



# 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.

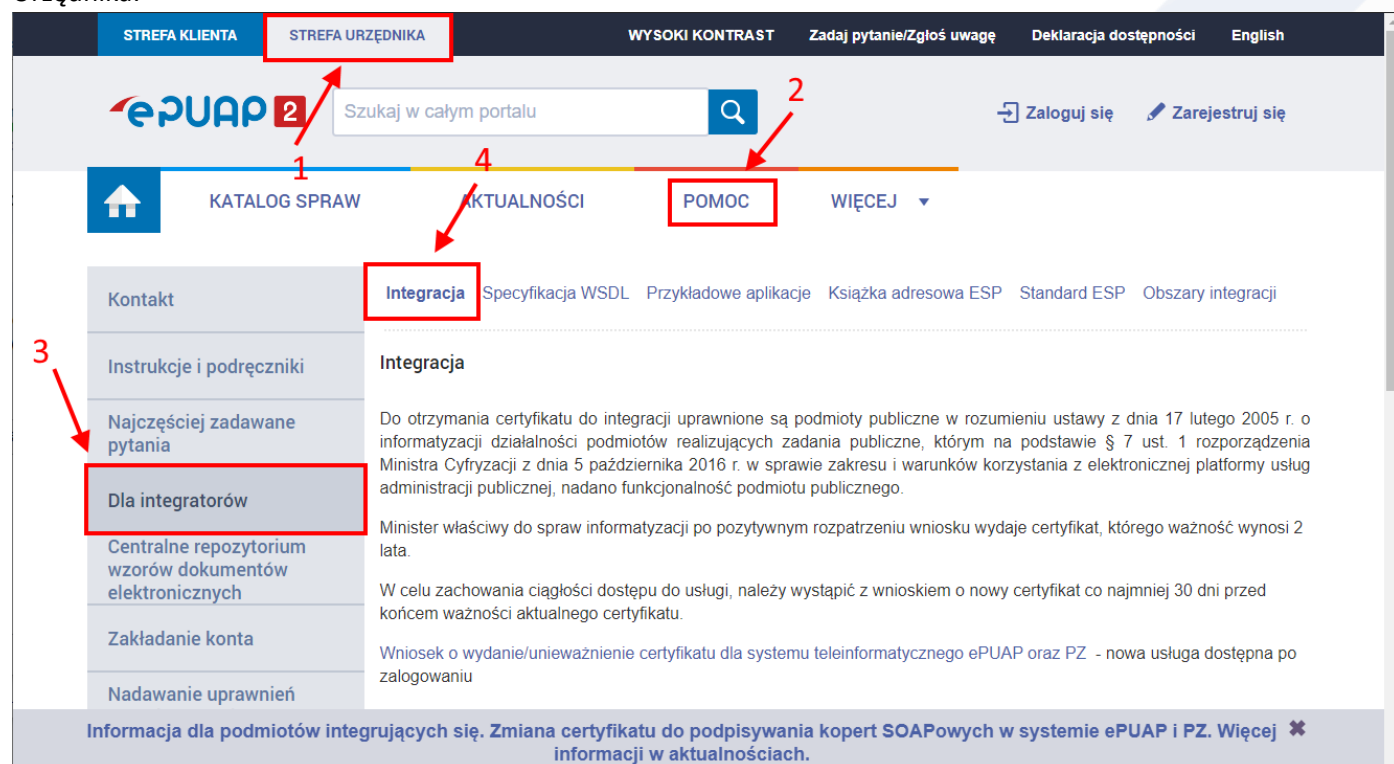
### Zawartość

Wprowadzenie .....	2
Uzyskanie i instalacja certyfikatu ePUAP dla systemu teleinformatycznego.....	3
Tworzenie keystore (tworzenie magazynu na certyfikat) .....	3
Generowanie żądania certyfikatu .....	5
Złożenie wniosku o wydanie certyfikatu do integracji systemu zewnętrznego z platformą ePUAP.....	7
Konfiguracja platformy ePUAP .....	11
Przygotowanie certyfikatu dla systemu Legislator .....	12
Import certyfikatu do systemu Windows i konfiguracja aplikacji Legislator .....	13
Konfiguracja lokalna.....	17
Komunikacja Proxy .....	19
Wymagane komponenty: .....	19
Import Certyfikatu z systemu ePUAP w systemie Windows Serwer .....	19
Instalacja usługi PROXY na serwerze Windows.....	23

## Wprowadzenie

W celu umożliwienia wysyłki aktów do nadzoru prawnego Wojewody Śląskiego 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 zarówno sam certyfikat z Ministerstwa Cyfryzacji, jak również w jaki sposób użyć go później do integracji EAP Legislators z kontem ePUAP urzędu, celem umożliwienia wysłania aktów do nadzoru prawnego bezpośrednio z aplikacji EAP Legislators.

# Uzyskanie i instalacja certyfikatu ePUAP dla systemu teleinformatycznego

## 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.

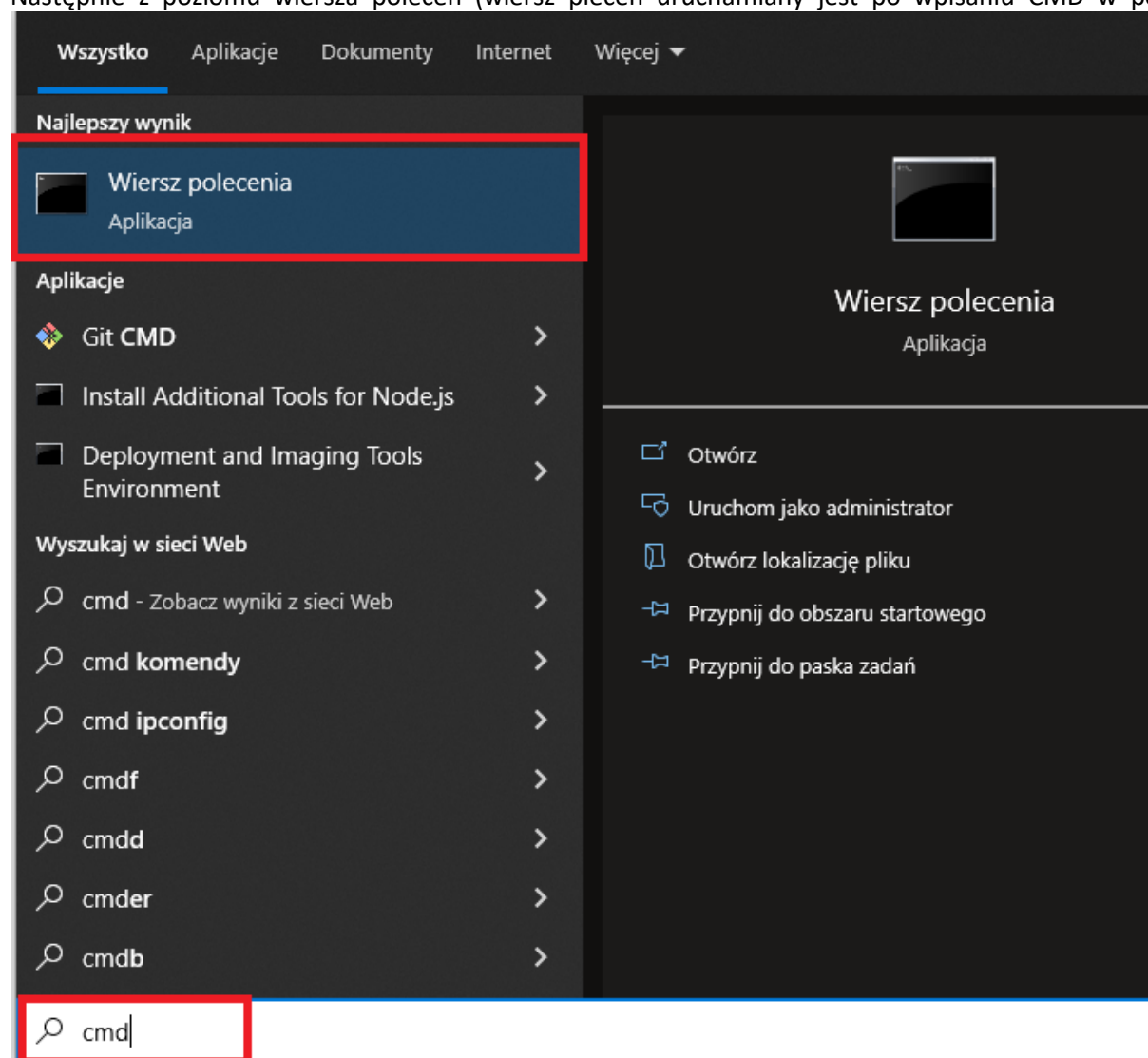
Aby utworzyć wniosek o wydanie certyfikatu można posłużyć się aplikacją keytool.exe. Aplikacja ta dostępna jest po instalacji środowiska Java JRE. Najnowsze środowisko JRE można pobrać ze strony producenta (na potrzeby instrukcji dostępna jest wersja JAVA JRE 8u311)

[https://javadl.oracle.com/webapps/download/AutoDL?BundleId=245479\\_4d5417147a92418ea8b615e228bb6935](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 poleceń uruchamiany jest po wpisaniu CMD w polu „Uruchom”)



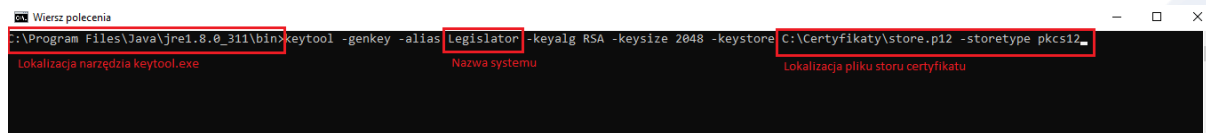
należy przejść do katalogu w którym znajduje się narzędzie keytool.exe i wykonać następujące polecenie:

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

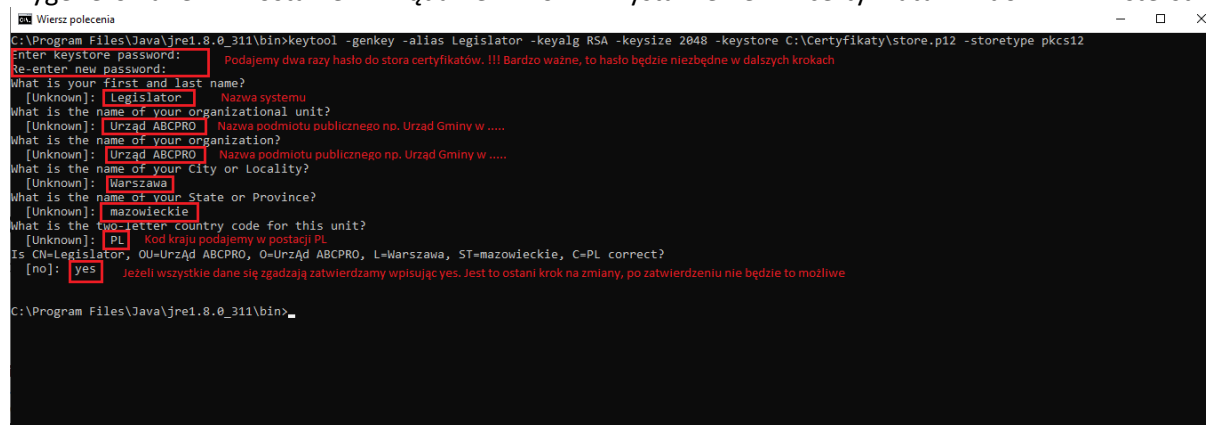
### PRZYKŁAD WYKONANIA POLECENIA

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

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

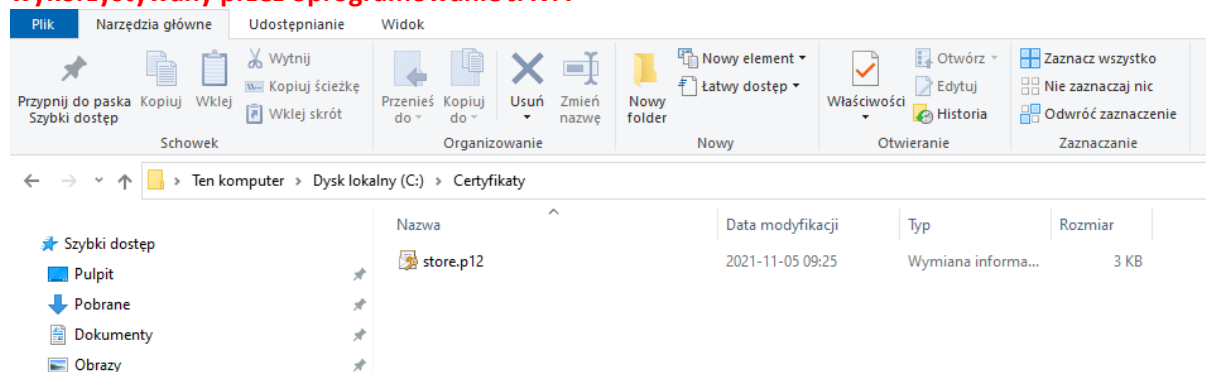


Po wykonaniu polecenia system wyświetli monit o uzupełnienie danych do magazynu na podstawie, którego wygenerowane zostanie żądanie o wystawienie certyfikatu do Ministerstwa Cyfryzacji.



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

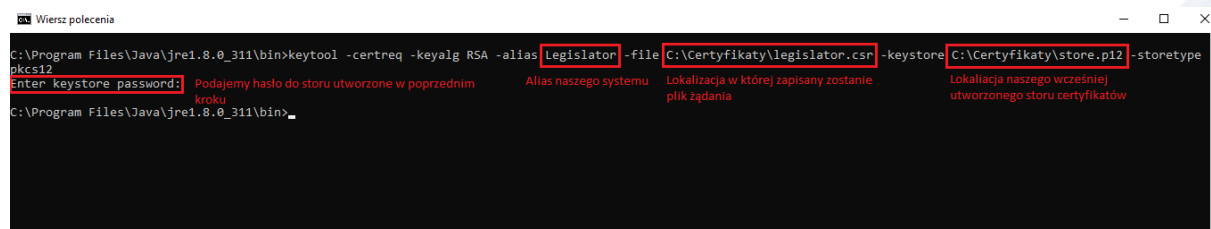
**UWAGA. Wygenerowany plik to nie jest jeszcze docelowy certyfikat, a jedynie magazyn na certyfikaty wykorzystywany przez oprogramowanie JAVA**



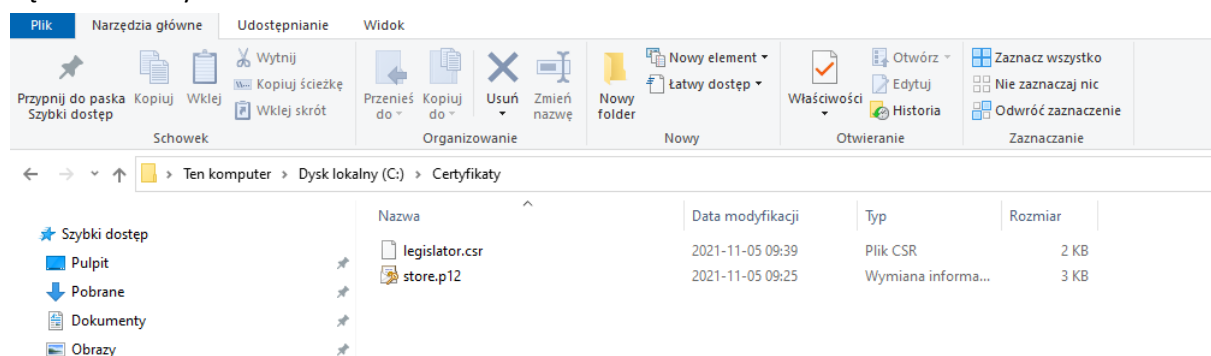
## Generowanie żądania certyfikatu

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:

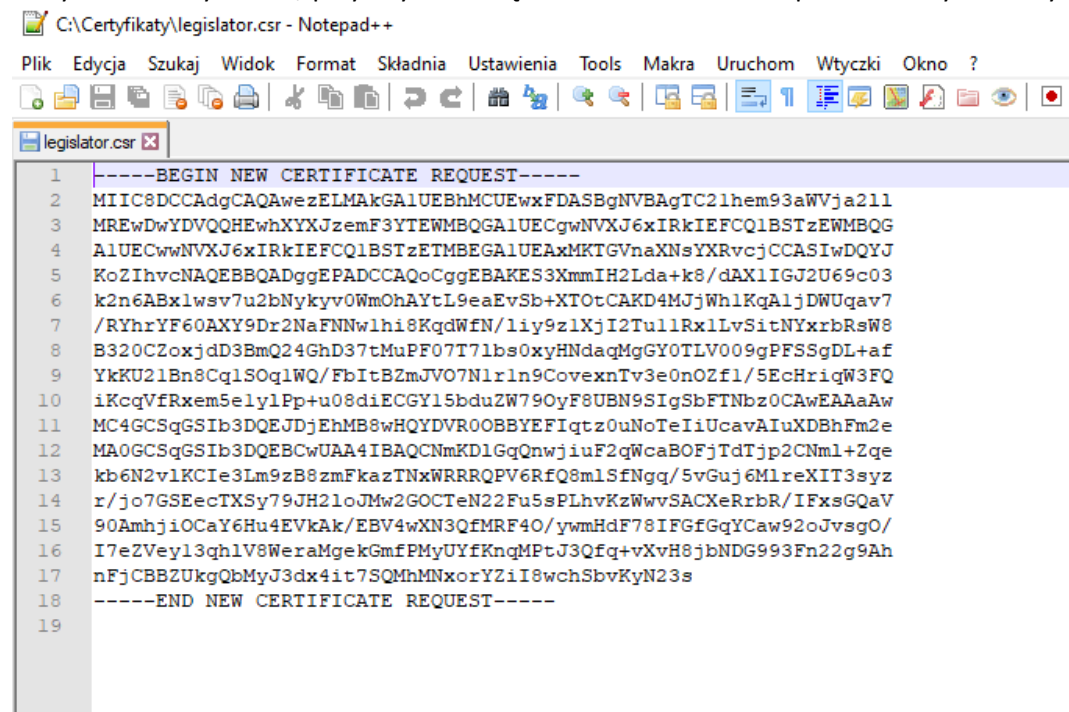
```
#keytool -certreq -keyalg RSA -alias Legislator -file C:\Certyfikaty\legislator.csr -keystore C:\Certyfikaty\store.p12 -storetype pkcs12
```



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



Zawartość tego pliku należy przestać 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.

C:\Certyfikaty\legislator.csr - Notepad++

Plik Edycja Szukaj Widok Format Składnia Ustawienia Tools Makra Uruchom Wtyczki Okno

legislator.csr

```

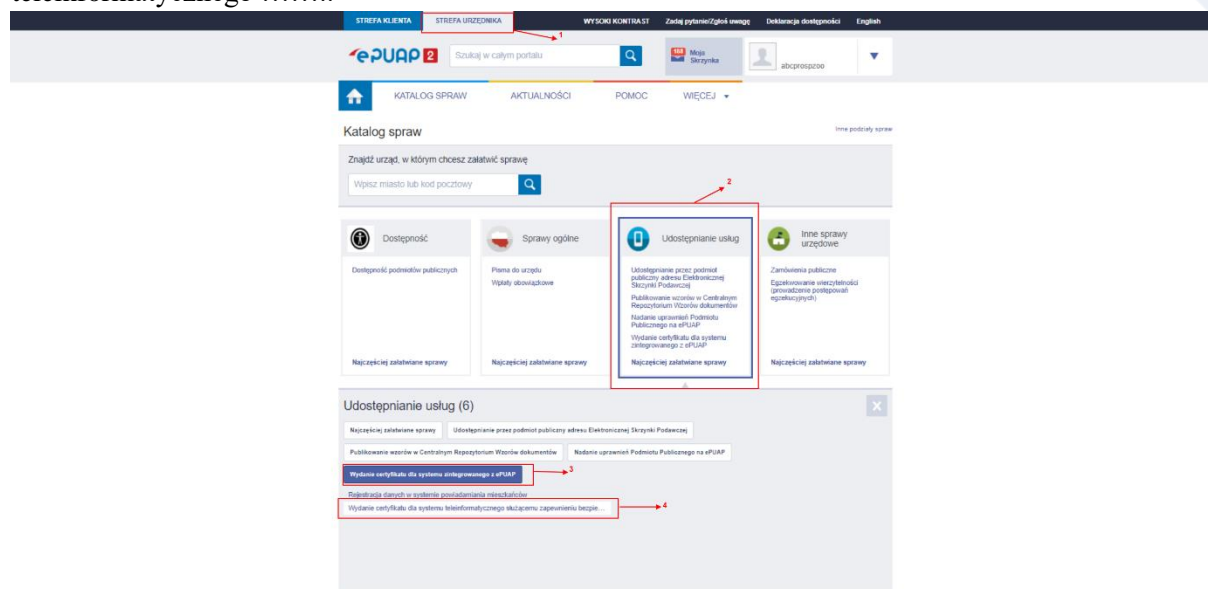
1 -----BEGIN NEW CERTIFICATE REQUEST-----
2 MIIC8DCCAdgCAQAwezELMAkGA1UEBhMCUEwxFDASBgNVBAgTC2lhem93aWVja211
3 MREwDwYDVQQHEwhXYXJzemF3YTEWMBQGA1UECgwNVXJ6xIRkIEFCQ1BSTzEWMBQG
4 A1UECwwNVXJ6xIRkIEFCQ1BSTzETMBEGA1UEAxEAMKTGVnaXNsYXRvcjCCASIwDQYJ
5 KoZIHvcNAQEBBQADggEPADCCAQoCggEBAKES3XmmIH2Lda+k8/dAX1IGJ2U69c03
6 k2n6ABx1wsv7u2bNykyv0WmOhAYtL9eaEvSb+XTOtCAKD4MJjWhlKqAljDWUqav7
7 /RYhrYF60AXY9Dr2NaFNNwlhi8KqdWfN/liy9z1XjI2TullRx1LvSitNYxrbRsW8
8 B320CZoxjdD3BmQ24GhD37tMuPF07T71bs0xyHNdaqMgGY0TLV009gPFSSgDL+af
9 YkKU21Bn8Cq1SOq1WQ/FbItBZmJVO7N1rln9CovexnTv3e0nOZf1/5EcHriqW3FQ
10 iKcqVfRxem5elylPp+u08diECGY15bduZW79OyF8UBN9SIgSbFTNbZ0CAwEAAaAw
11 MC4GCSqGSIb3DQEJJDjEhMB8wHQYDVROBBYEFIqtz0uNoTeIiUcavAIuXDBhFm2e
12 MA0GCSqGSIb3DQEBCwUAA4IBAQCnmKD1GqQnwjiuF2qWcaBOFjTdTjp2CNml+Zqe
13 kb6N2v1KCIE3Lm9zB8zmFkazTNxWRRRQPv6RfQ8m1SfNgq/5vGuJ6M1reXIT3syz
14 r/jo7GSEecTXSy79JH21oJMw2GOCTeN22Fu5sPLhvKzWwvSACXeRrbR/IFxsGQaV
15 90AmhjiOCaY6Hu4EVkAk/EBV4wXN3QfMRF40/ywmHdF78IFGfGqYCaw92oJvsgO/
16 I7e2Veyl3qhlV8WeraMgekGmfPMYUYfKnqMPtJ3Qfq+vXvH8jbNDG993Fn22g9Ah
17 nFjCBBZUkgQbMyJ3dx4it7SQMhMNxorYZiI8wchSbvKyN23s
18 -----END NEW CERTIFICATE REQUEST-----
19

```

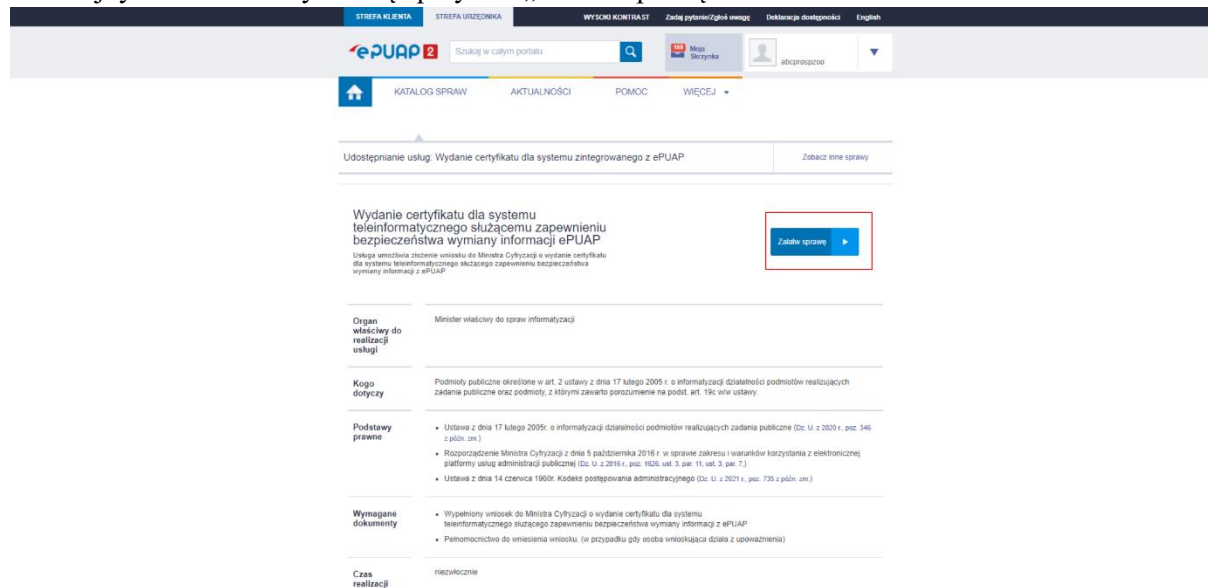


## Złożenie wniosku o wydanie certyfikatu do integracji systemu zewnętrznego z platformą ePUAP.

Aby złożyć wniosek o wydanie certyfikatu do integracji aplikacji zewnętrznej z platformą ePUAP należy zalogować się na konto z uprawnieniami administratora do systemu ePUAP, następnie wejść w zakładkę „Strefa Urzędnika” w katalogu spraw wybrać panel „Udostępnianie usług” i z listy dostępnych spraw wybrać „Wydanie certyfikatu dla systemu zintegrowanego z ePUAP” a następnie wskazać formularz wniosku „Wydanie certyfikatu dla systemu teleinformatycznego .....”



W kolejnym kroku należy kliknąć przycisk „Załatw sprawę”



Zostanie załadowany formularz wniosku, który w znacznej części jest już wypełniony danymi z profilu.

KATALOG SPRAW AKTUALNOŚCI POMOC WIĘCEJ ▾

Załatw sprawę Wybrana skrzynka: Domyślna 92 ▾

Odebrane 92 Wysłane Robocze Moje pliki Operacje

Wróć do Roboczych Kopiuj do roboczych Zapisz Usuń Pobierz Drukuj

Zaawansowane

**Twoja skrzynka nie została jeszcze aktywowana - wysyłanie wiadomości nie jest możliwe. Wniosek o nadanie uprawnień Podmiotu Publicznego został złożony. Trwa weryfikacja wniosku, po jej ukończeniu Twoje skrzynka zostanie aktywowana.**

**Edycja:**  
Wydanie certyfikatu dla systemu teleinformatycznego służącemu zapewnieniu bezpieczeństwa wymiany informacji ePUAP - Wniosek o Certyfikat ePUAPxml

Od: "ABC PRO" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ (abcprospzoo)  
Do: KPRM Cyfryzacja (/MA/C/certysys)  
Dokument nie posiada podpisów elektronicznych

**I DANE WNIOSKODAWCY:**

**Podmiot publiczny<sup>1</sup>**

Nazwa: "ABC PRO" SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ Identyfikator podmiotu publicznego<sup>2</sup>: abcprospzoo

Siedziba (adres podmiotu publicznego):

Województwo: Mazowieckie Powiat: Warszawa Gmina: Praga-Północ (dzielnica)

W pierwszej części należy podać stosowne dane (zgodnie z wymaganymi polami). Najistotniejszą częścią formularza jest sekcja wypełnienia danych dotyczących certyfikatu.

**III. DANE SYSTEMU TELEINFORMATYCZNEGO:**

Nazwa systemu teleinformatycznego:

Adres domeny lub stały numer IP systemu, który będzie uzyskiwał dostęp do ePUAP<sup>12</sup>:

Alternatywne nazwy domen lub stałe numery IP systemu, który będzie uzyskiwał dostęp do ePUAP<sup>13</sup>:

Oświadczenie:

Oświadczam, że certyfikat zostanie wykorzystany zgodnie z jego przeznaczeniem, określonym w § 11 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2016 r., poz. 1626).

CSR do wystawienia certyfikatu (Instrukcja generowania żądania certyfikatu znajduje się w POMOCY na ePUAP):

[1] W rozumieniu art. 2 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2017 poz. 570)  
[2] Identyfikator podmiotu publicznego w rozumieniu § 2 pkt 2 rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2016 r., poz. 1626)

W polu „Nazwa systemu teleinformatycznego” należy wpisać „Legislator”, w polu „Adres domeny lub stały numer IP” należy wpisać adres IP, którym urząd identyfikuje się w sieci publicznej. Adres taki możemy uzyskać sprawdzając to na stronie identyfikującej nasz publiczny adres IP.

<https://whatismyipaddress.com> (dla przykładu)

My IP Address is:

IPv4: ? **212.180.213.98**

IPv6: ? **Not detected**

What is a VPN  
Why Use a VPN  
Choosing a VPN  
VPN Comparison  
Free VPNs  
VPN Reviews

Następnie do pola „CSR do wystawienia certyfikatu” należy wkleić wcześniej przygotowane żądanie (zawartość pliku .csr łącznie z sekcjami --BEGIN NEW CERTIFICATE REQUEST-- oraz --END CERTIFICATE REQUEST--)



# **TIT. DANE SYSTEMU TELEINFORMATYCZNEGO:**

Nazwa systemu teleinformatycznego:  
Legislator

Aдрес domeny lub stały numer IP systemu, który będzie używany do ePUAP<sup>[1]</sup>:  
212.180.213.98

Alternatywne nazwy domen lub stałe numery IP systemu, który będzie używany do ePUAP<sup>[1]</sup>:

Oświadczanie:  
  
Oświadczam, że certyfikat zostanie wykorzystany zgodnie z jego przeznaczeniem, określonym w § 11 ust. 1 rozporządzenia Ministra Cyfrizacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2016 r., poz. 1626).

CSR do wystawienia certyfikatu (Instrukcja generowania żądania certyfikatu znajduje się w POMOCY na ePUAP):

-----BEGIN NEW CERTIFICATE REQUEST-----  
MIIC+CCAMCAAGAwTUCgAIBgKVBATBMMQoEYGVOVDIwHTXGJWZ7Bg  
ZERNMAGAUEBMVAFZFrcjphZeCvSzqZWNBABTCFYOcBOUGRlJA/AufgrtYSIP  
UEMBKGA1UECMsURFRSTJEFBSFYETUCqAZHkLMRMMEQGVODQGEVM5dWpzczh  
JCyOMIMBgkqhkiG9w0BAQAAQCIAADAMBCCQAQCEAEACAsIUAhMRCjcyQRBR  
IE4ELeUsKVIVXAAYTsYbfwVwJl3kgpbGaMYpkpzZBEOTVBCZEBOTVCZEBOTVBC  
ZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTV  
CZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTVCZEBOTV  
HRnTZLuzwJP0SLpcCBcwOVNHA4BDY3wtlf9T1uOB7PgeBD0T1TTrJJRpRRUMQG  
SeInMbteBIXHEBMT1TGdBrCNLTFEHgbylyVCGIGzpObxayruiGI  
ONPTLEtwlvHCUBKCDwrg9sbdb=MKUwTFZScAfzEDSbcAkaghtOpf  
YrfPIFDAGARsdAwg,qIKzNhNAQKmEQm=aHzAKZhwHMHQGTGQofMDXKOZKHPRP  
Tangp1TNaahavOWDoMZtc7BNAGEILBDAQpZGBALLCuyctAbbaApvgSGTXNYDU  
DJFDSFGFXRFBLVAHXpgppghHSasdaHwz=MB8chryUKyeSSIMDE1eqd  
ZCpYdC9nLS3CspAvdrLYUymybafwBVU7SA7mfswfshHMOCTCLedSh  
xmULUF38gbVFVfYUJCYCsBdcBoEXAcse192wOT24hVMWOOVdyWqeJIdc  
CPpblndflnrKVRZ72rFCsoZhnmMLBakSLszap7HHMeSCJduDRAdLUbvU  
eZWNVKZEd0IHme7yyrnSrStscvSEZELRLnMAbsCsmze7TA7NbKnpztHziB=  
-----END NEW CERTIFICATE REQUEST-----

[1] W rozumieniu art. 2 ust. 1 ustawy z dnia 17 lutego 2003 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2017, pos. 870)

[2] Identyfikator podmiotu publikującego w rozumieniu § 2 pkt 2 rozporządzenia Ministra Cyfrizacji z dnia 5 października 2016 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (Dz. U. z 2016 r., poz. 1626)

[3] Dane osobiste uprawnionej do przeprowadzenia postępowania rekrutacyjnego i konkursowego Wyższego.

Po przejściu do kolejnego kroku widoczne jest podsumowanie wniosku. Należy je podpisać podpisem kwalifikowanym lub profilem zaufanym i wysłać.

[illegible]

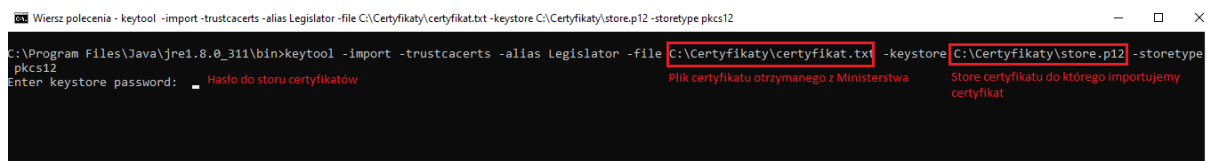
Czas odpowiedzi na uzyskanie certyfikatu to ok 14 dni. Po tym czasie na adres email wypełniony we wniosku otrzymamy maila zawierającego wydany certyfikat. Należy postępować zgodnie z krokami niniejszej instrukcji aby zaimportować certyfikat do wcześniej utworzonego magazynu certyfikatów.

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.



```
Wiersz polecenia - keytool -import -trustcacerts -alias Legislator -file C:\Certyfikaty\certyfikat.txt -keystore C:\Certyfikaty\store.p12 -storetype pkcs12
C:\Program Files\Java\jre1.8.0_311\bin>keytool -import -trustcacerts -alias Legislator -file C:\Certyfikaty\certyfikat.txt -keystore C:\Certyfikaty\store.p12 -storetype
pkcs12
Enter keystore password: Hasło do storu certyfikatów
```

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

- 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”


 rozbudowa elektronicznej platformy usług administracji publicznej
 
[NOTA PRAWNA](#)
[REGULAMIN](#)
[DEKLARACJA DOSTĘPNOŚCI](#)
[MAPA STRONY](#)

Portal nadzorowany przez [Ministra Cyfryzacji](#)

**!!! 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-----”.

[illegible]

## 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
```

Wiersz polecenia

```
c:\Certyfikaty>openssl.exe pkcs12 -nocerts -out c:\Certyfikaty\klucz.key -in c:\Certyfikaty\store.p12
Enter Import Password: Podajemy aktualne hasło do
Enter PEM pass phrase: store ustawione wcześniej,
Verifying - Enter PEM pass phrase: nadajemy hasło do
                             pliku klucza (jest to konieczne)
```

Lokalizacja gdzie zostanie zapisany plik z kluczem prywatnym

Plik store zawierający klucz prywatny, to z niego wyodrębniamy klucz prywatny

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.

Wiersz polecenia

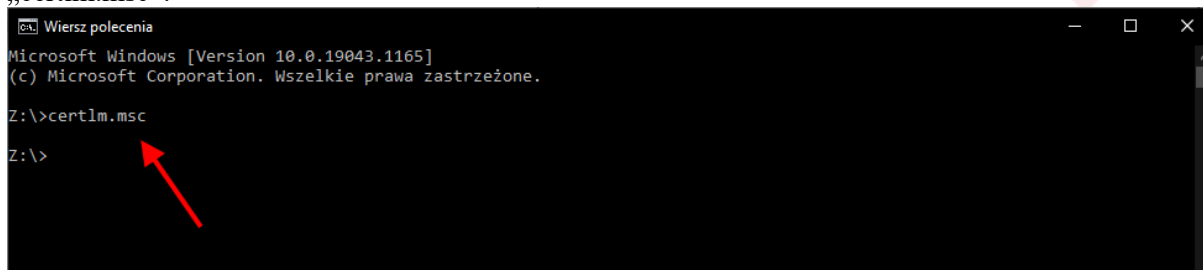
```
c:\Certyfikaty>openssl.exe pkcs12 -export -out c:\Certyfikaty\certyfikat.pfx -inkey c:\Certyfikaty\klucz.key -in c:\Certyfikaty\certyfikat.txt
Enter pass phrase for c:\Certyfikaty\klucz.key: Lokalizacja zapisania pliku wyjściowego pfx
Enter Export Password: Wcześniej wyeksportowany klucz
Verifying - Enter Export Password: Lokalizacja pliku certyfikatu otrzymanego z Ministerstwa Cyfryzacji
```

Podajemy aktualne hasło do klucza prywatnego

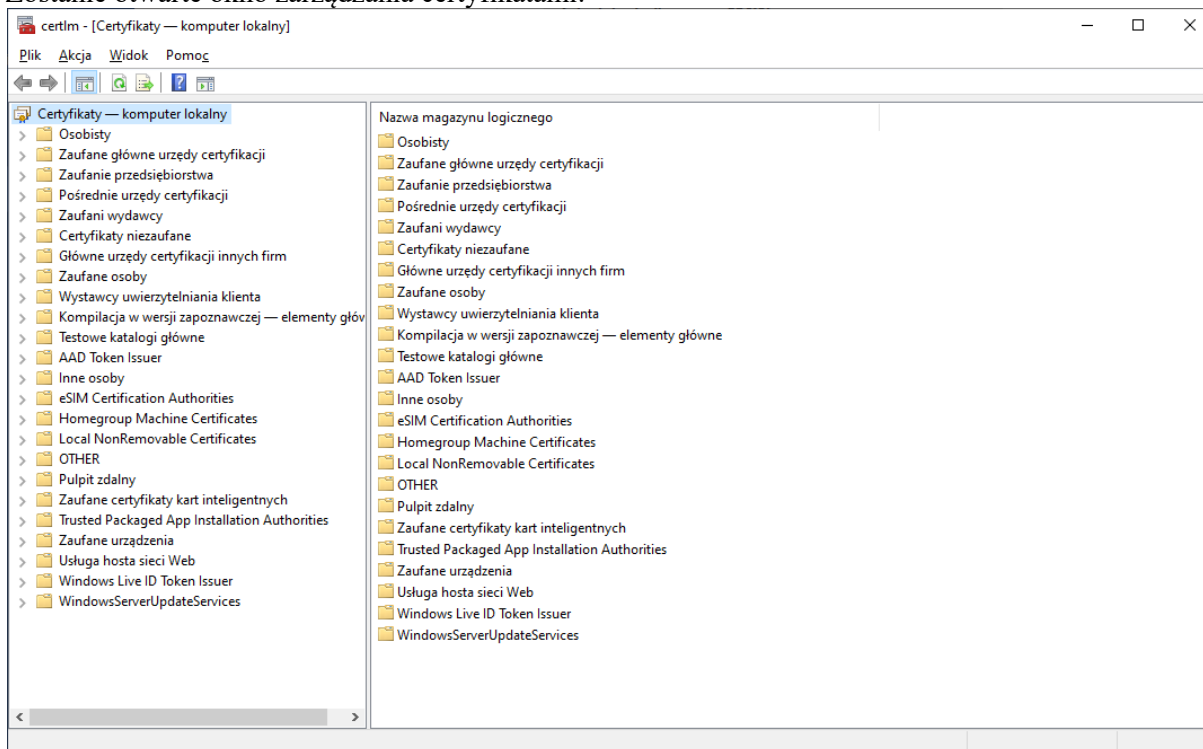
Nadajemy hasło, którym zabezpieczony zostanie otrzymany plik pfx (plik pfx zawiera klucz prywatny i certyfikat), który importujemy w systemie Windows

# Import certyfikatu do systemu Windows i konfiguracja aplikacji Legislator

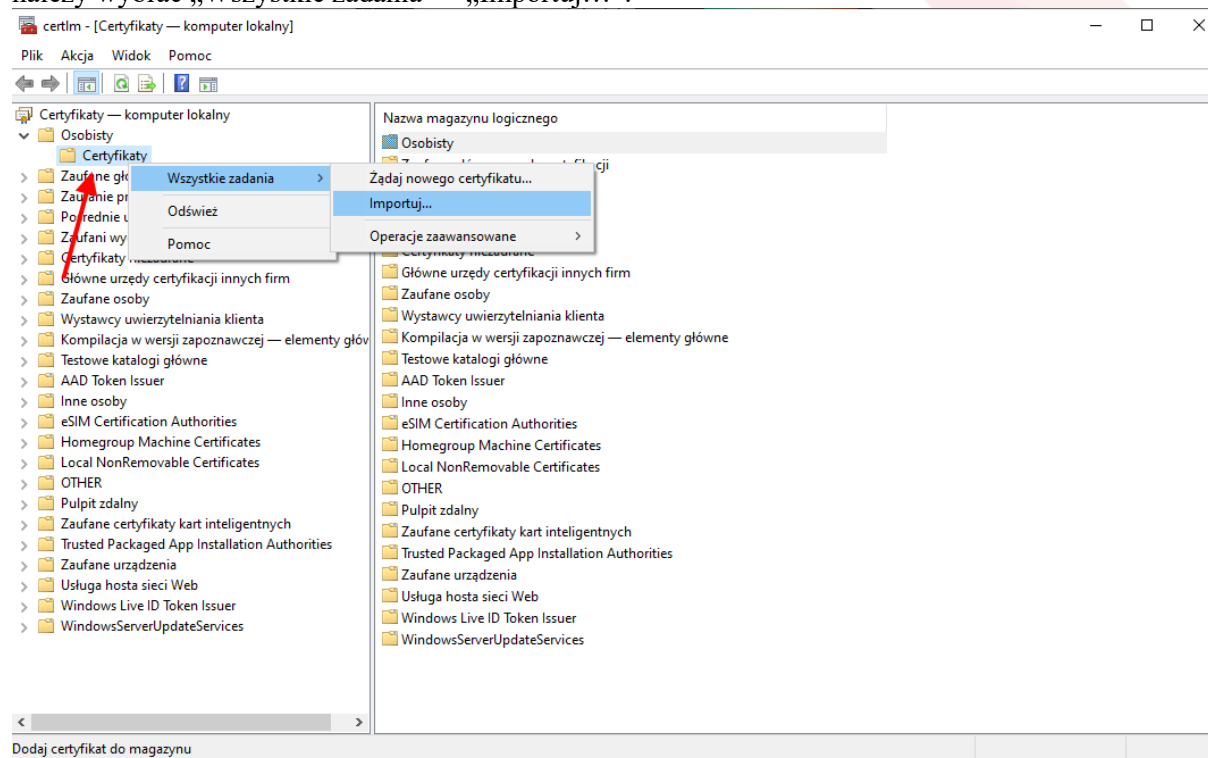
Z poziomu otwartego wiersza poleceń należy uruchomić konsolę zarządzania certyfikatami poprzez polecenie „certlm.msc”:



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)

X

← Kreator importu certyfikatów

## 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.

Dalej

Anuluj



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

×

← Kreator importu certyfikatów

#### Import pliku

Wybierz plik, który chcesz zaimportować.

Nazwa pliku:

D:\Dokumenty\Softros LAN Messenger\Tomasz Chabko - 2021 wrz

Przełącz...

Uwaga: używając następujących formatów, można przechować więcej niż jeden certyfikat w pojedynczym pliku:

Wymiana informacji osobistych — PKCS #12 (PFX, P12)

Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)

Magazyn certyfikatów seryjnych firmy Microsoft (SST)

Dalej

Anuluj

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

×

← Kreator importu certyfikatów

#### 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.

☐ Chroni klucz prywatny, używając zabezpieczeń opartych na wirtualizacji (nieeksportowalne)

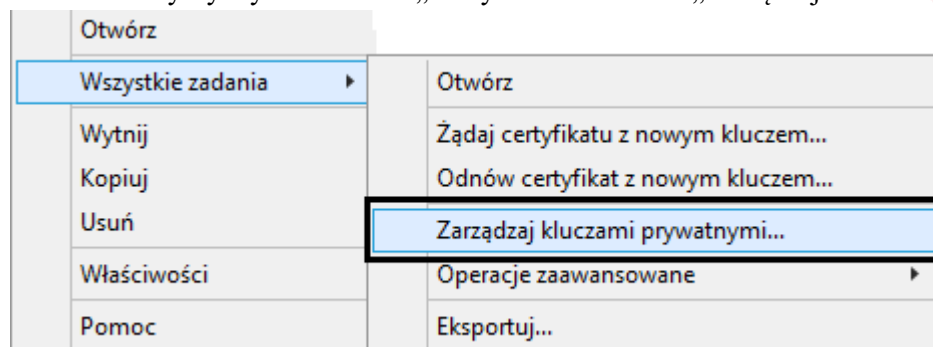
☒ Dołącz wszystkie właściwości rozszerzone.

Dalej

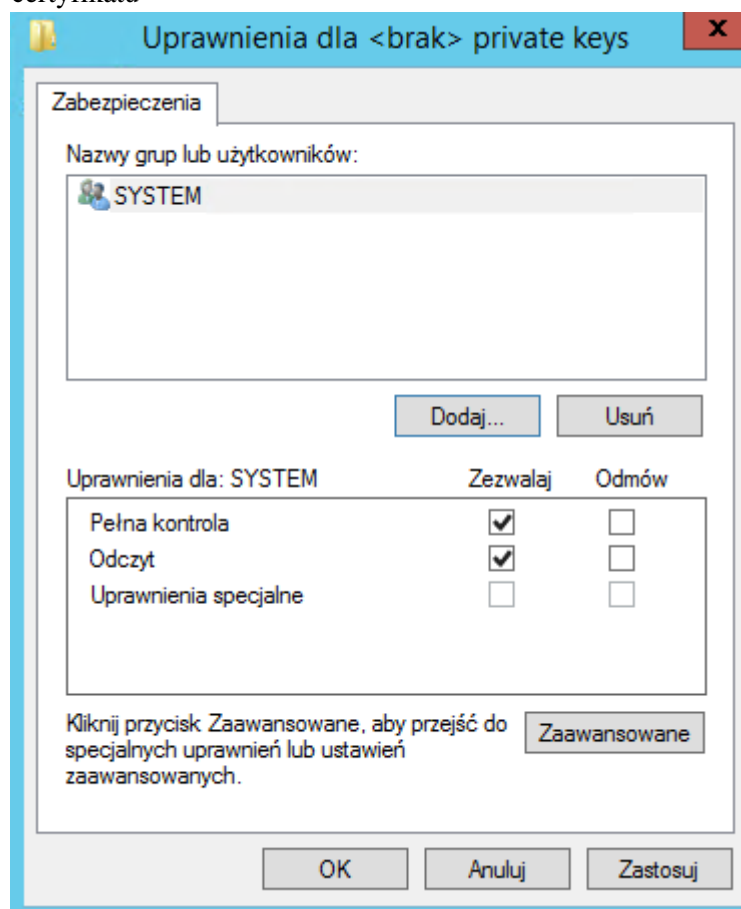
Anuluj

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



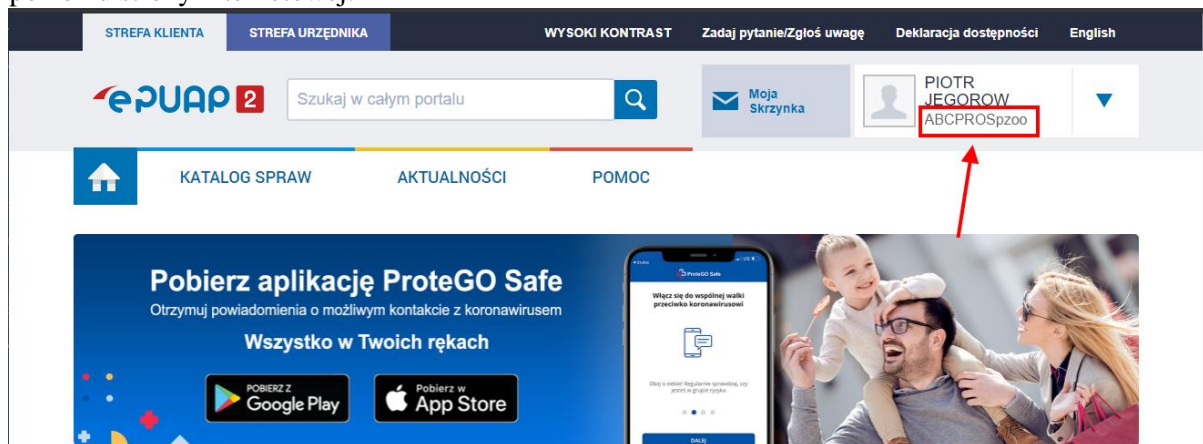
**Należy dodać użytkownika, który korzysta z systemu i przydzielić mu uprawnienie „Odczyt”.**

Po prawidłowej rejestracji zalecamy jest restart systemu operacyjnego.

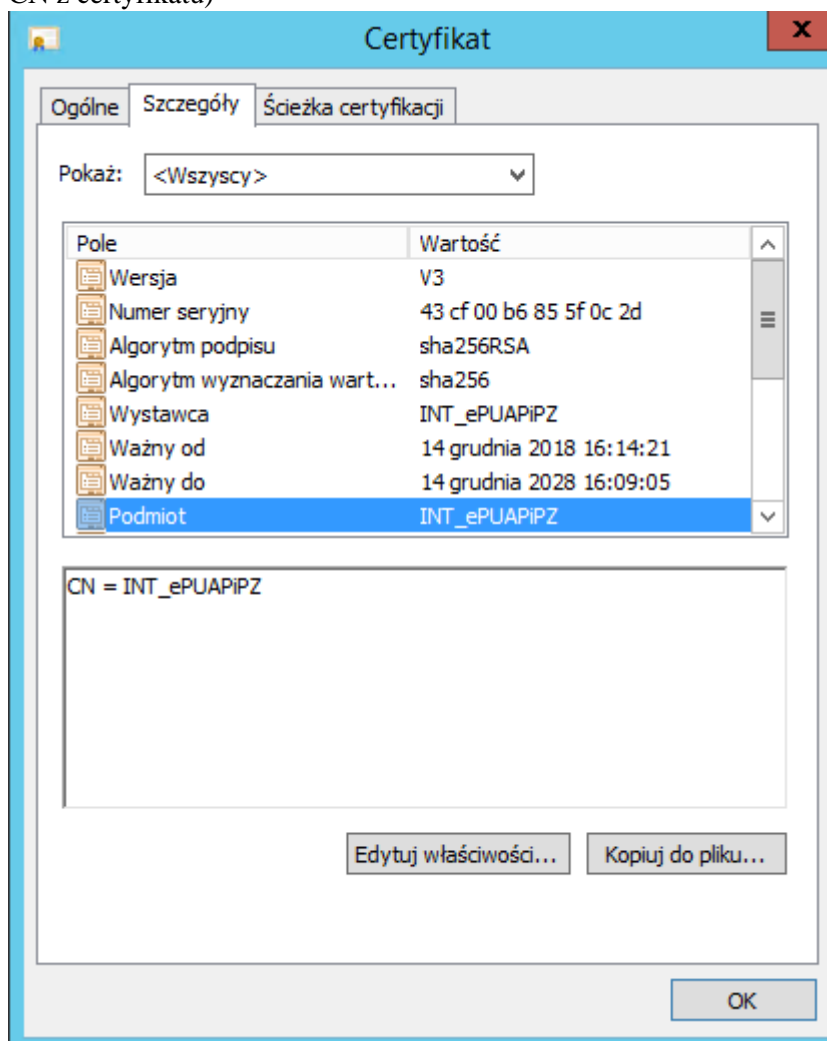
## Konfiguracja lokalna

Po wykonaniu restartu, należy uruchomić EAP Legislador 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) Skrytka odpowiedzi – należy wprowadzić adres skrytki ePUAP swojego urzędu, na który ma być przekazywana ewentualna korespondencja z nadzoru prawnego
- 4) Certyfikat – wskazujemy z listy wcześniej zaimportowany certyfikat.

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

## Komunikacja Proxy

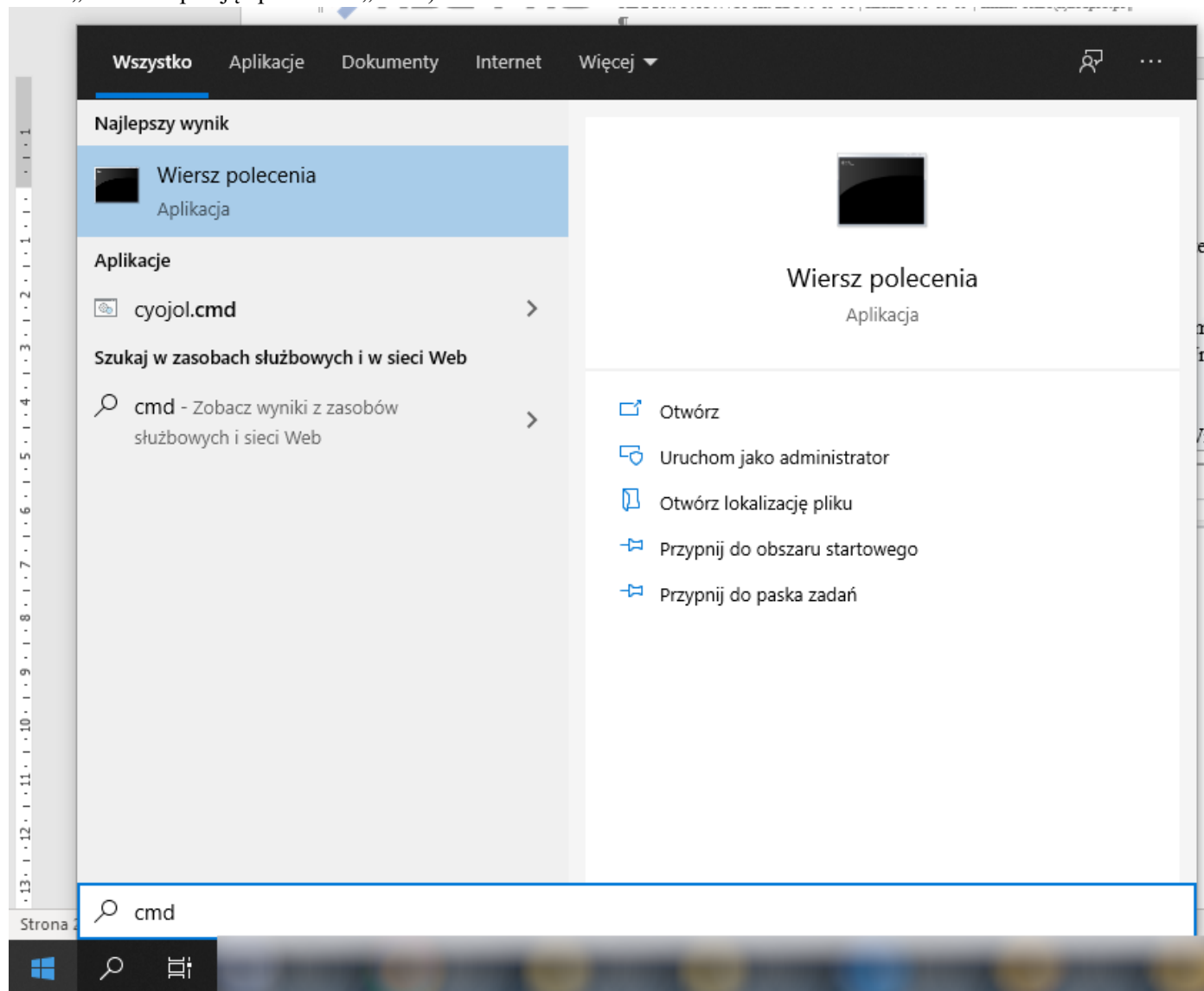
Wymagane komponenty:

- 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>)

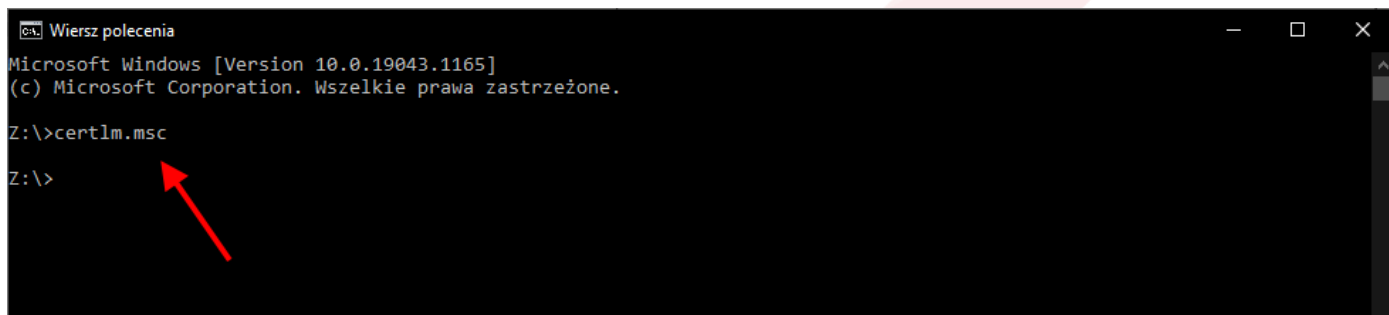
Import Certyfikatu z systemu ePUAP w systemie Windows Server

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

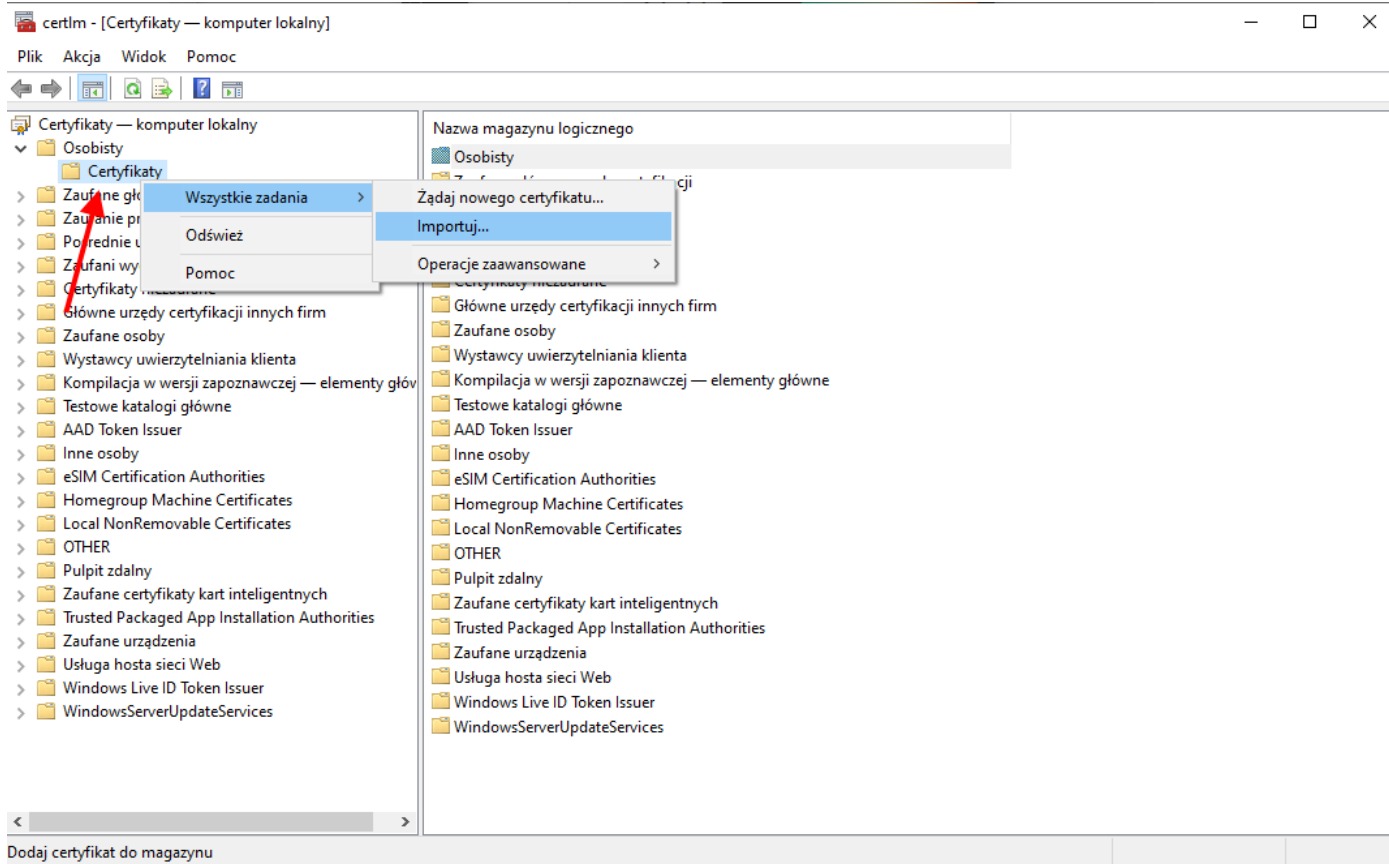
W celu importu certyfikatu do systemu Windows Server należy uruchomić aplikację Wiersz polecenia (wybierając menu „Start” i wpisując polecenie „cmd”):



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**)



←  Kreator importu certyfikatów

### 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.

Dalej

Anuluj

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



←  Kreator importu certyfikatów

### Import pliku

Wybierz plik, który chcesz zaimportować.

Nazwa pliku:

D:\Dokumenty\Softros LAN Messenger\Tomasz Chabko - 2021 wrz

Przełdaj...

Uwaga: używając następujących formatów, można przechować więcej niż jeden certyfikat w pojedynczym pliku:

Wymiana informacji osobistych — PKCS #12 (PFX, P12)

Standard składni wiadomości kryptograficznych — certyfikaty PKCS #7 (P7B)

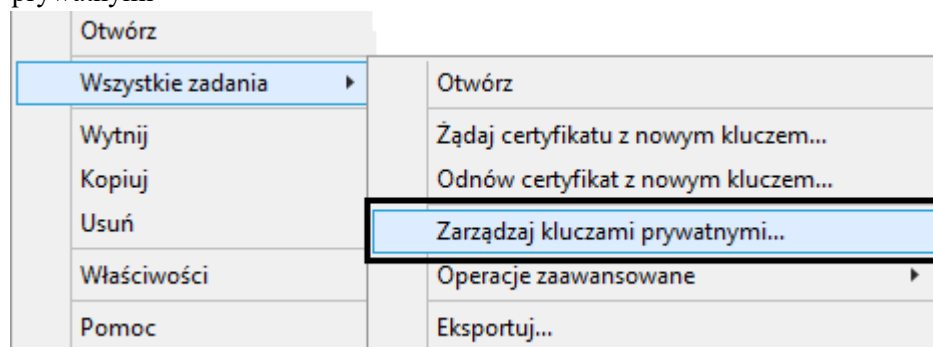
Magazyn certyfikatów seryjnych firmy Microsoft (SST)

Dalej

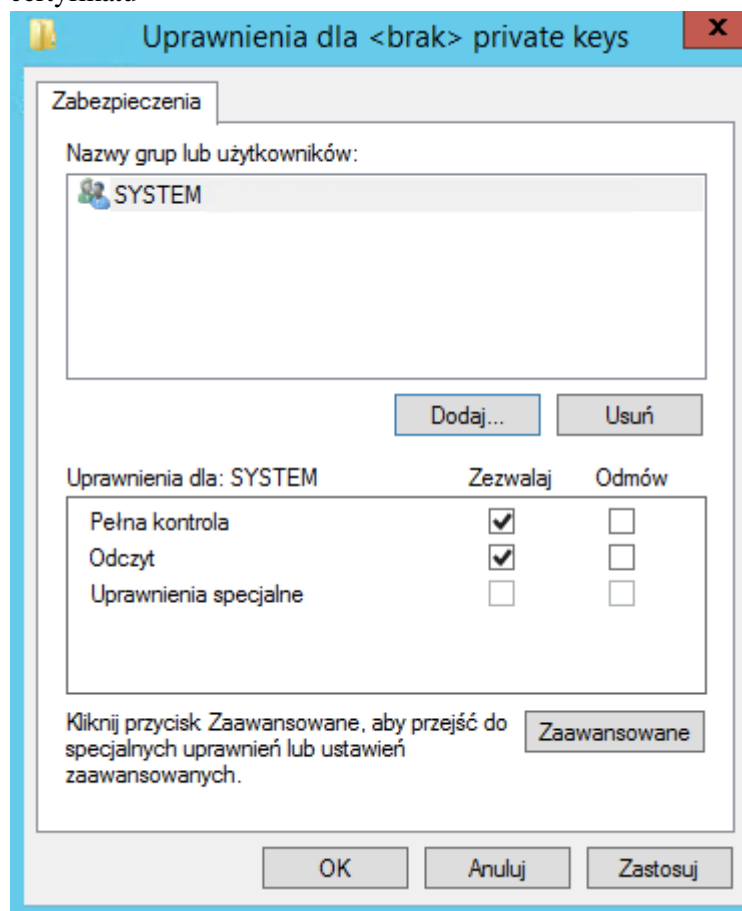
Anuluj

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](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",
    "ResponsePostbox": "/nazwa_uzytkownika/Skrytka"
```

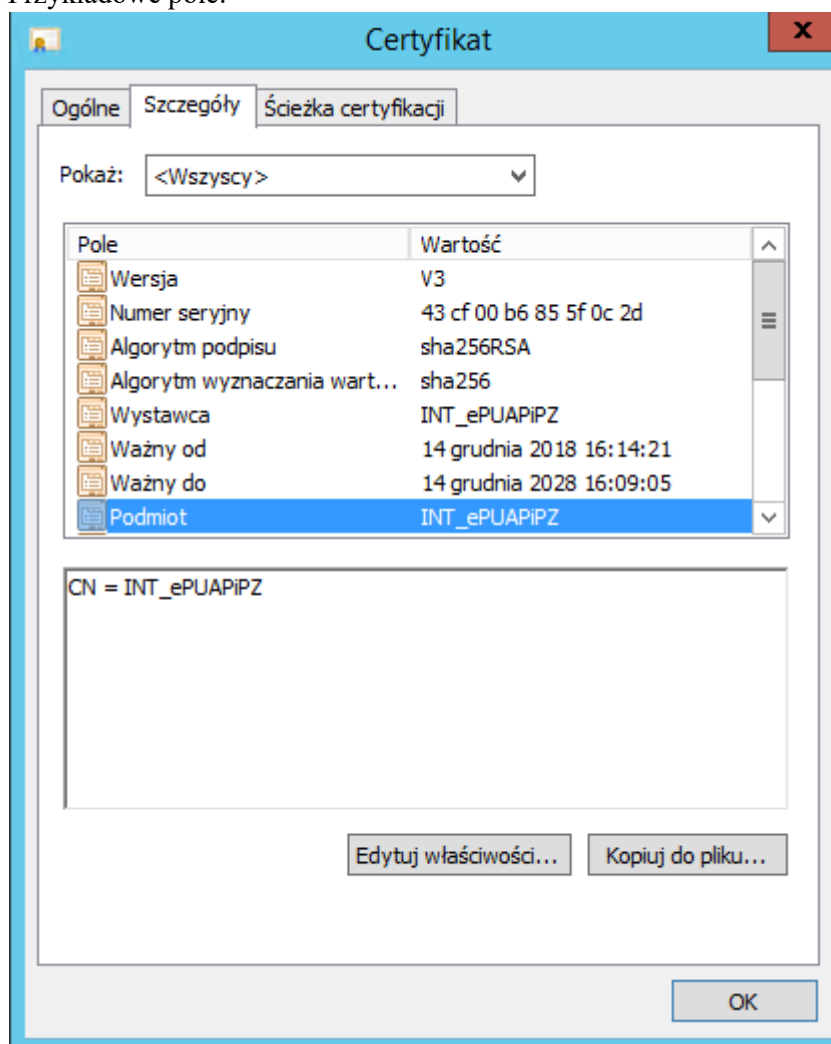
W sekcji „Urls” należy wpisać adres serwera i port, tu określamy adres na którym dostępny będzie serwis PROXY.

W Sekcji „Epuap” podajemy następujące dane:

„Id” – to pole oznacza identyfikator podmiotu nadany w systemie ePaup

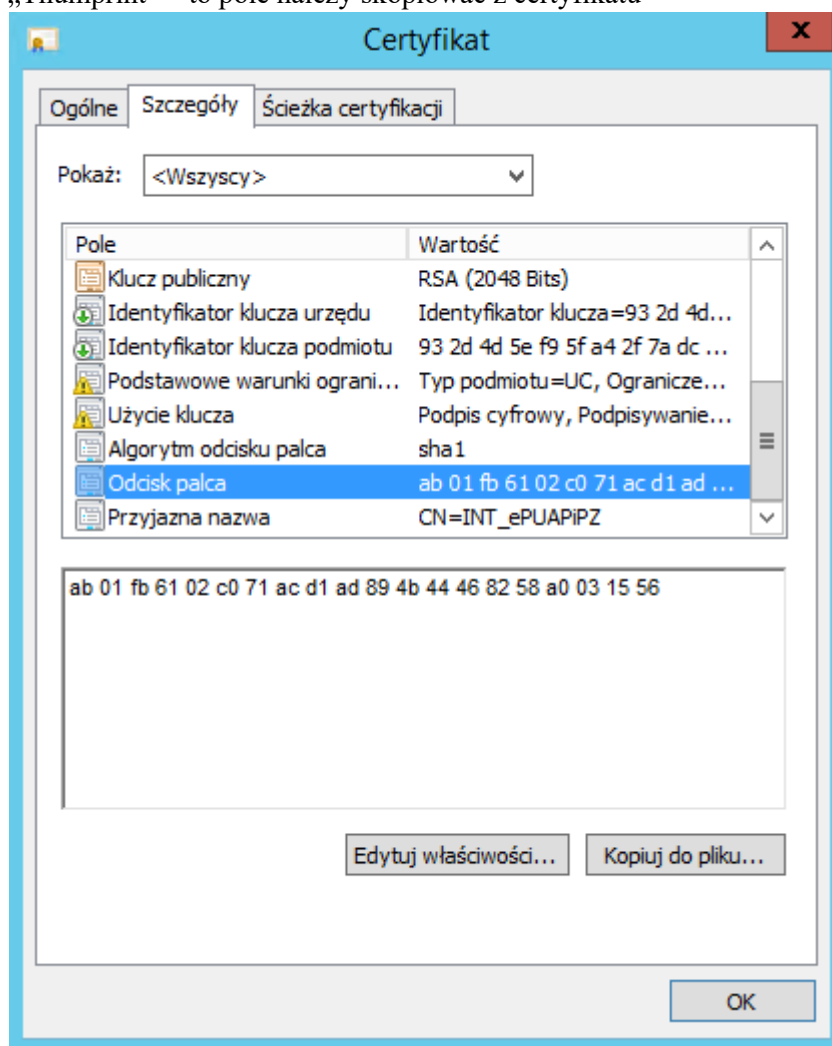
„Dns” – to pole oznaczone jest jako CN w certyfikacie wydanym dla systemu ePaup

Przykładowe pole:



„ResponsePostbox” – należy wprowadzić adres skrytki ePUAP swojego urzędu, na który ma być przekazywana ewentualna korespondencja z nadzoru prawnego

„Thumbprint” – to pole należy skopiować z certyfikatu



Przykładowe dane w pliku appsettings.json mogą wyglądać następująco:

```
"Urls": "http://192.168.0.63:4000;http://ABC-DEVELOP:4000",
"appSettings": {
  "Epuap": {
    "Id": "PiotrJ",
    "Dns": "22.180.213.98",
    "Thumbprint": "189216b3e8c44a3aebdf72bcfc8b17b7bcbb3d50",
    "ResponsePostbox": "/PiotrJ/eNadzor"
```

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 konsolę „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> )

Po prawidłowej rejestracji serwera Proxy należy podać jego adres w ustawieniach EAP Legislator

**Legislator**

Piotr Jęgorow, Kierownik Wydział Organizacyjny (Zalogowany jako Piotr Jęgorow)  
miastowolomierz (Email instytucji: pj@abc-grytner.pl)

**Ustawienia sieciowe**

☐ Używaj serwera Proxy

☒ Domyślne ustawienia Windows Internet Explorer  
☐ Ustawienia niestandardowe

Adres:  Port:

☐ Nie używaj serwera proxy dla adresów lokalnych

**Autentykacja dla serwera PROXY**

☒ Bez logowania (Domyślne)  
☐ Logowanie z domyślnymi ustawieniami  
☐ Logowanie jako

Nazwa użytkownika:   
Hasło:   
Domena:

☐ Pobieraj dane personalizacyjne z Active Directory

**Komunikacja z systemem ePUAP**

☐ Komunikacja lokalna

Epuap Id:   
DNS:   
Skrytka odpowiedzi:   
Certyfikat:

☒ Komunikacja proxy

Proxy url: