

Instrukcja Generowania Certyfikatów CEPIK

SPIS TREŚCI

1.	Słownik pojęć	2
2.	Zanim przystąpisz do generowania certyfikatu	3
2.1.	Wymagane oprogramowanie.....	3
2.2.	Konfiguracja oprogramowania.....	3
3.	Proces Generowania Certyfikatów.....	6
3.1.	Certyfikat Operatora (SSL)	6
3.2.	Certyfikat Infrastruktury (VPN)	9
3.3.	Przykładowe komunikaty pojawiające się przy procesie generowania certyfikatów.....	14

1. Słownik pojęć

Nazwa / skrót	Opis
Certyfikat	Plik zawierający dane o użytkowniku. Służy jako poświadczenia do logowania do aplikacji.
Poświadczenia	Dane logowania do aplikacji
Recertyfikacja	Proces odnowienia ważności certyfikatu
Checkbox	Pole wyboru o kształcie pustego kwadratu
Moduł zabezpieczeń	Biblioteka za pomocą, której aplikacja odczytuje i zapisuje dane na karcie
Przeglądarka	Aplikacja do otwierania stron internetowych (WWW)
Karta Kryptograficzna	Nośnik, na który wgrywany jest certyfikat operatora (SSL)
Certyfikat Operatora	Certyfikat zawierający dane osoby wprowadzającej zmiany do systemu. Wykorzystywany do logowania do aplikacji CEPIK. Wymagany jeden na użytkownika.
Certyfikat Infrastruktury	Certyfikat zawierający dane firmy (Instytucji). Wykorzystywany do łączenia się z siecią wewnętrzną CEPIK. Wymagany jeden na Instytucje.

2. Zanim przystąpisz do generowania certyfikatu

2.1. Wymagane oprogramowanie

- JAVA 8 32bit, Zalecana JAVA 8.151 32bit
- Przeglądarka: Internet Explorer, Firefox 32bit w wersji 51.0 bądź poniżej
- Sterowniki do karty kryptograficznej
- Sterowniki do czytnika

2.2. Konfiguracja oprogramowania

Wymagane aplikacje/oprogramowanie można pobrać z strony: <https://sd.coi.gov.pl> korzystając z nazwy użytkownika oraz hasła: cepik

1. JAVA:

- Należy włączyć obsługę JAVA dla przeglądarek oraz aplikacji, aby to wykonać należy:
 - Uruchomić „Java Control Panel” wpisując w „Start” polecenie „Configure Java”
 - Przechodzimy do zakładki „Security”
 - Zaznaczamy checkbox „Enable Java content for browser and Web Start applications”
 - Po wprowadzeniu zmian należy je zatwierdzić klikając przycisk „OK”
- Należy dodać adres strony do recertyfikacji do wyjątków bezpieczeństwa JAVA, aby to wykonać należy:
 - Uruchomić „Java Control Panel” wpisując w „Start” polecenie „Configure Java”
 - Przechodzimy do zakładki „Security”
 - Wybieramy opcję „Edit Site List...”
 - Następnie w nowym oknie klikamy „Add”
 - Wprowadzamy adres strony do recertyfikacji (możemy go skopiować z wiadomości wysłanej na adres mailowy podany na wniosku do kontaktu)
 - Po wprowadzeniu adresu strony zatwierdzamy wszystkie okna klikając „OK”

2. Przeglądarka:

a. Internet Explorer:

- i. Po wejściu na stronę może pojawić się okno z prośbą o włączenie obsługi JAVA, należy wtedy zezwolić aplikacji na działanie.

b. Firefox:

- i. W Firefox należy najpierw dodać moduł zabezpieczeń z którego ma korzystać aplikacja
 1. Przechodzimy do ustawień Firefox > Zaawansowane > Certyfikaty
 2. Następnie wybieramy "Urządzenia zabezpieczające"
 3. Wybieramy „Wczytaj” i wskazujemy lokalizację biblioteki z katalogu C:\Windows\System32 (biblioteka musi być 32 bitowa)
- ii. Po wejściu na stronę może pojawić się okno z prośbą o włączenie obsługi JAVA, należy wtedy zezwolić aplikacji na działanie.

c. Microsoft Edge:

- i. W przeglądarce należy ustawić tryb pracy jako Internet Explorer. Aby to wykonać należy:
 1. Przejść w Ustawienia > Przeglądarka domyślna,
 2. W polu „**Umożliwianie otwierania witryn przez program Internet Explorer w przeglądarce Microsoft Edge**” wybieramy opcję „**Tylko niezgodne witryny (Zalecane)**”
 3. W polu „**Zezwalaj na ponowne ładowanie witryn w trybie programu Internet Explorer (tryb IE)**” wybieramy opcję „**Zezwalaj**”
 4. W polu „**Strony trybu programu Internet Explorer**” wybieramy „**Dodaj**” a następnie wprowadzamy adres strony podanej w wiadomości mailowej.

3. Sterowniki do karty kryptograficznej:

a. ENCARD/ENIGMA

- i. Należy zainstalować najnowszą aplikację bez zmiany domyślnych ustawień instalatora.
- ii. Po zainstalowaniu aplikacji należy przekopiować biblioteki enigmap11.dll oraz enigmap11_x64.dll z katalogów C:\ProgramFiles | ProgramFiles(x86)\ENCARD do System32 oraz SysWOW64.

b. Certum – Unizeto/ASSECO

- i. Należy zainstalować najnowszą aplikację bez zmiany domyślnych ustawień instalatora.
- ii. Po zainstalowaniu w przypadku nowych kart należy zainicjować profil zwykły.
 1. W celu należy uruchomić aplikację „proCertum CardManager”
 2. Wybieramy opcję „Czytaj Kartę”
 3. Następnie wybieramy zakładkę „Profil Zwykły”
 4. Klikamy „Inicjalizuj profil”
 5. Następnie ustalamy PIN oraz PUK dla karty

c. CryptoTech/Sigillum

- i. Należy zainstalować najnowszą aplikację bez zmiany domyślnych ustawień instalatora
 1. **UWAGA!** – W przypadku instalacji starszej wersji aplikacji 64 bitowej należy najpierw zainstalować 32 bitową aplikację a następnie 64 bitową.
- ii. Po zainstalowaniu aplikacji należy przekopiować bibliotekę CCPkiP11.dll z katalogu C:\ProgramFiles\Cryptotech\CryptoCard do SysWOW64 oraz z katalogu C:\ProgramFiles (x86)\Cryptotech\CryptoCard do System32.

3. Proces Generowania Certyfikatów

W przypadku problemów z generowaniem certyfikatów lub konfiguracją stacji prosimy kontaktować się z Zespołem Service Desk

Czynny: Poniedziałek - Piątek: 07:00 – 19:00 oraz Sobota: 08:00 – 16:00

Tel: 42 253 54 99 (wybieramy 1 i następnie 1)

Email: service_desk_portal@coi.gov.pl

3.1. Certyfikat Operatora (SSL)

1. Przed wykonaniem poniższych punktów należy upewnić się:
 - a. Czy posiadamy dwie części kodu jednorazowego:
 - I. Pierwsza część znajduje się na pierwszej oraz ostatniej stronie wniosku papierowego.
 - II. Druga część znajduje się w wiadomości mailowej wysłanej w momencie zakończenia realizacji wniosku o certyfikat.
 - b. Czy posiadamy kartę, na którą zostanie nadany certyfikat.
 - c. Czy zostały zainstalowane wszystkie wymagane komponenty z punktu 3.1 instrukcji.
2. Przechodzimy na stronę podaną w wiadomości mailowej przesłanej z adresu cc.cepik@mc.gov.pl.
 - a. Jeżeli pojawi się komunikat okno „**Your Java version is out of date.**” Należy w takim przypadku wybrać opcję „Later”.



Your Java version is out of date.

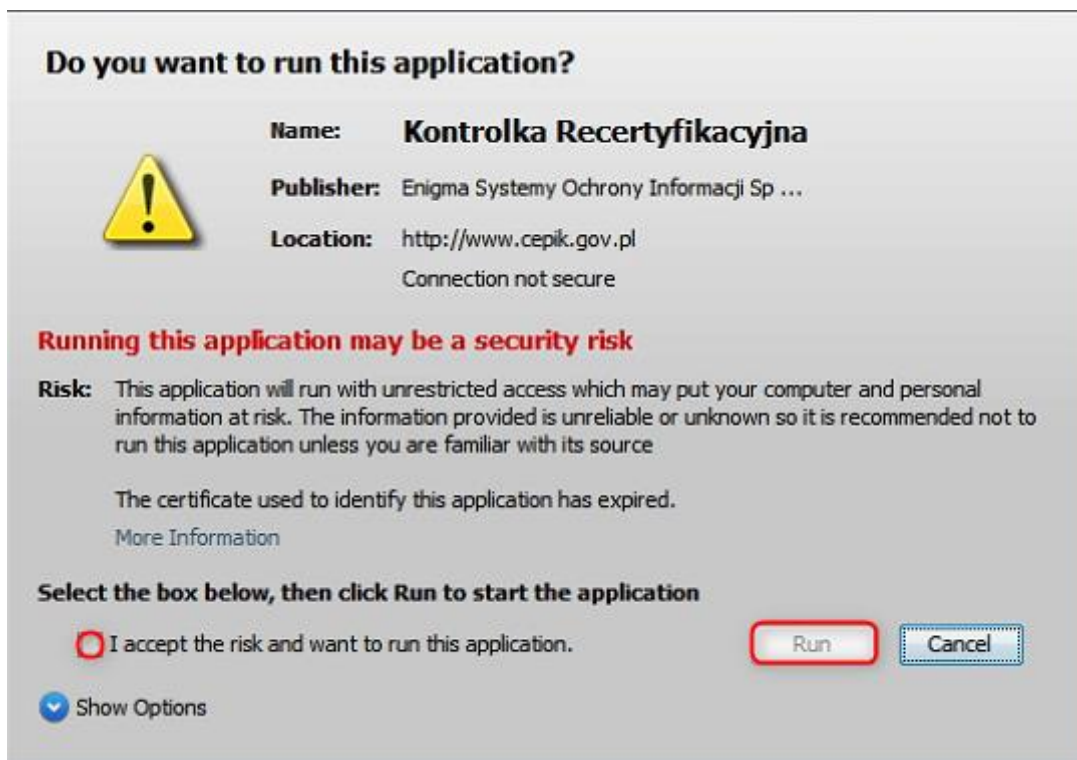
→ Update (recommended)
Get the latest security update from java.com.

→ Block
Block Java content from running in this browser session.

→ Later
Continue and you will be reminded to update again later.

☐ Do not ask again until the next update is available.

- b. Jeżeli pojawi się okno „Do you want to run this application?” zaznaczamy checkbox „I accept the risk and want to run this application” a następnie klikamy „Run”



3. Wybieramy opcję „Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia na karcie PKCS#11”



Centralna Ewidencja
Pojazdów i Kierowców



Kontrast A- A+ Słownik pojęć    

[Strona główna](#) | [CEPiK 2.0](#) | [Zdalna certyfikacja](#)

Zdalna certyfikacja - Operatorzy (środowisko produkcyjne)

Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia na karcie PKCS#11 >

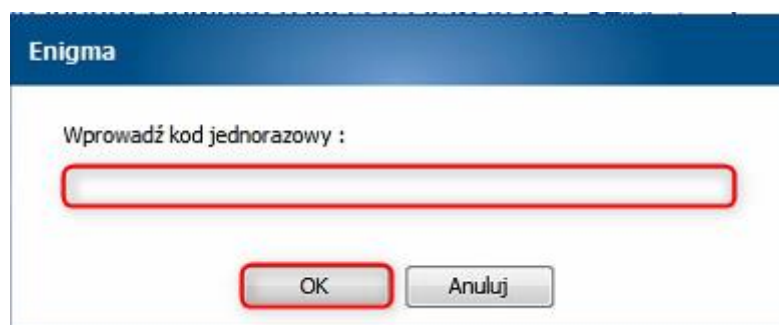
Odnowienie certyfikatu jest realizowane przez stronę WWW, na komputerze z systemem operacyjnym Windows (Windows XP lub nowszy). Wymagane jest także, aby na komputerze był zainstalowany bezpłatny pakiet oprogramowania Java.

4. Po chwili powinno pojawić się okno do wprowadzenia **PIN-u karty**. Wprowadzamy PIN i zatwierdzamy klikając „OK”



The screenshot shows a dialog box titled "Enigma". Inside, the text "Pin do karty: ENCARD Token kwalifikowany" is displayed above a text input field. Below the input field are two buttons: "OK" and "Anuluj". The input field and the "OK" button are highlighted with red rectangles.

5. Następnie pojawi się okno z prośbą wprowadzenia „**kodu jednorazowego**”. Kod jednorazowy wpisujemy jednym ciągiem bez przerw z **zachowaniem wielkości znaków** wpisując po pierwsze „**Pierwszą część kodu**” a następnie „**Drugą część kodu**”. Zatwierdzamy klikając „OK”



The screenshot shows a dialog box titled "Enigma". Inside, the text "Wprowadź kod jednorazowy :" is displayed above a long text input field. Below the input field are two buttons: "OK" and "Anuluj". The input field and the "OK" button are highlighted with red rectangles.

6. Jeżeli „**kod jednorazowy**” zostanie wpisany prawidłowo, powinniśmy otrzymać komunikat:

Zdalna certyfikacja - Operatorzy (środowisko produkcyjne)

[Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia na karcie PKCS#11 >](#)

Odnowienie certyfikatu jest realizowane przez stronę WWW, na komputerze z systemem operacyjnym Windows (Windows XP lub nowszy). Wymagane jest także, aby na komputerze był zainstalowany bezpłatny pakiet oprogramowania Java.

Operacja zakończona sukcesem

3.2. Certyfikat Infrastruktury (VPN)

1. Przed wykonaniem poniższych punktów należy upewnić się:
 - a. Czy posiadamy dwie części kodu jednorazowego:
 - I. Pierwsza część znajduje się na pierwszej oraz ostatniej stronie wniosku papierowego.
 - II. Druga część znajduje się w wiadomości mailowej wysłanej w momencie zakończenia realizacji wniosku o certyfikat.
 - b. Czy zostały zainstalowane wszystkie wymagane komponenty z punktu 3.1 instrukcji.
2. Przechodzimy na stronę podaną w wiadomości mailowej przesłanej z adresu cc.cepik@mc.gov.pl.
 1. Jeżeli pojawi się komunikat okno „**Your Java version is out of date.**” Należy w takim przypadku wybrać opcję „Later”.



Your Java version is out of date.

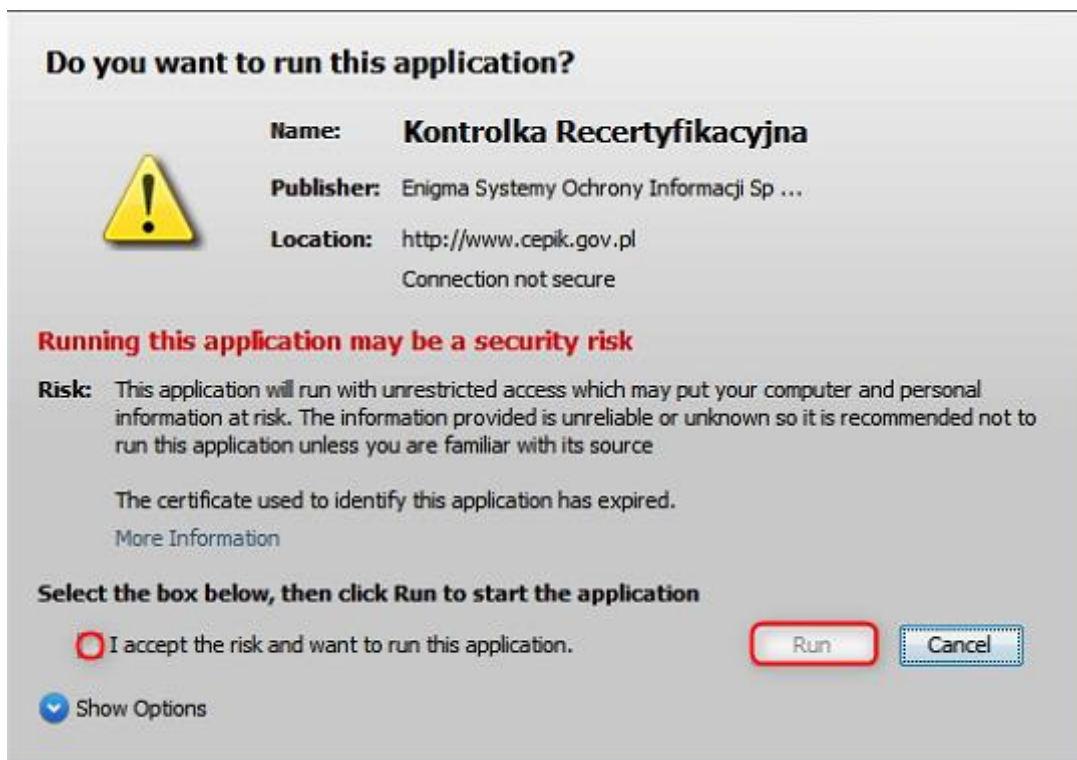
→ **Update (recommended)**
Get the latest security update from java.com.

→ **Block**
Block Java content from running in this browser session.

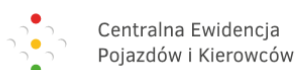
→ **Later**
Continue and you will be reminded to update again later.

☐ Do not ask again until the next update is available.

- Jeżeli pojawi się okno „Do you want to run this application?” zaznaczamy checkbox „I accept the risk and want to run this application” a następnie klikamy „Run”



- Wybieramy opcję „Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia w pliku *.p12”



Centralna Ewidencja
Pojazdów i Kierowców

Kontrast A- | A+ Słownik pojęć

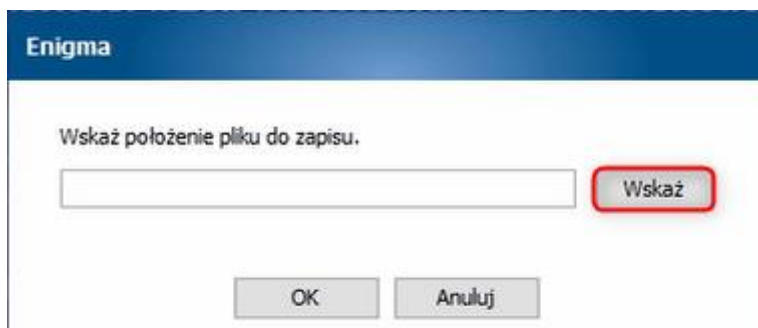
[Strona główna](#) | [CEPiK 2.0](#) | [Zdalna certyfikacja](#)

Zdalna certyfikacja - Infrastruktura (środowisko produkcyjne)

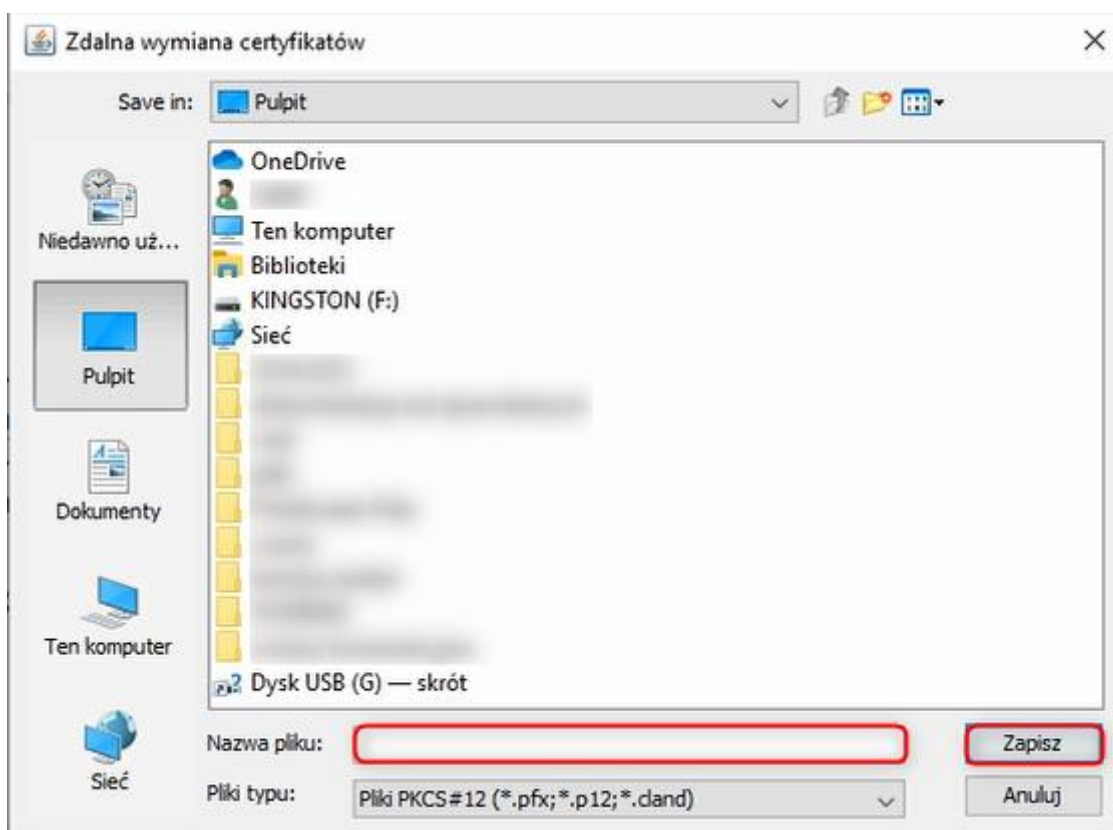
[Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia w pliku *.p12 >](#)

Odnowienie certyfikatu jest realizowane przez stronę WWW, na komputerze z systemem operacyjnym Windows (Windows XP lub nowszy). Wymagane jest także, aby na komputerze był zainstalowany bezpłatny pakiet oprogramowania Java.

4. Po chwili powinno pojawić się okno, w którym należy wskazać lokalizację gdzie certyfikat ma się zapisać. Wybieramy opcję „Wskaz”.

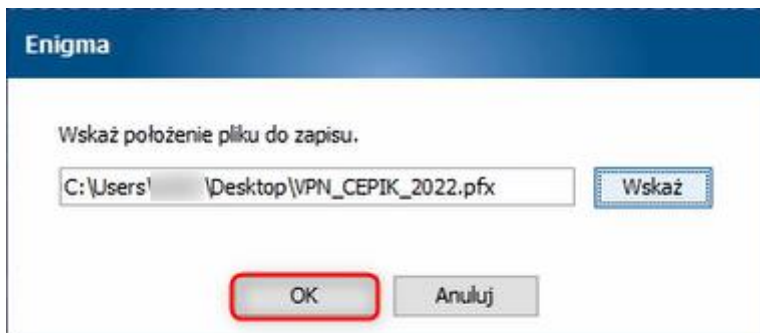


5. Następnie wybieramy miejsce zapisu pliku oraz ustalamy samodzielnie jego nazwę w polu „Nazwa pliku” końcowo zatwierdzając wszystko przyciskiem „Zapisz”.



6.

7. Po zatwierdzeniu poprzednie okno powinno uzupełnić się o lokalizację oraz nazwę, którą wskazaliśmy. Jeżeli lokalizacja się zgadza to zatwierdzamy okno klikając „OK”



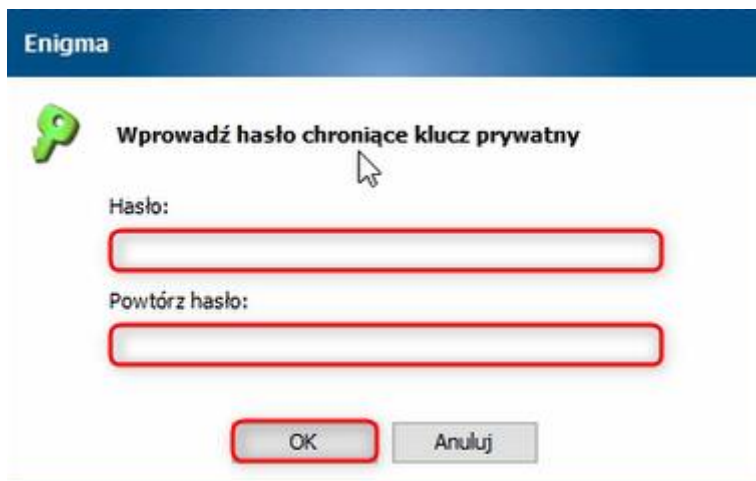
8. Następnie pojawi się okno, w którym należy wprowadzić „**hasło chroniące klucz prywatny**”.

Hasło powinno składać się z:

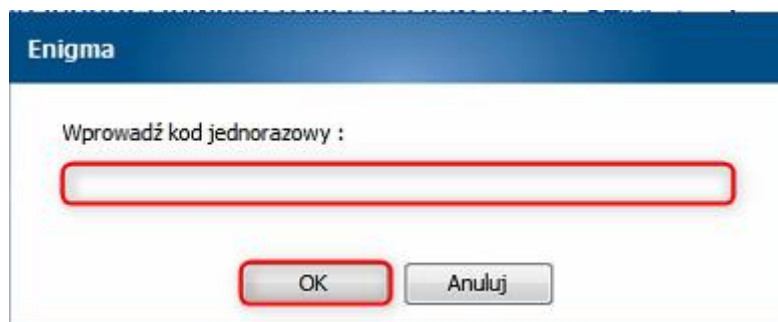
1. Minimum 4 znaków,
2. Mogą być to: Cyfry, Litery, Znaki specjalne.

Hasło jest przypisywane do klucza i nie ma możliwości zmiany jego na inne. W sytuacji gdy zapomnimy hasła do pliku trzeba wysłać wniosek o unieważnienie obecnie posiadanego certyfikatu oraz drugi wniosek o jego odnowienie.

Po ustaleniu hasła oraz jego powtórzeniu klikamy „OK”



9. Następnie pojawi się okno z prośbą wprowadzenia „**kodu jednorazowego**”. Kod jednorazowy wpisujemy jednym ciągiem bez przerw z **zachowaniem wielkości znaków** wpisując po pierwsze „**Pierwszą część kodu**” a następnie „**Drugą część kodu**”. Zatwierdzamy klikając „**OK**”



10. Jeżeli kod jednorazowy zostanie wpisany prawidłowo otrzymamy komunikat

Zdalna certyfikacja - Infrastruktura (środowisko produkcyjne)

Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia w pliku *.p12 >

Odnowienie certyfikatu jest realizowane przez stronę WWW, na komputerze z systemem operacyjnym Windows (Windows XP lub nowszy). Wymagane jest także, aby na komputerze był zainstalowany bezpłatny pakiet oprogramowania Java.

Operacja zakończona sukcesem

11. Podany certyfikat należy następnie zaimportować do systemu do „**Magazynu Użytkownika, Katalog Osobisty**”

Certyfikat Infrastruktury (VPN) jest certyfikatem wielokrotnego użytku dlatego warto skopiować go również w inne miejsce np. inny komputer, dysk przenośny. W przypadku uszkodzenia dysku na stacji na której został wygenerowany Certyfikat.

3.3. Przykładowe komunikaty pojawiające się przy procesie generowania certyfikatów

1. **Nie znaleziono karty w czytniku. Włóż kartę do czytnika** – Komunikat oznacza, iż karta nie znajduje się w czytniku, bądź nie zostały przeniesione biblioteki od karty do odpowiednich katalogów.
2. **ShowOperationEndDialog** – Komunikat oznacza iż nie została zainstalowana JAVA, bądź zainstalowano wersję 64 bitową.