Krajowy Depozyt Papierów Wartościowych

Zdalne odnawianie certyfikatów do SWI

Instrukcja użytkownika

Wersja 1.1

Spis treści

Wstęp

Instrukcja użytkownika ma za zadanie pomóc użytkownikom w zdalnym odnawianiu certyfikatów wykorzystywanych w Systemie Wymiany Informacji (SWI).

System zdalnego odnawiania certyfikatów, dostępny na stronie https://cert.kdpw.pl, pozwala użytkownikom na odnawianie certyfikatów na własnej stacji roboczej, bez konieczności składania wizyty w KDPW S.A. Certyfikat musi być w okresie ważności i nie może być unieważniony.

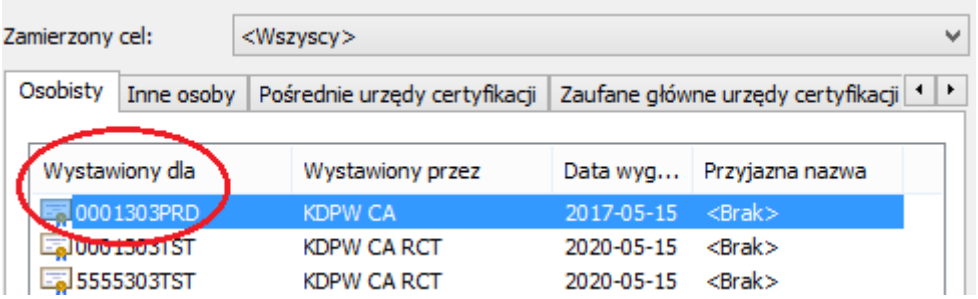
Zdalne odnawianie dotyczy certyfikatów umieszczonych na kartach kryptograficznych oraz w plikach PKCS#12.

Dostęp do systemu

Przed przystąpieniem do odnawiania certyfikatu do Systemu Wymiany Informacji należy wykonać następujące kroki:

1. Zweryfikować wymagania systemowe podane w punkcie „Wymagania systemowe”.

2. Przygotować certyfikat i PIN/hasło, jakim jest on zabezpieczony.
   Certyfikaty mogą się znajdować na karcie kryptograficznej lub w pliku PKCS#12.
   Przeznaczenie certyfikatu można rozpoznać po końcówce nazwy certyfikatu widocznej w polu „Wystawiony dla”. Certyfikaty wystawione przez KDPW, w polu „Wystawiony przez”, mają wpisane KDPW CA, KDPW CA RCT lub KDPW CA VPN.



   Końcówki oznaczają:

   PRD – certyfikat produkcyjnego systemu ESDI/WEB;

   TST – certyfikat testowego systemu ESDI/WEB;

   SDKP – certyfikat produkcyjnego systemu ESDK;

   SDKT – certyfikat testowego systemu ESDK;

   VPN – certyfikat do połączeń VPN.

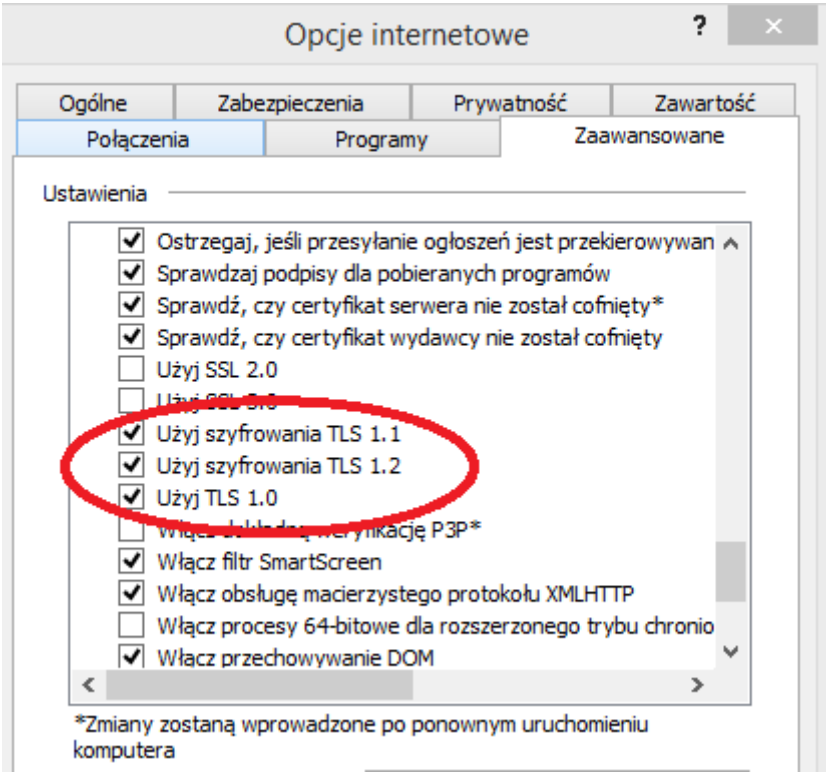
Wymagania systemowe

1. System operacyjny
   - Microsoft Windows 7, 8, 8.1, 10.
   - Oprogramowanie Java w wersji 8 (32-bit).
   - Oprogramowanie SafeSign w wersji 2.2 oraz czytnik kart kryptograficznych (jedynie w przypadku odnawiania certyfikatów umieszczonych na karcie).

2. Przeglądarka internetowa
   - Microsoft Internet Explorer w wersji 11.
   - Włączona obsługa protokołu TLS.
   - Witryna https://cert.kdpw.pl dodana do listy *Zaufane witryny.*

Obsługę protokołu TLS przez przeglądarkę internetową ustawiamy zgodnie z poniższą instrukcją:

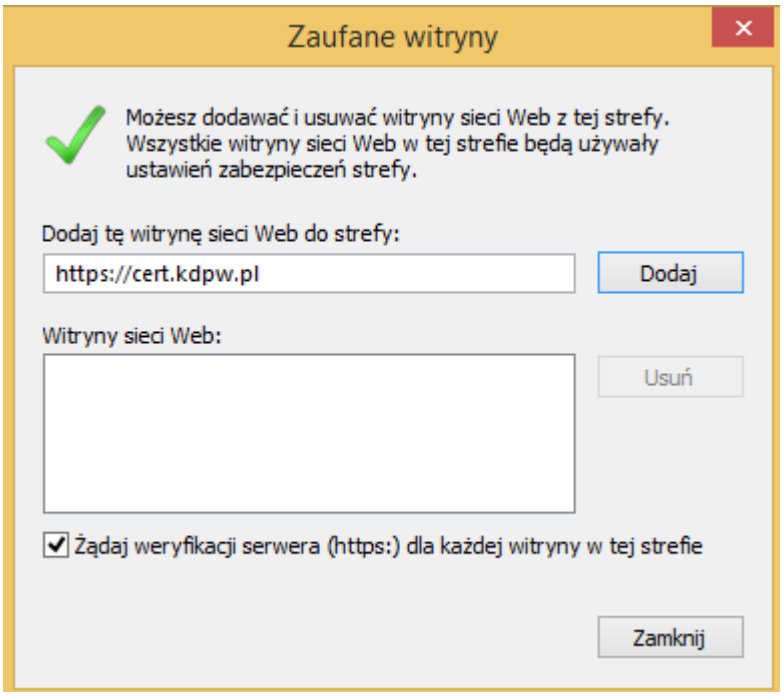
1. Zalogować się na konto użytkownika, który będzie odnawiał certyfikat.
2. Uruchomić przeglądarkę Internet Explorer.
3. Z menu wybrać „Narzędzia” → „Opcje internetowe”.
4. Przejść do zakładki „Zaawansowane”.
   Zakładka „Zaawansowane” może być niewidoczna w przypadku systemowego ograniczenia uprawnień użytkownika. W celu uzyskania dostępu należy skontaktować się z lokalnym administratorem komputera.
5. W oknie „Zaawansowane” sprawdzamy, czy jest zaznaczone użycie przynajmniej jednej z wersji protokołu TLS. Obsługiwane są protokoły: TLS 1.0, TLS 1.1 i TLS 1.2.



6. W celu zatwierdzenia zmian, należy nacisnąć „OK”.

Dodanie witryny https://cert.kdpw.pl do zaufanych należy przeprowadzić zgodnie z poniższą instrukcją:

1. Uruchomić przeglądarkę Internet Explorer.
2. Z menu wybrać opcję „Narzędzia” → „Opcje internetowe”.
3. Przejść do zakładki „Zabezpieczenia”.
   Zakładka „Zabezpieczenia” może być niewidoczna w przypadku systemowego ograniczenia uprawnień użytkownika. W celu uzyskania dostępu należy skontaktować się z lokalnym administratorem komputera.
4. Nacisnąć ikonę z napisem „Zaufane witryny” i nacisnąć przycisk „Witryny”.
5. W otwartym oknie wpisać adres: https://cert.kdpw.pl, a następnie zaznaczyć opcję „Żądaj weryfikacji serwera (https:) dla każdej witryny w tej strefie”.

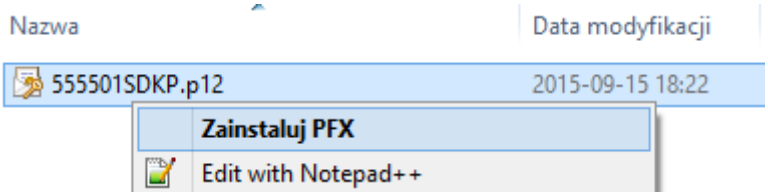


6. Następnie wybrać przycisk „Dodaj” i witryna powinna pojawić się na liście.
7. Po upewnieniu się, że dodana witryna pojawiła się na liście należy nacisnąć przycisk „Zamknij”.

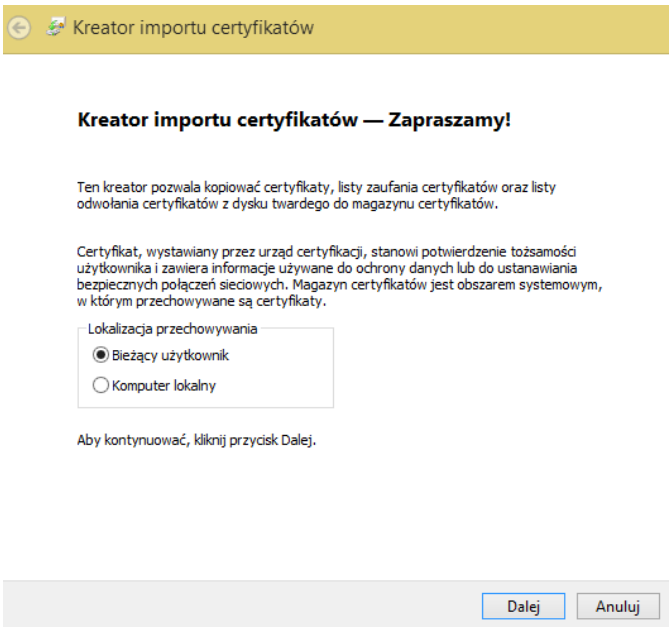
Instalacja certyfikatu użytkownika

W celu instalacji certyfikatu z pliku *.p12 lub *.pfx należy:

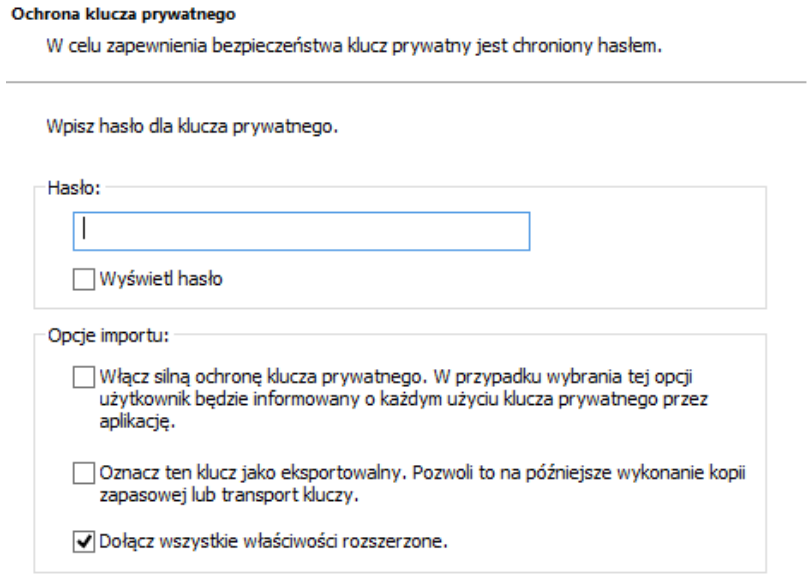
1. Zalogować się na konto użytkownika, który będzie korzystał z tego certyfikatu.
2. Kliknąć prawym przyciskiem myszy na pliku, zawierającym certyfikat, i wybrać z menu kontekstowego opcję „Zainstaluj PFX”.



3. Uruchomiony zostanie *Kreator importu certyfikatów*. Należy nacisnąć przycisk *Dalej.*

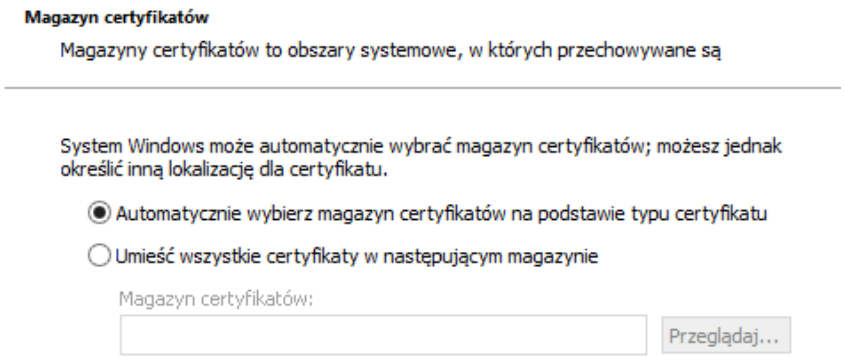


4. W następnym oknie należy podać hasło zabezpieczające plik z certyfikatem i potwierdzić je przyciskiem *Dalej*.



Zalecamy zaznaczenie opcji „Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikację.” Zaznaczenie tej opcji powoduje, że każde użycie certyfikatu będzie wymagało podania hasła chroniącego certyfikat.

5. W następnym oknie należy pozostawiać zaznaczoną opcję „Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu”.

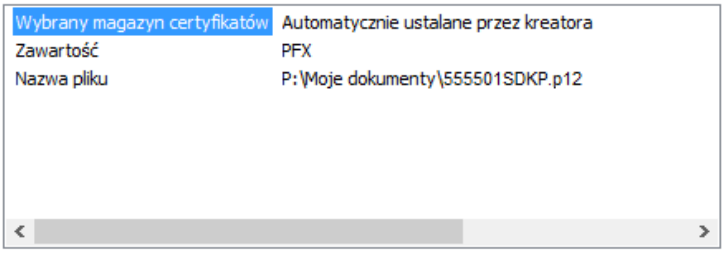


6. W następnym oknie należy nacisnąć przycisk „Zakończ”.

Kończenie pracy Kreatora importu certyfikatów

Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ.

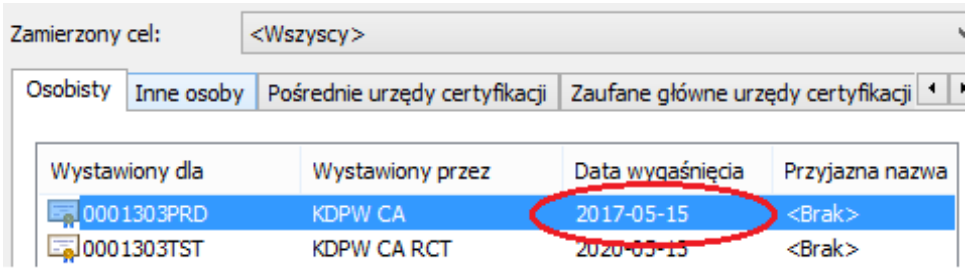
Wybrane zostały następujące ustawienia:



Sprawdzenie okresu ważności certyfikatu

W celu sprawdzenia okresu ważności certyfikatu należy:

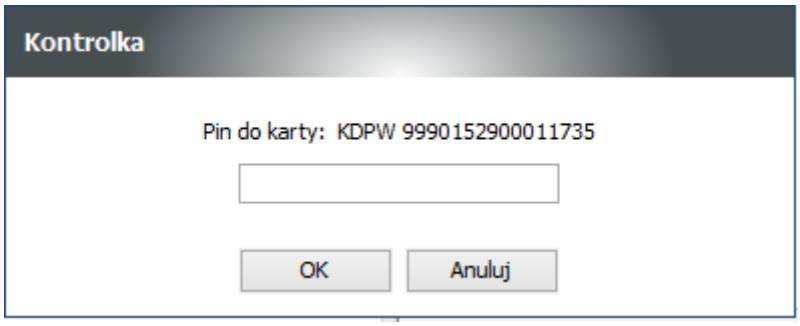
1. Posiadać zainstalowany certyfikat lub zainstalować go zgodnie z punktem „Instalacja certyfikatu użytkownika”.
2. Uruchomić przeglądarkę Internet Explorer.
3. W menu wybrać opcję „Narzędzia” → „Opcje internetowe” → „Zawartość” → „Certyfikaty”.
4. Przejść do zakładki „Osobisty”.
5. W oknie z listą certyfikatów w kolumnie „Data wygaśnięcia” można sprawdzić, do kiedy jest ważny dany certyfikat.



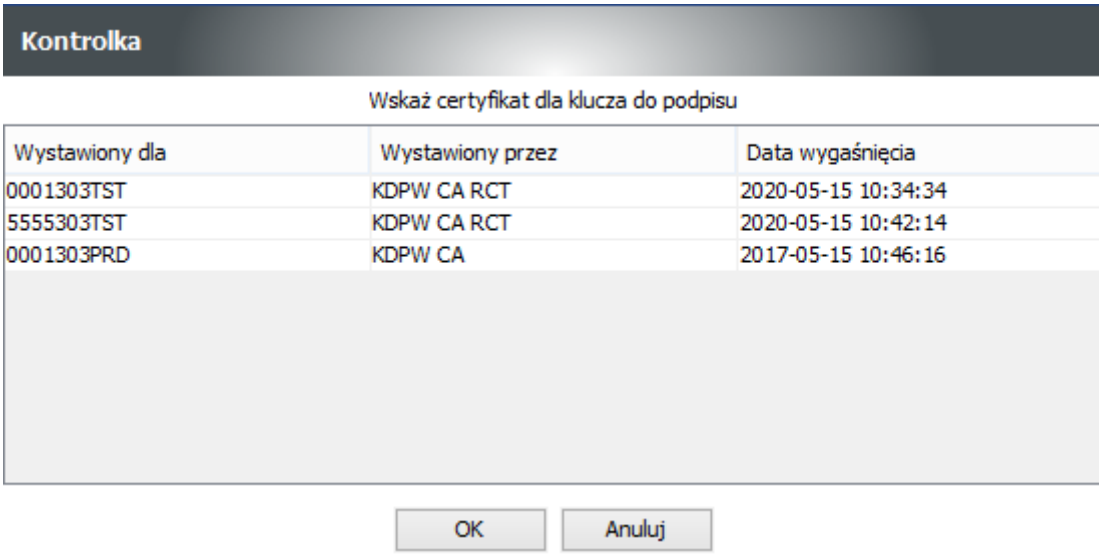
Zdalne odnawianie certyfikatu użytkownika systemu ESDI/WEB umieszczonego na karcie

W celu odnowienia certyfikatu użytkownika, należy:

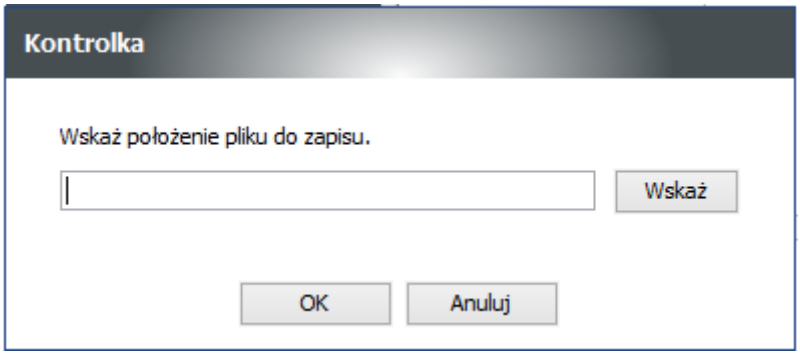
1. Włożyć kartę do czytnika kart kryptograficznych.
2. Uruchomić Internet Explorer i wejść na stronę https://cert.kdpw.pl.
3. Z menu wybrać opcję „SWI – Certyfikaty produkcyjne” lub „SWI – Certyfikaty testowe”.
4. Zaczekać około 15 sekund, aż załaduję się aplet Java i opcja „Certyfikat ESDI/WEB (karta)” stanie się aktywna.
5. Wybrać opcję „Certyfikat ESDI/WEB (karta)”.
6. W oknie „Kontrolka” należy wpisać PIN do karty i nacisnąć przycisk „OK”.



7. W następnym oknie należy wskazać certyfikat, który ma zostać odnowiony. Certyfikaty z końcówką PRD dotyczą środowiska produkcyjnego, a z końcówką TST dotyczą środowiska testowego.

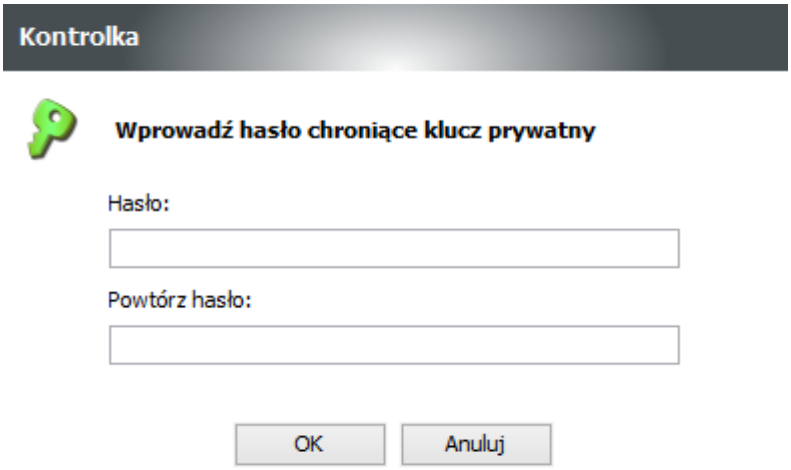


8. W kolejnym oknie należy wskazać położenie, gdzie zostanie zapisany certyfikat i nacisnąć przycisk *OK*.

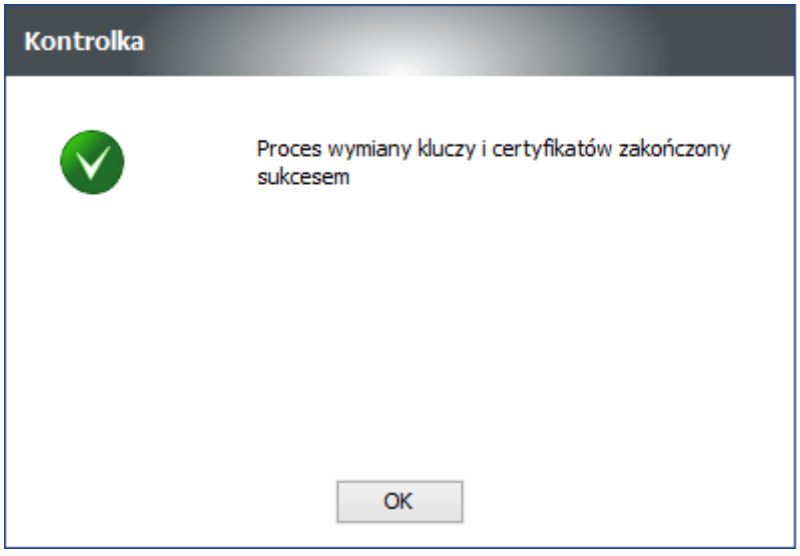


9. W kolejnym oknie należy wskazać nowe hasło do pliku z certyfikatem i nacisnąć przycisk *OK*.

   Uwaga! Proces zdalnego odnawiania zapisuje certyfikat jedynie do pliku – nie zapisuje na kartę.



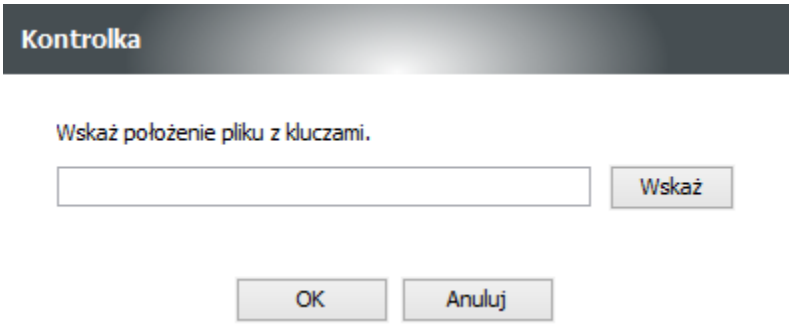
10. Po pomyślnym zakończeniu procesu odnawiania pojawi się komunikat.



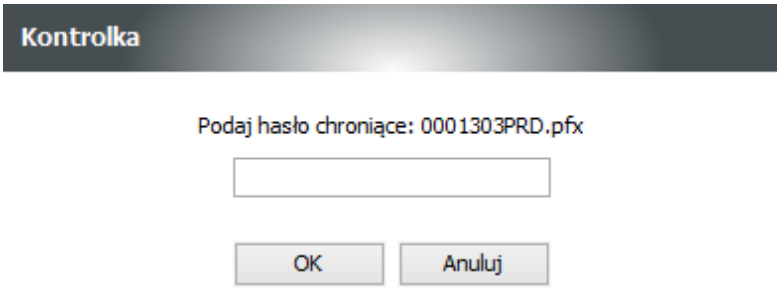
Zdalne odnawianie certyfikatu użytkownika systemu ESDI/WEB umieszczonego w pliku

W celu odnowienia certyfikatu użytkownika, należy:

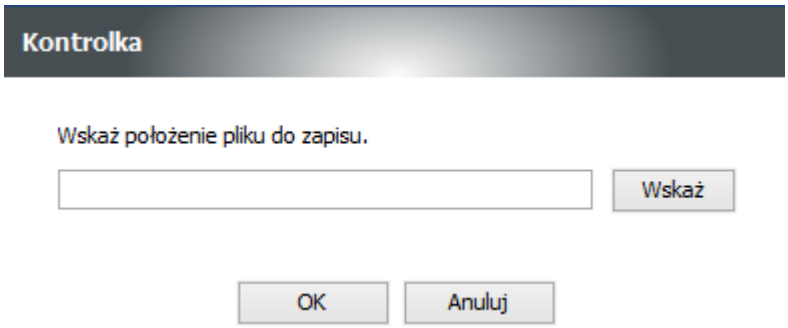
1. Uruchomić Internet Explorer i wejść na stronę https://cert.kdpw.pl.
2. Z menu wybrać opcję „SWI – Certyfikaty produkcyjne” lub „SWI – Certyfikaty testowe”.
3. Zaczekać około 15 sekund, aż załaduję się aplet Java i opcja „Certyfikat ESDI/WEB (plik PKCS#12)” stanie się aktywna.
4. Wybrać opcję „Certyfikat ESDI/WEB (plik PKCS#12)”.
5. W kolejnym oknie należy wskazać położenie pliku z certyfikatem.



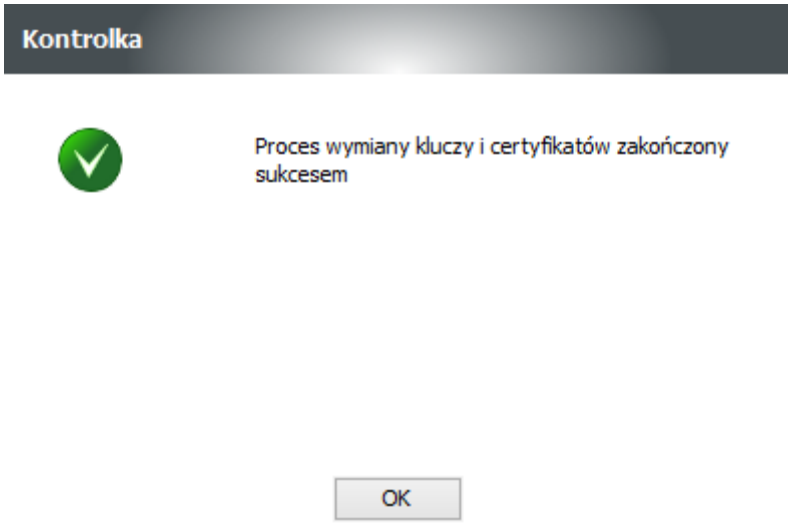
6. W kolejnym oknie należy wpisać hasło chroniące plik. Hasło zostało przekazane przez Głównego Poręczyciela na płycie CD. Nowy plik będzie miał takie samo hasło jak stary plik.



7. W kolejnym oknie należy wskazać położenie, gdzie zostanie zapisany certyfikat i nacisnąć przycisk „OK”.



8. Po pomyślnym zakończeniu procesu odnawiania pojawi się komunikat.

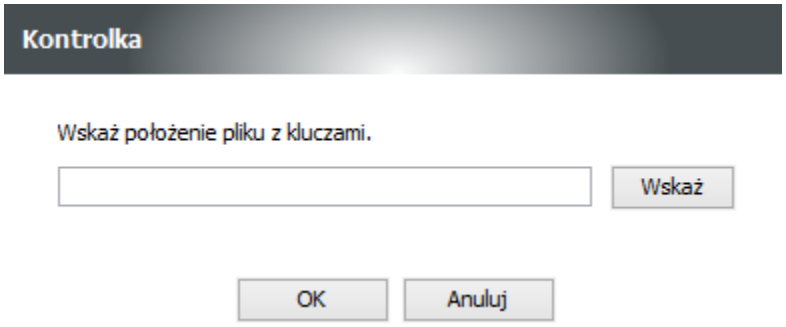


9. Po odnowieniu certyfikatu, użytkownik musi skontaktować się ze swoim Zespołem IT w celu podłączenia certyfikatu do swojej aplikacji wymieniającej komunikaty w trybie A2A z wykorzystaniem ESDI/WEB.

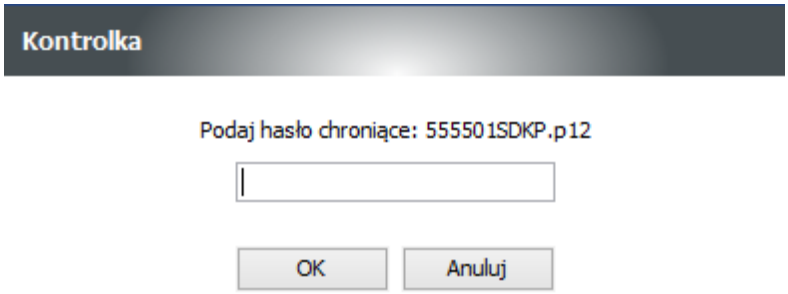
Zdalne odnawianie certyfikatu użytkownika systemu ESDK

W celu odnowienia certyfikatu użytkownika, należy:

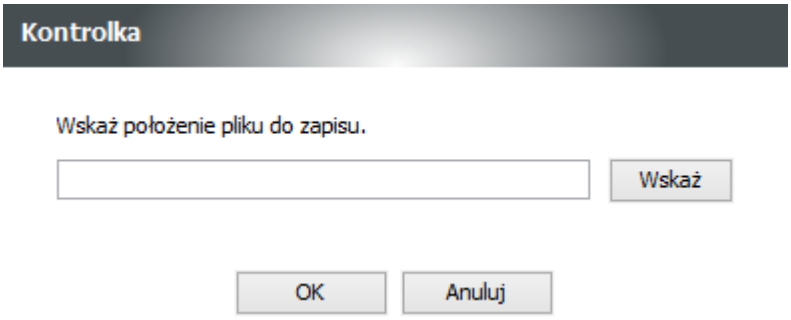
1. Uruchomić Internet Explorer i wejść na stronę https://cert.kdpw.pl.
2. Z menu wybrać opcję „SWI – Certyfikaty produkcyjne” lub „SWI – Certyfikaty testowe”.
3. Zaczekać około 15 sekund, aż załaduję się aplet Java i opcja „Certyfikat ESDK (plik PKCS#12)” stanie się aktywna.
4. Wybrać opcję „Certyfikat ESDK (plik PKCS#12)”.
5. W kolejnym oknie należy wskazać położenie pliku z certyfikatem.



6. W kolejnym oknie należy wpisać hasło chroniące plik. Hasło zostało przekazane przez Głównego Poręczyciela na płycie CD. Nowy plik będzie miał takie samo hasło jak stary plik.



7. W kolejnym oknie należy wskazać położenie, gdzie zostanie zapisany plik z certyfikatem i nacisnąć przycisk „OK”.

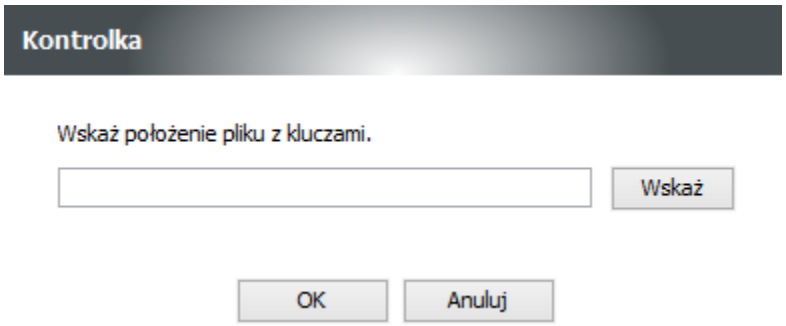


8. Po odnowieniu certyfikatu, użytkownik musi skontaktować się ze swoim Zespołem IT w celu podłączenia certyfikatu do swojej aplikacji wymieniającej komunikaty z wykorzystaniem ESDK.

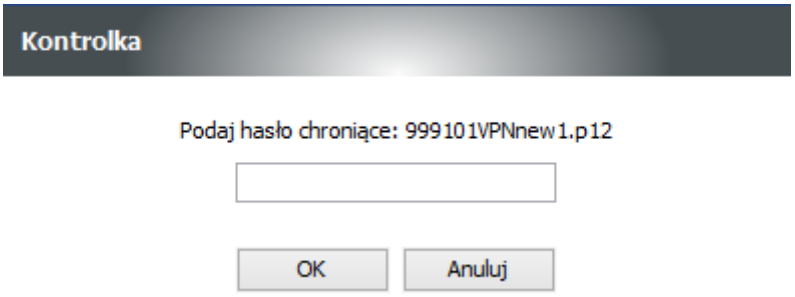
Zdalne odnawianie certyfikatu do połączeń VPN

W celu odnowienia certyfikatu do połączeń VPN, należy:

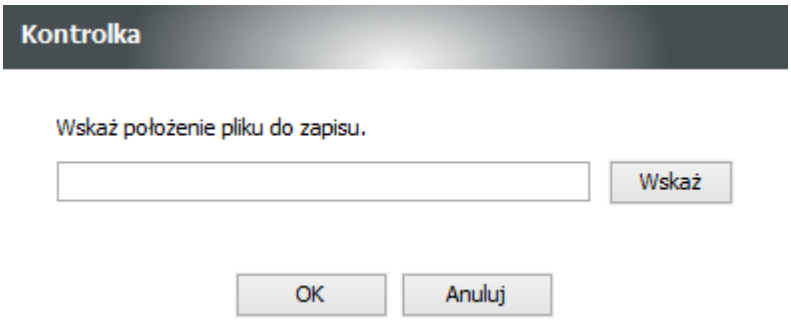
1. Uruchomić Internet Explorer i wejść na stronę https://cert.kdpw.pl
2. Z menu wybrać opcję „SWI – Certyfikaty VPN”.
3. Zaczekać około 15 sekund, aż załaduję się aplet Java i opcja „Certyfikat dla VPN (plik PKCS#12)” stanie się aktywna.
4. Wybrać opcję „Certyfikat dla VPN (plik PKCS#12)”.
5. W kolejnym oknie należy wskazać położenie pliku z certyfikatem.



6. W kolejnym oknie należy wpisać hasło chroniące plik. Hasło zostało przekazane przez Głównego Poręczyciela na płycie CD. Nowy plik będzie miał takie samo hasło jak stary plik.



7. W kolejnym oknie należy wskazać położenie, gdzie zostanie zapisany nowy certyfikat i nacisnąć przycisk „OK”.



8. Po odnowieniu certyfikatu, użytkownik musi skontaktować się ze swoim Zespołem IT w celu podłączenia certyfikatu do swojej aplikacji/rutera nawiązującego połączenie z KDPW.

Jak zdiagnozować problemy z uruchomieniem apletu Java?

W celu diagnozy problemów z uruchamianiem apletu Java, należy włączyć konsolę Java. W tym celu należy:

1. Z menu Windows uruchomić „Panel sterowania” → „Programy” → „Java (32-bitowy)”.
2. W oknie „Java Control Panel” należy wejść do zakładki „Advanced” i zaznaczyć następujące opcje:
    a. Debugging
        i. Enable tracing
        ii. Enable logging
        iii. Show aplet lifecycle exceptions
    b. Java console
        i. Show console
3. W trakcie procesu odnawiania certyfikatu wyświetli się konsola Java, monitorująca o wszystkich operacjach wykonywanych przez kontrolkę Java. Z informacji zawartych w tej konsoli można uzyskać informację o potencjalnych problemach. Natomiast, jeśli w konsoli nie pojawiają się żadne komunikaty, to oznacza, że Java nie uruchamia się i należy skontaktować się z lokalnym administratorem, który nada odpowiednie uprawnienia.