

---

**Dokumentacja  
administratora  
*PEM-HEART Signature***

---

Copyright © Enigma S.O.l. Sp. z o.o.

Dokumentacja opracowana przez:



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>

Historia wersji		
1.0	26.03.2010	Bartosz Sajnaj <bartosz.sajnaj@enigma.com.pl>
Wersja początkowa		
1.1	11.02.2011	Bartosz Sajnaj
Wersja zaktualizowana do obsługi najnowszej wersji programu. Dodana tabele wpieranych systemów operacyjnych.		
1.2	22.09.2011	Bartosz Sajnaj
Wersja zaktualizowana do obsługi najnowszej wersji programu.		
1.3	05.06.2012	Bartosz Sajnaj
Aktualizacja do wersji 3.9.5 oprogramowania.		
1.4	15.10.2013	Sławomir Szopa
Aktualizacja do wersji 3.9.9		
1.5	25.03.2014	Sławomir Szopa
Dodanie opisu konfiguracji logowania operacji z biblioteki pkcs#11 obsługującej kartę/token.		
1.6	03.03.2021	Dominika Hoszowska
Aktualizacja do wersji 3.9.15		

# Spis treści

1 Wstęp.....	4
2 Bezpieczeństwo produktu.....	5
2.1 Cele i funkcje zabezpieczeń.....	5
2.2 Zasady bezpiecznego użytkowania produktu.....	5
3 Instalacja w systemie Windows.....	6
3.1 Usuwanie oprogramowania z systemu.....	12
3.1.1 Usuwanie.....	13
3.1.3 Naprawa.....	14
4 Instalacja w systemie Linux.....	16
4.1 Instalacja poprzez menadżera plików.....	16
4.2 Instalacja poprzez linię komend.....	20
4.3 Usuwanie oprogramowania z systemu.....	20
5 Instalacja w systemie MacOSX.....	22
5.1 Usuwanie oprogramowania z systemu.....	26
6 Logi z operacji kartowych na systemie WINDOWS.....	26
7 Konfiguracja Proxy z poziomu administratora w systemie Windows.....	27

## 1 Wstęp

Oprogramowanie **PEM-HEART Signature** służy do składania i weryfikacji kwalifikowanych podpisów elektronicznych dla dokumentów w systemach rodziny Windows, Linux (*Debian* od wersji 5.0, *Ubuntu* od 8.04) oraz *MacOSX* (minimum wersja 10.6).

Oprogramowanie **PEM-HEART Signature** z komponentem technicznym w postaci czytnika i karty z kluczem kwalifikowanym stanowi całość i jest w myśl ustawy o podpisie elektronicznym, *bezpiecznym urządzeniem do składania i weryfikacji kwalifikowanych podpisów elektronicznych*.

Możliwe jest także: znakowanie czasem podpisu, składanie podpisów wielokrotnie równoległych (każdy podpis niezależny od pozostałych) oraz kontrasygnaty (podpis pod dokumentem i wcześniejszymi podpisami), tworzenie postaci LONG podpisu (podpis oznakowany czasem i uzupełniony o listy CRL lub OCSP w celu ułatwienia późniejszej weryfikacji), podpisywanie dokumentów XML zawierających załączniki, a także zmiana kodu PIN do karty oraz odblokowanie karty kodem PUK.

**PEM-HEART Signature** wykonuje podpis elektroniczny w formatach: **XAdES** zgodnym ze specyfikacją techniczną *ETSI TS 101 903 XML Advanced Electronic Signatures* (XAdES), **CAAdES CMS** i **CAAdES S/MIME** zgodnych ze specyfikacją techniczną *ETSI TS 101 733 Electronic Signature Format* (CAAdES to skrót od CMS Advanced Electronic Signatures) oraz **PAdES** (norma ETSI TS 102 778) - *PDF Advanced Electronic Signatures*. Standardy te zostały określone przez *European Telecommunications Standards Institute*. Formaty te określają strukturę pliku zawierającego podpis. Wybór określonego formatu pociąga za sobą

wymaganie na oprogramowanie, które będzie w stanie zweryfikować poprawność takiego podpisu.

Oprogramowanie umożliwia wykonywanie podpisów elektronicznych otaczających, gdzie zarówno podpis jak i podpisany plik jest zawarty w jednym pliku wyjściowym, jak i podpisów odłączonych, gdzie podpis jest zawarty w oddzielnym pliku. A także istnieje możliwość dołączenia „*typu zobowiązania*” (*Commitment type indication*): potwierdzenie pochodzenia, potwierdzenie otrzymania, potwierdzenie dostarczenia, potwierdzenie wysłania/nadania, formalne zatwierdzenie (*proof of approval*), potwierdzenie utworzenia.

**PEM-HEART Signature** może weryfikować wszystkie dokumenty zawierające podpisy elektroniczne zgodne z wyżej wymienionymi formatami, a także formaty stosowane przez działające w Polsce inne kwalifikowane centra certyfikacji.

Niniejszy dokument opisuje procedury instalacji oprogramowania **PEM-HEART Signature**.

## 2 Bezpieczeństwo produktu

### 2.1 Cele i funkcje zabezpieczeń

Program zapewnia składanie i weryfikację bezpiecznych podpisów elektronicznych, zgodnych z ustawą o podpisie elektronicznym, dla dokumentów w systemach Windows, Linux oraz MacOSX.

### 2.2 Zasady bezpiecznego użytkowania produktu

Program ma służyć do składania i weryfikacji bezpiecznych podpisów elektronicznych (równoważnych według prawa na mocy *Ustawy o podpisie elektronicznym* z podpisem odręcznym), należy więc przestrzegać następujących warunków użytkowania:

1. 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, Linux oraz MacOSX) oraz ustawiając takie prawa dostępu do katalogów z plikami wykonywalnymi, aby użytkownik nie miał prawa modyfikacji zawartych w nich plików wykonywalnych.
2. 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).
3. 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.

- 
4. 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 w systemie Windows



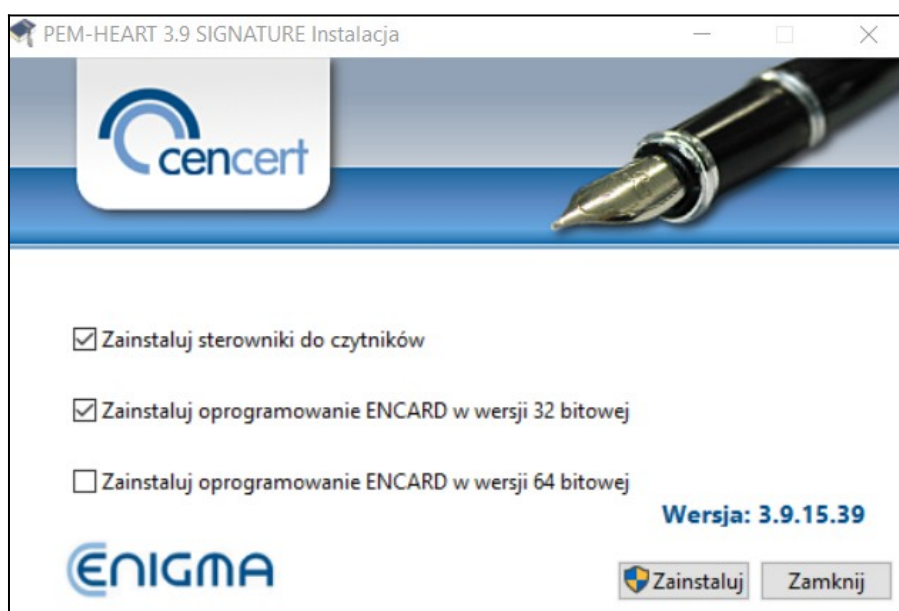
### Uwaga!

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

Instalacja przeprowadzana jest na przykładzie systemu Windows 10.

Do przeprowadzenia instalacji należy umieścić nośnik instalacyjny w odpowiednim dla niego napędzie/urządzeniu. Program instalacyjny powinien uruchomić się automatycznie. Jeśli funkcja autostartu w systemie jest wyłączona należy uruchomić plik *pemheart-signature.exe* z głównego katalogu nośnika instalacyjnego.

Program instalacyjny wyświetli okno wyboru komponentów do zainstalowania. Domyślnie zainstalowane zostaną sterowniki do czytników oraz oprogramowanie ENCARD w wersji 32 bitowej. Można pominąć instalację części komponentów lub zmienić wersję oprogramowania ENCARD, odznaczając lub zaznaczając pola z ich nazwami. Po dokonaniu wyboru, należy



wybrać

przycisk

Zainstaluj.

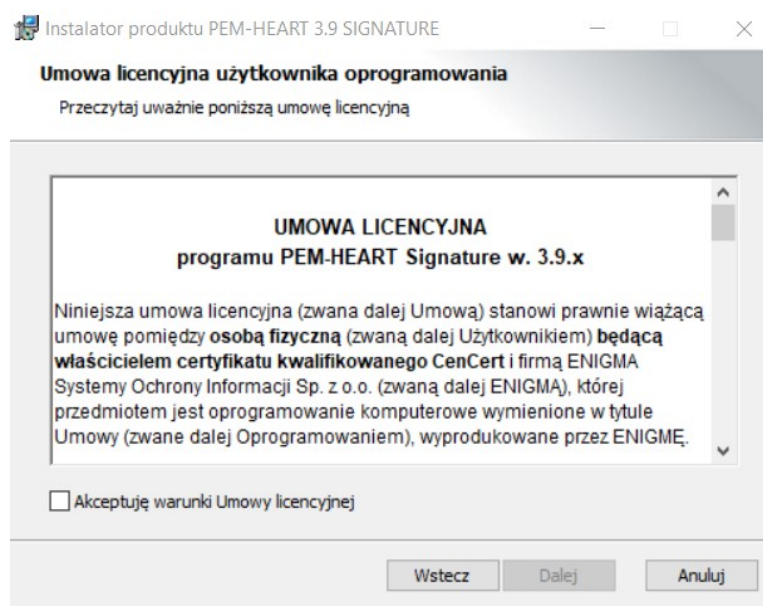
Rysunek 1 Okno wyboru komponentów do zainstalowania

Następnie program instalacyjny wyświetli okno powitalne, w którym należy wybrać przycisk *Dalej*, co spowoduje kontynuację procesu instalacji oprogramowania **PEM-HEART Signature**.



Rysunek 2 Okno powitalne instalatora

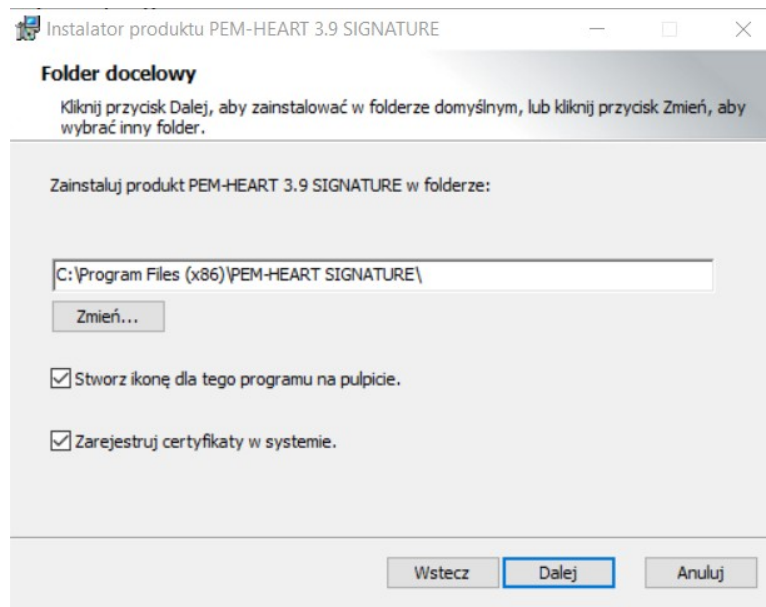
Program instalacyjny wyświetli okno umowy licencyjnej użytkownika oprogramowania. W celu kontynuowania procesu instalacji, należy zapoznać się ze wspomnianą umową, zaakceptować ją zaznaczając pole w dolnej części ekranu, a następnie wybrać przycisk *Dalej*.



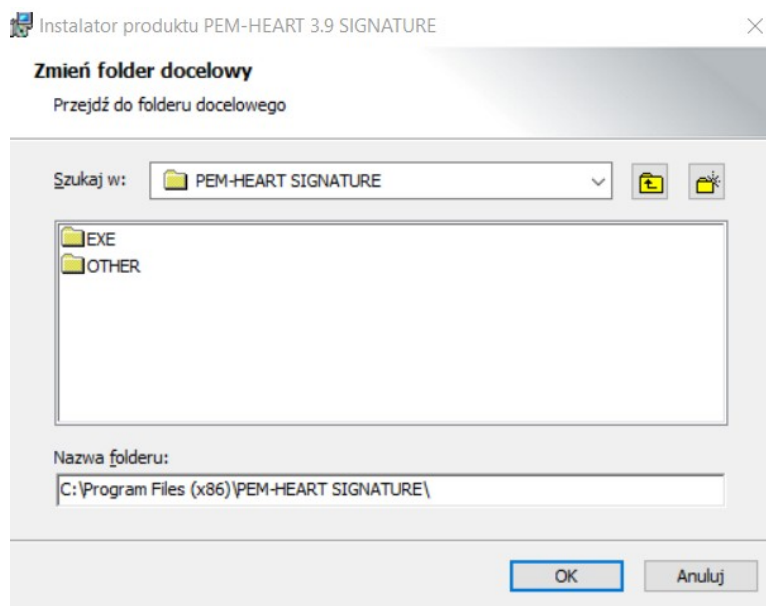
Rysunek 3 Okno umowy licencyjnej użytkownika oprogramowania

Następne okno pozwala na wybranie katalogu, w którym zostanie zainstalowany program. Domyślnie w systemie 64-bitowym instalacja odbywa się w katalogu *C:\Program Files (x86)\PEM-HEART SIGNATURE\* zaś w systemie 32-bitowym w katalogu *C:\Program Files\PEM-HEART SIGNATURE\*. Katalog można zmienić wybierając przycisk *Zmień*. Po zmianie katalogu lub zaakceptowaniu domyślnych ustawień, należy wybrać przycisk *Dalej*, co spowoduje kontynuację procesu instalacji.



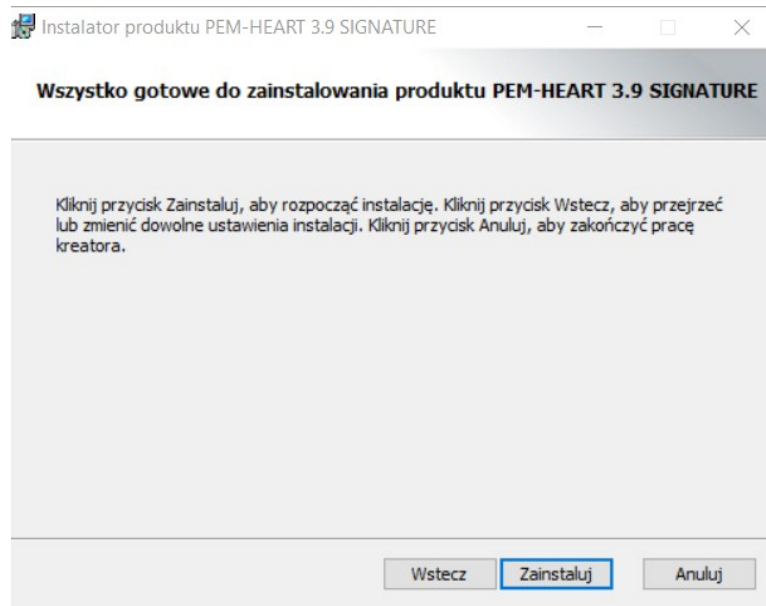


Rysunek 4 Konfiguracja katalogu instalacji

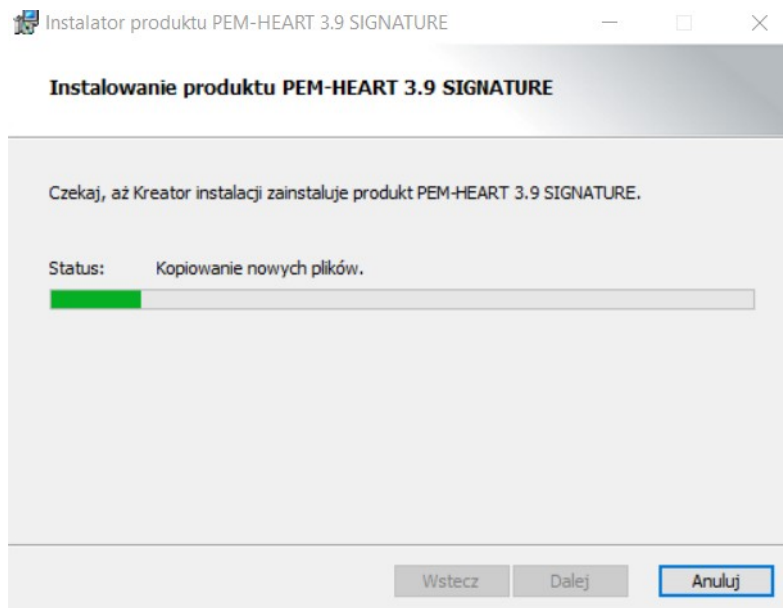


Rysunek 5 Konfiguracja katalogu instalacji cd.

Po ustawieniu wszystkich parametrów instalacji, program instalacyjny wejdzie w tryb gotowości do instalacji. Można wykorzystać przycisk *Wstecz*, aby ponownie ustawić część parametrów. Jeżeli wszystkie parametry zostały ustawione poprawnie, należy wybrać przycisk *Zainstaluj*, co spowoduje rozpoczęcie instalacji oprogramowania **PEM-HEART Signature**.



Rysunek 6 Okno gotowości do instalacji



Rysunek 7 Instalacja aplikacji

Zakończenie procesu instalacji oprogramowania **PEM-HEART Signature** sygnalizowane jest wyświetleniem poniższego okna. Wybranie przycisku *Zakończ* zamknie program instalacyjny i zostanie wyświetlone okno informujące o konieczności ponownego uruchomienia komputera.

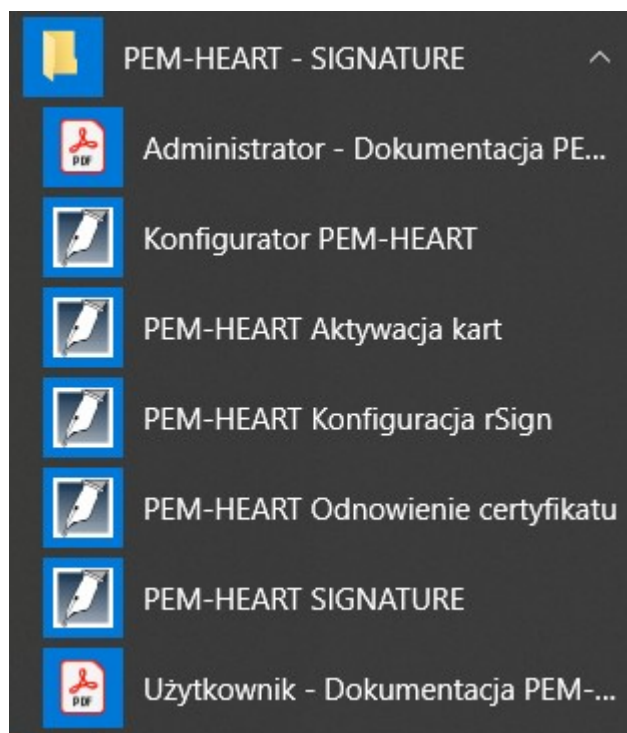


Rysunek 8 Zakończenie instalacji



Rysunek 9 Okno informujące o konieczności ponownego uruchomienia komputera

Po instalacji w *Menu Start* systemu będzie dostępna pozycja jak na rysunku poniżej:



Rysunek 10 Skrót do oprogramowania w Menu Start

Jeśli zaznaczona została opcja instalacji skrótu na pulpicie to zostanie na nim umieszczona ikonka programu.



Rysunek 11 Skrót do programu PEM-HEART Signature na pulpicie

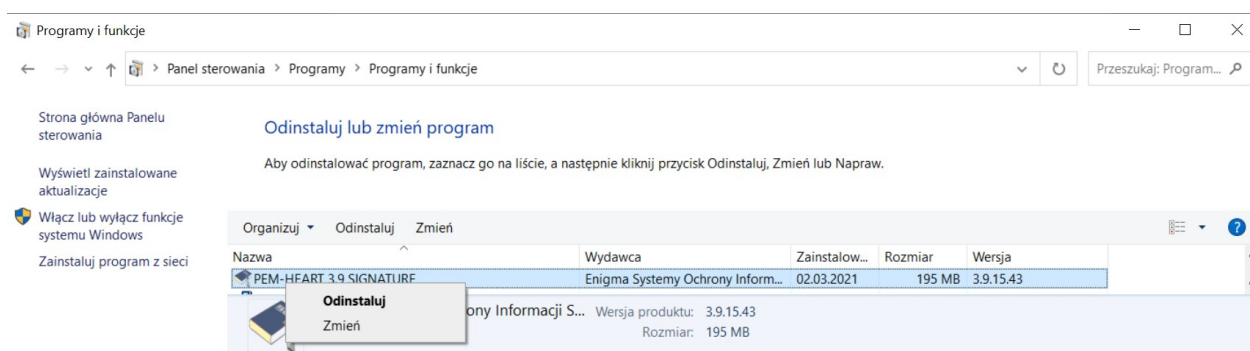


Aby aplikacja poprawnie działała na systemie Windows 7 należy zainstalować aktualizacje systemu KB4474419 oraz KB4490628.

Jeżeli po ich zainstalowaniu, uruchomieniu ponownym komputera i uruchomieniu aplikacji pojawia się komunikat informujący o problemie weryfikacji podpisu pod kodem programu należy kliknąć aplikację PEM-HEART Signature prawym przyciskiem myszy, wybrać „Właściwości”, a następnie w zakładce „Podpisy cyfrowe” wybrać podpis i nacisnąć przycisk „Szczegóły”. Powinna wyświetlić się informacja że podpis został poprawnie zweryfikowany. Po tej operacji aplikacja powinna działać poprawnie.

## 3.1 Usuwanie oprogramowania z systemu

W celu usunięcia, modyfikacji lub naprawy programu należy uruchomić aplikację zarządcy oprogramowania systemu (**Menu Start->Panel sterowania->Programy i funkcje**) lub też ponownie plik instalatora. Widok w systemie Windows 10 został przedstawiony na poniższym rysunku.



Rysunek 12 Widok aplikacja zarządcy oprogramowania systemu Windows 10

Do wyboru dostępne są następujące opcje:

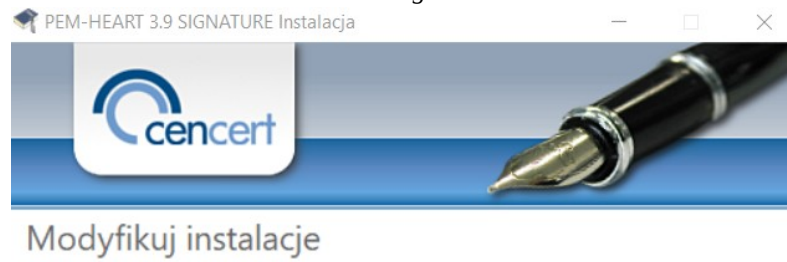
1. *Odinstaluj* - wybór tej opcji umożliwia przeprowadzenie operacji odinstalowywania programu z systemu.
2. *Zmień* - wybranie tej opcji umożliwia wybór przeprowadzenia operacji naprawy lub odinstalowywania programu.

Po uruchomieniu pliku instalatora zostanie wyświetlone okno wyboru operacji instalatora.

Do wyboru są opcje:

*Napraw* - wybranie tej opcji umożliwia przeprowadzenie operacji naprawy programu – przywrócenia stanu aplikacji tuż po instalacji

*Odinstaluj*- wybór tej opcji umożliwia bezpośrednie przeprowadzenie operacji usuwania programu z systemu.



Napraw

Odinstaluj

Zamknij

*Rysunek 13 Okno wyboru operacji instalatora*

W kolejnych podrozdziałach zostaną opisane przebiegi każdej z wyżej wymienionych procedur instalatora programu.

### 3.1.1 Usuwanie

W przypadku wybrania przycisku *Usuń* w programie zarządcy instalacji systemu Windows zostanie wyświetlone okno z poniższym komunikatem, po zaakceptowaniu którego zostanie od razu uruchomiona procedura usuwania programu.

Po wyborze opcji usunięcia programu zostanie wyświetlone następujące okno:

*Rysunek 14 Przebieg procedury usuwania programu*

Po zakończeniu procedury usuwania programu zostanie wyświetlone okno informujące o konieczności ponownego uruchomienia programu.



Rysunek 15 Okno informujące o konieczności ponownego uruchomienia komputera

### 3.1.3 Naprawa

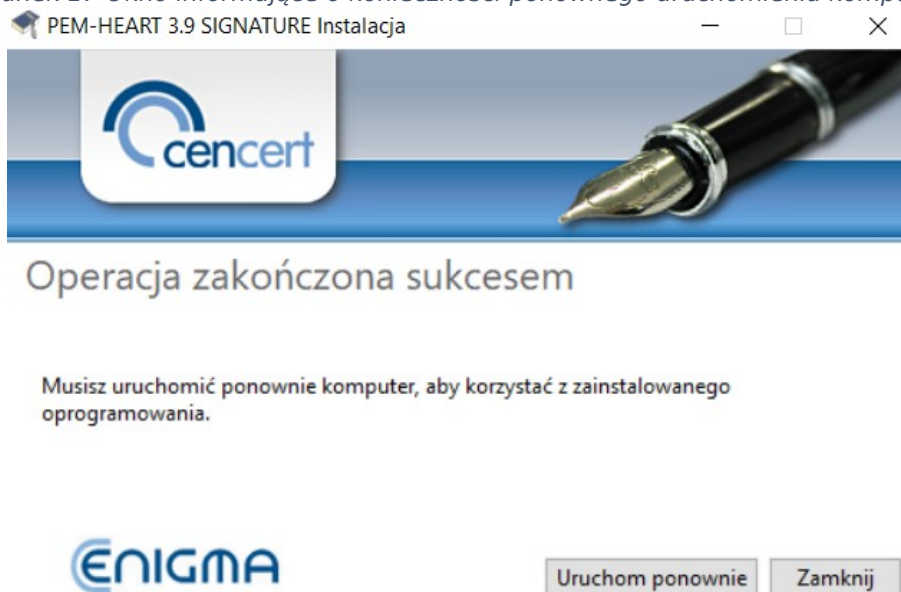
Po wyborze opcji naprawy zostanie rozpoczęta procedura naprawy instalacji programu.



Rysunek 16 Okno przebiegu naprawy

Po zakończeniu procedury naprawy zostanie wyświetlone okno informujące o konieczności ponownego uruchomienia komputera.

Rysunek 17 Okno informujące o konieczności ponownego uruchomienia komputera





## 4 Instalacja w systemie Linux



### Uwaga!

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

Instalacja przeprowadzana jest na przykładzie systemu *Ubuntu 20.04 LTS*.

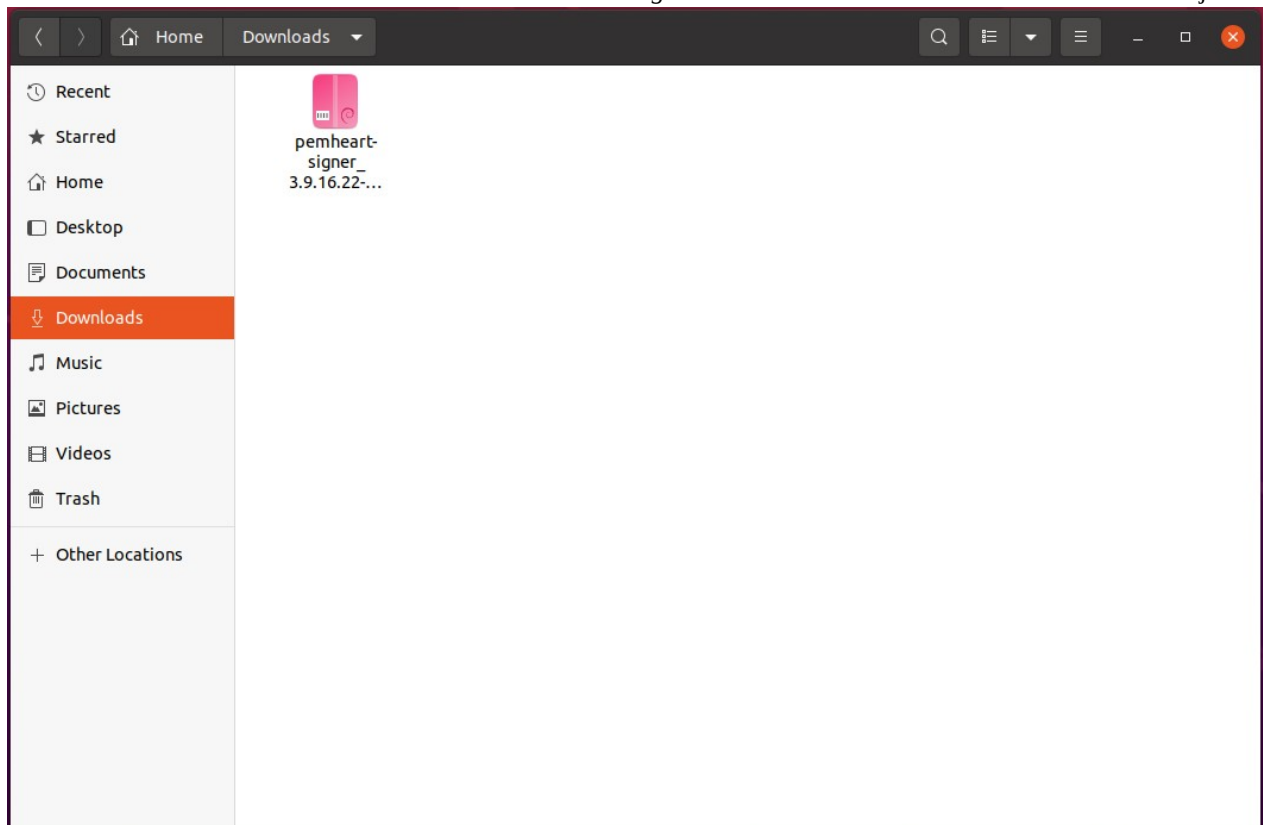
W systemowym menadżerze pakietów (np. Oprogramowanie Ubuntu) lub poprzez terminal z linii komend.

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

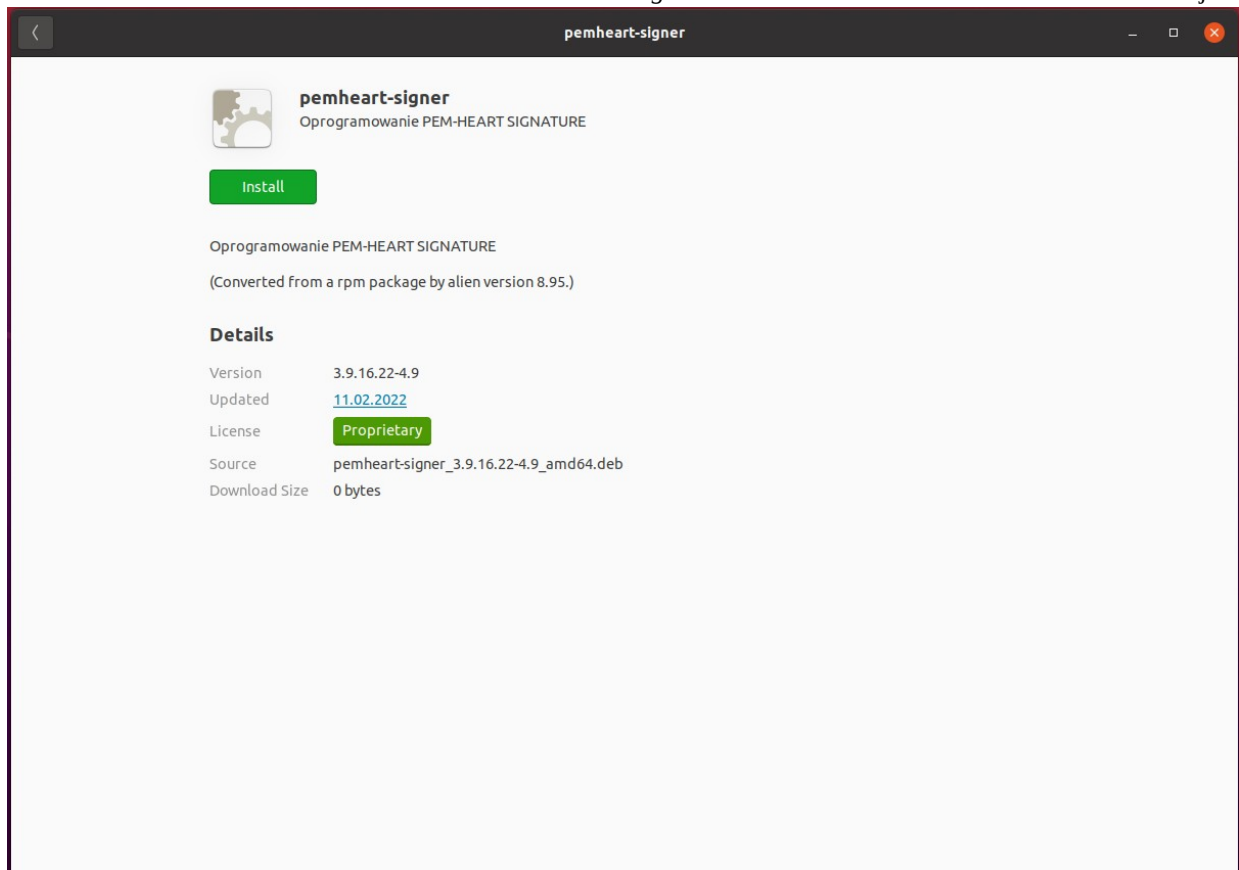
```
sudo apt-get install pcscd  
sudo apt-get install libncurses5
```

### 4.1 Instalacja poprzez menadżera plików

W menadżerze należy zlokalizować w strukturze plików miejsce, w którym znajdują się pliki instalacyjne *PEM-HEART Signature* (płyta CD, nośnik USB itp.).

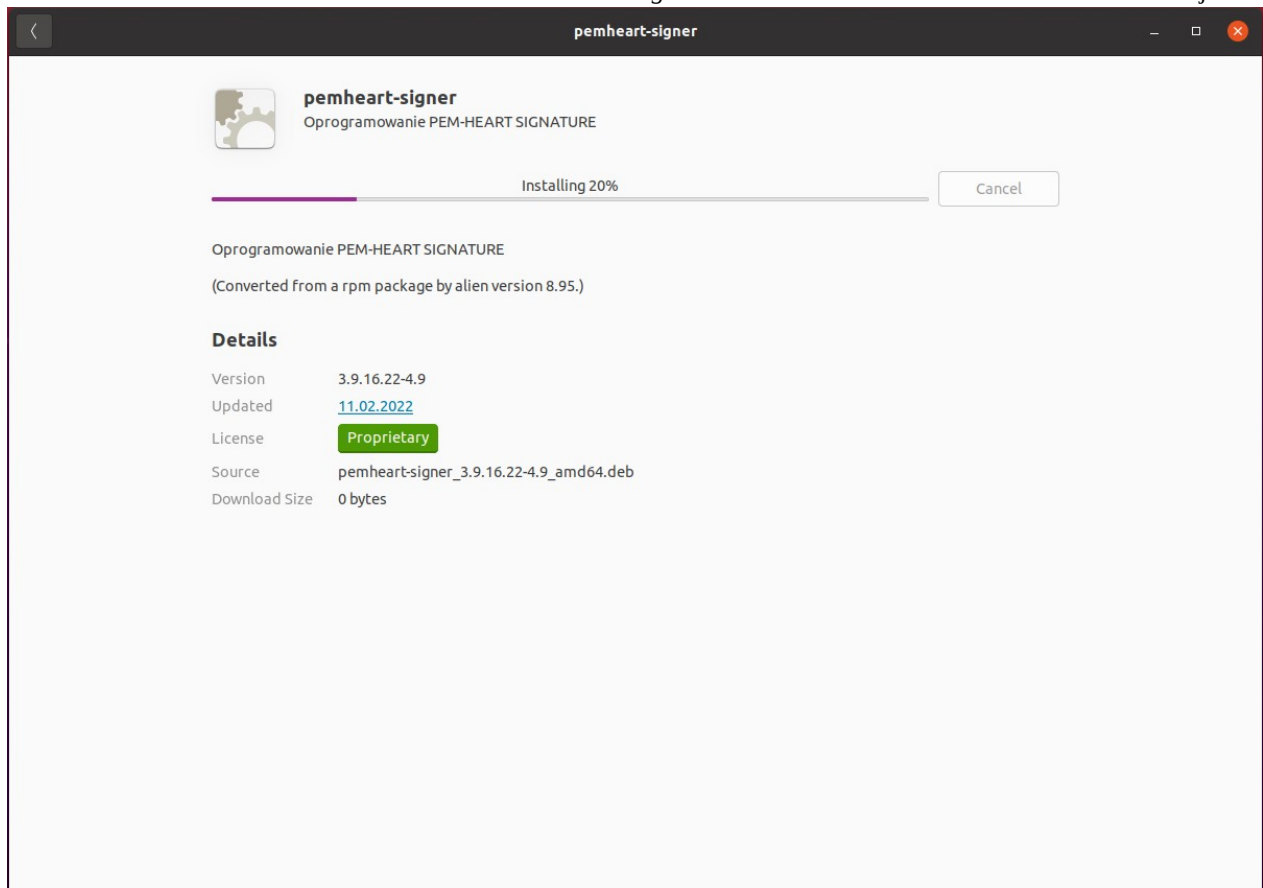
*Rysunek 18 Widok Menadżera plików*

Instalacji dokonuję się poprzez uruchomienie (dwuklik) danego pliku. Otwarty zostanie wtedy domyślnie skojarzony menadżer pakietów.



Rysunek 19 Okno z instalacją

Po wciśnięciu przycisku *Zainstaluj* PEM-HEART Signature zostaje zainstalowany w systemie.



Rysunek 20 Instalacja

Po zakończeniu instalacji zostanie wyświetlony odpowiedni komunikat i okno instalatora może zostać zamknięte.

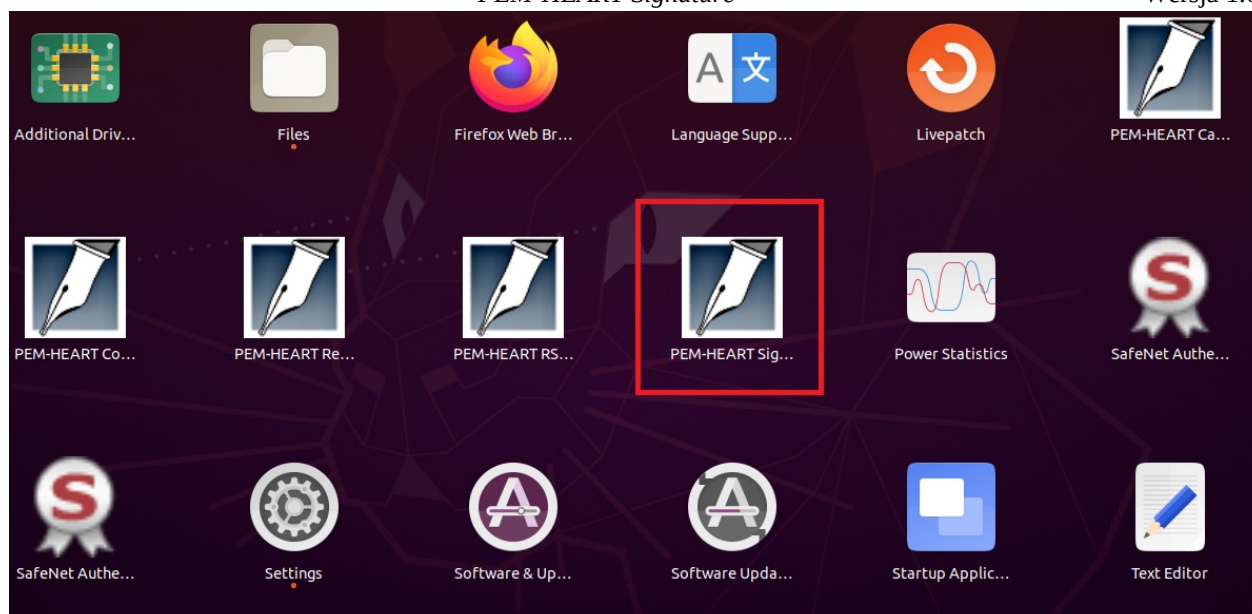
Na koniec należy zainstalować program *Safenet Authentication Client*, aby umożliwić korzystanie ze wszystkich dostępnych kart. Plik instalacyjny można znaleźć na stronie [cencert.pl](http://cencert.pl).



### Uwaga!

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 menu programów systemu:

*Rysunek 21 Widok programu w Menu Programy*

## 4.2 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 (płyta CD, nośnik USB itp.).

Oprogramowanie dystrybuowane jest w postaci pakietu instalacyjnego (plik z rozszerzeniem .deb):

```
PH-3.9.13.25_amd64.deb
```

Aby zainstalować pakiet "PEM-HEART Signature" w systemie Ubuntu 20.4 LTS, należy wywołać polecenie:

```
sudo dpkg -i PH-3.9.13.25_amd64.deb
```

## 4.3 Usuwanie oprogramowania z systemu

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

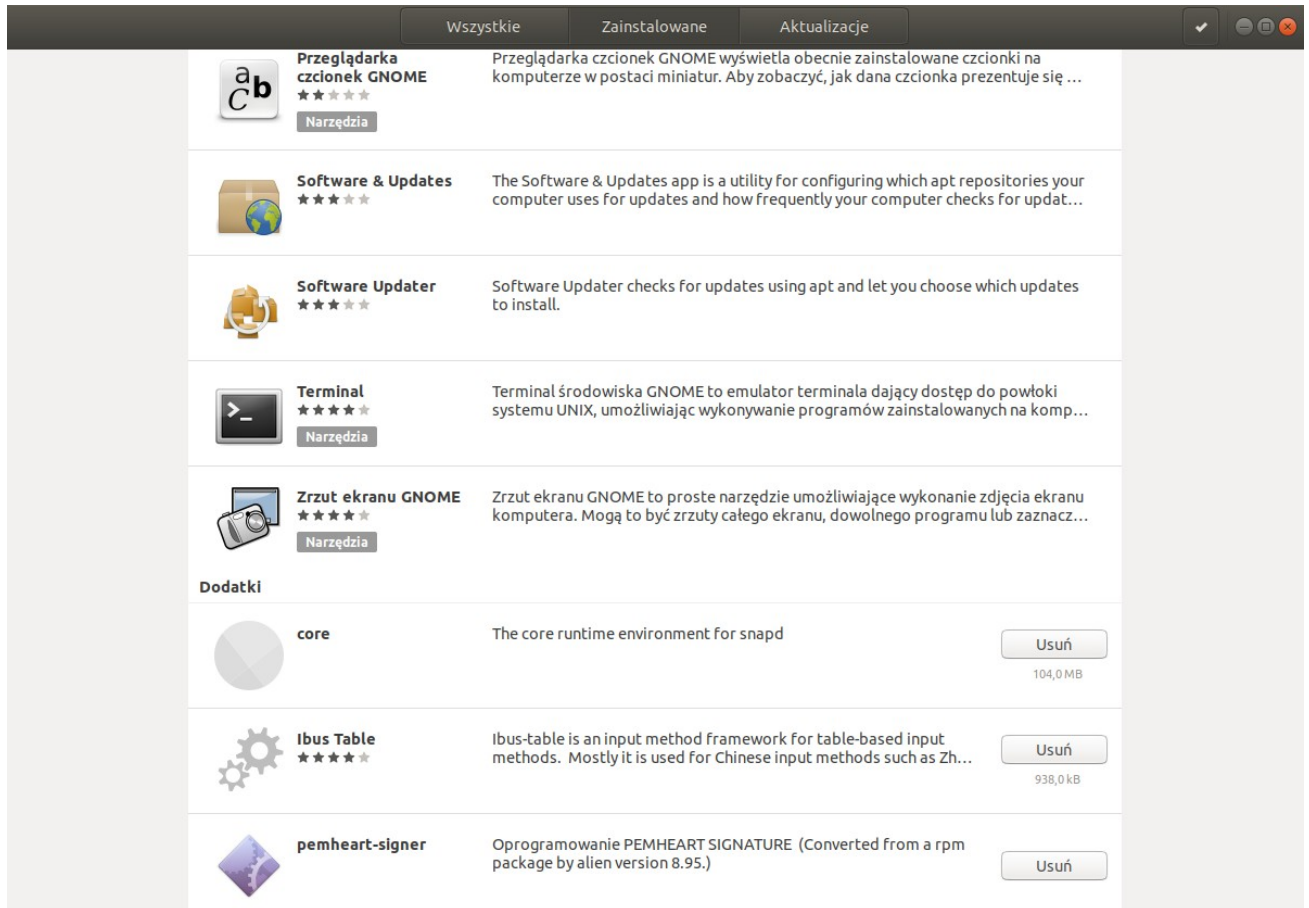
### 4.3.1.1 Usuwanie oprogramowania poprzez linię komend

Deinstalacja PEM-HEART Signature dokonywana jest za pomocą komendy:

```
sudo apt-get purge pemheart-signer
```

### 4.3.1.2 Usuwanie oprogramowania poprzez menadżera pakietów

Po uruchomieniu menadżera pakietów (w przykładzie wykorzystano *Oprogramowanie Ubuntu*) należy znaleźć w zakładce Zainstalowane pemheart-signer, a następnie kliknąć *Usuń*.



Rysunek 22 Widok menadżera pakietów

## 5 Instalacja w systemie MacOSX

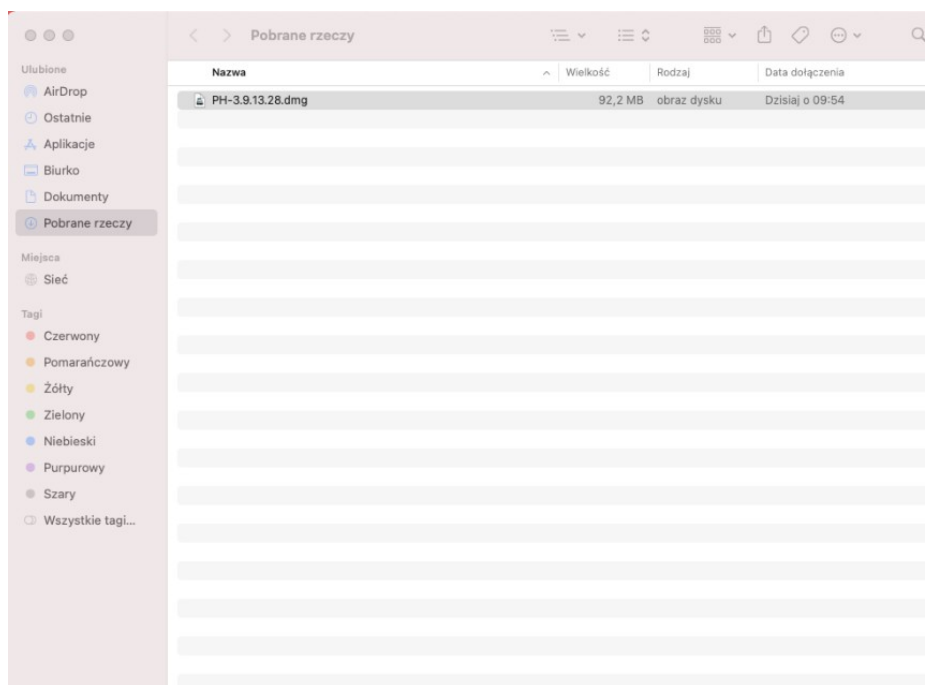


### Uwaga!

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

Instalacja przeprowadzana jest na przykładzie systemu *MacOS Big Sur*.

W menadżerze plików *Finder* należy zlokalizować w strukturze plików miejsce, w którym znajduje się plik instalacyjny *PEM-HEART Signature* (płyta CD, nośnik USB itp.).

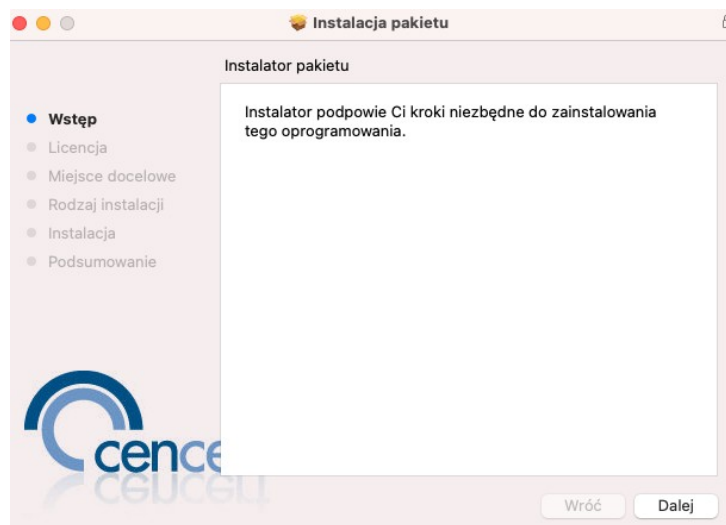


Rysunek 23 Lokalizacja pakietu instalacyjnego w strukturze plików

Następnie należy uruchomić plik instalacyjny. Zostanie wtedy wyświetlone okno instalatora.

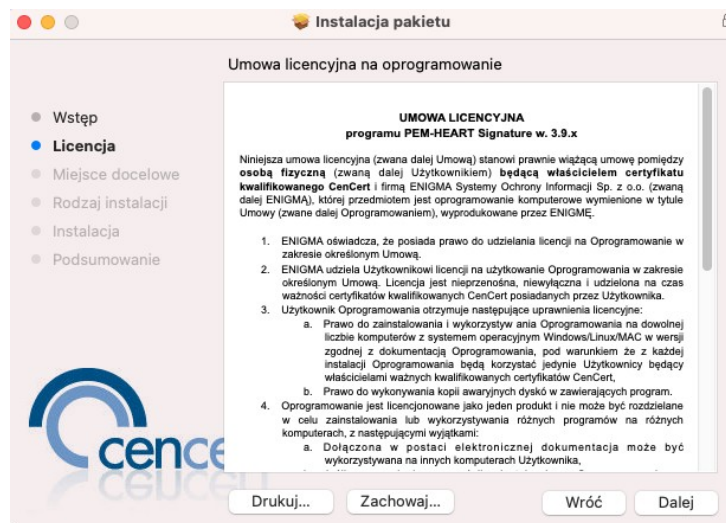


Rysunek 24 Widok pliku instalacyjnego



Rysunek 25 Okno powitalne instalatora

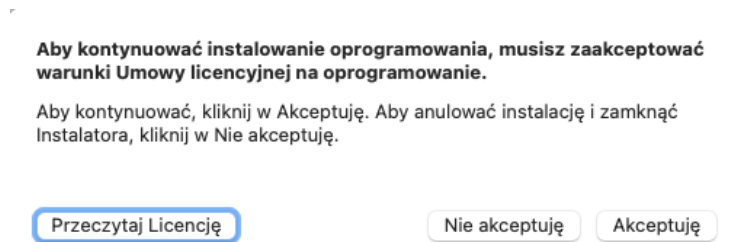
Program instalacyjny wyświetli okno umowy licencyjnej użytkownika oprogramowania. W celu kontynuowania procesu instalacji, należy zapoznać się ze wspomnianą umową i kliknąć przycisk *Dalej*.



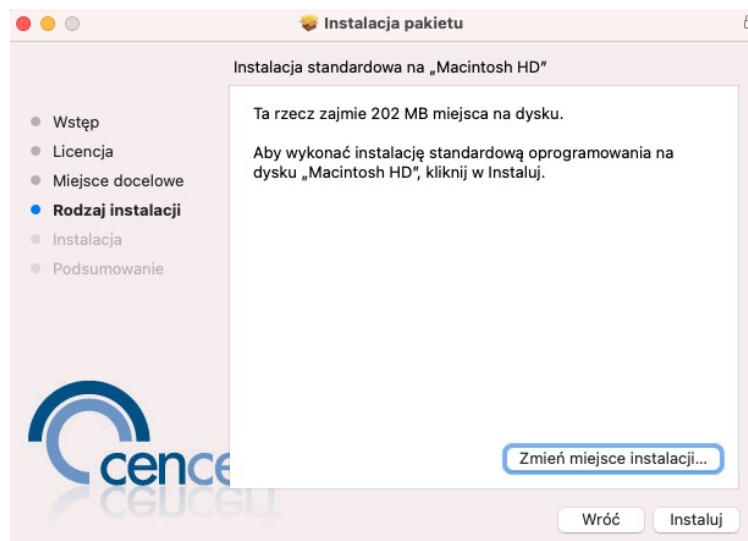
Rysunek 26 Okno z umową licencyjną



Aby kontynuować instalację należy zaakceptować wcześniej przeczytaną umowę licencyjną klikając przycisk *Akceptuję*.

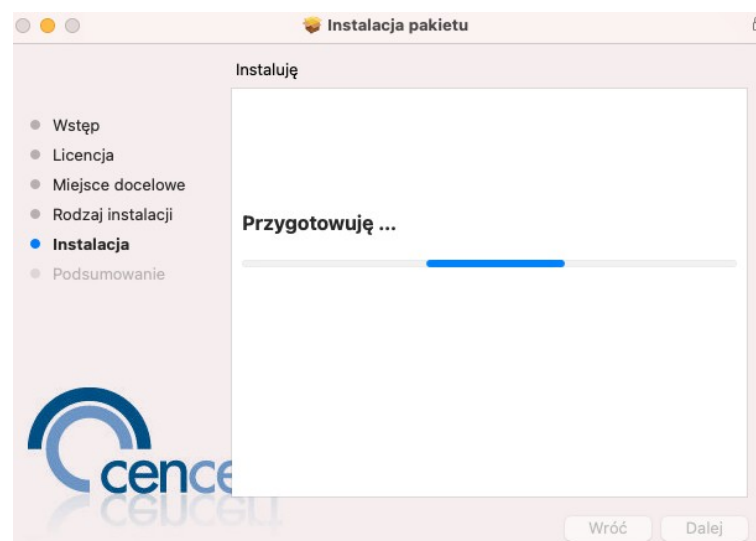


Rysunek 27 Akceptacja Umowy licencyjnej



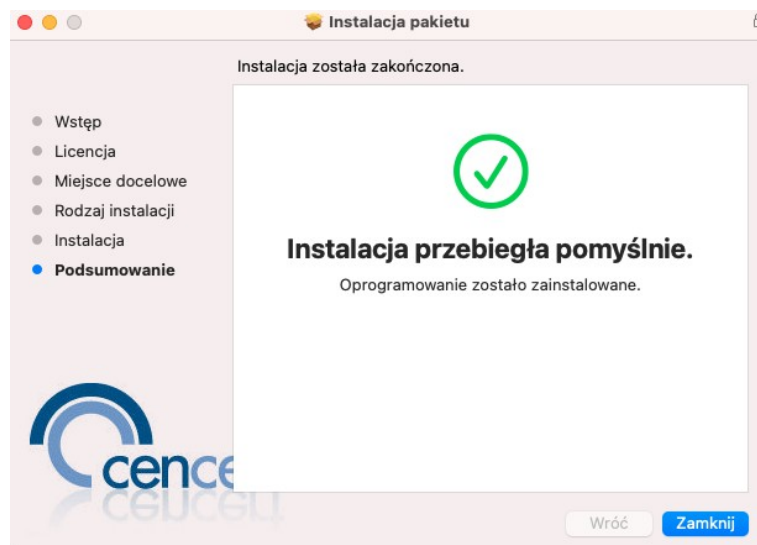
Rysunek 28 Konfiguracja katalogu instalacji

Po wciśnięciu przycisku *Instaluj* oprogramowanie jest instalowane w systemie.



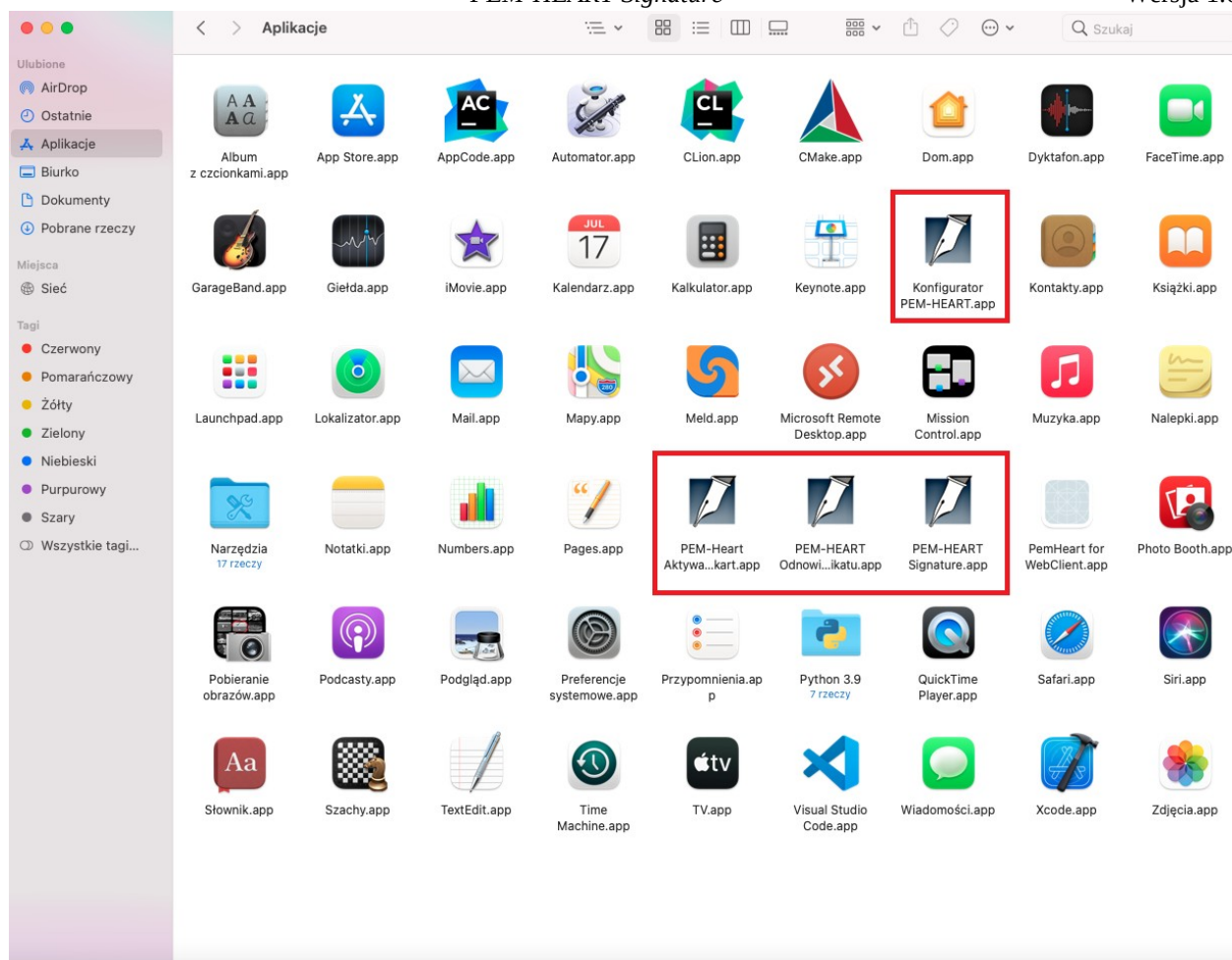
Rysunek 29 Instalacja

Zakończenie instalacji jest sygnalizowane wyświetleniem okna jak na rysunku poniżej.



Rysunek 30 Zakończenie instalacji

Po zamknięciu okna instalatora oprogramowanie *PEM-HEART Signature* jest dostępne do działania w systemie *MacOs*.



Rysunek 31 Widok zainstalowanych programów w katalogu aplikacji

## 5.1 Usuwanie oprogramowania z systemu

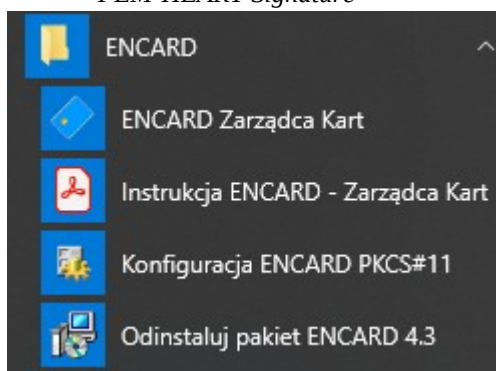
Aby usunąć oprogramowanie z systemu należy usunąć programy: Konfigurator PEM-HEART, PEM-HEART Aktywacja kart, PEM-HEART Odnowienie certyfikatu oraz PEM-HEART Signature z katalogu aplikacji.

## 6 Logi z operacji kartowych na systemie WINDOWS

Oprogramowanie umożliwia włączenie logowania dla operacji na karcie np. PODPIS pod dokumentem.

Celem włączenia dodatkowego logowania należy wywołać okno do konfiguracji biblioteki PKCS#11.

Opcja dostępna ze skrótu *Menu Start->Programy->ENCARD->Konfiguracja ENCARD PKCS#11*



Rysunek 32 Skrót do oprogramowania konfiguracji biblioteki PKCS#11 w Menu Start

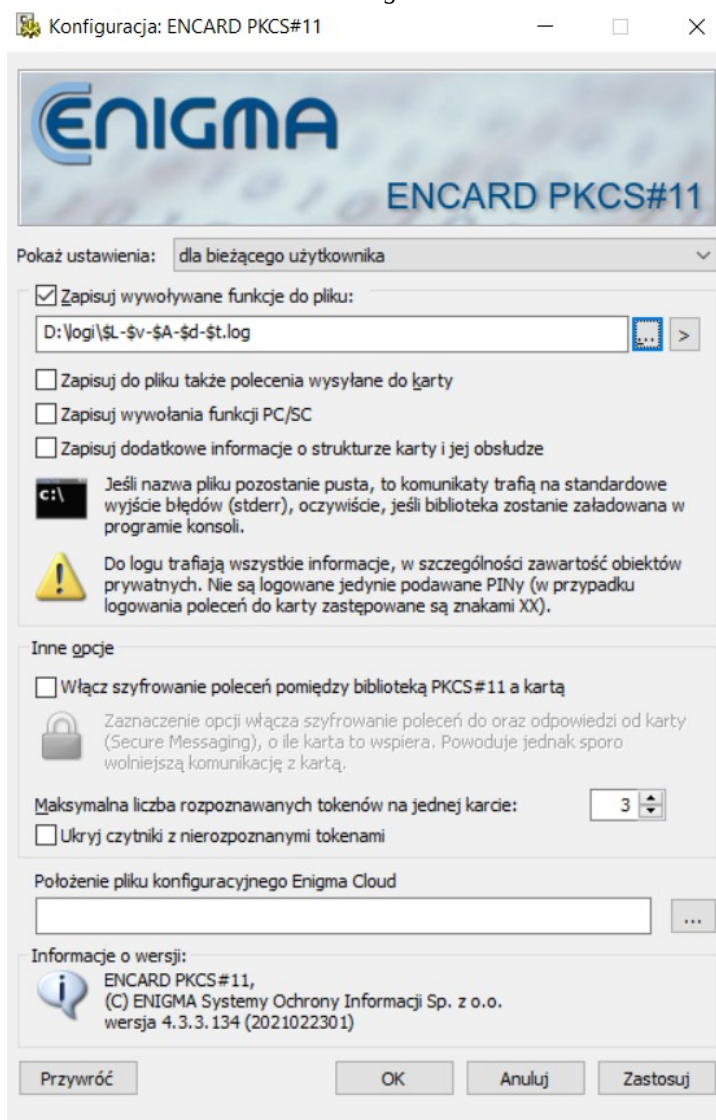
Wybranie opcji konfiguracji spowoduje wywołanie okna do konfiguracji biblioteki PKCS#11.

Zaznaczenie opcji *Zapisuj wywoływanie funkcje do pliku* (Rysunek 33) będącej jednocześnie nazwą ramki 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.

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 ładuje, 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 rozsz.).
- \$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 \$.



Rysunek 33 Konfiguracja biblioteki PKCS#11

Zaznaczenie opcji *Zapisuj do pliku także polecenia wysyłane do karty* powoduje umieszczanie w pliku logów również poleceń wysyłanych do karty.

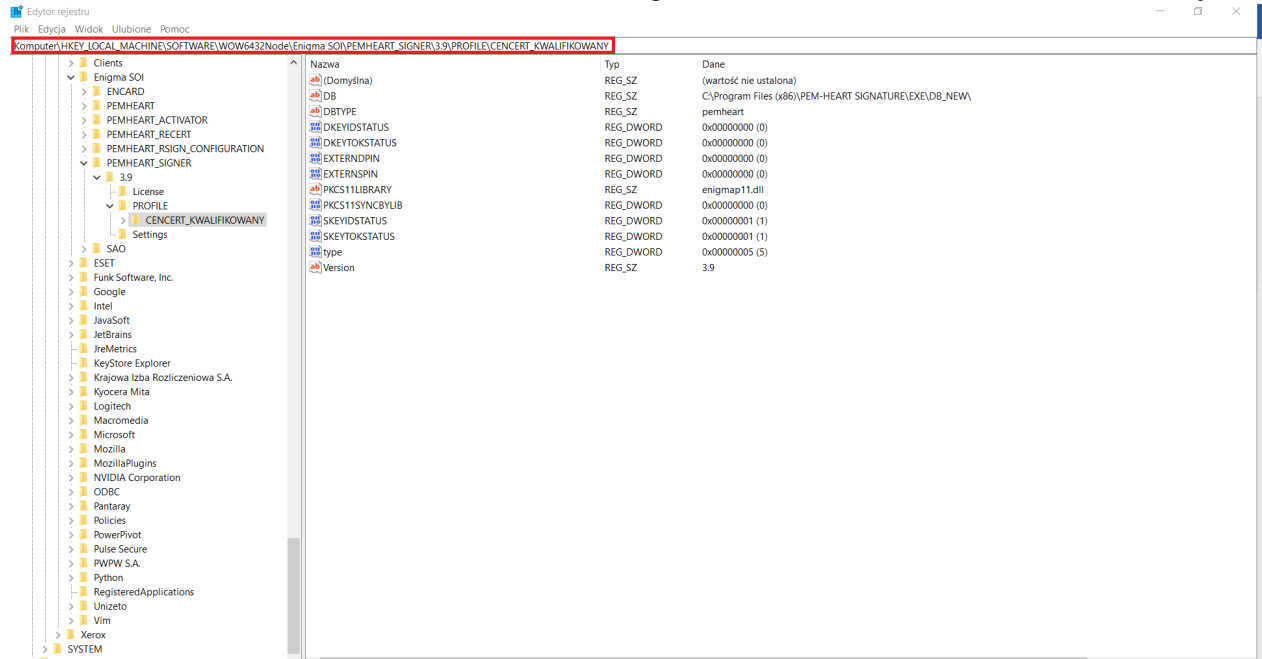
## 7 Konfiguracja Proxy z poziomu administratora w systemie Windows

Aby skonfigurować Proxy z poziomu administratora należy w Menu Start wyszukać Edytor Rejestru.

Następnie w polu zaznaczonym na Rysunku 34 wpisać:

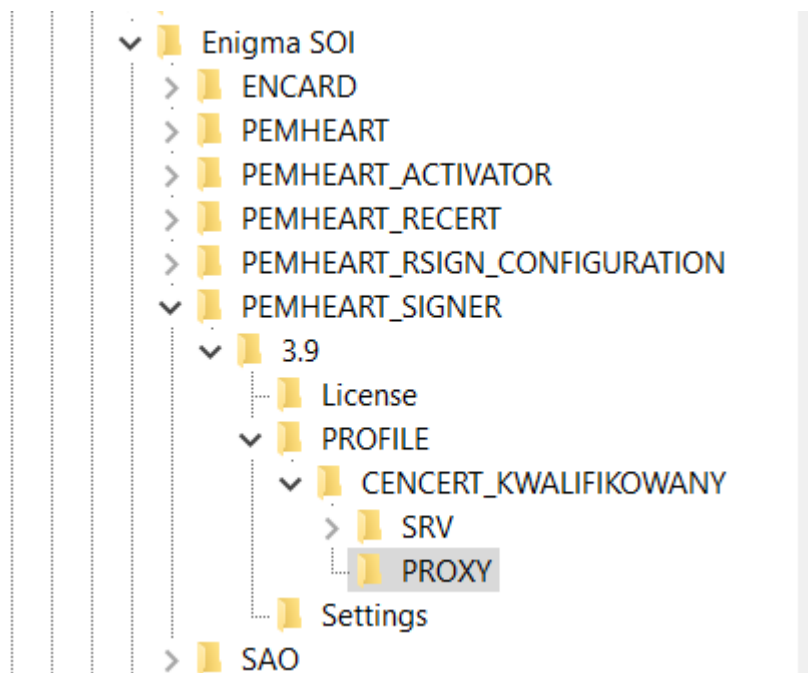
```
Komputer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Enigma SOI\
PEMHEART_SIGNER\3.9\PROFILE[NAZWA_PROFILU]
```

Domyślnym profilem przy instalacji jest CENCERT\_KWALIFIKOWANY.



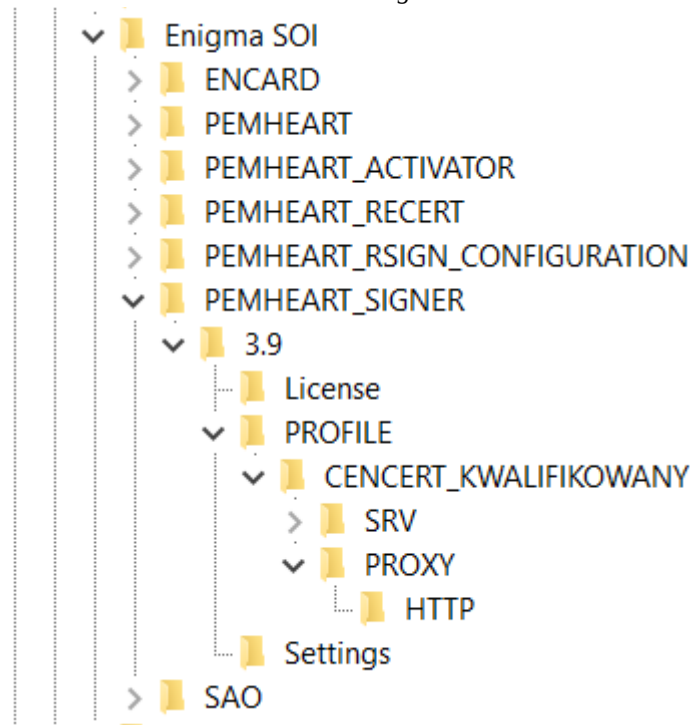
Rysunek 34 Widok Edytora Rejestru

Następnie należy dodać nowy klucz do wybranego profilu o nazwie PROXY jak na Rysunku 35.



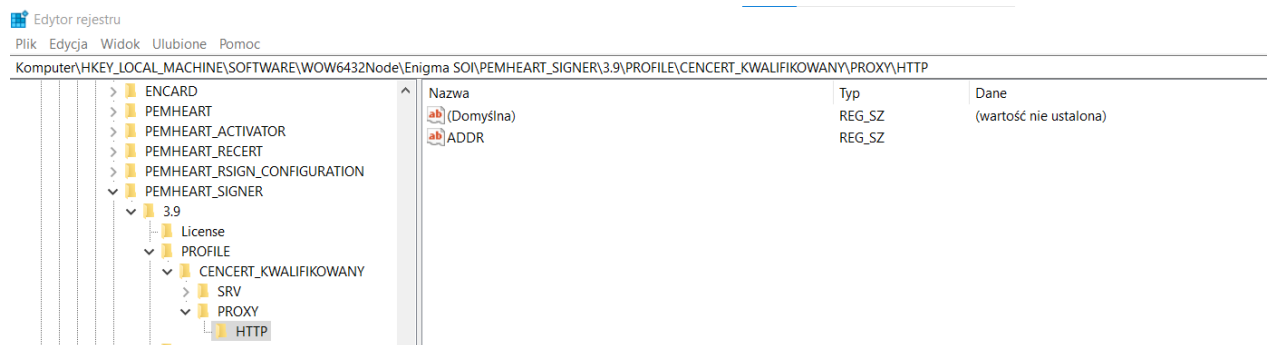
Rysunek 35 Widok rejestru po stworzeniu klucza PROXY

W kolejnym kroku we wcześniej stworzonym kluczu PROXY, należy stworzyć klucz HTTP, jak na rysunku 36.



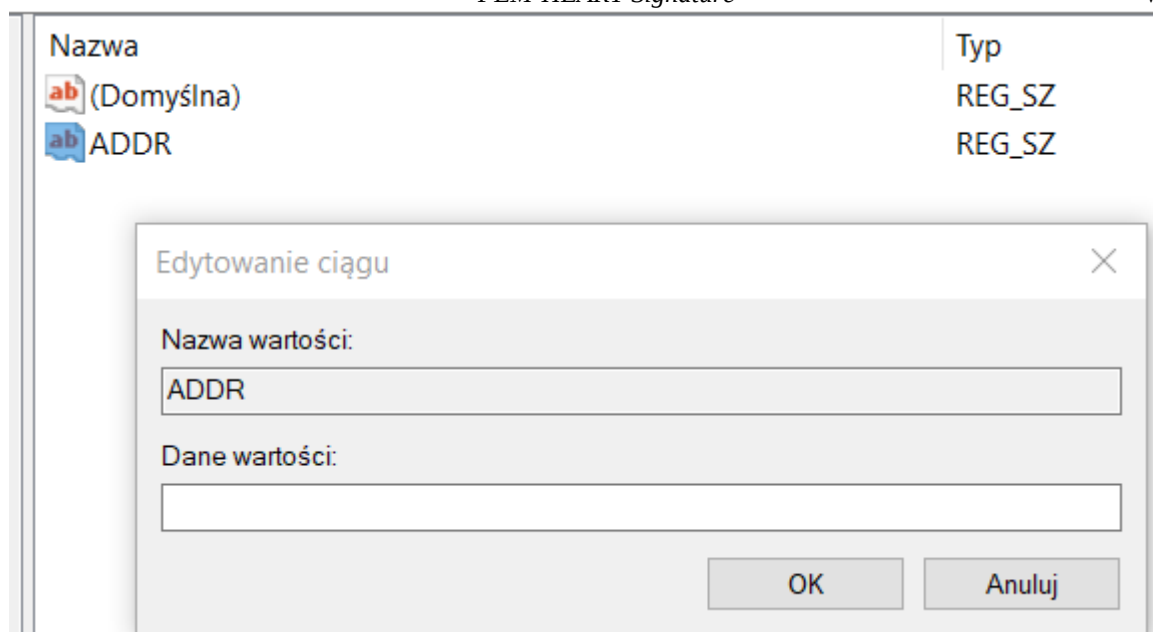
Rysunek 36 Widok rejestru po stworzeniu klucza http

Następnie otwieramy klucz HTTP i klikamy prawy->Nowy->Wartość ciągu i nadajemy ciągowi nazwę ADDR, jak na rysunku 37.



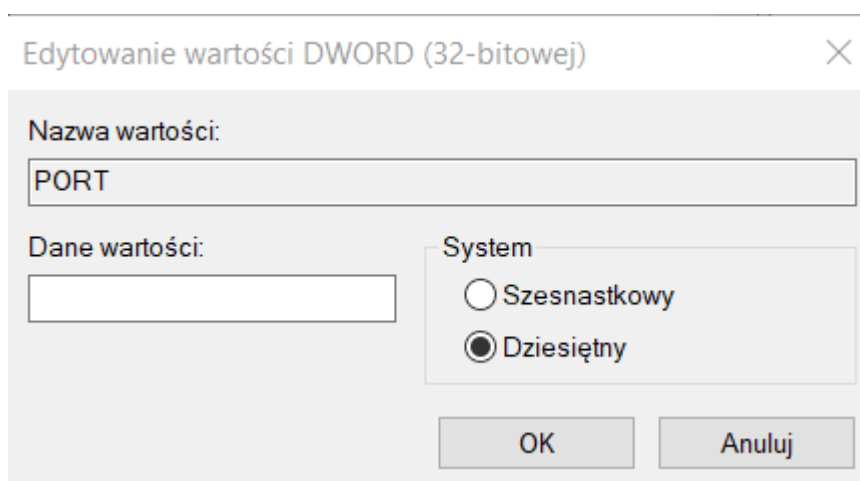
Rysunek 37 Rejestr po dodaniu ciągu ADDR do klucza HTTP

W kolejnym kroku uzupełniamy adres Proxy, najeżdżając na pole ADDR i klikając prawy przycisk myszy, a następnie *Modyfikuj*. W polu Dane wartości wpisujemy adres jak na rysunku 38.



Rysunek 38 Okno z uzupełnianiem ciągu ADDR

Analogicznie tworzymy pole z numerem portu klikając prawym przyciskiem myszy Nowy->Wartość DWORD (32-bitowa) o nazwie PORT. Następnie najeżdżamy na nią i klikamy prawym przyciskiem myszy oraz *Modyfikuj*.



Rysunek 39 Okno z uzupełnianiem ciągu PORT

Następnie należy uzupełnić Dane wartości w odpowiednim Systemie.