

## **Zdalne odnawianie certyfikatów do SWI**

### **Instrukcja użytkownika**

## Spis treści

Wstęp .....	3
Dostęp do systemu .....	4
Wymagania systemowe .....	5
Instalacja certyfikatu użytkownika .....	6
Sprawdzenie okresu ważności certyfikatu .....	9
Zdalne odnawianie certyfikatu użytkownika systemu ESDI/WEB .....	10
Zdalne odnawianie certyfikatu użytkownika systemu ESDK .....	13

## **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.

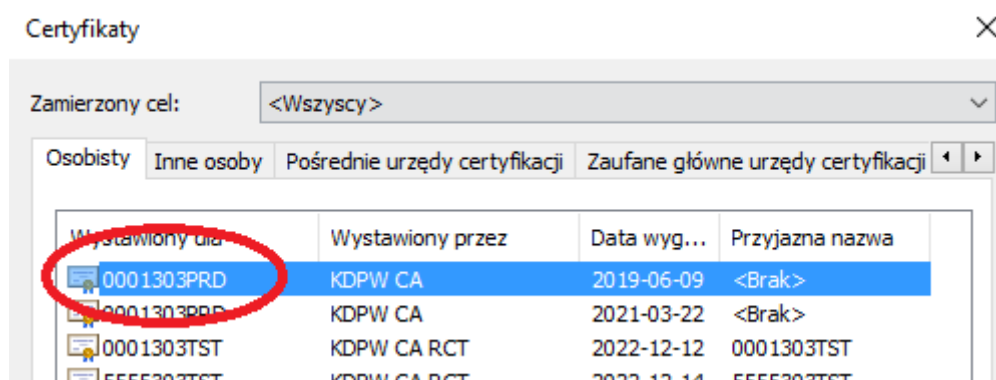
Zdalne odnawianie dotyczy certyfikatów umieszczonych w plikach PKCS#12.

## 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 hasło, jakim jest on zabezpieczony.

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 lub KDPW CA RCT.



Końcówki oznaczają:

PRD – certyfikat produkcyjnego systemu ESDI/WEB;

TST – certyfikat testowego systemu ESDI/WEB;

SDKP – certyfikat produkcyjnego systemu ESDK;

SDKT – certyfikat testowego systemu ESDK.

## **Wymagania systemowe**

### 1. System operacyjny

- Microsoft Windows 10
- oprogramowanie Java w wersji 8

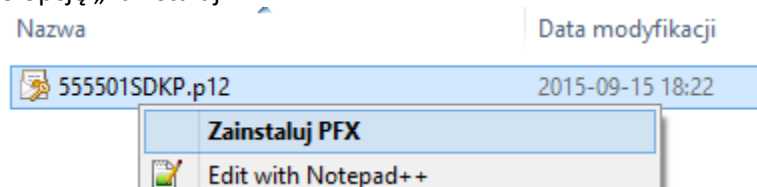
### 2. Przeglądarka internetowa

- Internet Explorer 11, Firefox, Chrome

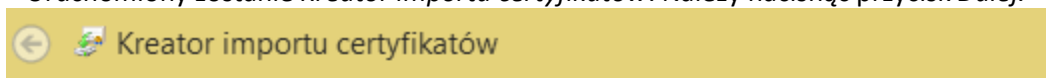
## Instalacja certyfikatu użytkownika

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*.



### Kreator importu certyfikatów — Zapraszamy!

Ten kreator pozwala kopiować certyfikaty, listy zaufania certyfikatów oraz listy odwołania certyfikatów z dysku twardego do magazynu certyfikatów.

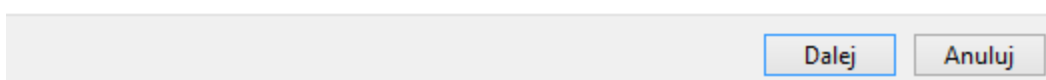
Certyfikat, wystawiany przez urząd certyfikacji, stanowi potwierdzenie tożsamości użytkownika i zawiera informacje używane do ochrony danych lub do ustanawiania bezpiecznych połączeń sieciowych. Magazyn certyfikatów jest obszarem systemowym, w którym przechowywane są certyfikaty.

Lokalizacja przechowywania

Bieżący użytkownik

Komputer lokalny

Aby kontynuować, kliknij przycisk *Dalej*.



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

### Ochrona klucza prywatnego

W celu zapewnienia bezpieczeństwa klucz prywatny jest chroniony hasłem.

---

Wpisz hasło dla klucza prywatnego.

Hasło:

Wyświetl hasło

Opcje importu:

Włącz silną ochronę klucza prywatnego. W przypadku wybrania tej opcji użytkownik będzie informowany o każdym użyciu klucza prywatnego przez aplikację.

Oznacz ten klucz jako eksportowalny. Pozwoli to na późniejsze wykonanie kopii zapasowej lub transport kluczy.

Dołącz wszystkie właściwości rozszerzone.

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

#### Magazyn certyfikatów

Magazyny certyfikatów to obszary systemowe, w których przechowywane są

---

System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizację dla certyfikatu.

Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu

Umieść wszystkie certyfikaty w następującym magazynie

Magazyn certyfikatów:

Przełóżaj...

6. W oknie

## Kończenie pracy Kreatora importu certyfikatów

Certyfikat zostanie zaimportowany po kliknięciu przycisku Zakończ.

Wybrane zostały następujące ustawienia:

Wybrany magazyn certyfikatów	Automatycznie ustalane przez kreatora
Zawartość	PFX
Nazwa pliku	P:\Moje dokumenty\555501SDKP.p12

Należy kliknąć Zakończ.



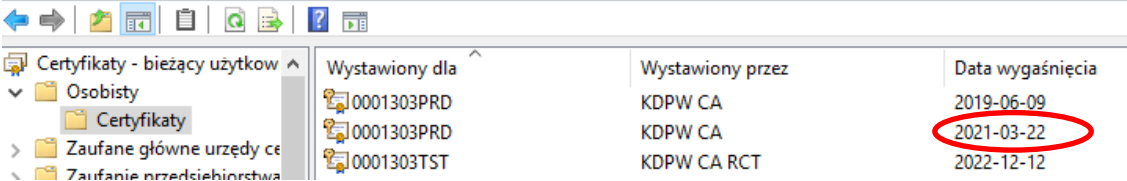
## Sprawdzenie okresu ważności certyfikatu

W celu sprawdzenia okresu ważności certyfikatu należy:

1. Posiadać zainstalowany certyfikat lub zainstalować go zgodnie z punktem „Instalacja certyfikatu użytkownika”.
2. Uruchomić przystawkę Certyfikaty (*Start* → *Uruchom* → *certmgr.msc*)
3. W menu wybrać opcję *Osobisty* → *Certyfikaty*
4. W oknie z listą certyfikatów w kolumnie „Data wygaśnięcia” można sprawdzić, do kiedy jest ważny dany certyfikat.

certmgr - [Certyfikaty - bieżący użytkownik\Osobisty\Certyfikaty]

Plik Akcja Widok Pomoc



Wystawiony dla	Wystawiony przez	Data wygaśnięcia
0001303PRD	KDPW CA	2019-06-09
0001303PRD	KDPW CA	2021-03-22
0001303TST	KDPW CA RCT	2022-12-12

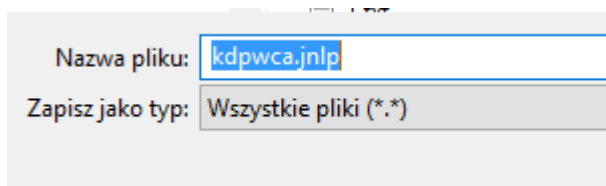
## Zdalne odnawianie certyfikatu użytkownika systemu ESDI/WEB

W celu odnowienia certyfikatu użytkownika, należy:

1. Uruchomić przeglądarkę internetową i wejść na stronę <https://cert.kdpw.pl>.
  2. Z menu wybrać opcję „SWI – Certyfikaty produkcyjne” lub „SWI – Certyfikaty testowe”.
  3. W zależności od używanej wersji przeglądarki są różne metody pobierania programu do zdalnej recertyfikacji
- 3.1 Jeżeli używasz Internet Explorera, należy kliknąć prawym przyciskiem myszy na obrazie



i wybrać opcję „Zapisz element docelowy jako”. W oknie „Zapisywanie jako” należy wybrać katalog w którym zapisany zostanie plik i zapisać go pod dowolną nazwą z rozszerzeniem „.jnlp”, np.:



Po zapisaniu pliku należy go otworzyć.

- 3.2 Jeżeli przeglądarką jest Firefox lub Chrome, należy kliknąć na obrazie



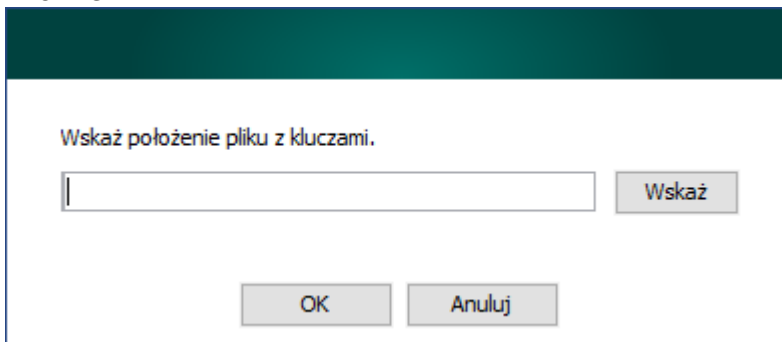
i uruchomić plik o rozszerzeniu .jnlp, który zostanie pobrany.

4. Uruchomi się program



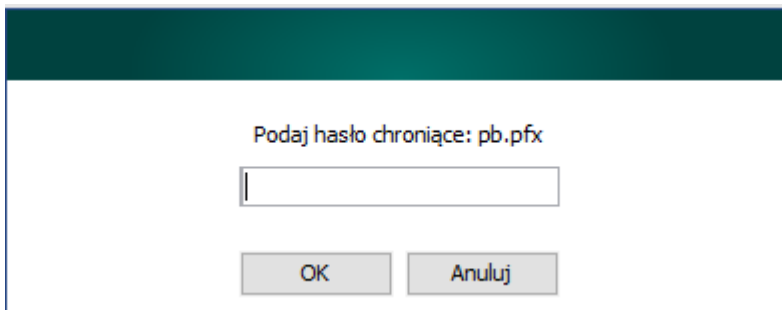
5. Wybrać opcję „Certyfikat ESDI/WEB”

6. W oknie



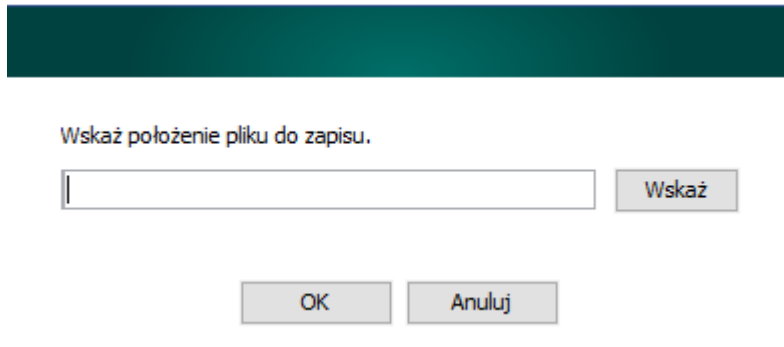
należy wskazać plik z kluczami, który będzie odnowiony.

7. W oknie



Należy podać hasło chroniące plik, a następnie nacisnąć OK.

8. W oknie



Wskaż położenie pliku do zapisu.

Wskaż

OK Anuluj

należy wskazać położenie zapisu nowego pliku. Hasło chroniące plik pozostaje takie samo jak starego pliku.

Uwaga! Wymagana jest instalacja nowego certyfikatu przez użytkownika.

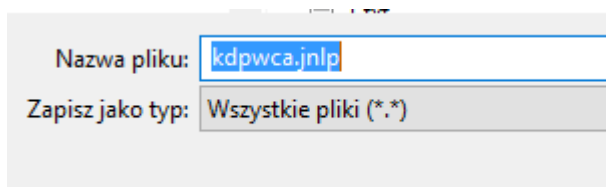
## Zdalne odnawianie certyfikatu użytkownika systemu ESDK

W celu odnowienia certyfikatu użytkownika, należy:

1. Uruchomić przeglądarkę internetową i wejść na stronę <https://cert.kdpw.pl>.
  2. Z menu wybrać opcję „SWI – Certyfikaty produkcyjne” lub „SWI – Certyfikaty testowe”.
  3. W zależności od używanej wersji przeglądarki są różne metody pobierania programu do zdalnej recertyfikacji.
- 3.1 Jeżeli przeglądarką jest Internet Explorer należy przycisnąć prawym przyciskiem myszy na obrazie



i wybrać opcję "Zapisz element docelowy jako" . W oknie „ Zapisywanie jako” należy wybrać katalogu w którym zapisany zostanie plik i zapisać go pod dowolną nazwą z rozszerzeniem „.jnlp”, np.:



Po zapisaniu pliku należy go otworzyć.

- 3.2 Jeżeli przeglądarką jest Firefox lub Chrome, należy kliknąć na obrazie



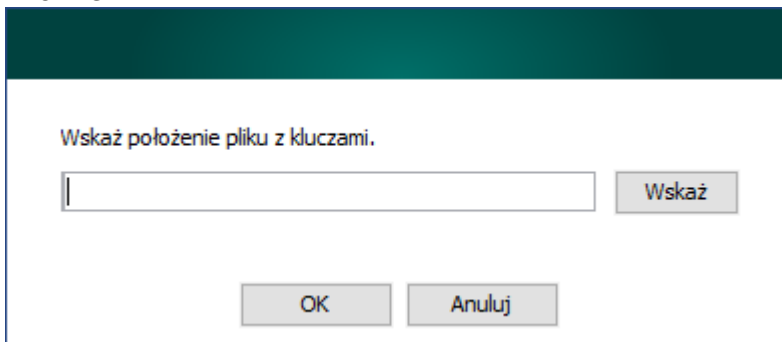
i uruchomić plik o rozszerzeniu .jnlp, który zostanie pobrany.

4. Uruchomi się program



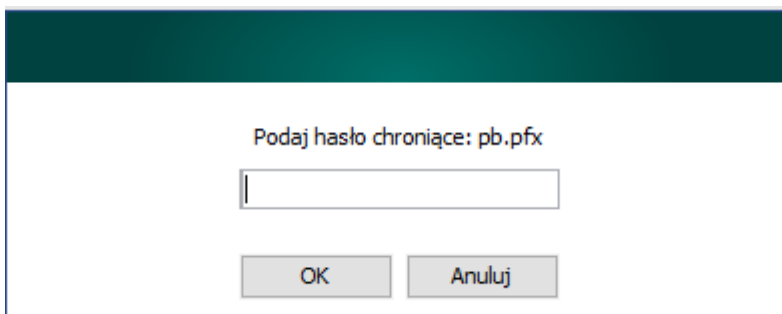
5. Wybrać opcję „Certyfikat ESDK”.

6. W oknie



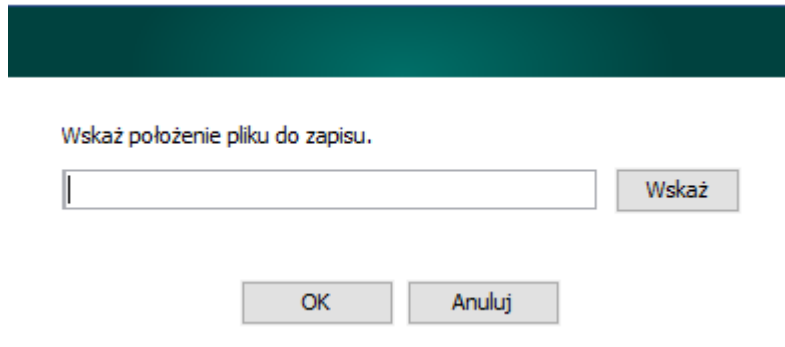
należy wskazać plik z kluczami, który będzie odnowiony.

7. W oknie



należy podać hasło chroniące plik a następnie nacisnąć OK.

8. W oknie



Wskaż położenie pliku do zapisu.

Wskaż

OK Anuluj

należy wskazać położenie zapisu nowego pliku. Hasło chroniące plik pozostaje takie samo jak starego pliku.

Uwaga! Wymagana jest instalacja nowego certyfikatu przez użytkownika.