Ministerstwo Finansów

Właściciel

Instrukcja postępowania w celu uzyskania certyfikatu celnego oraz wykonania podpisu elektronicznego

nazwa dokumentu

PUESC.P4.4

nazwa Projektu

2.14

Wersja

07.02.2023 r.

Spis treści

Słownik stosowanych skrótów i terminów

Skrót / termin	Wyjaśnienie
Certyfikat celny	W rozumieniu niniejszej instrukcji jest to elektroniczne zaświadczenie wydane przez Centrum Certyfikacji Ministerstwa Finansów, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny zarejestrowanej na PUESC i które umożliwiają identyfikację tej osoby.
ID SISC	Unikalny numer identyfikacyjny nadawany osobom podczas procesu rejestracji w SISC.
Instrukcja e-Klient	Instrukcja elektronicznej rejestracji dla potrzeb zarządzania użytkownikami korzystającymi z usług SISC.
PUESC	Platforma Usług Elektronicznych Skarbowo-Celnych.
Regulamin	Regulamin dla certyfikatów cyfrowych emitowanych przez Centrum Certyfikacji Ministerstwa Finansów.
SC	Służba Celno-Skarbowa
SISC	System Informacyjny Skarbowo-Celny

1. Konfiguracja komputera

1.1 Instalacja certyfikatów CCK MF

Dla prawidłowej obsługi procesów generowania certyfikatów oraz wykonania podpisu konieczne jest pobranie i zainstalowanie certyfikatów Centrum Certyfikacji Ministerstwa Finansów (CCK MF). Aplikacja CertSign instaluje przy pierwszym uruchomieniu niezbędne certyfikaty w systemie Windows (dostępne są one przeglądarkom Internet Explorer, Edge, Chrome oraz Firefox – po uprzedniej konfiguracji. Opis konfiguracji Firefox znajduje się w rozdziale 1.3. W przypadku konieczności manualnej instalacji certyfikatów, dostępne są one na stronie *https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny*, w menu *Elektroniczne podpisywanie dokumentów* > *Uzyskaj lub unieważnij certyfikat celny*, albo w *Moje dane* > *Certyfikaty celne*. Opis instalacji certyfikatów znajduje się w dodatku A.1

1.2 Konfiguracja zapory systemu Windows (Windows Firewall)

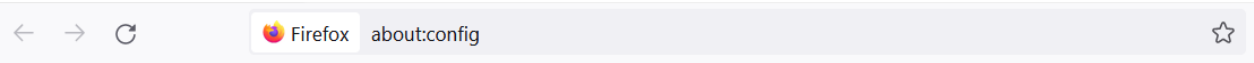
Aplikacja CertSign realizuje wewnątrz komputera połączenie ze stroną internetową. Konieczne może być manualne zezwolenie na komunikację pomiędzy przeglądarką i aplikacją, np. poprzez Windows Firewall. Może pojawić się ostrzeżenie, np. wyświetlane przez zaporę systemu Windows. Należy zaznaczyć wszystkie opcje zezwalające aplikacji CertSign na łączenie w sieciach i kliknąć na przycisk „Zezwalaj na dostęp”.
W przypadku stosowania oprogramowania antywirusowego z włączoną funkcją zapory (firewall), analizy ruchu, itp., należy w oprogramowaniu antywirusowym umożliwić:

- uruchomienie aplikacji CertSign
- odblokować komunikację pomiędzy przeglądarką a adresem localhost, porty 22443 oraz 22311.

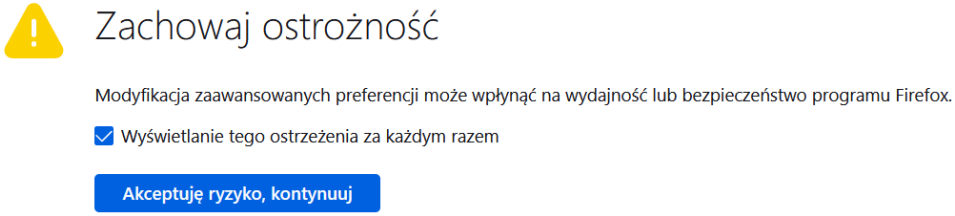
1.3 Konfiguracja przeglądarki Mozilla Firefox

Przeglądarka Firefox posiada własny *Menedżer certyfikatów*, w którym przechowywane są certyfikaty wymagane do poprawnej współpracy przeglądarki z aplikacją CertSign. Aby przeglądarka korzystała z certyfikatów zarejestrowanych w magazynie certyfikatów systemu Windows, należy:

W pasku adresu wpisać *about:config* (i zatwierdzić).



Potwierdzić komunikat ostrzeżenia i wybrać *Akceptuję ryzyko, kontynuuj*

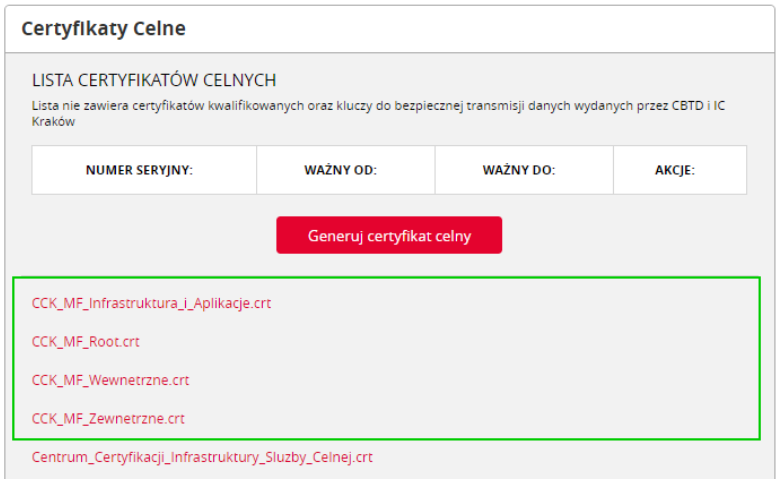


Wyszukać parametr *security.enterprise_roots.enabled* oraz ustawić jego wartość na *true* (wartość logiczna, zmiana strzałkami po prawej stronie).

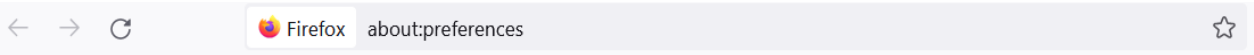
Zamknąć przeglądarkę.

Po ponownym uruchomieniu przeglądarka powinna być gotowa do korzystania z certyfikatów zarejestrowanych w magazynie certyfikatów Windows. W przypadku, gdyby to ustawienie nie działało, można manualnie zarejestrować certyfikaty CCK MF w *Menadżerze certyfikatów* Firefox.

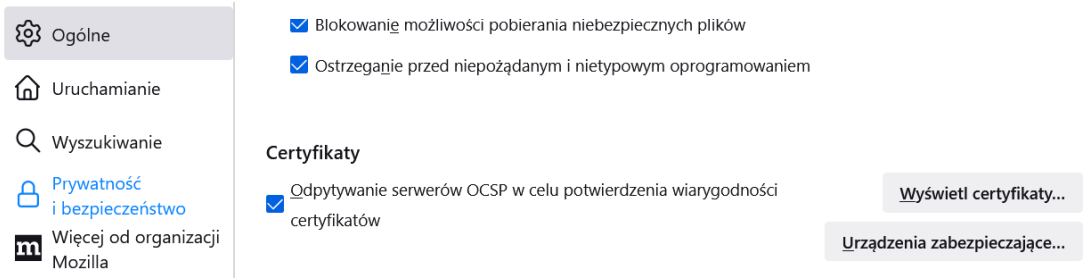
Ze strony https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny pobrać i zapisać na dysku certyfikaty CCK MF Root, CCK MF Infrastruktura i Aplikacje, CCK MF Wewnetrzne, CCK MF Zewnetrzne.



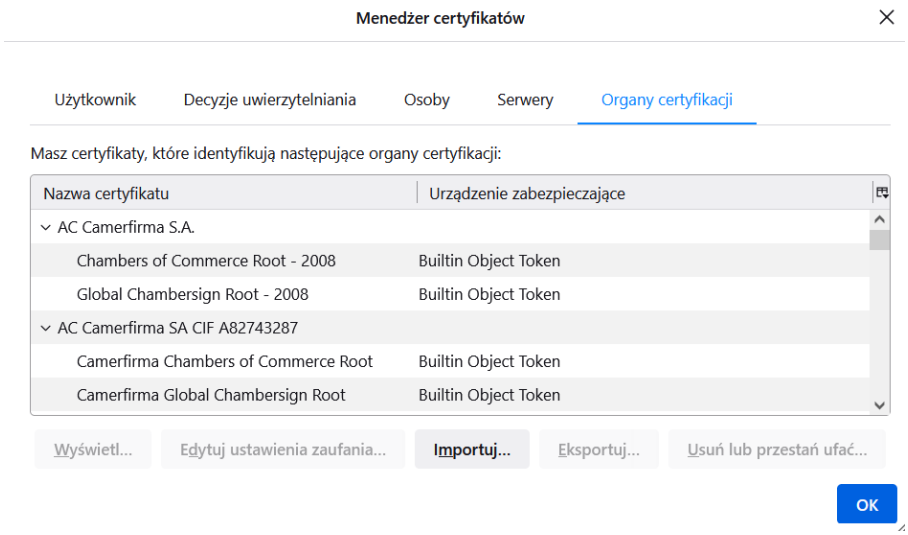
W przeglądarce wejść w menu Ustawienia albo w pasku wpisać *about:preferences* i zatwierdzić.



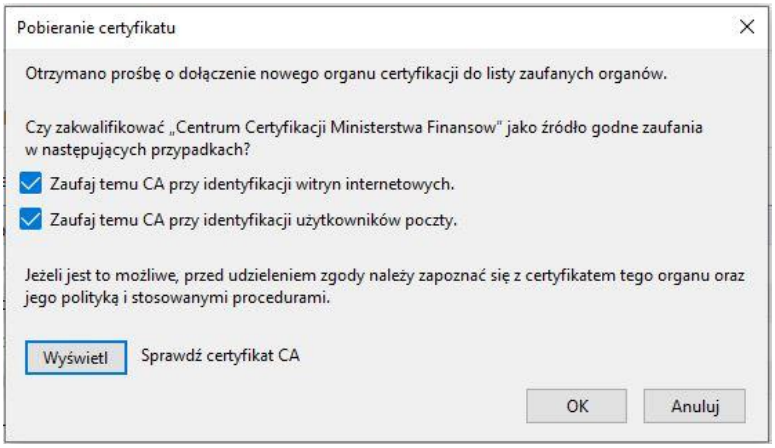
W ustawieniach przejść do *Prywatność i bezpieczeństwo* oraz wybrać *Wyświetl certyfikaty*.



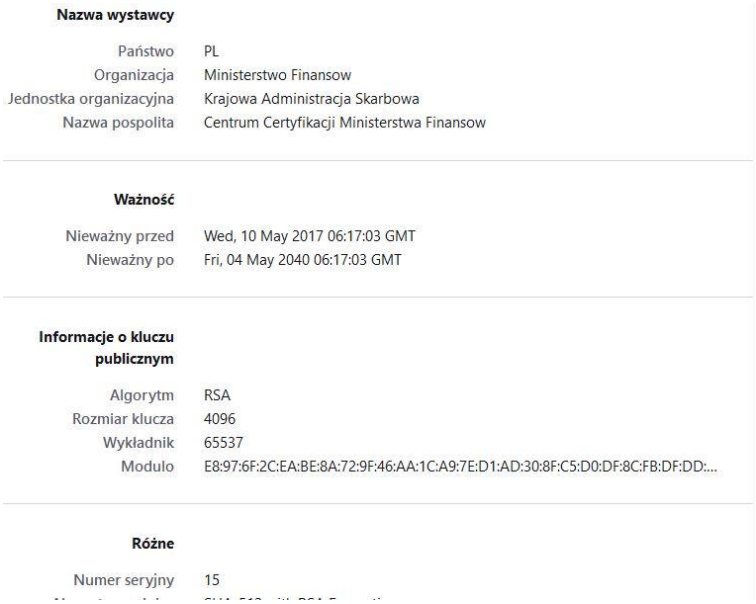
W *Menedżerze certyfikatów* wskazać *Organy certyfikacji*, wybrać *Importuj*, wskazać kolejno certyfikaty z dysku i zatwierdzić import.



Podczas zatwierdzania zweryfikować dane certyfikatu i ustawić zasady zaufania.



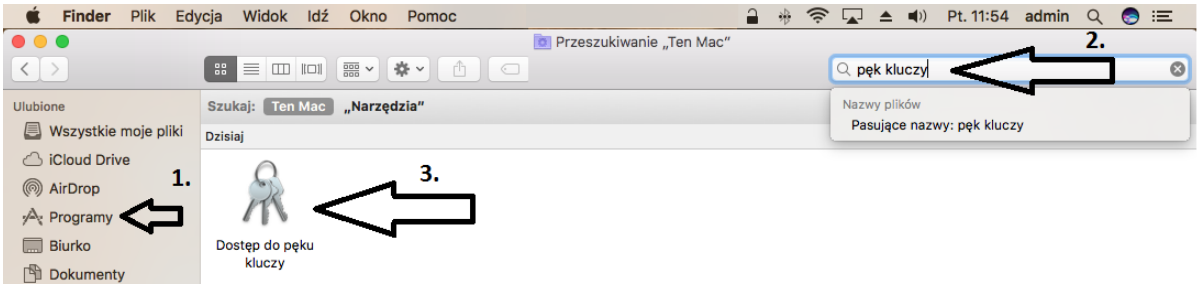
Opcja *Wyświetl* pozwala zweryfikować dane certyfikatu.



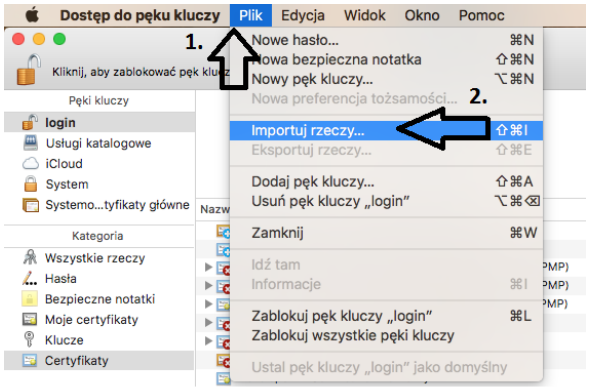
Operacje importu należy powtórzyć dla wszystkich certyfikatów CCK MF.

1.4 Konfiguracja w macOS

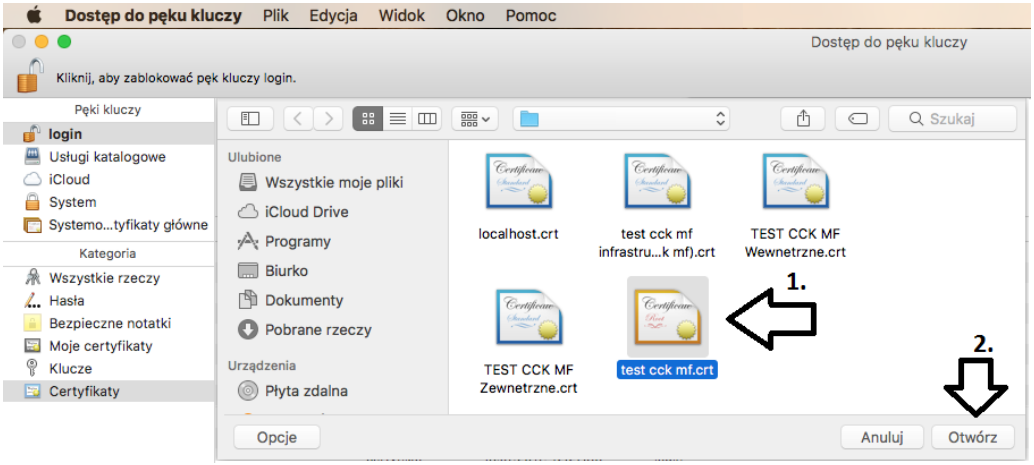
Należy zaimportować do *Pęku kluczy* certyfikaty centrów certyfikacji MF.



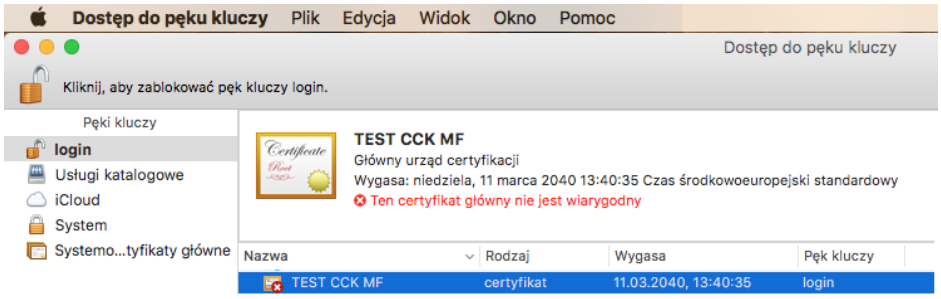
W *Dostęp do pęku kluczy* należy wybrać *Plik* > *Importuj rzeczy* …



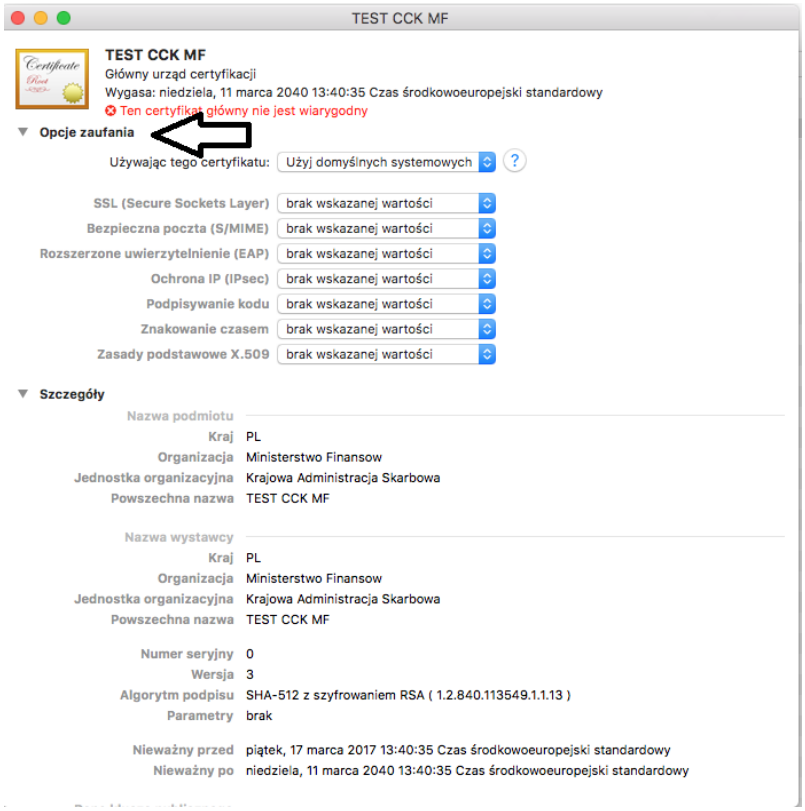
Zostanie otwarte okno umożliwiające wskazanie położenia plików z certyfikatami centrów certyfikacji.



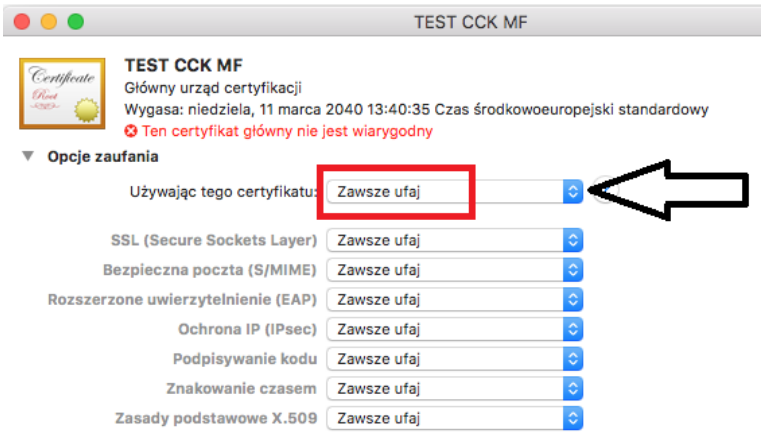
Należy wskazać plik z certyfikatem (1) i kliknąć *Otwórz* (2). Certyfikat zostanie zaimportowany i uzyska status „niewiarygodny”.



Należy kliknąć na certyfikat i rozwinąć *Opcje zaufania.*



W *Opcje zaufania* należy w polu *Używając tego certyfikatu* ustawić *Zawsze ufaj* i zapisać wprowadzone ustawienia.



Operacje należy powtórzyć dla wszystkich certyfikatów CCK MF.

2. Instalacja aplikacji CertSign

2.1 Pobranie i uruchomienie instalatora

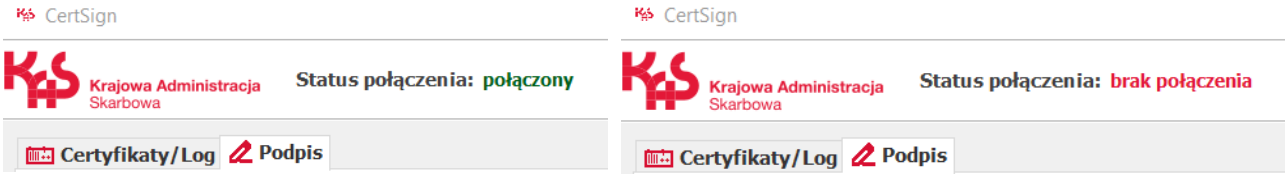
Pliki instalacyjne aplikacji CertSign dostępne są na portalu PUESC w menu *Elektroniczne podpisywanie dokumentów* > *Dowiedz się więcej o systemie PKI*
https://puesc.gov.pl/uslugi/elektroniczne-podpisywanie-dokumentow
Udostępnionych jest kilka wersji programu, spośród których należy wybrać wersję odpowiednią dla używanego systemu operacyjnego komputera. Po pobraniu należy uruchomić instalator aplikacji.

W systemach Microsoft Windows aplikacja instaluje się w profilu użytkownika, bez konieczności podnoszenia uprawnień do poziomu lokalnego administratora.

Aplikacje nie są przewidziane do używania na serwerowych wersjach systemów operacyjnych, ani do pracy terminalowej.

2.2 Status połączenia

Aplikacja wskazuje dwa możliwe statusy połączenia ze stroną internetową:



Bezpośrednio po uruchomieniu aplikacja wskazuje *Status połączenia:* brak połączenia, i jest to sytuacja prawidłowa.

Komunikat *Status połączenia:* **połączony** informuje, że strona PUESC prawidłowo nawiązała połączenie z aplikacją CertSign. Status **połączony** jest wymagany przy generowaniu certyfikatu oraz przy podpisywaniu dokumentu na PUESC. W przypadku podpisywania pliku z dysku komputera nie jest wymagane połączenie ze stroną PUESC. Status **brak połączenia** nie jest w takim przypadku objawem nieprawidłowego działania.

Aplikacja po ręcznym uruchomieniu będzie sygnalizowała status **brak połączenia** do czasu uruchomienia na stronie PUESC operacji podpisywania dokumentu lub generowania certyfikatu celnego.

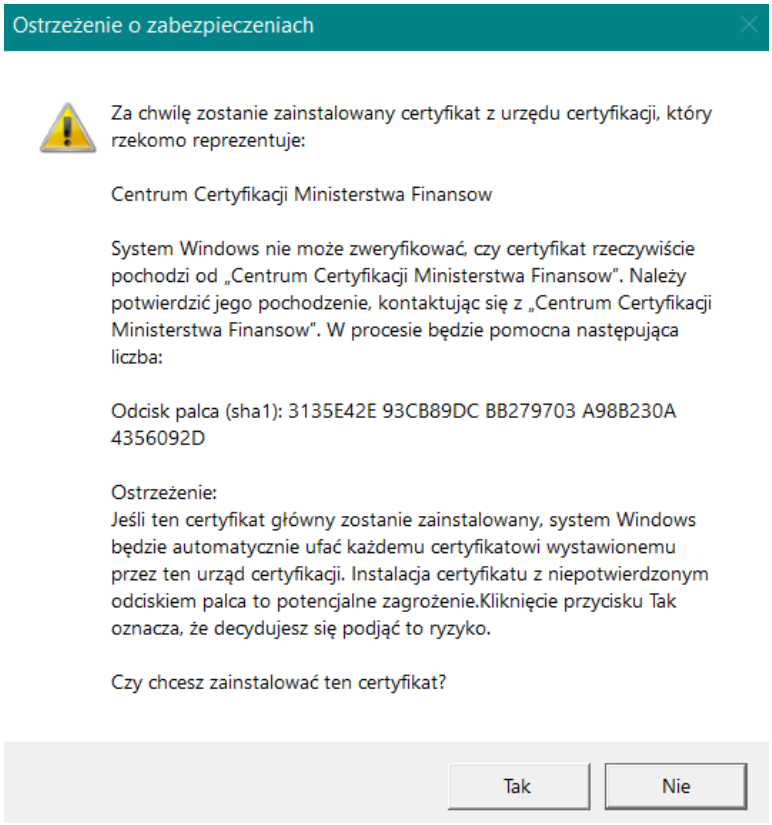
W przypadku braku połączenia podczas generowania certyfikatu lub podpisywania dokumentu na PUESC (*Status połączenia:* **brak połączenia**) należy skonfigurować komputer oraz przeglądarkę internetową zgodnie z opisami w rozdziale 1. W trybie **brak połączenia** możliwe jest podpisywanie plików z dysku na komputerze (offline), o ile użytkownik posiada certyfikat.

W systemach z rodziny Linux oraz Mac OS X rekomendowane jest używanie przeglądarki Firefox, po uprzednim skonfigurowaniu.

W przypadku występowania problemów z połączeniem należy postępować zgodnie z opisem znajdującym się w dodatku A.6

2.2 Automatyczna instalacja certyfikatów CCK MF

W systemach Microsoft Windows aplikacja przy pierwszym uruchomieniu sprawdza, czy zainstalowane są certyfikaty Centrum Certyfikacji Ministerstwa Finansow. W przypadku ich braku aplikacja automatycznie proponuje instalację.



Po poprawnej instalacji certyfikaty dostępne są dla przeglądarek: Internet Explorer, EDGE, Chrome (przeglądarki korzystające z Windows CSP) a także Firefox, po skonfigurowaniu zgodnie z opisem w rozdziale 1.3.

3. O aplikacji CertSign

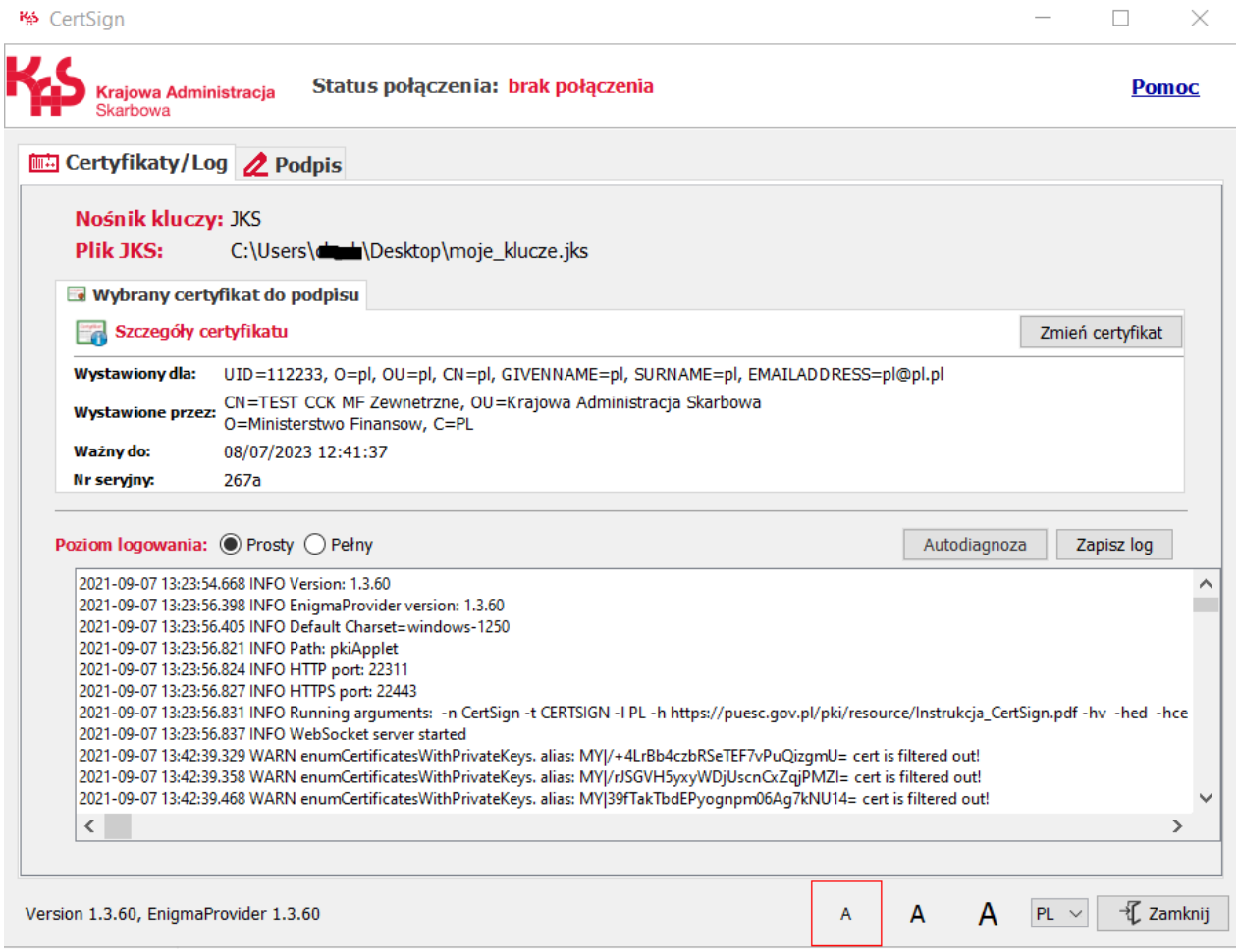
Aplikacja CertSign realizuje dwie funkcje:

1. generowanie certyfikatów i obsługa kluczy kryptograficznych,
2. wykonanie podpisu elektronicznego w trybach *online* i *offline*.

Aplikacja współpracuje z przeglądarkami: Chrome, Firefox, Internet Explorer 11, Edge.

3.1 Funkcje i ustawienia aplikacji CertSign

Status połączenia – informuje czy aplikacja nawiązała połączenie ze stroną PUESC. Status połączenia przyjmuje następujące wartości**:** **połączono** lub **brak połączenia**. Podczas pracy w trybie offline brak połączenia jest stanem prawidłowym.
W trybie połączono (*online)* aplikacja wykonuje operacje w tle strony internetowej i po ewentualnym wybraniu opcji należy zminimalizować okno CertSign do paska zadań.



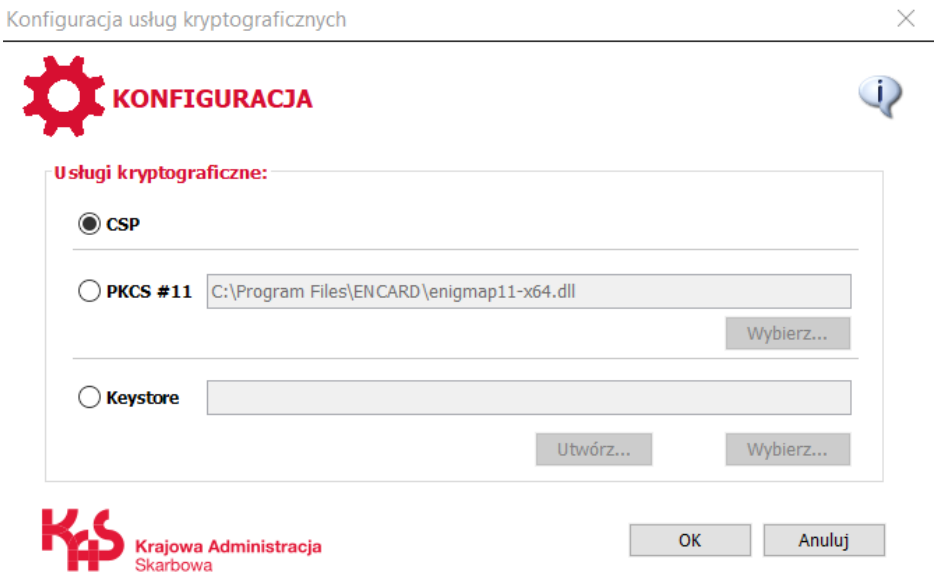
Klikając link „*Pomoc*” uzyskuje się dostęp do instrukcji działania aplikacji.

W zakładce ***„Certyfikaty/Log”*** prezentowany jest aktualny wybór certyfikatu służącego do wykonywania podpisu elektronicznego (przy pierwszym uruchomieniu okienko jest puste). Poniżej wyświetlany jest log aplikacji. Ustawienie poziomu logowania „*Pełny*” powinno być używane do gromadzenia informacji dla help-desku, w przypadku problemów z aplikacją.

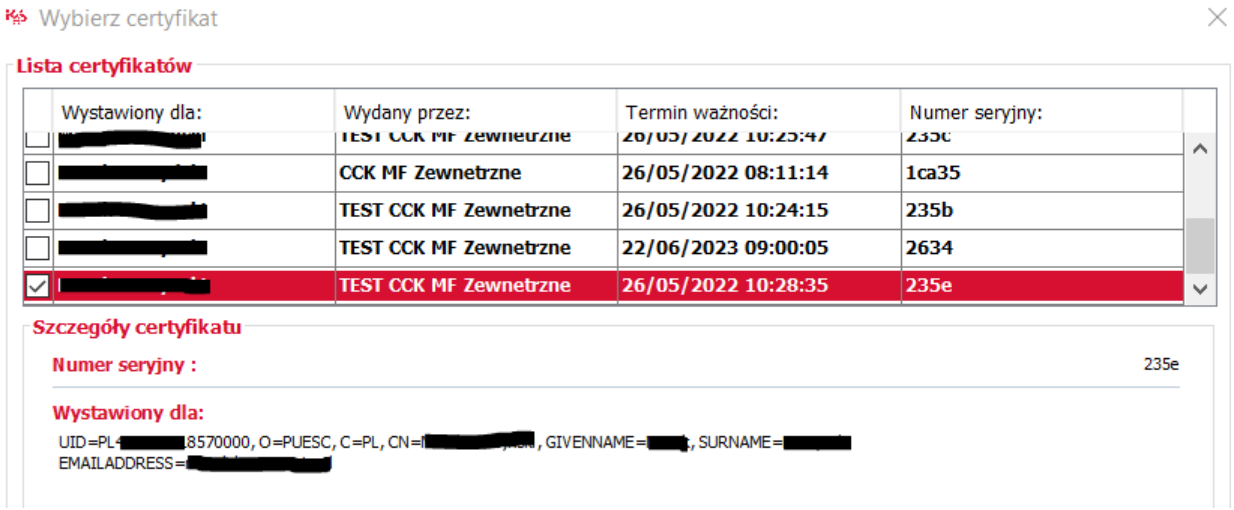
Opcja ***„Zmień certyfikat”*** uruchamia dostęp do konfiguracji usług kryptograficznych, gdzie możliwy jest wybór nośnika kluczy/certyfikatów zgodnego z CSP, PKCS#11 lub Java™ Keystore. Możliwe jest także

wskazanie położenia pliku sterownika (biblioteki *.dll) standardu PKCS#11, lub pliku do przechowywania zaszyfrowanych kluczy na dysku (Keystore). Opis poszczególnych opcji dostępny jest w dodatku A.5.

Wyboru certyfikatu używanego w procesie składania podpisu elektronicznego dokonuje się przyciskiem *Zmień certyfikat*. W pierwszej kolejności zostanie wyświetlone okno konfiguracji usług kryptograficznych, gdzie dokonuje się wyboru magazynu przechowującego certyfikaty.



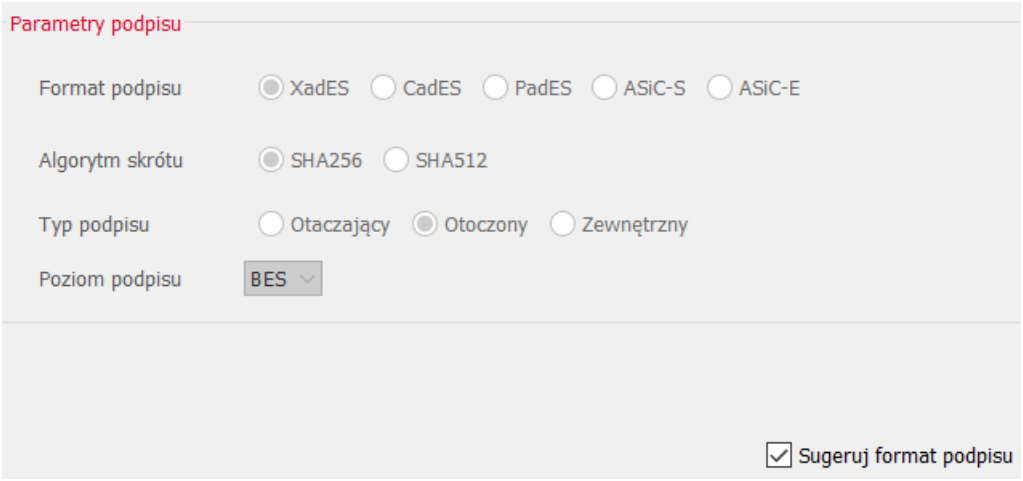
Po wybraniu żądanej usługi i zatwierdzeniu przyciskiem *OK,* wyświetlone zostanie okno wyboru certyfikatu ze wskazanego magazynu certyfikatów.



Wyboru certyfikatu dokonuje się z listy, zaznaczając certyfikat (zostanie on podświetlony kolorem) i klikając przycisk *OK.*

W zakładce ***„Podpis”*** dostępne są funkcje do lokalnego wykonania podpisu elektronicznego na pliku pobranym z dysku komputera. Do wykonania podpisu nie jest potrzebne uruchamianie PUESC ani nawiązywanie połączenia. Szczegóły opisane są w rozdziale 5.

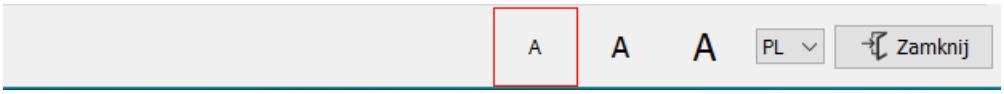
Zaznaczenie opcji ***„Sugeruj format podpisu”*** powoduje automatyczne wybranie formatu i typu podpisu, na podstawie typu pliku wybranego do podpisania. Domyślnie opcja jest włączona. Jej odznaczenie powoduje odblokowanie możliwości ręcznego ustawiania parametrów podpisu.



Aplikacja umożliwia **skalowanie czcionek ekranowych** do trzech rozmiarów:

- Standardowy
- Większy
- Największy

Aby zmienić rozmiar czcionek, należy wybrać jeden z przycisków skalowania (A A A), który nie jest aktualnie wybrany. Każdy kolejny rozmiar jest większy od poprzedniego półtorakrotnie. Oznacza to, że powiększenie rozmiaru *standardowego* do *większego* skutkuje wzrostem aktualnego rozmiaru czcionek o 150%, zaś do *największego* – o 225%. Tak samo, zmniejszenie z *największego* do *większego* zmniejszy poziom z 225% rozmiaru *standardowego* do 150%, a powrót do *standardowego* pomniejszy aktualny do wartości domyślnej (100%). Skalowanie może nie działać na wyświetlaczach o niższych rozdzielczościach – aplikacja weryfikuje ten parametr w celu ochrony przed nadmiernym powiększaniem elementów.



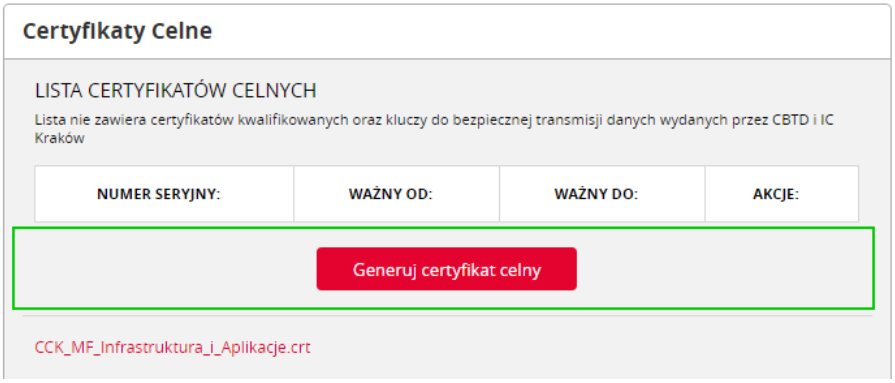
Zmianę wersji językowej na angielską wykonuje się klikając na pole PL.
Przycisk „Zamknij” kończy działanie aplikacji.

Aplikacja posiada funkcję ***„Autodiagnoza”***, która umożliwia sprawdzenie gotowości aplikacji do wykonywania podpisów. Aplikacja sprawdza dostępność portów sieciowych oraz wykonuje test podpisywania, używając certyfikatu wskazanego w zakładce *„Certyfikaty/Log”*. Aplikacja będzie żądać podania hasła zabezpieczającego klucz prywatny. Jeśli użytkownik nie posiada certyfikatu, test podpisu nie powiedzie się. Autodiagnoza zapisuje informacje o przebiegu testu w logu aplikacji i wyświetla okno raportu – Wynik autodiagnozy.

4. Generowanie certyfikatu

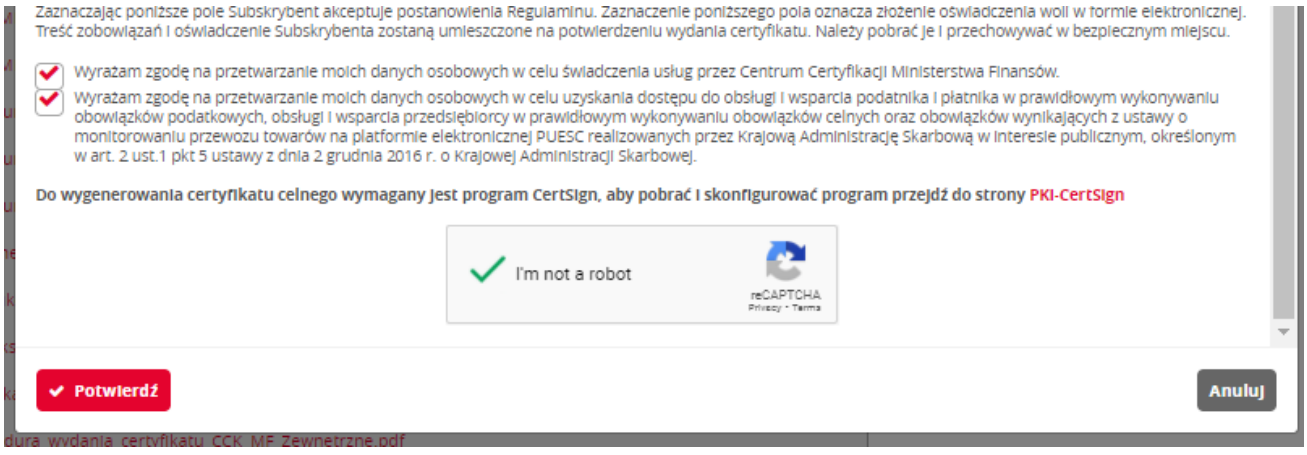
Certyfikat celny może uzyskać wyłącznie osoba posiadająca aktywny IdSISC i zarejestrowana w tzw. procedurze pełnej. Niezarejestrowany użytkownik PUESC powinien, w pierwszej kolejności, dokonać rejestracji, wypełniając *Wniosek o rejestrację osoby fizycznej w SISC*.

PUESC udostępnia funkcjonalność generowania certyfikatu celnego. Do zarządzania oraz generowania certyfikatów celnych system posiada dedykowany widok, dostępny w *Moje dane* > *Certyfikaty celne*. W celu wygenerowania nowego certyfikatu należy wybrać opcję „Generuj certyfikat celny”

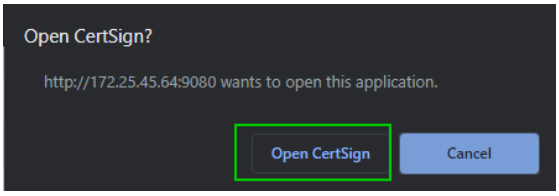


UWAGA: W celu wygenerowania kluczy kryptograficznych należy, przed wybraniem *Generuj certyfikat celny,* pobrać oraz zainstalować aplikację CertSign. Jeśli aplikacja nie będzie poprawnie zainstalowana, generowanie kluczy nie będzie możliwe.

Po wybraniu *Generuj certyfikat celny* system wyświetli komunikat z regulaminem usługi. Poniżej regulaminu, przed przejściem do kolejnego kroku, należy zaznaczyć oświadczenia, po czym przeprowadzić weryfikację captcha. Na koniec zatwierdzić akcję przyciskiem „**Potwierdź**”.

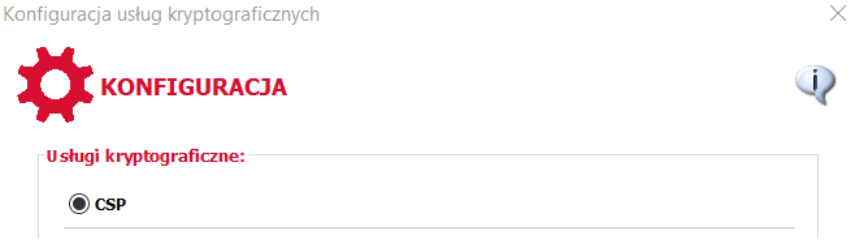


Uwaga: po wybraniu *Potwierdź* może pojawić się komunikat z pytaniem, czy otworzyć aplikację CertSign. Jeśli aplikacja nie była uruchomiona należy zatwierdzić, zezwalając przeglądarce na otwarcie programu.

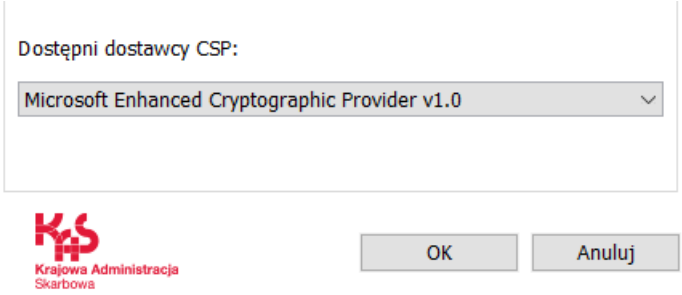


4.1. Generowanie certyfikatu do magazynu systemu Windows (CSP)

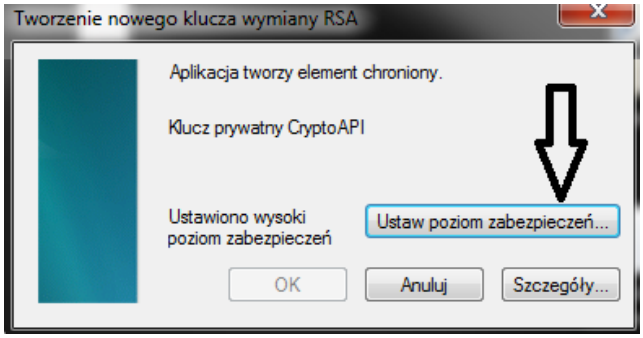
Po uruchomieniu aplikacji w trybie generowania certyfikatu zostanie wyświetlone okno konfiguracji usług kryptograficznych. Należy zaznaczyć opcję „*CSP*" i potwierdzić wybór przyciskiem „*OK*".



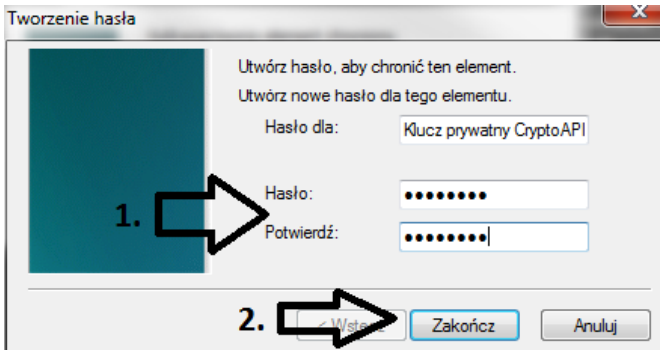
Jeśli aplikacja do generowania certyfikatów nigdy nie była uruchamiana, opcja CSP jest domyślnie wybrana. W następnym kroku należy dokonać wyboru dostawcy usługi CSP służącej do generowania certyfikatu.



W przypadku generowania kluczy do **magazynu systemowego Windows**, należy wybrać z listy rozwijanej ***Microsoft Enhanced Cryptographic Provider***… i zatwierdzić *„OK"*.
Wyświetli się okno zabezpieczeń generowanego klucza. Należy w nim wybrać opcję *Ustaw poziom zabezpieczeń …*

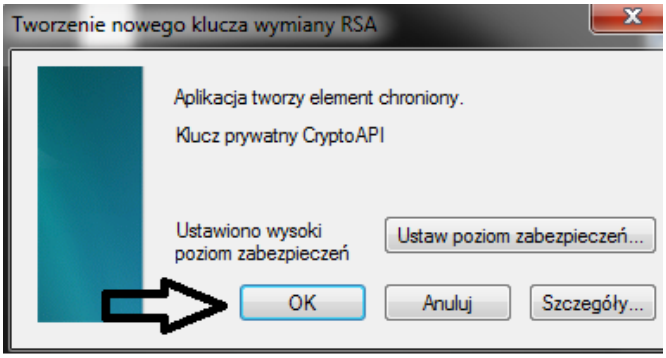


Należy ustawić hasło składające się z co najmniej 12 znaków (dużych i małych liter, cyfr oraz znaków specjalnych), a następnie zatwierdzić przyciskiem *Zakończ.*



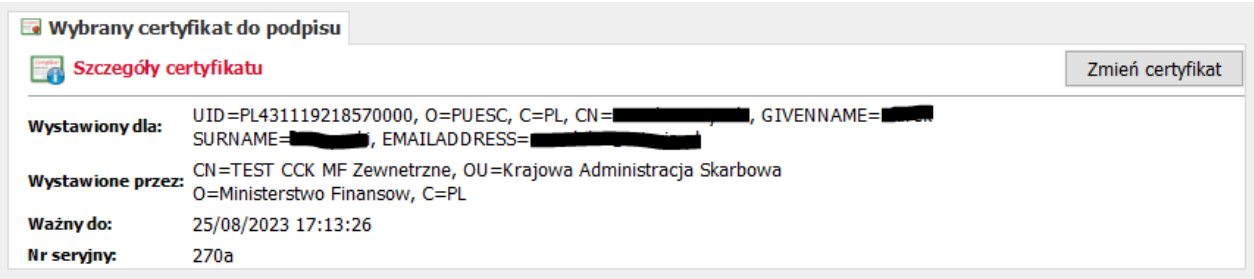
Hasło jest poufne i niezbędne do posługiwania się certyfikatem. Należy zabezpieczyć je w sposób uniemożliwiający dostęp innym osobom. **Hasła nie można odzyskać z PUESC** – jest ono tworzone i przechowywane lokalnie.

W kolejnym oknie należy potwierdzić wybór ustawienia wysokiego poziomu zabezpieczeń przyciskiem *OK.*

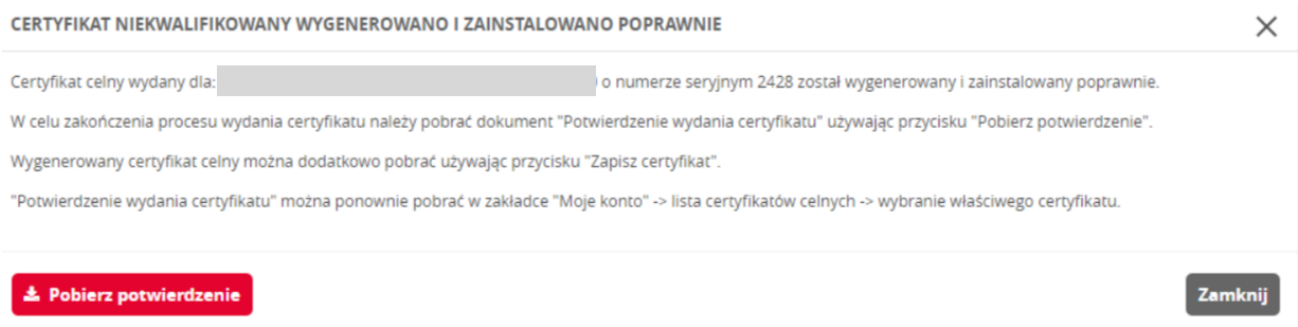


Następuje generowanie kluczy kryptograficznych i certyfikatu. Proces ten jest niewizualny i może potrwać kilka minut. Po jego zakończeniu certyfikat jest automatycznie instalowany w komputerze użytkownika. Wygenerowany w ten sposób certyfikat jest eksportowalny, co oznacza, że możliwe jest przeniesienie go na inny komputer.

Po wygenerowaniu certyfikatu jego dane będą wyświetlone w oknie *Szczegóły certyfikatu…* aplikacji CertSign.



W kolejnym kroku należy ze strony PUESC pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję ***Pobierz potwierdzenie***.



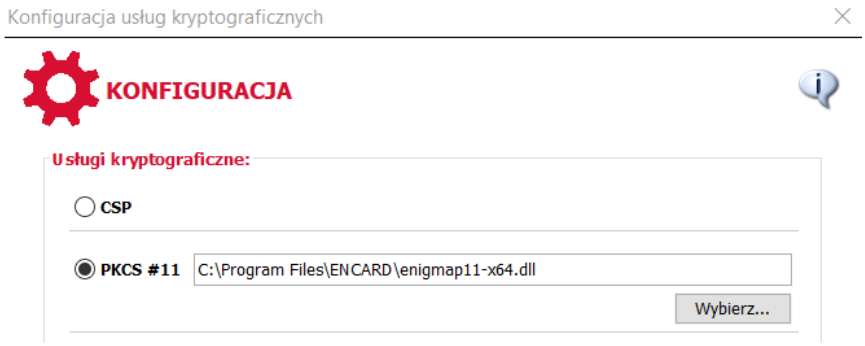
Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.

Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

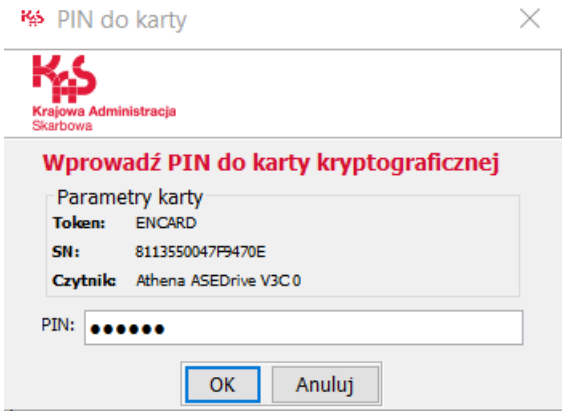
4.2. Generowanie certyfikatu przy wykorzystaniu PKCS#11

Opcja ta wykorzystywana jest w przypadku certyfikatów zapisywanych na kartach kryptograficznych, niezależnie od posiadanego systemu operacyjnego. Jest to najbezpieczniejsza metoda przechowywania kluczy kryptograficznych i certyfikatu. Wykorzystując tę metodę, użytkownik musi posiadać zgodny ze standardem PKSC#11 sterownik karty kryptograficznej, dostarczony przez jej producenta. Klucze generowane są bezpośrednio na karcie kryptograficznej, co umożliwia użytkownikowi bezpieczne wykorzystanie na wielu komputerach.

Nie zalecamy generowania certyfikatów niekwalifikowanych na kartach kryptograficznych zawierających certyfikaty kwalifikowane, ze względu na ryzyko ich przypadkowego usunięcia.



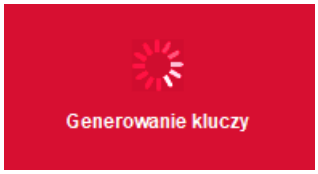
W trakcie procesu generowania certyfikatu należy wskazać ścieżkę dostępu do posiadanego sterownika PKCS#11. Po wskazaniu pliku sterownika PKCS#11 należy kliknąć *OK*



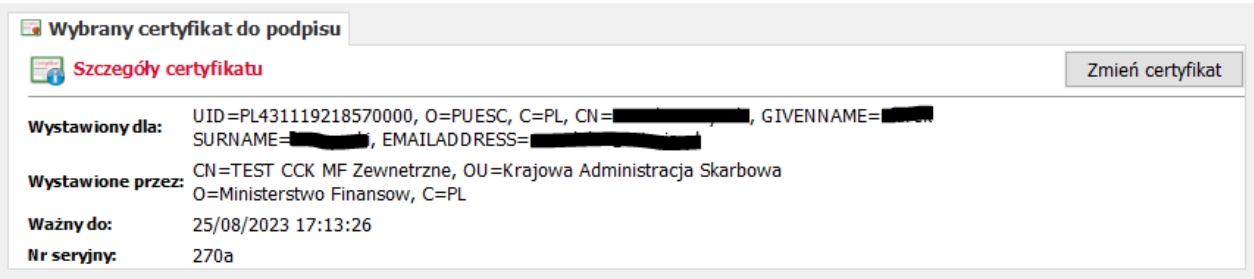
Następnie podać kod PIN do karty kryptograficznej i ponownie zatwierdzić *OK.*

PIN jest poufny. Należy zabezpieczyć go w sposób uniemożliwiający dostęp innym osobom.

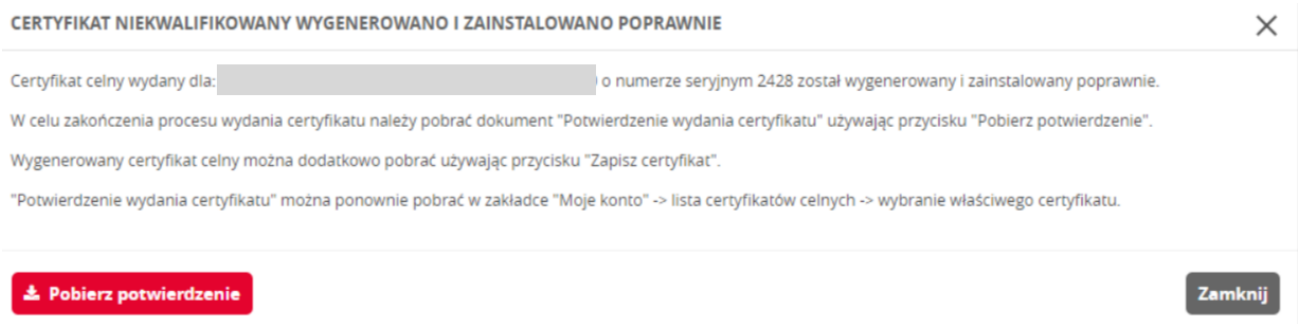
Certyfikat zostanie wygenerowany i zapisany na karcie. W trakcie operacji zapisu certyfikatu na karcie, konieczne będzie ponowne podanie kodu PIN do karty. Proces ten jest niewizualny i może potrwać kilka minut. W trakcie generowania kluczy zostaje wyświetlony komunikat:



Po wygenerowaniu certyfikatu jego dane będą prezentowane w oknie *„Szczegóły certyfikatu…”* aplikacji CertSign.



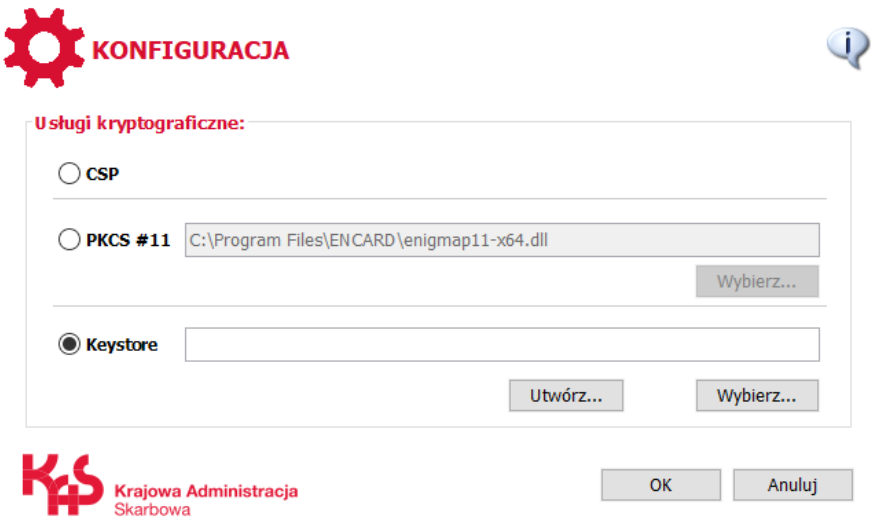
W kolejnym kroku należy pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję *Pobierz potwierdzenie*.



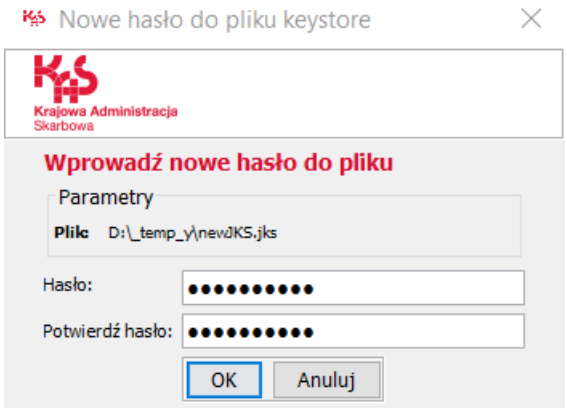
Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.
Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

4.3. Generowanie certyfikatu przy wykorzystaniu Keystore

Wybranie tej opcji umożliwia przechowywanie kluczy i certyfikatów w zaszyfrowanym pliku na komputerze, oraz proste ich przenoszenie pomiędzy komputerami. **Należy jednak mieć na uwadze, że wygenerowane w ten sposób certyfikaty mogą być niewidoczne dla innych aplikacji systemu Windows. Jest to jednocześnie najmniej bezpieczna metoda przechowywania kluczy.** Opcję tę można wykorzystywać m.in. w przypadku systemów operacyjnych z rodziny Linux oraz Mac OS X.
Po zaznaczeniu opcji „*Keystore*" uaktywnią się przyciski: „*Utwórz…"* oraz „*Wybierz…".*

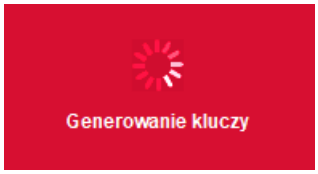


Jeśli plik *Keystore* nie został wcześniej utworzony, należy wybrać opcję *„Utwórz…”* (poniżej okna ścieżki do pliku). Jeśli plik *Keystore* był wcześniej utworzony, należy wskazać go przez *„Wybierz…”*. Wybór należy potwierdzić przyciskiem *OK*. Utworzone klucze i certyfikaty zostaną dopisane do tego pliku.
Następnie należy wprowadzić hasło chroniące dostęp do kluczy i certyfikatów zapisanych w pliku *Keystore*.

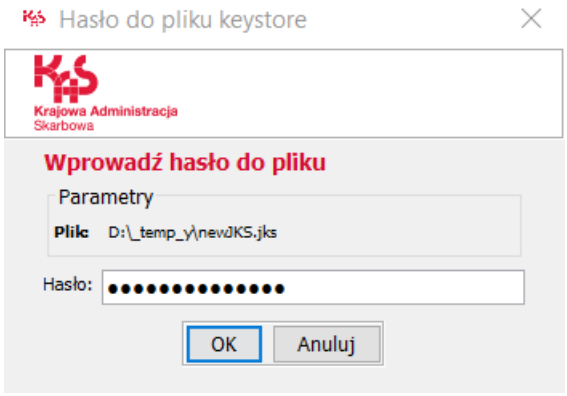


Wprowadzone hasło należy powtórzyć, w celu weryfikacji poprawności, po czym zatwierdzić przyciskiem *OK*. W przypadku gdy wprowadzone hasła będą różne, zwrócony zostanie komunikat błędu.
Po poprawnym wpisaniu hasła wyświetli się okno informujące o generowaniu kluczy.

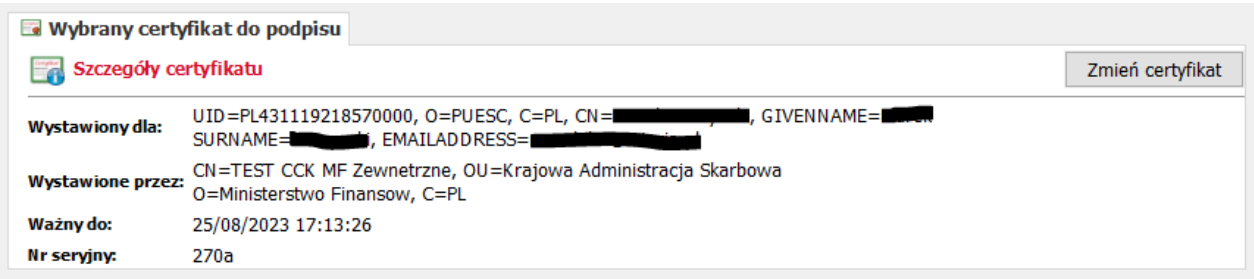
Zalecamy aby hasło było skomplikowane, tzn. składało się z liter małych i wielkich, cyfr oraz znaków specjalnych. Należy zabezpieczyć je w sposób uniemożliwiający dostęp innym osobom.



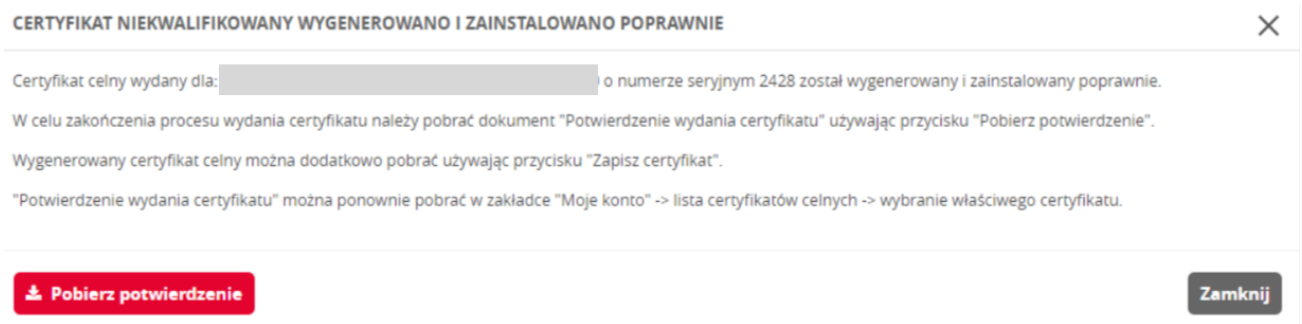
Następuje wygenerowanie certyfikatu i przesłanie go na komputer użytkownika. Proces ten jest niewizualny i może potrwać kilka minut. W celu zapisania wygenerowanego certyfikatu należy podać hasło wprowadzone w trakcie generowania klucza prywatnego (1) i zatwierdzić *OK* (2).



Po wygenerowaniu certyfikatu jego dane zostaną wyświetlone w oknie „*Szczegóły certyfikatu…*” aplikacji CertSign.



W kolejnym kroku należy pobrać dokument potwierdzający wydanie certyfikatu. Dokument pobiera się wybierając opcję *Pobierz potwierdzenie*.



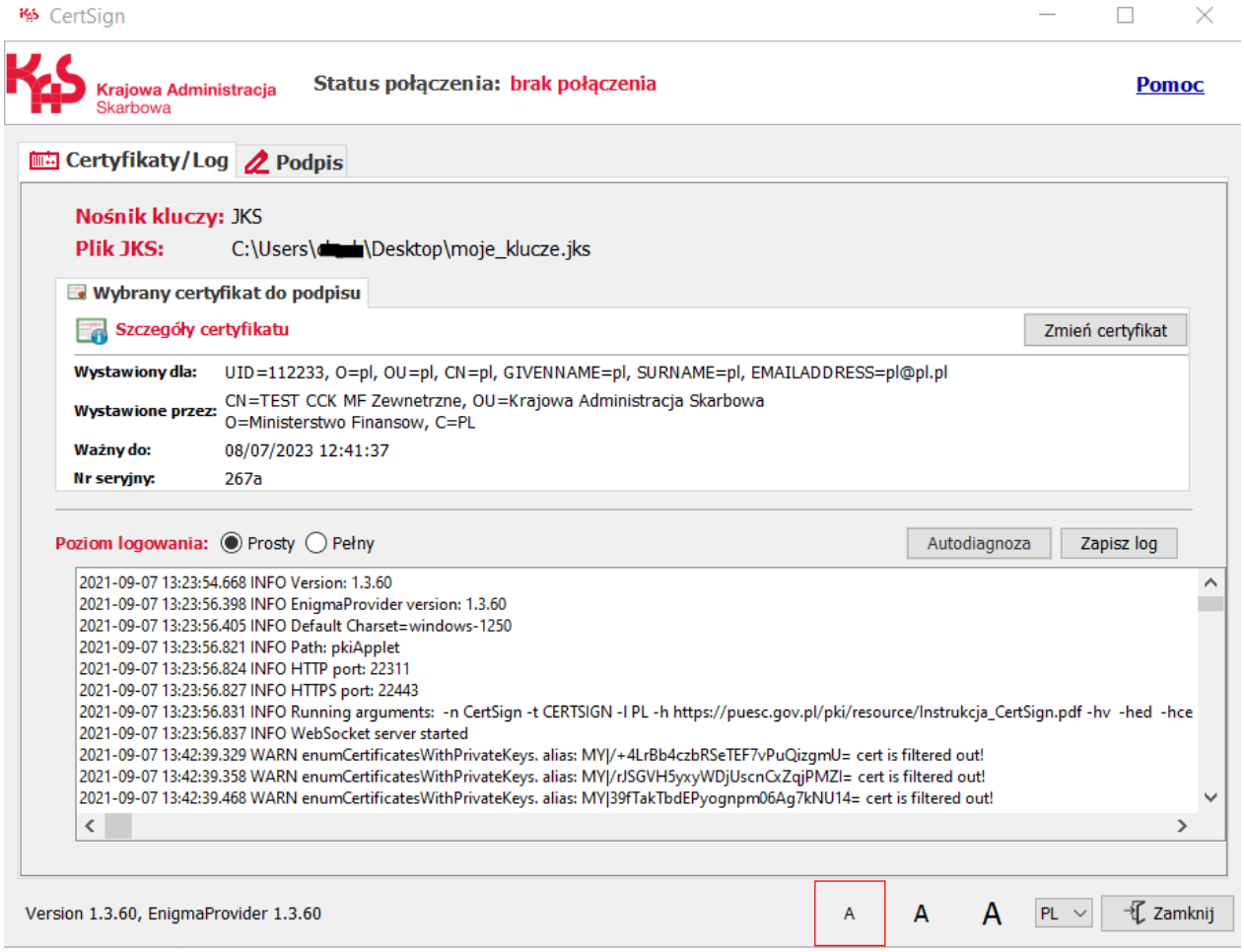
Dokument potwierdzający wydanie certyfikatu zalecamy wydrukować i przechowywać w bezpiecznym miejscu, ponieważ zawiera on kod pozwalający na zawieszenie lub unieważnienie certyfikatu za pośrednictwem help-desk.

Dokument potwierdzający wydanie certyfikatu oraz część publiczną certyfikatu (bez klucza prywatnego), można pobrać ponownie, zgodnie z opisem w rozdziale 7.

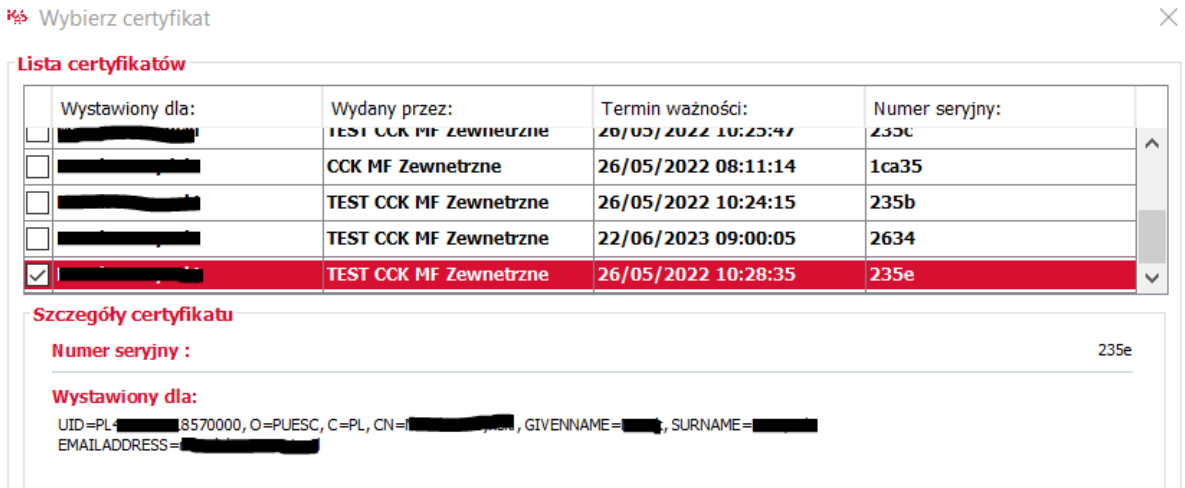
5. Wykonanie podpisu elektronicznego

Wykonanie podpisu elektronicznego jest możliwe w trybie online (na stronie PUESC), oraz w trybie offline – lokalnie, poprzez wskazanie plików z dysku komputera. W obu przypadkach aplikacja CertSign musi być uruchomiona, jednak przy podpisywaniu w trybie offline (lokalnym), nie jest konieczne nawiązywanie połączenia ze stroną PUESC.

Przycisk *Zmień certyfikat* w zakładce *Certyfikaty/Log*, służy do wybrania certyfikatu podpisującego.



Jeśli w zakładce *Certyfikaty/Log* nie jest wyświetlany żaden certyfikat, należy wybrać *Zmień certyfikat,* zaznaczyć na liście właściwy certyfikat (zostanie on podświetlony), następnie zatwierdzić przyciskiem *OK*.



Po wybraniu certyfikatu jego szczegóły zostaną wyświetlone oknie *Szczegóły certyfikatu do podpisów.* **Okno wyboru nie wyświetla certyfikatów, których termin ważności upłynął.**

W przypadku certyfikatów zapisanych na karcie kryptograficznej i poprawnie zainstalowanych w systemie operacyjnym, wyświetlą się one na liście dopiero **po włożeniu karty do czytnika.**

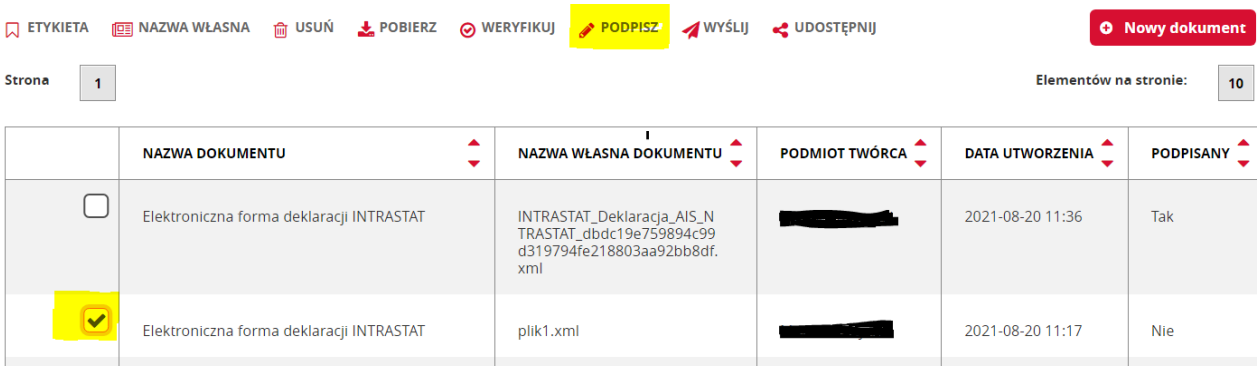
Certyfikaty kwalifikowane wykorzystywane w systemie Windows należy uprzednio zarejestrować w systemowym magazynie certyfikatów.

5.1 Wykonanie podpisu elektronicznego na PUESC

Wykonanie podpisu elektronicznego możliwe jest po poprawnym wypełnieniu i wygenerowaniu dokumentów na portalu. Podpisanie dokumentów (wniosków, pism) dostępne jest w widoku *Mój Pulpit* > *Do wysyłki i robocze* > *Dokumenty do wysyłki*.
Aplikacja CertSign umożliwia złożenie podpisu przy użyciu certyfikatu kwalifikowanego, certyfikatu zawartego w warstwie elektronicznej dowodu osobistego (podpis osobisty) lub certyfikatu celnego (niekwalifikowanego) – w zależności od rodzajów podpisów dopuszczonych dla danego dokumentu.
W przypadku wykorzystywania certyfikatu kwalifikowanego w systemie Windows - należy zainstalować dostarczone z nim oprogramowanie w komputerze użytkownika, a następnie przeprowadzić proces rejestracji posiadanego certyfikatu kwalifikowanego w systemowym magazynie certyfikatów (zgodnie z dokumentacją certyfikatu kwalifikowanego). Oprogramowanie dostarczane przez polskie centra kwalifikowane z reguły automatycznie instaluje certyfikat kwalifikowany w magazynie certyfikatów systemu Windows.
Analogicznie, **w przypadku wykorzystania podpisu osobistego (danymi w warstwie elektronicznej dowodu osobistego)** należy uprzednio zainstalować i skonfigurować czytnik i oprogramowanie. Opis jest w Dodatku B.

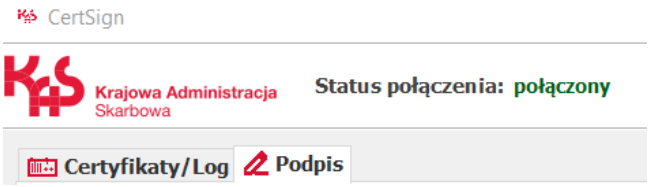
Operacja złożenia podpisu jest możliwa tylko w stosunku do dokumentów, które wcześniej nie zostały podpisane. Dokument niepodpisany oznaczony jest w kolumnie „*Podpisany*" wartością „*Nie*", a dokument podpisany wartością „*Tak*"
W celu złożenia podpisu elektronicznego na dokumencie do wysyłki należy:

a) w zakładce *Do wysyłki i robocze* > *Do wysyłki,* w pierwszej kolumnie tabeli, za pomocą check-box wskazać dokument do podpisu; następnie wybrać akcję *Podpisz*.

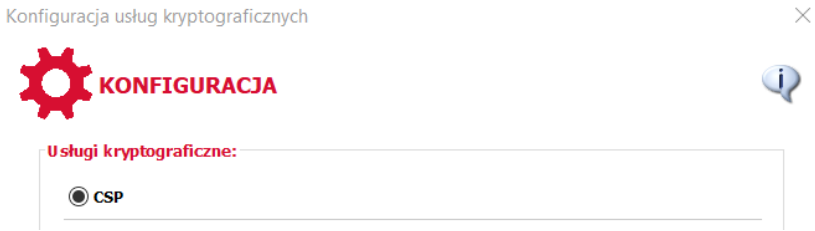


System wyświetli okno z opcją wyboru metody podpisywania dokumentu. Należy zaznaczyć właściwą metodę podpisu i zatwierdzić przyciskiem *Podpisz*.

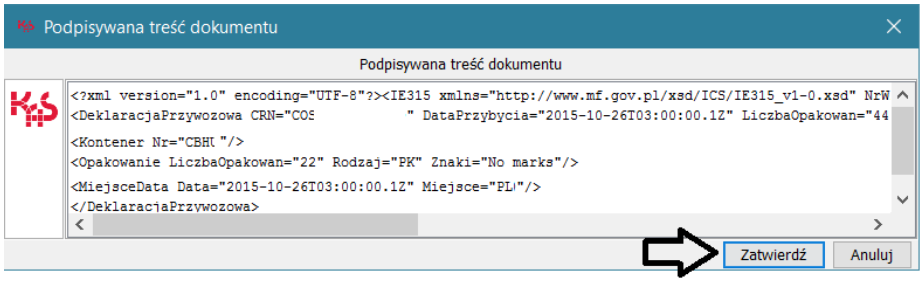
Opcje: ***podpis kwalifikowany, certyfikat celny, podpis osobisty,*** spowodują uruchomienie podpisywania w aplikacji CertSign. ***Podpis profilem zaufanym ePUAP*** przekieruje do serwisu dostawcy podpisu zaufanego.
Wybranie *Podpis kwalifikowany* lub *Certyfikat celny lub Podpis osobisty* uruchomi aplikację CertSign i spowoduje nawiązanie połączenia między stroną PUESC i aplikacją. Ponieważ połączenie nawiązywane jest przez kilka sekund, status połączenia może zmienić się po dłuższej chwili.



5.2 Wykonanie podpisu z certyfikatem w magazynie Windows (CSP)

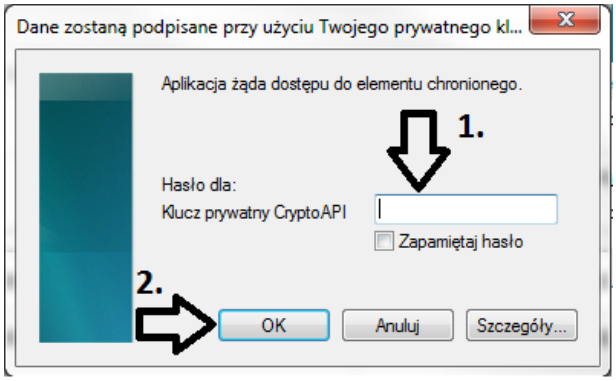


Po zatwierdzeniu sposobu dostępu do certyfikatu, aplikacja podpisująca wyświetli dane przeznaczone do podpisu w takiej formie, w jakiej trafiają do SISC.



Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem *Zatwierdź*. Aplikacja wykona podpis z użyciem wcześniej wskazanego certyfikatu.
Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego. W zależności od sposobu przechowywania certyfikatu i rodzaju samego certyfikatu, możliwe jest pojawienie się następujących okien:

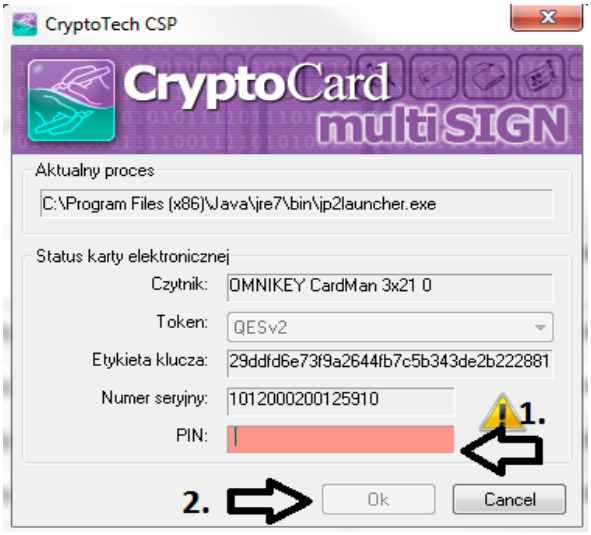
a) W przypadku certyfikatu celnego zapisanego w systemie Windows i nieznajdującego się na karcie kryptograficznej:



Należy podać hasło dostępu do certyfikatu (1) i następnie zatwierdzić przyciskiem „*OK*”(2)".

b) W przypadku certyfikatu kwalifikowanego, zapisanego na karcie kryptograficznej, zostanie wyświetlone okno dialogowe oprogramowania obsługującego kwalifikowaną kartę kryptograficzną. Okno to może mieć różny wygląd, w zależności od rodzaju posiadanej karty i zainstalowanego oprogramowania do jej obsługi.

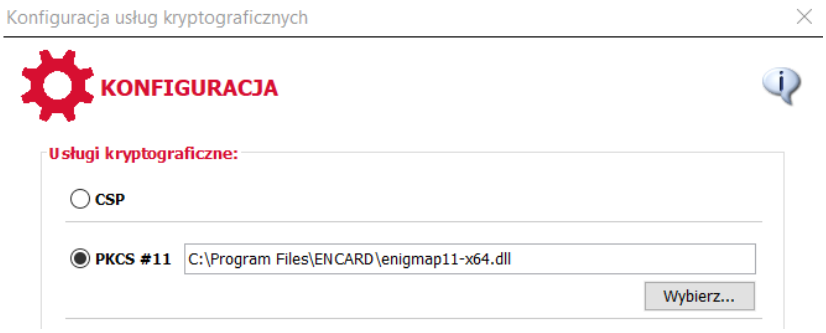
Przykładowy widok dla certyfikatu kwalifikowanego wydanego przez polskie centrum certyfikacji



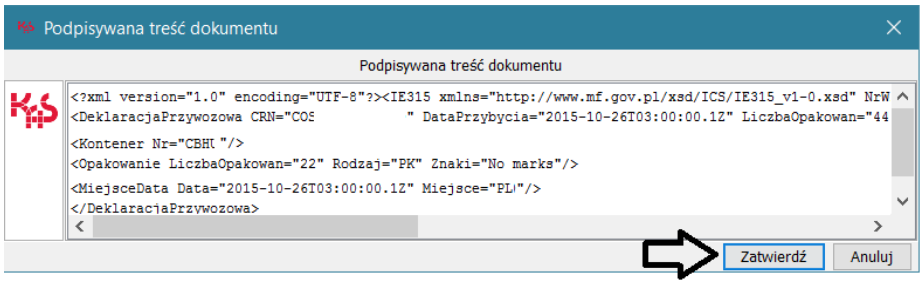
Należy podać PIN do karty (1) i zatwierdzić przyciskiem „OK” (2).
Po przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem „*Tak*” w kolumnie „*Podpisany*”

5.3 Wykonanie podpisu z karty kryptograficznej zgodnej z PKCS#11



Aplikacja podpisująca wyświetli dane przeznaczone do podpisu w takiej w formie, w jakiej trafiają do SISC.

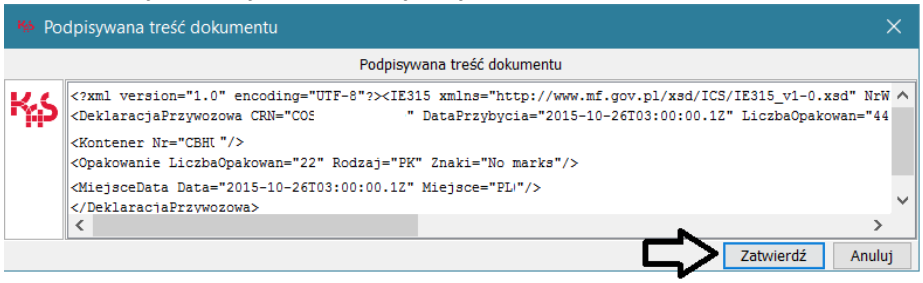


Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem *Zatwierdź*.
Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego. Okno może różnić się wyglądem, w zależności od rodzaju posiadanej karty i zainstalowanego oprogramowania do jej obsługi.
Po poprawnym przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem „*Tak*” w kolumnie „*Podpisany*”

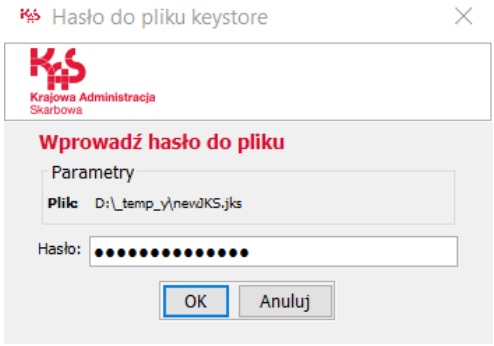
5.4 Wykonanie podpisu z certyfikatem (kluczem) zapisanym w pliku *Keystore*

Aplikacja korzysta z wybranego pliku *Keystore*, przechowującego klucze i certyfikaty. Podpisywany dokument jest prezentowany w takiej w formie, w jakiej trafia do SISC.



Należy potwierdzić prawidłowość wprowadzonych danych przyciskiem „Zatwierdź”.

Zostanie wyświetlone okno dialogowe, w którym należy podać hasło (PIN), chroniące dostęp do klucza prywatnego.

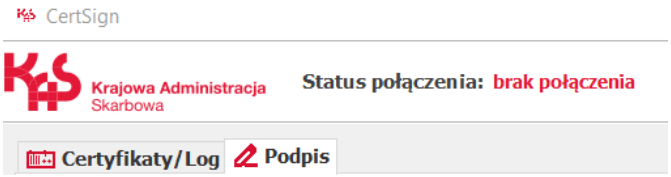


Po poprawnym przesłaniu podpisanego dokumentu portal PUESC wyświetla komunikat:

Podpisany dokument prezentowany jest w tabeli dokumentów do wysyłki ze statusem „*Tak*" w kolumnie „*Podpisany*"

5.5 Wykonanie podpisu elektronicznego lokalnie na komputerze – w trybie offline

Wykonanie podpisu lokalnie polega na wskazaniu, w aplikacji CertSign, położenia pliku do podpisania na dysku komputera. Plik ten może być uprzednio pobrany z PUESC. **W tym przypadku nie jest konieczne połączenie strony PUESC z aplikacją.**



By podpisanie pliku było możliwe, w zakładce *Certyfikaty/Log* powinien być wybrany certyfikat podpisujący.

W zakładce *Podpis* dostępne są funkcje wykonania podpisu elektronicznego. Należy wskazać położenie na dysku komputera pliku, lub plików do podpisania, oraz folderu docelowego; ewentualnie wybrać format i typ podpisu, następnie zatwierdzić operację przyciskiem *Podpisz pliki*.
W menu *Poziom podpisu* ustala się, czy na wskazanym pliku ma być wykonany wyłącznie podpis elektroniczny (poziom „BES") czy też do podpisu ma być dodany elektroniczny znacznik czasu (poziom „T").
W przypadku dodania znacznika czasu konieczne jest wskazanie, w *Ustawieniach,* adresu serwera znacznika czasu (do którego użytkownik ma dostęp).

Dla formularzy przesyłanych na PUESC należy w parametrach podpisu wybrać format podpisu XAdES, typ Otoczony.

Opcja ***Sugeruj formaty podpisu*** zapewnia automatyczne dostosowanie parametrów, na podstawie typu pliku wybranego do podpisania. Odznaczenie tej opcji odblokowuje możliwość ręcznego ustawiania parametrów.

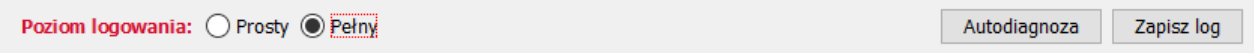
6. Zgłaszanie problemów, przeglądanie logów

6.1 Dane potrzebne do analizy problemów z działaniem aplikacji

- System operacyjny - rodzaj i wersja, wersja językowa systemu (np.: Windows 10 – wersja Polska)
- Rodzaj i wersja przeglądarki internetowej
- Log z konsoli aplikacji CertSign
- Widok ekranu z błędem – cały ekran (przycisk klawiaturowy PrtScr)
- Dokładny opis problemu, okoliczności wystąpienia.
- Wynik autodiagnozy aplikacji.

6.2 Włączanie logowania w aplikacji CertSign

Aplikacja CertSign umożliwia włączenie „pełnego” logowania zdarzeń z działania aplikacji. W celu uruchomienia pełnego logowania należy w oknie aplikacji przestawić Poziom logowania na „Pełny”.

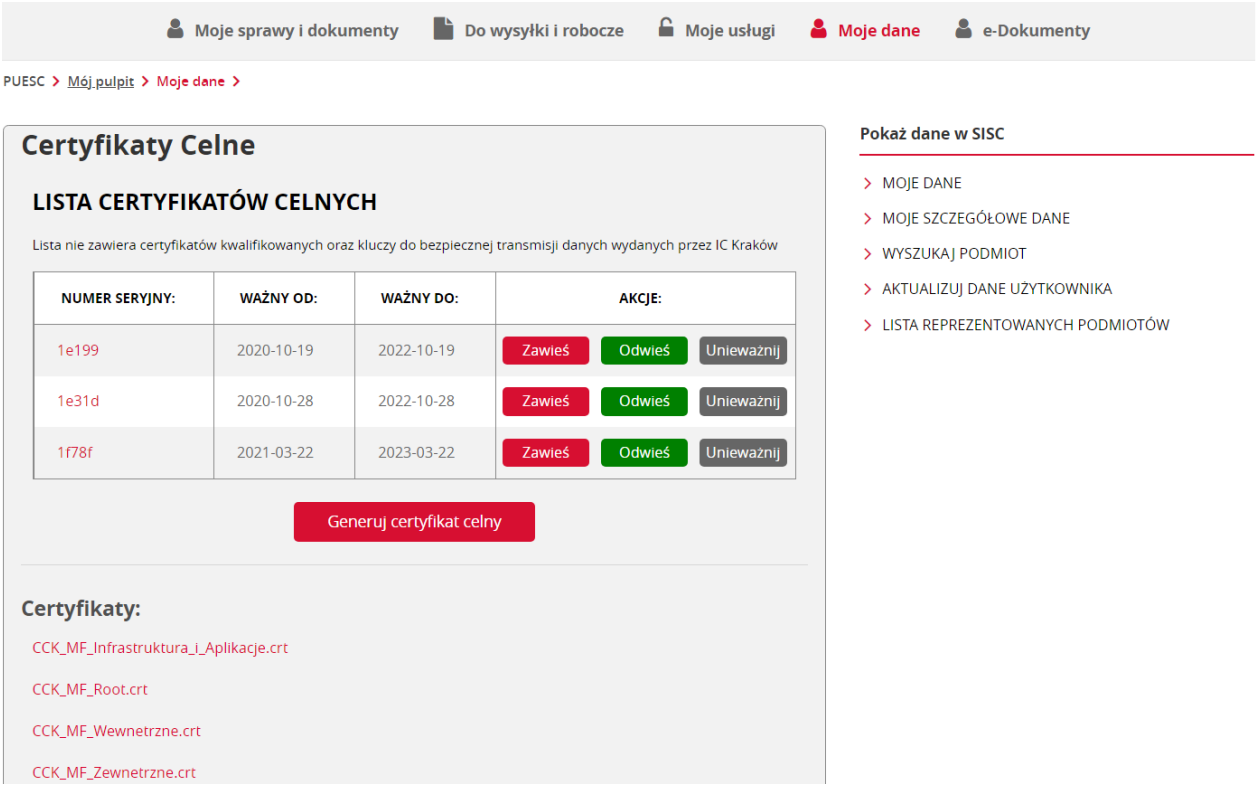


W oknie poniżej zaczną wyświetlać się logi z działania aplikacji, które można zapisać klikając przycisk „Zapisz log”
Zapisane logi w przypadku błędów należy załączyć do zgłoszenia w HELPDESK.

7. Pobranie certyfikatu lub dokumentu potwierdzenia z konta na PUESC

Dedykowany widok certyfikatów celnych na PUESC jest dostępny z bocznego menu w widoku Mój pulpit > Moje dane > Certyfikaty celne. Składa się on z dwóch głównych obszarów:

1. Lista certyfikatów celnych użytkownika – w tej części widoku użytkownik ma możliwość przeglądania listy swoich certyfikatów celnych. Klikając w wyróżniony na czerwono numer seryjny, użytkownik ma możliwość podglądu certyfikatu oraz jego pobrania.
2. Dodatkowe pliki – sekcja ta zawiera certyfikaty do pobrania oraz dokumentację związaną z certyfikatami.



W celu pobrania certyfikatu, lub dokumentu potwierdzenia wydania certyfikatu, należy kliknąć na nr seryjny certyfikatu. Zostanie wyświetlone okno:

W celu pobrania dokumentu potwierdzającego należy kliknąć przycisk *Pobierz potwierdzenie* (1). W celu pobrania certyfikatu (części publicznej) należy kliknąć przycisk *Zapisz certyfikat* (2).

UWAGA! Pobrana zostanie tylko część publiczna certyfikatu. Część prywatna nie jest przechowywana w SISC i nie jest możliwe jej odzyskanie.

8. Aktualizacja aplikacji CertSign

Aplikacja CertSign posiada wbudowany mechanizm sprawdzania aktualizacji. Po stwierdzeniu dostępności aktualizacji zostanie wyświetlony komunikat z propozycją jej pobrania. Możliwe jest pobranie aktualizacji lub rezygnacja (anulowanie). W przypadku pobrania aktualizacji instalator zaproponuje jej zainstalowanie. Instalację można wykonać od razu lub odłożyć na później. Instalacja nowej wersji nie kasuje ustawień dotyczących certyfikatu użytkownika.

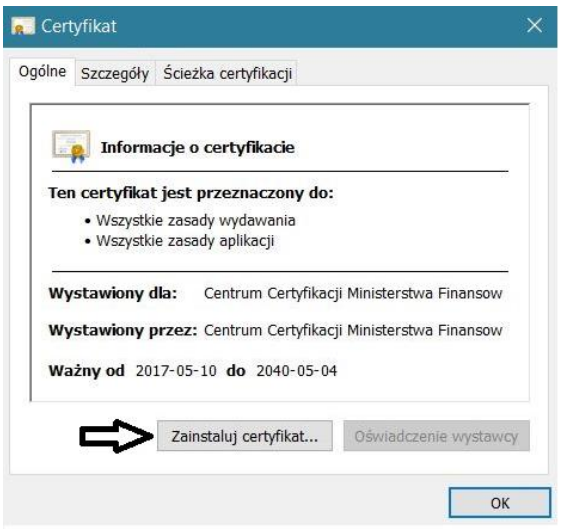
9. Dodatek A

A.1 Manualna instalacja certyfikatów w systemie Windows

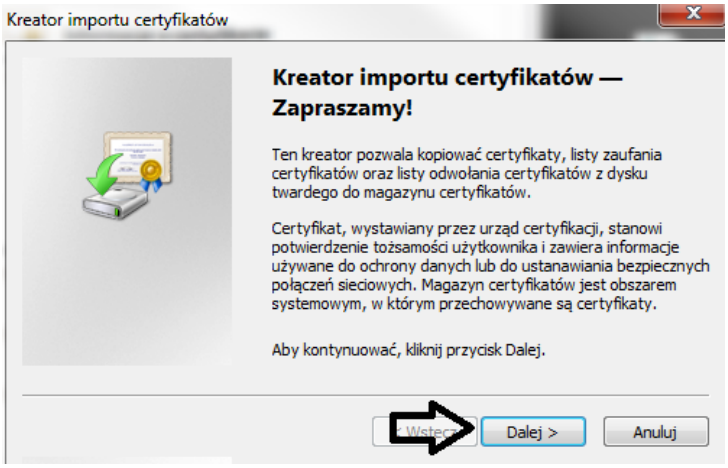
W celu poprawnej weryfikacji certyfikatów celnych konieczne jest zainstalowanie w systemie certyfikatów centrów certyfikacji, do których odnośniki znajdują się na https://puesc.gov.pl/uslugi/uzyskaj-lub-uniewaznij-certyfikat-celny
Aby zainstalować certyfikaty Centrum Certyfikacji MF należy w wyświetlonym widoku odszukać i pobrać na komputer certyfikaty:

- CCK MF Root,
- CCK MF Zewnetrzne,
- CCK MF Wewnetrzne,
- CCK MF Infrastruktura i Aplikacje

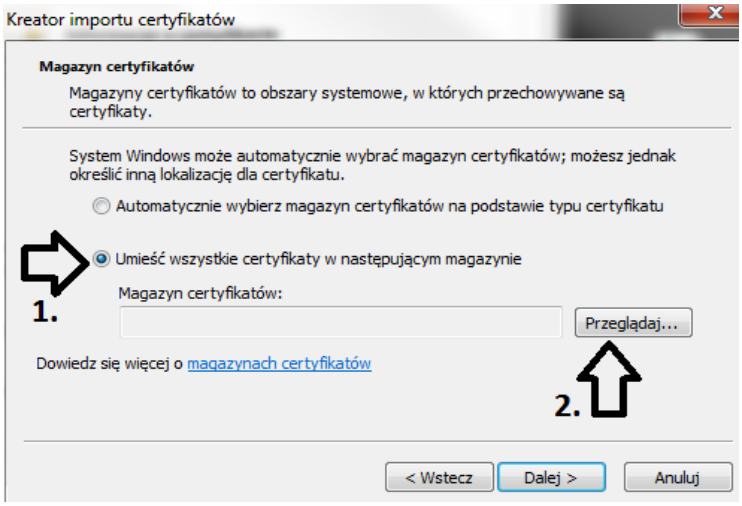
Po pobraniu pliku certyfikatu należy na nim dwukrotnie kliknąć – spowoduje to wyświetlenie okna prezentującego certyfikat. Następnie kliknąć przycisk „Zainstaluj certyfikat”



Zostanie uruchomiony „Kreator importu certyfikatów”.

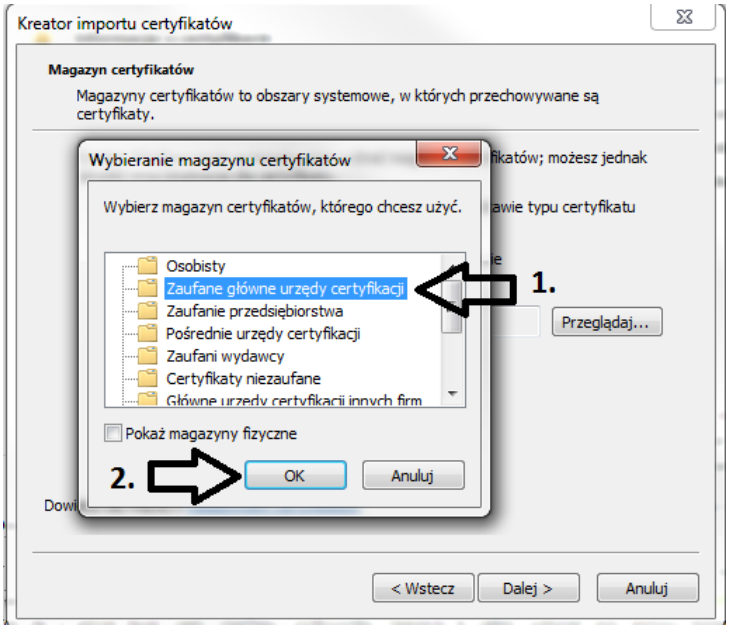


W oknie należy wybrać przycisk *„Dalej”.*
W kolejnym oknie należy zaznaczyć opcję *„Umieść wszystkie certyfikaty w następującym magazynie”(1),* następnie wybrać *„Przeglądaj” (2).*

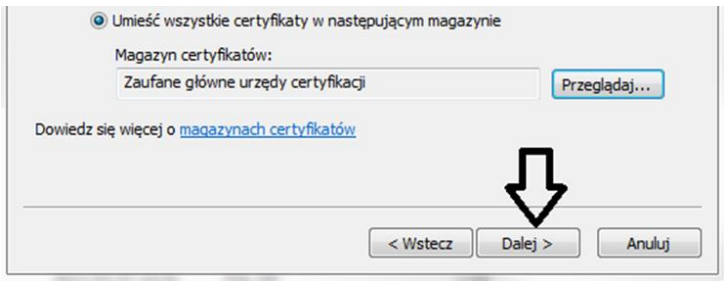


Certyfikat CCK MF Root należy umieszczać w magazynie „Zaufane główne urzędy certyfikacji". Certyfikaty CCK MF Zewnetrzne, CCK MF Wewnetrzne, CCK MF Infrastruktura i Aplikacje należy umieszczać w magazynie „Pośrednie urzędy certyfikacji"
W dalszej części pokazane zostały widoki ekranów dla procesu instalacji certyfikatu CCK MF Root.

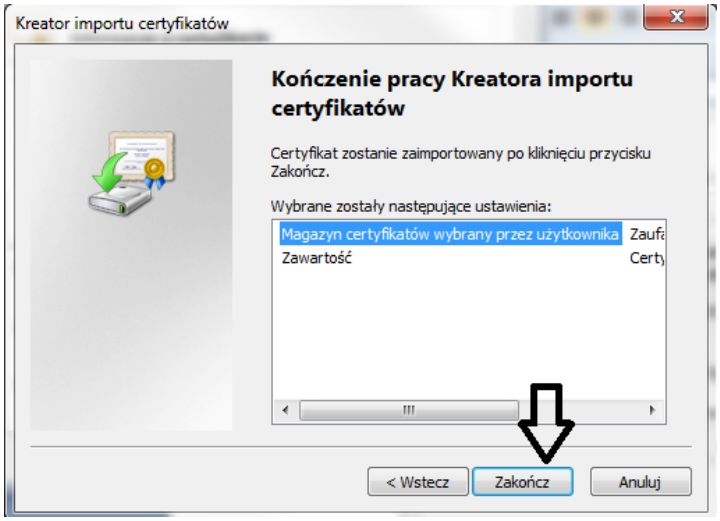
1. Otworzy się okno wyboru magazynu certyfikatów.



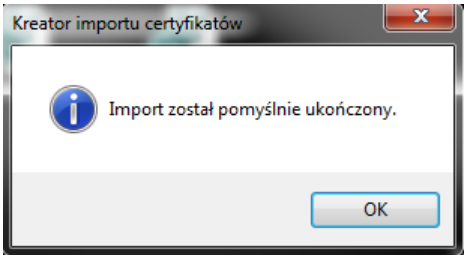
Należy wybrać *Zaufane główne urzędy certyfikacji* (1) i zatwierdzić wybór przyciskiem *OK* (2). Kontynuować zatwierdzając przyciskiem *Dalej.*



W oknie *Kończenie pracy kreatora importu certyfikatów* wybrać *Zakończ*.



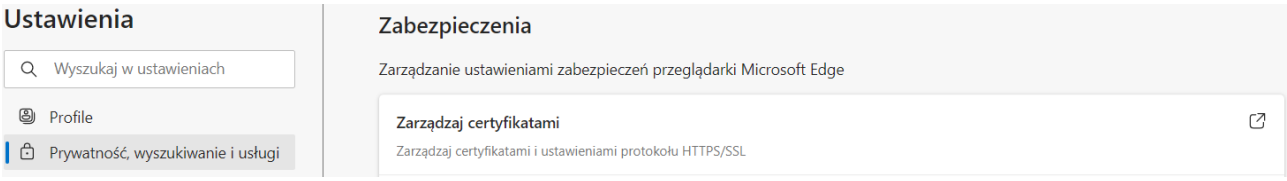
Po poprawnym zakończeniu importu certyfikatu pojawia się komunikat:



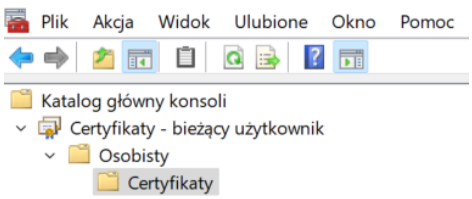
Procedurę należy powtórzyć dla pozostałych certyfikatów CCK MF.

A.2 Weryfikacja poprawności certyfikatu osobistego w systemie Windows

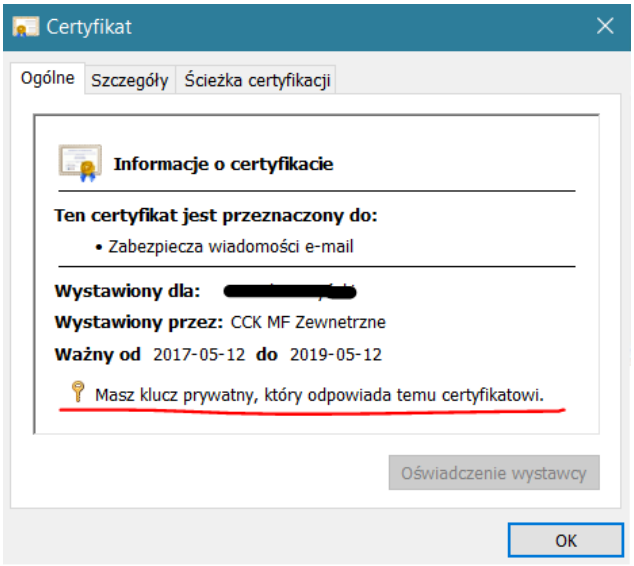
W celu sprawdzenia poprawności zainstalowanego w systemie Windows certyfikatu osobistego można uruchomić przeglądarkę Internet Explorer, następnie wybrać *Narzędzia* > *Opcje internetowe* > *Zawartość* > *Certyfikaty*
Podgląd magazynu certyfikatów można wywołać również z przeglądarki Edge, wybierając *Ustawienia* > *Prywatność, wyszukiwanie i usługi* > *Zabezpieczenia* > *Zarządzaj certyfikatami*



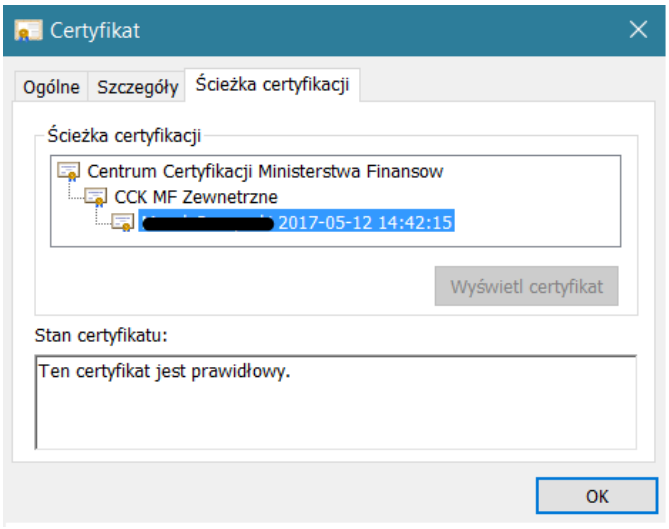
Trzecią możliwością (dla zaawansowanych użytkowników) jest uruchomienie systemowej konsoli *mmc*, dodanie przystawki *Certyfikaty – bieżący użytkownik* i wyświetlenie certyfikatów w gałęzi *Osobisty*.



W celu przeglądania wybranego certyfikatu należy kliknąć go dwukrotnie. Otwarty zostanie widok zawartości. W przypadku certyfikatu osobistego na pierwszej zakładce powinien znajdować się napis „**Masz klucz prywatny, który odpowiada temu certyfikatowi**”. Brak klucza prywatnego uniemożliwia złożenie podpisu elektronicznego.



Następnie należy przejść na zakładkę *Ścieżka certyfikacji*. W przypadku poprawnej instalacji certyfikatów, w wyświetlonym oknie będą znajdowały się certyfikaty centrum certyfikacji oraz certyfikat osobisty.

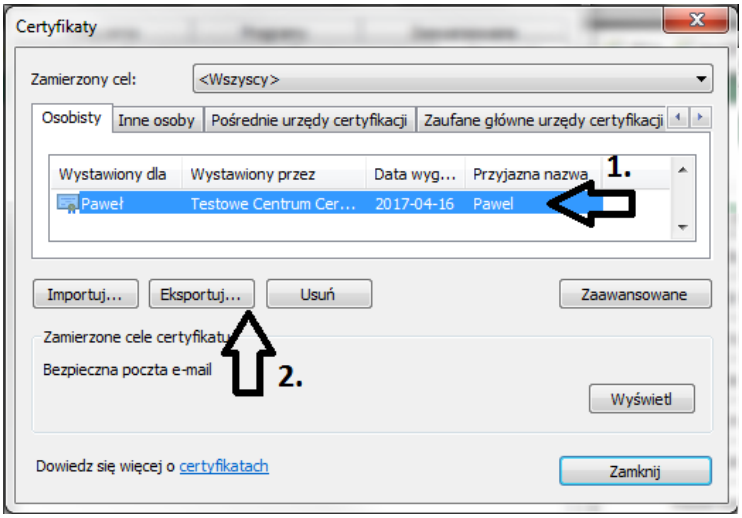


Jeśli na ikonie certyfikatów powyżej certyfikatu osobistego znajduje się dodatkowy znak („x” w czerwonym kole), oznacza to, że ten certyfikat nie został zainstalowany lub jest nieprawidłowy i ścieżka certyfikacji nie może zostać poprawnie zbudowana. Należy w takiej sytuacji pobrać i zainstalować brakujący certyfikat.

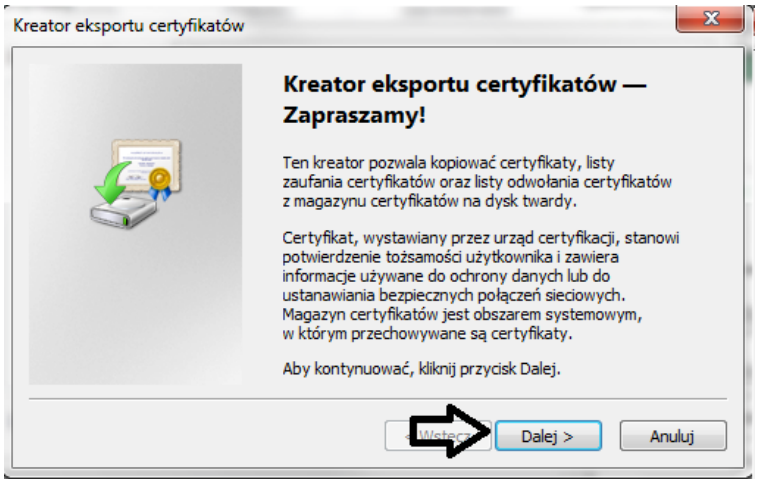
A.3 Eksport certyfikatu z magazynu certyfikatów systemu Windows

W celu wyeksportowania certyfikatu zainstalowanego w magazynie systemu Windows (CSP) należy wyświetlić magazyn certyfikatów poprzez przeglądarkę Internet Explorer (*Narzędzia* > *Opcje internetowe* > *Zawartość* > *Certyfikaty)* lub przeglądarkę Edge (*Ustawienia* > *Prywatność, wyszukiwanie i usługi* > *Zabezpieczenia* > *Zarządzaj certyfikatami)* – analogicznie jak opisano we wstępie do A.2.

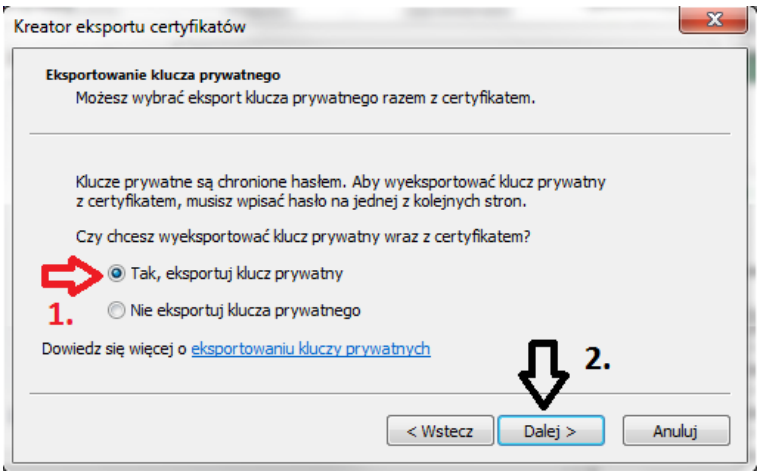
W oknie *Certyfikaty* na zakładce *Osobisty* należy zaznaczyć certyfikat do eksportu (1), a następnie kliknąć przycisk *Eksportuj* (2)



Zostanie wyświetlone okno Kreatora eksportu certyfikatów

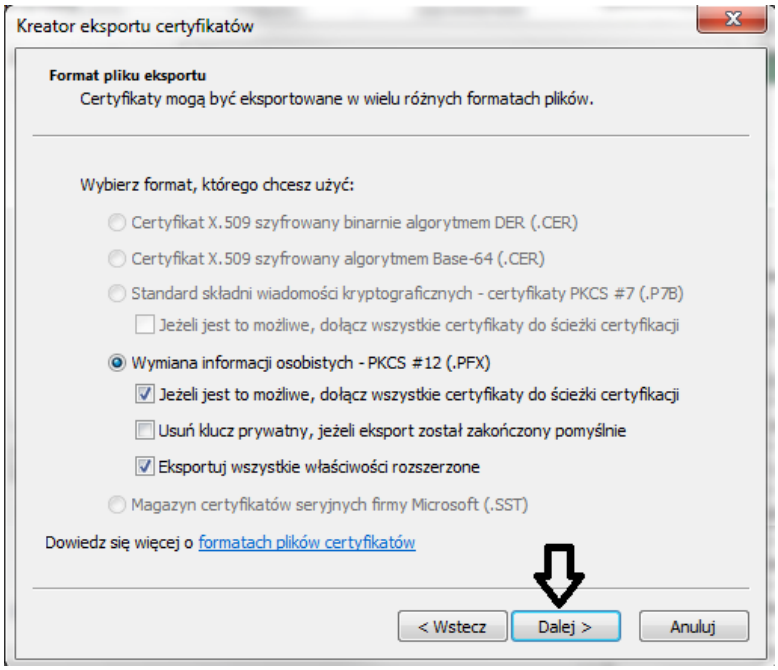


Następnie należy kliknąć przycisk *Dalej*
W oknie Eksportu klucza prywatnego należy zaznaczyć opcję *Tak, eksportuj klucz prywatny* (1)

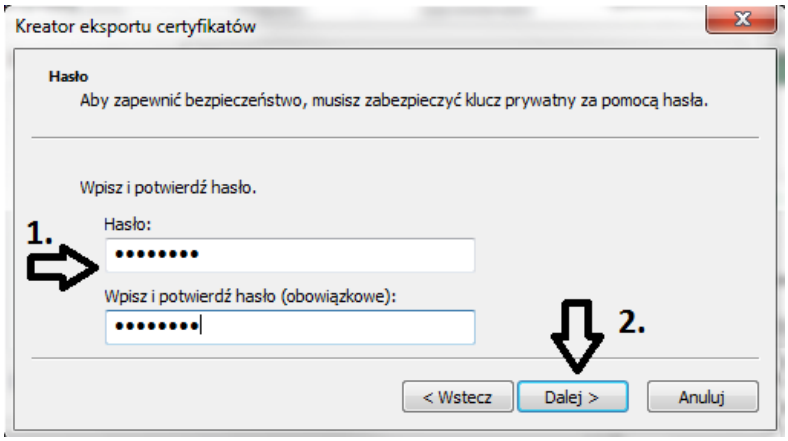


Następnie należy kliknąć przycisk *Dalej* (2)

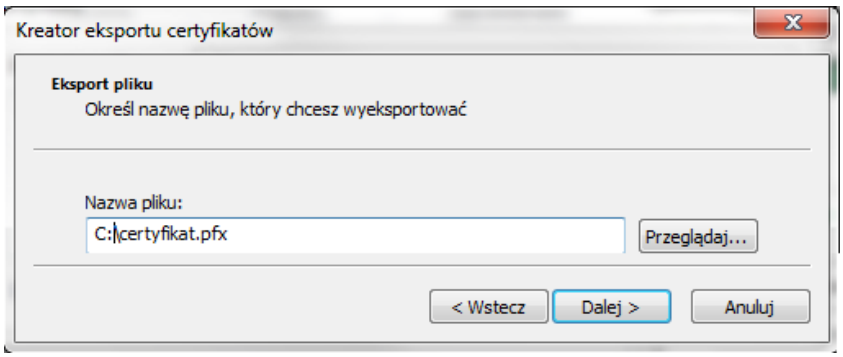
Jeśli certyfikat ma być nadal użytkowany na komputerze, z którego jest eksportowany, należy zaznaczyć opcje jak na widoku poniżej. W przeciwnym wypadku należy także zaznaczyć opcję *Usuń klucz prywatny* …



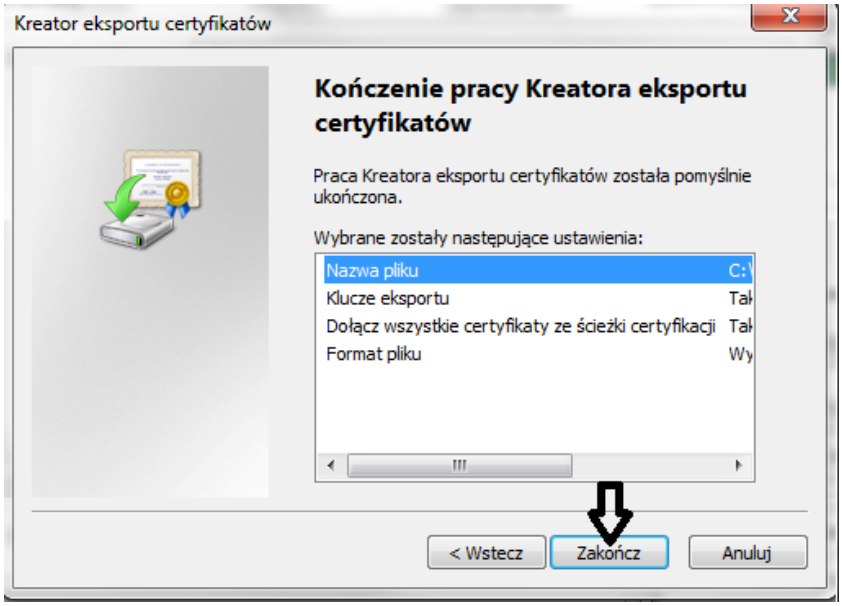
Następnie należy kliknąć przycisk *Dalej.* W kolejnym kroku należy ustawić hasło zabezpieczające eksportowany certyfikat (1) oraz kliknąć przycisk *Dalej.*



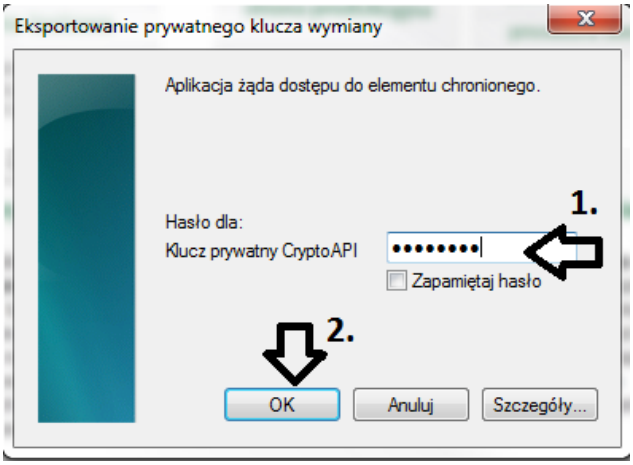
W kolejnym kroku podać nazwę pliku, do którego zostanie wyeksportowany certyfikat i wybrać *Dalej*.



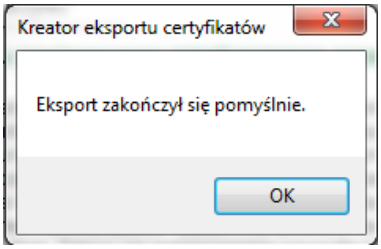
W celu zakończenia procesy należy kliknąć przycisk *Zakończ.*



System rozpocznie eksportowanie certyfikatu i wyświetli okno z pytaniem o hasło, którym jest zabezpieczony klucz prywatny. Jest to hasło, które zostało podane w momencie generowania certyfikatu - **nie jest to hasło podawane w kroku „*hasło zabezpieczające eksportowany certyfikat*”**.

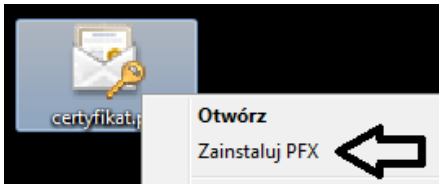


Należy podać poprawne hasło (1) i kliknąć przycisk *OK.* (2)
Jeśli zostało podane poprawne hasło, certyfikat zostanie wyeksportowany i zapisany we wskazanym pliku, a system wyświetli komunikat potwierdzający:

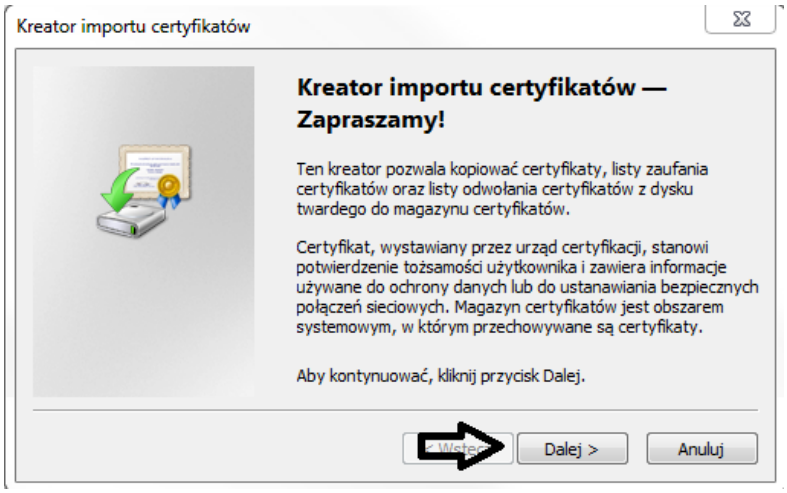


A.4 Import certyfikatu do magazynu certyfikatów systemu Windows (CSP)

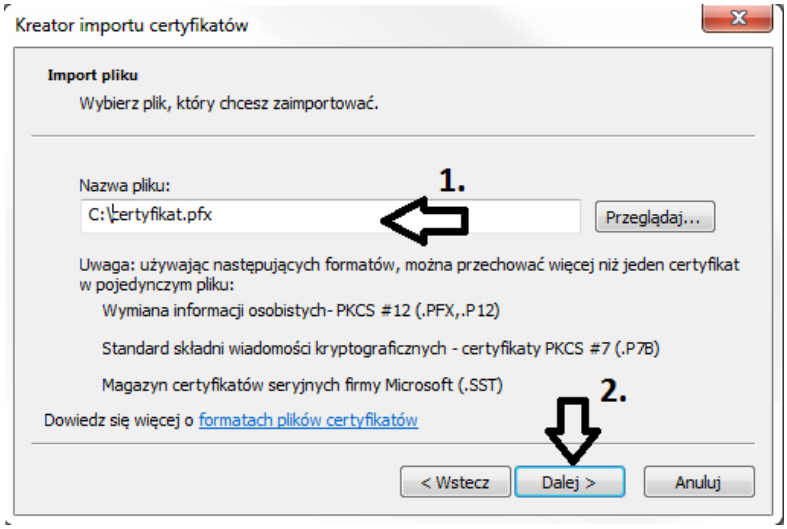
W celu zaimportowania uprzednio wyeksportowanego certyfikatu, należy zaznaczyć plik *.pfx (lub *.p12) z wyeksportowanym certyfikatem i kliknąć prawy przycisk myszy



Zostanie wyświetlone menu, z którego należy wybrać: „*Zainstaluj PFX”*

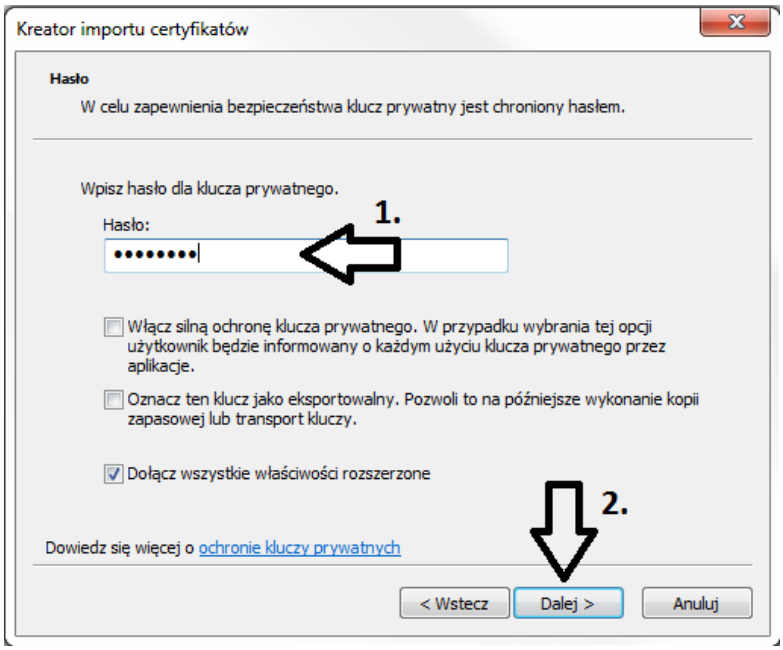


Następnie należy kliknąć przycisk *Dalej*. Zostanie wyświetlone okno Kreatora importu certyfikatów

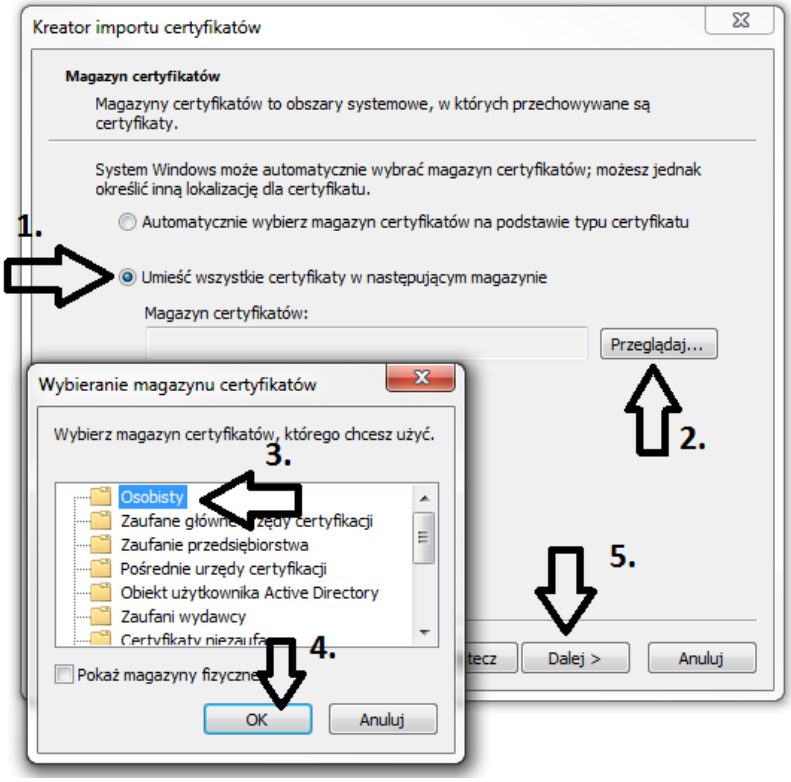


W polu *nazwa pliku* zostanie automatycznie wpisana ścieżka do pliku z wyeksportowanym certyfikatem. Jeśli pole jest puste, należy wskazać w nim plik z wyeksportowanym certyfikatem (1) i następnie kliknąć przycisk *Dalej* (2)
Zostanie wyświetlone okno z pytaniem o hasło zabezpieczające eksportowany certyfikat (1) – hasło zostało podawane w trakcie eksportu certyfikatu w oknie *Hasło* – kreatora eksportu certyfikatów.

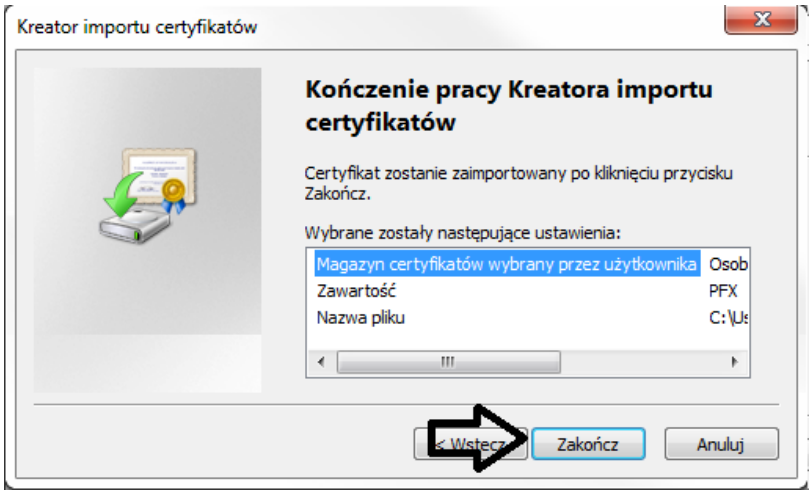
Jeżeli chcemy umożliwić dalszy eksport certyfikatu w przyszłości należy zaznaczyć opcję *Oznacz ten klucz jako eksportowany* … (aczkolwiek kolejne eksporty stanowią dodatkowe ryzyko utraty kontroli nad kluczem prywatnym, więc nie należy nadużywać tej opcji).)



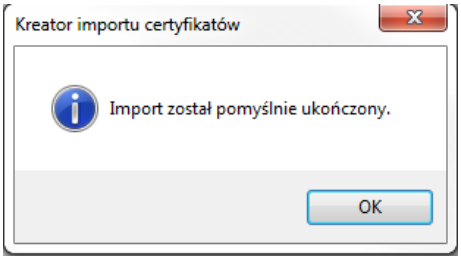
Następnie należy kliknąć przycisk *Dalej*. Zostanie wyświetlone okno wyboru magazynu certyfikatów w systemie Windows.



Należy zaznaczyć opcję *Umieść wszystkie certyfikaty w następującym magazynie* (1), następnie wybrać *Przeglądaj* (2). Otworzy się okno wyboru magazynu certyfikatów, gdzie należy wybrać *Osobisty* (3). Następnie kliknąć przycisk *OK* (4) i przycisk *Dalej* (5)



W celu zakończenia procesu należy kliknąć przycisk *Zakończ.*
Po poprawnym zakończeniu procesu importu certyfikatu zostanie wyświetlone okno z potwierdzeniem zakończenia procesu.



Należy kliknąć przycisk *OK.* Po zakończeniu procesu importu certyfikatu należy zweryfikować jego poprawność zgodnie z procedurą opisaną w Dodatku A.2. Jeśli konieczne jest doinstalowanie certyfikatów centrum certyfikacji, należy postępować zgodnie z instrukcjami z Dodatku A.1.

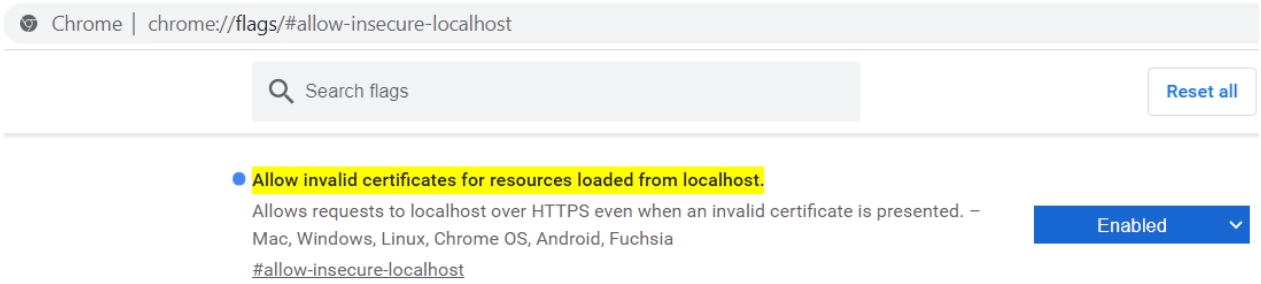
A.5 Opis opcji Konfiguracja usług kryptograficznych

1. **CSP** – domyślny sposób przechowywania certyfikatów w systemie Windows. Certyfikaty zapisane w systemie Windows umożliwiają wyeksportowanie ich i zainstalowanie na innym komputerze. Jeżeli w systemie Windows zainstalowano uprzednio sterowniki karty kryptograficznej, zgodne ze standardem CSP, możliwe będzie generowanie kluczy i zapisanie certyfikatu bezpośrednio na karcie kryptograficznej użytkownika. Jeśli aplikacja do generowania certyfikatów nigdy nie była uruchamiana, opcja CSP jest domyślnie wybrana.
2. **PKCS#11** – standard dla kart kryptograficznych, alternatywny sposób przechowywania certyfikatów, niezależny od posiadanego systemu operacyjnego. Może mieć zastosowanie między innymi w systemie Linux. Wygenerowany certyfikat zostanie zapisany na karcie kryptograficznej zgodnej z PKCS#11. Jest to najbezpieczniejsza metoda przechowywania kluczy kryptograficznych i certyfikatu, umożliwiająca wykorzystanie certyfikatu na wielu komputerach. W procesie konfiguracji konieczne będzie wskazanie lokalizacji sterownika PKCS#11 (informacje o tym powinny być uprzednio dostarczone przez producenta lub dystrybutora posiadanej karty kryptograficznej).
3. **Keystore** – alternatywny sposób przechowywania certyfikatów, obsługiwany przez mechanizmy Java™ (JKS – Java KeyStore). Metoda ta jest niezależna od posiadanego systemu operacyjnego. Należy mieć na uwadze, że wygenerowane w ten sposób certyfikaty mogą być niewidoczne dla aplikacji systemu Windows.

A.6 Rozwiązanie problemów z połączeniem strony PUESC z aplikacją CertSign

Strona PUESC nawiązuje połączenie z CertSign **w czasie generowania certyfikatu lub podpisywania dokumentu**. W pozostałym czasie CertSign wskazuje status **brak połączenia,** co jest sytuacją normalną. Główne przyczyny braku połączenia podczas generowania certyfikatu lub podpisywania dokumentu na PUESC (w trybie online) to brak certyfikatów CCK MF lub blokowanie połączeń localhost przez zaporę Windows, oprogramowanie antywirusowe lub inne mechanizmy zabezpieczeń. Mogą zdarzyć się specyficzne sytuacje, związane z indywidualną konfiguracją komputera czy oprogramowania.

W przeglądarce Chrome może wystąpić problem z połączeniem przeglądarki z aplikacją CertSign Rozwiązaniem jest zmiana w konfiguracji przeglądarki. Należy wejść w zaawansowane opcje Chrome, wpisując w pasku adresu: *chrome://flags/#allow-insecure-localhost* i ustawić wartość na *Enabled.*



Następnie należy ponownie uruchomić przeglądarkę.

A.7 Weryfikacja poprawności podpisu na portalu PUESC

W celu zweryfikowania poprawności podpisu na PUESC należy:

1. Wybrać dokument z *Mój pulpit* > *Do wysyłki i robocze*, klikając jego nazwę.
2. Wybrać akcję *Weryfikuj podpis.*

Po wybraniu akcji system zweryfikuje poprawność podpisu i wyświetli komunikat z wynikiem weryfikacji.

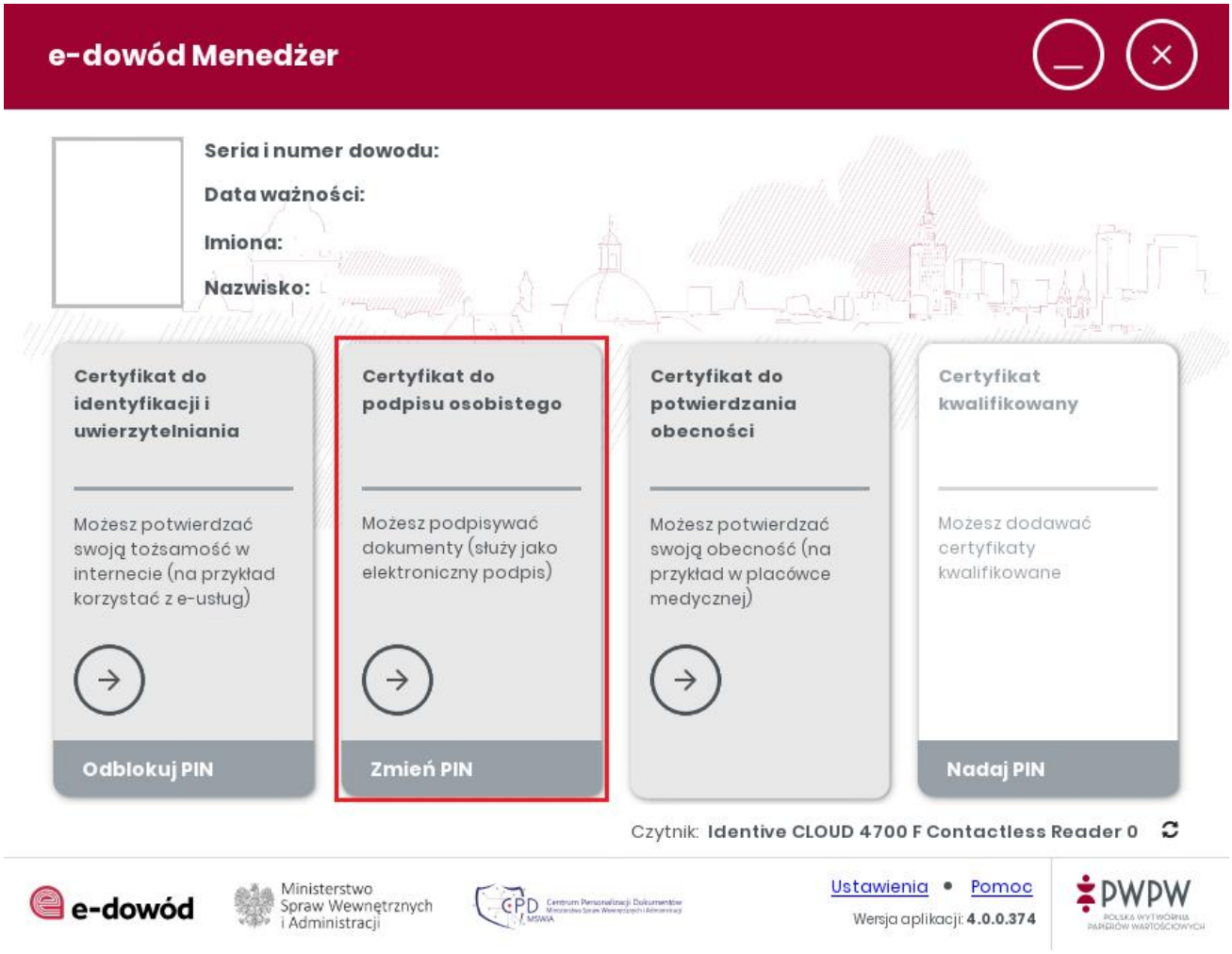
PUESC udostępnia również dedykowaną usługę ***Zweryfikuj podpis elektroniczny*** w sekcji ***Elektroniczne podpisywanie dokumentów***, dostępną też poprzez kafelek na stronie głównej.

Dodatek B

B.1 Podpisanie danymi z warstwy elektronicznej dowodu osobistego

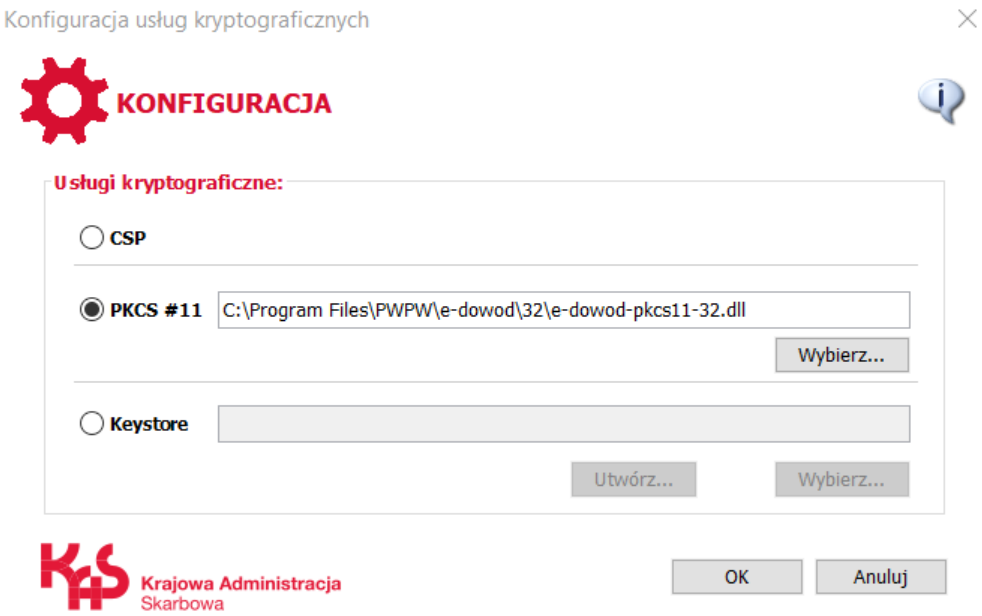
Aplikacja od wersji 1.3.60 obsługuje wykonywanie podpisów z wykorzystaniem danych warstwy elektronicznej dowodu osobistego. Aby wykonać podpis osobisty należy uprzednio zainstalować oprogramowanie ***E-dowód menedżer*** oraz ***E-dowód podpis elektroniczny***.
Więcej informacji o e-dowodzie na stronie https://www.gov.pl/web/e-dowod

Przed wykonaniem podpisu, w aplikacji *E-dowód Menedżer* powinien być odblokowany PIN certyfikatu do podpisu osobistego:

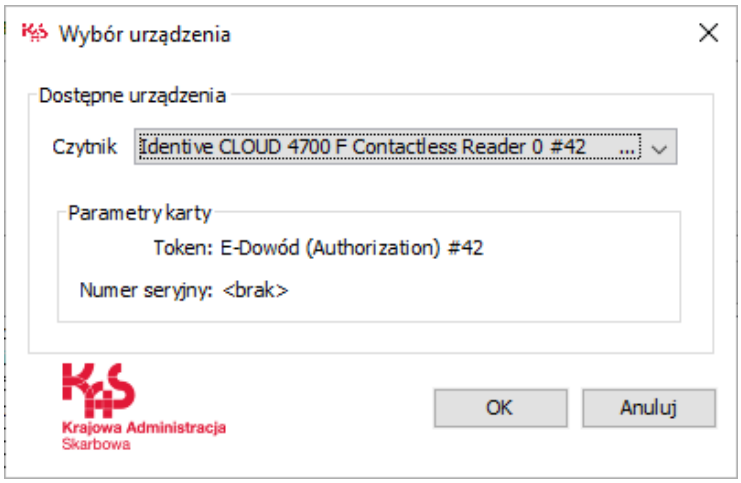


Jeśli PIN tego certyfikatu jest odblokowany, można dokonywać podpisów cyfrowych.

Sposób wykonania podpisu z użyciem CertSign jest taki jak dla innych nośników PKCS#11. Należy w konfiguracji usług kryptograficznych wskazać odpowiednią bibliotekę i token do podpisu, analogicznie jak opisano w rozdziale 5.3. Biblioteki PKCS#11 znajdują się w folderze instalacyjnym aplikacji *E-dowód Menedżer*. Należy wybrać wersję dostosowaną do posiadanej platformy, tzn. w przypadku architektury 32-bitowej oraz 32-bitowej dystrybucji CertSign, należy wskazać 32-bitową bibliotekę *e-dowod-pkcs11-32.dll,* jak na poniższym widoku:



W kolejnym kroku należy wybrać token do podpisu. Domyślnie do podpisów stosuje się token **Authorization**, zawierający certyfikat do podpisu osobistego.



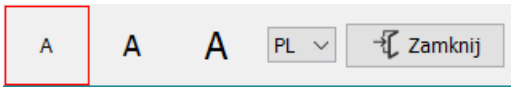
Kolejne operacje wykonuje się zgodnie z opisem w rozdziale 5.3.

B.2 Funkcje skalowania elementów interfejsu graficznego

Aplikacja od wersji 1.3.60 umożliwia skalowanie czcionek ekranowych do trzech rozmiarów:

- standardowy
- większy
- największy

Aby zmienić rozmiar czcionek należy wybrać jeden z przycisków skalowania, który nie jest aktualnie wybrany. Każdy kolejny rozmiar jest większy od poprzedniego półtorakrotnie. Oznacza to, że powiększenie rozmiaru *standardowego* do *większego* skutkuje wzrostem aktualnego rozmiaru czcionek o 150%, zaś do *największego* – o 225%. Tak samo, zmniejszenie z *największego* do *większego* zmniejszy poziom z 225% rozmiaru *standardowego* do 150%, a ponowny powrót do *standardowego* pomniejszy aktualny poziom półtorakrotnie, czyli powrót do 100%.
Kolejność skalowania nie ma znaczenia - można jej dokonywać w dowolnej kolejności.

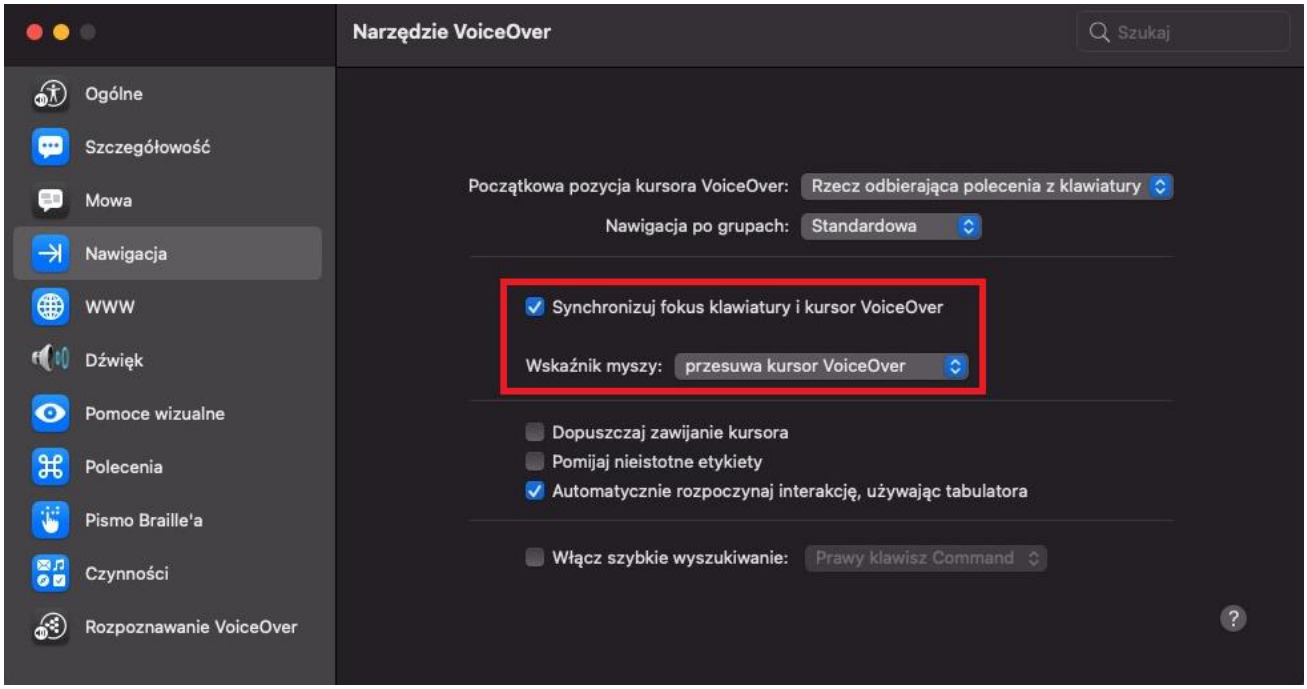


Przyciski powiększania czcionek są zaznaczone czerwoną ramką na powyższym widoku ekranu.

W przypadku wyświetlaczy o niższych rozdzielczościach aplikacja może blokować częściowo lub całkowicie możliwość skalowania, w celu uniknięcia błędów przeskalowania elementów interfejsu aplikacji.

B.3 Obsługa aplikacji przez czytnik ekranu

Aplikacja od wersji 1.3.60 jest przystosowana do obsługi przez czytnik NVDA dla Windows oraz VoiceOver dla macOS.
Domyślna konfiguracja aplikacji VoiceOver jest dostosowana do operowania klawiaturą. Wówczas, istnieje możliwość przechodzenia klawiszem *Tab* po kolejnych komponentach i ich odczytywanie bądź wybieranie. Jeśli jakiś komponent nie jest osiągalny klawiszem *Tab*, można wciąż przesuwać kursor programu VoiceOver za pomocą przycisków lewej oraz prawej strzałki na klawiaturze.
Jeśli jednak istnieje potrzeba, by każdy tekst był odczytywany przy najeżdżaniu na niego myszką, należy w ustawieniach programu VoiceOver wybrać opcję Synchronizuj fokus klawiatury i kursor VoiceOver.



Wówczas, kursor VoiceOver będzie ustawiany za pomocą najechania kursorem myszki na obiekt.

B.4 Nawigowanie i sterowanie klawiaturą

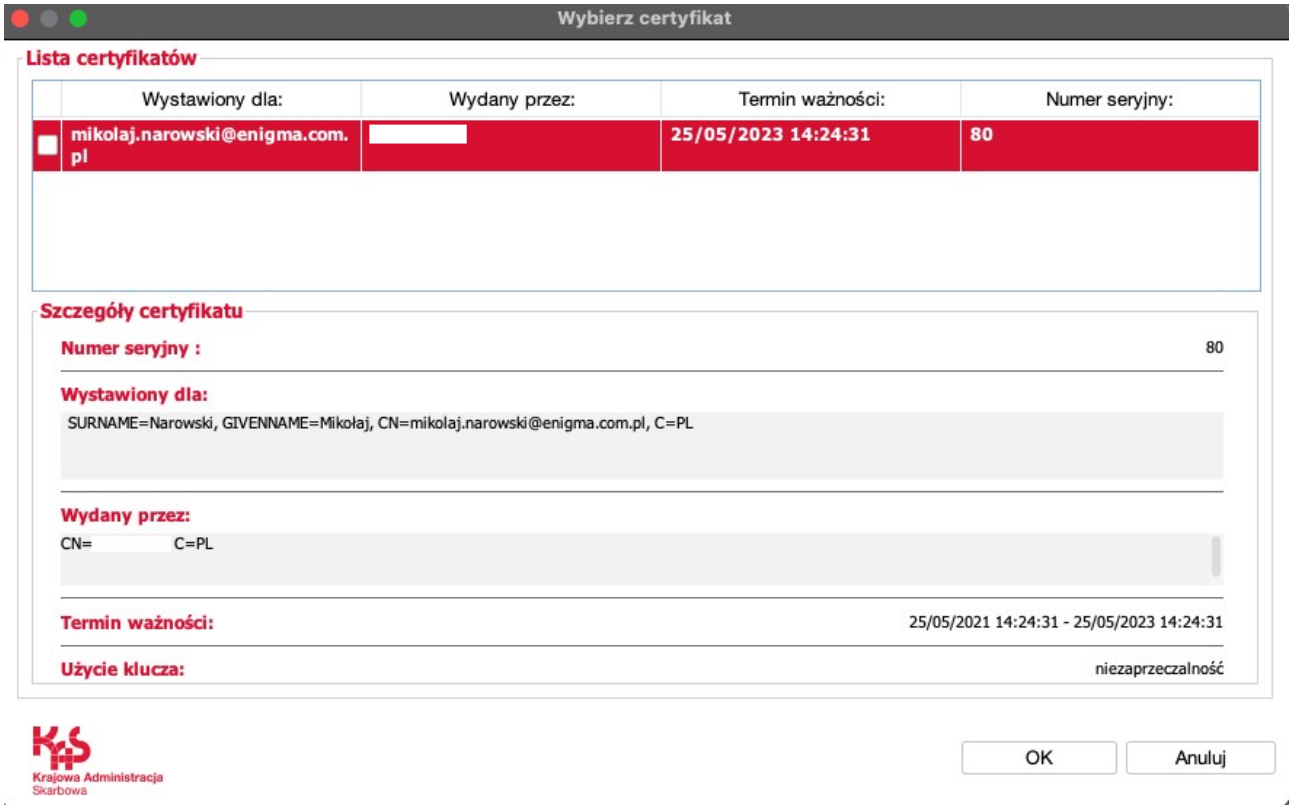
Aplikacja CertSign może być obsługiwana przy użyciu klawiatury. Przemieszczanie po kolejnych elementach realizowane jest klawiszem Tab. Cofanie można wykonać kombinacją Shift + Tab
W celu wybrania innej zakładki za pomocą klawiatury, mając wybrany pierwszy element można przechodzić w przód i w tył kombinacjami odpowiednio Ctrl + Tab oraz Shift + Ctrl + Tab.
Więcej wskazówek oraz domyślnych skrótów klawiszowych można znaleźć pod tym adresem https://www.ibm.com/docs/en/sdk-java-technology/8?topic=applications-default-swing-key-bindings

Obsługa obiektu typu ComboBox (lista rozwijana)
Aby wyświetlić listę elementów do wybrania, po najechaniu na obiekt typu ComboBox wcisnąć:

- Na Windows: *Alt* + strzałka w dół
- Na Linux oraz MacOS: *Spację*

Aby wybrać inny element, należy zjechać w odpowiednią stronę strzałką w górę lub w dół. Aby natychmiastowo wybrać dany element, należy przy rozwiniętej liście wybrać klawisz litery która zaczyna nazwę danego elementu.

Sterowanie w oknie wyboru certyfikatów



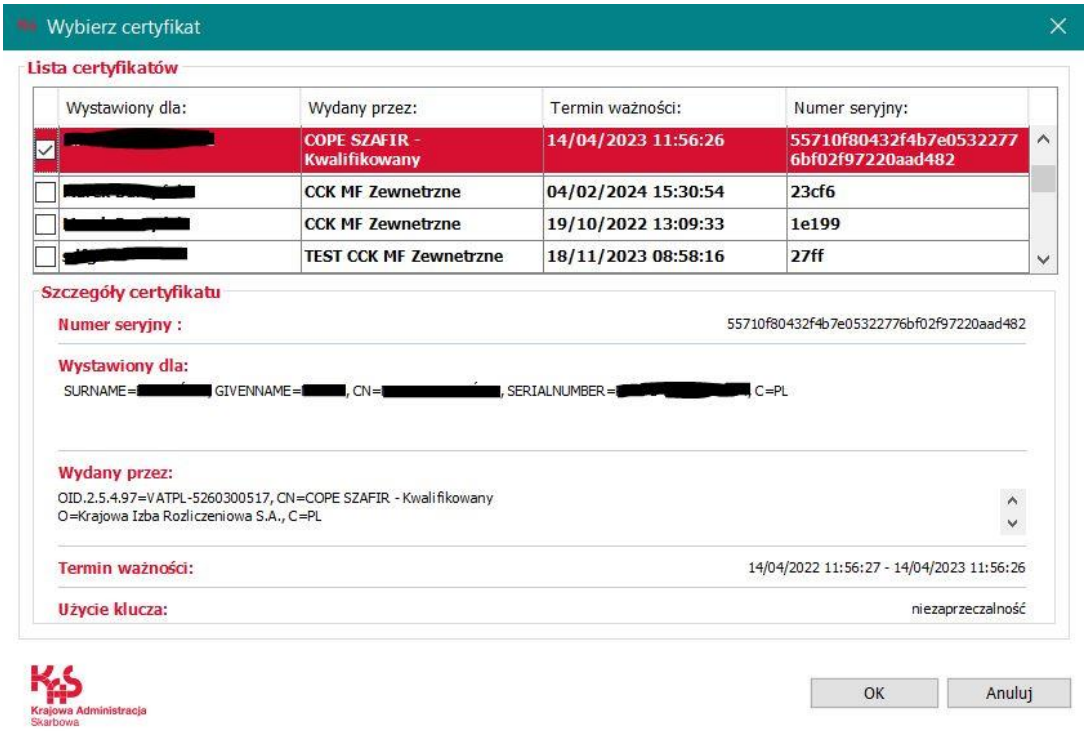
Poruszanie się klawiaturą w tym oknie ma dwojaki charakter, w zależności od aktualnie wybranego komponentu:
- Po każdym głównym elemencie (komponent tabeli, pola tekstowe oraz jego suwaki, przyciski) można przechodzić klawiszem Tab.
- Po wylistowanych certyfikatach w komponencie tabeli można przechodzić strzałkami w górę oraz w dół.

Aby wybrać certyfikat, oznaczony kolorem czerwonym, należy nacisnąć Enter lub Spację. Wybór certyfikatu jest sygnalizowany oznaczeniem check-box'a po lewej stronie wiersza tabeli.

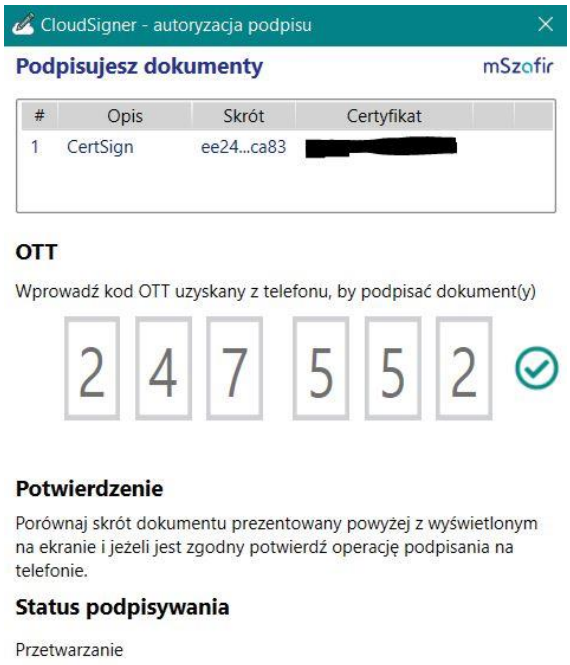
B.5 Współpraca z usługą mobilnego podpisu elektronicznego

Aplikacja CertSign może współpracować z mobilną usługą podpisu elektronicznego, o ile dostawca zapewnia oprogramowanie do emulacji obsługi karty kryptograficznej, umożliwiające rejestrację certyfikatów w magazynie certyfikatów Windows (CSP) lub dostęp przez sterownik PKCS#11. Przygotowanie CertSign do współpracy polega na wyborze certyfikatu dostarczonego w ramach usługi mobilnej w konfiguracji CSP (magazyn Windows) lub PKCS#11. Pozostałe kroki przebiegają jak dla zwykłego podpisu, z uwzględnieniem autoryzacji w aplikacji mobilnej. Poniżej opisano przykładowo współpracę z usługą mSzafir. W podobny sposób można uzyskać współpracę z inną usługą, np. SimplySign https://pomoc.certum.pl/pl/simplysign-faq/

W celu przygotowania mSzafir należy postępować zgodnie z instrukcją:
https://www.mszafir.pl/gfx/mszafir/userfiles/_public/tutoriale/jak_wykorzystac_certyfikat_mszafir_w_dowolnej_aplikacji_podpisujacej.pdf
Po aktywowaniu karty wirtualnej należy w CertSign wybrać opcję „Zmień certyfikat" i wskazać certyfikat usługi mobilnej, analogicznie jak w przypadku zwykłego certyfikatu (w konfiguracji CSP lub PKCS#11).



Po wybraniu certyfikatu można przejść do podpisania dokumentu, przy czym autoryzacji podpisu dokonuje się podając kod wygenerowany w aplikacji mobilnej.

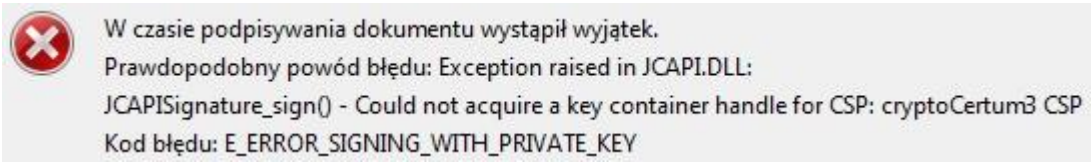


B.6 Szczególne przypadki dotyczące kart z certyfikatami kwalifikowanymi

W przypadku podpisu kwalifikowanego CertSign do komunikacji z kartą kryptograficzną wykorzystuje usługi CSP lub PKCS#11. W niektórych przypadkach może się jednak okazać, że specyfika interfejsów karty kryptograficznej i CertSign wymusza użycie tylko jednej z w/w usług.

UWAGA! Należy zainstalować również oprogramowanie dostawcy certyfikatu kwalifikowanego, gdyż zawiera ono sterowniki do kart kryptograficznych.

Jeśli podczas podpisywania z wybraną opcją CSP wystąpi błąd, np.:

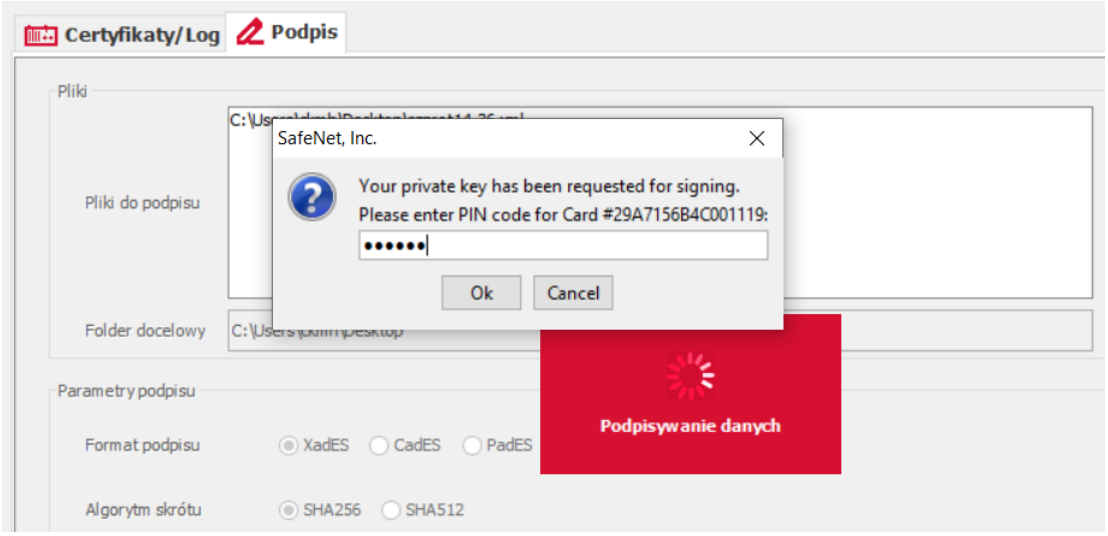


należy w CertSign wybrać opcję *Zmień certyfikat*, wskazać *PKCS#11* oraz ścieżkę do pliku .dll sterownika karty, dostarczonego z oprogramowaniem dostawcy certyfikatu. Należy przy tym zwrócić uwagę na wybór pliku odpowiedniego dla architektury systemu operacyjnego (32 lub 64 bitowej).
Informacji o lokalizacji tych plików należy poszukiwać na stronach lub w dokumentacji dostawcy certyfikatu.
W przypadku polskich dostawców **mogą** to być:
CERTUM:
C:\Windows\System32\cryptoCertum3PKCS64.dll
C:\Windows\System32\cryptoCertum3PKCS.dll
https://pomoc.certum.pl/pl/ekw-reczne-wskazanie-sterownika-karty-kryptograficznej/
SIGILLUM:
C:\Windows\System32\asepkcs.dll
EUROCERT:
C:\Windows\System32\cmP11.dll
C:\Windows\System32\cmP1164.dll
C:\Windows\SysWOW64\cmP11.dll
https://eurocert.freshdesk.com/support/solutions/articles/48001213718-niezb%C4%99dna-biblioteka-localizacja-
KIR (Szafir):
C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x64.dll
C:\Program Files\Krajowa Izba Rozliczeniowa S.A.\Szafir 2.0\bin\CCGraphiteP11p.x86.dll
https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/_public/informacje/instrukcje/instrukcja_konfiguracji_kart_cryptocard_graphite_w_jpk.pdf
C:\Program Files\CryptoTech\CCP1164.dll
C:\Program Files\CryptoTech\CCPkiP11.dll
https://www.elektronicznypodpis.pl/gfx/elektronicznypodpis/userfiles/_public/informacje/instrukcje/jpk_2.pdf
CENCERT:
C:\Program Files\ENCARD\enigmap11-x64.dll
C:\Program Files (x86)\ENCARD\enigmap11.dll

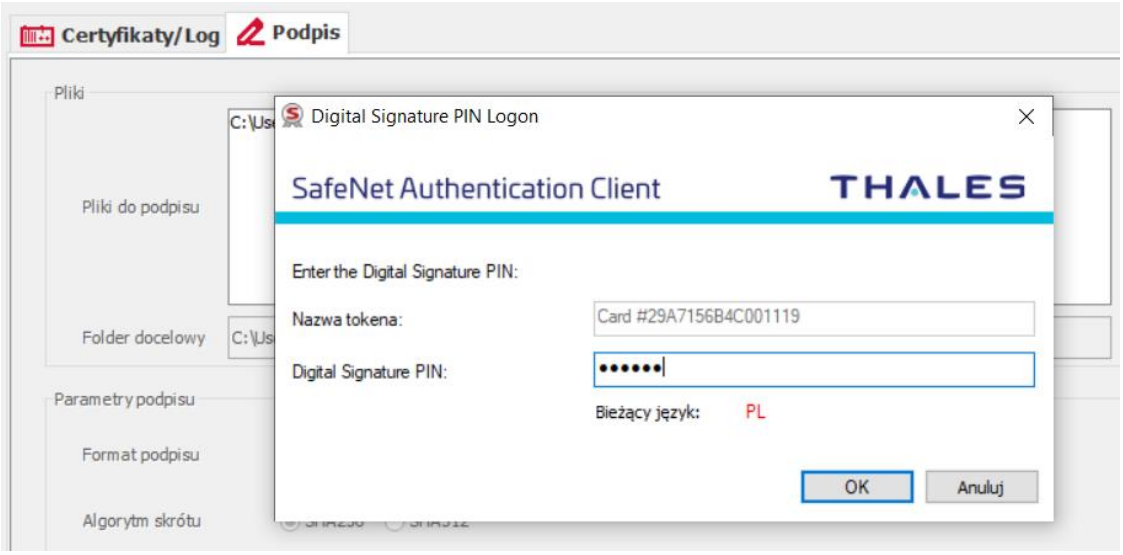
Szczególnym przypadkiem są karty kryptograficzne zabezpieczane na 2 poziomach: kodem PIN do karty oraz odrębnym PIN-em do wykonania podpisu. Przykładem może być karta IDPrime dostarczana przez CenCert (biała z niebieskim logo), która posiada PIN do karty oraz *Digital Signature PIN* do wykonania podpisu. Proces podpisania w CertSign wymaga wówczas podania kolejno obu PIN-ów i jest to dostępne **jedynie w konfiguracji CSP**. Użycie PKCS#11 spowoduje, że przekazywany będzie tylko PIN karty i podpis nie zostanie wykonany.

Poniżej pokazano dla przykładu, jak wykonać podpis z użyciem karty IDPrime od CenCert (wymaga ona zainstalowanego oprogramowania *SafeNet Authentication Client*).

Przy wybranej konfiguracji CSP i certyfikacie kwalifikowanym (zakładka *Certyfikaty/Log*) należy wskazać plik do podpisania i zatwierdzić podpisanie. W pierwszym kroku pojawi się pytanie o PIN do karty kryptograficznej.



Po podaniu prawidłowego PIN-u karty wyświetlone zostanie żądanie *Digital Signature PIN*.



Wykonanie podpisu zostanie potwierdzone komunikatem.