

ePUAP

Instrukcja generowania żądania certyfikatu

Wersja 1.1



Instrukcja generowania żądania certyfikatu

Spis treści

Wprowadzenie	3
1. Tworzenie keystore	3
2. Generowanie żądania certyfikatu	5
3. Informacja o wydaniu certyfikatu	6



Wprowadzenie

W celu zwiększenia bezpieczeństwa komunikacji systemów integrujących się z ePUAP został zmieniony mechanizm wystawiania certyfikatów. Podstawą wiarygodności certyfikatów jest bezpieczeństwo klucza prywatnego. **Klucz prywatny nigdy i nigdzie nie powinien być udostępniany.** Podmiot publiczny, który chce integrować się z ePUAP musi wygenerować żądanie certyfikatu. Podczas generowania żądania tworzony jest klucz prywatny (należy go odpowiednio zabezpieczyć) oraz „treść” żądania, którą należy wstawić w formularzu usługi „Wniosek o certyfikat”.

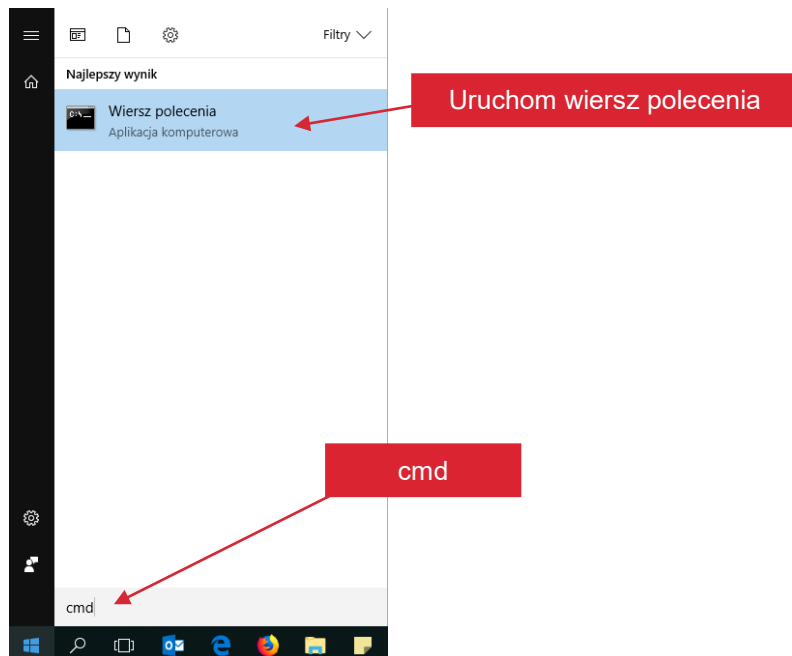
Do wygenerowania klucza prywatnego wraz z żądaniem można użyć narzędzia keytool, który jest częścią Java JRE. Należy sprawdzić i ewentualnie zainstalować Java JRE w wersji odpowiedniej dla platformy, na której będzie generowany CSR.

Poniżej przykład generowania CSR na platformie Windows. Przed wygenerowaniem CSR należy utworzyć keystore, w którym będzie przechowywany certyfikat.

1. Tworzenie keystore

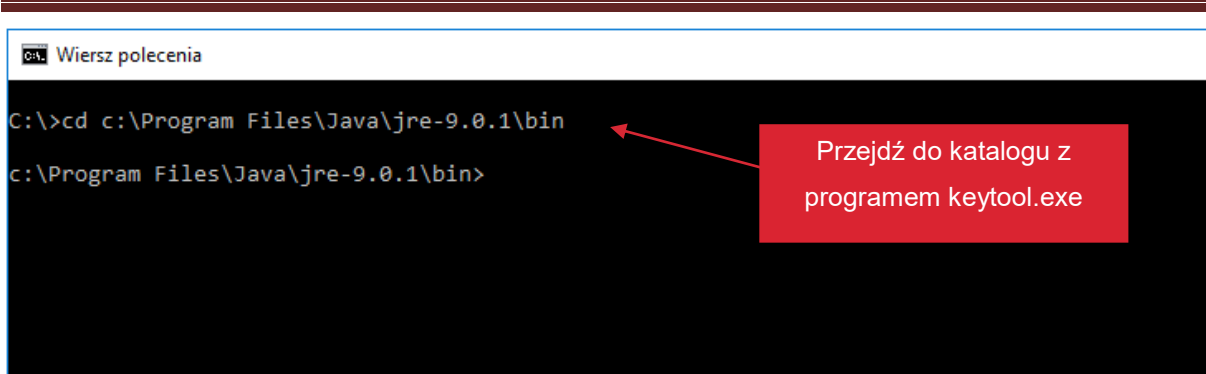
Wyszukaj program keytool.exe za pomocą wyszukiwarki Windows. W poniższym przykładzie program keytool znajduje się w katalogu C:\Program Files\Java\jre-9.0.1\bin.

Uruchom wiersz poleceń w systemie Windows wpisując CMD w polu „Uruchom”.



Przejdź do katalogu, w którym znajduje się narzędzie keytool.

Instrukcja generowania żądania certyfikatu



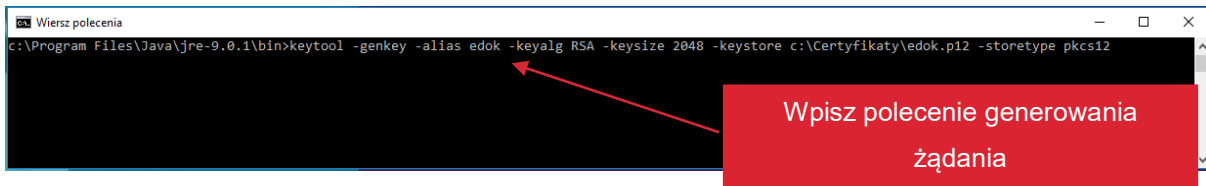
```
C:\>cd c:\Program Files\Java\jre-9.0.1\bin  
c:\Program Files\Java\jre-9.0.1\bin>
```

Przejdź do katalogu z
programem keytool.exe

Utwórz katalog, w którym zostanie zapisany keystore np. C:\Certyfikaty.

Utwórz keystore za pomocą polecenia:

keytool -genkey -alias <nazwa_systemu> -keyalg RSA -keysize 2048 -keystore <nazwa_pliku_z_pełną
ścieżką> -storetype pkcs12



```
c:\Program Files\Java\jre-9.0.1\bin>keytool -genkey -alias edok -keyalg RSA -keysize 2048 -keystore c:\Certyfikaty\edok.p12 -storetype pkcs12
```

Wpisz polecenie generowania
żądania

Zostaniesz poproszony o podanie hasła do keystore. Zapamiętaj jakie hasło podasz. Będzie Ci one potrzebne do wygenerowania żądania oraz aby dodać certyfikat, który od nas otrzymasz. Podaj wszystkie parametry, o które zostaniesz poproszony. Jeżeli wpiszesz inne dane niż w formularzu Wniosku o certyfikat to wystawimy certyfikat z danymi z Wniosku o certyfikat przesłanego do Ministerstwa Cyfryzacji.

Instrukcja generowania żądania certyfikatu

```
Wiersz polecenia

C:\Program Files\Java\jre-9.0.1\bin>keytool -genkey -alias edok -keyalg RSA -keysize 2048 -keystore c:\Certyfikaty\edok.p12
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: edok
What is the name of your organizational unit?
[Unknown]: COI
What is the name of your organization?
[Unknown]: COI
What is the name of your City or Locality?
[Unknown]: Warszawa
What is the name of your State or Province?
[Unknown]: mazowieckie
What is the two-letter country code for this unit?
[Unknown]: PL
Is CN=edok, OU=COI, O=COI, L=Warszawa, ST=mazowieckie, C=PL correct?
[no]: yes
yes

C:\Program Files\Java\jre-9.0.1\bin>
```

Adres domeny lub stały numer IP systemu, który będzie uzyskiwał dostęp do ePUAP

Nazwa podmiotu publicznego

Miejscowość

Województwo

PL

yes

2. Generowanie żądania certyfikatu

Utwórz żądanie certyfikatu za pomocą polecenia:

```
keytool -certreq -keyalg RSA -alias <nazwa_systemu> -file <nazwa_pliku_csr_z_pełną_ścieżką> -  
keystore <nazwa_keystore_utworzonego_w_rozdziale_poprzednim>
```

```
Wiersz polecenia - keytool -certreq -keyalg RSA -alias edok -file c:\Certyfikaty\edok.csr -keystore c:\Certyfikaty\edok.p12

C:\Program Files\Java\jre-9.0.1\bin>keytool -certreq -keyalg RSA -alias edok -file c:\Certyfikaty\edok.csr -keystore c:\Certyfikaty\edok.p12
Enter keystore password:
```

Podaj hasło ustawione w poprzednim kroku

Brak komunikatu błędu oznacza, że żądanie certyfikatu zostało utworzone.

```
Wiersz polecenia

C:\Program Files\Java\jre-9.0.1\bin>keytool -certreq -keyalg RSA -alias edok -file c:\Certyfikaty\edok.csr -keystore c:\Certyfikaty\edok.p12
Enter keystore password:

C:\Program Files\Java\jre-9.0.1\bin>
```

Przejdź do katalogu, który podałeś jako miejsce zapisu pliku CSR. Plik o rozszerzeniu .csr to plik żądania certyfikatu (CSR). Otwórz go w edytorze (np. Notepad++ lub Notatnik) a następnie jego zawartość wstaw do wniosku o certyfikat.

Instrukcja generowania żądania certyfikatu

Treść żądania rozpoczyna się od:

-----BEGIN NEW CERTIFICATE REQUEST-----

Na końcu znajduje się:

-----END NEW CERTIFICATE REQUEST-----

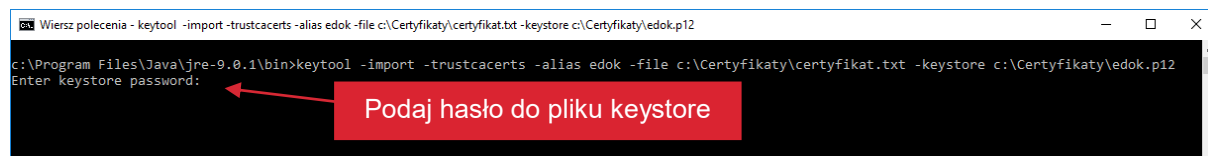
Skopiuj całą zawartość pliku o rozszerzeniu .csr (razem z -----BEGIN NEW CERTIFICATE REQUEST----- oraz -----END NEW CERTIFICATE REQUEST-----) . Nie wstawiaj w CSR dodatkowych białych znaków (spacja, tabulacja czy też znak przejścia do nowej linii (enter)).

3. Informacja o wydaniu certyfikatu

Po przesłaniu Wniosku o certyfikat do Ministerstwa Cyfryzacji wniosek zostanie zweryfikowany. Po pomyślnej weryfikacji certyfikat zostanie wygenerowany i wysłany w pliku certyfikat.txt na adres email osoby upoważnionej do odbioru nośników kluczy kryptograficznych podany we wniosku. Po otrzymaniu certyfikatu możesz dodać go do utworzonego wcześniej keystore. Możesz to zrobić za pomocą keytool. W tym celu wgraj otrzymany certyfikat do katalogu, w którym masz keystore. Następnie uruchom wiersz poleceń w systemie Windows (cmd) i przejdź do katalogu, w którym znajduje się narzędzie keytool.

Uruchom polecenie:

```
keytool -import -trustcacerts -alias <alias_certyfikatu> -file <plik_certyfikatu_wraz_z_pełną_ścieżką> -  
keystore <keystore_wraz_z_pełną_ścieżką>
```



Zostanie wyświetlona informacja o dodawanym certyfikacie.

Instrukcja generowania żądania certyfikatu

```
Wiersz polecenia

C:\Program Files\Java\jre-9.0.1\bin>keytool -import -trustcacerts -alias edok -file c:\Certyfikaty\certyfikat.txt -keystore c:\Certyfikaty\edok.p12
Enter keystore password:

Top-level certificate in reply:
Owner: CN=Root CA, O=Minister właściwy ds informatyzacji, C=PL
Issuer: CN=Root CA, O=Minister właściwy ds informatyzacji, C=PL
Serial number: 1
Valid from: Thu Dec 28 11:26:46 CET 2017 until: Wed Dec 31 23:59:59 CET 2031
Certificate fingerprints:
  SHA1: 7E:3B:58:56:0F:A8:8D:16:C0:39:E0:49:65:19:8E:76:F6:A9:51:C3
  SHA256: 96:2B:EC:47:22:F7:B6:3A:96:57:A1:DE:C3:05:F6:A7:DA:CC:57:56:59:AF:B8:75:B1:21:23:8C:63:E4:3B:DC
Signature algorithm name: SHA512withRSA
Subject Public Key Algorithm: 4096-bit RSA key
Version: 3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]
#2: ObjectId: 2.5.29.32 Criticality=false
CertificatePolicies [
  [CertificatePolicyId: [2.5.29.32.0]
  [] ]
]
#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
  Crl_Sign
]
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
  KeyIdentifier [
    0000: E7 FA B6 F1 9B CB 6C D2  00 97 07 42 90 D0 4E 8E  .....1....B..N.
    0010: 38 C7 64 D8                8.d.
  ]
]

... is not trusted. Install reply anyway? [no]: yes
Certificate reply was installed in keystore

C:\Program Files\Java\jre-9.0.1\bin>
```

Potwierdź wpisując yes

Szczegółową instrukcję instalacji certyfikatu w systemie integrującym się z ePUAP oraz PZ powinien podać jego dostawca.

Plik o rozszerzeniu .p12 jest certyfikatem zawierającym klucz prywatny. Należy odpowiednio go zabezpieczyć tak, aby nigdy nie trafił w niepowołane ręce.