SPIS TREŚCI

AKTYWACJA KARTY

Po podpisaniu dokumentów (Zamówienia-Wniosku o wystawienie certyfikatu do podpisu kwalifikowanego, Protokołu przekazania-odbioru oraz Informacji dla osób...) inspektor rejestracji potwierdzi tę czynność w systemie CenCert. Wówczas na wskazany we Wniosku adres mailowy otrzymają Państwo przesyłkę, która będzie zawierała:

- **informacje dotyczące dalszego postępowania**
- **link do pobrania oprogramowania**
- **załącznik o nazwie kod_aktywacyjny.cac.**

Należy:

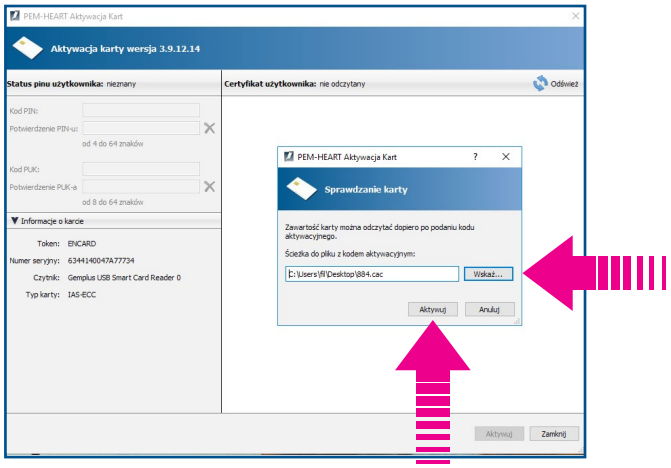
1. Załącznik kod_aktywacyjny.cac zapisać na pulpicie.

2. Uruchomić link i ze strony www.cencert.pl pobrać oprogramowania właściwe dla systemu operacyjnego swego komputera (Windows pozycja 1., MacOs pozycja 3. - oba pliki, Unix pozycja 4.).

3. Zainstalować pobrane oprogramowanie. Proszę pamiętać o przechodzeniu między kolejnymi oknami za pomocą klawiszy DALEJ lub ZAKOŃCZ. W wypadku MacOs proszę pamiętać o pobraniu obu plików z pozycji 3. i w takiej kolejności je instalować. Ponadto w wypadku MacOs konieczne jest posiadanie najnowszego oprogramowania systemowego (obecnie jest to wersja Catalina).

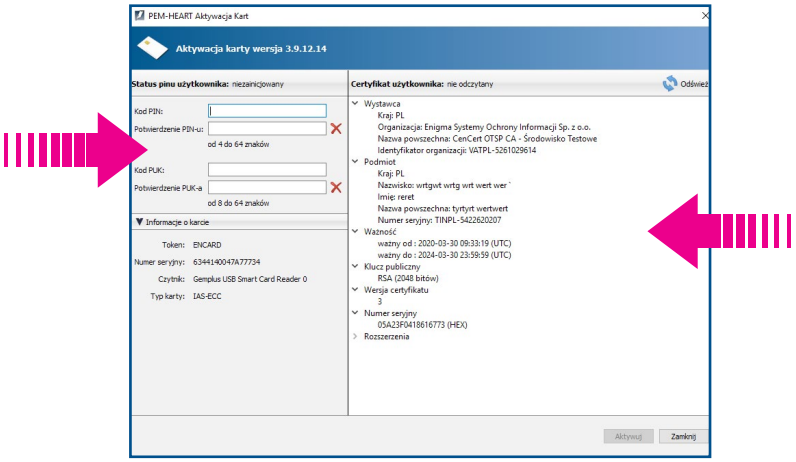
4. Po instalacji i ponownym uruchomieniu komputera (niezbędne tylko w Windows) należy włożyć do portu USB komputera otrzymany czytnik z kartą i poczekać na zapalenie się diody ciągłym światłem.

5. Należy dwukrotnym kliknięciem uruchomić wcześniej zapisany na pulpicie załącznik kod_aktywacyjny.cac. Otworzy się okno wskazujące na umiejscowienie zapisanego pliku kod_aktywacyjny.cac. Jeżeli ścieżka dostępu nie zostanie wyświetlona, należy wskazać, gdzie plik został zapisany i następnie nacisnąć przycisk AKTYWUJ [ryc. 1].



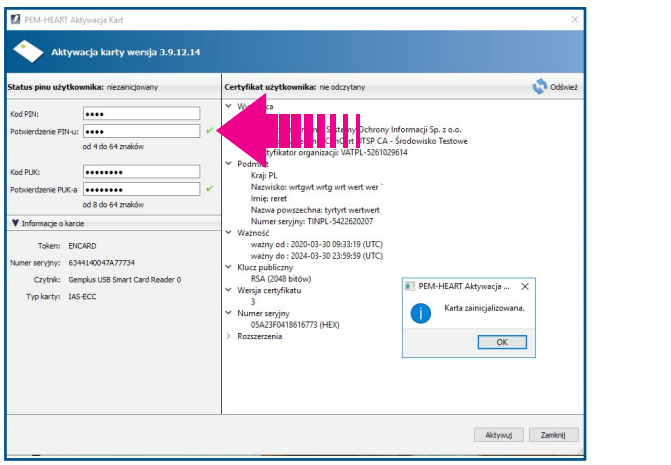
ryc. 1 - Aktywacja karty - okno otwarcia

6. Na ekranie ukaże się okno, które po prawej stronie wyświetli dane certyfikatu (proszę jeszcze raz upewnić się co do poprawności danych). Po lewej stronie pojawi się miejsce na wpisanie haseł PIN (dwukrotnie) i PUK (dwukrotnie) [ryc. 2].



ryc. 2 - Aktywacja karty - wpisanie PIN i PUK

7. Kiedy znikną czerwone znaki „x" i w ich miejsce pojawią się zielone znaki akceptacji [ryc. 3], oznacza to, że oba hasła (PIN i PUK) spełniają formalne wymogi dotyczące długości (PIN od 4 znaków, PUK od 8 znaków). Dobór znaków jest dowolny, hasła mogą zawierać: litery, cyfry i znaki specjalne.



ryc. 3 - Aktywacja karty - poprawny PIN i PUK

8. Proszę mieć świadomość, że oba nadane w tym momencie hasła PIN i PUK są jedynymi hasłami umożliwiającymi wykorzystanie certyfikatu i złożenie podpisu. Warto oba hasła zapisać w bezpiecznym miejscu.

9. Jeśli w trakcie użytkowania zdarzy się wpisać trzykrotnie kolejno błędnie PIN, karta zostanie zablokowana i do odblokowania konieczne będzie posłużenie się hasłem PUK.

10. Sposób odblokowania za pomocą hasła PUK został omówiony w rozdziale „Odblokowanie karty wcześniej zablokowanej przez trzykrotne błędne wpisanie hasła PIN", a zmiana hasła w rozdziale „Zmiana hasła PIN".

ODBLOKOWANIE KARTY WCZEŚNIEJ ZABLOKOWANEJ PRZEZ TRZYKROTNE BŁĘDNE WPISANIE HASŁA PIN

Jeśli PIN zostanie wpisany trzykrotnie kolejno błędnie, karta z certyfikatem do podpisu zostanie zablokowania. Do jej odblokowania należy użyć hasła PUK, które zostało nadane przez Państwa samodzielnie w trakcie aktywacji.

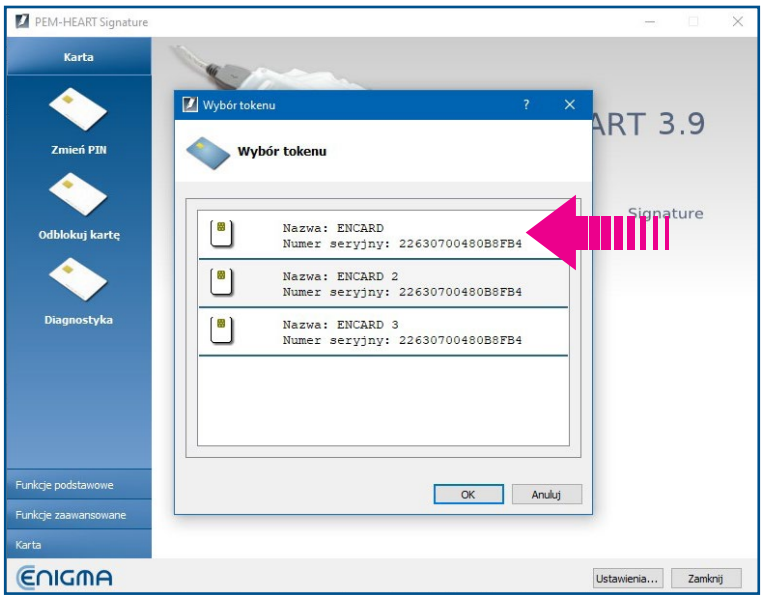
Wówczas należy:

1. Włożyć czytnik z kartą do portu USB, na którym zainstalowane jest oprogramowanie pobrane ze strony www.cencert.pl zgodnie z linkiem otrzymanym w mailu.
2. Po zapaleniu się diody ciągłym światłem uruchomić program PEM-Heart Signature.
3. W lewym dolnym rogu uruchomionego okna znajduje się zakładka KARTA [ryc. 4], po jej wybraniu należy uruchomić polecenie ODBLOKUJ KARTĘ [ryc. 5].

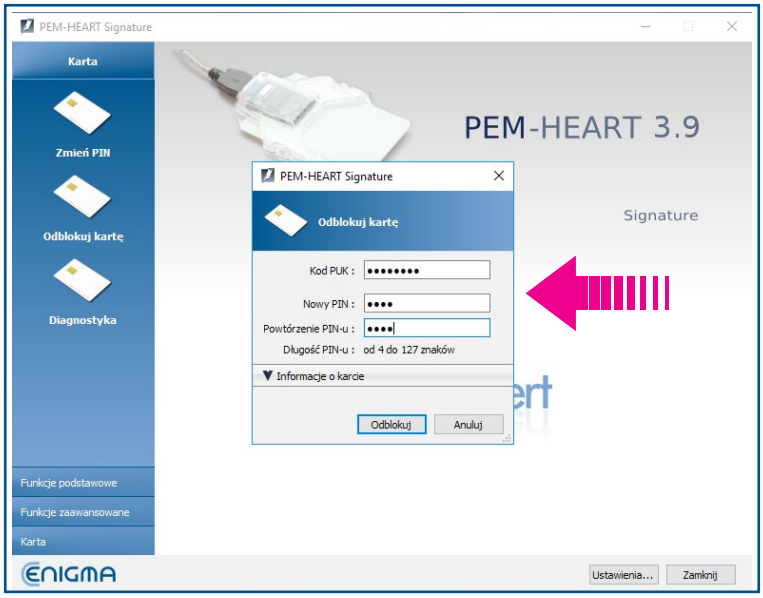
ryc. 4 - Zakładka KARTA

ryc. 5 - Odblokuj kartę

4. W oknie WYBÓR TOKENU należy wskazać pozycję pierwszą [ryc. 6] i w otwartym oknie zgodnie z wyświetlonym poleceniem wpisać PUK oraz dwukrotnie nowy PIN [ryc. 7].



ryc. 6 - Wybór tokenu



ryc. 7 - Wprowadzanie PUK i PIN

5. Pojawi się komunikat o odblokowaniu karty. Proszę pamiętać o zamykaniu kolejnych okien za pomocą przeznaczonych do tego przycisków (np. ZAPISZ, ZAMKNIJ). Korzystanie ze znaku „**X**" na górnej ramce okna może przerwać proces instalacji lub zapisywania wprowadzonych zmian.

ZMIANA HASŁA PIN

Hasła PIN i PUK umożliwiające skorzystanie z podpisu elektronicznego nadawane są przez użytkownika w trakcie aktywacji karty. Proces aktywacji opisany jest w rozdziale „Aktywacja karty”. **Program do podpisu elektronicznego PEM-Heart Signature nie wymaga cyklicznej zmiany hasła i stosowanie tej możliwości należy ograniczyć do sytuacji, kiedy obawiają się Państwo, że PIN poznały inne osoby. Ewentualnie jeśli czują się Państwo zagrożeni uznając, że hasło PIN jest zbyt proste lub zbyt skomplikowane i generuje niepotrzebnie błędy podczas wpisywania długiego ciągu znaków.**

Wówczas należy:

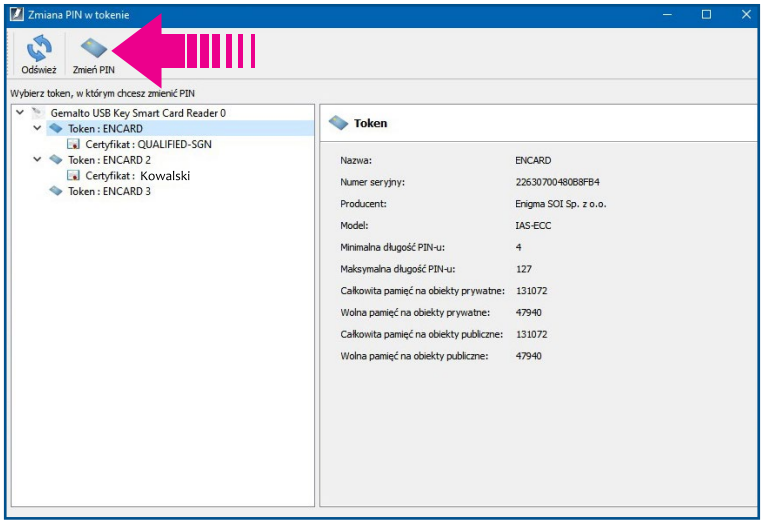
1. Włożyć czytnik z kartą do portu USB, na którym zainstalowane jest oprogramowanie pobrane ze strony www.cencert.pl zgodnie z linkiem otrzymanym w mailu.

2. Po zapaleniu się diody ciągłym światłem uruchomić program PEM-Heart Signature.

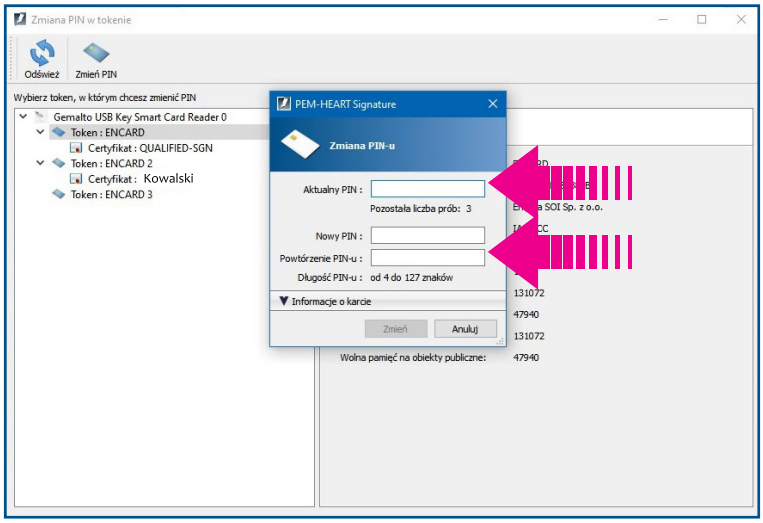
3. W lewym dolnym rogu uruchomionego okna znajduje się zakładka KARTA, po jej wybraniu należy uruchomić polecenie ZMIEŃ PIN [ryc. 8].

ryc. 8 - Zmień PIN

4. W oknie ZMIANA PINU W TOKENIE należy uruchomić przycisk ZMIEŃ PIN [ryc. 9] i po podaniu aktualnego hasła PIN wpisać dwukrotnie nowe hasło PIN [ryc. 10].



ryc. 9 - Przycisk ZMIEŃ PIN



ryc. 10 - Zmiana PIN

5. Pojawi się komunikat o zmianie hasła PIN. Proszę pamiętać o zamykaniu kolejnych okien za pomocą przeznaczonych do tego przycisków (np. ZAPISZ, ZAMKNIJ). Korzystanie ze znaku „**X**" na górnej ramce okna może przerwać proces instalacji lub zapisywania wprowadzonych zmian.

SPRAWDZENIE TERMINU WAŻNOŚCI CERTYFIKATU

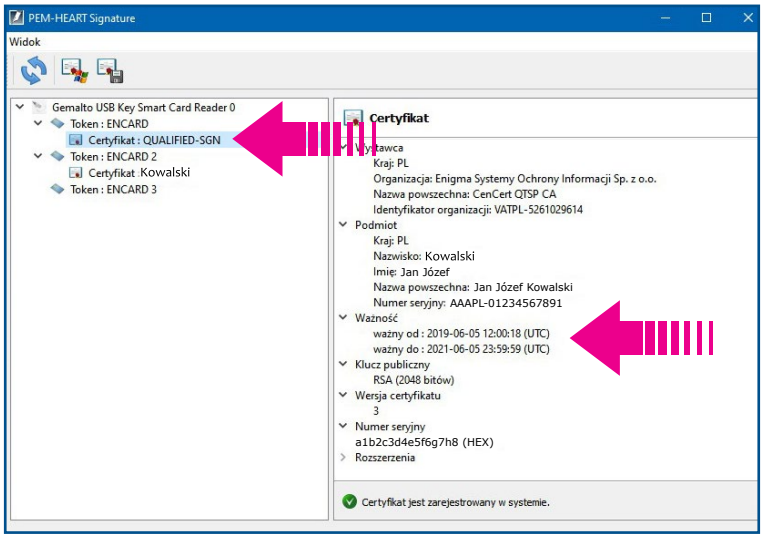
Certyfikaty do kwalifikowanego podpisu elektronicznego wydawane są na okres 1 roku lub 2, 3, 4, 5 lat. Po upływie terminu ważności certyfikatu nie ma możliwości podpisania dokumentu, ani też dokonania odnowienia certyfikatu w trybie on-line.

Aby sprawdzić termin ważności należy:

1. Włożyć czytnik z kartą do portu USB, na którym zainstalowane jest oprogramowanie pobrane ze strony cencert.pl zgodnie z linkiem otrzymanym w mailu.
2. Po zapaleniu się diody ciągłym światłem uruchomić program PEM-Heart Signature.
3. W lewym dolnym rogu uruchomionego okna znajduje się zakładka KARTA, po jej wybraniu należy uruchomić polecenie DIAGNOSTYKA [ryc. 11].

ryc. 11 - Diagnostyka

4. W oknie PEM-Heart Signature - WIDOK po lewej stronie należy wskazać pozycję CERTYFIKAT [ryc. 12].



ryc. 12 - Ważność certyfikatu

5. W oknie po prawej stronie wyświetlą się wówczas dane certyfikatu. Wśród nich w rubryce WAŻNOŚĆ sprawdzany jest termin ważności.

URUCHOMIENIE PODPISU NA NOWYM KOMPUTERZE

Jeżeli w trakcie ważności certyfikatu zmienią Państwo komputer lub dokonają reinstalacji systemu operacyjnego, należy ponownie zarejestrować certyfikat do składania kwalifikowanego podpisu elektronicznego. Jest to czynność jednorazowa, nie ma wpływu na nadane wcześniej hasła PIN i PUK.

Należy:

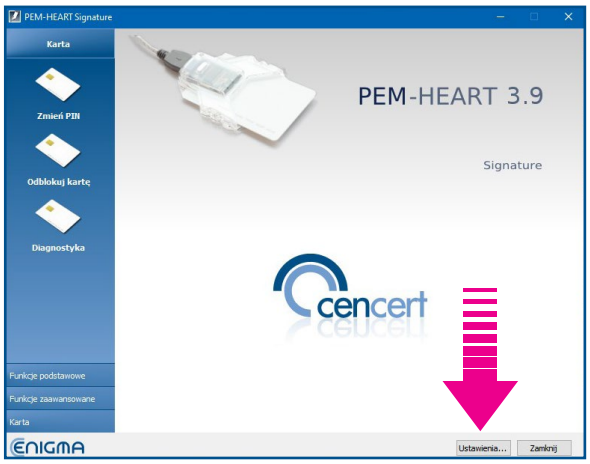
1. Ze strony www.cencert.pl/oprogramowanie PEMHEART pobrać oprogramowania właściwe dla systemu operacyjnego komputera (Windows pozycja 1., MacOs pozycja 3. - oba pliki, Unix pozycja 4.).

2. Zainstalować pobrane oprogramowanie. Proszę pamiętać o przechodzeniu między kolejnymi oknami za pomocą klawiszy DALEJ lub ZAKOŃCZ. W wypadku MacOs proszę pamiętać o pobraniu obu plików z pozycji 3. i w takiej kolejności je instalować. Ponadto w wypadku MacOs konieczne jest posiadanie najnowszego oprogramowania systemowego (obecnie jest to wersja Catalina).

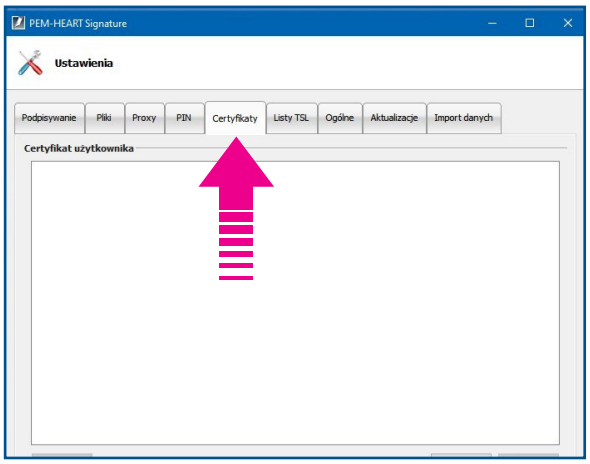
3. Po instalacji i ponownym uruchomieniu komputera (niezbędne tylko w Windows) należy włożyć do portu USB otrzymany czytnik z kartą i poczekać na zapalenie się diody ciągłym światłem.

4. Następnie uruchomić program PEM-Heart Signature.

5. W prawym dolnym rogu należy nacisnąć przycisk USTAWIENIA [ryc. 13], a następnie z listy zakładek wybrać tę oznaczoną CERTYFIKATY [ryc. 14].

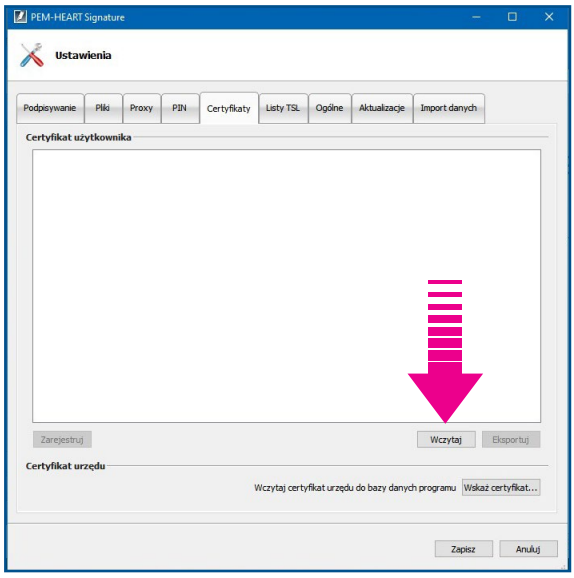


ryc. 13 - Wybór opcji Ustawienia



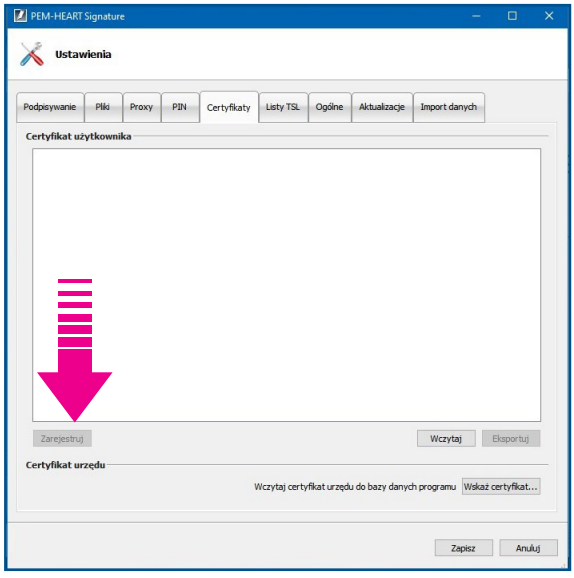
ryc. 14 - Wybór opcji Certyfikaty

6. W otwartym nowym oknie należy nacisnąć przycisk WCZYTAJ [ryc. 15]. Program zażąda podania hasła PIN. Wyświetli się certyfikat: dane wystawcy, właściciela, termin ważności oraz dane techniczne.



ryc. 15 - Wybór opcji WCZYTAJ

7. Następnie nacisnąć przycisk ZAREJESTRUJ [ryc. 16]. Komputer ponownie będzie wymagał podania hasła PIN. Po chwili pojawi się komunikat: CERTYFIKAT ZOSTAŁ ZAREJESTROWANY W SYSTEMIE.



ryc. 16 - Wybór opcji ZAREJESTRUJ

8. Wciśnięcie przycisku ZAPISZ kończy proces.

PODPISYWANIE PLIKÓW ZA POMOCĄ PODPISU ELEKTRONICZNEGO LUB PIECZĘCI

Aby skorzystać posiadanego certyfikatu i złożyć podpis elektroniczny, konieczne jest:

- **wcześniejsze zainstalowanie właściwego oprogramowania (instrukcja znajdzuje się w rozdziale** „Aktywacja karty”**)**
- **aktywacja posiadanej karty (instrukcja znajdzuje się w rozdziale** „Aktywacja karty”**).**

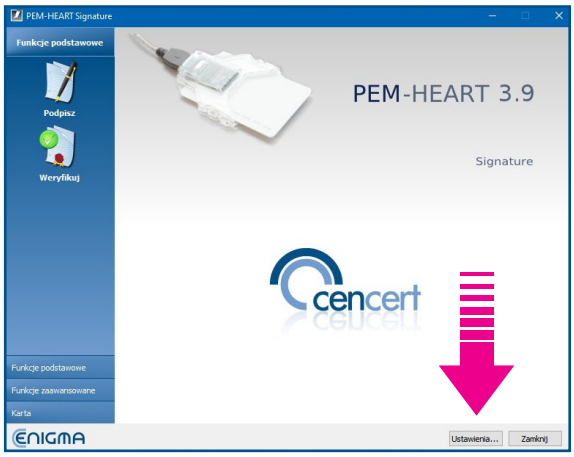
Jeśli powyższe czynności zostały wykonane wcześniej, należy:

1. Włożyć czytnik z kartą do portu USB komputera.
2. Uruchomić program PEM-Heart Signature (ikona programu – jeśli nie zmieniono tego w trakcie instalacji – jest na pulpicie komputera).
3. Widok otwartego programu [ryc. 17].

ryc. 17 – Widok otwartego programu

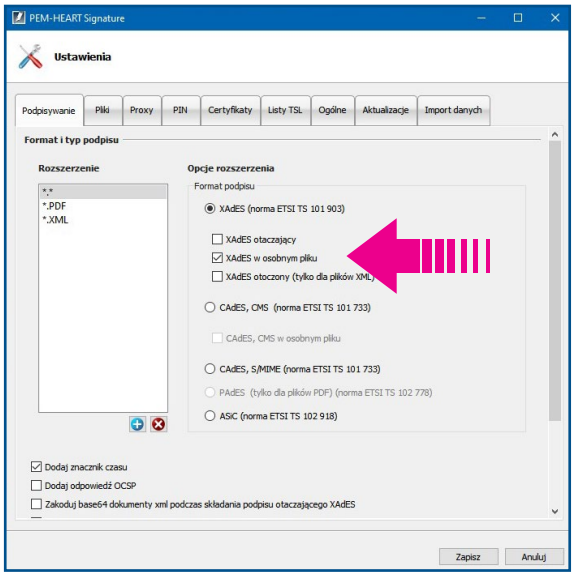
4. Jeśli użytkownik nie chce skorzystać z szerszej informacji o formatach składanych podpisów, proszę przejść bezpośrednio do punktu 10.

5. Podczas pierwszego uruchomienia warto skorzystać z opcji USTAWIENIA [ryc. 18]. Wyjaśnia ona różnice w formacie stosowanych podpisów.



ryc. 18 - Opcje USTAWIENIA

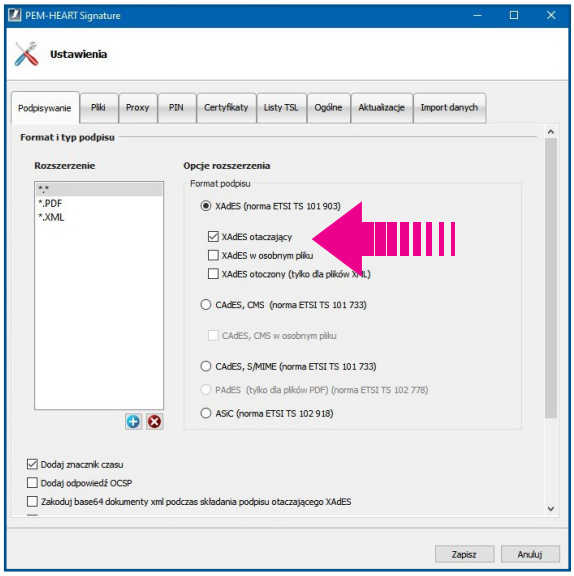
Wszystkie pliki elektroniczne bez względu na ich format (rozszerzenie) można zapisać za pomocą protokołu XAdES. Od decyzji użytkownika zależy (a także od wymagań odbiorcy podpisanego pliku/dokumentu) ostateczna forma podpisu. Jeśli pozostawione zostanie bieżące ustawienie [ryc. 19],



ryc. 19 - Podpis w osobnym pliku

to w trakcie podpisywania pliku powstanie dodatkowy plik z rozszerzeniem xades (i charakterystyczną ikoną), zawierający zaszyfrowane dane kontrolne i podpis. Wówczas odbiorcy przekazuje się dwa pliki: podpisywany oraz zawierający podpis.

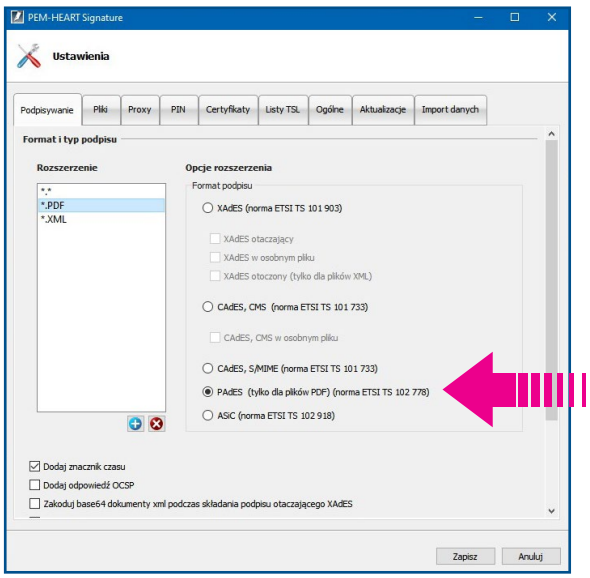
Jeśli użytkownik zdecyduje się na zmianę i wybierze opcję podpisu otaczającego [ryc. 20],



ryc. 20 – Podpis otaczający

to wówczas efektem podpisania jest utworzenie pliku z rozszerzeniem xades (i charakterystyczną ikoną), zawierającego zaszyfrowaną treść oraz podpis. Odbiorcy należy przekazać tylko jeden, właśnie utworzony plik.

6. Korzystając z opcji USTAWIENIA warto jeszcze wyjaśnić zasadę podpisywania pliku w popularnym formacie PDF. Może on być podpisany za pomocą protokołu XAdES, jednak ustawienie standardowe sugeruje użycie protokołu PAdES [ryc. 21].

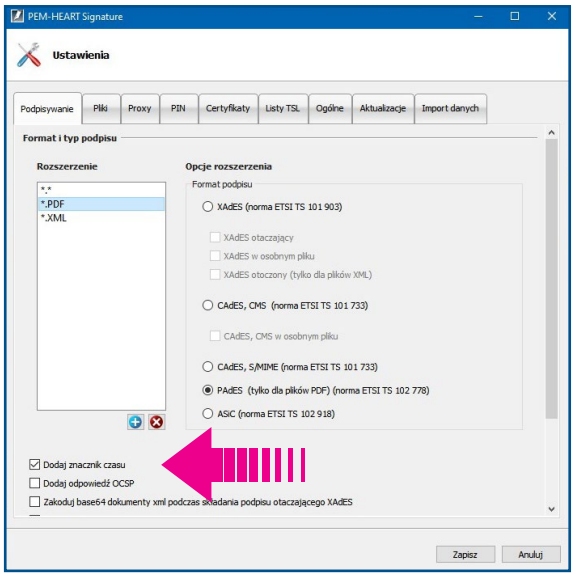


ryc. 21 – Podpis pliku PDF

Cechą charakterystyczną tej formy podpisu jest umieszczenie podpisu bezpośrednio w pliku podpisywanym. Oznacza to, że nie tworzy się nowy plik, a także nie zmienia się rozszerzenie ani ikona. Pozostaje PDF, odmiennie niż w wypadku korzystania z protokołu XAdES.

7. W USTAWIENIACH dostępna jest również możliwość konfiguracji podpisów składanych w plikach z rozszerzeniem XML. Najprostsze i niesprawiające kłopotów jest skorzystanie z opcji PODPIS OTACZAJĄCY lub PODPIS OTOCZONY (tylko dla plików XML). Podpisywany plik zachowuje się jak plik w formacie PDF (pozostaje rozszerzenie XML).

8. Jeśli dla użytkownika ważne jest, aby podpisywany plik zawierał datę i czas złożenia podpisu, należy skorzystać z opcji DODAJ ZNACZNIK CZASU [ryc. 22].



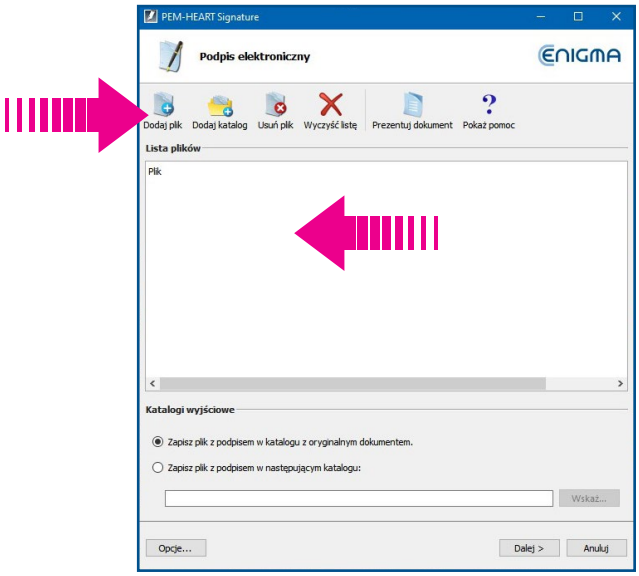
ryc. 22 - Dodaj Znacznik Czasu

Zaznaczenie jej powoduje, że do podpisu dołączana jest informacja o czasie podpisania pobierana nie z systemu komputerowego użytkownika, ale z niezależnego serwera czasu. Wówczas czas złożenia podpisu jest niepodważalny i ma wartość dowodową. Do skorzystania z tej możliwości konieczne jest podłączenie do internetu w trakcie składania podpisu. W innych wypadkach można robić to off-line.

9. Po dokonaniu zmian należy zapisać je korzystając z przycisku ZAPISZ.

10. Aby uruchomić procedurę składania podpisu należy wcisnąć IKONĘ PODPISZ.

11. W otwartym oknie można wybrać pierwszą ikonę z belki menu DODAJ PLIK lub złapać plik z pulpitu i upuścić w obrębie okna programu [ryc. 13].



ryc. 23- Dodaj plik

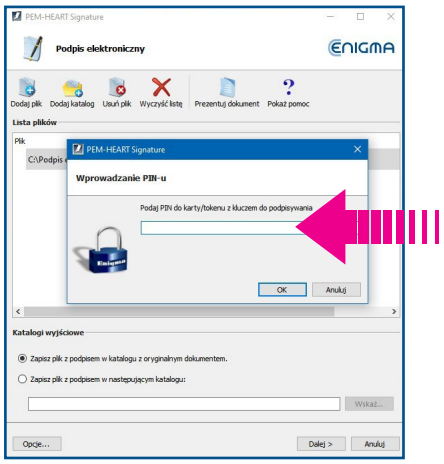
12. Jeśli planowane jest podpisanie większej liczby plików, można skorzystać z ikony DODAJ KATALOG, wówczas podpisane zostaną wszystkie pliki tam umieszczone.

13. Opcje ZAPISZ PLIK Z PODPISEM W KATALOGU Z ORYGINALNYM DOKUMENTEM/ZAPISZ PLIK Z PODPISEM W NASTĘPUJĄCYM KATALOGU dają możliwość wskazania, gdzie zostaną umieszczone podpisane pliki.

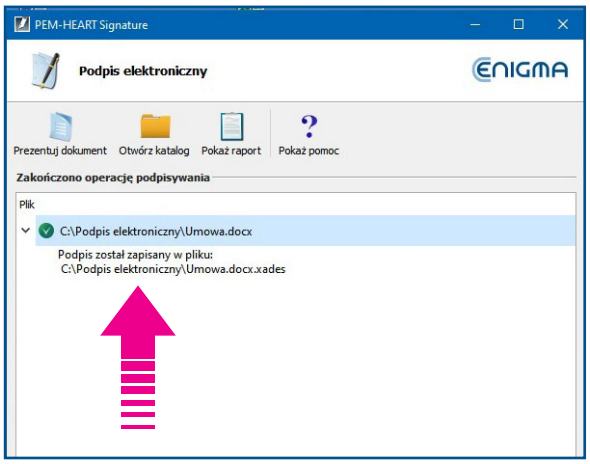
14. Uruchomienie przycisku OPCJE (już po wskazaniu pliku do podpisu) daje możliwość zmian parametrów programu wcześniej zdefiniowanych w USTAWIENIACH, ale tylko do wskazanego pliku. W standardowych czynnościach nie ma konieczności korzystania z tego rozwiązania.

15. Wciśnięcie klawisza DALEJ spowoduje otwarcie okna z komunikatem informującym o rozpoczęciu procesu podpisywania, a następnie żądaniem wpisania hasła PIN [ryc. 24].

16. Efektem wprowadzenia właściwego hasła będzie informacja [ryc. 25].



ryc. 24 - Wpisz PIN



ryc. 25 - Komunikat po poprawnie wpisanym PIN

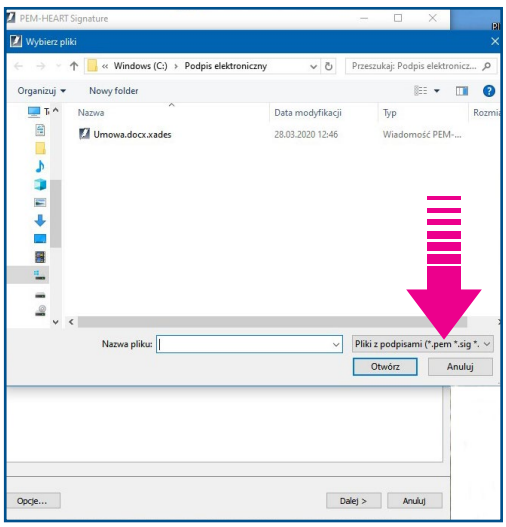
DODAWANIE PODPISÓW DO PLIKÓW WCZEŚNIEJ PODPISANYCH PRZEZ INNYCH UŻYTKOWNIKÓW

1. Aby podpisać plik podpisany wcześniej przez inną osobę (np. reprezentacja wieloosobowa) należy skorzystać z zakładki FUNKCJE ZAAWANSOWANE [ryc. 26].

ryc. 26 - Funkcje zaawansowane

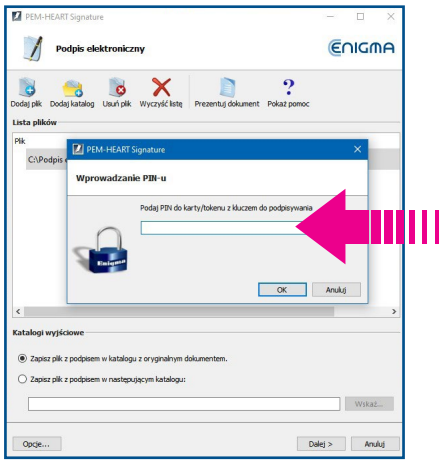
2. W otwartym oknie należy wybrać opcję DODAJ PODPIS i postępować zgodnie z opisem przedstawionym w rozdziale „Podpisywanie plików za pomocą podpisu elektronicznego lub pieczęci" w punktach 11-15.

3. Należy zwrócić uwagę, że okno WYBIERZ PLIK wyświetla tylko pliki z rozszerzeniem PEM, SIG, XADES oraz SIGNPRO. Aby dodać podpis do plików w formacie PDF lub XML, należy zaznaczyć to w oknie wyboru plików do dodania podpisu [ryc. 27].



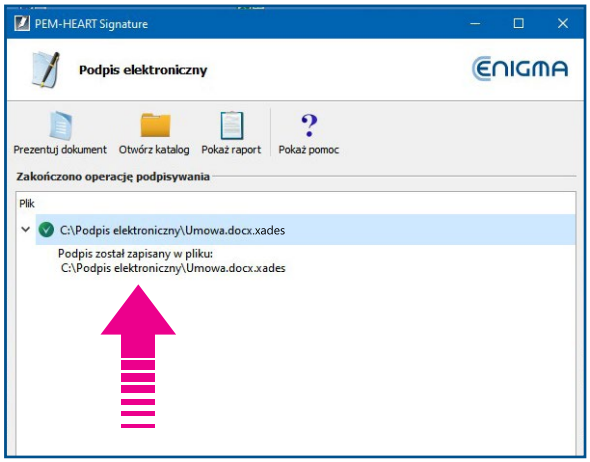
ryc. 27 - Opcja wyboru plików

4. Wciśnięcie klawisza DALEJ spowoduje otwarcie okna z komunikatem informującym o rozpoczęciu procesu podpisywania, a następnie żądaniem wpisania hasła PIN [ryc.28].



ryc. 28 - Wpisz PIN

5. Efektem wprowadzenia właściwego hasła będzie informacja [ryc. 29].



ryc. 29 - Komunikat po poprawnie wpisanym PIN

WERYFIKACJA PODPISU ELEKTRONICZNEGO

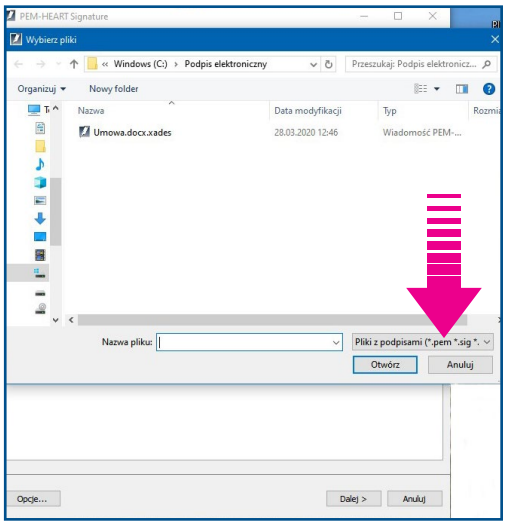
Plik opatrzony podpisem elektronicznym gwarantuje, że został on podpisany przez osobę posługującą się certyfikatem kwalifikowanym oraz że jego treść nie została zmieniona od momentu podpisania. A dodatkowo, jeśli użyto znacznika czasu, to potwierdza w sposób niepodważalny datę i czas złożenia podpisu. Aby upewnić się co do prawidłowości i ważności podpisu, należy wykonać jego weryfikację.

1. Weryfikację można przeprowadzić bez użycia czytnika z kartą. Konieczne jest posiadanie oprogramowania PEM-Heart Signature.

2. Należy uruchomić program, a następnie wcisnąć ikonę WERYFIKUJ.

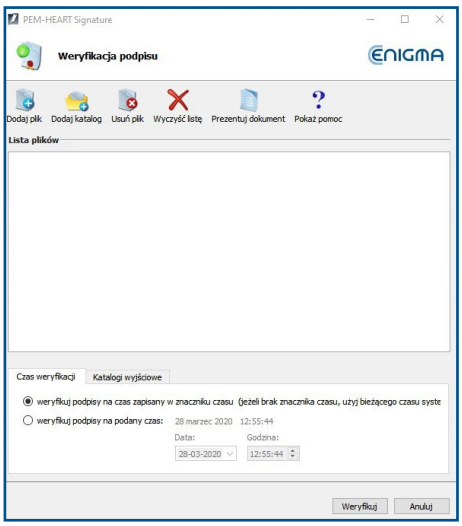
3. W otwartym oknie można wybrać pierwszą ikonę z belki menu DODAJ PLIK lub złapać podpisany plik z pulpitu i upuścić w obrębie okna programu.

4. Należy zwrócić uwagę, że okno WYBIERZ PLIK wyświetla tylko pliki z rozszerzeniem PEM, SIG, XADES oraz SIGNPRO. Aby zweryfikować podpis pliku w formacie PDF lub XML, należy zaznaczyć to w oknie wyboru plików do weryfikacji [ryc. 30]



ryc. 30 - Opcja wyboru plików

5. Opcja CZAS WERYFIKACJI daje możliwość wskazania, czy program ma wymagać znacznika czasu [ryc. 31].

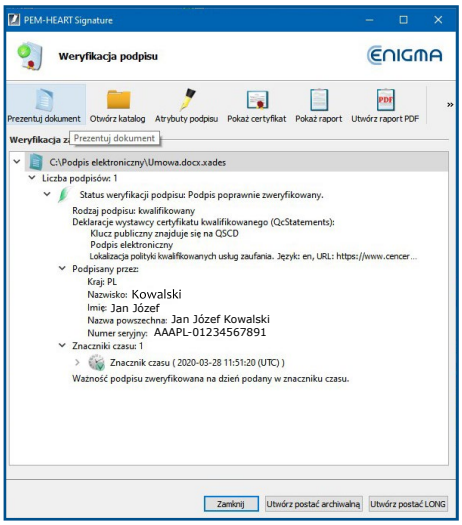


ryc. 31 - Opcja wymagania znacznika czasu

6. Opcje ZAPISZ PLIK Z DOKUMENTEM W KATALOGU Z ORYGINALNYM DOKUMENTEM/ZAPISZ PLIK Z PODPISEM W NASTĘPUJĄCYM KATALOGU dają możliwość wskazania, gdzie zostaną umieszczone weryfikowane pliki.

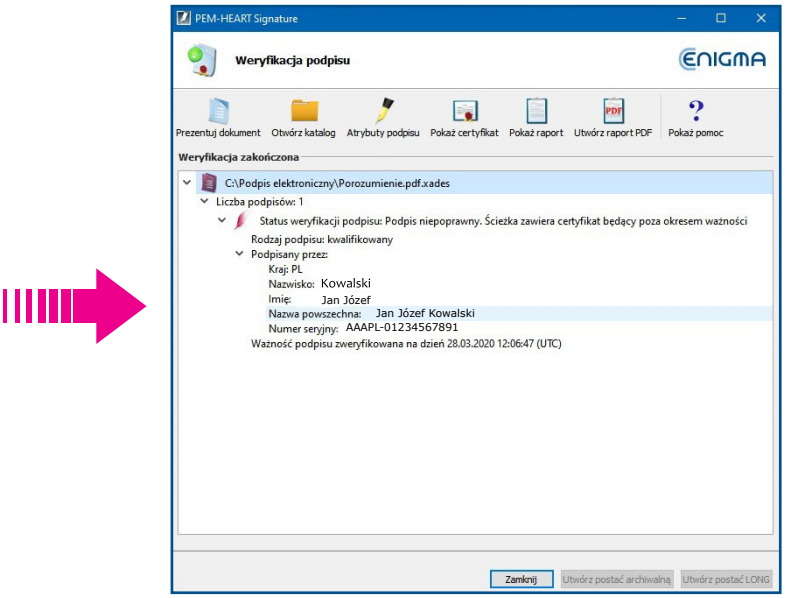
7. Wciśnięcie przycisku WERYFIKUJ uruchamia proces sprawdzania poprawności podpisu.

8. Po zakończeniu, jeśli podpis jest poprawny, pojawi się komunikat: STATUS WERYFIKACJI PODPISU: Podpis poprawnie zweryfikowany oraz dane osoby/osób podpisanych. Jeśli certyfikat do podpisu wystawiony był dla osoby działającej w imieniu instytucji, te dane zostaną także wyświetlone [ryc. 32].



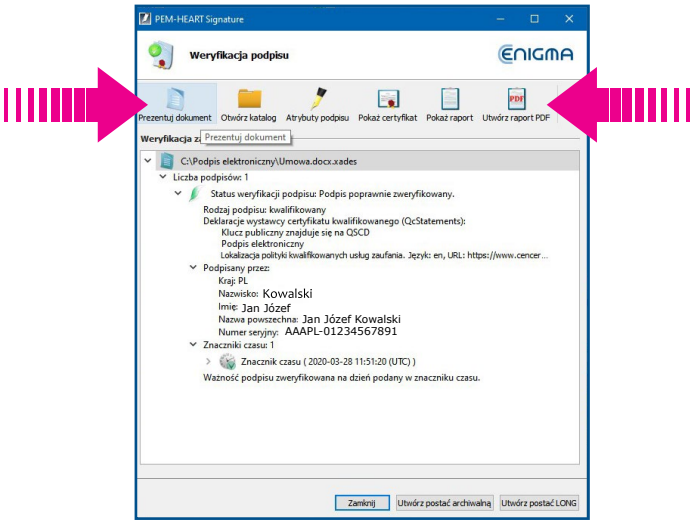
ryc. 32 - Status weryfikacji podpisu

9. Każdy inny komunikat wskazuje na nieprawidłową weryfikację, która może wynikać m.in. z przekroczenia (w chwili weryfikacji) terminu ważności certyfikatu użytego do podpisu, unieważnienia certyfikatu itp. [ryc. 33].



ryc. 33 - Podpis niepoprawny

10. Dopiero po prawidłowo przeprowadzonej weryfikacji można użyć polecenia PREZENTUJ DOKUMENT, a także wygenerować potwierdzenie przeprowadzonej weryfikacji i jej status [ryc. 34].



ryc. 34 - Status weryfikacji podpisu

PODPISANIE E-DEKLARACJI ZA POMOCĄ PODPISU ELEKTRONICZNEGO I WYSŁANIE JEJ DO URZĘDU SKARBOWEGO

Aby podpisać i wysłać e-Deklarację konieczne jest posiadanie wszystkich niżej wymienionych narzędzi:

- certyfikatu do podpisu elektronicznego
- zainstalowanego oprogramowania PEM-Heart Signature
- programu Adobe Acrobat Reader (do bezpłatnego pobrania na stronie Adobe Inc.: www.adobe.com)
- wtyczki e-deklaracje (do pobrania na stronie Ministerstwa Finansów: www.podatki.gov.pl/e-deklaracje/wtyczka-do-podpisywania-i-przesylania-danych-xml-z-interaktywnych-formularzy-pdf/

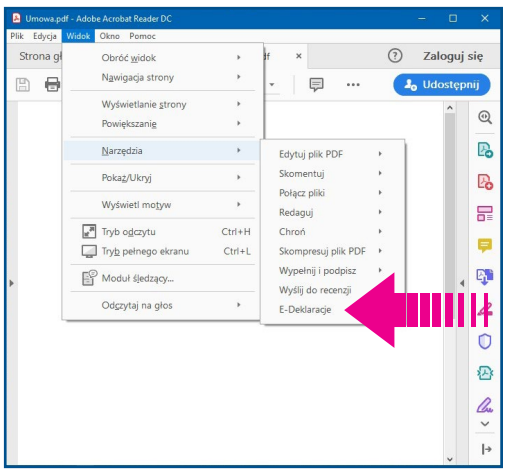
Instrukcja dotycząca korzystania z rozwiązania do wysyłania e-deklaracji znajduje się: www.podatki.gov.pl/e-deklaracje/jak-zlozyc-e-deklaracje

W trakcie wysyłania dokumentów program będzie wymagał złożenia podpisu elektronicznego. Należy:

1. Włożyć czytnik z kartą do portu USB. Nie trzeba uruchamiać programu PEM-Heart Signature, zostanie on wywołany automatycznie w dalszej procedurze.

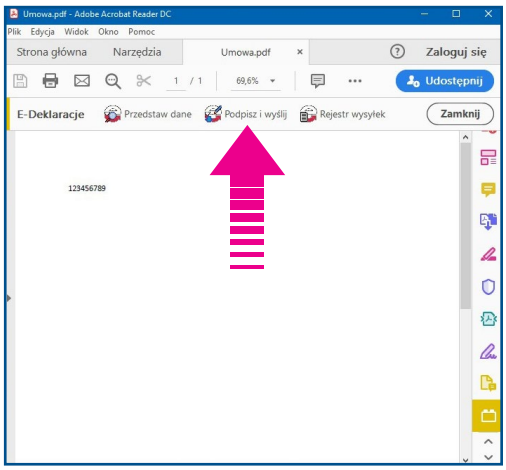
2. Otworzyć w programie Adobe Acrobat Reader deklarację wcześniej pobraną ze strony www.podatki.gov.pl/e-deklaracje/ i prawidłowo wypełnioną.

3. Z belki menu należy uruchomić opcję WIDOK, a następnie NARZĘDZIA i z rozwiniętej listy wybrać E-DEKLARACJE [ryc. 35].



ryc. 35 - Opcja e-Deklaracje

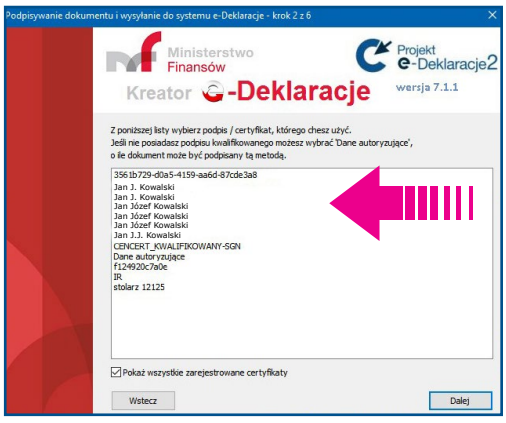
4. Powyżej otwartej deklaracji pojawi się nowe proste menu: PRZEDSTAW DANE, PODPISZ I WYŚLIJ, REJESTR WYSYŁEK. Należy wybrać opcję: PODPISZ I WYŚLIJ [ryc.36].



ryc. 36 - Opcja PODPISZ I WYŚLIJ

5. Następnie należy postępować zgodnie ze wskazówkami programu (przycisk DALEJ).

6. W kroku 2 z 6 program będzie wymagał wskazania certyfikatu służącego do podpisu [ryc. 37].



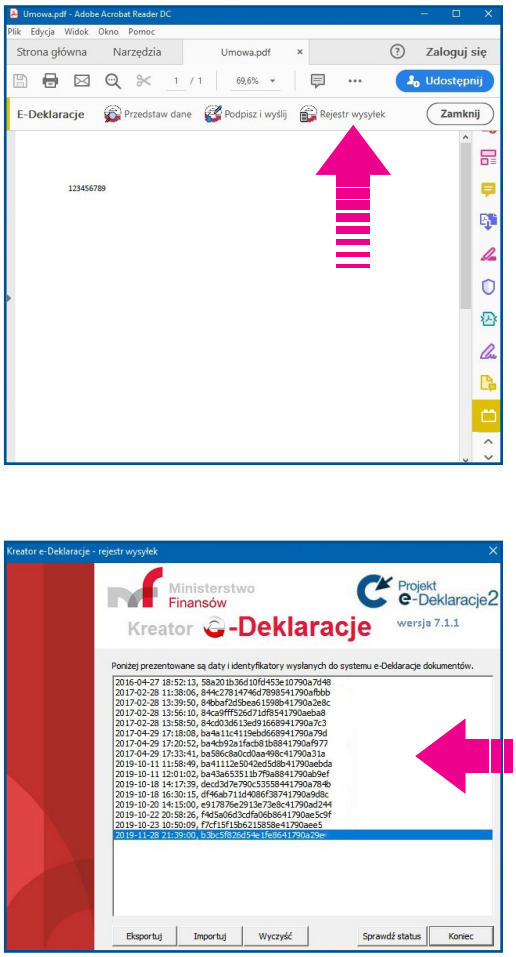
ryc. 37 - Wskazanie certyfikatu

Jeśli na liście będzie kilka (np. wymaganych przez zainstalowane programy), proszę wskazać opisany pełnym imieniem i nazwiskiem. Sprawdzenie poprawności dokonanego wyboru nastąpi w kolejnym kroku, gdy program wyświetli dane certyfikatu m.in. jego termin ważności. Błędny wcześniejszy wybór można cofnąć przyciskiem WSTECZ.

7. Wskazanie właściwego certyfikatu uruchomi program PEM-Heart Signature, który do podpisania i wysłania dokumentu będzie wymagał podania hasła PIN.

8. Proces zakończy wyświetlenie informacji o prawidłowym złożenie deklaracji i możliwości pobrania UPO (Urzędowego Potwierdzenia Odbioru). Potwierdzenie należy zachować, jako dowód przesłania i przyjęcia deklaracji.

9. Jeśli UPO nie zostanie wygenerowane, status przesłanego dokumentu można sprawdzić w późniejszym terminie korzystając z opcji REJESTR WYSYŁEK w menu E-DEKLARACJE [ryc. 38 ab].



ryc. 38 ab - Rejestr wysyłek

PODPISANIE JPK ZA POMOCĄ PODPISU ELEKTRONICZNEGO I WYSŁANIE DO URZĘDU SKARBOWEGO

Informacje szczegółowe dotyczące zasad i obowiązków związanych z przesyłaniem Jednolitych Plików Kontrolnych znajdują się na stronach Ministerstwa Finansów i są dostępne pod następującymi linkami:

- https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk_vat/informacje-jpk-vat/
- Do 31 marca 2020: https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk_vat/
- Do 1 kwietnia dla dużych przedsiębiorców i od 1 lipca dla pozostałych podatników: https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk-vat-z-deklaracja/
- Wszystkie informacje oraz przykładowe pliki są dostępne: https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk_vat/pliki-do-pobrania/
- Szczegółowy opis przygotowania i wysyłki plików JPK został opisany: https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk_vat/informacje-jpk-vat/wypelnij-i-wyslij-jpk_vat/

Proszę zwrócić uwagę na komunikat określający wymagany systemy operacyjny i programy dodatkowe:

UWAGA! Do uruchomienia aplikacji potrzebny jest komputer wyposażony w system Windows 7 lub nowszy w wersji 32-bitowej lub 64-bitowej, z zainstalowanym środowiskiem Java w wersji 1.8.0_151 lub wyższej.

Jeśli program księgowy ma możliwość wygenerowania oraz samodzielnego wysłania pliku JPK, proces złożenia podpisu w przygotowanym pliku sprowadzi się do automatycznego wywołania PEM-Heart Signature. Komunikat wyświetlony na monitorze wskaże konieczność wpisania hasła PIN i zatwierdzenia.

Jeśli program księgowy generuje jedynie plik w formacie CSV, do podpisu i wysłania pliku JPK potrzebny będzie program Klient JPK 2.0. W tej sytuacji należy:

1. Pobrać plik Klient JPK ze strony: https://www.podatki.gov.pl/jednolity-plik-kontrolny/jpk_vat/aplikacje-do-pobrania/

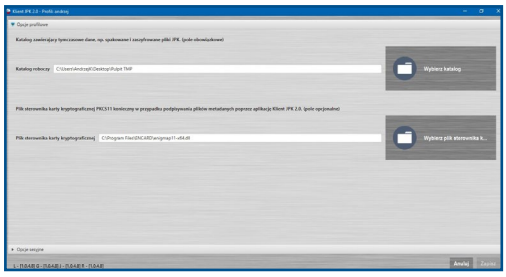
2. Po instalacji i uruchomieniu aplikacji konieczne jest założenie profilu: podanie nazwy oraz hasła, które będą służyły do logowania się do programu [ryc. 39].

ryc. 39 - Założenie profilu

3. Dalsze działania polegają na konfiguracji aplikacji zgodnie z poleceniami na ekranie [ryc. 40].

ryc. 40 - Konfiguracja profilu

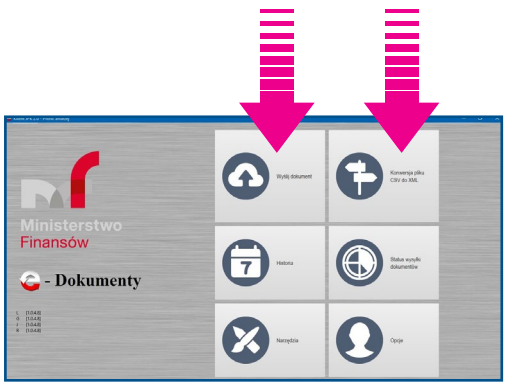
4. Niezbędnie w tym miejscu będzie wskazanie katalogu tymczasowego (roboczego) do ulokowania/przechowywania plików tymczasowych JPK oraz katalogu z plikami sterowników kart kryptograficznych służących do podpisywania danych [ryc. 41].



ryc. 41 - Wskazanie katalogu roboczego i sterowników

5. Dla oprogramowania PEM-Heart Signature należy wskazać zależnie od wybranej wersji Klienta JPK 2.0 następujące lokalizacje:
   - Klient JPK 64-bitowy: C:\Program Files\ENCARD\enigmap11-x64.dll
   - Klient JPK 32-bitowy: C:\Program Files (x86)\ENCARD\enigmap11.dll.

6. Dalsze czynności polegają na uruchomieniu opcji KONWERSJA PLIKU CSV DO XML, a jeśli plik do wysyłki jest już w formacie XML – opcji WYŚLIJ DOKUMENT [ryc. 42].



ryc. 42 - Konwersja do XML i wysyłka

7. Należy wskazać dokument z danymi, a dalsze działania wykonywać zgodnie z pojawiającymi się komunikatami systemu.

8. Program PEM-Heart Signature zostanie automatycznie wywołany. Konieczne będzie podanie hasła PIN.

9. Całość działań zakończy komunikat informujący o prawidłowym wysłaniu i odebraniu pliku z danymi.