

ePłatności



Instrukcja generowania żądania certyfikatu

wersja 1.1



COI



mObywatel

Spis treści

Wprowadzenie

1. Tworzenie keystore

2. Generowanie żądania certyfikatu

3. Informacja o wydaniu certyfikatu

Wprowadzenie

Podstawą wiarygodności certyfikatów jest bezpieczeństwo klucza prywatnego.

Klucz prywatny nigdy i nigdzie nie powinien być udostępniany.

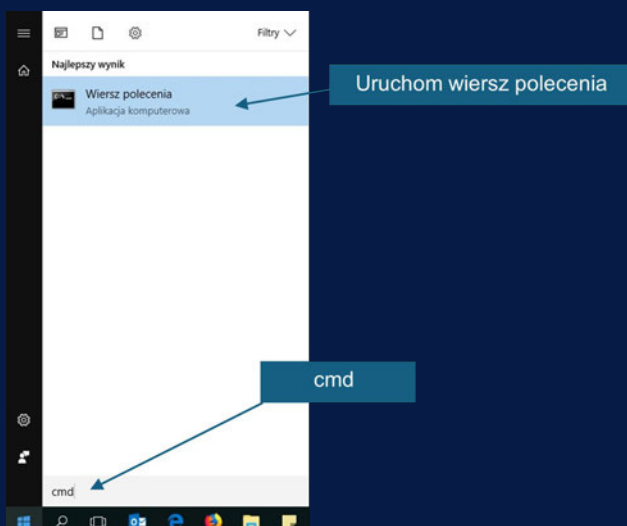
Podmiot publiczny, który chce integrować się z ePUAP musi wygenerować żądanie certyfikatu. Podczas generowania żądania, tworzony jest klucz prywatny (należy go odpowiednio zabezpieczyć) oraz „treść” żądania, którą należy wstawić w formularzu usługi „Wniosek o certyfikat”.

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.

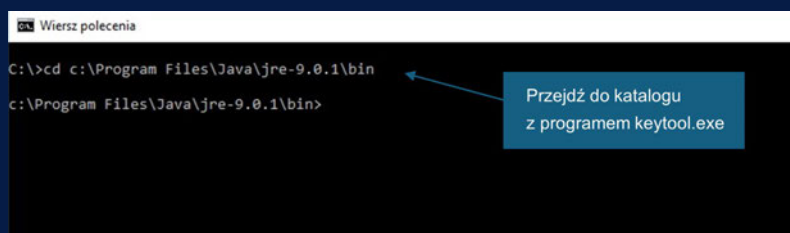
Przed wygenerowaniem CSR należy utworzyć keystore, w którym będzie przechowywany certyfikat.

1 Tworzenie keystore

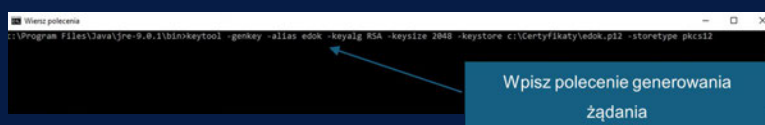
- Wyszukaj program keytool.exe za pomocą wyszukiwarki Windows. W poniższym przykładzie program keytool znajduje się w katalogu C:\Program Files\Java\jre-9.0.1\bin.
- Uruchom wiersz polecenia w systemie Windows wpisując CMD w polu „Uruchom”.



- Przejdź do katalogu, w którym znajduje się narzędzie keytool.



- 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`.



- Zostaniesz poproszony o podanie hasła do keystore, zapamiętaj je. Hasło będzie potrzebne do wygenerowania żądania i dodania certyfikatu, który od nas otrzymasz.
- Podaj wszystkie parametry, o które zostaniesz poproszony. Jeśli wpiszesz inne dane niż w formularzu Wniosku o certyfikat to wystawimy certyfikat z danymi z Wniosku o certyfikat przesłanego do Ministerstwa Cyfryzacji.
- W polu „Nazwa systemu teleinformatycznego” możesz wpisać nazwę: UM Nazwa Urzędu (bez polskich znaków, np. UM Torun) lub tak jak wskazujemy w instrukcji: EPlatnosci UM Nazwa Urzędu (bez polskich znaków, np. EPlatnosci UM Torun). W certyfikacie widoczna będzie nazwa z wniosku.
- W polu „Adres domeny lub stały numer IP systemu, który będzie uzyskiwał dostęp do ePUAP” możesz wpisać adres IP urzędu lub tak, jak wskazujemy w instrukcji tekst EPlatnosci (bez polskich znaków). W certyfikacie widoczna będzie wartość z wniosku.

```

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 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 C=edok, OU=COI, O=COI, L=Warszawa, ST=mazowieckie, C=PL correct?
[no]: yes
C:\Program Files\Java\jre-9.0.1\bin>

```

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> -storetype pkcs12`.

```

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 -storetype pkcs12
Enter keystore password:

```

- Brak komunikatu błędu oznacza, że żądanie certyfikatu zostało utworzone.

```

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 -storetype pkcs12
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 plik w edytorze (np. Notepad++ lub Notatnik) i wstaw jego zawartość do wniosku o certyfikat.

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.
- Wgraj otrzymany certyfikat do katalogu, w którym masz keystore.
- 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> -storetype pkcs12`.



- Otrzymasz informacje o dodanym certyfikacie.

```

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:38:58:56:0F:A8:8D:16:C0:39:E8:49:65:19:8E:76:F6:A9:51:C3
    SHA256: 96:28:EC:47:22:F7:86:3A:96:57:A1:DE:C3:05:F6:A7:DA:CC:57:56:59:AF:88:75:B1:21:23:8C:63:E4:38: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 86 F1 98 CB 6C D2  00 97 07 42 90 D0 4E 8E  .....1.....8..N.
        0010: 38 C7 64 08                      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>
  
```

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.