DATA UTWORZENIA DOKUMENTU: 8/03/2024

PEM-HEART SIGNATURE INSTRUKCJA UŻYTOWNIKA

CENCERT

DOKUMENT PUBLICZNY

STWORZONY PRZEZ ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O. 02-230 WARSZAWA

UL. JUTRZENKI 116 | TELEFON: +48 22 570 57 10 | FAX: +48 22 570 57 15

WWW.ENIGMA.COM.PL

DATA UTWORZENIA DOKUMENTU: 8/03/2024
TYP DOKUMENTU: PUBLICZNY

ENIGMA SYSTEMY OCHRONY INFORMACJI SP. Z O.O.
JUTRZENKI 116
02-230 WARSZAWA
POLSKA

TELEFON: +48 22 570 57 10
FAX: +48 22 570 57 15
STRONA INTERNETOWA: WWW.ENIGMA.COM.PL

SPIS TREŚCI

1 WSTĘP

Oprogramowanie PEM-HEART Signature służy do:

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

Dodatkowo:

- weryfikacja podpisów elektronicznych po zakończeniu okresu ważności certyfikatu, jeśli podpis ma formę archiwalną (patrz opis formy archiwalnej w rozdziale **4.3.1 Panel Weryfikacji, str. 33**),
- weryfikacja podpisów opartych o certyfikaty zwykłe (niekwalifikowane) wydane przez Cencert.

PEM-HEART Signature wykonuje podpis elektroniczny w formatach:

- XAdES zgodnym ze specyfikacją techniczną ETSI TS 101 903 XML Advanced Electronic Signatures (XadES),
- CAdES CMS zgodnym ze specyfikacją techniczną ETSI TS 101 733 Electronic Signature Format (CAdES to skrót od CMS Advanced Electronic Signatures),
- PAdES (norma ETSI TS 102 778) - PDF Advanced Electronic Signatures,
- ASiC (norma ETSI TS 102 918) - program wykonuje podpis w formie ASX podstawowej, tworząc plik z rozszezrzeniem .asics . (plik zawiera podstawowy kontener ASiC XadES otaczający).

Formaty te określają strukturę pliku zawierającego podpis. Wybór określonego formatu pociąga za sobą wymaganie na oprogramowanie, które będzie w stanie zweryfikować poprawność takiego podpisu.

Producentem rozwiązań dla Cencert jest ENIGMA Systemy Ochrony Informacji Sp. z o.o. Podstawowa działalność spółki ENIGMA polega na opracowywaniu, produkcji i wdrażaniu innowacyjnych systemów ochrony informacji. Wykorzystując własne rozwiązania sprzętowe i programistyczne zapewnia najlepszą ochronę danych w

administracji państwowej i samorządowej, instytucjach finansowych i przedsiębiorstwach. Wszystkie produkty firmy ENIGMA dają pełną ochronę kryptograficzną gromadzonych, przetwarzanych i przesyłanych informacji. Oferowane rozwiązania są certyfikowane pod względem bezpieczeństwa przez wyspecjalizowane komórki Służb Ochrony Państwa.

Cencert jest zastrzeżonym znakiem towarowym firmy ENIGMA Systemy Ochrony Informacji.
Cencert jest kwalifikowanym podmiotem świadczącym kwalifikowane i niekwalifikowane usługi zaufania od roku 2009 - w zakresie wystawiania certyfikatów, kwalifikowanych znaczników czasu oraz usługi poświadczania ważności certyfikatów (OCSP). Podstawą prawną świadczenia usług Cencert jest w szczególności eIDAS (Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014), a także ustawa o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2016 poz. 1579).

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 grona osób, komputery przypadkowych osób itd.).

Program powinien być użytkowany w środowisku, w którym kod programu jest chroniony przed zmianą przez system operacyjny. Można to zrealizować wykorzystując systemy operacyjne oferujące kontrolę dostępu (Windows, Linux oraz MacOSX) czy też ustawiając takie prawa dostępu do katalogów z plikami wykonywalnymi, aby użytkownik nie miał prawa modyfikacji zawartych w nich plików wykonywalnych.

Program powinien być użytkowany w środowisku, w którym system operacyjny zabezpiecza przed możliwością przechwytywania przez wrogie systemy danych przesyłanych przez porty komputera, jak również danych wprowadzanych z klawiatury komputera do okienek programu. Można to zrealizować wykorzystując systemy operacyjne oferujące kontrolę dostępu (Windows, Linux oraz MacOSX) oraz zapewniając odpowiedni poziom ochrony komputera przed uprawnionymi użytkownikami (ochrona poprzez ustalenie odpowiednich praw dostępu oraz uaktualnianie na bieżąco systemu operacyjnego), nieuprawnionymi użytkownikami oraz atakami z sieci komputerowej (ochrona poprzez uaktualnianie na bieżąco systemu operacyjnego, a w razie potrzeby zastosowanie urządzeń typu firewall).

Program, pracując jako „bezpieczne urządzenia do składania i weryfikacji bezpiecznych podpisów elektronicznych", nie może być wykorzystywany w „środowisku publicznym" - to jest w środowisku, w którym do oprogramowania w normalnych warunkach eksploatacji może mieć dostęp każda osoba fizyczna.

Komponent techniczny lub dostarczone do niego sterowniki, wchodzące obok programu w skład „bezpiecznego urządzenia do składania i weryfikacji bezpiecznych podpisów elektronicznych", posiadają funkcję niszczenia danych służących do składania podpisów (czyli klucza prywatnego) na życzenie użytkownika. Niszczenie wykonywane jest w takim stopniu, aby uniemożliwić odtworzenie tych danych na podstawie analizy zapisów w urządzeniach, w których były tworzone, przechowywane lub stosowane.

3 INSTALACJA

Paczki instalacyjne są udostępniane poprzez stronę www Cencert:

https://www.cencert.pl/do-pobrania/oprogramowanie-do-podpisu/

3.1 INSTALACJA DLA SYSTEMU WINDOWS

3.1.1 INSTALACJA

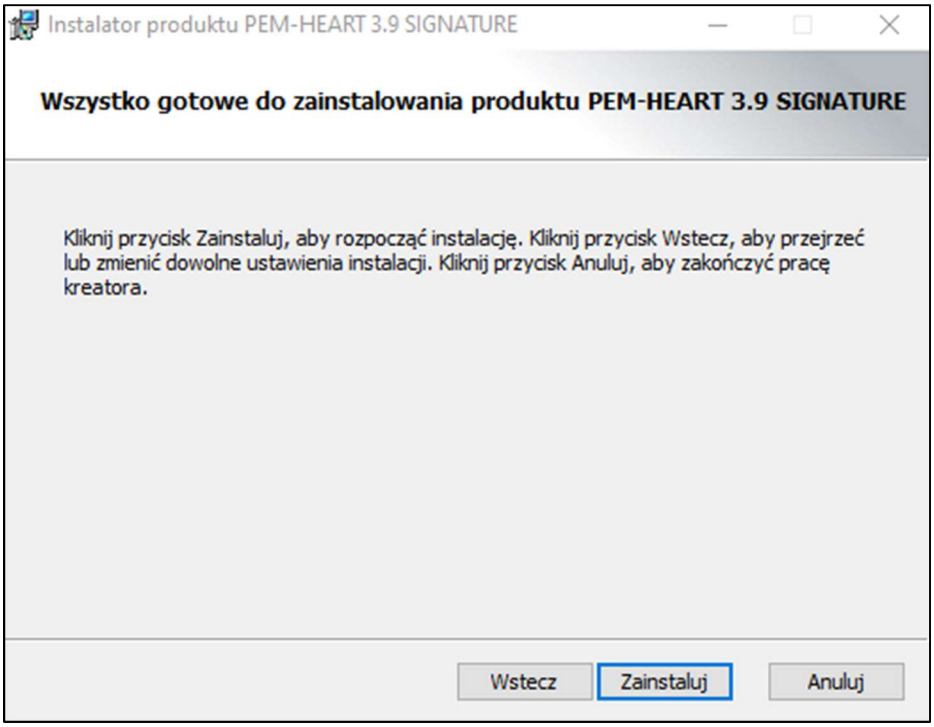
Instalację należy przeprowadzać z konta o uprawnieniach administratora. Zalecane jest, aby przed rozpoczęciem instalacji zakończyć działanie wszystkich aplikacji poza niezbędnymi dla działania systemu operacyjnego.

Poniższa procedura instalacji przedstawiona jest na przykładzie systemu Windows 11:

1. Należy uruchomić instalator *pemheart-signature.exe*, spowoduje to wyświetlenie startowego okna instalacji.

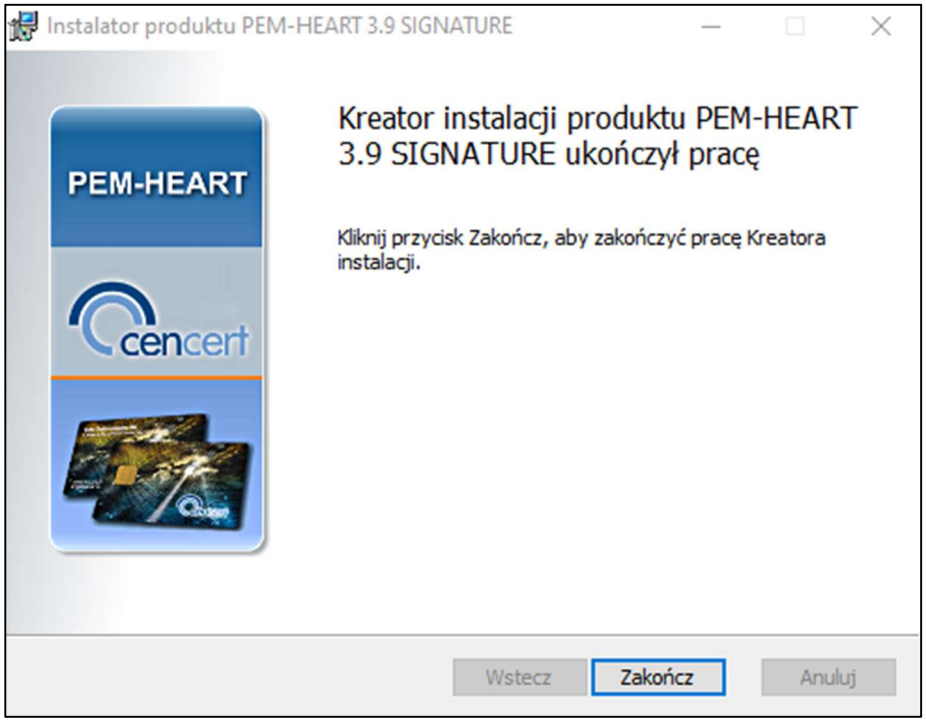
Rysunek 1 Okno startowe kreatora instalacji

2. Klikając przycisk *Zainstaluj* zostanie zainicjowany *Kreator instalacji produktu PEM-HEART 3.9 Signature*.



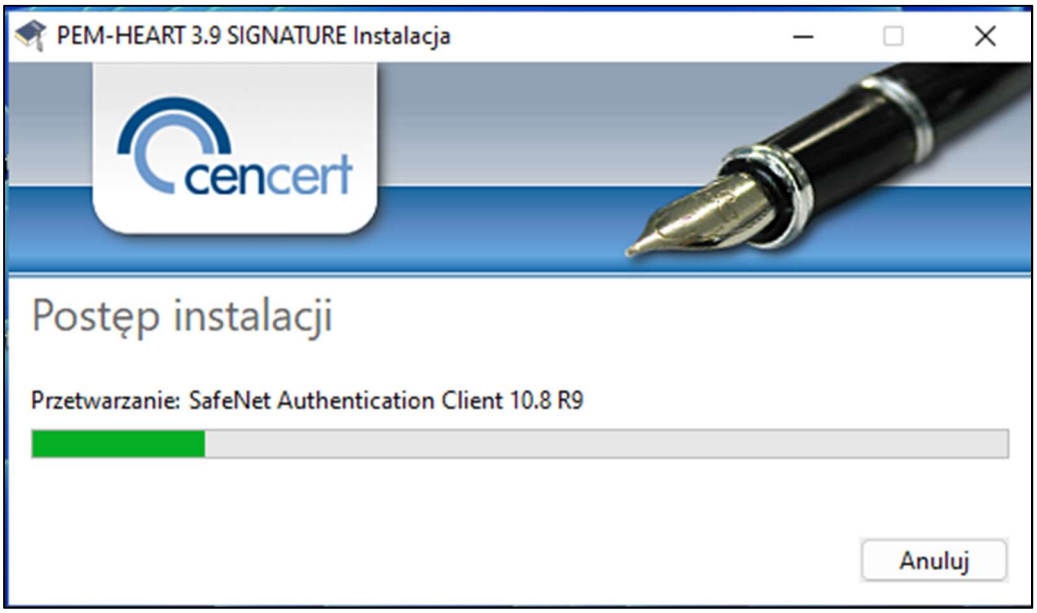
Rysunek 2 Okno kreatora instalacji

3. Kliknąć *Zainstaluj*, zostanie rozpoczęta instalacja oprogramowania.
4. Kliknąć *Zakończ* - zakończona zostanie praca kreatora. Spowoduje to również uruchomienie procesu instalacji oprogramowania Thales SafeNet.



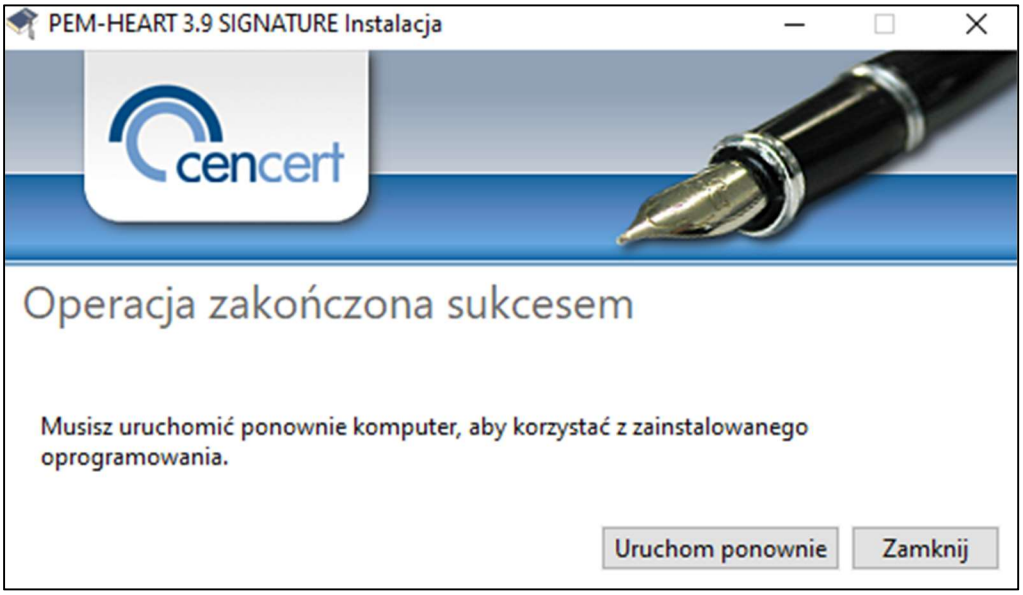
Rysunek 3 Okno kończące działanie kreatora instalacji

5. Wyświetlony zostanie kreator instalacji oprogramowania Thales SafeNet.



Rysunek 4 Instalacja programu Thales SafeNet

6. Kliknąć *Uruchom ponownie* - jest to wymagane w celu rozpoczęcia pracy z oprogramowaniem.

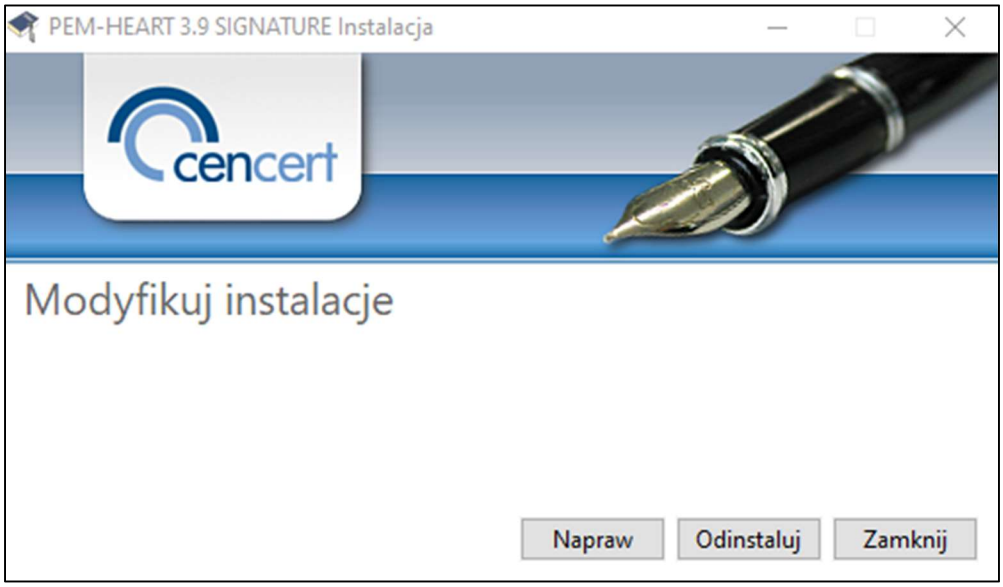


Rysunek 5 Okno zakończenia procesu instalacji

3.1.2 USUWANIE PROGRAMU

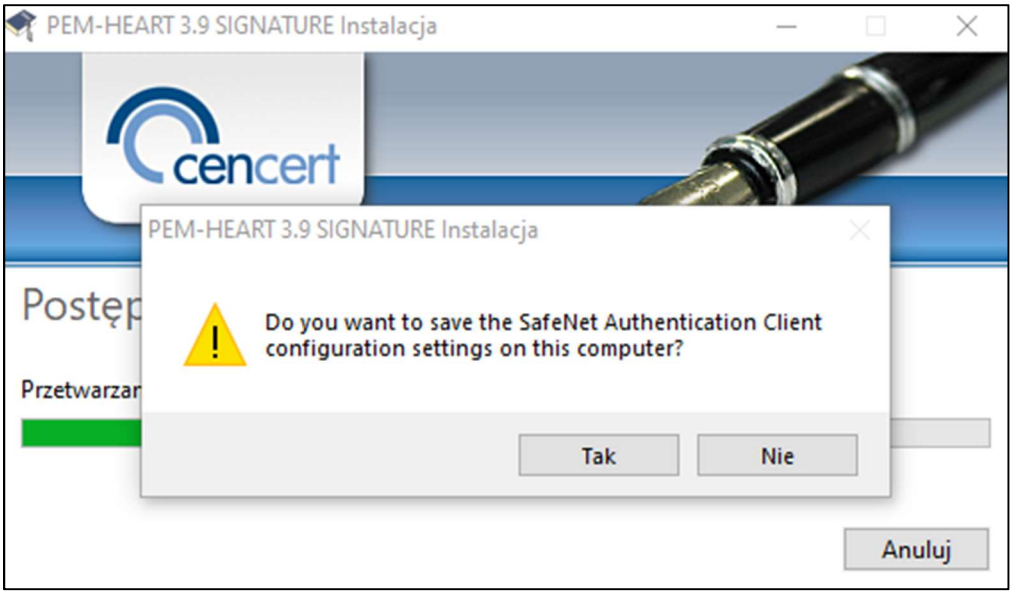
Usuwanie programu odbywa się poprzez wybranie pakietu „PEM-HEART SIGNATURE” z poziomu Panelu Sterowania Windows: Panel sterowania\Programy\Programy i funkcje.

1. Uruchomiony zostanie kreator instalacyjny. Należy kliknąć w przycisk *Odinstaluj* - program rozpocznie proces usuwania programu z zasobów systemu operacyjnego.



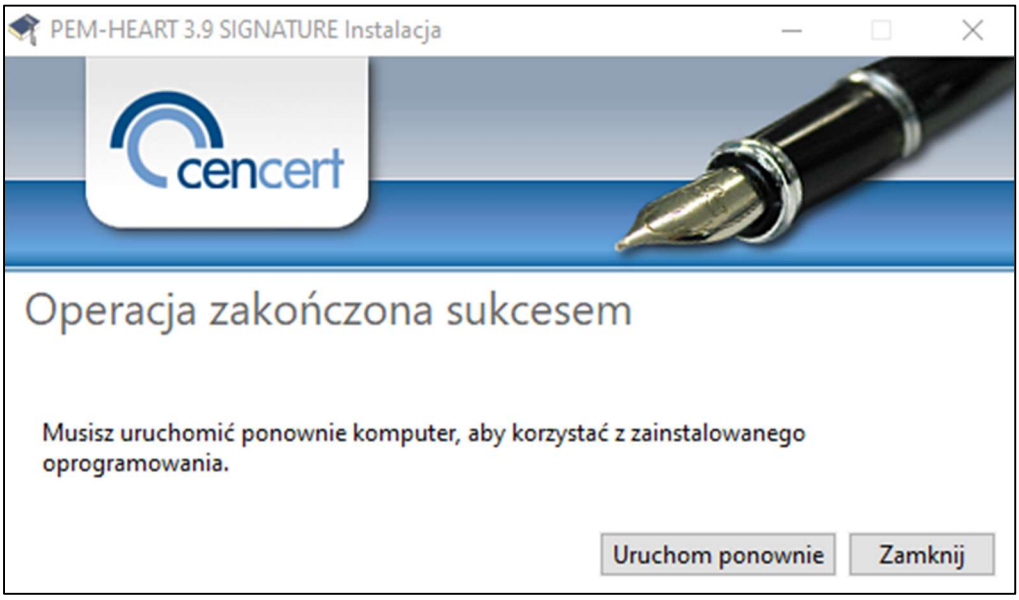
Rysunek 6 Opcje modyfikacji instalacji

2. W trakcie procesu wyświetlony zostanie komunikat z zapytaniem o usunięcie lub zachowanie konfiguracji dla programu SafeNet dla obsługi kart typu Thales.



Rysunek 7 Deinstalacja programu

3. Kreator instalacyjny poinformuje o zakończeniu procesu usuwania oprogramowania. Wymagane jest ponowne uruchomienie komputera, klikając w *Uruchom ponownie*.



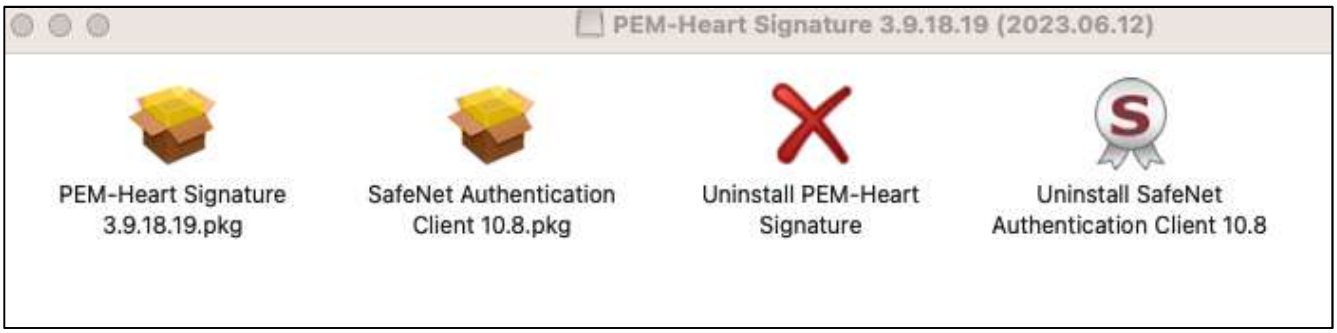
Rysunek 8 Potwierdzenie deinstalacji programu

3.2 INSTALACJA DLA SYSTEMU MACOS

Paczka pakietu Pem-Heart dla MacOS dystrybuowana jest poprzez format .dmg - zawiera on pliki instalacyjne i deinstalatory.

Pem-Heart posiada wsparcie dla systemów MacOS w wersjach: 13 (Ventura) i 14 (Sonoma)

Poniższa instrukcja powstała w oparciu o system MacOS Ventura.



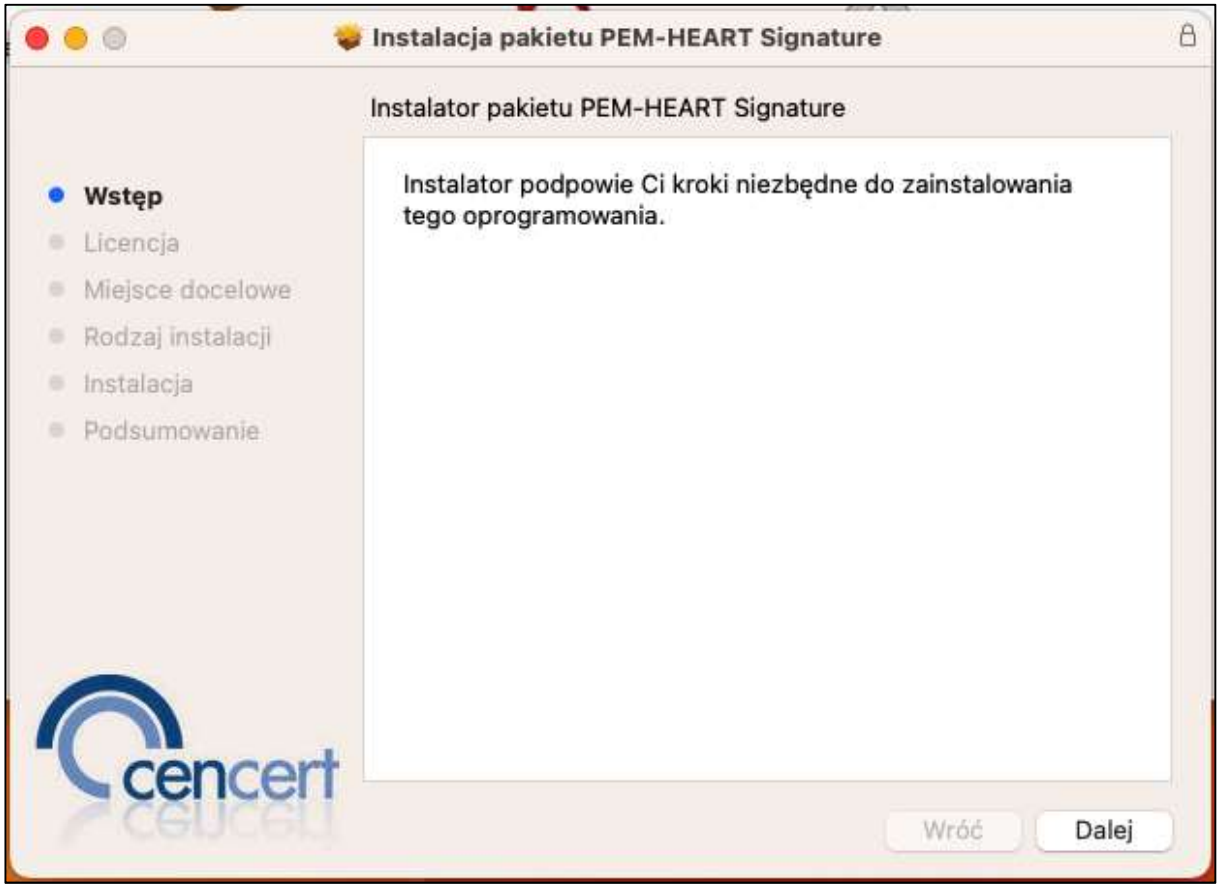
Rysunek 9 Paczka pakietu Pem-Heart dla MacOS

3.2.1 INSTALACJA POPRZEZ MENEDŻERA PLIKÓW

Instalację należy przeprowadzać z konta o uprawnieniach administratora. Zalecane jest, aby przed rozpoczęciem instalacji zakończyć działanie wszystkich aplikacji poza niezbędnymi dla działania systemu operacyjnego.

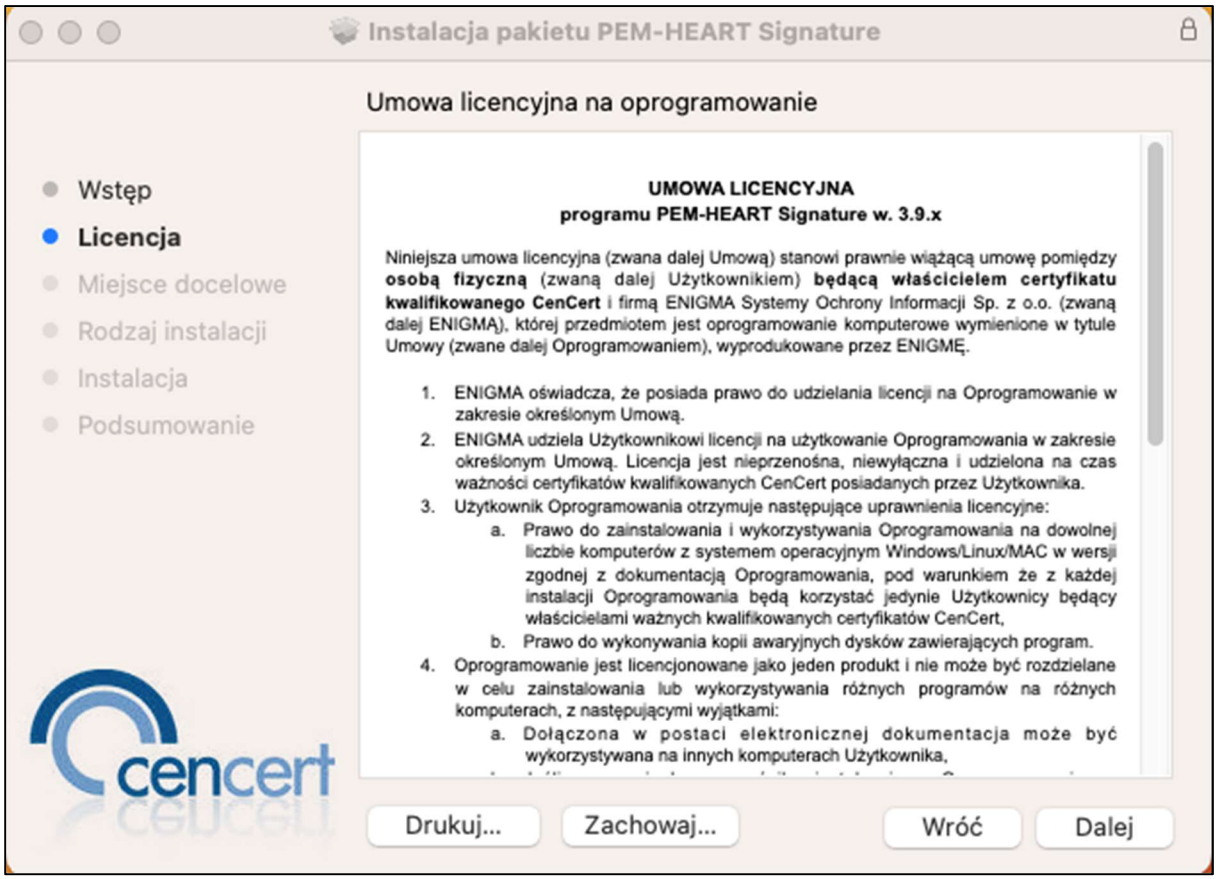
Dostępne są wersje programu pod architekturę procesorów INTEL oraz ARM

W menedżerze plików Finder należy zlokalizować w strukturze plików miejsce z plikiem instalacyjnym PEM-HEART Signature. Należy uruchomić plik, spowoduje to zainicjowanie instalatora.

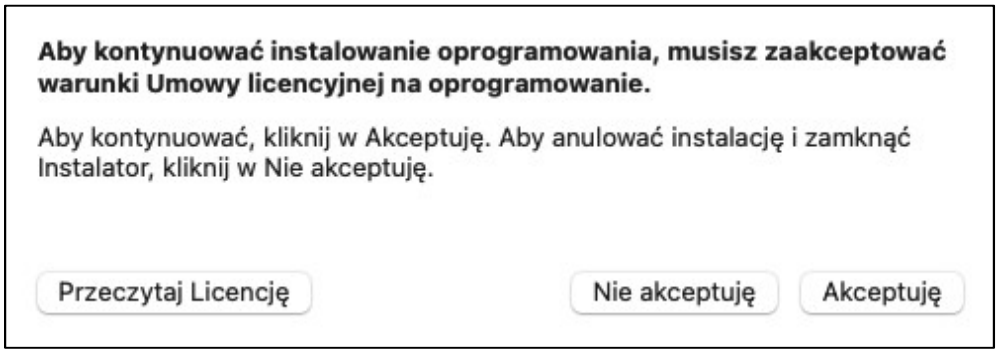


Rysunek 10 Instalator pakietu Pem-Heart - okno startowe

1. W pierwszym etapie instalacji użytkownik musi zaakceptować umowę licencyjną.

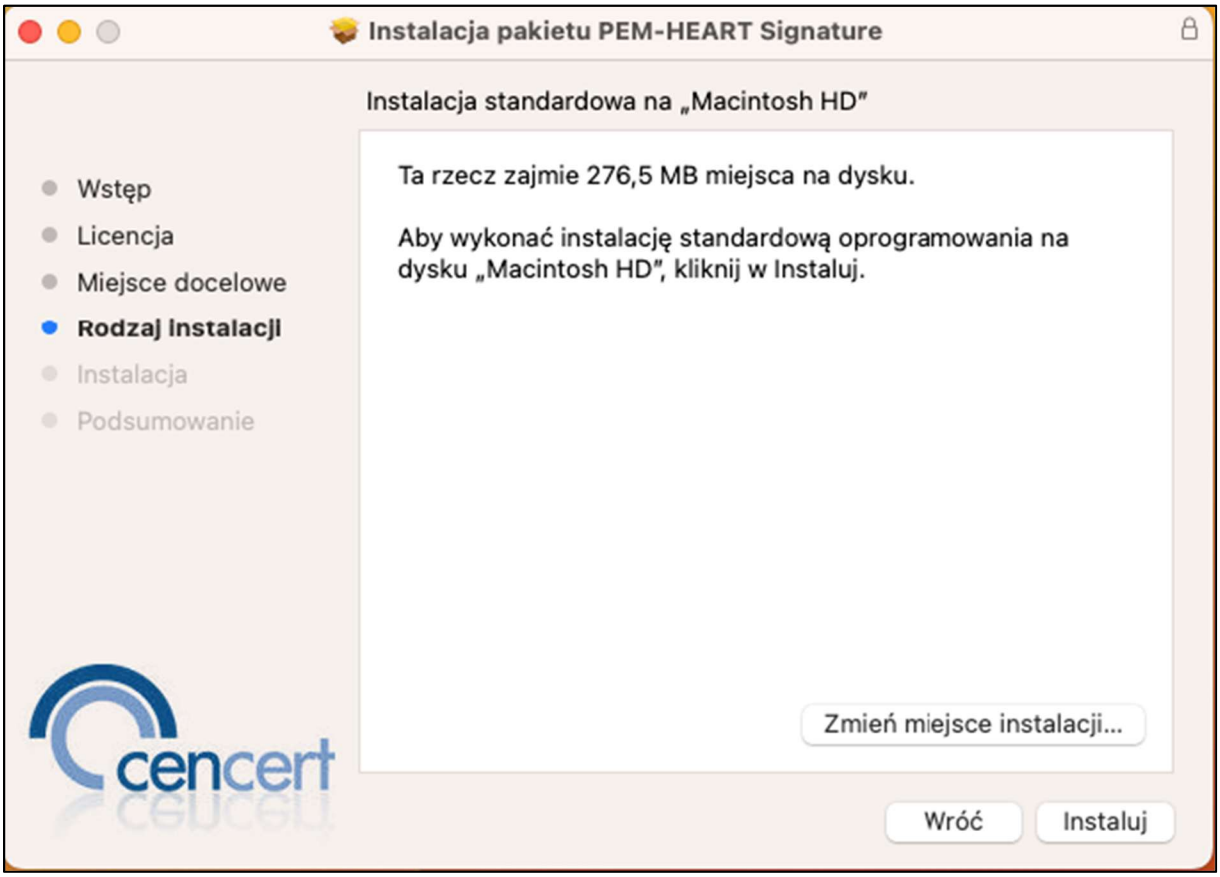


Rysunek 11 Instalator pakietu Pem-Heart - umowa licencyjna



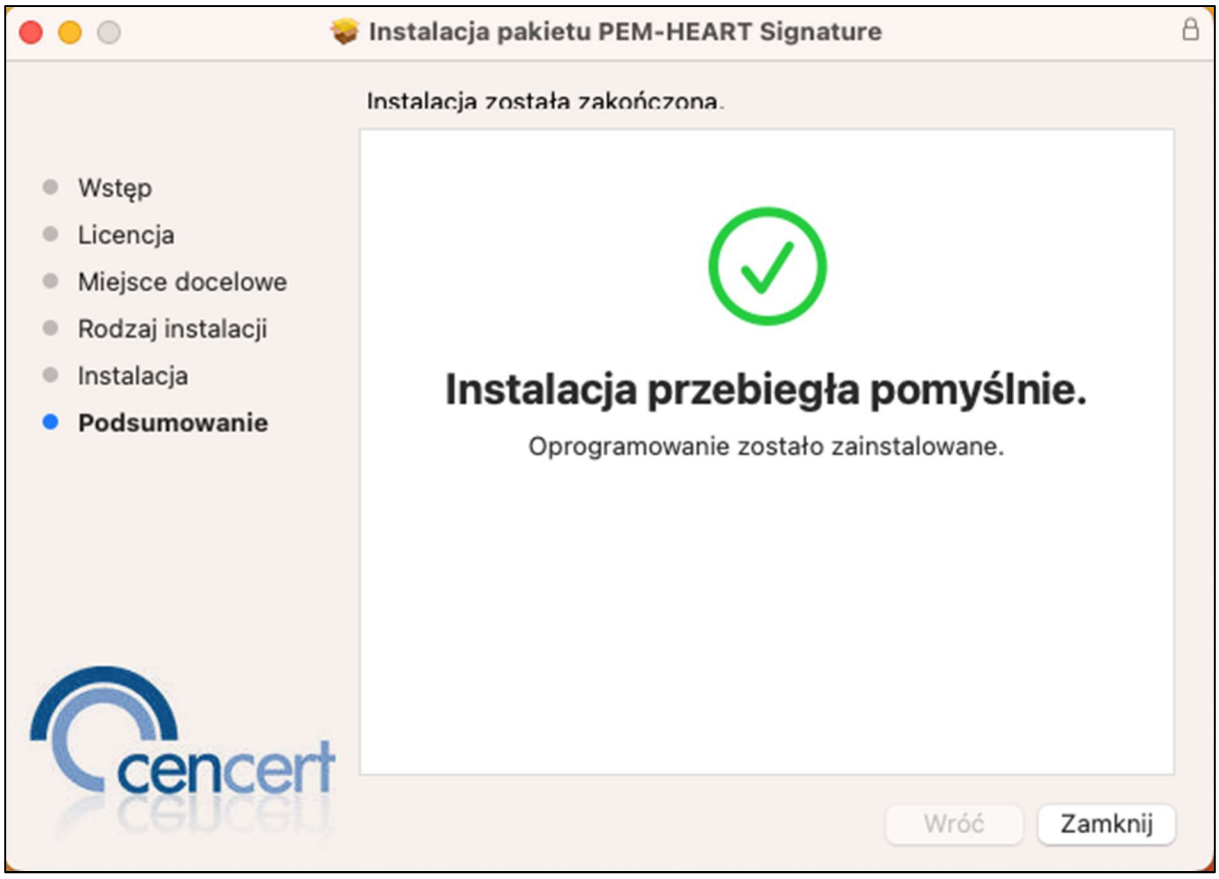
Rysunek 12 Instalator pakietu Pem-Heart - akceptacja umowy licencyjnej

2. Następnie potwierdzić zamiar instalacji poprzez kliknięcie przycisku *Instaluj* i wpisanie hasła do konta użytkownika - proces instalacji zostanie rozpoczęty. W tym momencie jest również możliwa zmiana miejsca docelowego instalacji klikając w „Zmień miejsce instalacji...".



Rysunek 13 Instalator pakietu Pem-Heart - informacja o instalacji

3. Po zakończonym procesie instalacji zostanie wyświetlony ekran podsumowujący.



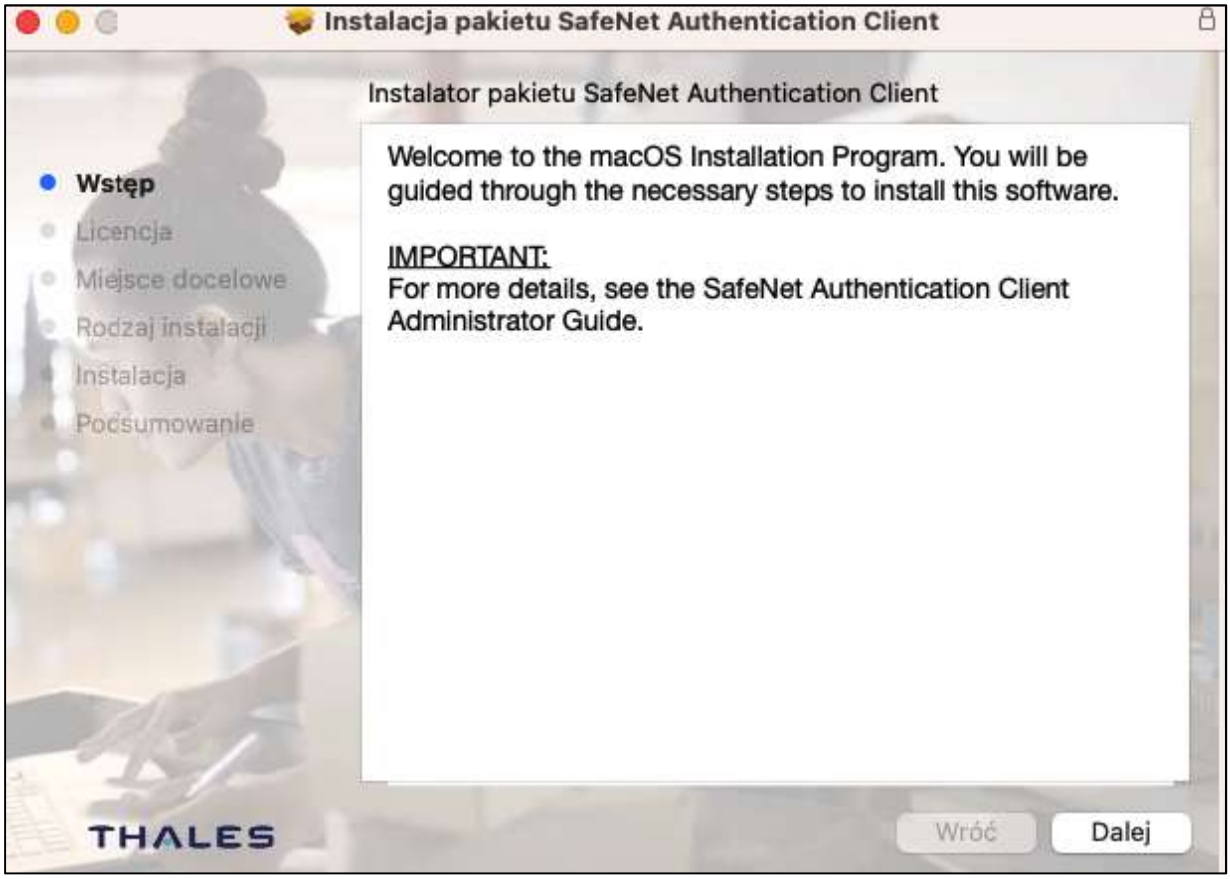
Rysunek 14 Instalator pakietu Pem-Heart - podsumowanie instalacji

3.2.2 INSTALACJA PROGRAMU SAFENET CLIENT

Program SafeNet firmy Thales obsługuje karty IDPrime.

Instalację należy przeprowadzać z konta o uprawnieniach administratora. Zalecane jest, aby przed rozpoczęciem instalacji zakończyć działanie wszystkich aplikacji poza niezbędnymi dla działania systemu operacyjnego.

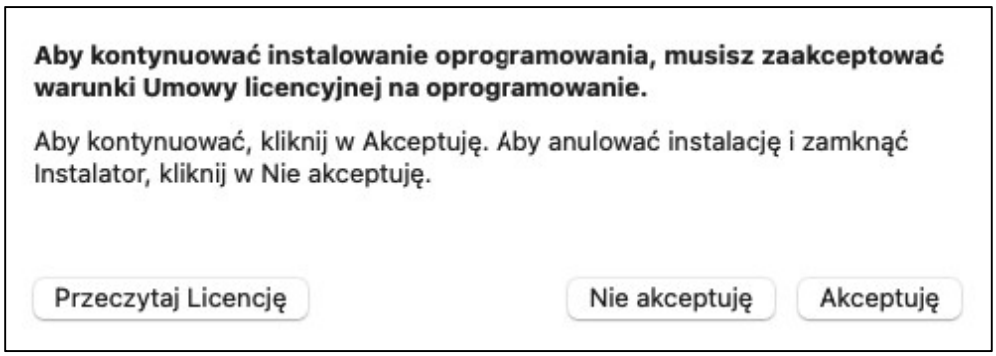
W menedżerze plików Finder należy zlokalizować w strukturze plików miejsce z plikiem instalacyjnym programu SafeNet Authentication Client. Uruchomienie pliku spowoduje zainicjowanie instalatora.



Rysunek 15 Instalator pakietu SafeNet Authentication Client - okno startowe

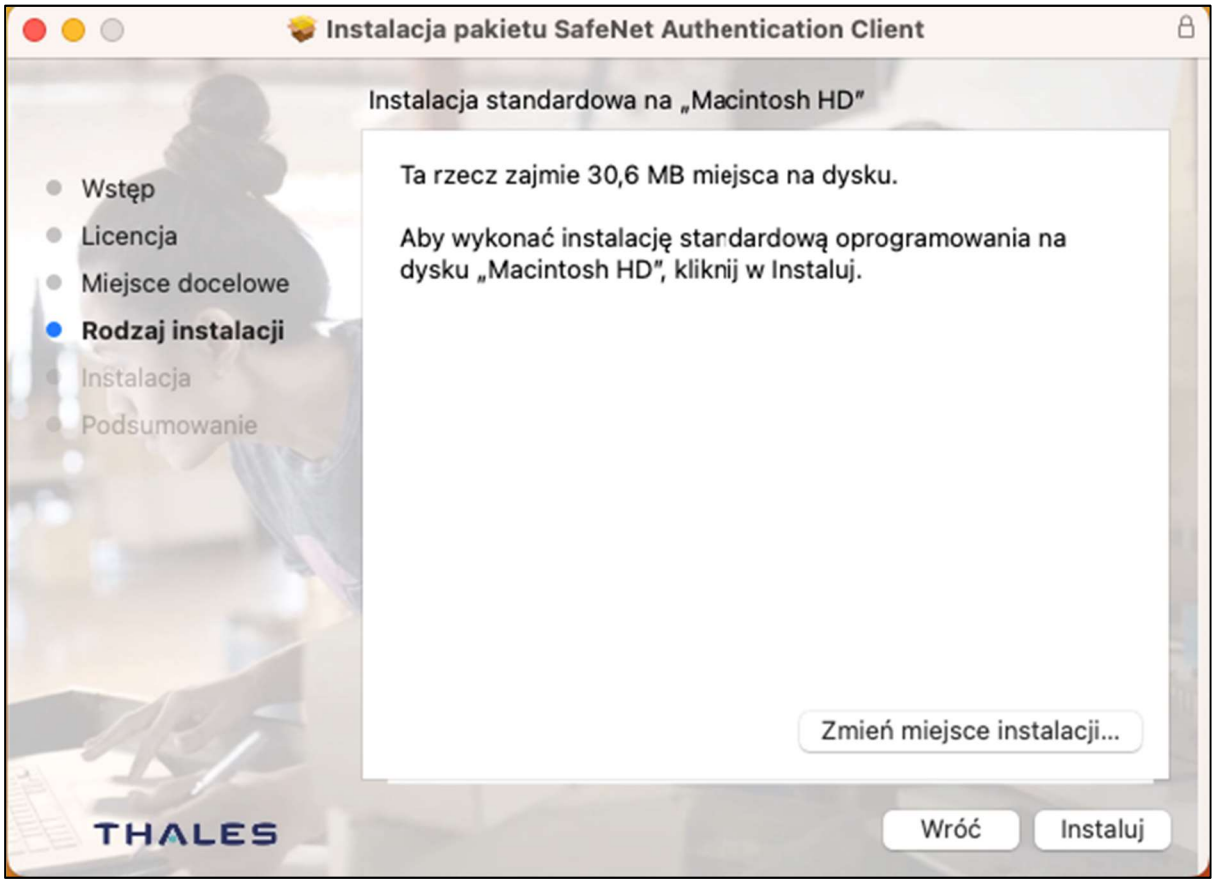
1. W pierwszym etapie instalacji użytkownik musi zaakceptować umowę licencyjną.

Rysunek 16 Instalator pakietu SafeNet Authentication Client – umowa licencyjna



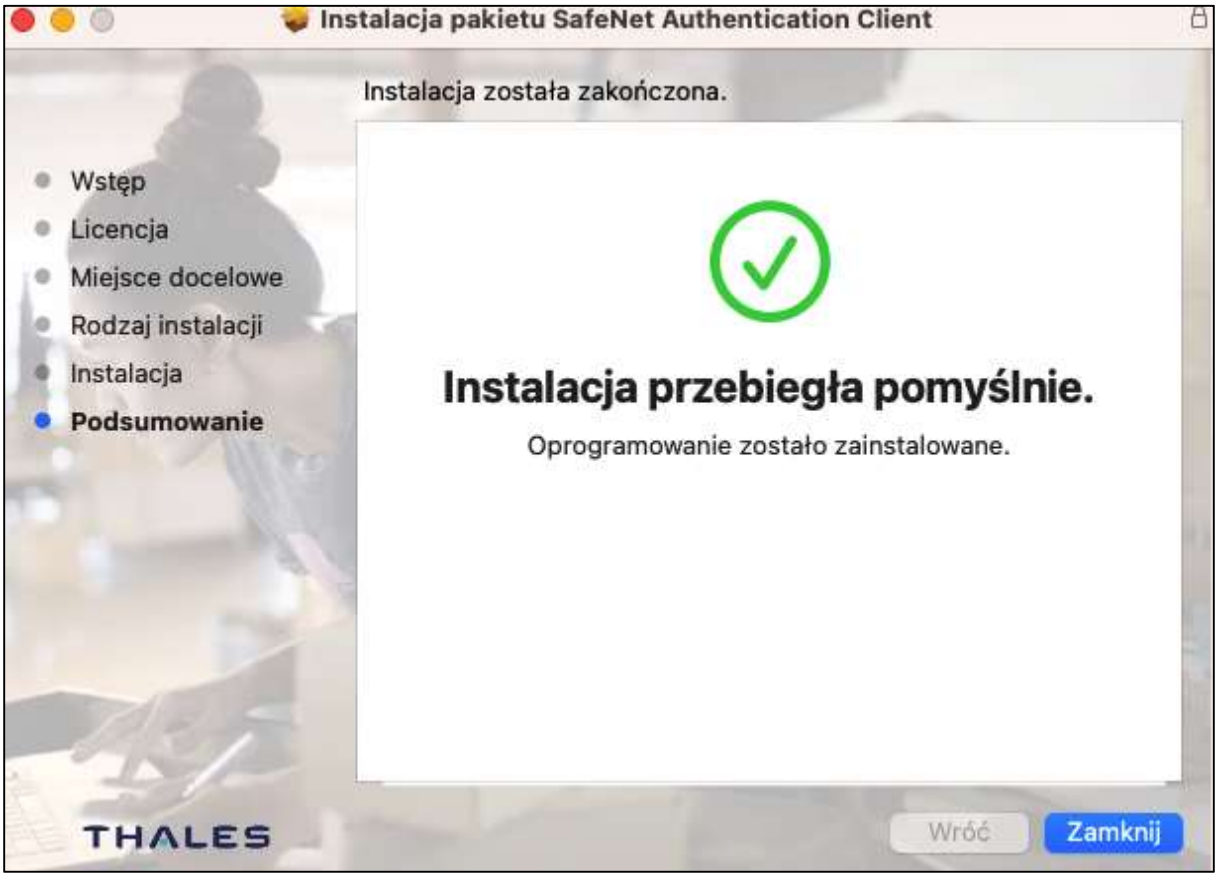
Rysunek 17 Instalator pakietu SafeNet Authentication Client - akceptacja umowy licencyjnej

2. Następnie potwierdzić zamiar instalacji poprzez kliknięcie przycisku *Instaluj* i wpisanie hasła do konta użytkownika - proces instalacji zostanie rozpoczęty. W tym momencie jest również możliwa zmiana miejsca docelowego instalacji poprzez kliknięcie w „Zmień miejsce instalacji...”.



Rysunek 18 Instalator pakietu SafeNet Authentication Client – informacja o instalacji

3. Po zakończonym procesie instalacji zostanie wyświetlony ekran podsumowujący.



Rysunek 19 Instalator pakietu SafeNet Authentication Client - podsumowanie instalacji

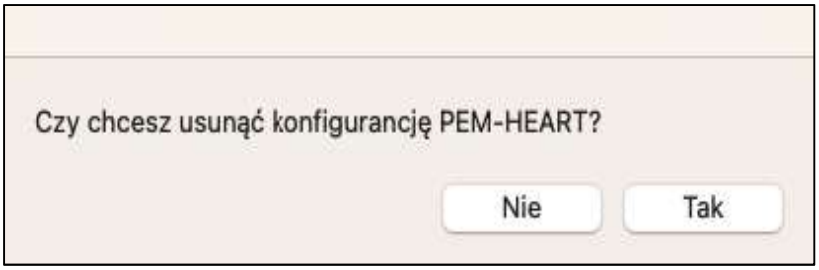
3.2.3 USUWANIE PROGRAMU

Deinstalacja jest wykonana po uruchomieniu programu *Uninstall PEM-Heart Signature*. Zostaną wyświetlone okna dialogowe z pytaniami odnośnie akceptacji usuwania:

- aplikacji PEM-HEART wraz z poszczególnymi składnikami oprogramowania,

Rysunek 20 Komunikat deinstalacyjny o usunięcie aplikacji Pem-Heart

- konfiguracji PEM-HEART z katalogów *opt*, *etc* i katalogu domowego,

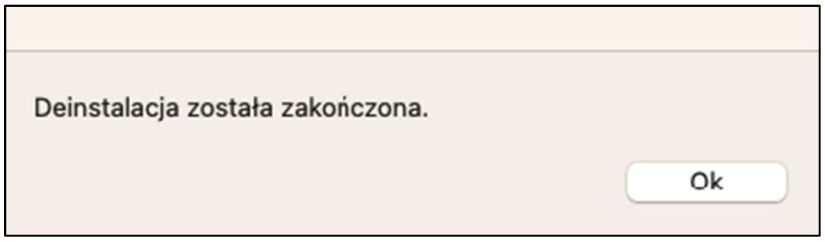


Rysunek 21 Komunikat deinstalacyjny o usunięcie konfiguracji Pem-Heart

- pliki konfiguracyjne rSign (enigmaCloud.ini).

Rysunek 22 Komunikat deinstalacyjny o usunięcie konfiguracji rSign

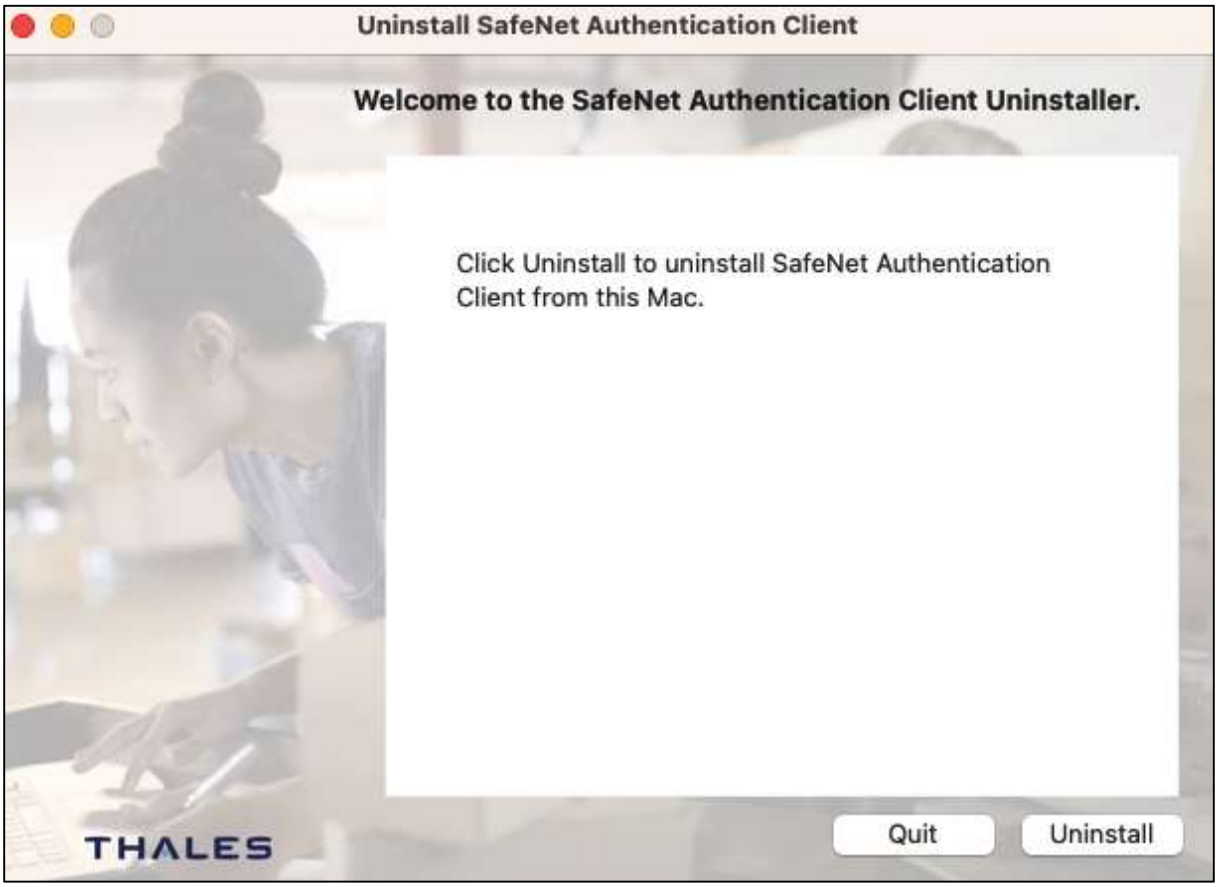
Na koniec procesu zostanie wyświetlone okno potwierdzające deinstalację:



Rysunek 23 Potwierdzenie deinstalacji programu

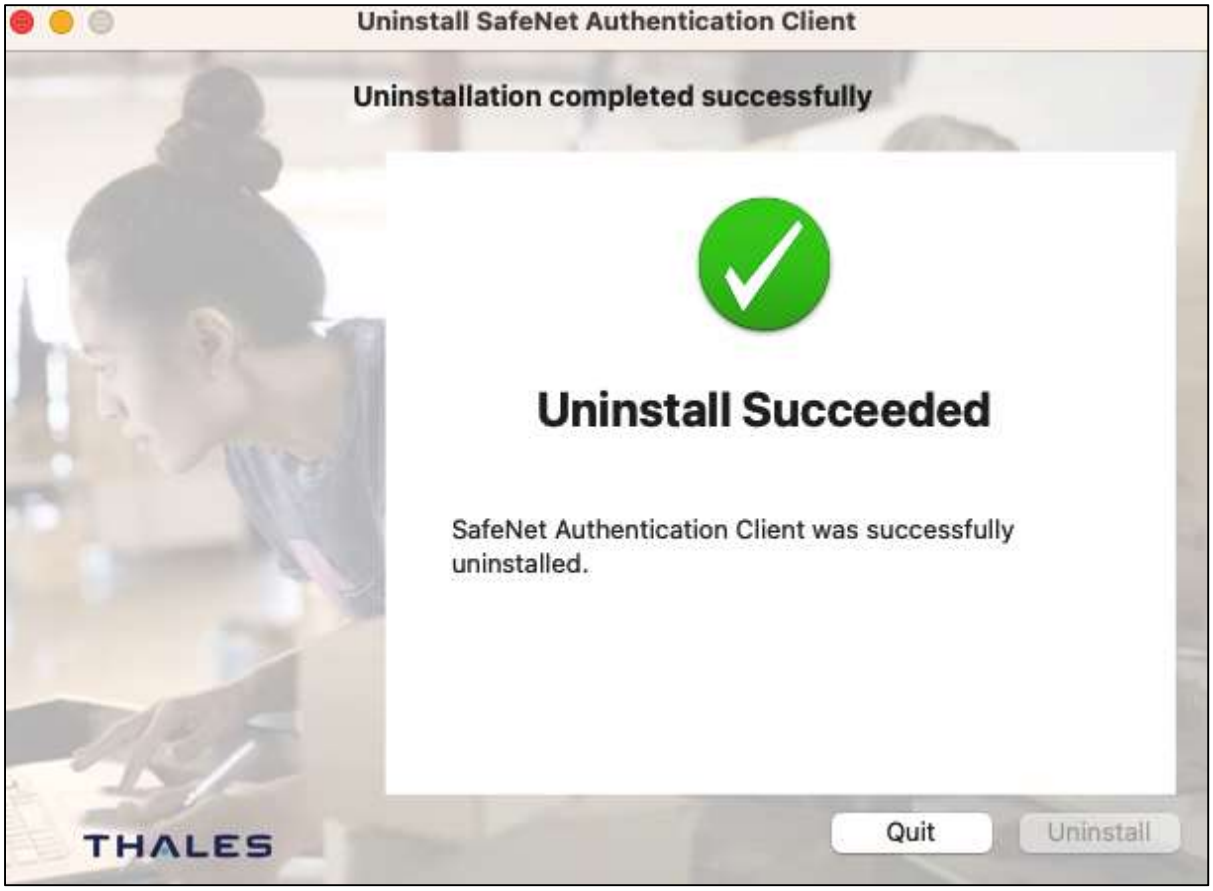
3.2.4 USUWANIE SAFENET CLIENT

Usuwanie oprogramowania do obsługi kart firmy Thales odbywa się z poziomu Panelu Sterowania, w opcji *Programy i funkcje*, gdzie z dostępnej listy trzeba wskazać program i wybrać opcję *Odinstaluj* lub *Odinstaluj/zmień*.



Rysunek 24 Deinstalator oprogramowania SafeNet Authentication Client – okno startowe

W oknie kreatora deinstalacji kliknąć *Uninstall* i wpisać hasło. Wyświetlone zostanie potwierdzenie procesu.



Rysunek 25 Deinstalator SafeNet Authentication Client – podsumowanie deinstalacji

3.3 INSTALACJA DLA SYSTEMU LINUX

Instalację należy przeprowadzać z konta o uprawnieniach administratora. Zalecane jest, aby przed rozpoczęciem instalacji zakończyć działanie wszystkich aplikacji poza niezbędnymi dla działania systemu operacyjnego.

Poniższa procedura instalacji przedstawiona jest na przykładzie systemu Ubuntu 20.04 LTS, w systemowym menedżerze pakietów (np. Oprogramowanie Ubuntu) oraz poprzez terminal z linii komend.

Operację instalacji pakietu należy poprzedzić zainstalowaniem wymaganych pakietów: pcscd oraz libncurses5. Można to zrobić przy użyciu komend:

sudo apt-get install pcscd

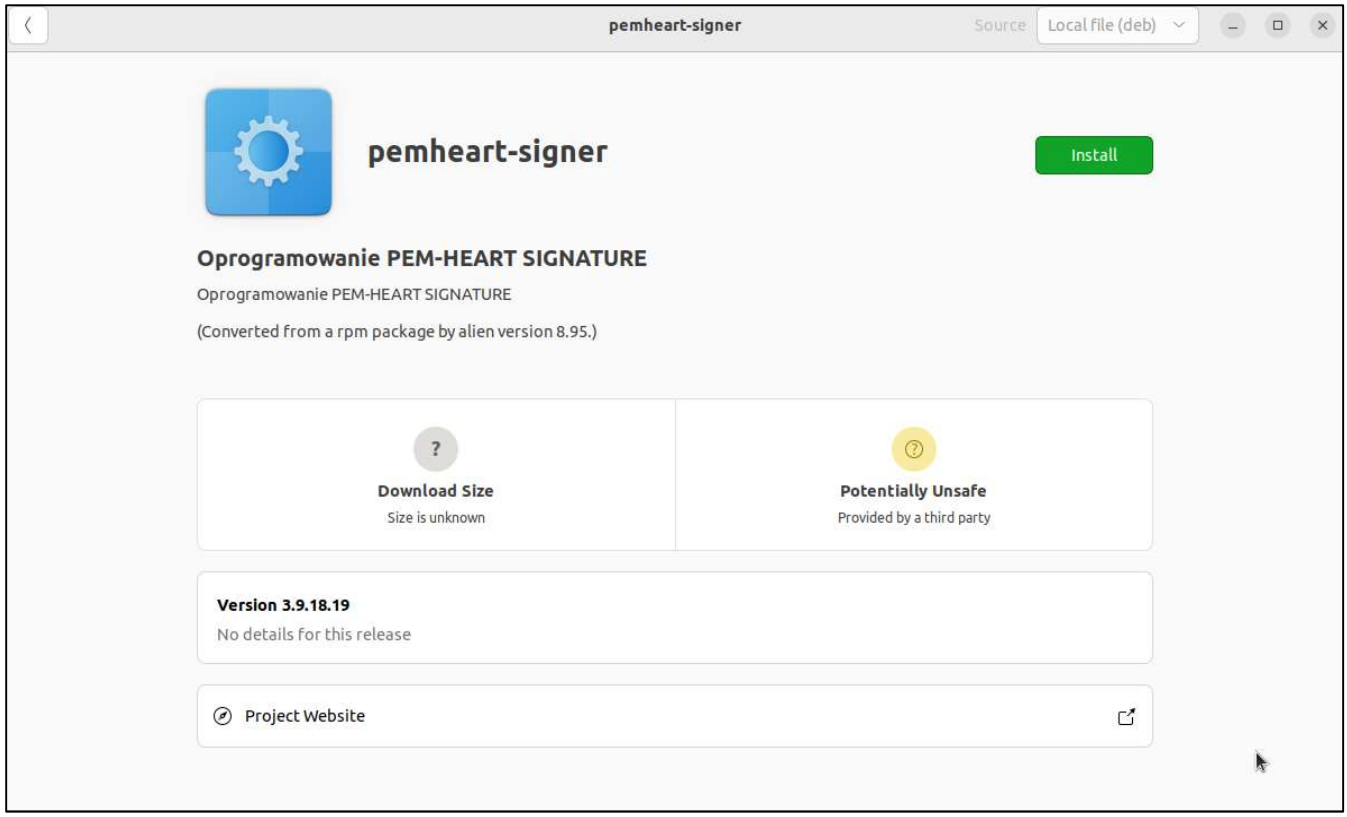
sudo apt-get install libncurses5

3.3.1 INSTALACJA POPRZEZ MENEDŻERA PLIKÓW

W menedżerze należy zlokalizować w strukturze plików miejsce, w którym znajdują się pliki instalacyjne PEM-HEART Signature. Instalacji dokonuje się poprzez uruchomienie (dwuklik) danego pliku. Otwarty zostanie wtedy domyślnie skojarzony menedżer pakietów. Po wciśnięciu przycisku *Zainstaluj* PEM-HEART Signature zostaje zainstalowany w systemie.

Po zakończeniu instalacji pojawi się odpowiedni komunikat i okno instalatora może zostać zamknięte. Na koniec należy zainstalować program Safenet Authentication Client, aby umożliwić korzystanie ze wszystkich dostępnych kart. Plik instalacyjny można pobrać ze strony cencert.pl.

Safenet Authentication Client podczas instalacji wymaga posiadania zainstalowanego w systemie pakietu libgdk-pixbuf2.0-0. Po instalacji dostęp do programu jest możliwy poprzez menu kontekstowe plików lub też poprzez systemowe menu programów.



Rysunek 26 Instalacja programu dla systemu Linux poprzez menedżer plików

W celu instalacji należy kliknąć w prawym górnym rogu zielony przycisk *Install*.

3.3.2 INSTALACJA POPRZEZ LINIĘ KOMEND

Poniżej przedstawiono opcję instalacji PEM-HEART Signature poprzez linię komend.

Po uruchomieniu okna terminala należy zlokalizować w strukturze plików miejsce, w którym znajdują się pliki instalacyjne. Oprogramowanie dystrybuowane jest w postaci pakietu instalacyjnego (plik z rozszerzeniem .deb). Aby zainstalować pakiet "PEM-HEART Signature" w systemie Ubuntu (tutaj w wersji 20.4 LTS), należy wywołać polecenie:

sudo dpkg -i PH-3.9.X.X_amd64.deb

gdzie X.X to numer wydanej wersji oprogramowania.

3.3.3 USUWANIE OPROGRAMOWANIA

Do usunięcia oprogramowania z systemu można wykorzystać terminal z linią komend lub też uruchomić menedżer pakietów.

- Usuwanie poprzez linię komend

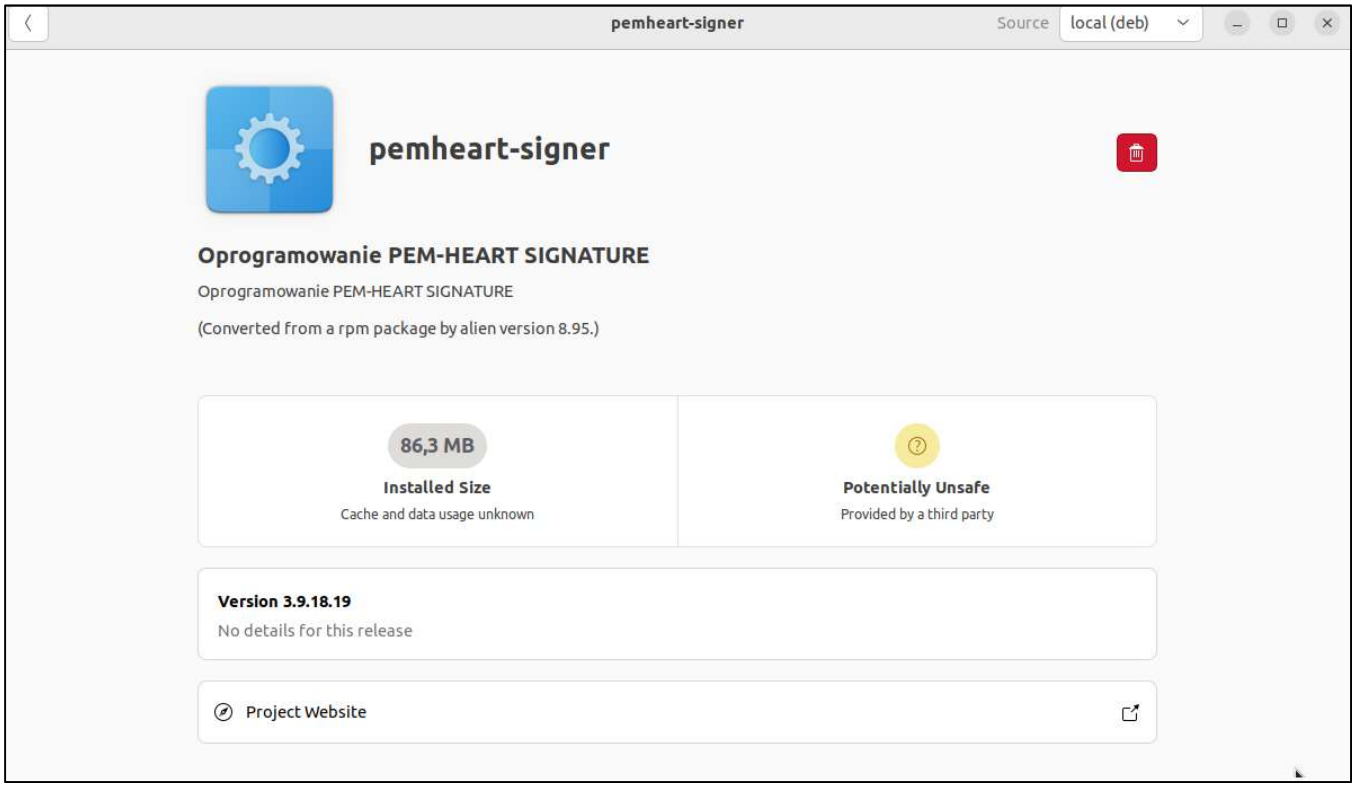
Deinstalacja PEM-HEART Signature dokonywana jest za pomocą dwóch programów konsolowych:

sudo apt-get purge pemheart-signer lub

sudo apt remove pemheart-signer

- Usuwanie poprzez menedżera plików

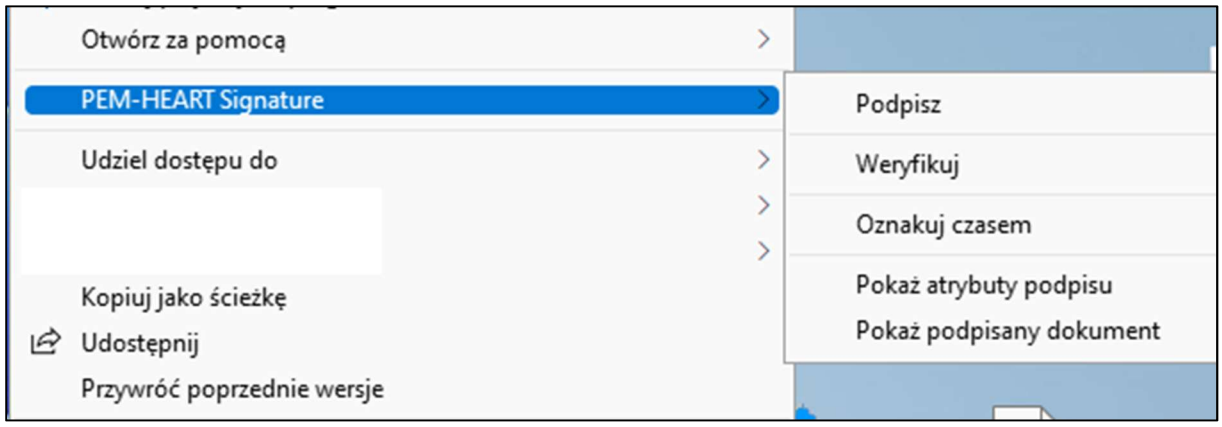
Po uruchomieniu menedżera pakietów (w przykładzie wykorzystano Oprogramowanie Ubuntu) należy znaleźć w zakładce „Zainstalowane” pemheart-signer, a następnie kliknąć czerwony kosz (***Rysunek 27 Deinstalacja programu dla systemu Linux poprzez menedżer plików***).



Rysunek 27 Deinstalacja programu dla systemu Linux poprzez menedżer plików

4 OPERACJE NA PLIKACH

Użytkownik niektóre operacje może dokonać bez bezpośredniego uruchamiania programu – klikając prawym przyciskiem myszy (PPM) na plik. Z poziomu menu kontekstowego są dostępne różne funkcje m.in. złożenia podpisu czy weryfikacji podpisu. W zależności od rodzaju pliku, wybór opcji może się różnić.



Rysunek 28 Przykładowe funkcje PPM dla pliku PDF

4.1 SKŁADANIE PODPISÓW – PODPIS NA KARCIE LUB TOKENIE USB

W celu złożenia podpisu włóż swoją kartę Cencert (do czytnika usb token do portu USB), a następnie kliknij prawym klawiszem myszy (PPM) na pliku do podpisu by rozwinąć menu kontekstowe - należy wybrać z niego kolejno opcje *PEM-HEART Signature -> Podpisz* (w przypadku wielu aplikacji, opcja może znajdować się pod *Pokaż więcej opcji*). Operację dokonuje się również z poziomu uruchomionej aplikacji PEM-HEART Signature (opis czynności przedstawiono w **5.2.1 Składanie podpisów – podpis na karcie lub tokenie USB, str. 37**)

Program automatycznie wybierze zalecany format podpisu, a następnie poprosi o PIN do karty.

Uwagi:

- Zaawansowane opcje, takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia, są dostępne pod przyciskiem *Opcje...*. Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są

zapamiętywane do późniejszego użycia. Patrz też rozdział **8.1 Zmiana parametrów podpisywania, str. 60**.

- W zależności od formatu podpisu, zostanie on zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
- W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. Wybranie tej opcji wymaga późniejszego przekazania odbiorcy dwóch plików: plik oryginalny i podpisu.
- Jeśli podpis ma zawierać znacznik czasu i/lub odpowiedź OCSP, w czasie składania podpisu niezbędne jest połączenie z Internetem. Potrzebne może być także wykupienie usługi znakowania czasem.

4.2 SKŁADANIE PODPISÓW – PODPIS RSIGN (PODPIS W CHMURZE)

W celu złożenia podpisu kliknij prawym przyciskiem myszy (PPM) na pliku do podpisu by rozwinąć menu kontekstowe - należy wybrać z niego kolejno opcje *PEM-HEART Signature -> Podpisz* (w przypadku wielu aplikacji, opcja może znajdować się pod *Pokaż więcej opcji*). Operację dokonuje się również z poziomu uruchomionej aplikacji PEM-HEART Signature (opis czynności przedstawiono w **5.2.2 Składanie podpisów – podpis rSign (podpis w chmurze), str.40**)

Program automatycznie wybierze zalecany format podpisu. Następnie należy kliknąć przycisk *Dalej* i wprowadzić PIN do podpisu (użytkownik zostanie poproszony o jego wpisanie). W kolejnym kroku wymagane jest uruchomienie aplikacji *rSign by Cencert* na swoim urządzeniu mobilnym, z której trzeba odczytać z ekranu kod „AKTYWNY PIN PODPISU” – należy wpisać go do aplikacji na komputerze i kliknąć OK. W dalszej kolejności należy zatwierdzić zamiar złożenia podpisu w aplikacji rSign, po którym program wykona podpis.

Uwaga! Zalecamy ustawienie w aplikacji opcji *Ustawienia -> PIN -> Zapamiętaj PIN na określony czas*, z czasem ustawionym na 3 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. W przypadku ustawienia podpisu na „Każdorazowo pytaj o PIN” wykonanie podpisu ze znacznikiem czasu będzie wymagać podwójnego zatwierdzenia podpisu na telefonie (podpis pod dokumentem, podpis pod żądaniem znakowania czasem).

Uwagi:

- Zaawansowane opcje, takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia, są dostępne pod przyciskiem *Opcje...* . Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział **8.1 Zmiana parametrów podpisywania, str. 60**.
- W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.
- W przypadku wybrania "podpisu w osobnym pliku", podpis zostanie zapisany w osobnym pliku. Wybranie tej opcji wymaga późniejszego przekazania odbiorcy dwóch plików: plik oryginalny i podpisu.
- W czasie składania podpisu niezbędne jest połączenie z Internetem.

4.3 WERYFIKACJA PODPISU

W celu weryfikacji podpisu należy kliknąć prawym przyciskiem myszy (PPM) na pliku do podpisu, a następnie wybrać polecenie *PEM-HEART Signature -> Weryfikuj* (w przypadku wielu aplikacji, opcja może znajdować się pod *Pokaż więcej opcji*). Zostanie wtedy wyświetlone okno weryfikacji podpisu. Następnie należy kliknąć przycisk *Weryfikuj*. Program zweryfikuje podpisy zapisane w dokumencie i wyświetli rezultat weryfikacji. Operację dokonuje się również z poziomu uruchomionej aplikacji PEM-HEART Signature (opis czynności przedstawiono w **5.3 Weryfikacja podpisu w programie, str. 44**)

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

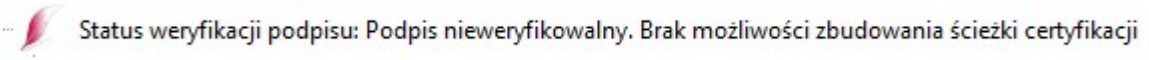
Jeśli podpis nie posiada znacznika czasu - podpis jest weryfikowany na moment bieżący lub na inny moment wpisany ręcznie do programu ("weryfikuj na podany czas: ..."). W przypadku ręcznego wpisywania momentu, na który weryfikowany jest podpis, odpowiedzialność za prawidłowość czasu (i ewentualnie możliwy 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).



4.3.1 PANEL WERYFIKACJI

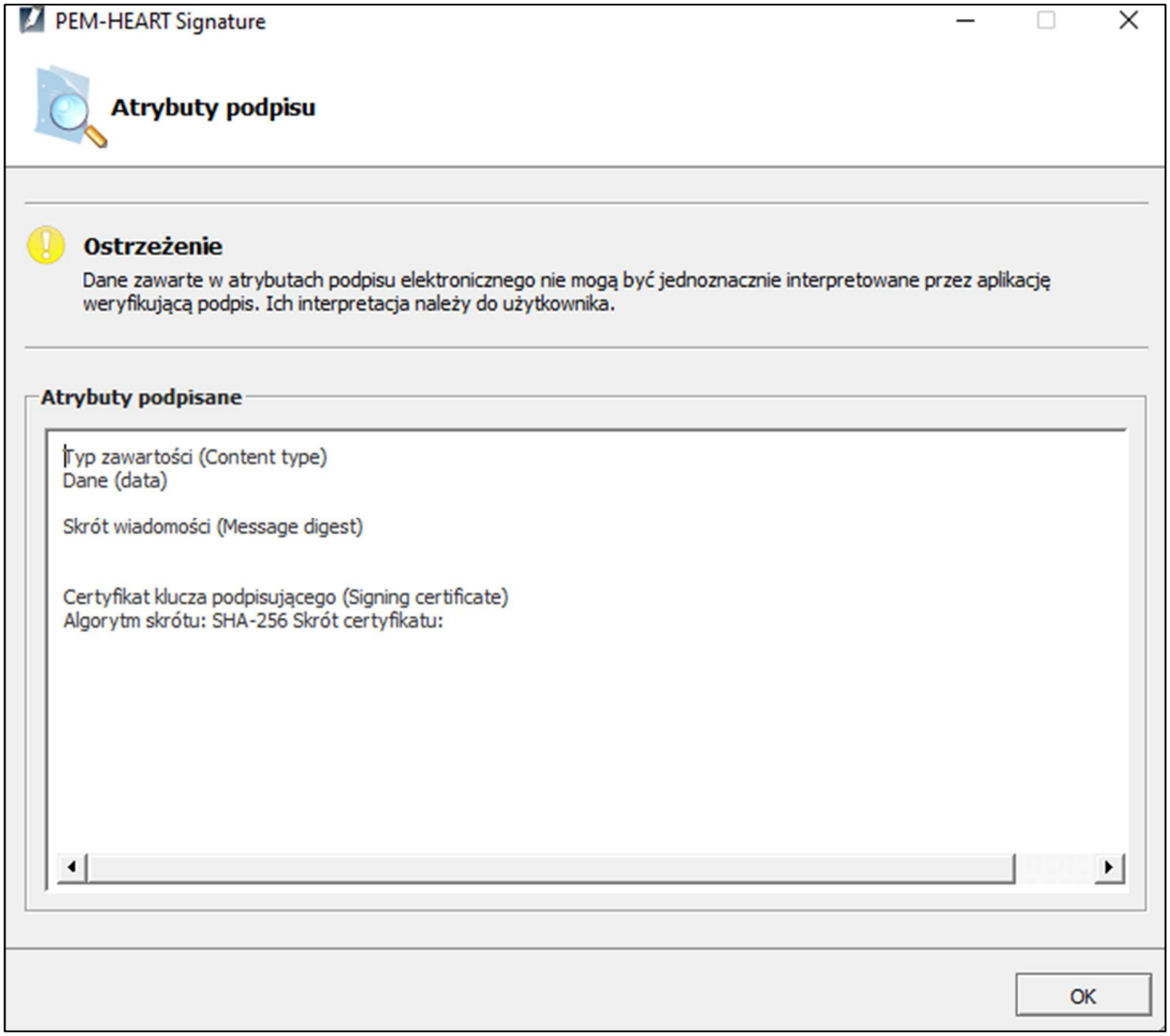
Po weryfikacji podpisu, w górnym menu są dostępne różne czynności dodatkowe, w tym:

- *Prezentuj dokument* - wyświetlenie oryginalnego (podpisanego) dokumentu, jeśli w systemie jest zainstalowany program służący do wyświetlania danego typu dokumentów.
- *Otwórz katalog* – otwarcie widoku katalogu na dysku, w którym zapisany jest dokument.
- *Atrybuty podpisu* - pokazanie dodatkowych danych dołączonych do podpisu.
- *Pokaż certyfikat* - wyświetlenie certyfikatu z danymi osoby, która podpisała dokument. Występuje tutaj możliwość wyeksportowania certyfikatu w formacie *.crt* poprzez przycisk *Eksportuj*.
- *Pokaż raport xml* – pokazanie raportu xml w oknie programu.
- *Utwórz raport PDF* - zapisanie na dysku czytelnego raportu (w formacie PDF) potwierdzającego weryfikację podpisu.
- *Pokaż pomoc* – zostanie ukazana instrukcja użytkownika pdf.

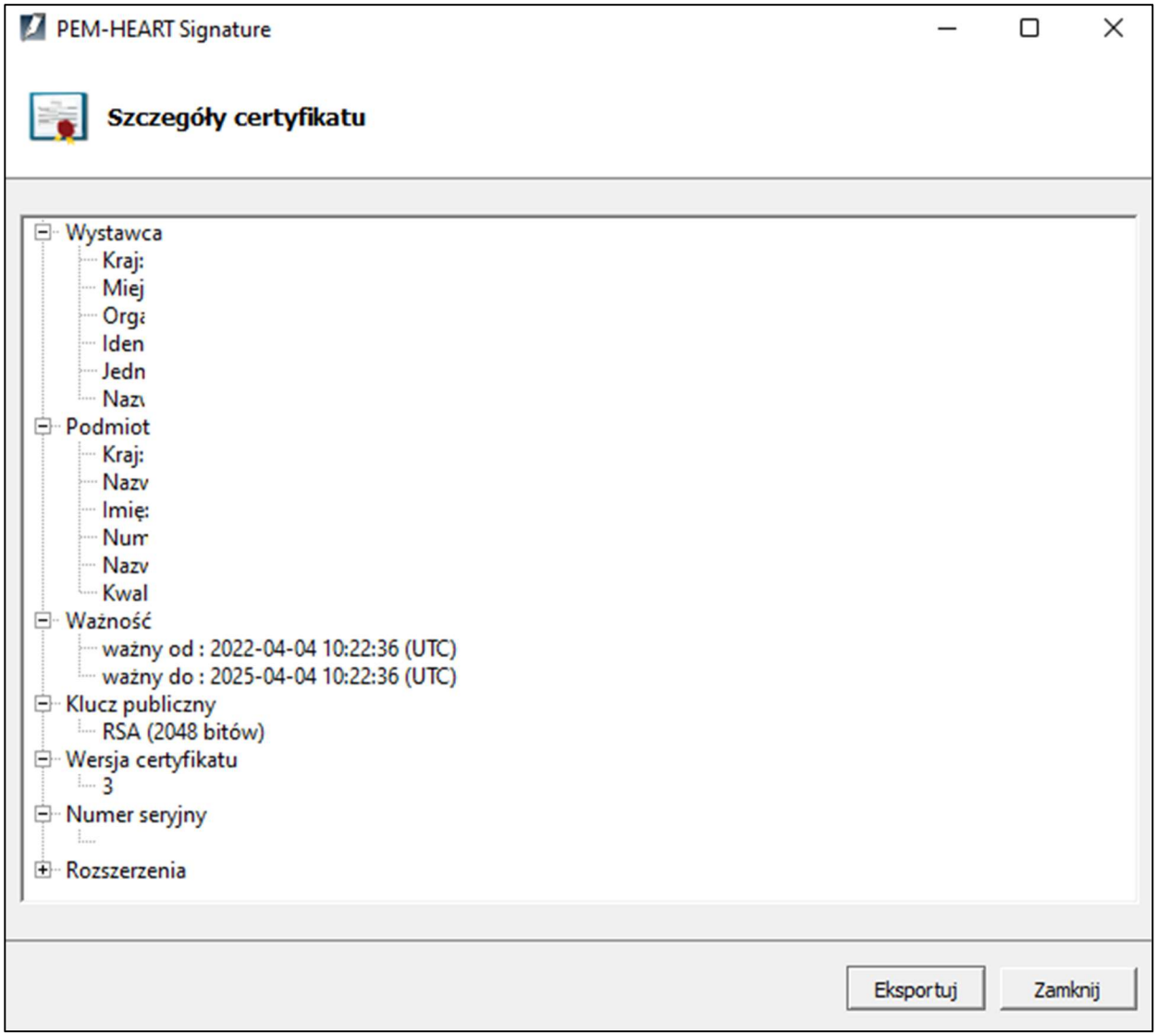
- Po poprawnej weryfikacji podpisu, można utworzyć zaawansowane formy podpisu:
  - *Utwórz postać archiwalną* - zabezpieczającą możliwość poprawnej weryfikacji podpisu na okres ważności znacznika czasu (praktycznie ok. 7-10 lat). Utworzenie formy archiwalnej wymaga dostępu do Internetu i pobrania m.in. 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.

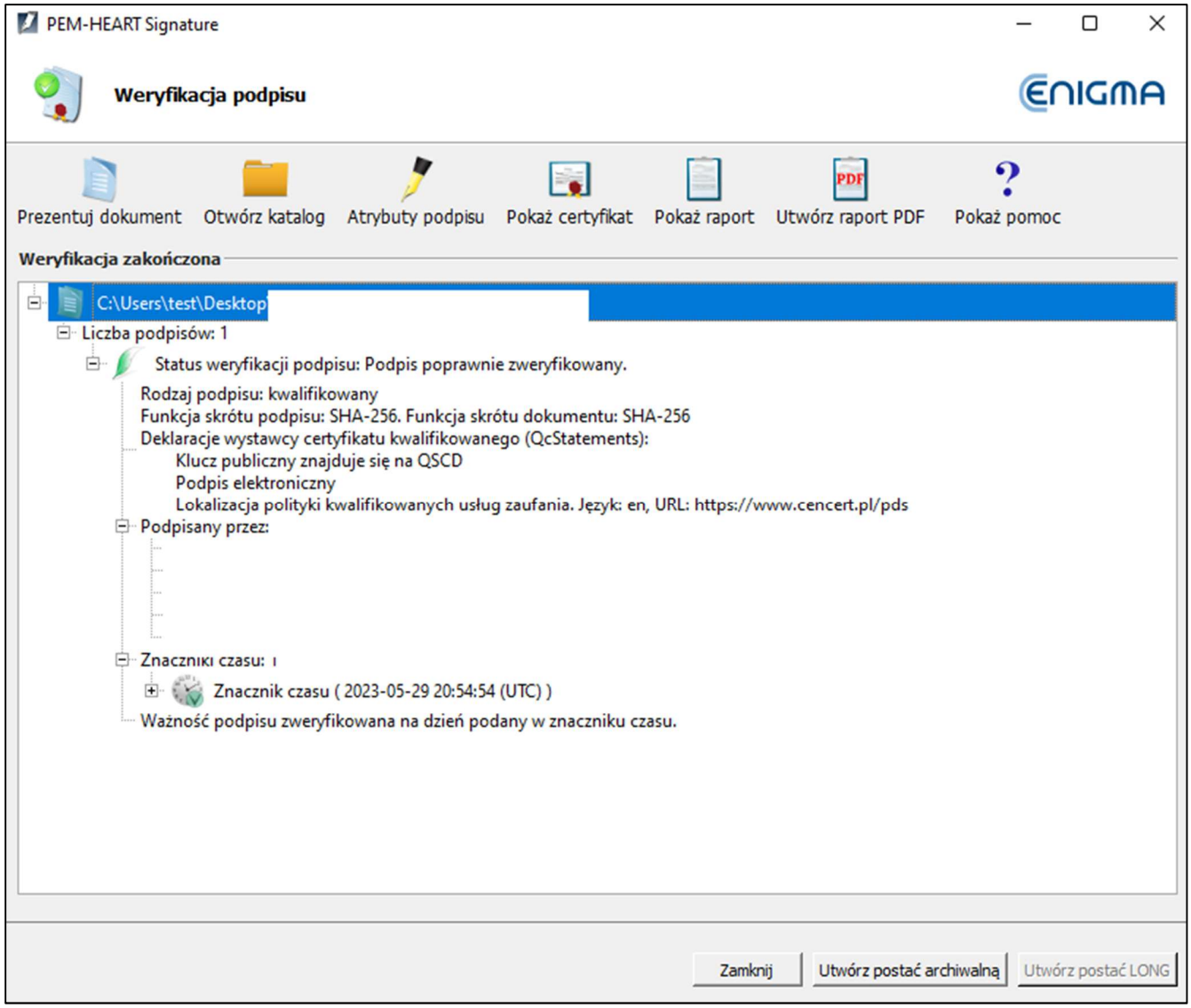
  - *Utwórz postać long* - zabezpieczającą możliwość poprawnej weryfikacji podpisu na okres ważności OCSP i znacznika czasu (praktycznie ok. 5-10 lat). Utworzenie postaci *long* wymaga dostępu do Internetu i pobrania m.in. znacznika czasu. Konieczne może być wykupienie pakietu znaczników czasu.



Rysunek 29 Okno z ukazaniem atrybutów podpisu



Rysunek 30 Okno z ukazaniem szczegółów certyfikatu



Rysunek 31 Status podpisu po weryfikacji

5 FUNKCJE PODSTAWOWE

5.1 URUCHOMIENIE PROGRAMU

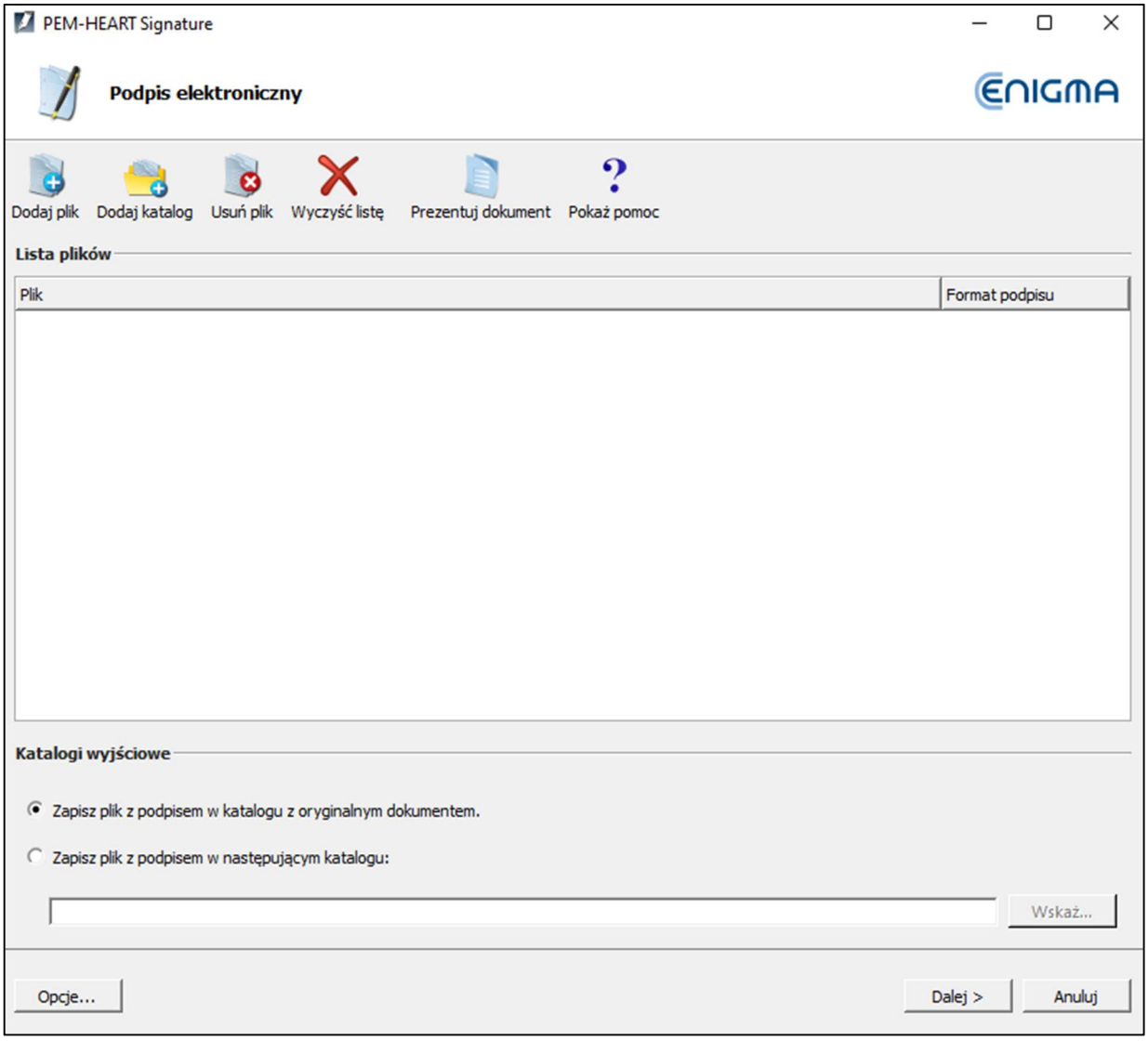
Wszystkie funkcje programu są dostępne po uruchomieniu programu *PEM-HEART Signature* z menu *Start* (Windows) lub z ikony na pulpicie. W innych systemach operacyjnych należy uruchomić program w sposób odpowiedni dla danego systemu. Wygląd programu jest taki sam, jak w systemie Windows.

5.2 PODPISYWANIE W PROGRAMIE

5.2.1 SKŁADANIE PODPISÓW – PODPIS NA KARCIE LUB TOKENIE USB

W celu złożenia podpisu po uruchomieniu programu należy kliknąć ikonę *Podpisz* (po lewej stronie okna, w panelu *Funkcje podstawowe*). Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do podpisu. Występuje tutaj możliwość dodania pliku lub plików które mają zostać podpisane (przycisk *Dodaj plik*) lub przeciąganie pliku do okna z listą plików. Jeśli zostanie wskazany cały katalog (przycisk *Dodaj katalog)*, na listę plików do podpisu wstawione zostaną wszystkie pliki z tego katalogu i jego podkatalogów. Po dodaniu wszystkich plików do podpisu, należy kliknąć przycisk *Dalej*. Jeśli do systemu operacyjnego jest podłączony jeden czytnik z certyfikatem program poprosi o PIN do karty. Jeśli jest więcej czytników z certyfikatami – program ukaże okno z wyborem tokenu. Po poprawnej operacji podpis zostanie wykonany.

Rysunek 32 Menu główne aplikacji PEM-HEART Signature - wybór opcji „Podpisz"



Rysunek 33 Okno składania podpisu elektronicznego

Uwagi:

1) Zaawansowane opcje, takie jak zmiana formatu podpisu, podpis w osobnym pliku, znakowanie czasem i inne ustawienia, są dostępne pod przyciskiem *Opcje...* . Ustawienia zmienione w ten sposób odnoszą się do konkretnego podpisu i nie są zapamiętywane do późniejszego użycia. Patrz też rozdział **8.1 Zmiana parametrów podpisywania, str. 60**.

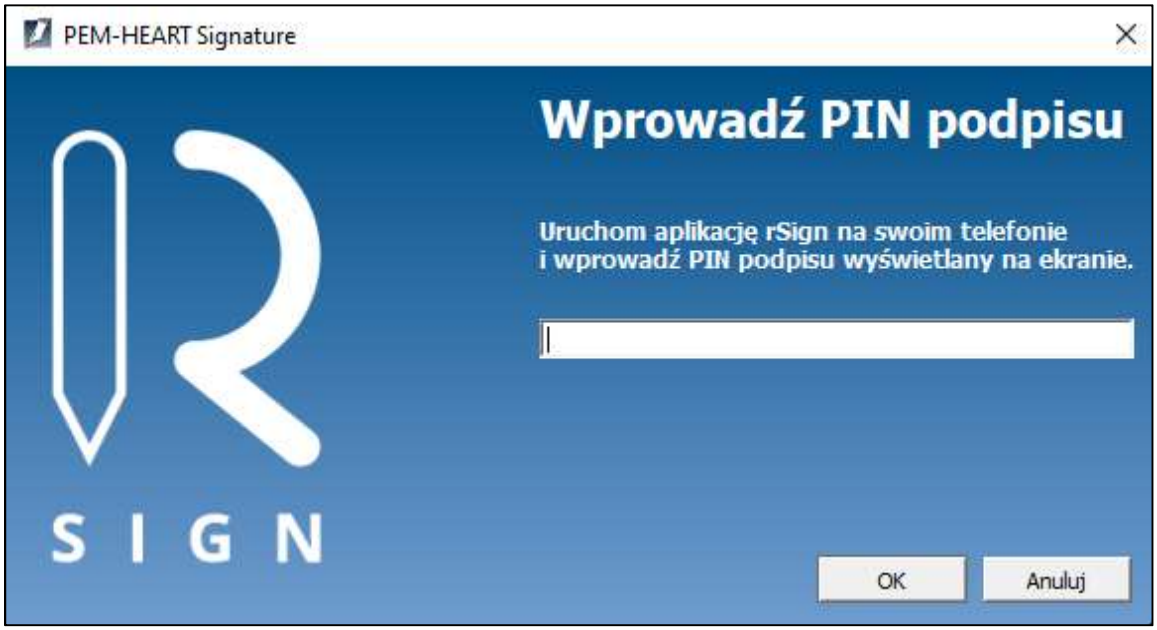
2) W zależności od formatu podpisu, podpis zostanie zapisany w tym samym pliku bez zmiany nazwy lub w nowym pliku ze zmienionym rozszerzeniem.

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 odpowiedź OCSP, w czasie składania podpisu niezbędne jest połączenie z Internetem. Potrzebne może być także wykupienie usługi znakowania czasem.

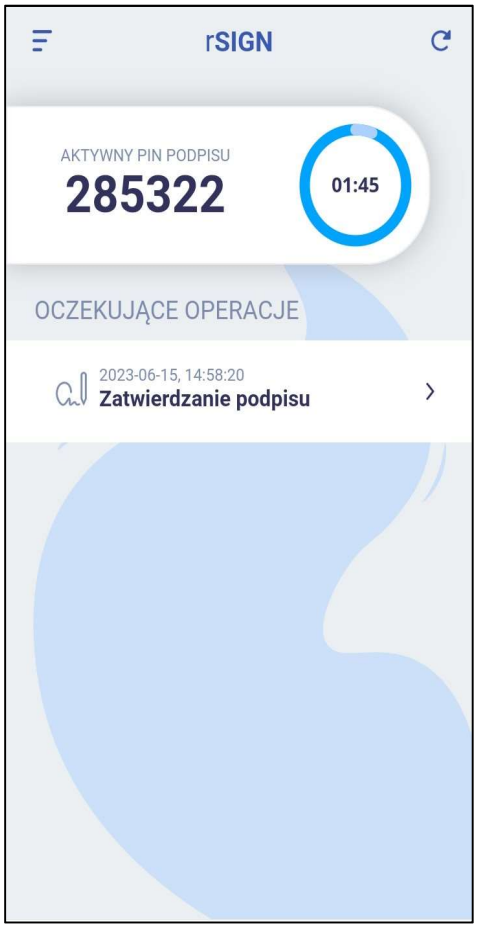
5.2.2 SKŁADANIE PODPISÓW – PODPIS RSIGN (PODPIS W CHMURZE)

W celu złożenia podpisu rSign po uruchomieniu programu należy kliknąć ikonę *Podpisz* (po lewej stronie okna, w panelu *Funkcje podstawowe*). Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do podpisu. Występuje tutaj możliwość dodania pliku lub plików które mają zostać podpisane (przycisk *Dodaj plik*) lub przeciąganie pliku do okna z listą plików. Jeśli zostanie wskazany cały katalog (przycisk *Dodaj katalog)*, na listę plików do podpisu wstawione zostaną wszystkie pliki z tego katalogu i jego podkatalogów. Po dodaniu wszystkich plików do podpisu, należy kliknąć przycisk *Dalej*. Po dodaniu wszystkich plików do podpisu, wciśnij przycisk *Dalej*. Jeśli do systemu operacyjnego jest podłączony jeden czytnik z certyfikatem program poprosi o PIN podpisu. Jeśli jest więcej czytników z certyfikatami – program ukaże okno z wyborem tokenu. Po poprawnej operacji podpis zostanie wykonany.



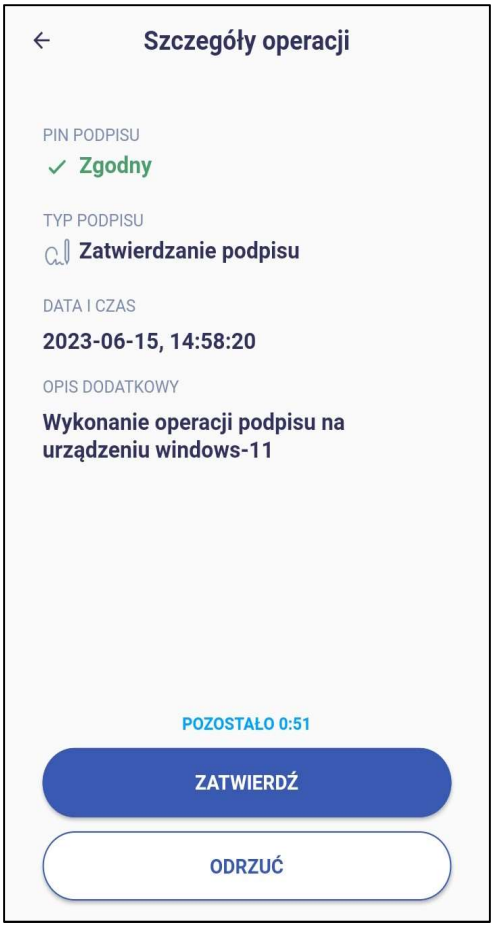
Rysunek 34 Komunikat dotyczący użycia aplikacji rSign na telefonie

Teraz należy uruchomić aplikację mobilną *rSign by Cencert*, a następnie odczytać *Aktywny PIN Podpisu* i przepisać go do programu na komputerze i zatwierdzić *OK*. Zamiar złożenia podpisu należy potwierdzić w aplikacji rSign.

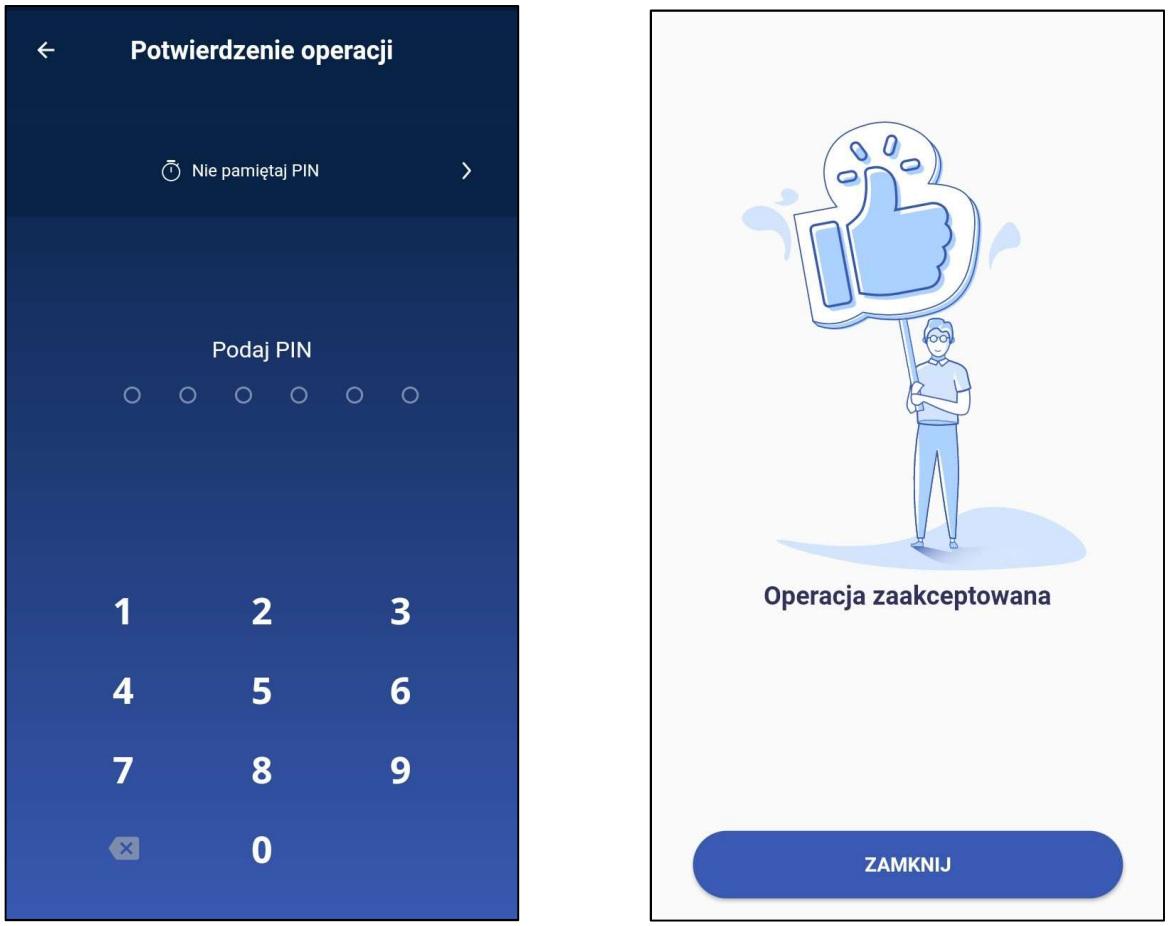


Rysunek 35 Ekran aplikacji rSign z Aktywnym Pinem Podpisu

W aplikacji należy zatwierdzić chęć złożenia podpisu klikając w przycisk *Zatwierdzanie podpisu* w sekcji *OCZEKUJĄCE OPERACJE* tuż pod wyświetlanym Aktywnym Pinie Podpisu (**Rysunek 35 Ekran aplikacji rSign z Aktywnym Pinem Podpisu**). Jeśli dane są poprawne, w kolejnym kroku należy potwierdzić operację poprzez kliknięcie *ZATWIERDŹ* (**Rysunek 36 Zatwierdzenie wykonania operacji podpisu elektronicznego**)

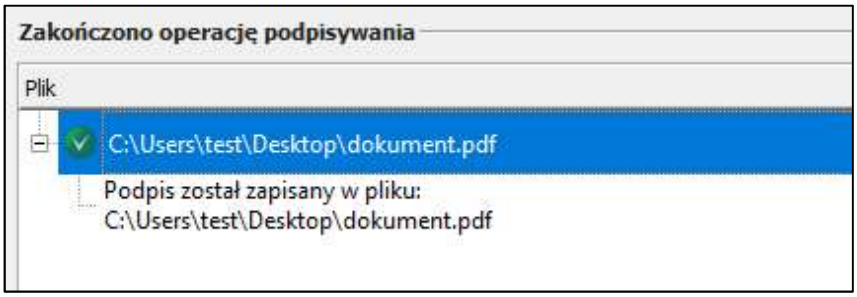


Rysunek 36 Zatwierdzenie wykonania operacji podpisu elektronicznego



Rysunek 37 Okno wpisania kodu PIN oraz potwierdzenie operacji złożenia podpisu (telefon)

Wyświetlony będzie ekran do wpisania kodu PIN, po którego wprowadzeniu należy oczekiwać na zatwierdzenie operacji – jeśli kod został poprawnie wpisany, procedura zostanie zaakceptowana i ukaże się okno jak na **Rysunek 37 Okno wpisania kodu PIN oraz potwierdzenie operacji złożenia podpisu**.

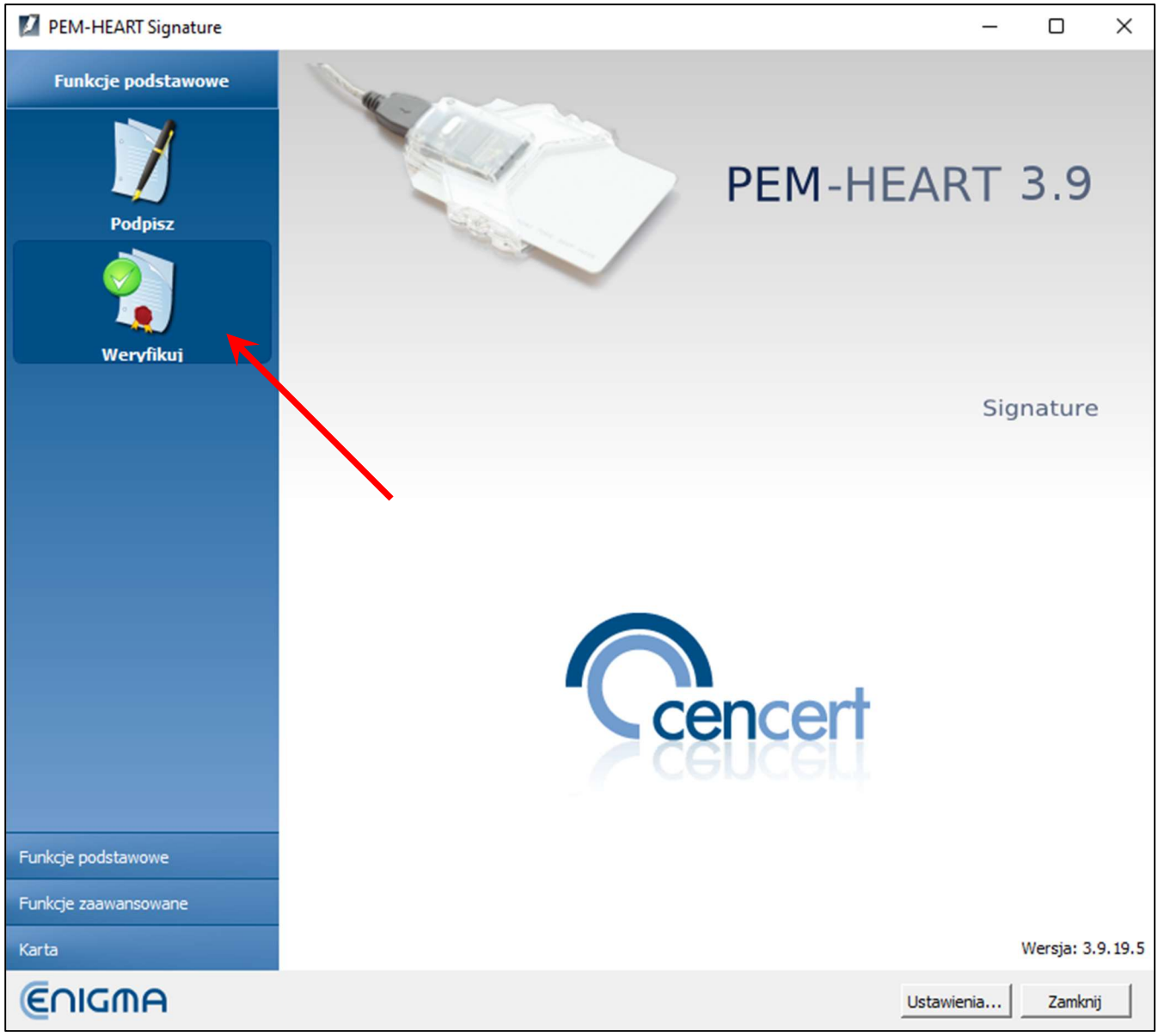


Rysunek 38 Potwierdzenie operacji złożenia podpisu (komputer)

W programie na komputerze ukaże się informacja o poprawnym podpisaniu dokumentu (**Rysunek 38 Potwierdzenie operacji złożenia podpisu (komputer)**).

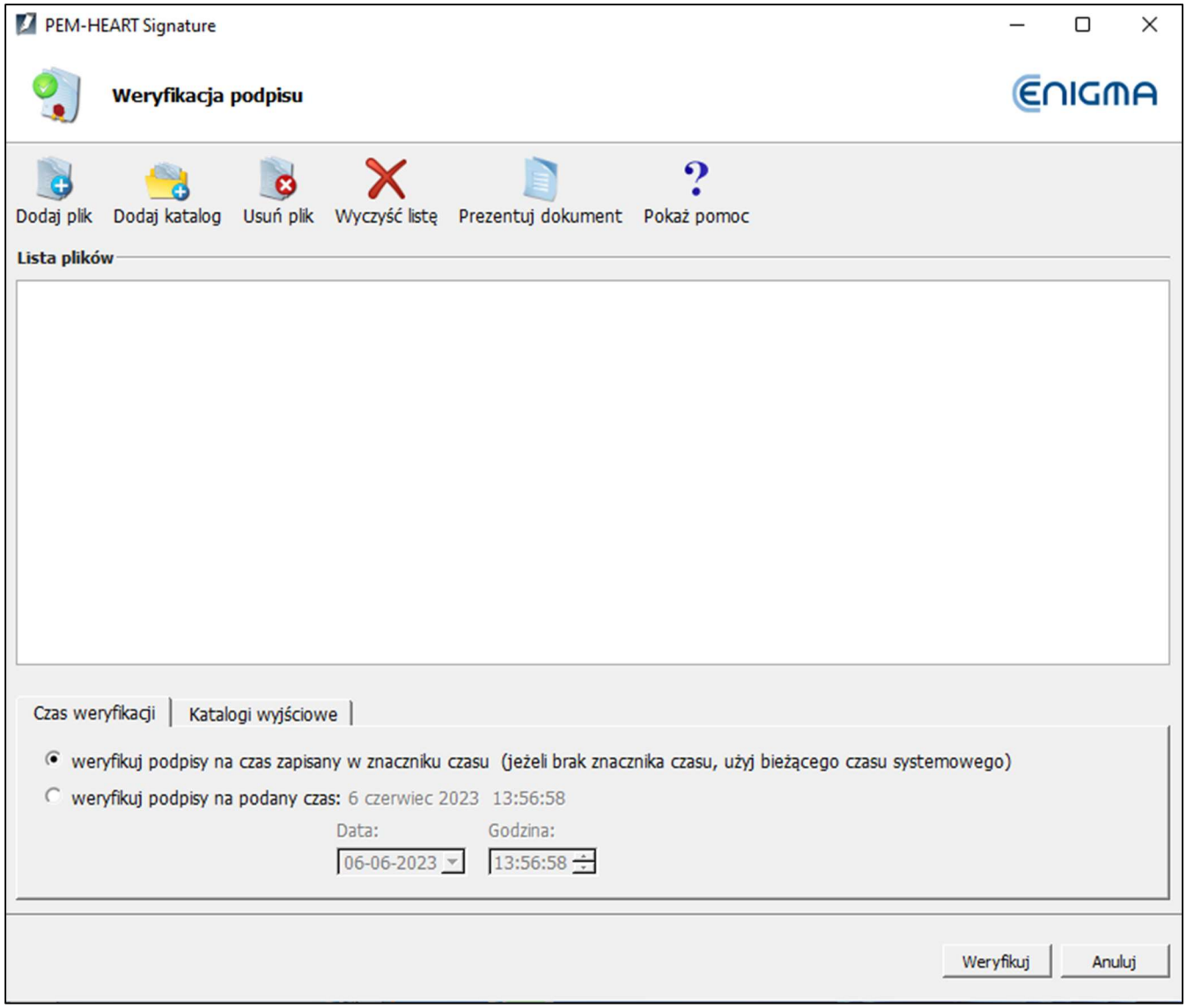
5.3 WERYFIKACJA PODPISU W PROGRAMIE

W celu weryfikacji podpisu, po uruchomieniu programu kliknij ikonę Weryfikuj (po lewej stronie okna, w panelu *Funkcje podstawowe*).



Rysunek 39 Menu główne aplikacji PEM-HEART Signature - wybór opcji „Weryfikuj"

Spowoduje to wyświetlenie okna pozwalającego na wskazanie plików do weryfikacji. Istnieje możliwość dodania jednego pliku lub wielu plików, które mają zostać sprawdzone (przycisk *Dodaj plik*) lub przeciągnąć plik do okna z listą plików. Jeśli zostanie wskazany cały katalog (przycisk *Dodaj katalog)* program na listę plików do sprawdzenia wstawi wszystkie pliki z tego katalogu i jego podkatalogów. Po dodaniu wszystkich plików należy kliknąć przycisk *Weryfikuj*.

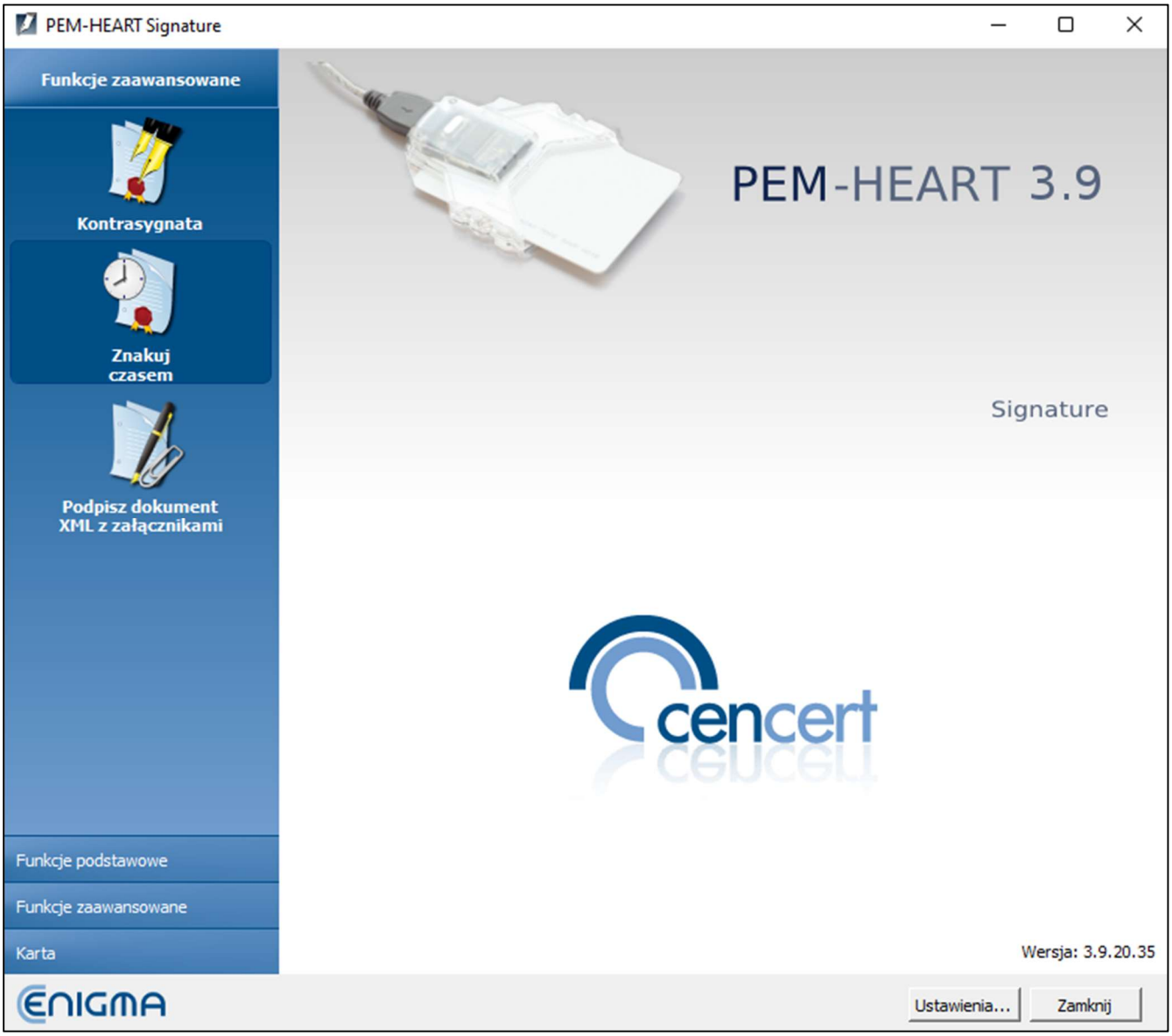


Rysunek 40 Okno weryfikacji podpisu elektronicznego

Program zweryfikuje podpisy zapisane w dokumencie i wyświetli rezultat weryfikacji.

Więcej informacji o weryfikacji zamieszczono w **4.3 Weryfikacja podpisu, str. 31**.

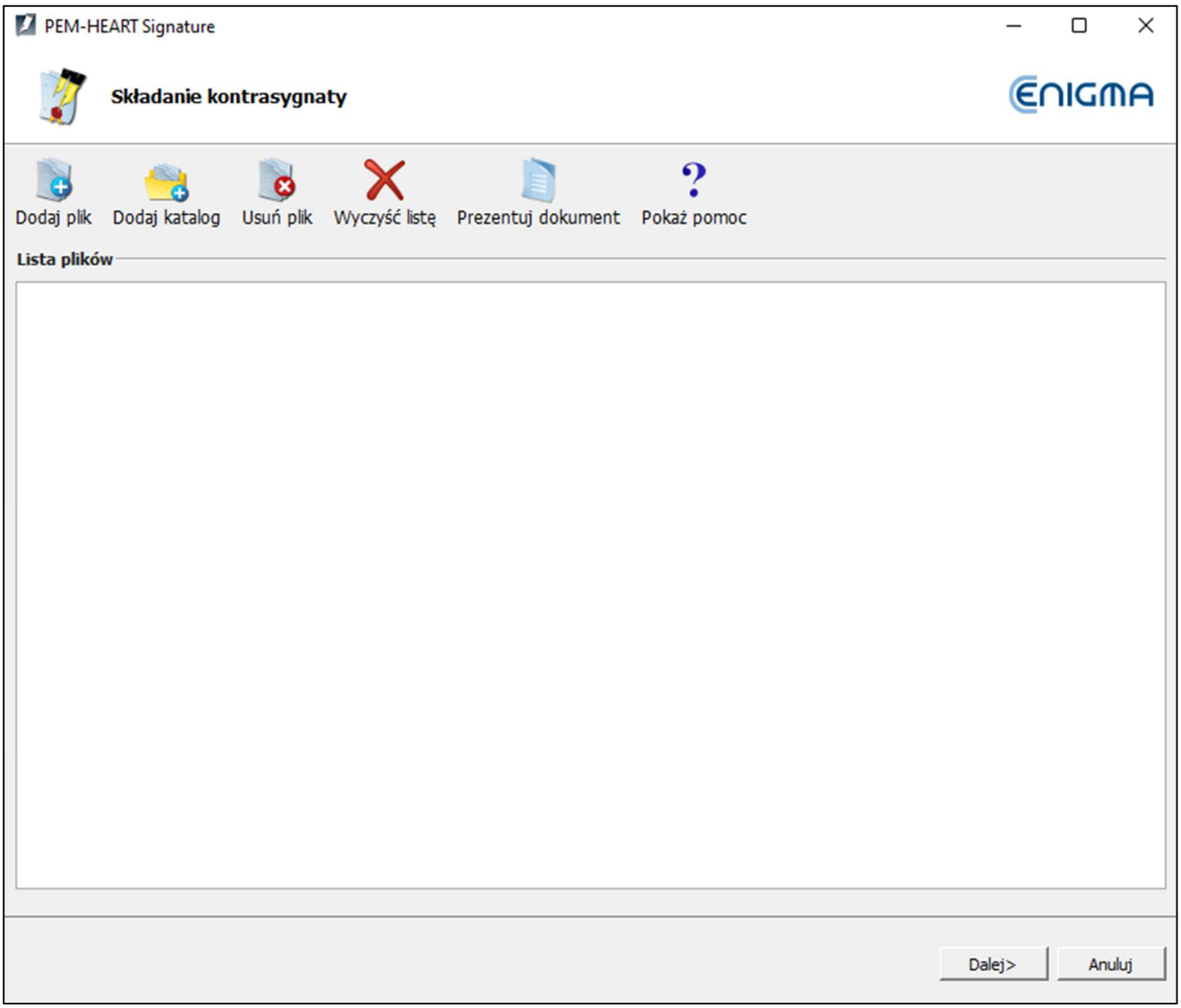
6 FUNKCJE ZAAWANSOWANE



Rysunek 41 Menu główne aplikacji PEM-HEART Signature - funkcje zaawansowane

6.1 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).

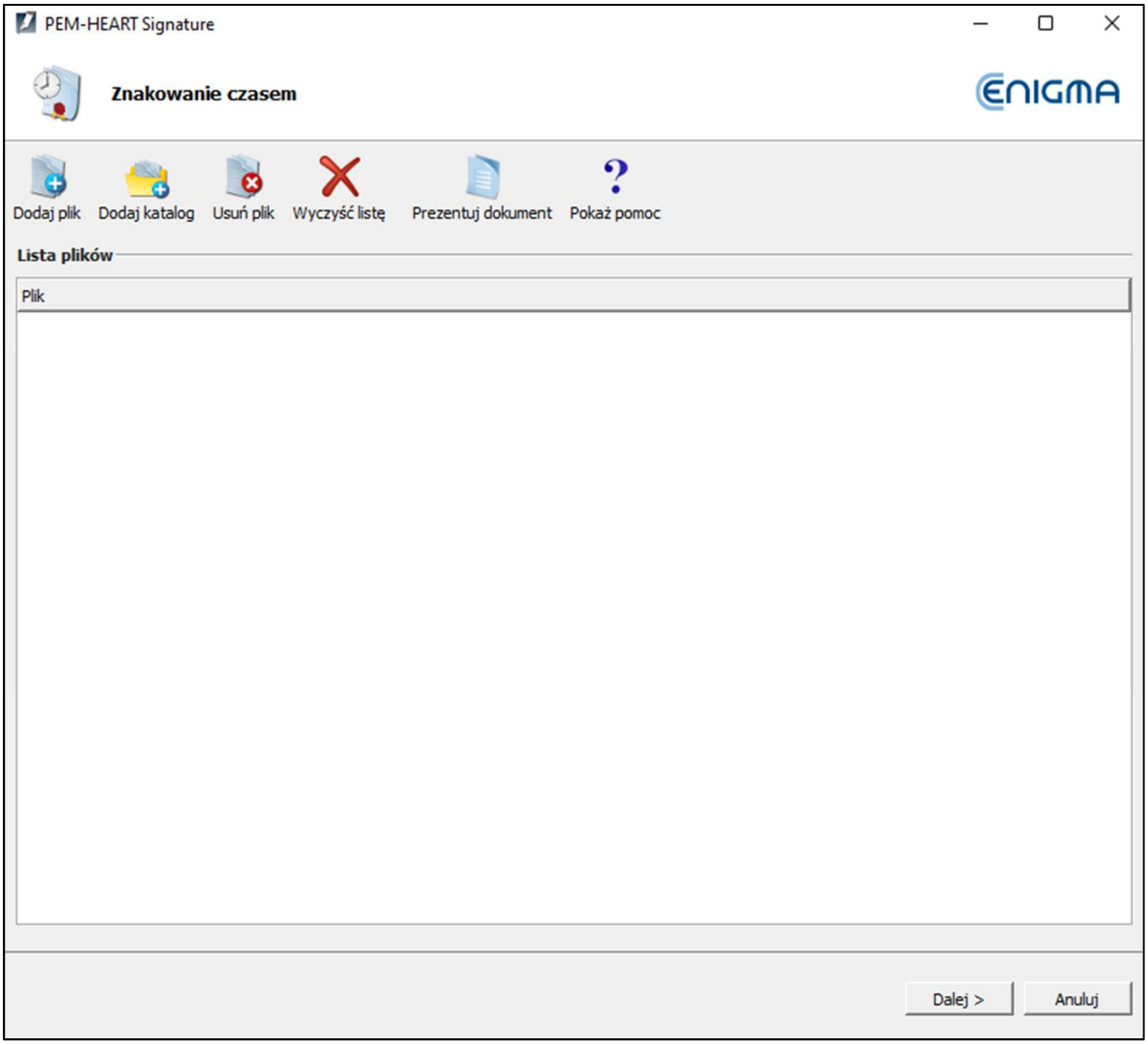


Rysunek 42 Okno składania kontrasygnaty

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 „kontrasygnata" opisana w niniejszym dokumencie funkcjonuje na takich samych zasadach, jak każdy inny podpis elektroniczny.

6.2 ZNAKOWANIE CZASEM

Kwalifikowany znacznik czasu stanowi dowód istnienia dokumentu w danym momencie. W polskim prawie czynność prawna opatrzona kwalifikowanym



Rysunek 43 Okno zastosowania znacznika czasu do podpisu elektronicznego

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 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 **4.3.1 Panel Weryfikacji, str. 33**). Formy te również mogą korzystać ze znaczników czasu, ale uzupełniają go o inne dane potrzebne przy weryfikacji.

Należy wybrać w menu *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wcisnąć 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) lub PIN rSign, następnie dodaje znacznik czasu do każdego podpisu znajdującego się w tym pliku.

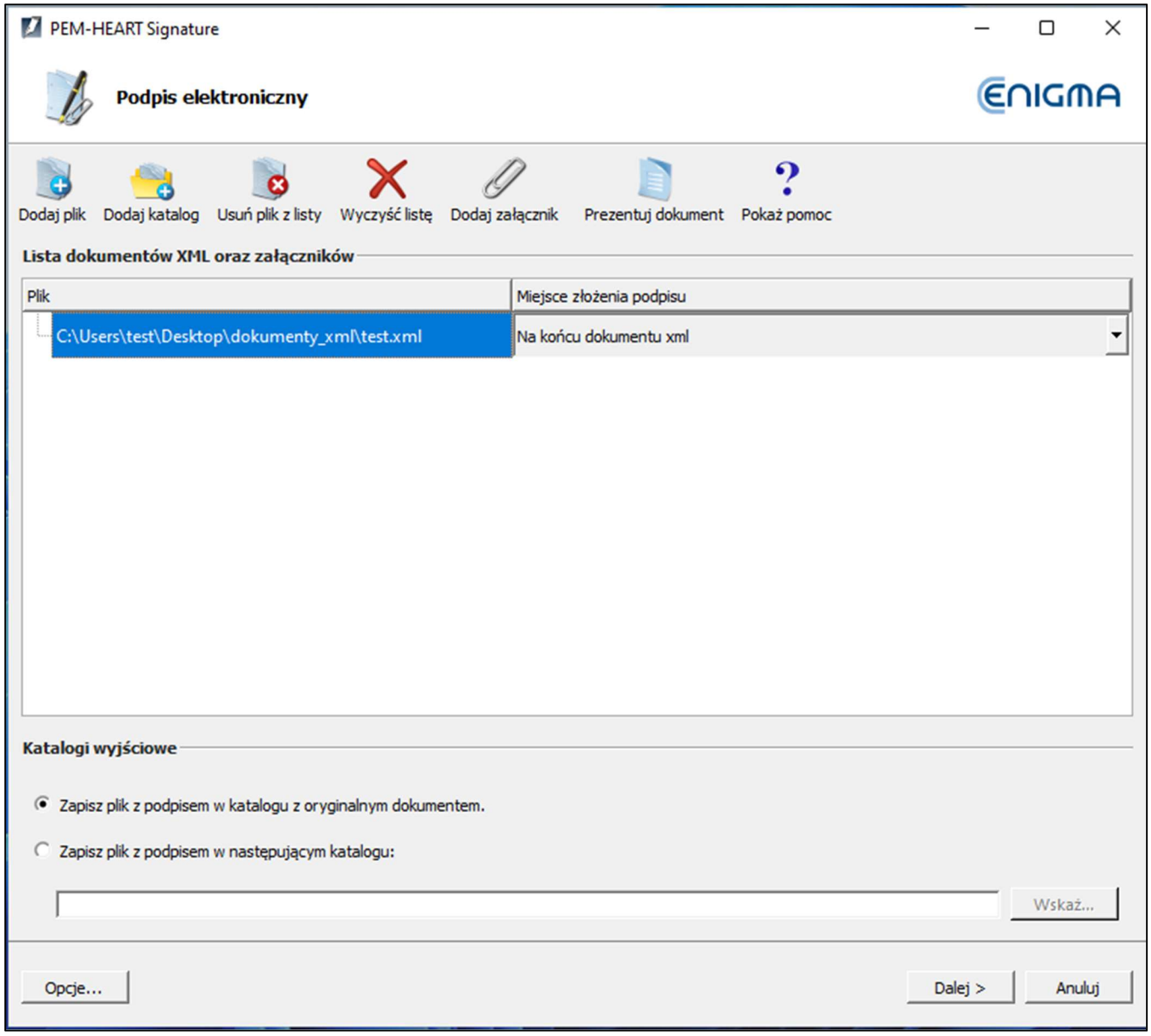
Uwaga: Pobieranie znaczników czasu może wymagać wykupienia pakietu znakowania czasem.

6.3 PODPISYWANIE DOKUMENTU XML Z ZAŁĄCZNIKAMI

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*).

Należy wybrać w menu zakładkę *Funkcje zaawansowane* (pasek po lewej stronie okna głównego) i wcisnąć ikonę *Podpisz dokument XML z załącznikami*. Gdy program

wyświetli okno dodawania plików do podpisu, należy wskazać plik XML (plik może ewentualnie wskazywać na załączniki). Jeśli podpis ma być złożony w innym miejscu niż koniec pliku, wymagane jest wskazanie miejsca odpowiedniego w strukturze dokumentu XML. Użytkownik w takim przypadku musi wybrać z sekcji *Miejsce złożenia podpisu* opcję *Dodaj nowy...*, co spowoduje wyświetlenie okna konfiguracji miejsca składania podpisu.



Rysunek 44 Podpisywanie dokumentu XML z załącznikami - przejście do konfiguracji umiejscowienia podpisu

Następnie w kolejnym oknie kliknąć przycisk  , wpisać swoją nazwę konfiguracji, podać 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.

Po zakończeniu podpisywania zostanie wyświetlone okno podsumowania. Składanie podpisu w formacie XAdES otoczony (*XAdES enveloped*) nie zmienia rozszerzenia pliku XML ani jego struktury.

7 OBSŁUGA KART KRYPTOGRAFICZNYCH W PROGRAMIE

7.1 ZMIANA PIN

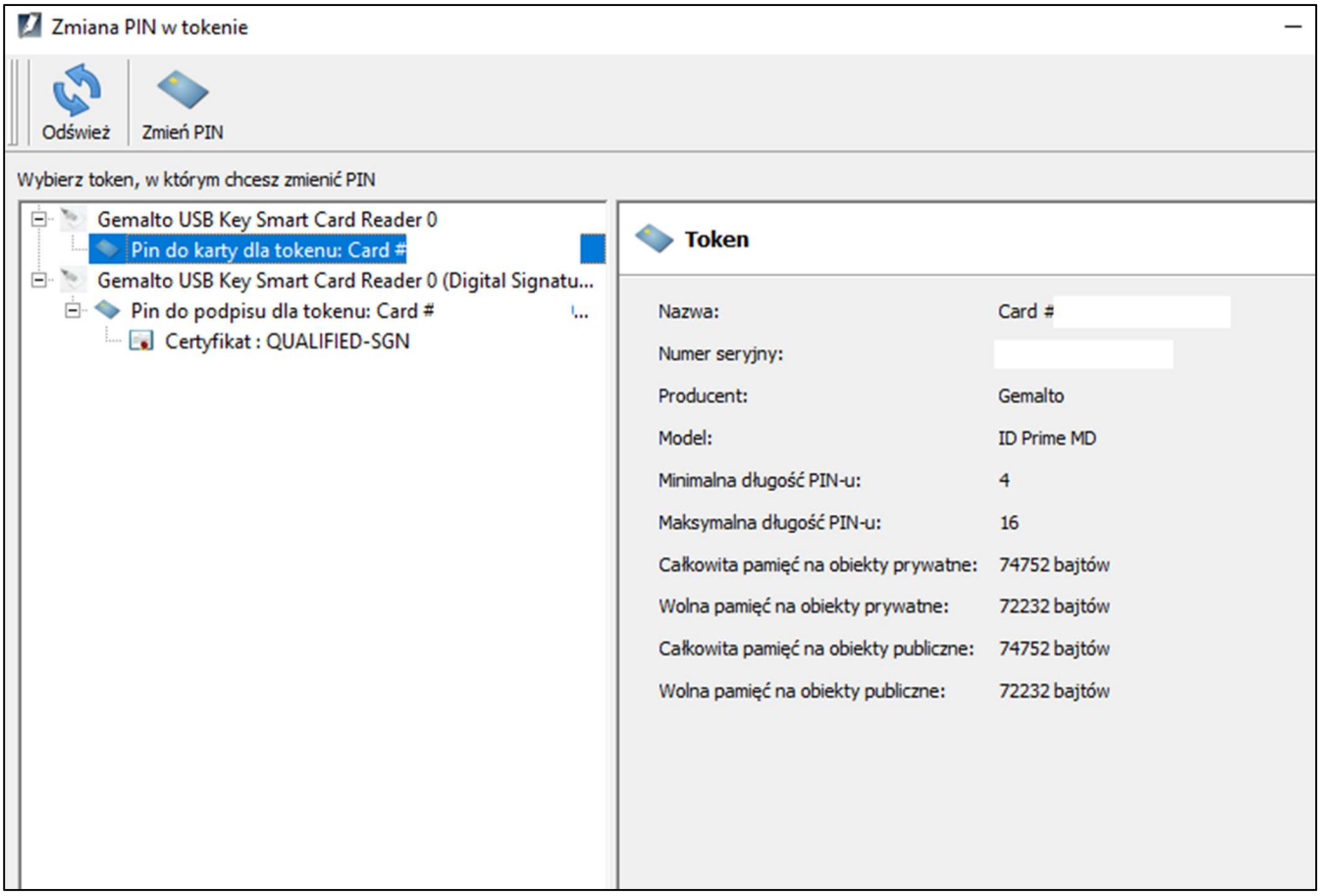
(Funkcja niedostępna dla podpisu rSign) W celu zmiany PIN-u do karty należy wybrać z menu głównego zakładkę *Karta* (pasek po lewej stronie okna głównego) i kliknąć ikonę *Zmień PIN*.

Rysunek 45 Menu główne aplikacji PEM-HEART Signature - wybór zakładki "Karta"

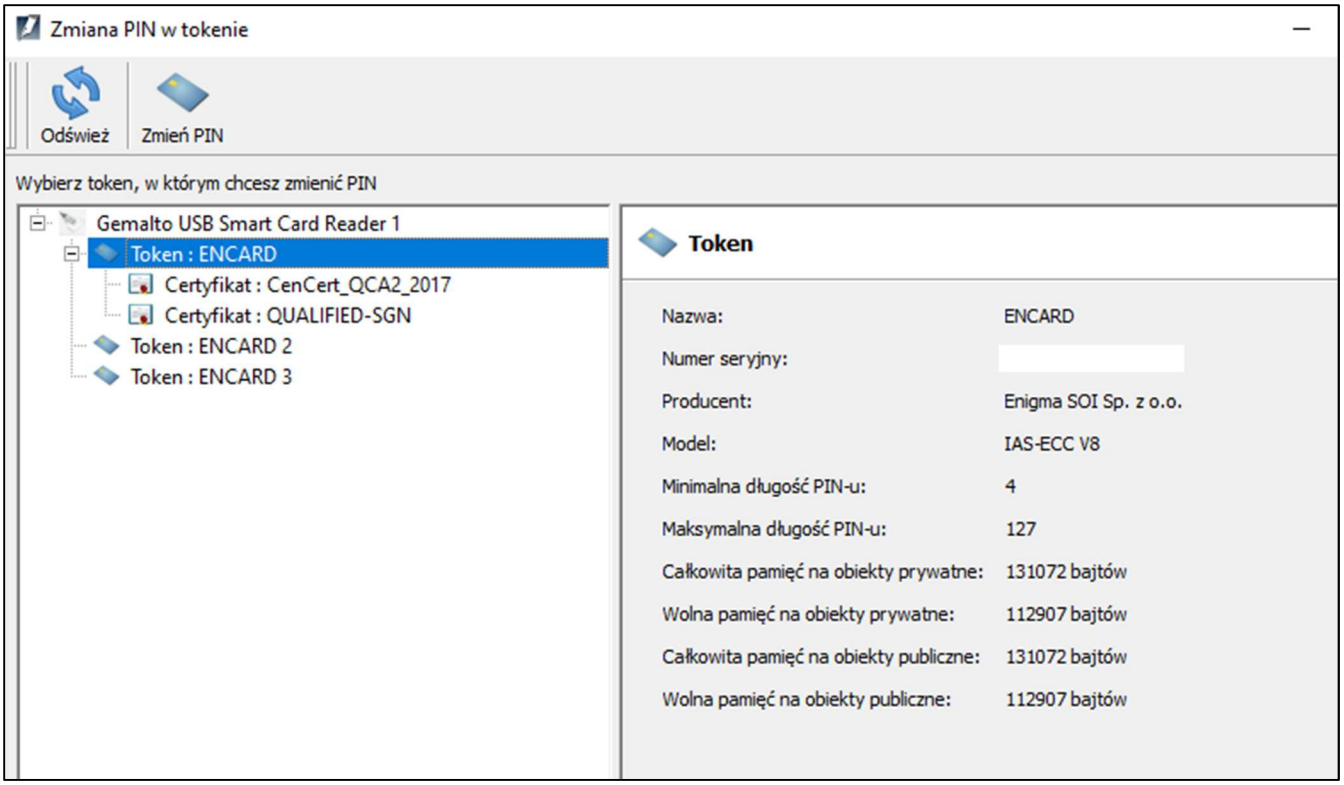
Następnie wymagane jest wskazanie tokenu do którego należy zmienić PIN.

Uwaga:

- Dla kart IDEMIA: obiekty związane z podpisem kwalifikowanym umieszczane są zawsze w pierwszym tokenie od góry; pozostałe tokeny mogą być używane do innych celów, np. do pieczęci elektronicznej.
- Dla kart IDPrime: obiekty związane z podpisem kwalifikowanym umieszczane są zawsze na drugim tokenie od góry – ma on nazwę „Digital Signature PIN”.

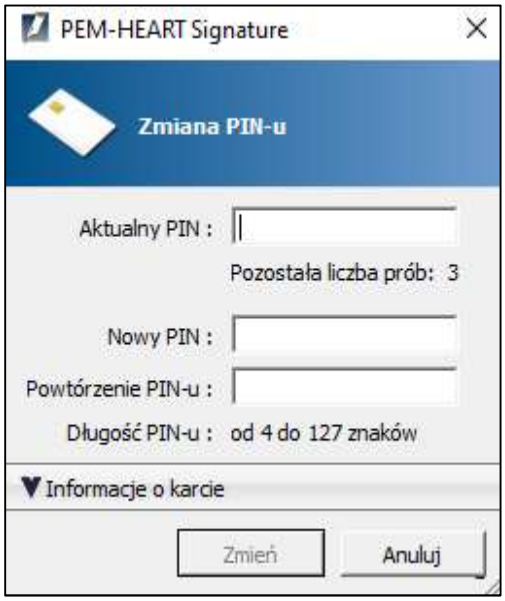


Rysunek 46 Przykładowy ekran programu dla karty Thales typ A



Rysunek 47 Przykładowy ekran programu dla karty IDEMIA Encard

By dokonać zmiany użytkownik wybiera opcję „Zmień PIN”, znajdującą się nad listą tokenów.



Rysunek 48 Ekran zmiany kodu PIN karta IDEMIA

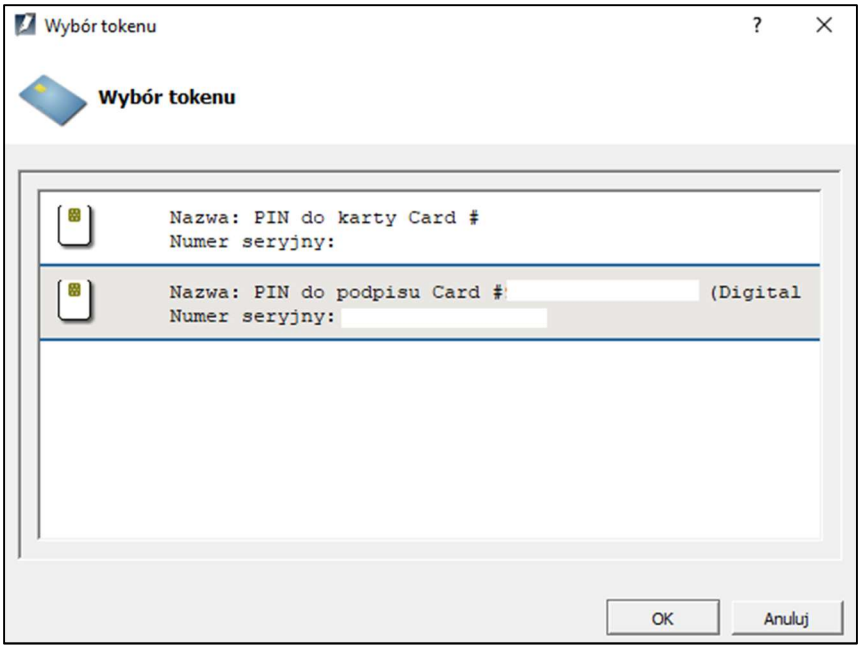
Do zmiany kodu należy podać poprawny aktualny kod PIN oraz dwa razy wpisać nowy kod. Nie zaleca się używania do kodu PIN polskich liter lub innych znaków, które przy różnych ustawieniach językowych klawiatury komputera mogą nie być poprawnie wprowadzane (karta się blokuje po 3 próbach podania nieprawidłowego kodu). Zalecane jest zapisanie kodu PIN w bezpiecznym miejscu (oddzielnie od karty), wyjątkiem jest tutaj PIN do kart thales (pierwszy token), w tym przypadku zablokuje się on po 5 próbach.

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

Kody PIN / PUK są nadawane przez użytkownika podczas aktywacji karty. Cencert nie posiada kodów PIN / PUK i nie ma możliwość odblokowania karty z powodu błędnego kodu PIN / PUK.

7.2 ODBLOKOWANIE KARTY

(Funkcja niedostępna dla podpisu rSign) 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* zostanie otwarte okno z wyborem tokenów.



Rysunek 49 Odblokowanie karty - wybór tokenu – karta IDPrime

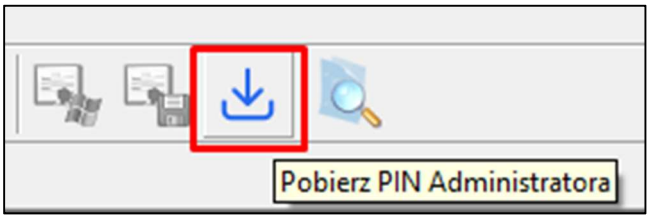
Po poprawnym podaniu kodu PUK, będzie możliwe ustawienie nowego kodu PIN i karta zostanie odblokowana.

Uwaga!! Dostępna jest ograniczona ilość prób odblokowania karty za pomocą kodu PUK. W przypadku błędnie wypełnionych danych przy każdej próbie, karta jest trwale zablokowana i nie ma możliwości jej dalszego użycia.

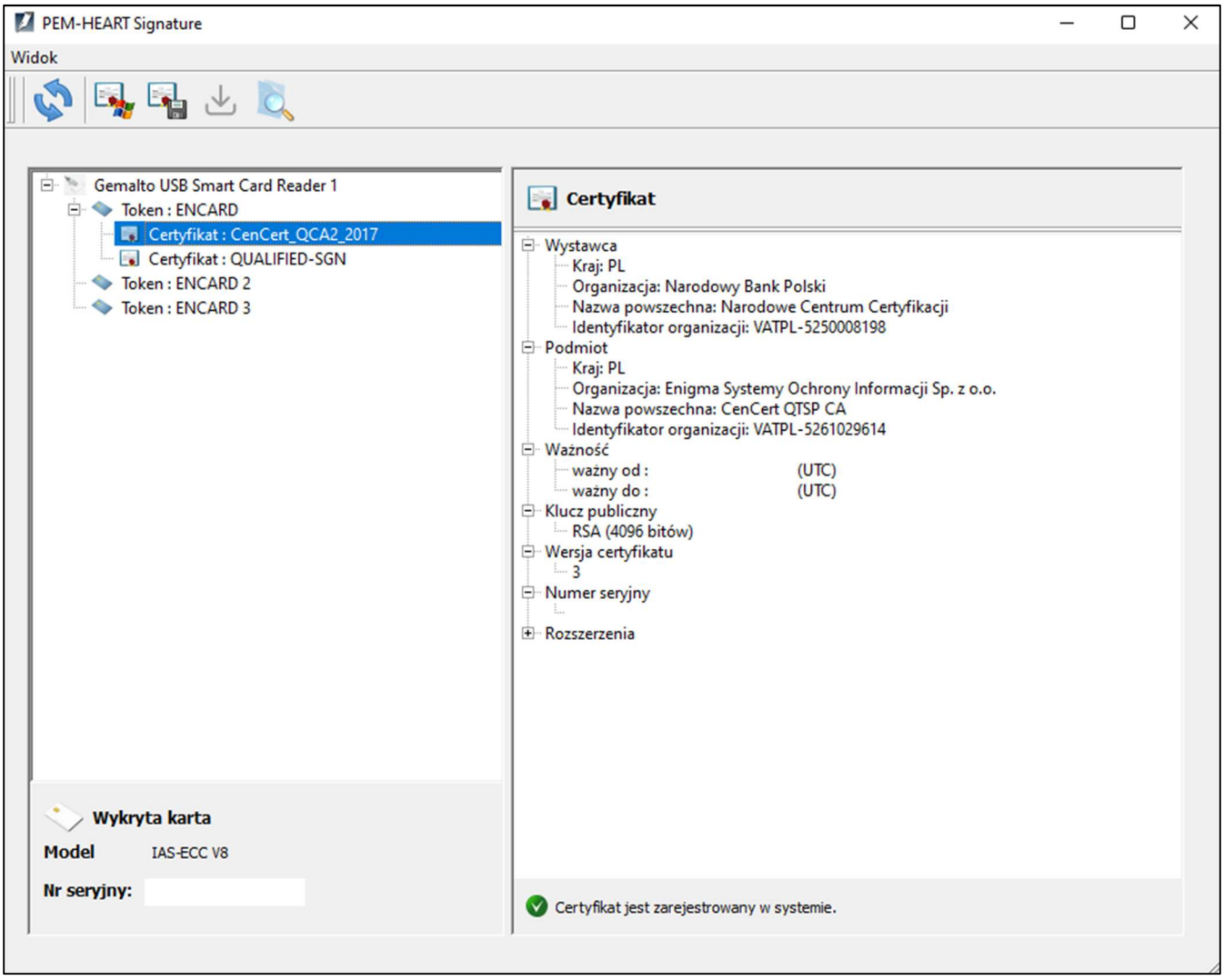
Kody PIN / PUK zostają nadane przez użytkownika podczas aktywacji karty. Cencert nie posiada kodów PIN / PUK i nie może pomóc w przypadku zablokowania karty z powodu błędnego kodu PIN / PUK.

7.3 DIAGNOSTYKA

Panel *Diagnostyka* ukazuje dodatkowe informacje odnośnie danych z certyfikatu, pozwala na zapisanie certyfikatu do pliku, zarejestrowanie go w systemie Windows, pobranie PIN Administratora (tylko dla kart IDPrime) oraz włączyć logowanie (tylko dla kart IDEMIA i rSign – funkcja opisana w **10.1 Logi operacji kart dla systemów Windows, str. 78**).



Rysunek 50 Dodatkowe opcje w ekranie *Diagnotyka*



Rysunek 51 Widok otwartego panelu *Diagnostyka* – wyświetlenie tokenu z karty oraz rSign

7.4 DODATKOWE OPCJE

7.4.1 ODNOWIENIE CERTYFIKATU

Następuje przekierowanie i otworzenie programu PEM-HEART Odnowienie cetyfikatu. Odnośnik do strony z poradnikiem dla użytkownika: https://www.cencert.pl/poradnik-uzytkownika/

7.4.2 KONFIGURACJA RSIGN

Następuje przekierowanie i otworzenie programu PEM-HEART Konfiguracja rSign

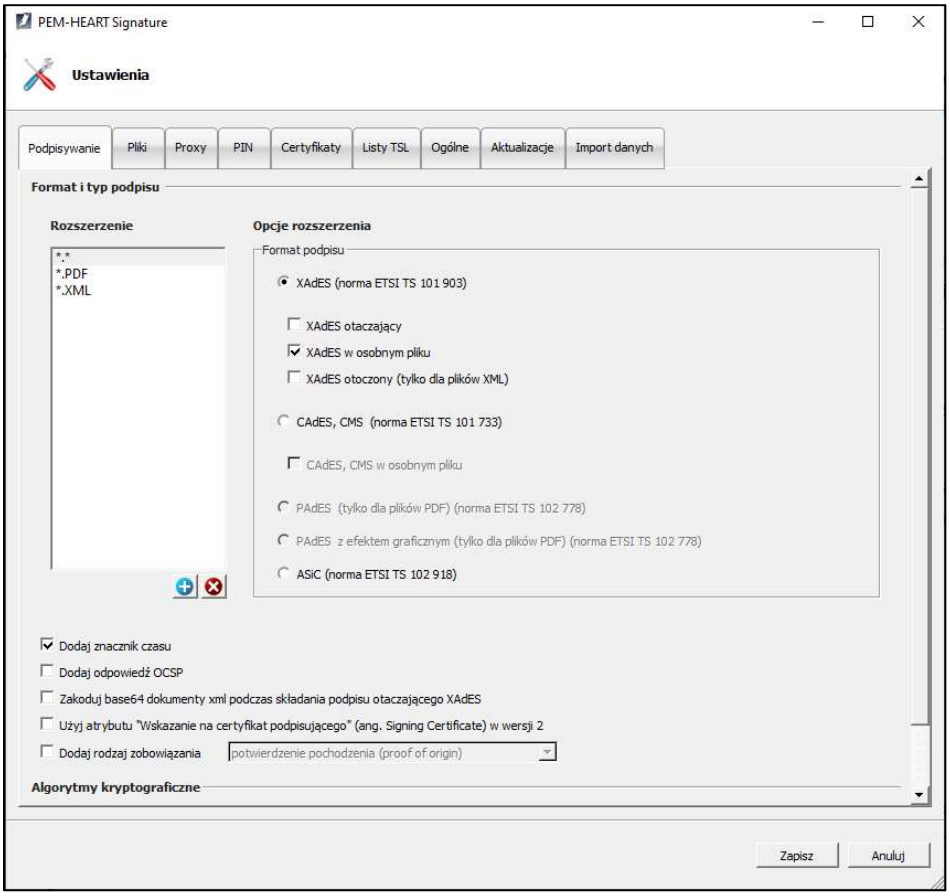
8 USTAWIENIA PROGRAMU

Uwaga!

Wszystkie operacje zmiany parametrów zostaną zapamiętane w pamięci programu po zapisaniu ich poprzez przycisk *Zapisz* w prawym dolnym rogu menu programu.

8.1 ZMIANA PARAMETRÓW PODPISYWANIA

W celu zmiany opcji podpisywania, w oknie głównym programu należy kliknąć przycisk Ustawienia (znajduje się w prawym dolnym rogu ekranu aplikacji, tuż obok przycisku Zamknij). Wyświetlone zostanie nowe okno ustawień, z otwartą kartą Podpisywanie. Wszystkie opcje określające format podpisu (XAdES, CAdES, PAdES, ASiC) będą zastosowane do plików o rozszerzeniu aktualnie zaznaczonym na liście Rozszerzenie. Wszystkie pliki o rozszerzeniach *.* (a więc wszystkie inne pliki niż zdefiniowane na liście pod tym rozszerzeniem) 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.



Rysunek 52 Okno zmiany ustawień podpisywania

W tym miejscu możliwe jest dodanie (lub usunięcie) rozszerzeń plików (za pomocą ikon  i ), dla których ma być stosowany inny domyślny format podpisu. Np. dodając nową pozycję „*.docx" i definiując, że dla tych plików ma być wykonywany podpis np. CAdES oraz CMS w osobnym pliku, to dla wywołania podpisu dla każdego pliku z dokumentem Ms Word (*.docx), program domyślnie zaproponuje podpis w formacie CAdES oraz CMS w osobnym pliku.

W sekcji poniżej wyboru rozszerzenia i ustawienia formatu podpisu dla danego rozszerzenia znajdują się 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 (zaznaczenie *Dodaj znacznik czasu* odblokowuje możliwość zaznaczenia *Dodaj odpowiedź OCSP*), do

podpisu zostanie dodana informacja o statusie certyfikatu użytego do podpisu (powstaje w ten sposób podpis w formie long – patrz też rozdział **4.3.1 Panel Weryfikacji, str. 33**).

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.

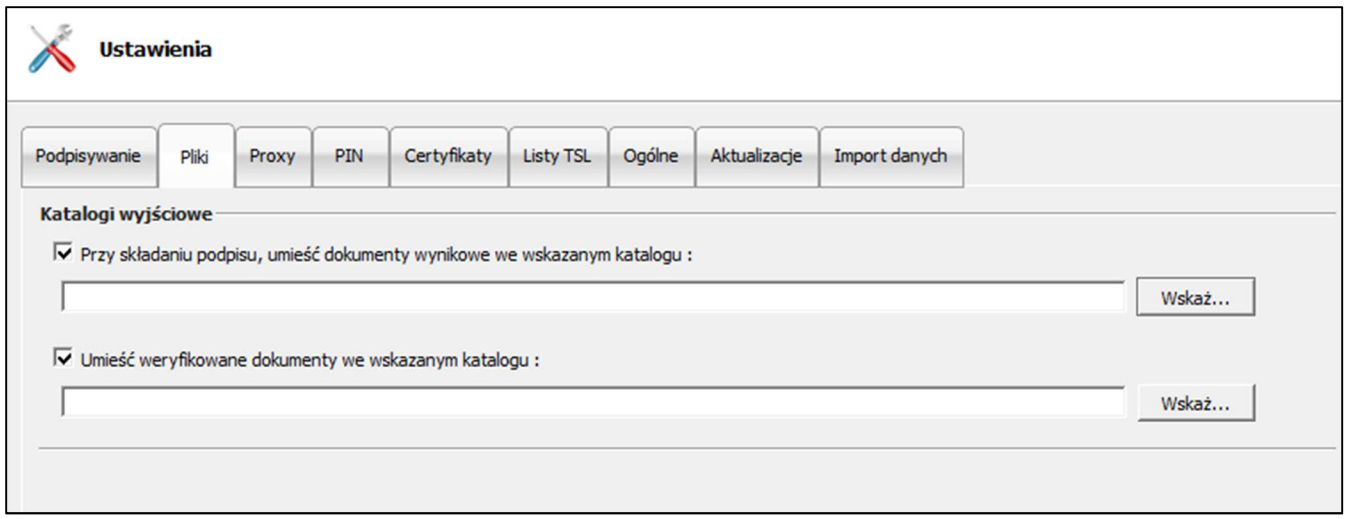
Zaznaczenie opcji *Dodaj rodzaj zobowiązania* powoduje dodanie podpisanego atrybutu, który wskazuje w jakim celu (w jakiej roli) podpisujący złożył podpis (np. jako „formalne zatwierdzenie", albo „potwierdzenie odbioru" itd.).

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

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.

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



Rysunek 53 Definiowanie katalogów wyjściowych dla przetwarzanych dokumentów

8.3 PROXY

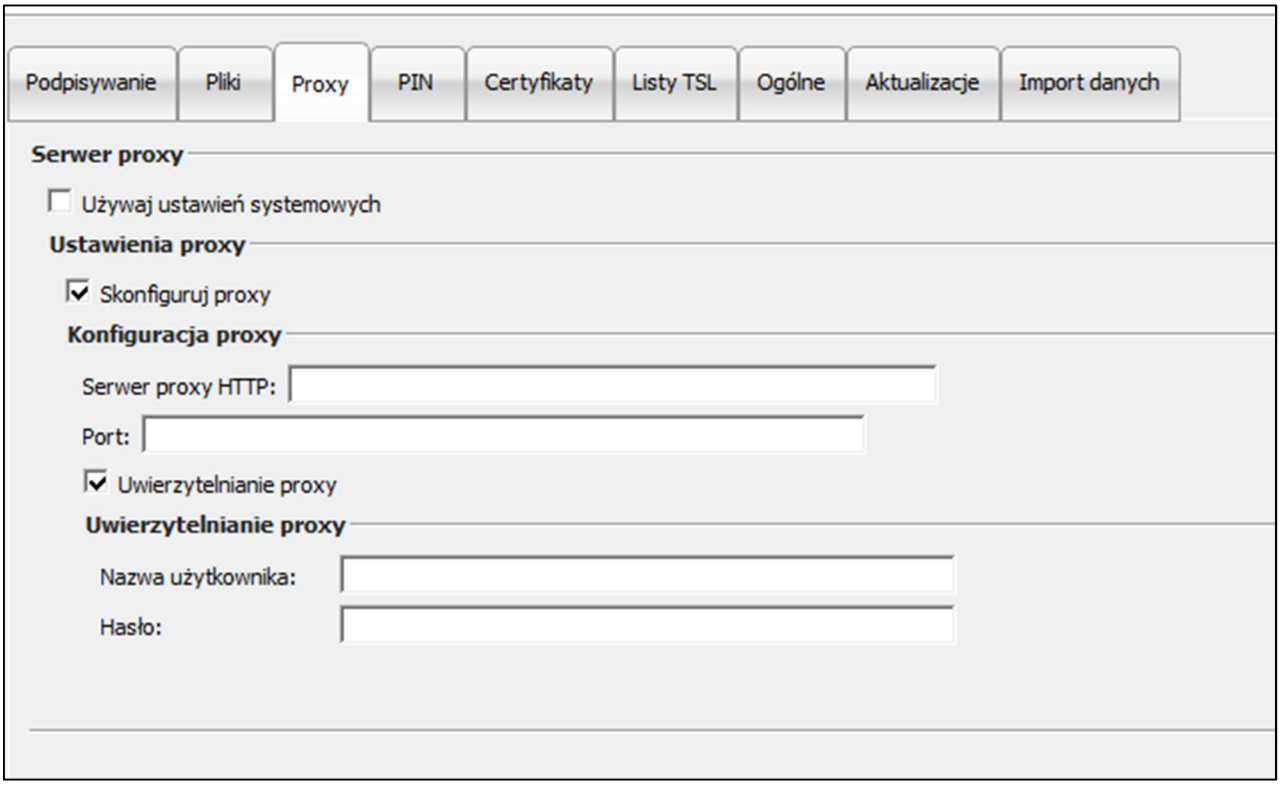
Zakładka służy do określenia połączenia z serwerem proxy. Występują do wyboru dwie możliwe konfiguracje:

- *Użyj ustawień systemowych* (tylko dla systemów Windows) – opcja domyślna, pobierana jest konfiguracja z ustawień systemu (rejestr)

Rysunek 54 Serwer proxy - ustawienia systemowe

- *Skonfiguruj proxy* – ręczne ustawienie konfiguracji, wskazanie adresu portu i/lub danych do uwierzytelnienia. Należy wypełnić wszystkie pola obowiązkowe dla danego serwera *proxy*. Aktywacja ustawień jest zatwierdzana poprzez przycisk *Zapisz* w prawym dolnym rogu programu. *Uwierzytelnianie proxy* jest tutaj wersją opcjonalną i nie jest wymagane

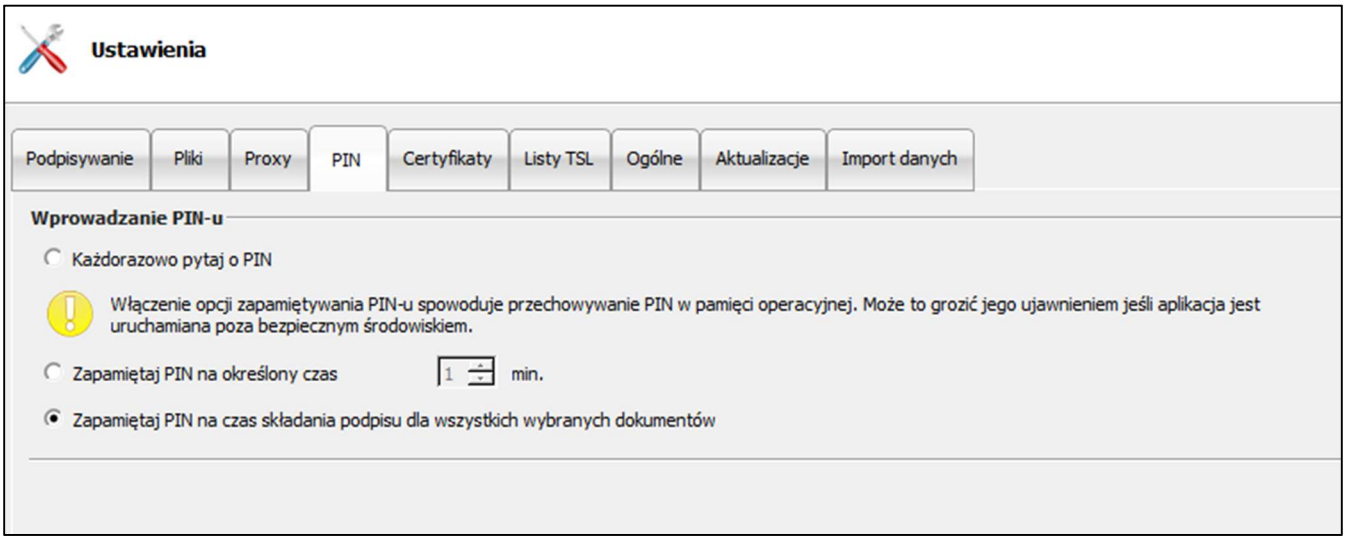
Błędne skonfigurowanie serwera powoduje brak dostępu programu do Internetu (nie da się pobrać znacznika czasu, może nie być możliwe weryfikowanie podpisów).



Rysunek 55 Serwer proxy - ustawienia ręczne

8.4 PIN

Zakładka PIN służy do ustawienia opcji zapamiętywania przez program PIN-u do karty kryptograficznej.



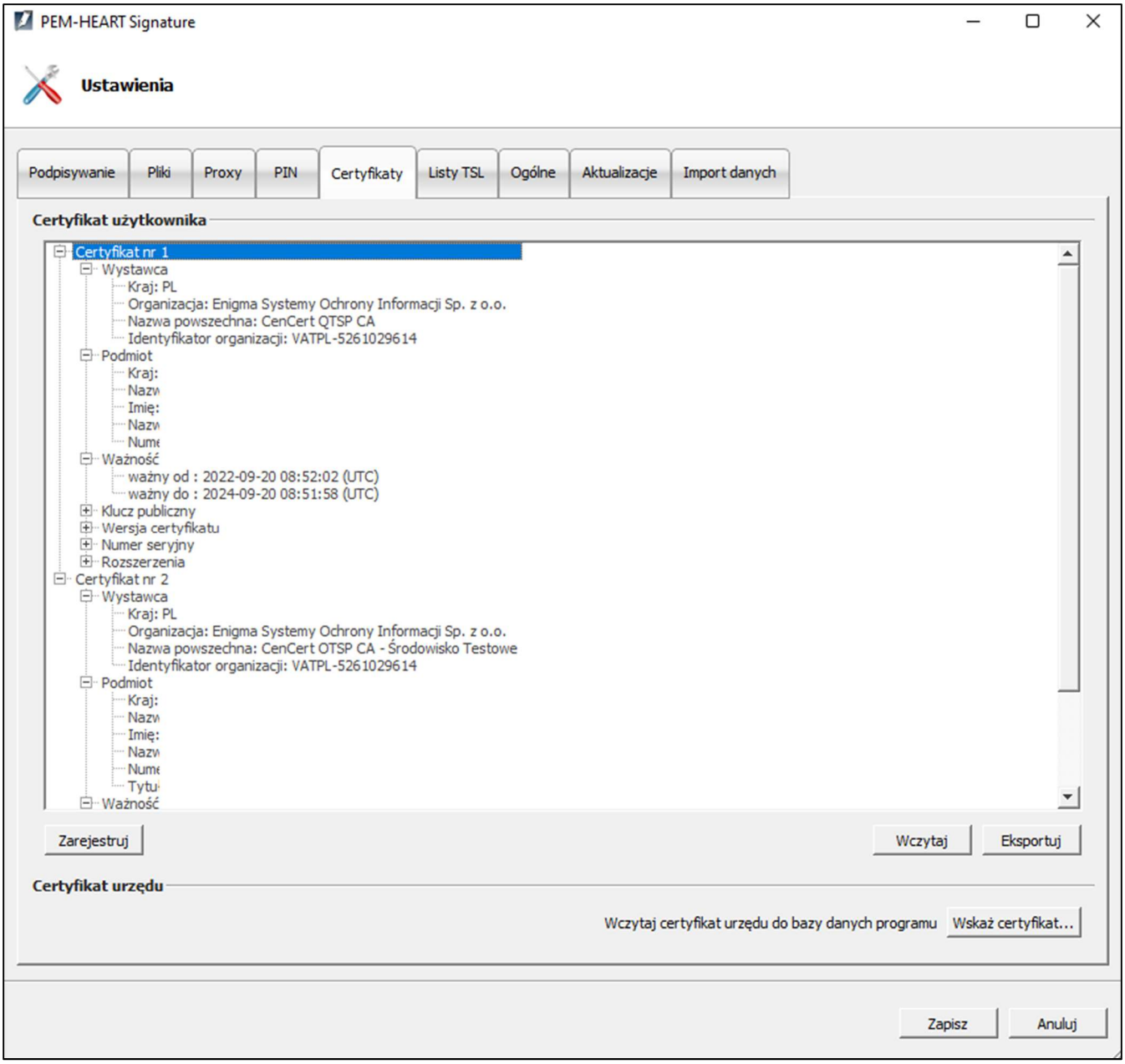
Rysunek 56 Ustawienia PIN-u

Uwaga! Opcja nie dotyczy podpisów rSign (w chmurze). Dla tego rodzaju podpisu ustawienia konfiguruje się w aplikacji mobilnej.

Domyślnie PIN jest zapamiętywany na czas składania podpisów dla wszystkich dokumentów w oknie podpisywania. 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 PIN-u. 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 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*. Jeśli został zainstalowany w systemie token rSign, po akcji *Wczytaj* także zostanie ukazany na liście.



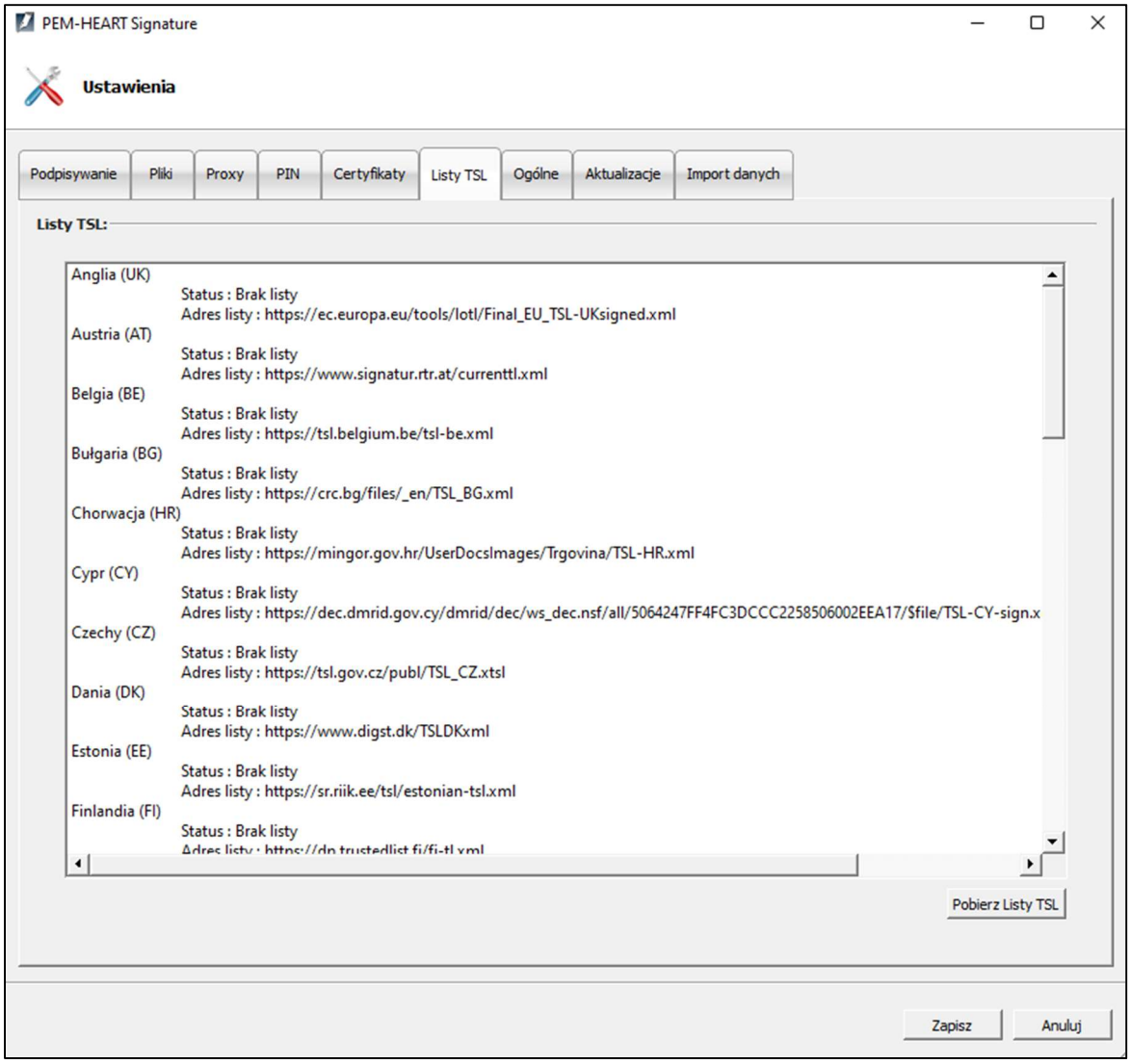
Rysunek 57 Ustawienia certyfikatów użytkownika

Przycisk *Zarejestruj* służy do rejestracji certyfikatu odczytanego z nośnika w magazynie systemowym. Eksport certyfikatu do pliku jest możliwy poprzez przycisk *Eksportuj*. Sekcja *Certyfikat 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.

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



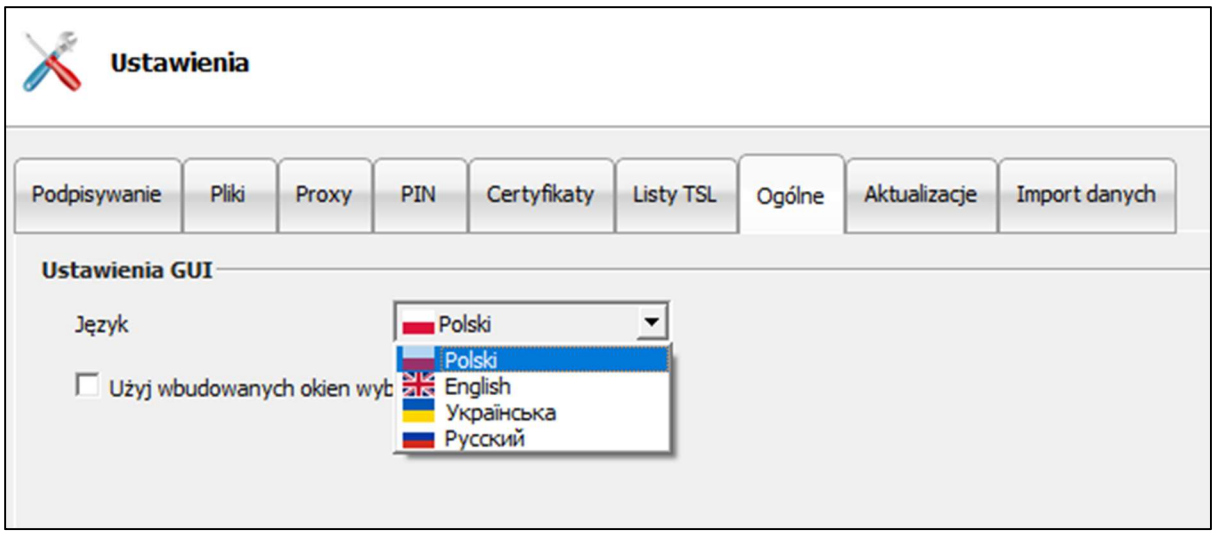
Rysunek 58 Ustawienia - listy TSL

weryfikacji podpisu natrafi na certyfikat niemożliwy do zweryfikowania w oparciu o posiadane przez program w danym momencie listy TSL). W celu pobrania list TSL należy kliknąć przycisk *Pobierz listy TSL*.

8.7 USTAWIENIA JĘZYKA

Zmiana języka programu jest możliwa poprzez zakładkę *Ogólne* w panelu *Ustawienia*. Języki do wyboru: *polski, angielski, ukraiński, rosyjski*.

Opcja *Użyj wbudowanych okien wyboru pliku* służy do zmiany wyglądu okien, które pokazują się z wyborem pliku np. do podpisu.



Rysunek 59 Wybór stosowanego języka w programie

8.8 AKTUALIZACJE

W oknie głównym (prawy dolny róg) PEM-HEART Signature jest podana wersja programu. Dodatkowo w zakładce *Aktualizacje* można sprawdzić, czy jest jego nowa wersja. Informacji o dostępnej aktualizacji można dokonywać manualnie poprzez naciśnięcie przycisku *Sprawdź aktualizacje* lub ustalić opcje automatycznego sprawdzania podczas uruchamiania programu. W przypadku wykrycia nowej wersji oprogramowania zostaną wyświetlone komunikaty.

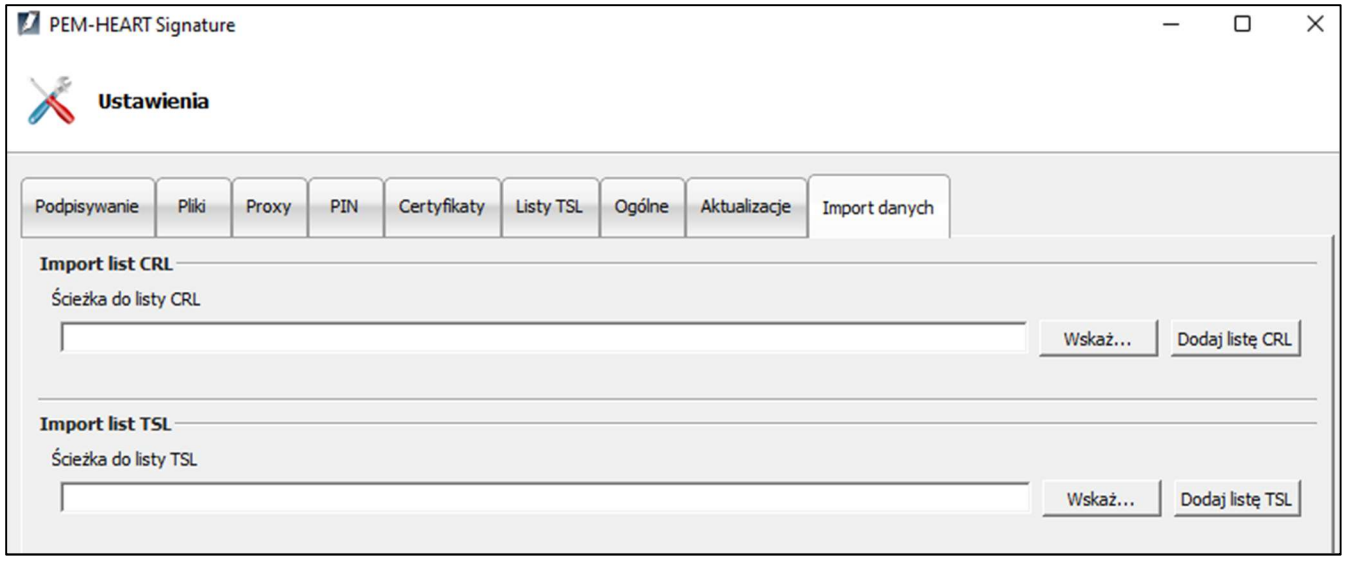
Rysunek 60 Okno z informacją o wersji oprogramowania

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 je do programu ręcznie.

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

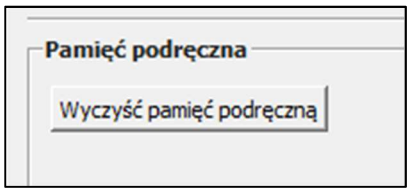
W celu wczytania pliku z listą CRL albo TSL, naciśnij klawisz *Wskaż* przy odpowiedniej liście (po czym trzeba wybrać odpowiedni plik na dysku), a następnie odpowiednio klawisz *Dodaj listę CRL* albo *Dodaj listę TSL*.



Rysunek 61 Ustawienia – import danych list CRL i TSL

8.9.1 CZYSZCZENIE PAMIĘCI PODRĘCZNEJ

Przycisk „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 automatycznie pobierze brakujące dane z zasobów sieciowych.



Rysunek 62 Opcja czyszczenia pamięci

9 PODPIS RSIGN

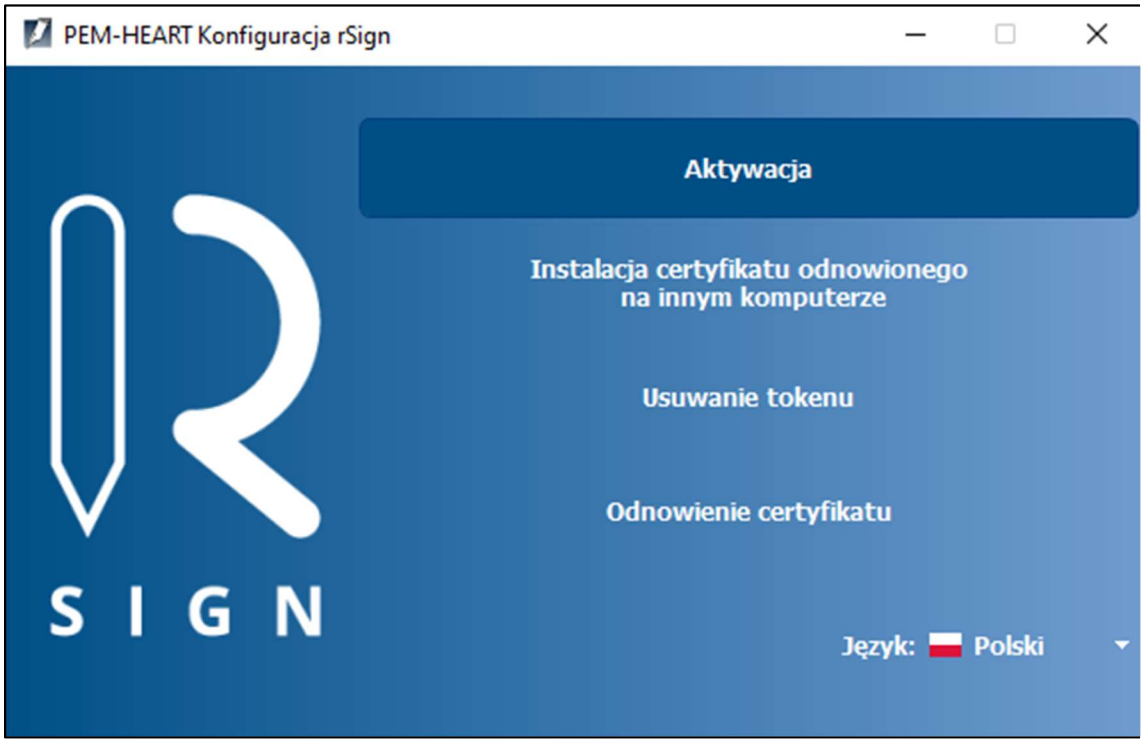
9.1 KONFIGURACJA NA KOMPUTERZE

9.1.1 DODAWANIE TOKENU RSIGN

Aby móc korzystać z podpisu rSign na danym komputerze (na danym koncie systemu Windows), należy skonfigurować podpis na każdym takim komputerze (koncie).

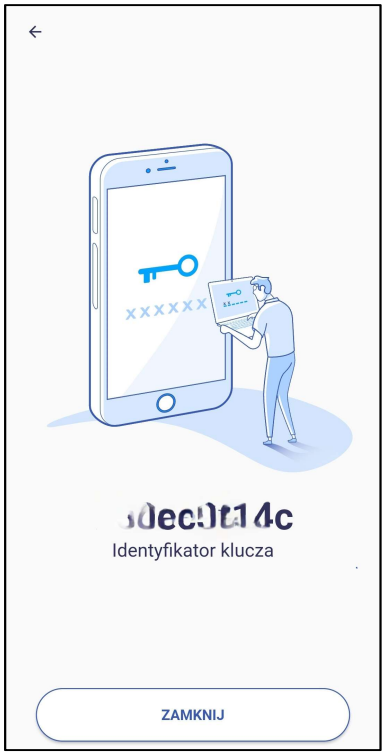
Cele tej operacji są dwojakie – po pierwsze, przy rozpoczynaniu składania podpisu program musi wiedzieć kto będzie składał podpis (jakim certyfikatem będzie składany podpis). Po drugie, istotnym celem jest zwiększenie bezpieczeństwa Twojego podpisu – podpis rSign można składać tylko na komputerze uprzednio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

W celu konfiguracji podpisu rSign uruchom program *PEM-HEART Signature -> Karta -> Konfiguracja rSign* lub z poziomu menu Windows *PEM-HEART Konfiguracja rSign*. Następnie należy wybrać przycisk *Aktywacja*

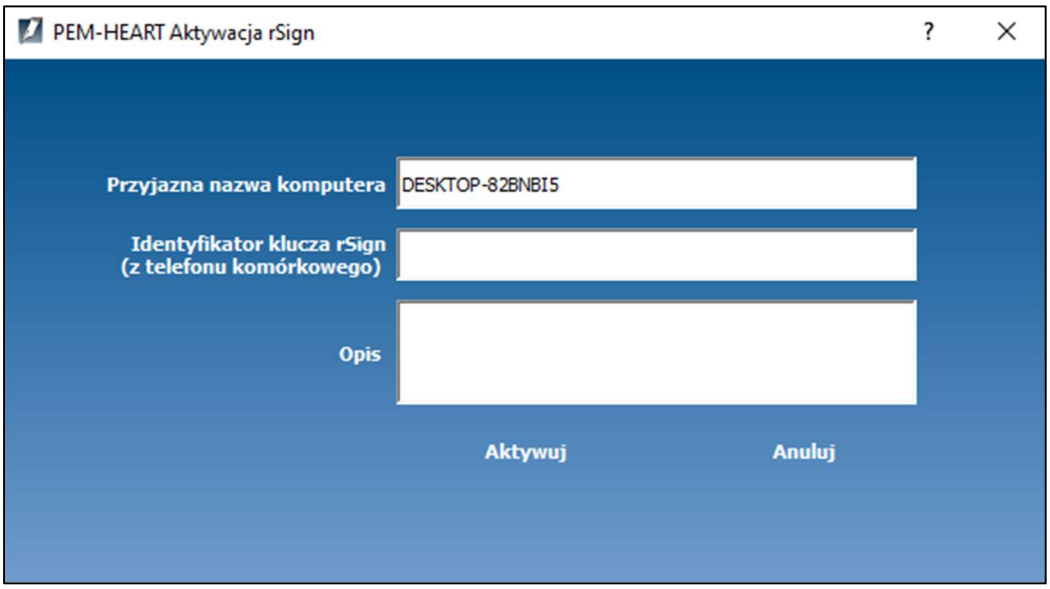


Rysunek 63 Konfiguracja podpisu rSign

Następnie przepisz Identyfikator klucza rSign z aplikacji na telefonie komórkowym.



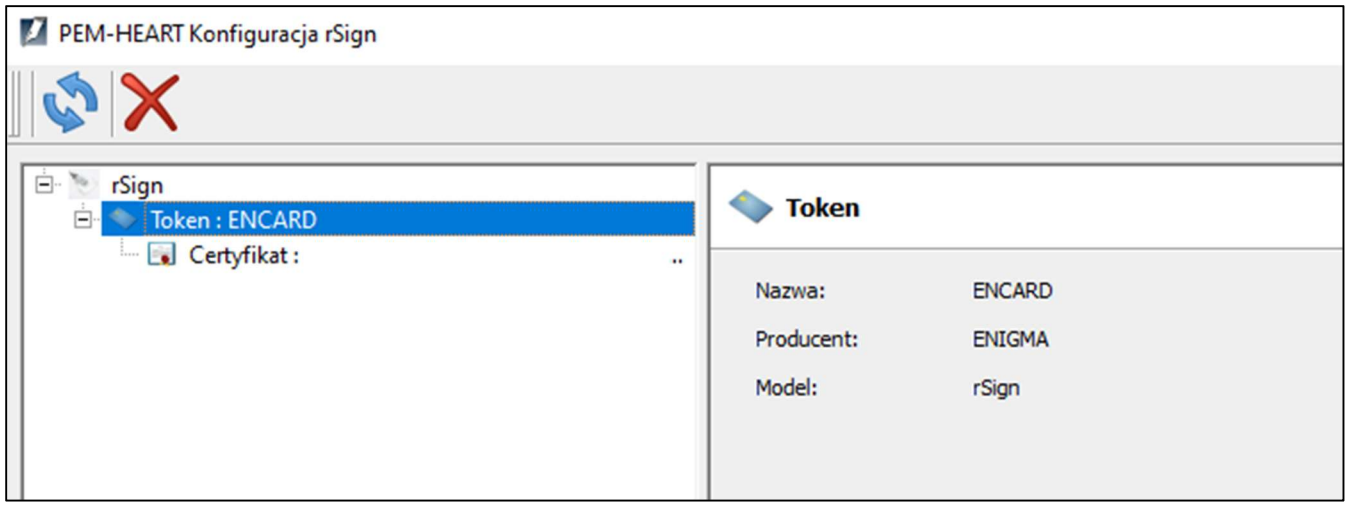
Rysunek 64 Okno aplikacji mobilnej z identyfikatorem klucza



Rysunek 65 Okno aktywacji podpisu rSign

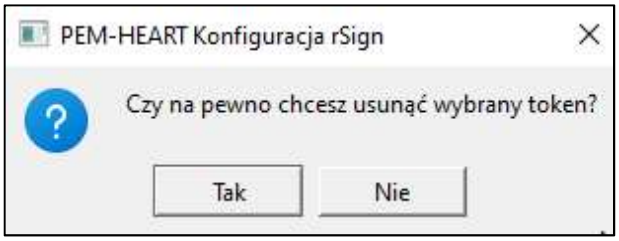
9.1.2 USUWANIE TOKENU RSIGN

Jeśli wystąpiła potrzeba usunięcia z komputera token rSign, taką operację można wykonać poprzez program *PEM-HEART Konfiguracja rSign*. Po uruchomieniu programu należy kliknąć w opcję *Usuwanie tokenu*. Następnie zostanie ukazany aktywny token rSign w konfiguracji oraz dane z certyfikatu.



Rysunek 66 Widok aktywnego tokenu rSign z danymi certyfikatu

Następnie należy kliknąć w lewym oknie na *Token: ENCARD*, co spowoduje  aktywację przycisku w górnym panelu – jego wybranie spowoduje proces usuwania tokenu. Użytkownik musi potwierdzić usunięcie w oddzielnym oknie:



Rysunek 67 Potwierdzenie usunięcia tokenu rSign

Kliknięcie *Tak* spowoduje usunięcie tokenu.

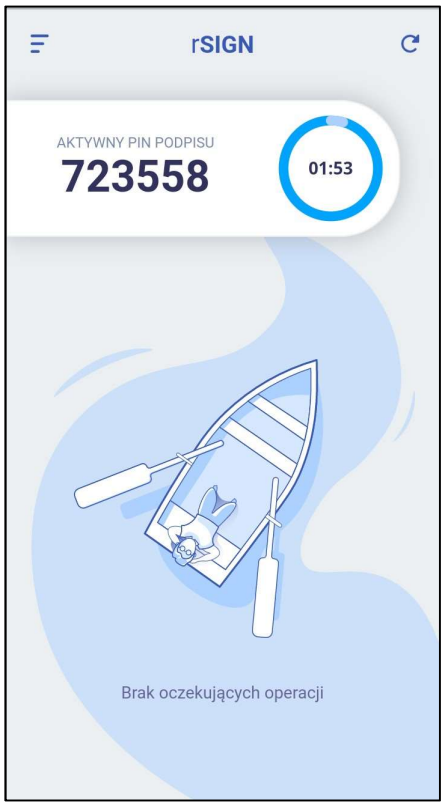
9.2 KONFIGURACJA APLIKACJI MOBILNEJ

9.2.1 INSTALACJA

Aplikacja dostępna do pobrania w sklepie AppStore oraz Google Play.

9.2.2 EKRAN GŁÓWNY

Po uruchomieniu aplikacji, domyślnie wyświetlany jest ekran z aktywnym PIN-em podpisu. W ramach widoku Użytkownik widzi kod PIN, timer określający czas na jego użycie oraz kolejkę oczekujących operacji. Oprócz tego, w prawym górnym rogu znajduje się ikona , której użycie odświeża widok powiadomień, oraz w lewym górnym rogu ikona , po wybraniu której wyświetlone zostaną opcje: *Operacje* (domyślnie wyświetlana opcja po uruchomieniu aplikacji), *Identyfikator klucza*, *Ustawienia*.

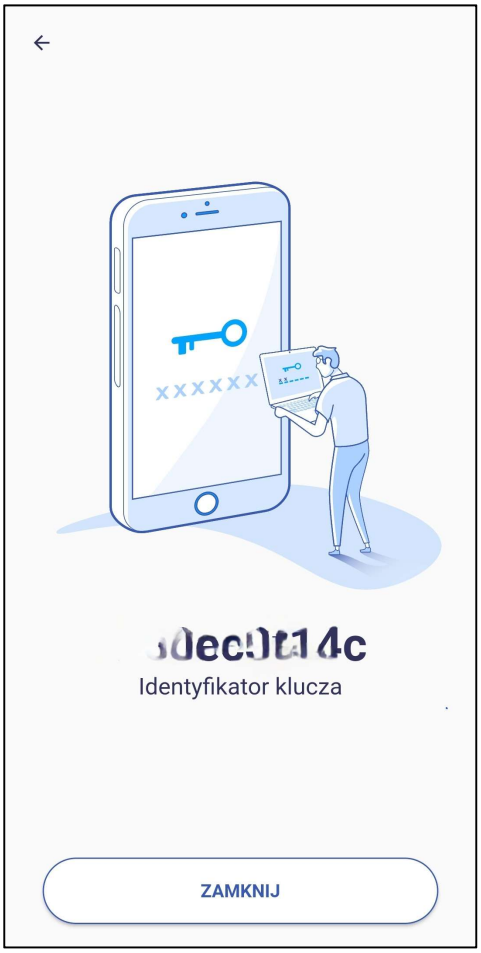


Rysunek 68 Ekran główny aplikacji mobilnej rSign

9.2.3 IDENTYFIKATOR KLUCZA

Wybranie opcji *Identyfikator klucza* spowoduje wyświetlenie ekranu z identyfikatorem klucza, stosowany

m. in. do konfiguracji użycia podpisu rSign na komputerze. Nim jednak Użytkownik będzie mógł go zobaczyć, program najpierw poprosi o podanie PIN-u – dopiero jego poprawne wprowadzenie i zatwierdzenie spowoduje wyświetlenie identyfikatora klucza.



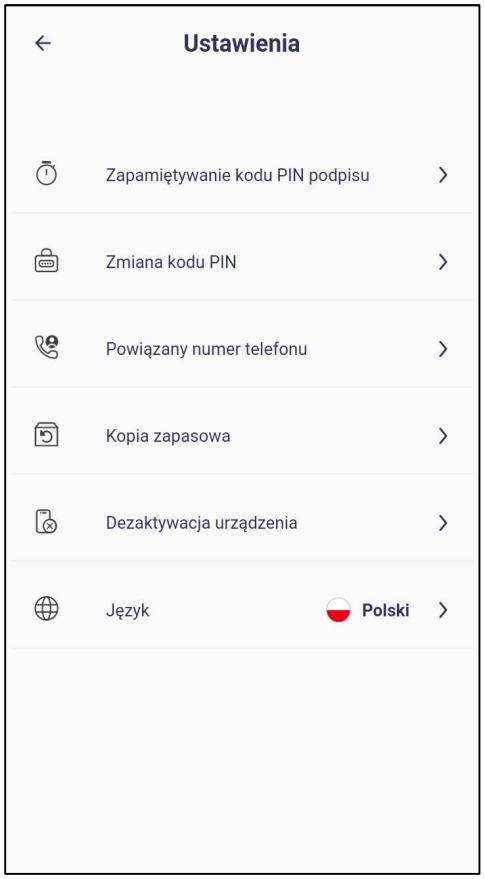
Rysunek 69 Ekran aplikacji po wybraniu opcji *Identyfikator klucza*

9.2.4 USTAWIENIA

Wybranie opcji *Ustawienia* wyświetli ekran z listą dostępnych ustawień aplikacji. Są to:

- *Zapamiętywanie kodu PIN podpisu* – opcja pozwalająca na zapamiętanie wprowadzonego kodu PIN na określony przez Użytkownika czas. Dostępne są cztery opcje – trzy predefiniowane: 3, 5 i 10minut oraz dowolna z zakresu od 1 do 60minut.
- *Zmiana kodu PIN* – opcja pozwalająca na zmianę kodu PIN.
- *Powiązany numer telefonu* – w tym miejscu Użytkownik wprowadza numer telefonu powiązany z kontem.
- *Kopia zapasowa* – umożliwia utworzenie kopii zapasowej służącej do aktywacji rSign na dowolnym urządzeniu.
- *Dezaktywacja urządzenia* – opcja pozwalająca na usunięcie danych aktywacji rSign z urządzenia.

- *Język* – umożliwia zmianę języka w aplikacji. Języki do wyboru: polski, angielski, rosyjski, ukraiński.

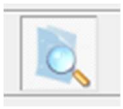


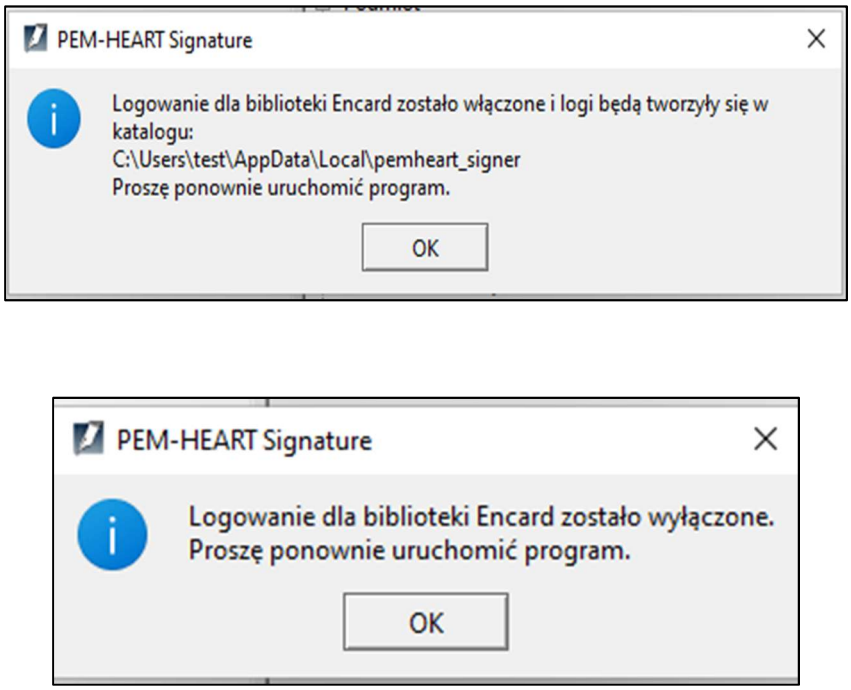
Rysunek 70 Ekran aplikacji po wybraniu opcji

10 ADMINISTROWANIE OPROGRAMOWANIEM PEM-HEART

10.1 LOGI OPERACJI KART DLA SYSTEMÓW WINDOWS

Oprogramowanie umożliwia włączenie logowania dla operacji wykonywanych z użyciem karty np. składanie podpisu pod dokumentem. Dostępne są dwie drogi włączenia takiej funkcjonalności:

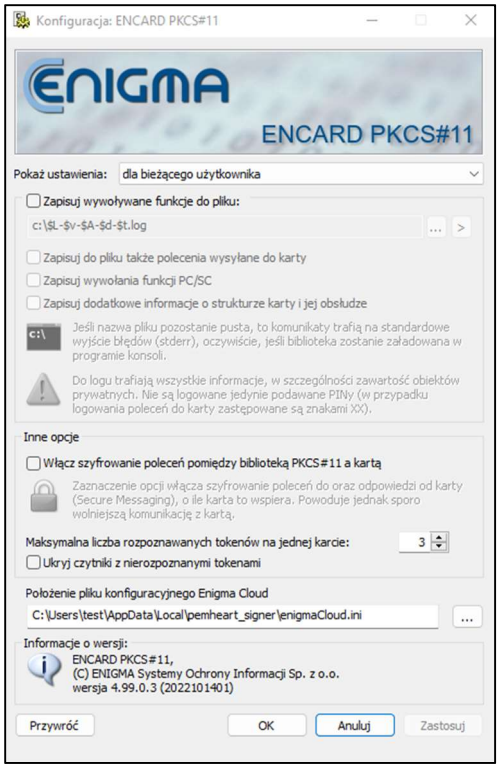
- Poprzez kliknięcie ikonki z „lupką” w panelu Diagnostyka uruchamianej przez funkcje zaawansowane.
-  - ikonka oznaczająca, że funkcja została włączona – przy jej pierwszym użyciu należy ponownie uruchomić program PEM-HEART Signature aby zmiany zostały zapisane,
-  - ikonka oznaczająca, że funkcja jest wyłączona – przy jej pierwszym włączeniu należy ponownie uruchomić program PEM-HEART Signature aby zmiany zostały zapisane.



Rysunek 71 Komunikat po operacji włączenia oraz wyłączenia logowania do kart IDEMIA

- Bardziej zaawansowana konfiguracja jest wywoływana przez okna do konfiguracji biblioteki PKCS#11. Należy wybrać odpowiednio *Menu Start->Programy->ENCARD->Konfiguracja ENCARD PKCS#11* Wybranie opcji konfiguracji spowoduje wywołanie okna do konfiguracji biblioteki PKCS#11.

Zaznaczenie opcji *Zapisuj wywoływane funkcje do pliku* (będącej jednocześnie nazwą pierwszej sekcji) służy do skonfigurowania zapisu do pliku logu wszystkich informacji, w szczególności zawartości obiektów prywatnych. Podawane PIN-y nie są zapisywane – w przypadku logowania polecenia do karty są zastępowane znakami XX.



Rysunek 72 Ekran konfiguracji biblioteki PKCS#11

Do ustalenia położenia i nazwy pliku logu służy przycisk ... Jeśli nazwa pliku pozostanie pusta, to komunikaty trafią na standardowe wyjście błędów (stderr), jeśli biblioteka zostanie załadowana w programie konsoli.

Biblioteka akceptuje w nazwie pliku specjalne makra, które umożliwiają zapis do różnych plików logu w zależności od aplikacji, która ją załaduje, czasu i daty bieżącej, wersji biblioteki i innych. Naciśnięcie przycisku > znajdującego się przy nazwie pliku logowania powoduje wyświetlenie dialogu konfiguracyjnego zawierającego listę wszystkich makr:

- $A - nazwa pliku aplikacji ładującej bibliotekę (bez ścieżki i rozszerzenia).
- $L - nazwa pliku załadowanej biblioteki (bez ścieżki i rozszerzenia).
- $l - nazwa wewnętrzna biblioteki.
- $D - data załadowania biblioteki w postaci YYYY-MM-DD.
- $d - data załadowania biblioteki w postaci YYYYMMDD.
- $T - czas załadowania biblioteki w postaci hh-mm-ss.
- $t - czas załadowania biblioteki w postaci hhmmss.

- $K - numer kompilacji biblioteki (np. 2008080901).
- $V - wersja główna biblioteki (np. 2.0).
- $v - pełna wersja biblioteki (np. 2.01.2.2).
- $$ - znak $.

W ramach zapisu wywoływanych funkcji do pliku, użytkownik może zaznaczyć pozostałe informacje, powodujące dodanie do logu dodatkowych informacji. Dodatkowe opcje to:

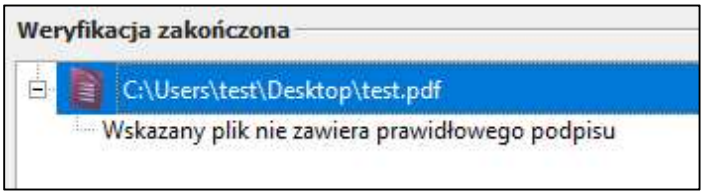
- *Zapisuj do pliku także polecenia wysyłane do karty*
- *Zapisuj wywołania funkcji PC/SC*
- *Zapisuj dodatkowe informacje o strukturze karty i jej obsłudze*

Druga sekcja okna konfiguracji biblioteki PKCS#11 umożliwia dodanie szyfrowania w połączeniu między biblioteką PKCS#11 a kartą, co następuje przez zaznaczenie opcji *Włącz szyfrowanie poleceń pomiędzy biblioteką PKCS#11 a kartą*. Oprócz tego można wskazać maksymalną liczbę rozpoznawanych tokenów na jednej karcie oraz ukryć czytniki z nierozpoznanymi tokenami.

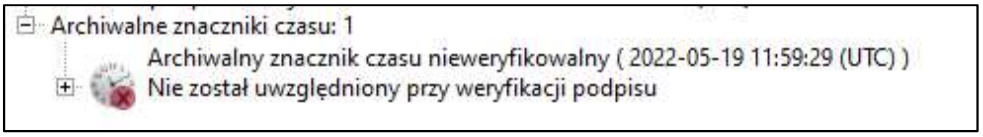
Tuż poniżej drugiej sekcji znajduje się miejsce do wskazania ścieżki położenia pliku konfiguracyjnego Enigma Cloud oraz informacje o oprogramowaniu konfigurującym.

Wszelkie zmiany zapisywane są przez wybranie przycisku *Zastosuj*. Wybranie *OK* również zapisuje zmiany oraz zamyka otwarte okno konfiguracji. Wszelkie zmiany opcji można anulować przez wybranie *Anuluj* (zamknięcie okna konfiguracji bez zapisywania zmian) lub *Przywróć* (przywrócenie ustawień z momentu tuż po uruchomieniu konfiguratora, bez zamykania programu).

11 ROZWIĄZYWANIE PROBLEMÓW



Rysunek 73 Komunikat o braku prawidłowego podpisu



Rysunek 74 Komunikat o nieweryfikowalnym archiwalnym znaczniku czasu

INSTALACJA		
Problem	Przyczyna	Rozwiązanie
Operacja zakończona niepowodzeniem	Użytkownik anulował proces instalacji programu	Ponownie uruchomić instalator

PODPISYWANIE		
Problem	Przyczyna	Rozwiązanie
Z żadnego z serwerów nie udało się pobrać znacznika czasu	Do certyfikatu nie jest przypisany żaden pakiet znaczników czasu	- spróbuj ponownie następnego dnia albo - wykup pakiet znakowania czasem (szczegóły: http://www.cencert.pl), albo - wyłącz opcję znakowania czasem podpisów (patrz rozdział **6.2 Znakowanie czasem**)
	Program nie ma dostępu do Internetu lub żądanie nie zostało zatwierdzone w	- sprawdź połączenie z Internetem - sprawdź ustawienia proxy (jeśli u Ciebie używany jest serwer

	aplikacji rSign	proxy) – patrz rozdział **8.3 Proxy**)
Funkcjonalność niedostępna dla aktualnego nośnika !!!	Brak zaimplementowanej funkcji obsługi weryfikacji danego pliku, podpis wykonany w nieobsługiwanym standardzie	Zgłoszenie do Cencert

WERYFIKACJA		
Problem	Przyczyna	Rozwiązanie
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)
Błąd otwarcia pliku wejściowego	Plik jest uszkodzony lub aktualnie otwarty w innym programie	Zamknij inny program a następnie spróbuj ponownie otworzyć plik w PEM-HEART Signature.
	Plik jest już otwarty w innym programie	
	Program nie ma dostępu do lokalizacji pliku	Zweryfikuj czy w danej lokalizacji faktycznie znajduje się plik
Żaden z plików nie zawiera prawidłowego podpisu	Plik jest uszkodzony lub został podpisany formatem nieobsługiwanym przez PEM-HEART SIgnature	Wskazanie innego pliku lub zgłoszenie do Cencert

12 SPIS RYSUNKÓW