Instrukcja instalacji programu PEM-HEART Signature w systemie macOS

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

Enigma Systemy Ochrony Informacji Sp. z o.o.
ul. 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 ZAWARTOŚĆ PAKIETU PEM-HEART SIGNATURE DLA SYSTEMU MACOS

Oprogramowanie PEM-HEART Signature dla systemu macOS jest dostępne do instalacji z pliku o nazwie PH-X.X.X.X.dmg (gdzie X oznacza numer wersji) pobranego ze strony http://www.cencert.pl

Do uruchomienia programu PEM-HEART Signature wymagane jest posiadanie systemu macOS Monterey lub Ventura z najnowszymi dostępnymi poprawkami.

Po uruchomieniu pobranego pliku dmg w systemie macOS użytkownik ma możliwość zainstalowania oprogramowania PEM-HEART Signature oraz programu SafeNet Authentication Client. Program SafeNet Authentication Client wymagany jest do obsługi kart Thales IDPrime (białe karty).

Brak instalacji oprogramowania SafeNet Authentication Client spowoduje brak możliwości podpisu takimi kartami

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 internetową Cencert:

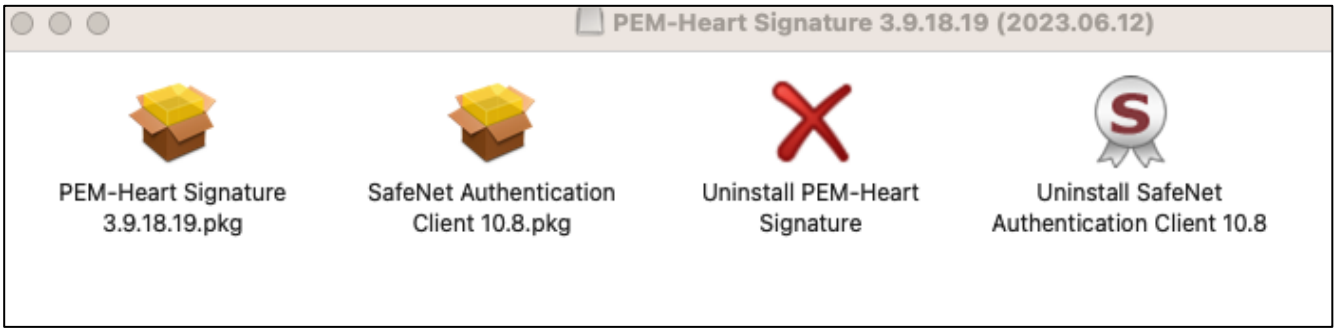
https://www.cencert.pl/do-pobrania/oprogramowanie-do-podpisu/

3.1 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.

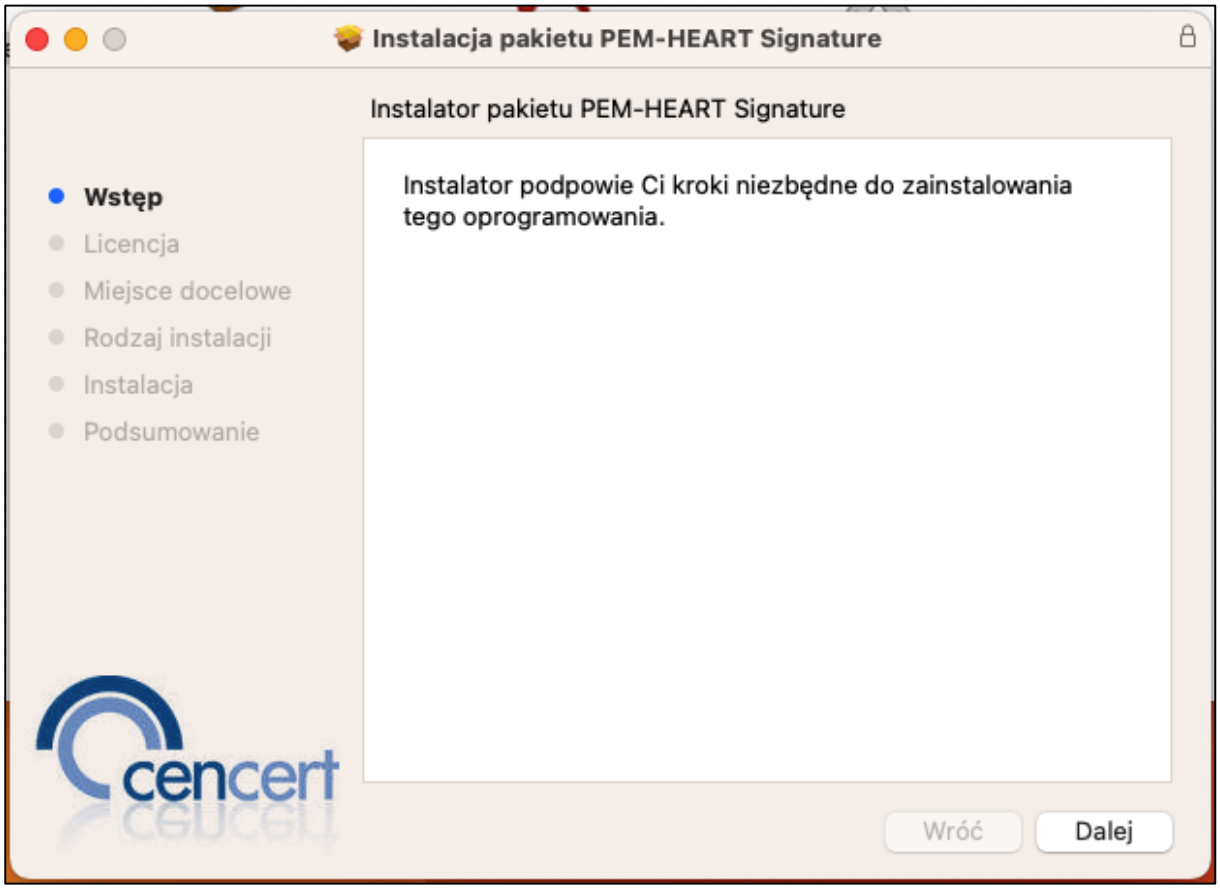


Rysunek 1 Paczka pakietu Pem-Heart dla MacOS

3.1.1 INSTALACJA POPRZEZ MENEDŻERA PLIKÓW

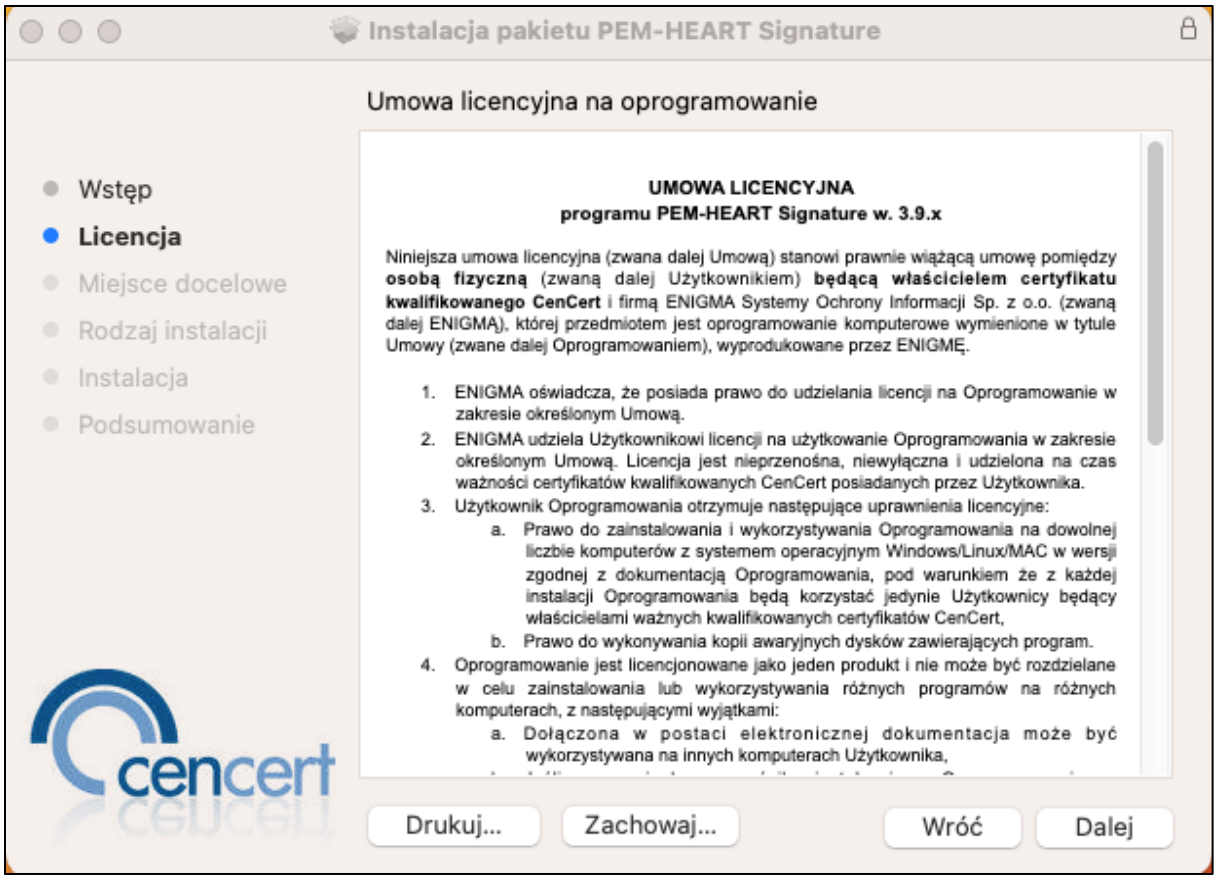
Instalację należy przeprowadzać z konta o uprawnieniach administratora. Zalecane jest, aby przed rozpoczęciem instalacji zakończyć działanie wszystkich aplikacji poza niezbędnymi dla działania systemu operacyjnego.

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



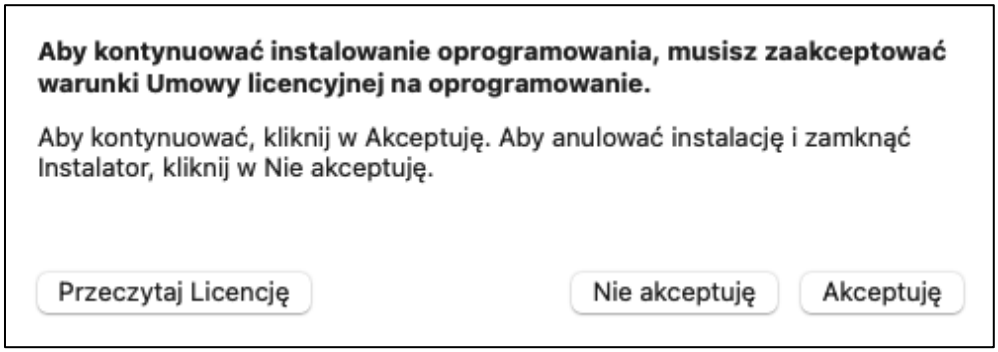
Rysunek 2 Instalator pakietu Pem-Heart - okno startowe

1. W pierwszym etapie instalacji użytkownik musi zaakceptować umowę licencyjną. Treść umowy licencyjnej może zostać wydrukowana (opcja "Drukuj...") lub zachowana na dysku komputera (opcja "Zachowaj...").



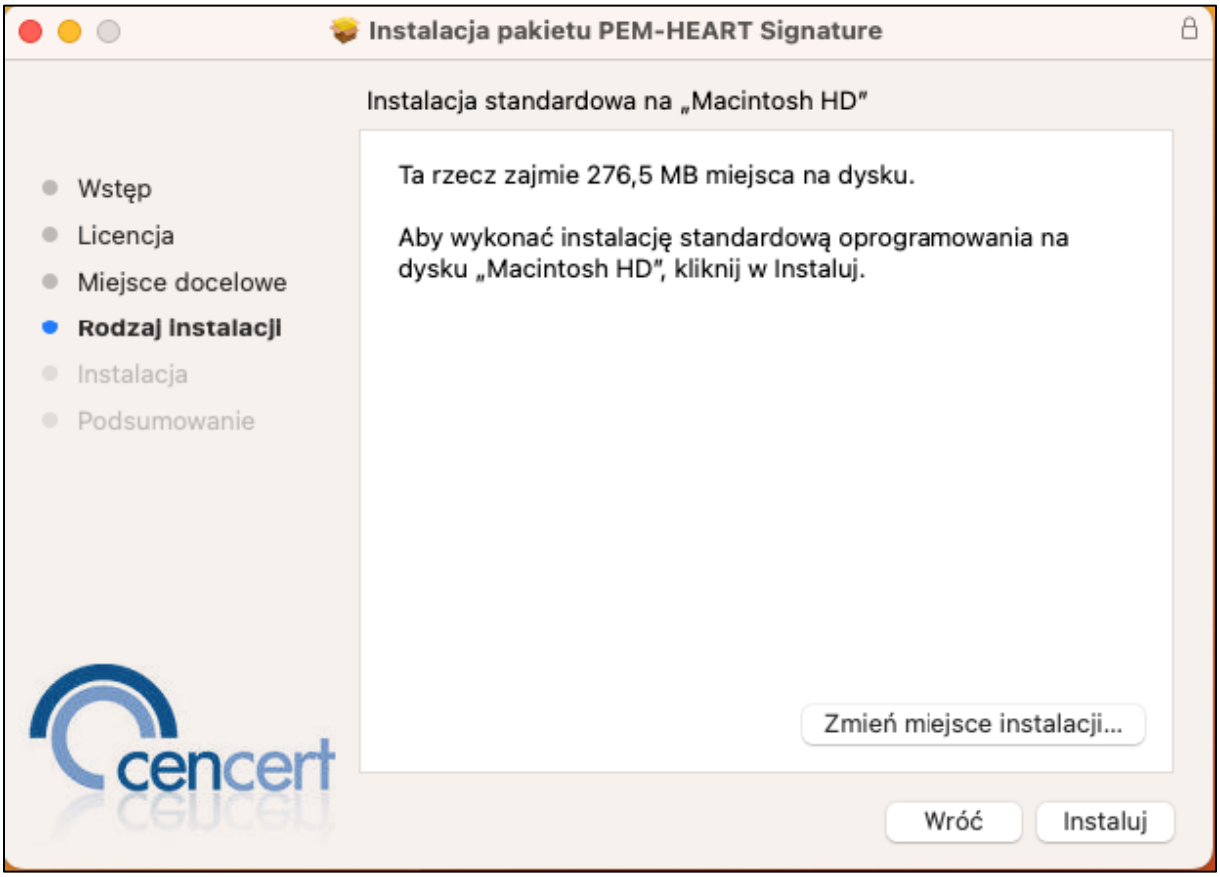
Rysunek 3 Instalator pakietu Pem-Heart - umowa licencyjna

Kliknięcie przycisku "Dalej" spowoduje wyświetlenie okna z prośbą o akceptację umowy licencyjnej.



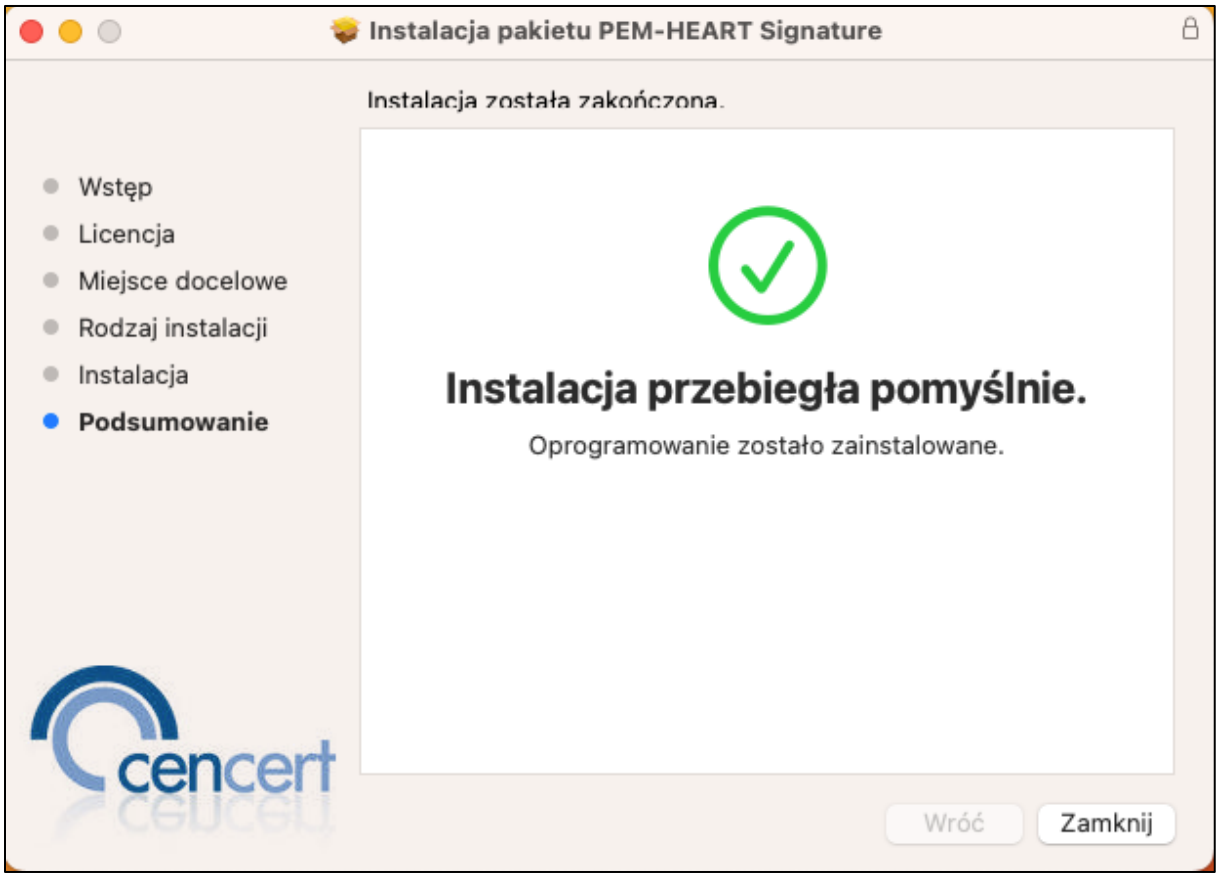
Rysunek 4 Instalator pakietu Pem-Heart - akceptacja umowy licencyjnej

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 5 Instalator pakietu Pem-Heart - informacja o instalacji

3. Instalator przystąpi do instalacji oprogramowania. Po zakończonym procesie zostanie wyświetlony ekran podsumowujący. Kliknięcie przycisku "Zamknij" zakończy działanie instalatora.



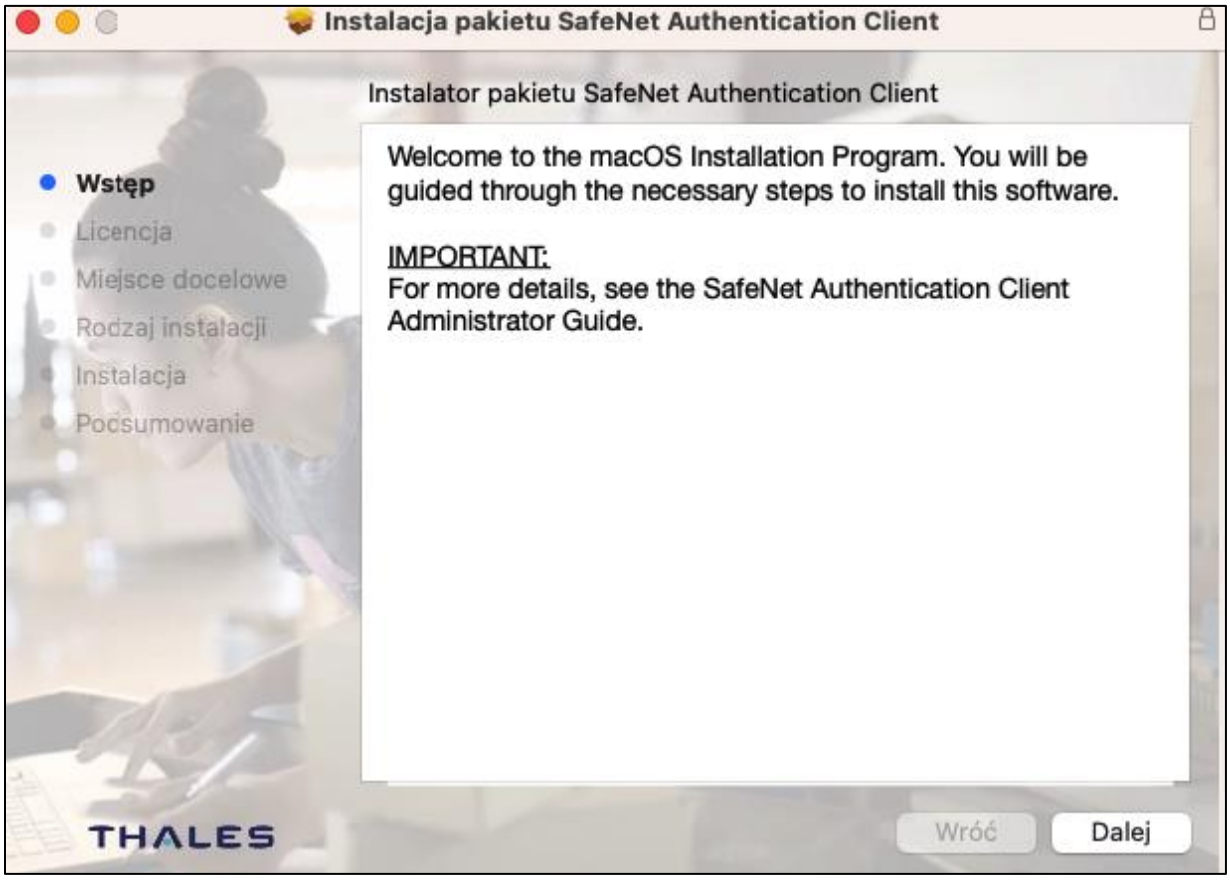
Rysunek 6 Instalator pakietu Pem-Heart - podsumowanie instalacji

3.1.2 INSTALACJA PROGRAMU SAFENET CLIENT

Po zakończonej instalacji oprogramowania PEM-HEART Signature należy zainstalować program SafeNet firmy Thales, obsługujący karty IDPrime. Zalecane jest nie pomijać instalacji oprogramowania SafeNet w celu zapobieganiu ewentualnym problemów z obsługą kart z certyfikatami Cencert.

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. Kliknięcie przycisku "Dalej" spowoduje wyświetlenie okna z umową licencyjną.

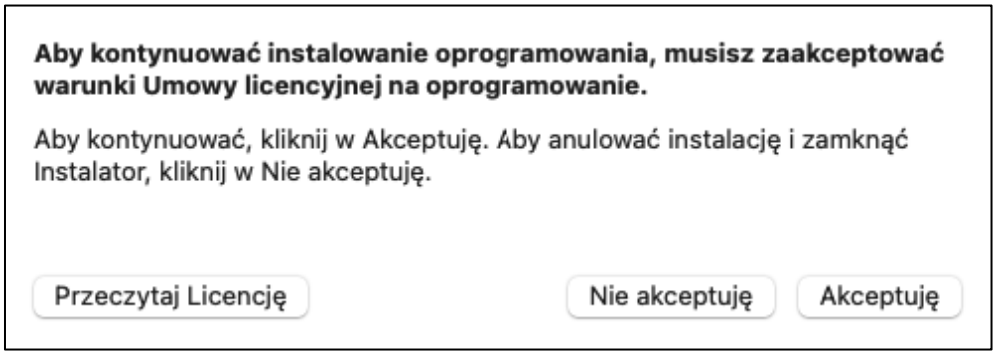


Rysunek 7 Instalator pakietu SafeNet Authentication Client - okno startowe

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

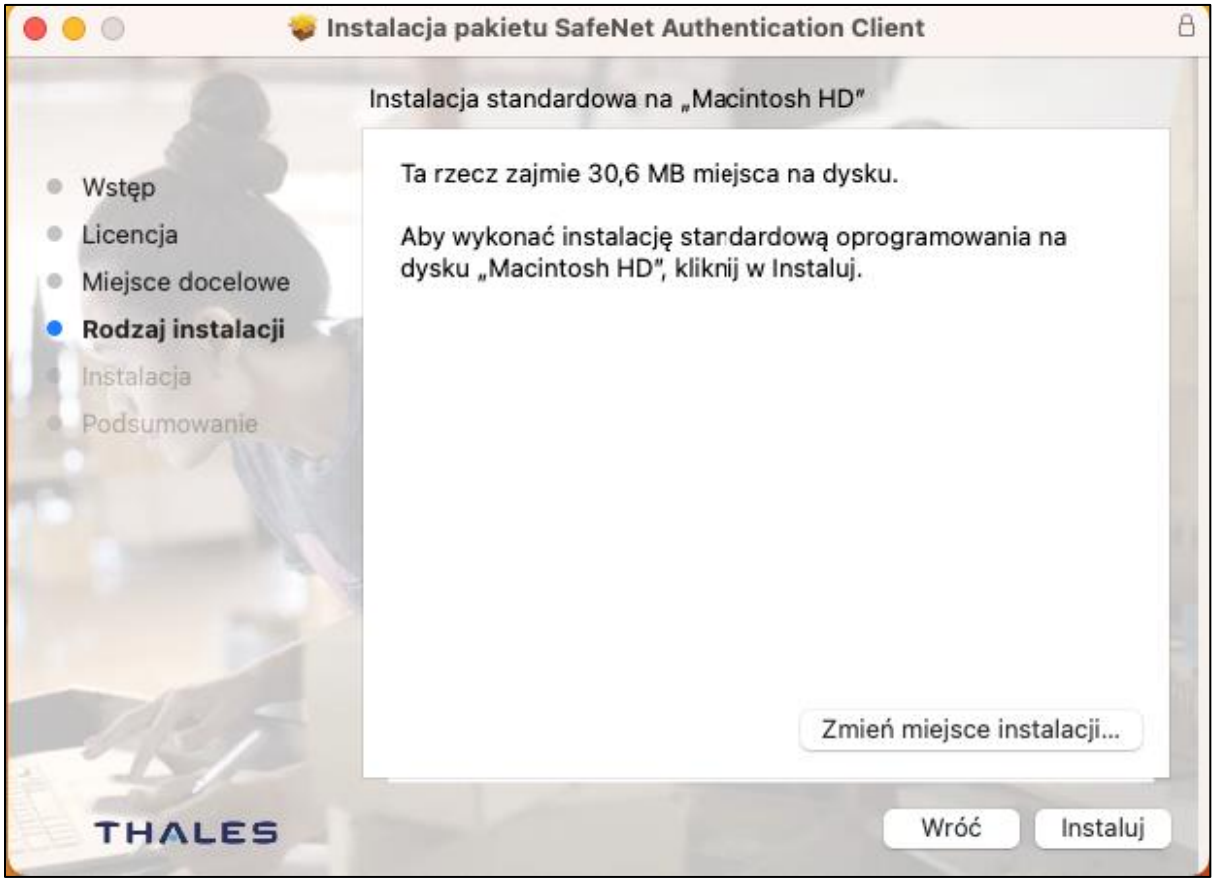
Rysunek 8 Instalator pakietu SafeNet Authentication Client – umowa licencyjna

Po kliknięciu "Dalej" użytkownikowi zostanie wyświetlone okno z prośbą o potwierdzenie akceptacji umowy licencyjnej.



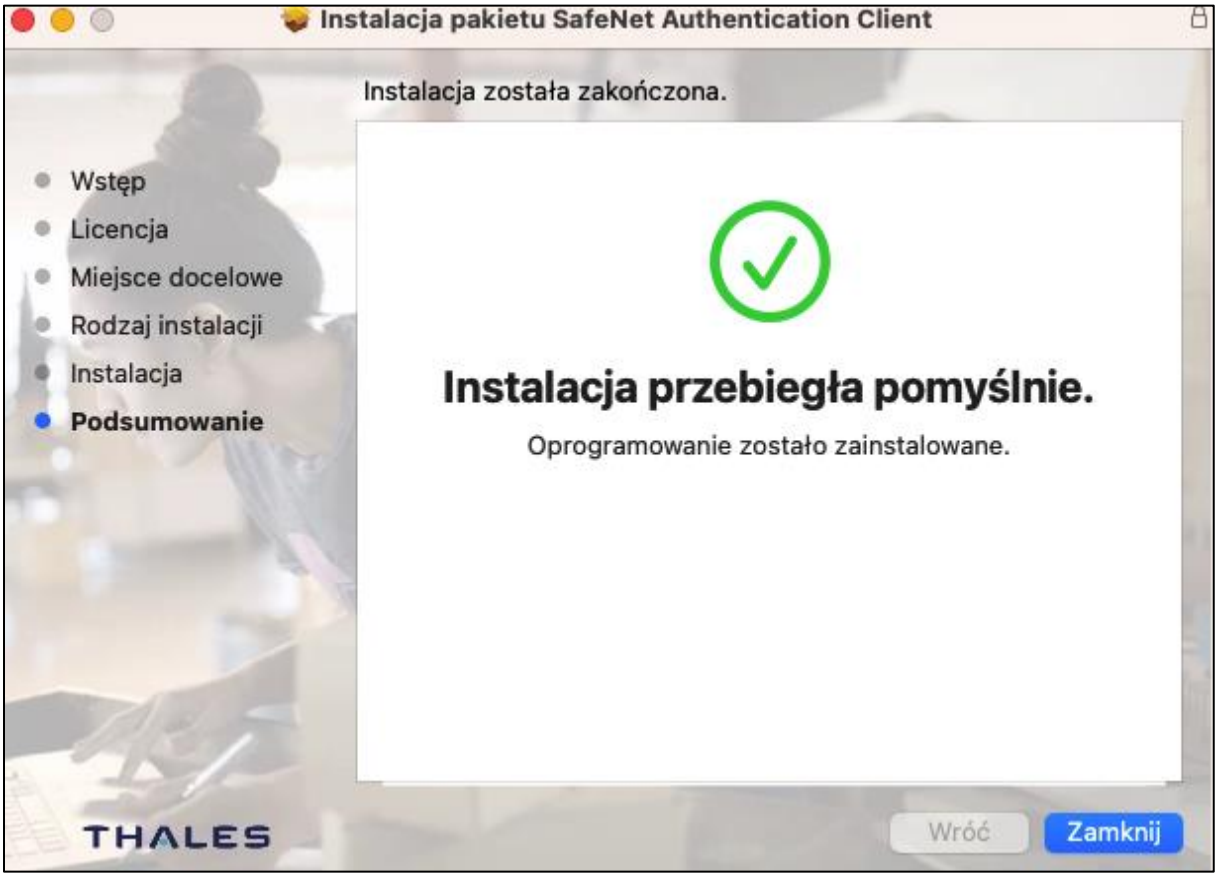
Rysunek 9 Instalator pakietu SafeNet Authentication Client - akceptacja umowy licencyjnej

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 10 Instalator pakietu SafeNet Authentication Client – informacja o instalacji

3. Instalator przystąpi do instalacji oprogramowania. Po zakończonym procesie instalacji zostanie wyświetlony ekran podsumowujący. Kliknięcie przycisku "Zamknij" zakończy działanie instalatora.



Rysunek 11 Instalator pakietu SafeNet Authentication Client - podsumowanie instalacji

Po włożeniu do czytnika nowej (jeszcze nie aktywowanej) karty Thales, użytkownik zostanie poinformowany przez system MacOS o konieczności zmiany PINu do karty. Nie należy tego robić - brak znajomości PINu transportowego, próba wykonania operacji zmiany PINu ze “zgadywaniem” jego poprzedniej wartości zakończy się zablokowaniem karty.

Jeżeli użytkownik zakupił certyfikat rSign, to w tym momencie należy uruchomić program PEM-HEART Konfiguracja rSign w celu aktywacji certyfikatu. Procedura aktywacji certyfikatu rSign zapomocą programu PEM-HEART Konfiguracja rSign została opisana w dokumencie „Dokumentacja użytkownika PEM-HEART Signature wraz z opisem aplikacji mobilnej rSign” dostępnym na stronie http://www.cencert.pl

4 SPIS RYSUNKÓW