Instrukcja uruchomienia projektu testowego dla usługi pobrania Digital Green Certificate

**„Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych" (P1) – faza 3**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Metryka | | | | | | | |
| Właściciel | | | Centrum e-Zdrowia | | | | |
| Autor | | | Centrum e-Zdrowia | | | | |
| Recenzent | | | Centrum e-Zdrowia | | | | |
| Liczba stron | | | 6 | | | | |
| Zatwierdzający | | | CeZ | | | Data zatwierdzenia | 2021-05-xx |
| Wersja | | | 1.0 | | | Status dokumentu | Zaakceptowany |
| Data utworzenia | | | 2021-05-24 | | | Data ostatniej modyfikacji | 2021-05-24 |
| Historia zmian | | | | | | | |
| Data | Wersja | | Autor zmiany | Opis zmiany | | | |
| 2021-05-24 | 1.0 | | CEZ | Wersja inicjalna dokumentu | | | |

Spis treści

[**1.** **Wstęp** 4](#_Toc61950935)

[1.1. Wymagania 4](#_Toc61950936)

[1.2. Zawartość przekazanego archiwum zip 4](#_Toc61950937)

[**2.** **Konfiguracja dodatkowa narzędzia SoapUI** 5](#_Toc61950938)

[2.1. Konfiguracja połączenia SSL: 5](#_Toc61950941)

[**3.** **Uruchomienie projektu SoapUI** 6](#_Toc61950942)

[3.1. Import projektu testów: 6](#_Toc61950944)

[3.2. Konfiguracja projektu: 6](#_Toc61950945)

[3.3. Uruchomienie testów: 6](#_Toc61950946)

# **Wstęp**

W celu usprawnienia integracji systemów zewnętrznych z Systemem P1 w zakresie pobrania wydruku Digital Green Certificate potwierdzającego zaszczepienie, przebycie choroby lub wykonanie testu został przygotowany projekt testów SoapUI. Projekt testów SoapUI obejmuje przypadek testowy, którego celem jest wygenerowanie wydruku Digital Green Certificate potwierdzającego szczepienie przeciwko COVID-19. Przygotowany przypadek testowy zawiera generowanie tokena dostępowego, wyszukanie pacjenta, zapis szczepienia (dawka 1 z 1) i podpisu pod szczepieniem oraz pobranie wydruku zawierającego Digital Green Certificate.

## Wymagania

W celu uruchomienia przekazanego projektu SoapUI należy wykonać instalację i konfigurację następującego oprogramowania:

1. JDK Oracle 1.8
2. SoapUI w wersji 5.5.0
3. Klucze i certyfikaty otrzymane od CEZ:
   1. Do uwierzytelnienia danych (wss)
   2. Do uwierzytelnienia systemu (tls)

## Zawartość przekazanego archiwum zip

Archiwum obejmuje:

1. Niniejszy dokument
2. *CEZ-pobranie-DGC-soapui-project.xml* - Projekt SoapUI
3. Katalog *wsdl* – definicje usług
4. Katalog k*lucze* – katalog na pliki p12 z kluczami i certyfikatami używanymi do WS-Security i składania podpisu
5. Katalog *parametryzacja* – katalog zawierający skrypty pomocnicze i pliki xml wykorzystywane w przypadku testowym

Plik zip należy rozpakować. W katalogu *klucze* należy umieścić otrzymany od CEZ plik p12 z kluczami i certyfikatami do WS-Security.

# **Konfiguracja dodatkowa narzędzia SoapUI**



## Konfiguracja połączenia SSL:

1. W menu *File* SoapUI należy wybrać *Preferences*
2. W oknie *Preferences* należy wybrać zakładkę *SSL Settings*
3. W polu *KeyStore* należy wskazać otrzymany od CEZ plik z kluczami i certyfikatami do połączenia TLS
4. W polu *KeyStore Password* należy wprowadzić hasło do pliku .p12
5. Należy zaznaczyć opcję *requires client authentication* w polu *Client Authentication*
6. Należy zatwierdzić przyciskiem *OK*

# **Uruchomienie projektu SoapUI**



## Import projektu testów:

1. Należy uruchomić narzędzie SoapUI
2. Z menu *File* należy wybrać opcję *Import Project* i wskazać plik *CEZ-pobranie-DGC-soapui-project*.xml

## Konfiguracja projektu:

1. Należy kliknąć 2x (dwa razy) w zaimportowany projekt SoapUI
2. W uruchomionym oknie konfiguracji projektu należy wybrać zakładkę *Overview*, a następnie zakładkę *Properties*, która umieszczona jest w dolnym pasku otwartego okna
3. W zakładce *Properites* należy uzupełnić zmienne:
   1. *hasloCertyfikatu* – hasło do pliku .p12 z certyfikatem do składania podpisu (certyfikat do uwierzytelnienia danych – wss)
   2. *aliasCertyfikatu* – nazwa atrybutu Common Name (CN) z certyfikatu
   3. *plikCertyfikatu* – nazwa pliku .p12
4. W uruchomionym oknie konfiguracji projektu należy wybrać zakładkę *WS-Security Configuration*, a następnie zakładkę *Keystores*
5. W zakładce *Keystores* należy dodać klucz wss podmiotu umieszczony wcześniej w katalogu *klucze*
6. Należy wprowadzić hasło i zatwierdzić przyciskiem OK
7. Na zakładce *Outgoing WS-Security Configurations* należy zaznaczyć *PodmiotSGZ*
8. Należy zaznaczyć *Signature*
9. W polu *Keystore* należy wskazać dodany keystore
10. W polu *Alias* należy wybrać dostępny alias
11. W polu *Password* należy wprowadzić hasło do pliku .p12 (certyfikat do uwierzytelnienia danych – wss)
12. Należy zamknąć okno konfiguracji projektu

## Uruchomienie testów:

1. Należy kliknąć dwa razy na wybrany przypadek testowy
2. W otwartym oknie wybranego przypadku należy uruchomić test za pomocą przycisku *Run*
3. Test powinien zakończyć się wynikiem pozytywnym