Elektroniczny Nadzór Prawny

Konfiguracja konta ePUAP w EAP Legislator

ABC PRO Sp. z o.o.

Dokument zawiera szczegółowy opis generowania certyfikatu dla systemu teleinformatycznego, do celów integracji EAP Legislator z kontem ePUAP urzędu na potrzeby przekazywania aktów do nadzoru prawnego.

Zawartość

Wprowadzenie

W celu umożliwienia wysyłki aktów do nadzoru prawnego Wojewody Podlaskiego z poziomu Edytora Aktów Prawnych Legislator, urząd musi posiadać stosowny certyfikat dla systemu teleinformatycznego. Certyfikat taki uzyskuje się wysyłając odpowiedni wniosek za pośrednictwem platformy ePUAP do Ministerstwa Cyfryzacji.

Ogólne informacje w tym zakresie dostępne są na stronie https://epuap.gov.pl/ w zakładce Pomoc w Strefie Urzędnika:

Przed złożeniem wniosku, w pierwszej kolejności należy w systemie klienta (na komputerze urzędu) przygotować żądanie wystawienia stosownego certyfikatu.

Niniejsza instrukcja opisuje krok po kroku w jaki sposób uzyskać zarówna sam certyfikat z Ministerstwa Cyfryzacji, jak również w jaki sposób użyć go później do integracji EAP Legislator z kontem ePUAP urzędu, celem umożliwienia wysłania aktów do nadzoru prawnego bezpośrednio z aplikacji EAP Legislator.

Tworzenie keystore (tworzenie magazynu na certyfikat)

Keystore – jest magazynem certyfikatów wykorzystywanym w środowisku JAVA. Jeśli do generowania żądania wykorzystujemy właśnie oprogramowanie JAVA będzie to niezbędny element w którym zamieszczone będą wszystkie niezbędne dane do otrzymania poprawnego certyfikatu. W Keystore przechowywany jest klucz certyfikatu, na jego podstawie generowane jest żądanie (plik o rozszerzeniu .csr), które wysyłamy w formularzu wniosku o certyfikat.

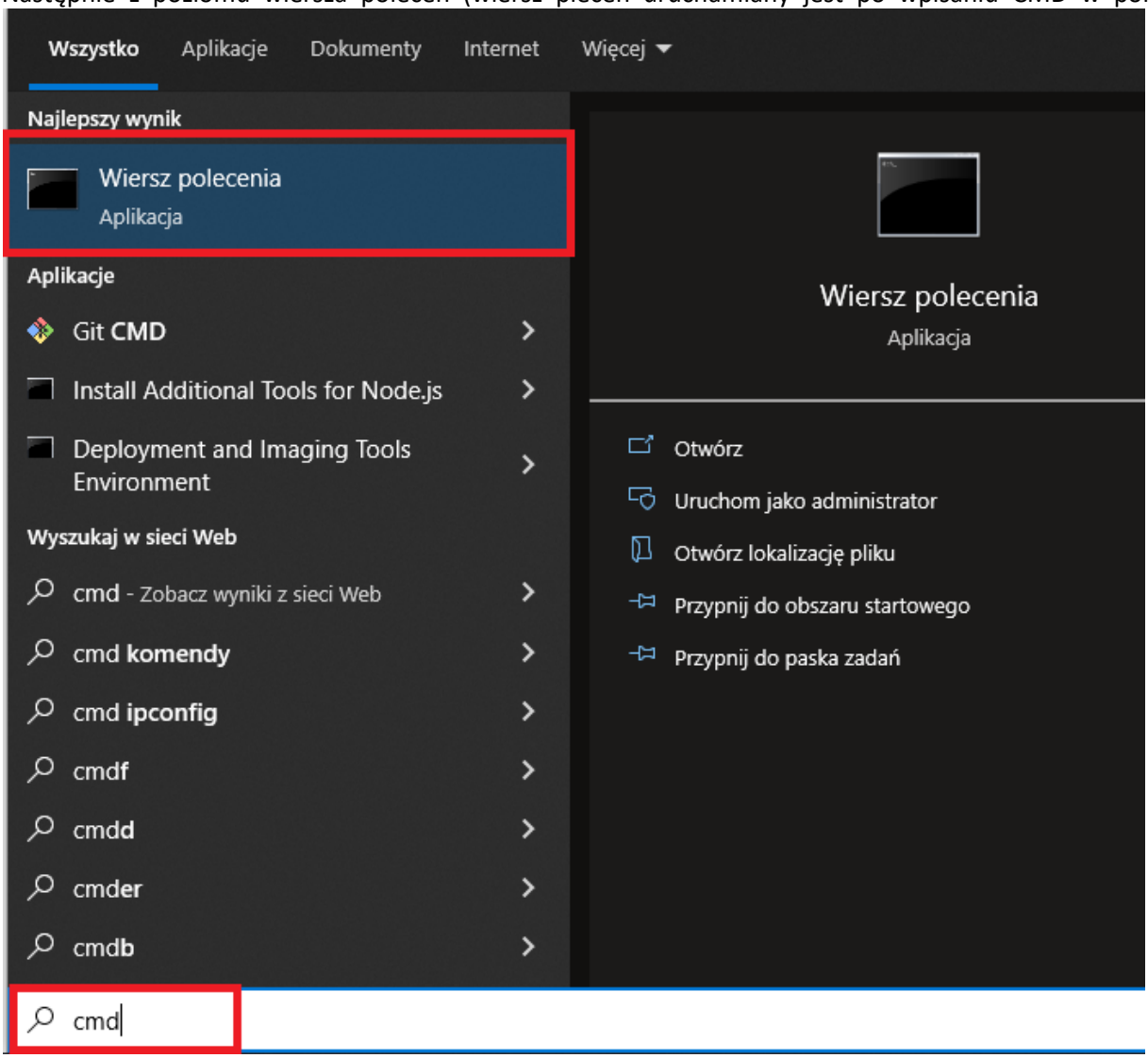
Aby utworzyć wniosek o wydanie certyfikatu można posłużyć się aplikacją keytool.exe. Aplikacja ta dostępna jest po instalacji środowiska Java JRE. Najnowsze środowisko JRE można pobrać ze strony producenta (na potrzeby instrukcji dostępna jest wersja JAVA JRE 8u311)

https://javadl.oracle.com/webapps/download/AutoDL?BundleId=245479_4d5417147a92418ea8b615e228bb6935

Po instalacji (dla systemu x64) narzędzie keytool.exe dostępne jest w lokalizacji C:\Program Files\Java\jre1.8.0_311\bin

W pierwszej kolejności należy utworzyć folder, do którego zostanie zapisane żądanie wystawienia certyfikatu (zostanie utworzony keystore) np. C:\Certyfikaty.

Następnie z poziomu wiersza poleceń (wiersz pleceń uruchamiany jest po wpisaniu CMD w polu „Uruchom”)



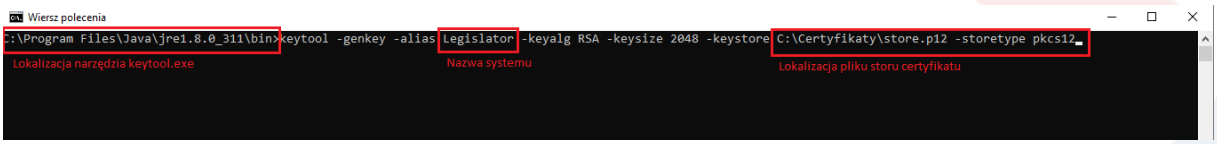
należy przejść do katalogu w którym znajduje się narzędzie keytool.exe i wykonać następujące polecenie:

keytool –genkey –alias <nazwa_systemu> -keyalg RSA –keysize 2048 –keystore <nazwa_pliku_dla_stora_certyfikatów> -storetype pkcs12

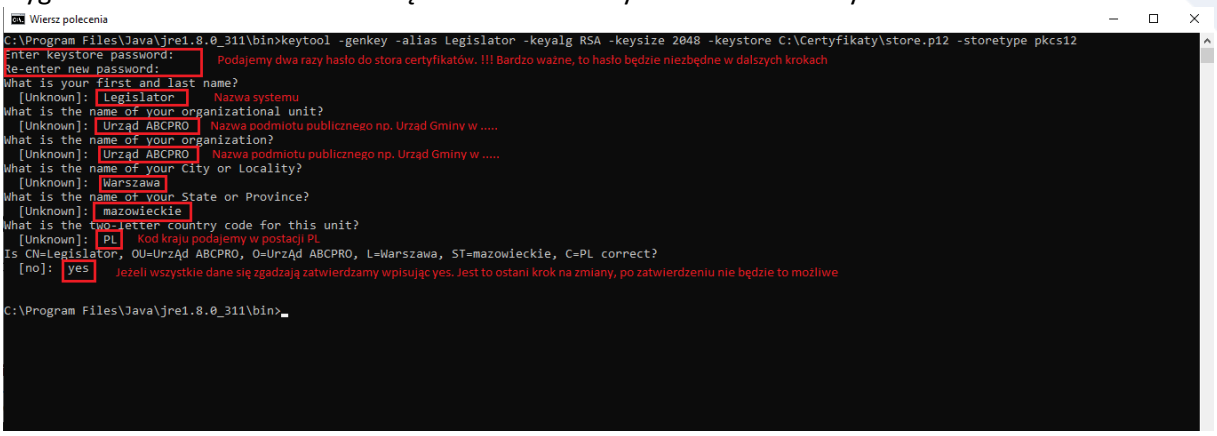
PRZYKŁAD WYKONANIA POLECENIA

Zakładając, że nasz system, dla którego ma być wystawiony certyfikat nazywa się „**Legislator**” a plik magazyny nazwiemy **store.p12** to należy wykonać polecenie:

keytool –genkey –alias Legislator -keyalg RSA –keysize 2048 –keystore C:\Certyfikaty\store.p12 -storetype pkcs12

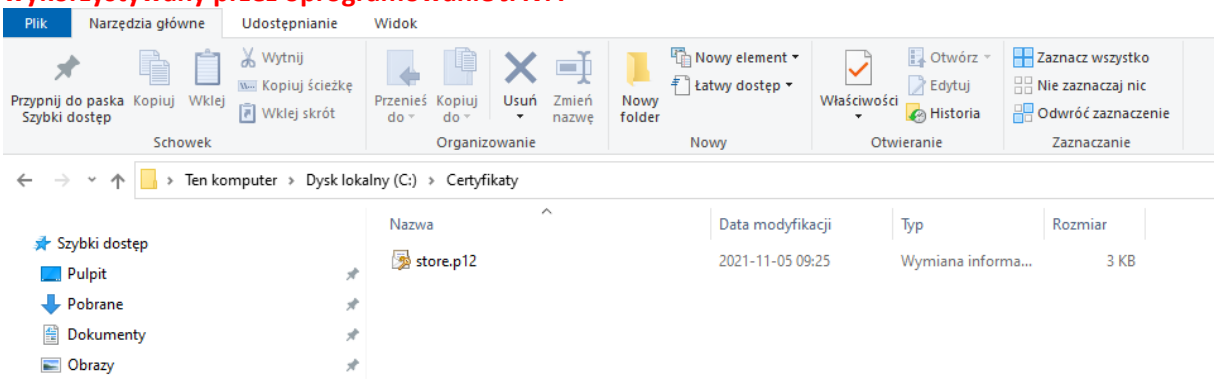


Po wykonaniu polecenia system wyświetli monit o uzupełnienie danych do magazynu na podstawie, którego wygenerowane zostanie żądanie o wystawienie certyfikatu do Ministerstwa Cyfryzacji.



Po wykonaniu powyższej operacji w lokalizacji C:\Certyfikaty zostanie utworzony plik magazynu (**store.p12**) dla certyfikatów.

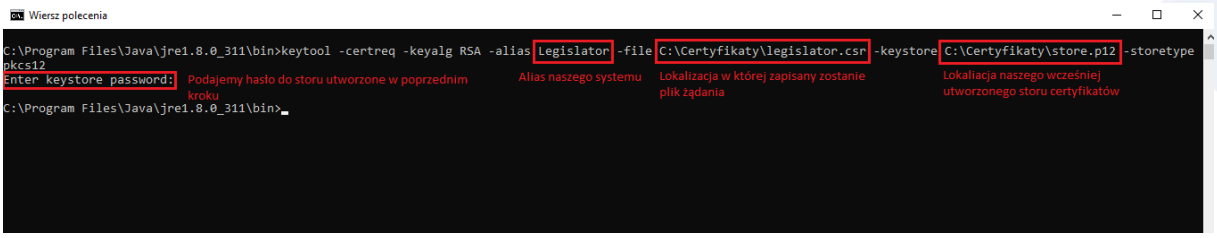
UWAGA. Wygenerowany plik to nie jest jeszcze docelowy certyfikat, a jedynie magazyn na certyfikaty wykorzystywany przez oprogramowanie JAVA



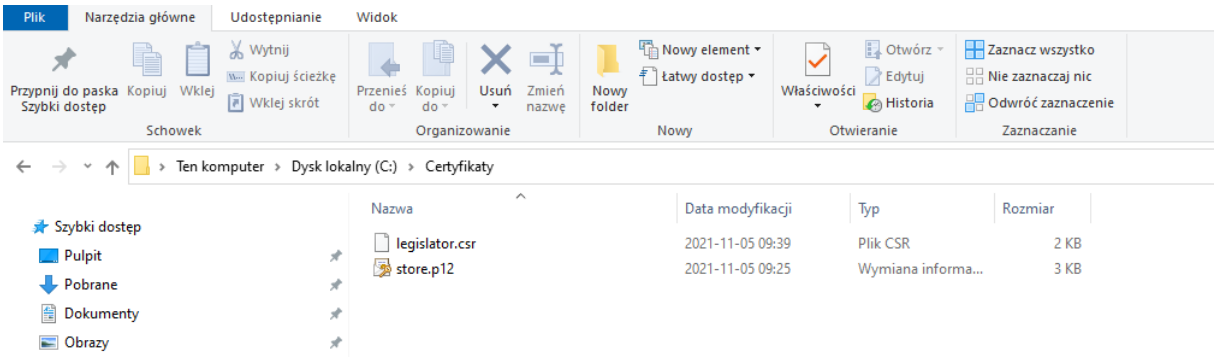
Generowanie żądania certyfikatu

W kolejnym kroku wygenerowane zostanie żądanie o docelowy certyfikat. W tym kroku niezbędne będzie hasło do utworzonego w poprzednim kroku magazynu certyfikatów. W celu wygenerowania żądania wykonać należy następujące polecenie:

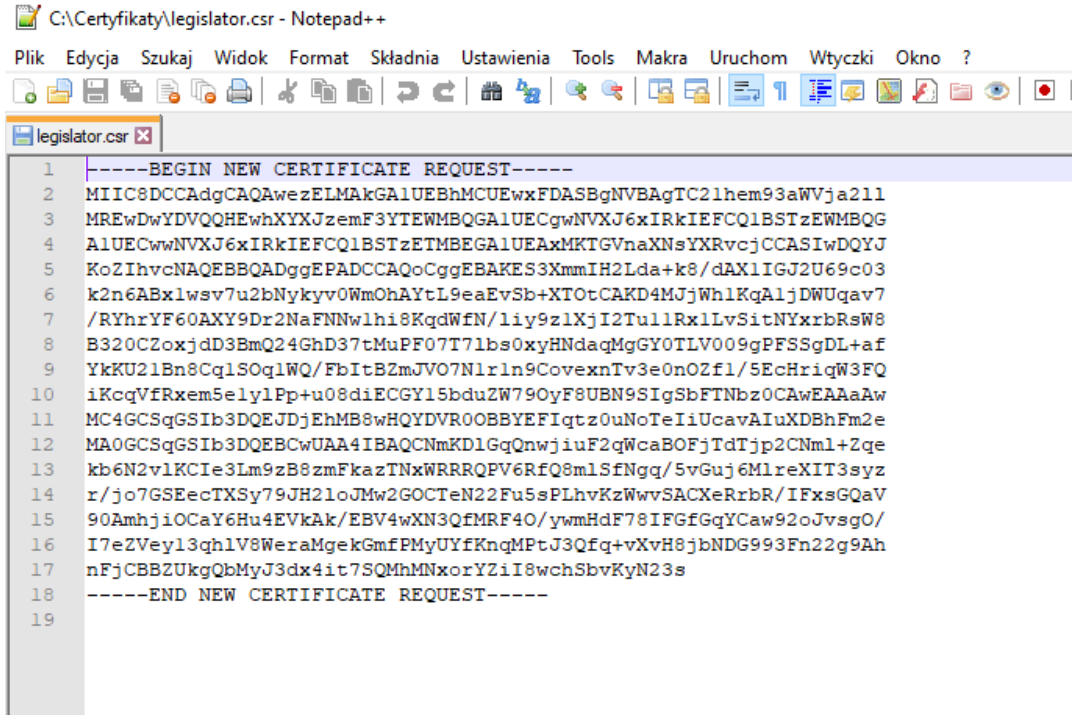
#keytool –certreq –keyalg RSA –alias Legislator –file C:\Certyfikaty\legislator.csr –keystore C:\Certyfikaty\store.p12 –storetype pkcs12



Teraz w lokalizacji C:\Certyfikaty zostanie utworzony drugi plik, tym razem z rozszerzeniem .csr . Ten plik jest właśnie żądaniem certyfikatu.

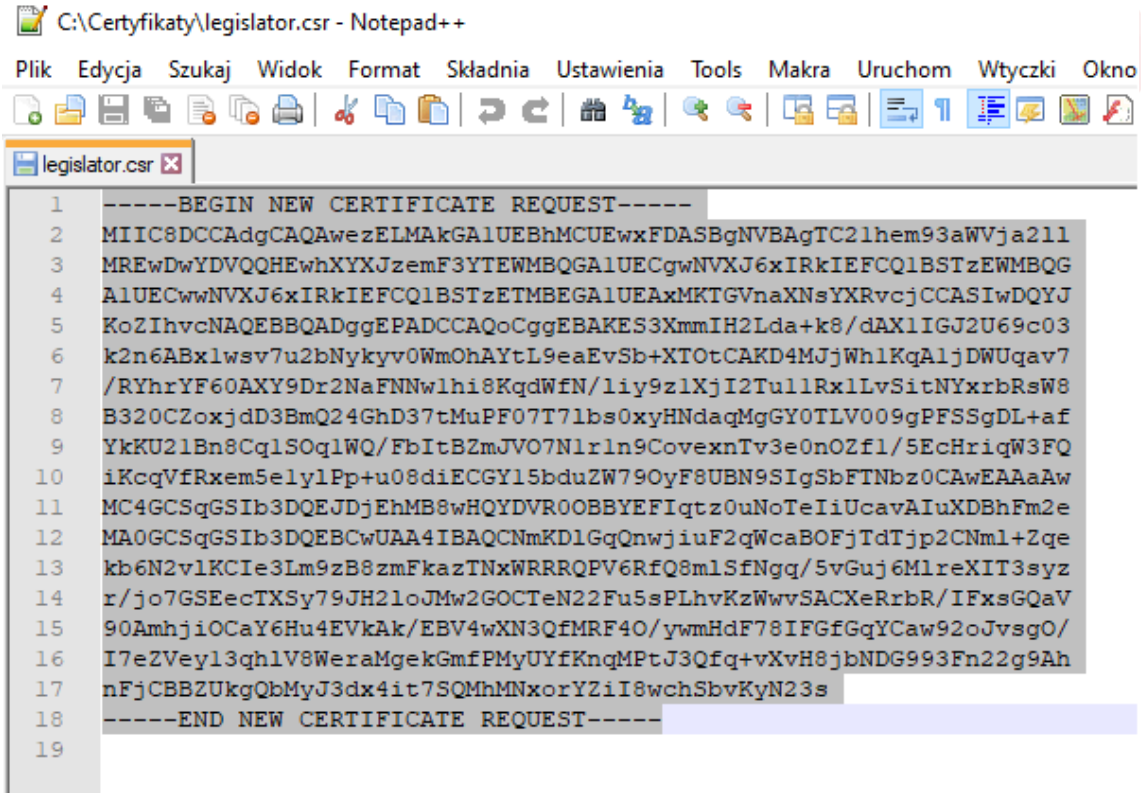


Zawartość tego pliku należy przesłać w treści wniosku do Ministerstwa Cyfryzacji w celu uzyskania docelowego certyfikatu. W tym celu, przy użyciu narzędzia Notatnik lub Notepad++ należy otworzyć plik żądania (legislator.csr)



I całą jego zawartość skopiować (łącznie z liniami -----BEGIN NEW CERTIFICATE REQUEST----- oraz -----END NEW CERTIFICATE REQUEST-----) i wkleić do formularza wniosku o certyfikat.

UWAGA: Bardzo ważne aby nie wkleić dodatkowych białych znaków typu spacja. Należy zaznaczyć tylko i wyłącznie tekst.



Po pomyślnej weryfikacji wniosku, urząd, w odpowiedzi, otrzyma z Ministerstwa właściwy certyfikat w formie pliku txt (**certyfikat.txt**). Certyfikat jest zapisany w formacie base64 i nie zawiera w sobie klucza prywatnego, klucz znajduje się w wygenerowanym wcześniej magazynie certyfikatów (w przypadku niniejszej instrukcji jest to plik **store.p12**).

Certyfikat należy zaimportować do wcześniej wygenerowanego magazynu wykonując polecenie

#keytool –import –trustcacerts –alias Legislator –file C:\Certyfikaty\certyfikat.txt –keystore C:\Certyfikaty\store.p12 –storetype pkcs12

Zostaniemy poproszeni o podanie hasła do magazynu certyfikatów.

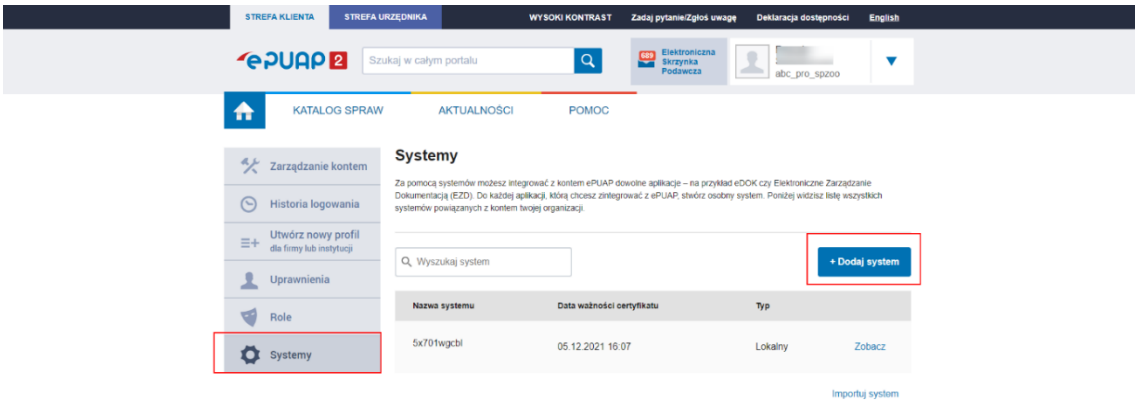
Po wykonaniu powyższego kroku magazyn certyfikatów jest już kompletny, zawiera klucz i certyfikat.

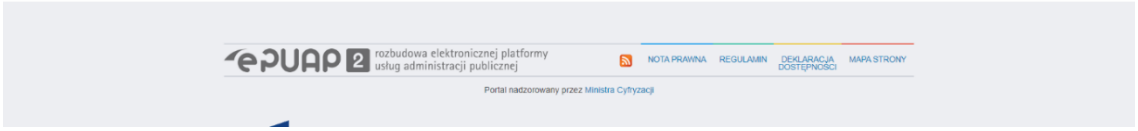
Konfiguracja platformy ePUAP

Po prawidłowym przygotowaniu certyfikatu, należy dokonać stosownej konfiguracji konta urzędu w systemie ePUAP.

W tym celu po zalogowaniu do systemu ePUAP na konto posiadające uprawnienia administratora należy:

1) w prawym rogu wybrać ikonę użytkownika i przejść do opcji „Zarządzanie kontem", a następnie do zakładki po lewej „Systemy" i wybrać opcję „Dodaj system"

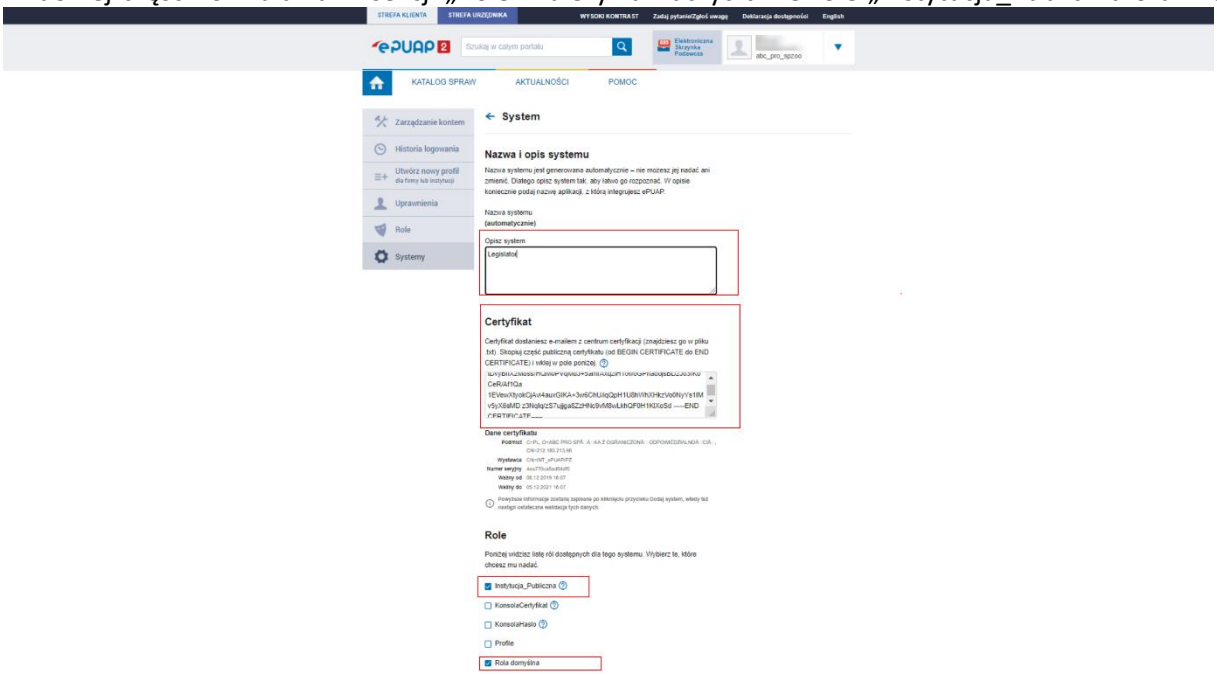




Należy podać opis systemu (dowolna nazwa) oraz wkleić certyfikat otrzymany z ministerstwa.

!!! Uwaga – certyfikat otrzymany z ministerstwa zawiera w sobie całą ścieżkę certyfikacji (certyfikat główny CA, które wydaje certyfikaty oraz certyfikat pośredni), przez co w otrzymanym pliku znajdują się 3 sekcje „-----BEGIN CERTIFICATE----- oraz -----END CERTIFICATE-----"). Do pola Certyfikat należy wkleić jedynie pierwszą sekcję łącznie z wpisami „-----BEGIN CERTIFICATE-----" oraz „-----END CERTIFICATE-----".

W dolnej części formularza w sekcji „Role" należy zaznaczyć dwie role „Instytucja_Publiczna oraz Rola domyślna":



Po zapisaniu systemu platforma ePUAP jest już gotowa do wysyłki wniosków z zewnętrznej aplikacji

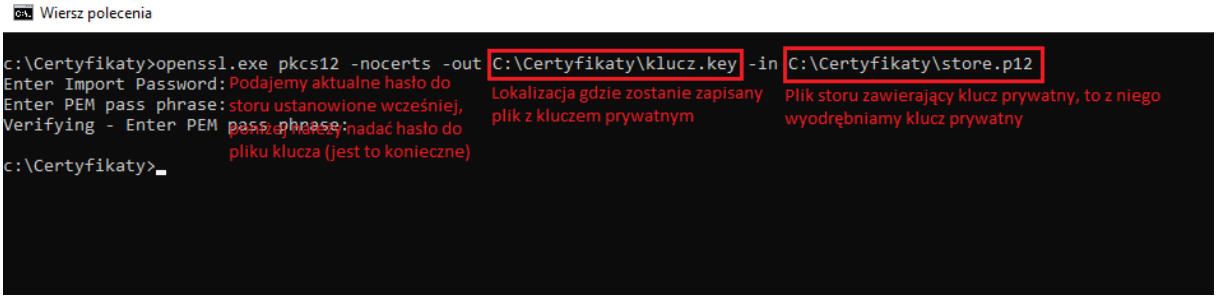
Przygotowanie certyfikatu dla systemu Legislator

Ostatnim krokiem jaki należy wykonać jest przygotowanie certyfikatu w formacie pfx, który zostanie zaimportowany w systemie Windows (na stanowisku, gdzie dokonywana będzie wysyłka dokumentów do nadzoru z poziomu EAP Legislator).

Aby przygotować certyfikat w formacie pfx należy dysponować kluczem prywatnym (w przypadku tej instrukcji znajduje się w pliku store.p12) oraz plikiem certyfikatu (certyfikat.txt) otrzymanym z Ministerstwa. Aby wyodrębnić plik klucza z magazynu certyfikatów należy posłużyć się narzędziem Openssl. Wersję portable można pobrać ze strony ABC PRO SP. z o.o.: https://files.abcpro.pl/download/gosc/OpenSSL.zip

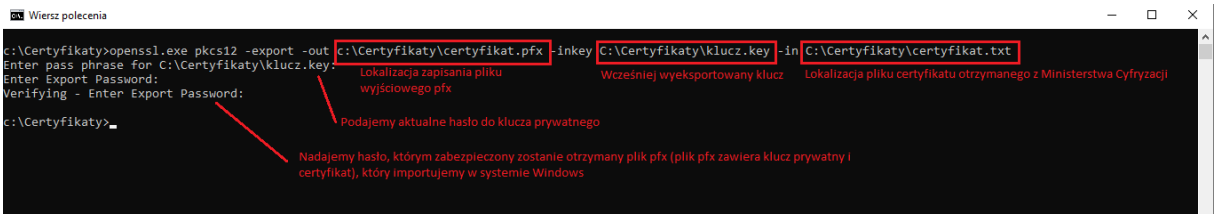
Po rozpakowaniu paczki (w naszym przypadku ta sama lokalizacja C:\Certyfikaty) należy uruchomić wiersz poleceń systemu Windows „CMD" i wykonać polecenie

#openssl pkcs12 –nocerts –out klucz.key –in store.p12



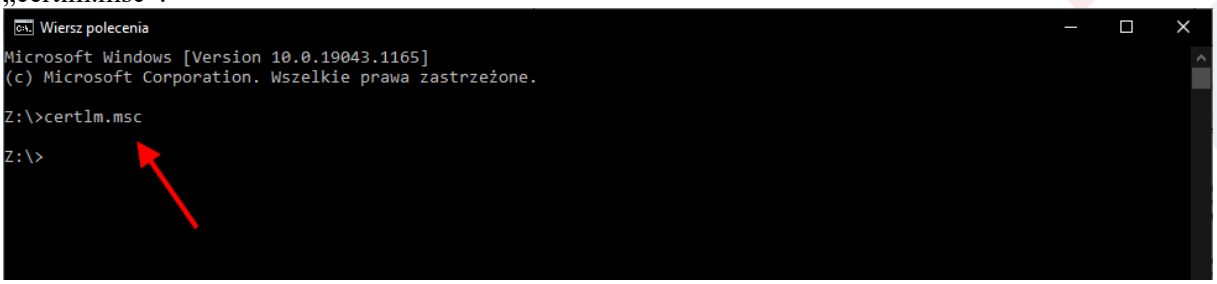
Podczas eksportu klucza, należy podać aktualne hasło do magazynu certyfikatów (te ustalone na początku instrukcji kiedy tworzony był magazyn), a następnie dwukrotnie podać hasło jakim zostanie zabezpieczony klucz prywatny. Jest to element niezbędny inaczej aplikacja wygeneruje błąd.

Kiedy dysponujemy już plikiem z kluczem możemy wygenerować końcowy plik pfx zawierający w sobie certyfikat i klucz prywatny, plik taki ostatecznie importujemy do systemu Windows i to z niego korzysta aplikacja Legislator.

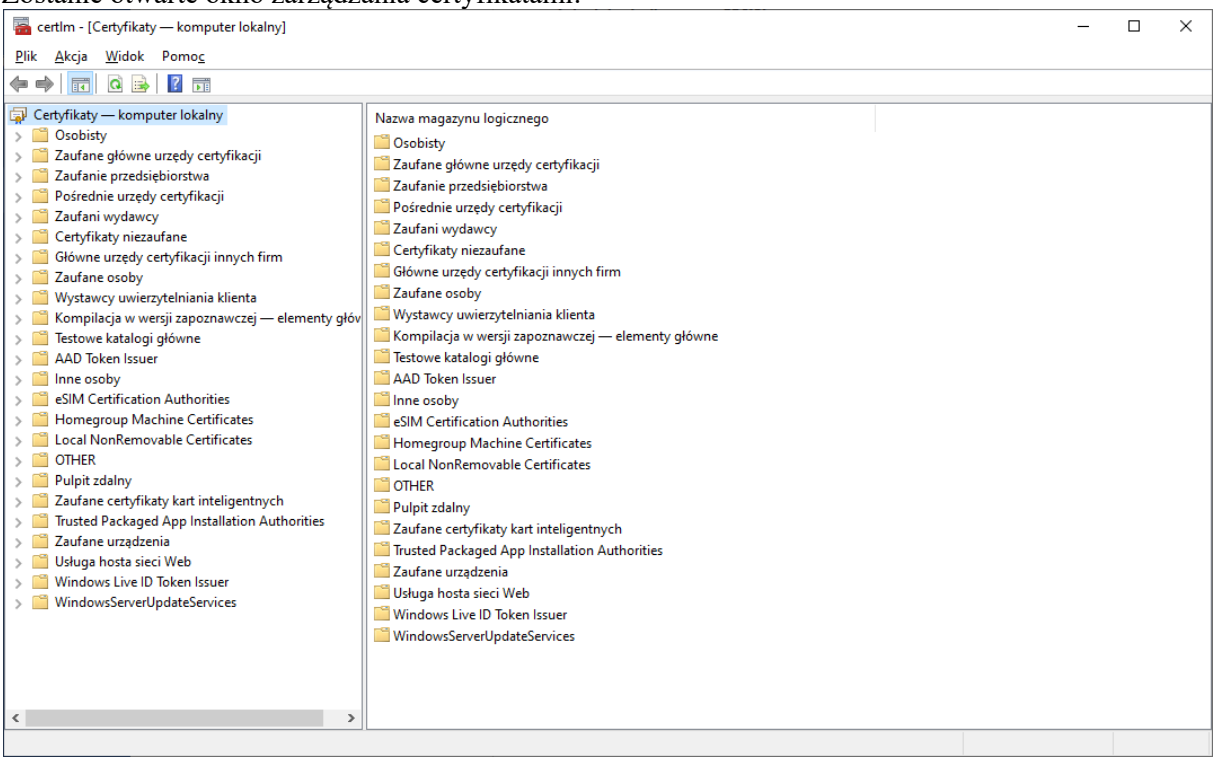


Import certyfikatu do systemu Windows i konfiguracja aplikacji Legislator

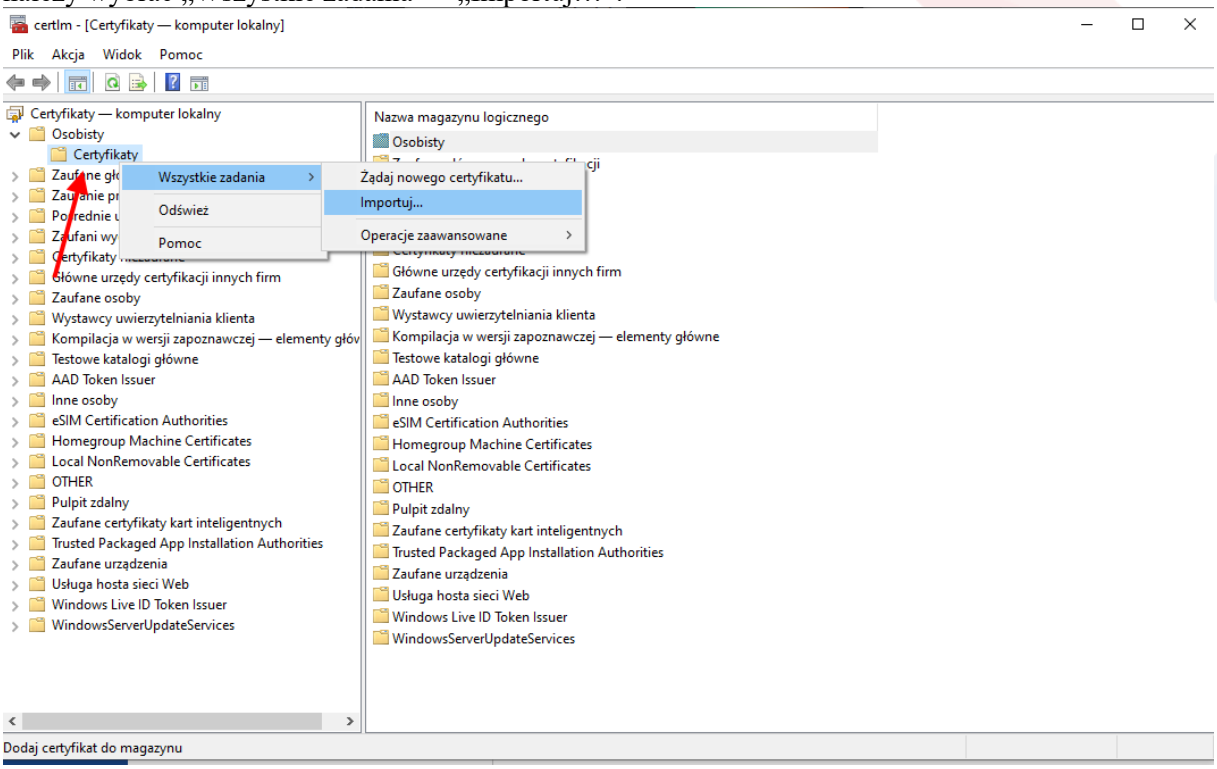
Z poziomu otwartego wiersza poleceń należy uruchomić konsolę zarządzania certyfikatami poprzez polecenie „certlm.msc”:



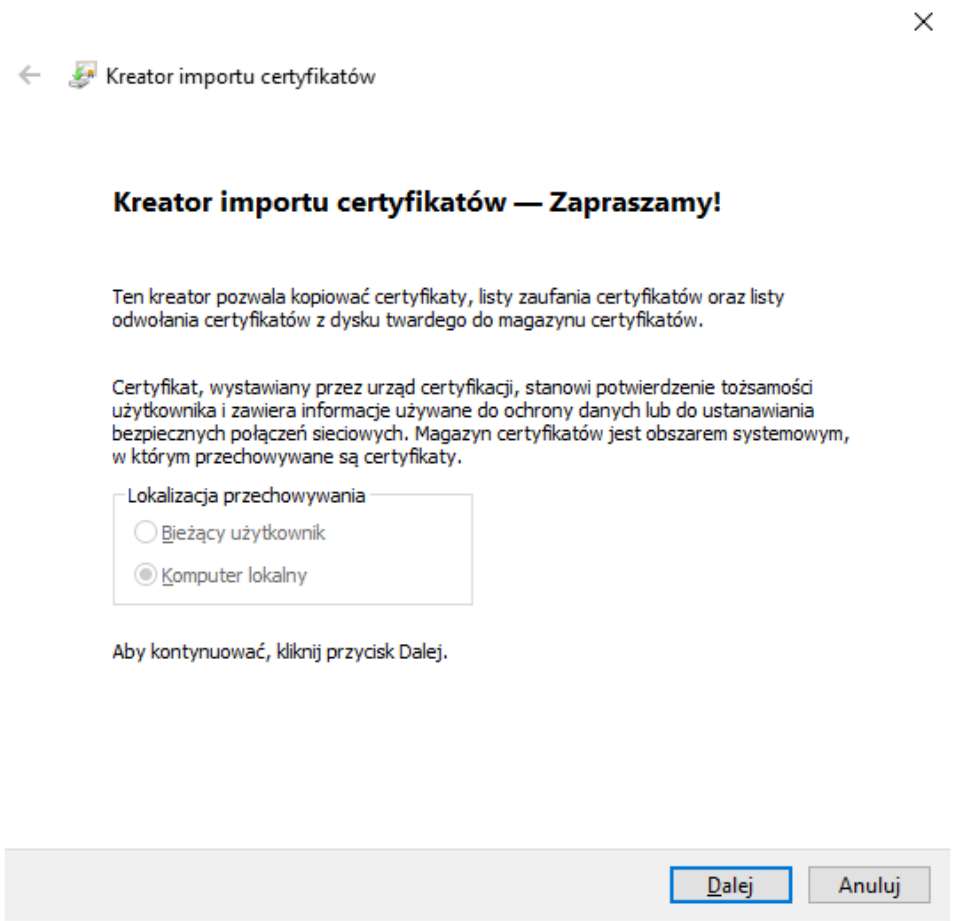
Zostanie otwarte okno zarządzania certyfikatami:



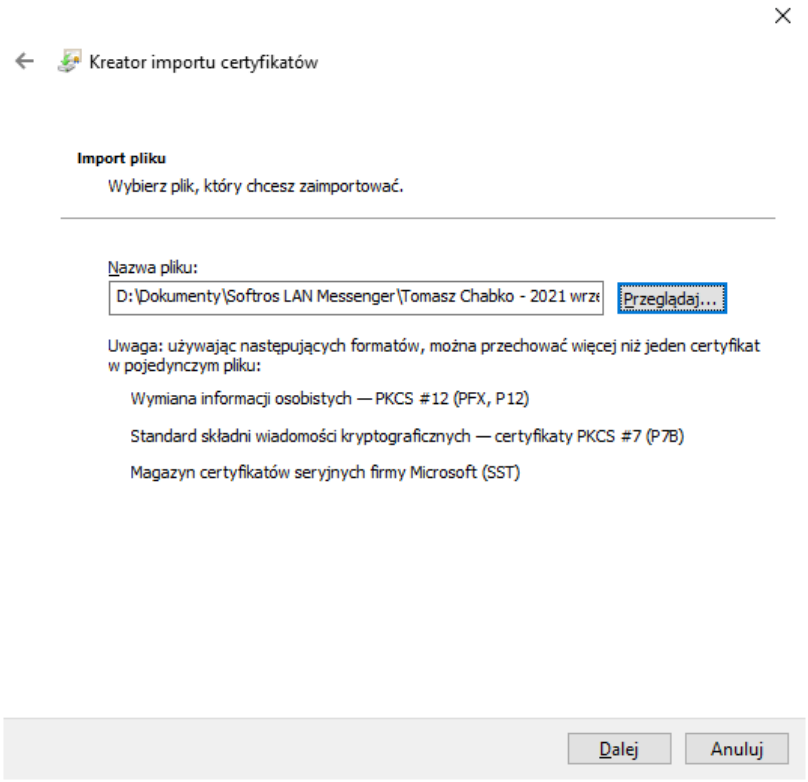
Następnie zaznaczając element Certyfikaty po lewej stronie okna, (prawy klawisz myszy) z menu kontekstowego należy wybrać „Wszystkie zadania” > „Importuj…”:



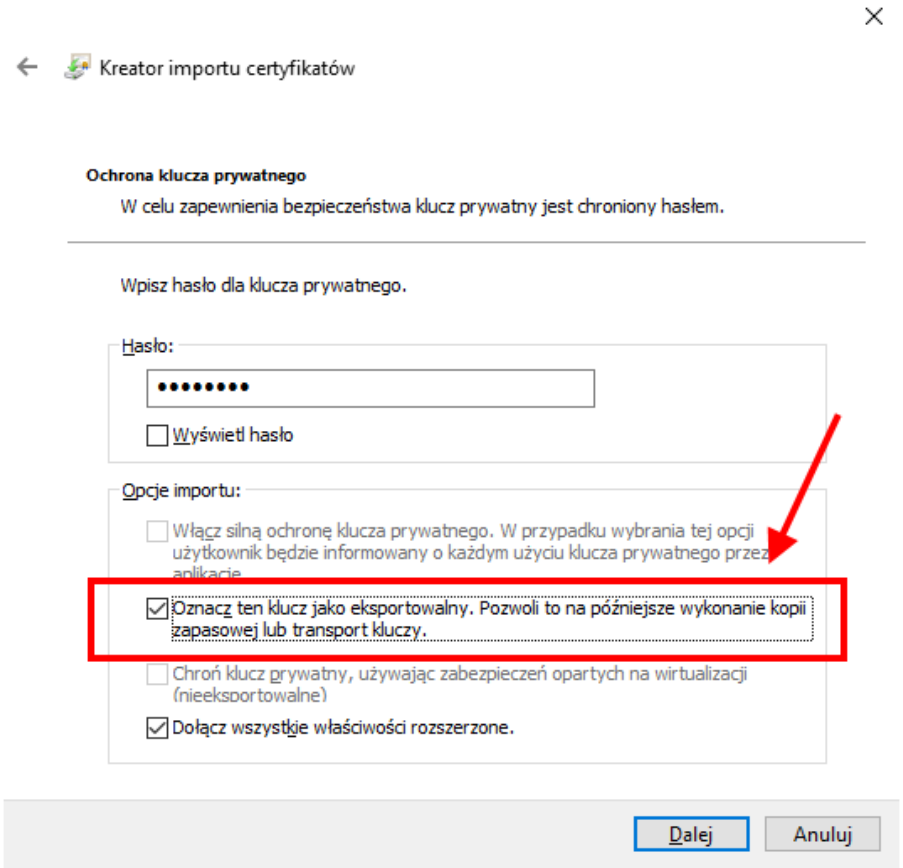
Zostanie wyświetlone okno importu certyfikatu (domyślnie powinna być zaznaczona opcja **Komputer lokalny – jeśli nie ma dostępnej tej opcji oznacza to, że użytkownik nie posiada uprawnień administratora i należy ponownie otworzyć konsolę certlm.msc jako Administrator)**



W kolejnym oknie (po wybraniu **Dalej**) należy wskazać plik z certyfikatem:

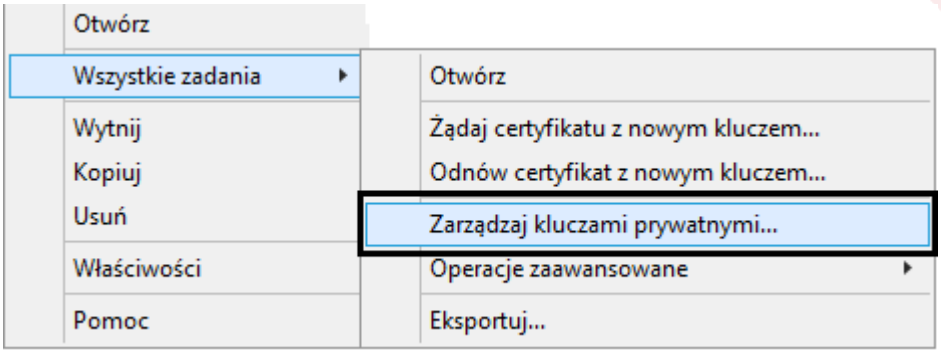


A po przejściu **Dalej** wpisać hasło do klucza certyfikatu oraz zaznaczyć opcję „**Oznacz ten klucz jako eksportowalny**”

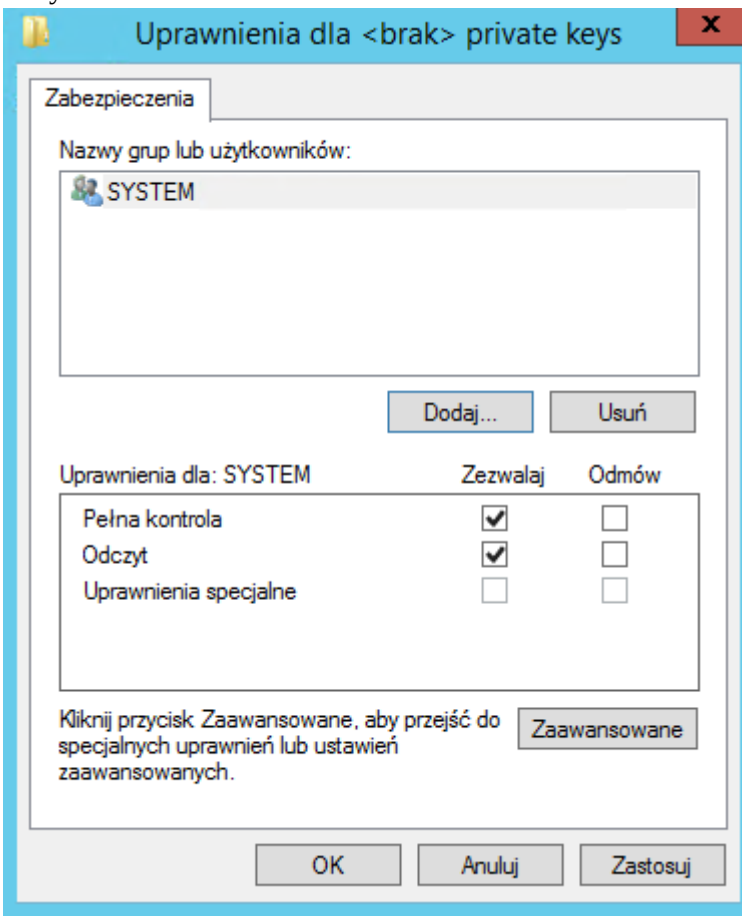


W przypadku, kiedy certyfikat importowany jest na stanowisku lokalnym nie będącym serwerem, konieczne jest nadanie uprawnień do odczytu klucza dla użytkownika, w przeciwnym wypadku po restarcie komputera użytkownik nie będzie mógł odczytać klucza do certyfikatu.

Aby nadać uprawnienia do klucza certyfikatu należy zaznaczyć zaimportowany certyfikat, następnie prawym klawiszem myszy wybrać z menu „Wszystkie zadania” > „Zarządzaj kluczami prywatnymi”



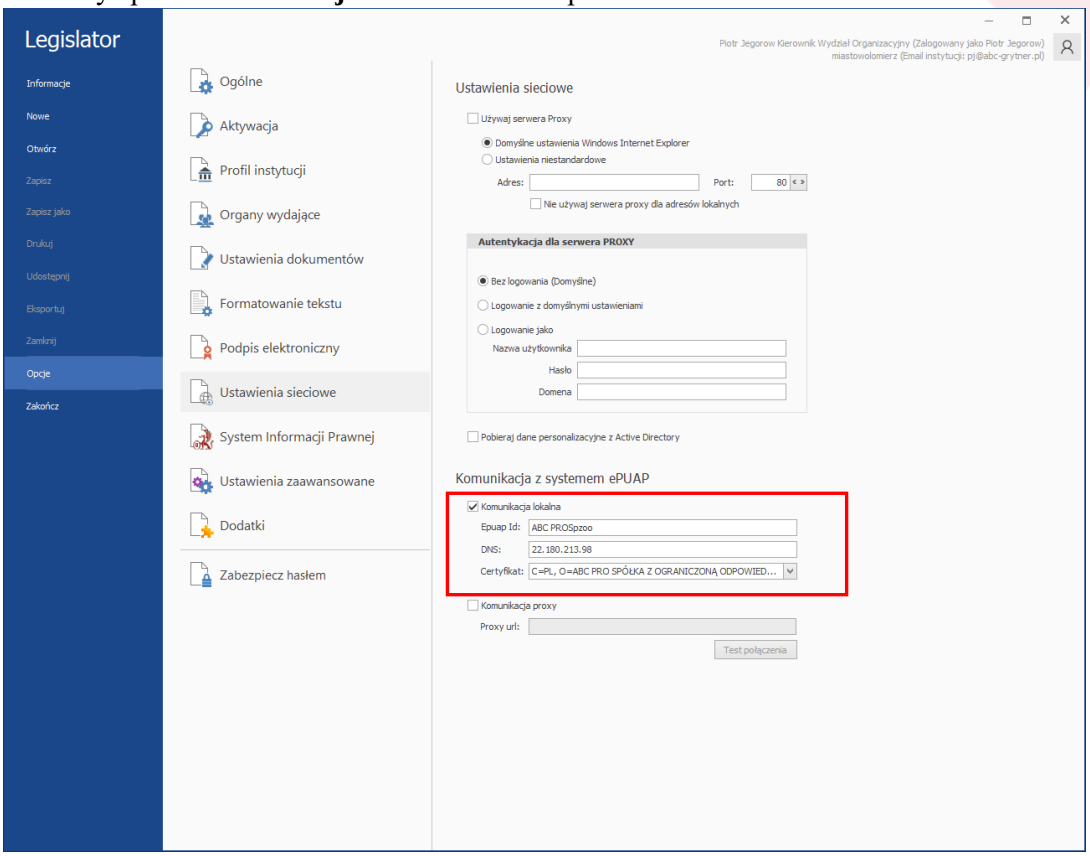
Wyświetlone zostanie okno z listą użytkowników i aktualnie przydzielonymi uprawnieniami do klucza prywatnego certyfikatu



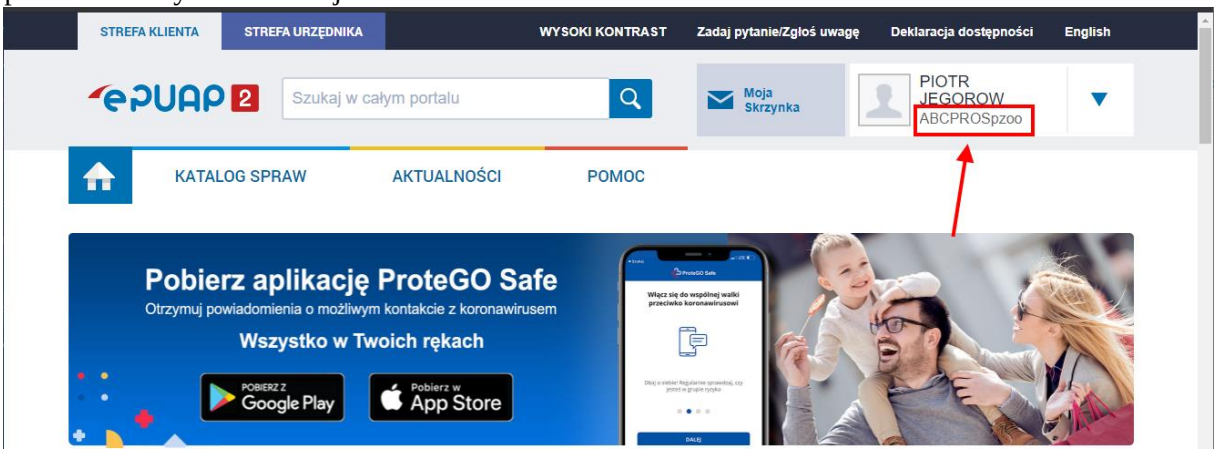
Należy dodać użytkownika, który korzysta z systemu i przydzielić mu uprawnienie „Odczyt”.
Po prawidłowej rejestracji zalecamy jest restart systemu operacyjnego.

Konfiguracja lokalna

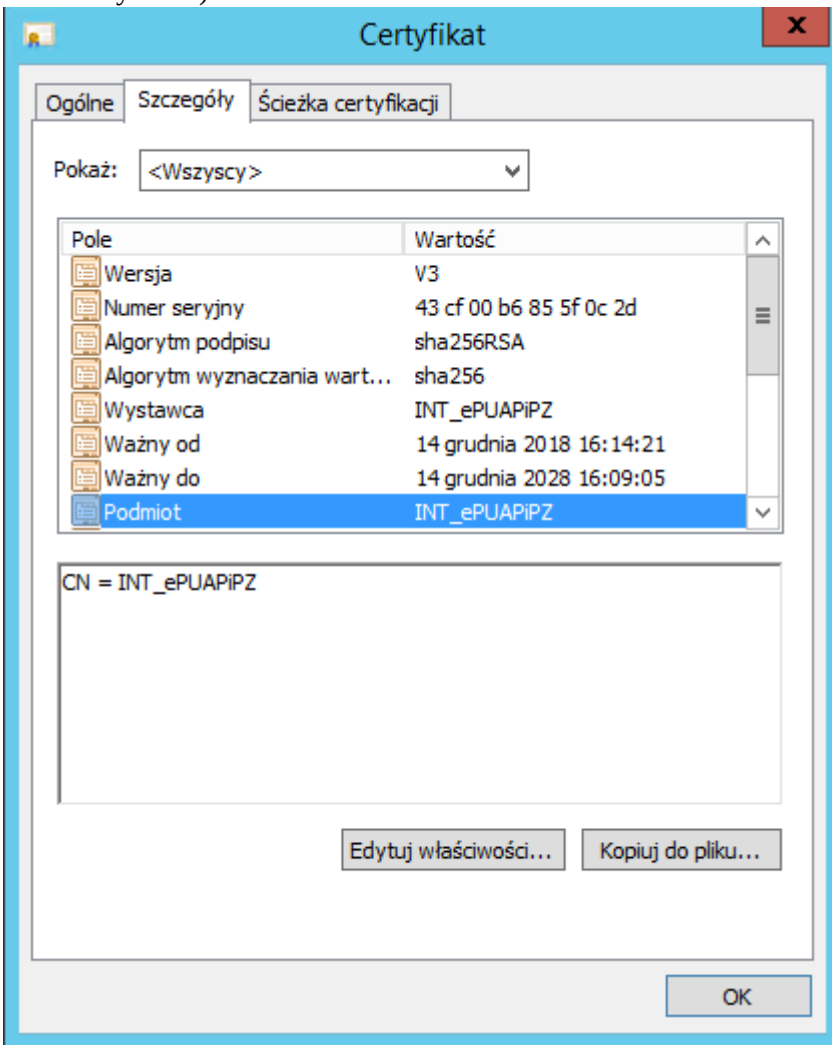
Po wykonaniu restartu, należy uruchomić EAP Legislator i przechodząc do Opcji programu - Ustawienia Sieciowe zaznaczyć pole **Komunikacja lokalna** oraz uzupełnić dane:



1) ePUAP ID – jest to ID z systemu ePUAP, które można w łatwy sposób znaleźć po zalogowaniu do ePUAP z poziomu strony internetowej:



2) DNS – informacje o wartości DNS Urząd otrzymuje wraz z certyfikatem dla systemu teleinformatycznego (Pole CN z certyfikatu)



3) Certyfikat – wskazujemy z listy wcześniej zaimportowany certyfikat.

Tak przygotowany system jest gotowy do wysyłki plików za pośrednictwem platformy ePUAP.

Komunikacja Proxy

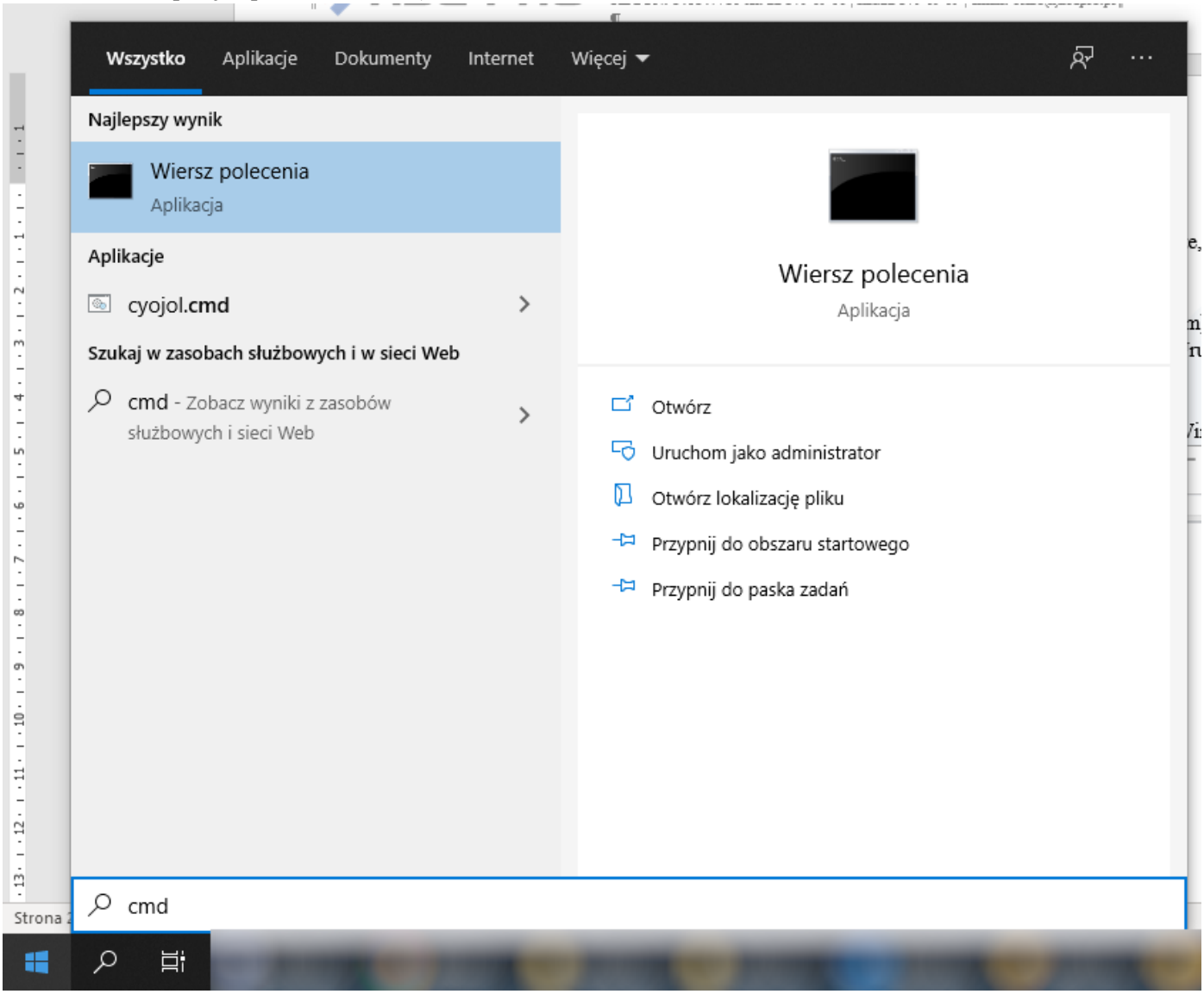
Wymagane komponenty:

- Pakiet ASP.NET Core Runtime w wersji 3.1 (link do pobrania https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-aspnetcore-3.1.18-windows-hosting-bundle-installer)
- Pakiet .NET Runtime 3.1 (https://dotnet.microsoft.com/download/dotnet/thank-you/runtime-3.1.18-windows-x64-installer)

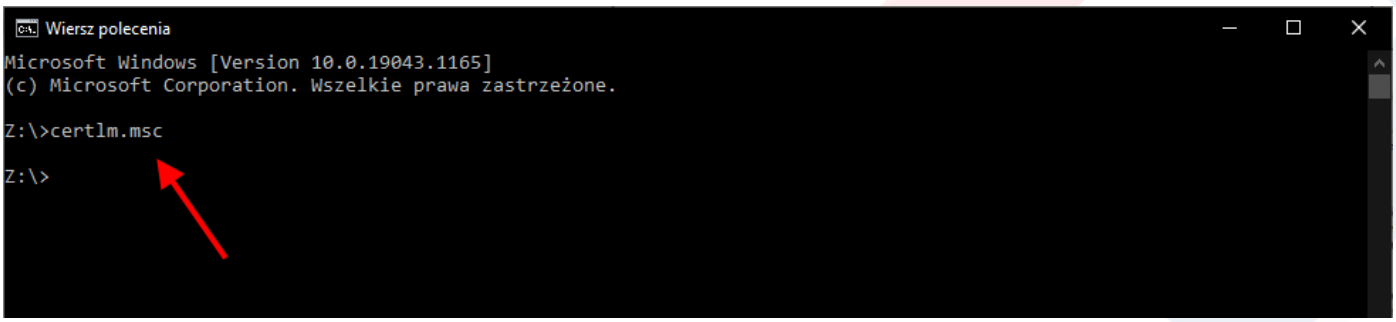
Import Certyfikatu z systemu ePUAP w systemie Windows Serwer

Rejestrowany certyfikat musi być zapisany w formacie pfx (Certyfikat razem z kluczem zabezpieczającym)

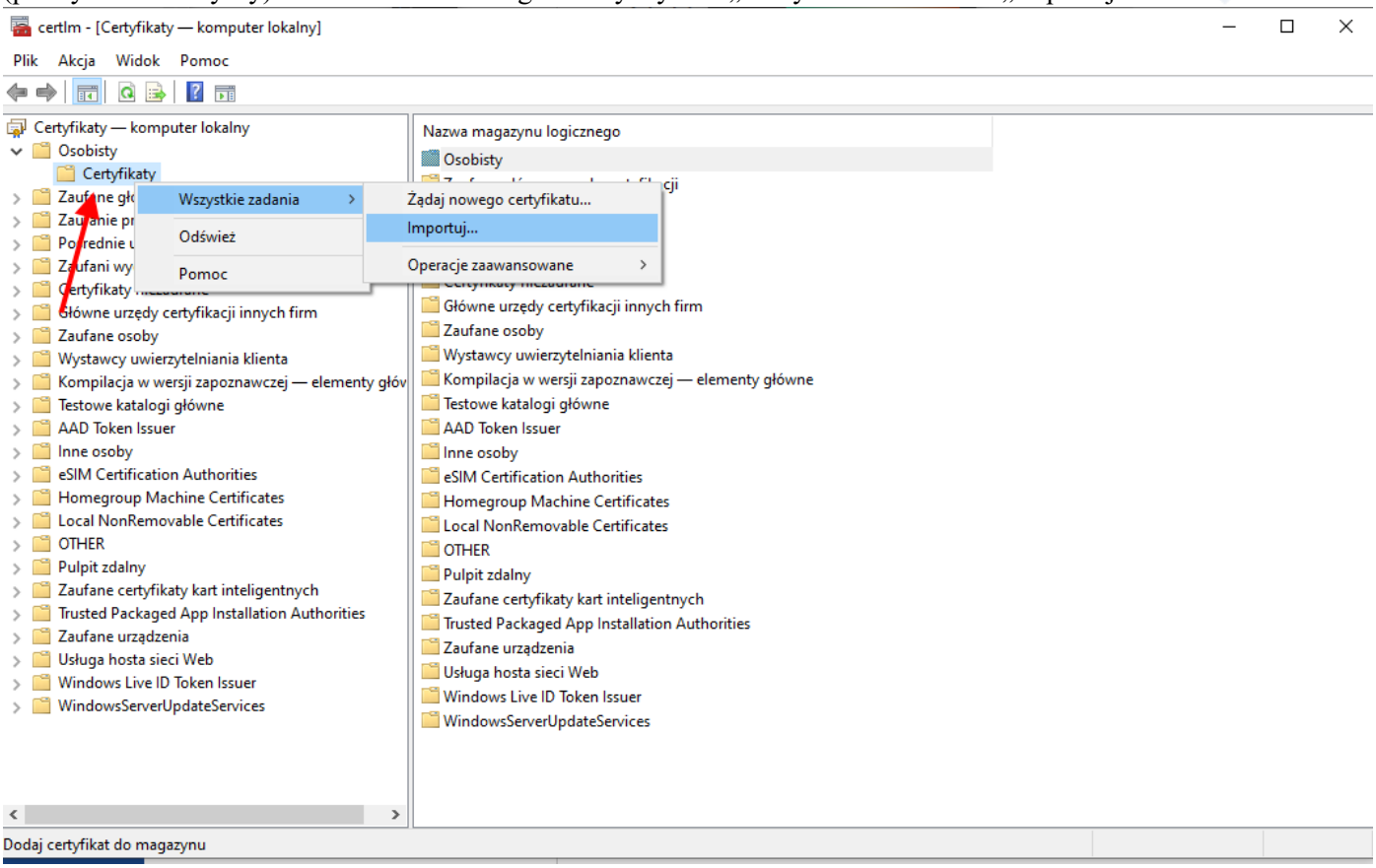
W celu importu certyfikatu do systemu Windows Serwer należy uruchomić aplikację Wiersz polecenia (wybierając menu „Start" i wpisując polecenie „cmd"):



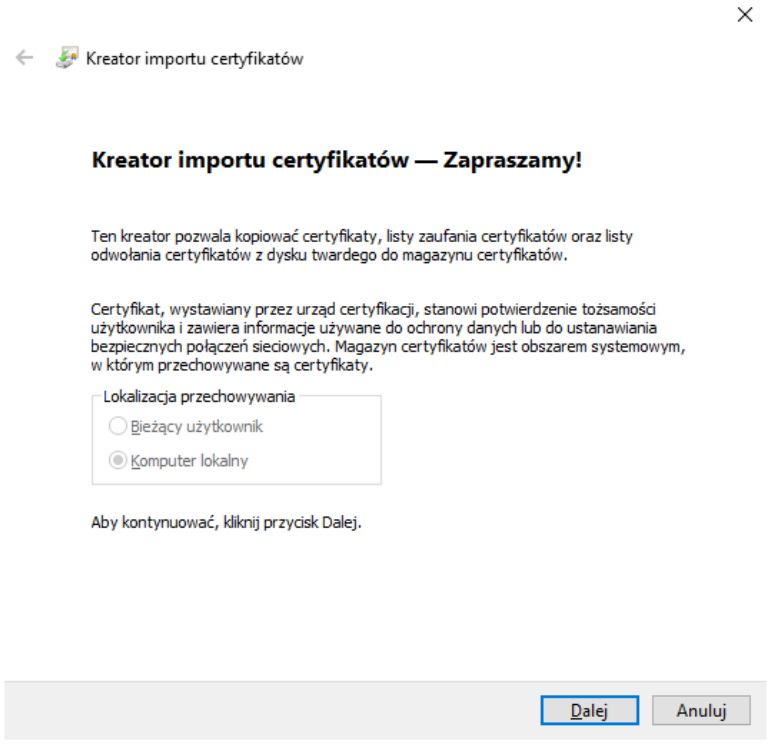
Z poziomu otwartego wiersza poleceń należy uruchomić konsolę zarządzania certyfikatami poprzez polecenie „certlm.msc":



Zostanie otwarte okno zarządzania certyfikatami. Następnie zaznaczając element Certyfikaty po lewej stronie okna, (prawy klawisz myszy) z menu kontekstowego należy wybrać „Wszystkie zadania” > „Importuj…”:

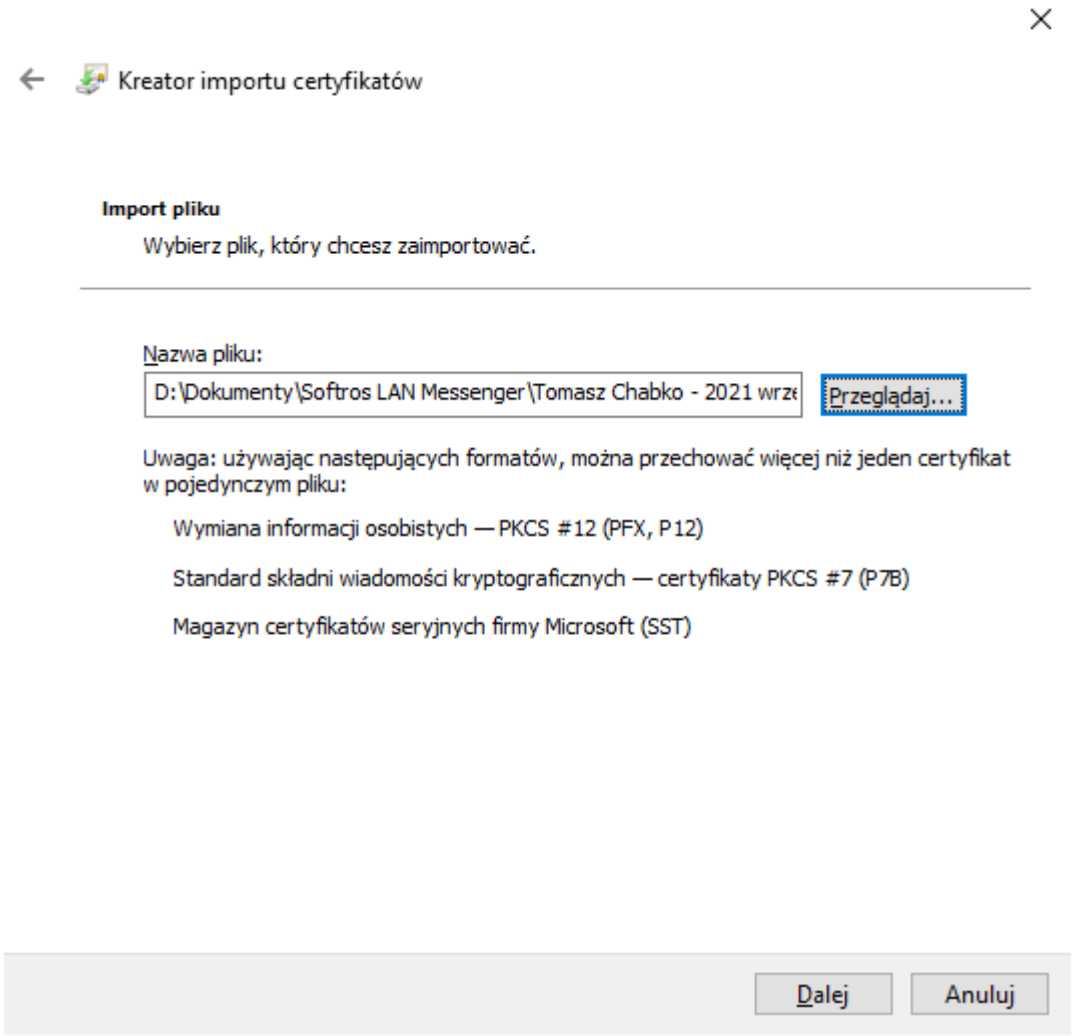


Zostanie wyświetlone okno importu certyfikatu (domyślnie powinna być zaznaczona opcja **Komputer lokalny)**

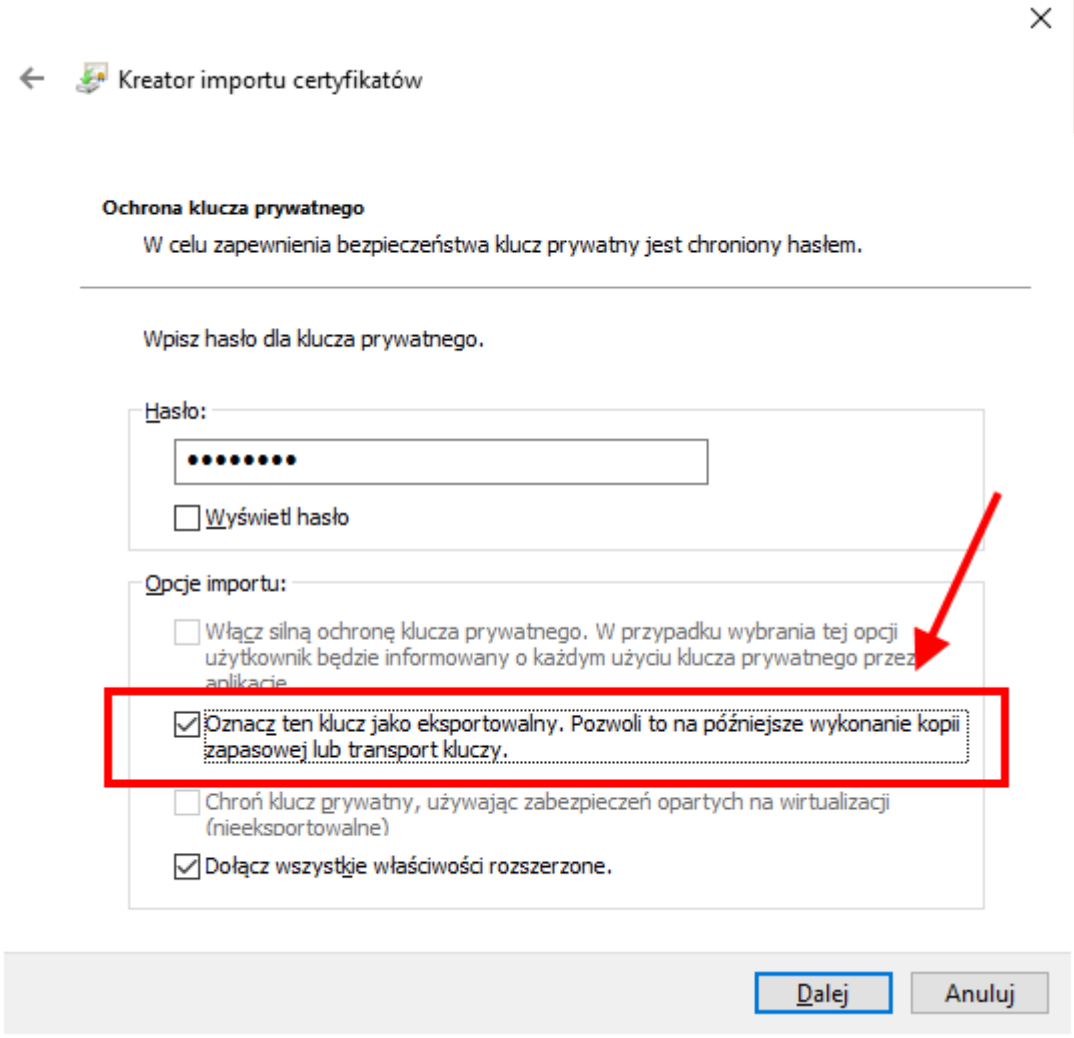


,

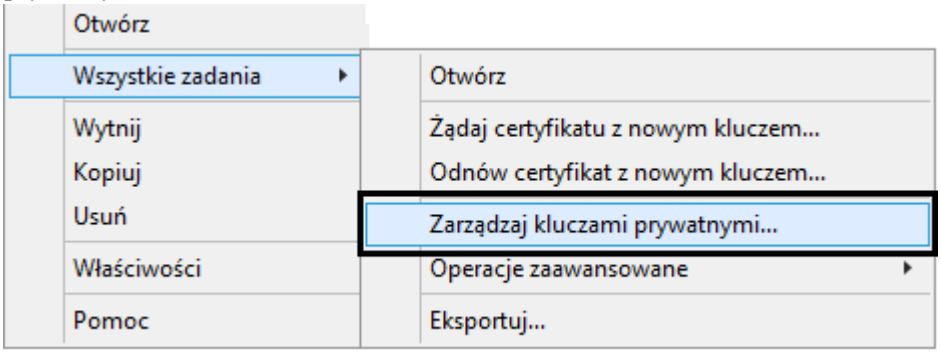
W kolejnym oknie (po wybraniu **Dalej**) należy wskazać plik z certyfikatem:



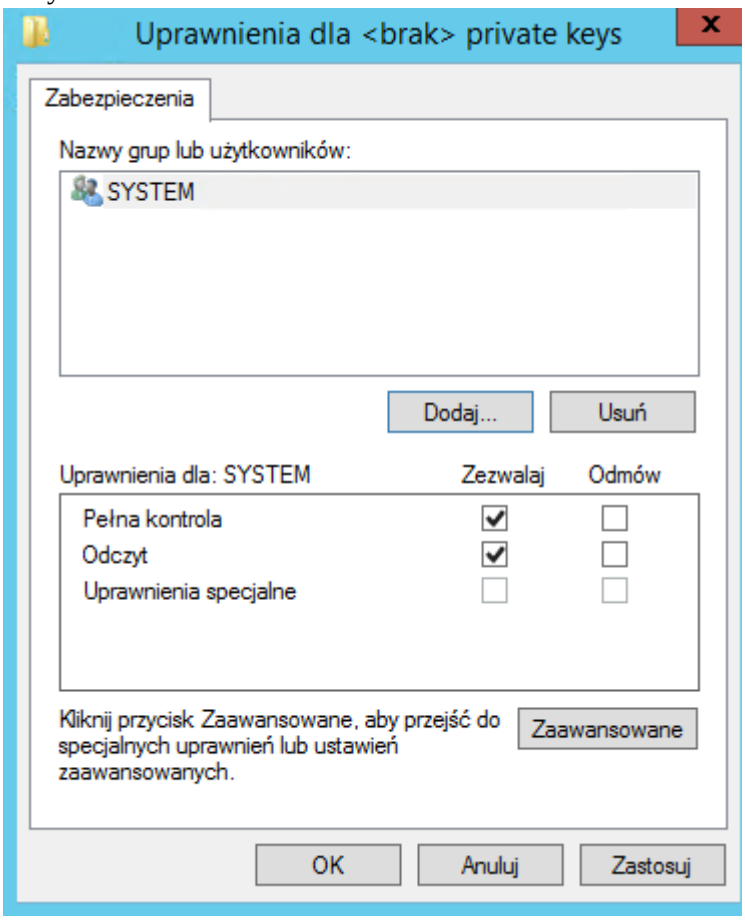
A po przejściu **Dalej należy** wprowadzić hasło do certyfikatu oraz zaznaczyć opcję „**Oznacz ten klucz jako eksportowalny**”:



Po prawidłowej rejestracji certyfikatu w konsoli zarządzania certyfikatami należy zaznaczyć zaimportowany certyfikat, następnie prawym klawiszem myszy wybrać z menu „Wszystkie zadania” > „Zarządzaj kluczami prywatnymi”



Wyświetlone zostanie okno z listą użytkowników i aktualnie przydzielonymi uprawnieniami do klucza prywatnego certyfikatu



Należy dodać użytkownika, który korzysta z systemu i przydzielić mu uprawnienie „**Odczyt**”.

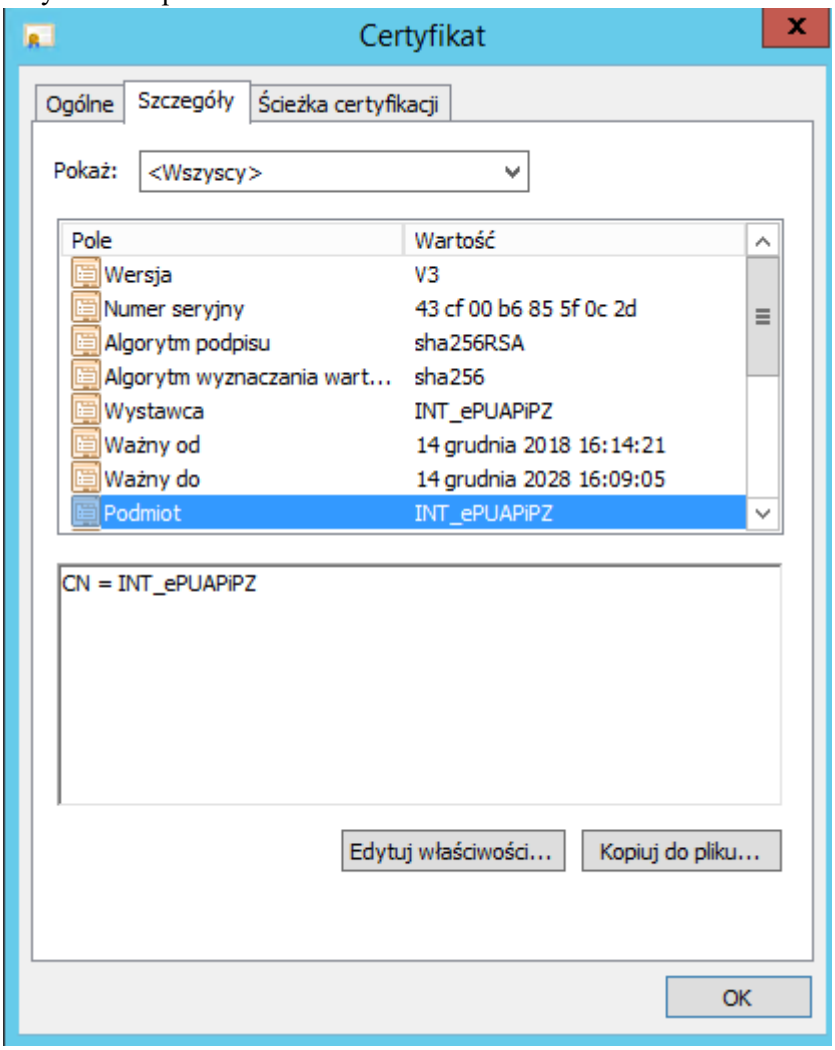
Instalacja usługi PROXY na serwerze Windows

Aby zainstalować usługę PROXY należy pobrać paczkę zawierającą pliki instalacyjne z poniższego adresu (https://files.abcpro.pl/download/legislator/paczka_proxy.zip)
Po rozpakowaniu paczki ZIP należy przejść do folderu Config i edytować plik appsettings.json

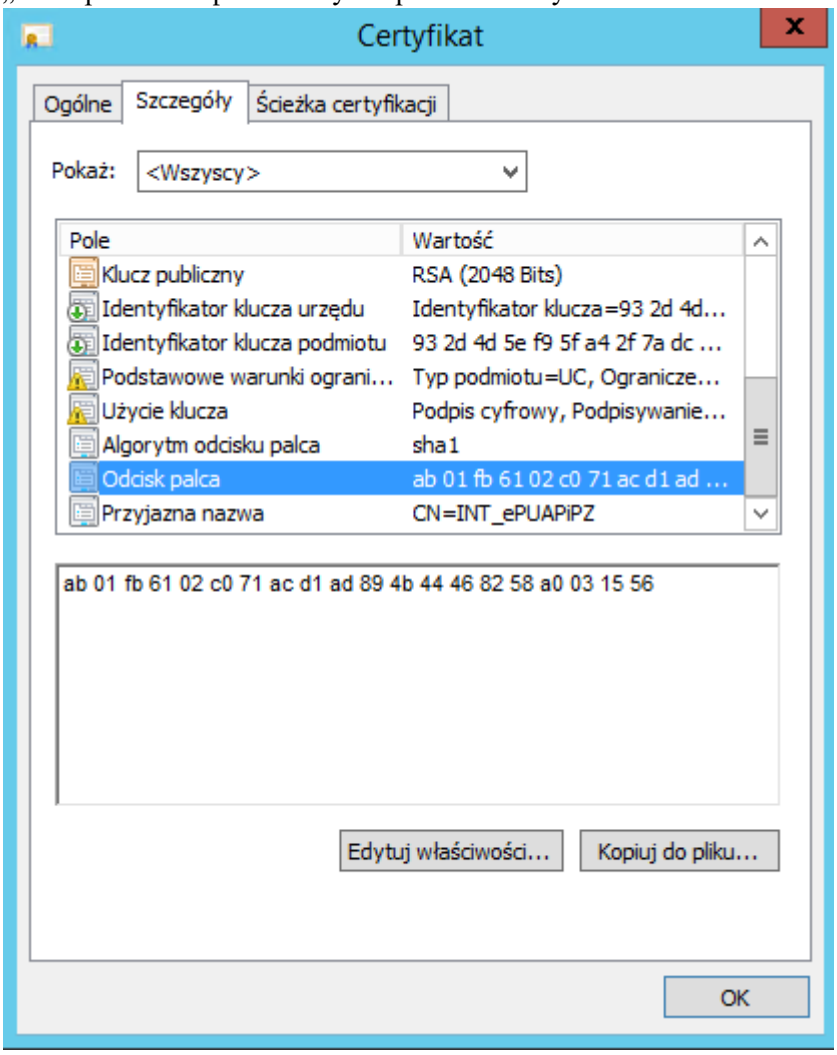
```
{
  "Urls": "http://SERVER:4000;",

  "appSettings": {
    "Epuap": {
      "Id": "identyfikator_podmiotu_systemu_epuap",
      "Dns": "pole_CN_z_certyfikatu",
      "Thumbprint": "odcisk_palca_z_certyfikatu"
    }
  }
}
```

W sekcji „Urls” należy wpisać adres serwera i port, tu określamy adres na którym dostępny będzie serwis PROXY.
W Sekcji „Epuap” podajemy następujące dane:
„Id” – to pole oznacza identyfikator podmiotu nadany w systemie ePaup
„Dns” – to pole oznaczone jest jako CN w certyfikacie wydanym dla systemu ePaup

Przykładowe pole:



„Thumprint” – to pole należy skopiować z certyfikatu



Jeżeli wszystkie dane ustawione są prawidłowo można przystąpić do instalacji usług PROXY jako usługi systemu Windows.

W tym celu na serwerze jako Administrator należy uruchomić konsole „Powershell”, następnie przejść do katalogu z paczką i wykonać polecenie:

New-Service –Name "ePuapProxy" - DisplayName "Usługa Proxy dla systemu ePuap" – StartupType Automatic – binaryPathName ePUAP_Proxy.exe

Szczegółowe informacje dotyczące dodawania usług w systemie Windows można znaleźć w dokumentacji programu powershell (https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.management/new-service?view=powershell-7.1)