Dokumentacja integracyjna Systemu P1

W zakresie udostępnienia danych potwierdzających szczepienie/ozdrowienie/test

„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 | 26 | | |
| Zatwierdzający | CeZ | **Data zatwierdzenia** | 2021-01-xx |
| Wersja | 1.3 | **Status dokumentu** | Zaakceptowany |
| Data utworzenia | 2021-01-11 | **Data ostatniej modyfikacji** | 2021-05-28 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Historia zmian** | | | |
| **Data** | **Wersja** | **Autor zmiany** | **Opis zmiany** |
| 2021-01-11 | 1.0 | CeZ | Wersja inicjalna dokumentu |
| 2021-01-19 | 1.1 | CeZ | Modyfikacja rozdziału „Adresy usług” |
| 2021-05-26 | 1.2 | CeZ | 1.Wycofanie operacji umożliwiającej pobieranie dowodu szczepienia *pobierzDowodSzczepieniaSzczepienieId.*  2.Dodanie operacji umożliwiającej pobranie pliku PDF zawierającego EU DIGITAL COVID CERT |
| 2021-05-28 | 1.3 | CeZ | Poprawki edytorskie |

| Dokumenty powiązane | |
| --- | --- |
| Nazwa pliku | P1-DS-Z1-Wniosek\_o\_nadanie uprawnien\_srodowisko\_integracyjne.docx |
| Zakres | Załącznik nr 1 - szablon wniosku o nadanie uprawnień do środowiska integracyjnego |
| Nazwa pliku | P1-DS-Z2-Plik\_REST\_20210112 |
| Zakres | Załącznik nr 2 - pliki interfejsu REST |
| Nazwa pliku | P1-DS-Z3\_Kody\_wyników\_operacji.xlsx |
| Zakres | Załącznik nr 3 - kody wyników operacji |

Spis treści

[1. Wstęp 6](#_Toc73052403)

[1.1. Cel i zakres dokumentu 6](#_Toc73052404)

[1.2. Wykorzystywane skróty i terminy 6](#_Toc73052405)

[2. Ogólny opis systemu P1 w zakresie udostępniania kodów QR potwierdzających szczepienie/ozdrowienie/test 9](#_Toc73052406)

[3. Dostęp do systemu P1 10](#_Toc73052407)

[3.1. Opis środowiska integracyjnego 10](#_Toc73052408)

[3.2. Zakres informacyjny wniosku o dostęp do środowiska integracyjnego 10](#_Toc73052409)

[3.3. Przebieg procesu nadawania dostępu do środowiska integracyjnego P1 11](#_Toc73052410)

[4. Dostęp do usług sieciowych 13](#_Toc73052411)

[4.1. Uwierzytelnienie systemu 13](#_Toc73052412)

[4.2. Uwierzytelnienie i autoryzacja do usług serwera CEZ w zakresie udostępnienia danych potwierdzających szczepienie / ozdrowienie / test 14](#_Toc73052413)

[4.2.1. Przebieg uwierzytelnienia i autoryzacji dostępu 14](#_Toc73052414)

[4.2.2. Przygotowanie TOKENA UWIERZYTELNIAJĄCEGO 15](#_Toc73052415)

[4.2.3. Przygotowanie i przekazanie żądania autoryzacji 17](#_Toc73052416)

[4.2.4. Komunikaty błędów uwierzytelnienia i autoryzacji 17](#_Toc73052417)

[5. Wykaz i opis usług 19](#_Toc73052418)

[5.1. Wykaz usług na środowisku integracyjnym 19](#_Toc73052419)

[5.2. Usługa System weryfikacji szczepień 19](#_Toc73052420)

[5.2.1. Operacja pobierzWydrukDigitalGreenCertificate 19](#_Toc73052421)

[6. Adresy usług 22](#_Toc73052422)

[7. Procedury 23](#_Toc73052423)

[7.1. Procedura nadania uprawnień Usługodawcy 23](#_Toc73052424)

[7.2. Sposób zgłaszania błędów i zagadnień 23](#_Toc73052425)

[8. Informacje uzupełniające 25](#_Toc73052426)

[9. Indeks tabel 26](#_Toc73052427)

# Wstęp

## Cel i zakres dokumentu

Niniejsze opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie udostępnienia plików PDF zawierających kody QR potwierdzających:

* Przyjęcie szczepionki na COVID-19, **albo**
* Negatywny wynik testu na COVID-19, **albo**
* Przebycie choroby COVID-19 (ozdrowienie)

Dla potrzeb przedmiotowej integracji CEZ udostępnia dedykowane w systemie P1 środowisko integracyjne zasilone danymi testowymi. Projekt testowy z przykładowymi żądaniami jest załącznikiem do niniejszego dokumentu. Ponadto w dokumencie przedstawione zostały procedury związane z uzyskaniem uprawnień do systemu P1, wraz z szablonem wniosku, oraz sposób zgłaszania do CEZ błędów i zagadnień.

Dokument obejmuje swoim zakresem specyfikację usług związanych z odczytem plików PDF zawierających kody QR wraz z metadanymi.

## Wykorzystywane skróty i terminy

Tabela 1. Wykorzystywane skróty i terminy

| Lp. | Skrót / termin | Wyjaśnienie skrótu / terminu |
| --- | --- | --- |
|  | CEZ | Centrum e-Zdrowia. |
|  | Certyfikat do uwierzytelnienia systemu | Certyfikat zdefiniowany w Art. 2 ust. 3a) Ustawy o SIOZ, używany do uwierzytelnienia systemu zewnętrznego w warstwie transportowej (TLS). |
|  | Certyfikat do uwierzytelnienia danych | Certyfikat zdefiniowany w Art. 2 ust. 3) Ustawy o SIOZ, używany do potwierdzenia pochodzenia i integralności danych przesyłanych przez system zewnętrzny (podpis komunikatu WS-Security). |
|  | Centrum Certyfikacji P1 | Komponent systemu P1 wystawiający certyfikaty cyfrowe na potrzeby komunikacji systemów zewnętrznych z systemem P1 oraz wzajemnego uwierzytelniania systemów teleinformatycznych Usługodawców. |
|  | System P1 | System pn.: „ELEKTRONICZNA PLATFORMA GROMADZENIA, ANALIZY I UDOSTĘPNIANIA ZASOBÓW CYFROWYCH O ZDARZENIACH MEDYCZNYCH", o którym mowa w Ustawie o SIOZ. |
|  | System zewnętrzny | System Usługodawcy lub innego podmiotu komunikujący się z systemem P1. |
|  | Środowisko integracyjne P1 | Środowisko dedykowane dla dostawców oprogramowania przeznaczone do testowania aplikacji w zakresie komunikacji z systemem P1. |
|  | Ustawa o SIOZ | Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. |
|  | Usługodawca | Podmiot w rozumieniu art. 2 pkt 15 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2011, nr 113, poz. 657 z późn. zm.). |
|  | Wnioskodawca | Dostawca oprogramowania, w tym Usługodawca wytwarzający oprogramowanie na własne potrzeby, wnioskujący o nadanie uprawnień do środowiska integracyjnego systemu P1. |
|  | Zasób | Pakiet danych odnoszący się do różnych pojęć klinicznych obejmujący: problemy zdrowotne, leczenie, diagnostykę, plany opieki, problemy finansowe a także pojęcia administracyjne takie jak: zdarzenie medyczne, procedura, rozpoznanie, pacjent, świadczeniodawca, organizacja i urządzenie. |
|  | Token do uwierzytelnienia | Token JWT przekazywany przez system zewnętrzny do serwera uwierzytelniającego. |
|  | Token dostępu (ACCESS TOKEN) | Token JWT przekazywany przez serwer uwierzytelniający w odpowiedzi na żądanie uwierzytelnienia. Token dostępu jest wymagany w żądaniach przekazywanych do serwera CEZ. |
|  | Serwer autoryzacyjny | Serwer obsługujący żądania autoryzacji - odpowiedzialny za generowanie tokenów dostępu. |
|  | DGC | Digital Green Certificate, Certyfikat generowany w postaci kodu QR, zgodnie ze specyfikacją: <https://github.com/ehn-digital-green-development/hcert-spec> potwierdzający zaszczepienie przeciw COVID-19, negatywny wynik testu na COVID-19 lub przebycie choroby COVID-19 (ozdrowienie) |
|  | EU DIGITAL COVID CERT | Patrz: DGC. |

# Ogólny opis systemu P1 w zakresie udostępniania kodów QR potwierdzających szczepienie/ozdrowienie/test

Celem Projektu P1 jest budowa elektronicznej platformy usług publicznych w zakresie ochrony zdrowia, umożliwiającej organom publicznym, w tym administracji państwowej i samorządowej, przedsiębiorcom i obywatelom na gromadzenie, analizę i udostępnianie zasobów cyfrowych o zdarzeniach medycznych.

Wygenerowane zaświadczenie będzie mogło zostać zweryfikowane za pomocą dedykowanej aplikacji („Zaszczepieni”) uruchamianej na urządzeniach mobilnych przygotowywanej przez Centrum e-Zdrowia.

Usługa ma na celu wspomagać otrzymanie kodu QR potwierdzającego szczepienie albo przebycie choroby albo negatywny wynik testu. Dzięki usłudze, Usługobiorca będzie mógł otrzymać kod QR w gabinecie.

# Dostęp do systemu P1

Dostęp do środowiska integracyjnego P1 przydzielany jest Wnioskodawcom, na podstawie złożonego do CEZ wniosku, opracowanego według szablonu stanowiącego załącznik do przedmiotowego dokumentu.

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

## Opis środowiska integracyjnego

Na środowisku integracyjnym utrzymywane są komponenty systemu P1 w wersji przeznaczonej dla dostawców oprogramowania, którzy pracują nad dostosowaniem swoich systemów informatycznych do funkcjonalności wytwarzanej w obszarze kodów QR potwierdzających szczepienie. Środowisko zasilone jest danymi testowymi pozwalającymi na przeprowadzenie testów komunikacji systemu P1 z Systemami zewnętrznymi.

CEZ w ramach prac konserwacyjnych zastrzega sobie możliwość usuwania danych zapisanych w tym środowisku w celu zapewnienia dostępności i prawidłowego działania systemu. W ramach prac utrzymaniowych (np. w związku z wdrażaniem zmian) możliwe są krótkotrwałe niedostępności systemu, które nie wymagają powiadamiania Wnioskodawców.

Na środowisku integracyjnym systemu P1 nie są przechowywane dane osobowe, dane medyczne czy inne dane wrażliwe.

## Zakres informacyjny wniosku o dostęp do środowiska integracyjnego

Wzór wniosku o dostęp do środowiska integracyjnego systemu P1 zawiera załącznik nr 1. Zakres informacyjny wniosku obejmuje:

1. Dane podmiotu, który wnioskuje o dostęp.
2. Wskazanie w jakiej roli podmiot będzie komunikował się z systemem P1[[1]](#footnote-2) (na formularzu dostępne do wyboru role: „**System zewnętrzny apteki**”[[2]](#footnote-3) oraz „**System zewnętrzny podmiotu leczniczego**”[[3]](#footnote-4)).
3. Wskazanie adresu email, na który przekazane zostaną dane uwierzytelniające wygenerowane po stronie CEZ, oraz który zostanie wykorzystany do innej niezbędnej komunikacji z podmiotem.
4. Wskazanie numeru telefonu komórkowego, na który poprzez SMS przekazane zostaną hasła niezbędne do odblokowania danych uwierzytelniających.
5. Akceptację zasad korzystania ze środowiska integracyjnego.
6. Podpis osoby reprezentującej Wnioskodawcę. Podpis może być wykonany w postaci elektronicznej.

## Przebieg procesu nadawania dostępu do środowiska integracyjnego P1

Nadanie dostępu do środowiska integracyjnego P1 wymaga przekazania do CEZ stosownego wniosku, a następnie po jego pozytywnej weryfikacji następuje:

1. Wygenerowanie dla Wnioskodawcy kompletu kluczy i certyfikatów do zabezpieczania w warstwie TLS oraz WS-Security.
2. Nadanie Wnioskodawcy unikalnego numeru – jest to odpowiednik numeru identyfikacyjnego nadawanego Usługodawcom w produkcyjnym systemie P1.
3. Przekazanie Wnioskodawcy kluczy i certyfikatów do zabezpieczenia komunikacji w warstwie TLS i WS-Security, oraz informacji niezbędnych do przeprowadzenia integracji ze środowiskiem integracyjnym systemu P1.
4. Przekazanie hasła do odblokowania danych uwierzytelniających.
5. Udostępnienie przykładowych komunikatów żądań i odpowiedzi wraz z zestawem danych testowych.

# Dostęp do usług sieciowych

Usługa sieciowa udostępnienia wydruków PDF zawierających DGC obsługuje komunikaty w oparciu o RESTful API. System zewnętrzny jest zobowiązany do używania pary certyfikatów wystawionych podmiotowi przez Centrum Certyfikacji P1, tj. certyfikatu do uwierzytelnienia systemu (TLS) i certyfikatu do uwierzytelnienia danych (WS-Security).

Aby korzystać z usług sieciowych systemu P1 w zakresie udostępnienia PDF zawierającego DGC należy wykonać następujące czynności:

1. Utworzyć do systemu P1 bezpieczne połączenie TLS z obustronnym uwierzytelnieniem (wykorzystując certyfikat do uwierzytelnienia systemu).
2. Przygotować token uwierzytelniający zgodnie z przekazaną specyfikacją, który podpisany jest z użyciem certyfikatu do uwierzytelnienia danych (token podpisany jest kluczem prywatnym).
3. Przygotować i przesłać do systemu P1 żądanie autoryzacji.
4. Zinterpretować żądanie autoryzacji z systemu P1. W odpowiedzi system zewnętrzny otrzyma token dostępowy, który należy użyć w żądaniu pobrania kodu QR poświadczającego szczepienie.
5. Przygotować i przesłać do systemu P1 żądanie pobrania kodu QR poświadczającego szczepienie.
6. Zinterpretować odpowiedź z systemu P1.

## Uwierzytelnienie systemu

Uwierzytelnienie Systemu zewnętrznego wywołującego usługę systemu P1 następuje w warstwie transportowej połączenia za pomocą protokołu TLS z obustronnym uwierzytelnieniem - oprócz uwierzytelnienia serwera przez system zewnętrzny następuje uwierzytelnienie klienta (Systemu zewnętrznego) przez serwer. Do nawiązania połączenia TLS system zewnętrzny zobowiązany jest użyć certyfikatu do uwierzytelnienia systemu wydanego przez Centrum Certyfikacji P1 (użycie przez klienta P1 klucza prywatnego powiązanego z certyfikatem do uwierzytelnienia systemu przekazanego przez CEZ w wyniku założenia konta).

Użycie tego certyfikatu jest niezbędne również do pobrania dodatkowych informacji o wykorzystaniu usług P1, w tym przykładów komunikatów.

## Uwierzytelnienie i autoryzacja do usług serwera CEZ w zakresie udostępnienia danych potwierdzających szczepienie / ozdrowienie / test

Uwierzytelnienie i autoryzacja dostępu do usług serwera CEZ w zakresie pobrania poświadczenia zawierającego DGC 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 CEZ, system zewnętrzny Usługodawcy (klient) pozyskuje z Systemu P1 (serwera autoryzacji) **TOKEN DOSTĘPOWY**.

Warunkiem uzyskania **TOKENA 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 pobrania kodu QR potwierdzającego szczepienie na serwerze CEZ. **TOKEN DOSTĘPOWY** umieszczany jest w nagłówku HTTP Authorization (**“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 uwierzytelnienia i autoryzacji dostępu

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 CEZ, system zewnętrzny Usługodawcy (klient) przygotowuje i przekazuje do Systemu P1 (serwera autoryzacyjnego) żądanie autoryzacji zawierające **TOKEN UWIERZYTELNIAJĄCY** (JSON Web Token).

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

### Przygotowanie TOKENA UWIERZYTELNIAJĄCEGO

Struktura **TOKENA UWIERZYTELNIAJĄCEGO** obejmuje:

**HEADER.PAYLOAD.SIGNATURE**

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

1. **Sekcja HEADER:**

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

Dla opisywanej usługi 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 tokena - 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) Identyfikator biznesowy (OID) podmiotu (Usługodawcy), który wywołuje usługi serwera 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 CEZ. Identyfikator OID podmiotu jest umieszczony w certyfikatach wydanych przez P1 – 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 tokena do uwierzytelnienia - wartość parametru musi być zgodna z formatem UUID (universally unique identifier).
* **‘exp'** - (ang. expiration time) termin ważności tokena, 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}.
* ‘**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 - inny profesjonalista medyczny
  + FIZJO - fizjoterapeuta
  + DIAG - diagnosta laboratoryjny
  + HIGSZKOL - higienistka szkolna
  + ASYS - Asystent Medyczny

Dodatkowy parametr opcjonalny umożliwiający dostęp do danych w sytuacjach szczególnych:

* ‘**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

1. **SIGNATURE:**

Sekcję **HEADER** oraz **PAYLOAD** należy podpisać z wykorzystaniem klucza prywatnego systemu zewnętrznego (Usługodawcy) zgodnego z kluczem publicznym zawartym 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/fhir>

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

Przykładowe żądanie autoryzacji znajduje się w projekcie SoapUI załączonym do niniejszego dokumentu.

### 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 uprawnienia lub token uwierzytelniający utracił ważność lub sygnatura tokena jest niepoprawna. |
| **422** | Żądanie było poprawnie sformułowane, ale było niemożliwe do kontynuowania z powodu semantycznych błędów. | Podano nieprawidłowe parametry tokena autoryzacyjnego. |
| **500** | Błąd wewnętrzny | Wystąpił błąd wewnętrzny, który uniemożliwił realizację usługi. |

# Wykaz i opis usług

## Wykaz usług na środowisku integracyjnym

Na środowisku integracyjnym systemu P1 udostępnione są:

1. usługa System weryfikacji szczepień, z operacjami:
   1. ~~pobierzDowodSzczepieniaSzczepienieId~~ (operacja wycofana)
   2. pobierzWydrukDigitalGreenCertificate

## Usługa System weryfikacji szczepień

Usługa *System weryfikacji szczepień* grupuje operacje związane z generowaniem i udostępnianiem kodów QR poświadczających szczepienie, negatywny wynik testu lub przebycie choroby (ozdrowienie).

### Operacja pobierzWydrukDigitalGreenCertificate

Operacja *pobierzWydrukDigitalGreenCertificate* służy do pobrania pliku PDF zawierającego kod QR (DGC), potwierdzający zaszczepienie przeciwko COVID-19, negatywnego wyniku testu na COVID-19 lub potwierdzający przebycie choroby (ozdrowienie).

W celu pobrania pliku PDF z wygenerowanym kodem QR (DGC), w Systemie P1 muszą zostać zarejestrowane szczepienia (zasoby Immunization), ponieważ to na podstawie zrealizowanych szczepień generowane są kody QR (DGC) potwierdzające szczepienie. Kod QR (DGC) poświadczający szczepienie zostanie wygenerowany **już po przyjęciu pierwszej dawki** szczepienia (liczba przyjętych dawek **nie musi** równać się liczbie wszystkich przepisanych dawek do przyjęcia). Dodatkowo wszystkie szczepienia (zasoby Immunization) na podstawie których generowane są kody QR (DGC) potwierdzające szczepienie muszą zostać podpisane elektroniczne przez pracownika wykonującego szczepienie (lub jego asystenta medycznego). Oznacza to, że dla zapisanych szczepień (zasobów Immunization) musi istnieć podpis elektroniczny, który w Systemie P1 jest zapisywany w zasobie Provenance. Sposób zapisu zasobu Immunization oraz Provenance został szczegółowo opisany w dokumencie „Dokumentacja integracyjna Systemu P1 w zakresie obsługi ZM”

Pobranie pliku PDF z wygenerowanym kodem QR (DGC) potwierdzającym negatywny wynik testu na COVID-19 możliwe jest **najwcześniej** po upływie **15 minut** od przesłania przez laboratorium wyniku testu do Systemu P1.

Pobranie pliku PDF z wygenerowanym kodem QR (DGC) potwierdzającym przebycie choroby (dodatni wynik testu na COVID-19) możliwe jest **najwcześniej** po upływie **11 dni** od przesłania przez laboratorium wyniku testu do Systemu P1.

Zakres ról biznesowych, które mają uprawnienia do wywołania operacji pobrania plików PDF zawierających kod QR (DGC):

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

Operacja *pobierzWydrukDigitalGreenCertificate* przyjmuje parametry:

1. Authorization – token dostępowy, który został uzyskany z Systemu P1 na podstawie żądania autoryzacyjnego.
2. DigitalGreenCertificateInput – obiekt zawierający:
   1. idUzytkownika – identyfikator biznesowy Usługobiorcy w formacie OID (np.: PESEL, numer paszportu), dla którego ma zostać wygenerowany plik PDF zawierający kod QR (DGC).
   2. typCertyfikatu – atrybut definiuje typ certyfikatu, dla którego ma zostać wygenerowany kod QR (DGC). Akceptowalne wartości:
      1. VACCINATION – dla kodu QR (DGC) potwierdzającego szczepienie
      2. TEST\_RESULT – dla kodu QR (DGC) potwierdzającego negatywy wynik testu
      3. RECOVERY – dla kodu QR (DGC) potwierdzającego przebycie choroby (ozdrowienie)

W rezultacie, użytkownik wywołujący operację otrzymuje:

* wynik – wynik operacji, który składa się z:
  + major – kod główny wyniku,
  + minor – kod uzupełniający wyniku,
  + komunikat – treść komunikatu związanego z wynikiem operacji
  + status – status HTTP odpowiedzi,
* dokumentPdf – binarny plik PDF zakodowany w Base64, zawierający kod QR oraz metadane.

Kody wyników operacji zostały załączone do niniejszego dokumentu.

#### Przykładowy scenariusz wywołania operacji

Poniżej znajduje się przykładowy scenariusz wywołania operacji, zakładający że przed wygenerowaniem kodu QR (DGC) potwierdzającego szczepienie, Usługobiorca przyjął co najmniej jedną dawkę szczepienia.

Scenariusz:

1. Pozyskanie tokena dostępowego na podstawie żądania autoryzacyjnego,
2. Rejestracja pierwszej dawki szczepienia – rejestracja zasobu Immunization w Systemie P1,
3. Zarejestrowane szczepienie w Systemie P1 musi zostać podpisane przez pracownika wykonującego szczepienie (lub jego asystenta) – rejestracja zasobu Provenance w Systemie P1,
4. Pobranie kodu QR potwierdzającego zaszczepienie na podstawie identyfikatora Usługobiorcy (np.: numer PESEL lub numer paszportu).

# Adresy usług

Adresy usług środowiska integracyjnego systemu P1 są dostępne na dedykowanej dla Wnioskodawców stronie.

Adres dla usługi pobrania pliku PDF zawierającego kodu QR (DGC), potwierdzającego szczepienie, negatywny wynik testu lub przebycie choroby (ozdrowienie): https://isus.ezdrowie.gov.pl/sws/digital-green-certificate/wydruk.

# Procedury

## Procedura nadania uprawnień Usługodawcy

Korzystanie ze środowiska integracyjnego wymaga posiadania uprawnień Usługodawcy w systemie P1. Ich uzyskanie jest realizowane zgodnie z poniższą procedurą:

1. Wypełnienie przed Wnioskodawcę wniosku o nadanie uprawnień zgodnie z udostępnionym przez CEZ szablonem.
2. Przekazanie skanu podpisanego wniosku lub podpisanego elektronicznie wniosku na adres **integracja\_p1@cez.gov.pl**.
3. Weryfikacja wniosku przez CEZ[[4]](#footnote-5):

A. *Pozytywna* – przekazanie wniosku do realizacji;

B. *Negatywna* – poinformowanie Wnioskodawcy o konieczności poprawienia wniosku.

1. Przesłanie przez CEZ na email wskazany we wniosku danych uwierzytelniających oraz innych istotnych informacji związanych ze środowiskiem integracyjnym P1.
2. Przesłanie przez CEZ na numer komórkowy wskazany we wniosku SMS-a z hasłami do danych uwierzytelniających.
3. Udostępnienie przez CEZ przykładowych komunikatów żądań i odpowiedzi wraz z zestawem danych testowych.
4. Skonfigurowanie przez Wnioskodawcę połączenia z systemem P1 w oparciu o otrzymane certyfikaty.

## Sposób zgłaszania błędów i zagadnień

W przypadku problemów z działaniem usług systemu P1 lub potrzebą uzyskania dodatkowych informacji niezbędnych do realizacji integracji, istnieje możliwość zgłoszenia błędu/zagadnienia do CEZ. W tym celu należy przesłać zgłoszenie drogą elektroniczną na adres: **integracja\_p1@cez.gov.pl**, przy czym zakres zgłoszenia powinien obejmować informacje umożliwiające jego sprawną obsługę, tj. co najmniej:

**W przypadku zgłoszenia błędu**:

1. Dane kontaktowe (nazwa podmiotu wraz z otrzymanym z Cez numerem Wnioskodawcy, imię i nazwisko zgłaszającego oraz adres e-mail, nr telefonu).
2. Czas wystąpienia błędu: datę, godzinę.
3. Miejsce wystąpienia błędu (np. nazwa operacji).
4. Szczegółowy opis sytuacji, która wywołuje błąd.
5. Załącznik z treścią żądania wysłanego do P1.
6. Załącznik z treścią odpowiedzi otrzymanej od P1.
7. Pliki logów, inne załączniki (maksymalna wielkość załączników to 6MB).

**W przypadku zgłoszenia zapytania**:

1. Dane kontaktowe (nazwa podmiotu, imię i nazwisko zgłaszającego oraz, adres e-mail, nr telefonu).
2. Szczegółowy opis zagadnienia.
3. Opcjonalnie załączniki (maksymalna wielkość załączników to 6MB).

# Informacje uzupełniające

Załącznik nr 1 - Szablon wniosku o nadanie uprawnień

Załącznik nr 2 – Plik interfejsu REST

Załącznik nr 3 – Kody wyników operacji

Załącznik nr 4 – przykładowy projekt testów z żądaniami

# Indeks tabel

Spis tabel

[Tabela 1. Wykorzystywane skróty i terminy 6](#_Toc73052396)

1. Jeżeli Wnioskodawca wnioskuje o jednoczesne nadanie obu ról wówczas otrzyma dwa oddzielne konta podmiotu   
   z dedykowanymi uprawnieniami, certyfikatami i kompletem danych. [↑](#footnote-ref-2)
2. System obsługujący apteki lub punkty apteczne. [↑](#footnote-ref-3)
3. System obsługujący podmioty lecznicze, w tym praktyki zawodowe. [↑](#footnote-ref-4)
4. wniosek musi być podpisany przez osobę uprawnioną do reprezentowania podmiotu [↑](#footnote-ref-5)