Dokumentacja integracyjna Platformy Usług Inteligentnych

**W zakresie realizacji usług diagnostyki cyfrowej (API)**

**„platforma usług inteligentnych" – faza 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Metryka** | | | |
| Właściciel | Centrum e-Zdrowia | | |
| Autor | Centrum e-Zdrowia | | |
| Recenzent | Centrum e-Zdrowia | | |
| Liczba stron | 17 | | |
| Zatwierdzający | CeZ | **Data zatwierdzenia** |  |
| Wersja | 1.0 | **Status dokumentu** |  |
| Data utworzenia | 2025-04-25 | 2025-04-18 | 2025-04-25 |

|  |  |  |  |
| --- | --- | --- | --- |
| Historia zmian | | | |
| Data | Wersja | Autor zmiany | Opis zmiany |
| 2025-04-18 | 1.0 | CeZ | Wersja inicjalna dokumentu |

| Dokumenty powiązane | |
| --- | --- |
| Nazwa pliku | pui-proces.yaml |
| Zakres | Zawiera specyfikację kontraktu w standardzie OpenAPI 3.0.3 dla procesu zlecania i odbioru wyników analizy SI |
| Nazwa pliku | pui-katalog-udc.yaml |
| Zakres | Zawiera specyfikację kontraktu w standardzie OpenAPI 3.0.3 dla interfejsu zawierającego katalog usług UDC |

Spis treści

[1. Wstęp 4](#_Toc1896341231)

[Cel i zakres dokumentu 4](#_Toc964867957)

[Wykorzystywane skróty i terminy 5](#_Toc1919034945)

[2. Opis rozwiązania 6](#_Toc1332011306)

[3. Serwer PUI CEZ 7](#_Toc111193230)

[Dostęp serwera PUI CEZ 7](#_Toc318985341)

[Komunikacja z serwerem PUI CEZ 7](#_Toc1547390161)

[Uwierzytelnienie i autoryzacja do usług serwera PUI CEZ 7](#_Toc271483718)

[Przebieg uwierzytelnienie i autoryzacji dostępu do usług serwera PUI CEZ 8](#_Toc1378435060)

[Przygotowanie TOKENU UWIERZYTELNIAJĄCEGO 8](#_Toc503425956)

[Przygotowanie i przekazanie żądania autoryzacji 11](#_Toc1447862570)

[Zabezpieczenie integralności zasobów Usług Diagnostyki Cyfrowej 12](#_Toc915312207)

[Komunikaty błędów uwierzytelnienia i autoryzacji 13](#_Toc1635872403)

[4. Opis realizacji Usług Diagnostyki Cyfrowej 14](#_Toc844326116)

[4.1. Scenariusz wywołania operacji 15](#_Toc1693039917)

[4.2. Wykaz operacji 17](#_Toc2116577707)

[4.3. Operacja pobrania tokenu dostępowego 18](#_Toc92042187)

[4.4. Operacje scenariusza Realizacji Usług Diagnostyki Cyfrowej 20](#_Toc111612741)

# Wstęp

## Cel i zakres dokumentu

Niniejsze opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z Platformą Usług Inteligentnych w zakresie realizacji Usług Diagnostyki Cyfrowej przez podmioty zewnętrzne.

Dokument obejmuje swoim zakresem specyfikację interfejsów w zakresie realizacji usług diagnostyki cyfrowej, udostępnionych w rozdziale 5 dokumentacji.

## Wykorzystywane skróty i terminy

| Lp. | Skrót / termin | Wyjaśnienie skrótu / terminu |
| --- | --- | --- |
| 1. | CeZ | Centrum e-Zdrowia |
| 2. | Platforma Usług Inteligentnych | Jest to zintegrowany system wspierający procesy diagnostyczne z wykorzystaniem Usług Diagnostyki Cyfrowej (PUI). |
| 3. | Usługa Diagnostyki Cyfrowej | Jest to proces analityczny przetwarzania danych z wykorzystaniem modeli Sztucznej Inteligencji (SI) |
| 4. | RESTful | Standard komunikacji www oparty o specyfikację protokołu HTTP. |
| 5. | Token do uwierzytelnienia | Token JWT przekazywany przez system zewnętrzny do serwera uwierzytelniającego. |
| 6. | Token dostępu (ACCESS TOKEN) | Token JWT przekazywany przez serwer uwierzytelniający w odpowiedzi na żądanie uwierzytelnienia. Token dostępu jest wymagany w żądaniach przekazywanych do serwera PUI CeZ. |
| 7. | Serwer autoryzacyjny CeZ | Serwer udostępniający komunikację z systemem PUI. |
| 8. | Serwer autoryzacyjny | Serwer obsługujący żądania autoryzacji - odpowiedzialny za generowanie tokenów dostępu. |

# Opis rozwiązania

Rozwiązanie zakłada użycie interfejsu REST API do komunikacji z serwerem autoryzacyjnym dla realizacji Usług Diagnostyki Cyfrowej oraz wykorzystaniem serwera PUI w celu umożliwienia realizacji Usług Diagnostyki Cyfrowej.

Rozwiązanie umożliwia zlecanie, weryfikację, pobieranie wyników oraz ocenę Usług Diagnostyki Cyfrowej na portalu gabinet.gov.pl

# Serwer PUI CEZ

## Dostęp serwera PUI CEZ

Dostęp do serwera PUI CEZ zabezpieczony jest protokołem TLS. Wymagane jest obustronne uwierzytelnienie. Do uwierzytelnienia podmiotu należy wykorzystać certyfikat TLS wystawiony przez Centrum Certyfikacji P1.

Dostępne są następujące środowiska:

Integracyjne: [https://tpui.ezdrowie.gov.pl](https://tpui.ezdrowie.gov.pl/)

Produkcyjne: https://pui.ezdrowie.gov.pl

## Komunikacja z serwerem PUI CEZ

Serwer PUI CEZ obsługuje komunikaty związane z obsługą Usług Diagnostyki Cyfrowej w oparciu o RESTFul API. Szczegóły dotyczące komunikacji w oparciu o RESTFul API znajdują się na stronie **https://ezdrowie.gov.pl/portal/home/dla-dostawcow/interfejsy**

**UWAGA!** Lista dostępnych parametrów wyszukiwania obejmuje tylko te, które w sposób jawny wymieniono w niniejszym dokumencie integracyjnym, w podrozdziałach dla poszczególnych operacji.

## Uwierzytelnienie i autoryzacja do usług serwera PUI CEZ

Uwierzytelnienie i autoryzacja dostępu do usług serwera PUI CEZ bazuje na standardzie **OAuth 2.0** i metodzie zgodnej z “[Client Credentials Grant](https://tools.ietf.org/html/rfc6749#section-4.4)”. W wyniku uwierzytelnienia się i autoryzacji dostępu do usług serwera PUI CEZ, system zewnętrzny Usługodawcy (klient) pozyskuje z Systemu P1 (serwera autoryzacji) **TOKEN DOSTĘPOWY**.

Warunkiem uzyskania **TOKENU DOSTĘPOWEGO** jest posiadanie aktualnego certyfikatu do uwierzytelnienia danych (WS-Security), wystawionego przez Centrum Certyfikacji P1.

**TOKEN DOSTĘPOWY** wymagany jest każdorazowo przy przekazaniu żądania wykonania operacji na serwerze PUI CEZ. **TOKEN DOSTĘPOWY** umieszczany jest w nagłówku Autorization (**“Authorization”** - “**Bearer ‘otrzymany z serwera autoryzacyjnego TOKEN DOSTĘPOWY**”).

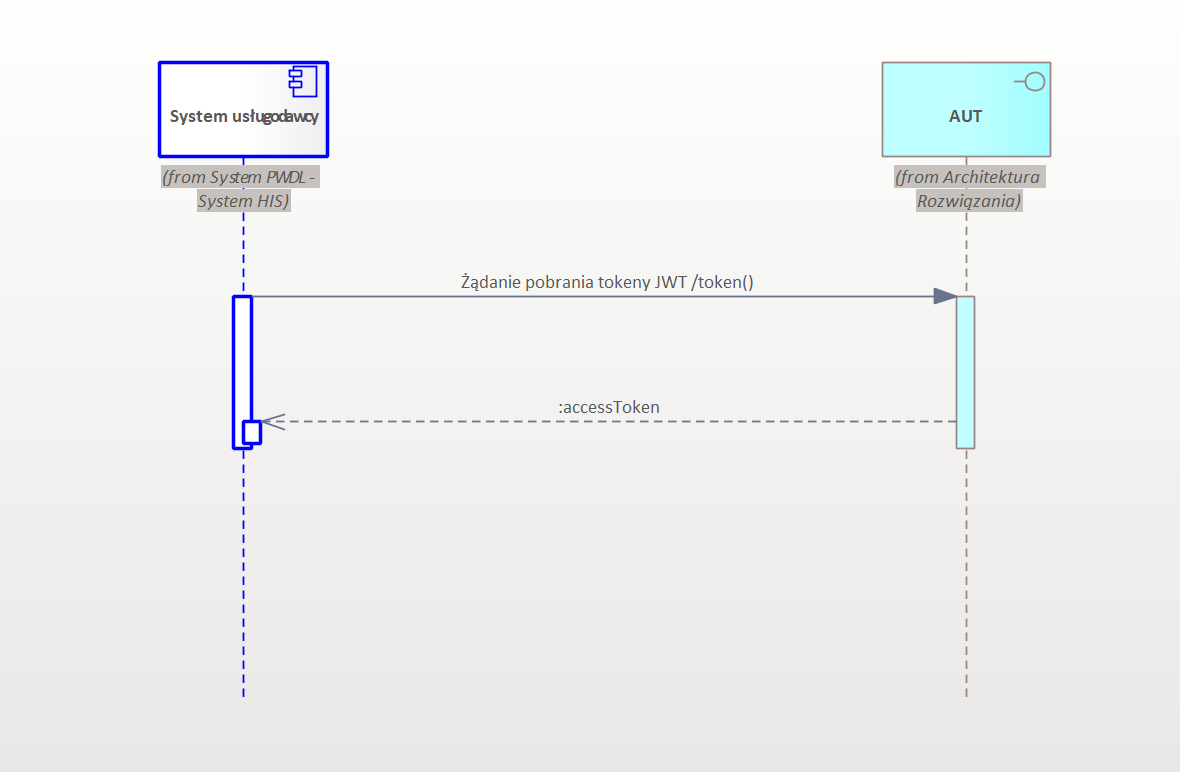
**TOKEN DOSTĘPOWY** obejmuje dane autoryzacyjne Usługodawcy, w tym uwierzytelniony identyfikator Usługodawcy oraz jego rolę w Systemie P1.

## Przebieg uwierzytelnienie i autoryzacji dostępu do usług serwera PUI CEZ

Uwierzytelnienie systemu zewnętrznego Usługodawcy (klienta) realizowane jest z użyciem metody **private\_key\_jwt** przedstawionej w [OpenID Connect 1.0](https://openid.net/specs/openid-connect-core-1_0.html#ClientAuthentication).

W procesie uwierzytelnienia i autoryzacji dostępu do usług serwera PUI CEZ system zewnętrzny Usługodawcy (klient) przygotowuje i przekazuje do Systemu P1 (serwera autoryzacyjnego) żądanie autoryzacji zawierające **TOKEN UWIERZYTELNIAJĄCY** (JSON Web Token). Czas jego życia to 900 sekund.

**Pozytywna** odpowiedź na żądanie autoryzacji posiada status **HTTP 200**. W treści odpowiedzi zwrócony jest **TOKEN DOSTĘPOWY** (JSON Web Token).



## Przygotowanie TOKENU UWIERZYTELNIAJĄCEGO

Struktura **TOKEN UWIERZYTELNIAJĄCEGO** obejmuje:

**HEADER.PAYLOAD.SIGNATURE**

Każda z sekcji z osobna zakodowana jest z użyciem **Base64**.

1. **Sekcja HEADER:**

Sekcja nagłówka - obejmuje wskazanie na typ tokenu oraz o algorytm, którym został podpisany token.

Dla tokenu do systemu Zdarzeń Medycznych sekcja nagłówka ma postać:

{

“alg”: “RS256”,

“typ”: ”JWT”

}

gdzie:

* **‘alg**’ - (ang. algorithm) wskazanie na rodzaj użytego algorytmu podczas stosowania podpisu - parametr musi mieć wartość “RS256”.
* **‘typ’** - (ang. type) rodzaj przekazywanego tokenu - parametr musi mieć wartość “JWT”.

1. **Sekcja PAYLOAD:**

Sekcja danych - zawiera dane, które identyfikują system zewnętrzny i pracownika wykonującego operacje w systemie zewnętrznym.

Lista wymaganych parametrów w sekcji jest następująca:

* **‘iss**’ - (ang. issuer) W przypadku uwierzytelnienia AUA identyfikator Aplikacji Usługodawców i Aptek lub w pozostałych przypadkach identyfikator biznesowy (OID) podmiotu (Usługodawcy), który wywołuje usługi serwera FHIR CEZ. Identyfikator biznesowy (OID) podmiotu jest umieszczony w certyfikatach wydanych przez P1 – wartość parametru musi być zgodna z formatem {root}:{extension}.
* **‘sub’** - (ang. subject) identyfikator biznesowy (OID) podmiotu (Usługodawcy), który wywołuje usługi serwera FHIR CEZ. Identyfikator OID podmiotu jest umieszczony w certyfikatach wydanych przez P1 – jeżeli uwierzytelnienie nie dotyczy Aplikacji Usługodawców i Aptek podana wartość parametru musi być zgodna z wartością podaną w atrybucie **‘iss’**.
* ‘**aud**‘ - (ang. audience) adres URL usługi (endpoint) serwera autoryzacji – parametr musi mieć wartość: „<https://ezdrowie.gov.pl/token>”.
* ‘**jti’** - (ang. JWT ID) unikalny identyfikator tokenu do uwierzytelnienia - wartość parametru musi być zgodna z formatem UUID (universally unique identifier).
* **‘exp'** - (ang. expiration time) termin ważności tokenu, po upływie którego token nie może być przetwarzany – wartość parametru musi być zgodna z formatem NumericDate ze specyfikacji JWT (RFC 7519).
* ‘**user\_id**’ - (ang. user identification) identyfikator biznesowy użytkownika (OID) – wartość parametru musi być zgodna z formatem {root}:{extension}.

Zakres identyfikatorów użytkowników dopuszczonych do obsługi Zdarzeń Medycznych w Systemie P1:

* + identyfikator pracownika medycznego art. 17c ust. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia - w przypadku pracownika medycznego;
  + numer PESEL, a w przypadku osób, którym nie nadano numeru PESEL – serię i numer paszportu albo innego dokumentu stwierdzającego tożsamość albo niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2015/1501 – w przypadku osoby niebędącej pracownikiem medycznym upoważnionej przez usługodawcę do przekazywania danych do SIM;
* ‘**user\_role**’ - (ang. user role) - rola użytkownika w systemie zewnętrznym – wartość parametru musi być zgodna z dopuszczalną listą ról.

Zakres ról dopuszczonych do obsługi Zdarzeń Medycznych w Systemie P1:

* LEK – lekarz
  + FEL – felczer
  + LEKD – lekarz dentysta
  + PIEL – pielęgniarka / pielęgniarz
  + POL - położna / położny
  + FARM - farmaceuta
  + RAT - ratownik medyczny
  + PROF - profesjonalista medyczny
  + PADM – pracownik administracyjny
  + ASYS – asystent medyczny
  + FIZJO – fizjoterapeuta
  + DIAG – diagnosta laboratoryjny
  + HIGSZKOL – higienistka szkolna

Dodatkowe parametry opcjonalne umożliwiające dostęp do danych:

* ‘**purpose**’ - (ang. purpose) – tryb dostępu do danych. Wartości dopuszczalne w Systemie P1 to:
  + CONTT – (ang. continuing treatment) – kontynuacja leczenia
  + BTG - (ang. break the glass) – tryb ratowania życia
* **‘con’** – (ang. context) – kontekst użytkownika zalogowanego do Systemu P1 w roli Asystenta Medycznego wskazanego w parametrze **user\_id.** Kontekstem w tym przypadku jest pracownik medyczny wykonujący daną czynność medyczną. W parametrze **user\_id** powinien się znajdowć identyfikator asystenta, natomiast w parametrze **‘con’** identyfikator pracownika medycznego wykonującego daną czynność:
* w przypadku gdy **user\_role = 'ASYS',** parametr jest obowiązkowy i przyjmuje postać: {OID Lekarza/Felczera/Dentysty}:{NPWZ Lekarza/Felczera/Dentysty}, wartość parametru musi być zgodna z formatem {root}:{extension}
* w przypadku gdy **user\_role <> 'ASYS',** parametr nie występuje.
* **‘child\_organization’** - identyfikator biznesowy (OID) miejsca udzielania świadczeń, w ramach którego jest realizowana operacja (odczyt/zapis/wyszukanie/...) w systemie P1. W przypadku, kiedy operacja jest realizowana w jednostce albo komórce organizacyjnej, powinien to być identyfikator jednostki/komórki organizacyjnej. Identyfikator zgodny z HL7 CDA. Przykładowa wartość dla komórki ogranizacyjnej - *2.16.840.1.113883.3.4424.2.3.3:000000001-001*.

1. **SIGNATURE:**

Sekcję **HEADER** oraz **PAYLOAD** należy podpisać z wykorzystaniem klucza prywatnego systemu zewnętrznego (Usługodawcy) zawartego w certyfikacie do uwierzytelnienia danych (WS-Security), wystawionym przez Centrum Certyfikacji P1.

W celu wykonania podpisu można wykorzystać bibliotekę dostępną na <https://github.com/jwtk/jjwt>.

## Przygotowanie i przekazanie żądania autoryzacji

Przekazanie żądania autoryzacji realizowane jest metodą POST (HTTP).

Nagłówek żądania autoryzacji obejmuje następujące parametry:

* **"Content-Type: application/x-www-form-urlencoded"**

Parametry żądania autoryzacji:

* **client\_assertion\_type**: urn:ietf:params:oauth:client-assertion-type:jwt-bearer
* **grant\_type**: client\_credentials
* **client\_assertion**: {**TOKEN UWIERZYTELNIAJĄCY** przygotowany zgodnie z powyższym opisem}.
* **scope**: <https://ezdrowie.gov.pl/pui>

Należy zwrócić uwagę na konieczność kodowania adresu URL zgodnie ze standardem ***Percent*-*encoding****.*

## Zabezpieczenie integralności zasobów Usług Diagnostyki Cyfrowej

Integralność zasobów PUI zabezpieczona jest z wykorzystaniem przekazywania sumy kontrolnej w formacie CRC32. Każdy plik przekazywany oraz udostępniany z Platformy Usług Inteligentnych za pośrednictwem interfejsu posiada wyliczoną sumę kontrolną aby jednoznacznie zweryfikować poprawność przesłanych danych. Suma kontrolna w formacie CRC32 składa z 32 bitowego ciągu znaków przekazywanego w żądaniach interfejsu RESTful API i jest zapisywana w postaci szesnastkowej np. 3AA15537.

## Komunikaty błędów uwierzytelnienia i autoryzacji

|  |  |  |
| --- | --- | --- |
| Kod błędu (Status odpowiedzi HTTP) | Opis słowny | Znaczenie |
| 400 | Błędne żądanie | Podano nieprawidłowe parametry żądania. |
| 401 | Nieautoryzowany dostęp | Wskazany w żądaniu podmiot nie posiada aktywnego konta w Systemie P1 lub nie posiada żadnych uprawnień lub token uwierzytelniający utracił ważność lub sygnatura tokenu jest niepoprawna. |
| 422 | Błąd semantyczny | Żądanie było poprawnie sformułowane, ale było niemożliwe do kontynuowania z powodu semantycznych błędów. |
| 500 | Błąd wewnętrzny | Wystąpił błąd wewnętrzny, który uniemożliwił realizację usługi. |

Tabela 1 Tabela kodów błędów uwierzytelnienia i autoryzacji

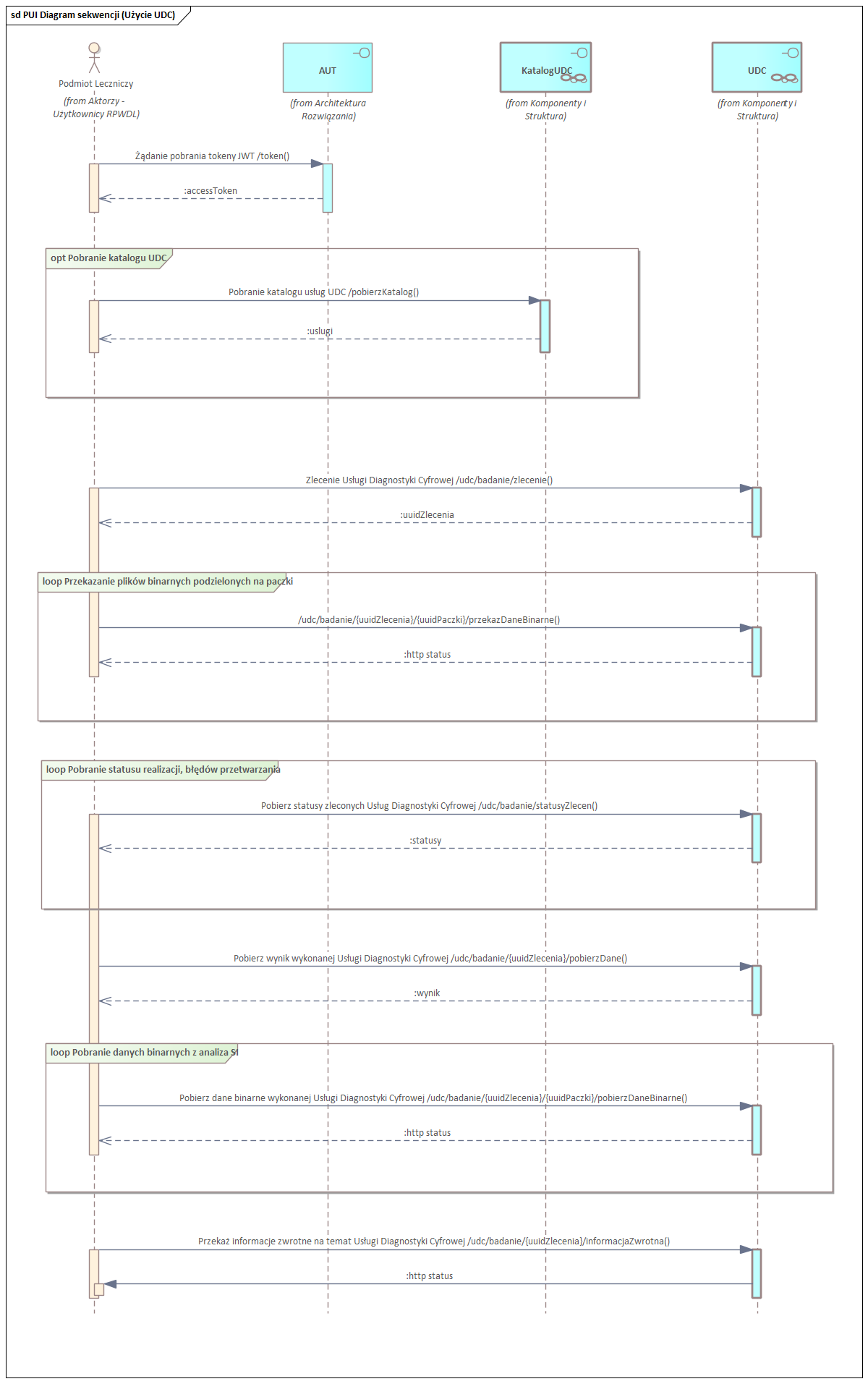
# Opis realizacji Usług Diagnostyki Cyfrowej

Zawiera opis działania usług wraz ze scenariuszami i diagramami sekwencji

# Scenariusz wywołania operacji

Wywołanie operacji przez pracownika odbywa się wg. następujących przypadków:

1. Pobranie raportu:
   1. **Operacja pobrania tokenu dostępowego –** uwierzytelnienie dostępu do systemu P1 w celu pobrania raportów w przypadku gdy nie posiadamy tokenu lub token stracił swoją ważność. Niezbędny do zrealizowania kolejnych etapów scenariusza.
   2. **Operacja pobrania katalogu Usług Diagnostyki Cyfrowej –** operacja pobrania katalogu Usług Diagnostyki Cyfrowej udostępnianych przez Platformę Usług Inteligentnych.
   3. **Operacja zlecenia Usługi Diagnostyki Cyfrowej –** operacja zlecenia odbywa się na podstawie dostępnych Usług Diagnostyki Cyfrowej w ramach katalogu. W ramach operacji przekazywane są dane strukturalne oraz informację na temat potencjalnych danych binarnych jeśli usługa takowych wymaga.
   4. **Operacja przekazania danych binarnych Usługi Diagnostyki Cyfrowej –** operacja przekazania danych binarnych odbywa się po wykonaniu zlecenia Usługi Diagnostyki Cyfrowej jako dodatkowa i integralna część przekazania danych niezbędnych do wykonania usługi, jeśli usługa wymaga danych binarnych.
   5. **Operacja pobrania statusów zleconych Usług Diagnostyki Cyfrowej –** operacja pobrania statusów zleconych Usług Diagnostyki Cyfrowej odbywa się po wykonaniu zlecenia oraz przekazania danych binarnych. Status zlecenia determinuje możliwość pobrania wyników oraz informacji zwrotnej na temat zrealizowanej usługi.
   6. **Operacja pobrania danych –** operacja pobrania danych Usługi Diagnostyki Cyfrowej wykonywana jest w momencie, gdy usługa została zrealizowana. W ramach operacji zwracane są informację na temat danych binarnych, jeśli usługa takowe zwraca.
   7. **Operacja pobrania danych binarnych –** operacja pobrania danych binarnych Usługi Diagnostyki Cyfrowej jest możliwa w momencie poprawnego zakończenia realizacji oraz zwrócenia informacji o dostępnych danych binarnych.
   8. **Operacja przekazania informacji zwrotnej –** operacja przekazania informacji zwrotnej na temat zrealizowanej Usługi Diagnostyki Cyfrowej.



# Wykaz operacji

Platforma Usług Inteligentnych udostępnia poniższe operacje:

|  |  |
| --- | --- |
| Nazwa operacji | Metoda |
| Operacja pobrania tokenu dostępowego | /token |
| Operacja pobrania katalogu Usług Diagnostyki Cyfrowej | ext/v1/udc/katalog/pobierzKatalog |
| Operacja zlecenia Usługi Diagnostyki Cyfrowej | ext/v1/udc/badanie/zlecenie |
| Operacja przekazania danych binarnych w ramach Usługi Diagnostyki Cyfrowej | ext/v1/udc/ badanie /{uuidZlecenia/{uuidPaczki}/przekazDaneBinarne |
| Operacja pobrania statusów zleconych Usług Diagnostyki Cyfrowej | ext/v1/udc/badanie /statusyZlecen |
| Operacja pobrania danych wykonanej Usługi Diagnostyki Cyfrowej | ext/v1/udc/badanie/{uuidZlecenia}/pobierzDane |
| Operacja pobrania danych binarnych wykonanej Usługi Diagnostyki Cyfrowej | ext/v1/udc/badanie/{uuidZlecenia}/pobierzDaneBinarne |
| Operacja przekazania informacji zwrotnej na temat zrealizowanej Usługi Diagnostyki Cyfrowej | ext/v1/udc/badanie/{uuidZlecenia}/informacjaZwrotna |

Tabela 2 Wykaz operacji udostępnionych w zakresie realizacji usług diagnostyki cyfrowej

# Operacja pobrania tokenu dostępowego

Operacja pobrania tokenu dostępowego polega na wywołaniu metody **/token** podając w żądaniu odpowiednie dane dotyczące tokena opisane w rozdziale 3. Sekcja Przygotowanie tokenu uwierzytelniającego

W odpowiedzi zwracany jest token dostępowy, którego należy używać w następnych operacjach.

Operacja pobierania tokenu dostępowego działa w analogiczny sposób jak przy wymianie **Zdarzeń Medycznych**. Możliwe jest wykorzystanie implementacji procesu uwierzytelniania zwracając uwagę na wartość parametru **scope** w żądaniu.

Opis parametrów żądania pokazany jest w rozdziale 3 dokumentu w sekcji Przygotowanie i przekazanie żądania autoryzacji

**Przykładowe żądanie:**

POST /token HTTP/1.1

Content-Type: application/x-www-form-urlencoded

**Parametry wywołania:**

client\_assertion\_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer&

grant\_type=client\_credentials&

client\_assertion= eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiIyLjE2Ljg0MC4xLjExMzg4My4zLjQ0MjQuMi4zLjE6MDAwMDAwMDEyMTA2IiwiYXVkIjoiaHR0cHM6Ly9lemRyb3dpZS5nb3YucGwvdG9rZW4iLCJ1c2VyX3JvbGUiOiJMRUsiLCJ1c2VyX2lkIjoiMi4xNi44NDAuMS4xMTM4ODMuMy40NDI0LjEuMS42MTY6MTIzNDU2Nzg5MTAiLCJwdXJwb3NlIjoiQlRHIiwiaXNzIjoiMi4xNi44NDAuMS4xMTM4ODMuMy40NDI0LjIuMy4xOjAwMDAwMDAxMjEwNiIsImV4cCI6IjE2NTM4NTc5MjAiLCJjaGlsZF9vcmdhbml6YXRpb24iOiIyLjE2Ljg0MC4xLjExMzg4My4zLjQ0MjQuMi4zLjM6MDAwMDAwMDEyMTA2LTAwMSIsImp0aSI6IjQ0MWM0OTZhLTMyOGUtNDBjYy04OGJkLWNjYzk0OWZjOGQxMCJ9.CSIvYxBZqbufrD8EAR1VzSbQfx3lJ8wqXvz7buGOv26-4fF66oEnFIroaDuqFWOWTto0lSDGDKbgJT-Q-MjDqP-uAr1uU638zkpZT0cXqMGxcxyqKlZySyb0N2WiMBwvGwn10auwV9FWQGYuWXjxfj\_XQtvYCqzxJ3Dqfo2zCTziVCvzIavoXNJmSpyibmL00EHnRVAirjNcBKVZV0PKy0vMRKQgSwymjKwajY8y7ttUigyTedNr\_XONh-VX7OKszuwnRoFC0bnfZFi1co-agpMPbI4WTsbXgryqhgThkHHmTyD-apW7AjxR7N3eltZYWuPtGVCPqXKzZBbKHNYoug&

scope=https://ezdrowie.gov.pl/fhir

Przykładowa odpowiedź:

{

"error": null,

"accessToken": "TOKEN\_DOSTEPOWY"

}

# Operacje scenariusza Realizacji Usług Diagnostyki Cyfrowej

Opis zawierający sposób wywołania operacji Usług Diagnostyki Cyfrowej znajduje się w pliku pui-proces.yaml oraz pui-katalog-udc.yaml dostarczonym wraz z tą dokumentacją. Zawartość pliku zawiera specyfikację kontraktu w standardzie OpenAPI 3.0.3.