ePłatności

Instrukcja generowania żądania certyfikatu

wersja 1.1

MC

BGK BANK GOSPODARSTWA KRAJOWEGO

COI

mObywatel

ePłatności

Spis treści

Wprowadzenie

1. Tworzenie keystore

2. Generowanie żądania certyfikatu

3. Informacja o wydaniu certyfikatu

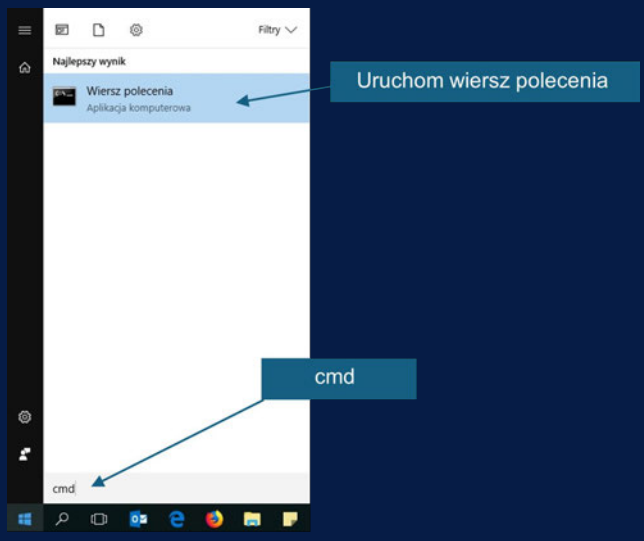
ePłatności

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

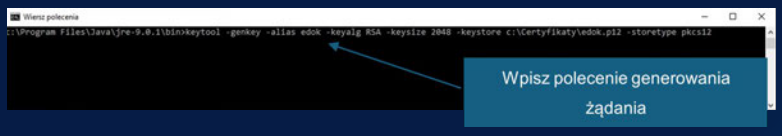
- Wyszukaj program keytool.exe za pomocą wyszukiwarki Windows. W poniższym przykładzie program keytool znajduje się w katalogu C:\Program Files\Java\jre-9.0.1\bin.
- Uruchom wiersz polecenia w systemie Windows wpisując CMD w polu „Uruchom".



ePłatności

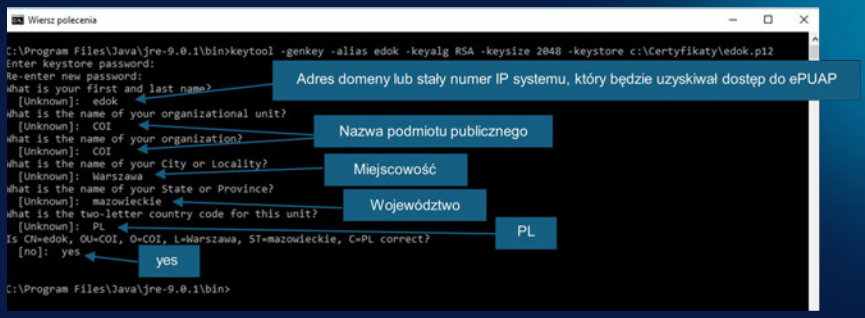
- Przejdź do katalogu, w którym znajduje się narzędzie keytool.

- 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.



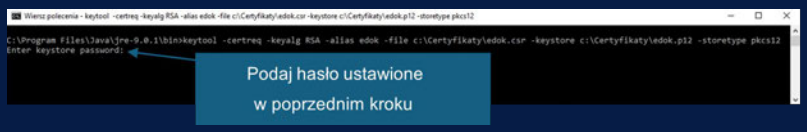
- Zostaniesz poproszony o podanie hasła do keystore, zapamiętaj je. Hasło będzie potrzebne do wygenerowania żądania i dodania certyfikatu, który od nas otrzymasz.
- Podaj wszystkie parametry, o które zostaniesz poproszony. Jeśli wpiszesz inne dane niż w formularzu Wniosku o certyfikat to wystawimy certyfikat 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.

ePłatności

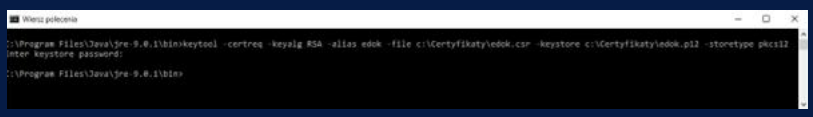


2 Generowanie żądania certyfikatu

- 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.



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



- 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.

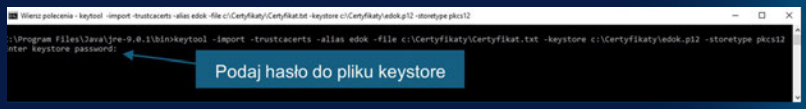
Treść żądania rozpoczyna się od:
-----BEGIN NEW CERTIFICATE REQUEST-----
Na końcu znajduje się:
-----END NEW CERTIFICATE REQUEST-----

- 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)).

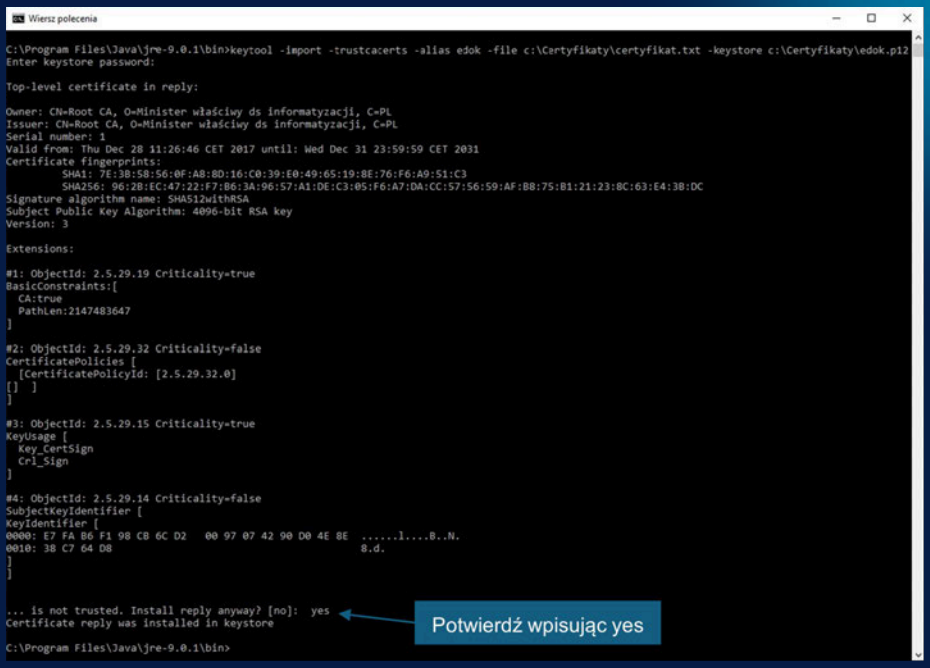
3 Informacja o wydaniu certyfikatu

- 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.

ePłatności



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.