PEM-HEART Signature

User's Guide

ul. Jutrzenki 116, 02-230 Warsaw

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

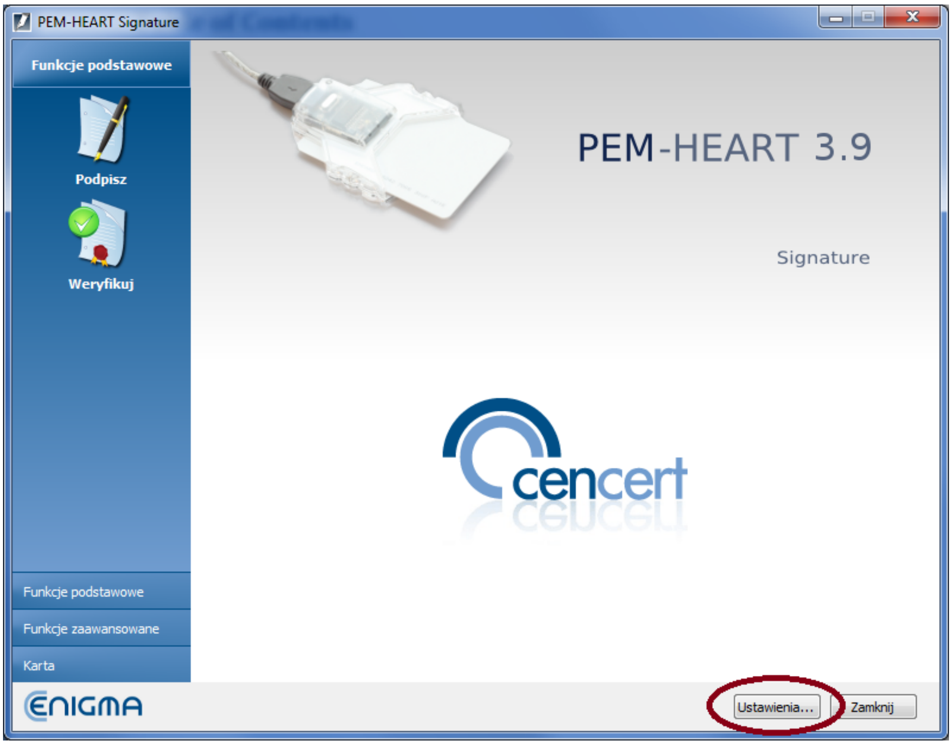
http://www.enigma.com.pl , biuro@enigma.com.pl

Table of Contents

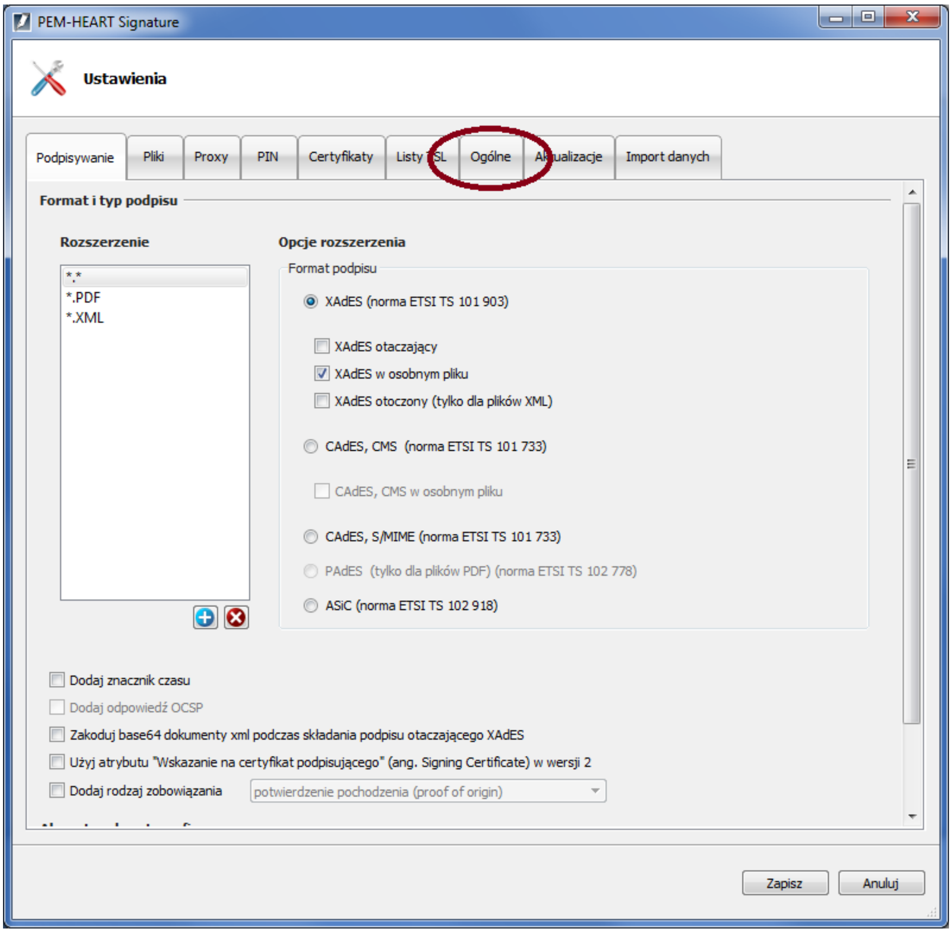
0 Setting the English language

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

Then click "Ustawienia" button.



Then choose "Ogólne" tab



Format i typ podpisu

Rozszerzenie

- *.*
- *.PDF
- *.XML

Opcje rozszerzenia

Format podpisu

● XAdES (norma ETSI TS 101 903)

□ XAdES otaczający
☑ XAdES w osobnym pliku
□ XAdES otoczony (tylko dla plików XML)

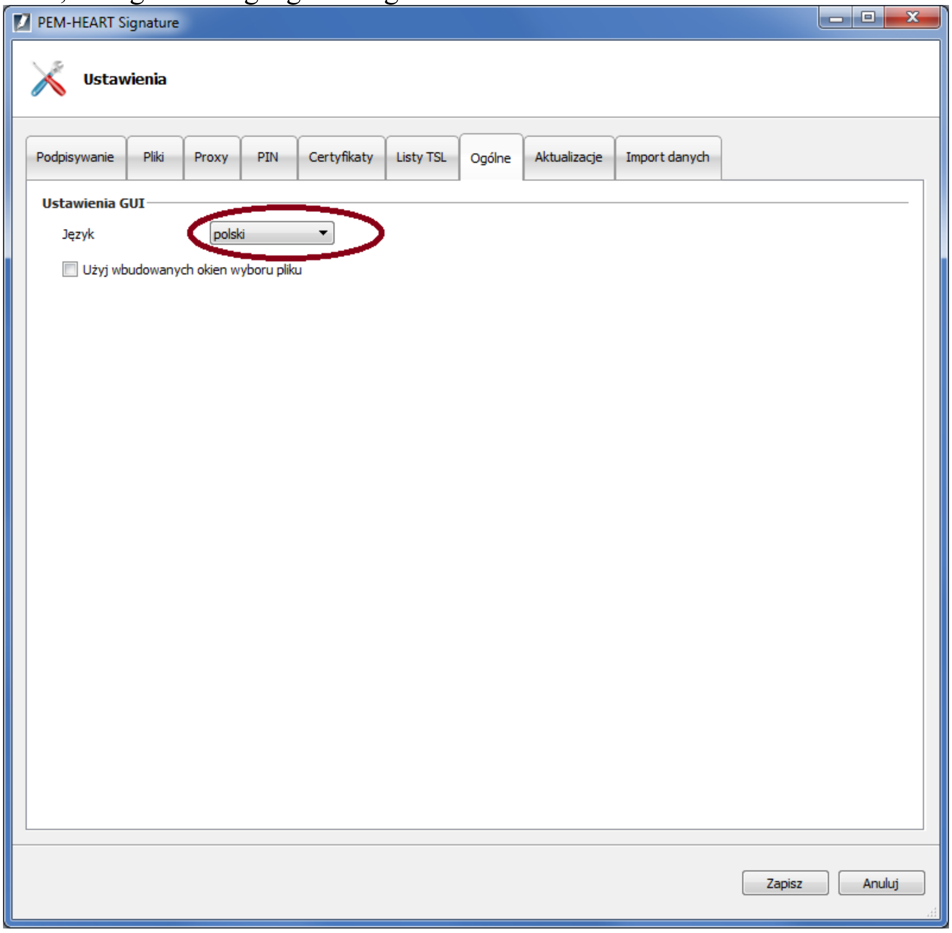
○ CAdES, CMS (norma ETSI TS 101 733)

□ CAdES, CMS w osobnym pliku

○ CAdES, S/MIME (norma ETSI TS 101 733)
○ PAdES (tylko dla plików PDF) (norma ETSI TS 102 778)
○ ASiC (norma ETSI TS 102 918)

□ Dodaj znacznik czasu
□ Dodaj odpowiedź OCSP
□ Zakoduj base64 dokumenty xml podczas składania podpisu otaczającego XAdES
□ Użyj atrybutu "Wskazanie na certyfikat podpisującego" (ang. Signing Certificate) w wersji 2
□ Dodaj rodzaj zobowiązania: potwierdzenie pochodzenia (proof of origin)

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



Ustawienia GUI

Język: polski

□ Użyj wbudowanych okien wyboru pliku

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

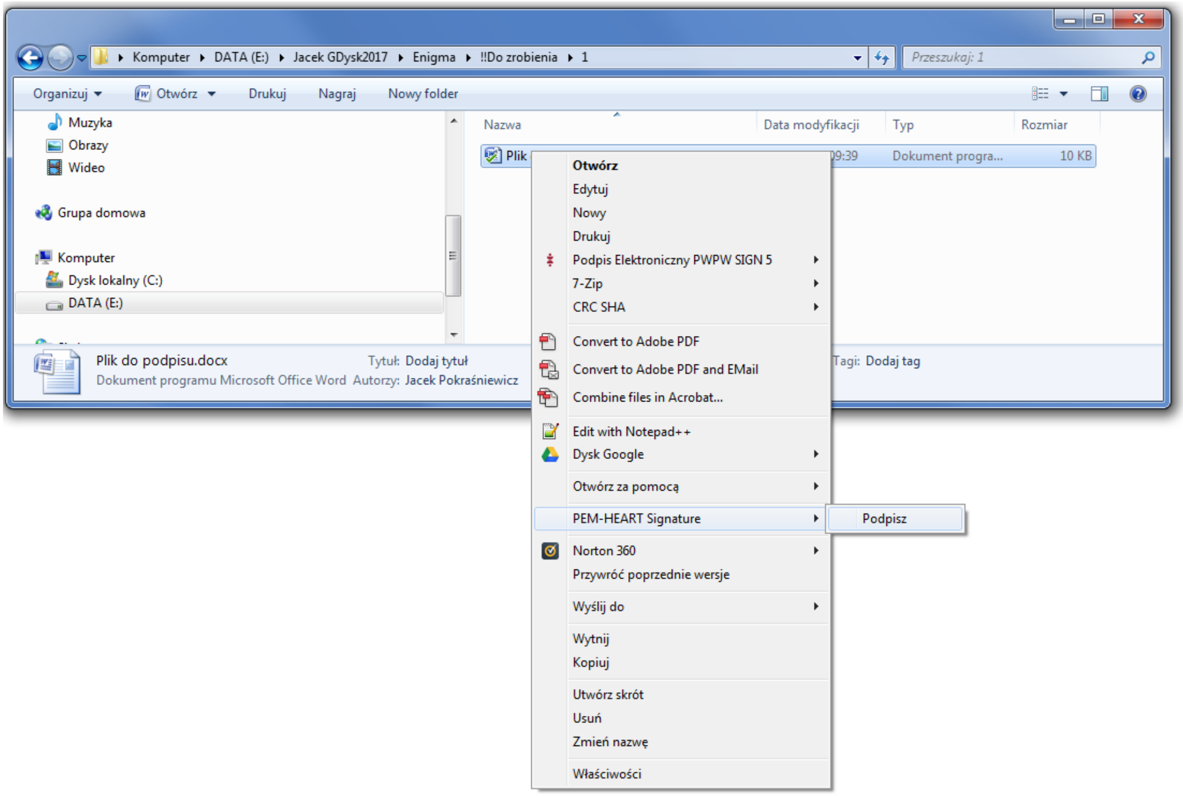
The program should be used on a computer which is under control of the certificate owner. The computer should be protected from access by unauthorized persons, have installed anti-virus software up to date and current operating system updates.

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.).

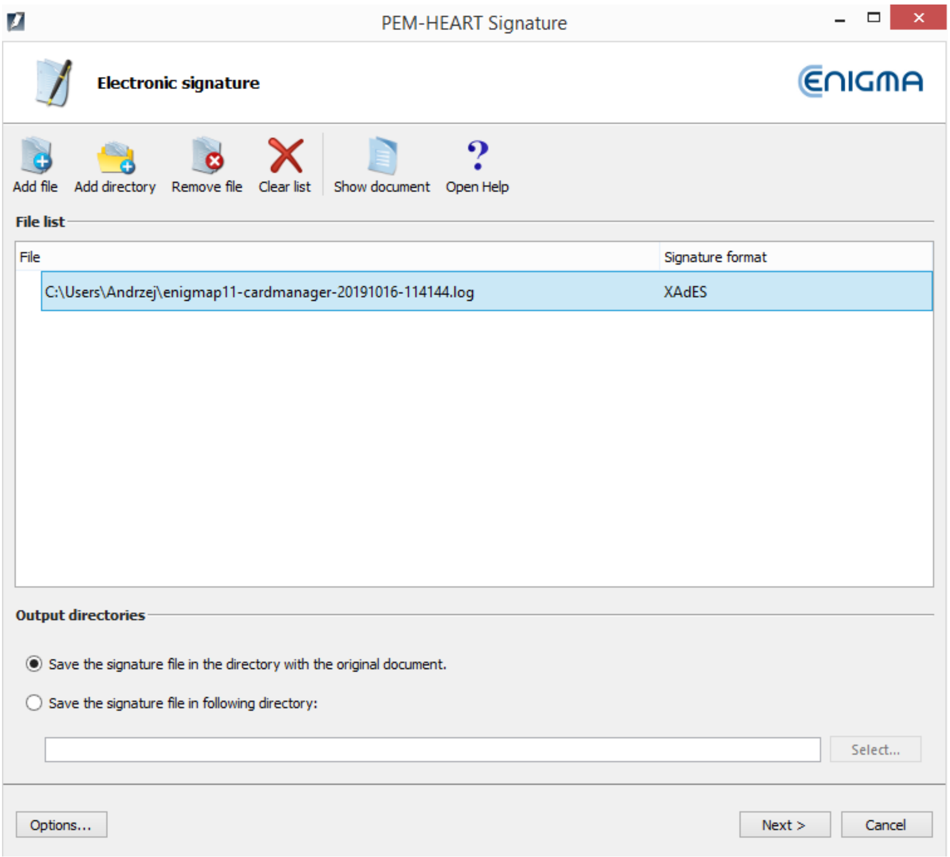
3 Signing

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:



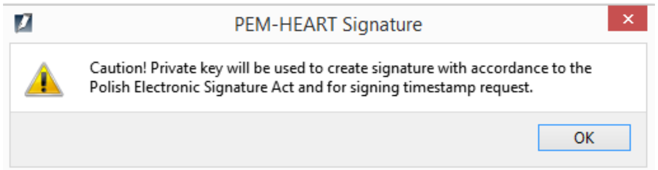
File	Signature format
C:\Users\Andrzej\enigmap11-cardmanager-20191016-114144.log	XAdES

● Save the signature file in the directory with the original document.

○ Save the signature file in following directory:

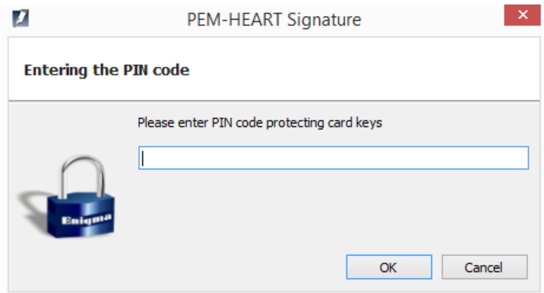
If the signature format suits you (in this case it's XAdES), press the *Next* button.

The program warns you that your private key will be used:



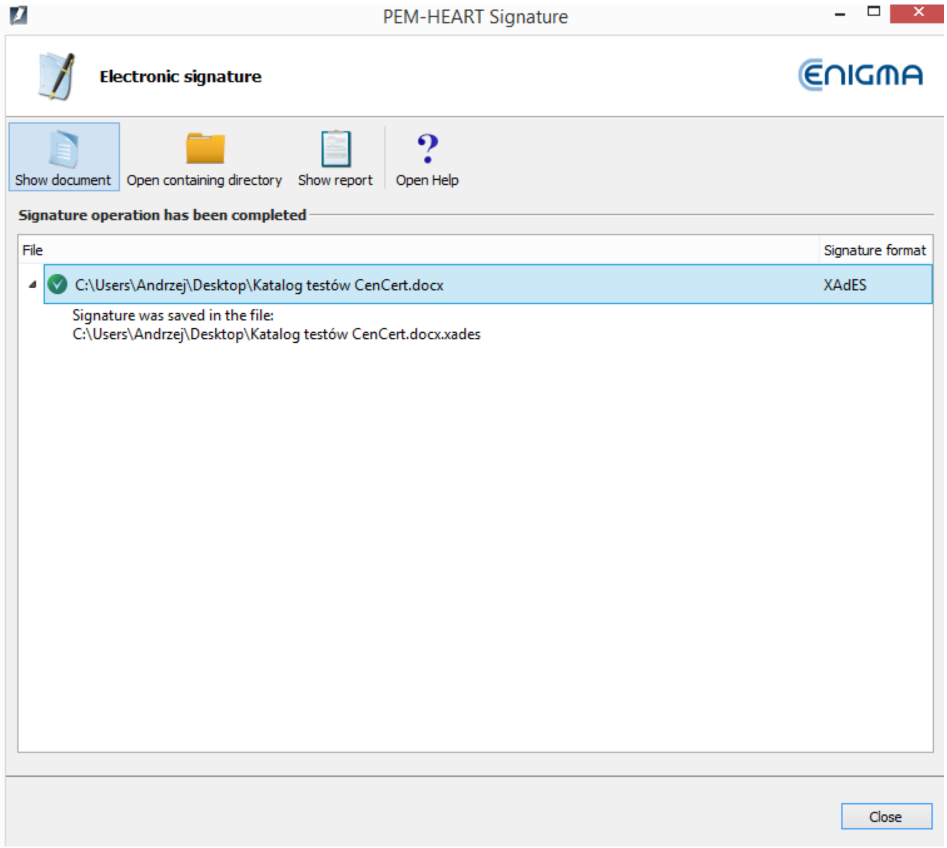
Caution! Private key will be used to create signature with accordance to the Polish Electronic Signature Act and for signing timestamp request.

Then the program asks for the PIN to your card:



Please enter PIN code protecting card keys

and generates qualified electronic signature:



Signature operation has been completed

File	Signature format
✓ C:\Users\Andrzej\Desktop\Katalog testów CenCert.docx	XAdES

Signature was saved in the file:
C:\Users\Andrzej\Desktop\Katalog testów CenCert.docx.xades

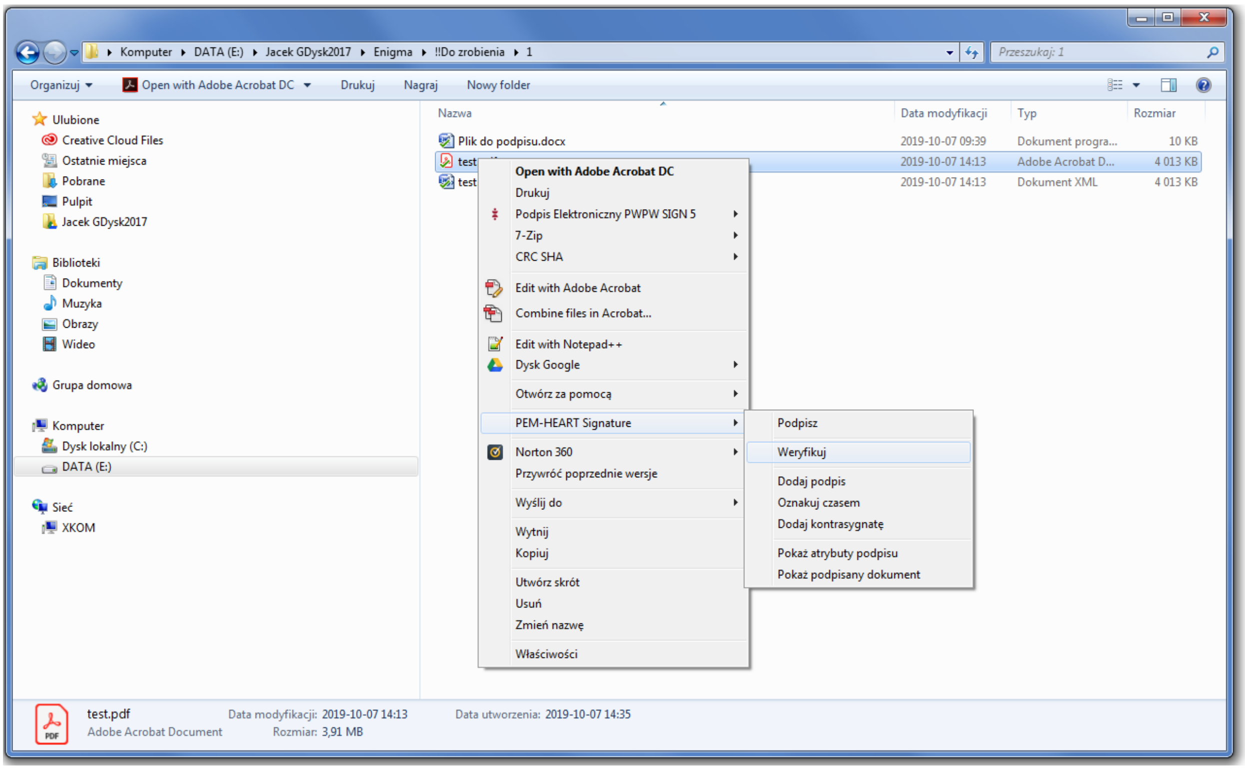
Comments:

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 7.1.
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.

4 Signature verification

If you work on *Mac OS* or *Linux* - go to chapter 5.3.

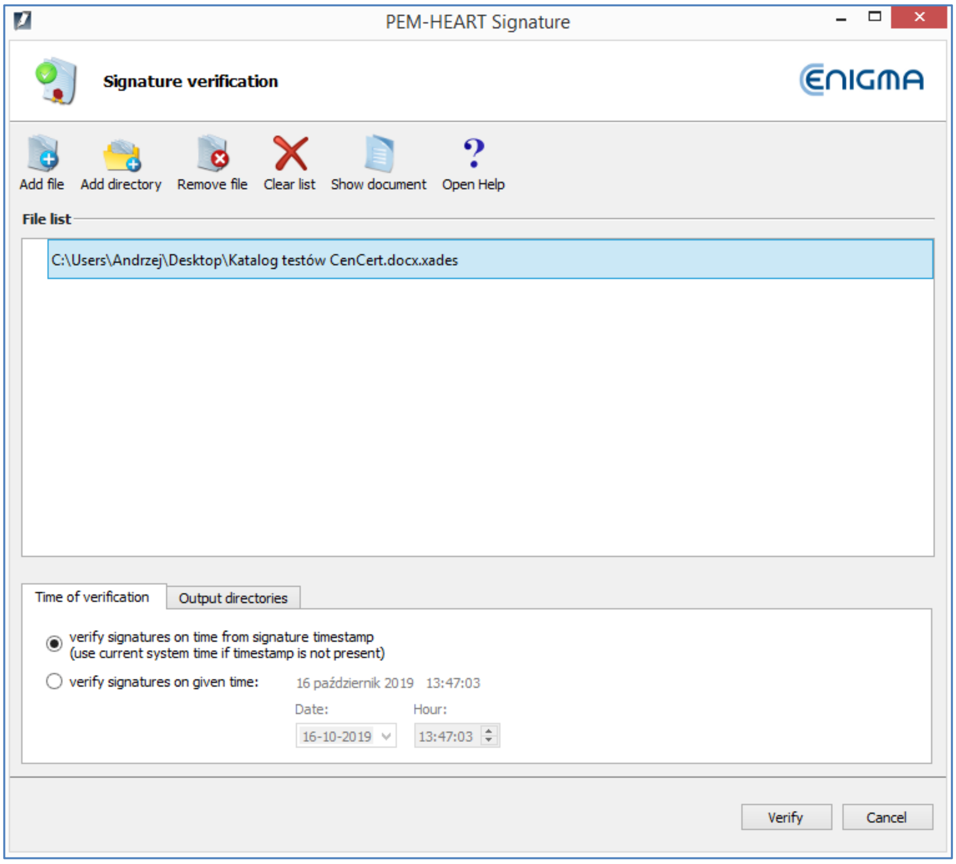
To verify a signature, **Right** click on the signature file (or signed filer) name, and then choose ***PEM-HEART Signature** -> **Weryfikuj***.



Nazwa	Data modyfikacji	Typ	Rozmiar
Plik do podpisu.docx	2019-10-07 09:39	Dokument progra...	10 KB
test	2019-10-07 14:13	Adobe Acrobat D...	4 013 KB
test	2019-10-07 14:13	Dokument XML	4 013 KB

test.pdf Data modyfikacji: 2019-10-07 14:13 Data utworzenia: 2019-10-07 14:35
Adobe Acrobat Document Rozmiar: 3,91 MB

Then program displays signature verification window:



C:\Users\Andrzej\Desktop\Katalog testów CenCert.docx.xades

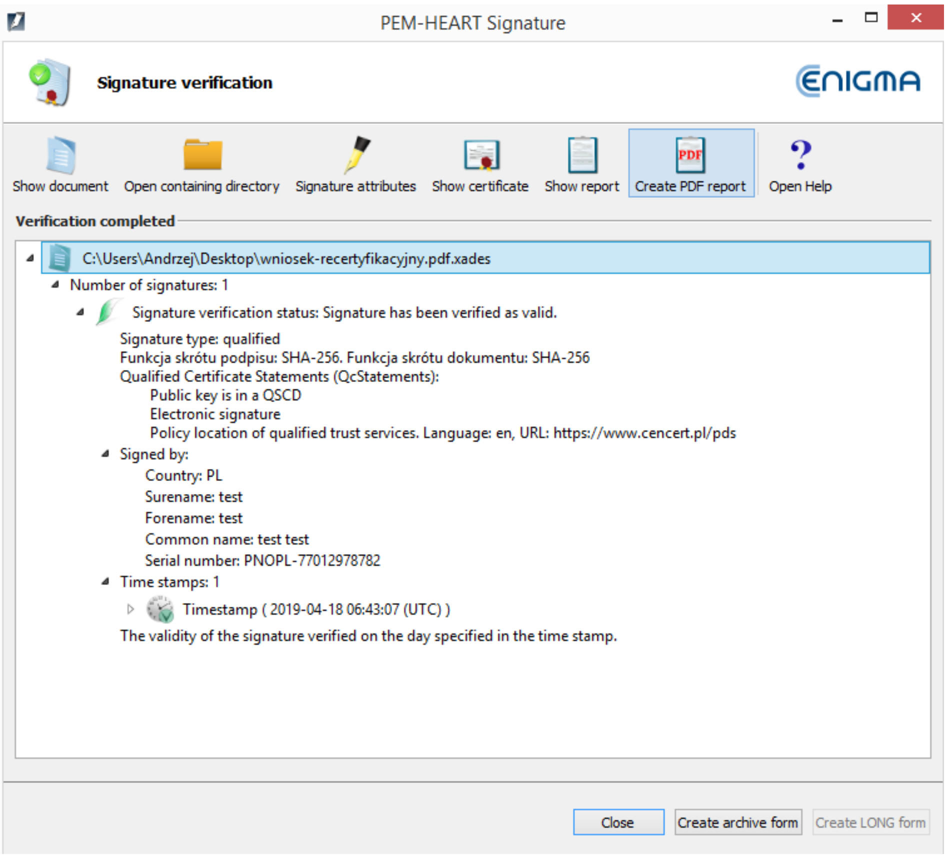
● verify signatures on time from signature timestamp (use current system time if timestamp is not present)

○ verify signatures on given time: 16 październik 2019 13:47:03

Date: 16-10-2019 Hour: 13:47:03

Press the *Verify* button.

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



C:\Users\Andrzej\Desktop\wniosek-recertyfikacyjny.pdf.xades
- Number of signatures: 1
  - Signature verification status: Signature has been verified as valid.
    - Signature type: qualified
    - Funkcja skrótu podpisu: SHA-256. Funkcja skrótu dokumentu: SHA-256
    - Qualified Certificate Statements (QcStatements):
      - Public key is in a QSCD
      - Electronic signature
      - Policy location of qualified trust services. Language: en, URL: https://www.cencert.pl/pds
    - Signed by:
      - Country: PL
      - Surename: test
      - Forename: test
      - Common name: test test
      - Serial number: PNOPL-77012978782
    - Time stamps: 1
      - Timestamp (2019-04-18 06:43:07 (UTC))
    - The validity of the signature verified on the day specified in the time stamp.

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:

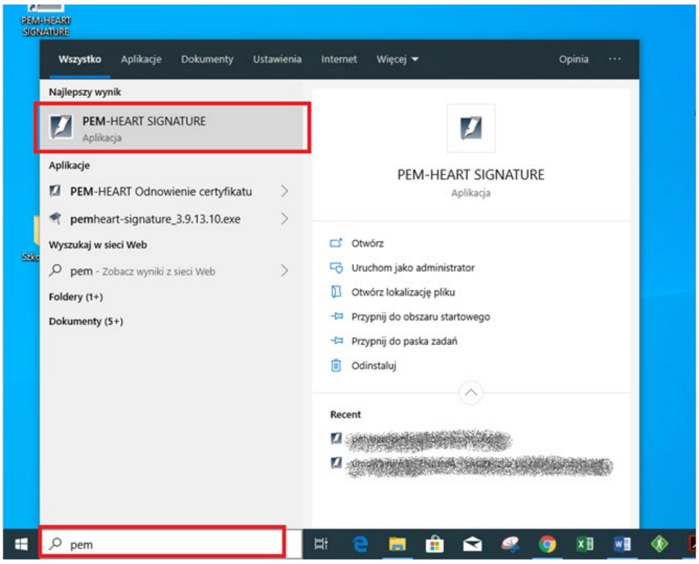
1) Additional actions are available at the top menu:
   a) *Create PDF report* - saves the clear report (in PDF) confirming the status of the signature verification.
   b) *Show certificate* - displays the certificate used to sign (and possibly personal data of person who has signed the document).
   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

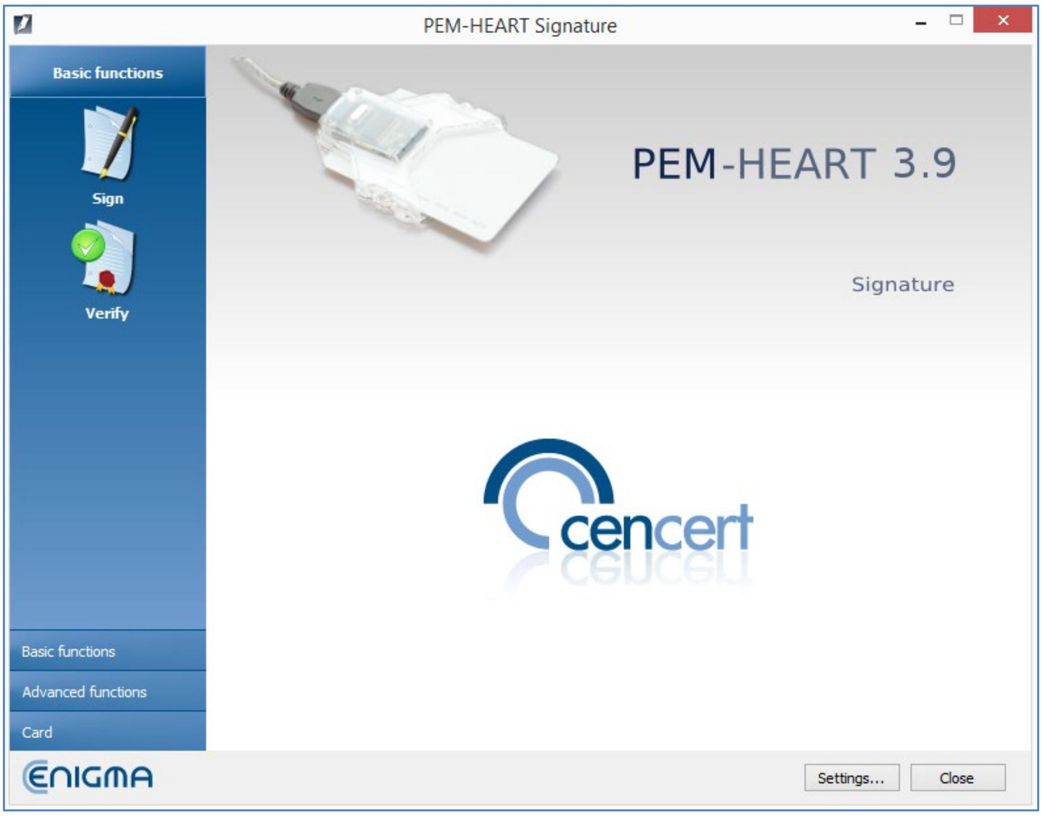
5.1 Starting the program

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.



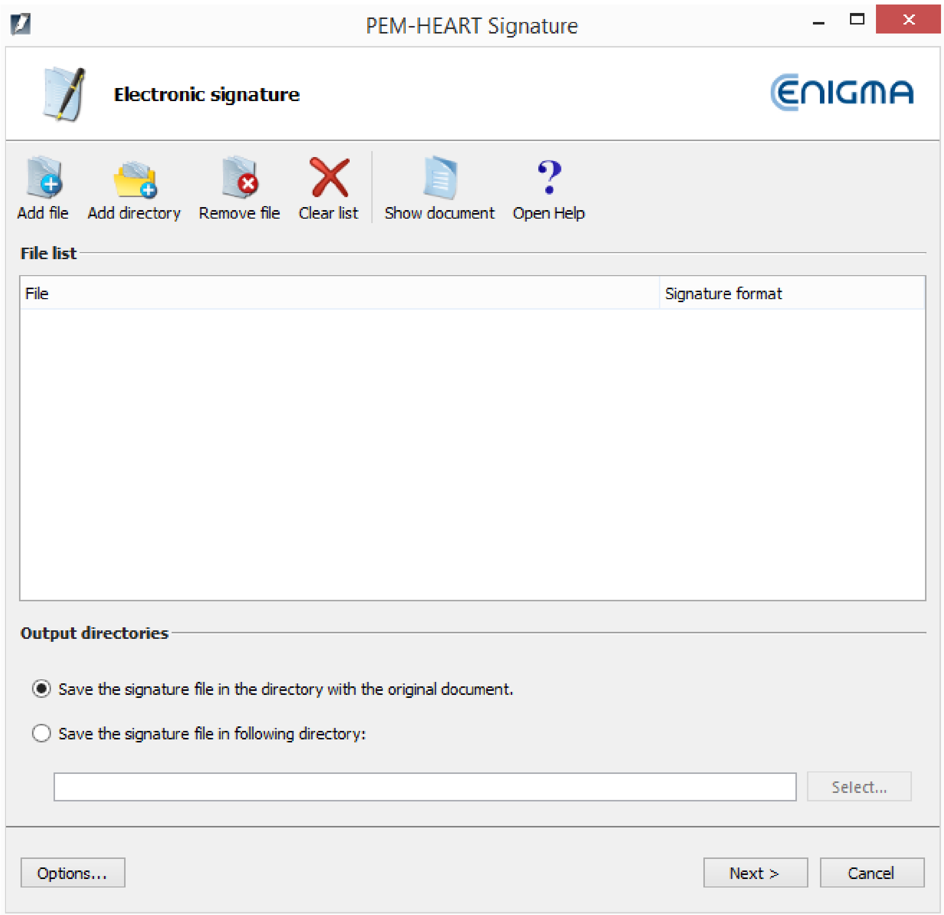
After starting the application the main program window is displayed:



5.2 Signing

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:



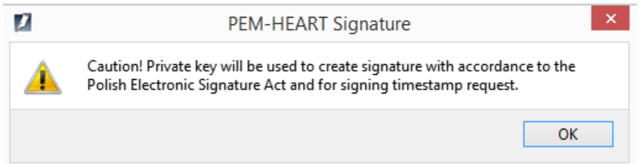
● Save the signature file in the directory with the original document.

○ Save the signature file in following directory:

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.

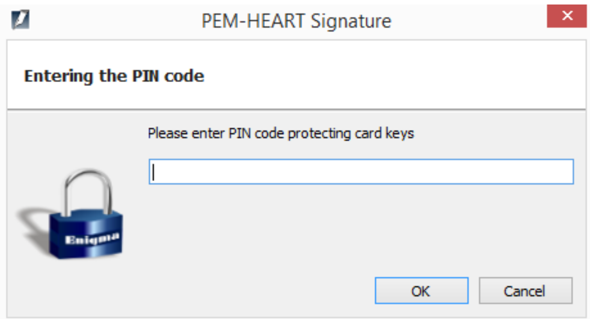
Press the *Next* button to proceed.

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



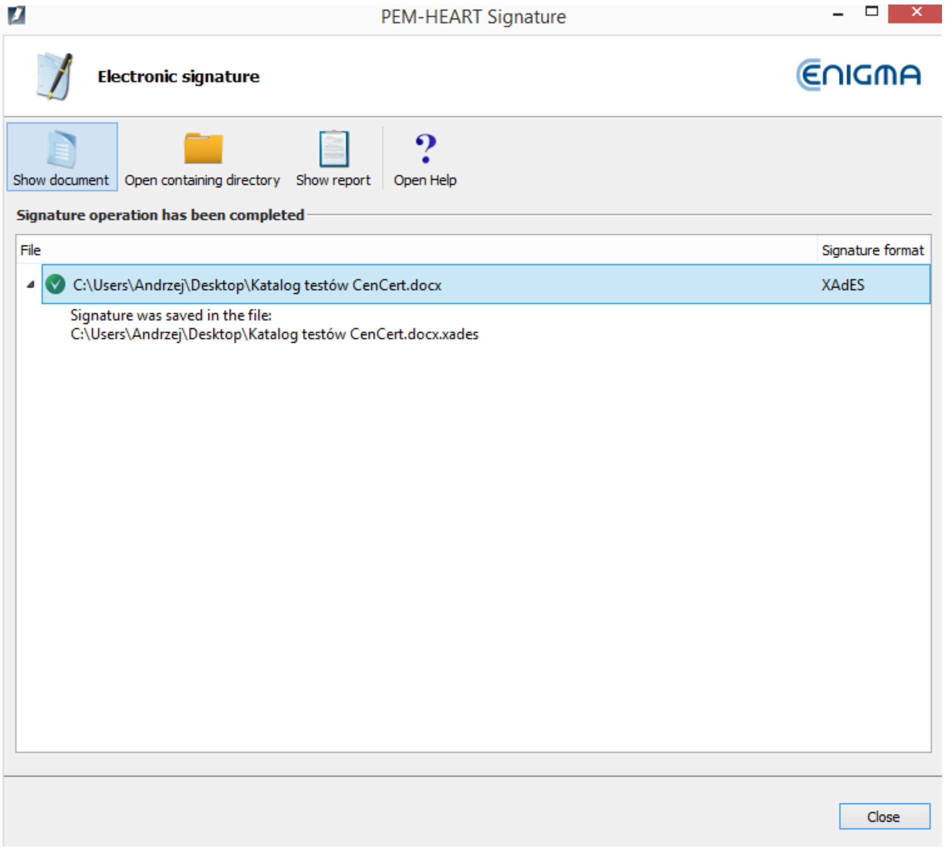
Caution! Private key will be used to create signature with accordance to the Polish Electronic Signature Act and for signing timestamp request.

Then it asks for the card PIN:



Please enter PIN code protecting card keys

and makes the signature:



Signature operation has been completed

File	Signature format
✓ C:\Users\Andrzej\Desktop\Katalog testów CenCert.docx	XAdES

Signature was saved in the file:
C:\Users\Andrzej\Desktop\Katalog testów CenCert.docx.xades

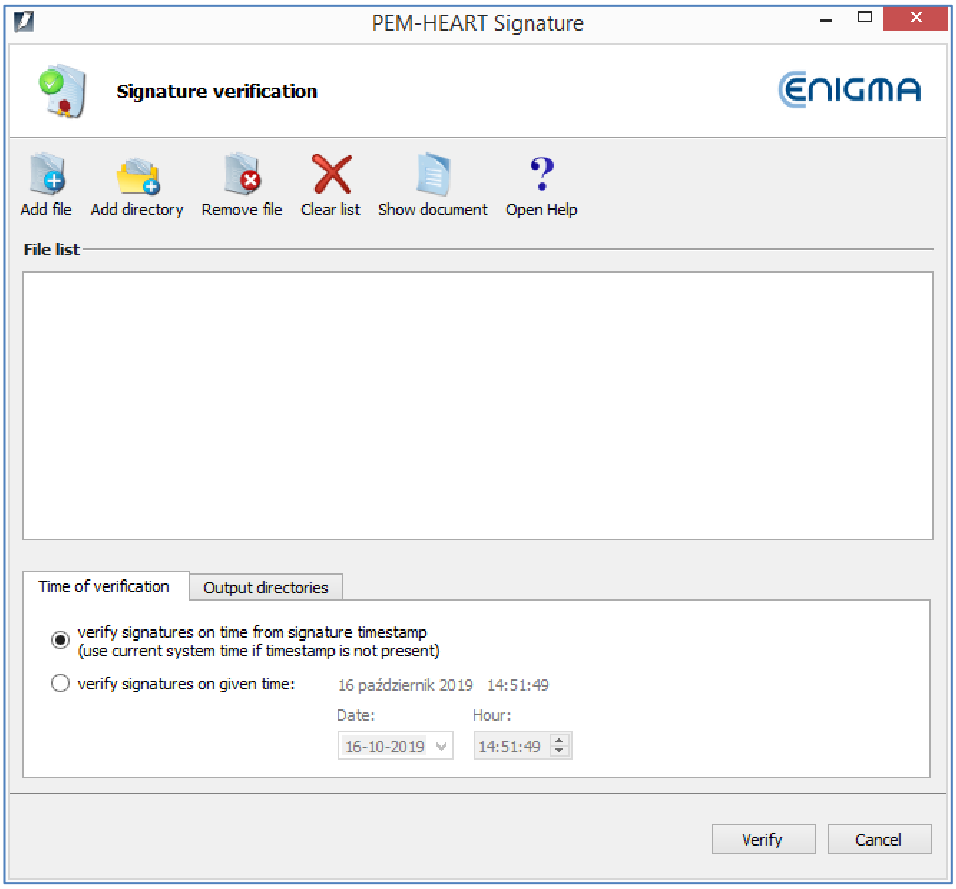
Comments:

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 7.1
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.

5.3 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:

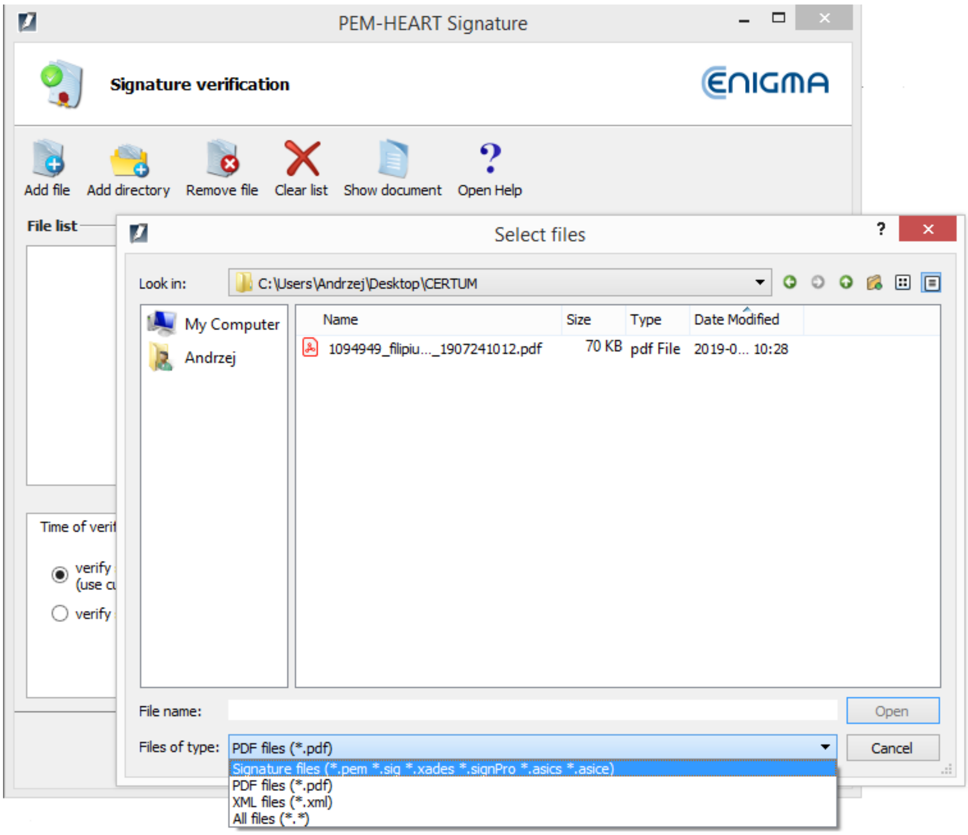


● verify signatures on time from signature timestamp
(use current system time if timestamp is not present)

○ verify signatures on given time: 16 październik 2019 14:51:49

Date: 16-10-2019 Hour: 14:51:49

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 "*.*").



Look in: C:\Users\Andrzej\Desktop\CERTUM

Name	Size	Type	Date Modified
1094949_filipiu..._1907241012.pdf	70 KB	pdf File	2019-0... 10:28

File name:

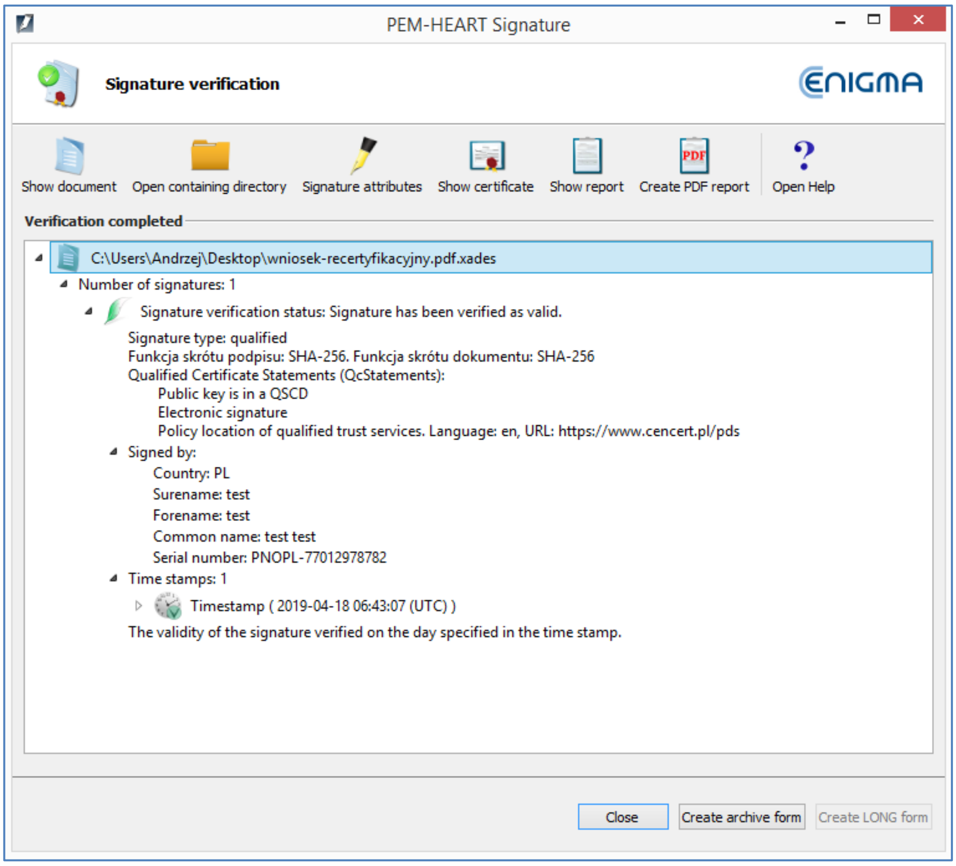
Files of type: PDF files (*.pdf)

- Signature files (*.pem *.sig *.xades *.signPro *.asics *.asice)
- PDF files (*.pdf)
- XML files (*.xml)
- All files (*.*)

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:



```
C:\Users\Andrzej\Desktop\wniosek-recertyfikacyjny.pdf.xades
  Number of signatures: 1
    Signature verification status: Signature has been verified as valid.
      Signature type: qualified
      Funkcja skrótu podpisu: SHA-256. Funkcja skrótu dokumentu: SHA-256
      Qualified Certificate Statements (QcStatements):
          Public key is in a QSCD
          Electronic signature
          Policy location of qualified trust services. Language: en, URL: https://www.cencert.pl/pds
      Signed by:
          Country: PL
          Surename: test
          Forename: test
          Common name: test test
          Serial number: PNOPL-77012978782
      Time stamps: 1
          Timestamp ( 2019-04-18 06:43:07 (UTC) )
      The validity of the signature verified on the day specified in the time stamp.
```

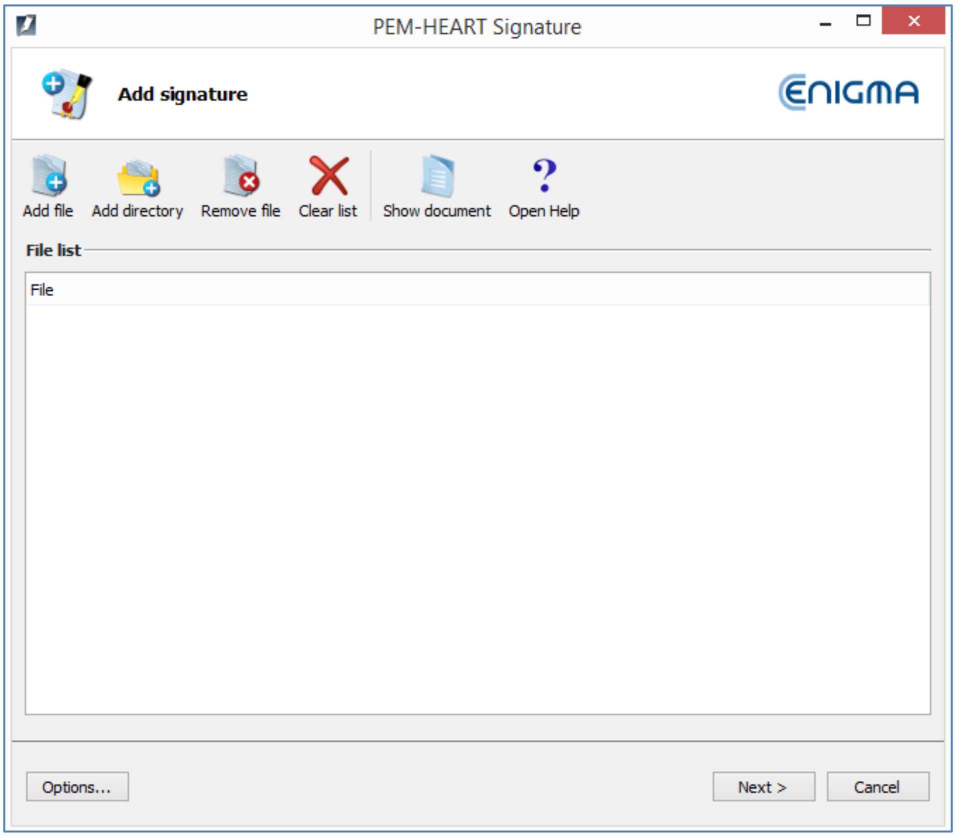
See also the verification notes in the chapter 4.

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.

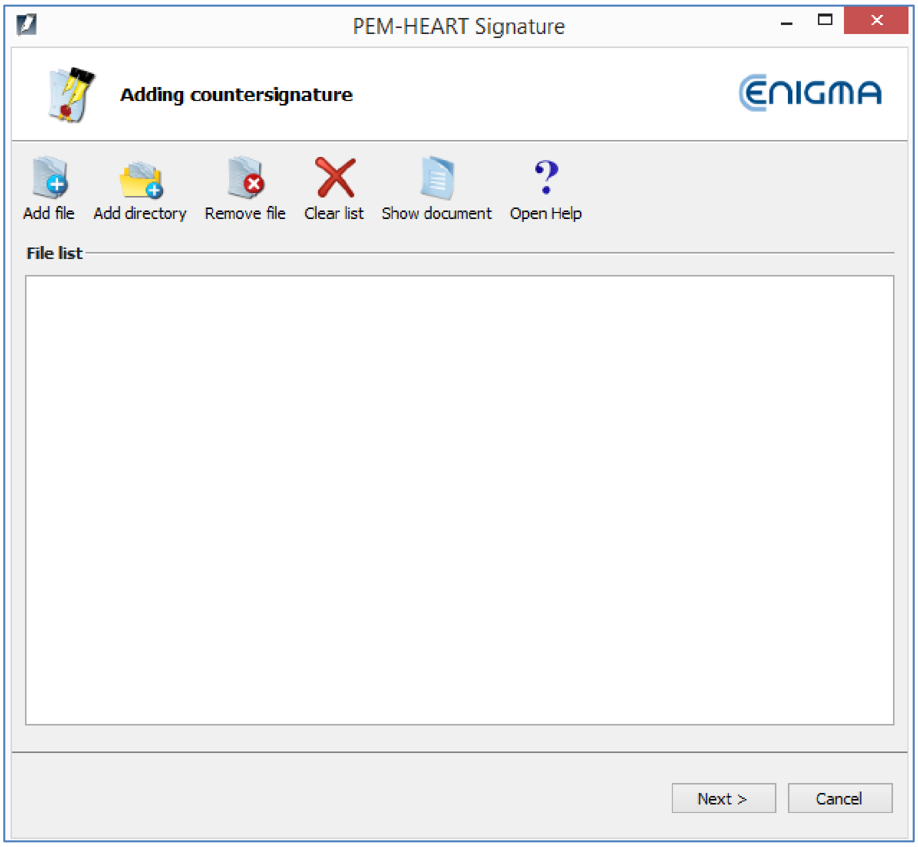
5.5 Countersignature

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*.

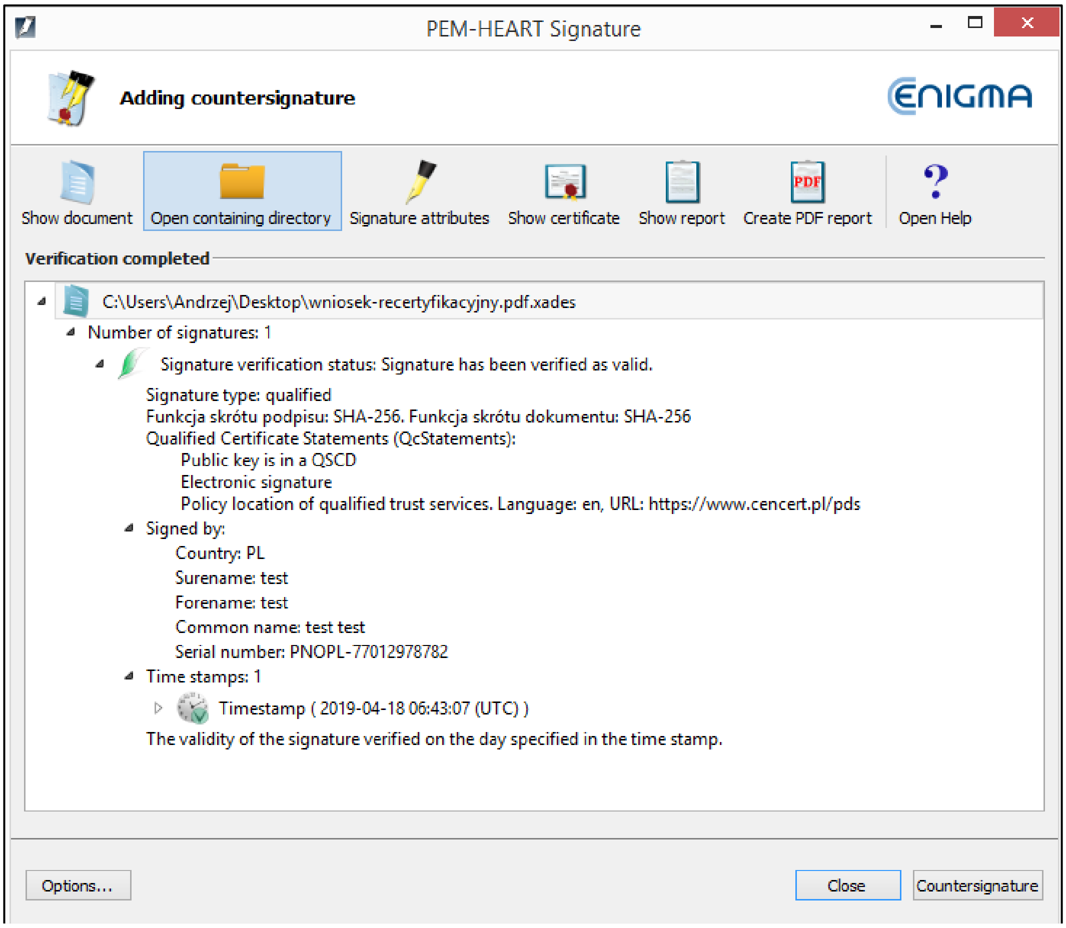
The countersign window is displayed:



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:



```
C:\Users\Andrzej\Desktop\wniosek-recertyfikacyjny.pdf.xades
  Number of signatures: 1
    Signature verification status: Signature has been verified as valid.
      Signature type: qualified
      Funkcja skrótu podpisu: SHA-256. Funkcja skrótu dokumentu: SHA-256
      Qualified Certificate Statements (QcStatements):
         Public key is in a QSCD
         Electronic signature
         Policy location of qualified trust services. Language: en, URL: https://www.cencert.pl/pds
      Signed by:
        Country: PL
        Surename: test
        Forename: test
        Common name: test test
        Serial number: PNOPL-77012978782
      Time stamps: 1
        Timestamp ( 2019-04-18 06:43:07 (UTC) )
      The validity of the signature verified on the day specified in the time stamp.
```

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 5.3). 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:

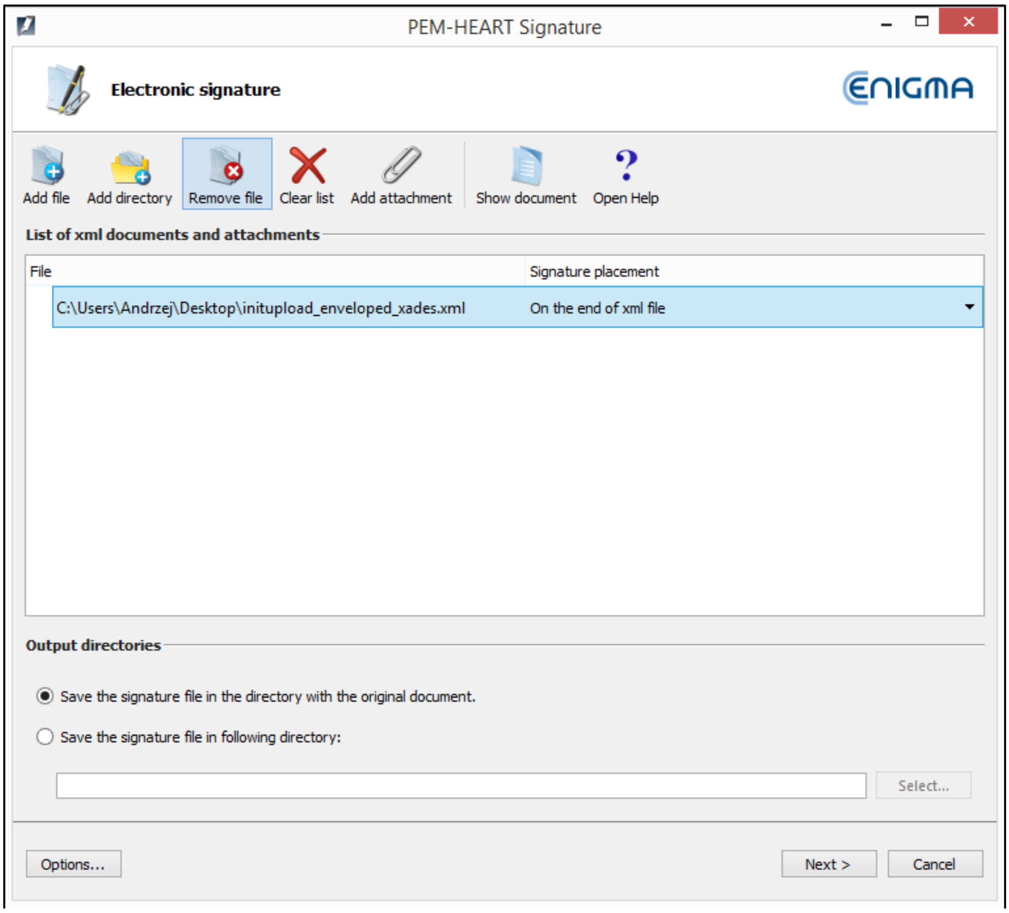
1) Purchasing of a time stamping service package may be required.

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:



List of xml documents and attachments

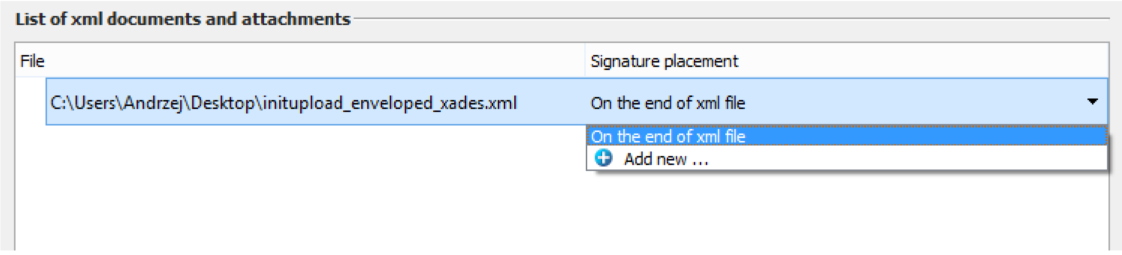
File	Signature placement
C:\Users\Andrzej\Desktop\initupload_enveloped_xades.xml	On the end of xml file

● Save the signature file in the directory with the original document.

○ Save the signature file in following directory:

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 5.3).

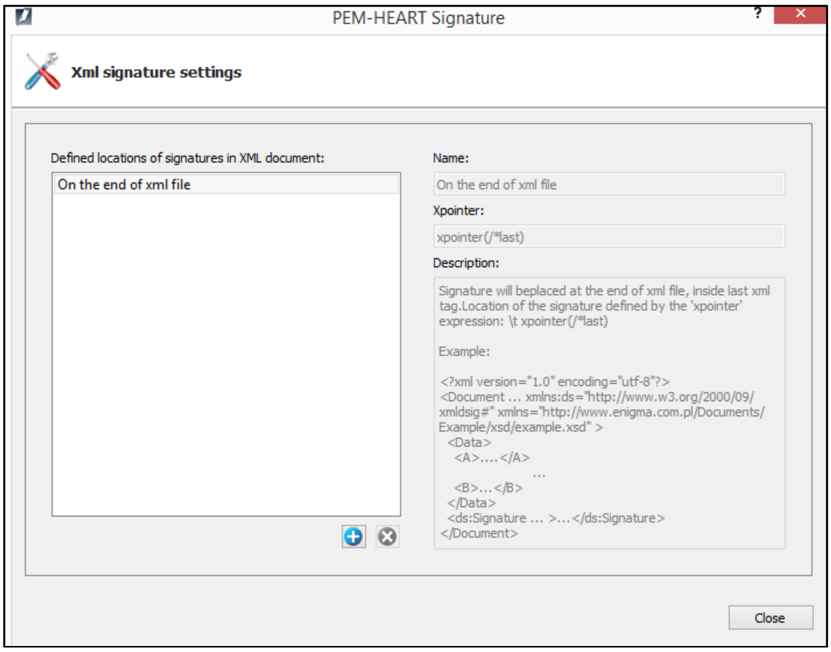
If the signature is to be located in a different place than at the end of the file, click with the mouse on the *On the end of the xml file* label.



List of xml documents and attachments

File	Signature placement
C:\Users\Andrzej\Desktop\initupload_enveloped_xades.xml	On the end of xml file

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



Xml signature settings

Defined locations of signatures in XML document:

On the end of xml file

Name: On the end of xml file

Xpointer: xpointer(/*last)

Description:

Signature will beplaced at the end of xml file, inside last xml tag.Location of the signature defined by the 'xpointer' expression: \t xpointer(/*last)

Example:

```
<?xml version="1.0" encoding="utf-8"?>
<Document ... xmlns:ds="http://www.w3.org/2000/09/
xmldsig#" xmlns="http://www.enigma.com.pl/Documents/
Example/xsd/example.xsd" >
 <Data>
  <A>....</A>
        ...
  <B>...</B>
 </Data>
 <ds:Signature ... >...</ds:Signature>
</Document>
```

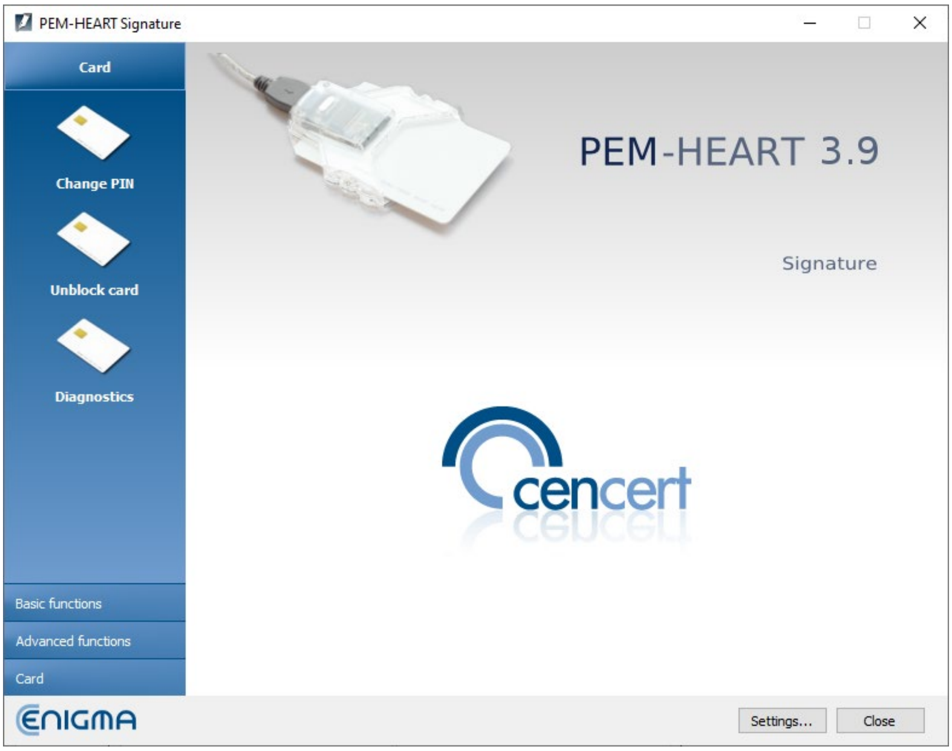
Click with mouse on the ⊕ icon, then type the name of your configuration, the structure *xpointer* and optionally a description of the configuration. Structure *xpointer* is defined as: `xpointer([`*`indication of the node XML`*`])`. Available forms of this structure are described in the *XML Pointer Language* (*XPointer*) 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.

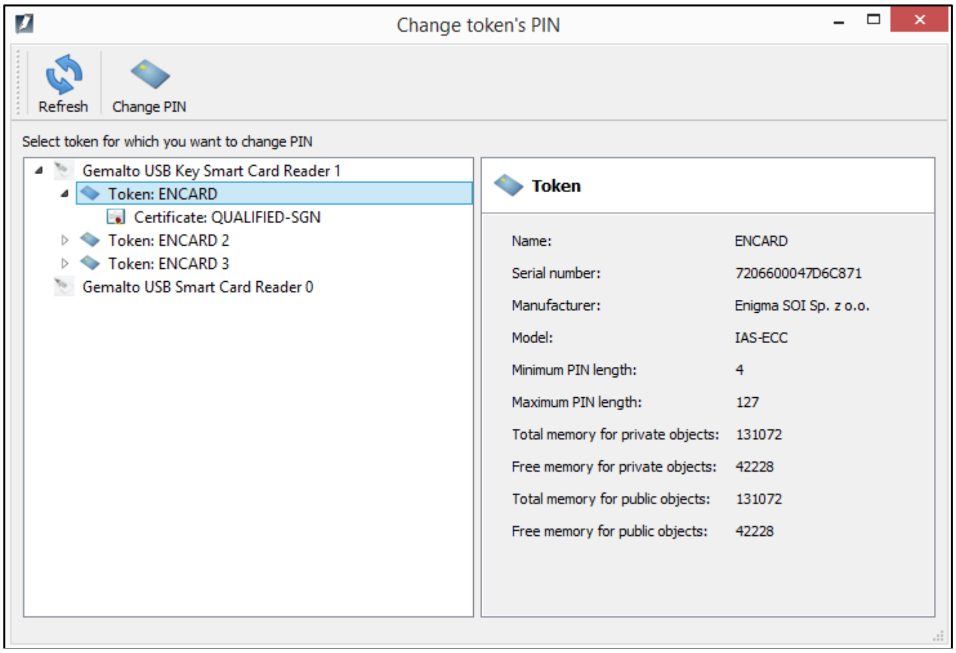
All operations described below are invoked from the main program window (see chapter 5.1) when you click on the ***Card*** label in the left menu (left-bottom on the main window).



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):



Change token's PIN

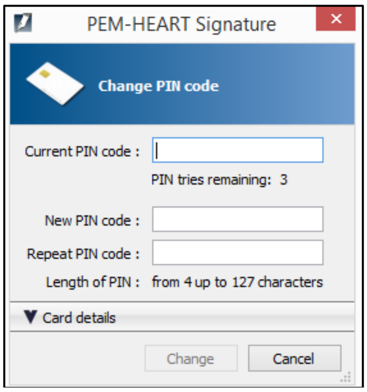
Select token for which you want to change PIN

- Gemalto USB Key Smart Card Reader 1
  - Token: ENCARD
    - Certificate: QUALIFIED-SGN
  - Token: ENCARD 2
  - Token: ENCARD 3
- Gemalto USB Smart Card Reader 0

Token

Name:	ENCARD
Serial number:	7206600047D6C871
Manufacturer:	Enigma SOI Sp. z o.o.
Model:	IAS-ECC
Minimum PIN length:	4
Maximum PIN length:	127
Total memory for private objects:	131072
Free memory for private objects:	42228
Total memory for public objects:	131072
Free memory for public objects:	42228

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



PEM-HEART Signature

Change PIN code

Current PIN code :

PIN tries remaining: 3

New PIN code :

Repeat PIN code :

Length of PIN : from 4 up to 127 characters

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).

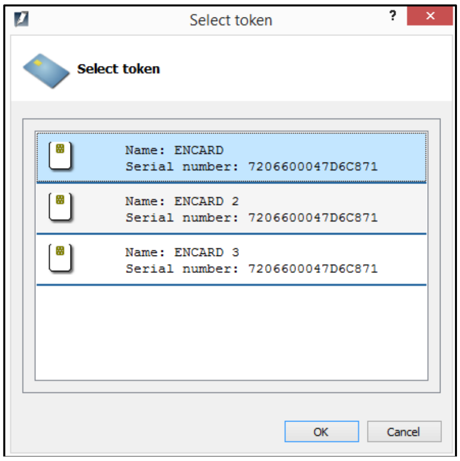
Note! If the PIN code is blocked, the card can be unblocked only with the PUK code.

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

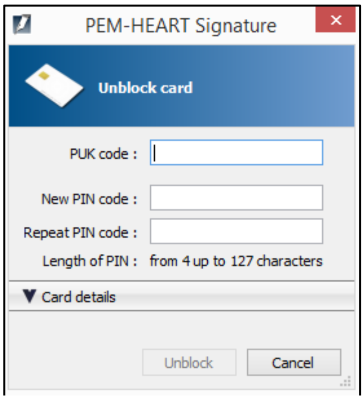
If your smart card has been blocked because of too many incorrect PINs, you can unlock it with the PUK. You have created the PUK code when your card was activated.

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



```
Name: ENCARD
Serial number: 7206600047D6C871
Name: ENCARD 2
Serial number: 7206600047D6C871
Name: ENCARD 3
Serial number: 7206600047D6C871
```

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



PUK code :

New PIN code :

Repeat PIN code :

Length of PIN : from 4 up to 127 characters

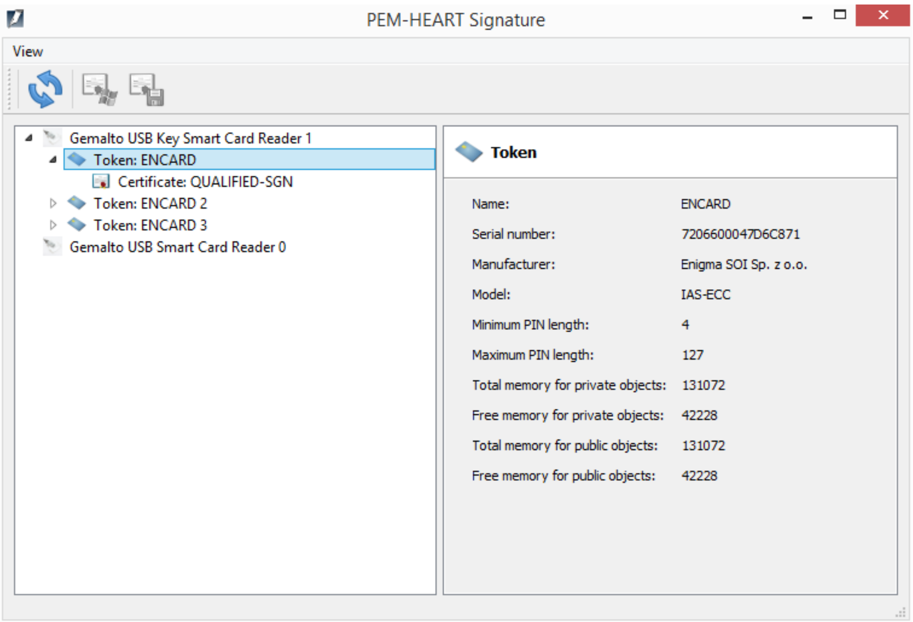
If you entered your PUK correctly, you can set (and repeat) the new PIN code and the card will be unblocked.

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.



- Gemalto USB Key Smart Card Reader 1
  - Token: ENCARD
    - Certificate: QUALIFIED-SGN
  - Token: ENCARD 2
  - Token: ENCARD 3
- Gemalto USB Smart Card Reader 0

Token

Name:	ENCARD
Serial number:	7206600047D6C871
Manufacturer:	Enigma SOI Sp. z o.o.
Model:	IAS-ECC
Minimum PIN length:	4
Maximum PIN length:	127
Total memory for private objects:	131072
Free memory for private objects:	42228
Total memory for public objects:	131072
Free memory for public objects:	42228

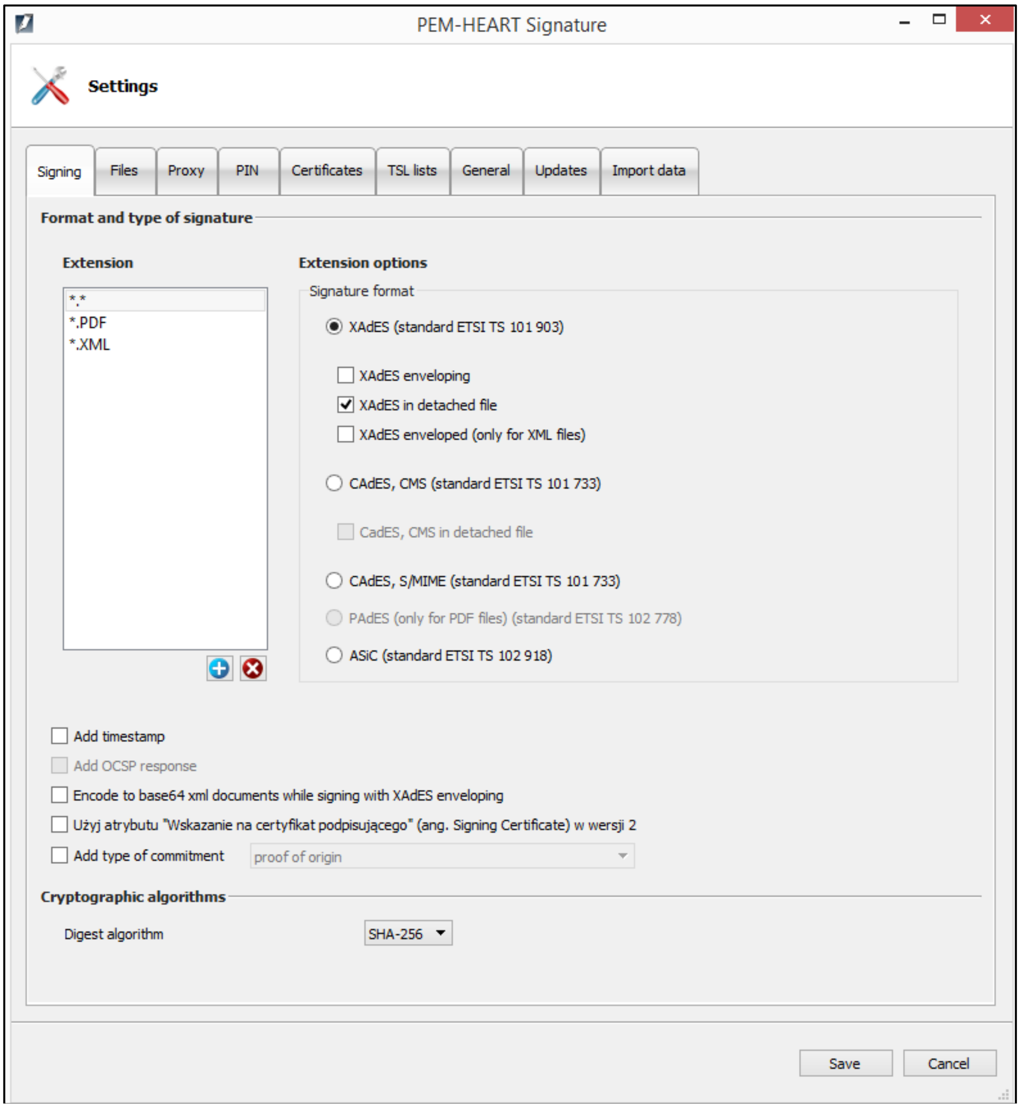
You can get information about the objects on the cards: tokens, keys, and certificates. After selecting the certificate, its structure and data are displayed. You can also (buttons at the top of the window) install the certificate in the Ms Windows system's store and / or save the certificate to a file.

7 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).

7.1 Options of signatures

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



Format and type of signature

Extension

- *.*
- *.PDF
- *.XML

Extension options

Signature format

● XAdES (standard ETSI TS 101 903)

□ XAdES enveloping
☑ XAdES in detached file
□ XAdES enveloped (only for XML files)

○ 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)

○ ASiC (standard ETSI TS 102 918)

□ Add timestamp
□ Add OCSP response
□ Encode to base64 xml documents while signing with XAdES enveloping
□ Użyj atrybutu "Wskazanie na certyfikat podpisującego" (ang. Signing Certificate) w wersji 2
□ Add type of commitment proof of origin

Cryptographic algorithms

Digest algorithm SHA-256

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.

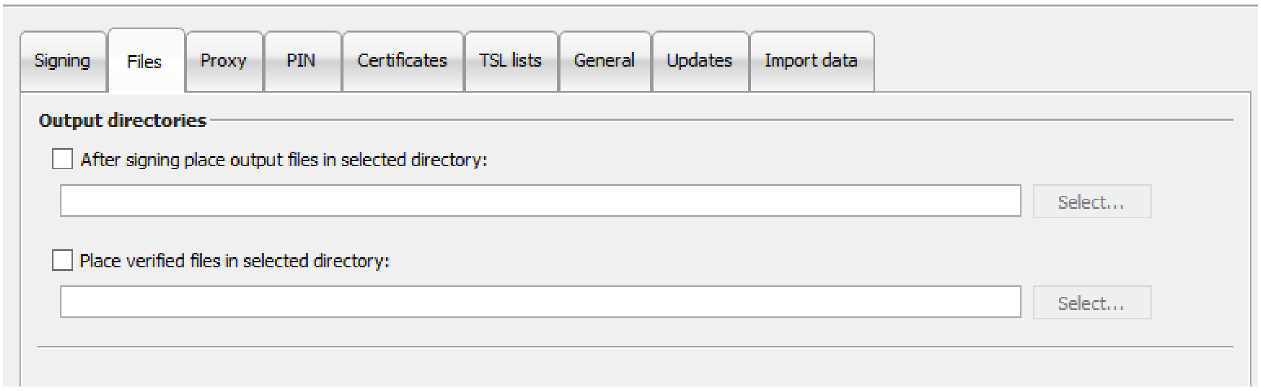
The option "*Use Signing Certificate attribute in version 2"* puts the signature with the certificate identification in a format compatible with newer versions of ETSI standards. Select the option if it is required by the signature verification system that uses only new formats.

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.

7.2 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.



Output directories

□ After signing place output files in selected directory:

□ Place verified files in selected directory:

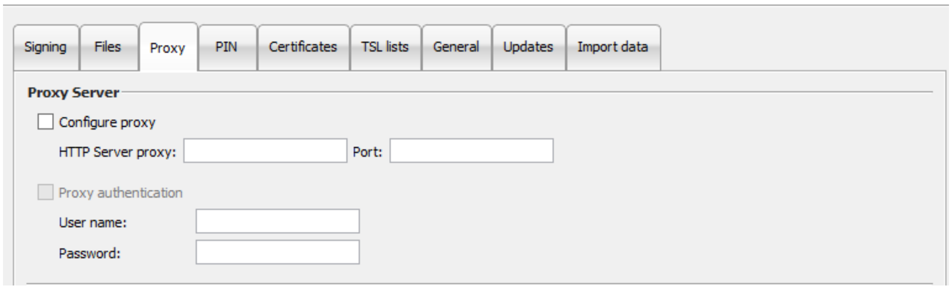
Figure 49 Output directory configuration

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

7.3 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 .



Proxy Server

□ Configure proxy

HTTP Server proxy: Port:

□ Proxy authentication

User name:

Password:

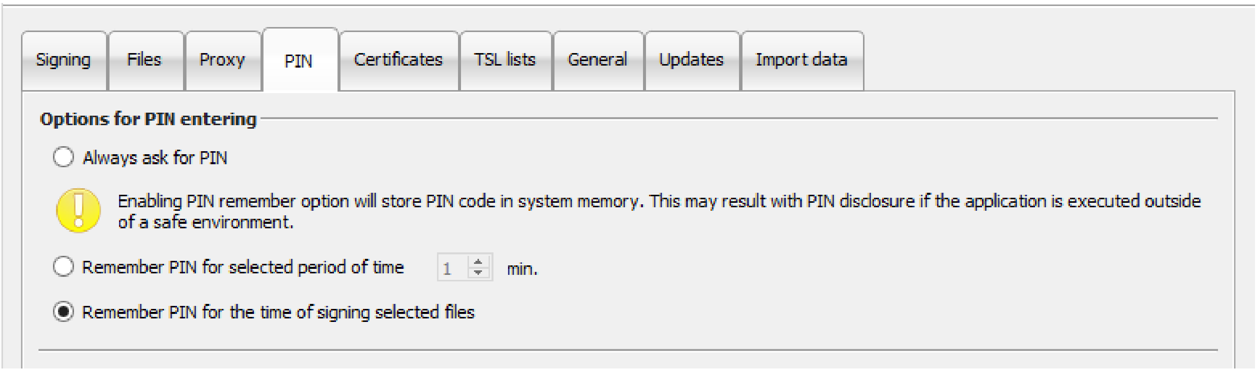
Note! Misconfiguration results in the lack of access to the Internet (the time stamp cannot be downloaded, it signature validation is very limited).

7.4 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.



Options for PIN entering

○ Always ask for PIN

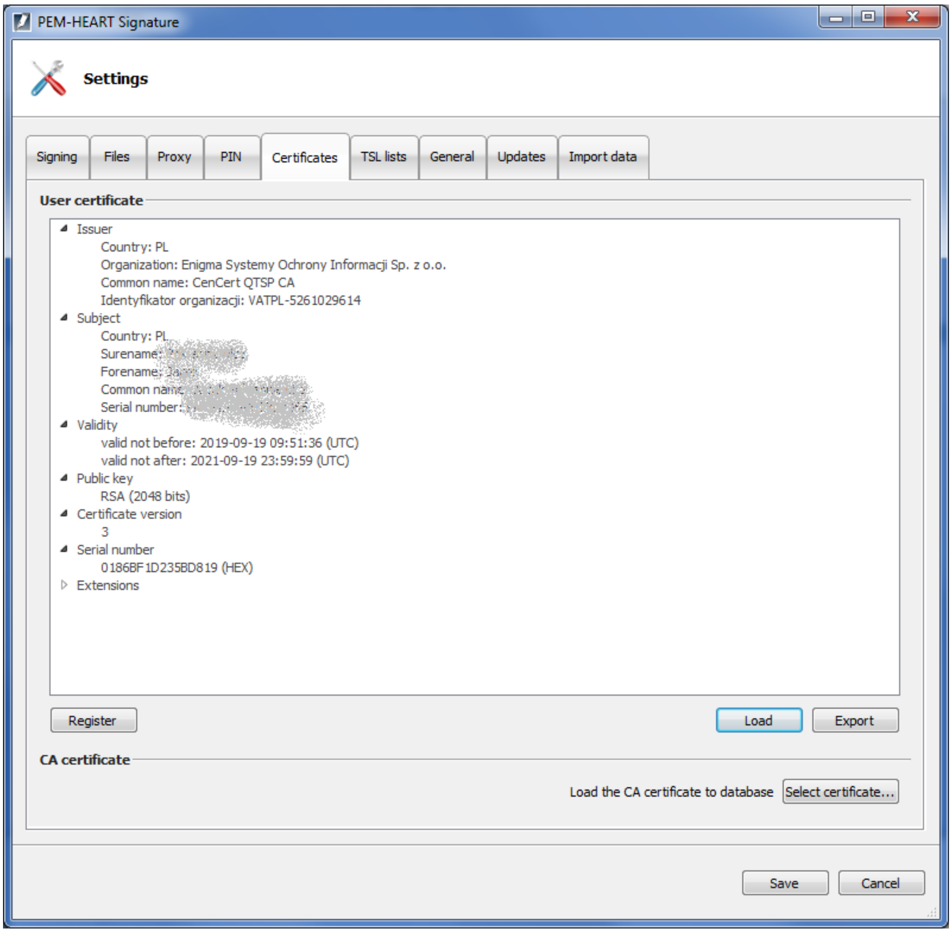
Enabling PIN remember option will store PIN code in system memory. This may result with PIN disclosure if the application is executed outside of a safe environment.

○ Remember PIN for selected period of time 1 min.

● Remember PIN for the time of signing selected files

7.5 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.



User certificate

- Issuer
  - Country: PL
  - Organization: Enigma Systemy Ochrony Informacji Sp. z o.o.
  - Common name: CenCert QTSP CA
  - Identyfikator organizacji: VATPL-5261029614
- Subject
  - Country: PL
  - Surename: [redacted]
  - Forename: [redacted]
  - Common name: [redacted]
  - Serial number: [redacted]
- Validity
  - valid not before: 2019-09-19 09:51:36 (UTC)
  - valid not after: 2021-09-19 23:59:59 (UTC)
- Public key
  - RSA (2048 bits)
- Certificate version
  - 3
- Serial number
  - 0186BF1D235BD819 (HEX)
- Extensions

CA certificate

Load the CA certificate to database

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

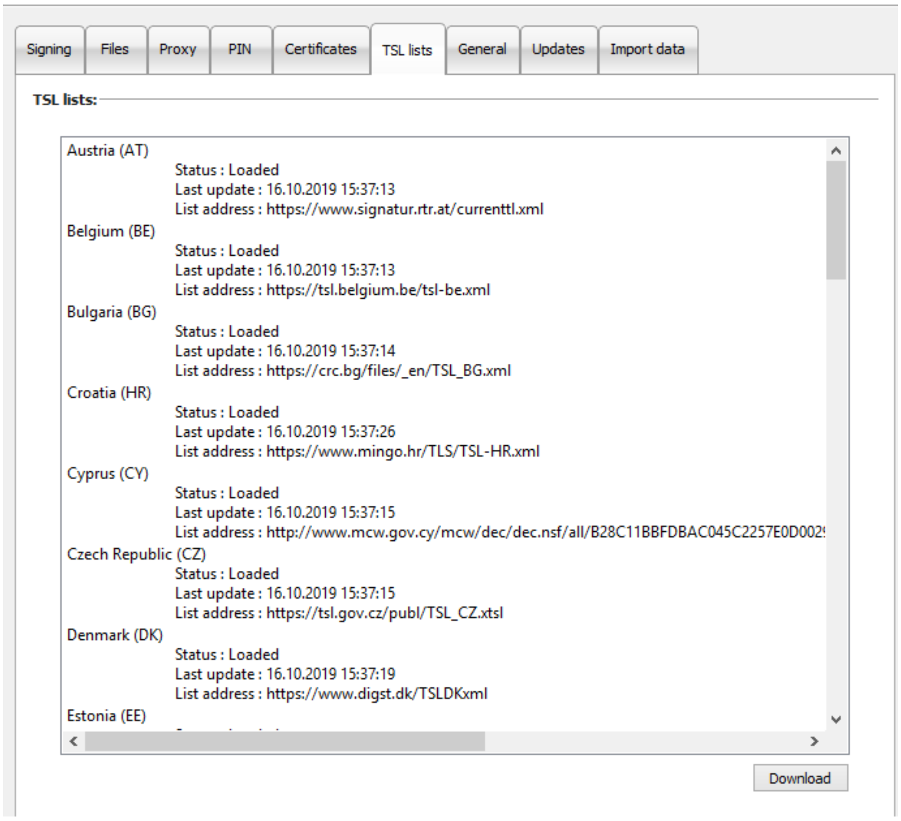
You may export the certificate to a file using the *Export* button .

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.

7.6 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.



TSL lists:

```
Austria (AT)
            Status : Loaded
            Last update : 16.10.2019 15:37:13
            List address : https://www.signatur.rtr.at/currenttl.xml
Belgium (BE)
            Status : Loaded
            Last update : 16.10.2019 15:37:13
            List address : https://tsl.belgium.be/tsl-be.xml
Bulgaria (BG)
            Status : Loaded
            Last update : 16.10.2019 15:37:14
            List address : https://crc.bg/files/_en/TSL_BG.xml
Croatia (HR)
            Status : Loaded
            Last update : 16.10.2019 15:37:26
            List address : https://www.mingo.hr/TLS/TSL-HR.xml
Cyprus (CY)
            Status : Loaded
            Last update : 16.10.2019 15:37:15
            List address : http://www.mcw.gov.cy/mcw/dec/dec.nsf/all/B28C11BBFDBAC045C2257E0D002
Czech Republic (CZ)
            Status : Loaded
            Last update : 16.10.2019 15:37:15
            List address : https://tsl.gov.cz/publ/TSL_CZ.xtsl
Denmark (DK)
            Status : Loaded
            Last update : 16.10.2019 15:37:19
            List address : https://www.digst.dk/TSLDKxml
Estonia (EE)
```

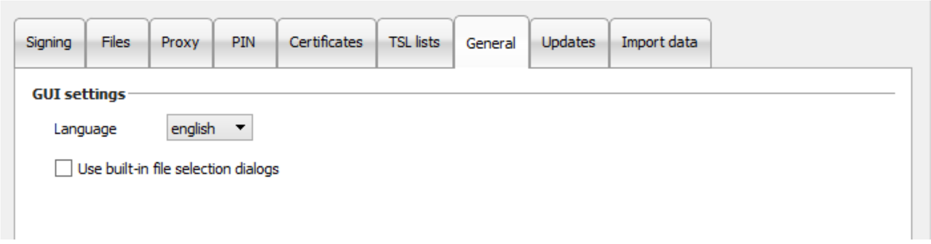
The tab presents the current status of TSL lists in the program's database.

The windows 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 .

7.7 General

Changing the program language to English or Polish:



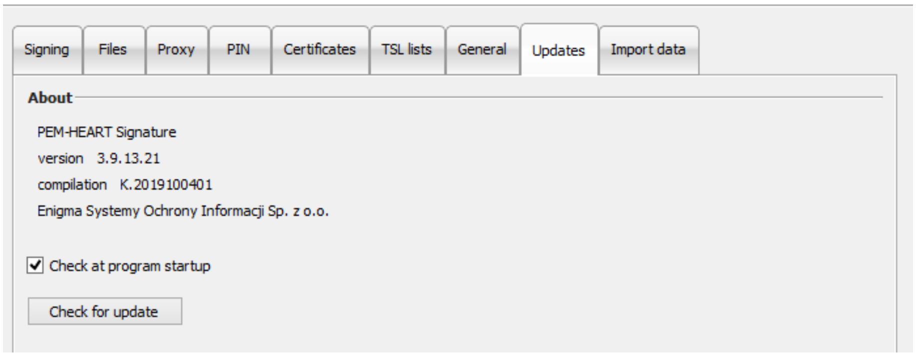
GUI settings

Language english

□ Use built-in file selection dialogs

7.8 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.



About

PEM-HEART Signature
version 3.9.13.21
compilation K.2019100401
Enigma Systemy Ochrony Informacji Sp. z o.o.

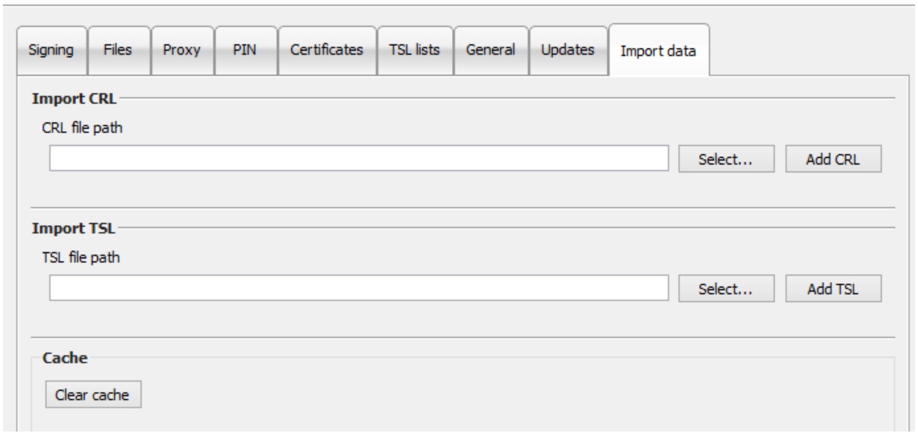
☑ Check at program startup

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 .

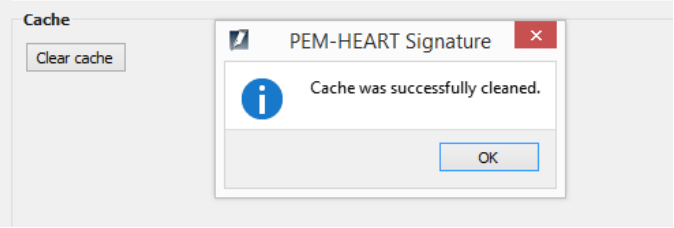
7.9 Import Data

The tab *Import data* is helpful when operating the program in an Internet-less environment. Is 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.



PEM-HEART Signature

Cache was successfully cleaned.

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.

8 Troubleshooting

Troubleshooting:

<table>
<tr><th colspan="4">SIGNING</th></tr>
<tr><th>lp</th><th>Problem</th><th>Cause</th><th>Solution</th></tr>
<tr><td>1.</td><td rowspan="2">No time stamp could be retrieved from any of the servers</td><td>No time stamp package is assigned to the certificate</td><td>- try again the next day (two time stamps per day can be downloaded for free), or
- buy a time stamping package (details: http://www.cencert.pl), or
- disable the option of time stamping signatures (see chapter 3 above)</td></tr>
<tr><td>2.</td><td>The program has no access to the Internet</td><td>- check internet connection
- check the proxy settings (if you use a proxy server) - see chapter 7.3 above)</td></tr>
<tr><td>3.</td><td>Signature failure: To make the next signature, select "Advanced features / add signature"</td><td>The file already contains a signature.</td><td>- add a signature using the "Add signature" command (see chapter 5.4 above)</td></tr>
<tr><th colspan="4">VERIFICATION</th></tr>
<tr><th>lp</th><th>Problem</th><th>Cause</th><th>Solution</th></tr>
<tr><td>1.</td><td>Indicate the location of the documents. Not all disconnected documents were found ....</td><td>The program can't find in the directory with the signature file, the file that was signed.</td><td>Indicate the file that has been signed (corresponding to the signature that is being verified) in the program window.</td></tr>
</table>