Dokumentacja użytkownika
PEM-HEART Signature

ul. Jutrzenki 116, 02-230 Warszawa

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

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

Spis treści

1 Wstęp

Oprogramowanie **PEM-HEART Signature** służy do:

1) składania kwalifikowanych podpisów lub pieczęci elektronicznych w oparciu o certyfikaty wydane przez CenCert,
2) weryfikacji kwalifikowanych podpisów elektronicznych (również podpisów opartych o certyfikaty wydane w innych krajach UE), w okresie ważności certyfikatu.

Jest możliwa także:

- weryfikacja podpisów elektronicznych po zakończeniu okresu ważności certyfikatu, jeśli podpis ma formę archiwalną (patrz opis formy archiwalnej w *Uwagach* w rozdziale 4),
- weryfikacja podpisów opartych o certyfikaty zwykłe (niekwalifikowane) wydane przez CenCert.

2 Bezpieczeństwo produktu

Program powinien być użytkowany na komputerze, który jest pod kontrolą właściciela certyfikatu. Komputer powinien być zabezpieczony przed dostępem przypadkowych osób, posiadać zainstalowane aktualne oprogramowanie antywirusowe oraz bieżące aktualizacje systemu operacyjnego.

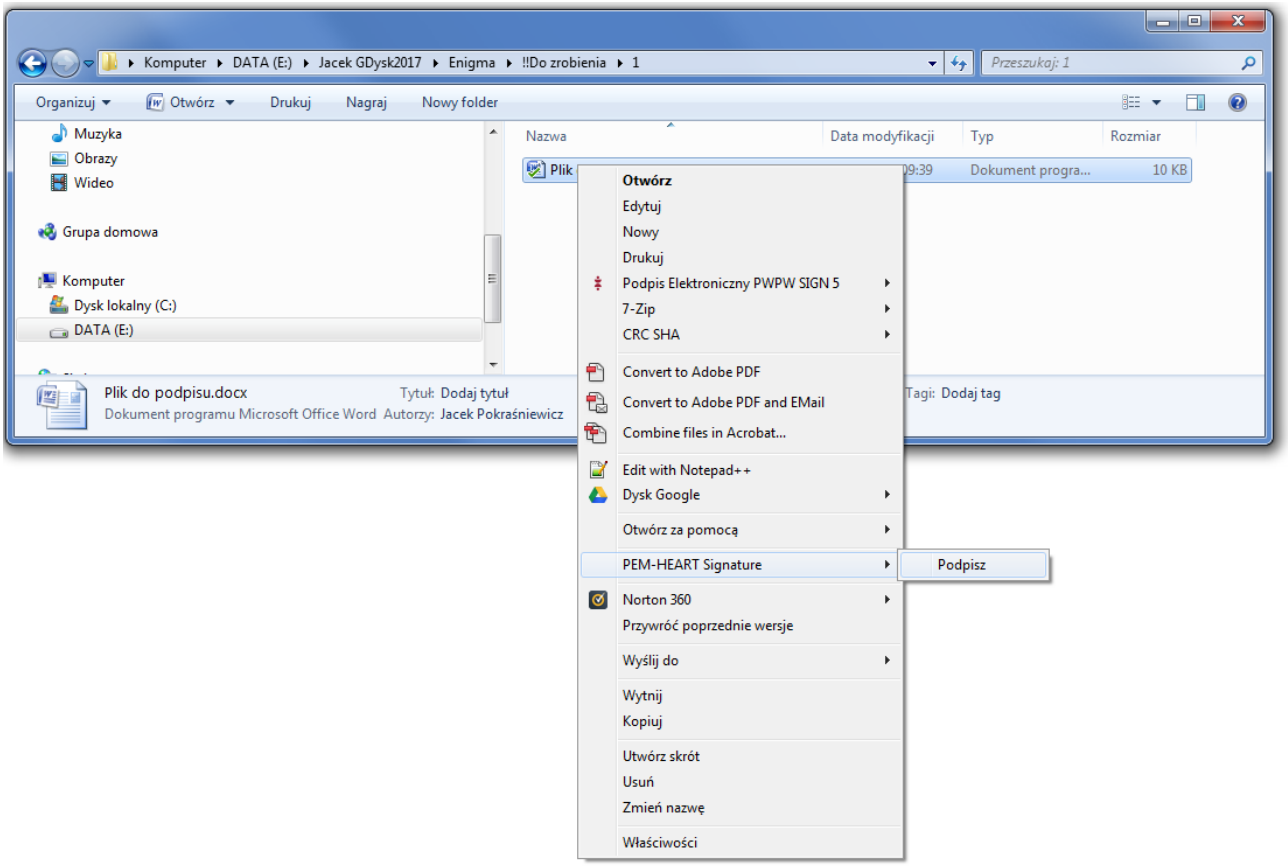
Podpisy elektroniczne nie mogą być składane na komputerach, których bezpieczeństwo nie jest znane (np. komputery dostępne publicznie lub dla szerokiego grana osób, komputery przypadkowych osób itd.).

3 Składanie podpisów

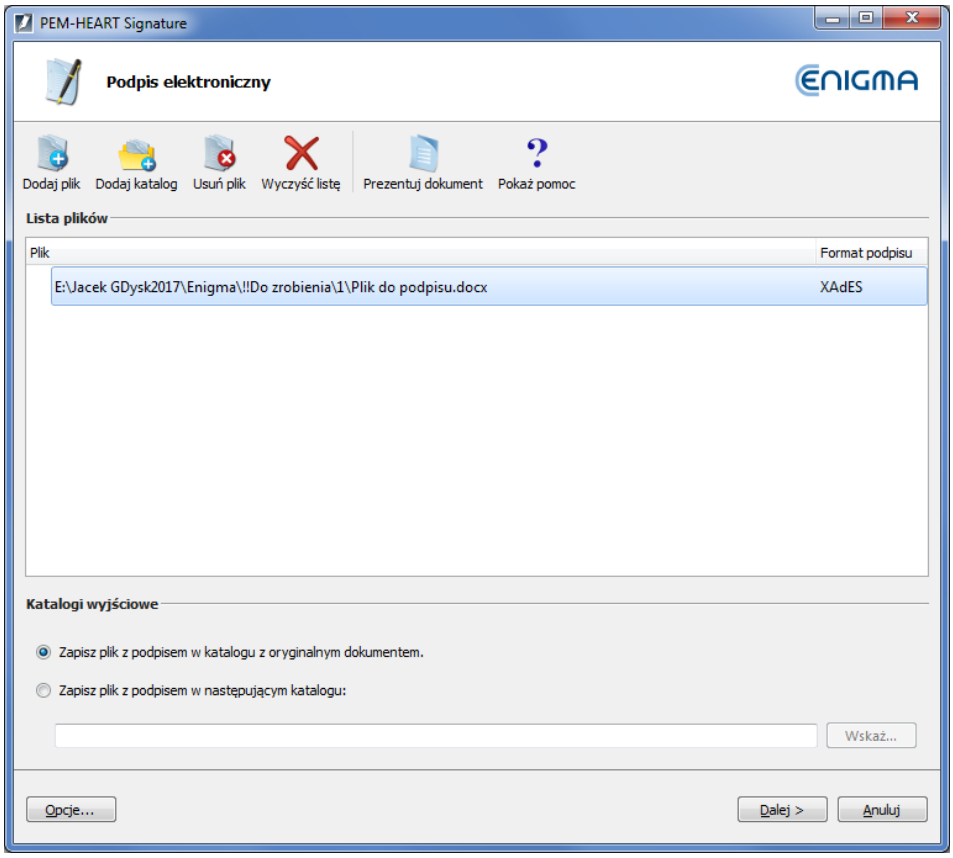
3.1 Składanie podpisów – jeśli używasz podpisu na karcie lub tokenie USB

Jeśli pracujesz na *Mac OS* lub *Linux* - idź do rozdziału 5.2 niżej.

W celu złożenia podpisu włóż swoją kartę CenCert do czytnika (lub token do portu USB), następnie kliknij **prawym** klawiszem myszy na pliku do podpisu, a następnie wybierz z menu polecenie ***PEM-HEART Signature -> Podpisz***.

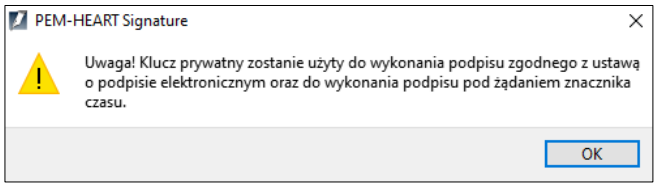


Zostanie wtedy wyświetlone okno podpisu:

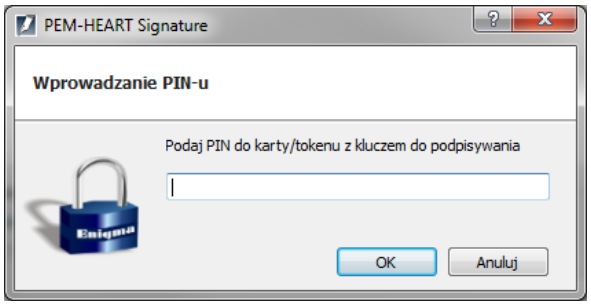


Jeśli format podpisu Ci odpowiada (w tym przypadku XAdES), wciśnij klawisz *Dalej*.

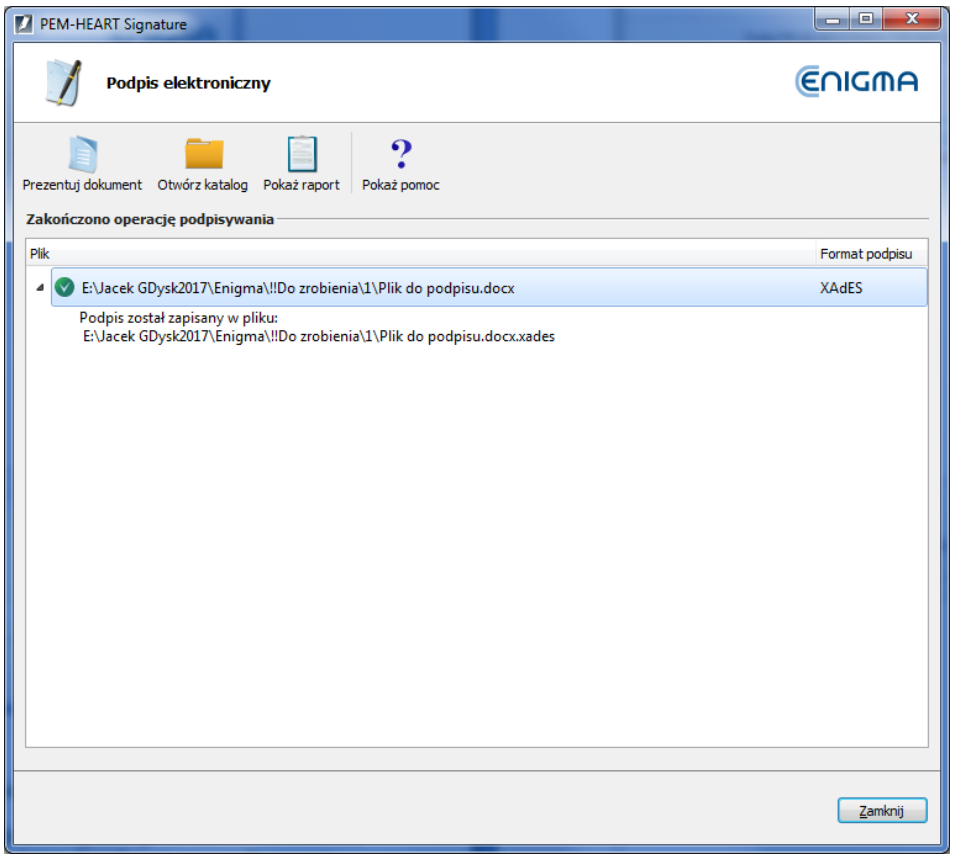
Program ostrzeże o tym, że użyje Twojego klucza do składania podpisów zapisanego na karcie:



Następnie poprosi o PIN do karty:



i wykona podpis:



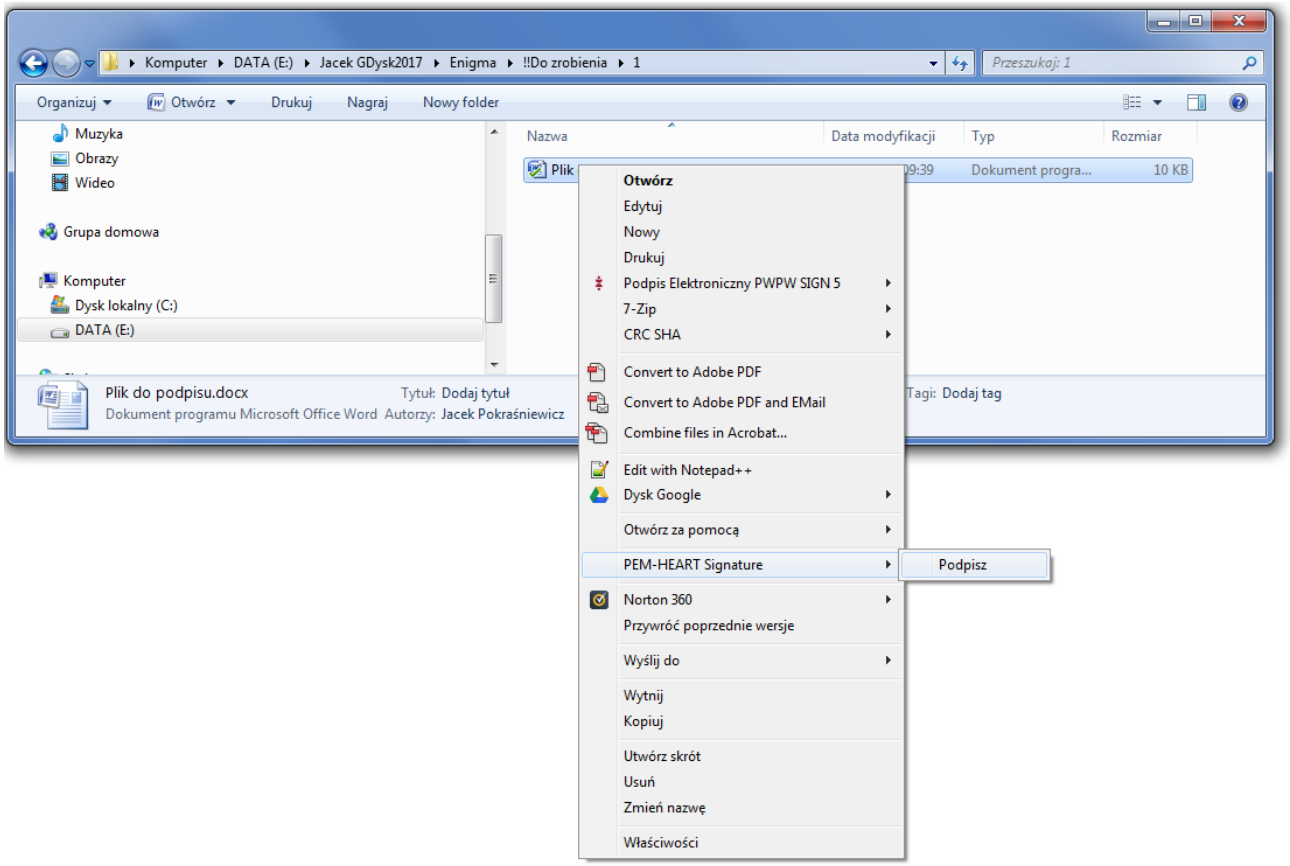
Uwagi:

1) Zaawansowane opcje takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia - są dostępne pod klawiszem *Opcje*. Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział 8.1 niżej.
2) W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
3) W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. W takim przypadku odbiorcy trzeba dostarczyć dwa pliki: plik oryginalny i podpisu.
4) Jeśli podpis ma zawierać znacznik czasu i/lub OCSP, w czasie składania podpisu niezbędne jest połączenie z Internetem. Potrzebne może być także wykupienie usługi znakowania czasem.

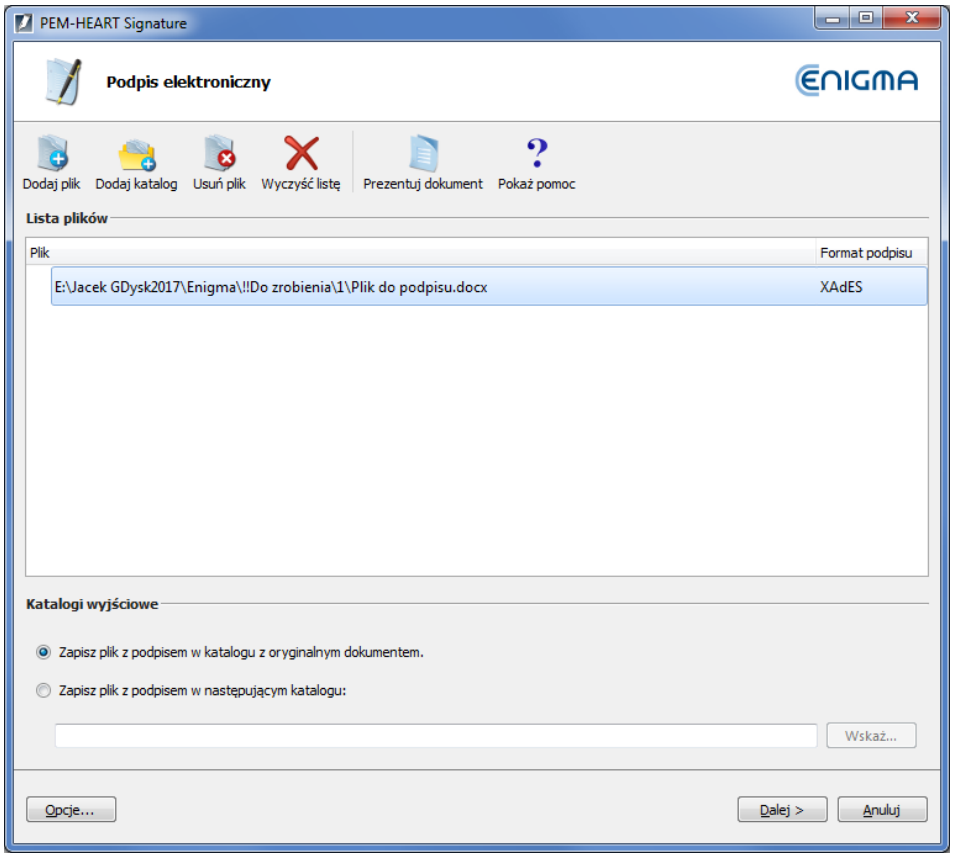
3.2 Składanie podpisów – jeśli używasz podpisu rSign (podpis w chmurze)

Jeśli pracujesz na *Mac OS* lub *Linux* - idź do rozdziału 5.2 niżej.

W celu złożenia podpisu kliknij **prawym** klawiszem myszy na pliku do podpisu, a następnie wybierz z menu polecenie ***PEM-HEART Signature*** -> ***Podpisz***.

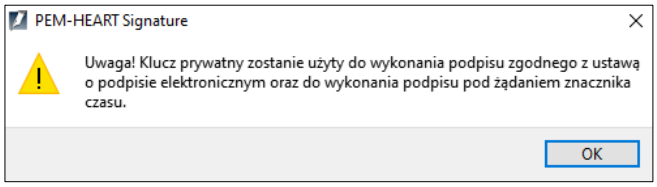


Zostanie wtedy wyświetlone okno podpisu:

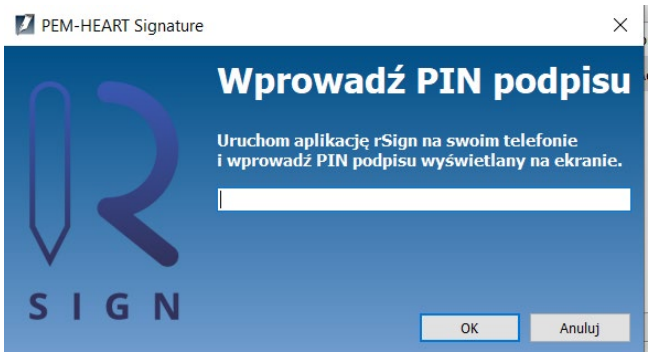


Jeśli format podpisu Ci odpowiada (w tym przypadku XAdES), wciśnij klawisz *Dalej*.

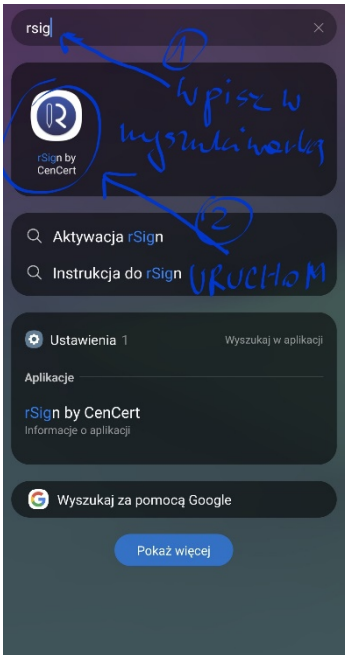
Program ostrzeże o tym, że użyje Twojego klucza do składania podpisów:



Następnie poprosi o PIN do podpisu:

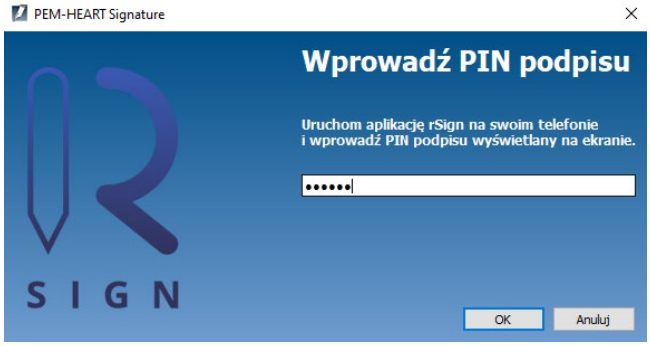


Teraz musisz uruchomić aplikację *rSign by CenCert* na telefonie komórkowym:

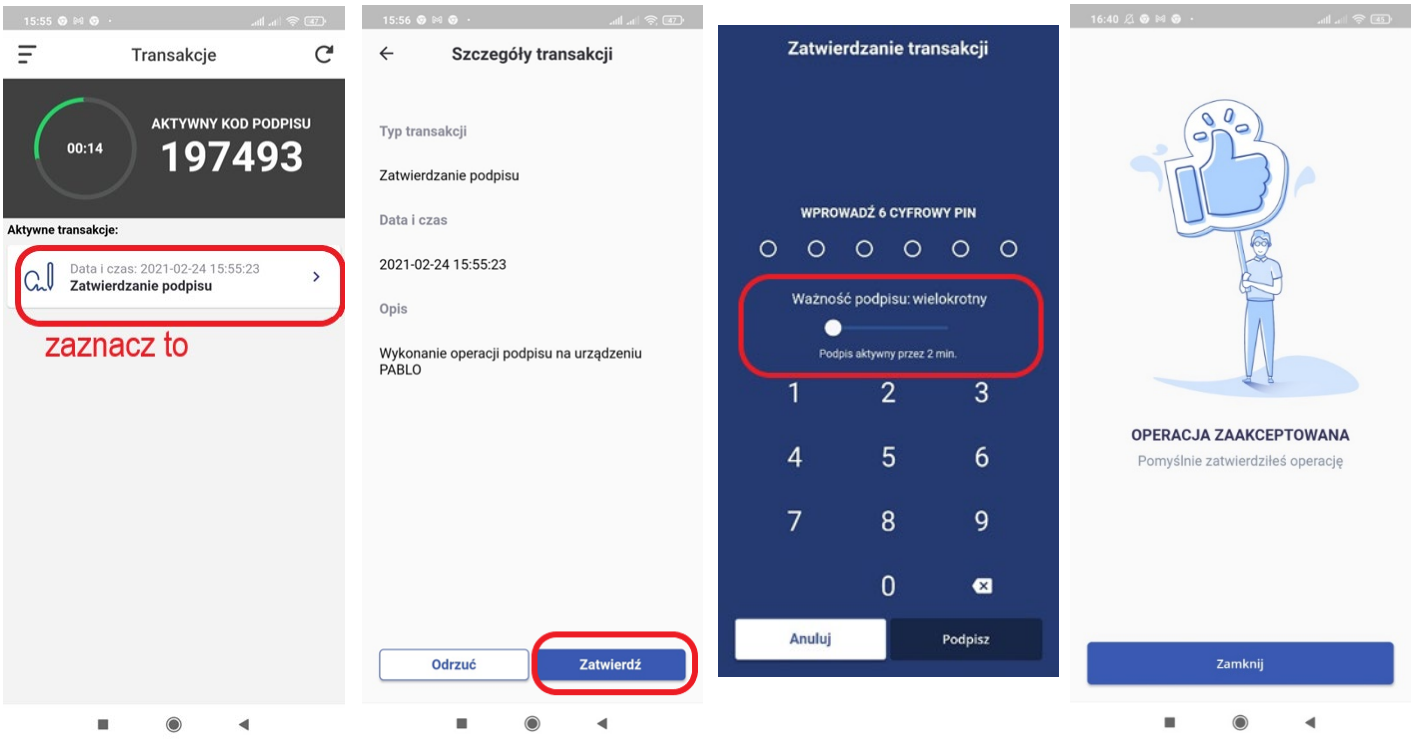


Po uruchomieniu aplikacji na telefonie, odczytaj z ekranu PIN do podpisu:

przepisz PIN podpisu do aplikacji na komputerze i kliknij *OK*

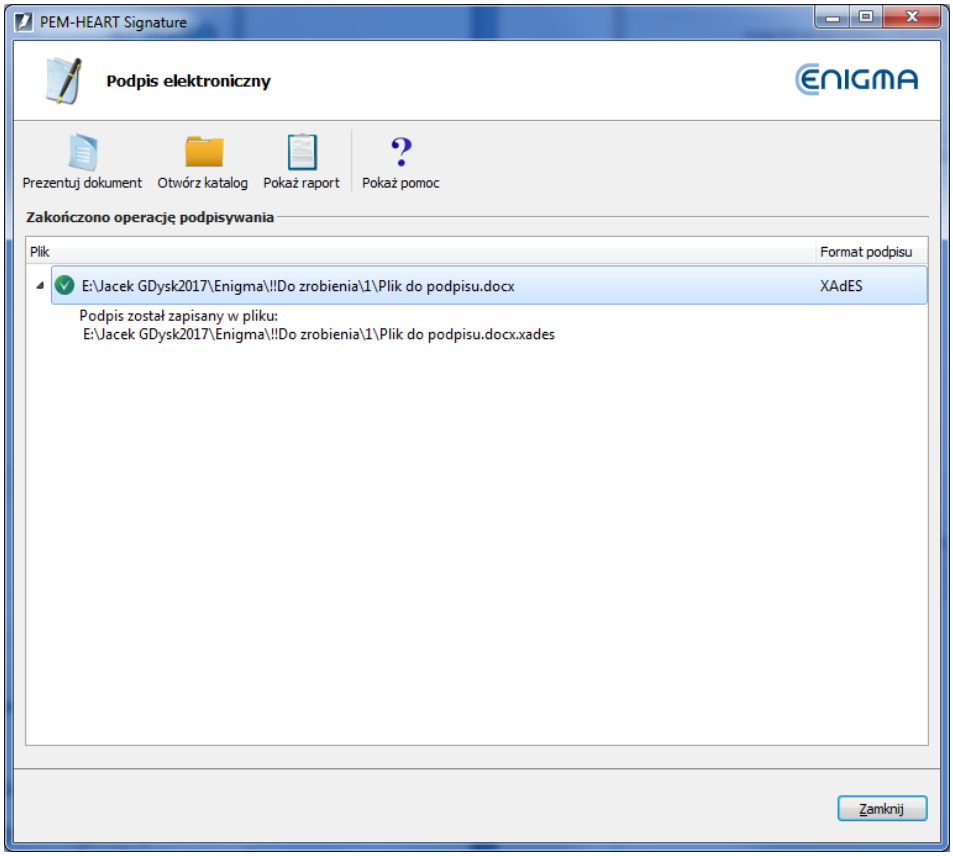


Teraz musisz zatwierdzić zamiar złożenia podpisu, na telefonie komórkowym (w aplikacji rSign):



Uwaga! Zalecamy ustawienie parametru *Ważność podpisu* na *wielokrotny*, z czasem nieaktywności rzędu 2 minuty. Pozwoli to na złożenie podpisu ze znakowaniem czasem albo nawet wielu podpisów (jeśli w programie wskazano wiele plików do podpisu), bez konieczności zatwierdzania każdej operacji podpisu na telefonie. Jeśli ustawisz podpis na jednokrotny – wykonanie podpisu ze znacznikiem czasu będzie wymagać podwójnego zatwierdzenia podpisu na telefonie (podpis pod dokumentem, podpis pod żądaniem znakowania czasem)

Po zatwierdzeniu operacji na telefonie program wykona podpis:



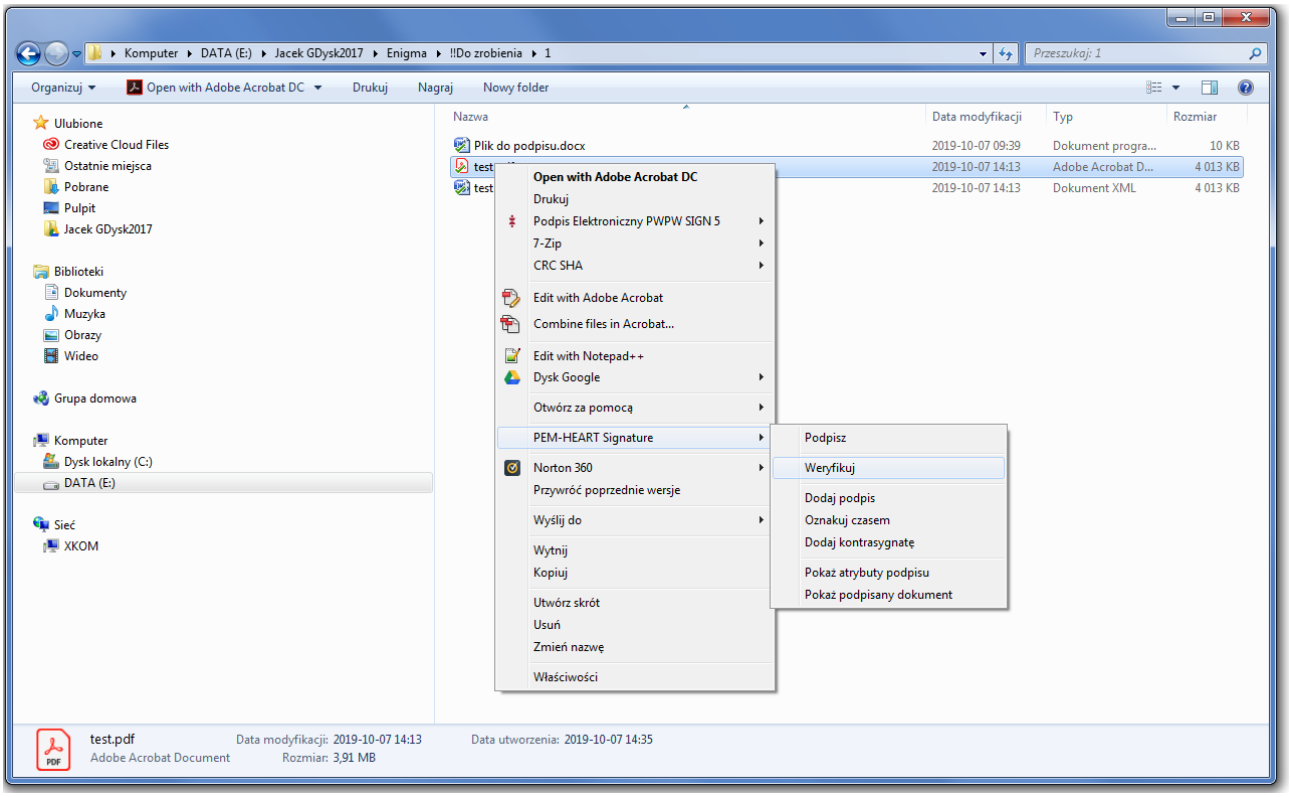
Uwagi:

1) Zaawansowane opcje takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia - są dostępne pod klawiszem *Opcje*. Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział 8.1 niżej.
2) W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
3) W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. W takim przypadku odbiorcy trzeba dostarczyć dwa pliki: plik oryginalny i podpisu.
4) W czasie składania podpisu niezbędne jest połączenie z Internetem.

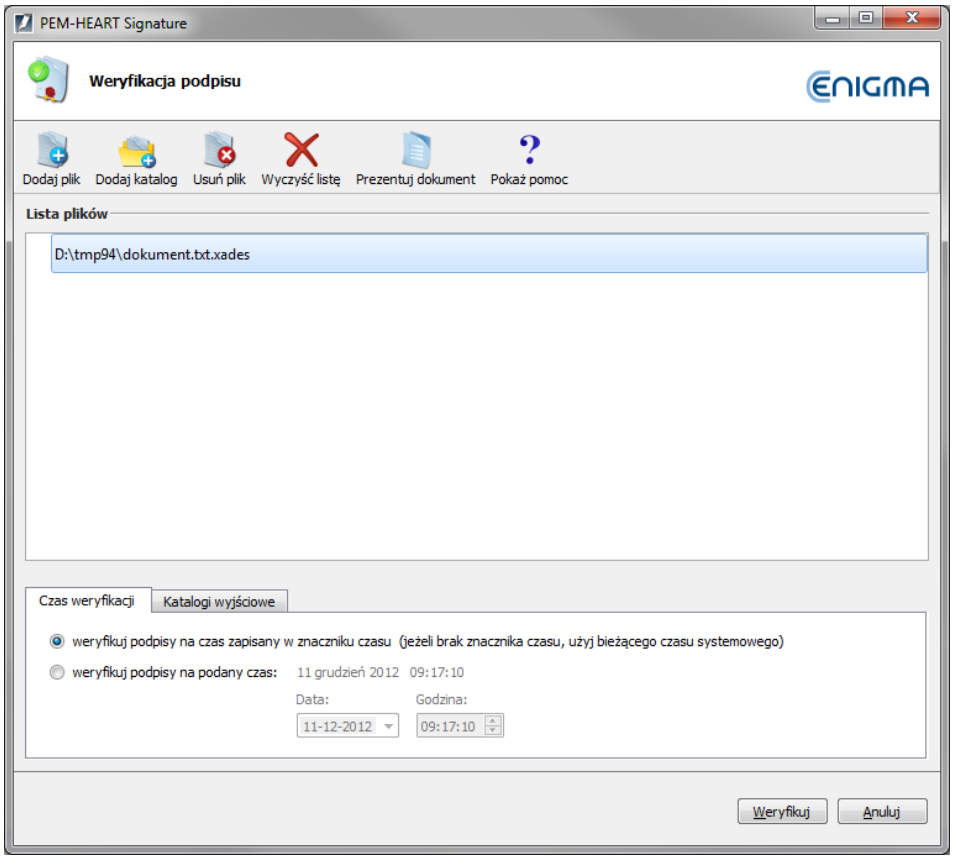
4 Weryfikacja podpisu

Jeśli pracujesz na *Mac OS* lub *Linux* - idź do rozdziału 0 niżej.

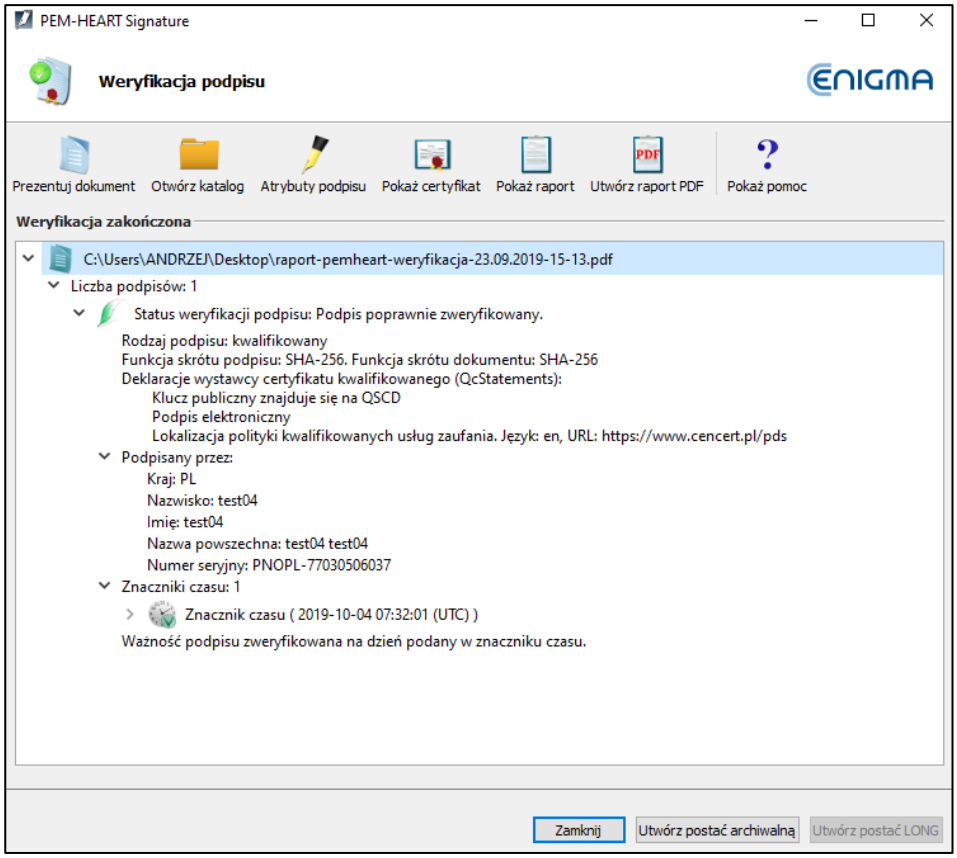
W celu weryfikacji podpisu kliknij **prawym** klawiszem myszy na pliku do podpisu, a następnie wybierz polecenie ***PEM-HEART Signature*** -> ***Weryfikuj***.



Zostanie wtedy wyświetlone okno weryfikacji podpisu:



Wciśnij klawisz *Weryfikuj*. Program zweryfikuje podpisy zapisane w dokumencie i wyświetli rezultat weryfikacji:



Jeśli podpis został oznaczony znacznikiem czasu - moment, na który weryfikowany jest podpis, jest pobierany ze znacznika czasu (a więc ewentualne późniejsze unieważnienie certyfikatu nie wpłynie na wynik weryfikacji takiego podpisu).

Jeśli podpis nie posiada znacznika czasu - podpis jest weryfikowany na moment bieżący lub na inny moment wpisany ręcznie do programu ("weryfikuj na podany czas:...."). W przypadku ręcznego wpisywania momentu, na który weryfikowany jest podpis, odpowiedzialność za to, że ten czas jest prawidłowy (i ewentualnie możliwy do udowodnienia) leży w całości po stronie użytkownika.

Wynik weryfikacji oznaczany jest kolorowymi symbolami dla wyraźnego jego odróżnienia:

- Kolor zielony oznacza poprawną weryfikację podpisu.
- Kolor żółty oznacza niekompletną weryfikację - podpis jest matematycznie poprawny, ale jeszcze nie ma możliwości potwierdzenia, czy w chwili składania podpisu certyfikat był ważny. W takim przypadku należy powtórzyć weryfikację później - np. za kilka godzin lub następnego dnia.
- Kolor czerwony oznacza niepowodzenie weryfikacji podpisu (np. matematyczna niezgodność, czyli naruszenie integralności dokumentu albo też stwierdzenie, że certyfikat jest nieważny).

Uwagi:

1) Po weryfikacji podpisu, w menu górnym, są dostępne różne czynności dodatkowe, w tym:
    a. *Utwórz raport PDF* - zapisanie na dysku czytelnego raportu (w formacie PDF) potwierdzającego weryfikację podpisu.
    b. *Pokaż certyfikat* - wyświetlenie certyfikatu z danymi osoby, która podpisała dokument.
    c. *Prezentuj dokument* - wyświetlenie oryginalnego (podpisanego) dokumentu, jeśli w systemie jest zainstalowany program służący do wyświetlania danego typu dokumentów.
    d. *Atrybuty podpisu* - dodatkowe dane dołączone do podpisu.
    e. *Otwórz katalog* – otwiera widok katalogu na dysku, w którym zapisany jest dokument.
2) Po poprawnej weryfikacji podpisu, można utworzyć zaawansowane formy podpisu[1]:
    a. *Postać archiwalną* - zabezpieczającą możliwość poprawnej weryfikacji podpisu na okres ważności znacznika czasu (praktycznie ok. 7-10 lat). Utworzenie formy archiwalnej wymaga dostępu do Internetu i pobrania m.in. dwóch znaczników czasu. Konieczne może być wykupienie pakietu znaczników czasu.

       Ważność archiwalnej formy podpisu może być dowolną liczbę razy przedłużana (poprzez dołożenie kolejnego znacznika czasu), każdorazowo na następne 7-10 lat.
    b. *Postać long* - zabezpieczającą możliwość poprawnej weryfikacji podpisu na okres ważności OCSP i znacznika czasu (praktycznie ok. 5-10 lat). Utworzenie postaci *long* wymaga dostępu do Internetu i pobrania m.in. znacznika czasu. Konieczne może być wykupienie pakietu znaczników czasu.

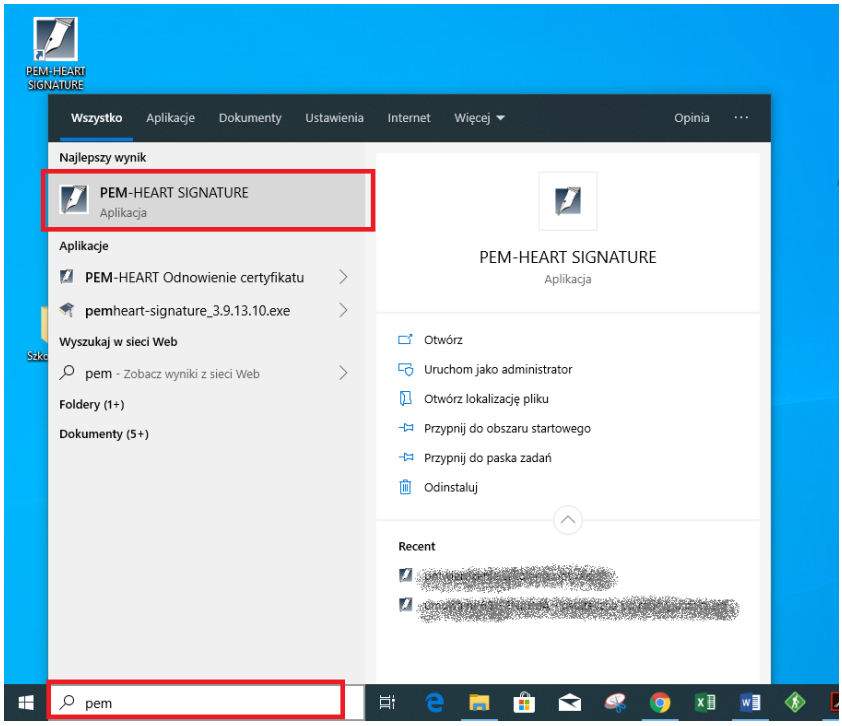
[1] W formacie podpisu PAdES nie jest możliwe dodanie do podpisu znacznika czasu, jeśli nie został dodany od razu przy składaniu podpisu

5 Praca w oknie programu

5.1 Uruchomienie programu

Wszystkie funkcje programu (również podpisywanie i weryfikacja podpisów) są dostępne po uruchomieniu programu ***PEM-HEART Signature*** z menu Start (Windows) lub z ikony na pulpicie. W innych systemach operacyjnych należy uruchomić program w sposób odpowiedni dla danego systemu. Wygląd programu jest taki sam, jak w systemie Windows.

Przykład uruchomienia programu z menu *Start* systemu Windows.



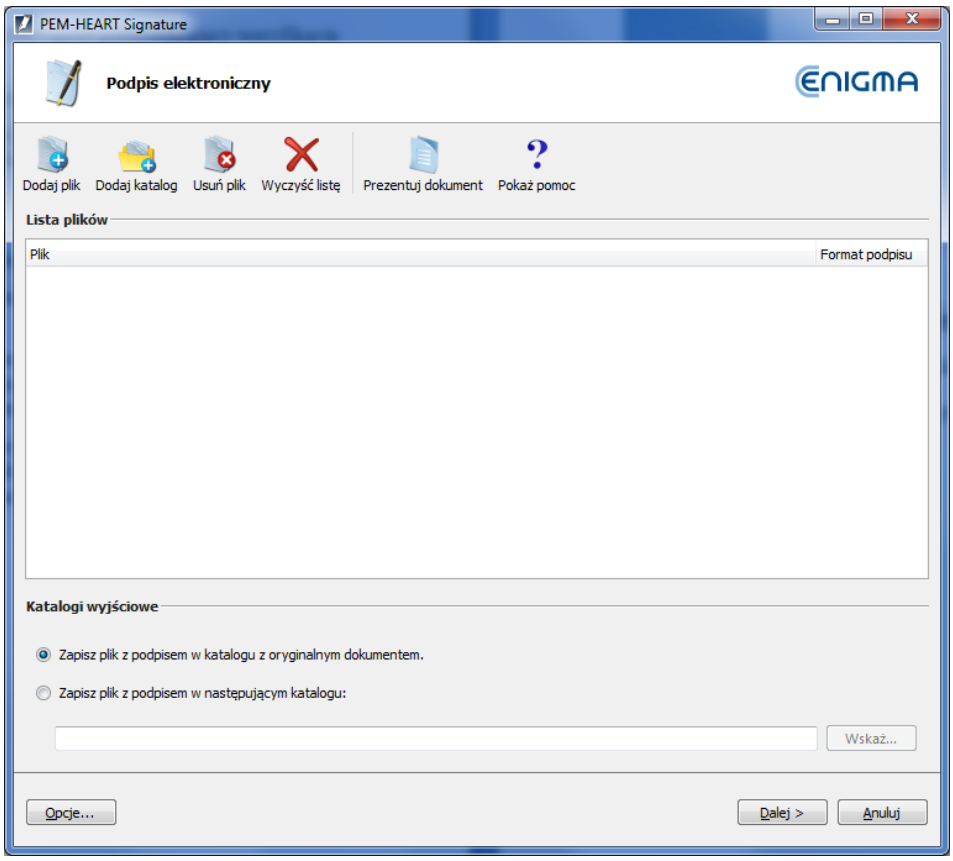
Po uruchomieniu aplikacji zostanie wyświetlone okno jak poniżej:

5.2 Składanie podpisu w oknie programu

5.2.1 Składanie podpisu w oknie programu – jeśli używasz podpisu na karcie lub tokenie USB

W celu złożenia podpisu - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wciśnij ikonę *Podpisz* (menu po lewej stronie).

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do podpisu:

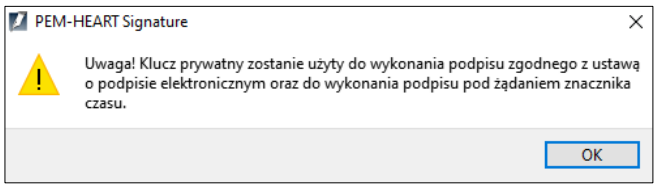


Dodaj plik lub pliki które mają zostać podpisane (klawisz *Dodaj plik*).

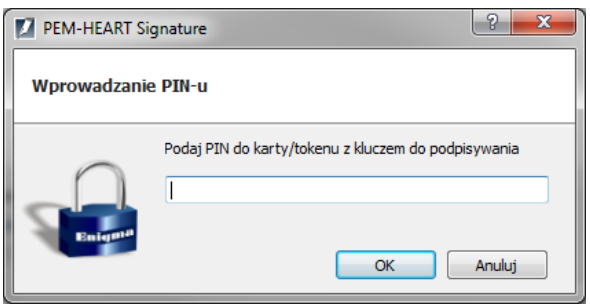
Jeśli wskażesz cały katalog (klawisz *Dodaj katalog),* to program na listę plików do podpisu wstawi wszystkie plików z tego katalogu i jego podkatalogów.

Po dodaniu wszystkich plików do podpisu, wciśnij klawisz *Dalej.*

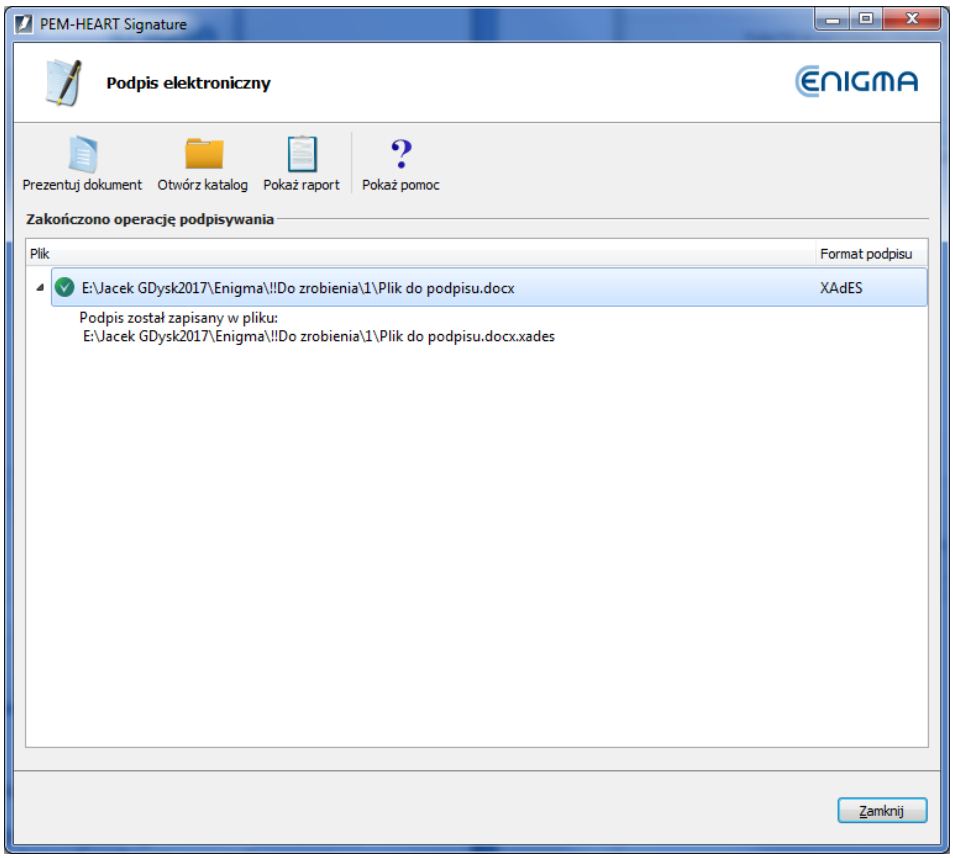
Program ostrzeże o tym, że użyje Twojego klucza do składania podpisów zapisanego na karcie:



Następnie poprosi o PIN do karty:



i wykona podpis:



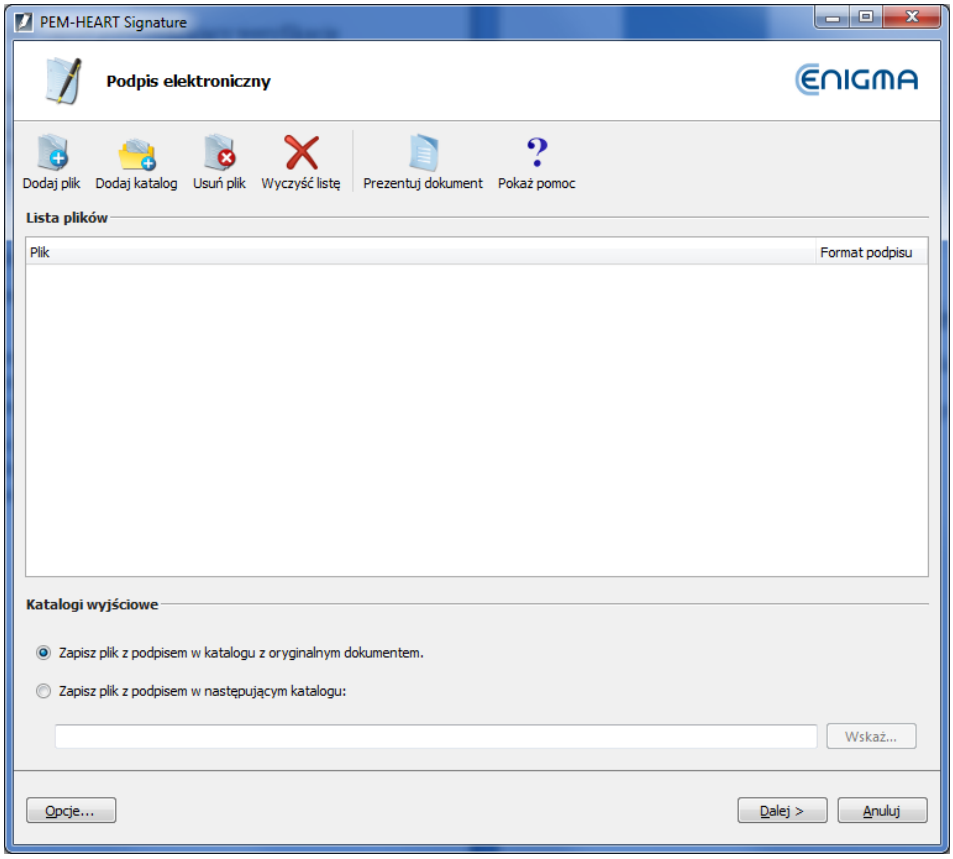
Uwagi:

1) Zaawansowane opcje takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia - są dostępne pod klawiszem *Opcje*. Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział 8.1 niżej.
2) W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
3) W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. W takim przypadku odbiorcy trzeba dostarczyć dwa pliki: plik oryginalny i podpisu.
4) Jeśli podpis ma zawierać znacznik czasu i/lub OCSP, w czasie składania podpisu niezbędne jest połączenie z Internetem. Potrzebne może być także wykupienie usługi znakowania czasem.

5.2.2 Składanie podpisu w oknie programu – – jeśli używasz podpisu rSign (podpis w chmurze)

W celu złożenia podpisu - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wciśnij ikonę *Podpisz* (menu po lewej stronie).

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do podpisu:

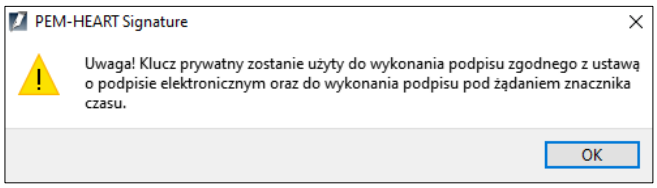


Dodaj plik lub pliki które mają zostać podpisane (klawisz *Dodaj plik*).

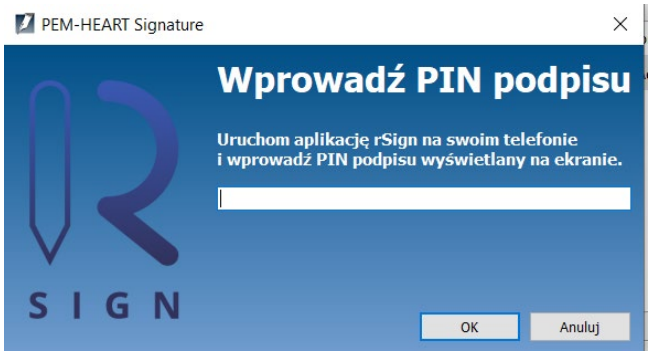
Jeśli wskażesz cały katalog (klawisz *Dodaj katalog),* to program na listę plików do podpisu wstawi wszystkie plików z tego katalogu i jego podkatalogów.

Po dodaniu wszystkich plików do podpisu, wciśnij klawisz *Dalej.*

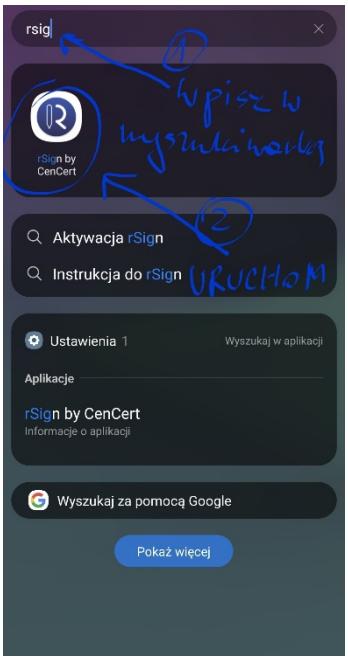
Program ostrzeże o tym, że użyje Twojego klucza do składania podpisów zapisanego na karcie:



Następnie poprosi o PIN do podpisu:

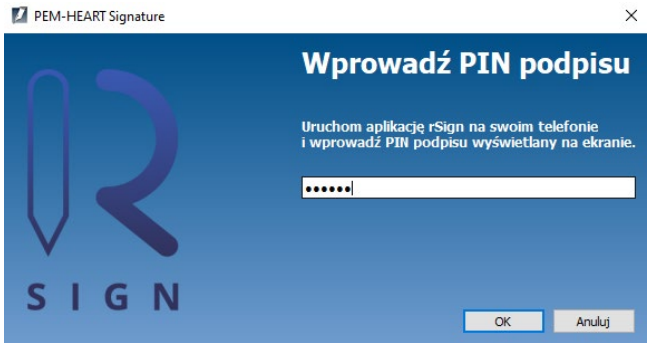


Teraz musisz uruchomić aplikację *rSign by CenCert* na telefonie komórkowym:

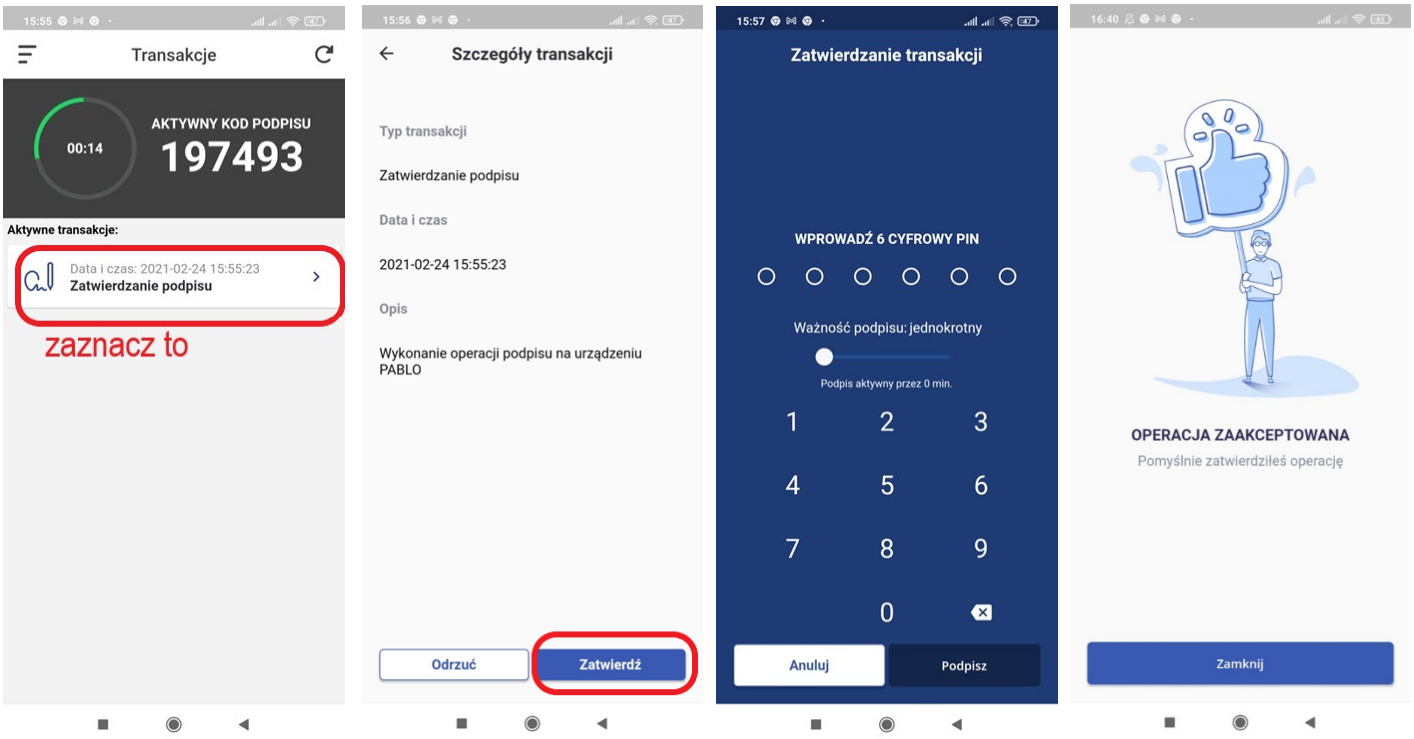


Po uruchomieniu aplikacji na telefonie, odczytaj z ekranu PIN do podpisu:

przepisz PIN podpisu do aplikacji na komputerze i kliknij *OK*

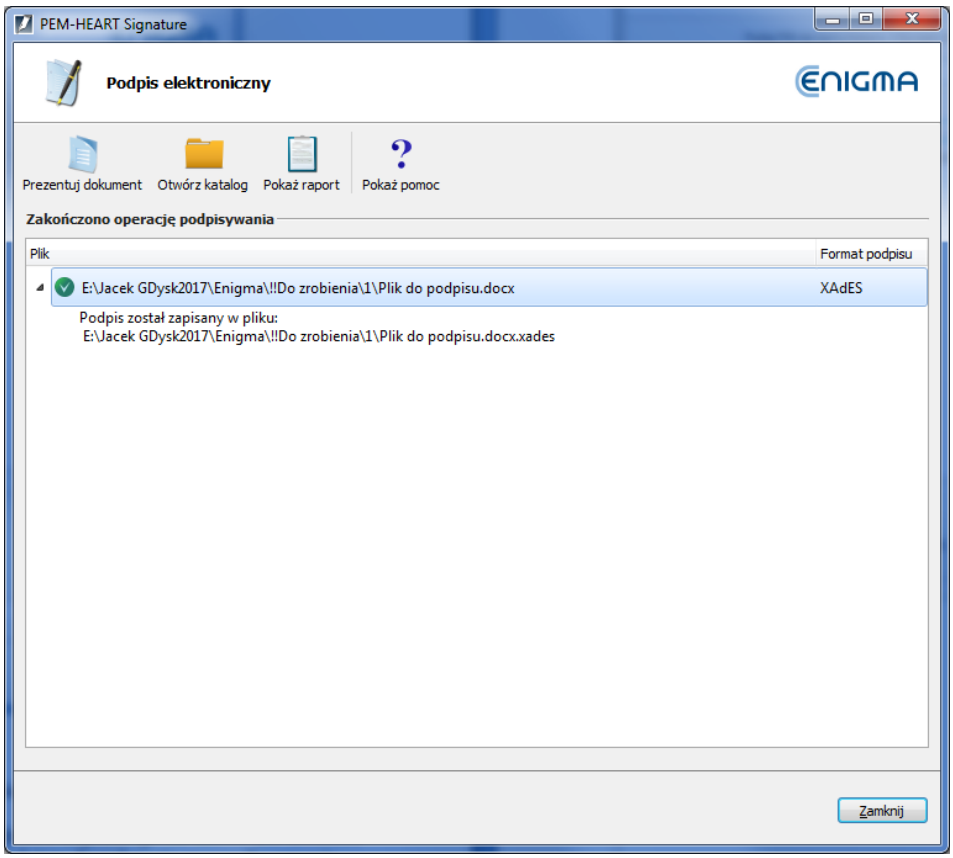

PEM-HEART Signature
Wprowadź PIN podpisu
Uruchom aplikację rSign na swoim telefonie
i wprowadź PIN podpisu wyświetlany na ekranie.
SIGN
OK
Anuluj

Teraz musisz zatwierdzić zamiar złożenia podpisu, na telefonie komórkowym (w aplikacji rSign):



Uwaga! Zalecamy ustawienie parametru *Ważność podpisu* na *wielokrotny*, z czasem nieaktywności rzędu 2 minuty. Pozwoli to na złożenie podpisu ze znakowaniem czasem albo nawet wielu podpisów (jeśli w programie wskazano wiele plików do podpisu), bez konieczności zatwierdzania każdej operacji podpisu na telefonie. Jeśli ustawisz podpis na jednokrotny – wykonanie podpisu ze znacznikiem czasu będzie wymagać podwójnego zatwierdzenia podpisu na telefonie (podpis pod dokumentem, podpis pod żądaniem znakowania czasem)

Po zatwierdzeniu operacji na telefonie program wykona podpis:



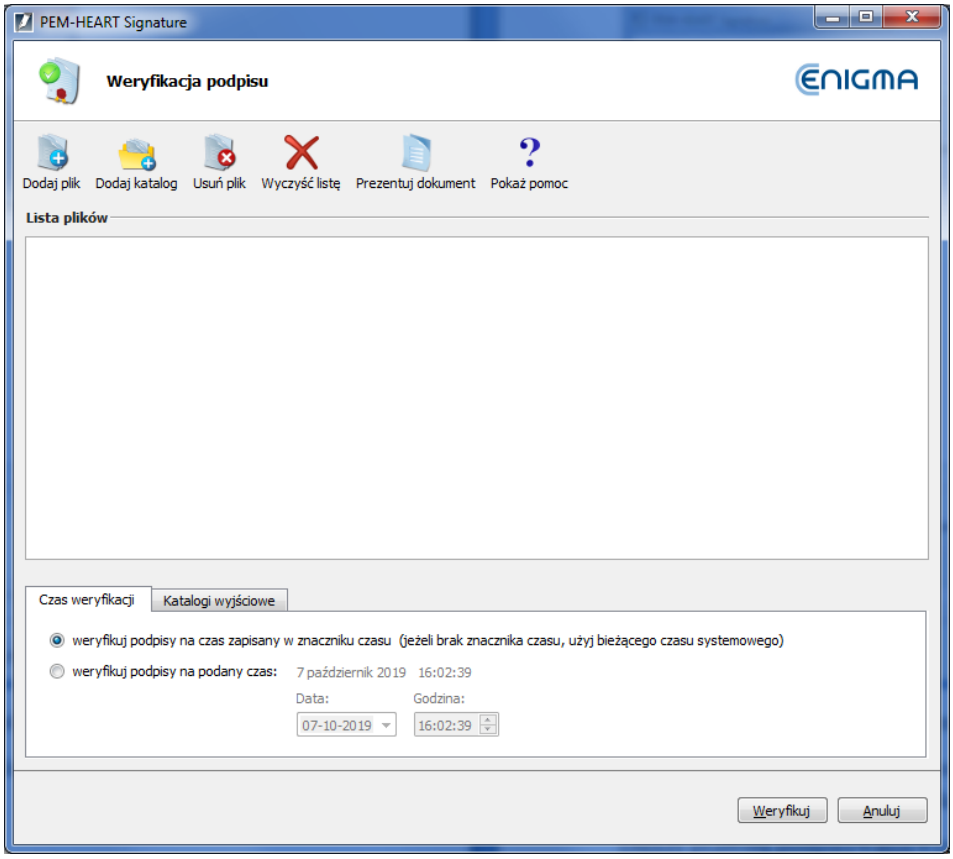
Uwagi:

1) Zaawansowane opcje takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia - są dostępne pod klawiszem *Opcje*. Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział 8.1 niżej.
2) W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
3) W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. W takim przypadku odbiorcy trzeba dostarczyć dwa pliki: plik oryginalny i podpisu.
4) W czasie składania podpisu niezbędne jest połączenie z Internetem.

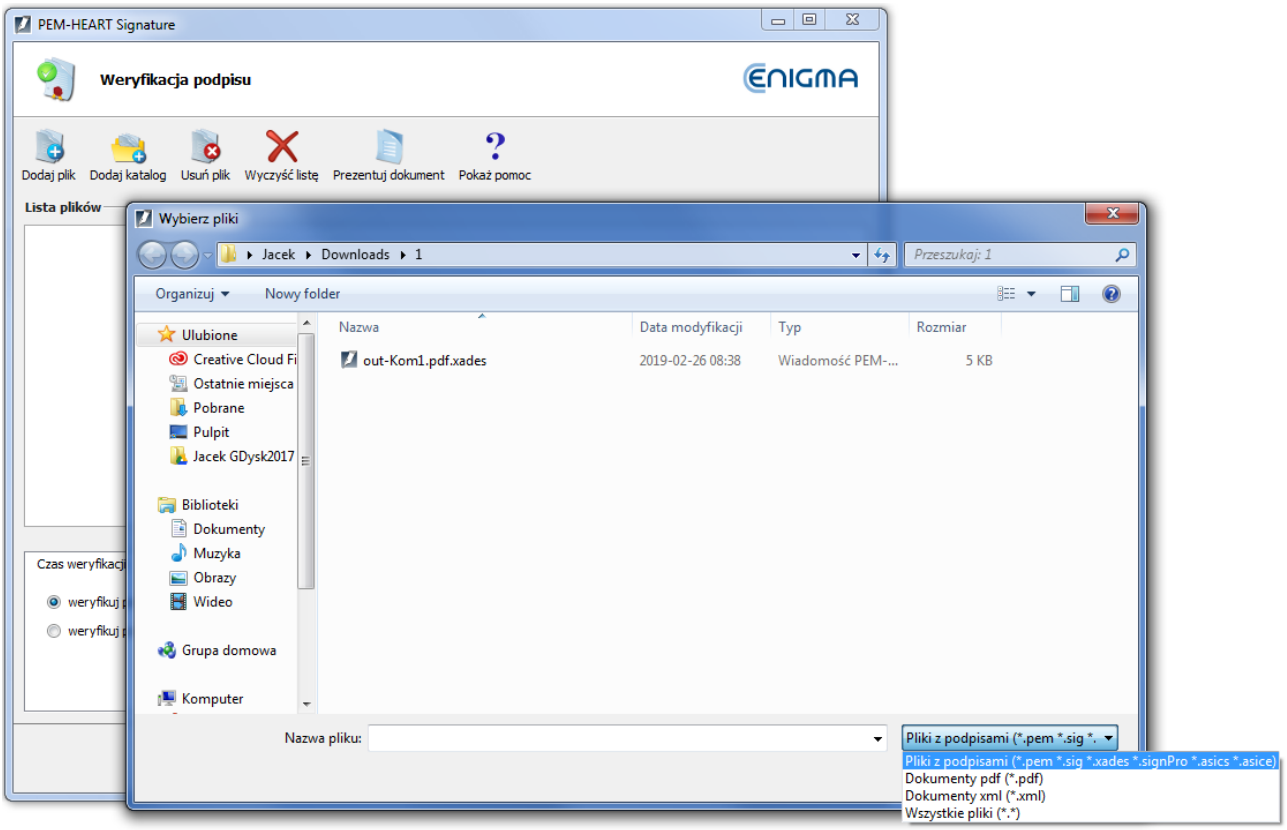
5.3 Weryfikacja podpisu

W celu weryfikacji podpisu - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wciśnij ikonę *Weryfikuj* (menu po lewej stronie okna głównego).

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do weryfikacji:

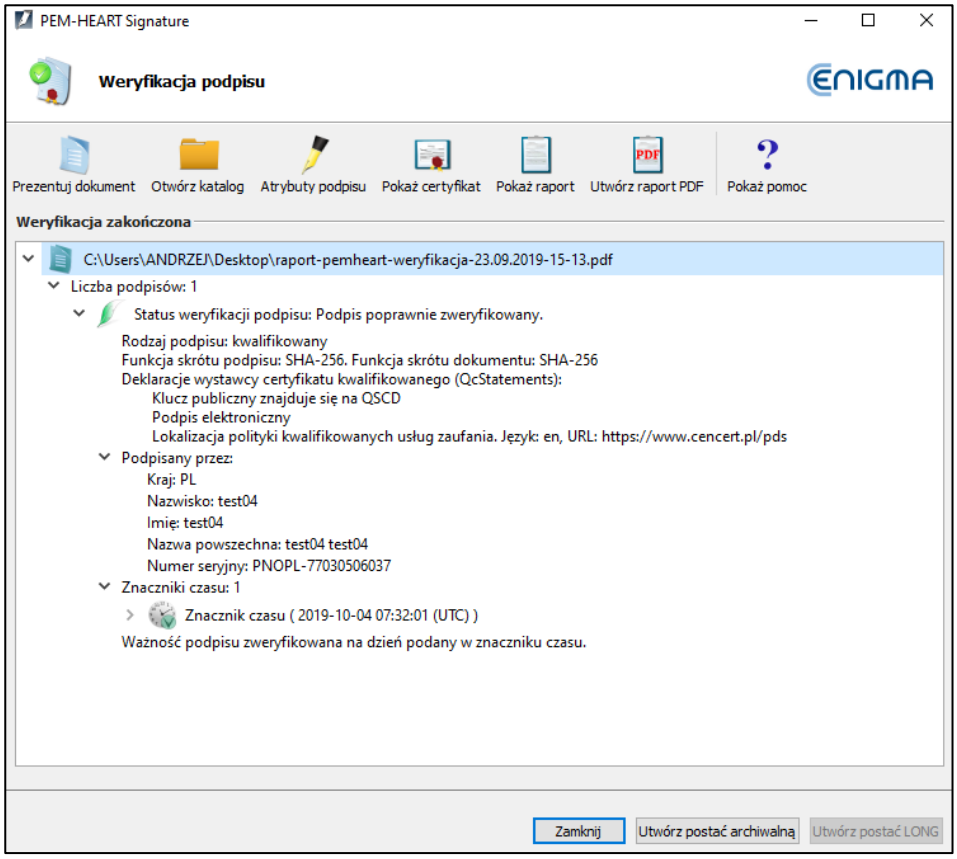


Teraz dodaj plik lub pliki do weryfikacji (klawisz *Dodaj plik*). W razie potrzeby możesz zmienić filtr rozszerzeń nazw plików (np. na "*.*"):



Wskazanie katalogu (klawisz *Dodaj katalog)* spowoduje dodanie do listy wszystkich plików z tego katalogu i jego podkatalogów.

Wciśnij klawisz *Weryfikuj*. Program zweryfikuje podpisy zapisane w dokumencie i wyświetli rezultat weryfikacji:



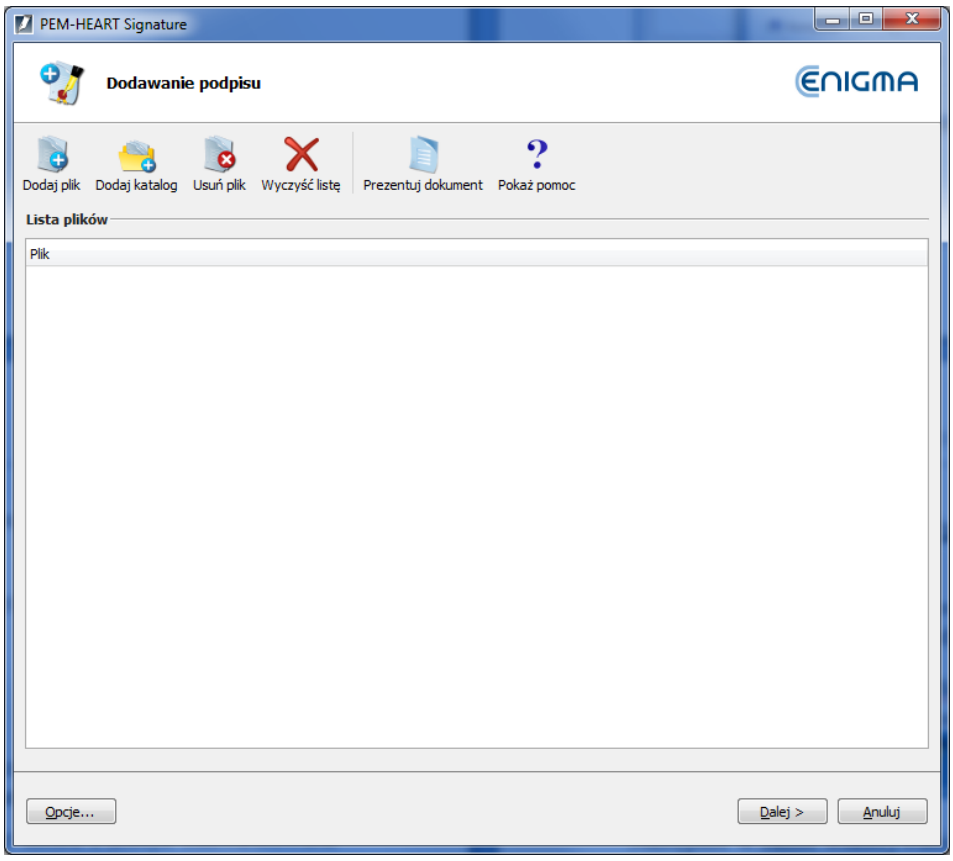
Patrz też uwagi dotyczące weryfikacji w rozdziale 4 wyżej.

5.4 Dodawanie następnego podpisu

Dokument, który został już podpisany, może być dodatkowo podpisany przez tę samą lub inną osobę. Dla każdego następnego podpisu program automatycznie wybiera taki sam format, jaki ma pierwszy podpis.

W celu dodania następnego podpisu - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wybierz menu *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wciśnij ikonę *Dodaj podpis*.

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do podpisu:



Wskazanie katalogu (klawisz *Dodaj katalog)* spowoduje dodanie do listy plików do podpisu wszystkich plików z tego katalogu i jego podkatalogów.

Dalszy przebieg podpisywania wygląda jak opisano w rozdziale 5.2 wyżej.

Uwagi:

1) W przypadku formatu podpisu XAdES, sposób umieszczenia wielu podpisów w jednym dokumencie nie jest jednoznacznie opisany w normach. Z tego względu - zwłaszcza w przypadku gdy podpisy są składane przez oprogramowanie pochodzące od różnych producentów, mogą się zdarzyć różne błędy zgodności formatów - np. dodanie następnego podpisu może zniszczyć możliwość weryfikacji podpisu poprzedniego. Z tego względu zalecamy wykonanie próby weryfikacji podpisów po dodaniu kolejnego podpisu w formacie XAdES do pliku XML.

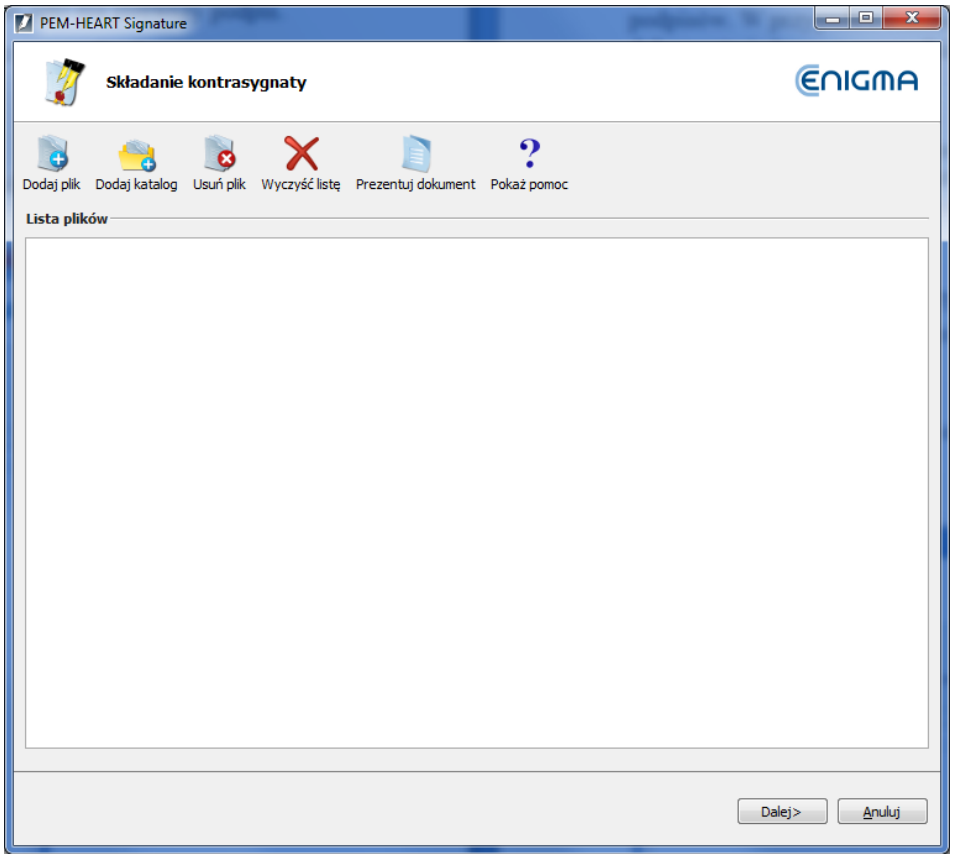
5.5 Kontrasygnata

Kontrasygnatą nazywamy specjalny sposób składania podpisu polegający na tym, że podpis jest technicznie składany nie tyle pod samym dokumentem, ile pod poprzednimi podpisami (dokument jest podpisywany w sposób pośredni). Taka realizacja podpisu zabezpiecza przed usunięciem z dokumentu poprzednich podpisów. W przypadku standardowych podpisów wielokrotnych może być technicznie możliwe usunięcie z dokumentu jednego z poprzednich podpisów, przy zachowaniu ważności podpisów pozostałych („kontrasygnata” powoduje, że staje się to niemożliwe).

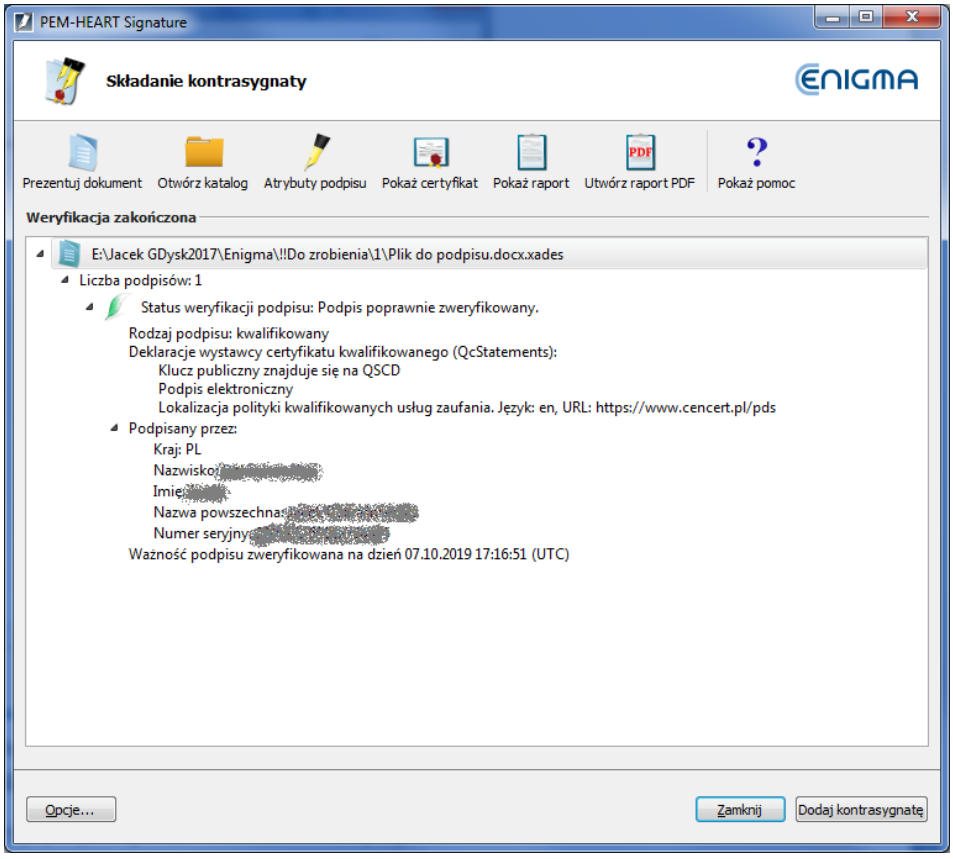
Terminu "kontrasygnata" w znaczeniu powyższym nie należy mylić z takim samym terminem funkcjonującym w obiegu prawnym. Złożenie podpisu elektronicznego jako "kontrasygnaty" (w sensie opisanym powyżej) nie jest umocowane w zapisach prawnych dotyczących podpisów elektronicznych. Zastosowanie mają przepisy dotyczące podpisów elektronicznych w ogólności. W sensie prawnym ta „kontrasygnata” funkcjonuje na takich samych zasadach, jak każdy inny podpis elektroniczny.

W celu złożenia "kontrasygnaty" - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wybierz menu *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wciśnij ikonę *Kontrasygnata*.

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików i/lub katalogów:



Po wskazaniu pliku/plików, weryfikowane są podpisy elektroniczne, po czym program wyświetla status podpisów:



Po wciśnięciu klawisza *Dodaj kontrasygnatę,* program prosi o PIN do karty i dodaje podpis w formie "kontrasygnaty".

5.6 Znakowanie czasem

Kwalifikowany znacznik czasu stanowi dowód istnienia dokumentu w danym momencie. W polskim prawie czynność prawna opatrzona kwalifikowanym znacznikiem czasu ma "datę pewną". W całej UE (na podstawie rozporządzenia *eIDAS*), *kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone.*

W przypadku zastosowania znacznika czasu do podpisu, poświadcza on nie tylko fakt istnienia podpisanego dokumentu, ale też samego podpisu, co zabezpiecza przed skutkami prawnymi późniejszego unieważnienia certyfikatu użytego do podpisu.

Znacznik czasu (za wyjątkiem podpisów w formacie PAdES) może być dołączony do podpisu również później, nawet przez odbiorcę dokumentu (w istocie to odbiorca dokumentu jest często bardziej zainteresowany możliwością długoterminowej poprawnej weryfikacji podpisu). Warto również rozważyć bardziej zaawansowane formy podpisu - to jest *long* oraz *archiwalną* (patrz rozdział 4 wyżej). Formy te również korzystają ze znaczników czasu, ale uzupełniają go o inne dane potrzebne przy weryfikacji.

W celu dodania znaczników czasu do pliku zawierającego podpis - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wybierz menu *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wciśnij ikonę *Znakuj czasem*.

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików i/lub katalogów, jak przy podpisywaniu i weryfikacji podpisu. Po wskazaniu plików i wciśnięciu klawisza *Dalej*, program prosi o PIN do karty (w celu podpisania żądania znakowania czasem), następnie dodaje znacznik czasu do każdego podpisu znajdującego się w tym pliku.

Uwaga:

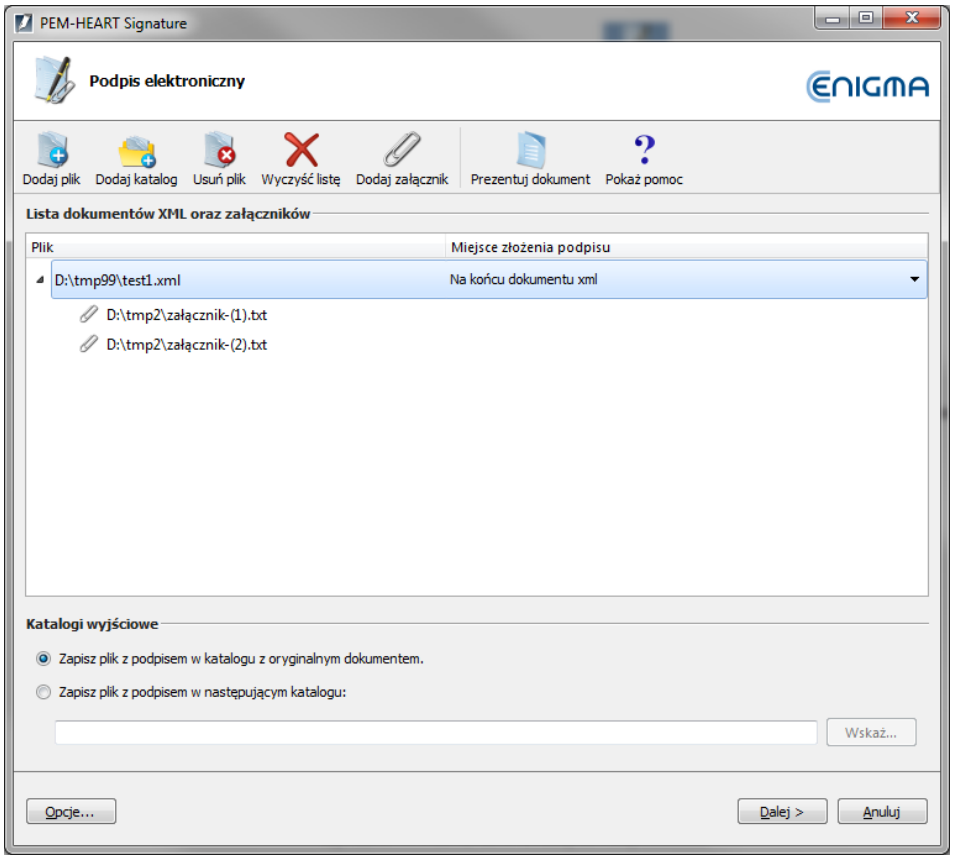
1) Pobieranie znaczników czasu może wymagać wykupienia pakietu znakowania czasem.

5.7 Podpisywanie dokumentu XML z wyborem miejsca w dokumencie

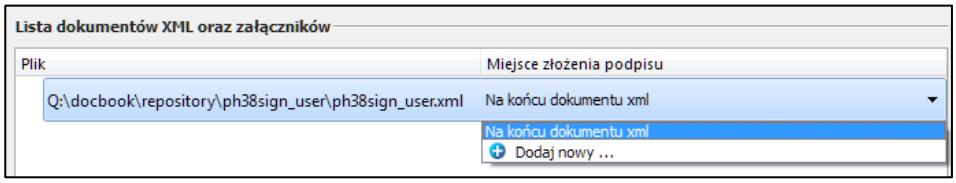
Standardowo, gdy program podpisuje dokument XML podpisem otoczonym (*XAdES enveloped*), umieszcza podpis na końcu struktury dokumentu. W zdecydowanej większości przypadków takie zachowanie programu jest wystarczające i spełnia wymagania systemów wykorzystujących podpisy. Gdyby jednak była potrzeba innego położenia podpisu wewnątrz dokumentu, należy użyć opcji *Podpisz dokument XML z załącznikami*. Użycie tej opcji jest dedykowane dla zaawansowanych użytkowników i wymaga wiedzy na temat budowy plików XML, w szczególności znajomości dokumentacji *XML Pointer Language* (*XPointer*).

W celu złożenia takiego podpisu - po uruchomieniu programu (patrz rozdział 5.1 wyżej) - wybierz menu *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wciśnij ikonę *Podpisz dokument XML z załącznikami.*

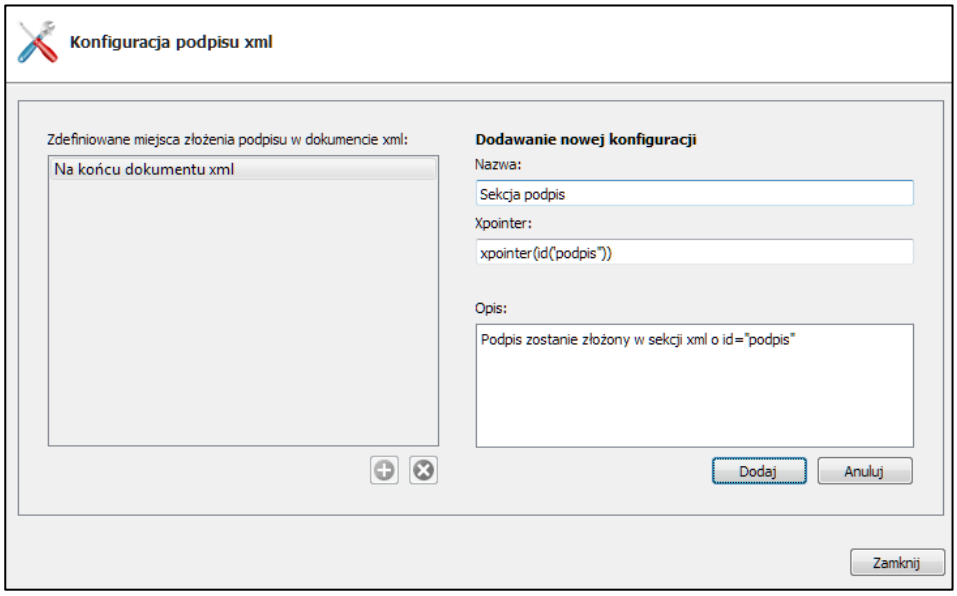
Gdy program wyświetli okno dodawania plików do podpisu, wskaż plik XML (plik może ewentualnie wskazywać na załączniki).



Jeśli podpis ma być złożony w innym miejscu niż koniec pliku, wskaż miejsce odpowiednie miejsce w strukturze dokumentu XML:



Wybierz *Dodaj nowy...,* co spowoduje wyświetlenie okna konfiguracji miejsca składania podpisu:



Kliknij przycisk  , następnie wpisz swoją nazwę konfiguracji, podaj strukturę *xpointer* oraz ewentualnie opis definiowanej konfiguracji. Strukturę *xpointer* określa się w postaci: `xpointer([wskazanie na węzeł XML])`. Dostępne formy określania tego miejsca opisuje dokumentacja języka *XML Pointer Language* (*XPointer*) dostępna m.in. na stronach http://www.w3.org/TR/WD-xptr.

W przedstawionym powyżej na rysunku przykładzie zostanie podpisany dokument XML, a podpis zostanie umieszczony w części o atrybucie *id* o nazwie *podpis*.

Po zakończeniu podpisywania zostanie wyświetlone okno podsumowania:

Składanie podpisu w formacie XAdES otoczony (*XAdES enveloped*) nie zmienia rozszerzenia pliku XML ani jego struktury.

6 Obsługa kart kryptograficznych

Program umożliwia uproszczoną obsługę kart procesorowych wydawanych przez CenCert.

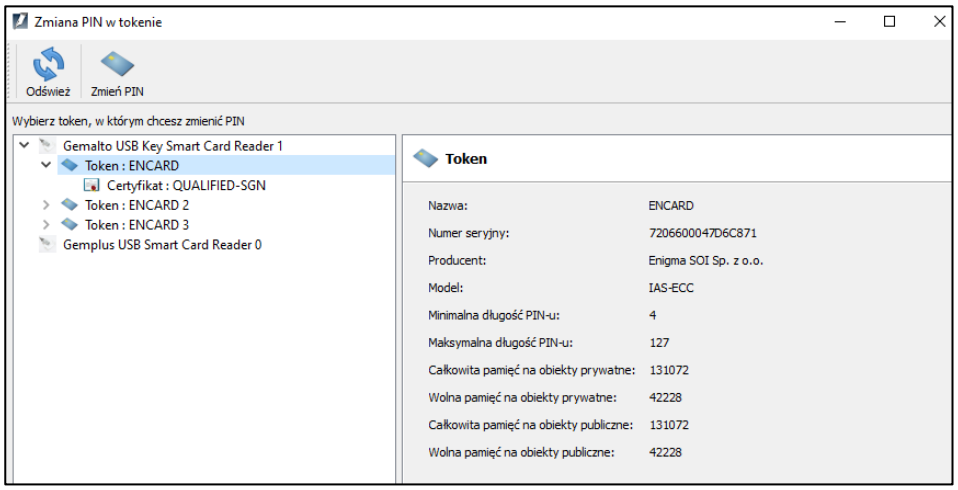
Wszystkie operacje opisane poniżej dotyczą operacji wywoływanych z okna głównego programu, wyświetlanego po jego uruchomieniu - patrz rozdział 5.1 wyżej.

6.1 Zmiana kodu PIN

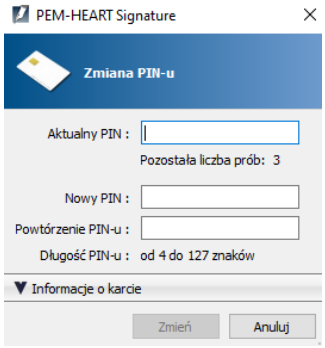
Uwaga! Funkcja nie działa dla podpisu rSign (w chmurze).

W celu zmiany PINu wybierz menu *Karta* (pasek po lewej stronie okna głównego) i wciśnij ikonę *Zmień PIN*.

Następnie wskaż token, do którego zmieniasz PIN (Uwaga: obiekty związane z podpisem kwalifikowanym umieszczane są zawsze w pierwszym tokenie od góry; inne tokeny mogą być używane do innych celów, np. do pieczęci elektronicznej lub do podpisów niekwalifikowanych):



Następnie kliknij ikonę *Zmień PIN* (na górnym pasku).



Do zmiany kodu należy podać poprawny aktualny kod PIN oraz dwa razy wpisać nowy kod. Nie zalecamy używania do kodu PIN polskich liter lub innych znaków, które przy różnych ustawieniach językowych klawiatury komputera mogą nie być poprawnie wprowadzane (karta się blokuje po 3 próbach podania nieprawidłowego kodu). Zalecamy zapisanie kodu PIN w bezpiecznym miejscu (oddzielnie od karty).

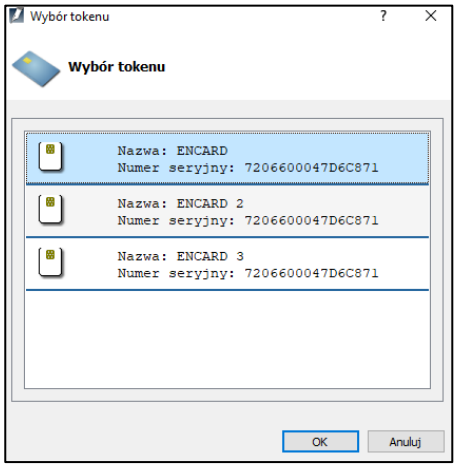
Uwaga! W przypadku zablokowania kodu PIN, kartę można odblokować tylko kodem PUK.

Kody PIN / PUK zostały nadane przez Ciebie podczas aktywacji karty. **Nie posiadamy Twoich kodów PIN / PUK i nie możemy pomóc w przypadku zablokowania karty z powodu błędnego kodu PIN / PUK.**

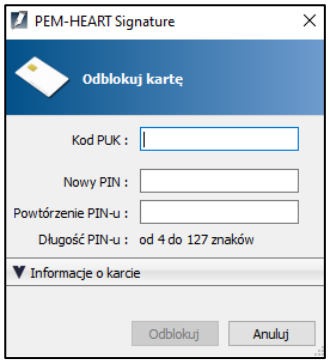
6.2 Odblokowanie karty

Uwaga! Funkcja nie działa dla podpisu rSign (w chmurze).

W przypadku zablokowania karty po podaniu zbyt wielu błędnych kodów PIN możliwe jest jej odblokowanie za pomocą kodu PUK. Kod PUK jest nadawany samodzielnie przez użytkownika podczas aktywacji karty. Po użyciu przycisku *Odblokuj kartę* wyświetlane jest poniższe okno:



Należy wybrać odpowiedni token (dla podpisu kwalifikowanego: pierwszy od góry)



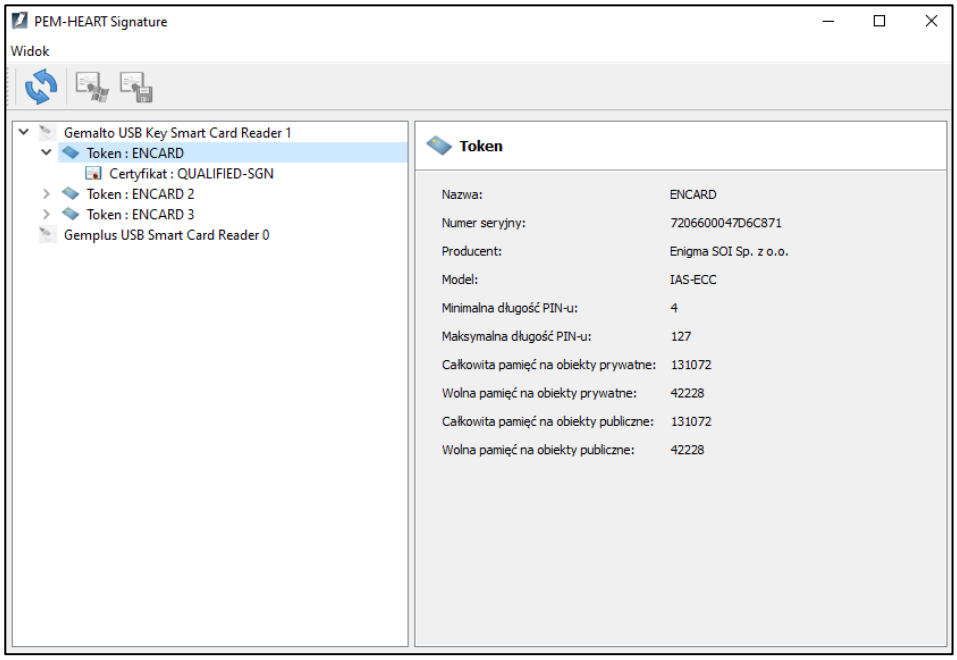
Po poprawnym podaniu kodu PUK, będzie możliwe ustawienie nowego kodu PIN i karta zostanie odblokowana.

Uwaga!! Dostępnych jest 10 prób odblokowania karty za pomocą kodu PUK. Po 10. błędnie podanym kodzie PUK karta jest trwale zablokowana i nie ma możliwości jej dalszego użycia.

Kody PIN / PUK zostały nadane przez Ciebie podczas aktywacji karty. **Nie posiadamy Twoich kodów PIN / PUK i nie możemy pomóc w przypadku zablokowania karty z powodu błędnego kodu PIN / PUK.**

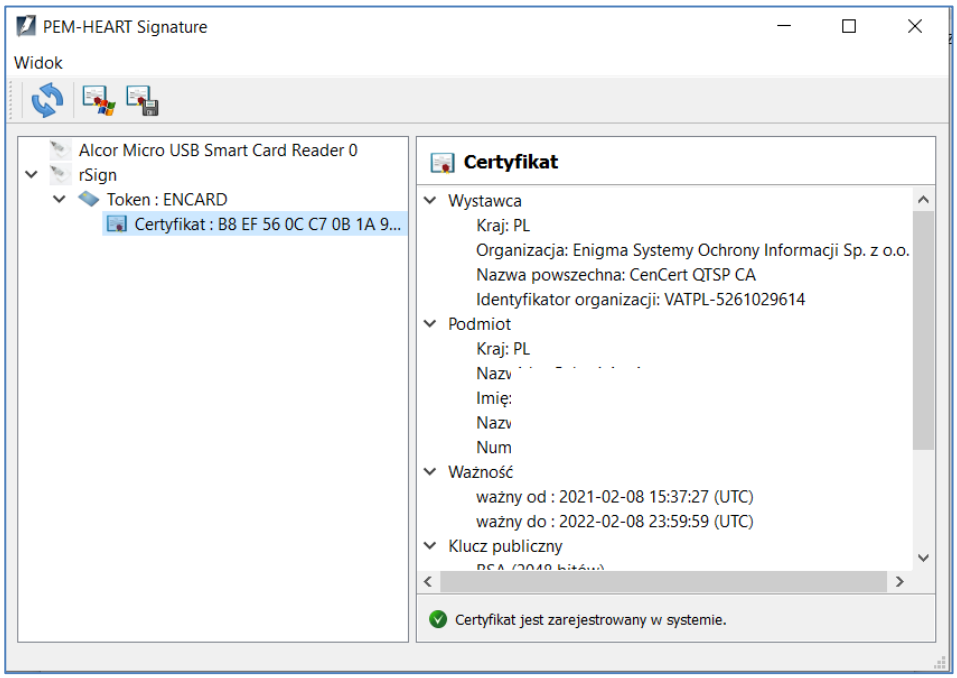
6.3 Diagnostyka

W przypadku, gdy w systemie jest dostępnych więcej czytników oraz kart, pomocna jest funkcja *Diagnostyka* w meny *Karta*. Po jej wyborze zostanie wyświetlona lista czytników w systemie oraz informacje na temat włożonych w nich kart.



Można tu uzyskać informacje na temat obiektów na kartach: tokenów oraz certyfikatów. Po zaznaczeniu certyfikatu jest wyświetlana jego struktura i dane. Można też (przyciski na górze okna) zainstalować certyfikat magazynie systemu Windows i/lub zapisać go do pliku.

W przypadku podpisu w chmurze (jeśli skonfigurowano podpis na bieżącym koncie użytkownika komputera) „karta" jest zawsze obecna w czytniku, stąd widać będzie „czytnik kart" rSign, a w nim kartę z tokenem ENCARD oraz bieżącym certyfikatem.



7 Podpis rSign (w chmurze)

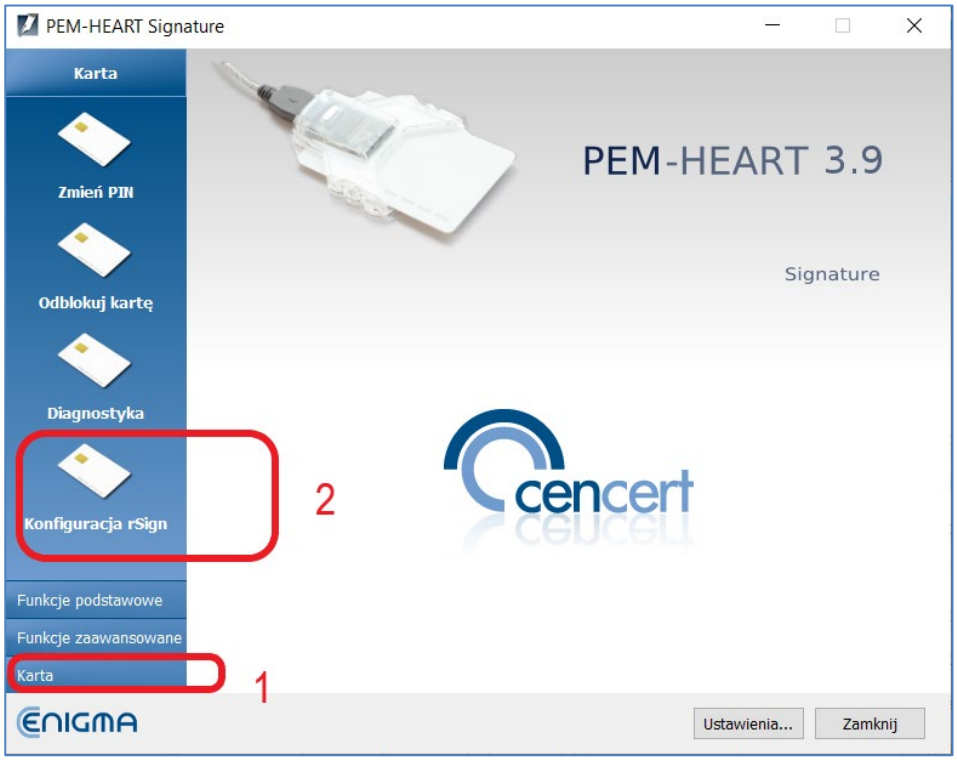
7.1 Konfiguracja na komputerze

Zanim będziesz miał możliwość składania podpisu rSign na danym komputerze (na danym koncie systemu Windows), musisz skonfigurować podpis na każdym takim komputerze (koncie).

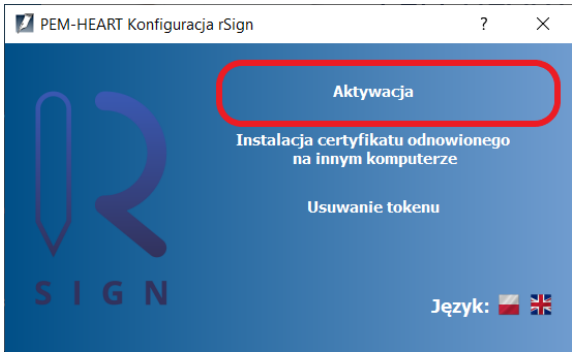
Cele tej operacji są dwojakie – po pierwsze, przy rozpoczynaniu składania podpisu program musi wiedzieć kto będzie składał podpis (jakim certyfikatem będzie składany podpis). Po drugie, istotnym celem jest zwiększenie bezpieczeństwa Twojego podpisu – podpis rSign można składać tylko na komputerze uprzednio uznanym przez Ciebie jako zaufany.

W celu konfiguracji podpisu rSign uruchom program *PEM-HEART Signature* (uruchomienie programu jest opisane w rozdziale 5.1).

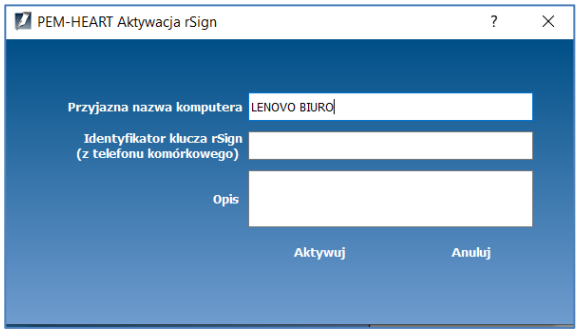
Następnie wybierz polecenie *Karta -> Konfiguracja rSign*



Następnie wybierz polecenie *Aktywacja*

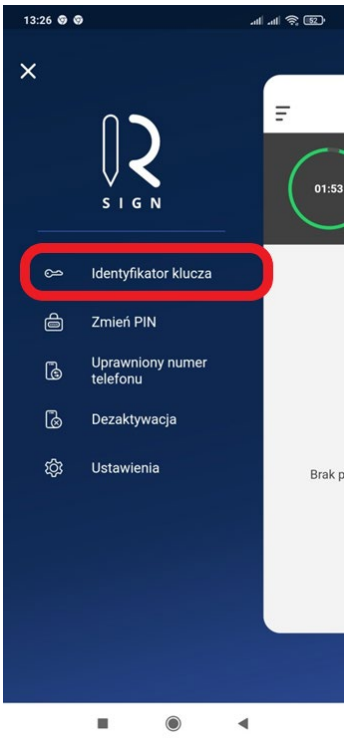


W oknie poniżej wpisz nazwę komputera (będzie się ona wyświetlać na Twoim telefonie przy operacjach podpisu):

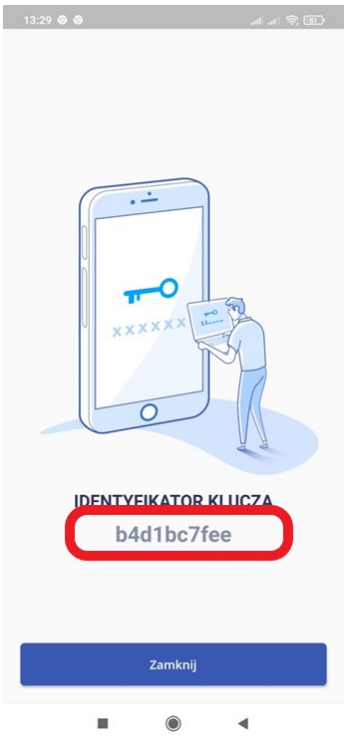


Następnie przepisz Identyfikator klucza rSign z aplikacji na telefonie komórkowym.

W tym celu uruchom aplikację rSign na telefonie, następnie:
- wybierz menu (kreski w lewym górnym roku)
- wybierz polecenie Identyfikator klucza.

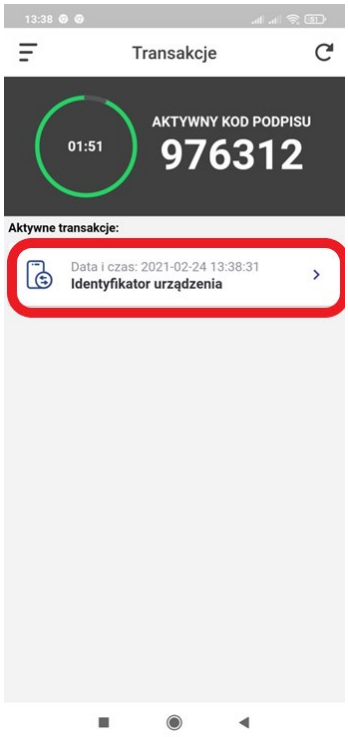


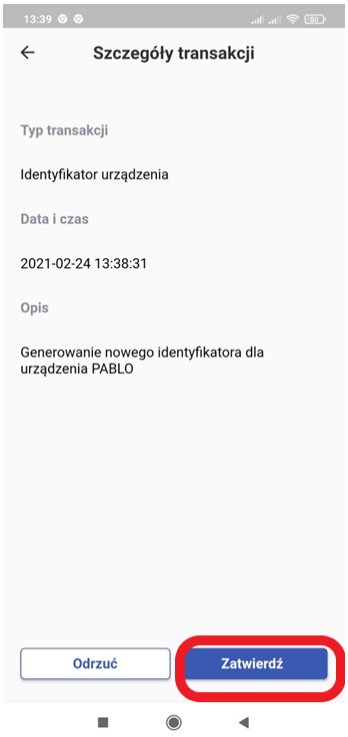
Następnie podaj PIN do aplikacji na telefonie, odczytaj i przepisz Identyfikator klucza do okna w aplikacji na komputerze.



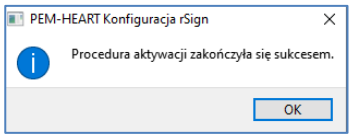
Następnie kliknij *Aktywuj*.

Program wyświetli informację, że konieczne jest jeszcze zatwierdzenie urządzenia (komputera) jako zaufanego na Twoim telefonie. W tym celu, otwórz aplikację rSign na telefonie (patrz obrazy poniżej).





Program na komputerze wyświetli komunikat o zakończeniu konfiguracji podpisu rSign na danym komputerze (koncie systemowym).



Uwaga!:

1) *Na jednym koncie systemowym na komputerze możesz mieć skonfigurowanych wiele certyfikatów rSign. W celu dodania następnego certyfikatu do konfiguracji, należy powtórzyć operacje opisane w tym rozdziale, podając następny Identyfikator klucza (odczytany z aplikacji rSign skonfigurowanej na innym telefonie komórkowym).*
2) *Z punktu widzenia programów do składania podpisów, jeśli skonfigurujesz kilka certyfikatów, program będzie rozpoznawał tę sytuację tak, jakbyś miał włożonych jednocześnie do czytników kilka kart do składania podpisu. Sposób reakcji na taką sytuację zależy od programu. PEM-HEART Signature w takiej sytuacji wyświetli okno wyboru certyfikatu, którym ma być złożony podpis. Prośba o zatwierdzenie podpisu będzie wysłana do telefonu komórkowego skojarzonego z wybranym certyfikatem.*
3) *W celu usunięcia jakiegoś certyfikatu z konfiguracji na komputerze – patrz rozdział 7.3. Certyfikat usunięty z konfiguracji można będzie w każdej chwili skonfigurować na nowo.*

7.2 Instalacja certyfikatu odnowionego online na innym (kolejnym) komputerze

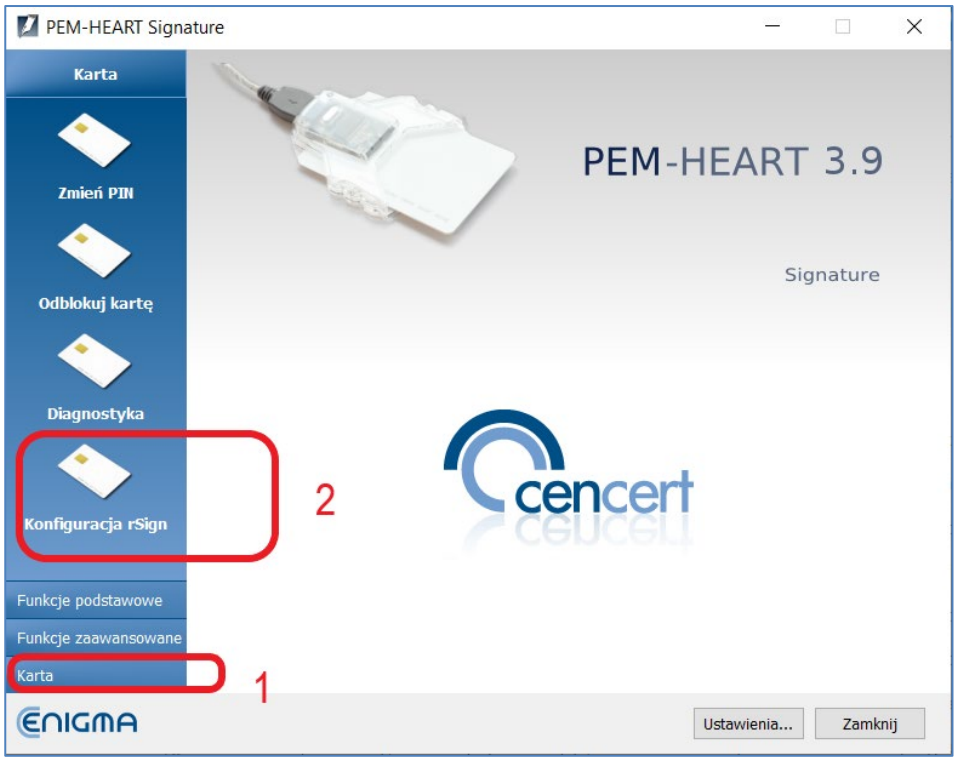
Odnowienie certyfikatu online oznacza operację pozyskania nowego certyfikatu, z nowym okresem ważności, przy użyciu certyfikatu poprzedniego, którego termin ważności upływa. Odnowienie online wykonuje się przy użyciu oprogramowania *PEM-HEART Odnowienie certyfikatu*. Podczas odnowienia certyfikatu nie ma konieczności wczytywania kodu *QR* do aplikacji rSign na telefonie, tak jak to się odbywa przy zakupie pierwszego certyfikatu.

Uwaga! Jeśli przy zakupie nowego certyfikatu była konieczność (ponownego) zainicjowania aplikacji na telefonie komórkowym przy użyciu kodu QR, to znaczy, że to wydanie certyfikatu nie było „operacją odnowienia online" i treść niniejszego rozdziału nie ma zastosowania. W takim przypadku, w celu skonfigurowania podpisu rSign na komputerze, należy to wykonać zgodnie z rozdziałem 7.1)

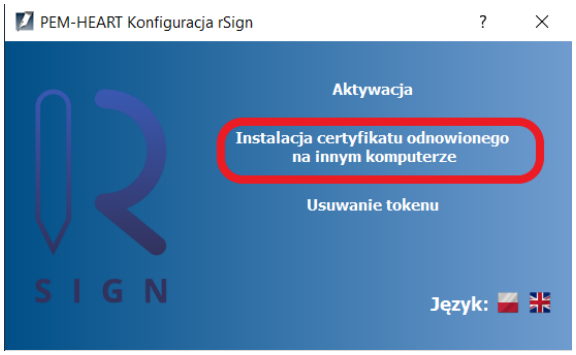
Jeśli odnowiłeś online certyfikat do podpisu rSign (w chmurze), Twój nowy certyfikat zapisał się automatycznie na tym komputerze, na którym wykonywałeś operację odnowienia. Jeśli jednak korzystasz z Twojego podpisu rSign na wielu komputerach – na pozostałych musisz uaktualnić konfigurację, aby Twój program podpisujący „wiedział" o Twoim nowym certyfikacie.

W celu instalacji certyfikatu odnowionego online na innym (kolejnym) komputerze uruchom program *PEM-HEART Signature* (uruchomienie programu jest opisane w rozdziale 5.1).

Następnie wybierz polecenie *Karta -> Konfiguracja rSign*



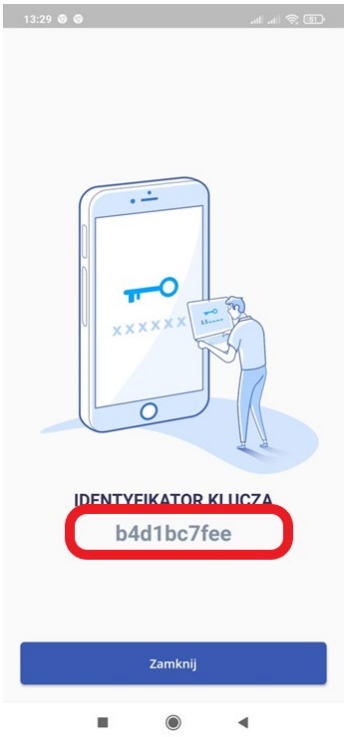
Następnie wybierz polecenie *Instalacja certyfikatu odnowionego na innym komputerze*.



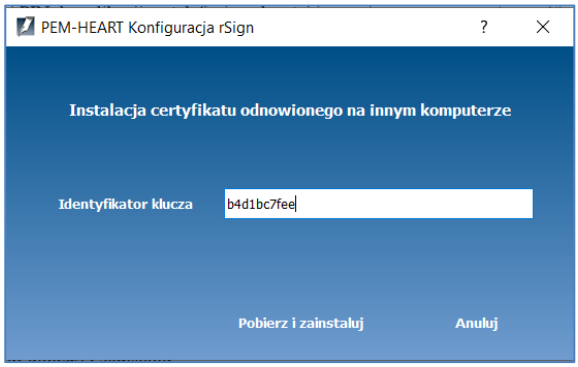
Następnie wpisz identyfikator Twojego klucza do podpisywania:

W tym celu uruchom aplikację rSign na telefonie, następnie:
- wybierz menu (kreski w lewym górnym roku)
- wybierz polecenie Identyfikator klucza.

Następnie podaj PIN do aplikacji na telefonie, odczytaj i przepisz Identyfikator klucza do okna w aplikacji na komputerze.



Następnie kliknij Pobierz i zainstaluj.

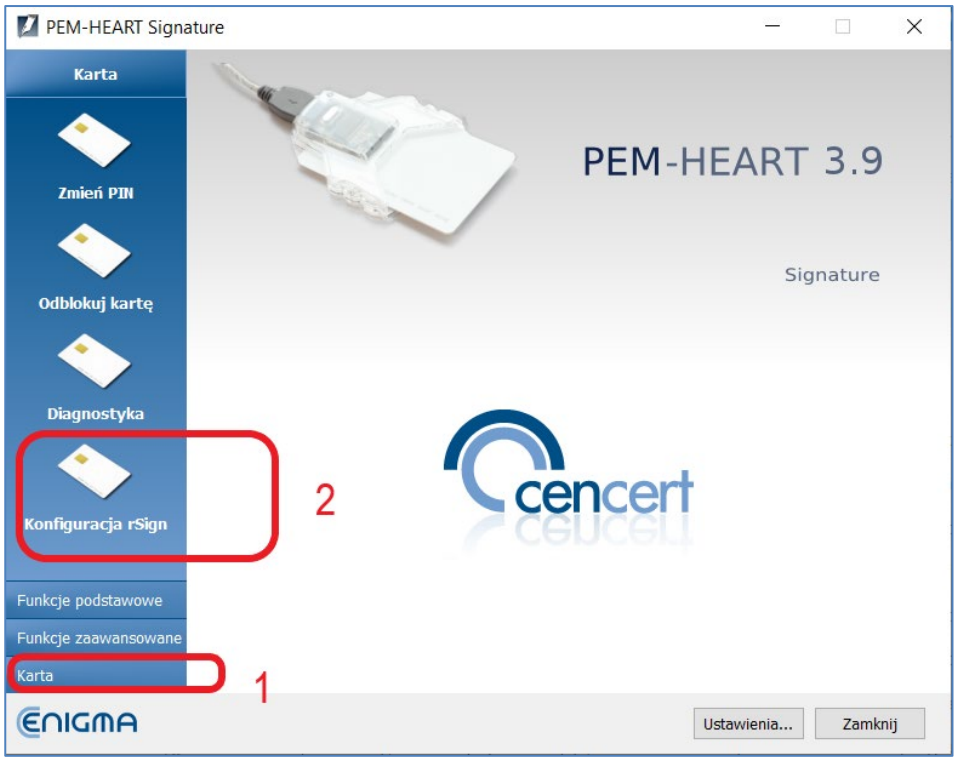


Program pobierze z serwera i zainstaluje w komputerze Twój nowy certyfikat.

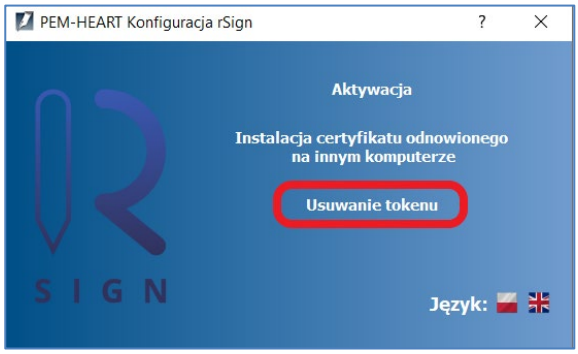
7.3 Usunięcie konfiguracji certyfikatu (lub jednego z certyfikatów) rSign z komputera

W celu usunięcia konfiguracji certyfikatu rSign z komputera uruchom program *PEM-HEART Signature* (uruchomienie programu jest opisane w rozdziale 5.1).

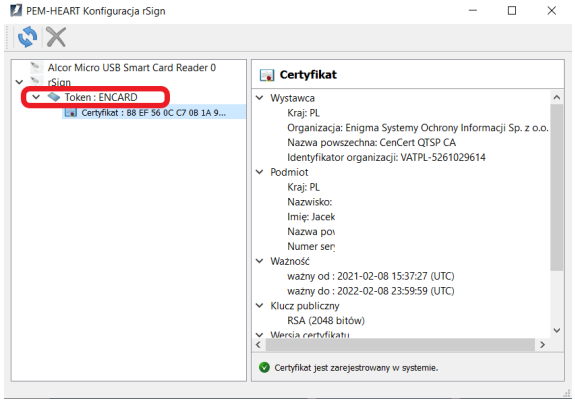
Następnie wybierz polecenie *Karta -> Konfiguracja rSign*



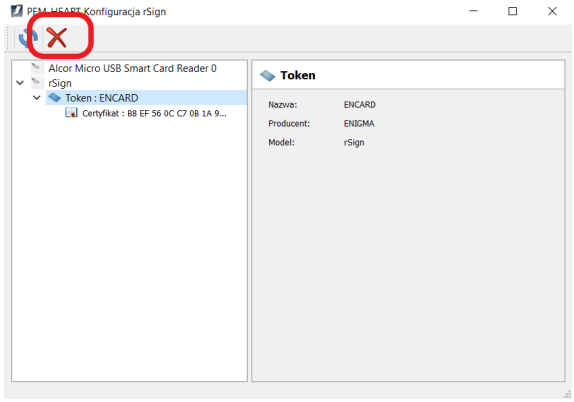
Następnie wybierz polecenie *Usuwanie tokenu*.



Program wyświetli listę dostępnych „tokenów” (w tym tokenów na kartach fizycznych, jeśli są dostępne). Zaznacz token rSign do usunięcia.



Po zaznaczeniu tokenu kliknij klawisz usunięcia tokenu:



Program usunie zaznaczony token rSign.

Usunięty token można dodać do konfiguracji na komputerze ponownie, poprzez wykonanie operacji opisanych w rozdziale 7.1.

7.4 Aplikacja rSign na telefonie komórkowym

7.4.1 Ekran główny aplikacji

Ekran główny aplikacji wygląda tak:

Opis obszarów ekranu:

1 – **Aktywny PIN podpisu**.
PIN ten należy przepisać do aplikacji która składa podpis (na komputerze) – jako „PIN do podpisu" lub „PIN do karty". Kod PIN jest zmienny czasowo.
2 – **Menu aplikacji**. Patrz rozdział ……
3 – **Odświeżenie informacji o operacjach do zatwierdzenia** (jeśli informacje nie pobrały się same).

7.4.2 Odczytanie identyfikatora klucza

Identyfikator klucza jest informacją która powinna być chroniona (poufna). Powinien być używany jedynie do konfiguracji komputerów zaufanych, na których można będzie składać Twój podpis (w tym może być przekazywany innym, zaufanym podmiotom, zarządzającym systemami w których będziesz składał podpisy serwerowe).
Każda operacja podpisu wymaga zatwierdzenia za pomocą aplikacji na Twoim telefonie - posiadanie identyfikatora klucza nie daje możliwości składania podpisów w Twoim imieniu.

W celu odczytania identyfikatora klucza, wybierz menu aplikacji (patrz rozdział 7.4.1).

Następnie wybierz polecenie *Identyfikator klucza*, podaj PIN do aplikacji – i odczytaj identyfikator.

7.4.3 Backup danych aplikacji mobilnej

Backup danych aplikacji mobilnej jest niezbędny do przeniesienia danych aktywujących podpis na inny telefon. Jeśli chcesz zmienić aparat telefoniczny albo utracisz obecny telefon (albo telefon się zepsuje), albo dane na telefonie zostaną skasowane – będziesz mógł odtworzyć dane aktywujące podpis (nie będziesz musiał ponosić kosztów nabycia nowego certyfikatu) pod warunkiem, że posiadasz aktualny backup danych aplikacji mobilnej rSign.

Aplikacja proponuje zrobienie bakupu pod razu przy aktywacji. Operację backupu możesz jednak wykonać także później.

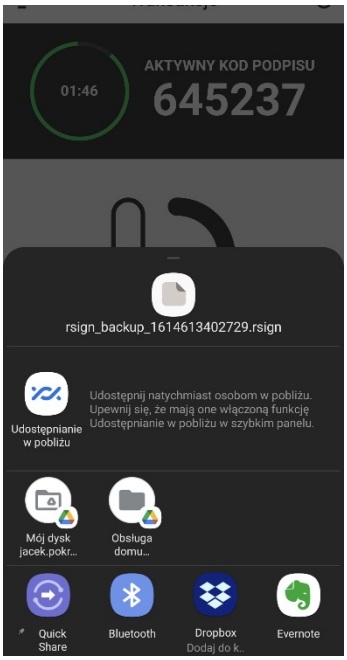
Zdecydowanie zalecamy przechowywanie pliku backupu poza telefonem (np. na Google Dysk lub w iCloud). Plik backupu jest zaszyfrowany oraz zawiera tylko część danych potrzebnych do aktywacji Twojego podpisu, może więc być przechowywany w środowisku o ograniczonym zaufaniu.

Raz wykonany backup jest aktualny (i nie musi być ponawiany), chyba że zmienisz PIN do aplikacji mobilnej.

W celu usunięcia danych aktywujących podpis z telefonu wybierz menu aplikacji (patrz rozdział 7.4.1).

Następnie wybierz polecenie *Opcje*, a następnie polecenie *Kopia zapasowa*.

Aplikacja poprosi o PIN do aplikacji, a następnie o wskazanie miejsca zapisu pliku z backupem.



Zdecydowanie zalecamy zapisanie pliku backupu poza telefonem (np. w chmurze Google, Apple, Dropbox itp.).

7.4.4 Zmiana PINu do aplikacji

W celu zmiany PINo do aplikacji mobilnej wybierz menu aplikacji (patrz rozdział 7.4.1).

Następnie wybierz polecenie *Zmień PIN*, podaj stary (dotychczasowy) PIN do aplikacji, następnie podaj dwa razy nowy PIN.

UWAGA!

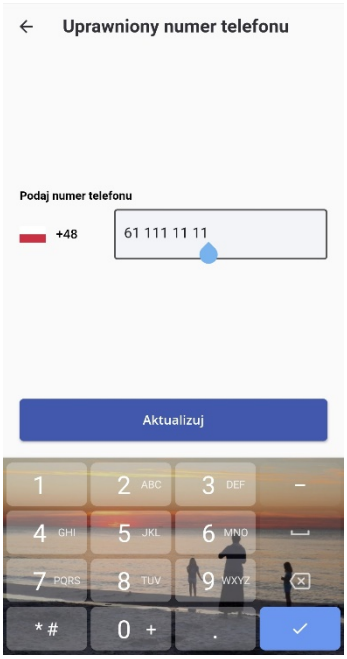
1) **PIN do aplikacji mobilnej jest daną krytyczną.** Jeśli zapomnisz PIN, utracisz dostęp do Twojego klucza do podpisywania na zawsze - jedyną możliwością przywrócenia możliwości składania podpisów będzie zakup nowego certyfikatu. Jeśli nie jesteś pewien, czy zapamiętasz PIN – zalecamy zapisanie go w bezpiecznym miejscu.
2) **Po zmianie PINu musisz wykonać ponownie backup danych aplikacji mobilnej** (patrz rozdział 7.4.3). Stary backup jest zaszyfrowany starym PINem i nie będzie mógł być już użyty.

7.4.5 Uprawniony numer telefonu

Jest ważne, aby w bazie CenCert był Twój aktualny numer telefonu komórkowego. Jeśli w przyszłości będziesz chciał przenieść dane aktywujące Twój podpis na inny telefon, system CenCert **wyśle NA TEN NUMER** SMS z kodem autoryzującym transakcję przeniesienia danych aktywujących.

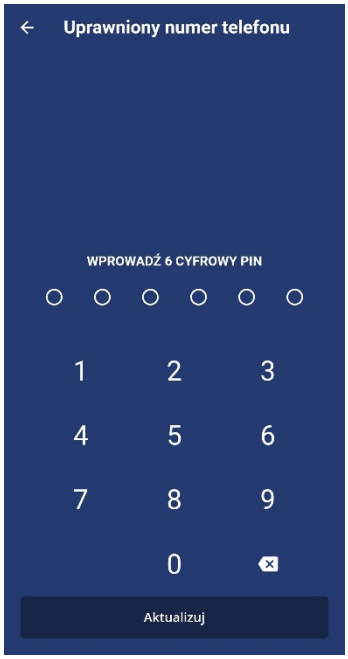
W celu uaktualnienia Twojego numeru telefonu wybierz menu aplikacji (patrz rozdział 7.4.1).

Następnie wybierz polecenie *Uprawniony numer telefonu*.



Wpisz nowy numer i zatwierdź go w następnym oknie (powyżej).

Następnie wpisz kod PIN do aplikacji mobilnej, powodując zapisanie nowego numeru na serwerze.



7.4.6 Czas aktywności podpisu

Każdy podpis rSign musi być autoryzowany przez Ciebie poprzez aplikację mobilną rSign. Możesz aktywować każdorazowo jeden podpis, ale możesz też dać możliwość składania wielu podpisów bez konieczności zatwierdzania każdej operacji w aplikacji mobilnej.

Jeśli przy zatwierdzaniu operacji ustawisz czas podpisu na np. 1 minutę, to znaczy, że kolejne operacje podpisu przychodzące z tego samego komputera będą wykonywane bez przesyłania kolejnych zapytań do Twojej aplikacji mobilnej, o ile czas pomiędzy kolejnymi podpisami nie będzie dłuższy niż ustawiona 1 minuta (czas „nieaktywności" podpisu). W każdym razie – niezależnie od tego ustawienia – po upływie 60 minut od pierwszego podpisu, status podpisu się wyzeruje (kolejna operacja znowu będzie potrzebowała zatwierdzenia).

Ustawienie czasu nieaktywności podpisu jest przydatne wszędzie tam, gdzie chcesz składać wiele podpisów na raz (np. gdy w oknie podpisywania programu *PEM-HEART Signature* umieściłeś wiele plików do podpisu). Opcja ta jest też przydatna przy składaniu podpisów ze znakowaniem czasem – ponieważ wtedy na każdym razem są składane dwa podpisy (jeden pod dokumentem, drugi pod żądaniem znakowania czasem).

Ustawienie czasu nieaktywności podpisu (ustawienie podpisu wielokrotnego) jest przydatne i może być zalecane jeśli zawsze wykonujesz podpisy z komputerów, które są pod Twoją wyłączną kontrolą i którym ufasz. Jeśli składasz podpis z komputera, do którego masz ograniczoną kontrolę, bezpieczniej jest ustawić opcję zatwierdzanie jednego podpisu.

Jeśli chcesz zmienić opcję zatwierdzania podpisu (i ewentualnie ustawić dopuszczalny czas nieaktywności podpisu) – w menu aplikacji wybierz polecenie *Ustawienia*, a następnie *Zmiana czasu podpisu*.

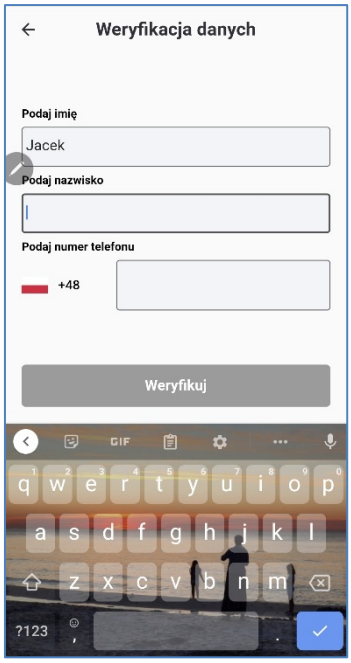
7.4.7 Przeniesienie danych z innego telefonu

Jeśli chcesz przenieść dane z innego telefonu, na nowym telefonie zainstaluj aplikację „rSign by CenCert" ze sklepu Google Play lub AppStore.

Następnie, w oknie głównym aplikacji, wybierz polecenie Przenieś aktywację.

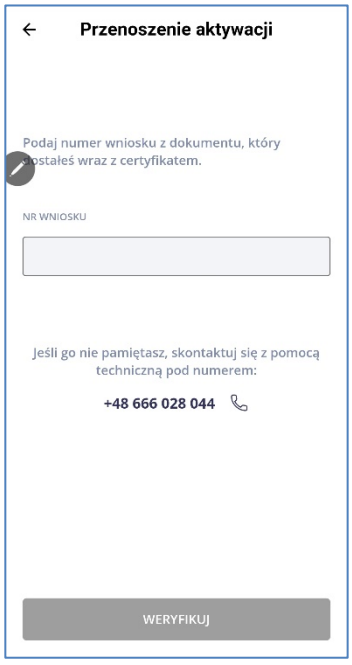
Następnie wciśnij zaznaczony obszar DODAJ PLIK, co spowoduje wyświetlenie okna wyboru pliku.

Wskaż plik backupu (plik standardowo ma nazwę *rsign_backup_XXXXXXXX.rsign*) i wciśnij klawisz *Wczytaj plik*.



Następnie wpisz Twoje imię i nazwisko oraz numer telefonu komórkowego (który został ustalony w systemie CenCert):

Wciśnij klawisz *Weryfikuj*.

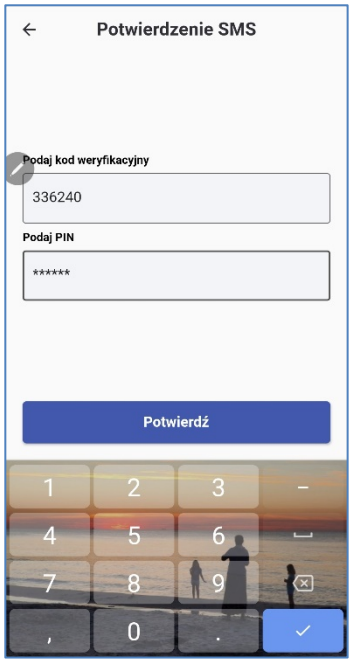


Jeśli w przeszłości wiązałeś Twój telefon z kilkoma certyfikatami rSign, program poprosi Cię jeszcze o numer wniosku certyfikacyjnego, który podpisywałeś (odręcznie lub elektronicznie) przy wydawaniu certyfikatu Twojego obecnego certyfikatu:

Numer *wniosku* ma postać np. numeru takiego jak „2021022600768”.

Jeśli nie znasz tego numeru, możesz zadzwonić na pomoc techniczną CenCert w godzinach pracy, kiedy jest czynna. Personel CenCert będzie mógł znaleźć numer Twojego wniosku na podstawie Twoich danych osobowych i przybliżonej daty nabycia certyfikatu. Możesz napisać też w tej sprawie maila na adres biuro@cencert.pl

Wciśnij klawisz *Weryfikuj*.



Wpisz kod weryfikacyjny, który otrzymałeś SMSem oraz PIN do aplikacji mobilnej (stary PIN – ten który ustawiłeś jak robiłeś backup danych aplikacji mobilnej)

Wciśnij *Potwierdź*.

Zakończyłeś przenoszenie danych aktywacyjnych.

Teraz jest dobry moment na zrobienie nowego backupu. Plik backupu, z którego odczytałeś dane **stał się w tym momencie BEZUŻYTECZNY**. Nie będzie mógł być ponownie wykorzystany.

Musisz wykonać nowy backup – najlepiej teraz – poprzez wciśnięcie klawisza ***Zapisz nową kopię zapasową***.

Po wykonaniu nowego backupu – wciśnij klawisz ***Dalej***.

Zakończyłeś aktywację podpisu na nowym telefonie. Możesz usunąć (zdezaktywować) dane do podpisu na starym telefonie, jeśli masz jeszcze do niego dostęp.

7.4.8 Dezaktywacja danych do podpisu na telefonie

W celu usunięcia danych aktywujących podpis z telefonu wybierz menu aplikacji (patrz rozdział 7.4.1).

Następnie wybierz polecenie *Dezaktywacja urządzenia*.

Ponowne przywrócenie danych aktywacyjnych podpis jest możliwe na tym (lub innym) telefonie, pod warunkiem, że:

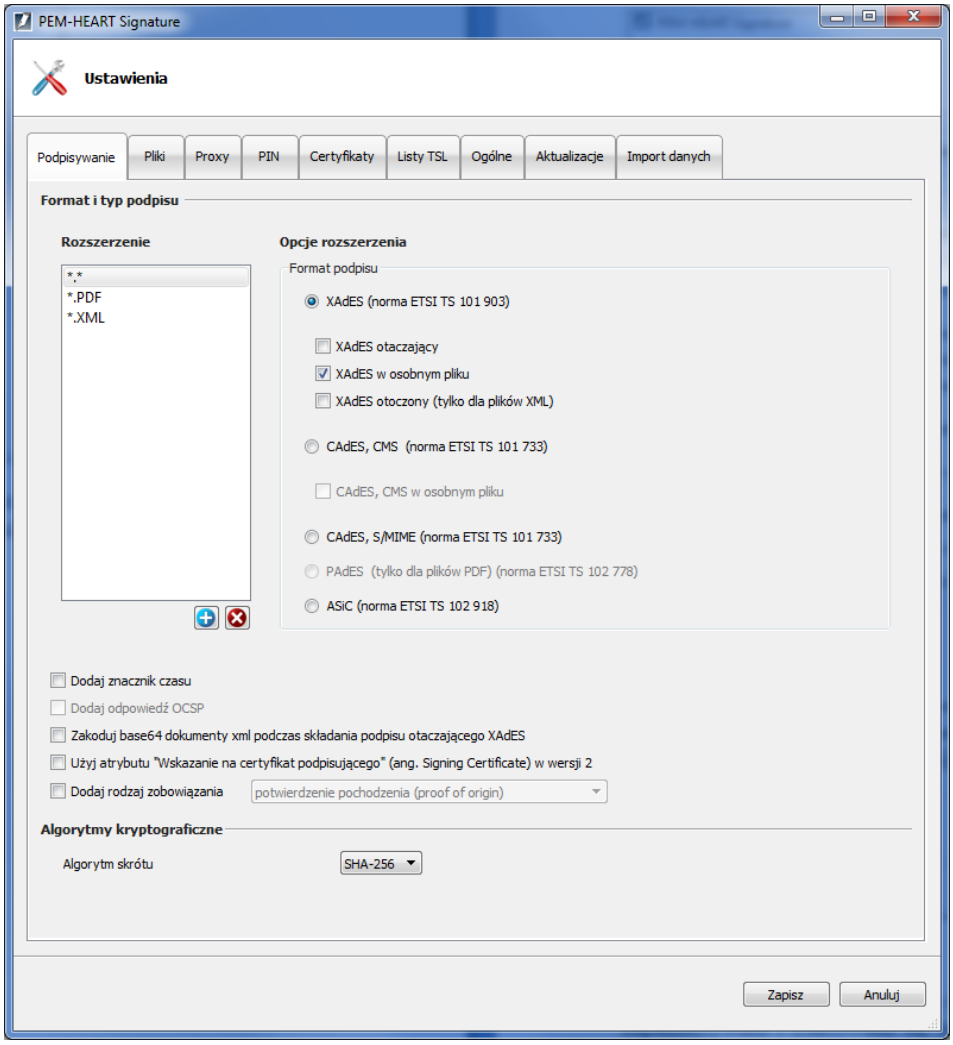
1) posiadasz aktualny backup danych mobilnych,
2) znasz PIN do aplikacji mobilnej (który był ważny w chwili wykonywania backupu),
3) może odbierać SMSy ze zdefiniowanego w CenCert numeru telefonu.

8 Opcje programu, praca bez Internetu

Wszystkie operacje opisane poniżej dotyczą operacji wywoływanych z okna głównego programu, wyświetlanego po jego uruchomieniu - patrz rozdział 5.1 wyżej.

8.1 Podpisywanie

W celu zmiany opcji podpisywania, w oknie głównym programu kliknij klawisz *Ustawienia.*



Wszystkie opcje określające format podpisu (XAdES, CAdES, ASiC) będą zastosowane do plików o rozszerzeniu aktualnie zaznaczonym na liście ***Rozszerzenie***. Na rysunku powyżej, wszystkie pliki o rozszerzeniach *.* (a więc wszystkie inne pliki niż zdefiniowane na liście poniżej) będą domyślnie podpisywane w formacie: *XAdES w osobnym pliku*. Jednocześnie pliki *.PDF i *.XML mają swoje własne domyślne formaty podpisu, które będą widoczne po zaznaczeniu na liście odpowiednio wiersza *.PDF lub *.XML.

W tym miejscu możesz również dodać inne rozszerzenia plików (za pomocą ikon  i ), dla których ma być stosowany inny domyślny format podpisu. Np. jeśli dodasz nową pozycję „*.docx" i zdefiniujesz, że dla tych plików ma być wykonywany podpis np. *CAdES, CMS w osobnym pliku*, to dla wywołania podpisu dla każdego pliku z dokumentem Ms Word (*.docx), program domyślnie zaproponuje podpis w formacie *CAdES, CMS w osobnym pliku*.

W dalszej części okna (poniżej, od opcji *Dodaj znacznik czasu*) możesz określić dodatkowe opcje dla podpisów. Ustawienia te dotyczą wszystkich podpisów – niezależnie od nazwy pliku.

Opcja „***dodaj znacznik czasu***" oznacza, że do każdego podpisu zostanie dodany znacznik czasu (***Uwaga! Do poprawnego działania może być wymagane wykupienie pakietu znaczników czasu***).

Opcja „***dodaj odpowiedź OCSP***" oznacza, że oprócz znacznika czasu (który też trzeba wtedy zaznaczyć), do podpisu zostanie dodana informacja o statusie certyfikatu użytego do podpisu (powstaje w ten sposób podpis w formie *long* – patrz też rozdział 4 wyżej).

Opcja „*Zakoduj base64 dokumenty xml podczas składania podpisu otaczającego XAdES*" jest potrzebna w specyficznych sytuacjach, jeśli system weryfikujący podpisane dokumenty ma ograniczone możliwości weryfikacji różnych formatów podpisów i tego wymaga.

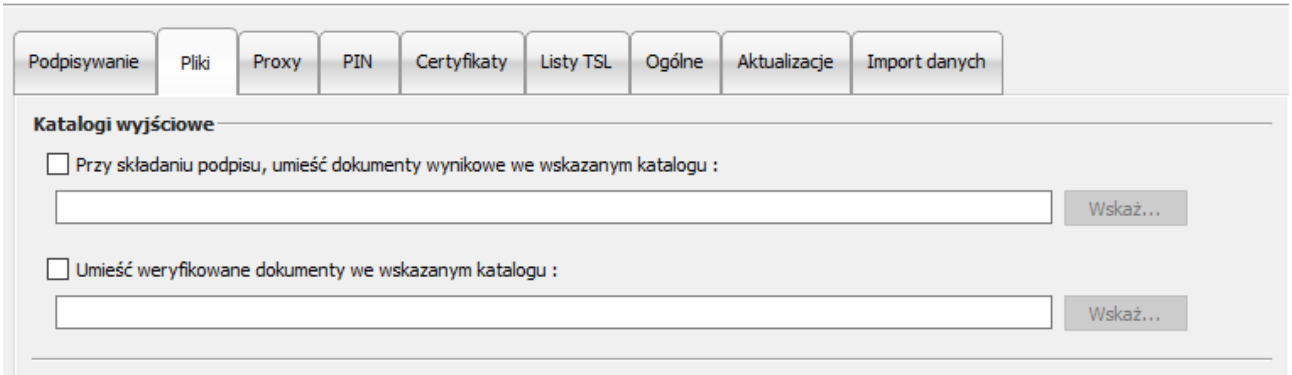
Opcja „*Użyj atrybutu „Wskazanie na certyfikat podpisującego (ang. Signing Certificate) w wersji 2"* powoduje umieszczenie w podpisie wskazania na certyfikat w formacie zgodnym z nowszymi wersjami norm ETSI dotyczących formatu podpisu. Należy zaznaczyć tę opcję w przypadku, gdy jest to wymagane przez system weryfikujący podpisy, posługujący się wyłącznie nowymi formatami.

Zaznaczenie opcji „*Dodaj rodzaj zobowiązania*" powoduje dodanie podpisanego atrybutu, który wskazuje w jakim celu (w jakiej roli) podpisujący złożył podpis (np. jako „formalne zatwierdzenie", albo „potwierdzenie odbioru" itd.).

Opcja „*Algorytm skrótu"* określa algorytm skrótu kryptograficznego używany do wystawienia podpisu. Program umożliwia wyłącznie wybór spośród dobrych algorytmów, gwarantujących (gdy dana wersja programu jest aktualna) odpowiednie bezpieczeństwo.

8.2 Pliki

Zakładka zawiera opcje ustalania katalogów wyjściowych dla przetwarzanych dokumentów. Domyślnie program przetwarza dokumenty w tym samym katalogu, w którym dany dokument się znajduje. Możliwe jest ustalenie innych katalogów, do których będą zapisywane dokumenty podpisane lub zweryfikowane.



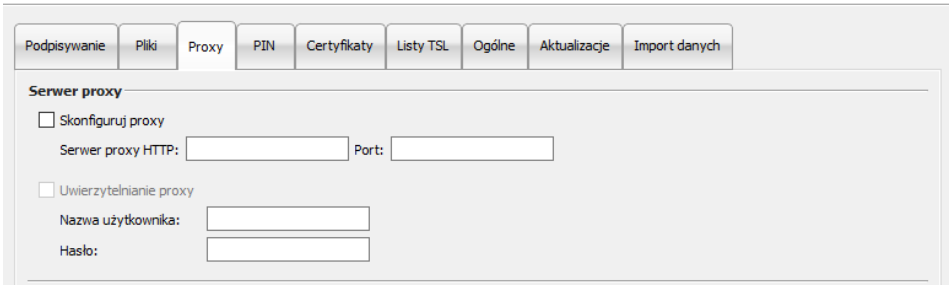
Rysunek 49 Konfiguracja katalogów wyjściowych

Aby zdefiniować katalog należy zaznaczyć pole przed opisem opcji, zostanie wtedy aktywowany przycisk *Wskaż,* za pomocą którego można wskazać dany katalog w systemie plików.

8.3 Proxy

Zakładka służy do określenia serwera *proxy* (jeśli Twój dostęp do Internetu tego wymaga). Trzeba wypełnić wszystkie pola obowiązkowe dla danego serwera *proxy*.

Aktywacja opcji dokonywana jest po zaznaczenia pola wyboru *Skonfiguruj proxy*.



Błędne skonfigurowanie serwera powoduje brak dostępu programu do Internetu (nie da się pobrać znacznika czasu, może nie być możliwe weryfikowanie popdisów).

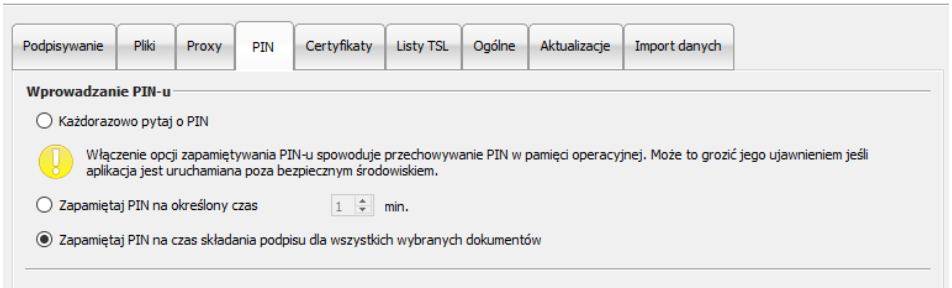
8.4 PIN

Zakładka PIN służy do ustawienia opcji zapamiętywania przez program PINu do karty.

Uwaga! Opcja nie dotyczy podpisów rSign (w chmurze). Tam opcje podpisów wielokrotnych ustawia się w aplikacji na telefonie komórkowym.

Domyślnie PIN jest zapamiętywany na czas składania podpisów pod wybranymi w oknie podpisywania plikami. W celu podpisania wszystkich plików znajdujących się w oknie programu wystarczy podać PIN jeden raz; po wykonaniu podpisów, ponowny wybór plików do podpisu (nawet bez zamknięcia programu) oznacza konieczność ponownego podania PINu.

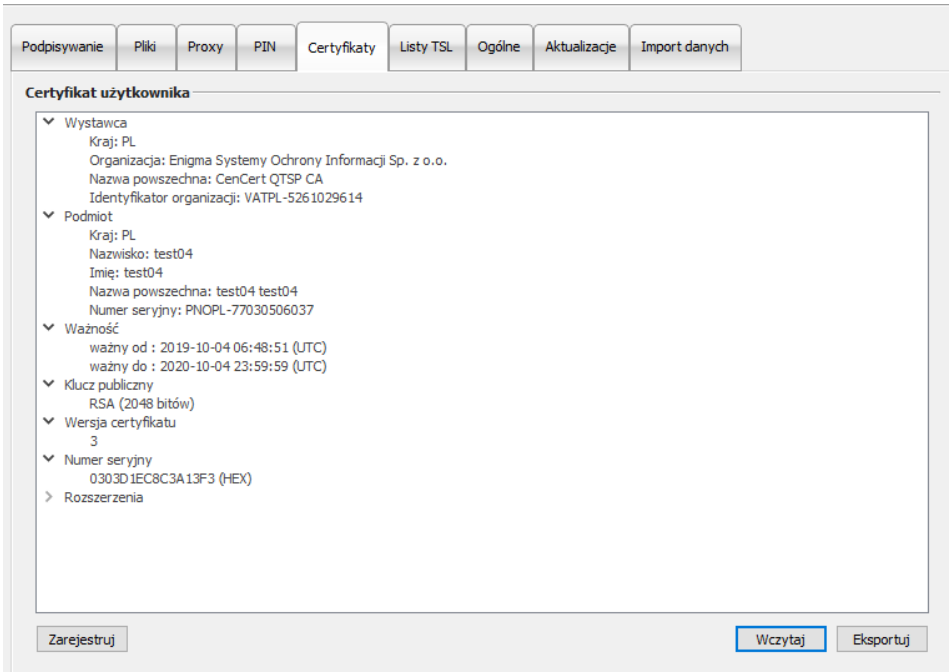
Możliwe jest także inne ustawienie opcji: że PIN będzie podawany zawsze dla każdego pojedynczego dokumentu albo też będzie zapisywany w pamięci komputera na określony zakres czasu.



8.5 Certyfikaty

Zakładka ta dotyczy prezentacji, rejestracji w systemie i eksportowania certyfikatu użytkownika. Jeśli w czytniku jest umieszczona karta to program automatycznie odczyta z niej dane i zostaną one wyświetlone w okienku.

Jeśli certyfikat nie zostanie odczytany należy sprawdzić umieszczenie karty i użyć przycisku *Wczytaj*.



W przypadku podpisu rSign (w chmurze) odczytanie certyfikatu wymaga zalogowania się do tokenu, co oznacza, że musisz (analogicznie jak przy podpisywaniu):

- Wpisać PIN podpisu (przepisany z aplikacji rSign na telefonie komórkowym)
- Zatwierdzić w telefonie operację podpisu (co oznacza w tym przypadku zalogowanie się przez program do Twojej wirtualnej karty)

Przycisk *Zarejestruj* służy do rejestracji certyfikatu odczytanego z nośnika w magazynie systemowym.

Eksport certyfikatu do pliku jest możliwy poprzez przycisk *Eksportuj*.

Sekcja *Certyfikat zakładkowy urzędu* służy do wskazania i wczytania takiego certyfikatu dostawcy usług zaufania do bazy danych programu. Opcja jest wykorzystywana w specyficznych sytuacjach dotyczących podpisów niekwalifikowanych – gdy program nie ma w bazie danych aktualnego certyfikatu „urzędu pośredniego" dostawcy usług zaufania.

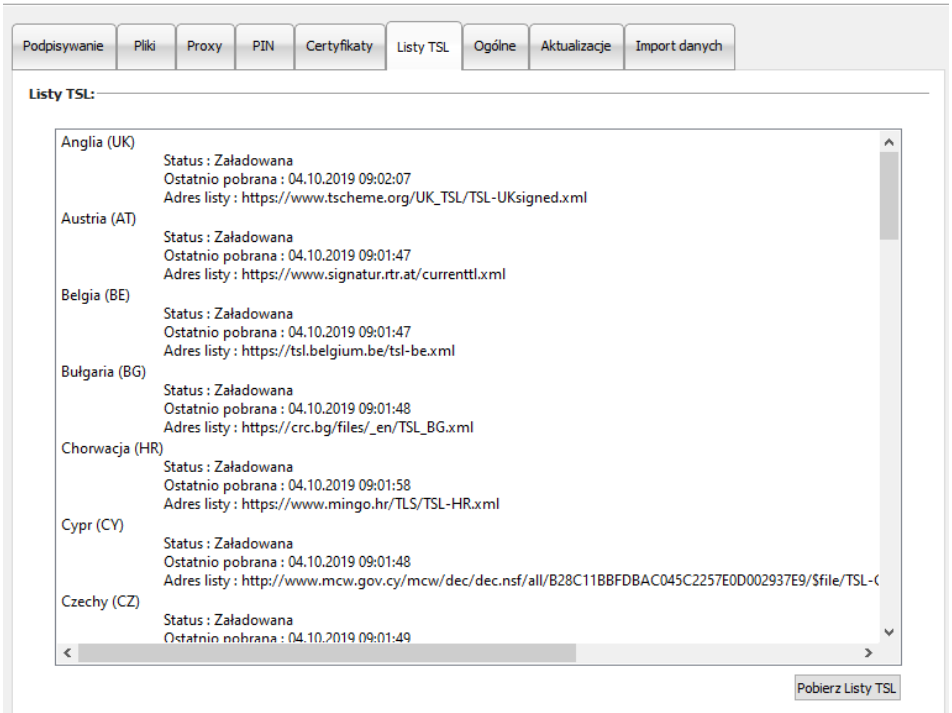
Wszystkie powyższe operacje można też wykonać z menu Karta (patrz rozdział 6 wyżej).

8.6 Listy TSL

Listy TSL zawierają wszystkie niezbędne dane na temat kwalifikowanych dostawców usług zaufania w UE (w tym polskich). Umożliwiają weryfikowanie podpisów złożonych przy użyciu kwalifikowanych certyfikatów wystawionych przez polskich, i innych unijnych, dostawców usług zaufania.

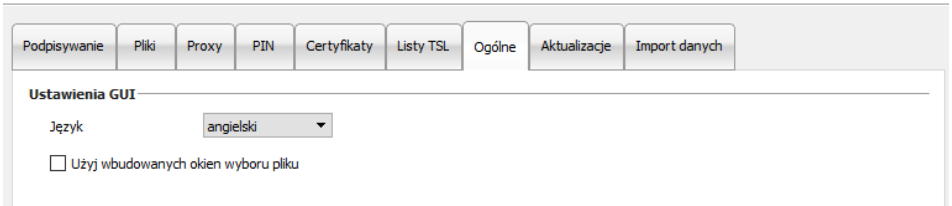
Zakładka przedstawia aktualny status list TSL, którymi dysponuje program. Udostępnia również możliwość ręcznego pobrania aktualnych list TSL wystawianych w poszczególnych krajach (przy czym pobieranie ręczne nie jest niezbędne do normalnej pracy, ponieważ program automatycznie pobiera nowe listy TSL w przypadku, gdy przy weryfikacji podpisu natrafi na certyfikat, który nie może być zweryfikowany w oparciu o posiadane przez program w danym momencie listy TSL).

W celu pobrania list TSL wciśnij klawisz *Pobierz listy TSL*.



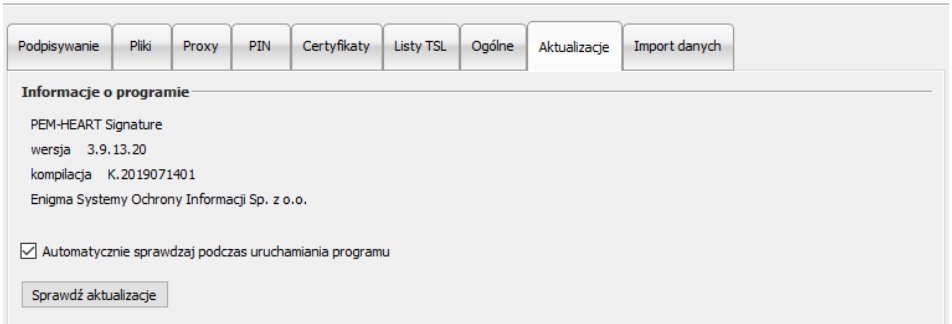
8.7 Ogólne

Zmiana języka programu na angielski lub polski:



8.8 Aktualizacje

W zakładce *Aktualizacje* można znaleźć informacje na temat wersji używanego programu oraz sprawdzić czy jest jego nowa wersja.

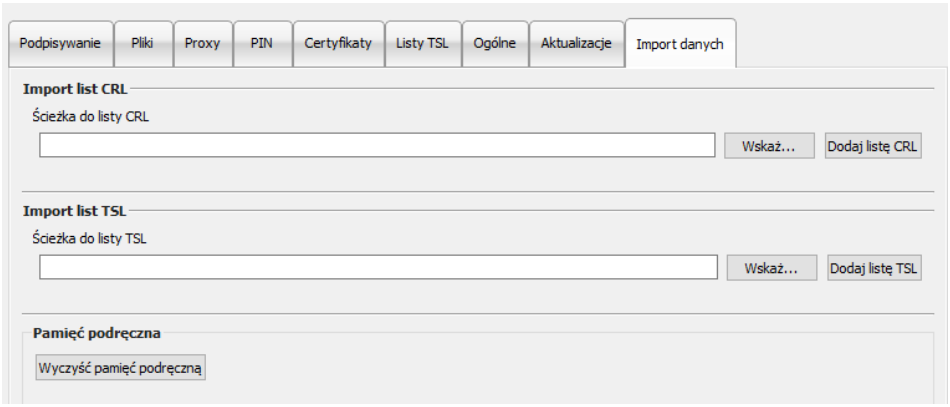


Informacji o dostępnej aktualizacji można dokonywać manualnie poprzez naciśnięcie przycisku *Sprawdź aktualizacje* lub ustalić opcje automatycznego sprawdzania czy podczas uruchamiania programu. W przypadku wykrycia nowej wersji oprogramowania zostaną wyświetlone komunikaty.

8.9 Import danych

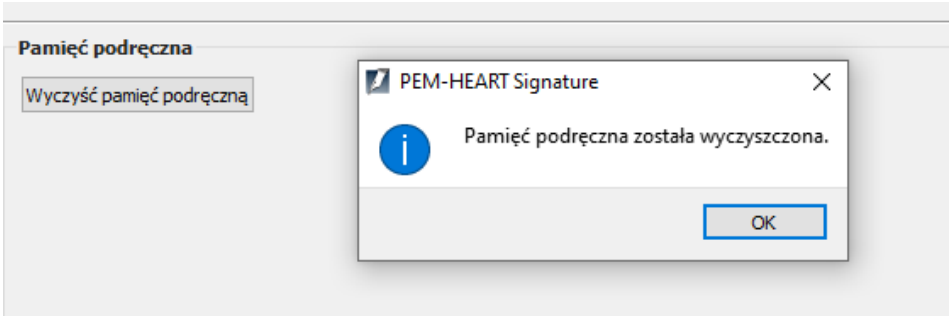
Opcje dotyczące importu danych służą do funkcjonowania programu w środowisku, w którym nie ma dostępu do Internetu. Dodawanie znaczników czasu i sprawdzanie statusu certyfikatu na podstawie OCSP jest w takiej sytuacji niemożliwe, ale składanie i weryfikacja podpisu wciąż są możliwe, pod warunkiem posiadania przez program aktualnych list TSL i CRL – które w tym przypadku trzeba przenieść i wczytać do programu ręcznie.

Uwaga! Składanie podpisów rSign (w chmurze) zawsze wymaga dostępu do Internetu.



W celu wczytania pliku z listą CRL albo TSL, naciśnij klawisz *Wskaż* przy odpowiedniej liście (po czym wskaż odpowiedni plik na dysku), a następnie odpowiednio klawisz *Dodaj listę CRL* albo *Dodaj listę TSL*.

Klawisz „Wyczyść pamięć podręczną” powoduje usunięcie bazy danych programu *PEM-HEART Signature*. Należy tego spróbować w specyficznych przypadkach, np. gdy występuje błąd bazy danych.



Baza danych zawiera dane podręczne (np. aktualną listę CRL), usunięcie jej nie powoduje negatywnych konsekwencji, ponieważ program po prostu pobierze brakujące dane z Internetu.

9 Rozwiązywanie problemów

Rozwiązywanie problemów:

PODPISYWANIE			
l.p.	**Problem**	**Przyczyna**	**Rozwiązanie**
1.	Z żadnego z serwerów nie udało się pobrać znacznika czasu	Do certyfikatu nie jest przypisany żadnej pakiet znaczników czasu	- spróbuj ponownie następnego dnia (dwa znaczniki dziennie można pobrać na darmo), albo - wykup pakiet znakowania czasem (szczegóły: http://www.cencert.pl), albo - wyłącz opcję znakowania czasem podpisów (patrz rozdział 3 wyżej)
2.		Program nie ma dostępu do Internetu	- sprawdź połączenie z Internetem - sprawdź ustawienia proxy (jeśli u Ciebie używany jest serwer proxy) – patrz rozdział 8.3 wyżej)
3.	Błąd wykonania podpisu: W celu złożenia następnego podpisu wybierz "Funkcje zaawansowane/dodaj podpis"	Plik zawiera już popis.	- dodaj podpis za pomocą polecenia „Dodaj podpis” (patrz rozdział 5.4 wyżej)
WERYFIKACJA			
l.p.	**Problem**	**Przyczyna**	**Rozwiązanie**
1.	Wskaż położenie dokumentów. Nie wszystkie dokumenty odłączone zostały znalezione….	Program nie znalazł w katalogu z podpisem pliku, który został podpisany.	Wskaż plik, który został podpisany (odpowiedni do podpisu, który jest weryfikowany)