Dokumentacja użytkownika
PEM-HEART Signature

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	10.02.2011	Bartosz Sajnaj
Wersja zaktualizowana do obsługi najnowszej wersji programu. Poprawki edycyjne.		
1.2	26.04.2011	Bartosz Sajnaj
Dodanie opisu opcji rejestracji certyfikatu w systemie (rozdział 7.5).		
1.3	22.09.2011	Bartosz Sajnaj
Wersja zaktualizowana do najnowszej wersji programu. Poprawki edycyjne.		
1.4	05.06.2012	Bartosz Sajnaj
Aktualizacja do wersji 3.9.5 oprogramowania.		
1.5	13.08.2012	Bartosz Sajnaj
Aktualizacja do wersji 3.9.7 oprogramowania. Zmiany: składanie podpisu dla plików *xml* (rozdział 5.4) oraz menu podręczne Windows (**Rysunek 3**). Nowe opcje: dodatkowa forma podpisu (na tronie 39) oraz diagnostyka karty (rozdział 6.4).		
1.6	22.10.2012	Grzegorz Mroziewicz
Zmiany: weryfikacja podpisu przez Adobe Reader *xml* (rozdział 4.2.1)		
1.7	11.12.2012	Grzegorz Mroziewicz
Aktualizacja widoku okienek, screeny z wersji 3.9.7.17 oprogramowania.		
1.8	15.10.2013	Sławomir Szopa
Aktualizacja do wersji 3.9.9		
1.9	03.01.2014	Radosław Wolak
Aktualizacja procesu aktywacji karty.		
1.91	25.03.2014	Radosław Wolak
Aktualizacja procesu personalizacji karty		

Spis treści

1 Wstęp

Oprogramowanie **PEM-HEART Signature** służy do składania i weryfikacji kwalifikowanych podpisów elektronicznych dla dokumentów w systemach rodziny Windows *(XP SP3/2003/2008/Vista*/7/8), 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 wielokrotne 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 obsługuje następujące formaty podpisów elektronicznych:

- **XAdES** - zgodnie ze specyfikacją techniczną *ETSI TS 101 903 XML Advanced Electronic Signatures* (XAdES)
- **CAdES CMS** i **CAdES S/MIME -** zgodnie 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*. 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 od aproval*), potwierdzenie utworzenia.

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

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 (*Windows XP/2003/2008/Vista/7/8*, 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 XP/2003/2008/Vista/7/8*, 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 Definicje

W dokumencie następujące pojęcia zostały użyte w znaczeniu określonym poniżej w tabeli.

Definicja	Opis definicji
Certyfikat kwalifikowany	Certyfikat spełniający warunki określone w Ustawie o podpisie elektronicznym, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne. *Art. 5.2 Ustawy o podpisie elektronicznym* stanowi, że: "*Dane w postaci elektronicznej opatrzone bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu są równoważne pod względem skutków prawnych dokumentom opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne stanowią inaczej*".
Punkt zaufania	Zaufany klucz publiczny służący do weryfikacji ścieżek certyfikatów. Każda ścieżka certyfikatów musi kończyć się w jednym z punktów zaufania. Punkty zaufania są przekazywane w formie autocertyfikatów (certyfikatów wystawionych dla samego siebie) lub zaświadczeń certyfikacyjnych (certyfikatów wystawionych przez inny urząd). Zaufanie do punktów zaufania ustalane jest metodami poza kryptograficznymi, np. bezpieczna dystrybucja wraz z oprogramowaniem, zaufany kurier itp. Dla podpisów kwalifikowanych ścieżka certyfikacji musi kończyć się na głównym urzędzie certyfikacyjnym dla infrastruktury bezpiecznego podpisu elektronicznego w Polsce.
PKI (*Public Key Infrastructure*)	System wystawiania i dystrybucji certyfikatów, kluczy publicznych i list unieważnionych certyfikatów.
Identyfikator wyróżniający (DN – *Distinguished Name*)	Identyfikator zgodny ze składnią X.509 pozwalający na jednoznaczną identyfikację użytkownika certyfikatu w ramach użytkowników obsługiwanych przez jeden urząd ds. certyfikatów. W każdym certyfikacie zapisany jest identyfikator wyróżniający użytkownika (właściciela klucza publicznego) oraz identyfikator wyróżniający wystawcy certyfikatu (Centrum Certyfikacji Kluczy, które wystawiło certyfikat).
Lista CRL – *Certificate Revocation List*)	Wiadomość elektroniczna podpisana przez urząd ds. certyfikatów, zawierająca numery unieważnionych certyfikatów. Lista CRL jest sposobem na dystrybucję w systemie PKI informacji o unieważnionych certyfikatach.
Lista ARL (ang. *Authority Revocation List*)	Lista ta zawiera numery unieważnionych zaświadczeń certyfikacyjnych. Lista ARL jest sposobem na dystrybucję w systemie PKI informacji o unieważnionych urzędach certyfikacji.
Serwer datowania	Serwer wystawiający znaczniki czasu dla żądań wysyłanych przez oprogramowanie PEM-HEART podczas zabezpieczania wiadomości ze znakowaniem czasu.
Serwer list CRL/ARL	Serwer, z którego PEM-HEART pobiera listy CRL/ARL punktu zaufania, dla którego skonfigurowany jest serwer. Listy CRL/ARL są pobierane automatycznie podczas przetwarzania wiadomości, gdy są potrzebne nowsze niż posiadane.
Serwer proxy	Serwer pośredniczy w transferze danych pomiędzy użytkownikiem a serwerami zdalnymi. Użycie *proxy* zwiększa bezpieczeństwo, ponieważ jego praca realizowana jest w warstwie aplikacyjnej modeli ISO/OSI, i jako taka może analizować logiczną zawartość pakietów, a nie jedynie ich formalną zgodność ze standardem.

Tabela 1. Tabela definicji

4 Praca z aplikacją

W dokumencie opisano i przedstawiono pracę z aplikacją w systemie Windows 7. Wersje dla systemów Linux oraz MacOSX działają w sposób identyczny, natomiast wygląd okien programu jest specyficzny dla danego systemu.

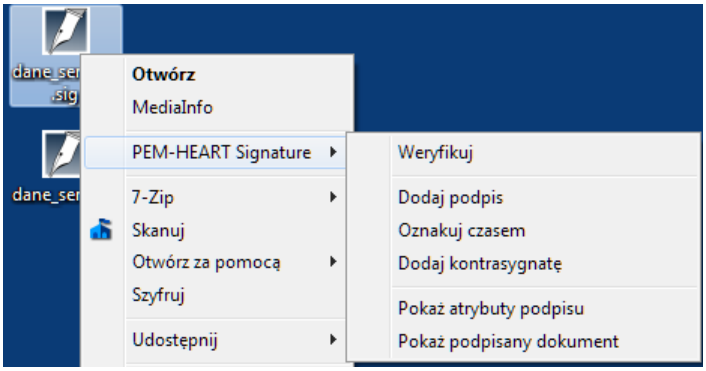
Aplikację uruchamia się poprzez skróty w *Menu Start* lub na pulpicie. Ikonka programu wygląda jak na rysunku poniżej:

Rysunek 1 Ikonka programu

Po uruchomieniu aplikacji zostanie wyświetlone okno jak przedstawiono poniżej na rysunku:

Rysunek 2 Widok okna głównego

Uruchomienie programu jest również dostępne poprzez systemowe menu kontekstowe (prawy przycisk myszki na wybranym dokumencie lub dokumentach) zarówno dla plików niepodpisanych (jedynie opcja złożenia podpisu) jak i dla dokumentów zawierających podpisy elektroniczne (domyślnie są to: *.pem, *.sig, *.xades, *.SignPro).



Rysunek 3 Menu kontekstowe dla dokumentów

Dalej w bieżącym rozdziale zostaną opisane czynności związane z funkcjami podstawowymi programu, czyli ze składaniem i weryfikacją podpisów elektronicznych.

W rozdziale 5 zostaną opisane funkcje zaawansowane programu – takie jak składanie kontrasygnaty, podpisu dodatkowego, znakowania czasem oraz składania podpisów dla dokumentów XML.

W rozdziale 6 zostaną opisane funkcje obsługi kart kryptograficznych.

W rozdziale 7 zostanie opisana konfiguracja parametrów pracy programu.

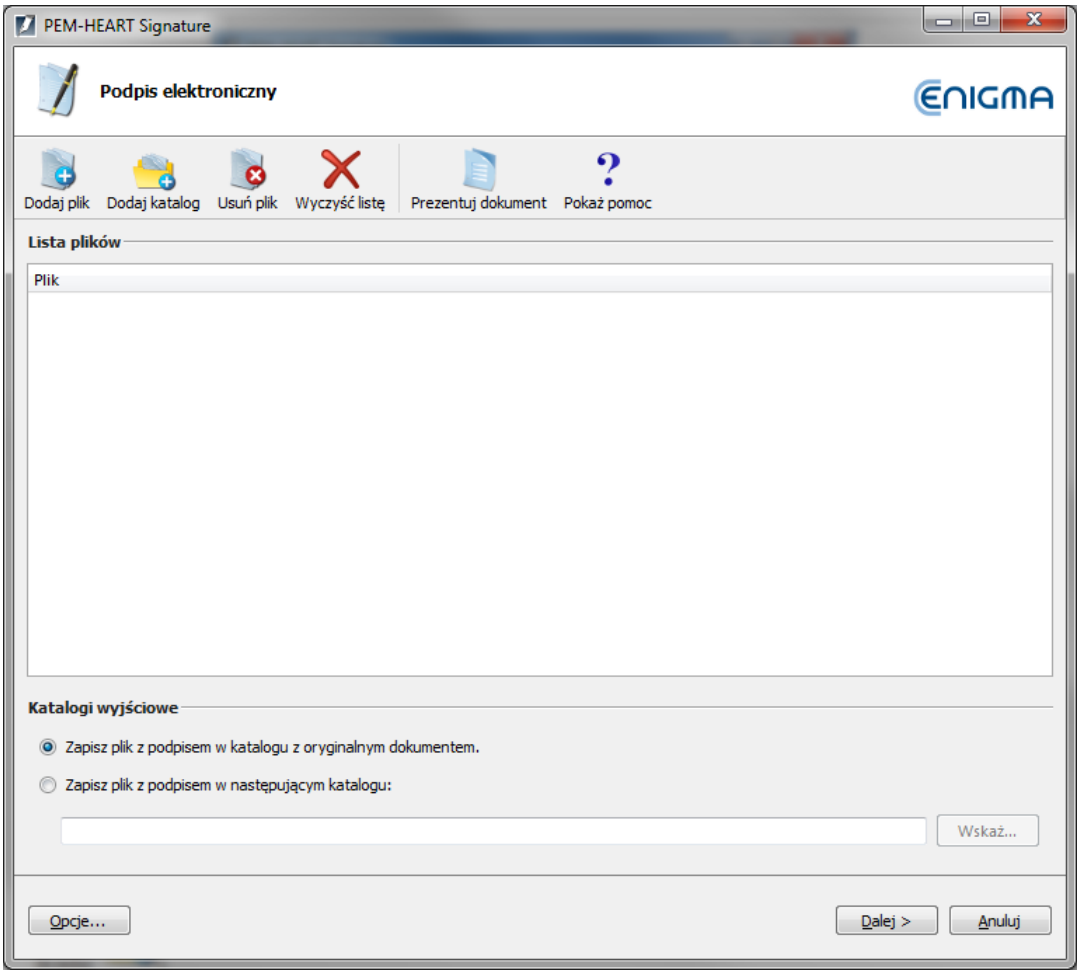
4.1 Podpisywanie

Podpisywanie plików za pomocą bezpiecznego podpisu elektronicznego daje użytkownikowi w myśl ustawy o podpisie elektronicznym pewność, że podpis ten jest przyporządkowany wyłącznie do osoby składającej ten podpis oraz jest dodany w taki sposób, że jakakolwiek późniejsza zmiana dokumentu podpisanego jest rozpoznawalna. Wszelkie skutki prawne złożenia takiego podpisu mają skutek jak podpis odręczny.

Podpisywanie plików bezpiecznym podpisem elektronicznym może być wykorzystywane przy autoryzacji dokumentów i zabezpieczaniu przed modyfikacją (np. prac autorskich, umów, komunikacji z urzędami, ZUS itp.).

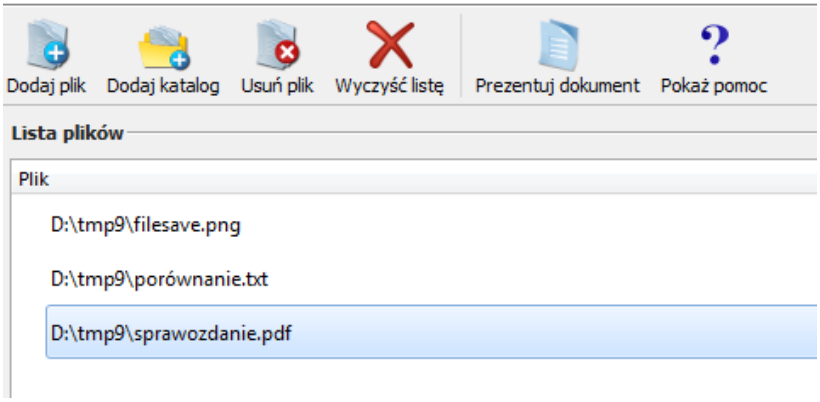
Aby podpisać plik należy wybrać przycisk 

z listy zakładek funkcji podstawowych w oknie głównym programu. Po jego wybraniu zostanie wyświetlone okno wskazywania plików do podpisania.



Rysunek 4 Wybór pliku lub plików do podpisania

Następnie należy wybrać plik (poprzez ikonkę ) lub wszystkie pliki z katalogu wraz z podkatalogami (poprzez ikonkę ).



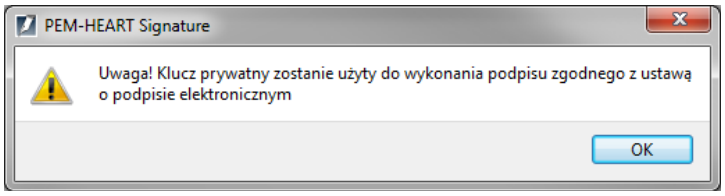
Rysunek 5 Po wybraniu plików do podpisania

Do obsługi listy plików służą przyciski: - skasowanie wybranej pozycji oraz - usunięcie wszystkich wybranych pozycji.

Po wybraniu plików można (w opcjach zapisu pliku na dole okna wyboru plików) zdefiniować katalog, w którym pliki podpisane mają zostać umieszczone. W przypadku, gdy ten katalog został określony w opcjach konfiguracji programu, zostanie on automatycznie wpisany w pole *Zapisz plik z podpisem w następującym katalogu.*

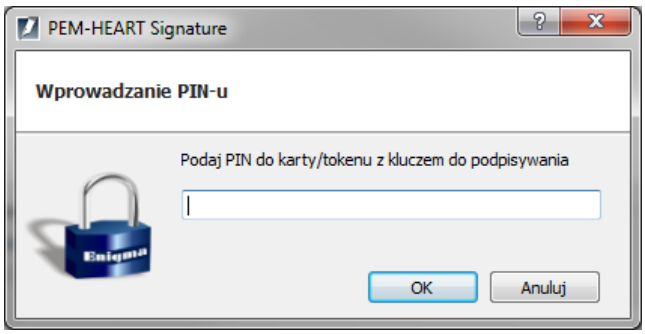
Możliwe jest również określenie opcji formy podpisu poprzez przycisk *Opcje*, znajdujący się w lewym dolnym rogu okna wyboru plików. Szczegóły pozostałych opcji składania podpisu (w tym wyboru algorytmu oraz jego typu, a także skojarzenia plików o danych rozszerzeniach z określonymi parametrami podpisu) zostały opisane w rozdziale 7 o konfiguracji programu.

Wciśnięcie przycisku *Dalej >* spowoduje wyświetlenie okienka zawierającego komunikat o konieczności potwierdzenia użycia kluczy prywatnych użytkownika do wykonania podpisu (a także pobrania znacznika czasu jeśli została wybrana taka forma podpisu). Jest to wymaganie stawiane przez ustawę o podpisie elektronicznym.



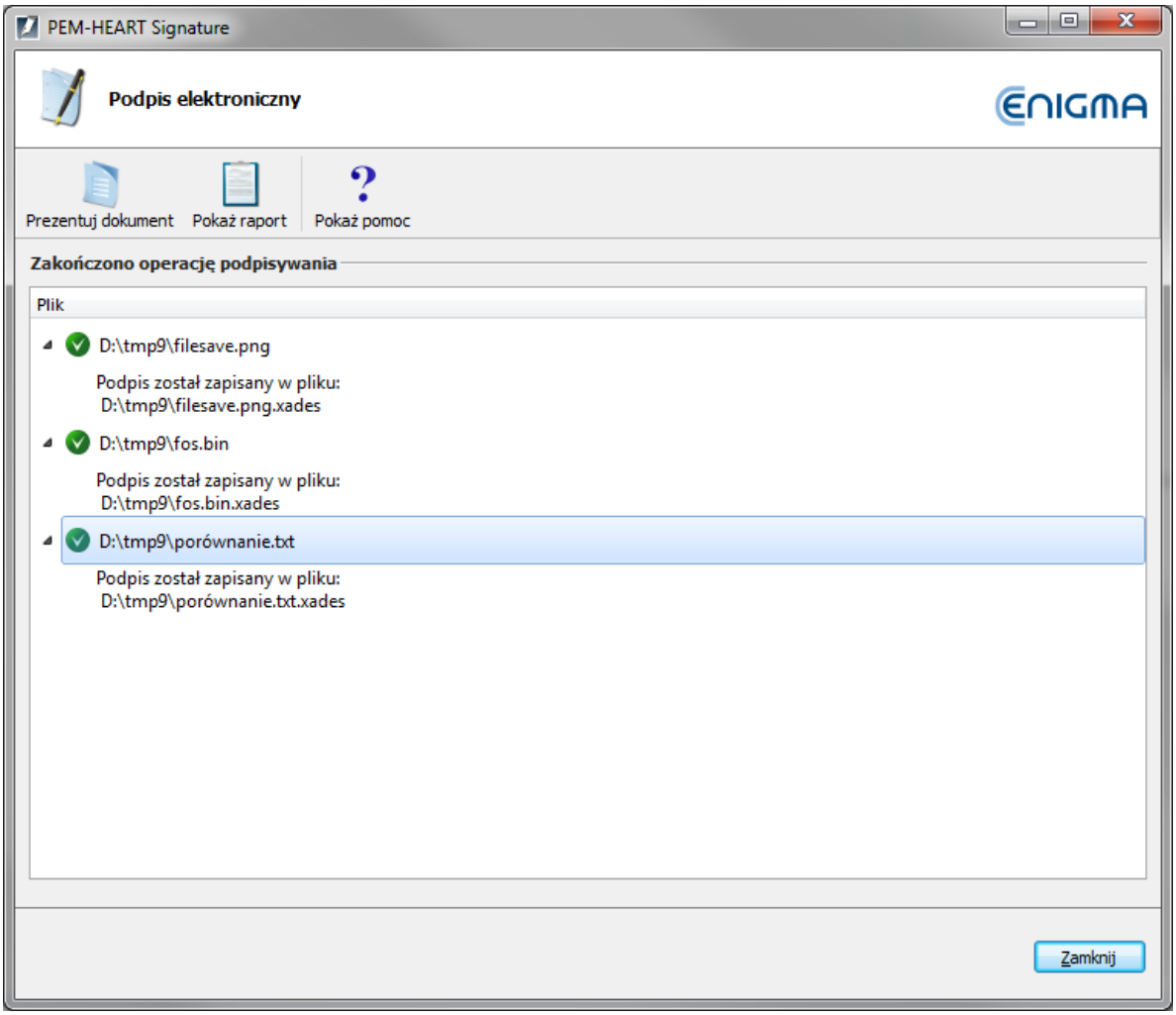
Rysunek 6 Potwierdzenie wykonania podpisu

Po zatwierdzeniu komunikatu zostanie wyświetlone okno, w którym należy wpisać kod PIN, zabezpieczający dostęp do kluczy kryptograficznych na nośniku.



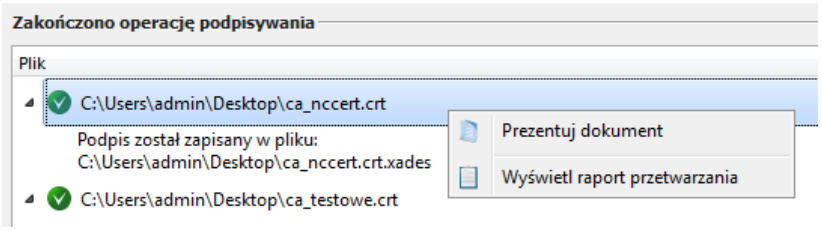
Rysunek 7 Podawanie hasła

Po podaniu poprawnego hasła program wykonuje podpisywanie dokumentu. Wynik działania prezentowany jest w oknie podsumowującym. W zależności od wybranego formatu podpisu plik wynikowy może mieć rozszerzenie *.xades* (format *XAdES*) lub *.sig* (formaty *CAdES* CMS oraz S/MIME). W przypadku plików *pdf* z wybranym podpisywaniem w formacie *PAdES* rozszerzenie pliku nie jest zmieniane.



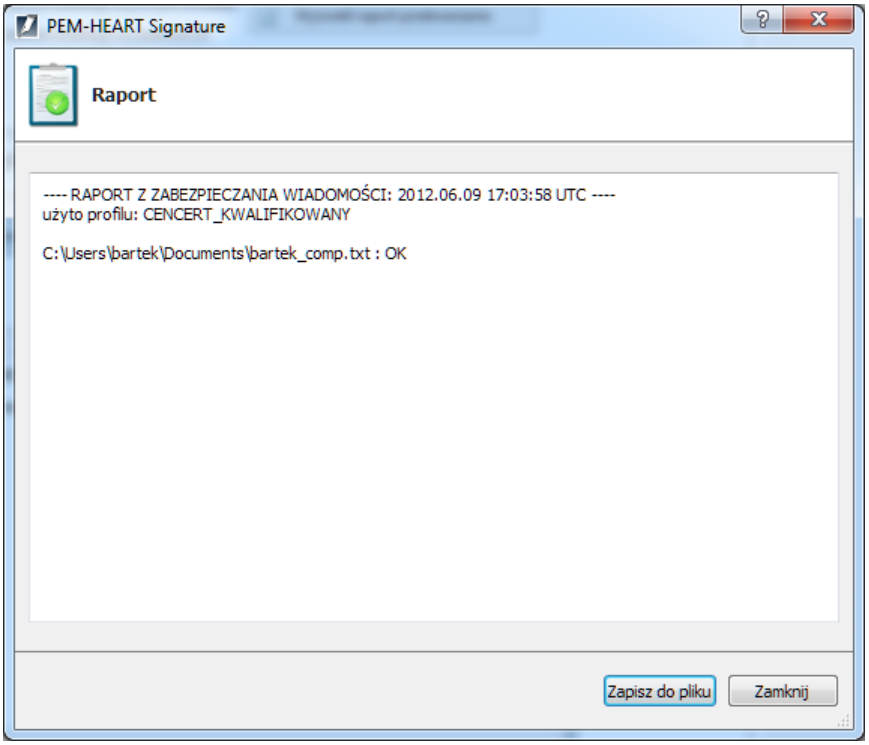
Rysunek 8 Prezentacja wyniku podpisywania

Poprzez ikonki i menu kontekstowe dostępne jest wyświetlenie raportu z przetwarzania danego pliku oraz wyświetlenie zawartości dokumentu.



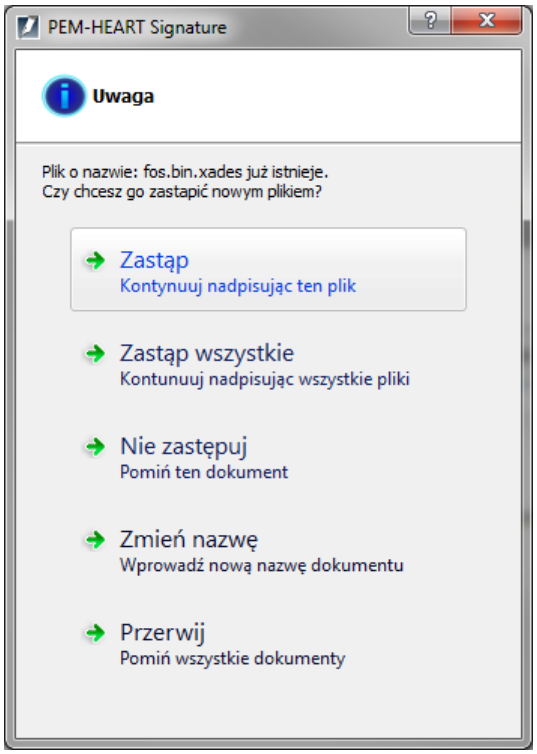
Rysunek 9 Menu raportów

Wybranie opcji raportu spowoduje wyświetlenie okienka, w którym prezentowane są informacje o przebiegu danego procesu. Raport można zapisać do pliku tekstowego. Poniżej przedstawiono raport z pomyślnego przebiegu składania podpisu.



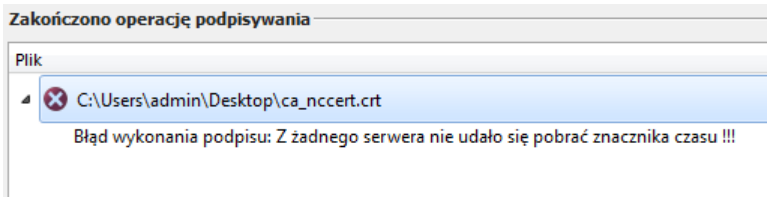
Rysunek 10 Okienko raportu

W przypadku, gdy dokument został już wcześniej podpisany i program wykryje obecność podpisanego pliku w katalogu docelowym zostanie wyświetlone okno z wyborem opcji zastępowania istniejącego dokumentu.



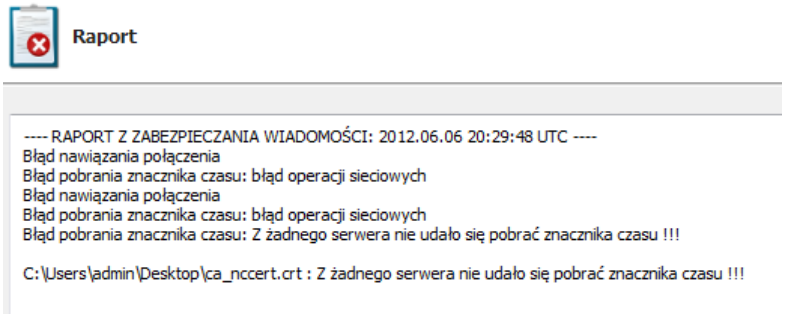
Rysunek 11 Opcje zastępowania

W przypadku niepowodzenia operacji składania podpisu w oknie podsumowania zostanie wyświetlony powód niepowodzenia.



Rysunek 12 Błąd podpisywania

Dokładniejsze przyczyny są umieszczane w raporcie przetwarzania.



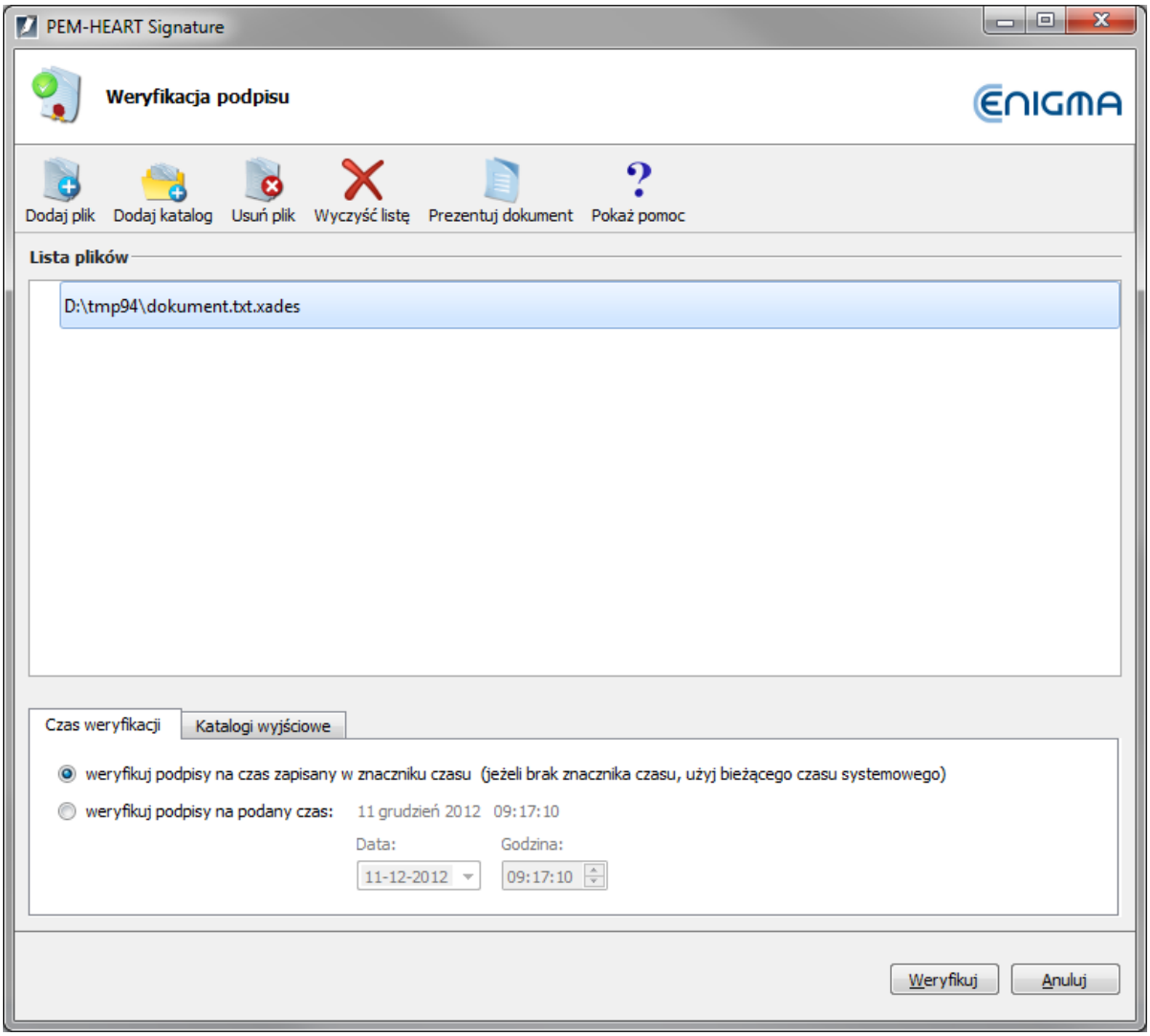
Rysunek 13 Raport z opisem błędów

4.2 Weryfikacja podpisu

Weryfikacja podpisu umożliwia stwierdzenie czy dokument został podpisany przez daną osobę, nie został zmodyfikowany oraz czy jego podpis jest ważny.

Aby zweryfikować podpis należy użyć przycisku  z okna głównego aplikacji. Zostanie wyświetlone okno wyboru plików. Okno to jest identyczne z opisanym w poprzednim rozdziale. Za pomocą przycisków należy wybrać dokumenty do weryfikacji. Widok listy dokumentów w oknie dodawania plików jest domyślnie filtrowany do rozszerzeń plików zawierających podpisy elektroniczne: *.pem, *.sig, *.xades, *.SignPro. Filtr ten można zmienić na wyświetlenie tylko plików *pdf* lub też wszystkich plików.

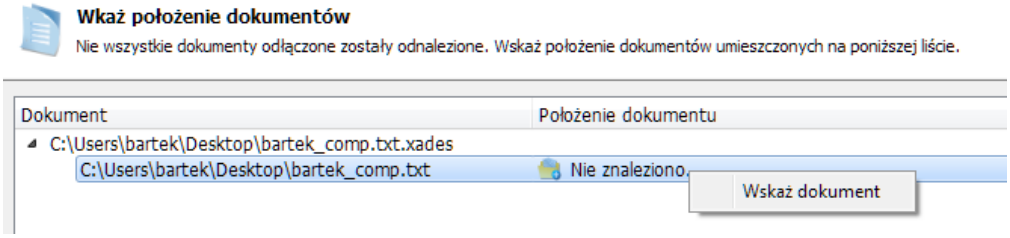
Poniżej przedstawiono okno po wyborze podpisanego pliku.



Rysunek 14 Wybranie plików do weryfikacji

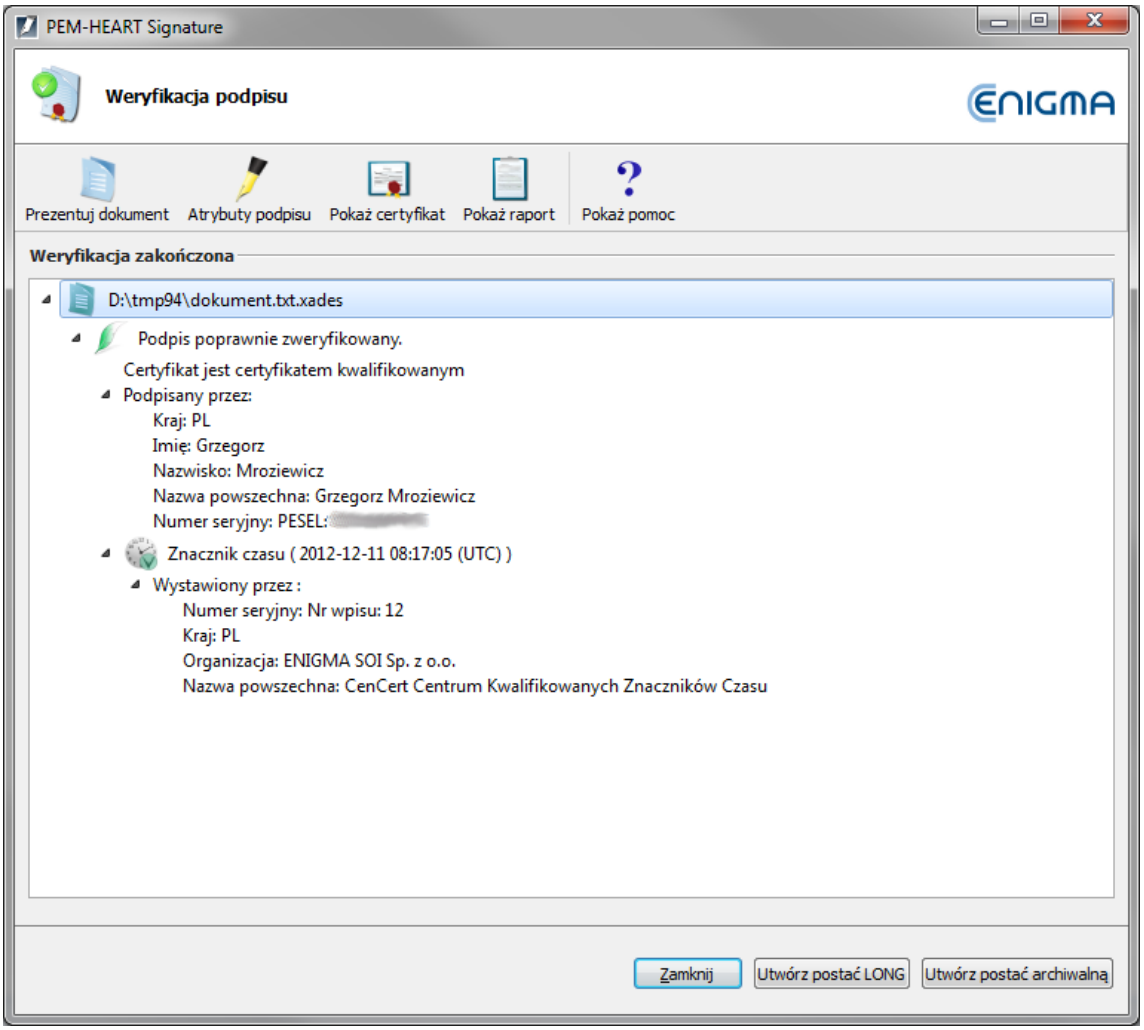
Weryfikacji dokumentu (lub wielu dokumentów) dokonuje się po użyciu przycisku *Weryfikuj*. Podobnie jak w przypadku podpisu można wskazać w jakim katalogu mają zostać umieszczone pliki wynikowe operacji.

W przypadku, gdy weryfikowany jest dokument z podpisem odłączonym i plik z podpisem nie znajduje się w tym samym katalogu co plik weryfikowany zostanie wyświetlone okno z komentarzem informującym o tym. Za pomocą menu kontekstowego lub dwukrotnego kliknięcia na danej pozycji można wskazać położenie dokumentu.



Rysunek 15 Wskazywanie dokumentu dla podpisu odłączonego

Wyniki weryfikacji prezentowane są w oknie jak na rysunku poniżej.

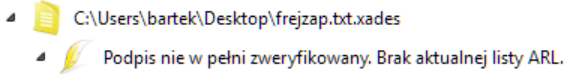


Rysunek 16 Wynik weryfikacji

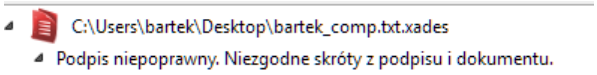
Przycisk *Utwórz postać LONG* możliwe jest przekształcenie podpisywanego dokumentu do tego formatu. Operacja jest opisana w podrozdziale 4.3.

Wynik weryfikacji oznaczany jest kolorowymi symbolami dla wyraźnego jego odróżnienia. Kolor zielony oznacza pełne powodzenie weryfikacji.

Kolor żółty oznacza częściowe powodzenia operacji - np. podpis jest poprawny, ale niemożliwe było pobranie aktualnych list CRL, aby sprawdzić jego ważność.



Kolor czerwony oznacza niepowodzenie weryfikacji podpisu.

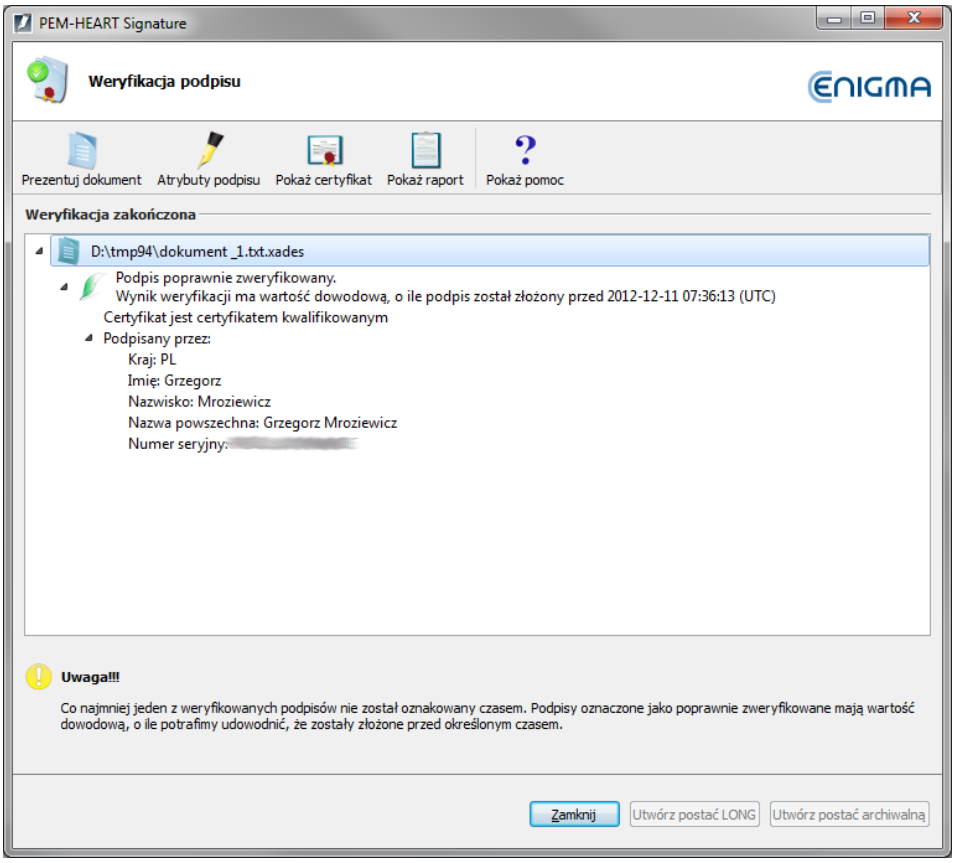


Szczególnym przypadkiem jest weryfikacja pliku podpisanego podpisem kwalifikowanym, zakończona wynikiem prawidłowym ale z zastrzeżeniem czasowej ważności wyniku weryfikacji.

Przypadek ten zdarza się wtedy, gdy spełnione są wszystkie poniższe warunki:

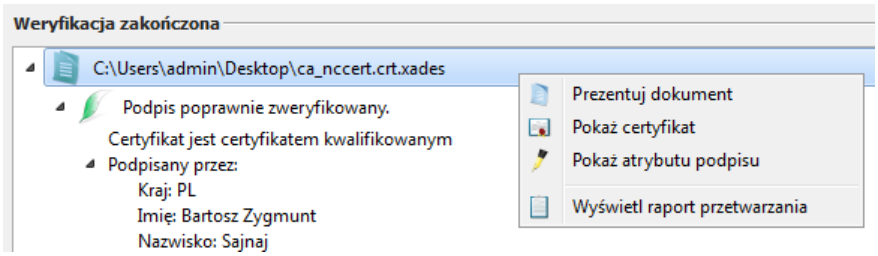
- weryfikowany podpis nie został opatrzony znacznikiem czasu lub żaden ze znaczników czasu nie został w pełni lub częściowo zweryfikowany
- użytkownik nie posiada listy CRL wystawionej po czasie złożenia podpisu potrzebnej do pełnej weryfikacji certyfikatu użytkownika. Data wystawienia listy CRL obecnej w bazie programu jest wcześniejsza od daty, na którą podpis jest weryfikowany (domyślnie, w przypadku braku pozytywnie zweryfikowanego znacznika czasu, jest to czas systemowy użytkownika
- użytkownik nie posiada odpowiedzi OCSP potrzebnej do pełnej weryfikacji certyfikatu użytkownika. (np. brak połączenia internetowego)

W zastrzeżeniu o wartości dowodowej podpisu podana jest data wystawienia posiadanej listy CRL (przykład na rysunku poniżej). Pozostałe szczegóły wyniku weryfikacji są dostępne w raporcie przetwarzania.



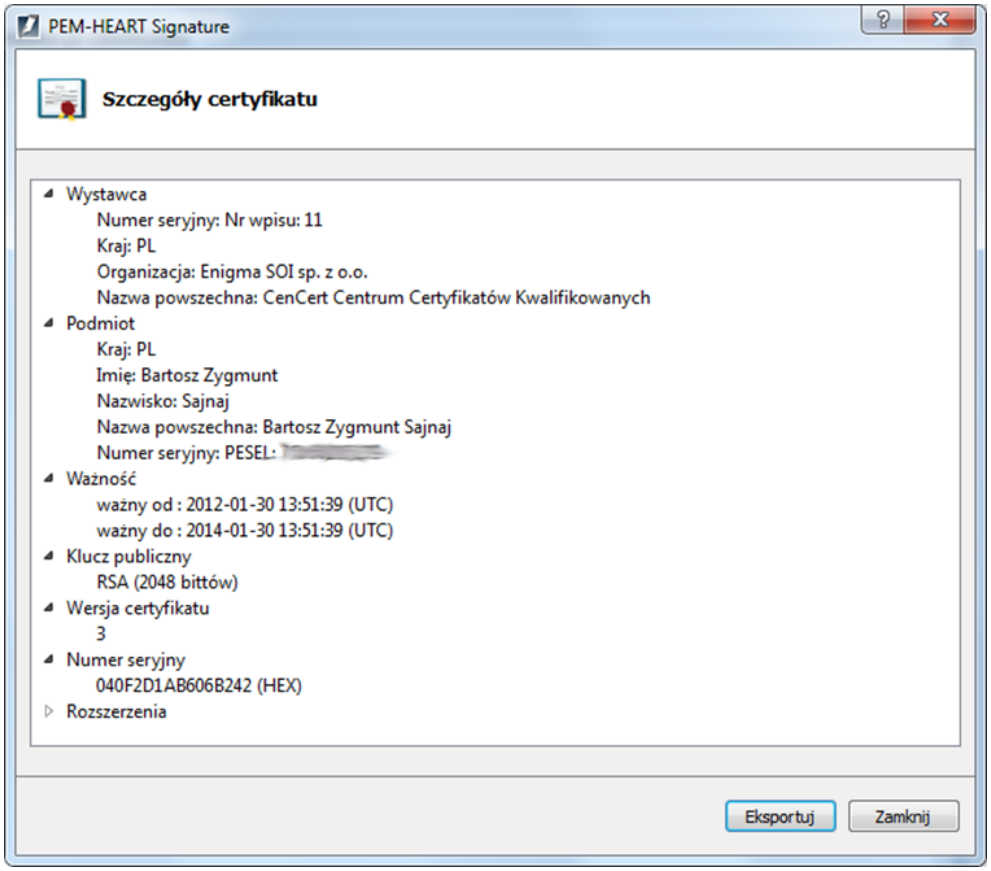
Rysunek 17 Weryfikacja podpisu z zastrzeżeniem jego ważności

Poprzez ikonki oraz menu kontekstowe można znaleźć szczegółowe informacje na temat przebiegu weryfikacji i jego wyników:



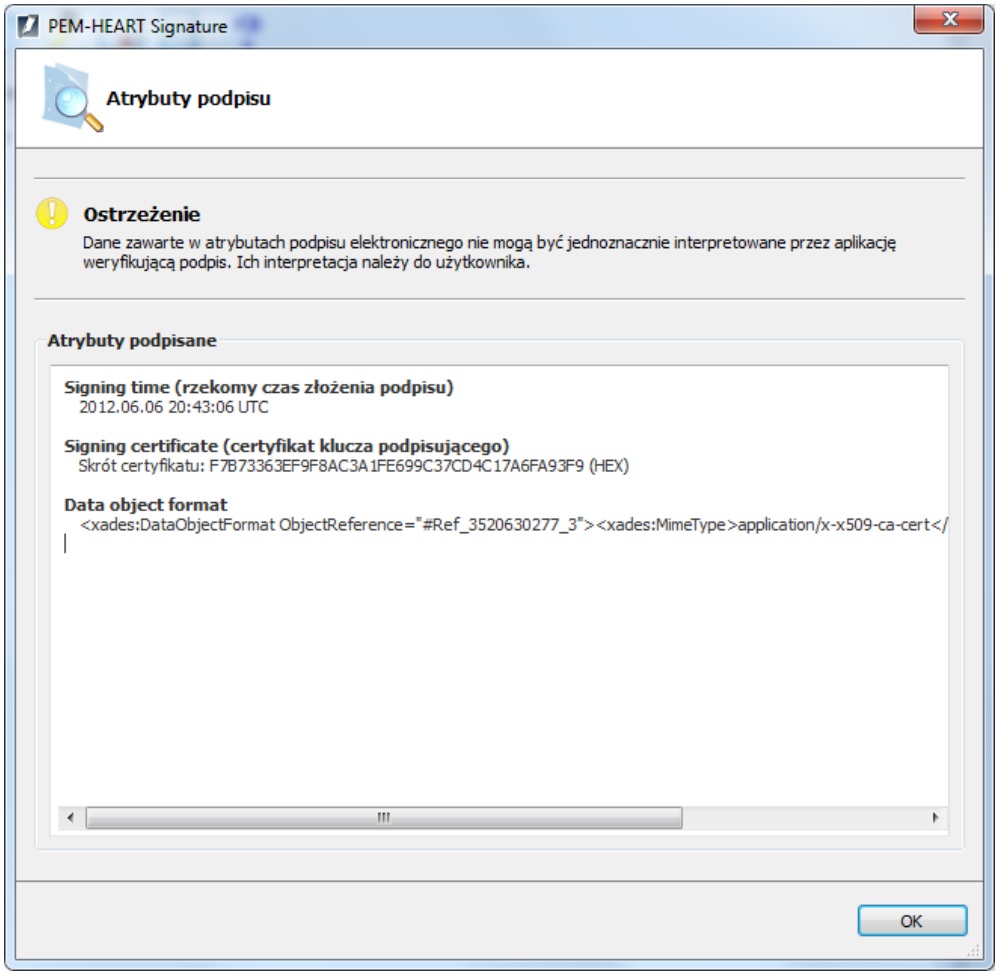
Rysunek 18 Opcje menu kontekstowego

Po wybraniu prezentacji certyfikatu wyświetlane jest okienko z certyfikatem podpisującym:



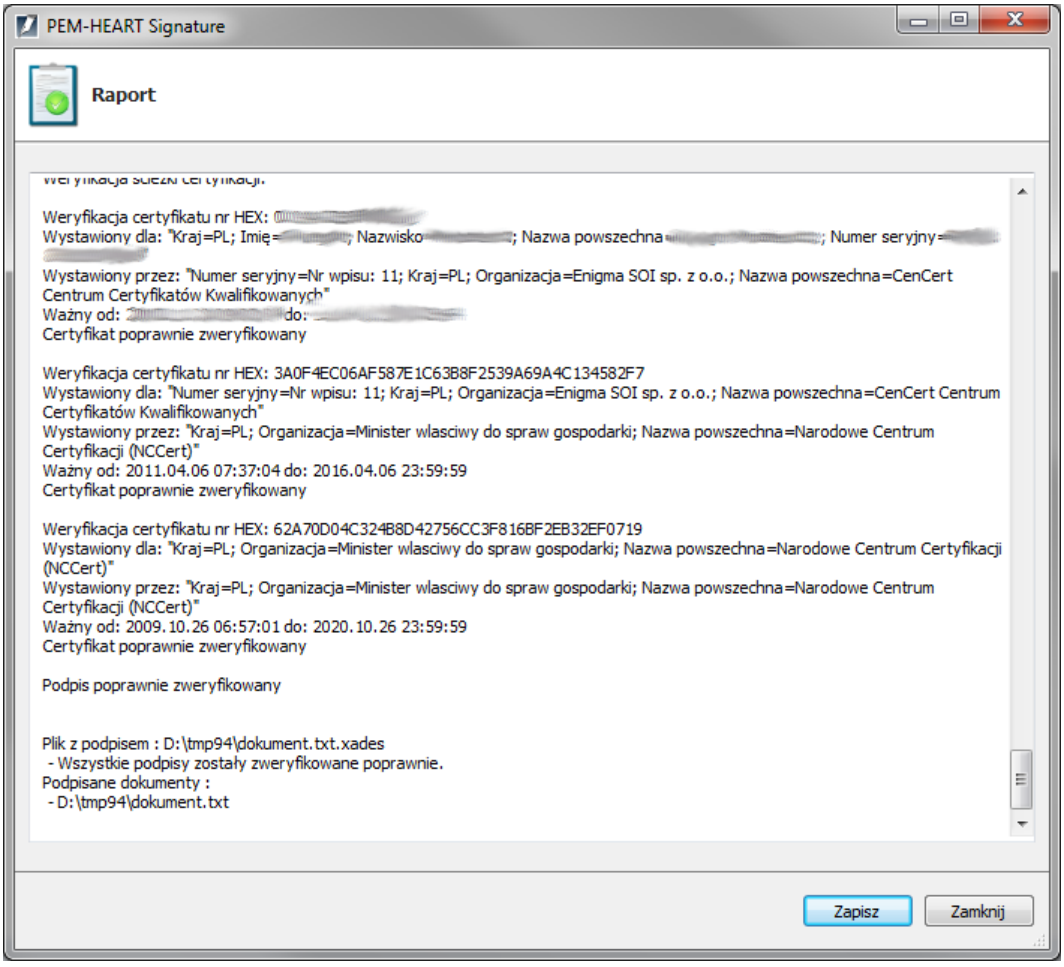
Rysunek 19 Prezentacja certyfikatu

Opcja wyświetlania atrybutów podpisu służy do wyświetlenia okienka z ich listą. Atrybuty są to dodatkowe dane, które są dołączane do podpisu, czyli np. skrót certyfikatu klucza podpisującego, czas złożenia podpisu, skrót z podpisywanego dokumentu i inne.



Rysunek 20 Okno atrybutów podpisu

Poprzez opcje menu kontekstowego *Wyświetl raport przetwarzania* (Rysunek 18) można uzyskać informacje o przebiegu i stanach weryfikacji. Poniżej przedstawiono okno takiego raportu:



Rysunek 21 Raport z weryfikacji

W raporcie umieszczane są takie informacje jak:

- Dane o czasie weryfikacji.
- Prezentacja kompletnej ścieżki certyfikacji wraz z danymi certyfikatów.
- Stan weryfikacji wraz z danymi listy CRL.
- Status weryfikacji.

4.2.1 Weryfikacja plików PDF zabezpieczonych w formacie *PAdES*

Uwaga!

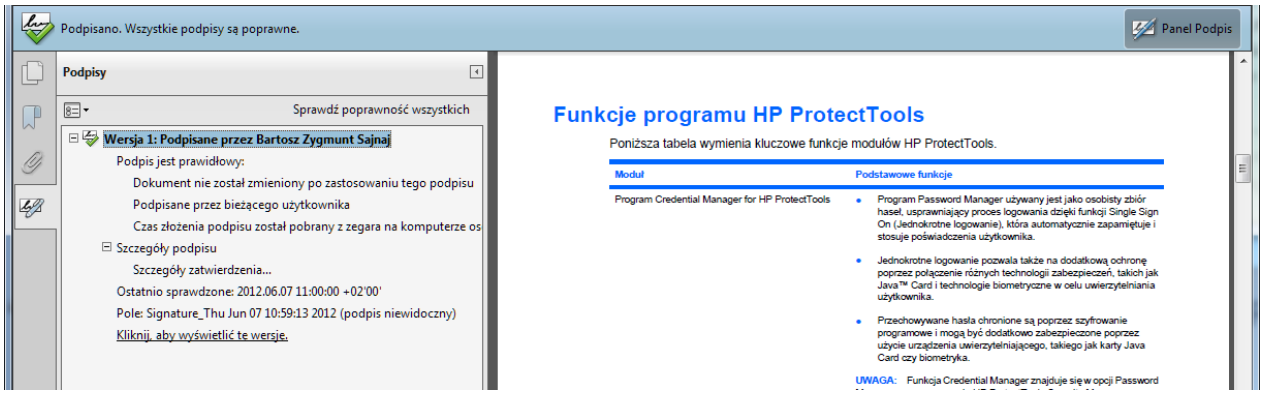
Do prawidłowego wyświetlania informacji o podpisie oraz jego weryfikacji potrzebny *Adobe Acrobat Reader* w wersji 10.x lub nowszej. Wcześniejsze wersje *Adobe Acrobat Reader* nie rozpoznają prawidłowo formatu podpisu.

Aby program *Adobe Acrobat Reader* poprawnie wyświetlał informacje na temat weryfikacji podpisu, należy go skonfigurować zgodnie z instrukcją podaną w rozdziale 8.

Wybór w konfiguracji programu (Rysunek) formatu podpisu *PAdES* jako domyślnego dla plików PDF skutkuje zapisaniem podpisu w tym pliku bez zmiany jego rozszerzenia.

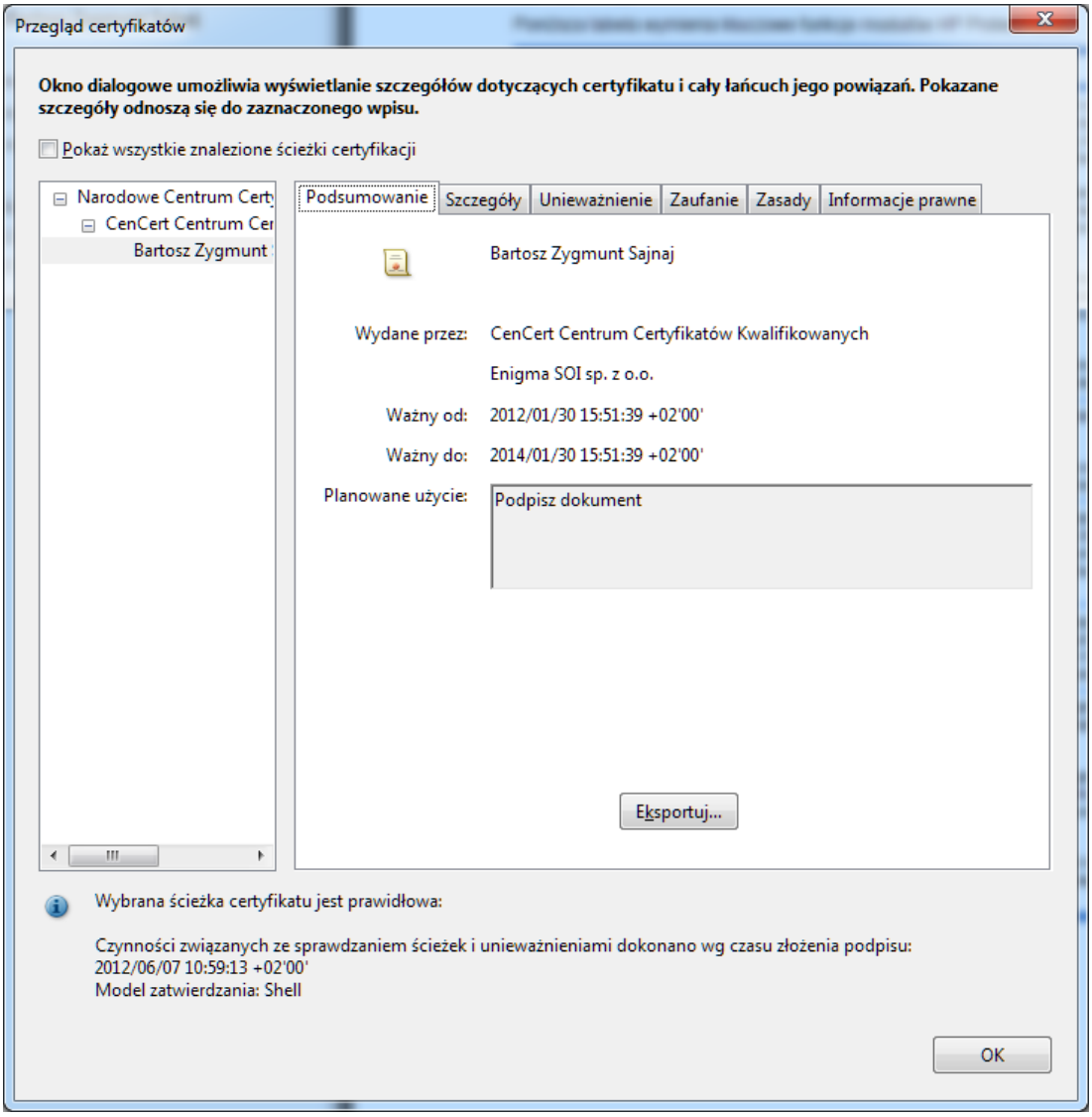
Tak podpisany plik można weryfikować zarówno poprzez oprogramowania ***PEM-HEART Signature*** jak i programy do wyświetlenia tego typu plików. Jednak programy te muszą obsługiwać podpis elektroniczny zgodny z normą ETSI TS 102 778.

Jako przykład można podać wynik otwarcia podpisanego pliku *pdf* w programie *Adobe Acrobat Reader* i po rozwinięciu panelu podpisu zostanie wyświetlona zakładka *Podpisy*, w której przedstawiony będzie wynik weryfikacji.



Rysunek 22 Widok weryfikacji w pliku pdf (*Adobe Acrobat Reader* wersja 10.1.3)

W celu sprawdzenia szczegółów certyfikatu podpisującego należy kliknąć napis *Szczegóły zatwierdzenia* i zostanie otwarte okno jak na rysunku poniżej:



Rysunek 23 Okno podglądu certyfikatu podpisującego

Więcej informacji na temat tego typu podpisu i jego obsługi w dokumentach pdf należy szukać w materiałach udostępnianych przez firmę Adobe.

4.3 Rozszerzanie formy podpisy. Postać LONG i archiwalna

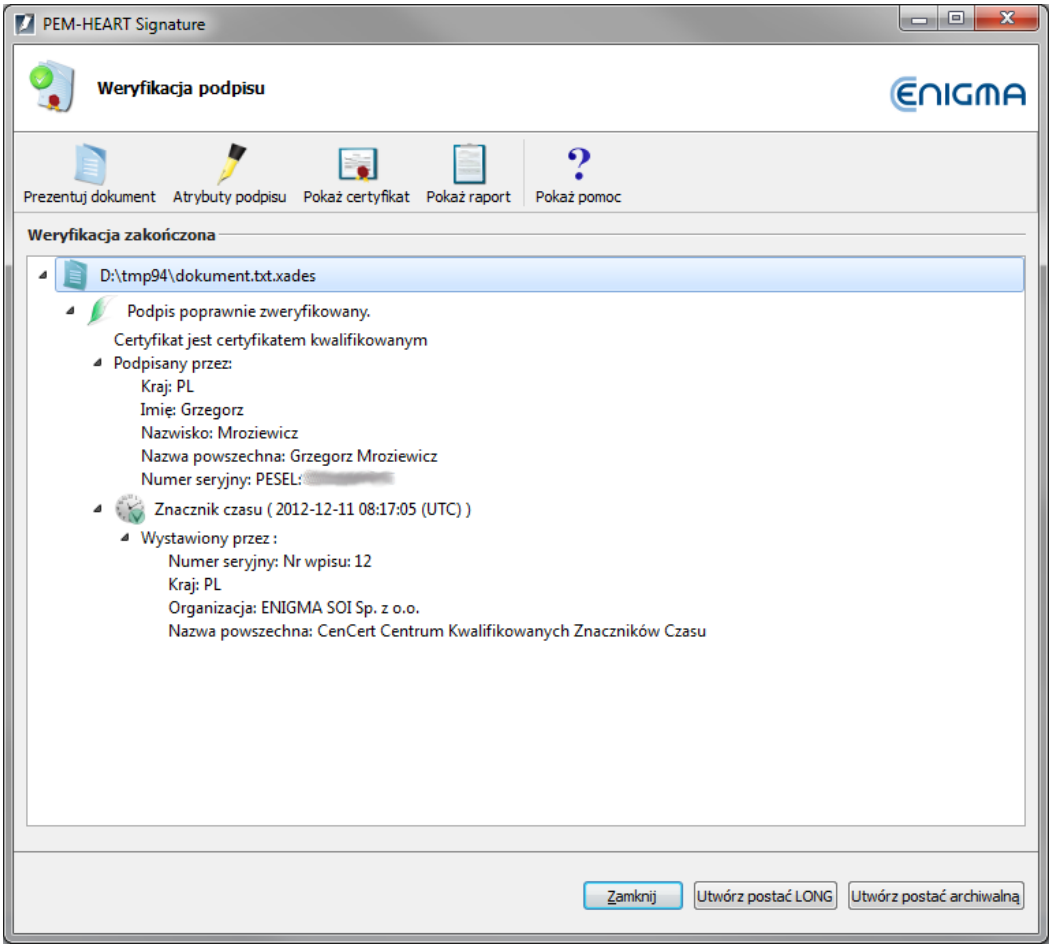
Format LONG podnosi bezpieczeństwo długoterminowego przechowywania podpisanych elektronicznie dokumentów, poprzez umożliwienie weryfikacji podpisu elektronicznego po długim czasie (wiele lat) od jego złożenia. W dokumencie przetworzonym dodawane są wszystkie niezbędne informacje do jego weryfikacji (podpis, znaczniki czasu, listy CRL i/lub OCSP). Taki podpis jest ważny do momentu, gdy najpóźniej złożony pod dokumentem znacznik czasu jest ważny.

Rozszerzanie podpisu do postaci archiwalnej pozwala dodatkowo zabezpieczyć się przed utratą utraty bezpieczeństwa użytych algorytmów kryptograficznych w przyszłości.

Uwaga!

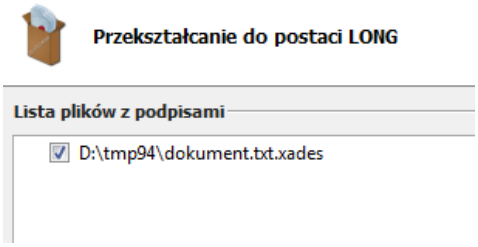
Konwersja jest możliwa tylko w wypadku poprawnej weryfikacji podpisu dokumentu.

Aby przekształcić podpis pliku do formatu LONG należy po weryfikacji dokumentu wybrać przycisk *Utwórz postać LONG*.



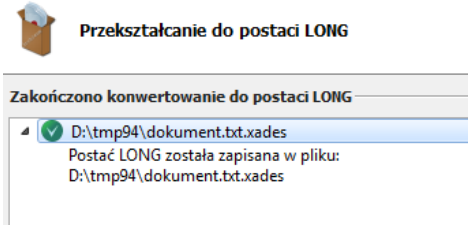
Rysunek 24 Okno po weryfikacji podpisu

Zostanie wyświetlona lista plików, które zostały poddane weryfikacji i na niej można zaznaczyć, które podpisane pliki zostaną przekształcone.



Rysunek 25 Lista plików do przekształcania

Zatwierdzenie listy plików i rozpoczęcie procedury odbywa się za pomocą przycisku *Utwórz postać LONG*. Poniżej przedstawiono fragment okna z wynikiem operacji:



Rysunek 26 Konwersja do formatu LONG

5 Funkcje zaawansowane

Dla przywołania funkcji zaawansowanych programu należy kliknąć napis *Funkcje zaawansowane* w menu głównym programu.

Rysunek 27 Widok opcji zaawansowanych

Każda z funkcji zostanie poniżej opisana poniżej w osobnym rozdziale.

5.1 Dodawanie podpisu

Opcja ta pozwala na dodanie podpisu do już podpisanego pliku np. dokument podpisywany przez jego wszystkich autorów. Każdy dodawany w ten sposób podpis jest równorzędny.

Aby dodać podpis należy wykorzystać systemowe menu kontekstowe dla dokumentu lub z programu użyć przycisku 

.

Operacja dodawania podpisu wykonywana jest tak samo jak składanie podpisu opisanego już we wcześniejszym rozdziale z tym, że lista plików do wyboru jest filtrowana i zawiera tylko dokumenty zawierające podpis (z rozszerzeniami wymienionymi w rozdziale poprzednim [15]).

Kliknięcie na przycisk *Opcje* dostępny podczas wskazywania pliku pozwala na wybranie jedynie formy podpisu (czyli podpisu bez lub ze znacznikiem czasu) z tego względu, że pozostałe opcje są już określone przez format dokumentu, dla którego dodawany jest podpis.

5.2 Kontrasygnata

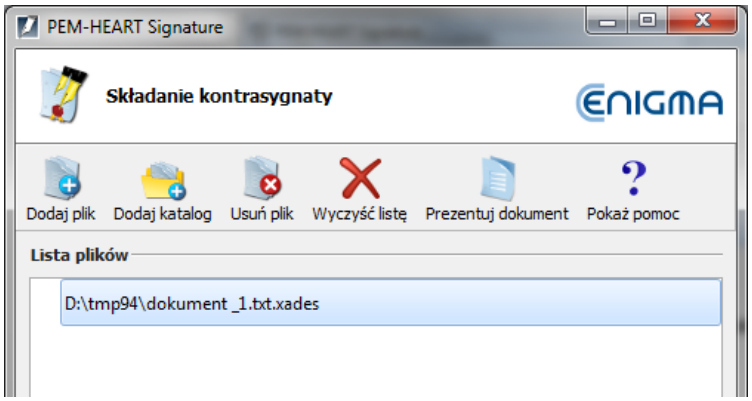
Kontrasygnata jest to dodatkowe złożenie podpisu w dokumencie przez drugą osobę, potwierdzające jego ważność i przenoszące pełną odpowiedzialność prawną na podpisującego.

W programie **PEM-HEART Signature** złożenie kontrasygnaty podpisu odbywa się w podobny sposób jak podpisywanie pliku. Aby ją dodać należy wykorzystać systemowe menu kontekstowe dla dokumentu lub z programu użyć przycisku 

.

Następnie w oknie wskazywania plików należy wybrać dokument, na którym ma być złożona kontrasygnata. Lista widocznych plików jest domyślnie filtrowana i wyświetlane są tylko te zawierające podpisy elektroniczne. Po zatwierdzeniu wybranego pliku w kolejnym kroku programu zostanie zweryfikowana ważność podpisu tego pliku.

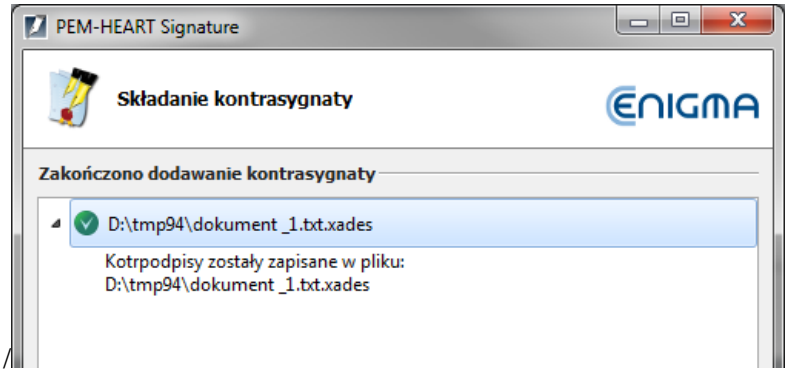
Po weryfikacji podpisu zostanie wyświetlone okno przedstawiające jej wynik. Złożenie kontrasygnaty jest także możliwe w przypadku zakończenia się weryfikacji wynikiem niepomyślnym. Od użytkownika zależy czy złoży podpis pod takim dokumentem.



Rysunek 28 Składanie kontrasygnaty

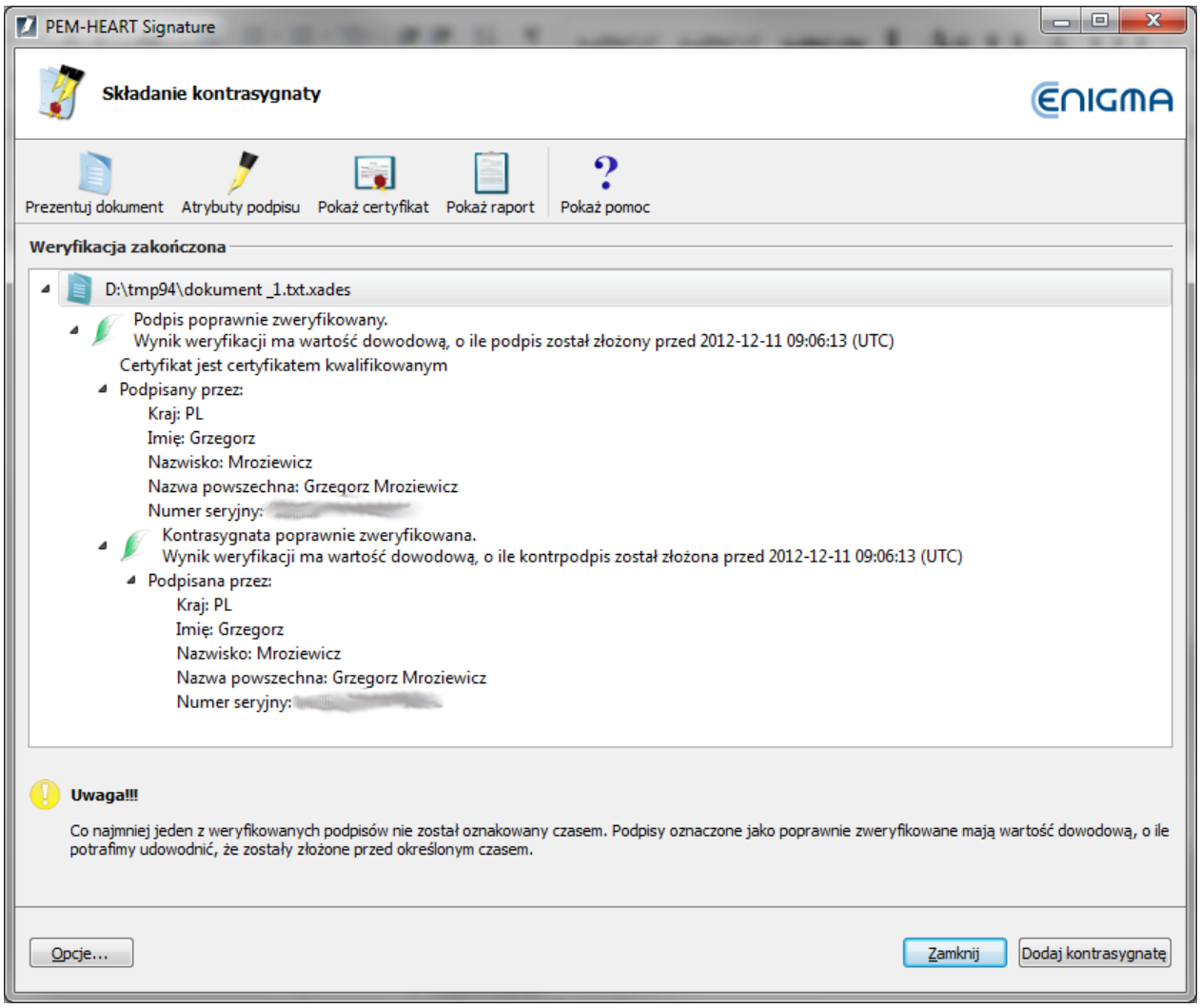
Do złożenia kontrasygnaty należy wybrać przycisk *Dodaj kontrasygnatę* i po jego użyciu dokument zostanie kontrasygnowany.

Szczegóły procesu składania kontrasygnaty można wyświetlić za pomocą menu kontekstowego programu i opcji raportu z przetwarzania.



Rysunek 29 Komunikat o wyniku składania kontrasygnaty

Wynik weryfikacji pliku kontrasygnowanego przedstawiono na rysunku poniżej.



Rysunek 30 Weryfikacja kontrasygnowanego pliku

5.3 Znakowanie czasem

Program umożliwia oznakowanie czasem już istniejącego w dokumencie podpisu elektronicznego. Operacja ta polega na dodaniu nowego znacznika czasu do każdego z podpisów występujących w dokumencie. Znaczniki czasu są pobierane z serwera datowania **CenCert**.

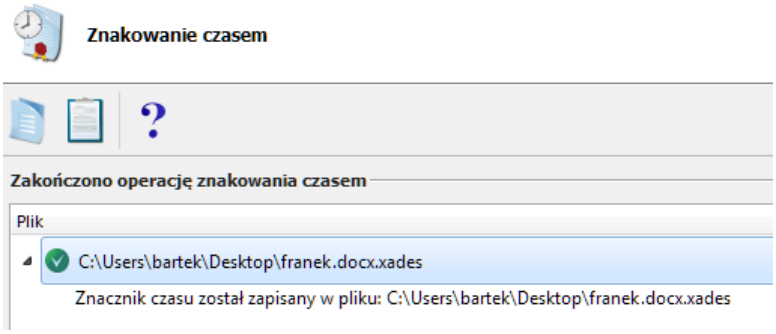
Dodanie znacznika czasu do dokumentu gwarantuje, że dokument elektroniczny istniał w momencie oznaczania go czasem oraz stanowi dowód, iż od tego momentu dokument nie był zmodyfikowany.

Uwaga!

W wersji podstawowej pakietu istnieje limit 2 darmowych znaczników czasu na dzień do wykorzystania. Aby móc korzystać z większej ilości należy zamówić

Dla dodania znacznika należy użyć systemowego menu kontekstowego lub użyć przycisku 

z menu głównego. Po wyborze dokumentu (lub wielu dokumentów), którego podpisy mają być oznakowane i zatwierdzeniu operacji, znacznik czasu jest pobierany z serwera datowania i dodawany jest następnie do dokumentu.



Rysunek 31 Zakończenie operacji dodawania znacznika czasu

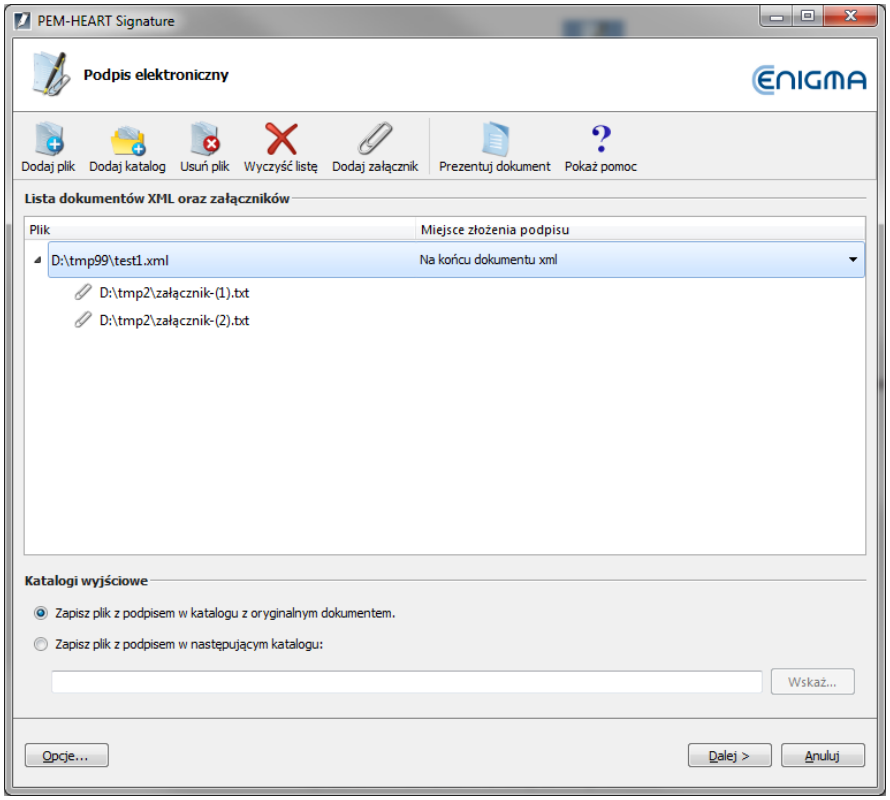
Szczegóły procesu można wyświetlić za pomocą menu kontekstowego programu i opcji raportu z przetwarzania.

5.4 Podpisywanie dokumentu XML z załącznikami

Program umożliwia również podpisywanie plików XML, wraz z wyborem miejsca (*węzła XML*) w strukturze dokumentu, w której ma zostać umieszczony podpis. Opcja podpisywanie dokumentów XML dostępna jest poprzez przycisk 

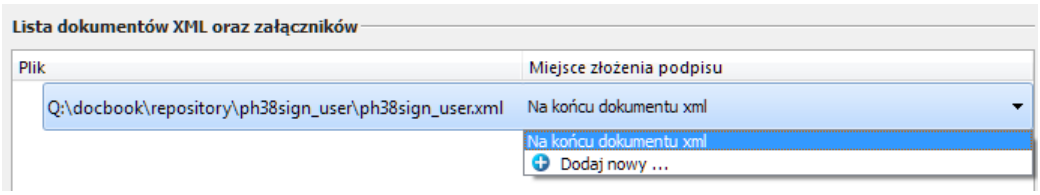
z menu funkcji zaawansowanych.

Do wybranego dokumentu XML można dołączać załączniki (pliki graficzne, inne dokumenty XML, pliki tekstowe, itp.).



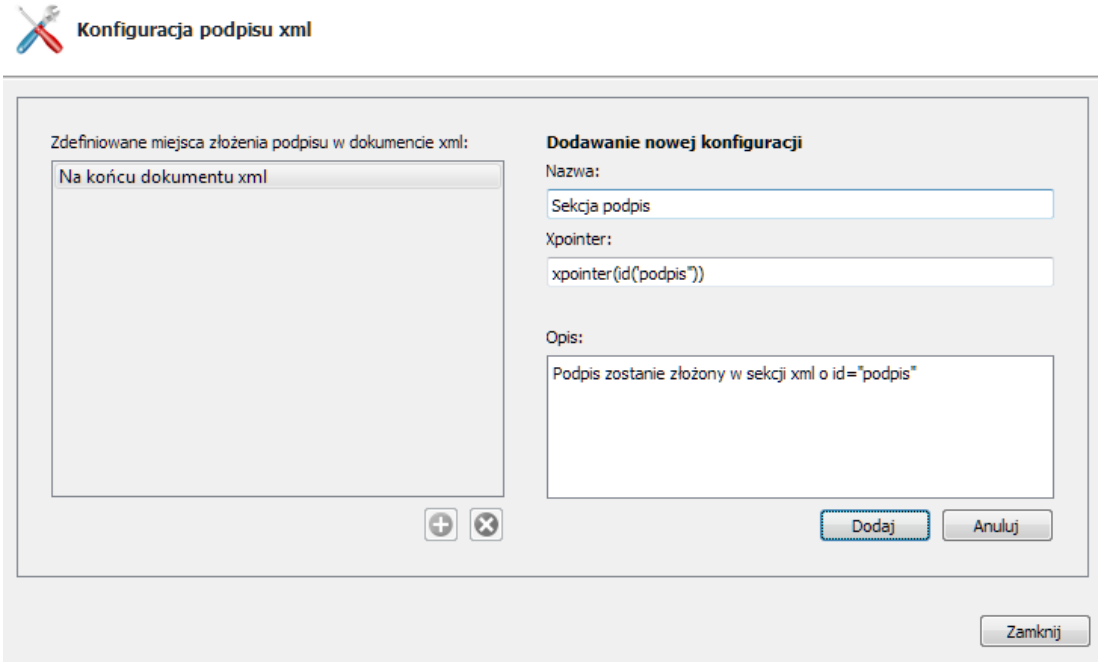
Rysunek 32 Plik XML z dodanymi załącznikami

Kolejnym krokiem, zanim zostanie złożony podpis, powinno być wskazanie z listy miejsca w strukturze dokumentu XML, w którym zostanie umieszczony podpis.



Rysunek 33

Program dostarczany jest z domyślną konfiguracją pozwalającą umieszczać podpisy XML na końcu dokumentu. W przypadku gdy istnieje potrzeba umieszczenia podpisu w innym miejscu struktury XML, należy najpierw odpowiednio skonfigurować nowe miejsce składania podpisu. Wybranie pozycji *Dodaj nowy* spowoduje wyświetlenie okna konfiguracji miejsca składania podpisu.



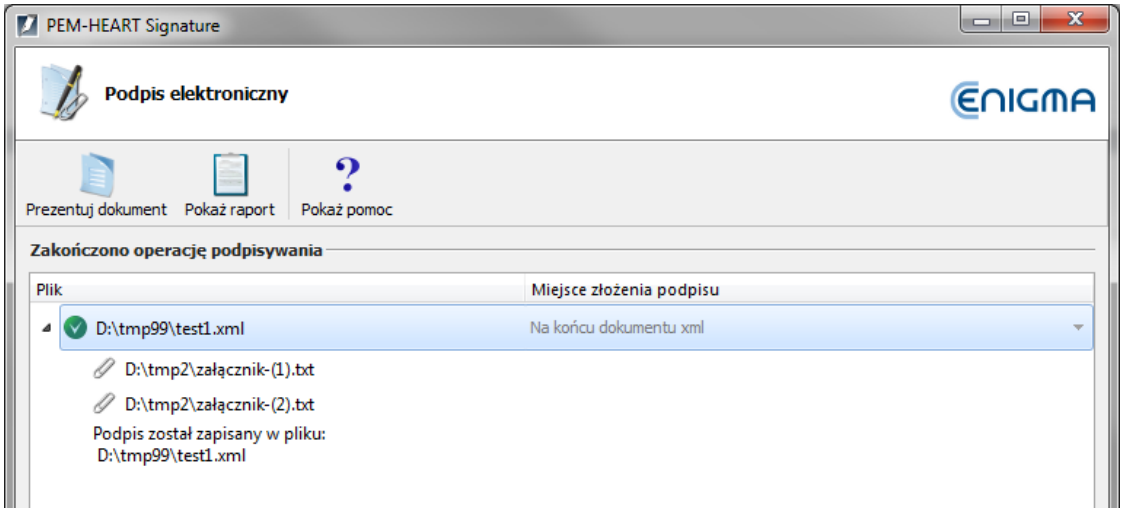
Rysunek 34 Konfiguracja miejsca składania podpisu

W celu definiowania nowej pozycji należy kliknąć przycisk  . W nowej konfiguracji należy ustalić jej nazwę wyświetlaną na liście wyboru, podać strukturę *xpointer* oraz zamieścić opis definiowanej konfiguracji (pomocny w przypadku tworzenia skomplikowanych deklaracji).

Strukturę *xpointer* określa się w postaci: `xpointer([wskazanie na węzeł XML])`. Dostępne formy określania tego miejsca opisuje dokumentacja języka *XML Pointer Language* (*XPointer*) dostępna m.in. na stronach http://www.w3.org/TR/WD-xptr.

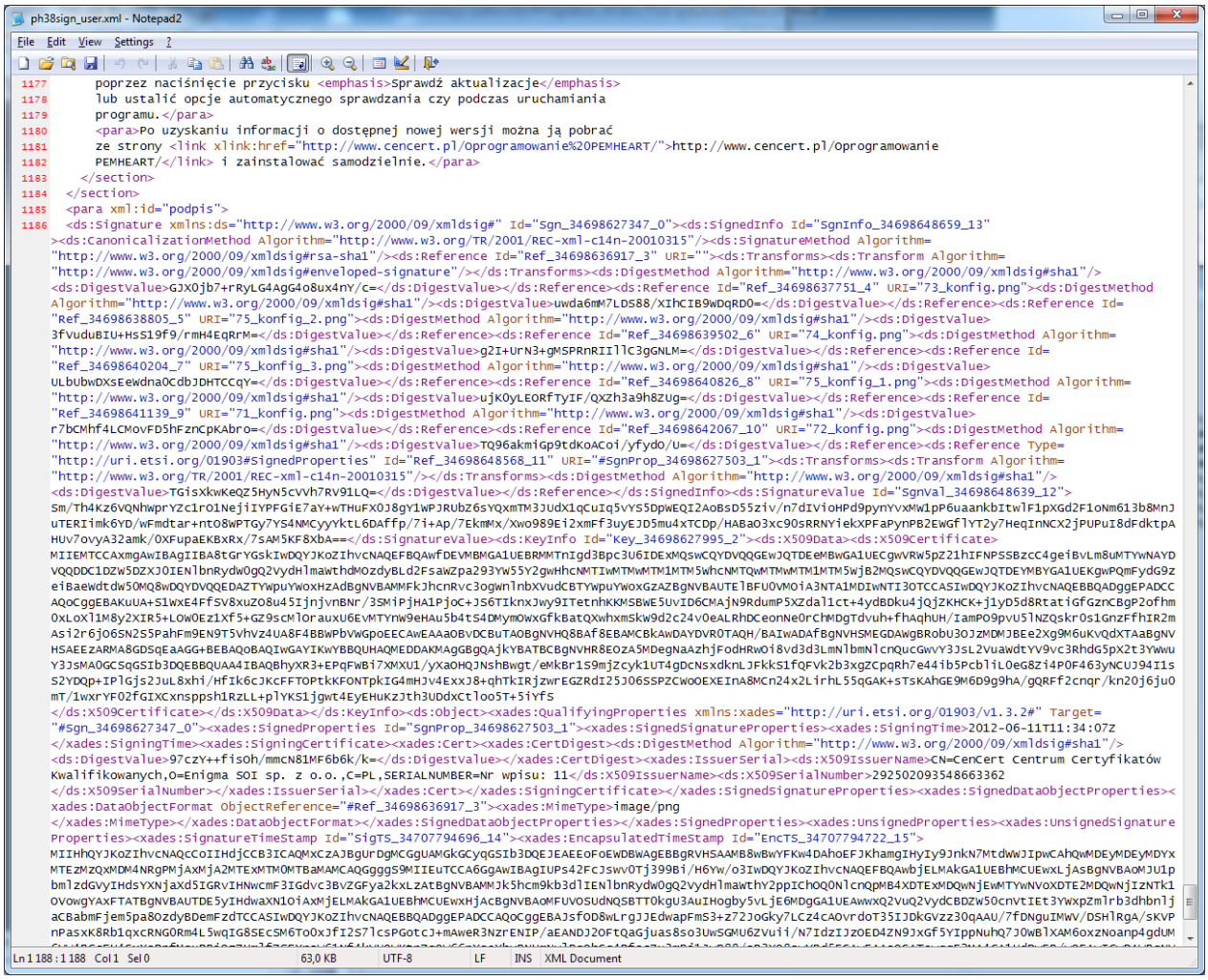
W przedstawionym powyżej na rysunku przykładzie zostanie podpisany dokument XML, a podpis zostanie umieszczony w części o atrybucie *id* o nazwie *podpis*.

Po zakończeniu podpisywania zostanie wyświetlone okno podsumowania:



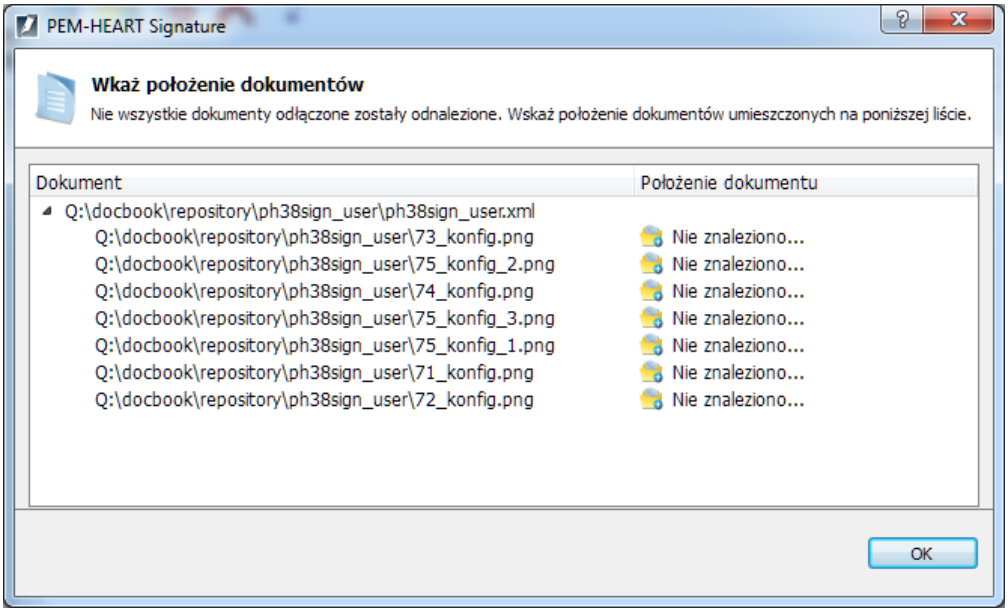
Rysunek 35 Wynik podpisania pliku XML z załącznikami

Szczegóły procesu można wyświetlić za pomocą raportu z przetwarzania. Składanie podpisu nie zmienia rozszerzenia pliku XML ani jego struktury. Poniżej przedstawiono przykładowy plik XML z umieszczonym podpisem.



Rysunek 36 Przykładowy podpis wpisany w strukturę pliku XML

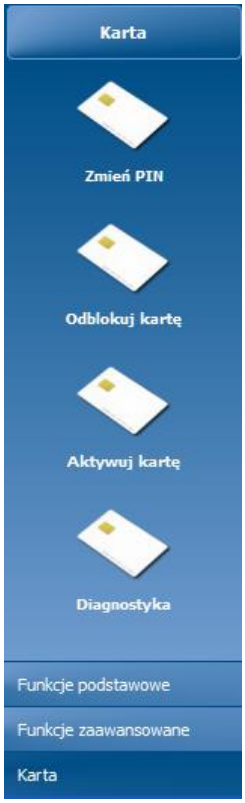
Podczas weryfikacji pliku XML z załącznikami należy wskazać (poprzez menu kontekstowe) ich położenie, jeśli nie znajdują się w tym samym katalogu, w którym jest weryfikowany plik.



Rysunek 37 Wskazanie położenia załączników do podpisanego pliku XML

6 Obsługa kart kryptograficznych

Do obsługi kart kryptograficznych służy zakładka *Karta* dostępna w oknie głównym programu.

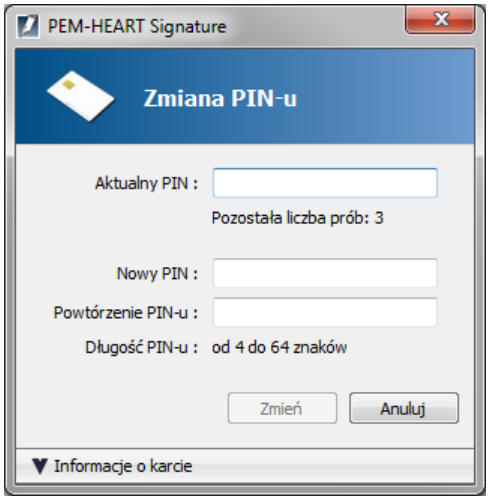


Rysunek 38 Sekcja *Karty* zakładki okna głównego

Opcje obsługi kart kryptograficznych zostaną opisane w kolejnych podrozdziałach.

6.1 Zmiana kodu PIN

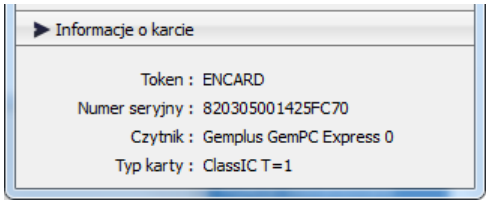
Po kliknięciu na przycisk *Zmień PIN* wyświetlane jest okno, w którym można dokonać zmiany kodu PIN dla karty umieszczonej w czytniku.



Rysunek 39 Okno zmiany kody PIN

Do zmiany kodu należy podać poprawny aktualny kod oraz dwa razy wpisać nowy kod. Kod może zawierać od 4 do 16 liter, cyfr oraz znaków specjalnych.

Można wyświetlić również informacje o karcie, poprzez kliknięcie paska napisu:



Rysunek 40 Informacje o karcie

6.2 Odblokowanie karty

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

Rysunek 41 Odblokowanie karty

Po poprawnym podaniu danych kod PIN jest ponownie aktywny i możliwe jest dalsze korzystanie z karty.

Uwaga!

Dostępne są tylko 3 próby odblokowywania karty za pomocą kodu PUK. Po 3 błędnie podanym kodzie PUK karta jest blokowana w sposób uniemożliwiający dalsze użycie. O tym fakcie należy niezwłocznie poinformować CPR w celu ustalenia dalszej procedury.

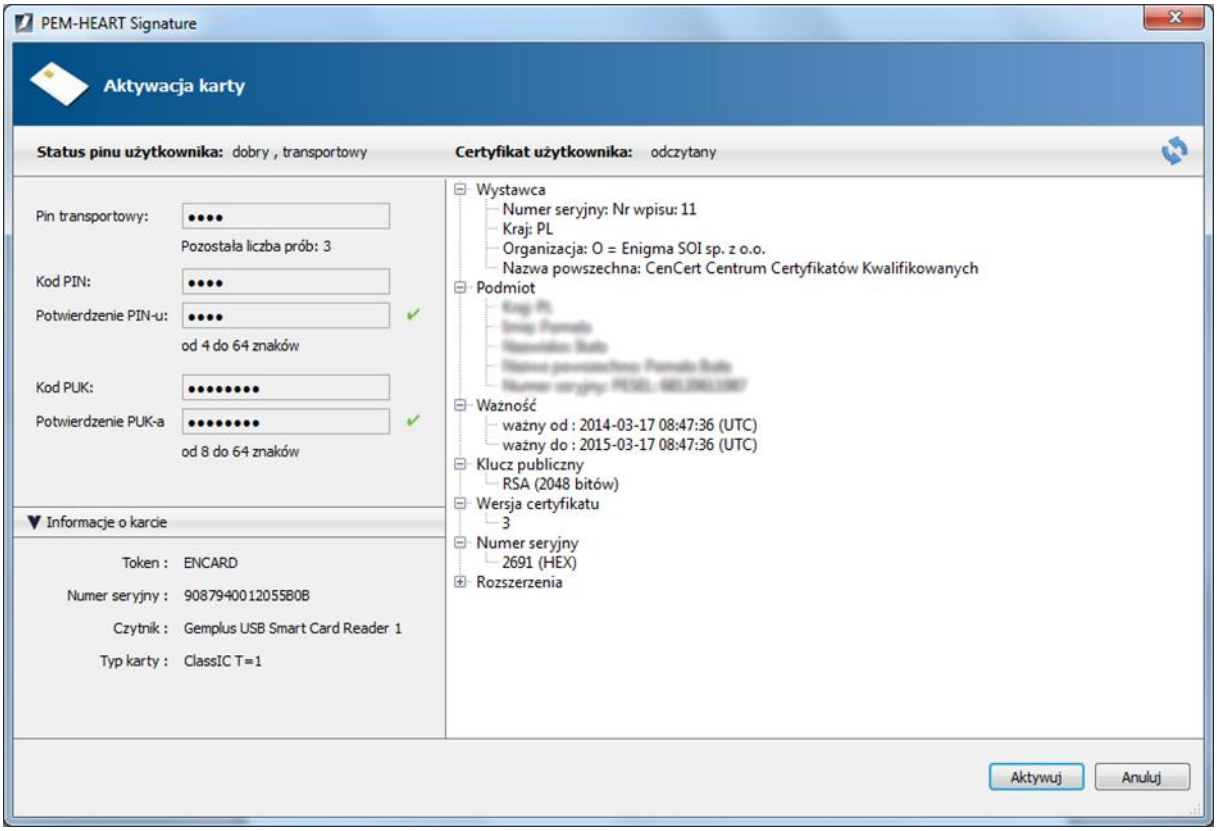
6.3 Aktywacja karty

Aktywacja karty odbywa się w momencie, gdy użytkownik będzie miał zarówno tą kartę jak i kod transportowy do niej. Kod transportowy użytkownik otrzymuje w emailu poprzez link do serwisu www.

Proces aktywacji jest spersonalizowany dla konkretnego modelu karty i został opisany poniżej.

6.3.1 Aktywacja karty ClassIC T=1

Kartę należy umieścić w czytniku. Następnie w zakładce *Karta* w okienku *Aktywacja karty* należy wpisać w odpowiednich polach otrzymany kod transportowy oraz określić kody PIN oraz PUK.

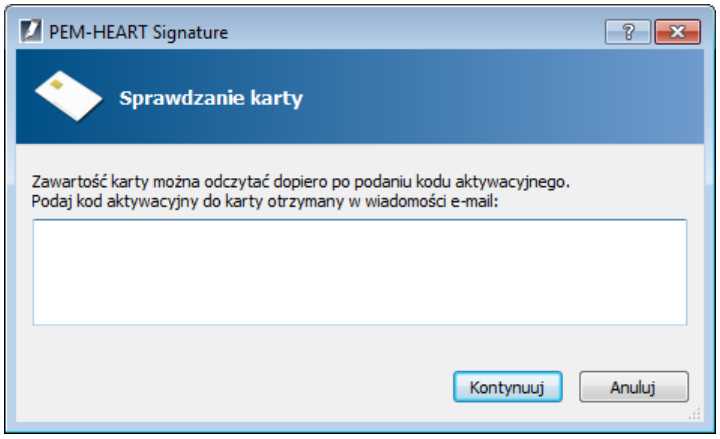


Rysunek 42 Aktywacja karty ClassIC T=1

Po wykonaniu operacji aktywacji poprzez przycisk *Aktywuj* karta jest gotowa do użytkowania.

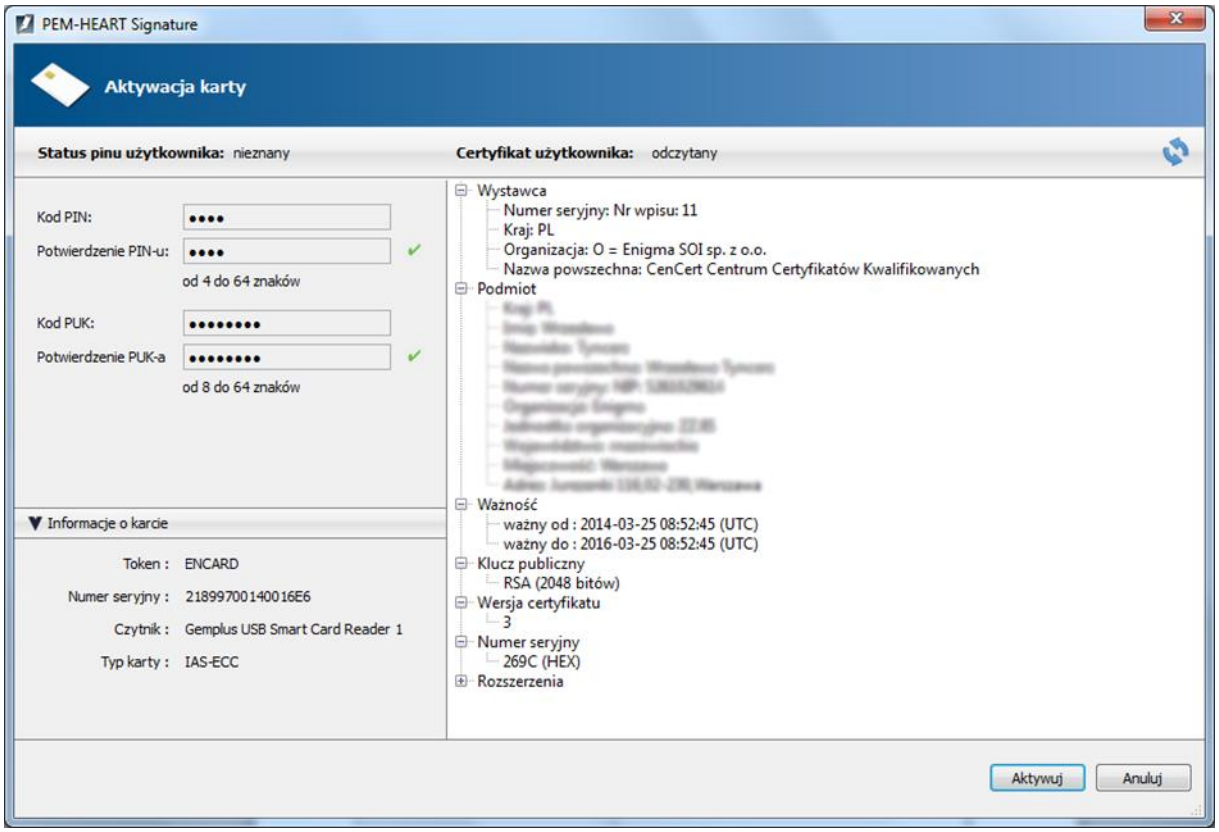
6.3.2 Aktywacja karty IAS-ECC

Kartę należy umieścić w czytniku. Następnie w zakładce *Karta* w okienku *Aktywacja karty* należy wprowadzić kod aktywacyjny otrzymany w wiadomości email.



Rysunek 43 Aktywacja karty IAS-ECC

W oknie *Aktywacja karty* należy ustalić w odpowiednich polach kody PIN oraz PUK, a następnie zatwierdzić operację przyciskiem *Aktywuj*.

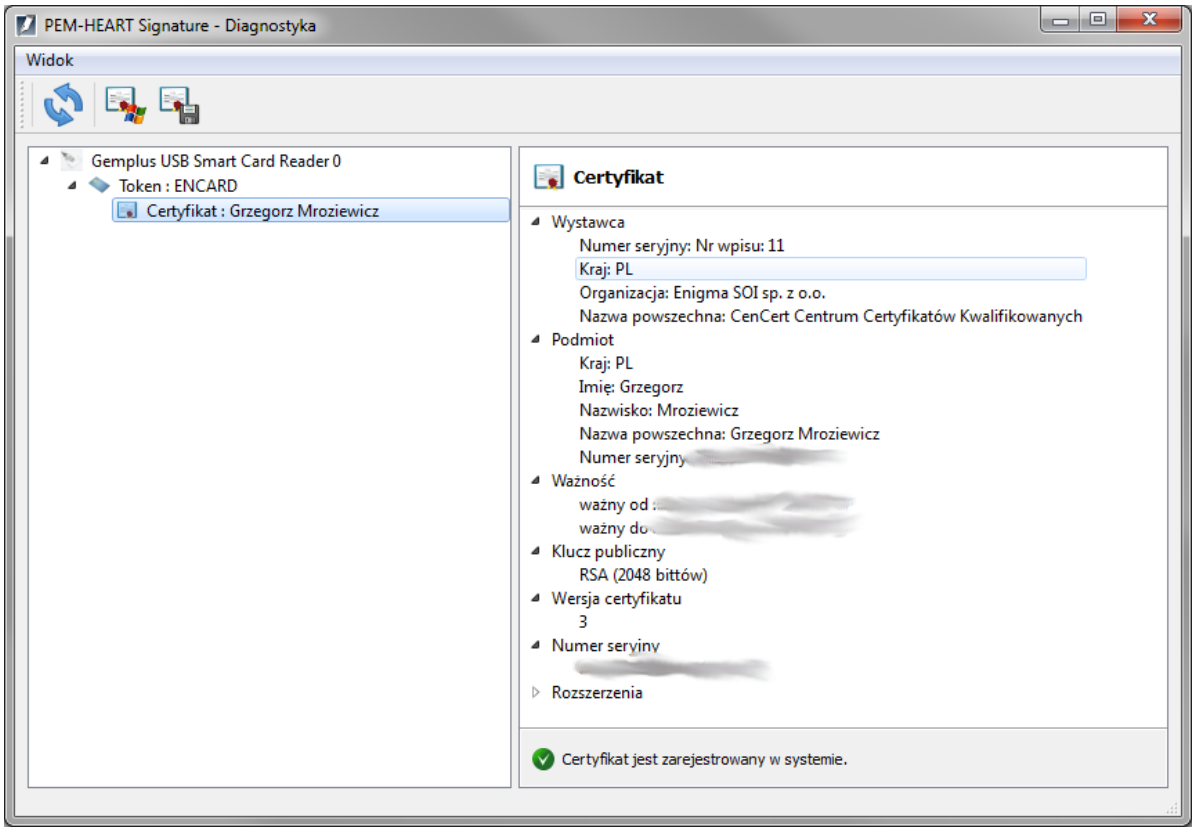


Rysunek 44 Aktywacja karty IAS-ECC

Po wykonaniu operacji karta jest gotowa do użytkowania.

6.4 Diagnostyka

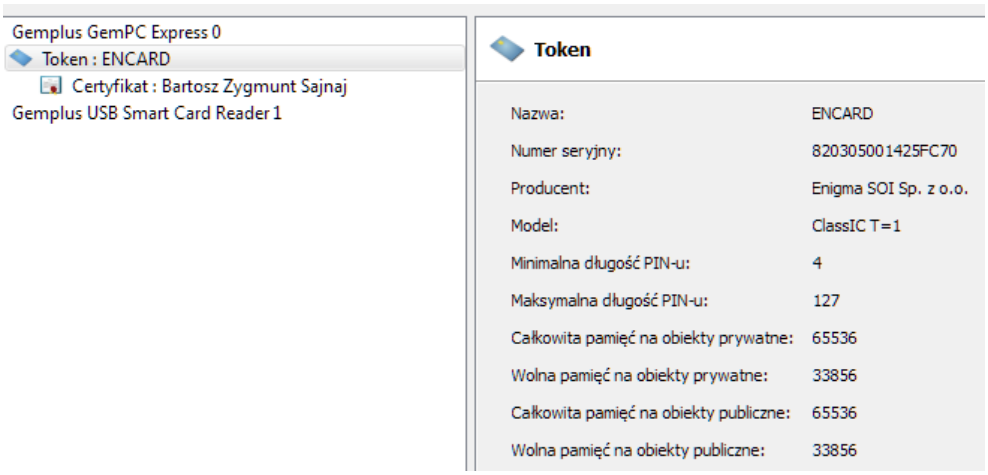
W przypadku gdy w systemie jest dostępnych więcej czytników oraz kart pomocna jest pozycje *Diagnostyka* w sekcji obsługi kart. Po jej wyborze zostanie wyświetlona lista czytników w systemie oraz informacje na temat włożonych w nich kart.



Rysunek 45 Dane certyfikatu w zakładce diagnostyki

Można uzyskać informacje na temat obiektów na kartach: tokenów oraz certyfikatów. Po zaznaczeniu certyfikatu jest wyświetlana jego struktura i dane. Za pomocą przycisków menu można umieścić certyfikat w systemowym magazynie certyfikatów lub zapisać go do pliku.

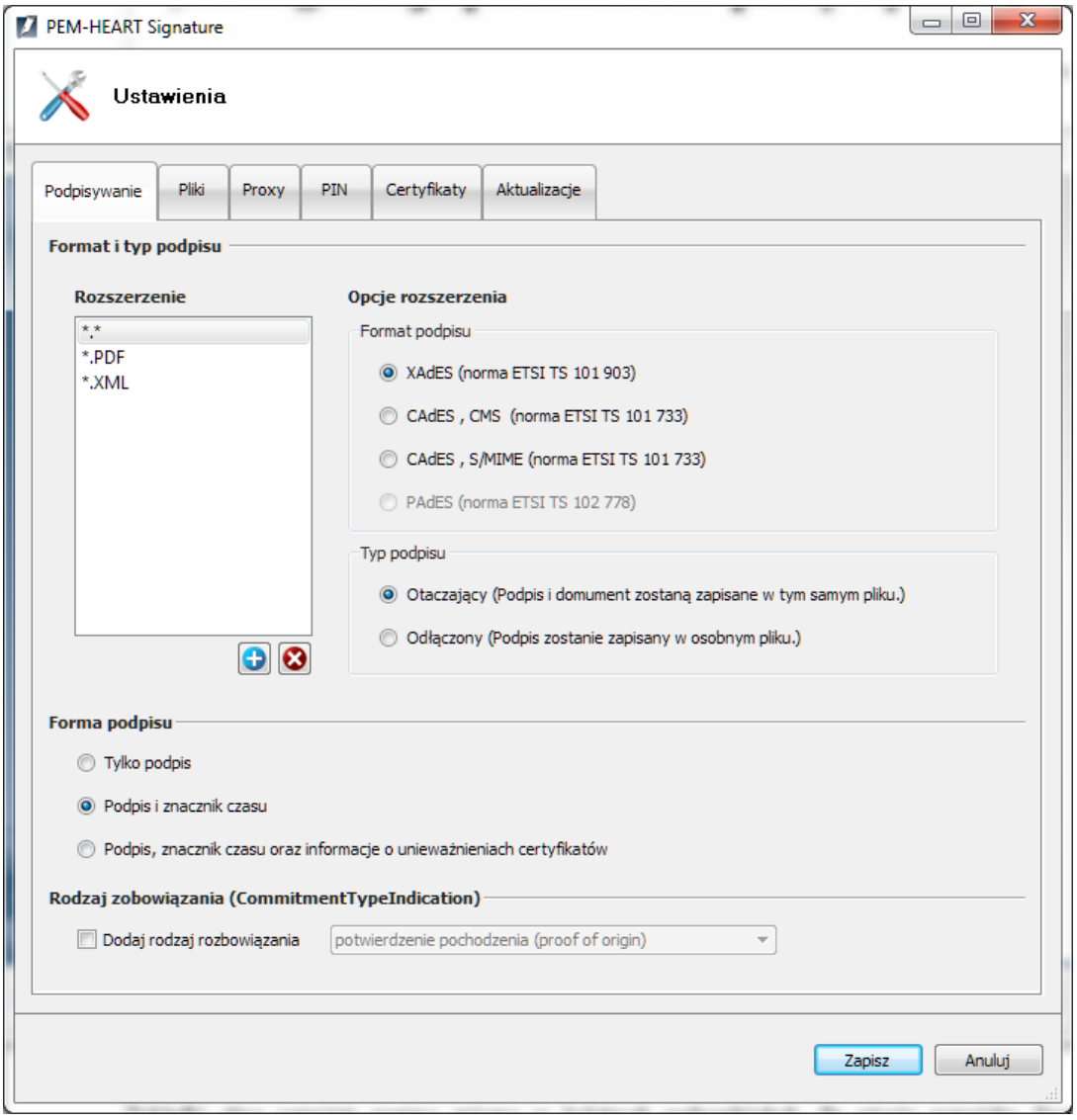
Po zaznaczeniu na liście tokena wyświetlane są podstawowe informacje o nim:



Rysunek 46 Dane na temat tokena

7 Konfiguracja parametrów pracy aplikacji

Do konfiguracji parametrów pracy aplikacji służy przycisk *Ustawienia* w oknie głównym aplikacji. Po jego użyciu zostanie wyświetlone okno jak na rysunku poniżej:



Rysunek 47 Okno ustawień programu

Zakładki okna ustawień zostaną opisane w kolejnych podrozdziałach. Po użyciu przycisku *Zapisz* opcje są zapamiętywane i traktowane są, jako domyślne.

7.1 Podpisywanie

Widok tej zakładki prezentowany jest po wyświetleniu okna ustawień. W programie możliwe jest zdefiniowane i wykonanie następujących parametrów podpisu:

- Format podpisu - rodzaj standardu użyty do zapisu dokumentu zawierającego podpis elektroniczny.
  - **XAdES** (norma ETSI TS 101 903) - *XML Advanced Electronic Signatures (XAdES).*

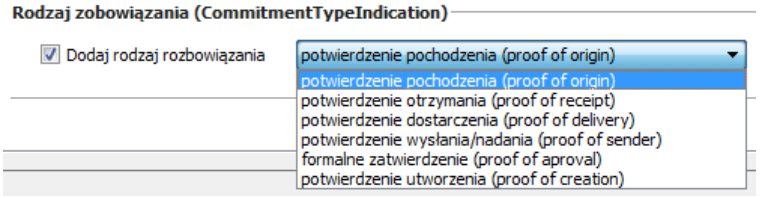
- **CAdES**, CMS (norma ETSI TS 101 733) - *CMS Advanced Electronic Signatures (CAdES)*.
- **CAdES**, S/MIME (norma ETSI TS 101 733) - rodzaj standardu CMS zgodny ze specyfikacją S/MIME.
- **PAdES** (norma ETSI TS 102 778) - *PDF Advanced Electronic Signatures;* natywne podpisywanie plików PDF – opcja ta jest dostępna tylko dla plików *pdf*, równocześnie wybór tej opcji określa stosowania typu podpisu zapisywanego w pliku.

- Typ podpisu - określa gdzie ma być umieszczony podpis:
  - *Otaczający* - podpis i dokument zostaną zapisane w tym samym pliku.
  - *Odłączony* - podpis zostanie zapisany w osobnym pliku.

W tabelce *Rozszerzenia* można określać własne skojarzenia formatów i typów podpisu dla określonych plików. Za pomocą ikonki  można dodać rozszerzenie plików, a następnie przypisać mu format i typ podpisu. Zatwierdzenie tak zdefiniowanego schematu dokonuje się za pomocą przycisku *Zapisz*. Przycisk  służy do skasowania zaznaczonej pozycji z listy skojarzeń. Predefiniowanych pozycji *.*, *.*PDF* oraz *.*XML* nie można skasować.

- Forma podpisu określa, jakie dane ma zawierać podpis:
  - *Tylko podpis* - zostanie wykonany tylko podpis dokumentu.
  - *Podpis i znacznik czasu* - zostanie wykonany zarówno podpis, jak i znacznik czasu. Znacznik ten gwarantuje, że dokument elektroniczny istniał w momencie oznaczania go czasem oraz stanowi dowód, iż od tego momentu dokument nie był zmodyfikowany.
  - *Podpis, znacznik czasu oraz informacje o unieważnieniach certyfikatów* – Do podpisu i znacznika zostanie dodana najnowsza lista CRL.

- Rodzaj zobowiązania:
  - Po zaznaczeniu tej opcji zostanie udostępniona lista typów zobowiązań, spośród których należy dokonać wyboru:



Rysunek 48 Opcje rodzaju zobowiązania

Opcje te mają za zadanie określić rodzaj składanego podpisu, ponieważ nie zawsze musi to być jednoznaczne z podpisaniem treści dokumentu. Rodzaje zobowiązań zostały określone w specyfikacji *ETSI TS 101 733*.

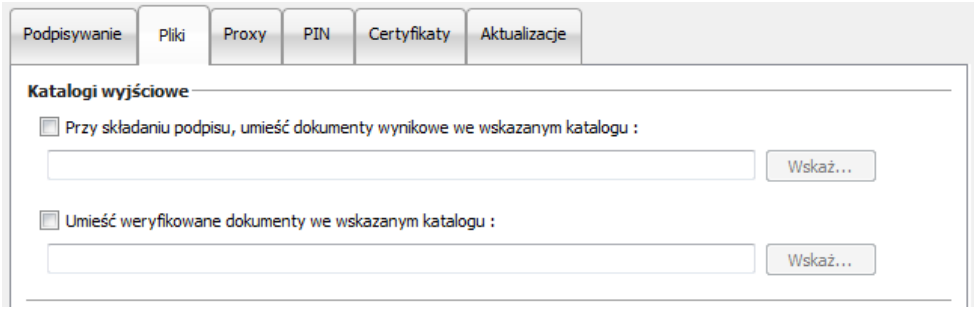
- potwierdzenie pochodzenia (*proof of origin*) – osoba podpisująca potwierdza, że utworzyła, zatwierdziła i wysłała (przeznaczyła do publikacji) podpisany dokument lub dane;
- potwierdzenie otrzymania (*proof of receipt*) – osoba podpisująca potwierdza otrzymanie podpisywanych danych;
- potwierdzenie dostarczenia (*proof of delivery*) – oznacza, że firma generująca tego rodzaju potwierdzenie (ang. *Trusted Service Provider*) dostarczyła podpisane dane do miejsca, w którym adresat może je odebrać;

- potwierdzenie wysłania/nadania (*proof of sender*) – oznacza, że osoba podpisująca dokument przesłała go (nie oznacza to jednak, że go utworzyła);
- potwierdzenie zaakceptowania (*proof of aproval*) – oznacza, że podpisujący zatwierdził treść dokumentu;
- potwierdzenie utworzenia (*proof of creation*) – oznacza, że podpisujący utworzył dokument (ale nie zatwierdzał go, ani nie wysłał/nadał).

Do opcji podpisywania jest także dostęp podczas składania podpisu. W oknie wyboru dokumentów znajduję się przycisk *Opcje*, w którym można ustalić opcje ważne tylko podczas bieżącej operacji składania podpisu.

7.2 Pliki

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



Rysunek 49 Konfiguracja katalogów wyjściowych

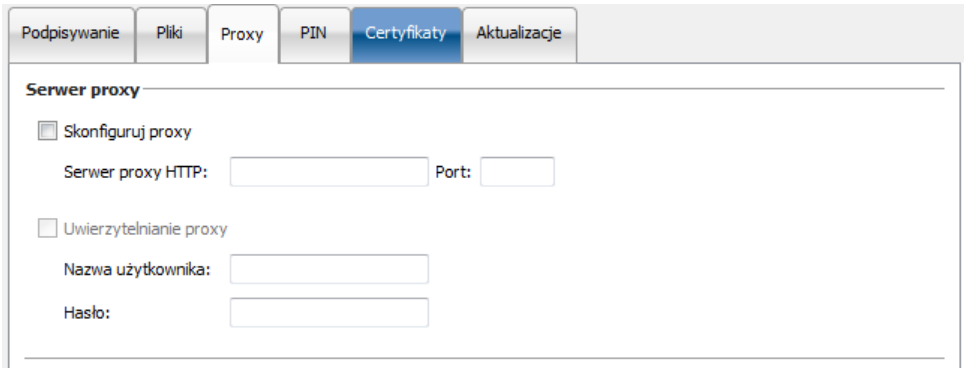
Aby zdefiniować katalog należy zaznaczyć pole przed opisem opcji, zostanie wtedy aktywowany przycisk *Wskaż*, za pomocą którego można wskazać dany katalog w systemie plików.

Po ustaleniu tych opcji ich wartości będą automatycznie wpisywane w okienkach wskazywania dokumentów podczas podpisywania lub weryfikacji w sekcjach opcji umieszczania plików wyjściowych.

7.3 Proxy

W konfiguracji możliwe jest też określanie serwera *proxy* dla usług korzystających z tej usługi np. dla serwera datowania, OCSP czy pobierania list CRL. Należy wypełnić wszystkie pola obowiązkowe dla danego serwera *proxy*.

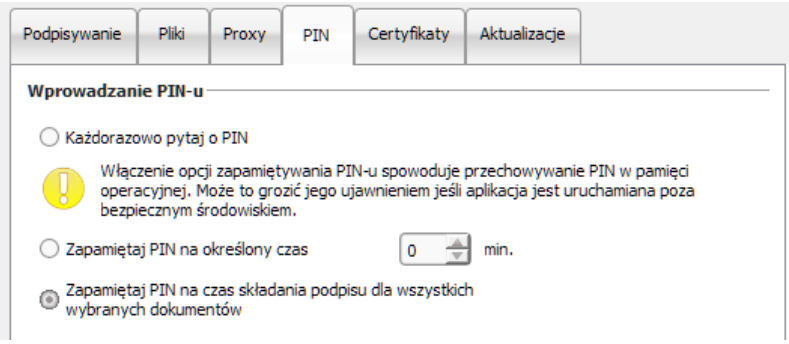
Aktywacja opcji dokonywana jest po zaznaczenia pola wyboru *Skonfiguruj proxy*.



Rysunek 50 Opcje zakładki *Serwer proxy*

7.4 PIN

Zakładka PIN służy do określenia postępowania z wymaganiem podawania kodu PIN podczas odczytu kluczy kryptograficznych z karty. Możliwe jest ustalenie, że kod będzie podawany zawsze dla każdego pojedynczego dokumentu albo też będzie zapisywany w pamięci komputera na określony zakres czasu lub dla wszystkich wybranych (podczas dodawania ich do podpisu) dokumentów.

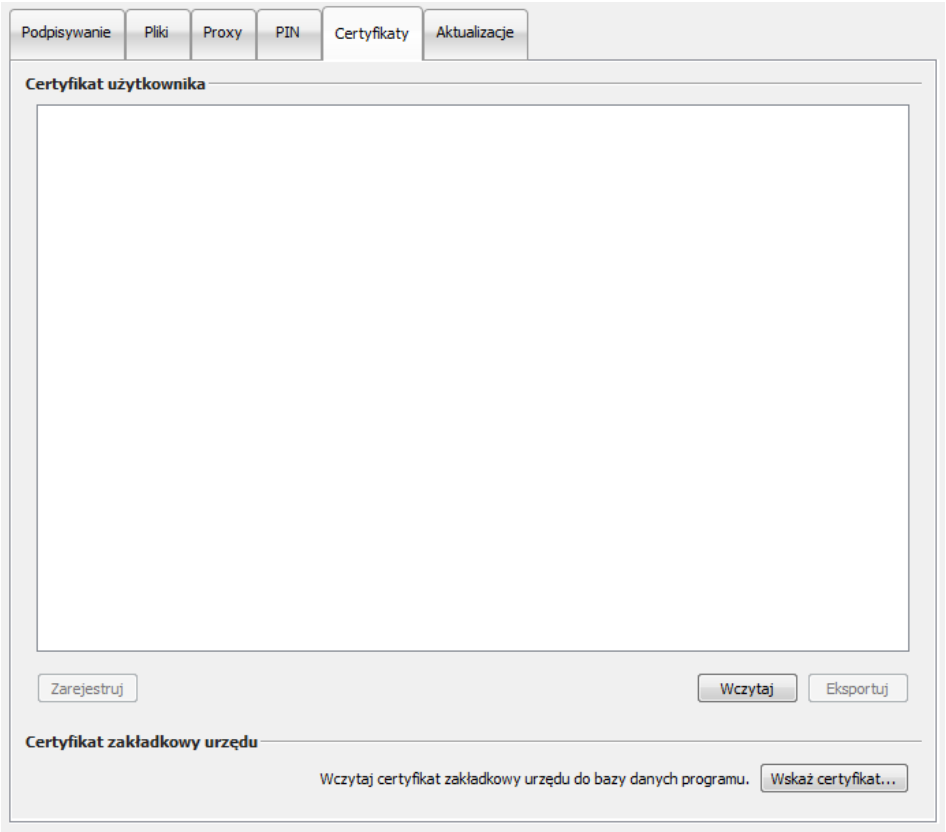


Rysunek 51 Zakładka *PIN*

Gdy jest ustawione jedna z dwóch ostatnich opcji to podczas składania podpisu program nie będzie wyświetlał okienka podawania kodu PIN, lecz będzie pobierał kod z pamięci.

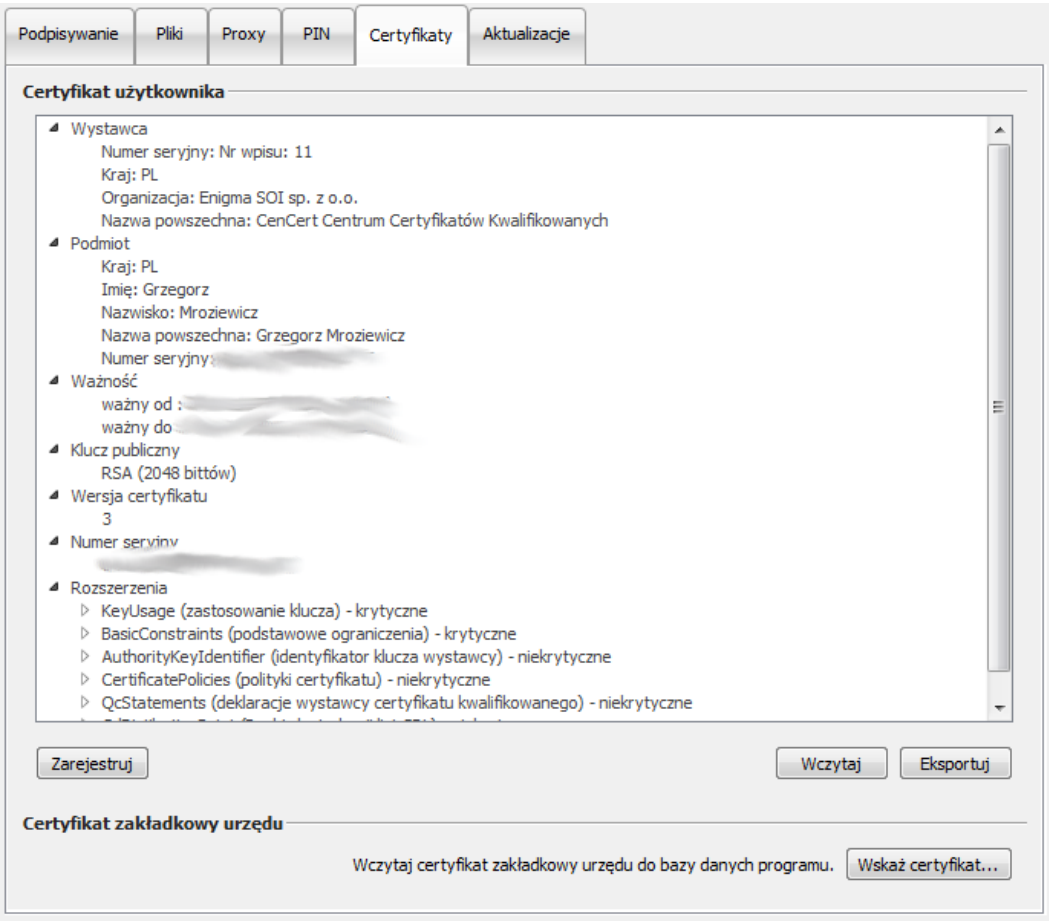
7.5 Certyfikaty

Zakładka ta dotyczy prezentacji, rejestracji w systemie i eksportowania certyfikatu użytkownika. Jeśli w czytniku jest umieszczona karta to program automatycznie odczyta z niej dane i zostaną one wyświetlone w okienku. Jeśli certyfikat nie zostanie odczytany należy sprawdzić umieszczenie karty i użyć przycisku *Wczytaj*.



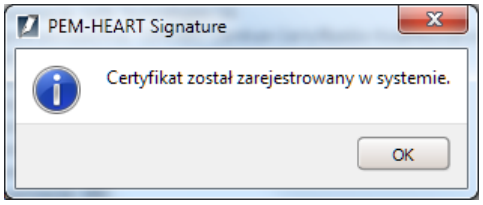
Rysunek 52 Zakładka prezentacji certyfikatu użytkownika

Poniżej przedstawiono widok okienko z odczytanymi z karty danymi certyfikatu:



Rysunek 53 Prezentacja treści certyfikatu

Przycisk *Zarejestruj* służy do rejestracji certyfikatu odczytanego z nośnika w magazynie systemowym. Wynik operacji jest prezentowany w postaci komunikatu jak na rysunku poniżej.



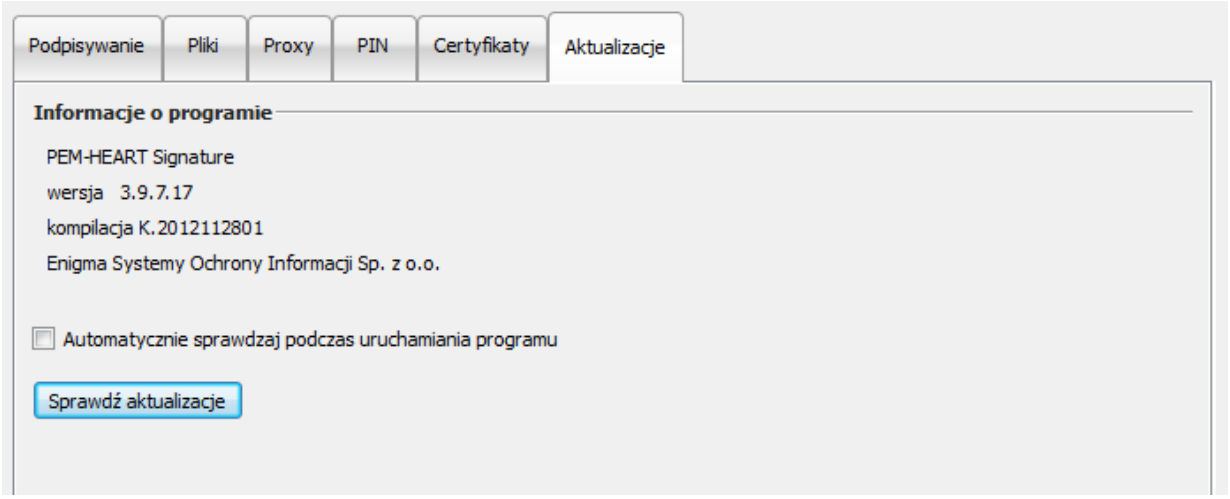
Rysunek 54 Komunikat o wyniku operacji rejestracji certyfikatu

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

Sekcja *Certyfikat zakładkowy urzędu* służy do wskazania i wczytania takiego certyfikatu do bazy danych programu. Certyfikat ten wykorzystywany jest do zapewnienia poprawności weryfikacji certyfikatu użytkownika w przypadku, gdy w urzędzie certyfikacji zostanie wprowadzony nowy klucz, a stary klucz nie stracił jeszcze ważności.

7.6 Aktualizacje

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



Rysunek 55 Zakładka *Aktualizacje*

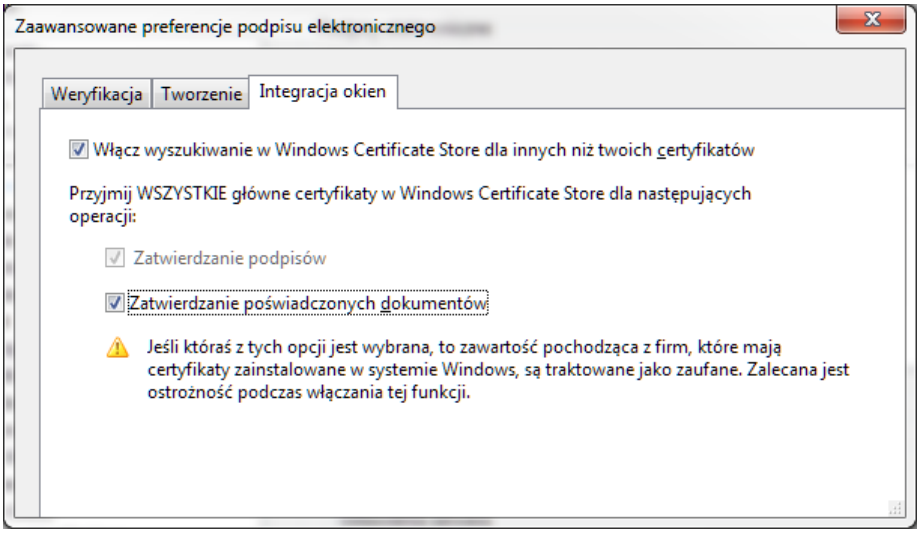
Informacji o dostępnej aktualizacji można dokonywać manualnie poprzez naciśnięcie przycisku *Sprawdź aktualizacje* lub ustalić opcje automatycznego sprawdzania czy podczas uruchamiania programu. W przypadku wykrycia nowej wersji oprogramowania zostaną wyświetlone komunikaty jak to przedstawiono na poniższych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

Po uzyskaniu informacji o dostępnej nowej wersji można ją pobrać ze strony http://www.cencert.pl/Oprogramowanie PEMHEART/ i zainstalować samodzielnie.

8 Konfiguracja programu *Adobe Acrobat Reader*

Aby poprawnie zweryfikować podpis elektroniczny poprzez wbudowane narzędzia oprogramowania do odczytu pliku *pdf* należy odpowiednio skonfigurować to oprogramowanie. Poniżej opisano konfigurację programu *Adobe Acrobat Reader*.

Poprzez opcję menu: **Edycja→Preferencje→Zabezpieczenie→Preferencje zaawansowane→Integracja okien** należy włączyć opcje jak na poniższym rysunku:



Rysunek 56 Opcje weryfikacji pliku PDF w *Adobe Acrobat Reader*.

Konieczne jest również dodanie certyfikatu centrum certyfikacji (jeśli nie został wcześnie dodany – dla ***CenCer***t odbywa się to podczas procesu instalacji oprogramowania), które wystawiło klucz podpisujący, do certyfikatów systemowych w magazynie *Zaufane główne urzędy certyfikacji*.