Instrukcja Generowania Certyfikatów CEPIK

SPIS TREŚCI

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
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.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

1. Zanim przystąpisz do generowania certyfikatu

1.1. Wymagane oprogramowanie

- JAVA 8 32bit, Zalecana JAVA 8.151 32bit: JAVA
- Przeglądarka: Microsoft Edge, Internet Explorer, Firefox 32bit w wersji 51.0 bądź poniżej: Firefox 51
- Sterowniki do karty kryptograficznej (najczęściej: ProCertum, ENCARD, CryptoTech)
- Sterowniki do czytnika kart

1.2. Konfiguracja oprogramowania

Wymagane aplikacje/oprogramowanie można pobrać z strony: https://sd.coi.gov.pl korzystając z nazwy użytkownika: **cepik** oraz hasła: **CEpik2024!@**

1.2.1. JAVA

a. Należy włączyć obsługę JAVA dla przeglądarek oraz aplikacji, aby to wykonać należy:
   i. Uruchomić „**Java Control Panel**” wpisując w „**Start**” polecenie „**Configure Java**”,
   ii. Przechodzimy do zakładki „**Security**”,
   iii. Zaznaczamy checkbox „**Enable Java content for browser and Web Start applications**”,
   iv. Przechodzimy do zakładki “**Advanced**”,
   v. Zaznaczamy checkbox "**Enable tracing”, “Enable logging”, “Show applet lifecycle exceptions**”,
   vi. Zaznaczamy checkbox “**Show console**”,
   vii. Zaznaczamy checkbox "**Mozilla family**”.
   viii. Po wprowadzeniu zmian należy je zatwierdzić klikając przycisk „**OK**”.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

b. Należy dodać adres strony do recertyfikacji do wyjątków bezpieczeństwa JAVA, aby to wykonać należy:
    i. Uruchomić „**Java Control Panel**” wpisując w „**Start**” polecenie „**Configure Java**”,
    ii. Przechodzimy do zakładki „**Security**”,
    iii. Wybieramy opcję „**Edit Site List…**”,
    iv. Następnie w nowym oknie klikamy „**Add**”,
    v. Wprowadzamy adres strony do recertyfikacji (możemy go skopiować z wiadomości wysłanej na adres mailowy podany na wniosku do kontaktu),
    vi. Po wprowadzeniu adresu strony zatwierdzamy wszystkie okna klikając „**OK**”.

1.2.2. 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
    ii. Przechodzimy do ustawień Firefox > „**Zaawansowane**” > „**Certyfikaty**”,
    iii. Następnie wybieramy "**Urządzenia zabezpieczające**”,
    iv. Wybieramy „**Wczytaj**” i wskazujemy lokalizację biblioteki z katalogu C:\Windows\System32 (biblioteka musi być 32 bitowa), w zależności od karty może być to „**enigmap11.dll**”, „**crypto3PKCS.dll**” lub „**CCPkiP11.dll**”.
    v. Po wejściu na stronę może pojawić się okno z prośbą o włączenie obsługi JAVA, należy wtedy zezwolić aplikacji na działanie.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

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

1.2.3. 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.
   iii. W tym celu należy uruchomić aplikację „**proCertum CardManager**”,
   iv. Wybieramy opcję „**Czytaj Kartę**”,

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

v. Następnie wybieramy zakładkę „**Profil Zwykły**”,
vi. Klikamy „**Inicjalizuj profil**”,
vii. Następnie ustalamy ***PUK*** oraz ***PIN*** dla karty.

c. CryptoTech/Sigillum
   i. Należy zainstalować najnowszą aplikację bez zmiany domyślnych ustawień instalatora
   ii. ***UWAGA!*** – W przypadku instalacji starszej wersji aplikacji 64 bitowej należy najpierw zainstalować 32 bitową aplikację a następnie 64 bitową.
   iii. 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.

2. 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

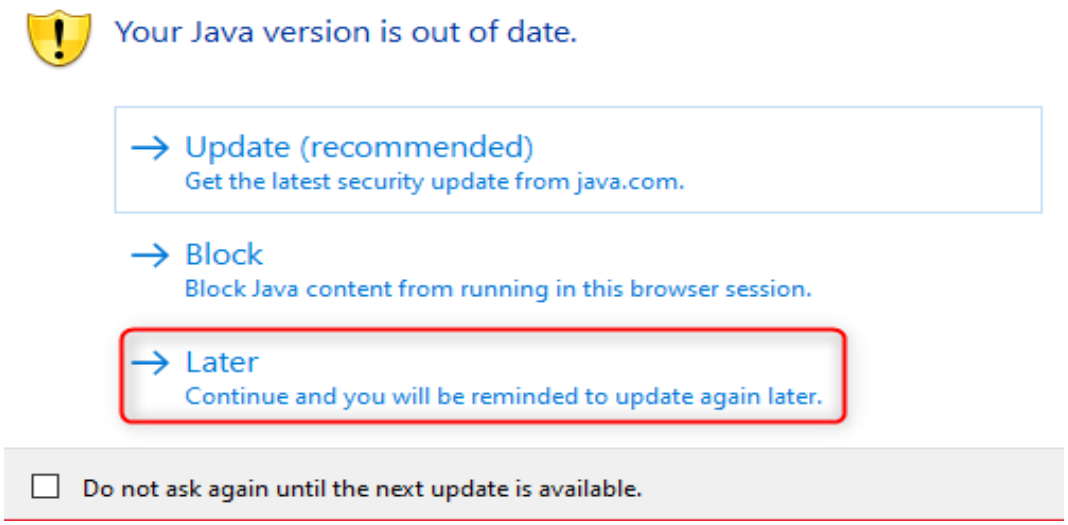
2.1. Certyfikat Operatora (SSL)

1. Przed wykonaniem poniższych punktów należy upewnić się:
   a. Czy posiadamy dwie części kodu jednorazowego:
      I. Pierwsza część znajduję się na pierwszej oraz ostatniej stronie wniosku papierowego.
      II. Druga część znajduję się w wiadomości mailowej wysłanej w momencie zakończenia realizacji wniosku o certyfikat.
   b. Czy zostały zainstalowane wszystkie wymagane komponenty z punktu 3.1 instrukcji.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

2. Przechodzimy na stronę podaną w wiadomości mailowej przesłanej z adresu cc.cepik@cyfra.gov.pl.

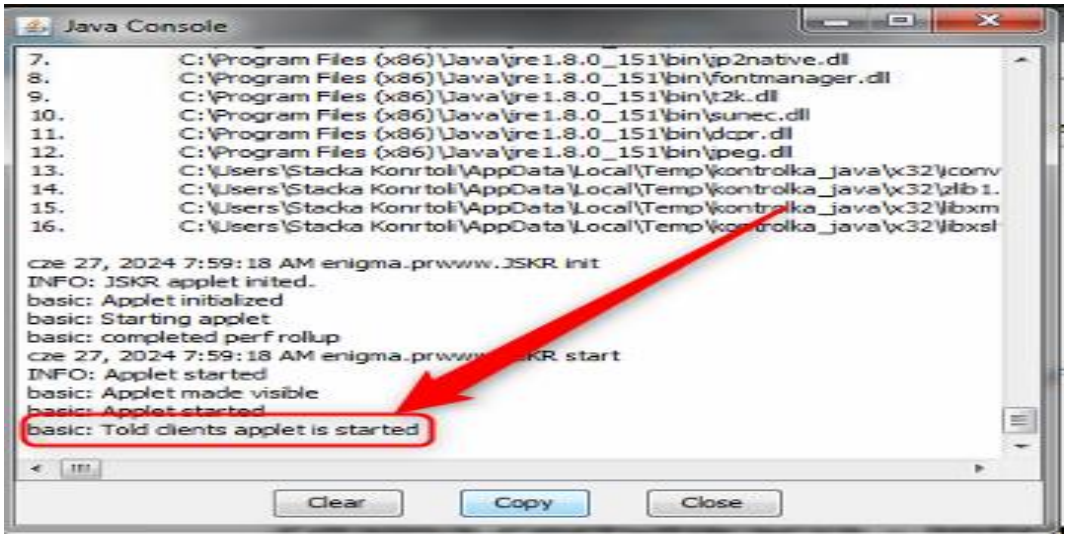
3. Jeżeli pojawi się komunikat okno „**Your Java version is out of date**” Należy w takim przypadku wybrać opcję „**Later**”.



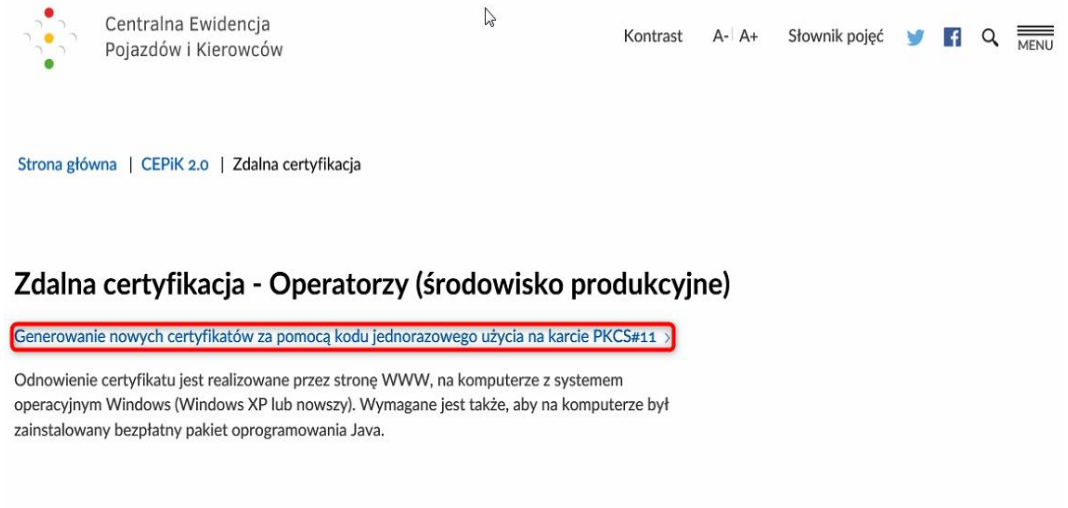
4. Jeżeli pojawi się okno „**Do you want to run this application?”** zaznaczamy checkbox „**I accept the risk and want to run this application**” a następnie klikamy “**Run**”.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

a. Po wybraniu przycisku “**Run**” powinno uruchomić się okno konsoli Java. Prosimy poczekać kilkanaście sekund na pojawienie się komunikatu “**Applet is started**”. Okno konsoli może się minimalizować kilkukrotnie.



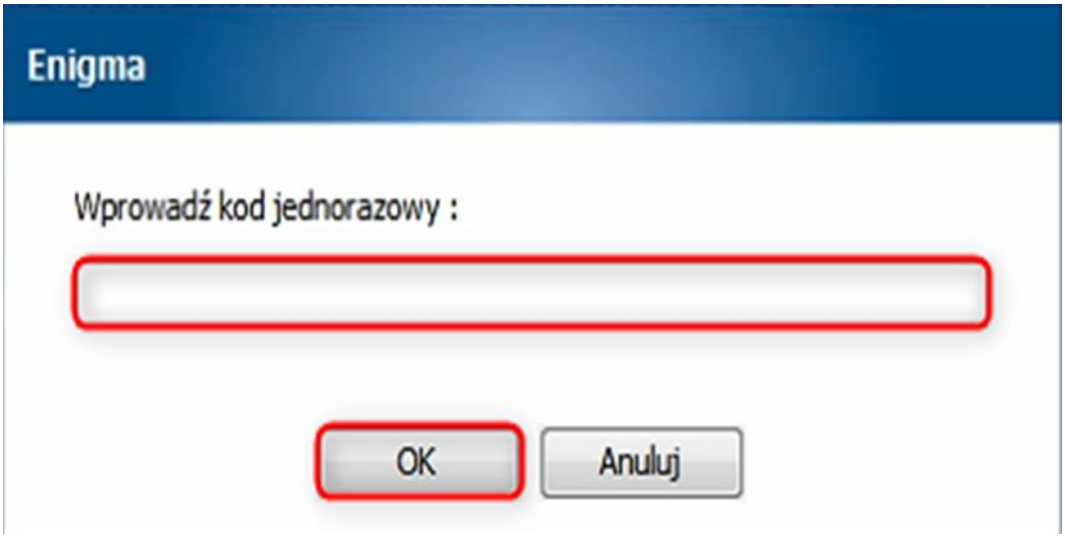
5. Wybieramy opcję „**Generowanie nowych certyfikatów za pomocą kodu jednorazowego użycia na karcie PKCS#11**”.



Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

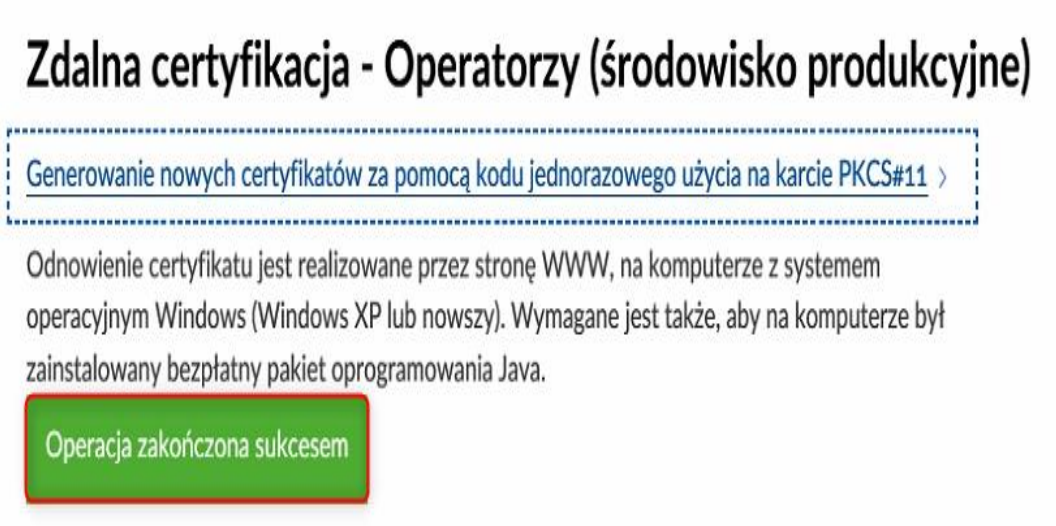
6. Po chwili powinno pojawić się okno do wprowadzenia **PIN-u karty**. Wprowadzamy PIN i zatwierdzamy klikając „**OK**”.

7. 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**”.



Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

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

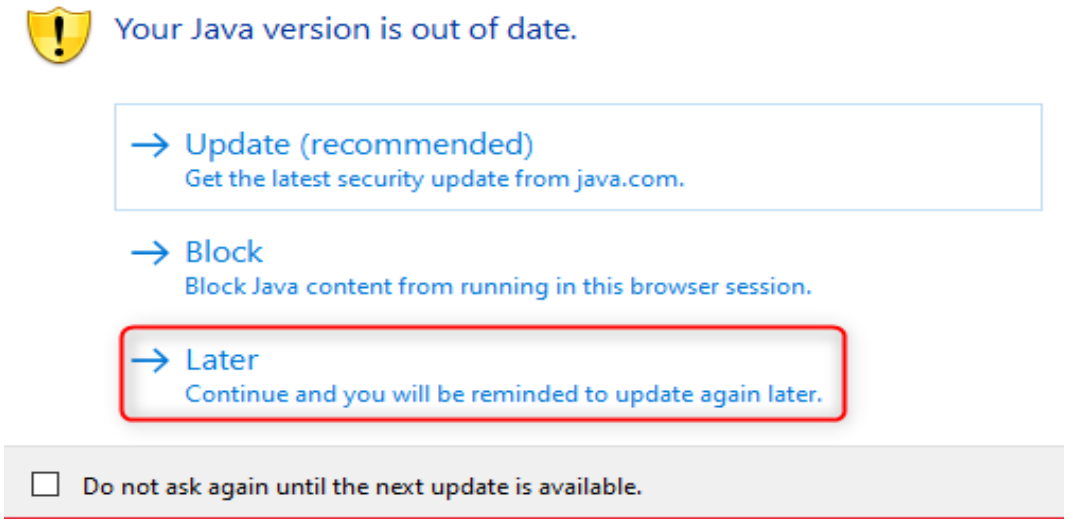


2.2. Certyfikat Infrastruktury (VPN)

1. Przed wykonaniem poniższych punktów należy upewnić się:
   a. Czy posiadamy dwie części kodu jednorazowego:
      I. Pierwsza część znajduję się na pierwszej oraz ostatniej stronie wniosku papierowego,
      II. Druga część znajduję 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@cyfra.gov.pl.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

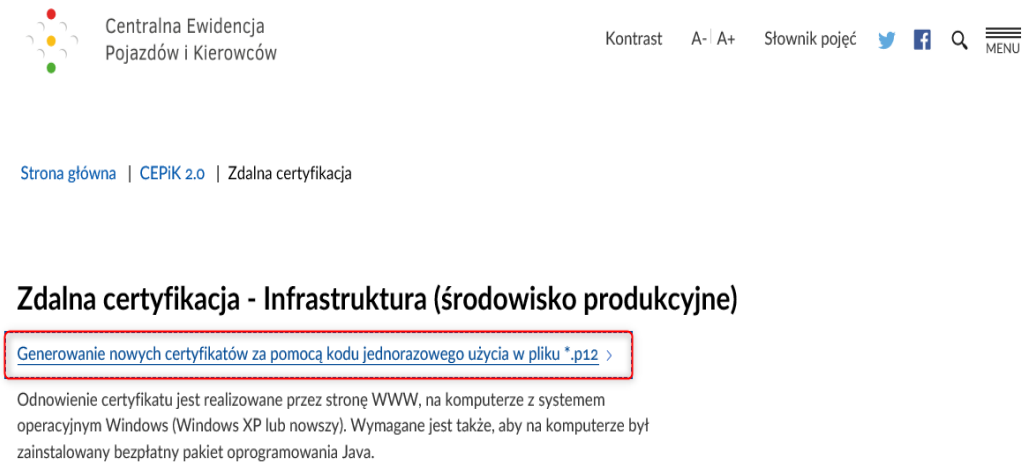
3. Jeżeli pojawi się komunikat „**Your Java version is out of date**” Należy w takim przypadku wybrać opcję „**Later**”.



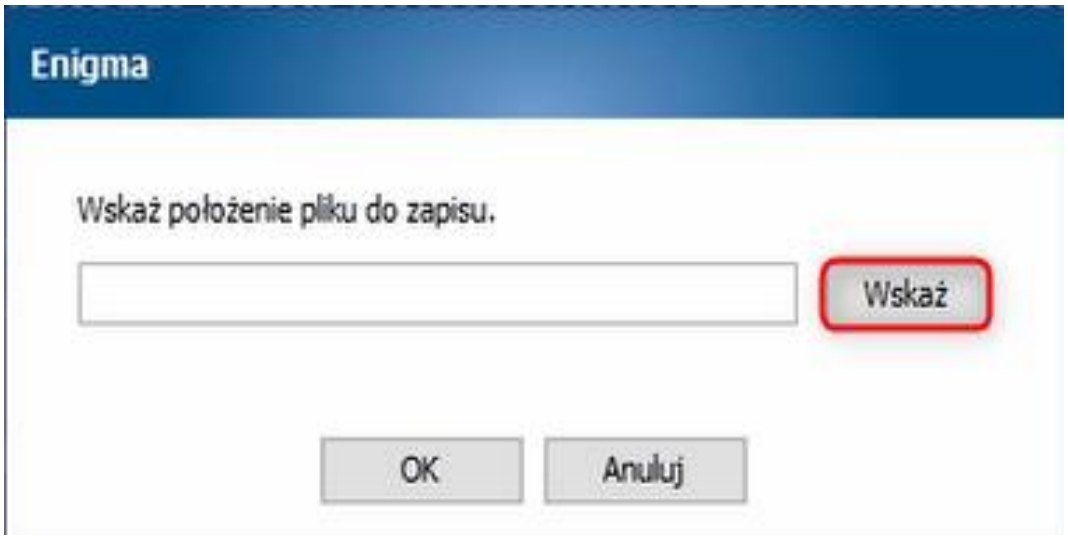
4. Jeżeli pojawi się okno „**Do you want to run this application?**” zaznaczamy checkbox „**I accept the risk and want to run this application**” a następnie klikamy „**Run**”.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

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



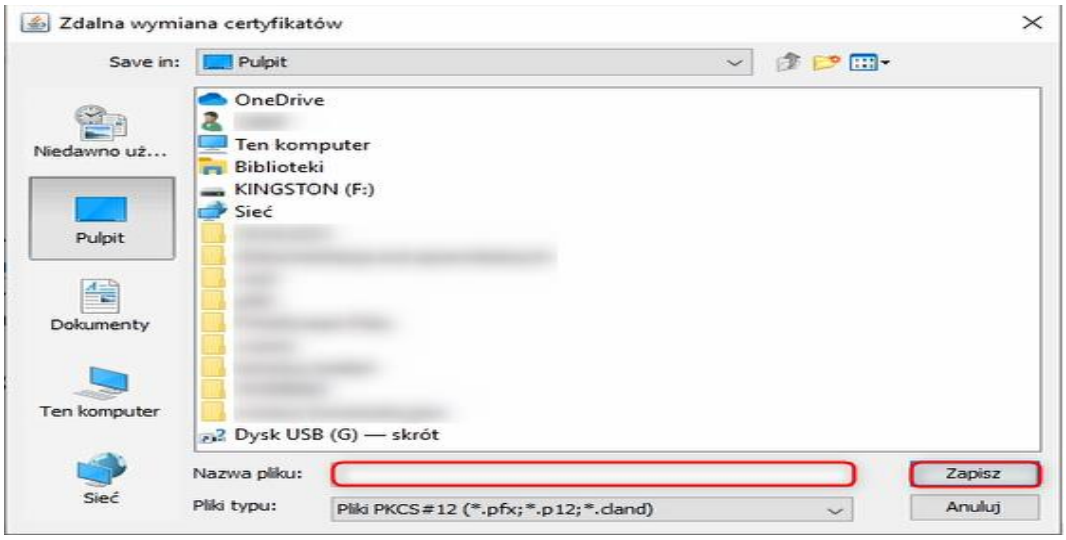
6. Po chwili powinno pojawić się okno, w którym należy wskazać lokalizację gdzie certyfikat ma się zapisać. Wybieramy opcję „**Wskaż**”.



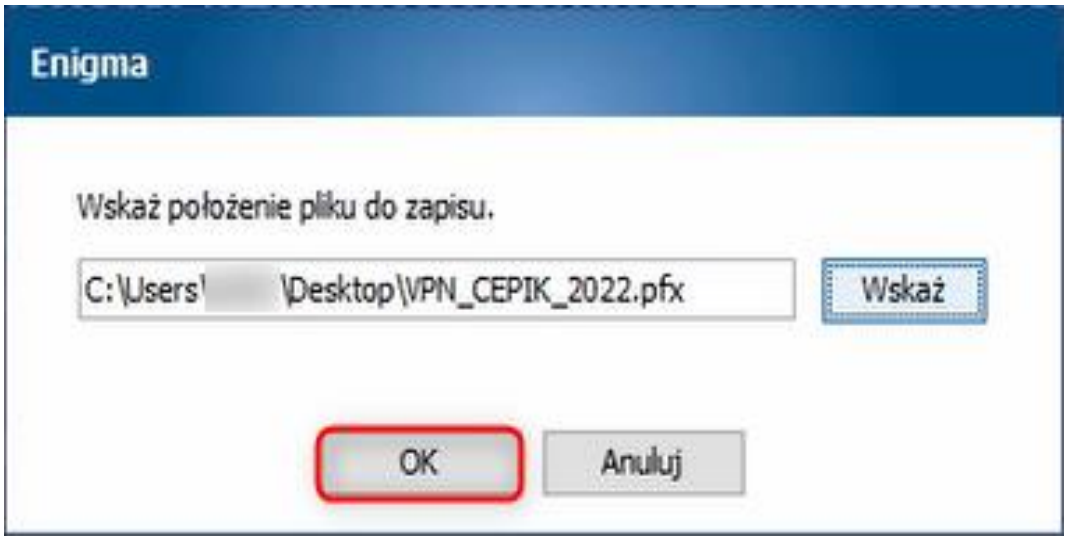
Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

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

   ***Prosimy nie wpisywać w danym polu „kodu jednorazowego”**



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

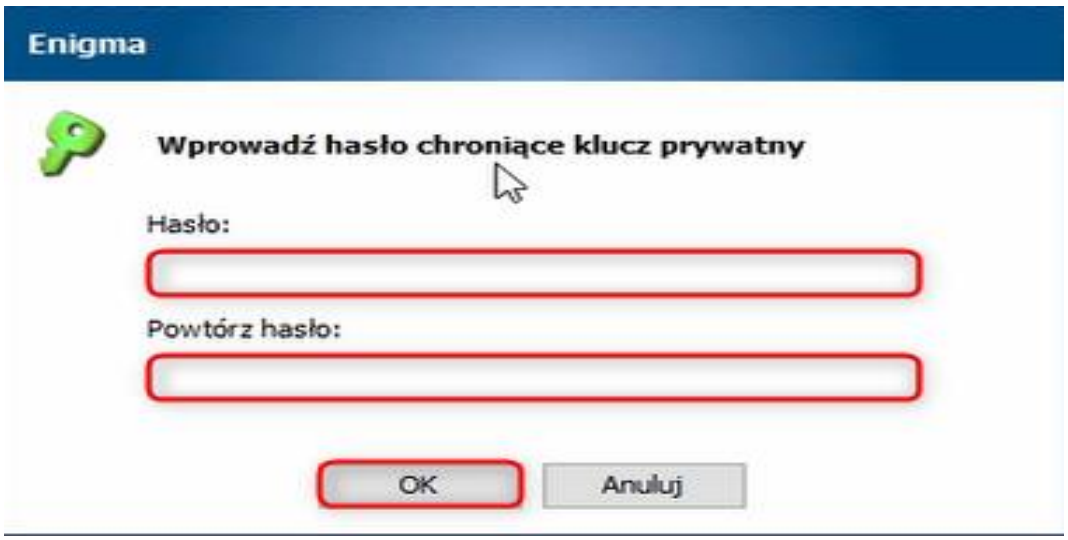


Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

9. Następnie pojawi się okno, w którym należy wprowadzić „**hasło chroniące klucz prywatny**”. Hasło powinno składać się z:
    1. Minumum 4 znaków,
    2. Mogą być to: Cyfry, Litery, Znaki specjalne,
    3. Nie korzystamy z Polskich znaków.

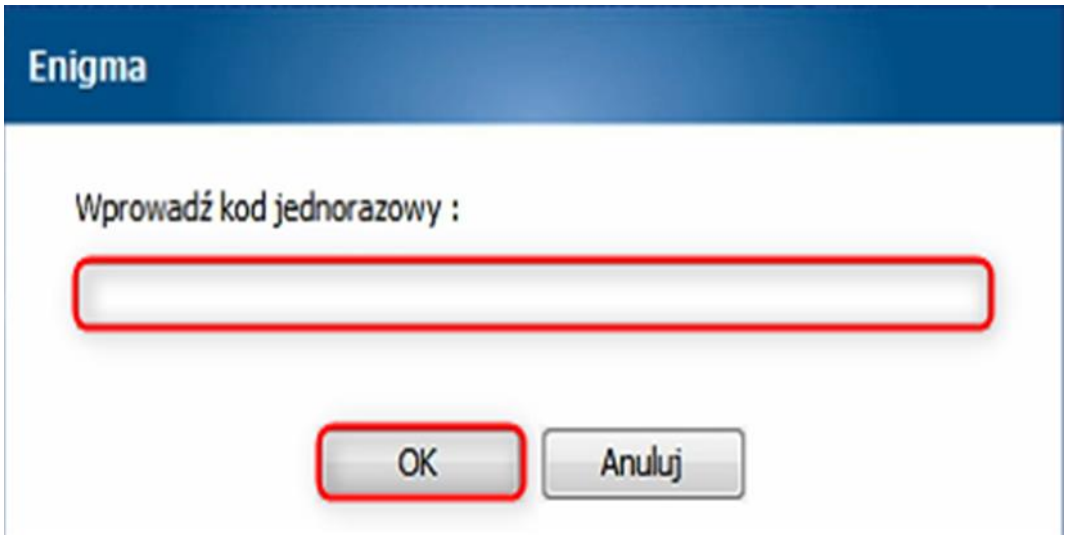
    Hasło jest przypisywane do klucza i nie ma możliwości zmiany jego na inne. W sytuacji gdy zapomnimy hasła do pliku trzeba wysłać wniosek o unieważnienie obecnie posiadanego certyfikatu oraz drugi wniosek o jego odnowienie.

    Po ustaleniu hasła oraz jego powtórzeniu klikamy „**OK**”.

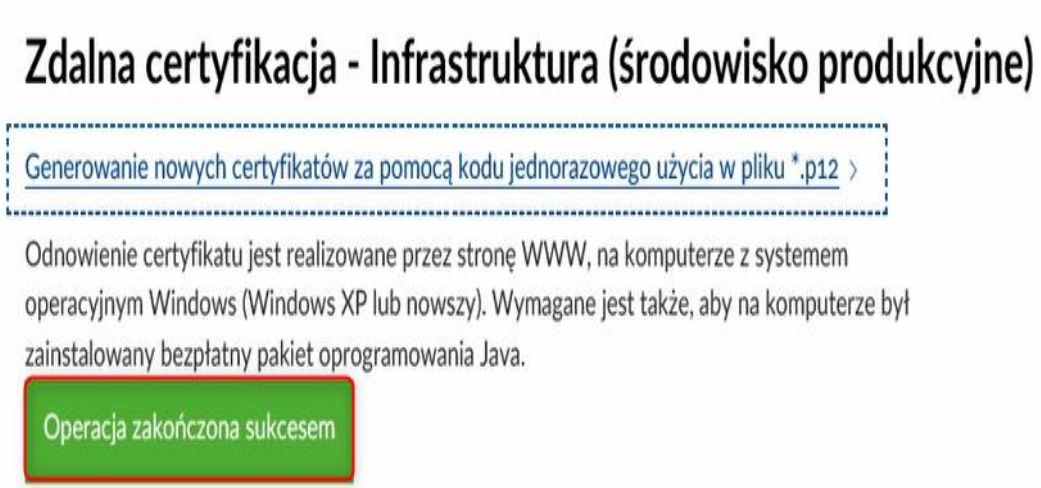


Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

10. 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**”.



11. Jeżeli kod jednorazowy zostanie wpisany prawidłowo otrzymamy komunikat



Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl

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

    Certyfikat Infrastruktury (VPN) zapisany na dysku z rozszerzeniem „.pfx” 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.

13. Po zaimportowaniu certyfikatu głównego do magazynu osobistego należy również pobrać dodatkowe obowiązkowe certyfikaty VPN za pomocą odnośnika Dodatkowe certyfikaty VPN oraz wgrać je do „**Magazynu Użytkownika**”, **Katalog Zaufany główne urzędy certyfikacji**”.

3. Przykładowe komunikaty pojawiające się przy procesie generowania certyfikatów

1. **Nie znaleziono karty w czytniku. Włóż kartę do czytnika** – Komunikat oznacza, iż karta nie znajduję się w czytniku lub sam czytnik jest uszkodzony, bądź nie zostały przeniesione biblioteki od karty do odpowiednich katalogów lub nowa karta nie została zainicjowana(nie nadano **PUK** oraz **PIN** w „**Profilu zwykłym**” w aplikacji **ProCertum**).
2. **ShowOperationEndDialog** – Komunikat oznacza iż nie została zainstalowana JAVA, bądź zainstalowano wersję 64 bitową.
3. **W przeglądarce jest wyłączona obsługa javy. Proszę włączyć obsługę java i spróbować ponownie -** Należy ponownie przejść przez konfigurację Javy lub użyć przeglądarki **Internet Explorer** lub **Firefox 51**.
4. **Do domeny nie jest przypisany wskazany schemat certyfikacji – operacja certyfikacji nie może zostać wykonana** – Oznacza **niewłaściwy adres**, należy skopiować ten z maila w którym otrzymali Państwo drugą część kodu jednorazowego.

Aleje Jerozolimskie 132-136, 02-305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl