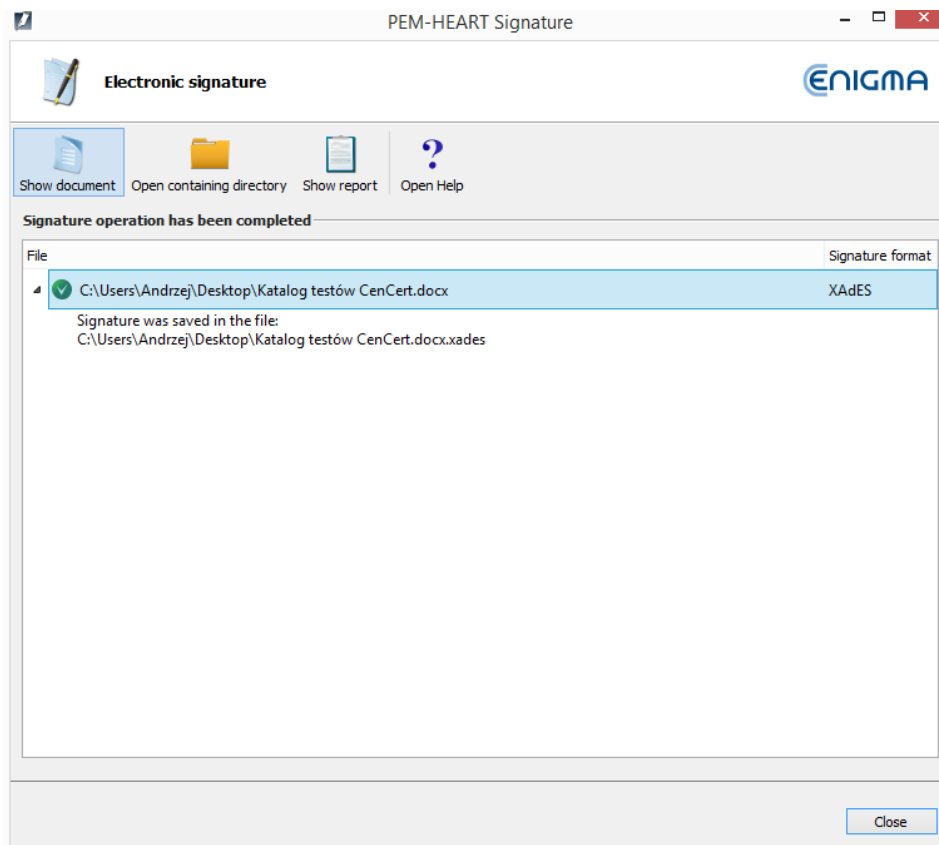


If the signature format suits you (in this case it's XAdES), press the *Next* button.

Then the program asks for the PIN to your card:



and generates qualified electronic signature:



#### Comments:

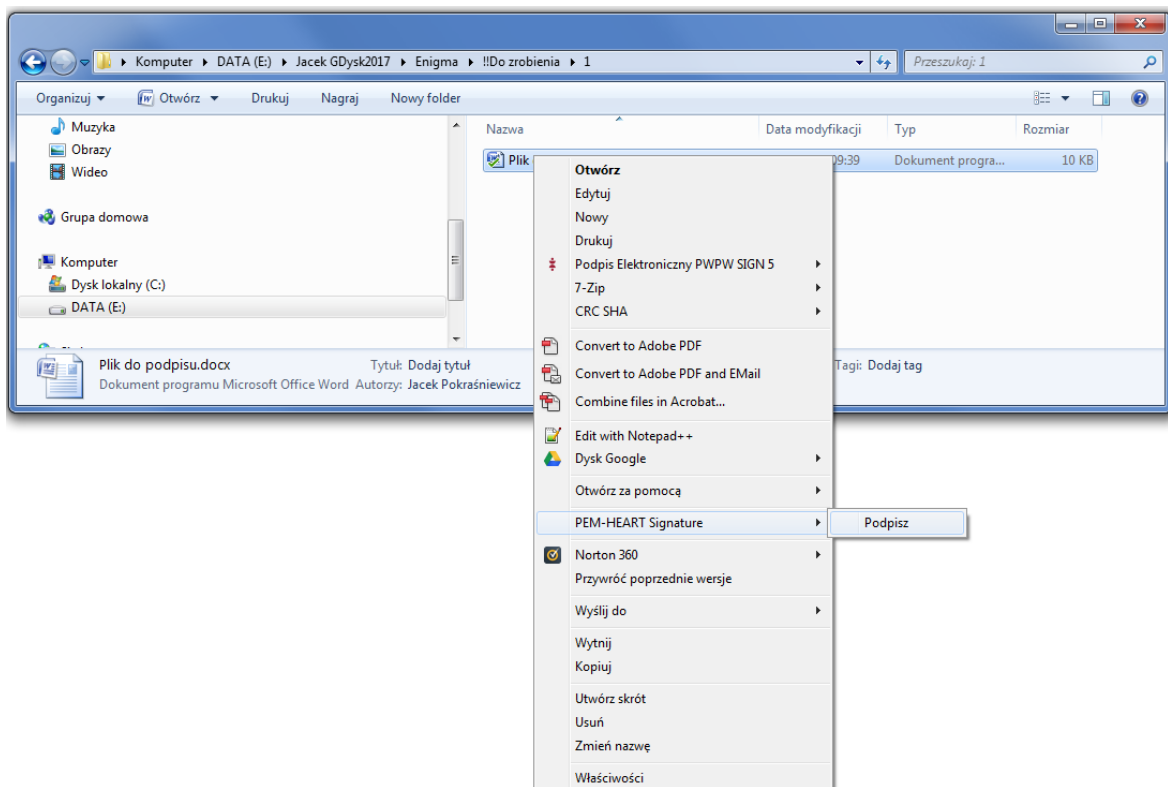
- 1) Advanced options such as a format of signatures, placing signatures in a separate files, time stamping, and other settings - are available under the button *Options*. Settings changed in this way refer to one signature and are not remembered for later use. For general options see chapter 8.1.
- 2) Depending on the signature format, a signature will be saved in the same file without changing the name or in a new file with the changed file name extension.
- 3) If you choose "signature in a separate file", the signature will be saved in a separate file. In this case, you must provide two files to the recipient: the original (signed) file and the signature file.
- 4) If the signature is to contain a time stamp and / or OCSP token, an Internet connection is required when signing. You may also need to buy a time stamping service package.

## 3.2 Signing - if you use rSign (cloud signing)

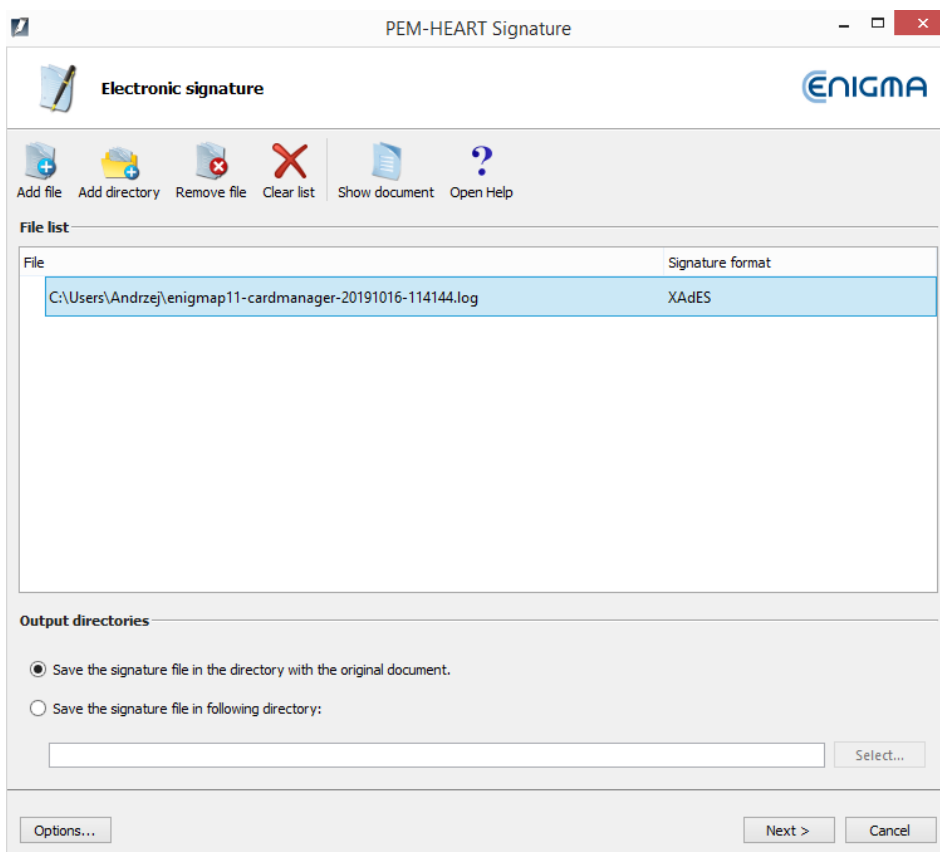
If you work on *Mac OS* or *Linux* - go to chapter 5.2.

For sign a file on a disk, insert your CenCert card into a card reader (or insert USB token to the USB port), then **Right** click on the file name. Then select the menu command **PEM-HEART Signature** -> **Podpisz**.



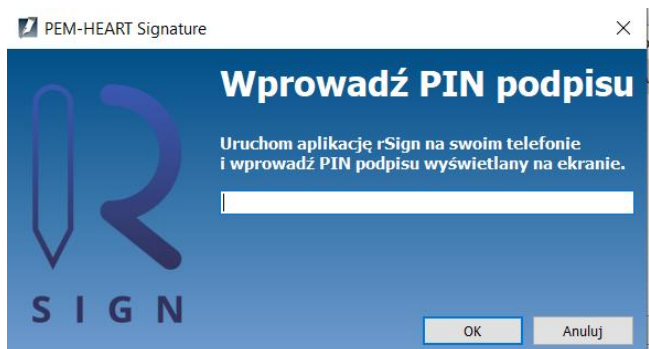


The signature window is displayed:

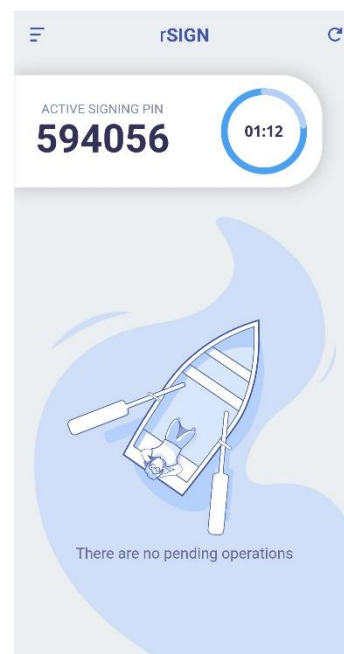


If the signature format suits you (in this case it's XAdES), press the *Next* button.

Then the program asks for your signature PIN:

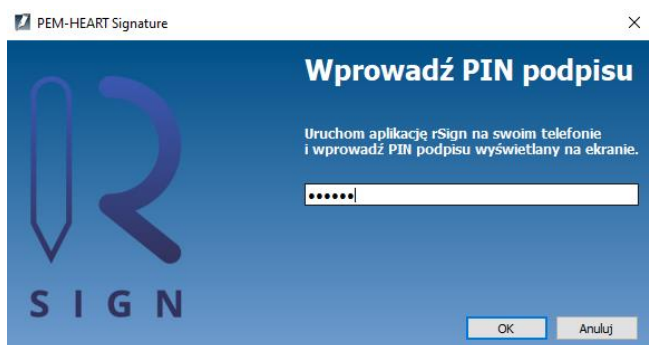


Now, you should activate the application *rSign by CenCert* on your mobile.

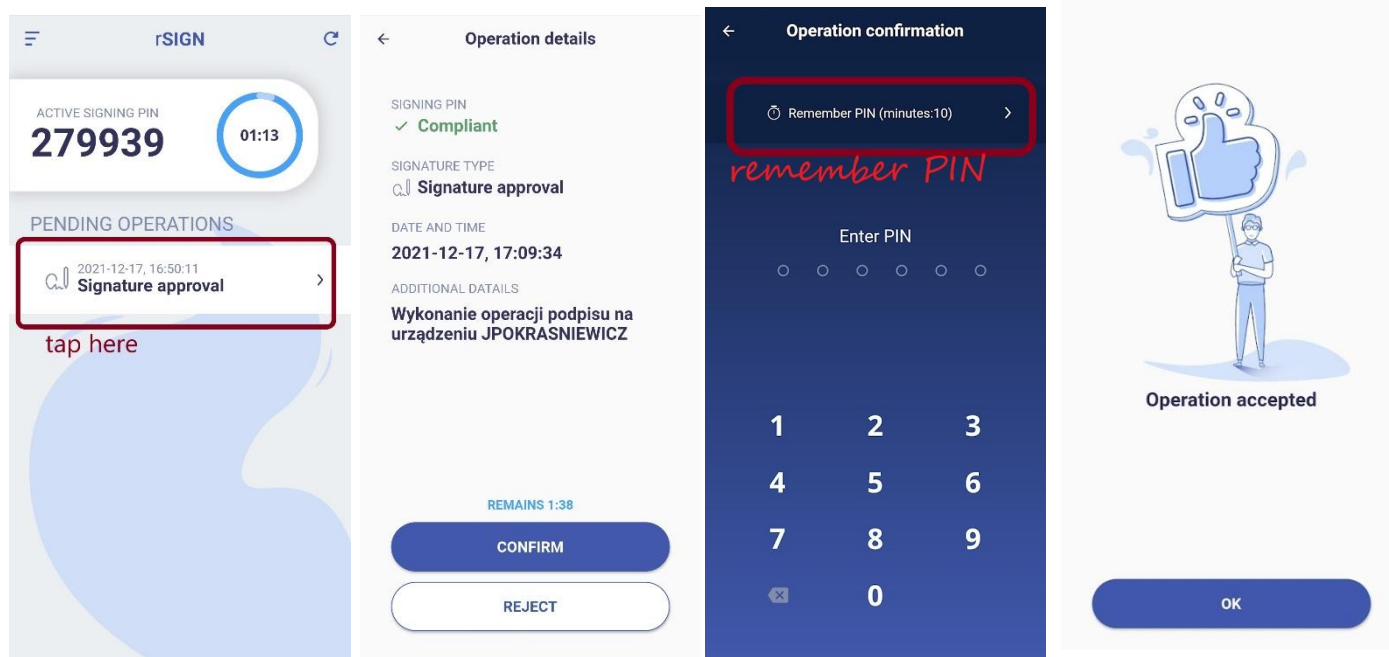


When you activate the application on your mobile, read the ACTIVE SIGNING PIN

and rewrite this PIN into the desktop signature application:

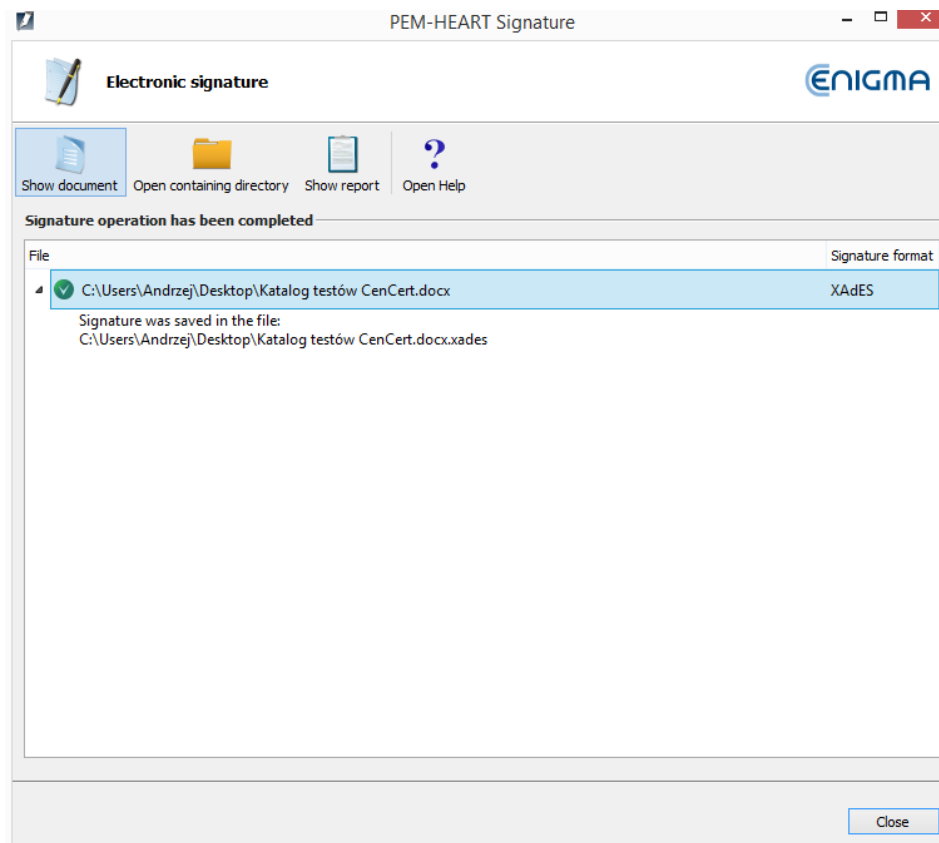


Now you must confirm the signature on your mobile (in the rSign application).



Attention! We recommend setting the *Remember PIN* option, with a value of at least 2 minutes. It allows you to place a signature with time stamping or even multiple signatures (if many files have been indicated in the program to be signed), without the need to approve each signature operation on the phone separately. If you set the signature to one-time (*don't remember PIN* option), then performing a signature with a time stamp will require double approval of the signature on the phone (signature under the document, signature under the request for time stamping).

After confirming the operation on the phone, the program will perform the signature:

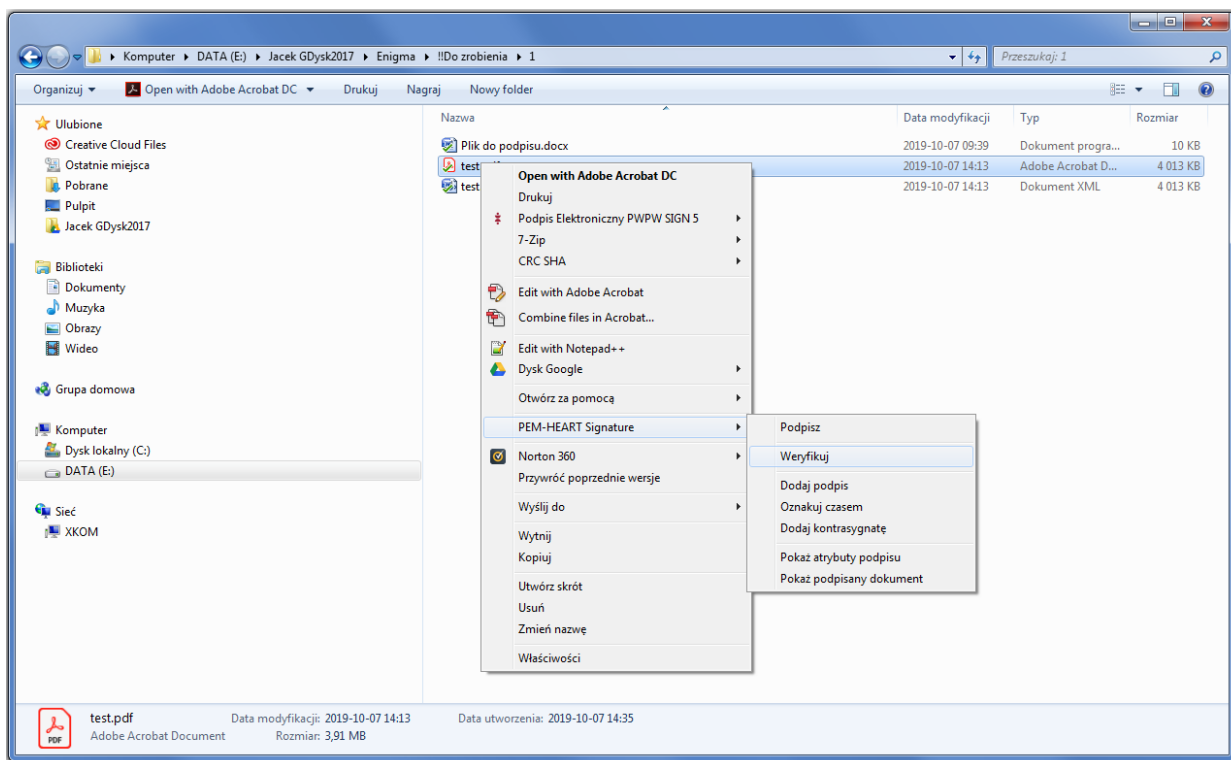
**Comments:**

- 1) Advanced options such as a format of signatures, placing signatures in a separate files, time stamping, and other settings - are available under the button *Options*. Settings changed in this way refer to one signature and are not remembered for later use. For general options see chapter 8.1.
- 2) Depending on the signature format, a signature will be saved in the same file without changing the name or in a new file with the changed file name extension.
- 3) If you choose "signature in a separate file", the signature will be saved in a separate file. In this case, you must provide two files to the recipient: the original (signed) file and the signature file.
- 4) An Internet connection is required when signing.

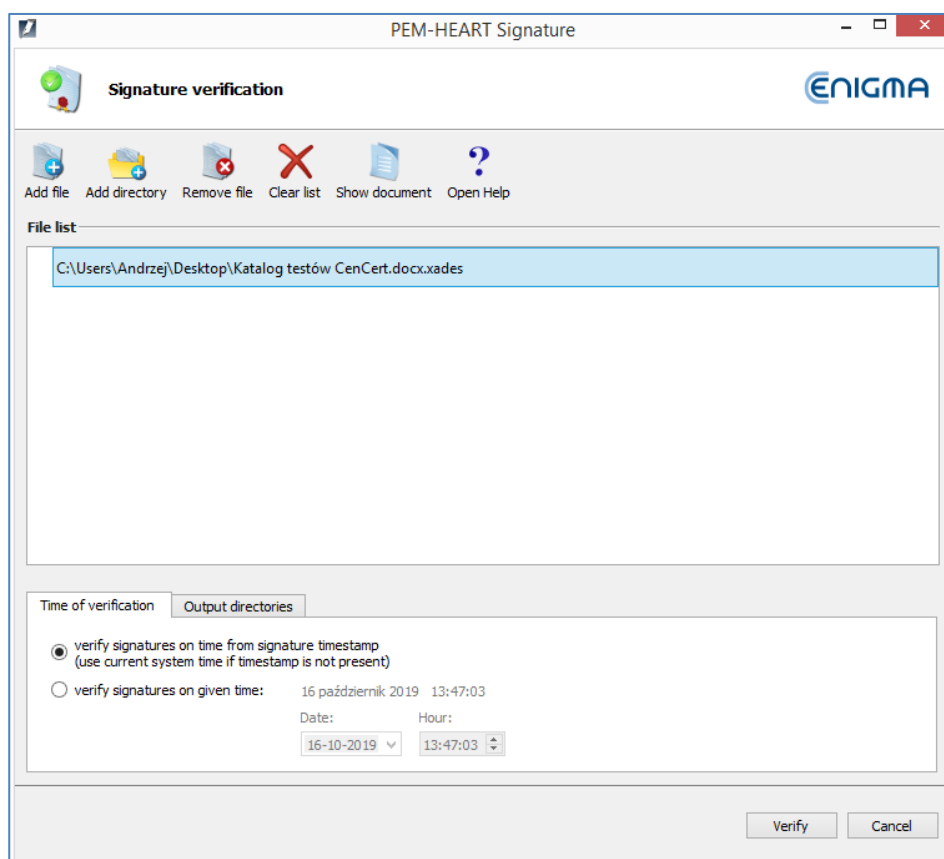
## 4 Signature verification

If you work on *Mac OS* or *Linux* - go to chapter 5.2.2.

To verify a signature, **Right** click on the signature file (or signed filer) name, and then choose **PEM-HEART Signature** -> **Weryfikuj**.

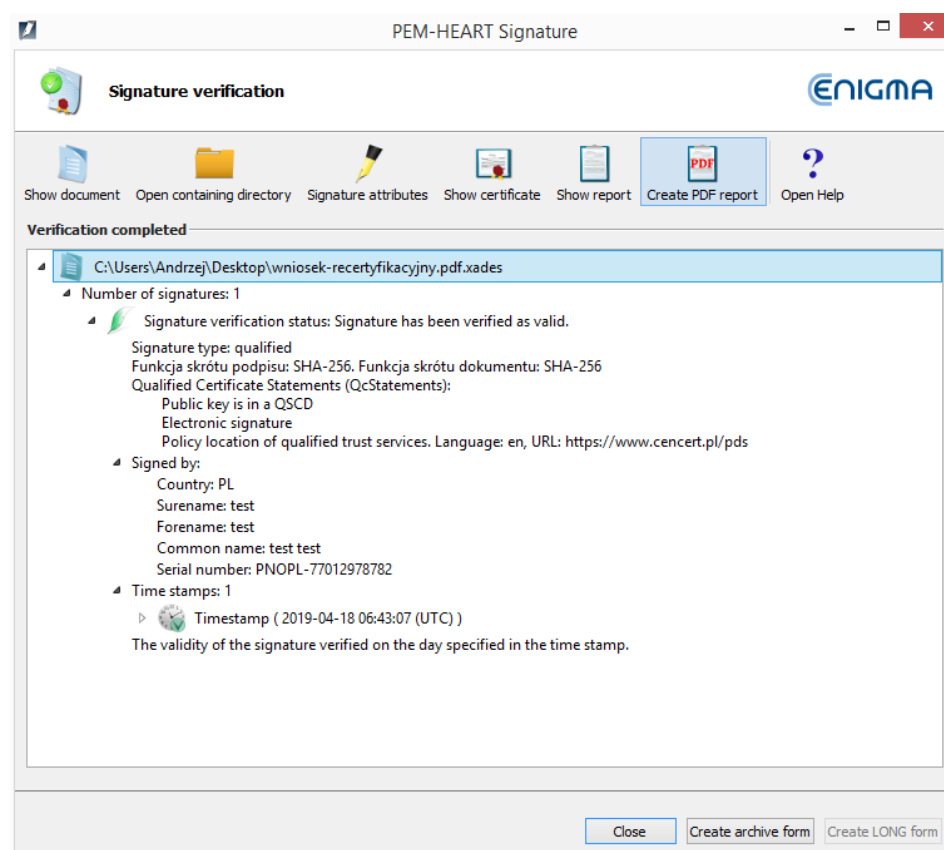


Then program displays signature verification window:



Press the *Verify* button.

The program verifies the signatures (or seals) saved in the document and displays the verification result:



If the signature has been time stamped - the time on which the signature is verified is taken from the time stamp (so any subsequent revocation of signing certificate doesn't affect the result of verification).

If the signature does not have a time stamp - the signature is verified on current time or on another time manually entered ("verify signatures on a given time: ..."). In the case of manual entry of time, the responsibility of the correctness of this time (if needed also proving that the signature existed at that moment) lies solely on the user.

The verification result is marked with colorful symbols for clear identification:

- Green means correct signature verification.
- Yellow means incomplete verification - the signature is mathematically correct, but it cannot be confirmed yet whether the certificate was valid at the time of signing. In this case, the verification should be repeated later - e.g. in a few hours or the next day.
- Red indicates a failure to verify the signature (e.g. mathematical incompatibility, i.e. a violation of the document's integrity or the case of revoked certificate) .

### Comments:

1) Additional actions are available at the top menu:

- a) *Create PDF report* - saves the clear report (in PDF) confirming the status of the signature verification.
- b) *Show certificate* - displays the certificate used to sign (and possibly personal data of person who has signed the document).
- c) *Show document* - displays the original (signed) document, if there is a program installed on the computer for displaying a given document type.
- d) *Signature attributes* - displays additional data attached to the signature.
- e) *Open containing directory* - opens the directory view on the disk where the signed document exists.

2) After validating the signature, you can create advanced forms of signature:

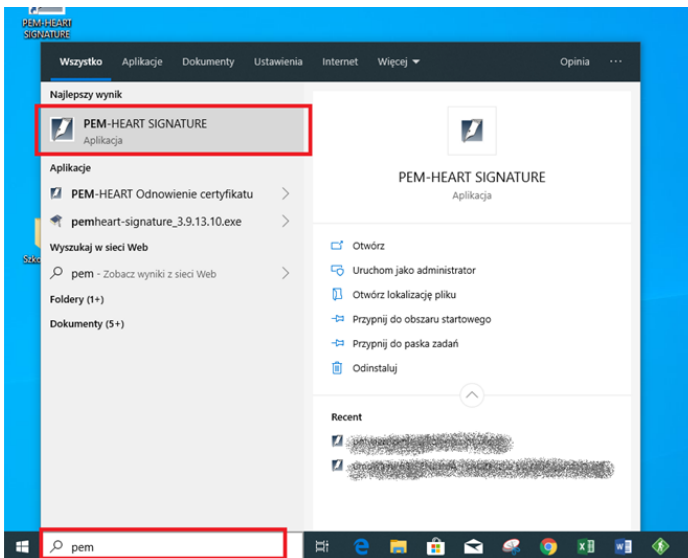
- a) *Archive form* - secures the possibility of the correct signature verification for the period of validity of a time stamp (practically about 7-10 years). Creating an archive form requires access to the Internet and downloading, among others, two time stamps. You may need to buy a time stamping service package.
- b) *Long form* - secures the possibility of the correct signature verification for the period of validity of a OCSP and a time stamp (practically about 5 -10 years). Creating a *long* character requires access to the Internet and download, among others, one timestamp. You may need to buy a time stamping service package.

# 5 Work in the main program window

## 5.1 Starting the program

All program functions (including signing and signature verification) are available after starting the **PEM-HEART Signature program** from the Start menu (MS Windows) or from the icon on the desktop. If you use other operating system (MacOS or Linux), run the program in a way appropriate for your system. The program's appearance is the same as in MS Windows.

Example run from the menu *Start Windows*.



After starting the application the main program window is displayed:



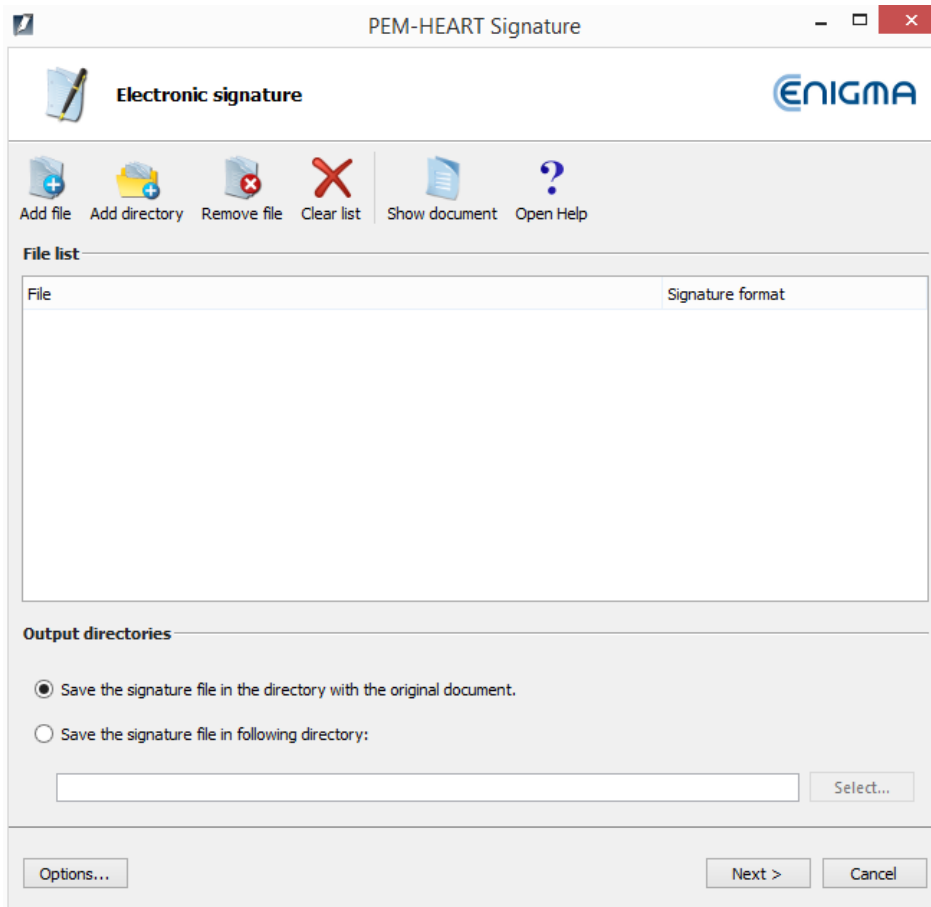


## 5.2 Signing from the main program window

### 5.2.1 Signing from the main program window – if you use the smartcard or USB token.

In order to sign, in the main program window (see chapter 5.1), press the *Sign* icon (menu on the left).

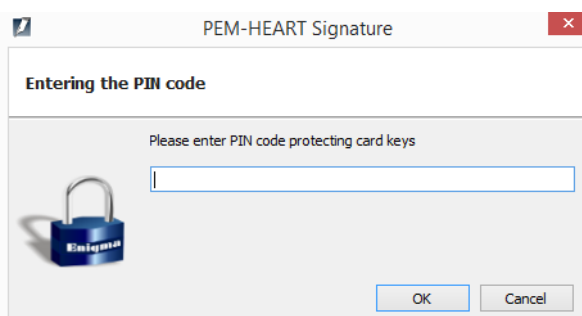
The signature window is displayed:



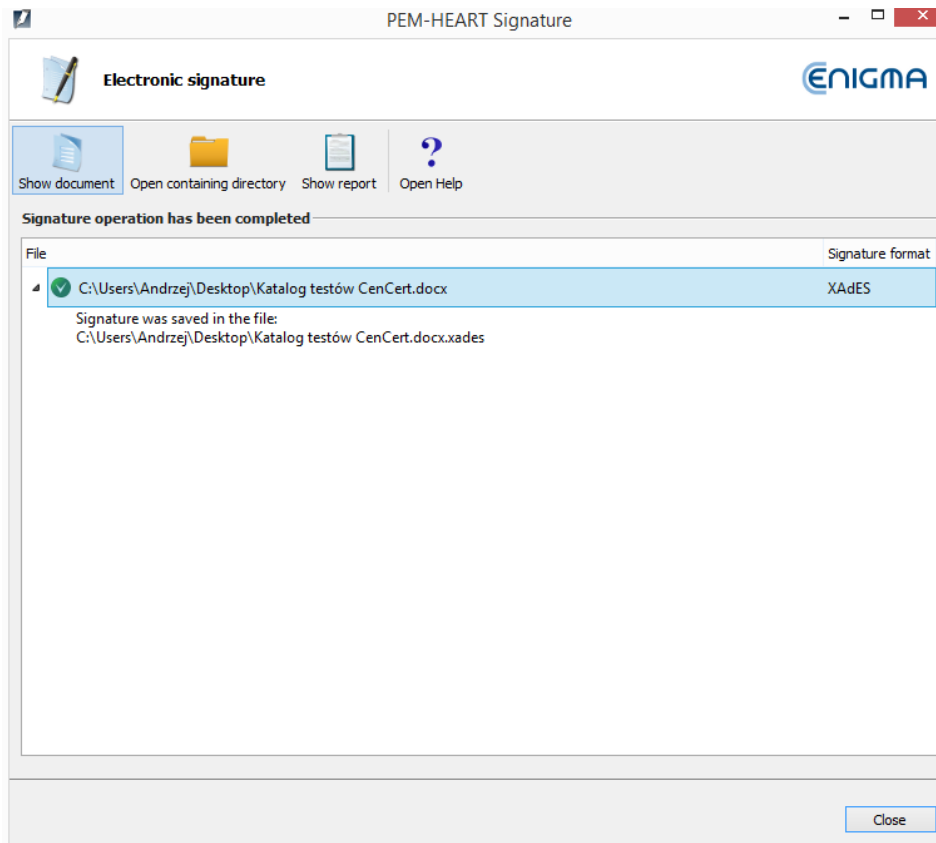
Add file or files (icon *Add file* on the top menu). If you prefer to specify the directory (icon *Add directory*), all files in this directory and its subdirectories will be chosen.

Press the *Next* button to proceed.

Then it asks for the card PIN:



and makes the signature:

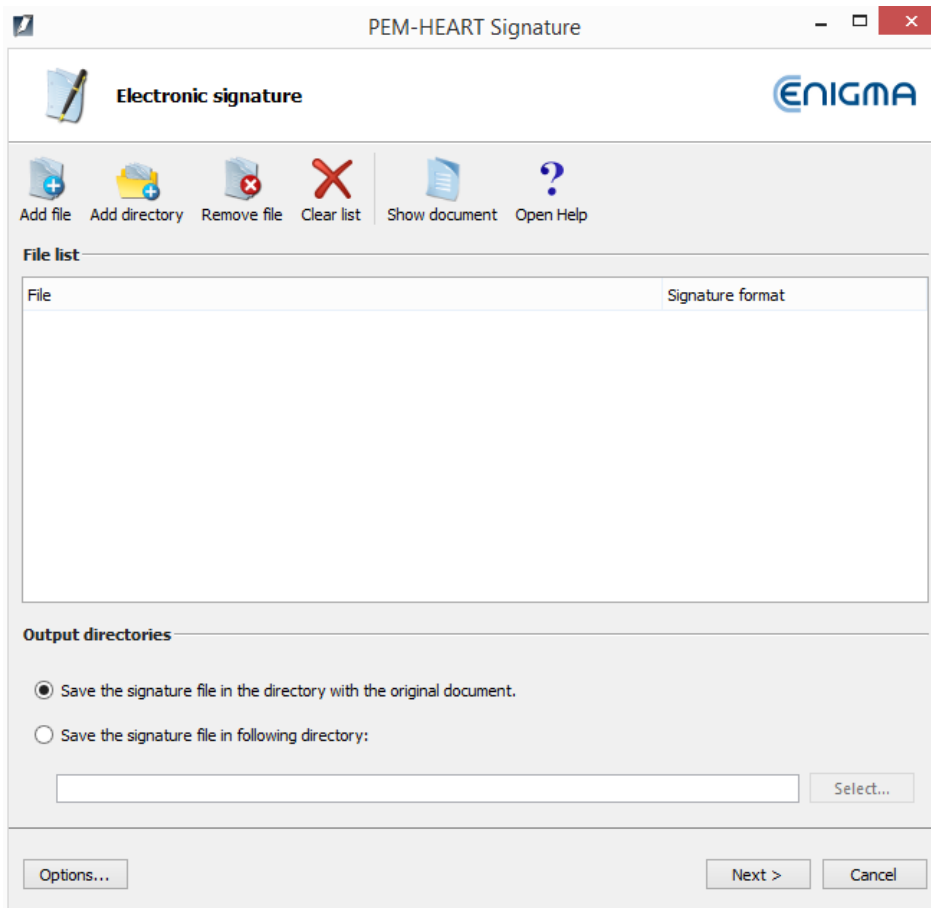
**Comments:**

- 1) Advanced options such as a format of signatures, placing signatures in a separate files, time stamping, and other settings - are available under the button *Options*. Settings changed in this way refer to only one signature and are not remembered for later use. See also general settings in chapter 8.1
- 2) Depending on the signature format, the signature will be saved in the same file without changing the name or in a new file with the changed file name extension.
- 3) If you choose "signature in a separate file", the signature will be saved in a separate file. In this case, you need to provide two files to the recipient: the original file and the file with the signature.
- 4) If the signature is to contain a time stamp and / or OCSP, an Internet connection is required when signing. You may also need to buy a time stamping service package.

### **5.2.2 Signing from the main program window - if you use rSign (cloud signing)**

In order to sign, in the main program window (see chapter 5.1), press the *Sign* icon (menu on the left).

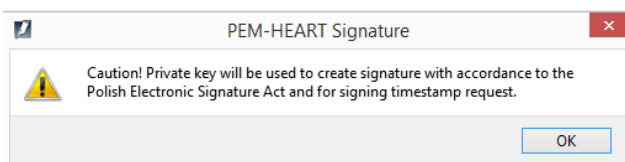
The signature window is displayed:



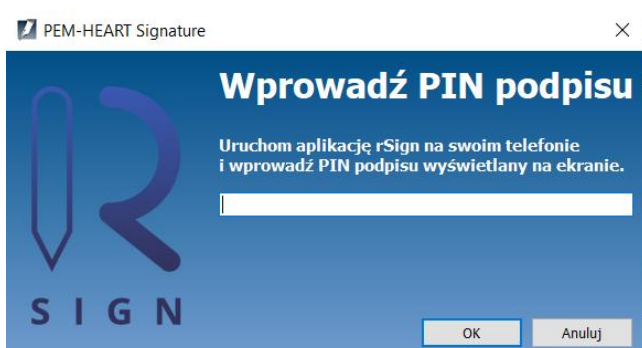
Add file or files (icon *Add file* on the top menu). If you prefer to specify the directory (icon *Add directory*), all files in this directory and its subdirectories will be chosen.

Press the *Next* button to proceed.

The program gives a warning that your private key will be used:

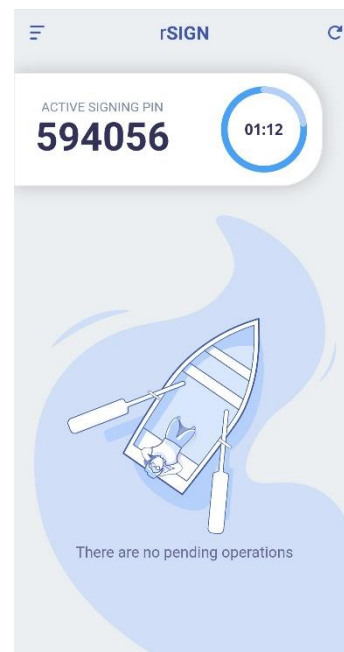


Then the program asks for your signature PIN:

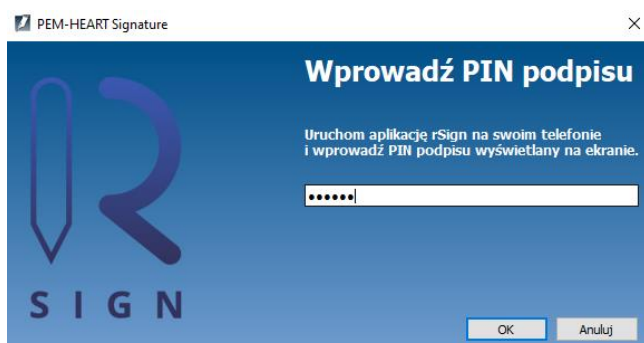


Now, you should activate the application *rSign* by *CenCert* on your mobile.

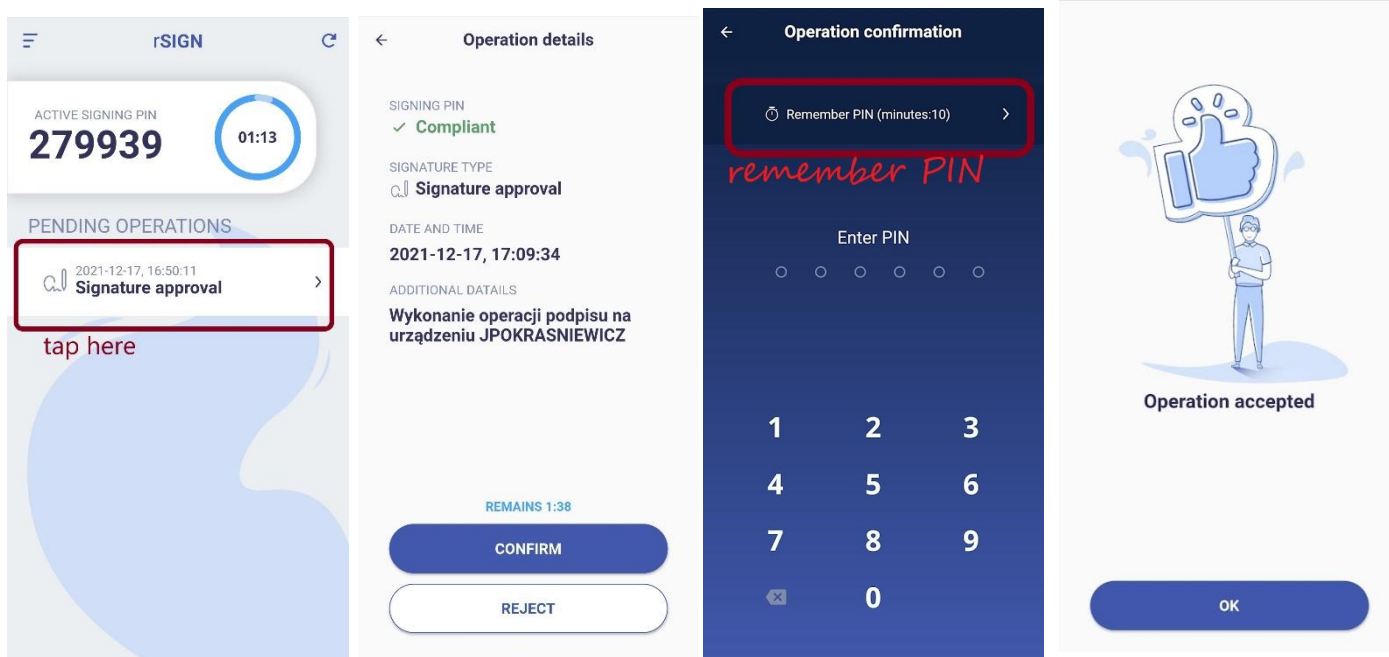
When you activate the application on your mobile, read the ACTIVE SIGNING PIN



and rewrite this PIN into the desktop signature application:

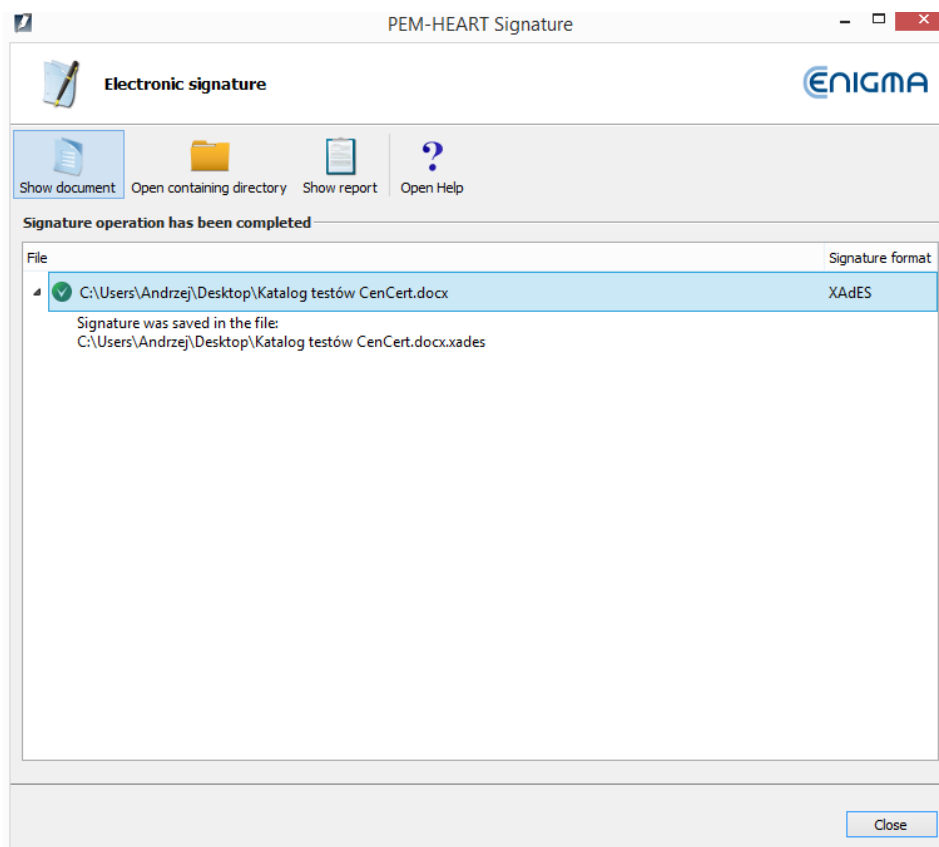


Now you must confirm the signature on your mobile (in the rSign application).



Attention! We recommend setting the *Remember PIN* option, with a value of at least 2 minutes. It allows you to place a signature with time stamping or even multiple signatures (if many files have been indicated in the program to be signed), without the need to approve each signature operation on the phone separately. If you set the signature to one-time (*don't remember PIN* option), then performing a signature with a time stamp will require double approval of the signature on the phone (signature under the document, signature under the request for time stamping).

After confirming the operation on the phone, the program will perform the signature:



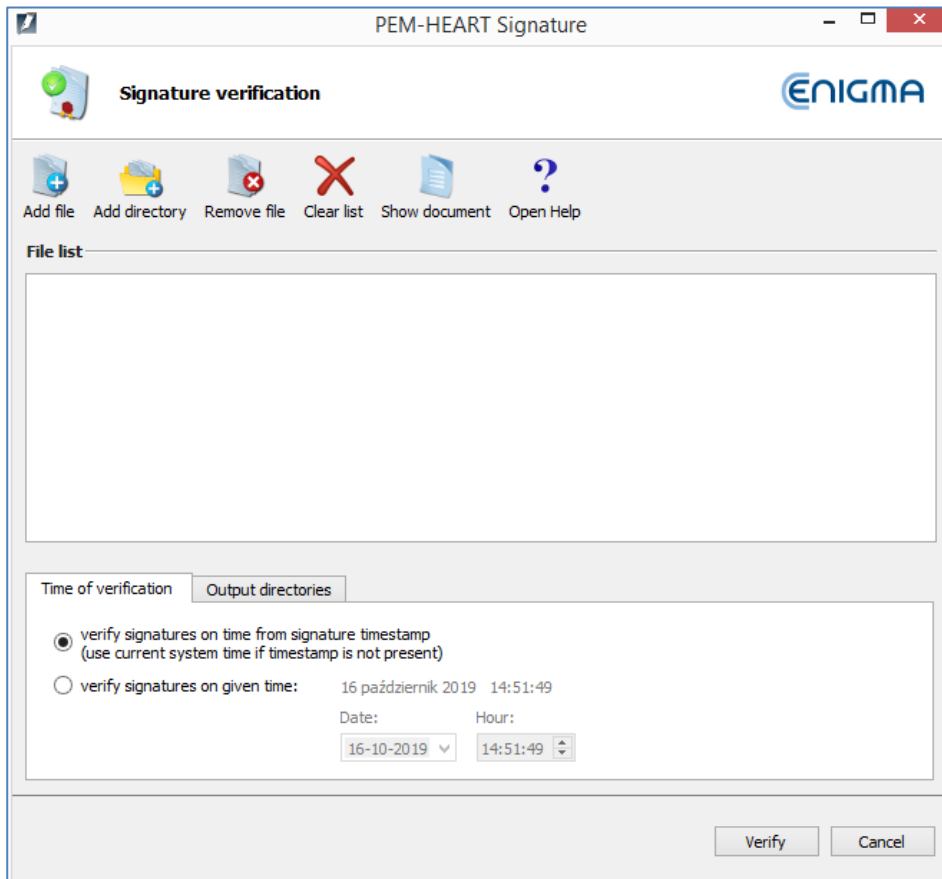
#### Comments:

- 1) Advanced options such as a format of signatures, placing signatures in a separate files, time stamping, and other settings - are available under the button *Options*. Settings changed in this way refer to one signature and are not remembered for later use. For general options see chapter 8.1.
- 2) Depending on the signature format, a signature will be saved in the same file without changing the name or in a new file with the changed file name extension.
- 3) If you choose "signature in a separate file", the signature will be saved in a separate file. In this case, you must provide two files to the recipient: the original (signed) file and the signature file.
- 4) An Internet connection is required when signing.

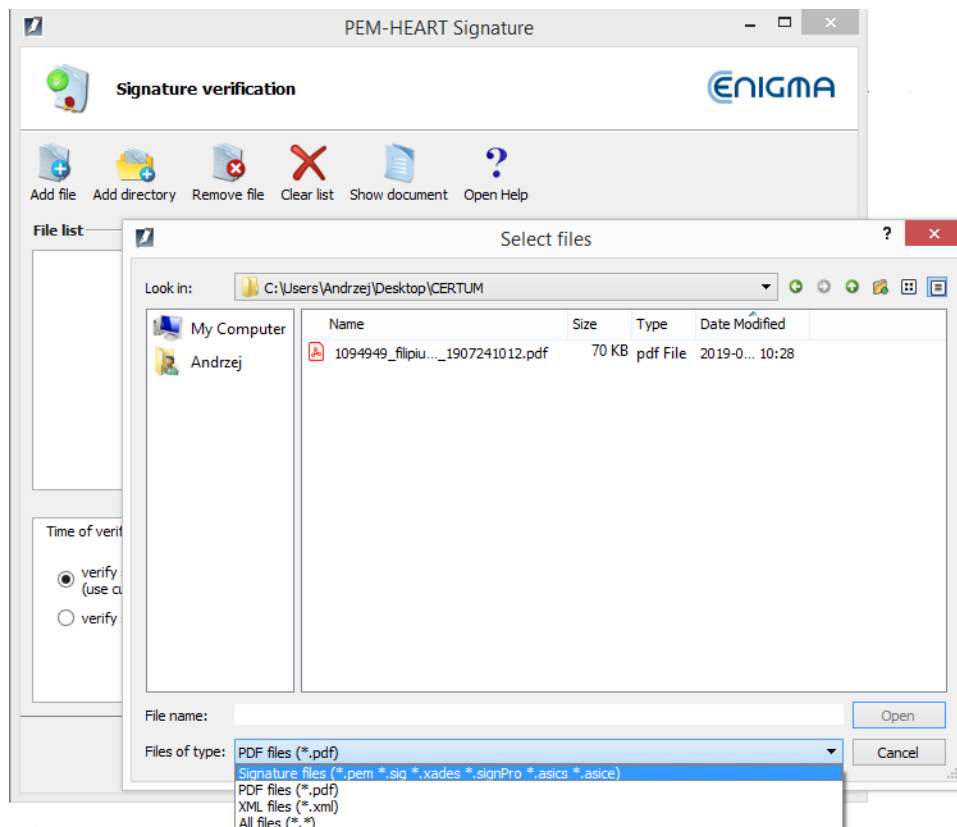
## 5.3 Signature verification

To verify the signature, in the main program window (see chapter 5.1), press the *Verify* icon (menu on the left side of the main window).

The signature window is displayed:



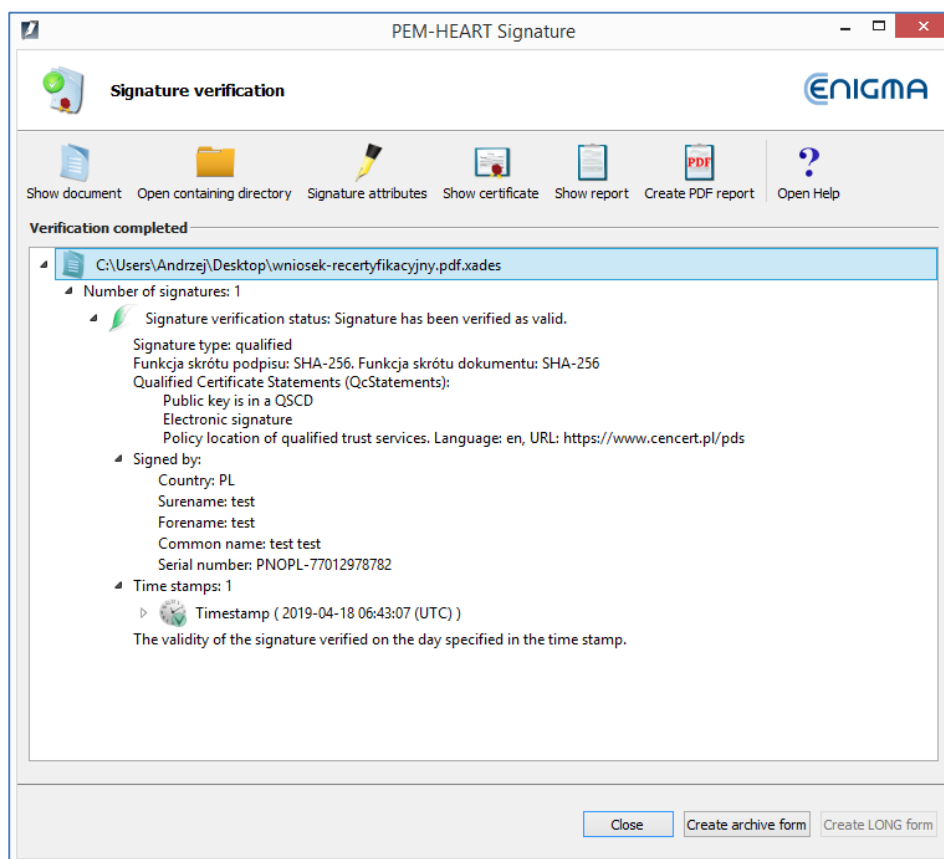
Now add the file or files to verify (*Add file* button on the top menu). If necessary, you may change the file name extension filter (e.g. to "\*.pdf").



Choosing the directory (*Add directory* button) makes all files from this directory and its subdirectories to be chosen.

When you choose files, press the *Verify* button to proceed.

The program verifies electronic signatures saved in the documents and displays the result of the verification:



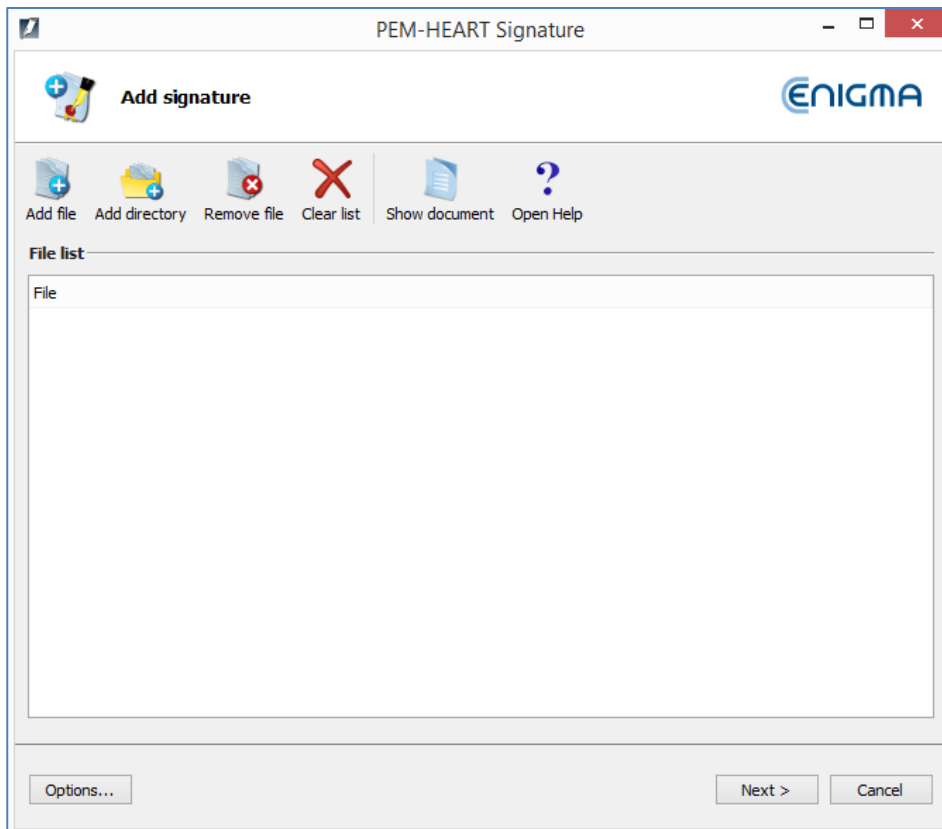
See also the verification notes in the chapter 4.

## 5.4 Signing a file that has been already signed

A document that has been already signed may be additionally signed by the same or another person. The next signature should be in the same format as previous ones - the program automatically chooses proper options when you add the next signature.

To add a signature, in the main program window (see chapter 5.1), select menu *Advanced functions* (left side bar of the main program window - see 5.1) and press the *Add signature* icon.

The signature window is displayed:



The further signing process is the same as when you place the first signature in the document (see chapter 5.2). The only difference is that you can't change the signature format (*Options...*) - it must be the same as of previous signatures.

#### Comments:

- 1) In the case of the XAdES signature format, the method of placing multiple signatures in one document is not described in standards. Various format compatibility errors may occur, adding the next signature may destroy previous signature, especially when signatures were made by software prepared by various companies. Because of that, we recommend to check (verify) signatures after adding the next signature in the XAdES format.

## 5.5 Countersignature

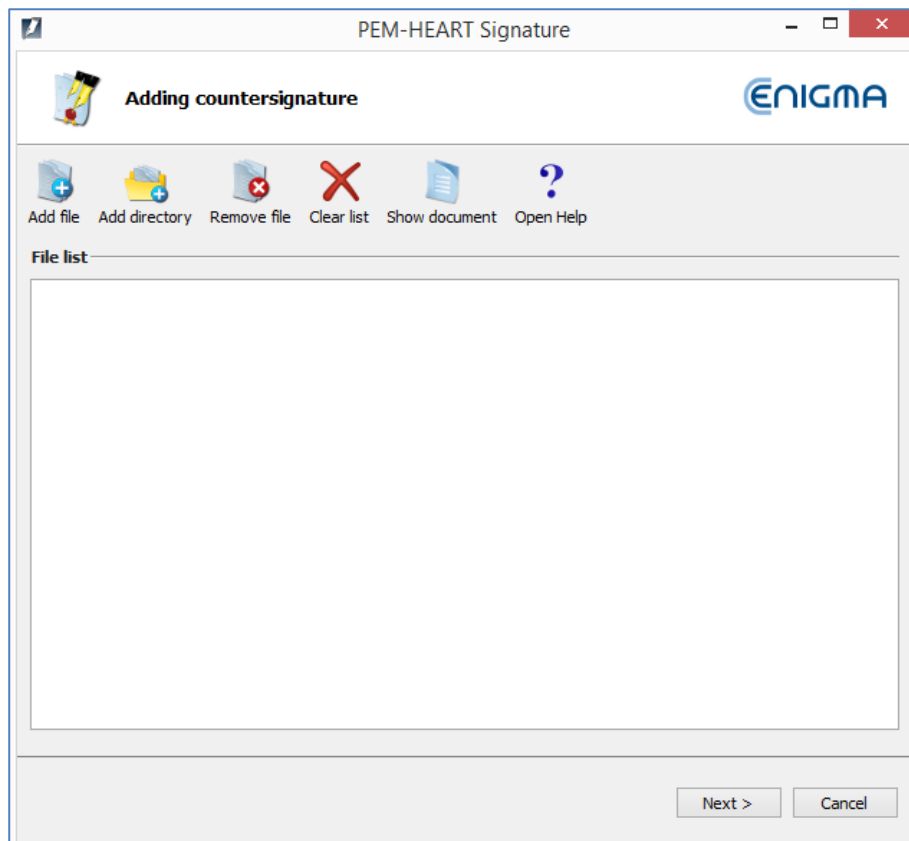
A "countersignature" is a special way of creating signatures, in which you technically don't sign the document itself but you sign previous signature instead (the document is signed indirectly). That mode of signing prevents the possibility of removal previous signatures from the document (when your signature is still valid). In the case of standard multiple signatures, one may be able to remove the previous signature from the document while retaining your signature valid (the "countersignature" makes this impossible) .

The term "countersignature" in the above sense should not be confused with the same legal term. The submission of an electronic signature as a "countersignature" (in the sense described above) is not reflected in legal records regarding electronic signatures. The general provisions on electronic signatures apply. In legal terms, this technical "qualified countersignature" is the same, as any other "qualified electronic signature".



In order to make a "countersign", in the main program window (see chapter 5.1), select menu *Advanced functions* (left side bar of the main program window - see 5.1) and press the icon *Countersignature*.

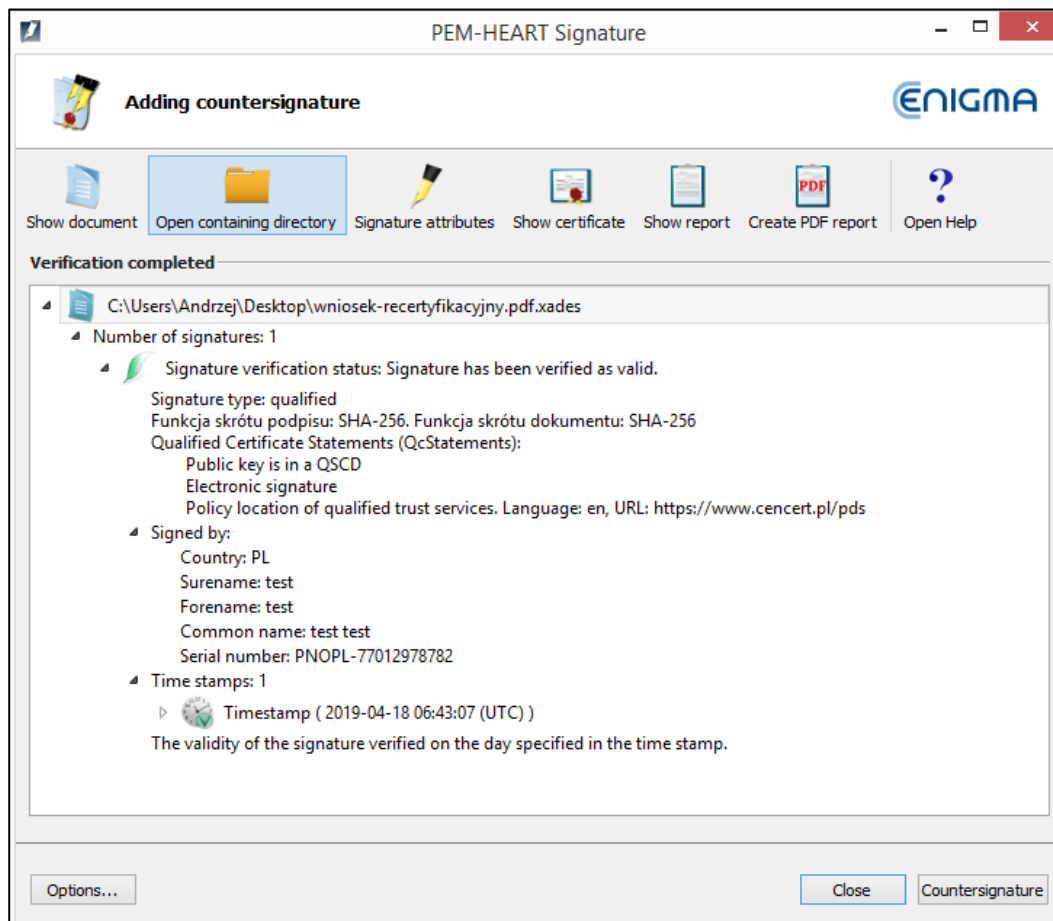
The countersign window is displayed:



Add file or files (icon *Add file* on the top menu) or directories (icon *Add directory*).

Then press the *Next* button to proceed.

Present electronic signatures are verified and the program displays the status of the verification:



Press the *Countersignature* to proceed. The program asks for the PIN for your card and creates the signature in the form of "countersignature".

## 5.6 Time stamping

A qualified time stamp gives the evidence of the existence of a document at given time. In Polish law, a document with a qualified time stamp has a legal "certain date". In the whole EU (under *eIDAS* regulation), qualified electronic time stamp benefits from a presumption of accuracy the date and time, which indicates and the integrity of the data that has been stamped.

If a time stamp is added to a electronic signature, it confirms not only the existence of the signed document, but also the signature itself, which protects against the legal consequences of subsequent revocation of the certificate used for the signature.

The time stamp (except for signatures in the PAdES format) may also be attached to the signature later, even by the recipient of the document (in fact, the recipient of the document is often more interested in the possibility of long-term signature verification). Other advanced forms of signatures should also be considered - a *long* and an *archival* forms (see comments in chapter 4). These forms also use time stamps, among other data needed for verification.

In order to add time stamp to the signature, in the main program window (see chapter 5.1), select menu *Advanced functions* (left side bar of the main program window) and press the icon *Add timestamp*.

The time stamping window is displayed. Choose file, files or directories (icons *Add file*, *Add directory* on the top menu) - as in the case of signing or signature verification mode (see chapter 5.2 or 5.2.2). When you push the *Next* button, the program asks for the PIN for your card (to sign a time stamping request), then adds a time stamp to each signature contained in chosen files.

**Warning:**

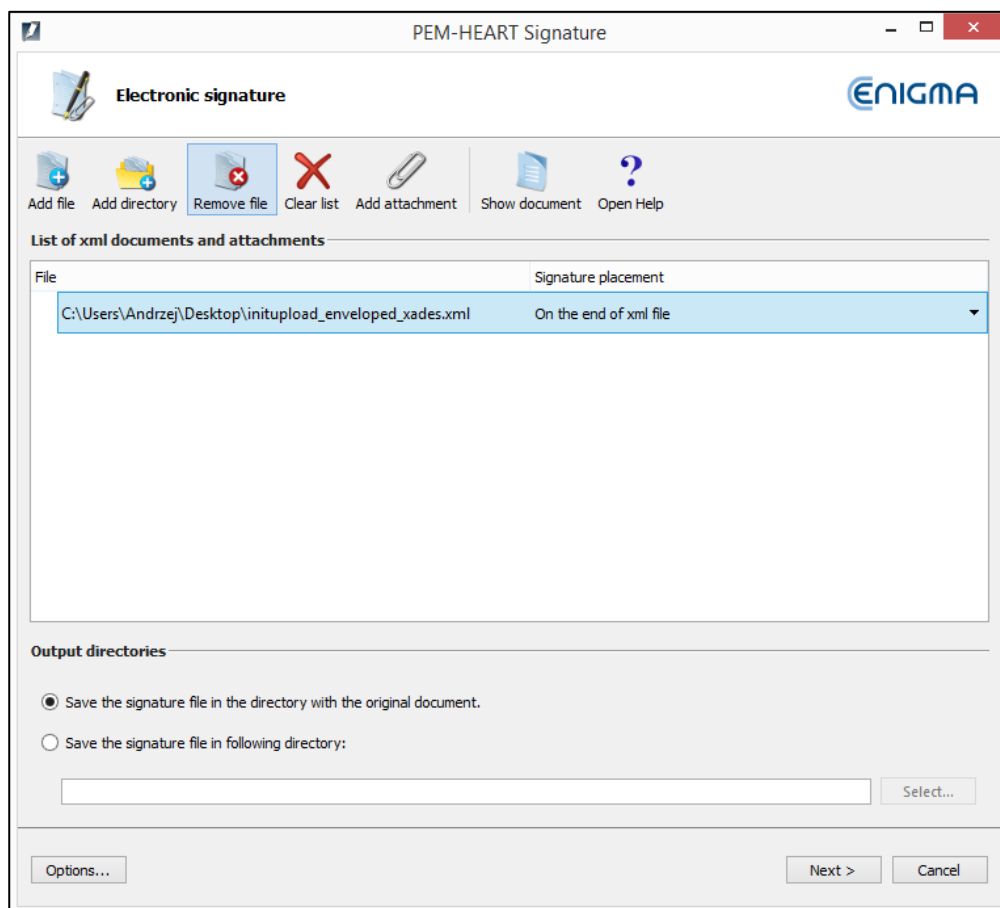
- 1) Purchasing of a time stamping service package may be required.

## 5.7 Placing the XML document signature in specified position

By default, when a program signs an XML document (*XAdES enveloped* format), it places the signature at the end of the document structure. In the majority of cases, this is sufficient and meets the requirements of systems using signatures. If, however, there is a need for a different signature location inside the XML document, use the *Sign XML document with attachments* option. This option is dedicated to advanced users and requires the knowledge of the construction of XML files, in particular knowledge of *XML Pointer Language (XPointer)* documentation.

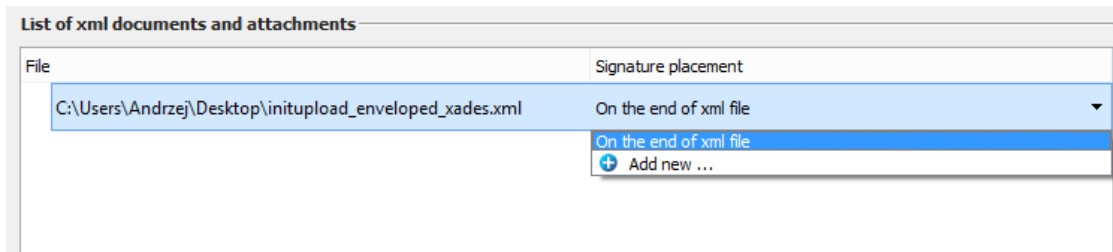
In order to make such a signature, in the main program window (see chapter 5.1), select menu **Advanced functions** (left side bar of the main program window) and press the icon **Sign an XML document with attachments**.

The special signature window is displayed:

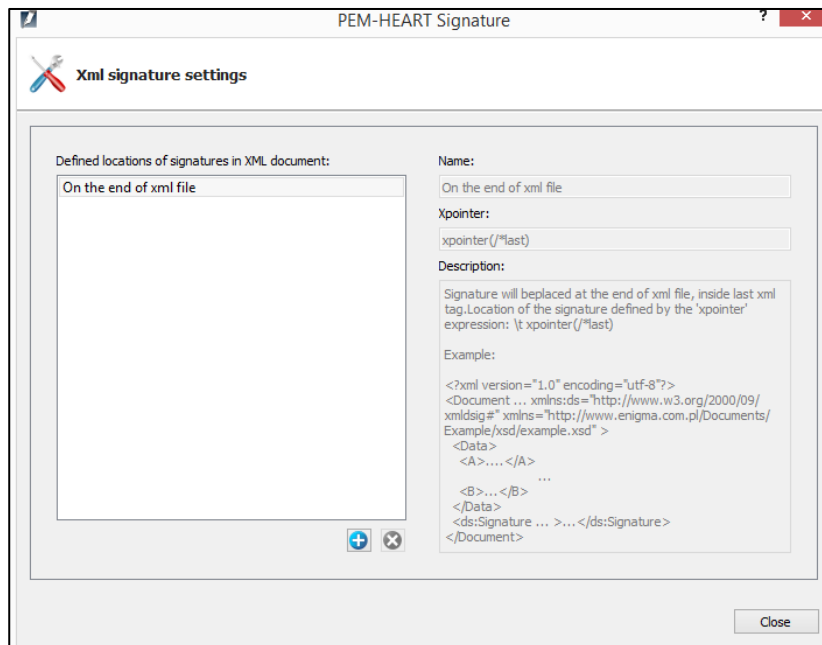



Choose file, files or directories (icons *Add file*, *Add directory* on the top menu) - as in the case of signing or signature verification mode (see chapter 5.2 or 5.2.2).

If the signature is to be located in a different place than at the end of the file, click with the mouse on the *On the end of the xml file* label.



Choose *Add New ...* menu, then program displays the configuration of the signature position:



Click with mouse on the  icon, then type the name of your configuration, the structure *xpointer* and optionally a description of the configuration. Structure *xpointer* is defined as: *xpointer([indication of the node XML])*. Available forms of this structure are described in the *XML Pointer Language (XPath)* documentation available, among others, at <http://www.w3.org/TR/WD-xptr>.

Signing in XAdES enveloped format does not change the extension of the XML file or its structure.

## 6 Smart card support

The program enables simplified handling of smart cards issued by CenCert.

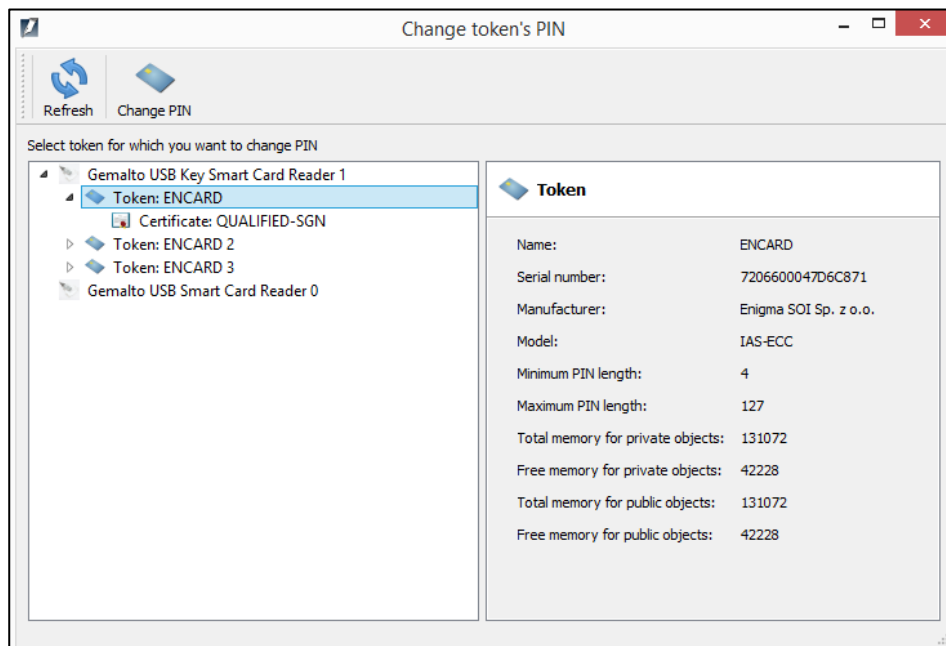
All operations described below are invoked from the main program window (see chapter 5.1) when you click on the **Card** label in the left menu (left-bottom on the main window).



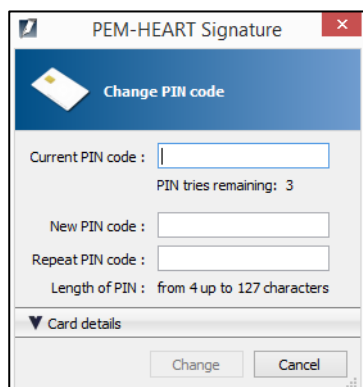
### 6.1 Changing the PIN

In order to change the PIN, select menu **Card** (the left side bar of the main window) and press the icon **Change PIN**.

Then indicate the card token for which you want to change a PIN (Note: a qualified signature objects are always placed in the first card token; other tokens can be used for other purposes, e.g. for electronic stamps or non-qualified signatures):



Then click the **Change PIN** icon (in the top bar) .



Enter the correct valid PIN code and enter (and repeat) the new code.

We do not recommend using national letters nor other characters for the PIN code, which may not be entered correctly with different language settings of the computer keyboard. The smart card locks after 3 wrong attempts to enter the code. We recommend saving the PIN in a secure place (separate from the card).

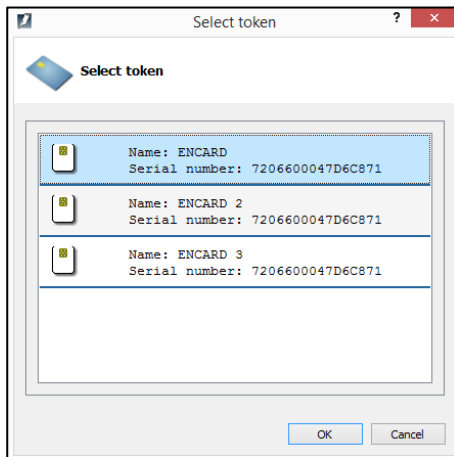
**Note! If the PIN code is blocked, the card can be unblocked only with the PUK code.**

You have entered first PIN / PUK codes when activating the card. **We don't have your PIN / PUK and we cannot help in case of blocking the card because of an incorrect PIN / PUK.**

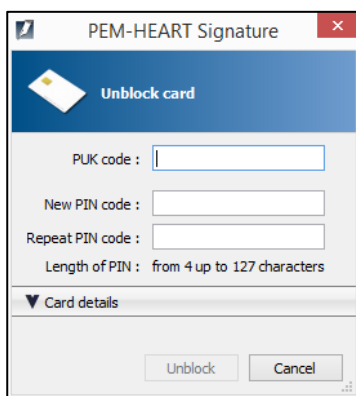
## 6.2 Unlocking the card

If your smart card has been blocked because of too many incorrect PINs, you can unlock it with the PUK. You have created the PUK code when your card was activated.

To unblock the card click the *Unlock card* icon:



Then select the appropriate token (for qualified signature: the first one)



If you entered your PUK correctly, you can set (and repeat) the new PIN code and the card will be unblocked.

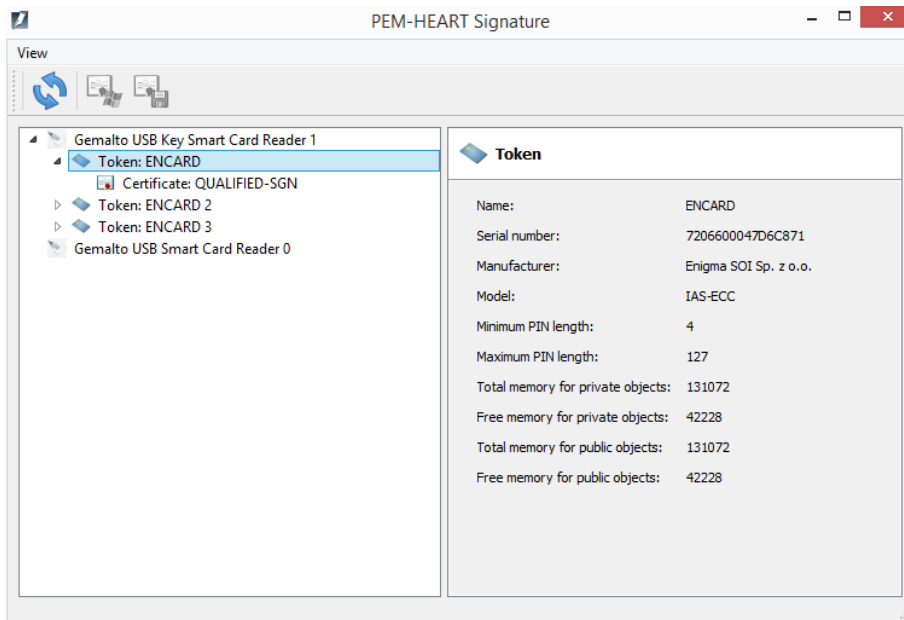
**Note! There are 10 attempts to unblock the card with the PUK.** If the PUK was entered incorrectly more times, the card is permanently blocked and it cannot be used again.

You have created your PIN / PUK when activating the card. **We don't have your PIN / PUK and we can't help if your card has been blocked due to an incorrect PIN / PUK code.**

## 6.3 Diagnostics

When you have many card readers and/or cards, the *Diagnostics* menu may be helpful.

After selection of the *Diagnostics* icon, the list of connected readers and information about present cards is displayed.



You can get information about the objects on the cards: tokens, keys, and certificates. After selecting the certificate, its structure and data are displayed. You can also (buttons at the top of the window) install the certificate in the Ms Windows system's store and / or save the certificate to a file.



# 7 Signing with rSign (cloud signing)

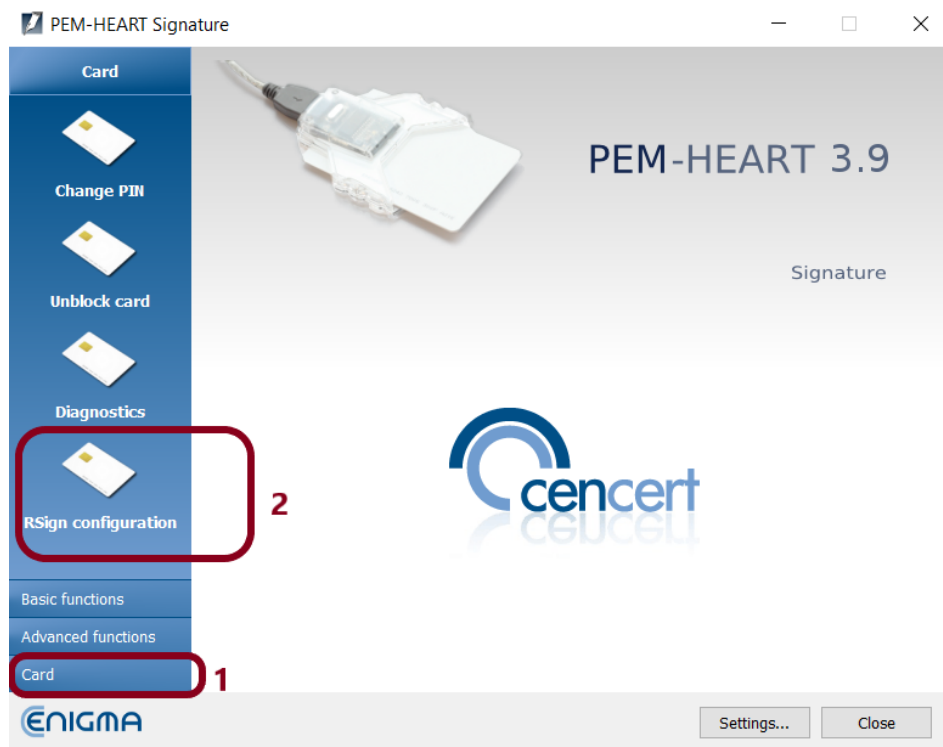
## 7.1 The configuration on your desktop

Before you can use rSign signatures on a given computer (on a given Windows account), you need to configure a signature on each such computer (account).

The purposes of this operation are twofold - first, when starting to sign, the program must know who is going to sign (which certificate should be used). Secondly, an important goal is to increase the security of your signature - the rSign signature can only be made on computers previously trusted by you.

In order to configure the rSign signature, run the PEM-HEART Signature program (starting the program is described in chapter 5.1).

Then select *Card* -> *rSign Configuration*



If needed, you may change the language (into *English*) in the next window.

Then, choose the *Activation*.

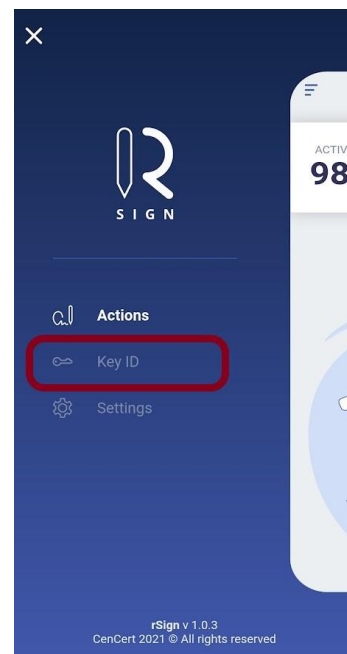
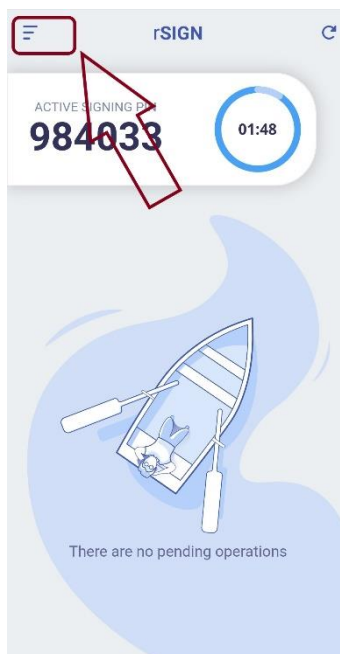


In the window below, enter the computer name (it will be displayed on your phone during signature operations):

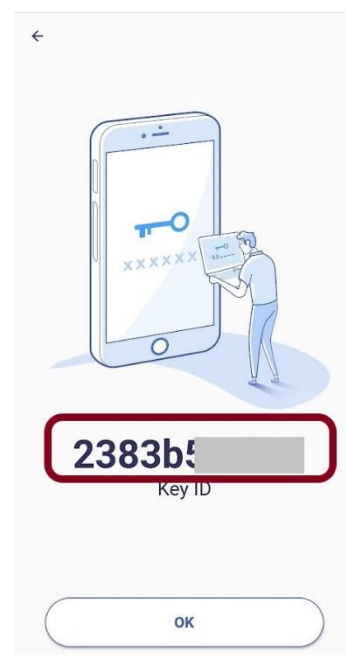
Then rewrite the rSign key ID from the application on the mobile phone.

To do this, run the rSign application on the mobile, then:

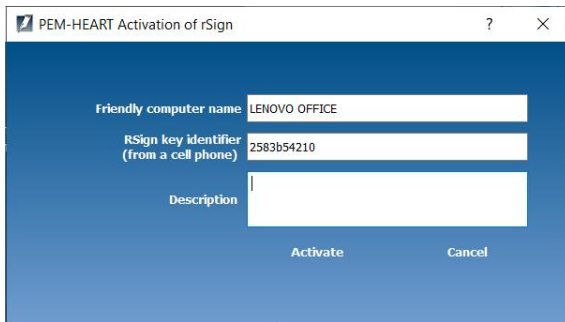
- select the menu (dashes in the upper left corner)
- select the Key ID command.



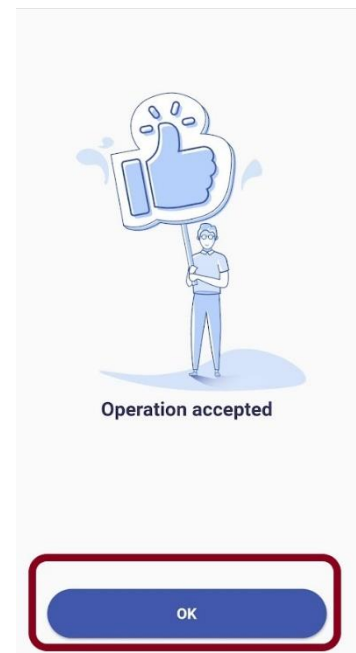
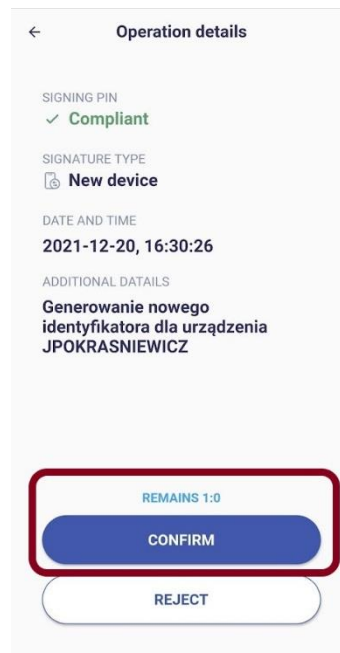
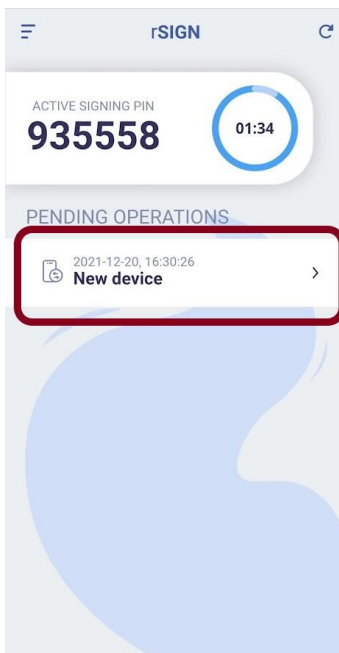
Then enter the PIN for the application on the mobile, rewrite the Key ID for the window in the application on the desktop.



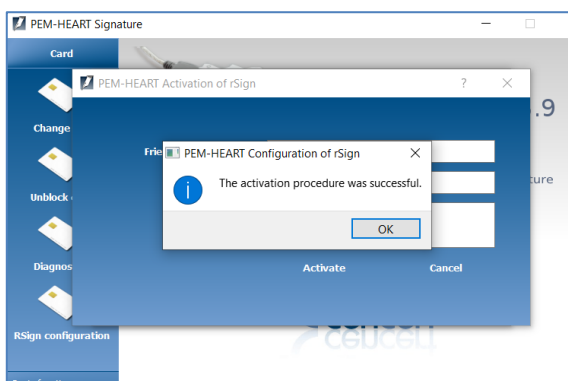
Then click **Activate**.



The program then displays information that it is still necessary to approve the device (desktop) as trusted on your mobile. To do this, open the rSign app on your mobile (see images below).



The program on the desktop displays a message about the completion of rSign signature configuration on the given computer (system account).



#### Comments:

1) You can have multiple rSign certificates configured on one system account on your desktop. In order to add another certificate to the configuration, repeat the operations described in this chapter, entering the next Key ID (read from the rSign application configured on another mobile phone).

2) From the point of view of signature creation programs, if you configure several certificates, the program will recognize this situation as if you had several signature creation cards inserted into the readers at the same time. How you respond to this depends on the program. In such a situation, PEM-HEART Signature will display the window where you can choose the certificate to be used. A signature approval request will be sent to the mobile phone associated with the selected certificate.

3) To remove a certificate from the configuration on the computer - see chapter 7.3. The certificate removed from the configuration may be added again at any time.

## 7.2 Installing the certificate that was renewed online on another computer

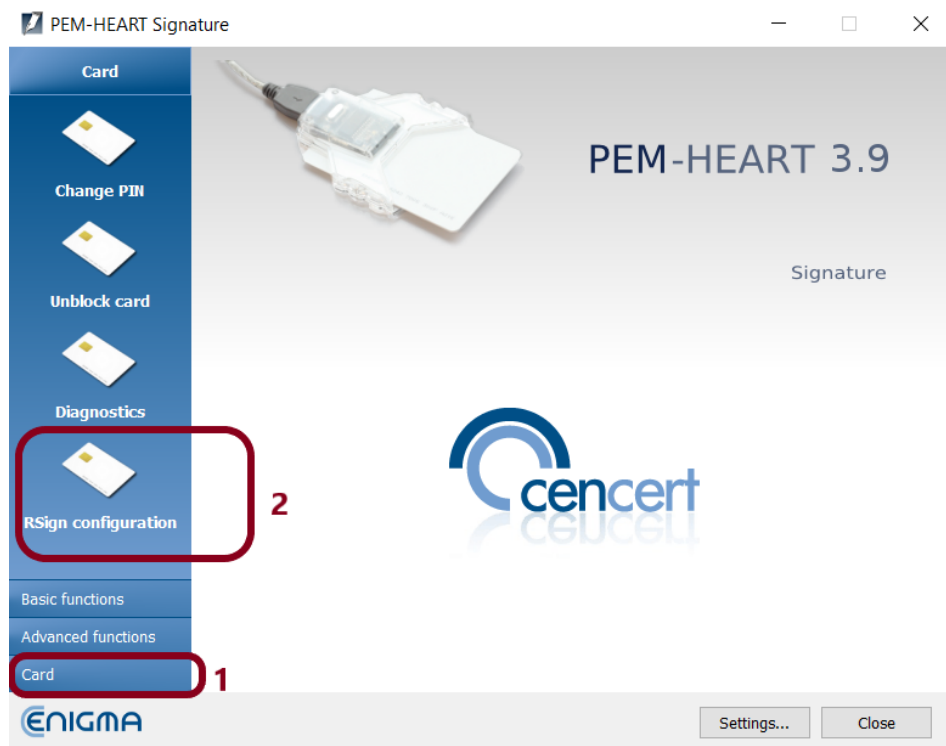
Online certificate renewal means the operation of obtaining a new certificate, with a new validity period, using the previous (expiring) certificate. Online renewal is performed using the *PEM-HEART Recertification* software. When renewing the certificate, it is not necessary to load the QR code into the rSign application on the phone, as it is done when purchasing the first certificate.

*Caution! If you had to (re)initiate the application on the mobile using a QR code when purchasing a new certificate, then this wasn't really an "online renewal operation" and the content of this chapter does not apply. In this case, you should configure the rSign on the desktop according to chapter 7.1.*

If you renewed your rSign signature certificate online (in the cloud), your new certificate was automatically saved on the desktop on which the renewal operation was performed. However, if you use your rSign signature on many computers - on the others, you need to update the configuration so that your signer application "knows" about your new certificate.

In order to install the renewed online certificate on another computer, start the *PEM-HEART Signature* program (starting the program is described in chapter 5.1).

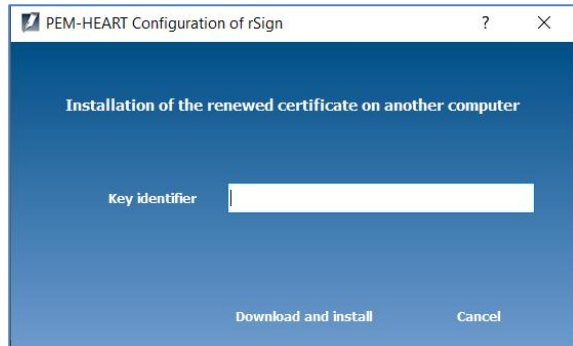
Then select *Card* -> *rSign Configuration*.



Then select *Install a renewed certificate on another computer*.

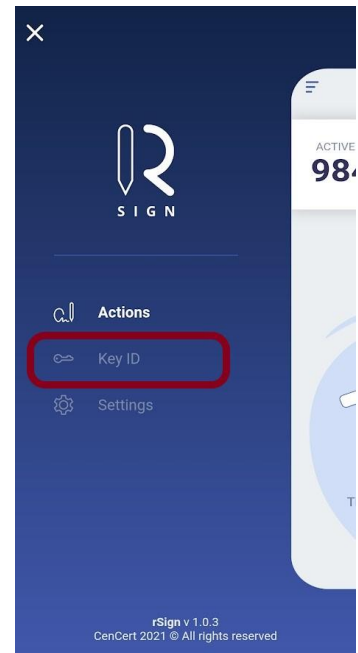
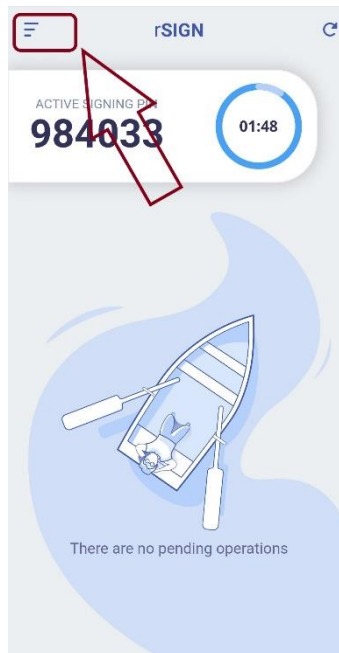


Then enter the ID of your signing key:

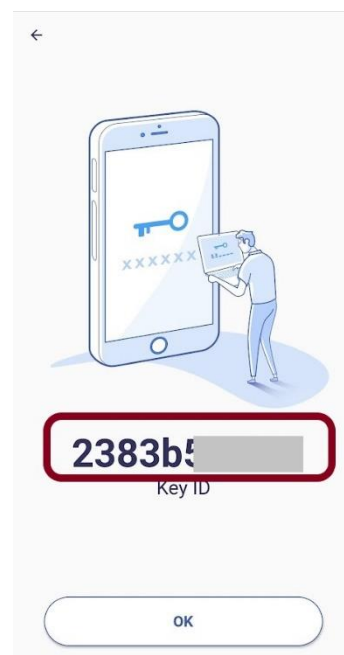


To do this, run the rSign application on the mobile, then:

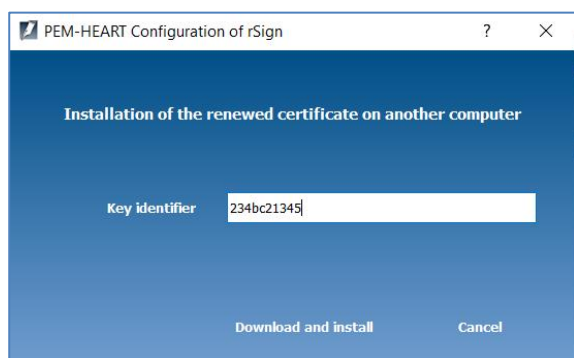
- select the menu (dashes in the upper left corner)
- select the Key ID command.



Then enter the PIN for the application on the mobile, rewrite the Key ID for the window in the application on the desktop.



Then click *Download and install*.

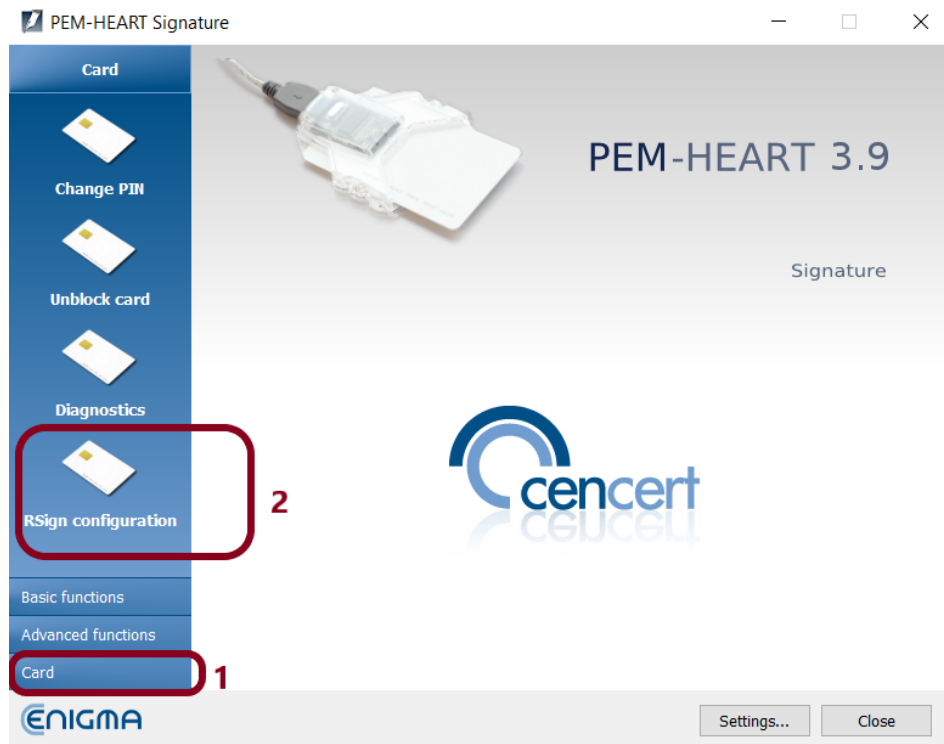


The program downloads your new certificate from the server and installs it on your desktop computer.

## 7.3 Removing the certificate configuration (or one of the rSign certificates) from the computer

In order to configure the rSign signature, run the *PEM-HEART Signature* program (starting the program is described in chapter 5.1).

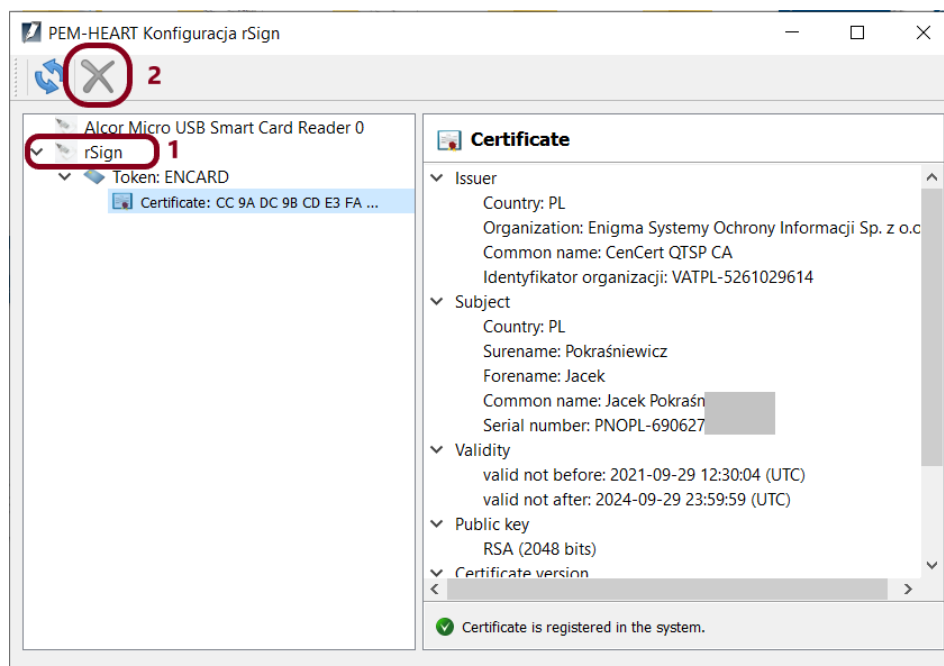
Then select *Card -> rSign Configuration*.



Then select *Delete token*.



The program will display a list of available "tokens" (including tokens on some physical cards, if available). Select the rSign token to be removed.



The program removes the selected rSign token.

The removed token may be added again at any time – see chapter 7.1.

## 7.4 rSign application on your mobile phone

### 7.4.1 Main windows

The main screen of the application looks like this:

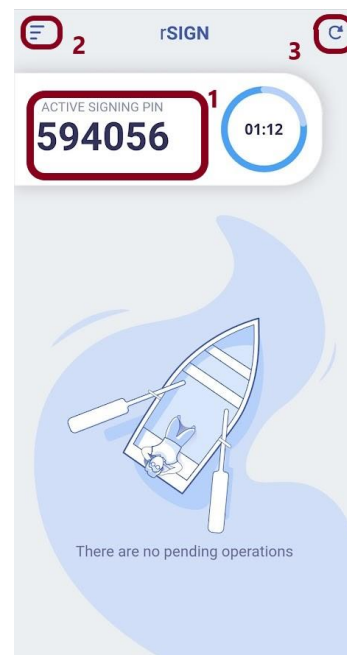
Description of the screen areas:

1 – Active signing PIN.

This PIN must be entered into the application that generates the signature (on the desktop computer) - as "signature PIN" or "card PIN". The PIN code is time-varying.

2 - Application menu.

3 - Refreshing information on operations to be approved (if the information did not download itself).



### 7.4.2 Reading the key ID

The key identifier is information that should be protected (confidential). It should be used only for the configuration of trusted computers on which you can sign your signature (including it may be transferred to other, trusted entities managing systems in which you will sign server signatures).

Each signature operation requires approval using the application on your phone - having a key identifier (without your mobile) does not allow anybody to sign on your behalf.

To read the key identifier, select the application menu (see chapter 7.4.1).

Then select Key ID, enter the PIN for the application - and read the Key ID.

### 7.4.3 Backup of mobile application data

The backup of mobile application data is necessary to transfer the signature activation data to another phone. If you want to change your phone or if you lose your current phone (or the phone breaks) or the data on the phone is deleted - you will be able to restore the signature activation data (you will not have to incur the cost of acquiring a new certificate), provided that you have a current data backup of the rSign mobile application.

The application suggests making a backup immediately upon activation. However, you can also perform the backup operation later.



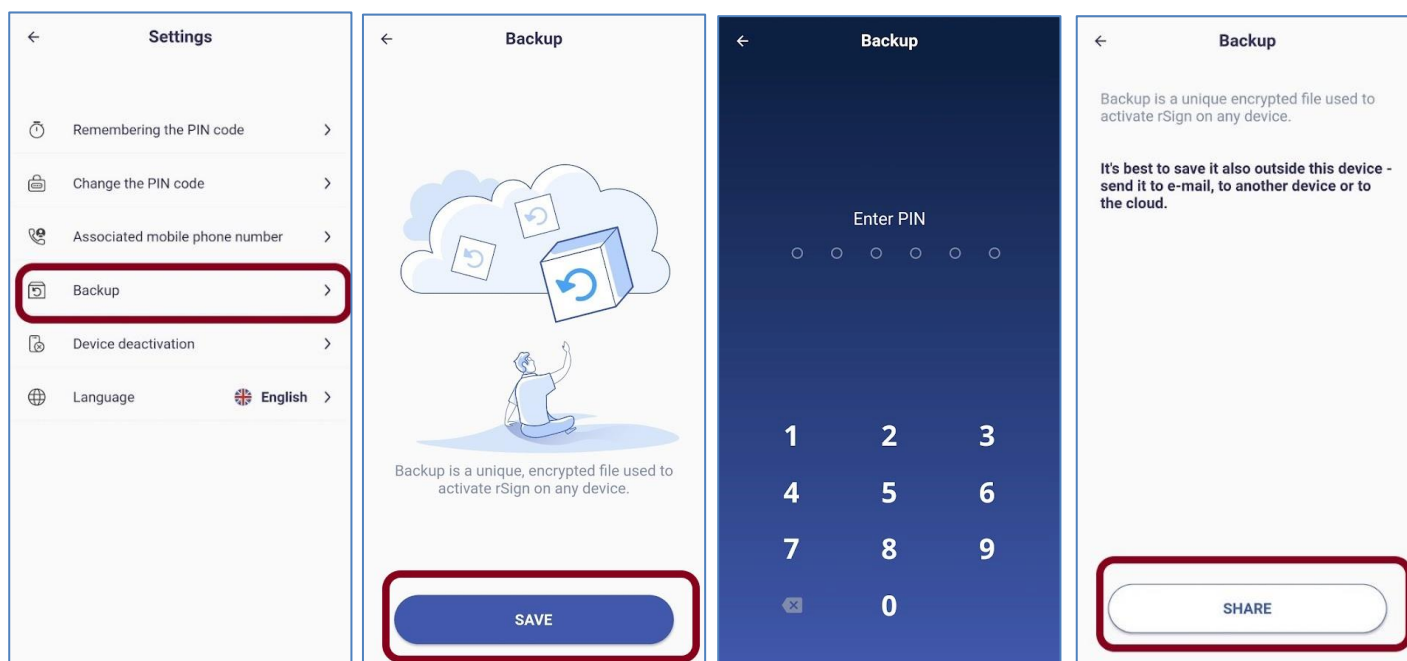
We strongly recommend that you store the backup file outside of your phone (e.g. on Google Drive or iCloud). The backup file is encrypted and contains only part of the data needed to activate your signature, so it can be stored in a limited trust environment.

A backup performed once is up-to-date (and does not have to be repeated), unless you change the PIN to the mobile application.

To delete the signature activation data from the phone, select the application menu (see chapter 7.4.1).

Then select *Options* and then select *Backup*.

The application will ask for a PIN to the application and then to indicate where to save the backup file.



## 7.4.4 Changing the application PIN

In order to change the PIN to the mobile application, select the application menu (see chapter 7.4.1).

Then select *Change PIN*, enter the old (current) PIN for the application, then enter the new PIN twice.

Comments:

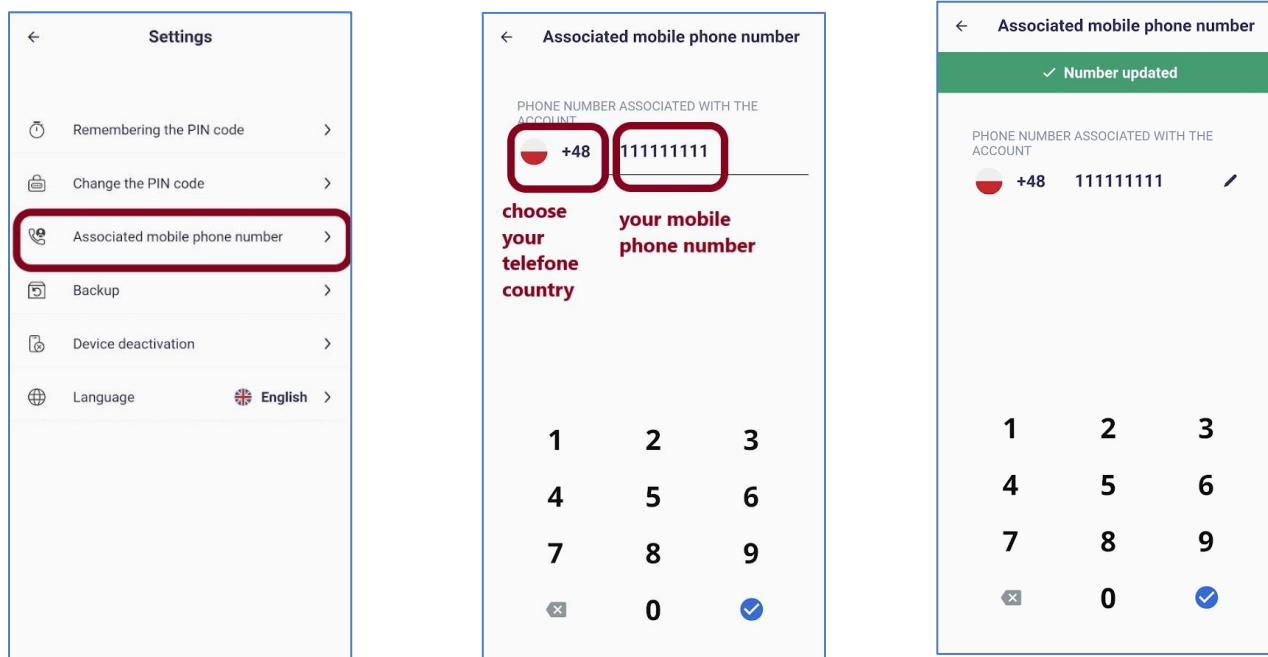
- 1) PIN for the mobile application is a critical data. If you forget your PIN, you will lose access to your signing key forever - the only way to restore signing is to purchase a new certificate. If you are not sure whether you will remember the PIN, we recommend that you write it down in a safe place.
- 2) After changing the PIN, you need to backup the data of the mobile application again (see chapter 7.4.3). The old backup is encrypted with the old PIN and cannot be used anymore.

## 7.4.5 Authorized mobile telephone number

It is important that your current mobile number is in the CenCert database. If you want to transfer your signature activation data to another phone, the CenCert system will send an SMS **TO THIS NUMBER** with the code authorizing the transaction of transferring the activation data.

To update your phone number, select the application menu (see chapter 7.4.1).

Then select *Associated mobile phone number*. If needed, change your telephone country and write down your current mobile phone number (to delete number use backspace button), then press the accept button. Give your application PIN code and the number is updated on CenCert servers and you are informed of it by the application (see pictures below).



## 7.4.6 Signature PIN timeout (remembering the signature PIN)

Each rSign signature must be authorized by you via the rSign mobile application. You may activate one signature at a time, but you can also enable multiple signatures without the need to approve each operation in the mobile application.

If, when confirming the operation, you set the signature time to e.g. 1 minute, it means that subsequent signature operations coming from the same computer will be performed without sending further queries to your mobile application, as long as the time between each signature is not longer than the set 1 minute (signature 'inactivity' time). In any case - regardless of this setting - after 60 minutes from the first signature, the signature status will be reset (the next operation will need approval again).

Setting the signature inactivity time is useful wherever you want to sign many signatures at once (e.g. when you have placed many files for signature in the signing window of the *PEM-HEART Signature* or if you use an application that doesn't ask for PIN for subsequent documents signed, as for example Acrobat DC or Acrobat Reader DC). This option is also useful when placing signatures with time stamping - because then two signatures are made each time (one under the document, the other on request for time stamping).

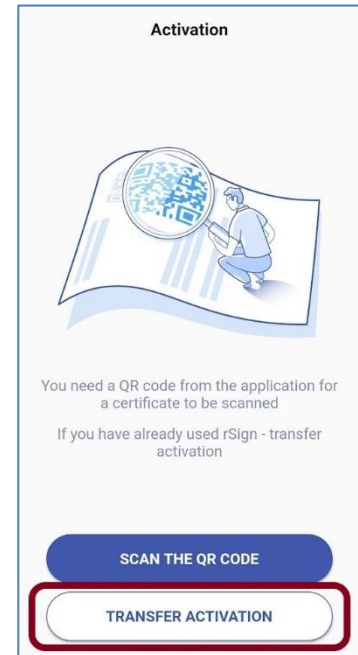
Setting the signature inactivity time (setting multiple signatures) is useful and may be recommended if you are always signing from computers that are under your sole control and that you trust. If you are signing from a computer where you have limited control, it is safer to set the option to validate one signature only.

If you want to change the signature approval option (and possibly set the signature inactivity timeout period) - select *Settings* in the application menu, and then *Remembering the PIN code*. Then set your preferred value of the signing PIN.

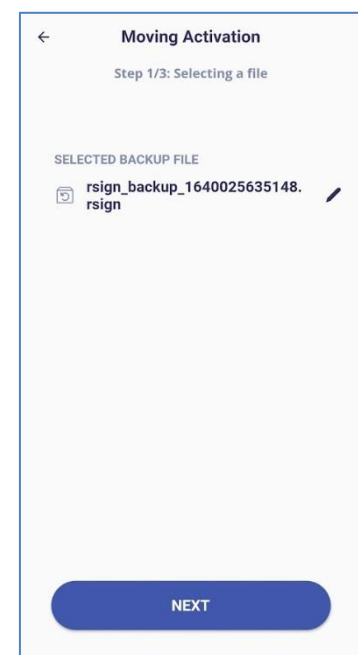
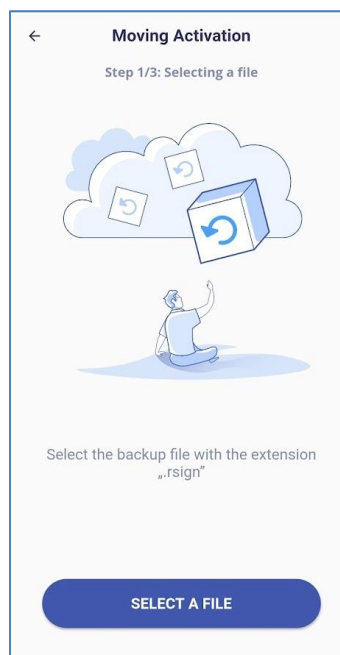
## 7.4.7 Transferring activation data from another phone

If you want to transfer data from another phone, install the "rSign by CenCert" application from the Google Play or AppStore on the new phone.

Then, in the main application window, select the command *TRANSFER ACTIVATION*.

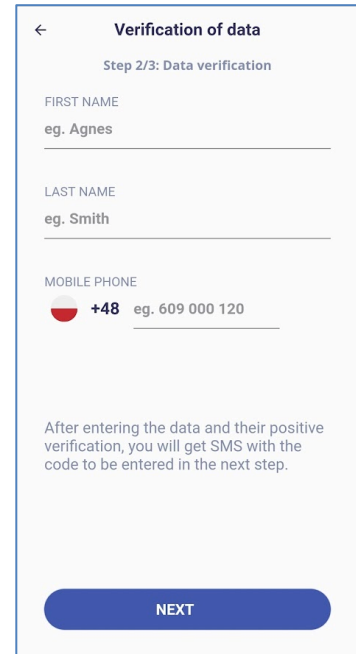


Then press the *SELECT A FILE* button and select the backup file (the default file name is *rsign\_backup\_XXXXXXXXX.rsign*) and press the *Next* file button.



Then enter your name and surname and mobile phone number (which was set in the CenCert system). If needed, change your phone country (press the flag button).

Press the *NEXT* button.



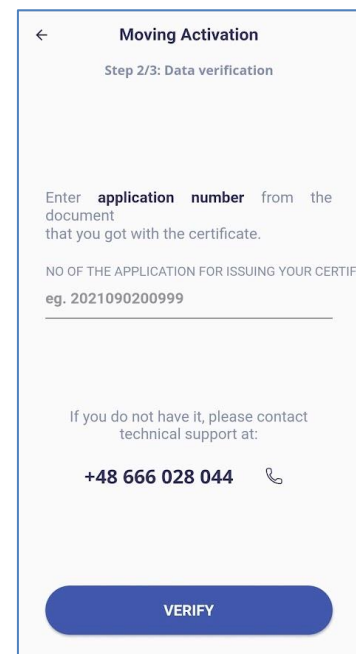
The screenshot shows a mobile application screen titled "Verification of data" with a back arrow on the top left. Below the title is the subtitle "Step 2/3: Data verification". There are three input fields: "FIRST NAME" with the example "eg. Agnes", "LAST NAME" with the example "eg. Smith", and "MOBILE PHONE" with a flag icon, "+48", and the example "eg. 609 000 120". Below these fields is a paragraph: "After entering the data and their positive verification, you will get SMS with the code to be entered in the next step." At the bottom is a blue button labeled "NEXT".

In rare cases, if you have associated your phone with several still valid rSign certificates (and the system doesn't know which certificate activation is to be used), the application asks you for the certification request number that you have signed (manually or electronically) when issuing your certificate.

The application number is, for example, a number such as "2021022600768".

If you do not know this number, you may call CenCert Technical Support during its business hours. CenCert staff will be able to find the number based on your personal information and the approximate date of acquiring the certificate. You can also write an e-mail to the following address: [biuro@cencert.pl](mailto:biuro@cencert.pl).

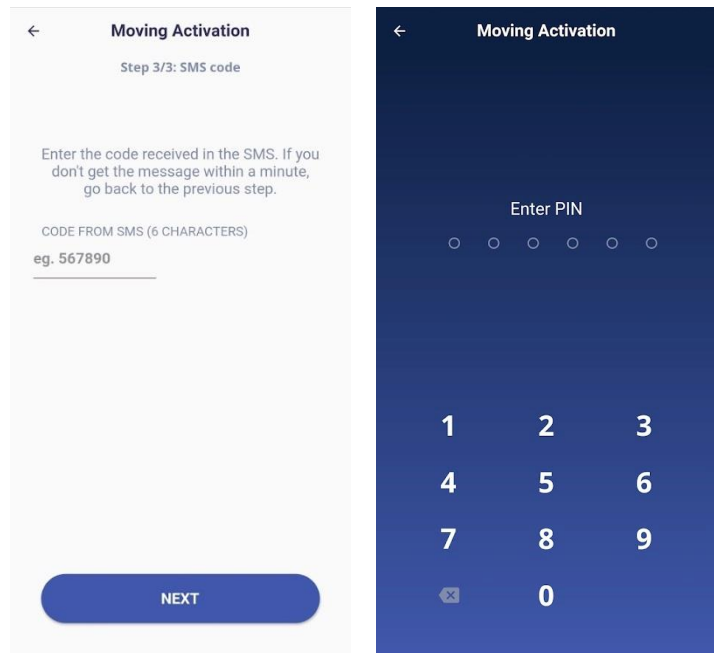
Then press the *VERIFY* button.



The screenshot shows a mobile application screen titled "Moving Activation" with a back arrow on the top left. Below the title is the subtitle "Step 2/3: Data verification". There is a text prompt: "Enter **application number** from the document that you got with the certificate." Below this is an input field with the label "NO OF THE APPLICATION FOR ISSUING YOUR CERTIFICATE" and the example "eg. 2021090200999". Below the input field is a paragraph: "If you do not have it, please contact technical support at:" followed by the phone number "+48 666 028 044" and a phone icon. At the bottom is a blue button labeled "VERIFY".

Enter the verification code you received via SMS and the PIN for the mobile application (old PIN - the one you set up when you backed up the data of the mobile application)

Press Confirm.



Now is a good time to make a new backup – the application propose making the backup. The previous backup file (from which you've just read the data) is now useless. It cannot be reused.

After making the backup - you have really finished activating the signature on the new phone. You can remove (deactivate) the signature data on your old phone if you still have access to it.

## 7.4.8 Deactivating the signature data on the phone

To delete the signature activation data from the phone, select the application menu (see chapter 7.4.1), the *Settings* and *Device deactivation*.

The signature activation data can be restored on this (or another) phone, provided that:

- 1) you have an up-to-date backup of mobile data,
- 2) you know the PIN for the mobile application (which was valid at the time of the backup),
- 3) you can receive SMSs from the phone number defined in CenCert.

# 8 Program options, working without Internet

All operations described below relate to operations invoked from the main program window displayed after its launch (how to launch the program - see Chapter 5.1).



## 8.1 Options of signatures

To change the options of signing operations, click the *Settings* button in the main program window. Then choose the *Signing* tab.

The screenshot shows the 'PEM-HEART Signature' application window with the 'Settings' button highlighted. The 'Signing' tab is selected in the settings pane. The 'Format and type of signature' section is active, showing a list of file extensions (\*.\*) and a list of signature format options. The 'XAdES (standard ETSI TS 101 903)' option is selected. Below this, there are checkboxes for 'XAdES enveloping', 'XAdES in detached file' (checked), and 'XAdES enveloped (only for XML files)'. Other options include 'CAdES, CMS (standard ETSI TS 101 733)', 'CAdES, CMS in detached file', 'CAdES, S/MIME (standard ETSI TS 101 733)', 'PAdES (only for PDF files) (standard ETSI TS 102 778)', 'PAdES with a graphic effect (only for PDF files) (standard ETSI TS 102 778)', and 'ASiC (standard ETSI TS 102 918)'. At the bottom, there are checkboxes for 'Add timestamp', 'Add OCSP response', 'Encode to base64 xml documents while signing with XAdES enveloping', 'Use attribute "Signing Certificate" version 2', and 'Add type of commitment' (set to 'proof of origin'). The 'Cryptographic algorithms' section shows 'SHA-256' as the selected digest algorithm. 'Save' and 'Cancel' buttons are at the bottom right.

All options specifying the signature format (XAdES, CAdES, ASiC) will be applied to files with the name extension as currently selected in the **Extension** list. The "\*" is a special symbol that means "all the files except specified below".

For example - in the picture above - the name extension "\*" is selected. That means that all files except PDF and XML files, will be signed using the format: *XAdES in detached file* (as selected in the window on the picture above). At the same time PDF and XML files may have their own signature formats selected. It will be visible when you select the \*.PDF or \*.XML line respectively.

In this window you can also add other file extensions (using the icons  and ) for which you want to use a different default signature format. E.g. if you add a new position "\*.docx" and you choose the format of a signature e.g. *CAdES CMS in a separate file*, then when creating the signature of the Ms Word file (docx), the program will make a signature in *CAdES, CMS format in a separate file*.

In the next part of the window (below, starting from the option *Add timestamp* ), you can specify additional options for signatures. These settings apply to all signatures - regardless of the file name.

The *Add time stamp* option means that a time stamp will be added to each signature (*Note! You may need to buy a time stamp service package for correct operation*).

The *Add OCSP response* option means that in addition to the time stamp (which must also be selected then), information about the status of the certificate used for the signature will be added (this creates a signature in the *long* form - see also Notes in Chapter 4).

The option *Encode to base64 documents while signing with XAdES enveloping* is needed in specific situations when the system verifying signed documents has limited verification capabilities and requires the base64 encoding.

The option *"Use Signing Certificate attribute in version 2"* puts the signature with the certificate identification in a format compatible with newer versions of ETSI standards. Select the option if it is required by the signature verification system that uses only new formats.

Selecting the *Add type of commitment* option adds a signed attribute that indicates for what purpose (in what role) the signer has signed (e.g. "formal approval" or "acknowledgment of receipt", etc.).

Option *Digest algorithm* specifies cryptographic hash algorithm used to create the signature. The program allows only good algorithms that guarantee (when the version of the program is current) adequate security.

## 8.2 Files

The tab *Files* gives options for setting destination folders for processed documents. By default, the program puts processes documents in the same folder in which the original document is located. However, it is possible to specify other directories to which processed (signed or verified) documents will be saved.

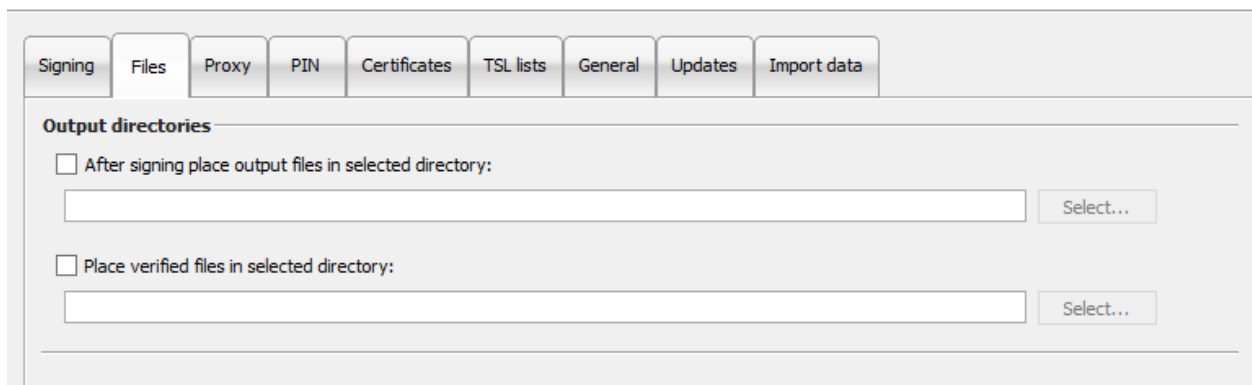


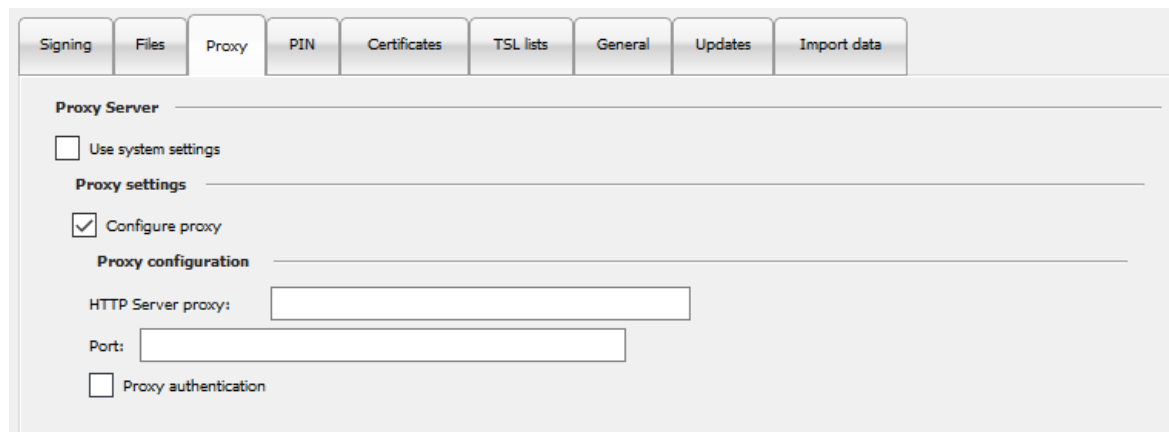
Figure 49 Output directory configuration

To define destination directory check the appropriate check-box, then click the *Select* button and choose the folder.

## 8.3 Proxy

The tab is used to specify the Internet proxy server (use it when your Internet connection needs it). You must complete all mandatory fields for the *proxy* .

The option is activated after selecting the *Configure proxy* check-box .



The screenshot shows the 'Proxy' tab selected in a software window. The tab bar at the top includes 'Signing', 'Files', 'Proxy', 'PIN', 'Certificates', 'TSL lists', 'General', 'Updates', and 'Import data'. The 'Proxy' tab content is titled 'Proxy Server' and contains the following options:

- ☐ Use system settings
- Proxy settings**
  - ☒ Configure proxy
- Proxy configuration**
  - HTTP Server proxy:
  - Port:
  - ☐ Proxy authentication

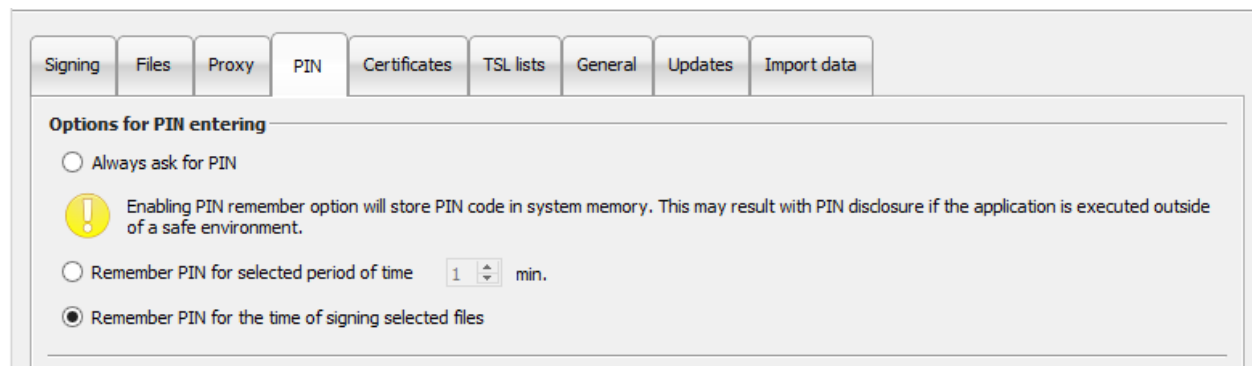
Note! Misconfiguration results in the lack of access to the Internet (the time stamp cannot be downloaded, it signature validation is very limited).

## 8.4 PIN


The PIN tab is used to set options referring to storing the card PIN .

By default, the PIN is stored in program memory during signing all the files selected in the signing window - in order to sign all the selected files you have to enter the PIN only once. If you re-select files for signature later (even without closing the program) you need to re-enter the PIN.

There are also other possibilities of this option: that the PIN will be given always to each individual signature or will be stored in the computer memory for a specified time range.



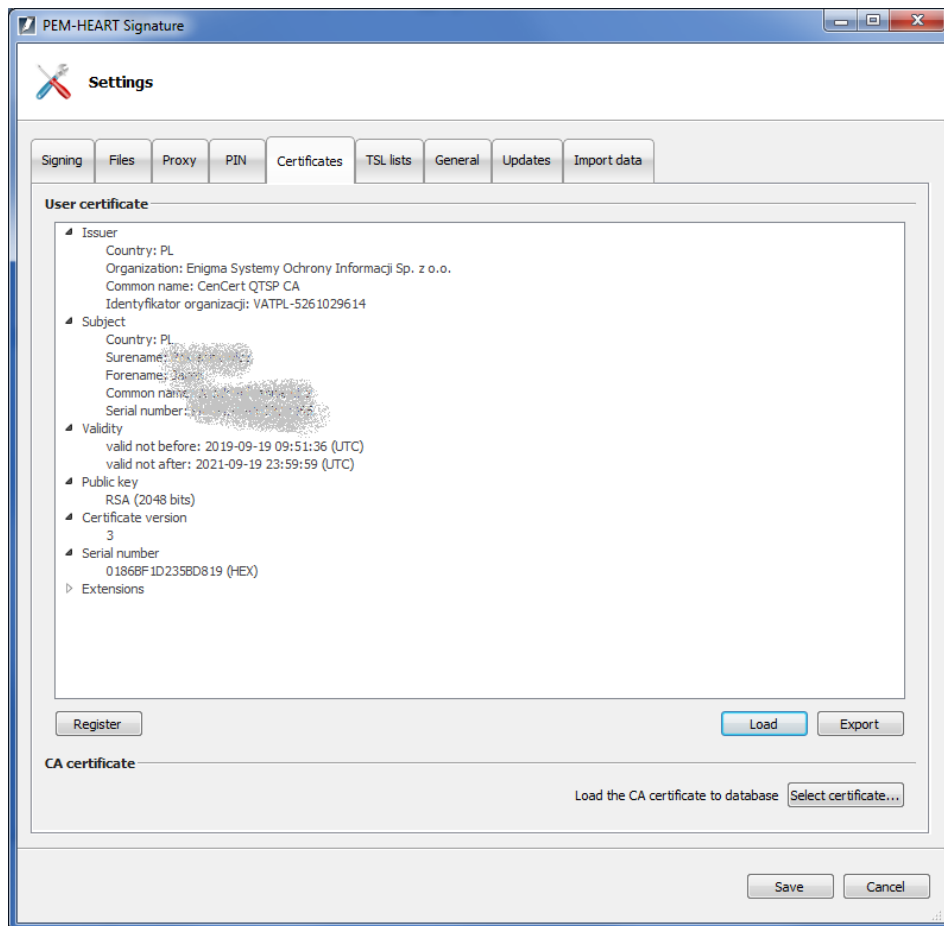
The screenshot shows the 'PIN' tab selected in the same software window. The tab bar at the top is the same as in the previous screenshot. The 'PIN' tab content is titled 'Options for PIN entering' and contains the following options:

- ☐ Always ask for PIN
-  Enabling PIN remember option will store PIN code in system memory. This may result with PIN disclosure if the application is executed outside of a safe environment.
- ☐ Remember PIN for selected period of time  min.
- ☒ Remember PIN for the time of signing selected files

## 8.5 Certificates

The tab *Certificates* refers to your certificate. If your card is present in the reader, the program automatically reads data from it and displays it in the window. If the certificate couldn't be read, check the card placement and then use the *Load* button to try again.





You may use the *Register* button to register your certificate to the *Ms Windows* system store.

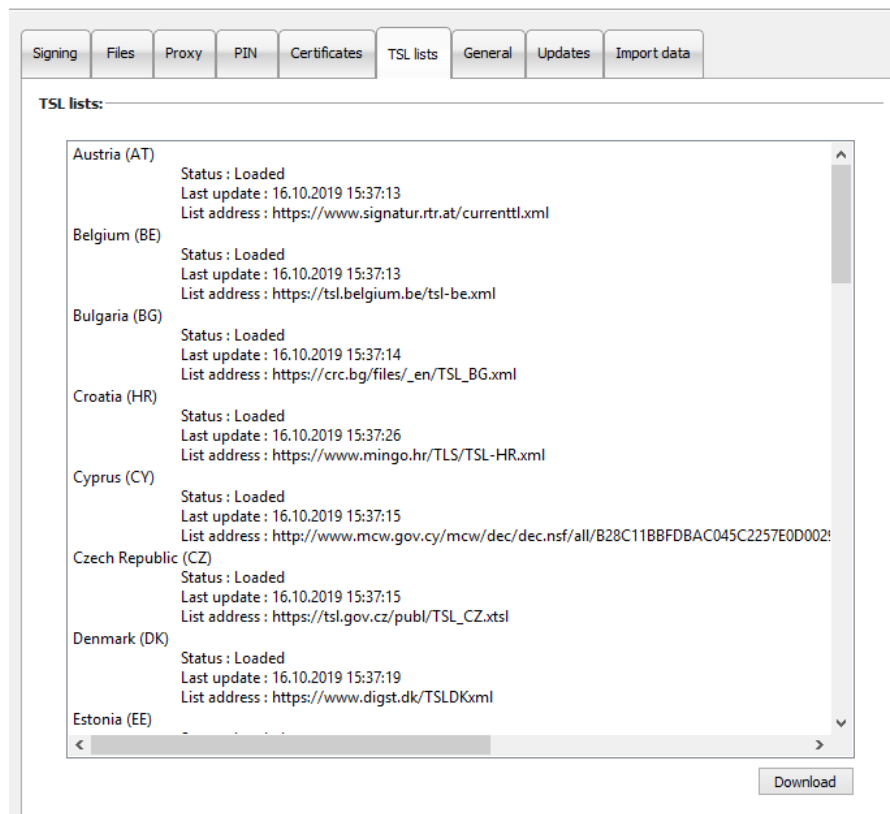
You may export the certificate to a file using the *Export* button .

All of the above operations can also be performed from the Card menu (see chapter 6 above ).

The *CA's* tab certificate section (lower part of the window) is used to indicate and load a certificate of the trust service provider into the program's database. The option is used in specific situations regarding commercial (non-qualified) signatures - when the program does not have a valid "intermediate authority" certificate of the trust service provider in the database.

## 8.6 TSL lists

TSLs contain all necessary data on qualified trust service providers in the EU (including Poland). It enables the program to verify signatures made using qualified certificates issued by Polish and other EU trust service providers.



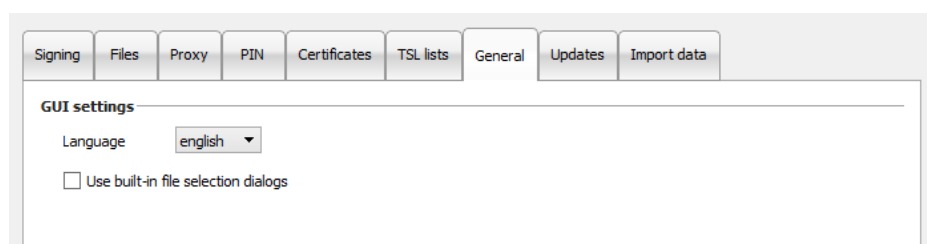
The tab presents the current status of TSL lists in the program's database.

The window also provides the ability to manually download current TSLs issued in EU countries (the manual download is not required for normal operation, as the program automatically downloads new TSL list when it is needed).

To download TSLs, press the *Download* button.

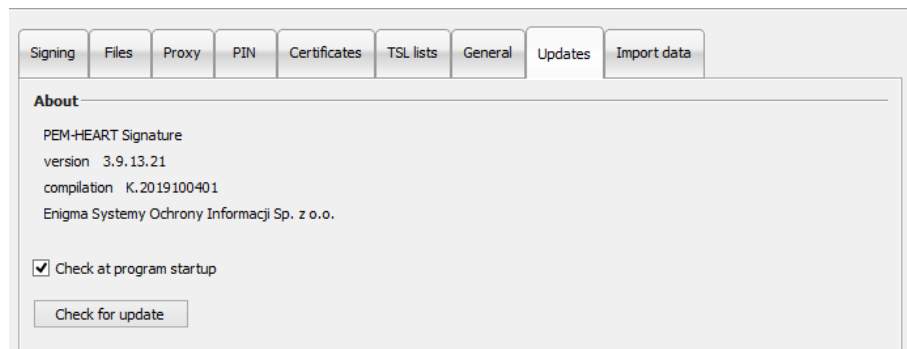
## 8.7 General

Changing the program language to English or Polish:



## 8.8 Updates

In the *Updates* tab you can find information about program version and you can check if there is a new version on the server.

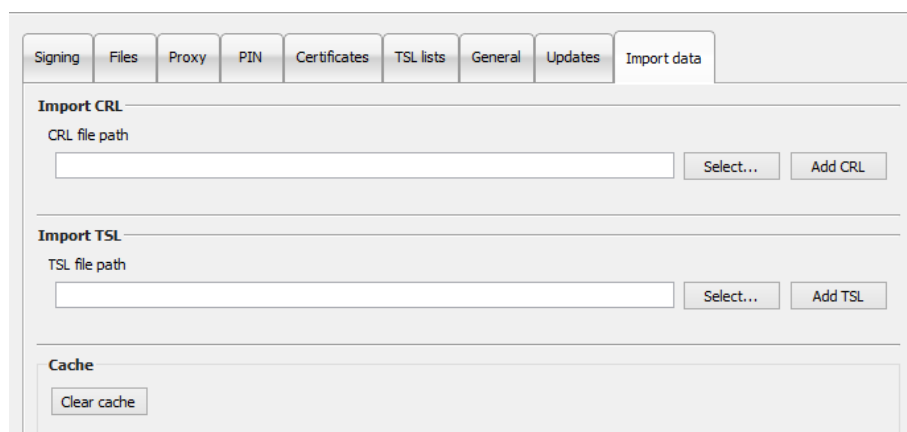


Information about the available update can be obtained by pressing the *Check for updates* button.

You may also set options for automatic checking during program startup. If a new version is detected, a message will be displayed .

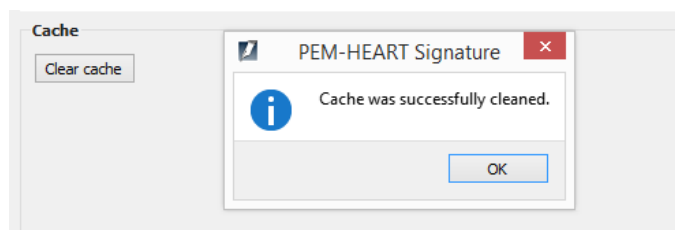
## 8.9 Import Data

The tab *Import data* is helpful when operating the program in an Internet-less environment. In such situation placing time stamps or checking the status of the certificate (based on OCSP) is not possible. Signing and verification of signatures are still possible, provided that the program has current TSL and CRL lists - which in such case must be transferred and loaded into the program manually.



To load a file with the CRL or TSL list, press the *Select* button next to *Import CRL* or *Import TSL* respectively, then point on the appropriate file on the disk. Then push *Add CRL* or *Add TSL* button respectively.

The "Clear cache" button deletes the *PEM-HEART Signature* database. This should be tried in specific cases, e.g. when there is a database error.



The database contains cached data (e.g. current CRL list). Deleting it does not cause negative consequences, because the program will simply download the missing data from the Internet.

## 9 Troubleshooting

Troubleshooting:

SIGNING			
lp	Problem	Cause	Solution
1.	No time stamp could be retrieved from any of the servers	No time stamp package is assigned to the certificate	- try again the next day (two time stamps per day can be downloaded for free), or - buy a time stamping package (details: <a href="http://www.cencert.pl">http://www.cencert.pl</a> ), or - disable the option of time stamping signatures (see chapter 3 above )
2.		The program has no access to the Internet	- check internet connection - check the proxy settings (if you use a proxy server) - see chapter 7.3 above )
3.	Signature failure: To make the next signature, select "Advanced features / add signature"	The file already contains a signature.	- add a signature using the "Add signature" command (see chapter 5.4 above )
VERIFICATION			
lp	Problem	Cause	Solution
1.	Indicate the location of the documents. Not all disconnected documents were found ....	The program can't find in the directory with the signature file, the file that was signed.	Indicate the file that has been signed (corresponding to the signature that is being verified) in the program window.