Instrukcja uruchomienia projektu testowego dla usługi nadania uprawnień w systemie P1 do danych pacjentów dla pracowników medycznych z wykorzystaniem autoryzacji SMS.

# Wstęp

W celu usprawnienia integracji P1 w zakresie nadawania uprawnień dostępu do danych medycznych pacjenta dla pracowników medycznych, z wykorzystaniem autoryzacji SMS został przygotowany projekt testów SoapUI. Projekt testów SoapUI obejmuje trzy przypadki testowe dostępne na wydanie I8. Domyślnie testy uruchamiane są na Środowisku Integracyjnym.

# Wymagania

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

1. JDK Oracle 1.8
2. SoapUI w wersji 5.3.0 (wybrać wersję bez JAVA – „java not included”)
3. Klucze i certyfikaty otrzymane od CSIOZ:
   1. Do uwierzytelnienia danych (wss)
   2. Do uwierzytelnienia systemu (tls)

# Zawartość przekazanego archiwum zip

Archiwum obejmuje:

1. Niniejszy dokument
2. *ObslugaUprawnienDoDokMedWS-CSIOZ-P3I8.xml* - Projekt SoapUI
3. Katalog *z wsdl wymaganym do przeprowadzenia testu*
4. Katalog k*lucze* – katalog na pliki p12 z kluczami i certyfikatami używanymi do WS-Security i składania podpisu

Plik zip należy rozpakować. W katalogu *klucze* należy umieścić otrzymany od CSIOZ 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 wybieramy zakładkę SSL Settings
3. W polu KeyStore wskazujemy otrzymany od CSIOZ plik z kluczami i certyfikatami do połączenia TLS
4. W polu KeyStore Password wprowadzamy hasło do pliku p12
5. Zaznaczamy opcję requires client authentication w polu Client Authentication
6. Klikamy OK

# Uruchomienie projektu SoapUI

Import projektu testów:

1. Uruchamiamy narzędzie SoapUI
2. Z menu File wybieramy opcję Import Project i wskazujemy plik ObslugaUprawnienDoDokMedWS-CSIOZ-P3I8.xml

Konfiguracja projektu:

1. Klikamy 2x w zaimportowany projekt SoapUI
2. W uruchomionym oknie konfiguracji projektu wybieramy zakładkę WS-Security Configuration a następnie zakładkę Keystores
3. W zakładce Keystores dodajemy klucz wss podmiotu umieszczony wcześniej w katalogu klucze
4. Wprowadzamy hasło i klikamy OK
5. Na zakładce Outgoing WS-Security Configurations zaznaczamy *NadanieUprawnien\_Integracyjne*
6. Zaznaczamy Signature
7. W polu Keystore wskazujemy dodany keystore
8. W polu Alias wybieramy dostępny alias
9. W polu Password wprowadzamy hasło do p12
10. Zamykamy okno konfiguracji projektu

Uruchomienie testów:

1. Klikamy dwa razy na wybrany przypadek testowy
2. W otwartym oknie wybranego przypadku uruchamiamy przycisk Run
3. Test powinien zakończyć się pozytywnie