

# **Instrukcja uruchomienia projektu testowego dla pobierania raportów MZT**

**„ELEKTRONICZNA PLATFORMA GROMADZENIA, ANALIZY I  
UDOSTĘPNIANIA ZASOBÓW CYFROWYCH O ZDARZENIACH  
MEDYCZNYCH" (P1) – FAZA 2**

Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania  
zasobów cyfrowych o Zdarzeniach Medycznych (P1)

Metryka			
Właściciel	Centrum e-Zdrowia		
Autor	Centrum e-Zdrowia		
Recenzent	Centrum e-Zdrowia		
Liczba stron	7		
Zatwierdzający	CeZ	Data zatwierdzenia	2022-06-21
Wersja	1.0	Status dokumentu	Zaakceptowany
Data utworzenia	2022-06-21	Data ostatniej modyfikacji	2022-06-21
Historia zmian			
Data	Wersja	Autor zmiany	Opis zmiany
2022-06-21	1.0	CEZ	Wersja inicjalna dokumentu

## Spis treści

<b>1. WSTĘP</b> .....	4
1.1. Wymagania.....	4
1.2. Zawartość przekazanego archiwum zip.....	4
<b>2. KONFIGURACJA DODATKOWA NARZĘDZIA SOAPUI</b> .....	5
2.1. Konfiguracja połączenia SSL: .....	5
<b>3. URUCHOMIENIE PROJEKTU SOAPUI</b> .....	6
3.1. Import projektu testów: .....	6
3.2. Konfiguracja projektu: .....	6
3.3. Uruchomienie testów: .....	7

# 1. WSTĘP

W celu usprawnienia integracji systemów zewnętrznych z Systemem P1 w zakresie obsługi pobierania raportów MZT został przygotowany projekt testów SoapUI.

## 1. 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:
  - a. Do uwierzytelnienia danych (wss)
  - b. Do uwierzytelnienia systemu (tls)

## 2. ZAWARTOŚĆ PRZEKAZANEGO ARCHIWUM ZIP

Archiwum obejmuje:

1. Niniejszy dokument
2. *TestyDlaIntegratorowMZT.xml* – Projekt SoapUI
3. Katalog *keys* – katalog na pliki p12 z kluczami i certyfikatami używanymi do WS-Security i składania podpisu

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

## 2. KONFIGURACJA DODATKOWA NARZĘDZIA SOAPUI

### 3. 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*

## 3. URUCHOMIENIE PROJEKTU SOAPUI

### 4. IMPORT PROJEKTU TESTÓW:

1. Należy uruchomić narzędzie SoapUI
2. Z menu *File* należy wybrać opcję *Import Project* i wskazać plik *TestyDlaIntegratorowMZT.xml*

### 5. 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 *Properties* należy uzupełnić zmienne:
  - a. *ServiceAddress* – <https://isus.ezdrowie.gov.pl> – adres środowiska dla integratorów.

#### Dane dotyczące danych testowych:

- a. *idRaportu1* i *idRaportu2* – kody możliwych do wygenerowania raportów w AUA, np. 'COVID' i 'PACPOZ' (możliwe do wygenerowania są również inne raporty pochodzące ze słownika 'PLAuaAvailableReports').

#### Dane dotyczące Miejsca Udzielania Świadczeń:

- a. *idPodmiotuOidRoot* – root podmiotu,
- b. *idPodmiotuOidExt* – numer księgi rejestrowej podmiotu,
- c. *idMiejscaPracyOidRoot* – root miejsca udzielania świadczenia,
- d. *idMiejscaPracyOidExt* – extension miejsca udzielania świadczenia.

#### Dane dotyczące pracownika medycznego działającego w ramach MUŚ:

- a. *idPracownikaOidRoot* – root uprawnionego pracownika medycznego, np. '2.16.840.1.113883.3.4424.1.6.2',
- b. *idPracownikaOidExt* – numer NPWZ pracownika medycznego,
- c. *rolaPracownika* – kod zawodu przypisany do pracownika medycznego, np. 'LEK'.

#### Dane dotyczące tokena dostępowego:

- a. *aliasCertyfikatu* – nazwa aliasu certyfikatu,
- b. *hasloCertyfikatu* – hasło do certyfikatu,
- c. *grantTypeParam* – stała wartość 'client\_credentials',
- d. *plikCertyfikatu* – nazwa pliku z certyfikatem,
- e. *scopeParam* – adres usługi, której dotyczy żądanie autoryzacji np. <https://ezdrowie.gov.pl/fhir>,

- f. *assertionTypeParam* – stała wartość 'urn:ietf:params:oauth:client-assertion-type:jwt-bearer',
- g. *aud* – adres usługi uwierzytelnienia, np. <https://ezdrowie.gov.pl/token>,
- h. *jti* – unikalny identyfikator tokenu,
- i. *exp* – termin ważności tokena (termin w formacie NumericDate), np. '1763814320'.

## 6. URUCHOMIENIE TESTÓW:

1. Należy kliknąć dwa razy na Test Case *TestyDlaIntegratorowMZT* i uruchomić test za pomocą przycisku *Run*.
2. Testy można uruchamiać wielokrotnie.
3. Test powinien zakończyć się pozytywnie.