

# Definicja wymagań dla Platformy MSIM oraz infrastruktury techniczno- systemowej

Załącznik nr 2 do SOPZ



## Spis treści

1	Wstęp .....	6
1.1	Słownik wymagań .....	7
2	Aplikacje portalowe .....	8
2.1	Portal pacjenta .....	8
2.1.1	Moduł „Uwierzytelnianie użytkownika” .....	8
2.1.2	Moduł „Zarządzanie danymi pacjenta” .....	8
2.1.3	Moduł „Informacje o placówkach medycznych” .....	13
2.1.4	Moduł „Wyszukiwanie i pobieranie dokumentów medycznych” .....	16
2.1.5	Moduł „Informacje o udostępnieniu dokumentów” .....	26
2.1.6	Moduł „Umawianie wizyt” .....	28
2.2	Portal pracownika medycznego .....	36
2.2.1	Moduł „Uwierzytelnianie i zarządzanie kontem użytkownika” .....	36
2.2.2	Moduł „Wyszukiwanie pacjenta” .....	36
2.2.3	Moduł „Informacje o placówkach medycznych” .....	38
2.2.4	Moduł „Wyszukiwanie i pobieranie dokumentów medycznych” .....	41
2.2.5	Moduł „Digitalizacja dokumentu medycznego” .....	51
2.2.6	Moduł „Umawianie wizyt” .....	54
2.3	Wymagania niefunkcjonalne aplikacji portalowych .....	61
2.3.1	Wymagania wydajnościowe .....	61
2.3.2	Wymagania dotyczące dostępności .....	61
2.3.3	Wymagania dotyczące skalowalności .....	64
2.3.4	Wymagania dotyczące bezpieczeństwa i niezawodności .....	65
3	Komponenty usługowe .....	68
3.1	Regionalna baza pacjentów .....	68
3.1.1	Wymagania funkcjonalne .....	68
3.1.2	Model przypadków użycia .....	69
3.1.3	Diagram aktywności .....	69
3.1.4	Model danych .....	71
3.1.5	Komponenty i transakcje .....	72
3.2	Regionalny rejestr dokumentów .....	75
3.2.1	Perspektywa systemów lokalnych .....	75
3.2.2	Wymagania funkcjonalne .....	79
3.2.3	Model przypadków użycia .....	80
3.2.4	Diagram aktywności .....	81
3.2.5	Model danych .....	82

3.2.6	Komponenty i transakcje.....	84
3.3	Regionalne repozytorium dokumentów medycznych.....	86
3.3.1	Wymagania funkcjonalne .....	86
3.3.2	Model przypadków użycia .....	88
3.3.3	Diagram aktywności .....	89
3.3.4	Model danych.....	91
3.3.5	Komponenty i transakcje.....	92
3.4	Walidator dokumentów medycznych .....	99
3.4.1	Wymagania funkcjonalne .....	99
3.4.2	Model przypadków użycia.....	100
3.4.3	Diagram aktywności .....	101
3.4.4	Model danych.....	102
3.4.5	Komponenty i transakcje.....	102
3.5	Komponent wtórnego wykorzystania danych.....	103
3.5.1	Wymagania funkcjonalne .....	103
3.5.2	Model przypadków użycia .....	104
3.5.3	Diagram aktywności .....	104
3.5.4	Model danych.....	105
3.5.5	Komponenty i transakcje.....	107
3.6	Regionalny broker wolnych terminów i rezerwacji.....	109
3.6.1	Wymagania funkcjonalne .....	109
3.6.2	Model przypadków użycia.....	109
3.6.3	Model danych.....	110
3.6.4	Komponenty i transakcje.....	111
3.7	Regionalne repozytorium zdarzeń na potrzeby audytu .....	113
3.7.1	Wymagania funkcjonalne .....	113
3.7.2	Model przypadków użycia.....	114
3.7.3	Model danych.....	115
3.7.4	Komponenty i transakcje.....	116
3.8	Regionalna bramka wymiany dokumentów (bramka XCA).....	117
3.8.1	Wymagania funkcjonalne .....	117
3.8.2	Model przypadków użycia .....	118
3.8.3	Komponenty i transakcje.....	118
3.9	Komponent administracyjny MSIM.....	119
3.9.1	Wymagania funkcjonalne .....	119
3.9.2	Model przypadków użycia .....	121

3.9.3	Model danych .....	123
3.9.4	Komponenty i transakcje .....	127
3.10	Wymagania нефункционалне komponentów usługowych .....	130
3.10.1	Wymagania wydajnościowe .....	130
3.10.2	Wymagania dotyczące skalowalności .....	130
3.10.3	Wymagania dotyczące bezpieczeństwa i niezawodności .....	130
4	Infrastruktura techniczno-systemowa .....	133
4.1	Wymagania ogólne .....	133
4.1.1	Kolokacja .....	133
4.1.2	Konfiguracja ITS .....	135
4.1.3	Wymagania ogólne dot. sprzętu .....	137
4.2	Warstwa sieciowa .....	137
4.2.1	Zapora ogniowa .....	137
4.2.2	Zapora ogniowa – zarządzanie .....	140
4.2.3	Równoważnik obciążenia i WAF .....	143
4.2.4	Przełącznik Ethernet .....	146
4.2.5	Przełącznik Ethernet – zarządzanie .....	148
4.2.6	Przełącznik SAN .....	149
4.3	Warstwa sprzętowa .....	151
4.3.1	Obudowa Blade .....	151
4.3.2	Serwer Blade .....	152
4.3.3	Serwer RACK .....	152
4.3.4	Biblioteka taśmowa .....	153
4.3.5	Deduplikator .....	154
4.3.6	Macierz dyskowa .....	156
4.3.7	HSM .....	157
4.3.8	Bramka SMS .....	158
4.4	Warstwa oprogramowania .....	158
4.4.1	Wymagania ogólne .....	158
4.4.2	Wirtualizator .....	158
4.4.3	Oprogramowanie Kopii Zapasowych .....	160
4.4.4	SIEM .....	161
4.4.5	System operacyjny .....	163
4.4.6	Baza Danych .....	164
4.4.7	Baza Danych dokumentów XML .....	165
4.4.8	Szyna Danych .....	166

4.4.9	Serwer aplikacyjny.....	167
4.4.10	Centralny System Logów .....	167
4.4.11	Antywirus.....	168
4.5	Wydajność .....	170
4.5.1	Liczba realizowanych świadczeń .....	170
4.5.2	Prognozowane wywołania usług aplikacyjnych .....	171
4.5.3	Prognozowana wolumetria danych.....	171
Wykaz rysunków.....		173
Wykaz tabel .....		177

## 1 Wstęp

Dokument zawiera definicję wymagań dla poszczególnych komponentów Platformy MSIM oraz infrastruktury techniczno-systemowej, które muszą zostać zaimplementowane przez Wykonawcę w produktach dostarczanych w ramach realizacji Umowy. Stosując konwencję opisu architektury MSIM, przedstawioną w Załączniku nr 1 do SOPZ, zastosowano grupowanie wymagań dla poszczególnych komponentów Platformy MSIM. W ten sposób informacje zawarte w Załączniku nr 1 i Załączniku nr 2 do SOPZ zapewniają spójny i pełny opis oczekiwań Zamawiającego wobec poszczególnych elementów Platformy MSIM.

W Rozdziałach 2 i 3 przedstawiono opis komponentów Platformy MSIM, dla którego przyjęto ujednoliconą strukturę sposobu opisu w celu zapewnienia przejrzystości dokumentacji. Do opisu wymagań funkcjonalnych dla komponentów Platformy MSIM wykorzystano różne perspektywy modelowania (przypadki użycia, model danych, aktywności, GUI, interfejsy) dzięki którym możliwe jest zrozumienie projektu Platformy MSIM wychodząc od realizowanych przezeń potrzeb - wartości biznesowej dostarczanej przez poszczególne komponenty. W związku z powyższym do opisu komponentów został wykorzystany jednolity szablon poprzez przedstawienie dla każdego z nich poniższych perspektyw modelowania:

1. Wymagania funkcjonalne,
2. Model przypadków użycia,
3. Diagram aktywności,
4. Model danych,
5. Komponenty i transakcje,
6. Model interfejsu użytkownika.

Należy mieć na uwadze, że dla niektórych komponentów Platformy MSIM nie wszystkie perspektywy modelowania zostały opisane i tam, gdzie wartość (tj. wpływ na zrozumienie projektu Platformy MSIM) z zaprezentowania danej perspektywy była znikoma lub nie istniała (np. brak interfejsu GUI), została ona pominięta.

W przypadku Wymagań funkcjonalnych zastosowano identyfikację wymagań, która odpowiada identyfikacji wymagań zawartych w budowanym przez Zamawiającego Modelu Architektury (model w formacie Enterprise Architect Project), tak aby umożliwić pełną identyfikację przedstawionych opisów komponentów z materiałem zawartym w Modelu Architektury. W przypadku opisu Modelu przypadków użycia, Diagramów aktywności, Modelu danych oraz Komponentów i interakcji, w dokumencie zawarte zostały diagramy UML przedstawiające wymienione obszary. Model w formacie Enterprise Architect Project, na bazie którego przygotowano diagramy UML zawarte w niniejszym dokumencie zostanie udostępniony Wykonawcy Platformy MSIM na etapie realizacji Umowy.

Określenie „system” używane w Wymaganiach funkcjonalnych odnosi się do tej aplikacji portalowej lub komponentu usługowego, którego dotyczy dany rozdział niniejszego dokumentu – chyba, że w treści wymagania wskazano inaczej.

W uzupełnieniu przedstawionych wymagań funkcjonalnych w dokumentacji zawarte zostały wymagania нефункциональные, które zostały przedstawione w podziale na Aplikacje portalowe (Rozdział 2.3) oraz Komponenty usługowe (Rozdział 3.10).

W przypadku komponentów zawierających Model interfejsu użytkownika przedstawiono makiety jego ekranów. Są to makiety poglądowe do wykorzystania przez Wykonawcę w procesie realizacji Zamówienia i nie można ich traktować jako zatwierdzonych wersji ostatecznych. Ostateczny kształt makiet GUI zostanie dostarczony przez Wykonawcę na podstawie przeprowadzonej analizy przedwdrożeniowej i zaakceptowane przez Zamawiającego w ramach Projektu wykonawczego MSIM.

W Rozdziale 4 przedstawione zostały wymagania dotyczące infrastruktury techniczno-systemowej, która ma być dostarczona i utrzymywana przez Wykonawcę w ramach realizacji Umowy. Wymagania dotyczące ITS zostały podzielone na następujące grupy:

- Wymagania ogólne – wymagania, które odnoszą się do wszystkich elementów ITS jakie będą dostarczone przez Wykonawcę w ramach realizacji Umowy oraz wymagania dotyczące usługi kolokacji i usługi konfiguracji ITS,
- Warstwa sieciowa – wymagania związane z zapewnieniem komunikacji i bezpieczeństwa infrastrukturalnego dostarczonego rozwiązania,
- Warstwa sprzętowa – wymagania dotyczące ogólnie pojętej infrastruktury serwerowej oraz pamięci masowych, koniecznych dla budowy i uruchomienia Platformy MSIM,
- Warstwa oprogramowania – wymagania dotyczące oprogramowania koniecznego do wytworzenia i uruchomienia oprogramowania Platformy MSIM oraz uruchomienia usług bezpieczeństwa Platformy MSIM,
- Wydajność – wymagania określające minimalne parametry wydajnościowo jakie muszą zostać osiągnięte przez Platformę MSIM po jej wdrożeniu przez cały okres utrzymania Platformy MSIM przez Wykonawcę.

W przypadku urządzeń fizycznych dokument zawiera informacje o oczekiwanej minimalnej liczbie tych urządzeń jakie muszą zostać zaplanowane przez Wykonawcę w architekturze MSIM i dostarczone w ramach realizacji Umowy.

## 1.1 Słownik wymagań

W dokumentacji stosuje się następujące mapowanie skrótów wymagań w zakresie obszarów realizacji umowy zgodnie z poniższą tabelą.

Oznaczenie wymagania	Obszar
<b>FE.</b>	<b>Aplikacje portalowe</b>
<b>FE.MAdm</b>	Moduł (komponent) administracyjny
<b>FE.PPacj</b>	Portal Pacjenta
<b>FE.PPMed</b>	Portal Pracownika Medycznego
<b>FE.NFun</b>	Wymagania нефunkcjonalne FE
<b>BE.</b>	<b>Komponenty usługowe</b>
<b>BE.BGWW</b>	Broker udostępnionych grafików i wolnych terminów
<b>BE.BPac</b>	Regionalna Baza Pacjentów
<b>BE.BPMed</b>	Regionalna Baza Pracowników Medycznych
<b>BE.BPMR</b>	Baza Placówek Medycznych w Regionie
<b>BE.BRUU</b>	Baza Ról i Uprawnień Użytkowników
<b>BE.BRW</b>	Baza rezerwacji wizyt
<b>BE.BUPP</b>	Baza użytkowników portalu pacjenta
<b>BE.RejDM</b>	Regionalny Rejestr Dokumentów
<b>BE.RepoDM</b>	Regionalne Repozytorium Dokumentów
<b>BE.RLA</b>	Repozytorium zdarzeń na potrzeby audytu
<b>BE.WalDM</b>	Walidator Dokumentów

<b>BE.NFun</b>	Wymagania niefunkcjonalne BE
<b>ITS.</b>	<b>Infrastruktura techniczno-systemowa</b>
<b>ITS.WO</b>	Wymagania ogólne
<b>ITS.Siec</b>	Warstwa sieciowa
<b>ITS.Sprz</b>	Warstwa sprzętowa
<b>ITS.Opr</b>	Oprogramowanie
<b>ITS.Wyd</b>	Wydajność

Tabela nr 1.1 Definicja oznaczeń wymagań

## 2 Aplikacje portalowe

### 2.1 Portal pacjenta

#### 2.1.1 Moduł „Uwierzytelnianie użytkownika”

##### 2.1.1.1 Wymagania funkcjonalne

**FE.PPacj.1.** System umożliwia użytkownikowi logowanie się za pomocą Krajowego Węzła Identyfikacji Elektronicznej.

**FE.PPacj.2.** System umożliwia logowanie się za pomocą profilu zaufanego.

#### 2.1.2 Moduł „Zarządzanie danymi pacjenta”

##### 2.1.2.1 Wymagania funkcjonalne

**FE.PPacj.3.** System umożliwia prezentację danych pacjentów, do których danych ma dostęp użytkownik portalu pacjenta.

**FE.PPacj.4.** System umożliwia prezentację danych innych osób, które mają dostęp do danych pacjenta.

**FE.PPacj.5.** System umożliwia nadawanie i odbieranie dostępu do danych pacjenta.

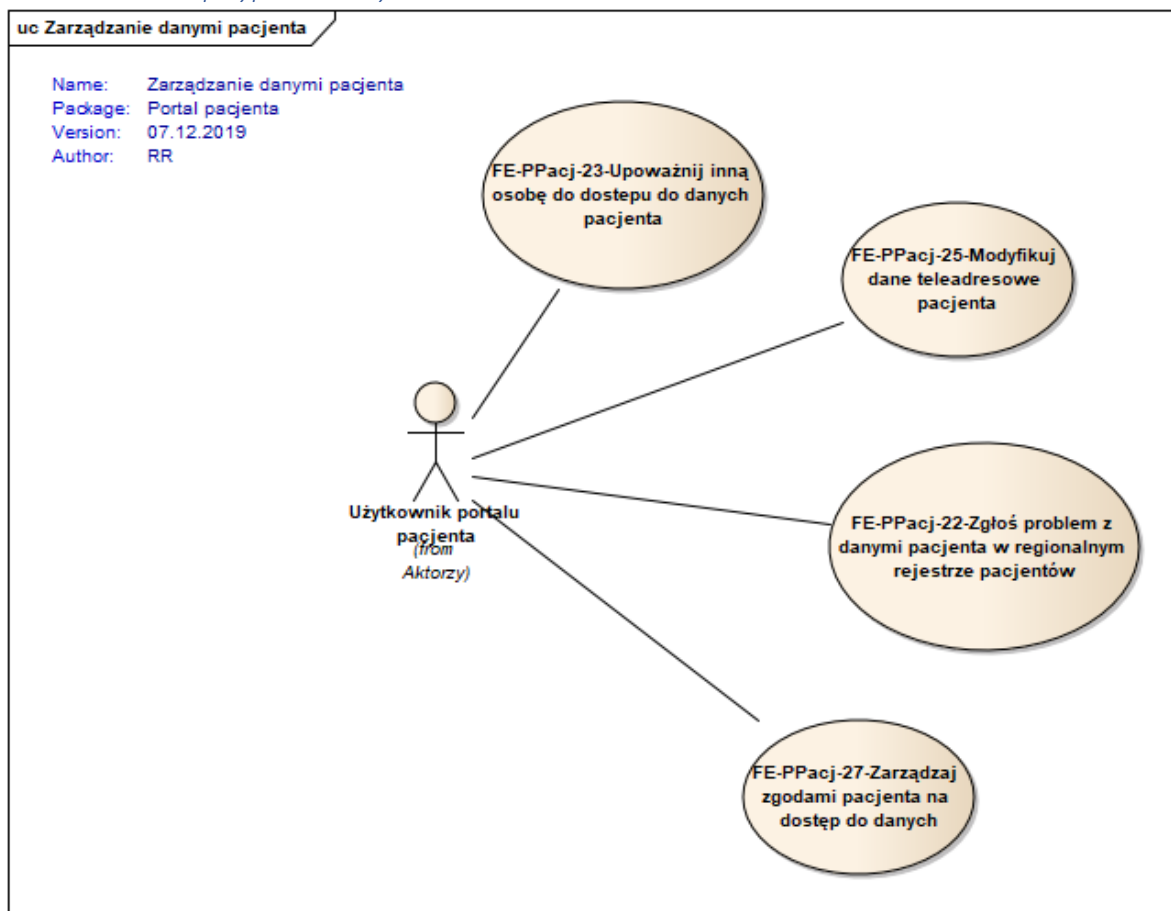
**FE.PPacj.6.** System umożliwia edycję danych kontaktowych pacjenta.

**FE.PPacj.7.** System umożliwia zgłoszenie problemu z danymi pacjenta w regionalnym rejestrze pacjentów.

**FE.PPacj.8.** System umożliwia zarządzanie zgodami pacjenta na dostęp do danych.

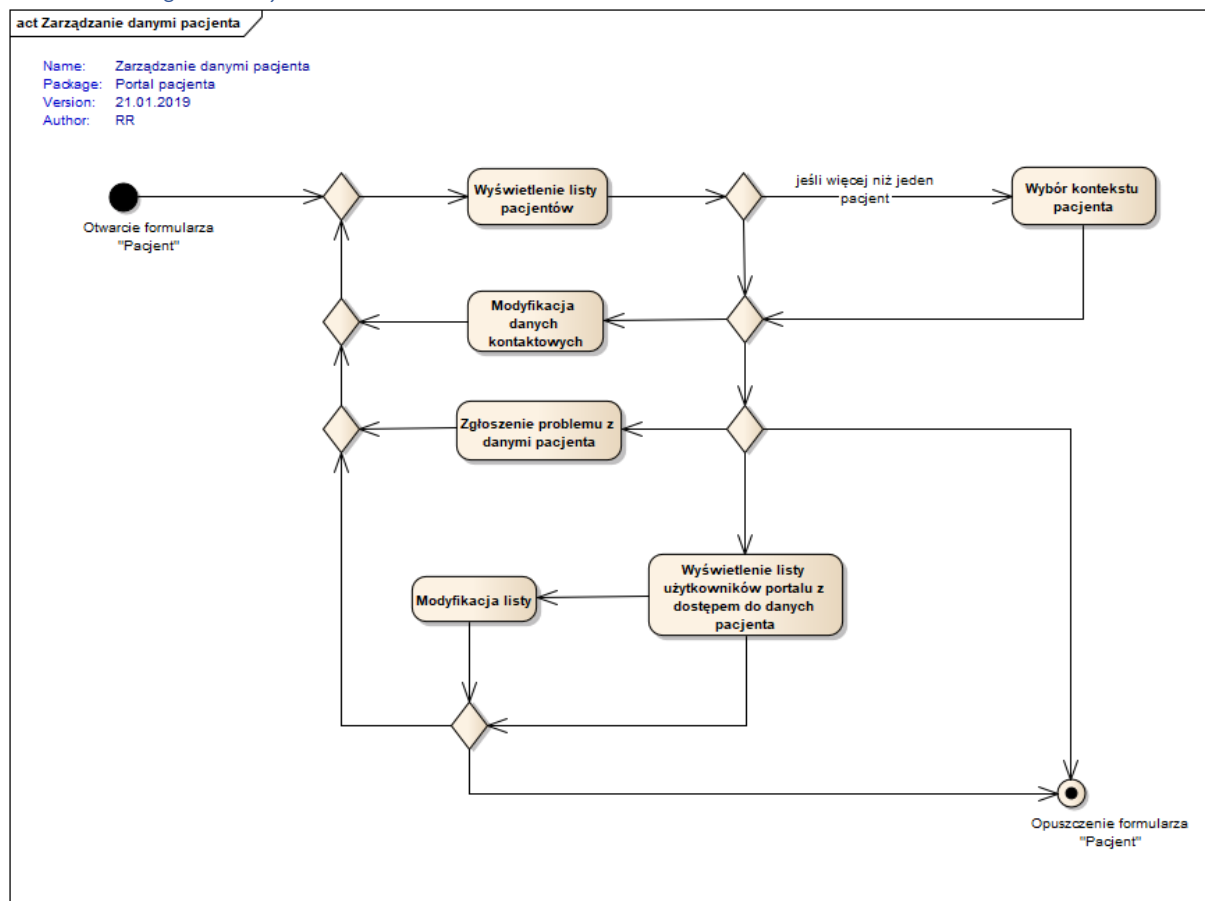


### 2.1.2.2 Model przypadków użycia



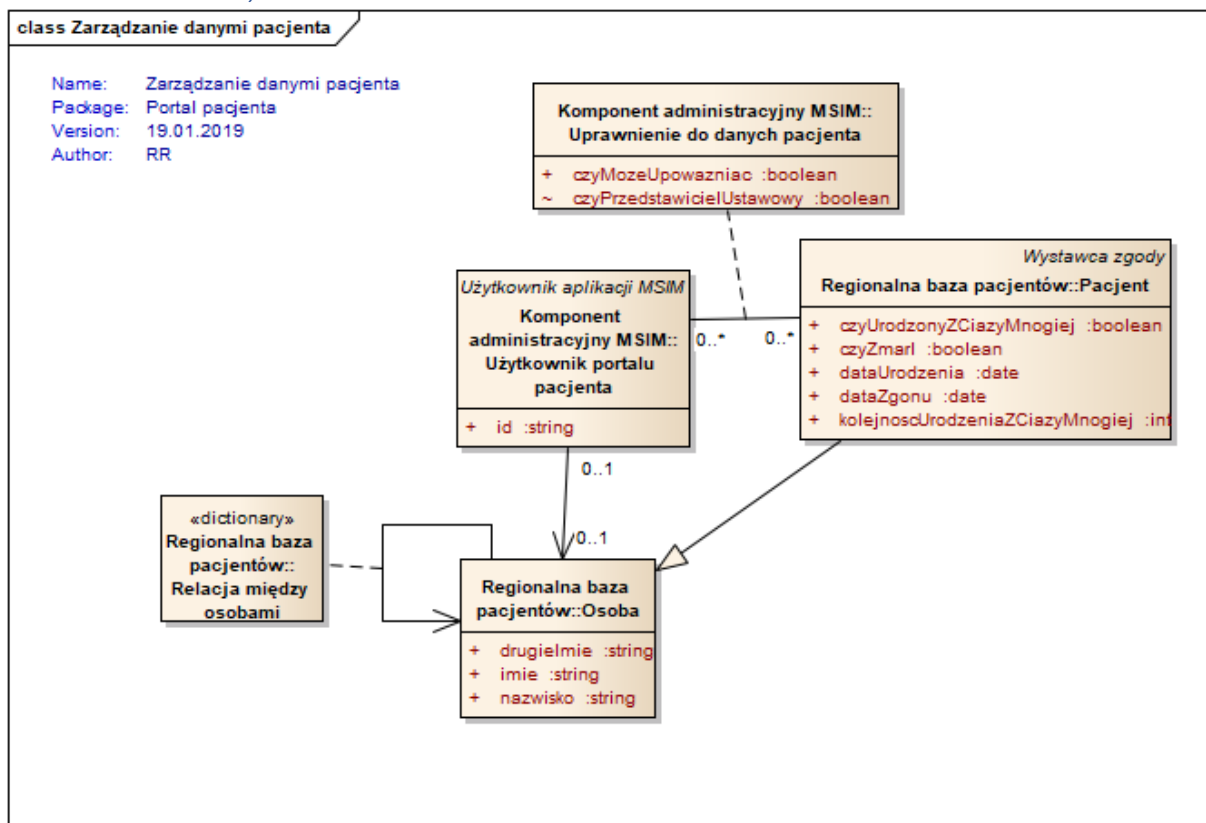
Rysunek nr 2.1 Diagram przypadków użycia obszaru „Zarządzanie danymi pacjenta”

### 2.1.2.3 Diagram aktywności

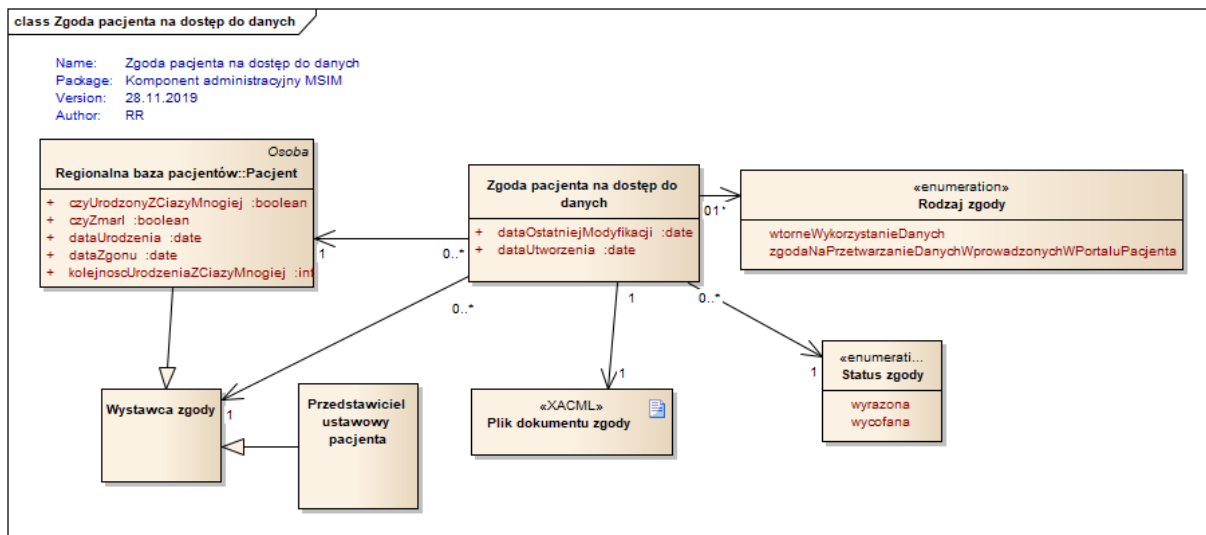


Rysunek nr 2.2 Diagram aktywności obszaru „Zarządzanie danymi pacjenta”

#### 2.1.2.4 Model danych



Rysunek nr 2.3 Diagram klas obszaru „Zarządzanie danymi pacjenta”



Rysunek nr 2.4 Diagram klas obszaru „Zgody pacjenta na dostęp do danych”

### 2.1.2.5 Model interfejsu użytkownika

Pacjent Dokumenty pacjenta Udostępnianie dokumentów Umawianie wizyt Placówki medyczne Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

Maria Kowalska, PESEL 8888888888

Jan Kowalski, PESEL 9999999999

31-567 Kraków, ul. Wiśniowa 2 m 208

telefon: 12 345 67 89 Edytuj

email: mkowalska@gmail.com Edytuj

Tomasz Kowalski, PESEL 7777777777

Zgłoś problem z danymi pacjenta Lista upoważnionych

Zgoda na dostęp do danych

☒ Zgadzam się na przetwarzanie danych wprowadzanych do systemu

☒ Zgadzam się na wtórne wykorzystanie danych z dokumentów medycznych

Data wystawienia zgody: 25.05.2018

Wystawca zgody: Jan Kowalski, PESEL 9999999999

Zapisz

Rysunek nr 2.5 Makieta ekranu „Dane pacjenta”

Zgłoszenie problemu z danymi pacjenta

Pacjent

Jan Kowalski

PESEL

9999999999

Identyfikator regionalny

123456789

Opis problemu

Wpisz tekst zgłoszenia

Anuluj Wyślij zgłoszenie

Rysunek nr 2.6 Makieta ekranu „Zgłoszenie problemu z danymi pacjenta”

Pacjent	Dokumenty pacjenta	Udostępnianie dokumentów	Umawianie wizyt	Placówki medyczne	Wyloguj
---------	--------------------	--------------------------	-----------------	-------------------	---------

**Pacjent: Jan Kowalski, PESEL 9999999999**

Lista użytkowników portalu z dostępem do danych pacjenta

Imię i nazwisko	PESEL	
Marian Kowalski	3333333333	Przedstawiciel ustawowy
Joanna Nowak	2222222222	<a href="#">Anuluj uprawnienie</a>

**Dodaj kolejną osobę**

Rysunek nr 2.7 Makieta ekranu „Lista upoważnionych”

Upoważnienie innego użytkownika portalu pacjenta do dostępu do danych pacjenta

**Pacjent: Jan Kowalski, PESEL**

Dane użytkownika portalu pacjenta

Nazwisko	<input type="text" value="Kowalski"/>
PESEL	<input type="text" value="99999999"/>

☐ Może upoważniać inne osoby

**Upoważniam wskazaną osobę do dostępu do danych pacjenta**

Rysunek nr 2.8 Makieta ekranu „Upoważnienie innego użytkownika”

### 2.1.3 Moduł „Informacje o placówkach medycznych”

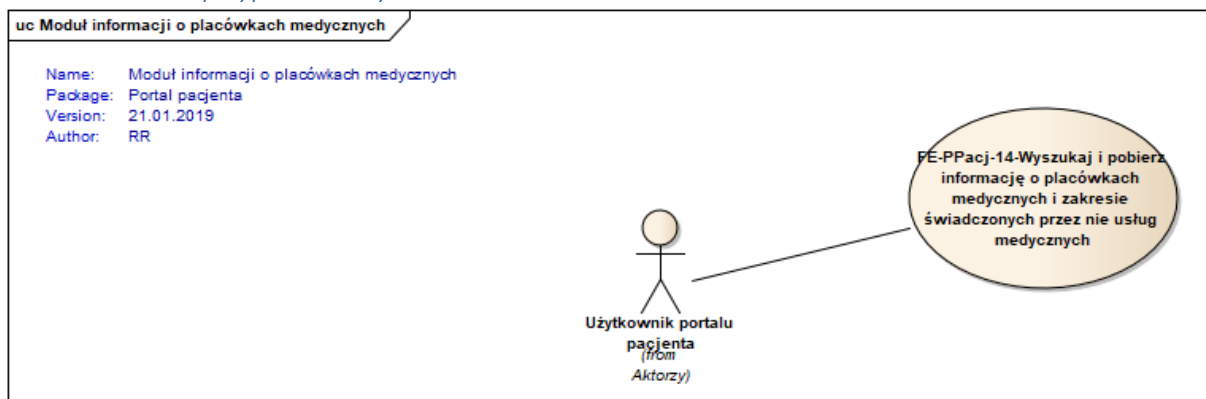
#### 2.1.3.1 Wymagania funkcjonalne

**FE.PPacj.9.** System udostępnia informacje teleadresowe placówek medycznych w regionie.

**FE.PPacj.10.** System udostępnia opis zakresu świadczonych przez placówkę medyczną usług.

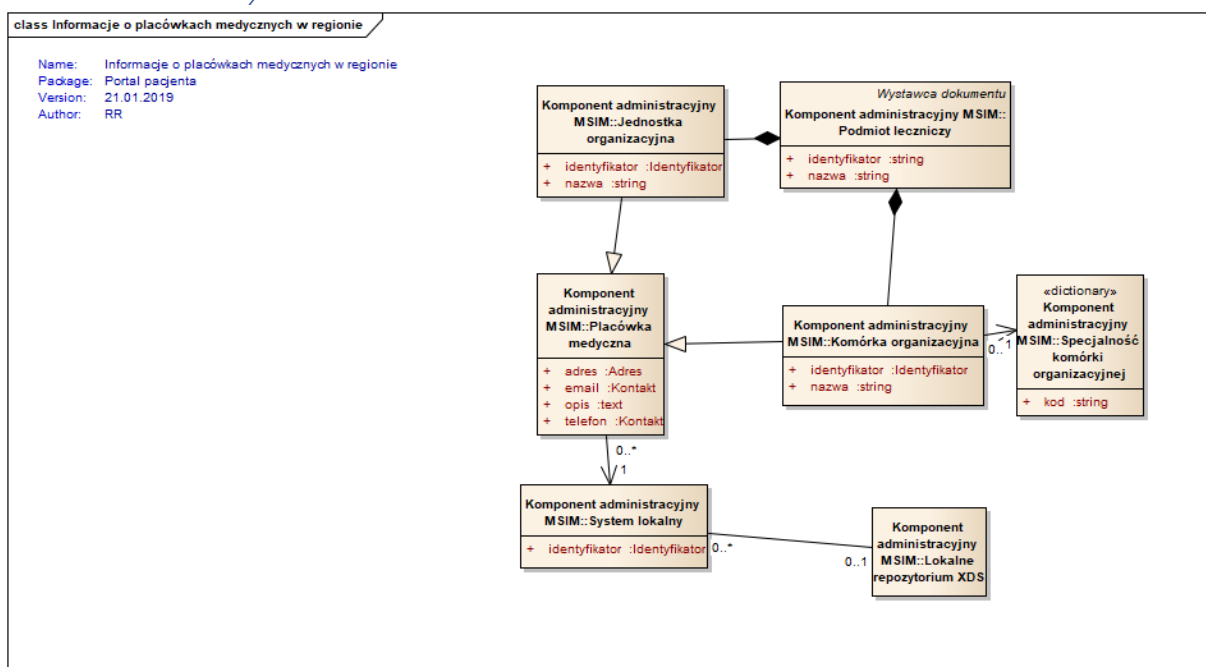
**FE.PPacj.11.** System udostępnia informację o tych usługach medycznych realizowanych przez daną placówkę medyczną, które są dostępne za pomocą e-Rejestracji regionalnej.

### 2.1.3.2 Model przypadków użycia



Rysunek nr 2.9 Diagram przypadków użycia obszaru „Informacje o placówkach medycznych”

### 2.1.3.3 Model danych



Rysunek nr 2.10 Diagram klas obszaru „Informacje o placówkach medycznych”

#### 2.1.3.4 Model interfejsu użytkownika

[Pacjent](#) [Dokumenty pacjenta](#) [Udostępnianie dokumentów](#) [Umawianie wizyt](#) [Placówki medyczne](#) [Wyloguj](#)

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Placówki medyczne](#) > ...

Lista placówek medycznych w regionie

Parametry filtrowania

Miejscowość

☐ Szukaj w pobliżu

Podmiot leczniczy

Specjalność placówki

Nazwa placówki	Miejscowość	Adres	Podmiot leczniczy
<a href="#">Poradnia kardiologiczna</a>	Kraków	os. Złotej Jesieni 1	Szpital Specjalistyczny im. Ludwika Rydygiera
<a href="#">Poradnia neurologiczna</a>	Kraków	Prądnicka 80	Krakowski Szpital Specjalistyczny

Rysunek nr 2.11 Makieta ekranu „Lista placówek”





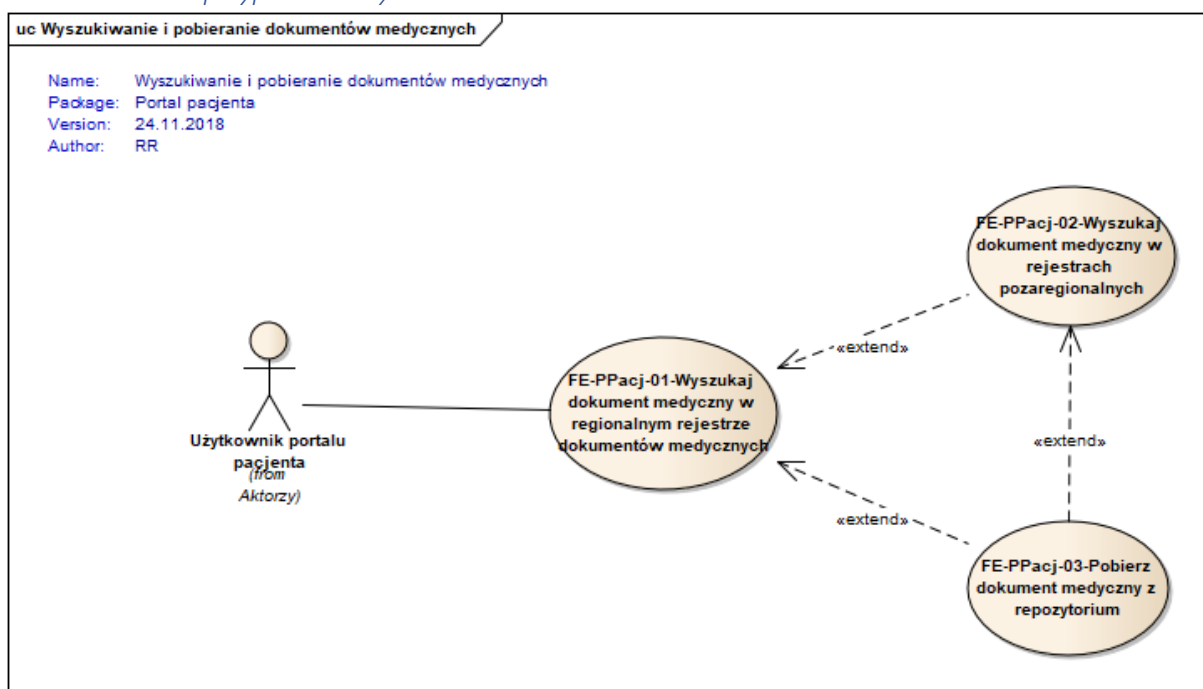
**FE.PPacj.16.** System umożliwia prezentację dokumentu medycznego zgodnego z HL7 CDA lub zapisanego w formacie XACML znajdującego się w repozytorium dokumentów za pomocą transformaty referencyjnej.

**FE.PPacj.17.** System umożliwia prezentację wyniku badania obrazowego w przeglądarce obiektów DICOM.

**FE.PPacj.18.** System umożliwia zapisanie prezentowanego dokumentu medycznego we wskazanej przez użytkownika lokalizacji.

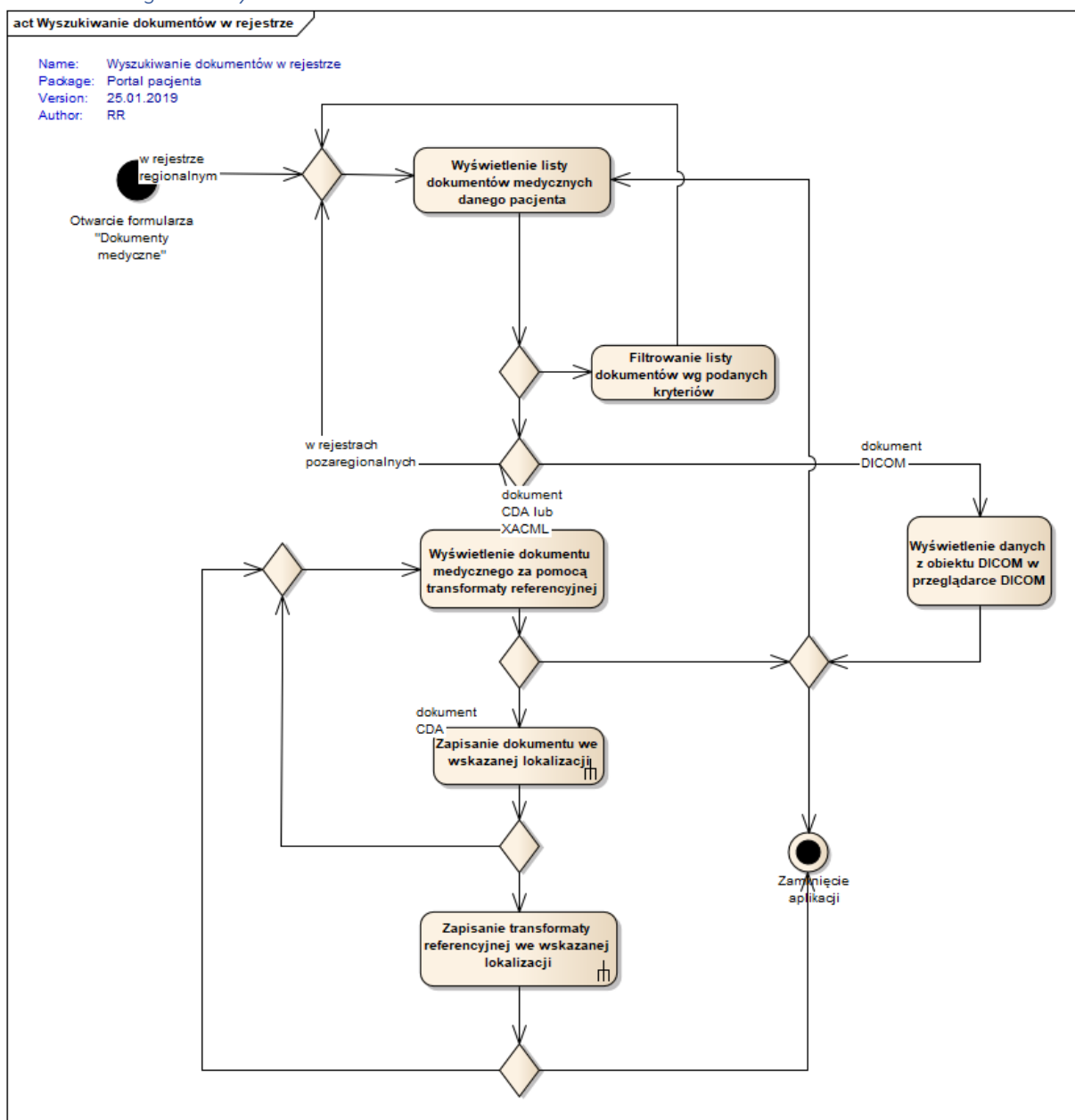
**FE.PPacj.19.** System umożliwia zapisanie transformaty referencyjnej we wskazanej przez użytkownika lokalizacji.

#### 2.1.4.2 Model przypadków użycia



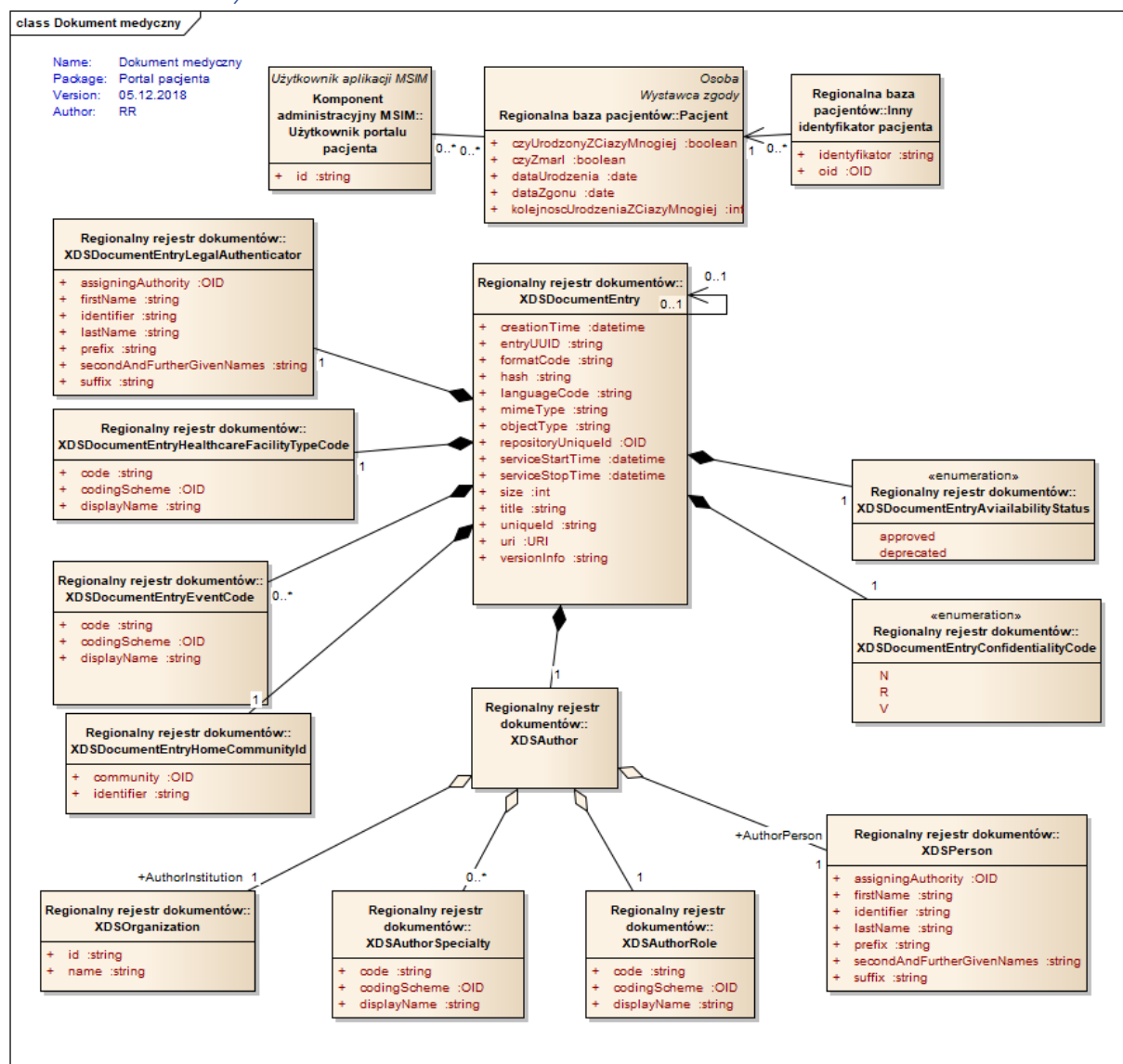
Rysunek nr 2.13 Diagram przypadków użycia obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

### 2.1.4.3 Diagram aktywności



Rysunek nr 2.14 Diagram aktywności obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

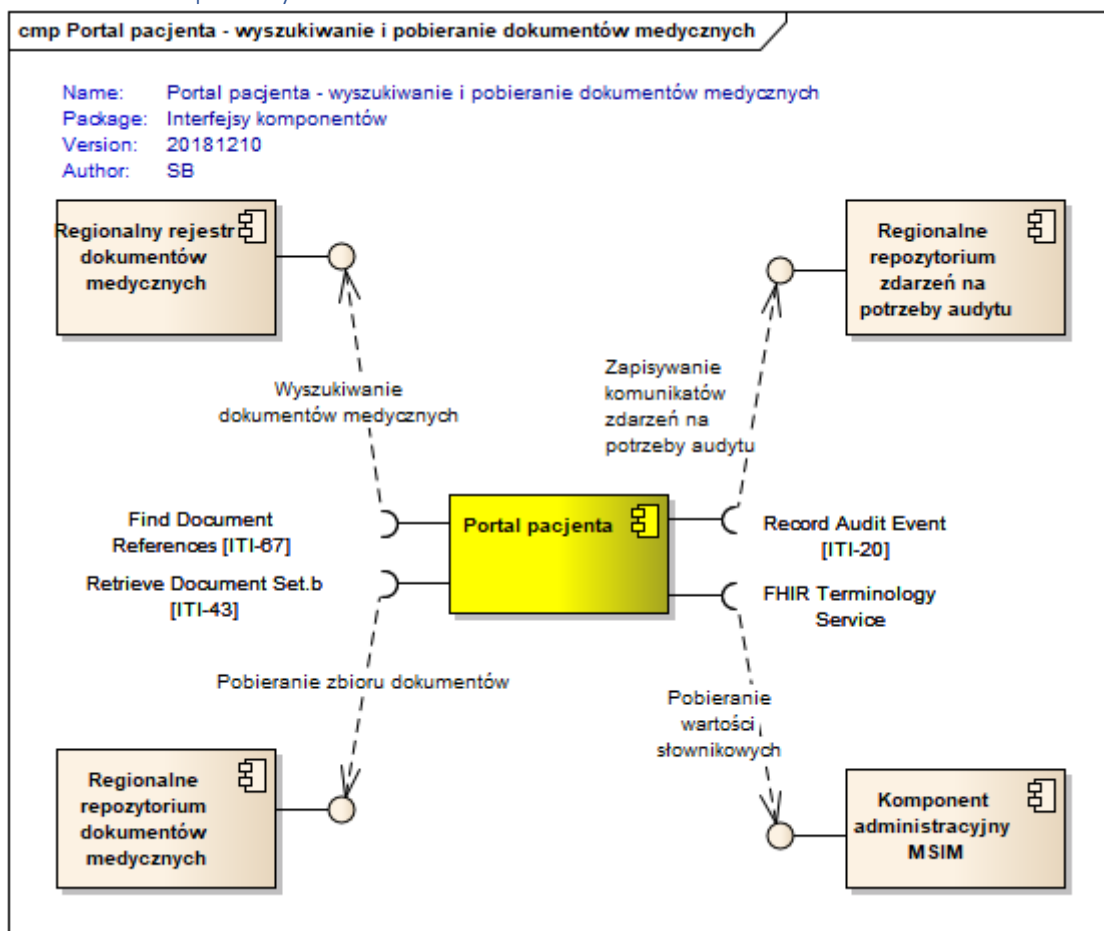
#### 2.1.4.4 Model danych



Rysunek nr 2.15 Diagram klas obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

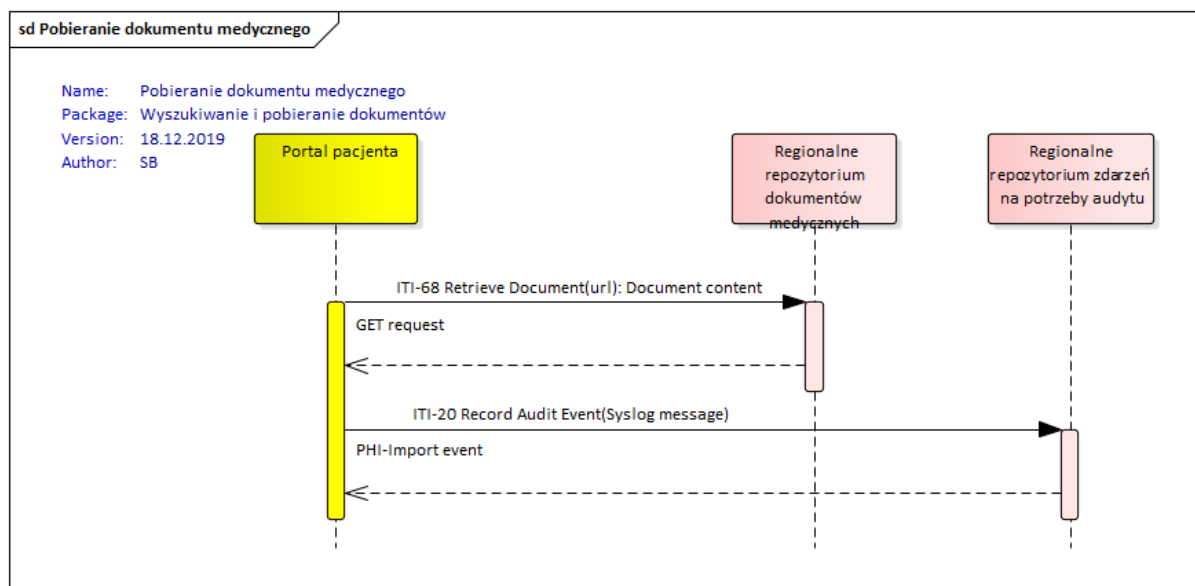
## 2.1.4.5 Komponenty i transakcje

### 2.1.4.5.1 Komponenty

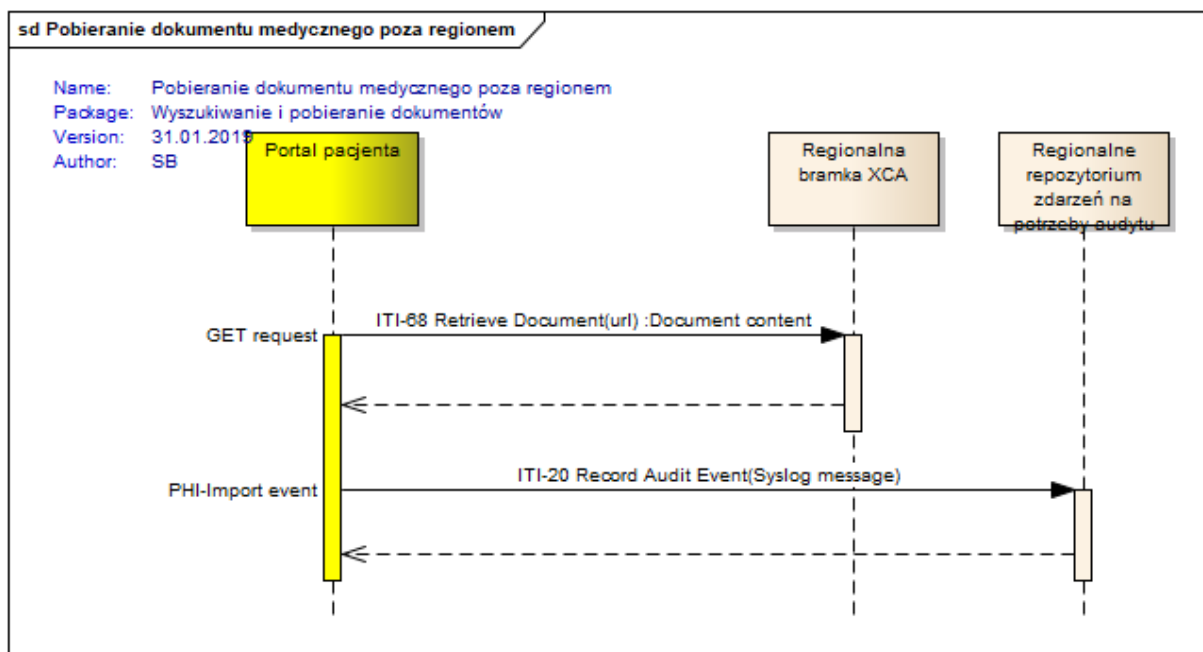


Rysunek nr 2.16 Diagram komponentów obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

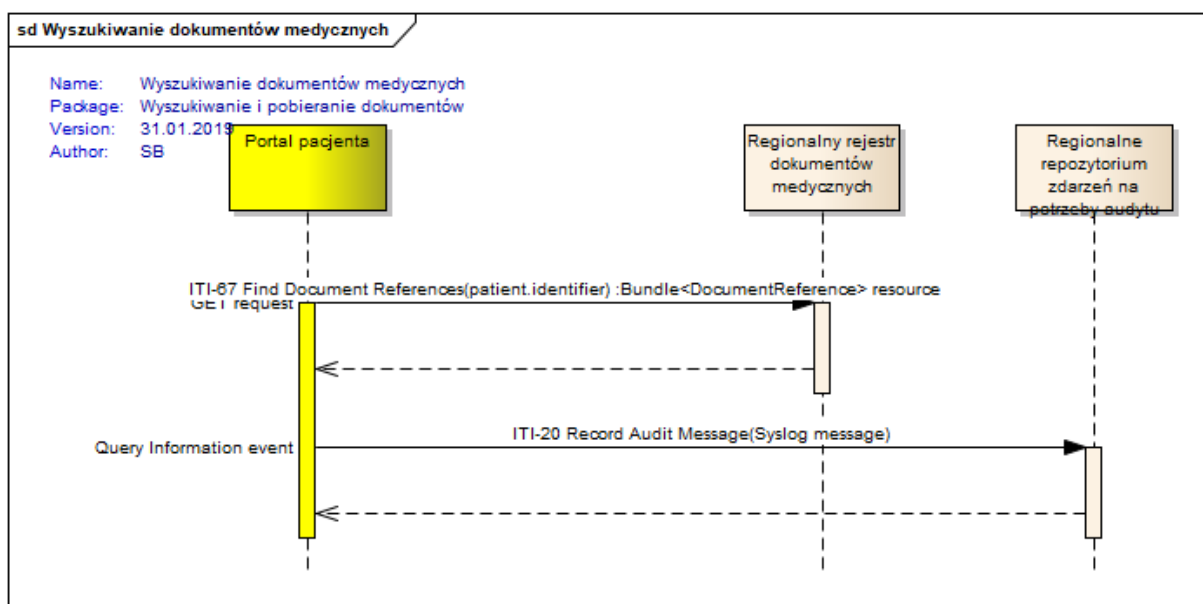
### 2.1.4.5.2 Transakcje



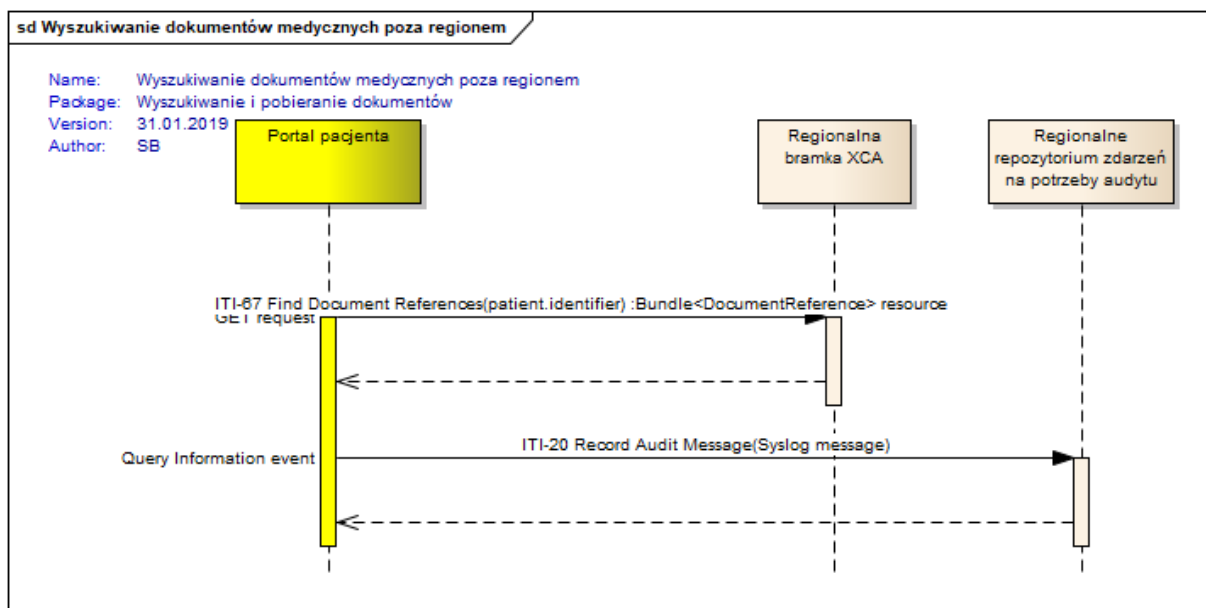
Rysunek nr 2.17 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego”



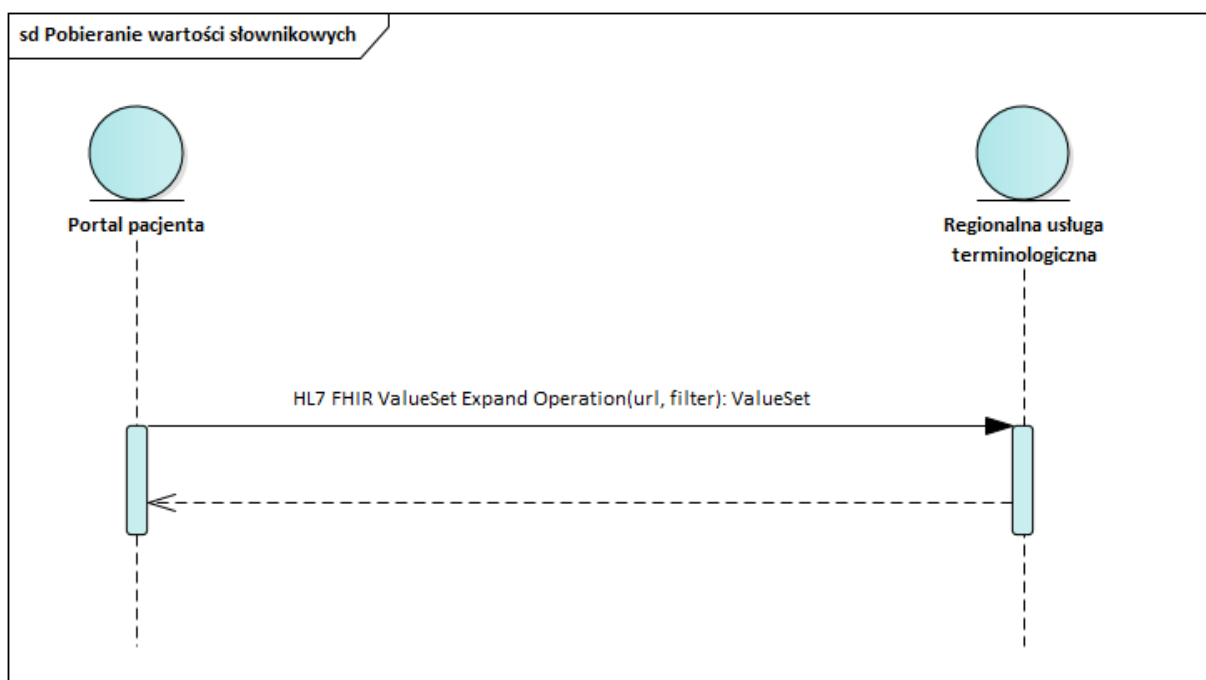
Rysunek nr 2.18 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego poza regionem”



Rysunek nr 2.19 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych”



Rysunek nr 2.20 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych poza regionem”



Rysunek nr 2.21 Diagram sekwencji transakcji „Pobieranie wartości słownikowych”

### 2.1.4.6 Model interfejsu użytkownika

Pacjent
Dokumenty pacjenta
Udostępnianie dokumentów
Umawianie wizyt
Placówki medyczne
Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

Wyszukaj dokumenty poza regionem

Filtrowanie listy dokumentów

Data wystawienia
od  /  do  /

Typ dokumentu

Wybierz

Usługa medyczna

Wpisz fragment nazwy

Data usługi/wizyty/pobytu
od  /  do  /

Rodzaj placówki

Wpisz fragment nazwy

Wystawca dokumentu

Wpisz fragment nazwiska

Podmiot medyczny

Wpisz fragment nazwy

☐ Zaznacz wszystkie

Pobierz zaznaczone

	Data wystawienia	Typ dokumentu	Rodzaj placówki	Wystawca	Źródło
<input type="checkbox"/>	21.11.2018	<a href="#">Karta informacyjna leczenia szpitalnego</a>	Oddział kardiologiczny	dr Piotr Nowak	Szpital Wojewódzki w Krakowie
<input type="checkbox"/>	19.10.2018	<a href="#">Odmowa przyjęcia do szpitala</a>	Izba przyjęć szpitala	lek. Jan Wolski	Szpital Wojewódzki w Krakowie
<input type="checkbox"/>	15.09.2018	<a href="#">Sprawozdanie z badania laboratoryjnego</a>	Pracownia diagnostyki laboratoryjnej	mgr Wojciech Dąbrowski	Laboratorium Medyczne nr 1

Rysunek nr 2.22 Makieta ekranu „Dokumenty medyczne pacjenta”

Pacjent

Dokumenty pacjenta

Udostępnianie dokumentów

Umawianie wizyt

Placówki medyczne

Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Dokumenty](#) > Karta informacyjna leczenia szpitalnego (21.11.2018)

Zapisz dokument

Pokaż historię udostępniania

Dokument medyczny

Rysunek nr 2.23 Makieta ekranu „Dokument medyczny”



Pacjent

Dokumenty pacjenta

Udostępnianie dokumentów

Umawianie wizyt

Placówki medyczne

Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

[Dokumenty](#) > Rezonans magnetyczny niskopółowy głowy (06.01.2019)

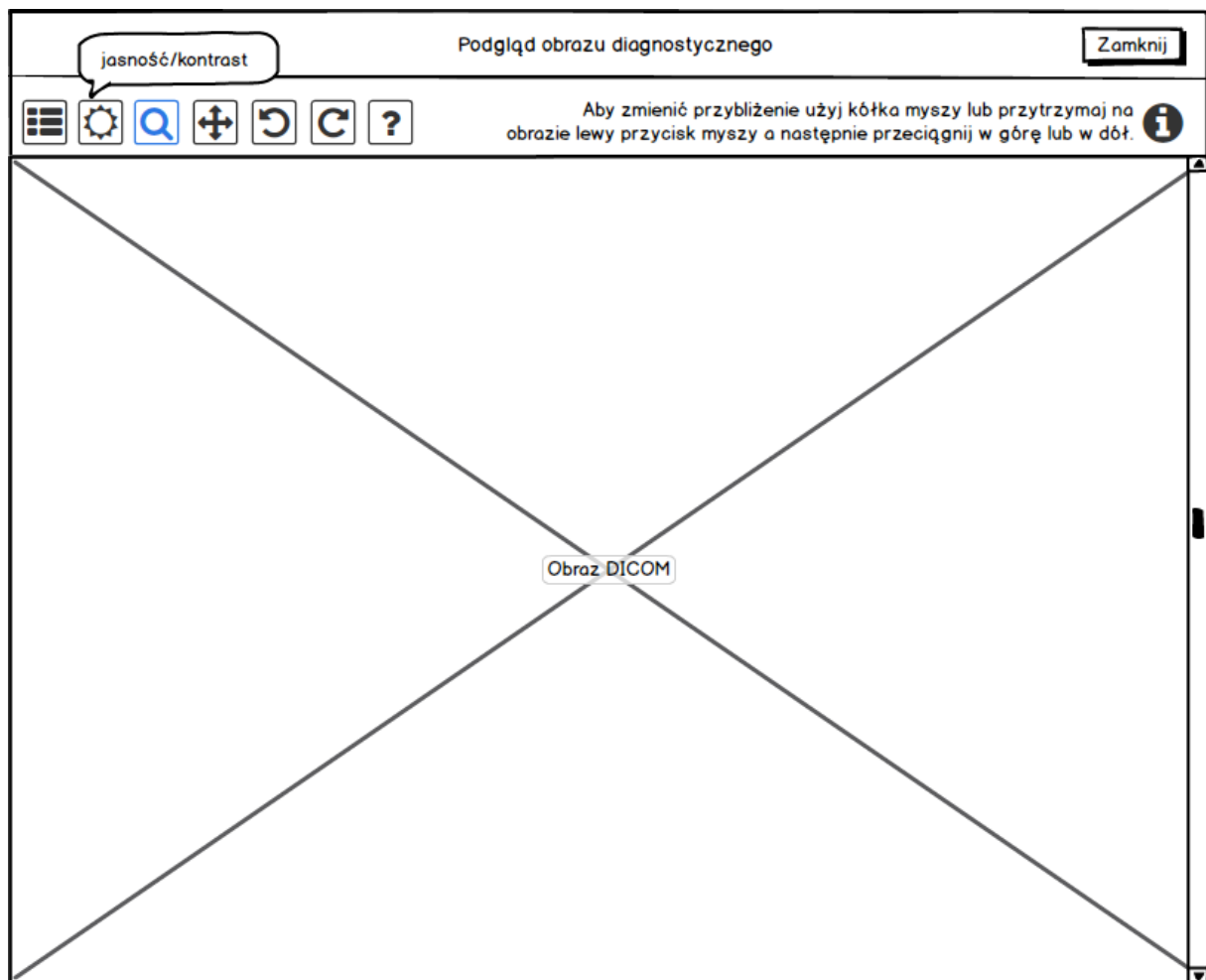
[Pokaż obrazy diagnostyczne](#)

Zapisz dokument

Pokaż historie udostępniania

Opis badania obrazowego w standardzie HL7 CDA

Rysunek nr 2.24 Makieta ekranu „Podgląd opisu badania”



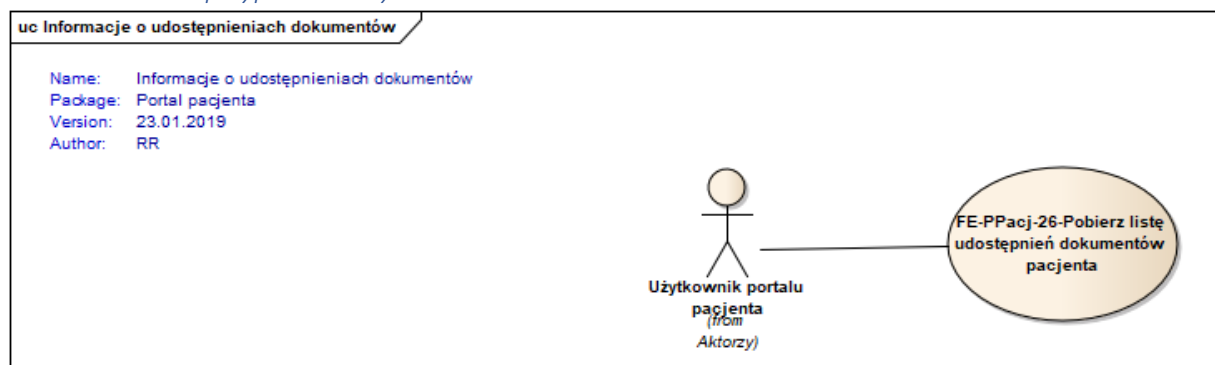
Rysunek nr 2.25 Makieta ekranu „Podgląd obrazu DICOM”

## 2.1.5 Moduł „Informacje o udostępnieniu dokumentów”

### 2.1.5.1 Wymagania funkcjonalne

**FE.PPacj.20.** System udostępnia informacje o zdarzeniach udostępnienia dokumentów medycznych pacjenta.

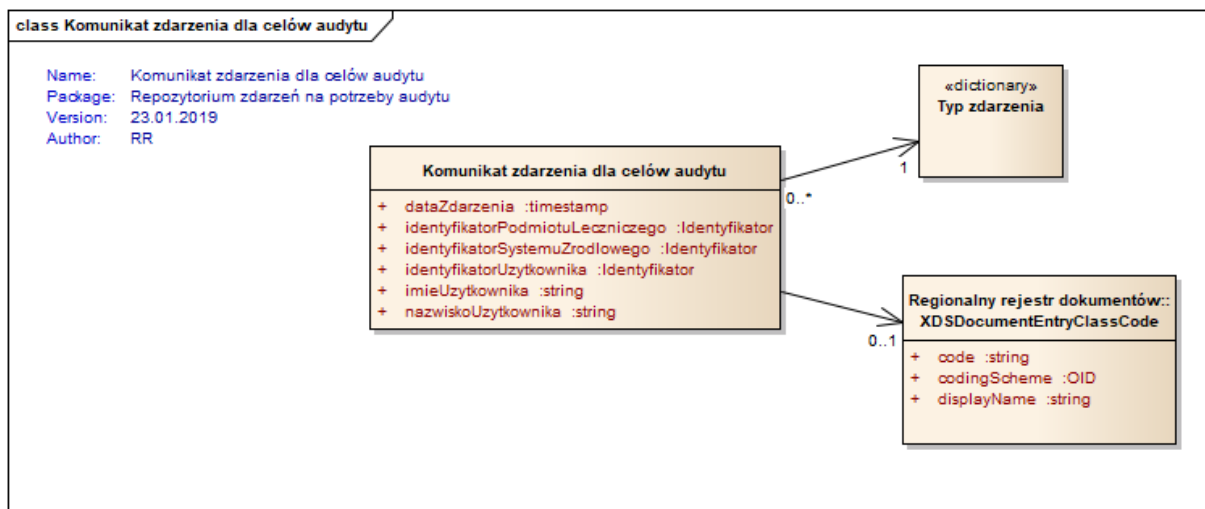
### 2.1.5.2 Model przypadków użycia



Rysunek nr 2.26 Diagram przypadków użycia obszaru „Informacje o udostępnieniach dokumentów”

### 2.1.5.3 Model danych

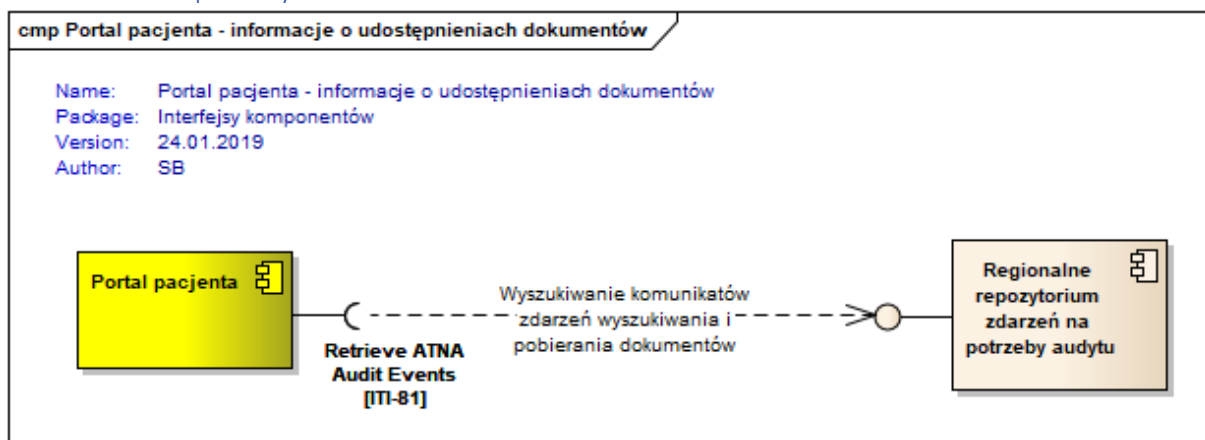
Moduł „Informacje o udostępnieniach dokumentów” korzysta z danych gromadzonych w komponente Repozytorium zdarzeń na potrzeby audytu, którego model danych przedstawiono poniżej.



Rysunek nr 2.27 Diagram klas obszaru „Informacje o udostępnieniach dokumentów”

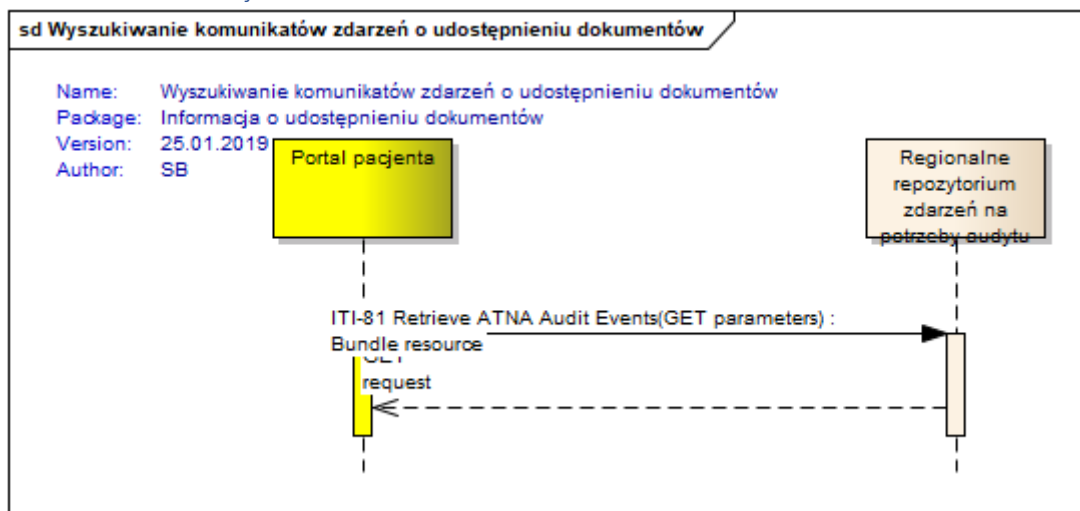
### 2.1.5.4 Komponenty i transakcje

#### 2.1.5.4.1 Komponenty



Rysunek nr 2.28 Diagram komponentów obszaru „Portal pacjenta - informacje o udostępnieniach dokumentów”

## 2.1.5.4.2 Transakcje



Rysunek nr 2.29 Diagram sekwencji transakcji „Wyszukiwanie komunikatów zdarzeń o udostępnieniu dokumentów”

## 2.1.5.5 Model interfejsu użytkownika

Pacjent
Dokumenty pacjenta
**Udostępnianie dokumentów**
Umawianie wizyt
Placówki medyczne
Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

[Udostępnianie dokumentów](#) > ...

Lista udostępnień dokumentów Pokaż również wyszukiwania

Parametry filtrowania

Pokaż zdarzenia w okresie od  /  do  /

Data zdarzenia	Typ zdarzenia	Typ dokumentu	Użytkownik	Aplikacja/podmiot
21.01.2019	pobranie dokumentu	<a href="#">Karta odmowy przyjęcia do szpitala</a>	Jan Kowalski	Portal pacjenta
21.01.2019	wyszukiwanie dokumentów		Jan Kowalski	Portal pacjenta
10.01.2019	wyszukiwanie dokumentów		Piotr Nowak	Szpital Specjalistyczny im. Ludwika Rydygiera
12.10.2018	wyszukiwanie dokumentów		Wojciech Malinowski	Krakowski Szpital Specjalistyczny

Rysunek nr 2.30 Makietę ekranu „Lista udostępnień dokumentów”

## 2.1.6 Moduł „Umawianie wizyt”

### 2.1.6.1 Wymagania funkcjonalne

**FE.PPacj.21.** System umożliwi użytkownikowi wyszukiwanie wolnych terminów wizyt w grafiku udostępnionym przez podmiot medyczny.

**FE.PPacj.22.** System umożliwia użytkownikowi dokonanie rezerwacji wybranego terminu wizyty w grafiku udostępnionym przez podmiot medyczny.

**FE.PPacj.23.** System umożliwia użytkownikowi przeglądanie listy jego zarezerwowanych wizyt.

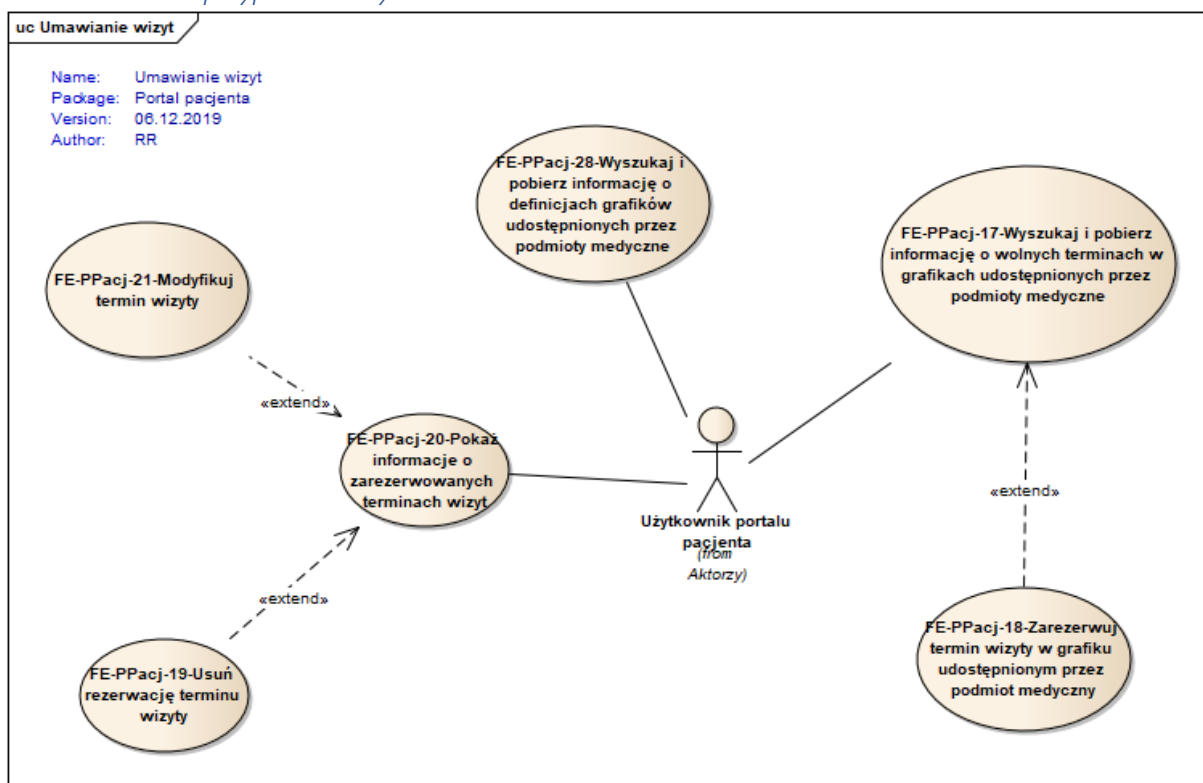
**FE.PPacj.24.** System umożliwia użytkownikowi przeglądanie szczegółów jego zarezerwowanej wizyty, w tym:

1. danych kontaktowych i teleadresowych placówki medycznej,
2. informacji o świadczeniu medycznym,
3. informacji o wykonującym je pracowniku medycznym.

**FE.PPacj.25.** System umożliwia użytkownikowi zmianę terminu jego zarezerwowanej wizyty.

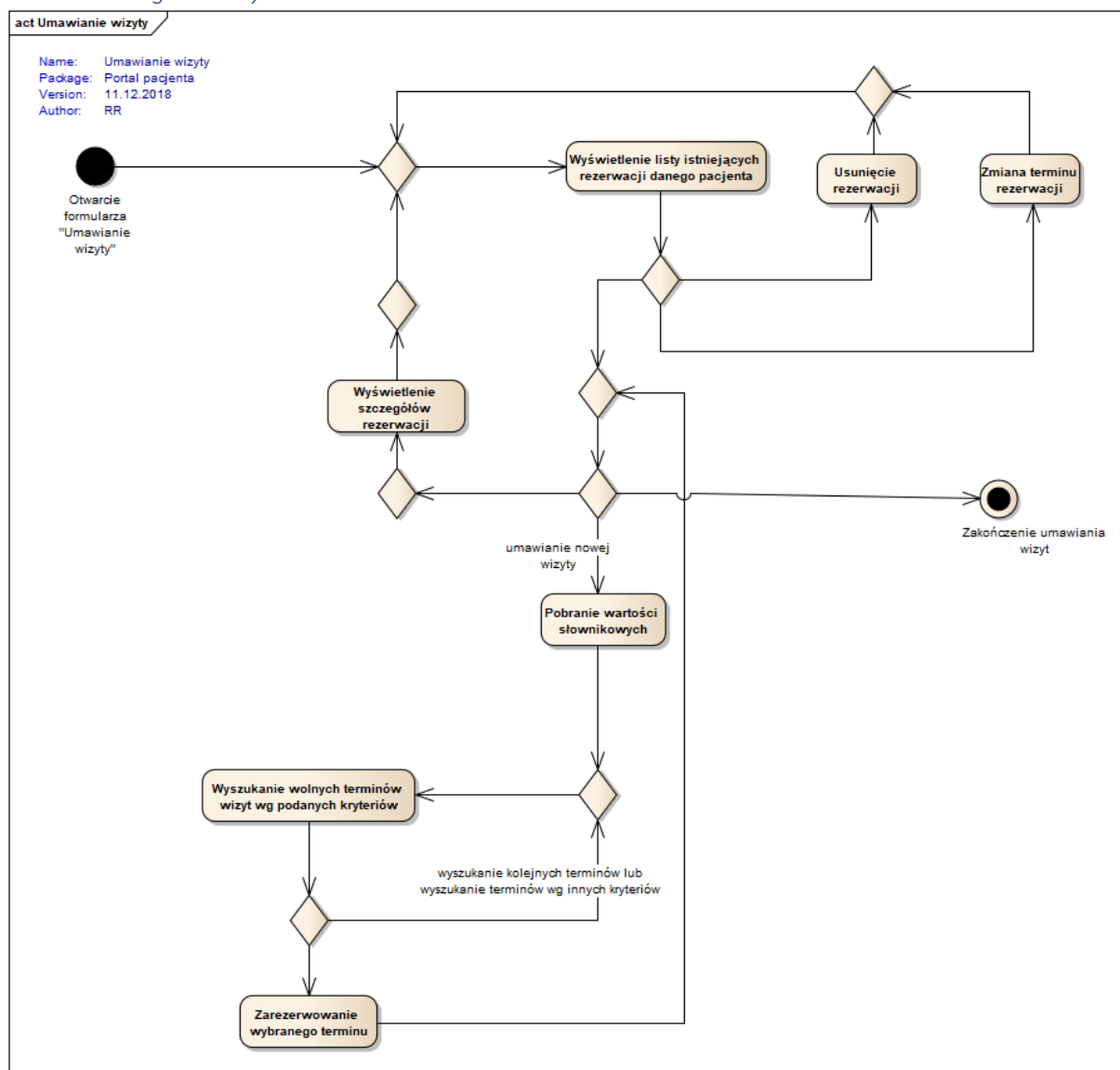
**FE.PPacj.26.** System umożliwia użytkownikowi odwołanie terminu jego zarezerwowanej wizyty.

#### 2.1.6.2 Model przypadków użycia



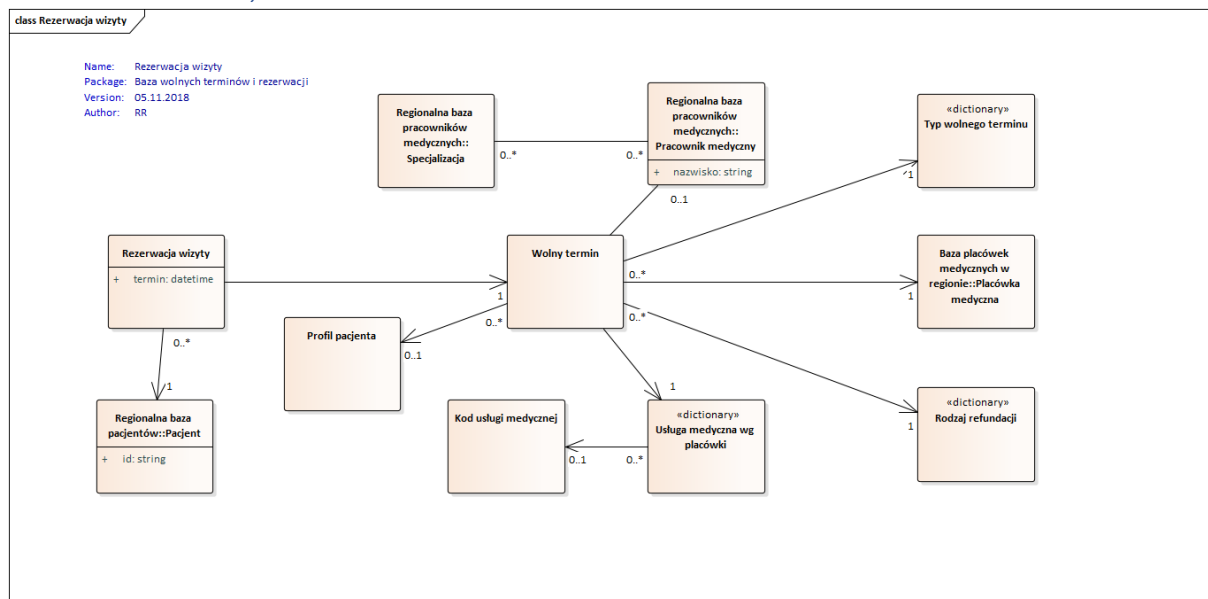
Rysunek nr 2.31 Diagram przypadków użycia obszaru „Ustawianie wizyt”

### 2.1.6.3 Diagram aktywności



Rysunek nr 2.32 Diagram aktywności obszaru „Umawianie wizyty”

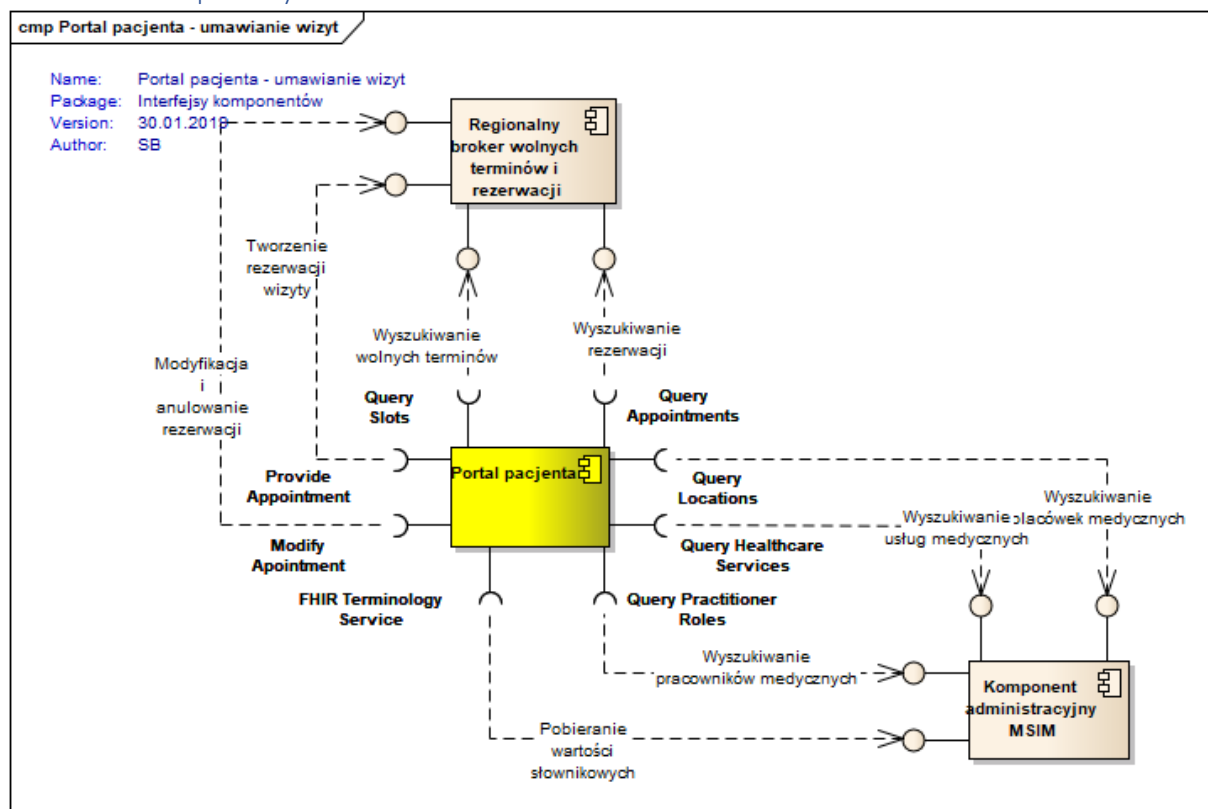
## 2.1.6.4 Model danych



Rysunek nr 2.33 Diagram klas obszaru „Umawianie wizyt”

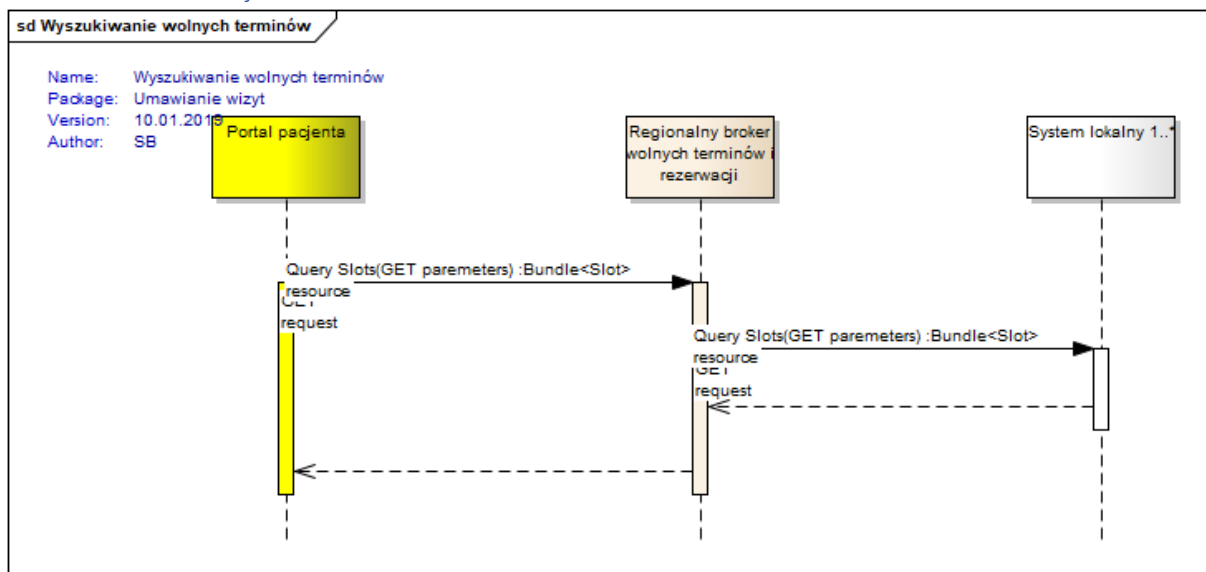
## 2.1.6.5 Komponenty i transakcje

### 2.1.6.5.1 Komponenty

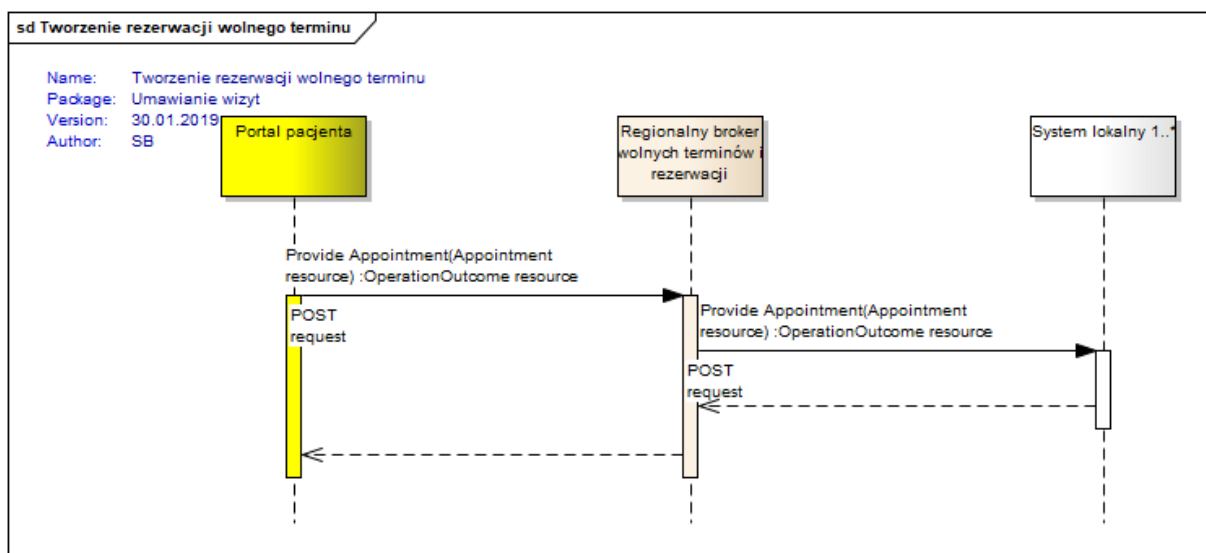


Rysunek nr 2.34 Diagram komponentów obszaru „Portal pacjenta - umawianie wizyt”

## 2.1.6.5.2 Transakcje

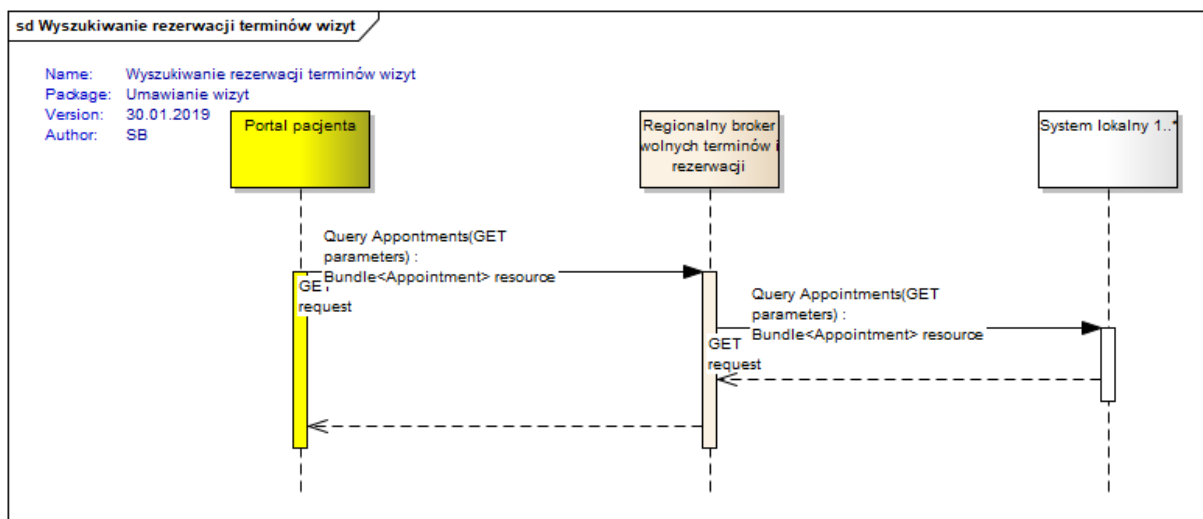


Rysunek nr 2.35 Diagram sekwencji interakcji „Wyszukiwanie wolnych terminów”

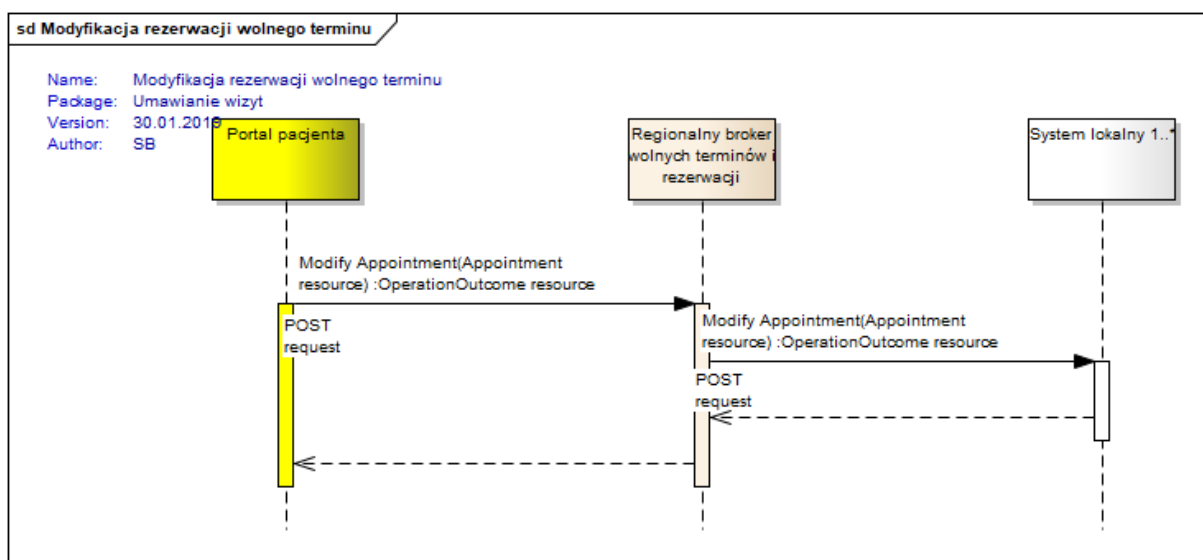


Rysunek nr 2.36 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu”

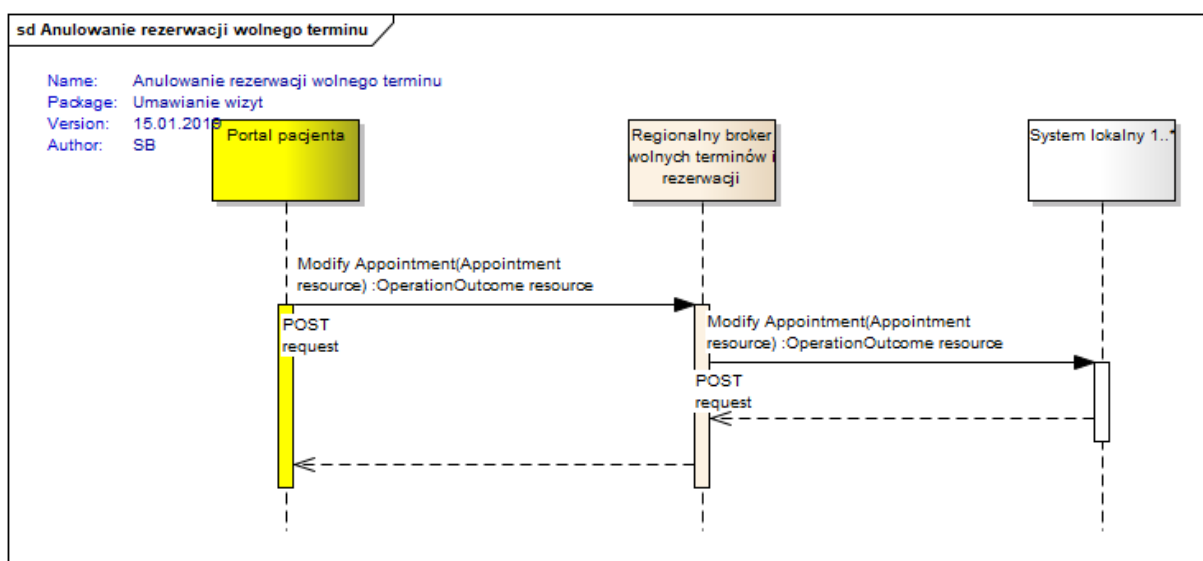




Rysunek nr 2.37 Diagram sekwencji transakcji „Wyszukiwanie rezerwacji terminów wizyt”



Rysunek nr 2.38 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu”



Rysunek nr 2.39 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu”

### 2.1.6.6 Model interfejsu użytkownika

Poniżej przedstawiono makiety interfejsu użytkownika dla obszaru „Umawianie wizyt”.

Pacjent

Dokumenty pacjenta

Umawianie wizyt

Placówki medyczne

Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

Umów nową wizytę

Data i godz. wizyty	Usługa	Lekarz	Placówka medyczna	Podmiot leczniczy
<a href="#">15.07.2018 14:15</a>	Konsultacja neurologa	prof. Nowak	Przyszpitalna poradnia specjalistyczna Kraków, os. Złotej jesieni 1	Szpital Specjalistyczny im. Ludwika Rydygiera
<a href="#">22.09.2018 10:30</a>	USG j. brzusznej		Pracownia diagnostyki obrazowej Kraków, ul. Prądnicka 80	Krakowski Szpital Specjalistyczny im. Jana Pawła II
<a href="#">26.09.2018 12:40</a>	Gastroskopia		Pracownia endoskopii Kraków, ul. Prądnicka 35	Szpital Miejski Specjalistyczny im. G. Narutowicza

Rysunek nr 2.40 Makieta ekranu „Umawianie wizyt”

Pacjent

Dokumenty pacjenta

Umawianie wizyt

Placówki medyczne

Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

[Wizyty](#) > Konsultacja neurologa (15.07.2018)

Zmień termin wizyty

Odwołaj rezerwację

Termin wizyty: 15.07.2018 godz. 14:15  
Usługa: Konsultacja neurologa  
Lekarz: prof. Jan Nowak

Placówka medyczna:  
Przyszpitalna poradnia specjalistyczna  
Kraków, os. Złotej jesieni 1  
Szpital Specjalistyczny im. Ludwika Rydygiera

Rysunek nr 2.41 Makieta ekranu "Szczegóły rezerwacji wizyty"

Pacjent
Dokumenty pacjenta
**Umawianie wizyt**
Placówki medyczne
Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Wizyty](#) > Nowa wizyta

Parametry wyszukiwania

Miejscowość

Kraków

☐ Szukaj w pobliżu

Usługa

Wpisz fragment nazwy

Pracownik medyczny

Wpisz fragment nazwiska

Specjalność pracownika

Wpisz fragment nazwy specjalności

Placówka/podmiot

Wpisz fragment nazwy

Rodzaj placówki

Wpisz fragment nazwy

Typ wizyty

Wybierz z listy

Refundacja

Wybierz z listy

Wyszukaj

Pokaż od: / /

26.05.2018 10:20

Konsultacja kardiologa, dr Piotr Kowalczyk

Poradnia kardiologiczna, ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

29.05.2018 10:20

Konsultacja kardiologa, dr Janusz Budny

Poradnia kardiologiczna, ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

10.05.2018 10:20

Konsultacja kardiologa, prof. Wojciech Mleczko

Przyszpitalna poradnia specjalistyczna, ul. Prądnicka 80, Kraków

Krakowski Szpital Specjalistyczny im. Jana Pawła II

Pokaż kolejne

Rysunek nr 2.42 Makieta ekranu „Wyszukiwanie wolnych terminów”

Pacjent
Dokumenty pacjenta
**Umawianie wizyt**
Placówki medyczne
Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Wizyty](#) > [Nowa wizyta](#) > Konsultacja kardiologa (25.06.2018)

Termin wizyty:

26.05.2018 godz. 10:20

Usługa:

Konsultacja kardiologa

Lekarz:

dr Piotr Kowalczyk

Placówka medyczna:

Poradnia kardiologiczna

ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

Zarezerwuj ten termin

Rysunek nr 2.43 Makieta ekranu „Nowa wizyta”

## 2.2 Portal pracownika medycznego

### 2.2.1 Moduł „Uwierzytelnianie i zarządzanie kontem użytkownika”

#### 2.2.1.1 Wymagania funkcjonalne

**FE.PPMed.1.** System umożliwia dostęp za pomocą Krajowego Węzła Identyfikacji Elektronicznej użytkownikom, którzy są reprezentowani w regionalnej bazie pracowników medycznych oraz korzystają z profilu zaufanego (PZ)/podpisu osobistego.

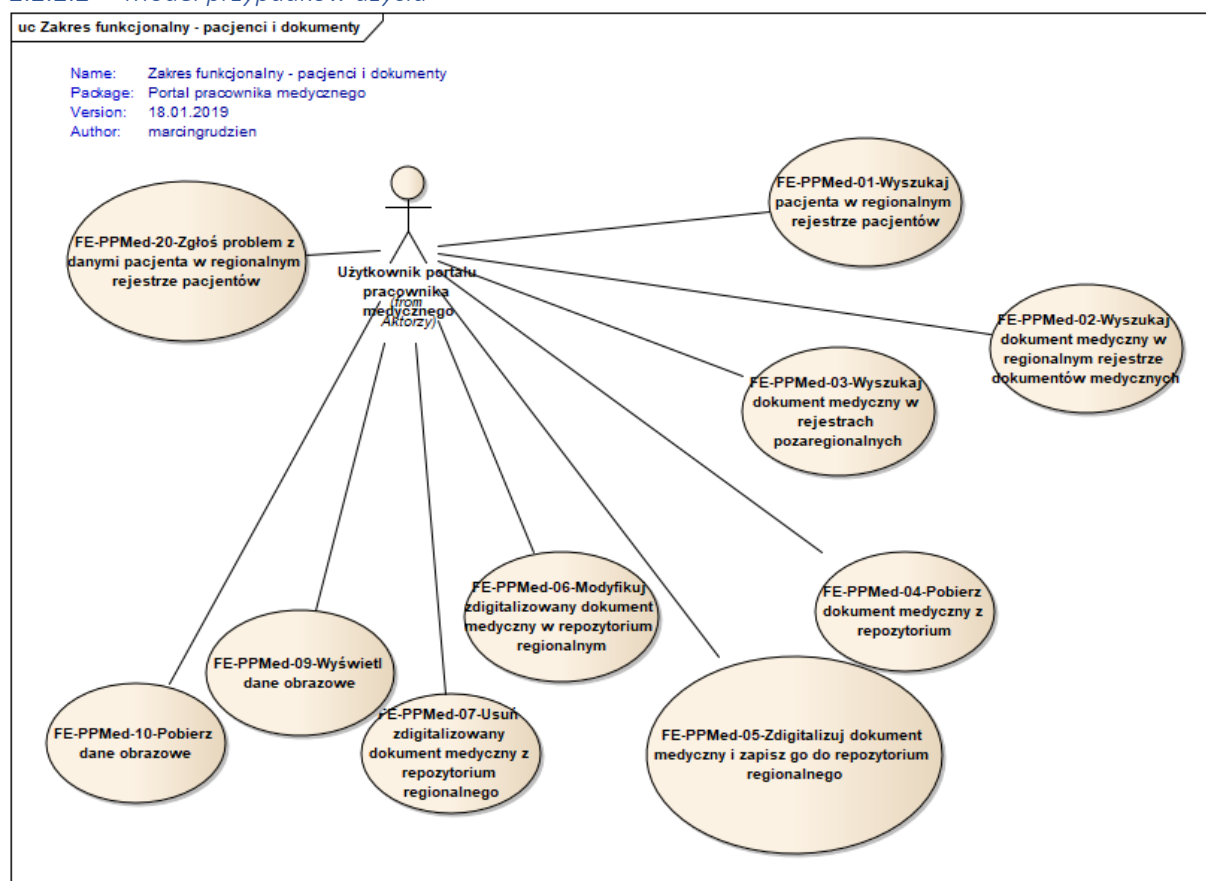
### 2.2.2 Moduł „Wyszukiwanie pacjenta”

#### 2.2.2.1 Wymagania funkcjonalne

**FE.PPMed.2.** System umożliwia pracownikowi medycznemu wyszukiwanie pacjenta w regionalnej bazie pacjentów.

**FE.PPMed.3.** System umożliwia pracownikowi medycznemu zgłoszenie problemu z danymi pacjenta.

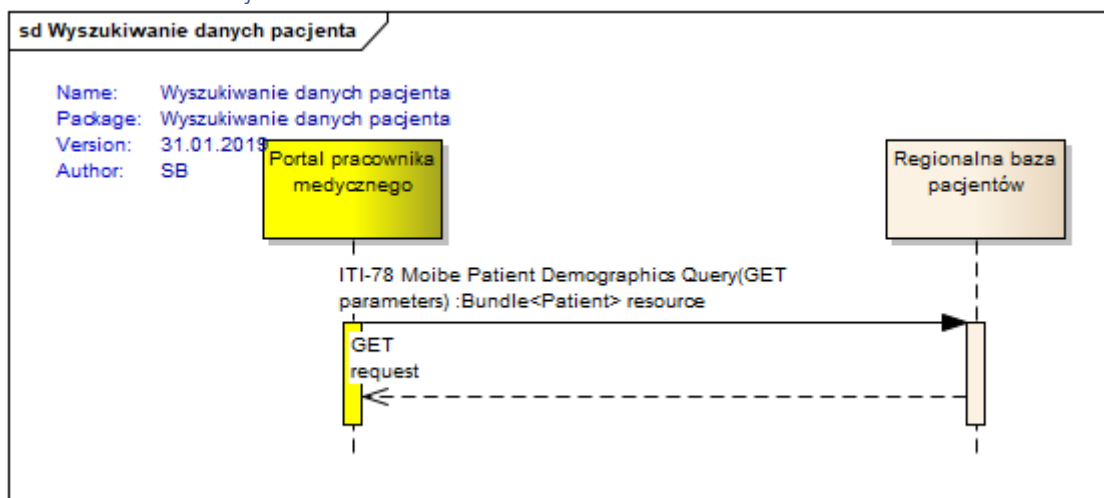
#### 2.2.2.2 Model przypadków użycia



Rysunek nr 2.44 Diagram przypadków użycia uwzględniający obszar „Wyszukiwanie pacjenta”

### 2.2.2.3 Komponenty i transakcje

#### 2.2.2.3.1 Transakcje



Rysunek nr 2.45 Diagram sekwencji transakcji „Wyszukiwanie danych pacjenta”

#### 2.2.2.4 Model interfejsu użytkownika

**Pacjent** | Dokumenty pacjenta | Umawianie wizyt | Placówki medyczne | Wyloguj

**Wyszukiwanie pacjenta**

Nazwisko

PESEL

Szukaj

**Dane osobowe**

Imię i nazwisko	PESEL	Nr telefonu
Jan Kowalski	9999999999	12 345 67 89
Płeć	Data urodzenia	Email
Mężczyzna	15-04-1982	jkowalski@gmail.com

**Adres zamieszkania**

Ulica	Miasto	Kod pocztowy
Wiśniowa 2 m 208	Kraków	31-567

Zgłoś problem z danymi pacjenta

Rysunek nr 2.46 Makieta ekranu „Wyszukiwanie pacjenta”

Zgłoszenie problemu z danymi pacjenta	
Pacjent	Jan Kowalski
PESEL	9999999999
Identyfikator regionalny	123456789
Opis problemu	<div style="border: 1px solid black; padding: 10px; min-height: 100px;"> Wpisz tekst zgłoszenia </div>
<div style="display: flex; justify-content: space-between; margin-top: 10px;"> <span>Anuluj</span> <span>Wyślij zgłoszenie</span> </div>	

Rysunek nr 2.47 Makieta ekranu „Zgłoszenie problemu z danymi pacjenta”

## 2.2.3 Moduł „Informacje o placówkach medycznych”

### 2.2.3.1 Wymagania funkcjonalne

**FE.PPMed.4.** System umożliwia wyszukiwanie placówek medycznych w regionie, w szczególności według kryteriów:

1. miejscowość,
2. podmiot leczniczy,
3. specjalność placówki.

**FE.PPMed.5.** System umożliwia wyszukiwanie placówek medycznych w pobliżu wybranej miejscowości.

**FE.PPMed.6.** System używa współrzędnych geograficznych do określenia placówek w pobliżu wybranej miejscowości.

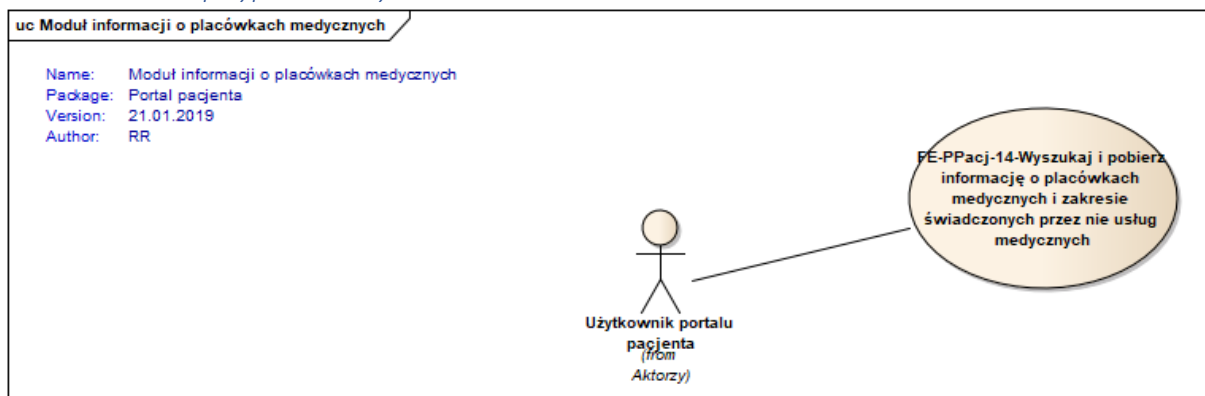
**FE.PPMed.7.** System umożliwia wyszukiwanie po fragmencie nazwy.

**FE.PPMed.8.** System udostępnia informacje teleadresowe placówek medycznych w regionie.

**FE.PPMed.9.** System udostępnia opis zakresu świadczonych przez placówkę medyczną usług.

**FE.PPMed.10.** System udostępnia informację o tych usługach medycznych realizowanych przez daną placówkę medyczną, które są dostępne za pomocą e-Rejestracji regionalnej.

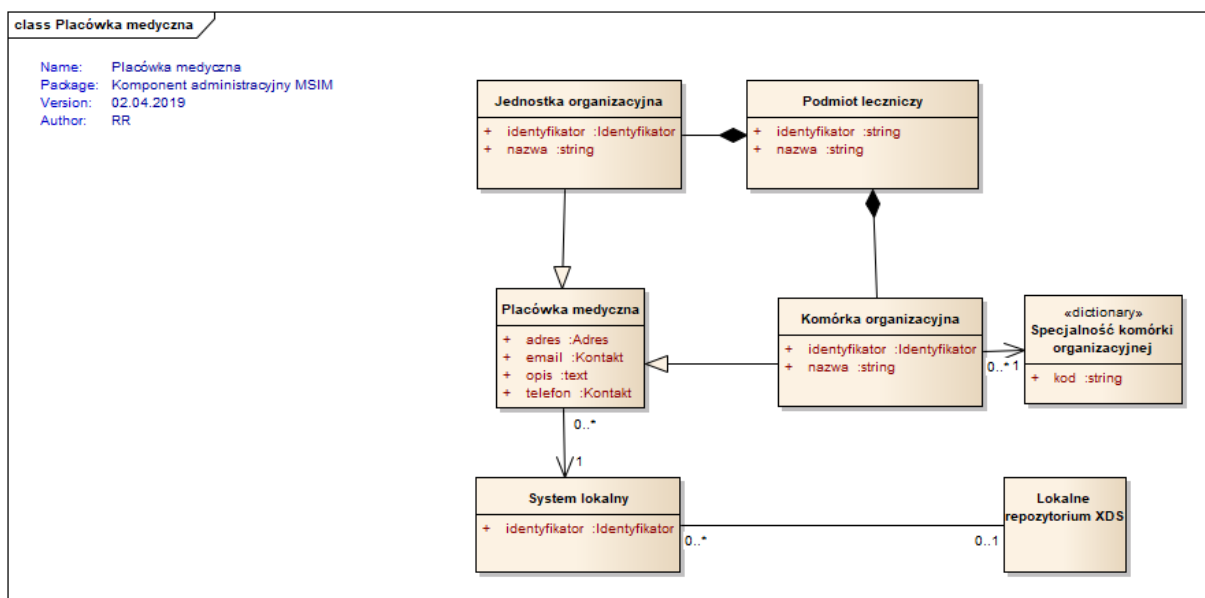
### 2.2.3.2 Model przypadków użycia



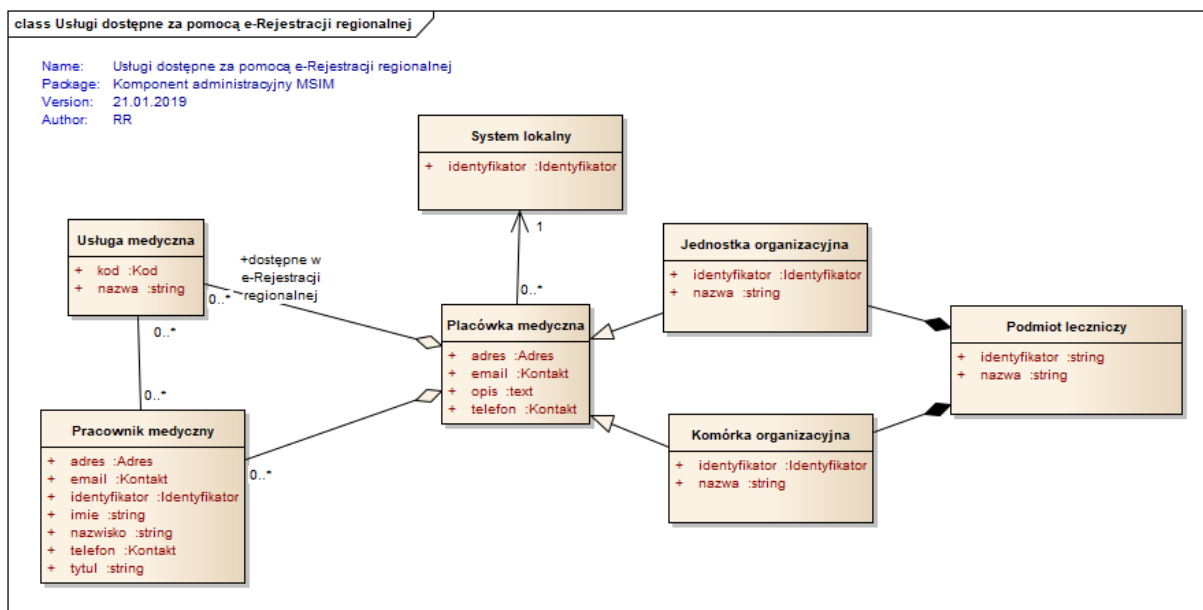
Rysunek nr 2.48 Diagram przypadków użycia obszaru „Informacje o placówkach medycznych”

### 2.2.3.3 Model danych

Moduł Informacje o placówkach medycznych korzysta z danych gromadzonych w komponentie Komponent administracyjny MSIM, którego model danych dla obszaru placówek medycznych przedstawiono poniżej.



Rysunek nr 2.49 Model danych obszaru „Placówka medyczna”



Rysunek nr 2.50 Model danych obszaru „Usługi dostępne za pomocą e-Rejestracji regionalnej”

#### 2.2.3.4 Model interfejsu użytkownika

Pacjent
Dokumenty pacjenta
Udostępnianie dokumentów
Umawianie wizyt
**Placówki medyczne**
Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Placówki medyczne](#) > ...

Lista placówek medycznych w regionie

Parametry filtrowania

Miejscowość

Wpisz fragment nazwy

☐ Szukaj w pobliżu

Podmiot leczniczy

Wpisz fragment nazwy

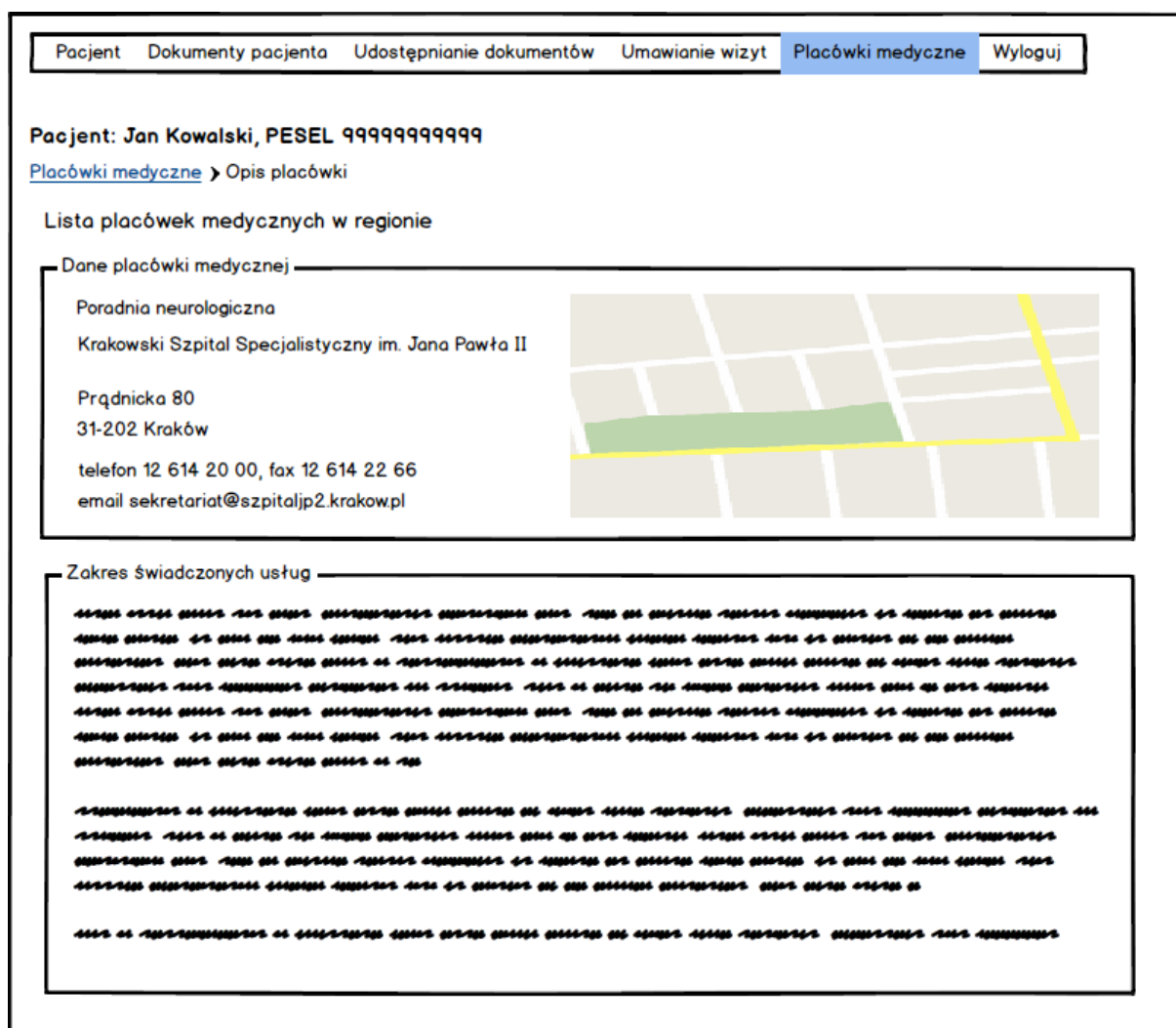
Specjalność placówki

Wpisz fragment nazwy

Nazwa placówki	Miejscowość	Adres	Podmiot leczniczy
<a href="#">Poradnia kardiologiczna</a>	Kraków	os. Złotej Jesieni 1	Szpital Specjalistyczny im. Ludwika Rydygiera
<a href="#">Poradnia neurologiczna</a>	Kraków	Prądnicka 80	Krakowski Szpital Specjalistyczny

Rysunek nr 2.51 Makieta ekranu „Lista placówek”





Rysunek nr 2.52 Makieta ekranu "Opis placówki"

## 2.2.4 Moduł „Wyszukiwanie i pobieranie dokumentów medycznych”

### 2.2.4.1 Wymagania funkcjonalne

**FE.PPMed.11.** System umożliwia wyszukanie pacjenta w regionalnej bazie pacjentów.

**FE.PPMed.12.** Pacjenci mogą być wyszukiwani wg wybranych przez użytkownika kryteriów: imię, nazwisko, PESEL, data urodzenia, płeć, nr telefonu, adres email.

**FE.PPMed.13.** System umożliwia prezentację listy dokumentów medycznych pacjenta reprezentowanych w regionalnym rejestrze dokumentów.

**FE.PPMed.14.** System umożliwia prezentację listy dokumentów medycznych pacjenta reprezentowanych w pozaregionalnych rejestrach dokumentów obsługujących wymianę międzydomenową w oparciu o profil IHE XCA.

**FE.PPMed.15.** System umożliwia zadeklarowanie przez użytkownika potrzeby uzyskania dostępu do dokumentów medycznych pacjenta w trybie zapewnienia ciągłości leczenia lub trybie dostępu ratunkowego.

**FE.PPMed.16.** Dokumenty są wyszukiwane w kontekście wybranego pacjenta.

**FE.PPMed.17.** Lista prezentowanych dokumentów medycznych zawiera następujące informacje: data wystawienia dokumentu, typ dokumentu, rodzaj placówki, wystawca dokumentu oraz źródło dokumentu.

**FE.PPMed.18.** Lista prezentowanych dokumentów medycznych może być filtrowana wg wybranych przez użytkownika parametrów, w szczególności: daty wystawienia dokumentu, typu dokumentu, nazwy realizowanej usługi, daty usługi/wizyty/pobytu, rodzaju placówki, nazwiska wystawcy lub nazwy podmiotu będącego wystawcą dokumentu.

**FE.PPMed.19.** System umożliwia prezentację dokumentu medycznego zgodnego z HL7 CDA lub zapisanego w formacie XACML znajdującego się w repozytorium dokumentów za pomocą transformaty referencyjnej.

**FE.PPMed.20.** System umożliwia prezentację wyniku badania obrazowego w przeglądarce obiektów DICOM.

**FE.PPMed.21.** System umożliwia zapisanie prezentowanego dokumentu medycznego we wskazanej przez użytkownika lokalizacji.

**FE.PPMed.22.** System umożliwia zapisanie transformaty referencyjnej we wskazanej przez użytkownika lokalizacji.

**FE.PPMed.23.** System umożliwia prezentację podstawowych danych pacjenta takich jak: imię, nazwisko, PESEL, data urodzenia, płeć, nr telefonu, adres email, adres zamieszkania.

**FE.PPMed.24.** System umożliwia zgłoszenie problemu z danymi pacjenta w regionalnej bazie pacjentów.

**FE.PPMed.25.** System umożliwia pobieranie (eksport) danych obrazowych poprzez przeglądarkę PACS.

**FE.PPMed.26.** System umożliwia powiększanie i pomniejszanie obrazu w przeglądarce PACS.

**FE.PPMed.27.** System umożliwia przesuwanie obrazu w przeglądarce PACS.

**FE.PPMed.28.** System umożliwia obracanie obrazu w przeglądarce PACS.

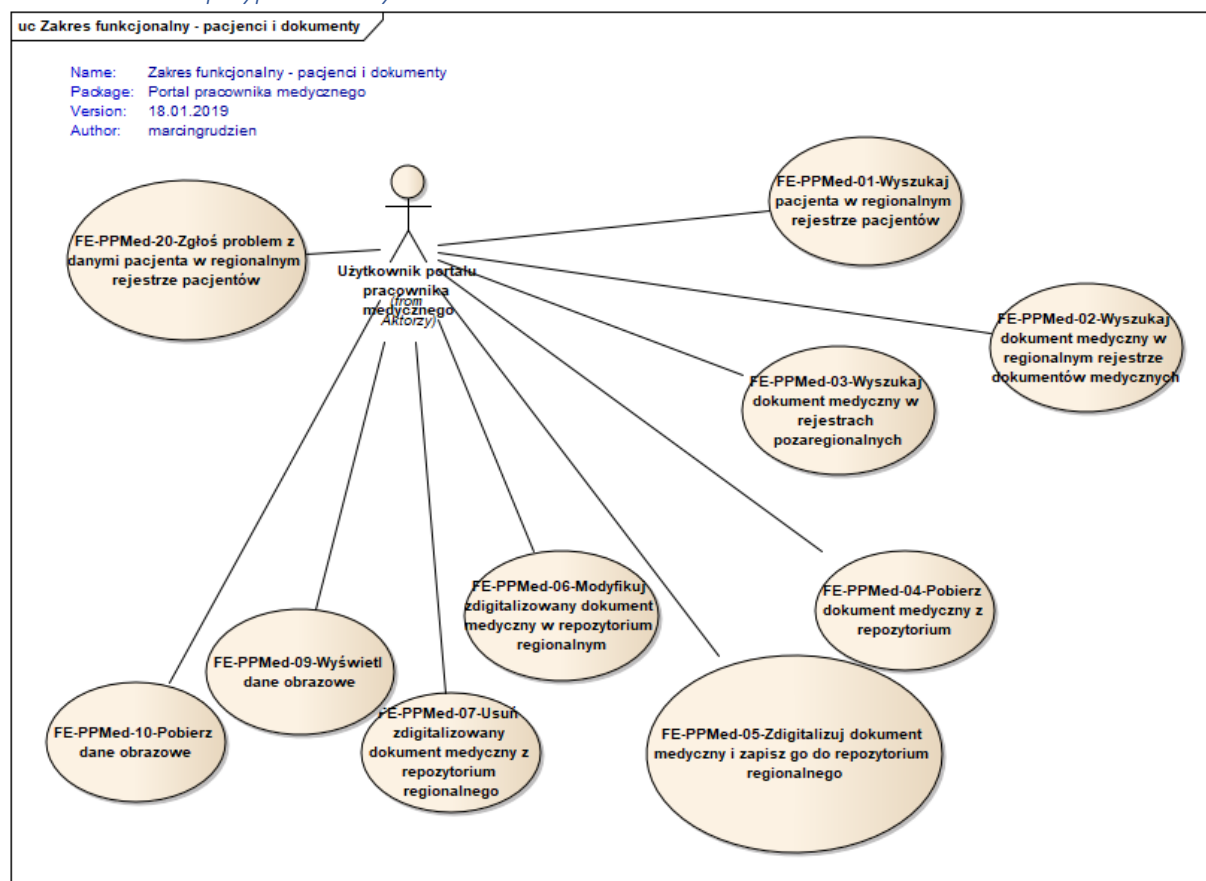
**FE.PPMed.29.** System umożliwia ustawianie jasności i kontrastu w przeglądarce PACS.

**FE.PPMed.30.** System umożliwia przeglądanie serii obrazów w przeglądarce PACS.

**FE.PPMed.31.** System posiada ekran pomocy dla użytkownika przeglądarki PACS z instrukcją jej obsługi.

**FE.PPMed.32.** System posiada pomoc kontekstową każdej z opcji przeglądarki PACS.

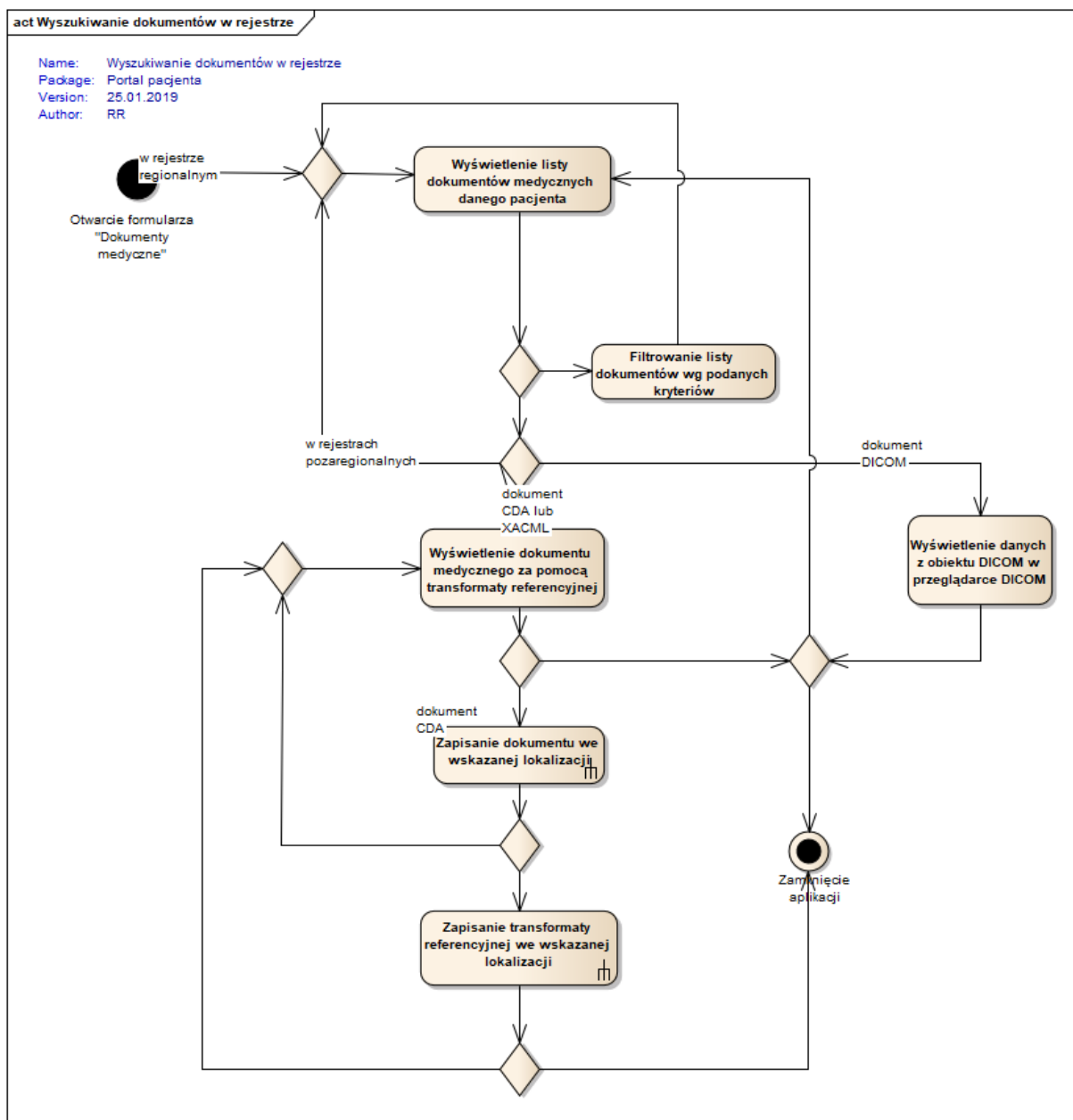
### 2.2.4.2 Model przypadków użycia



Rysunek nr 2.53 Diagram przypadków użycia uwzględniający obszar „Wyszukiwanie i pobieranie dokumentów medycznych”

### 2.2.4.3 Diagram aktywności

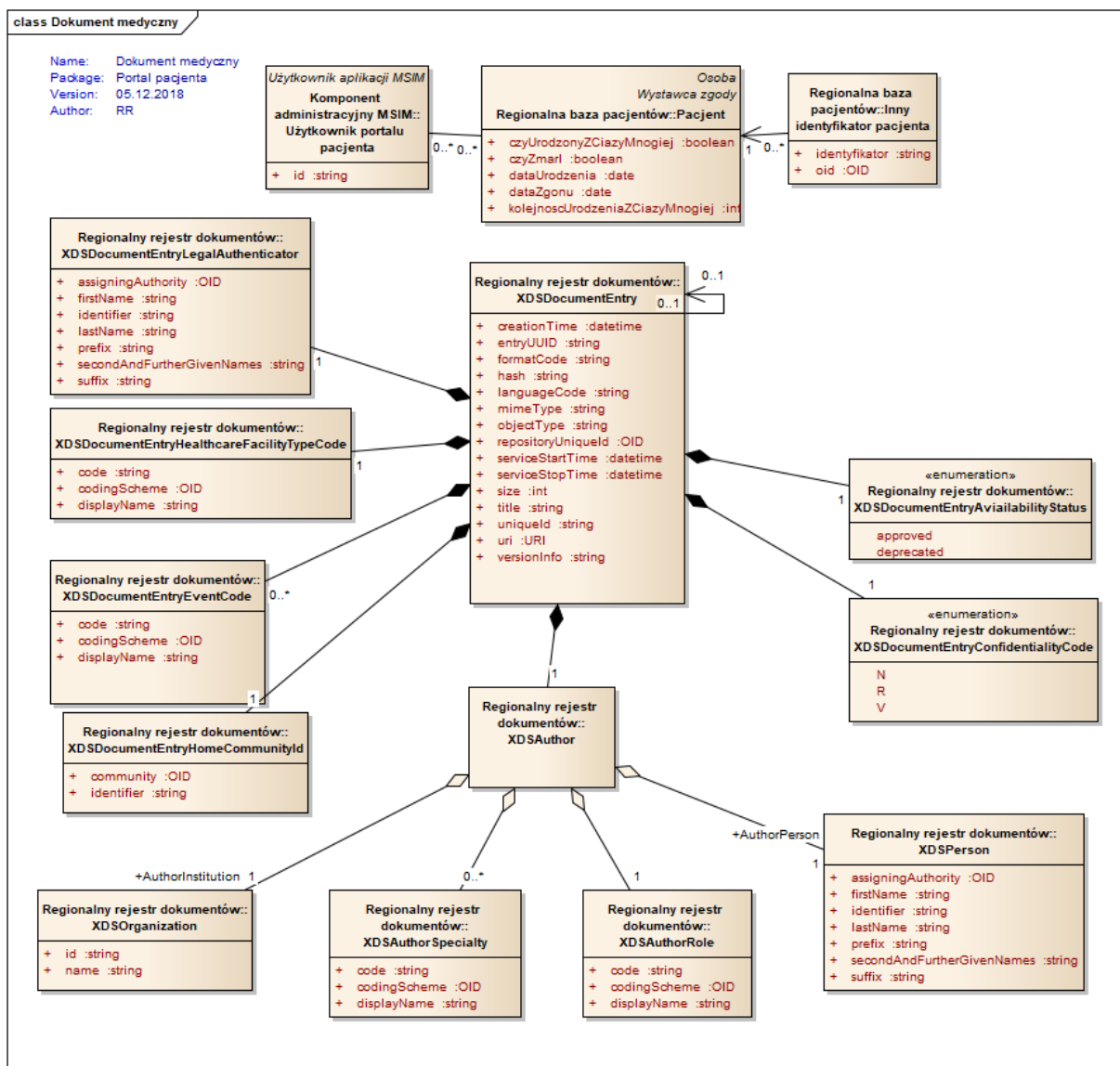
Moduł „Wyszukiwanie i pobieranie dokumentów medycznych” realizuje procesy w analogiczny sposób do odpowiadającego mu nazwą modułu aplikacji Portal pacjenta. Poniżej przedstawiono wspólny dla tych modułów obu aplikacji diagram aktywności.



Rysunek nr 2.54 Diagram aktywności obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

#### 2.2.4.4 Model danych

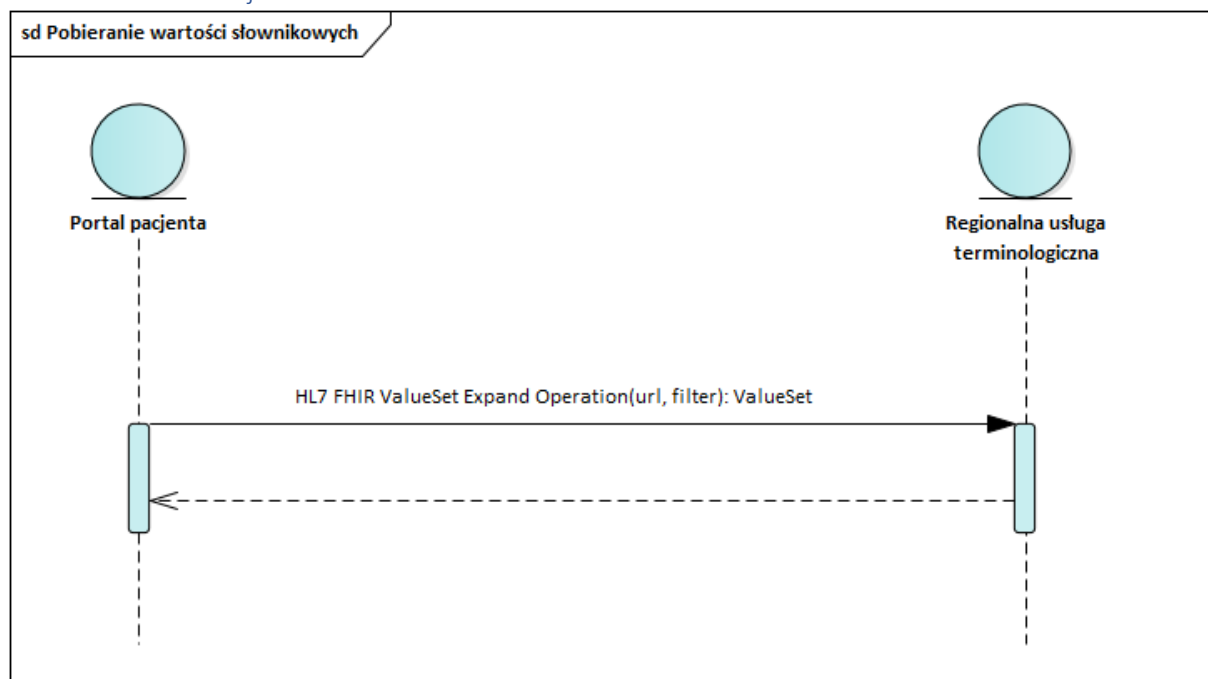
Moduł „Wyszukiwanie i pobieranie dokumentów medycznych” korzysta z tego samego modelu danych, co odpowiadający mu nazwą moduł aplikacji Portal pacjenta. Poniżej przedstawiono wspólny dla tych modułów obu aplikacji diagram klas obrazujący model danych.



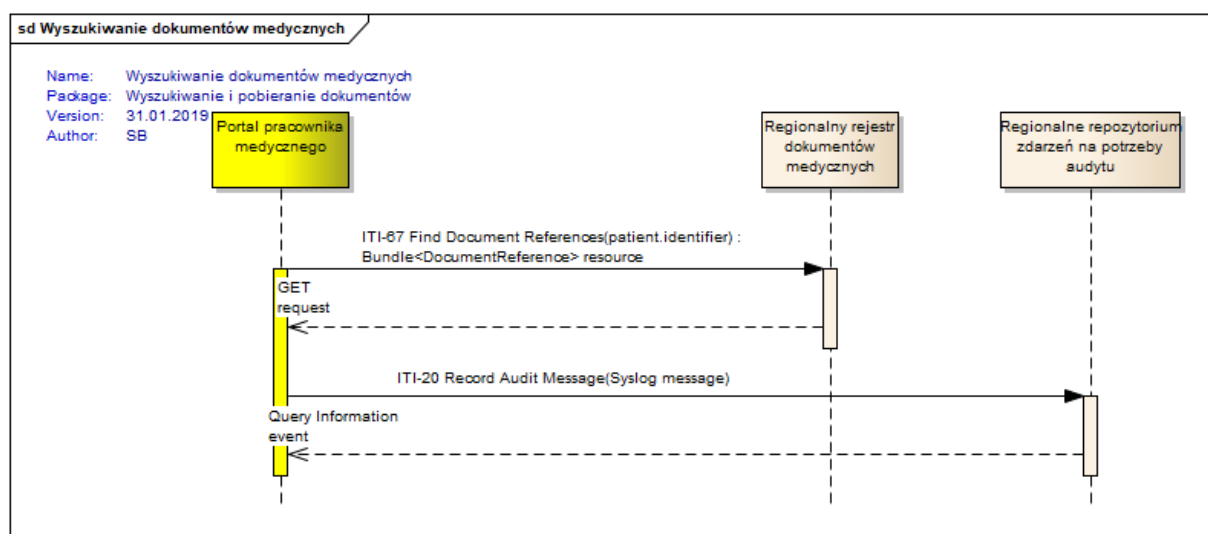
Rysunek nr 2.55 Diagram klas obszaru „Wyszukiwanie i pobieranie dokumentów medycznych”

## 2.2.4.5 Komponenty i transakcje

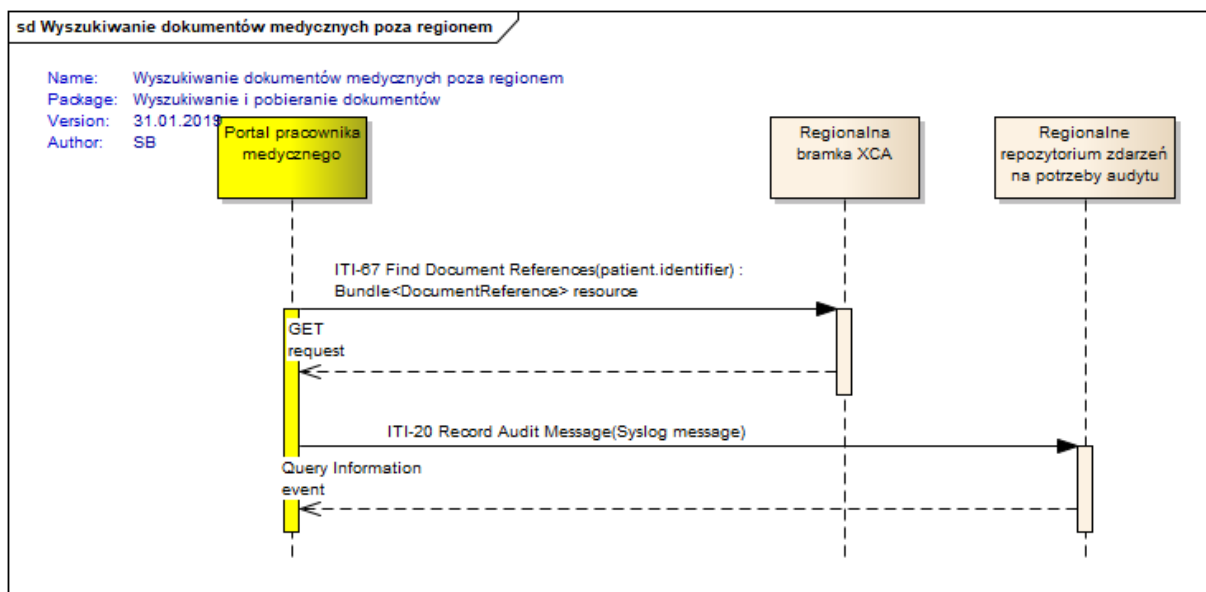
### 2.2.4.5.1 Transakcje



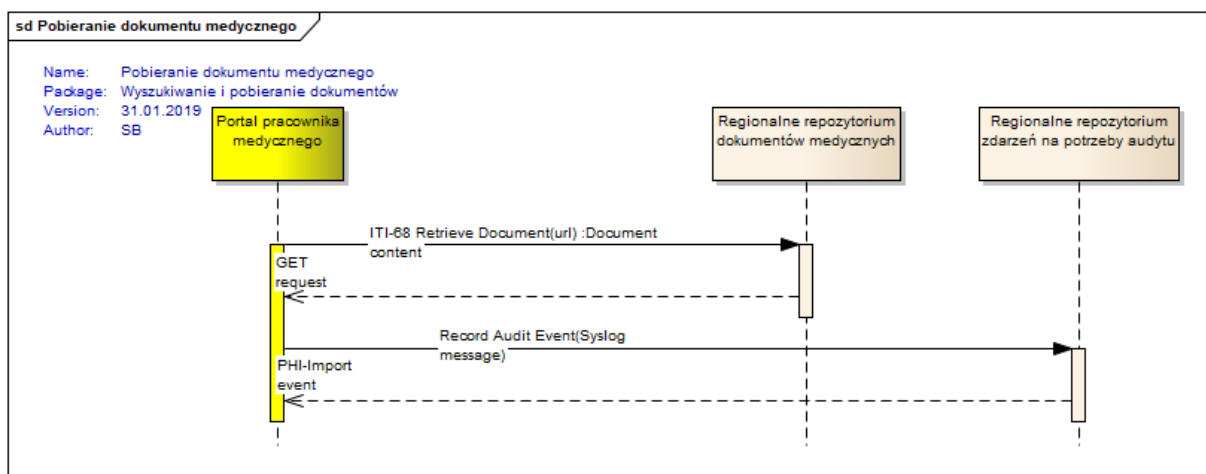
Rysunek nr 2.56 Diagram sekwencji transakcji „Pobieranie wartości słownikowych”



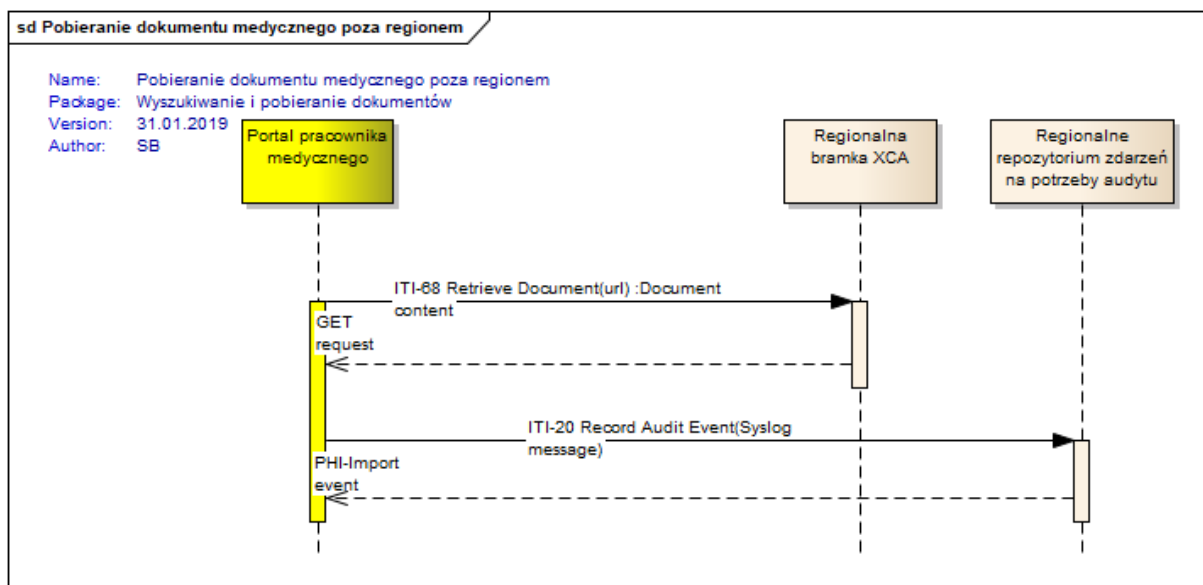
Rysunek nr 2.57 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych pacjenta”



Rysunek nr 2.58 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych pacjenta poza regionem”



Rysunek nr 2.59 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego”



Rysunek nr 2.60 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego poza regionem”

#### 2.2.4.6 Model interfejsu użytkownika

Pacjent **Dokumenty pacjenta** Umawianie wizyt Placówki medyczne Wyloguj

[Dokumenty pacjenta](#) > Jan Kowalski, PESEL 9999999999

Wyszukaj dokumenty poza regionem Dodaj dokument

Filtrowanie listy dokumentów

Data wystawienia od / / do / /

Typ dokumentu Wybierz Usługa medyczna Wpisz fragment nazwy

Data usługi/wizyty/pobytu od / / do / / Rodzaj placówki Wpisz fragment nazwy

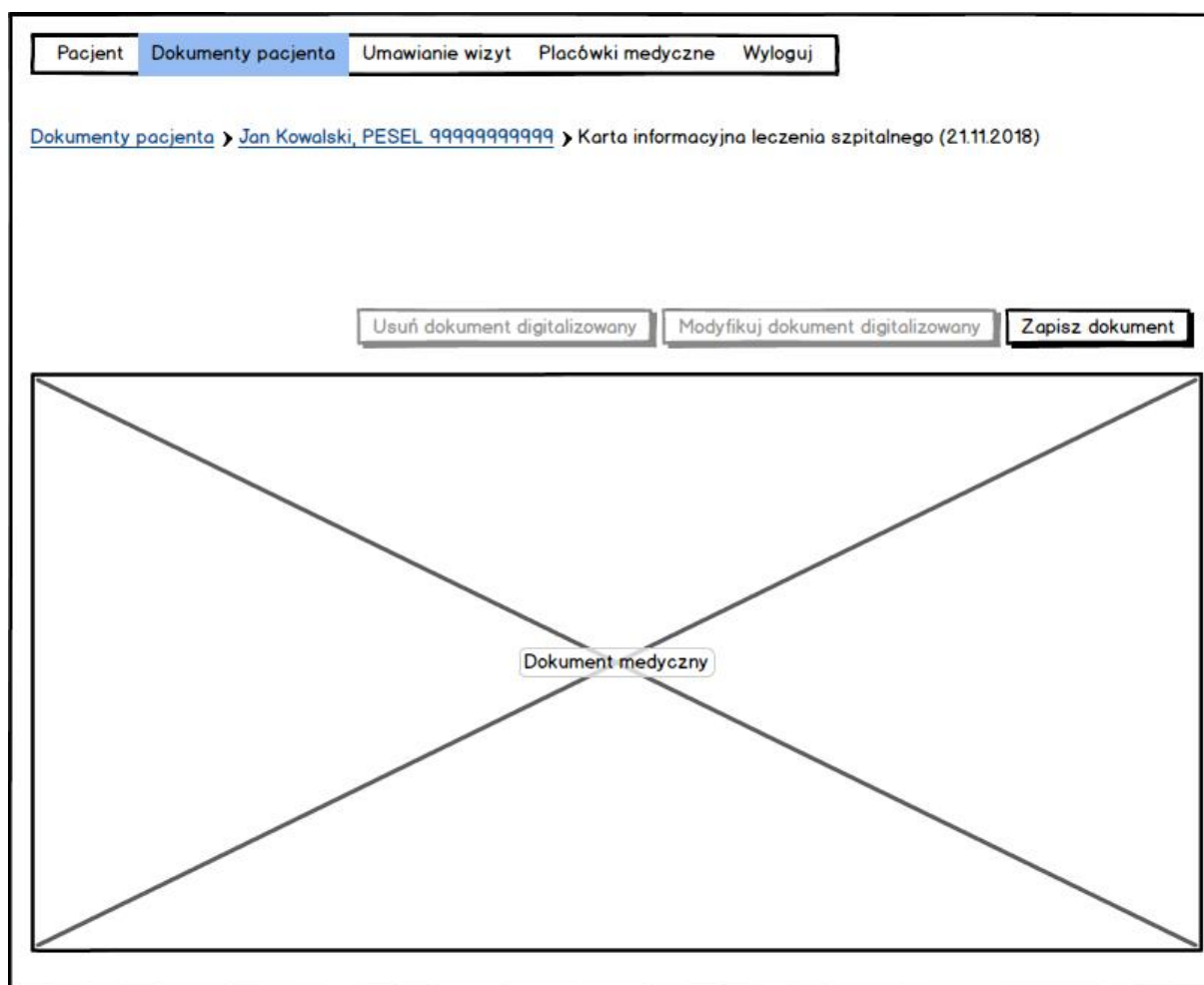
Wystawca dokumentu Wpisz fragment nazwiska Podmiot medyczny Wpisz fragment nazwy

☐ Zaznacz wszystkie Pobierz zaznaczone

	Data wystawienia	Typ dokumentu	Rodzaj placówki	Wystawca	Źródło
<input type="checkbox"/>	21.11.2018	<a href="#">Karta informacyjna leczenia szpitalnego</a>	Oddział kardiologiczny	dr Piotr Nowak	Szpital Wojewódzki w Krakowie
<input type="checkbox"/>	19.10.2018	<a href="#">Odmowa przyjęcia do szpitala</a>	Izba przyjęć szpitala	lek. Jan Wolski	Szpital Wojewódzki w Krakowie
<input type="checkbox"/>	15.09.2018	<a href="#">Sprawozdanie z badania laboratoryjnego</a>	Pracownia diagnostyki laboratoryjnej	mgr Wojciech Dąbrowski	Laboratorium Medyczne nr 1

Rysunek nr 2.61 Makieta ekranu „Dokumenty medyczne pacjenta”





Rysunek nr 2.62 Makieta ekranu „Dokument medyczny”

Pacjent

Dokumenty pacjenta

Umawianie wizyt

Placówki medyczne

Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

[Dokumenty](#) > Rezonans magnetyczny niskopoloowy głowy (06.01.2019)

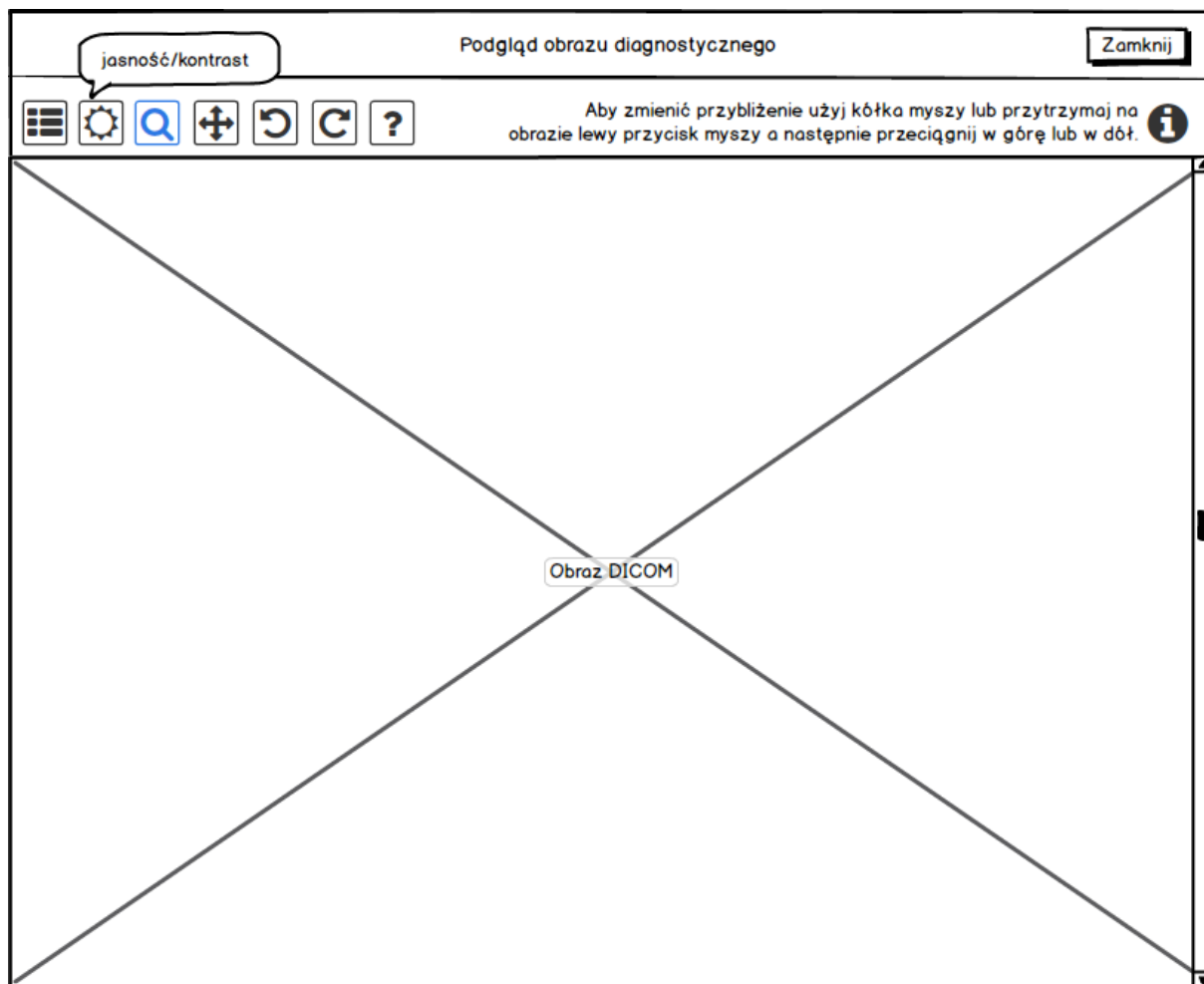
[Pokaż obrazy diagnostyczne](#)

Zapisz dokument

Pokaż historie udostępniania

Opis badania obrazowego w standardzie HL7 CDA

Rysunek nr 2.63 Makieta ekranu „Dokument medyczny dla opisu badania obrazowego”



Rysunek nr 2.64 Makieta ekranu „Przeglądarka obrazów diagnostycznych”

## 2.2.5 Moduł „Digitalizacja dokumentu medycznego”

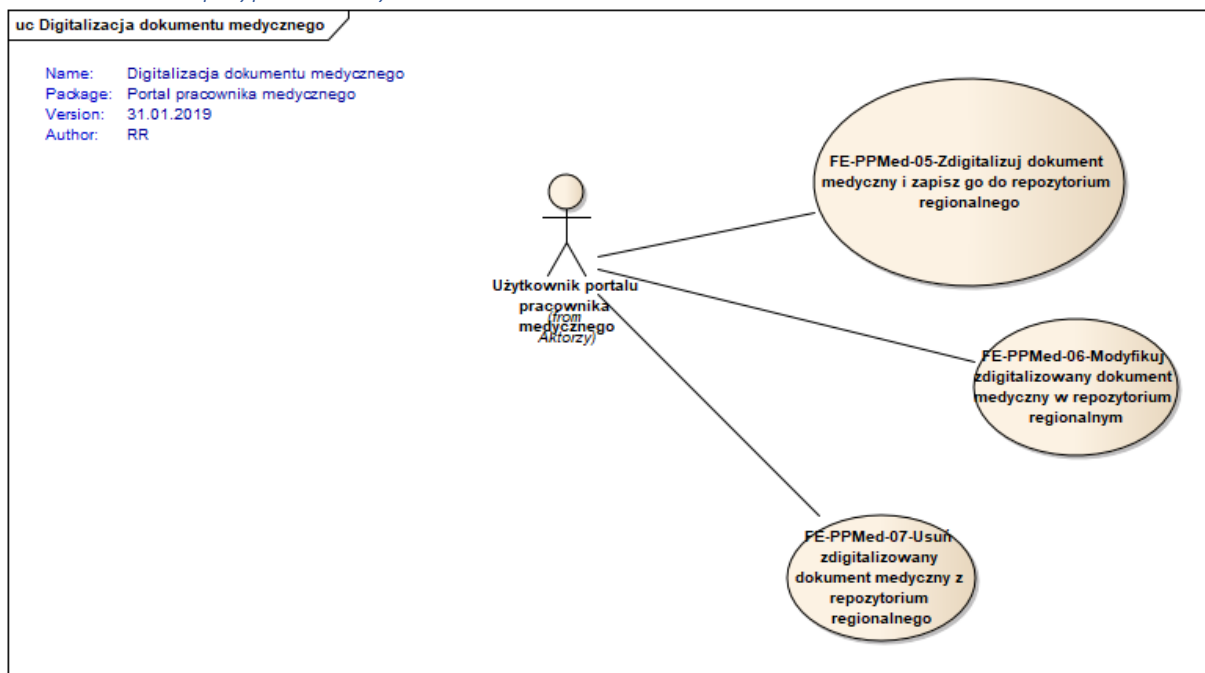
### 2.2.5.1 Wymagania funkcjonalne

**FE.PPMed.33.** System umożliwia tworzenie dokumentów HL7 CDA na poziomie 1 na podstawie wskazanego w zasobach lokalnych pliku skanu dokumentu medycznego oraz danych dodatkowych pochodzących z kontekstu działania aplikacji oraz wprowadzonych przez jej użytkownika.

**FE.PPMed.34.** System umożliwia usuwanie dokumentów zdigitalizowanych użytkownikowi, który je wytworzył.

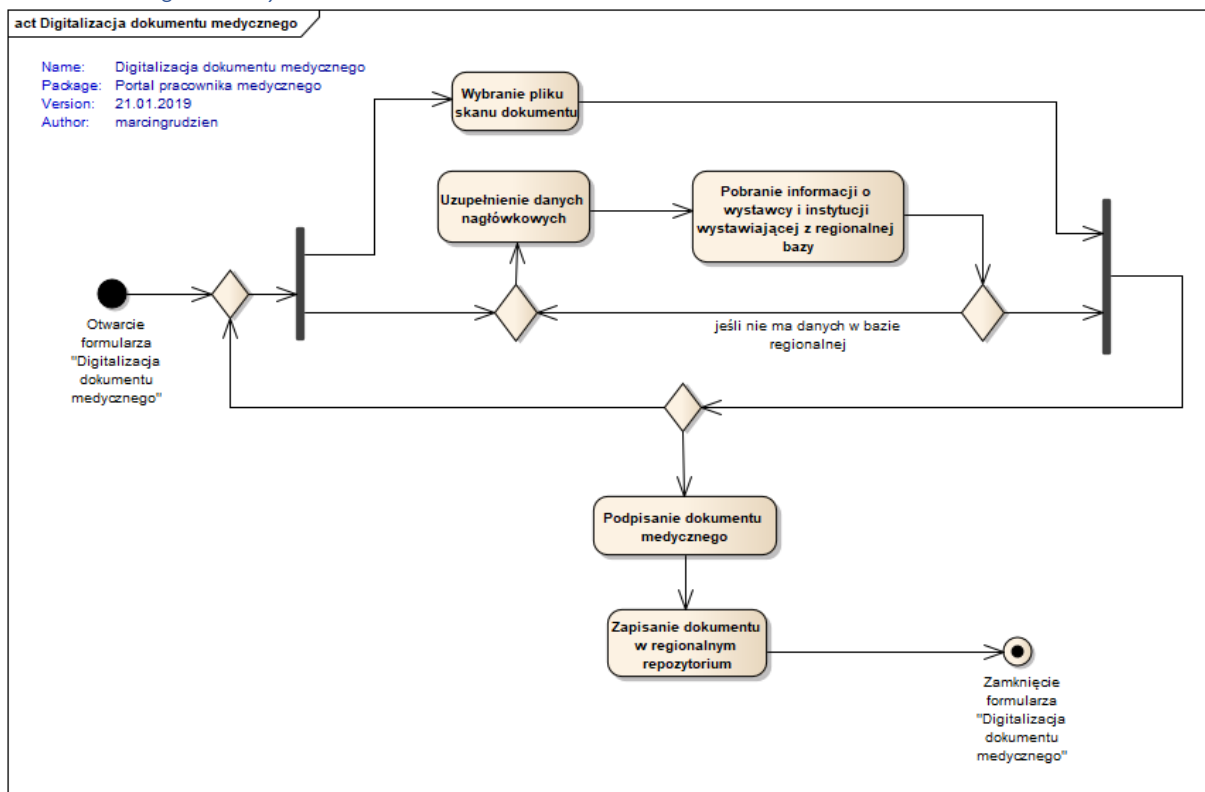
**FE.PPMed.35.** System umożliwia tworzenie nowej wersji dokumentu zdigitalizowanego na podstawie jego wersji przechowywanej w regionalnym repozytorium dokumentów.

### 2.2.5.2 Model przypadków użycia



Rysunek nr 2.65 Diagram przypadków użycia obszaru „Digitalizacja dokumentu medycznego”

### 2.2.5.3 Diagram aktywności



Rysunek nr 2.66 Diagram aktywności obszaru „Digitalizacja dokumentu medycznego”

#### 2.2.5.4 Model interfejsu użytkownika

Digitalizacja dokumentu medycznego			
Skan dokumentu	<input type="button" value="Wybierz plik..."/>		
Typ dokumentu	<input type="button" value="Wybierz"/>	Data wystawienia	<input type="text" value="/ /"/>
Tytuł dokumentu	<input type="text"/>	<input type="button" value="Skopiuj nazwę typu dokumentu"/>	
Język dokumentu	<input type="button" value="polski"/>	Poziom poufności	<input type="button" value="Zwykły"/>
Typ identyfikatora autora dokumentu	<input type="button" value="Wybierz"/>	Identyfikator autora/ wystawcy dokumentu	<input type="text"/>
Imię autora/wystawcy	<input type="text"/>	Nazwisko autora/wystawcy	<input type="text"/>
Identyfikator instytucji wystawiającej dokument	<input type="text"/>		
Nazwa instytucji wystawiającej dokument	<input type="text"/>		
<input type="button" value="Anuluj"/>		<input type="button" value="Zapisz w repozytorium"/>	

Rysunek nr 2.67 Makieta ekranu „Digitalizacja dokumentu medycznego”

Modyfikacja dokumentu digitalizowanego			
Skan dokumentu	<input type="button" value="Zmień plik"/>		
Typ dokumentu	<input type="button" value="Odmowa przyjęcia do szpitala"/>	Data wystawienia	<input type="text" value="/ /"/>
Tytuł dokumentu	<input type="text" value="Odmowa przyjęcia do szpitala"/>	<input type="button" value="Skopiuj nazwę typu dokumentu"/>	
Język dokumentu	<input type="button" value="polski"/>	Poziom poufności	<input type="button" value="Zwykły"/>
Typ identyfikatora autora dokumentu	<input type="button" value="NPWZ lekarza"/>	Identyfikator autora/ wystawcy dokumentu	<input type="text" value="6787873"/>
Imię autora/wystawcy	<input type="text" value="Piotr"/>	Nazwisko autora/wystawcy	<input type="text" value="Nowak"/>
Identyfikator instytucji wystawiającej dokument	<input type="text" value="10012-123"/>		
Nazwa instytucji wystawiającej dokument	<input type="text" value="CSK WUM w Warszawie"/>		
<input type="button" value="Anuluj"/>		<input type="button" value="Zapisz nową wersję dokumentu w repozytorium"/>	

Rysunek nr 2.68 Makieta ekranu „Modyfikacja dokumentu digitalizowanego”

## 2.2.6 Moduł „Umawianie wizyt”

### 2.2.6.1 Wymagania funkcjonalne

**FE.PPMed.36.** System umożliwia pracownikowi medycznemu wyszukanie w grafikach udostępnionych przez systemy lokalne wolnych terminów wizyt spełniających podane kryteria wyszukiwania.

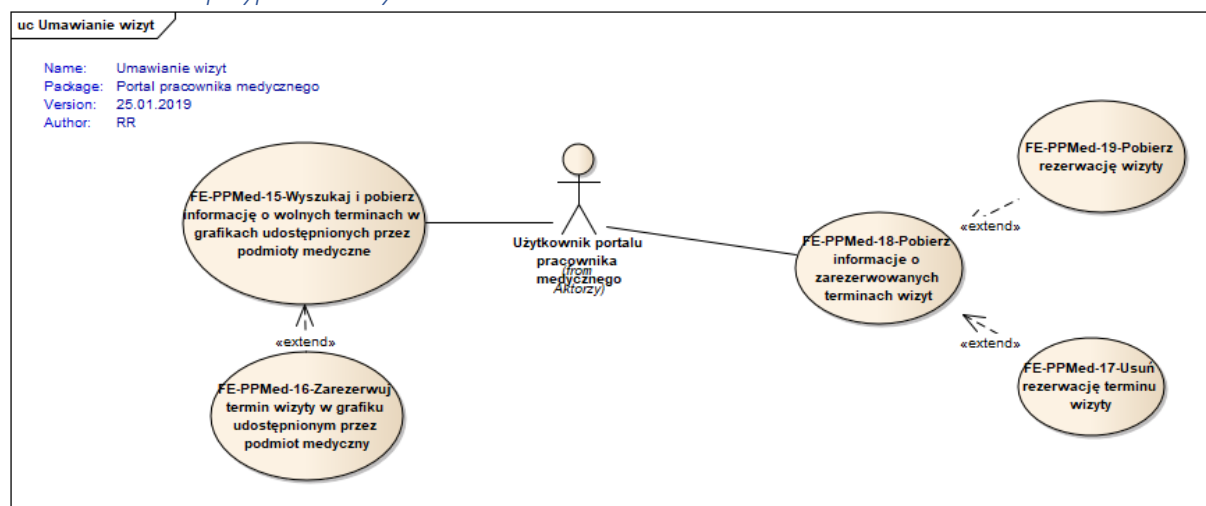
**FE.PPMed.37.** System umożliwia pracownikowi medycznemu dokonanie rezerwacji terminu wizyty w grafiku udostępnionym przez system lokalny.

**FE.PPMed.38.** System udostępnia pracownikowi medycznemu informacje o rezerwacjach terminów wizyt danego pacjenta dokonanych za pośrednictwem platformy MSIM.

**FE.PPMed.39.** System umożliwia pracownikowi medycznemu modyfikację rezerwacji terminu wizyty dokonanej za pośrednictwem platformy MSIM.

**FE.PPMed.40.** System umożliwia pracownikowi medycznemu usunięcie rezerwacji terminu wizyty dokonanej za pośrednictwem platformy MSIM.

### 2.2.6.2 Model przypadków użycia



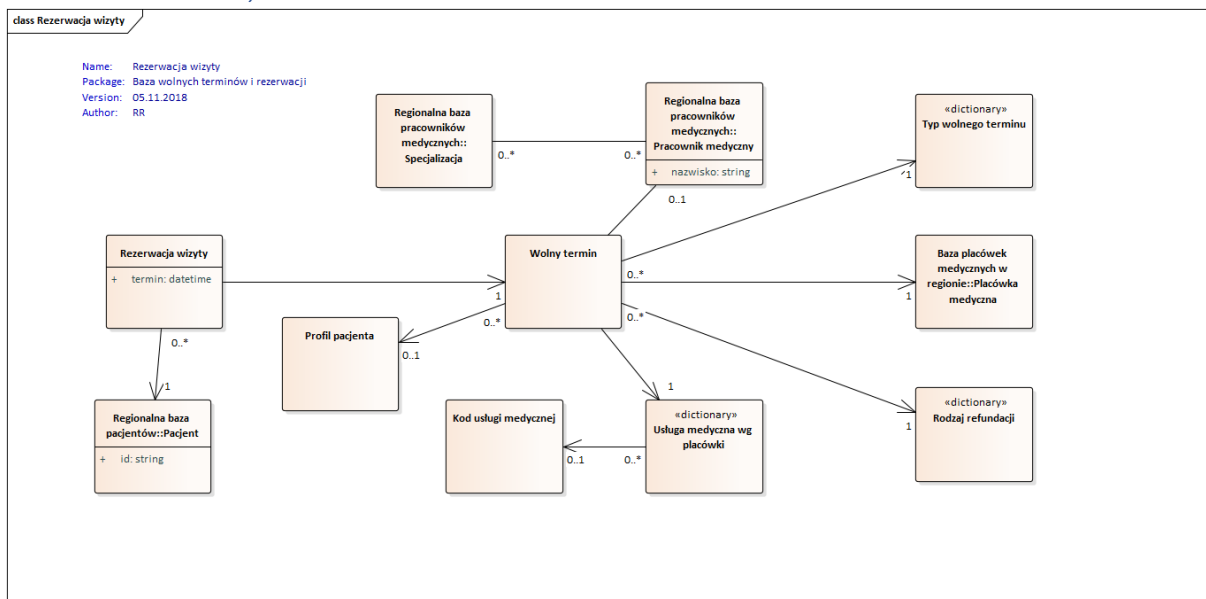
Rysunek nr 2.69 Diagram przypadków użycia obszaru „Umawianie wizyt”

### 2.2.6.3 Diagram aktywności

Moduł „Umawianie wizyt” realizuje procesy w analogiczny sposób do odpowiadającego mu nazwą modułu aplikacji Portal pacjenta. Poniżej przedstawiono wspólny dla tych modułów obu aplikacji diagram aktywności.



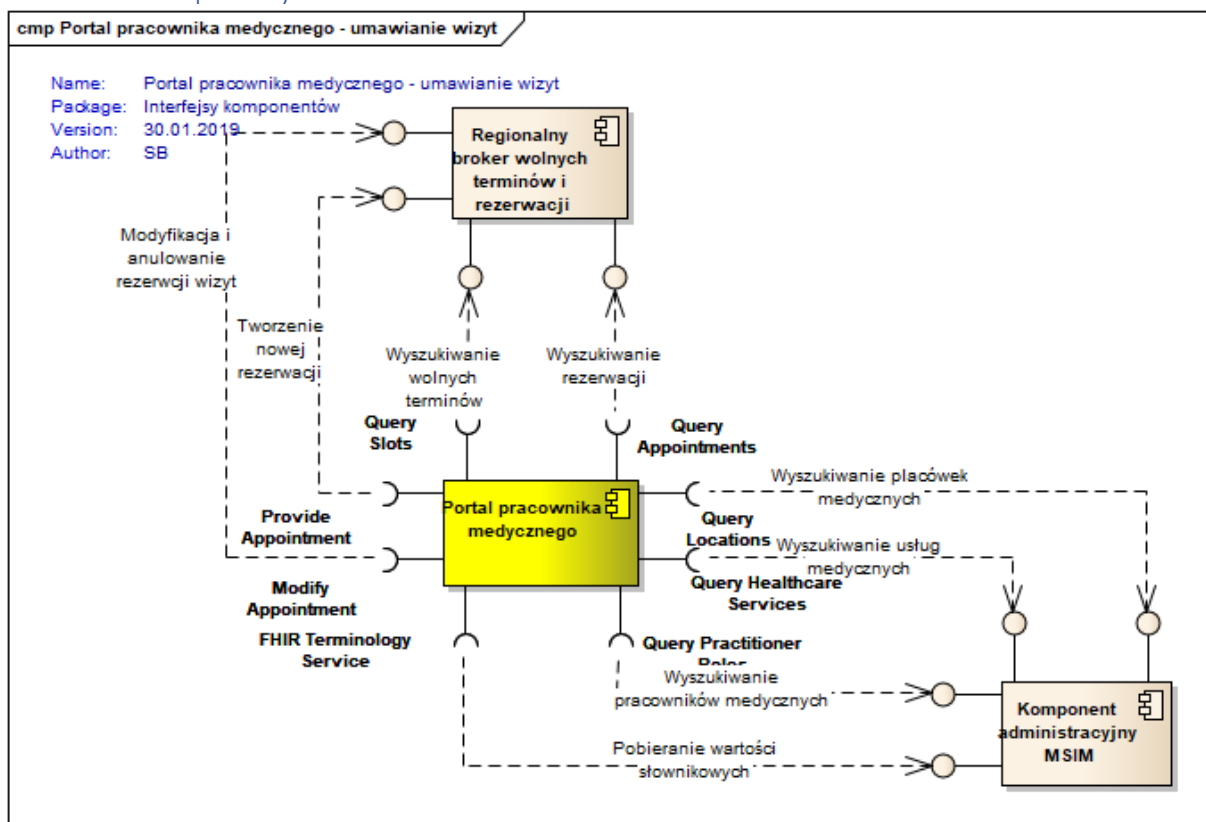
## 2.2.6.4 Model danych



Rysunek nr 2.71 Diagram klas obszaru „Umawianie wizyt”

## 2.2.6.5 Komponenty i transakcje

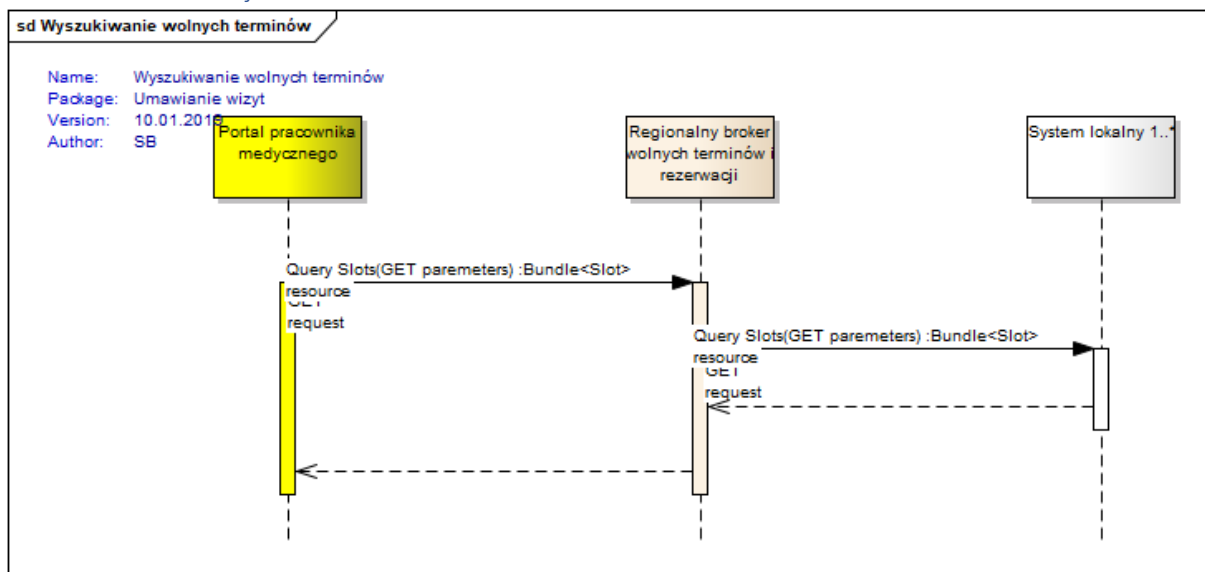
### 2.2.6.5.1 Komponenty



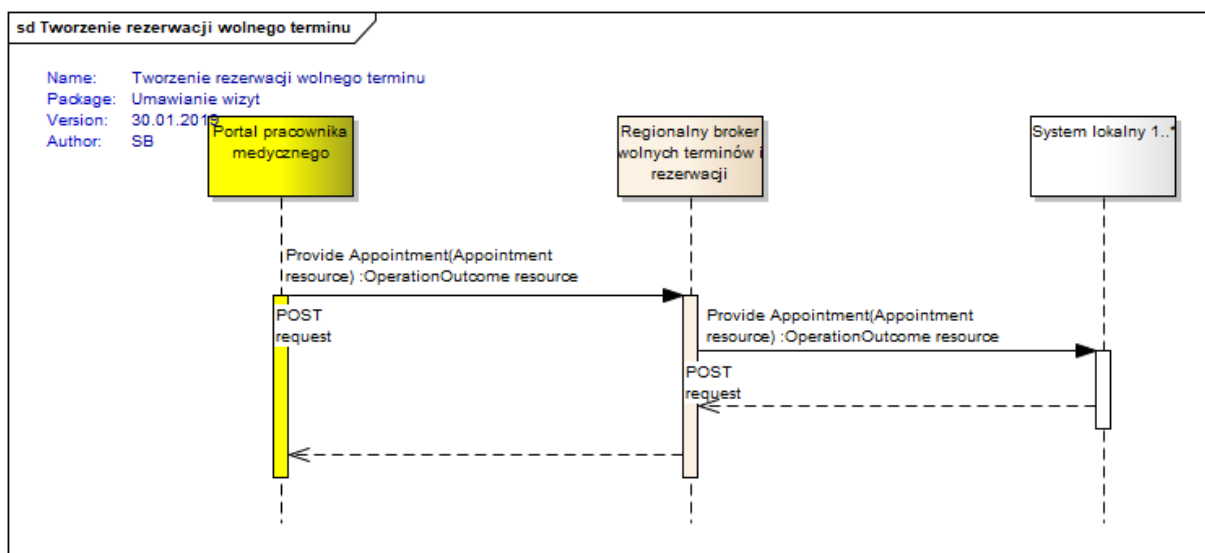
Rysunek nr 2.72 Diagram komponentów obszaru „Umawianie wizyt”



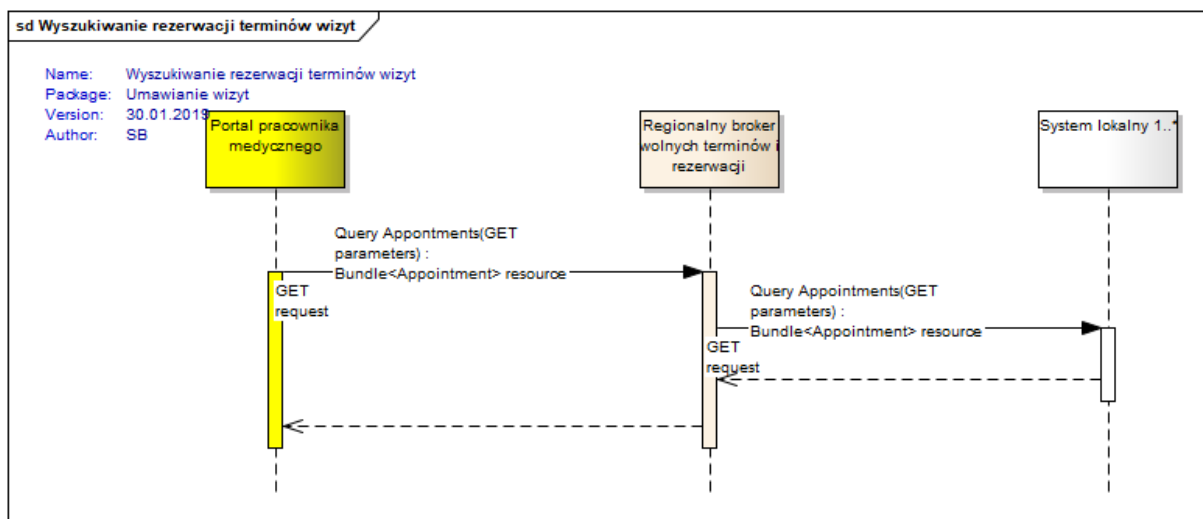
## 2.2.6.5.2 Transakcje



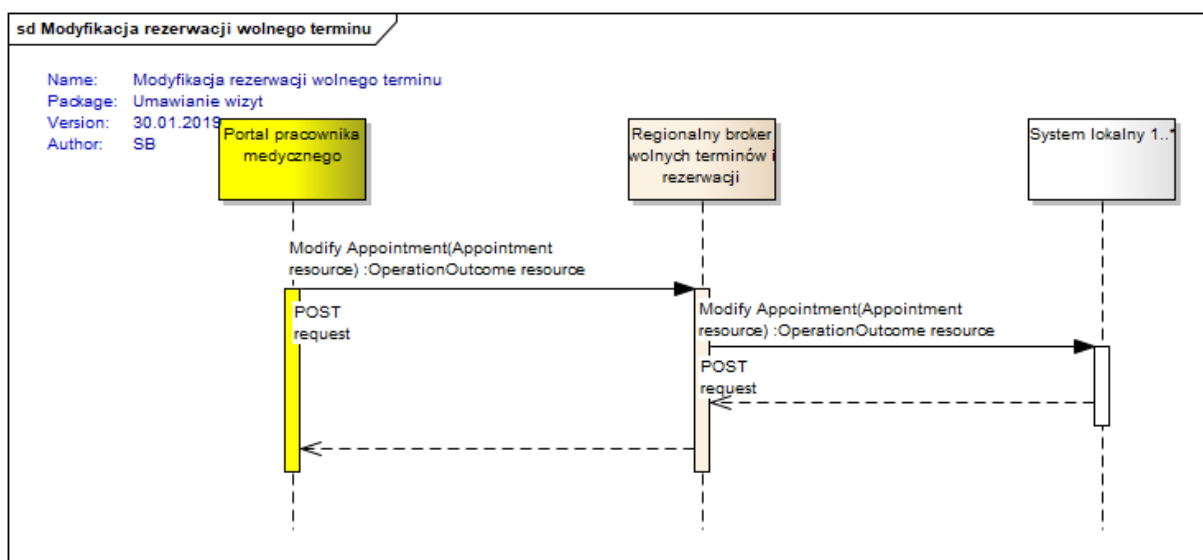
Rysunek nr 2.73 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów”



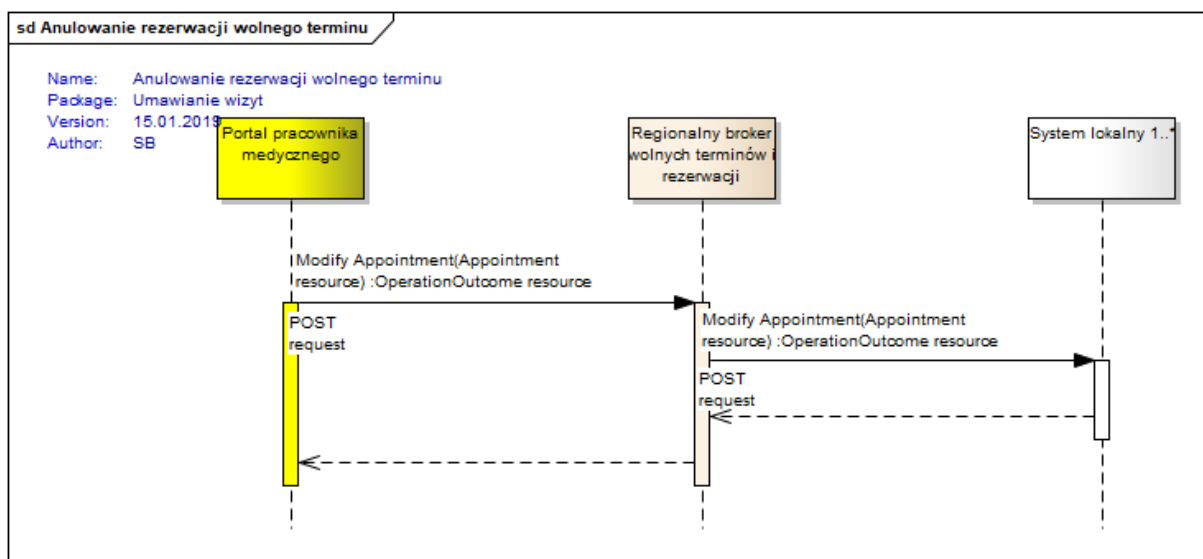
Rysunek nr 2.74 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu”



Rysunek nr 2.75 Diagram sekwencji transakcji „Wyszukiwanie rezerwacji terminów wizyt”



Rysunek nr 2.76 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu”



Rysunek nr 2.77 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu”

### 2.2.6.6 Model interfejsu użytkownika

Pacjent
Dokumenty pacjenta
Umawianie wizyt
Placówki medyczne
Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

Umów nową wizytę

Data i godz. wizyty	Usługa	Lekarz	Placówka medyczna	Podmiot leczniczy
<a href="#">15.07.2018 14:15</a>	Konsultacja neurologa	prof. Nowak	Przyszpitalna poradnia specjalistyczna Kraków, os. Złotej jesieni 1	Szpital Specjalistyczny im. Ludwika Rydygiera
<a href="#">22.09.2018 10:30</a>	USG j. brzusznej		Pracownia diagnostyki obrazowej Kraków, ul. Prądnicka 80	Krakowski Szpital Specjalistyczny im. Jana Pawła II
<a href="#">26.09.2018 12:40</a>	Gastroskopia		Pracownia endoskopii Kraków, ul. Prądnicka 35	Szpital Miejski Specjalistyczny im. G. Narutowicza

Rysunek nr 2.78 Makieta ekranu „Umawianie wizyt”

Pacjent
Dokumenty pacjenta
Umawianie wizyt
Placówki medyczne
Wyloguj

Pacjent: Jan Kowalski, PESEL 9999999999

[Wizyty](#) > Konsultacja neurologa (15.07.2018)

Zmień termin wizyty    Odwołaj rezerwację

Termin wizyty: 15.07.2018 godz. 14:15  
Usługa: Konsultacja neurologa  
Lekarz: prof. Jan Nowak

Placówka medyczna:  
Przyszpitalna poradnia specjalistyczna  
Kraków, os. Złotej jesieni 1  
Szpital Specjalistyczny im. Ludwika Rydygiera

Rysunek nr 2.79 Makieta ekranu „Szczegóły rezerwacji wizyty”

Pacjent
Dokumenty pacjenta
**Umawianie wizyt**
Placówki medyczne
Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Wizyty](#) > Nowa wizyta

Parametry wyszukiwania

Miejscowość

Kraków

☐ Szukaj w pobliżu

Usługa

Wpisz fragment nazwy

Pracownik medyczny

Wpisz fragment nazwiska

Specjalność pracownika

Wpisz fragment nazwy specjalności

Placówka/podmiot

Wpisz fragment nazwy

Rodzaj placówki

Wpisz fragment nazwy

Typ wizyty

Wybierz z listy

Refundacja

Wybierz z listy

Wyszukaj

Pokaż od: / /

26.05.2018 10:20

Konsultacja kardiologa, dr Piotr Kowalczyk

Poradnia kardiologiczna, ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

29.05.2018 10:20

Konsultacja kardiologa, dr Janusz Budny

Poradnia kardiologiczna, ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

10.05.2018 10:20

Konsultacja kardiologa, prof. Wojciech Mleczko

Przyszpitalna poradnia specjalistyczna, ul. Prądnicka 80, Kraków

Krakowski Szpital Specjalistyczny im. Jana Pawła II

Pokaż kolejne

Rysunek nr 2.80 Makieta ekranu „Wyszukiwanie wolnych terminów”

Pacjent
Dokumenty pacjenta
**Umawianie wizyt**
Placówki medyczne
Wyloguj

**Pacjent: Jan Kowalski, PESEL 9999999999**

[Wizyty](#) > [Nowa wizyta](#) > Konsultacja kardiologa (25.06.2018)

Zarezerwuj ten termin

Termin wizyty:

26.05.2018 godz. 10:20

Usługa:

Konsultacja kardiologa

Lekarz:

dr Piotr Kowalczyk

Placówka medyczna:

Poradnia kardiologiczna

ul. Prądnicka 35, Kraków

Szpital Miejski Specjalistyczny im. G. Narutowicza

Rysunek nr 2.81 Makieta ekranu "Nowa wizyta"

## 2.3 Wymagania нефункционалне aplikacji portalowych

Poniższe wymagania нефункционалне dotyczą wszystkich modułów obu aplikacji portalowych Platformy MSIM.

### 2.3.1 Wymagania wydajnościowe

**FE.NFun.1.** Strony serwisów www muszą być generowane w czasie poniżej 1 sekundy, czyli czas kliknięcia przez użytkownika w odpowiedni element serwisu a otrzymaniem i uzyskaniem odpowiedzi, nie może przekraczać 1s.

**FE.NFun.2.** Czas dostępu do dokumentów w aplikacjach portalowych nie może być dłuższy niż 10s.

**FE.NFun.3.** Pojedyncza akcja związana z nawigacją w aplikacjach portalowych nie może być dłuższa niż 1 s.

**FE.NFun.4.** Pojedyncza akcja związana z zatwierdzeniem wprowadzanych lub pobieranych danych w aplikacjach portalowych nie może być dłuższa niż 5s.

**FE.NFun.5.** Wynik wyszukiwania w aplikacjach portalowych nie może być dłuższy niż 5s w ramach rejestru regionalnego.

**FE.NFun.6.** Testy wydajności zrealizowane zostaną na urządzeniach brzegowych Platformy MSIM i będzie mierzone jako czas od momentu pojawienia się żądania informacji od systemu do czasu pojawienia się odpowiedzi z systemu.

**FE.NFun.7.** Aplikacje portalowe zapewniają możliwość obsługi minimum 5 000 000 nazwanych kont użytkowników.

**FE.NFun.8.** Aplikacje portalowe zapewniają możliwość jednoczesnej pracy dla 2500 użytkowników.

### 2.3.2 Wymagania dotyczące dostępności

**FE.NFun.9.** Aplikacje portalowe umożliwiają pracę w co najmniej 3 najpopularniejszych w Polsce silnikach przeglądarek, określonych na moment zakończenia analizy przedwdrożeniowej.

**FE.NFun.10.** Aplikacje portalowe stosują mechanizmy responsywności w celu umożliwienia prawidłowego korzystania z wszystkich funkcjonalności i treści na różnych rozdzielczościach.

**FE.NFun.11.** Aplikacje portalowe umożliwiają pracę na komputerach z użyciem rozdzielczości co najmniej 1280x720px.

**FE.NFun.12.** Aplikacje portalowe umożliwiają pracę na urządzeniach mobilnych z użyciem rozdzielczości co najmniej 320x568dp.

**FE.NFun.13.** Aplikacje portalowe spełniają wytyczne WCAG 2.0 co najmniej na poziomie AAA.

**FE.NFun.14.** Jeżeli na moment rozpoczęcia prac wykonawczych standard WCAG zostanie zaktualizowany o nowszą wersję którejkolwiek z wytycznych lub kryteriów ich spełnienia na poziomie AAA, pierwszeństwo wobec niniejszych wymagań będą miały wytyczne z aktualnego standardu WCAG.

**FE.NFun.15.** Aplikacje portalowe zapewniają tekst alternatywny dla każdej informacji nietekstowej.

- FE.NFun.16.** Aplikacje portalowe umożliwiają skorzystanie z zabezpieczenia typu CAPTCHA przez osoby niewidome.
- FE.NFun.17.** Aplikacje portalowe zapewniają napisy do każdego materiału audio lub wideo posiadającego dźwięk.
- FE.NFun.18.** Aplikacje portalowe zapewniają audiodeskrypcję dla każdego materiału wideo.
- FE.NFun.19.** Materiały wideo, w których synchronizacja ścieżki dźwiękowej uniemożliwia dodanie audiodeskrypcji, mają zapewnioną wersję alternatywną z pauzami, które tę audiodeskrypcję umożliwią.
- FE.NFun.20.** Aplikacje portalowe zapewniają tłumaczenie w języku migowym dla każdego materiału audio lub wideo posiadającego dźwięk.
- FE.NFun.21.** Aplikacje portalowe zapewniają transkrypcję opisową dla materiałów wideo.
- FE.NFun.22.** Aplikacje portalowe implementują znaczniki semantyczne HTML zgodnie z ich przeznaczeniem, w sposób umożliwiający prawidłową pracę programom czytającym.
- FE.NFun.23.** Aplikacje portalowe implementują kolejność informacji w strukturze stron HTML zgodnie z ich logiczną kolejnością, w sposób umożliwiający prawidłową pracę programom czytającym.
- FE.NFun.24.** Aplikacje portalowe nie opierają elementów nawigacyjnych ani komunikatów wyłącznie na charakterystykach zmysłowych.
- FE.NFun.25.** Aplikacje portalowe nie używają koloru jako jedynej metody przekazywania treści i rozróżniania elementów.
- FE.NFun.26.** Aplikacje portalowe umożliwiają wyłączanie i włączanie dźwięku na każdej stronie, która odtwarza dźwięk.
- FE.NFun.27.** Aplikacje portalowe prezentują treści tekstowe z zachowaniem wysokiego kontrastu, domyślnie lub w formie przełączania w dedykowany tryb wysokiego kontrastu.
- FE.NFun.28.** Aplikacje portalowe umożliwiają wyświetlanie zawartości tekstowej w powiększeniu do 200% bez utraty zawartości lub funkcjonalności, z zastosowaniem natywnego mechanizmu przeglądarki lub dedykowanego mechanizmu strony internetowej.
- FE.NFun.29.** Aplikacje portalowe nie używają grafiki do wyświetlenia tekstu, z wyjątkiem tekstów lub logotypów marki lub produktu.
- FE.NFun.30.** Treści audio zawierające głównie mowę publikowane w aplikacjach portalowych nie mają utrudniającego odbiór tła dźwiękowego.
- FE.NFun.31.** Aplikacje portalowe przedstawiają tekst w sposób nieutrudniający jego odczytania osobom z problemami poznawczymi.
- FE.NFun.32.** Aplikacje portalowe umożliwiają zmianę kolorów tekstu i kolorów tła.
- FE.NFun.33.** Aplikacje portalowe przedstawiają tekst w blokach o szerokości nie przekraczającej 80 znaków.
- FE.NFun.34.** Aplikacje portalowe przedstawiają tekst w blokach bez wyjustowania.

- FE.NFun.35.** Aplikacje portalowe przedstawiają tekst z zachowaniem interlinii minimum 1,5 oraz odstępem między akapitami minimum 150% wartości interlinii.
- FE.NFun.36.** Aplikacje portalowe przedstawiają tekst w blokach umożliwiającym odczytanie wiersza po powiększeniu do 200% bez konieczności przewijania poziomego.
- FE.NFun.37.** Aplikacje portalowe umożliwiają nawigację przy użyciu samej klawiatury, w całej aplikacji bez wyjątków.
- FE.NFun.38.** Aplikacje portalowe nie ograniczają czasu na wykonanie czynności.
- FE.NFun.39.** Aplikacje portalowe umożliwiają zatrzymanie lub ukrycie automatycznie aktualizujących się informacji lub komponentów GUI.
- FE.NFun.40.** Aplikacje portalowe, przy ponownym zalogowaniu po uprzednim upływie czasu sesji, zapamiętują wprowadzone przed wylogowaniem dane wprowadzone w formularzach.
- FE.NFun.41.** Aplikacje portalowe nie zawierają treści migających z częstotliwością większą niż 3Hz.
- FE.NFun.42.** Aplikacje portalowe umożliwiają pomijanie stałych elementów nawigacji przez programy czytające.
- FE.NFun.43.** Aplikacje portalowe stosują tytuły stron odzwierciedlające zawartość.
- FE.NFun.44.** Aplikacje portalowe zapewniają kolejność zaznaczania elementów zgodną z ich logicznym pogrupowaniem.
- FE.NFun.45.** Aplikacje portalowe zapewniają jednoznaczne określenie celów linków dla programów czytających.
- FE.NFun.46.** Aplikacje portalowe udostępniają minimum dwa alternatywne sposoby nawigacji spośród następujących: spis treści, mapa serwisu, wyszukiwarka, lista powiązanych podstron.
- FE.NFun.47.** Aplikacje portalowe stosują unikalne nagłówki oraz unikalne etykiety pól formularzy.
- FE.NFun.48.** Aplikacje portalowe wyróżniają element strony, na którym znajduje się fokus, przy nawigacji z użyciem klawiatury i klawisza tab.
- FE.NFun.49.** Aplikacje portalowe prezentują użytkownikowi miejsce w mapie strony, w którym aktualnie się znajduje.
- FE.NFun.50.** Aplikacje portalowe stosują nagłówki w sekcjach treści tekstowych.
- FE.NFun.51.** Aplikacje portalowe implementują określenie głównego języka strony w sposób obsługiwany przez programy czytające.
- FE.NFun.52.** Aplikacje portalowe implementują określenie języka elementów strony w sposób obsługiwany przez programy czytające.
- FE.NFun.53.** Aplikacje portalowe udostępniają tłumaczenia i definicje dla nietypowych słów lub fachowego żargonu.
- FE.NFun.54.** Aplikacje portalowe udostępniają rozwinięcia stosowanych w tekstach skrótów.
- FE.NFun.55.** Aplikacje portalowe udostępniają streszczenia, ilustracje, filmy lub inne media wyjaśniające treści o poziomie skomplikowania wymagającym wykształcenia wyższego niż gimnazjalne.

**FE.NFun.56.** Aplikacje portalowe nie wykonują akcji w odpowiedzi na samą zmianę fokusa między komponentami GUI.

**FE.NFun.57.** Aplikacje portalowe zmieniają kontekst (nowe okno, popup, nowa zakładka, odświeżenie strony, znaczna zmiana rozmieszczenia komponentów GUI) tylko na żądanie użytkownika, lub udostępniają mechanizm wyłączenia automatycznej zmiany kontekstu.

**FE.NFun.58.** Aplikacje portalowe stosują stały układ dla powtarzających się elementów nawigacji.

**FE.NFun.59.** Aplikacje portalowe mają stały sposób identyfikacji komponentów GUI realizujących tę samą funkcjonalność.

**FE.NFun.60.** Aplikacje portalowe stosują walidację pól formularzy z komunikatami jednoznacznie wskazującymi na przyczynę błędów możliwych do poprawy przez użytkownika.

**FE.NFun.61.** Aplikacje portalowe stosują walidację pól formularzy z komunikatami sugerującymi sposób rozwiązania błędów możliwych do poprawy przez użytkownika.

**FE.NFun.62.** Aplikacje portalowe mają etykiety pól formularzy informujące o wymaganej treści oraz formacie danych do wprowadzenia.

**FE.NFun.63.** Aplikacje portalowe wymagają potwierdzenia operacji modyfikacji lub usuwania danych lub umożliwiają przywrócenie poprzedniej ich wersji.

**FE.NFun.64.** Aplikacje portalowe wymagają potwierdzenia zobowiązań prawnych lub transakcji finansowych podejmowanych przez użytkownika.

**FE.NFun.65.** Aplikacje portalowe udostępniają pełną informację o sposobie wprowadzania, zmiany lub kasowania danych, wszędzie tam gdzie ono występuje.

**FE.NFun.66.** Aplikacje portalowe implementują HTML w wersji co najmniej 5 oraz CSS w wersji co najmniej 3, z zachowaniem standardów W3C w sposób pozwalający na pomyślne przejście walidacji składni.

**FE.NFun.67.** Aplikacje portalowe stosują jednoznaczną identyfikację standardowych oraz niestandardowych (wytworzonych przez Wykonawcę) komponentów GUI.

### 2.3.3 Wymagania dotyczące skalowalności

**FE.NFun.68.** System zapewnia skalowalność pionową poprzez możliwość rozbudowy poszczególnych elementów infrastruktury techniczno-systemowej:

1. procesor, pamięć, dyski, interfejsy;
2. dodatkowe półki dyskowe, dodatkowe dyski;
3. zwiększenie zasobów dla systemu operacyjnego.

**FE.NFun.69.** System zapewnia skalowalność poziomą poprzez:

1. Możliwość rozbudowy o kolejne węzły obliczeniowe: serwery fizyczne, urządzenia sieciowe, macierze dyskowe, oprogramowanie narzędziowe, komponenty aplikacyjne;
2. Klastry wysokiej dostępności.

**FE.NFun.70.** W przypadku awarii lub aktualizacji, wyłączenie jednego z elementów nie ma wpływu na funkcjonowanie systemu.

**FE.NFun.71.** Zapewniona jest wysoka wydajność (klaster HA) – możliwość zwiększania o dodatkowe systemy, serwery aplikacyjne, bazy danych, aplikacje.



- FE.NFun.72.** Brak jest technicznych i licencyjnych ograniczeń na ilość danych gromadzonych w Systemie, zasobów infrastrukturalnych.
- FE.NFun.73.** Brak jest technicznych i licencyjnych ograniczeń na ilość procesów zaimplementowanych w Systemie.
- FE.NFun.74.** Zapewniona jest możliwość zmiany wymaganych parametrów usług i ich skalowania zgodnie z potrzebami.
- FE.NFun.75.** Zapewniona jest możliwość automatycznego skalowania mocy obliczeniowej Platformy MSIM.

#### 2.3.4 Wymagania dotyczące bezpieczeństwa i niezawodności

- FE.NFun.76.** Dostęp do danych i wymiany danych jest możliwy tylko w ramach zestawionego szyfrowanego protokołu TLS w wersji minimum 1.2.
- FE.NFun.77.** Dostęp do danych i wymiany danych może zostać zabezpieczony dodatkowo za pomocą VPN w ramach połączenia site-to-site zabezpieczonego certyfikatem i hasłem.
- FE.NFun.78.** Komunikacja między komponentami Platformy MSIM musi być szyfrowana zgodnie z założeniami profilu IHE ATNA.
- FE.NFun.79.** Wzajemne uwierzytelnienie komponentów Platformy MSIM musi być zgodne z założeniami profilu IHE ATNA.
- FE.NFun.80.** Ruch z i do Internetu musi być filtrowany i poddawany inspekcji.
- FE.NFun.81.** Wszystko co nie jest dozwolone jest zabronione.
- FE.NFun.82.** Poszczególne komponenty muszą być umieszczone w wydzielonych strefach, pomiędzy którymi ruch jest filtrowany i wykonywana jest inspekcja.
- FE.NFun.83.** Wykonywana jest cykliczna aktualizacja infrastruktury techniczno-systemowej.
- FE.NFun.84.** Wykonywany jest comiesięczny raport poprawek wydawanych przez producentów każdego ze składników infrastruktury techniczno-systemowej, wraz z rekomendacjami dotyczącymi ich wdrażania.
- FE.NFun.85.** Sesje zalogowanych użytkowników wygasają po określonym, możliwym do skonfigurowania czasie.
- FE.NFun.86.** Administracja platformą w zakresie infrastruktury techniczno-systemowej jest możliwa tylko poprzez bezpieczne kanały komunikacji (VPN)
- FE.NFun.87.** Elementy infrastruktury techniczno-systemowej muszą być poddawane okresowemu tzw. utwardzaniu (ang. hardening).
- FE.NFun.88.** Utwardzanie odbywa się nie rzadziej niż co 3 miesiące.
- FE.NFun.89.** Dokumenty medyczne przechowywane w repozytorium są szyfrowane. Szyfrowanie wykonywane jest przy wykorzystaniu sprzętowych modułów kryptograficznych.
- FE.NFun.90.** Przyjmowane do repozytorium regionalnego dokumenty muszą podlegać inspekcji antywirusowej przy wykorzystaniu urządzeń typu UTM.
- FE.NFun.91.** Musi być zapewniona integralność dokumentów poprzez podpis cyfrowy przewidziany przepisami prawa w zakresie podpisywania dokumentacji medycznej.

- FE.NFun.92.** Każda interakcja komponentów MSIM między sobą oraz z systemami lokalnymi wymaga synchronizacji czasu zgodnie z założeniami profilu IHE CT.
- FE.NFun.93.** Rozliczalność zdarzeń jest zapewniona.
- FE.NFun.94.** Zdarzenia związane z przetwarzaniem danych osobowych, w szczególności pozyskaniem, wytworzeniem, dostępem (odczytem), zmianą lub usunięciem, są rejestrowane z wskazaniem osoby i okoliczności ich zaistnienia (w szczególności czasu).
- FE.NFun.95.** Zdarzenia związane z wyrażeniem lub cofnięciem zgody podmiotu danych osobowych na ich przetwarzanie, są rejestrowane z wskazaniem okoliczności ich zaistnienia (w szczególności daty i godziny, sposobu pozyskania).
- FE.NFun.96.** Dostęp do logów aplikacyjnych i systemowych zawierających dane osobowe, w szczególności adresy IP indywidualnych użytkowników, podlega rejestrowaniu z wskazaniem osoby i czasu jego zaistnienia.
- FE.NFun.97.** System musi tworzyć cyklicznie kopie zapasowe:
1. Kopie przyrostowe - minimum w cyklu dobowym,
  2. Pełne kopie systemu - minimum w cyklu tygodniowym,
  3. Pełny backup z kopią systemów operacyjnych - minimum w cyklu czterotygodniowym,
  4. Kopie zapasowe muszą być odmiejszczawiane.
- FE.NFun.98.** W momencie przystąpienia do realizacji prac wykonawczych, procedura i częstotliwość wykonywania kopii zapasowych może zostać ustalona przez Zamawiającego na innym poziomie.
- FE.NFun.99.** Przywrócenie usług do punktu w czasie sprzed awarii (RPO) wynosi 1h.
- FE.NFun.100.** Dostępność usług Platformy MSIM wynosi 99,0% w skali miesiąca.
- FE.NFun.101.** System umożliwia ciągły dostęp do danych medycznych i do dokumentów medycznych gromadzonych w Systemie co najmniej z ostatnich pięciu lat. W tym czasie dane i dokumenty nie są archiwizowane ani poddawane działaniom, które zwiększałyby czas dostępu do nich.
- FE.NFun.102.** Logi mogą być poddawane archiwizacji.
- FE.NFun.103.** System przechowuje dane medyczne i dokumenty medyczne przez okres wymagany obowiązującymi przepisami prawa dla każdej z kategorii danych medycznych i dokumentów medycznych.
- FE.NFun.104.** Okres ciągłego dostępu oraz okresy przechowywania dla poszczególnych kategorii danych medycznych i dokumentów medycznych jest możliwy do skonfigurowania.
- FE.NFun.105.** System musi być zgodny z politykami bezpieczeństwa opracowywanymi w toku projektu, w tym polityką bezpieczeństwa administratora danych platformy MSIM.
- FE.NFun.106.** System musi być zgodny z polityką kopii zapasowych Zamawiającego:
1. Testy odtworzenia wybranych elementów nie rzadziej niż raz w miesiącu,

2. Testy odtworzenia całości systemu nie rzadziej niż raz na trzy miesiące,
3. Testy podatności systemu wraz z rekomendacjami nie rzadziej niż raz w miesiącu oraz po każdej aktualizacji.

**FE.NFun.107.** System musi uniemożliwiać nieautoryzowany dostęp.

**FE.NFun.108.** Uwierzytelnienie jest wykonywane przy wykorzystaniu zaufanych dostawców tożsamości m.in. KWIE (Krajowy Węzeł Identyfikacji Elektronicznej).

**FE.NFun.109.** Uwierzytelnienie systemów pomiędzy Platformą regionalną a podmiotami medycznymi jest wykonywane przy wykorzystaniu wzajemnego uwierzytelniania (Mutual Authentication). Platforma regionalna jest dostawcą tożsamości.

**FE.NFun.110.** Interfejsy oparte o standard HL7 FHIR muszą wykorzystywać OAuth w wersji co najmniej 2.0 dla uwierzytelniania użytkowników.

**FE.NFun.111.** Dostęp do danych musi być realizowany poprzez prawa dostępu dla poszczególnych użytkowników i musi być rozliczalny.

**FE.NFun.112.** Uprawnienia dla użytkowników są nadawane wg zasady najmniejszego uprzywilejowania.

**FE.NFun.113.** Uprawnienia dla użytkowników są pogrupowane w konfigurowalne role systemowe.

**FE.NFun.114.** Poszczególne komponenty systemu muszą działać niezależnie na odseparowanych węzłach. Wyłączenie jednego z komponentów z klastra wysokiej dostępności nie będzie miało wpływu na pozostałe komponenty.

**FE.NFun.115.** System musi obsługiwać awarie poszczególnych węzłów danego komponentu. Ruch musi być przekierowany na inny dostępny węzeł.

**FE.NFun.116.** Poszczególne komponenty systemu muszą być przynajmniej zdublowane w celu zapewnienia ciągłości działania.

**FE.NFun.117.** Musi być zapewniona wysoka dostępność systemu, w tym zdublowanie komponentów systemu oraz infrastruktury techniczno-systemowej (redundantne elementy wyposażenia sprzętu i zasilania, praca urządzeń w klastrze)

**FE.NFun.118.** Musi być zapewnione monitorowanie i raportowanie zasobów infrastruktury techniczno-systemowej oraz komponentów i realizowanych procesów biznesowych.

**FE.NFun.119.** System musi być wykonany w architekturze wielowarstwowej oddzielającej dane, logikę biznesową i interfejs użytkownika oraz zapewniając odpowiednie role i uprawnienia dla użytkowników.

**FE.NFun.120.** Przechowywanie i obsługa danych kryptograficznych wykonywana jest przy wykorzystaniu urządzeń HSM.

**FE.NFun.121.** Kontroli poprawności wprowadzanych danych jest realizowana przy pomocy formularzy elektronicznych.

**FE.NFun.122.** Weryfikacja poprawności wymienianych dokumentów elektronicznych odbywa się na podstawie schematów XSD i reguł schematronowych oraz weryfikacja zgodności metadanych XDS z danymi nagłówka CDA.

- FE.NFun.123.** Logowanie wszystkich zdarzeń w systemie, w tym błędów, jest zgodne z profilem IHE ATNA.
- FE.NFun.124.** Korelacja zdarzeń, w tym błędów, jest wykonywana przy wykorzystaniu rozwiązania SIEM.
- FE.NFun.125.** Komunikaty żądania (message request) i komunikaty odpowiedzi (message response) dla transakcji IHE muszą być walidowane przez odbiorcę na zgodność ze specyfikacjami IHE.
- FE.NFun.126.** Komunikaty realizowane w technologii Web Services muszą wykorzystywać SOAP w wersji 1.2.
- FE.NFun.127.** Interfejsy realizowane w technologii Web Services muszą wykorzystywać WS Security na potrzeby przekazywania informacji o uprawnieniach użytkownika zgodnie z profilem IHE XUA.
- FE.NFun.128.** Interfejsy realizowane w technologii Web Services dla transakcji IHE. muszą być zgodne z sekcją ITI TF-2x: Appendix V: Web Services for IHE Transactions
- FE.NFun.129.** System musi umożliwiać separację danych medycznych i dokumentów medycznych od danych niemiedycznych poprzez ich pseudonimizację.

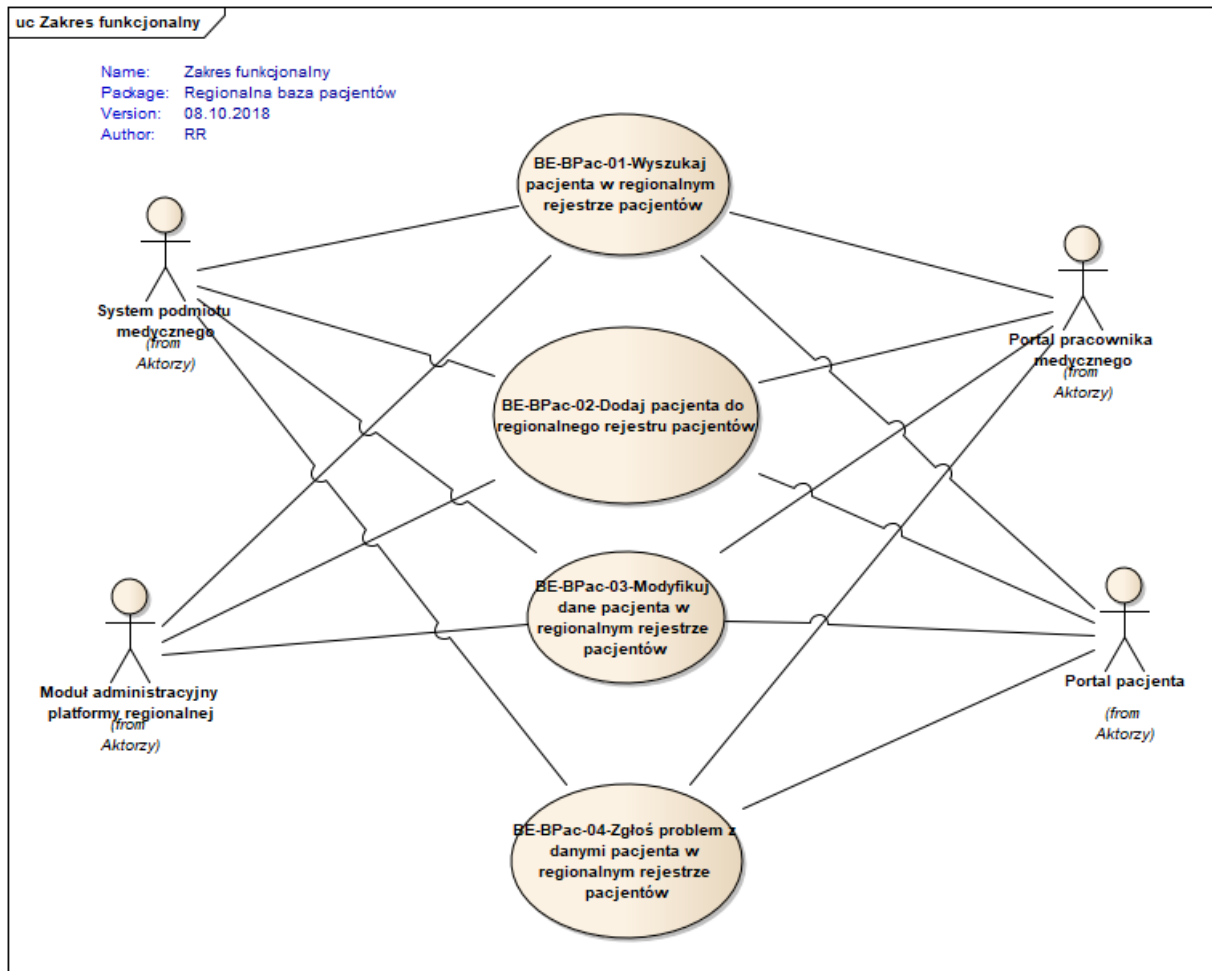
### 3 Komponenty usługowe

#### 3.1 Regionalna baza pacjentów

##### 3.1.1 Wymagania funkcjonalne

- BE.BPac.1.** System umożliwia wyszukanie pacjenta w regionalnym rejestrze pacjentów.
- BE.BPac.2.** System umożliwia dodanie pacjenta do regionalnego rejestru pacjentów.
- BE.BPac.3.** System umożliwia modyfikację danych pacjenta w regionalnym rejestrze pacjentów.
- BE.BPac.4.** System umożliwia zgłoszenie problemu z danymi pacjenta w regionalnym rejestrze pacjentów.
- BE.BPac.5.** System umożliwia zgłoszenie połączenia zdublowanych rekordów pacjenta.

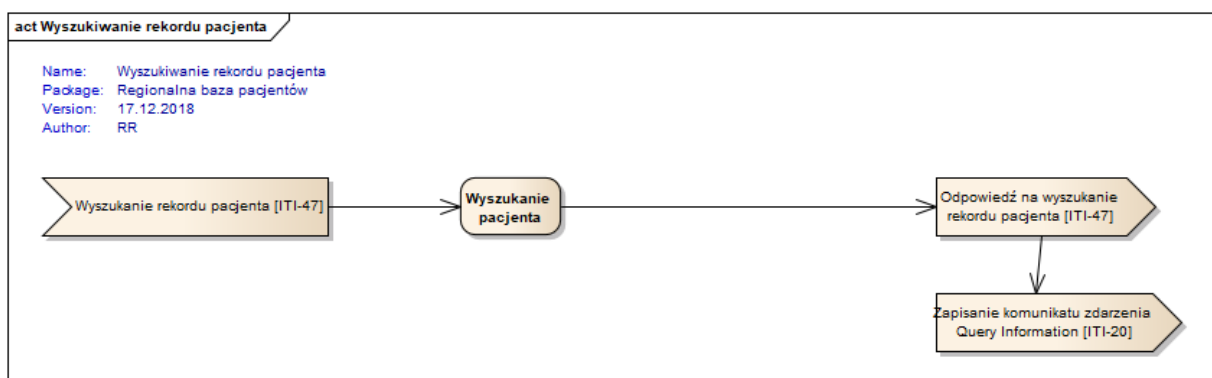
### 3.1.2 Model przypadków użycia



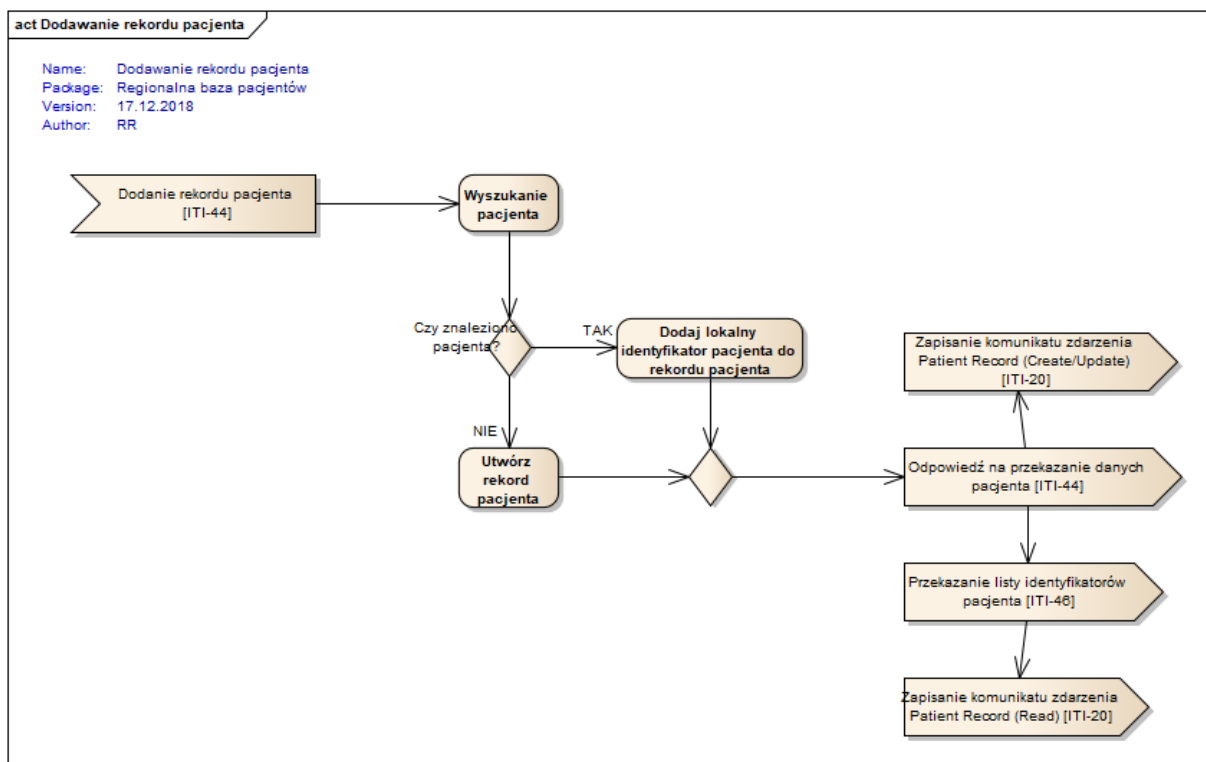
Rysunek nr 3.1 Diagram przypadków użycia obszaru „Regionalna baza pacjentów”

### 3.1.3 Diagram aktywności

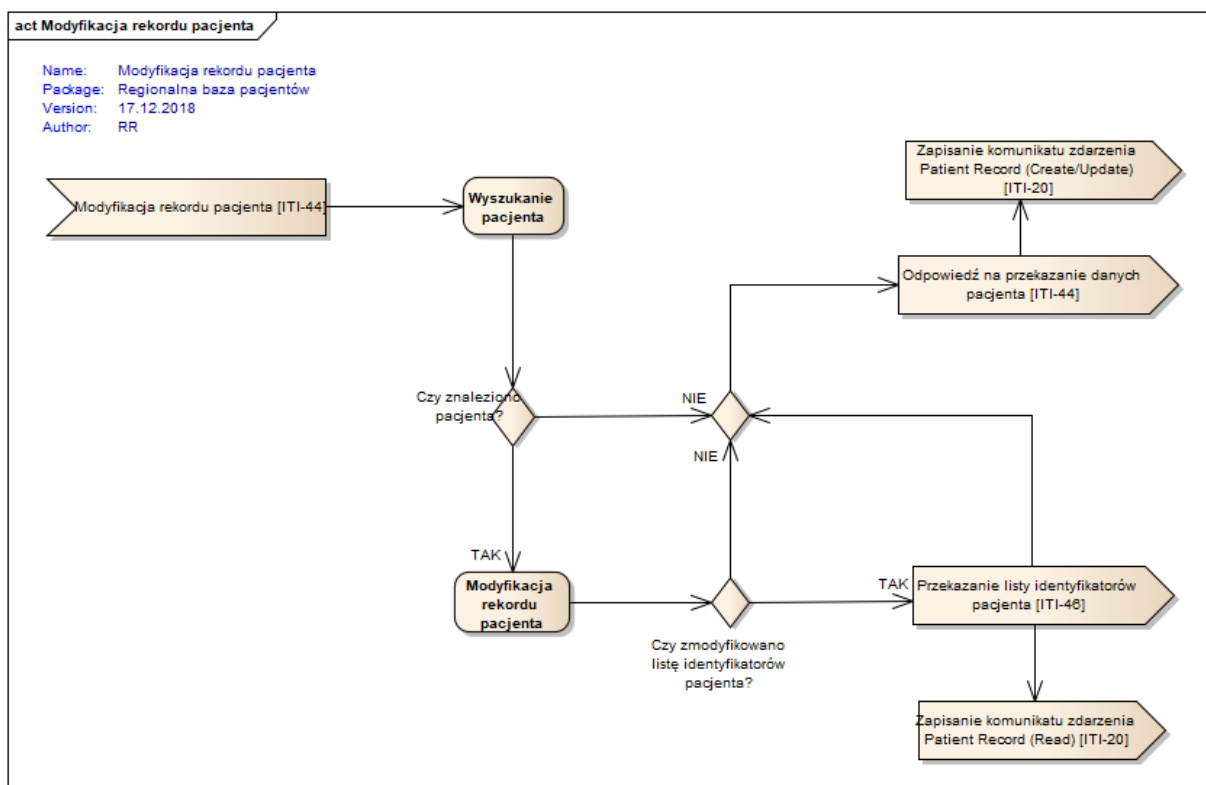
Poniżej przedstawiono diagramy aktywności dla obszaru „Regionalna baza pacjentów”:



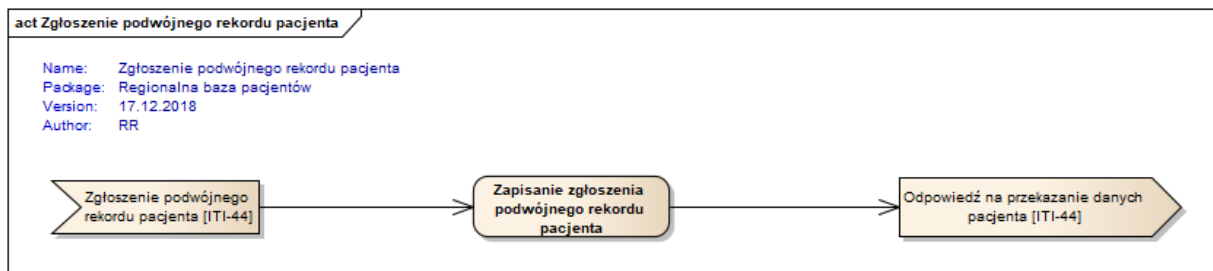
Rysunek nr 3.2 Diagram aktywności obszaru „Wyszukiwanie rekordu pacjenta”



Rysunek nr 3.3 Diagram aktywności obszaru „Dodawanie rekordu pacjenta”

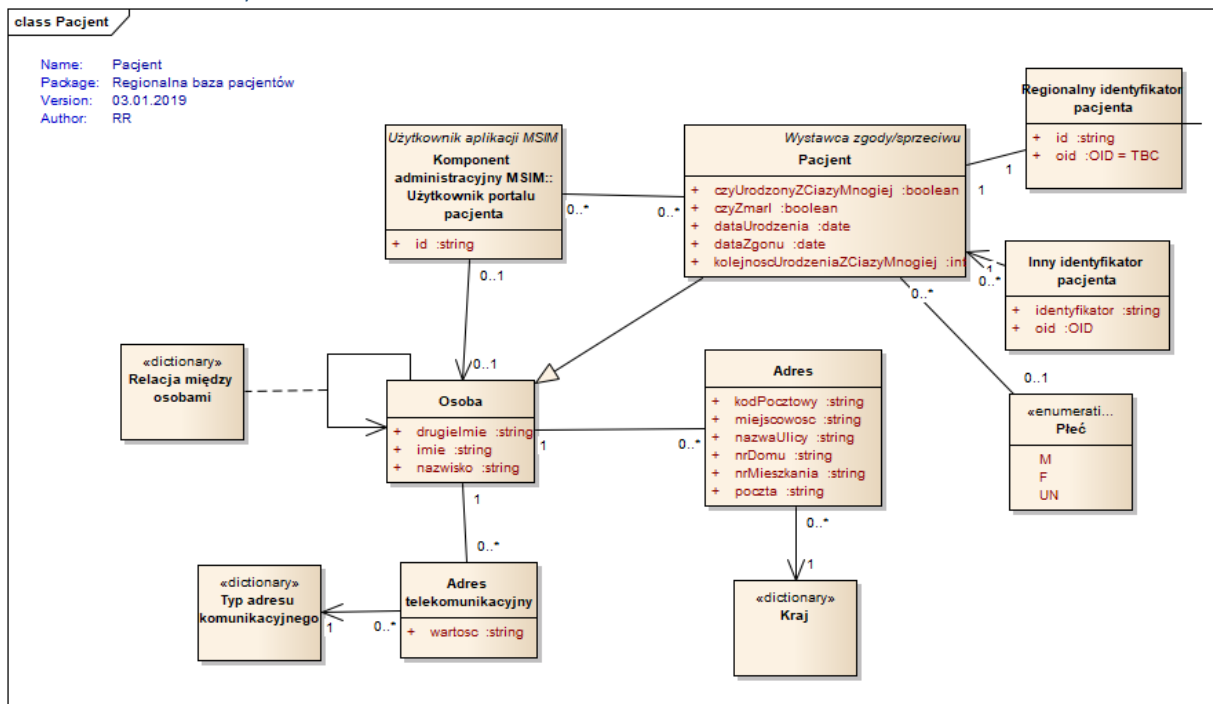


Rysunek nr 3.4 Diagram aktywności obszaru „Modyfikacja rekordu pacjenta”

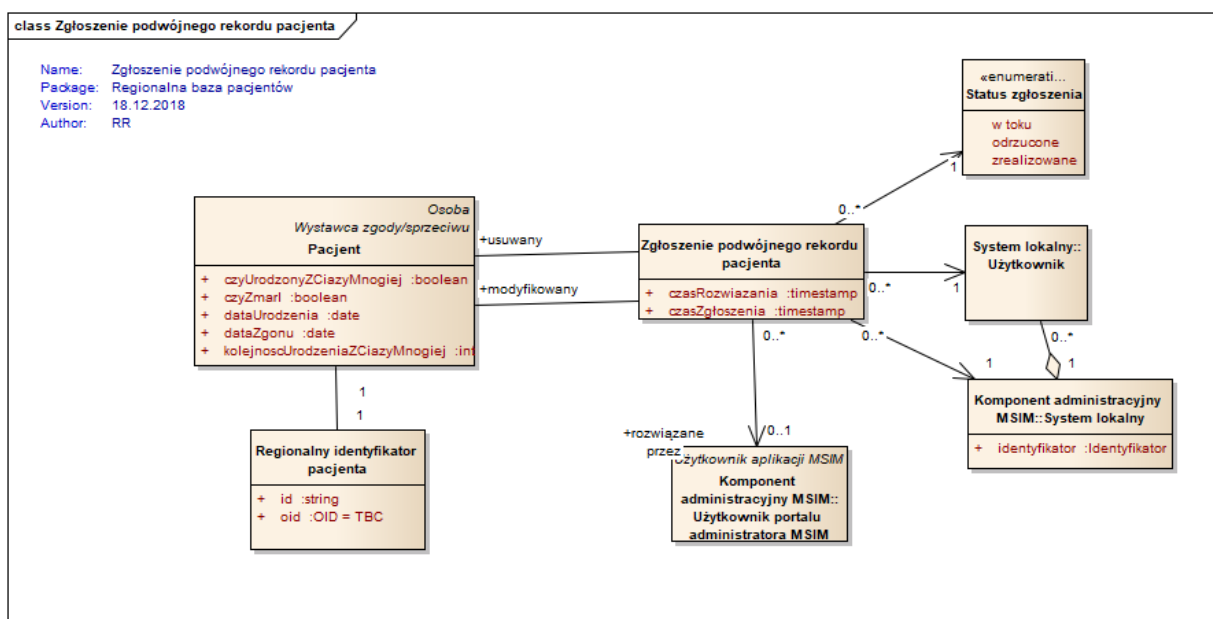


Rysunek nr 3.5 Diagram aktywności obszaru „Zgłoszenie podwójnego rekordu pacjenta”

### 3.1.4 Model danych



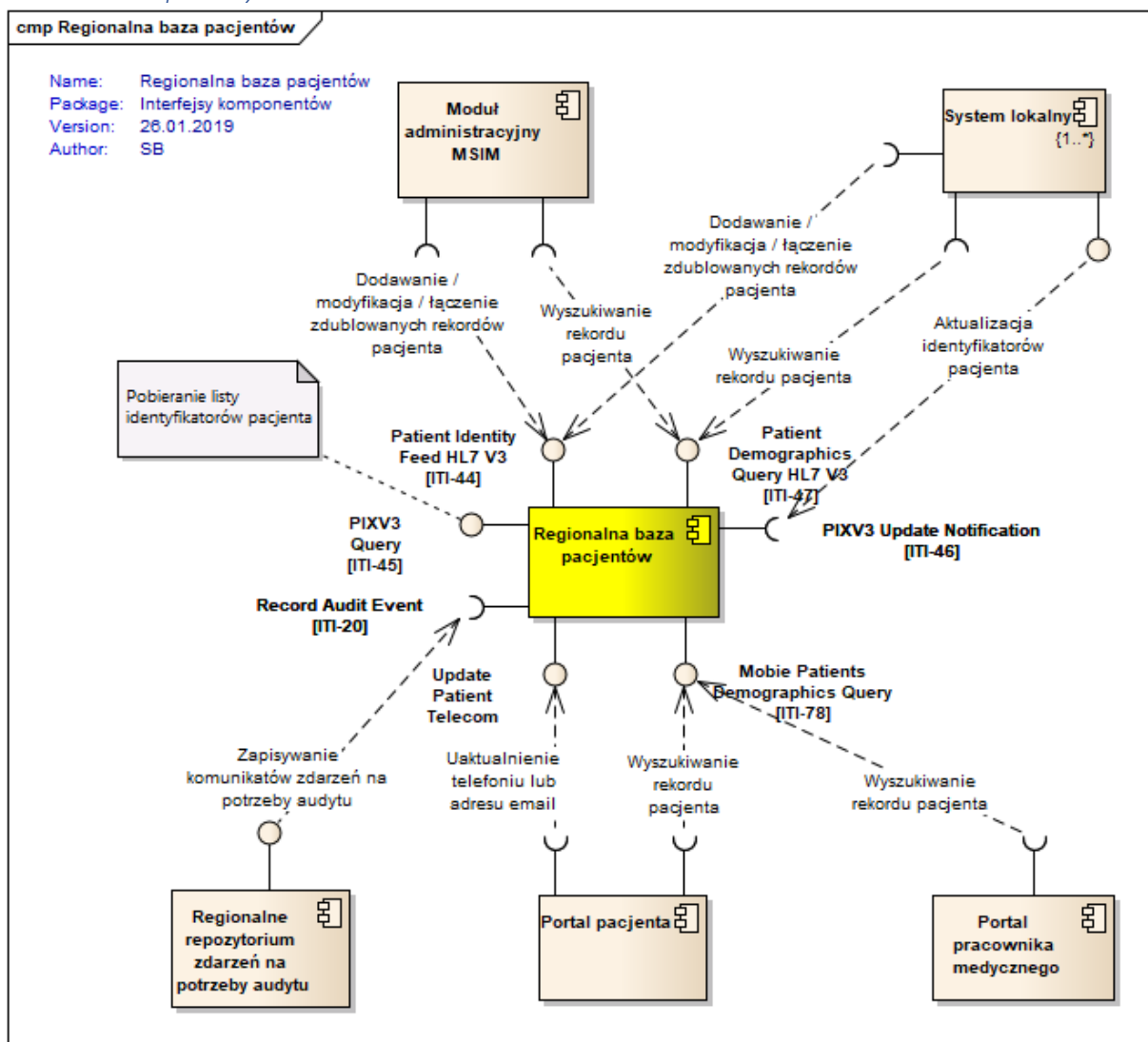
Rysunek nr 3.6 Diagram klas obszaru „Pacjent”



Rysunek nr 3.7 Diagram klas obszaru „Zgłoszenie podwójnego rekordu pacjenta”

### 3.1.5 Komponenty i transakcje

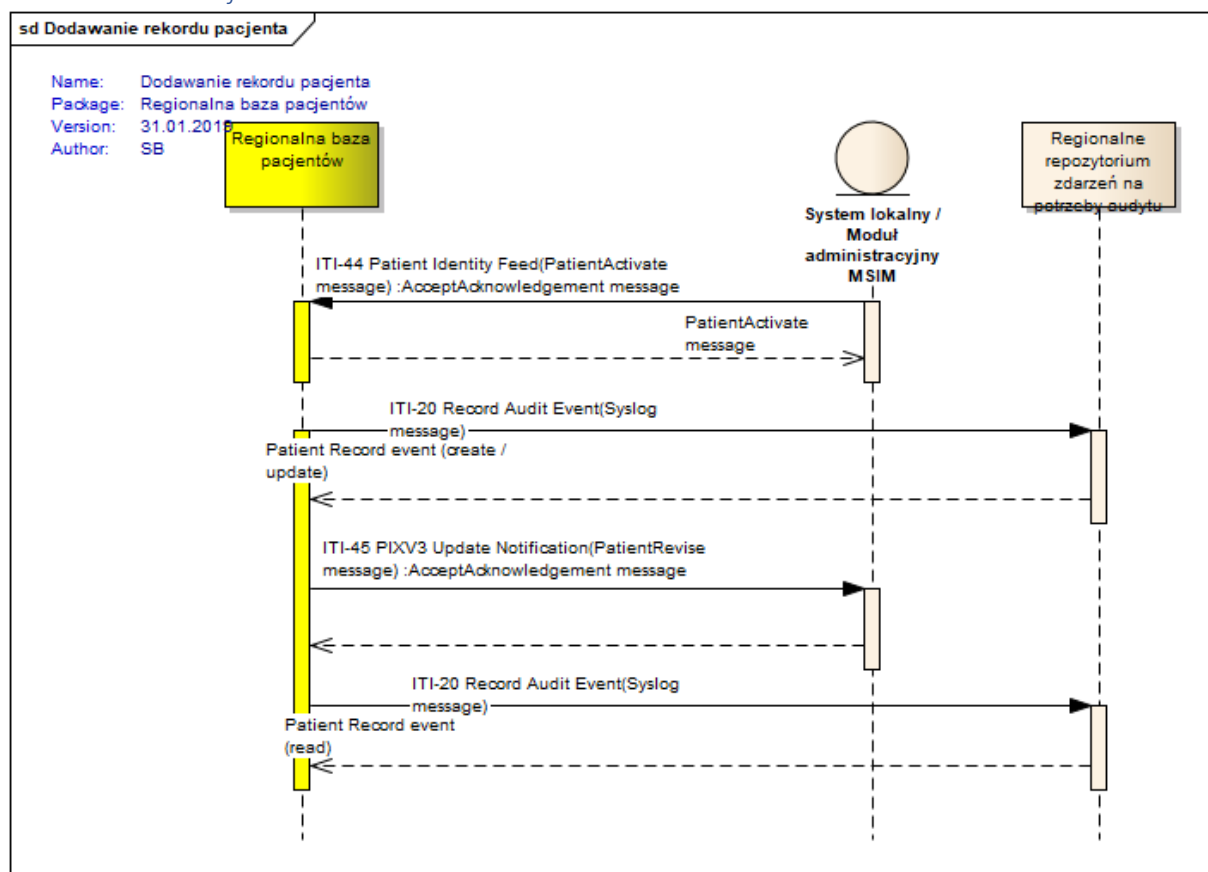
#### 3.1.5.1 Komponenty



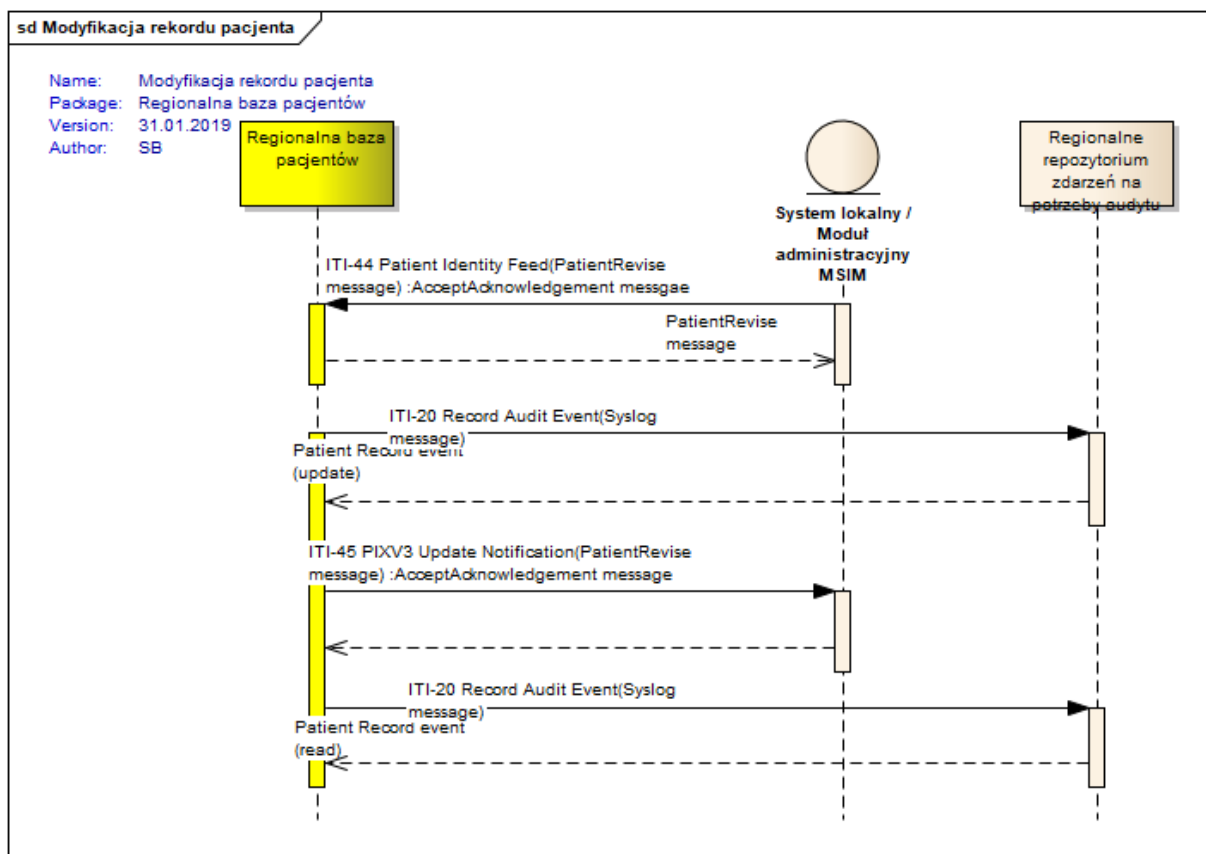
Rysunek nr 3.8 Diagram klas obszaru "Regionalna baza pacjentów"



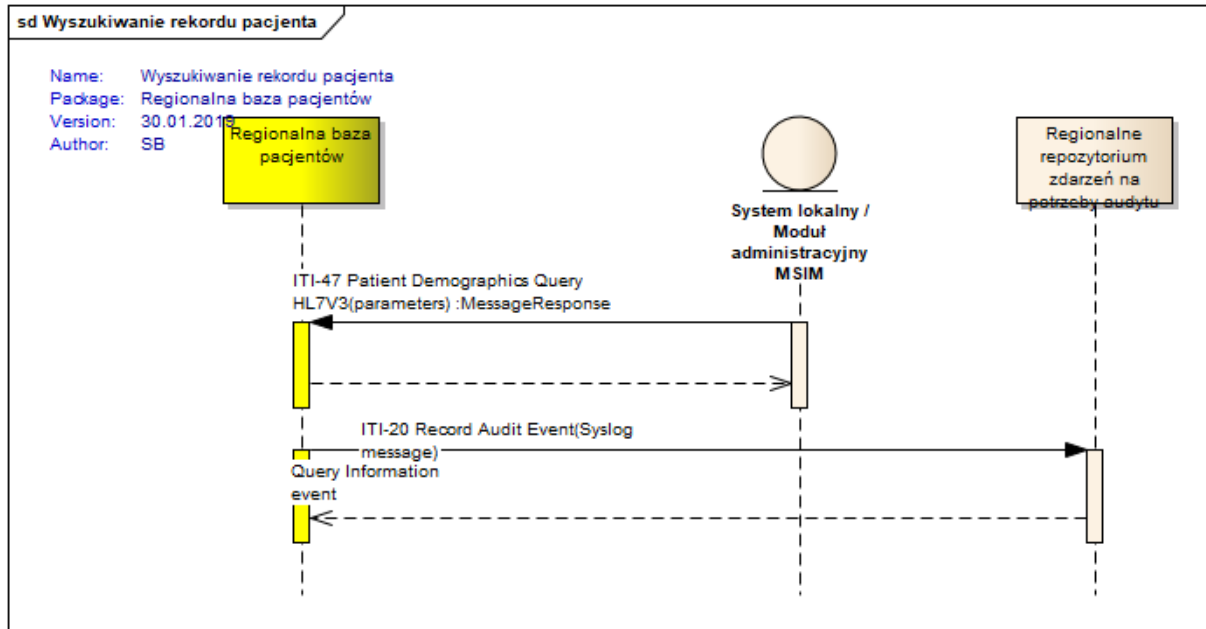
### 3.1.5.2 Transakcje



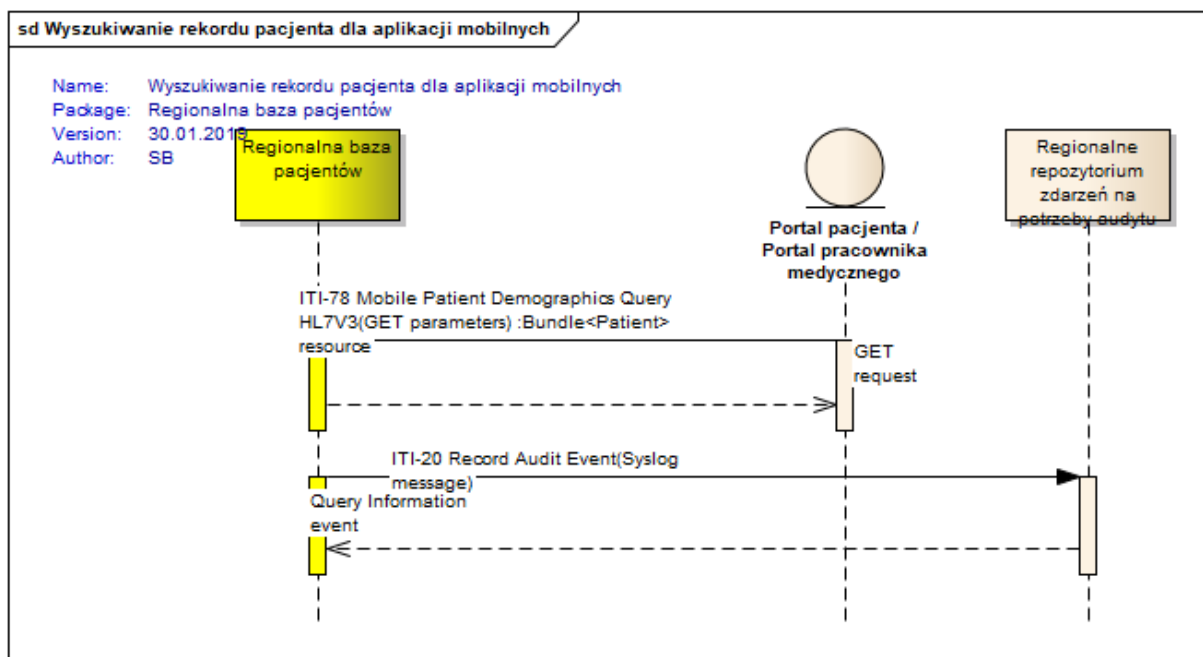
Rysunek nr 3.9 Diagram sekwencji transakcji „Dodawanie rekordu pacjenta”



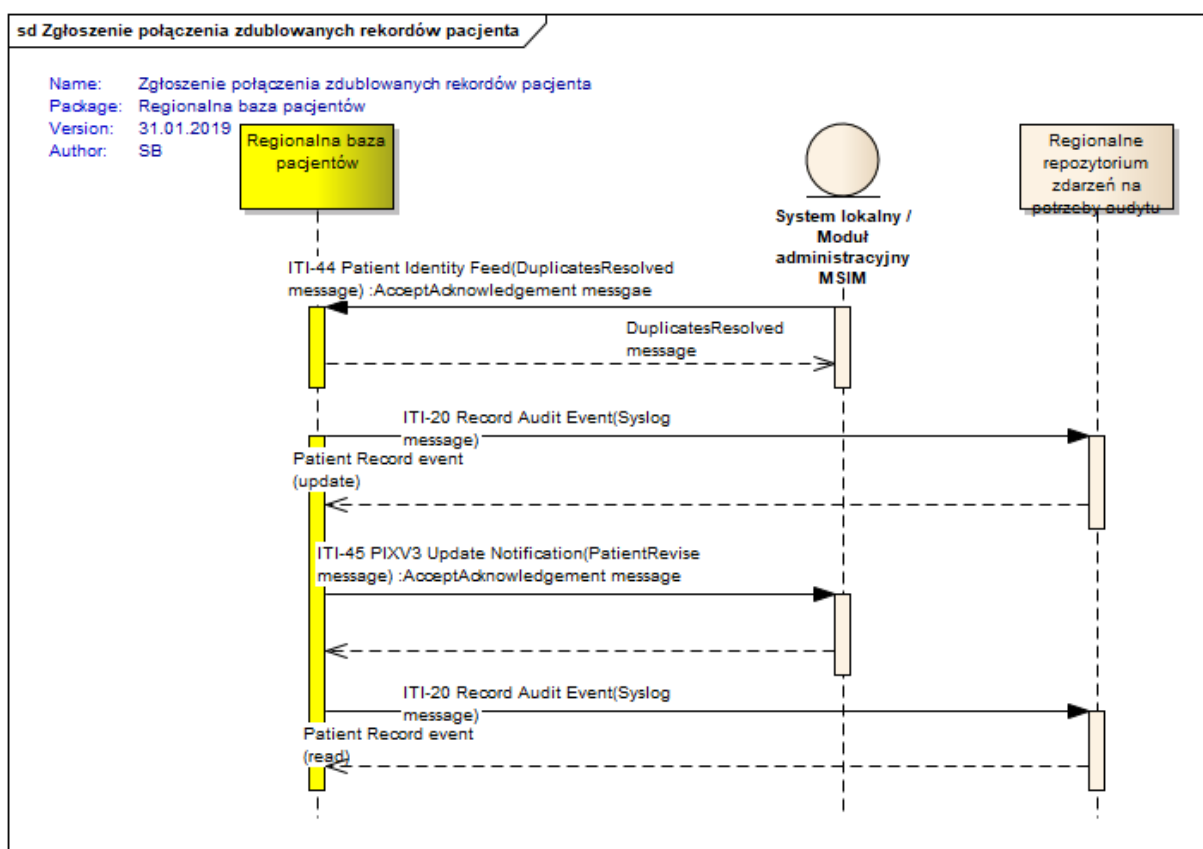
Rysunek nr 3.10 Diagram sekwencji transakcji „Modyfikacja rekordu pacjenta”



Rysunek nr 3.11 Diagram sekwencji transakcji „Wyszukiwanie rekordu pacjenta”



Rysunek nr 3.12 Diagram sekwencji transakcji „Wyszukiwanie rekordu pacjenta dla aplikacji mobilnych”



Rysunek nr 3.13 Diagram sekwencji transakcji „Zgłoszenie połączenia zdublowanych rekordów pacjenta”

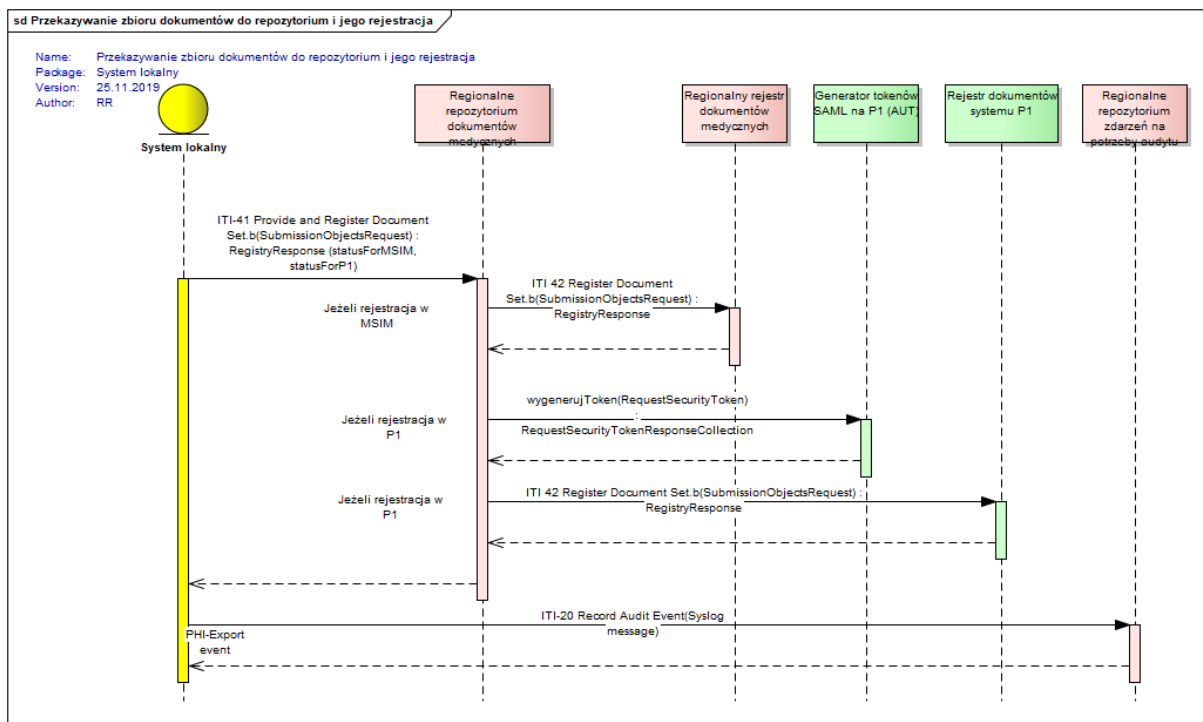
## 3.2 Regionalny rejestr dokumentów

### 3.2.1 Perspektywa systemów lokalnych

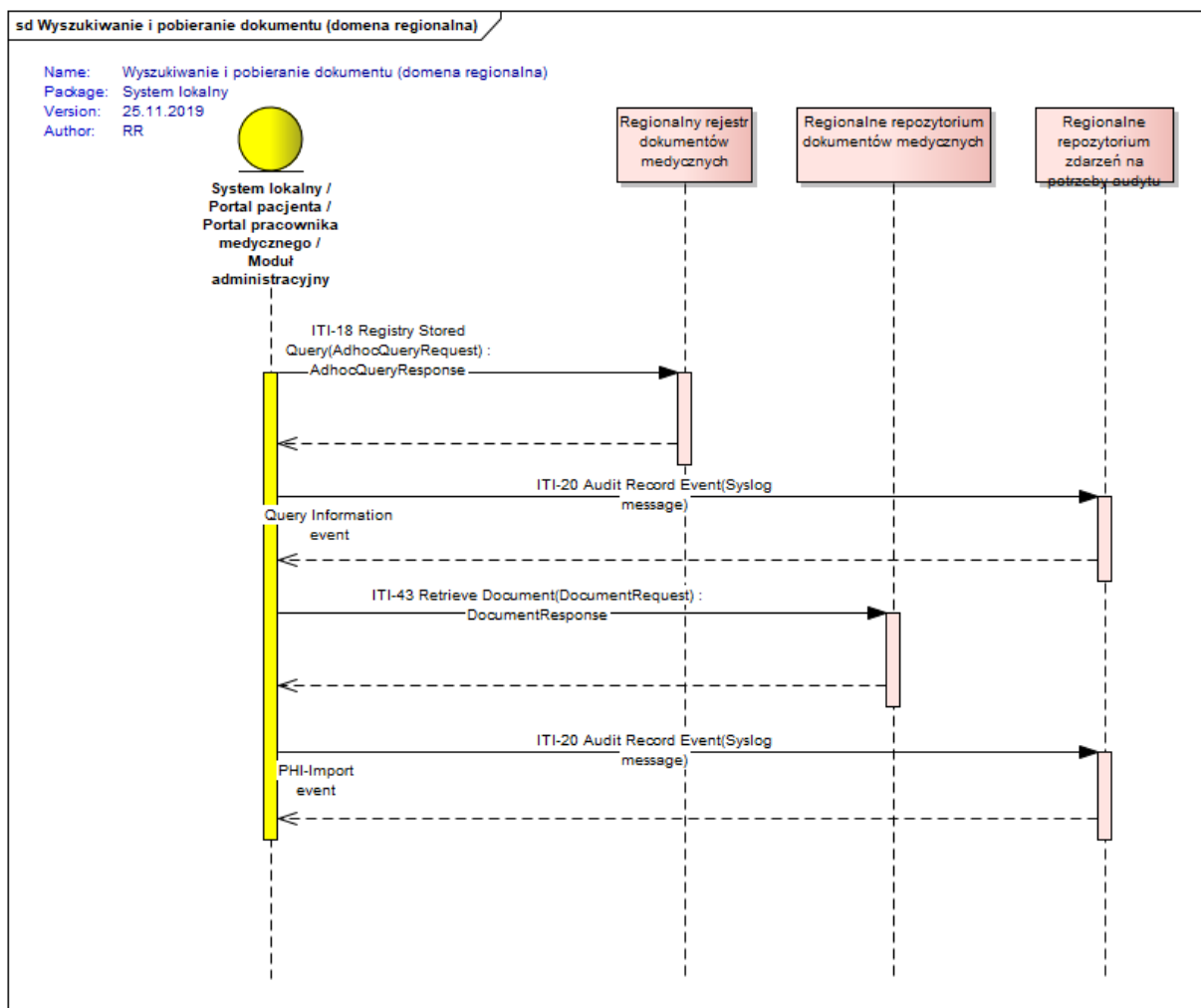
Dla lepszego ukazania działania regionalnego repozytorium dokumentów medycznych oraz regionalnego rejestru dokumentów medycznych w integracji z Platformą P1, poniżej zamieszczono

diagramy przekazywania dokumentów oraz ich wyszukiwania i pobierania, przedstawione z perspektywy systemu lokalnego podmiotu medycznego. Diagramy opisują sekwencje transakcji w zależności od:

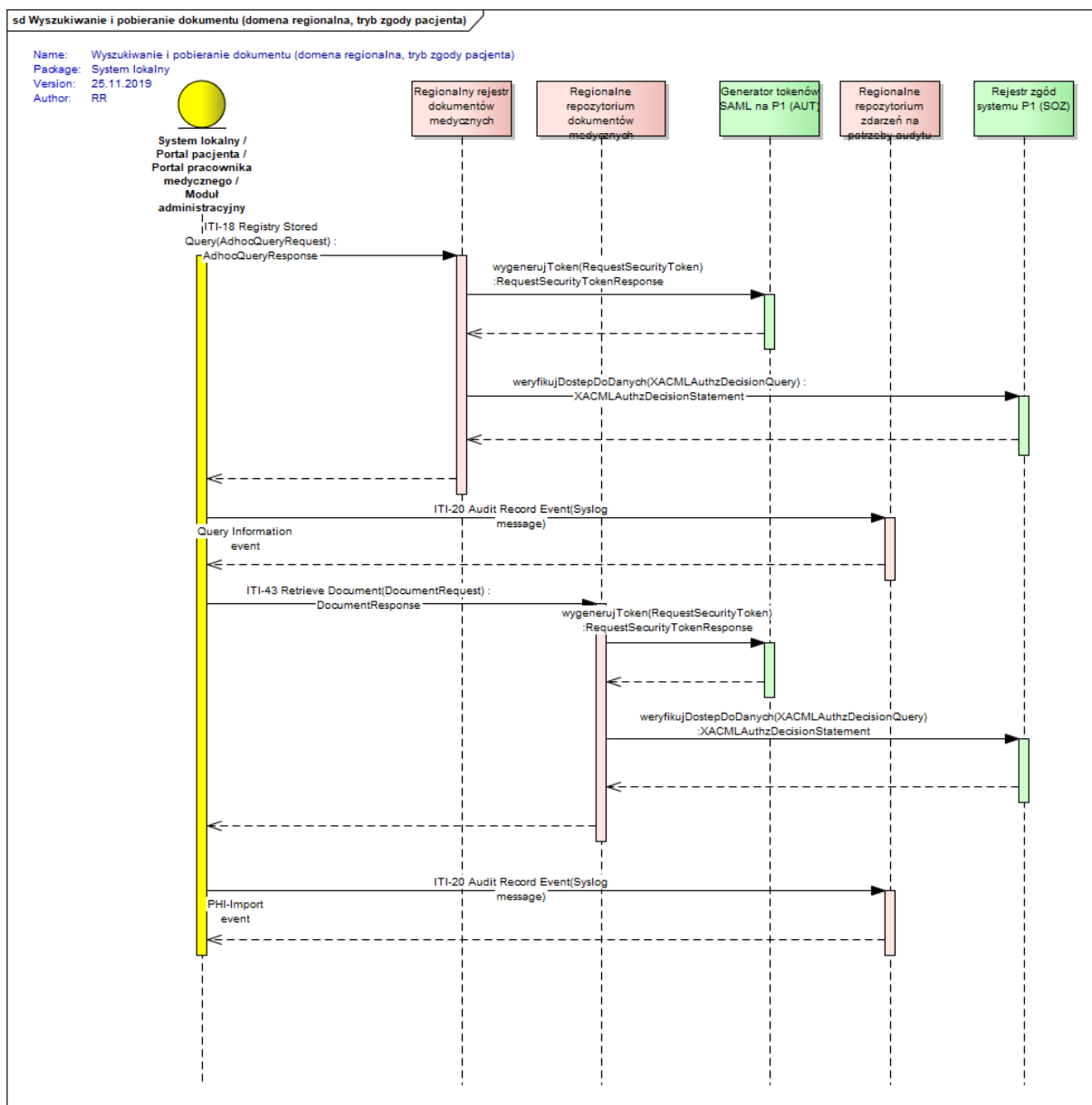
- trybu wymiany dokumentów – za zgodą pacjenta lub inne (dla pacjenta którego dotyczy dokument, dla autora dokumentu, zapewnienia ciągłości leczenia)
- domeny, w której zarejestrowano dokument – domena regionalna lub domena krajowa.



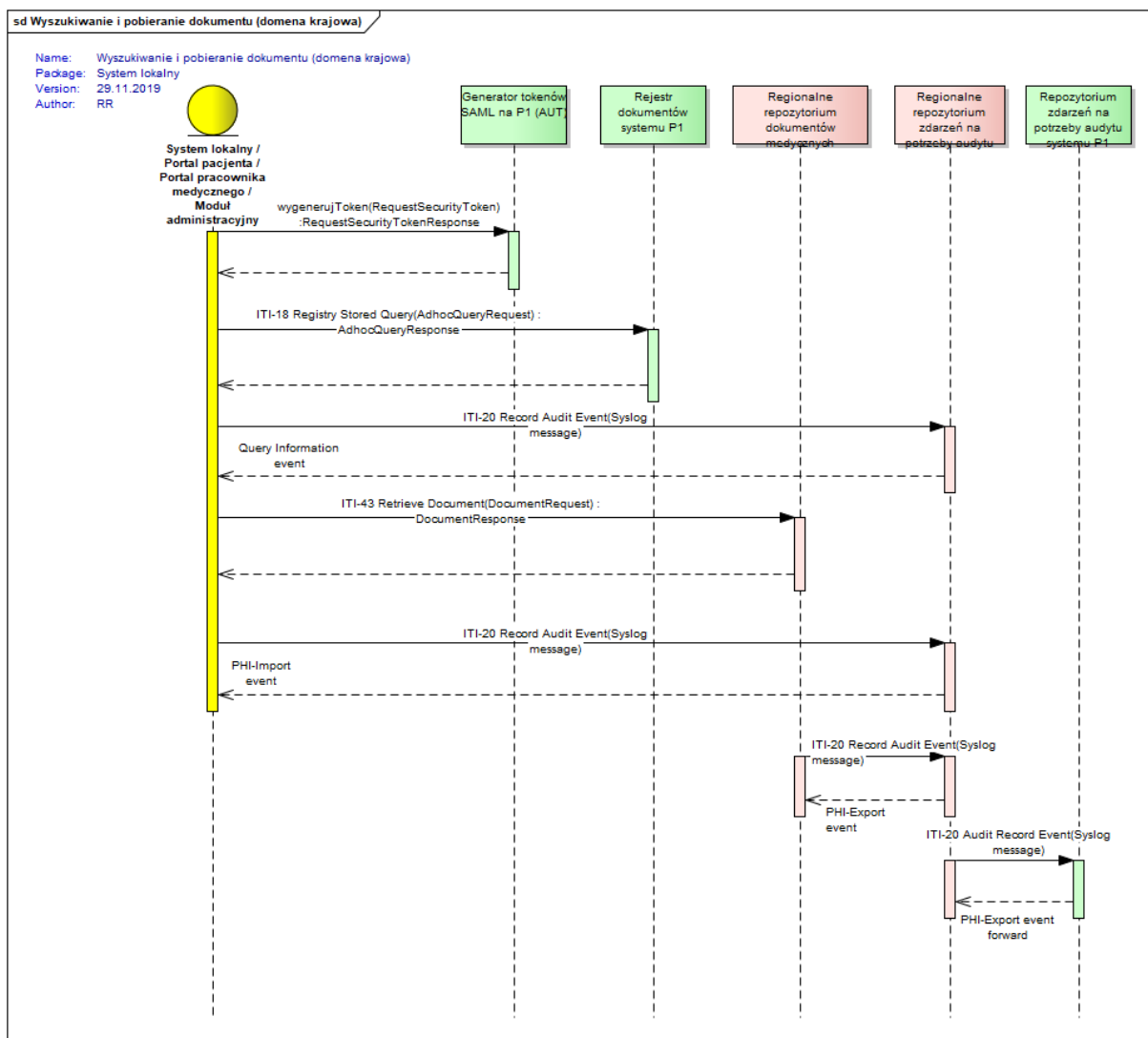
Rysunek nr 3.14 Diagram sekwencji "Przekazywanie zbioru dokumentów do repozytorium i jego rejestracja"



Rysunek nr 3.15 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena regionalna)"



Rysunek nr 3.16 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena regionalna, tryb zgody pacjenta)"



Rysunek nr 3.17 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena krajowa)"

### 3.2.2 Wymagania funkcjonalne

**BE.RejDM.1.** System umożliwia wyszukanie dokumentu medycznego w regionalnym rejestrze.

**BE.RejDM.2.** System umożliwia wyszukanie zgłoszenia dokumentu medycznego w regionalnym rejestrze.

**BE.RejDM.3.** System umożliwia wyszukanie powiązań między dokumentami medycznymi w regionalnym rejestrze.

**BE.RejDM.4.** System umożliwia wyszukanie zgłoszenia dokumentu medycznego i zawartego w tym zgłoszeniu dokumentu w regionalnym rejestrze.

**BE.RejDM.5.** System umożliwia wyszukanie dokumentów powiązanych do dokumentu medycznego w regionalnym rejestrze.

**BE.RejDM.6.** System umożliwia zarejestrowanie dokumentu medycznego w regionalnym rejestrze.

**BE.RejDM.7.** System rozróżnia 5 trybów wymiany dokumentów medycznych:

- a. zapewnienia ciągłości leczenia,

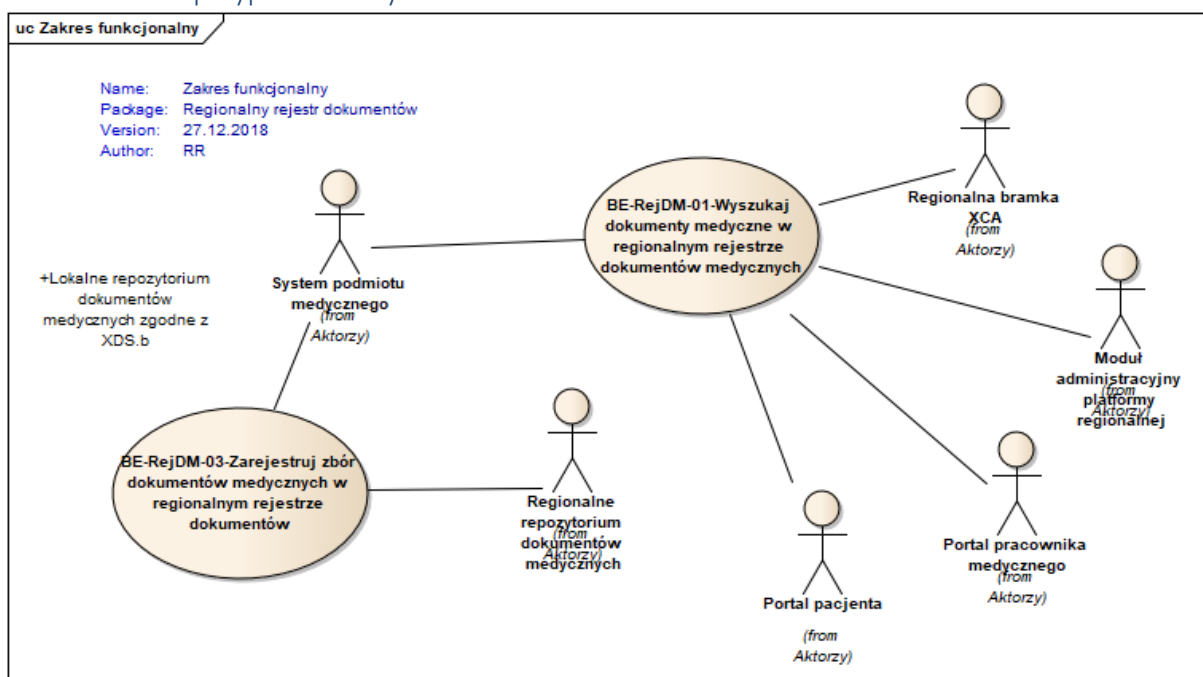
- b. za zgodą pacjenta,
- c. dla pacjenta, którego dotyczy dokument;
- d. dla autora dokumentu,
- e. dostęp ratunkowy.

**BE.RejDM.8.** System weryfikuje uprawnienia użytkownika do dokumentu medycznego na podstawie atrybutów dokumentu i zadeklarowanego trybu wymiany.

**BE.RejDM.9.** System umożliwia weryfikację uprawnień do dokumentu medycznego poprzez weryfikację w rejestrze zgód Platformy P1 zgody pacjenta na dostęp do dokumentu.

**BE.RejDM.10.** Rejestr dokumentów dokonuje w repozytorium dokumentów medycznych aktualizacji metadanych dokumentu, gdy wpis w rejestrze dotyczący tego dokumentu zostanie zmodyfikowany.

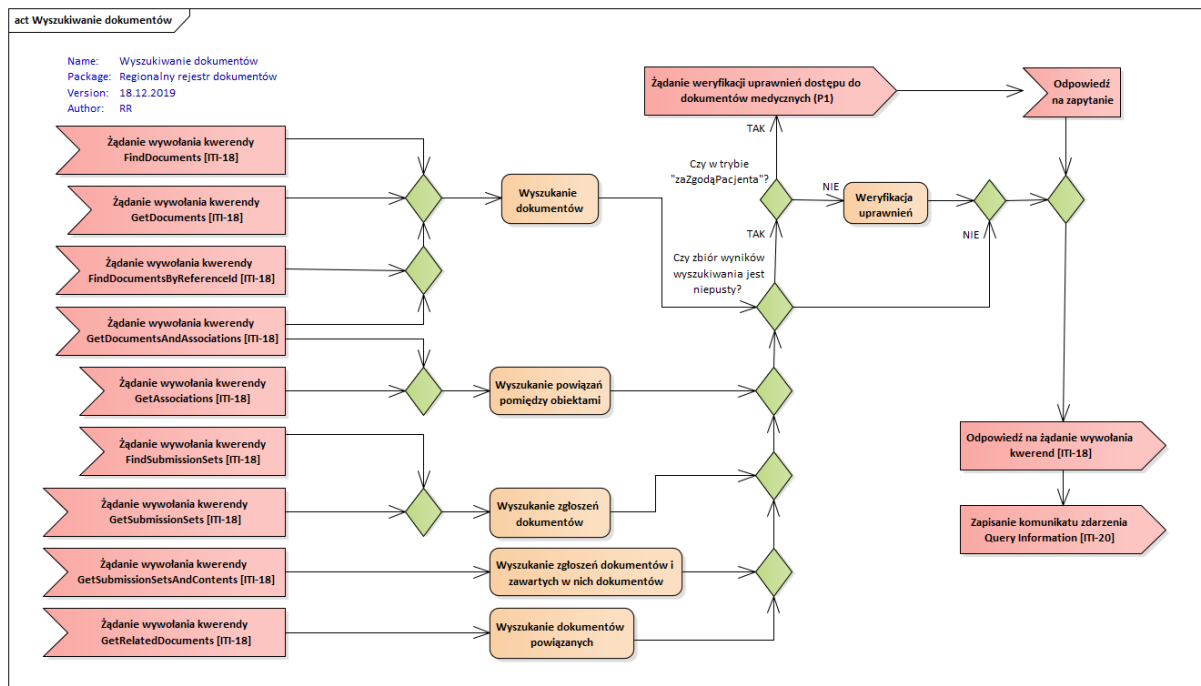
### 3.2.3 Model przypadków użycia



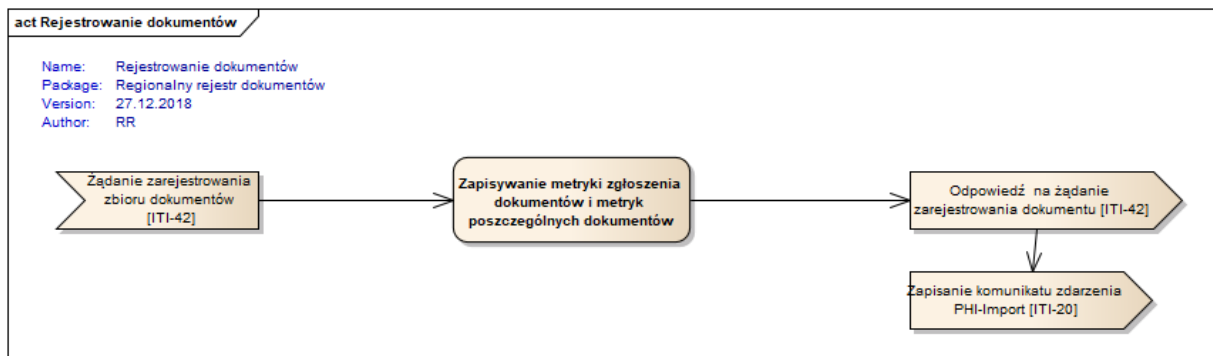
Rysunek nr 3.18 Diagram przypadków użycia komponentu „Regionalny rejestr dokumentów”



### 3.2.4 Diagram aktywności

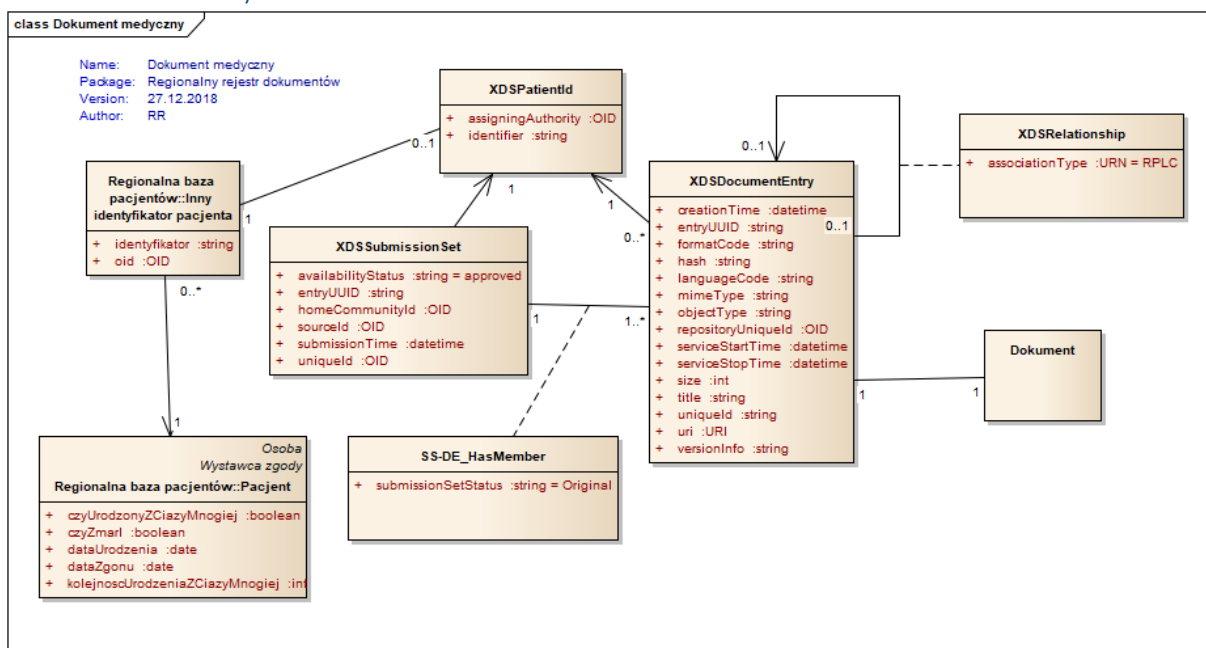


Rysunek nr 3.19 Diagram aktywności obszaru „Wyszukiwanie dokumentów”

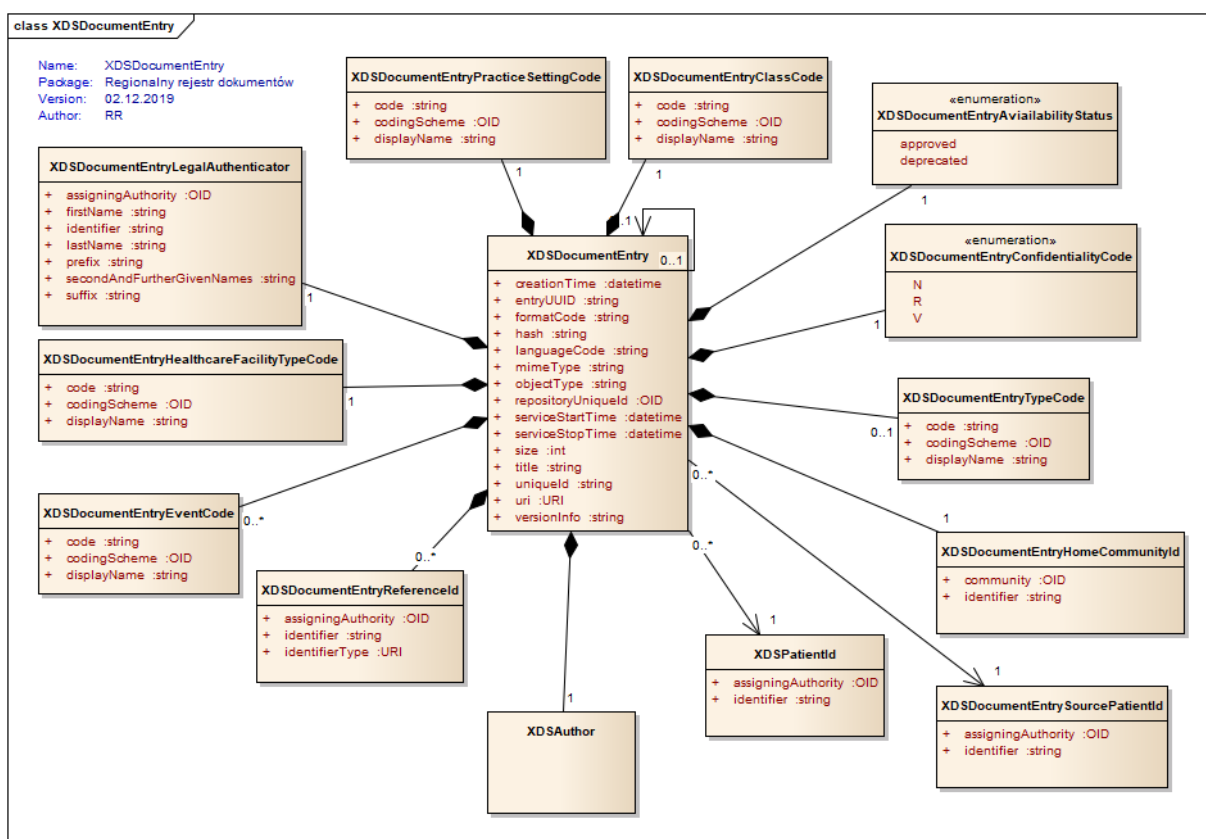


Rysunek nr 3.20 Diagram aktywności obszaru „Rejestrowanie dokumentów”

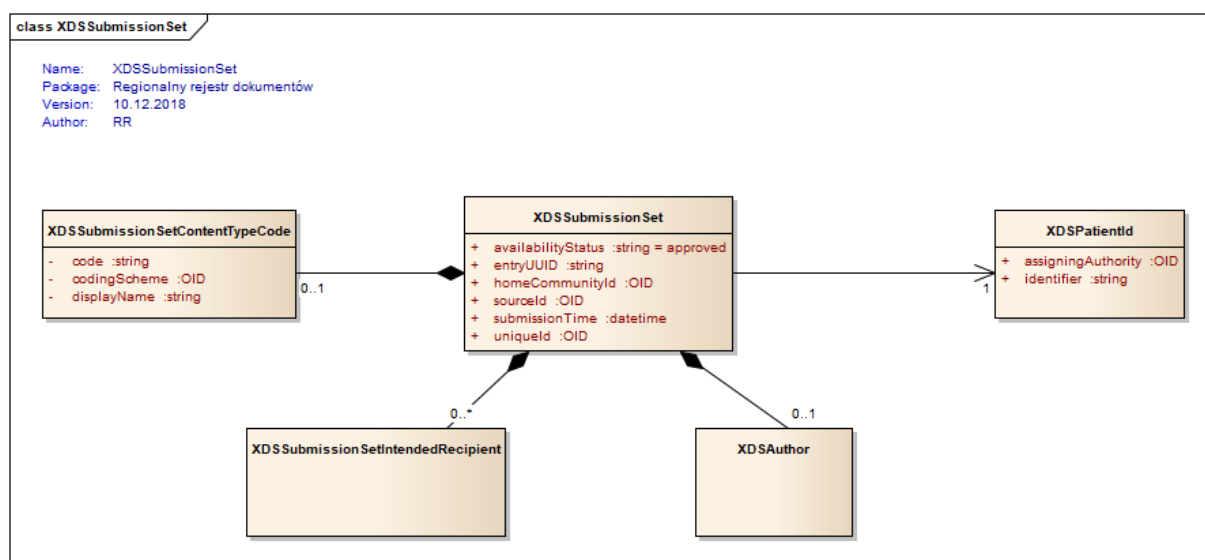
### 3.2.5 Model danych



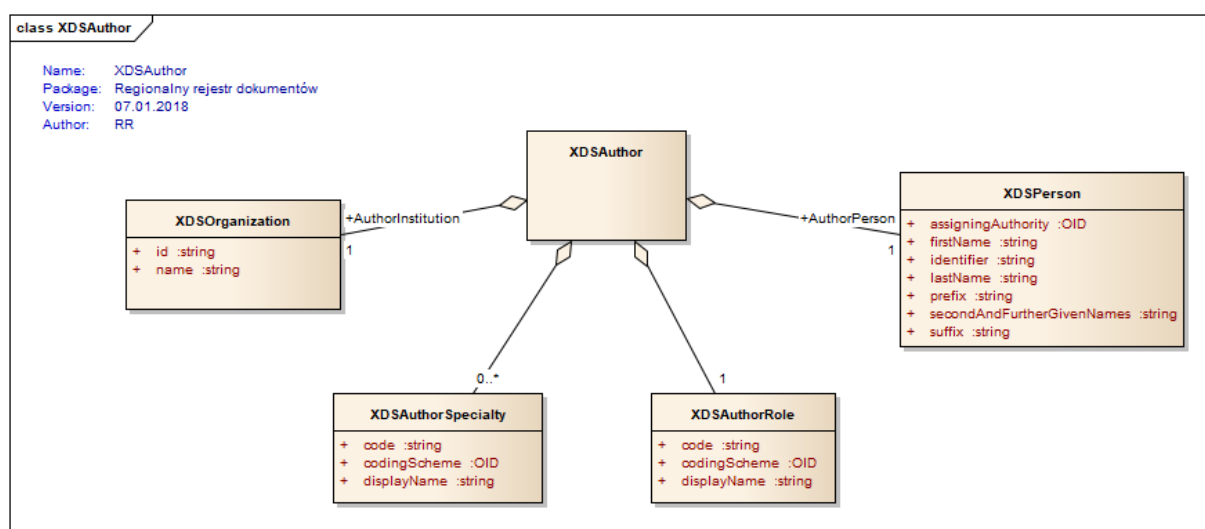
Rysunek nr 3.21 Diagram klas obszaru „Dokument medyczny”



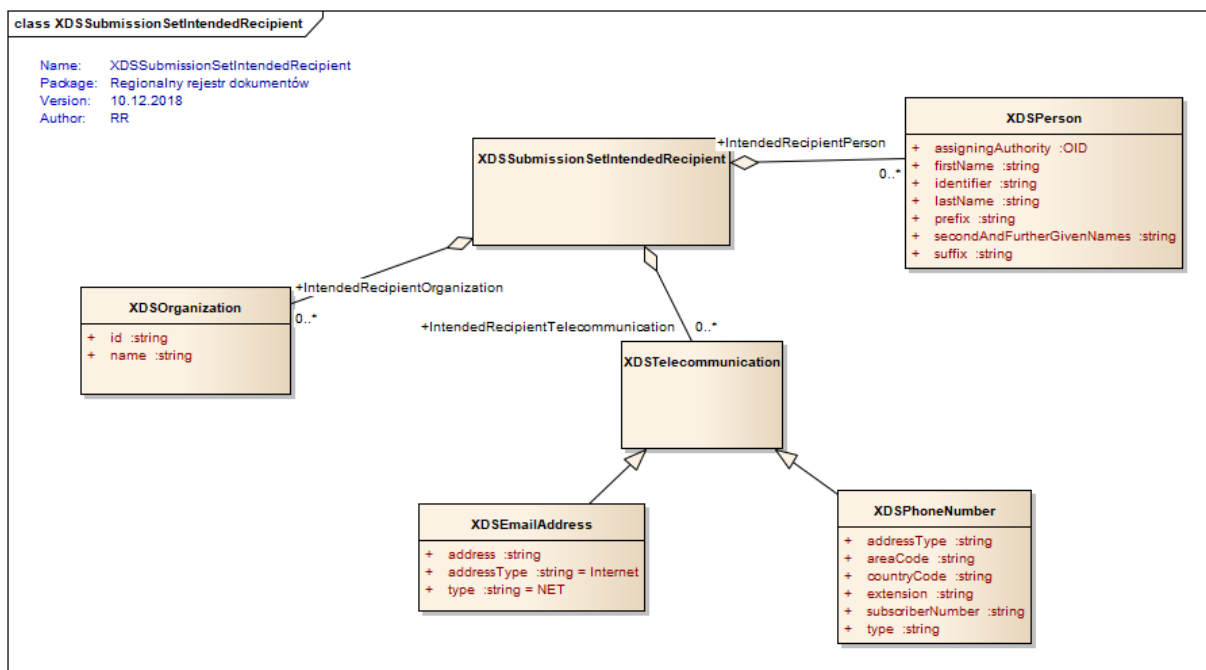
Rysunek nr 3.22 Diagram klas składających się na złożoną klasę XDSDocumentEntry



Rysunek nr 3.23 Diagram klas składających się na złożoną klasę XDSSubmission Set



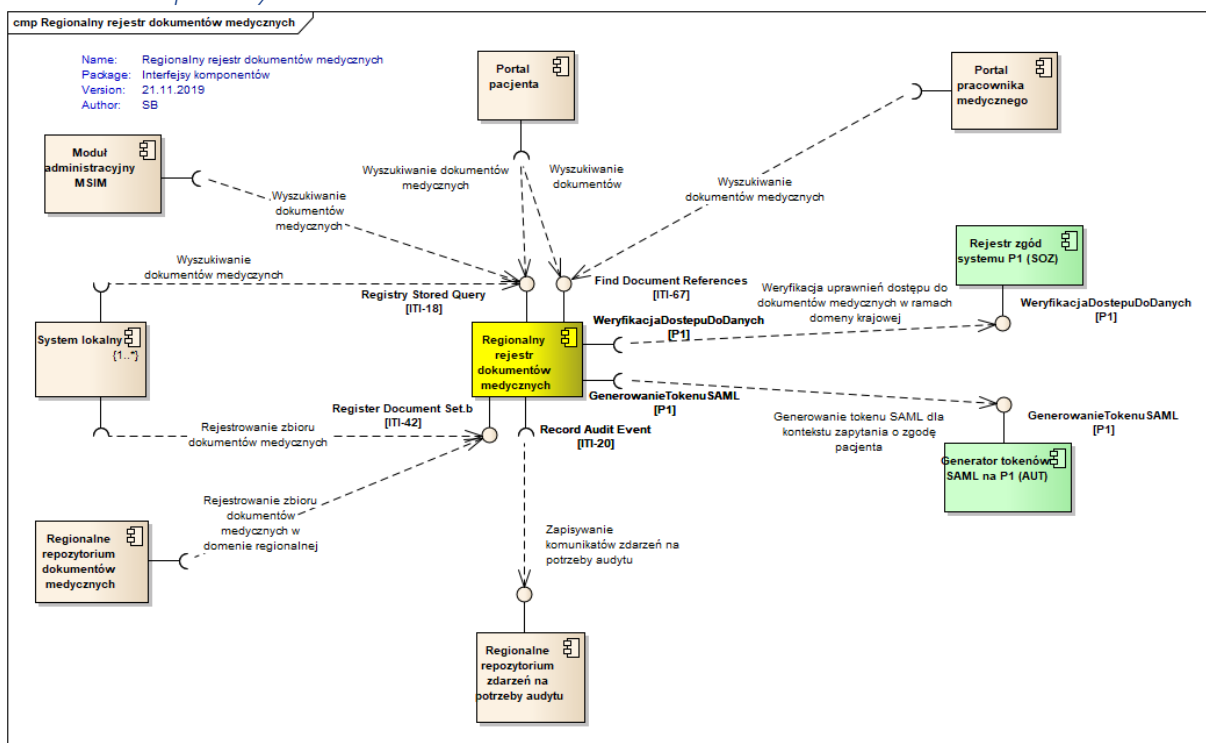
Rysunek nr 3.24 Diagram klas składających się na złożoną klasę XDSAuthor



Rysunek nr 3.25 Diagram klas składających się na złożoną klasę XDSSubmissionSetIntendedRecipient

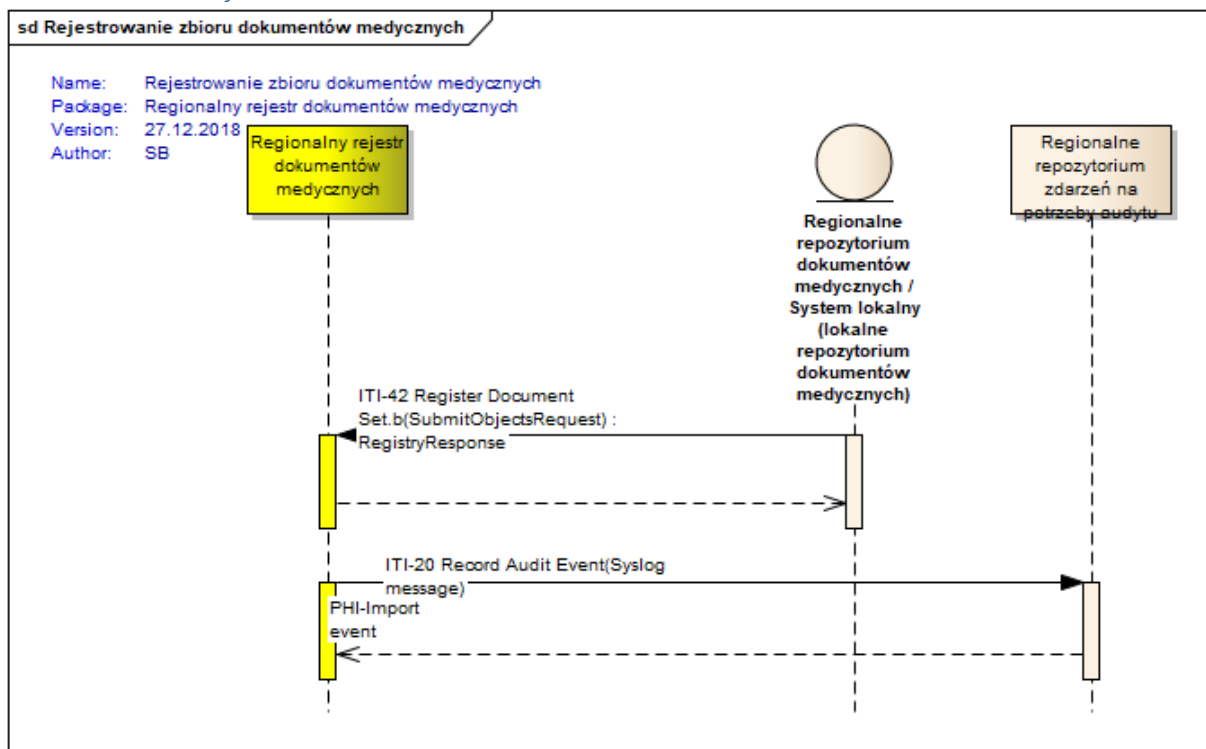
## 3.2.6 Komponenty i transakcje

### 3.2.6.1 Komponenty

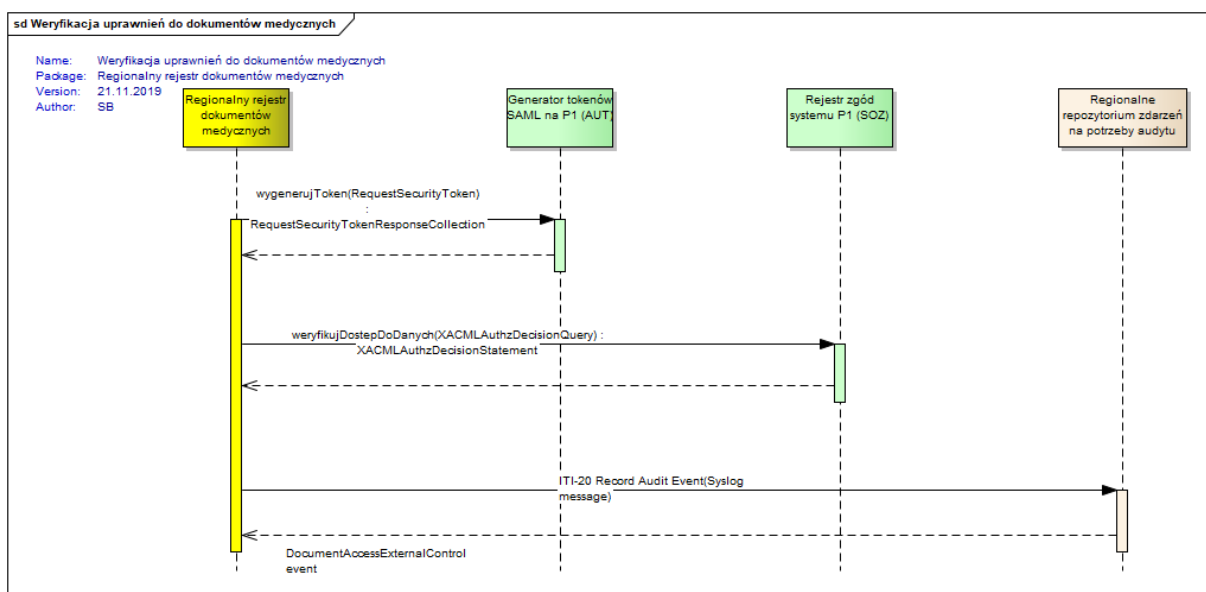


Rysunek nr 3.26 Diagram komponentów obszaru „Regionalny rejestr dokumentów medycznych”

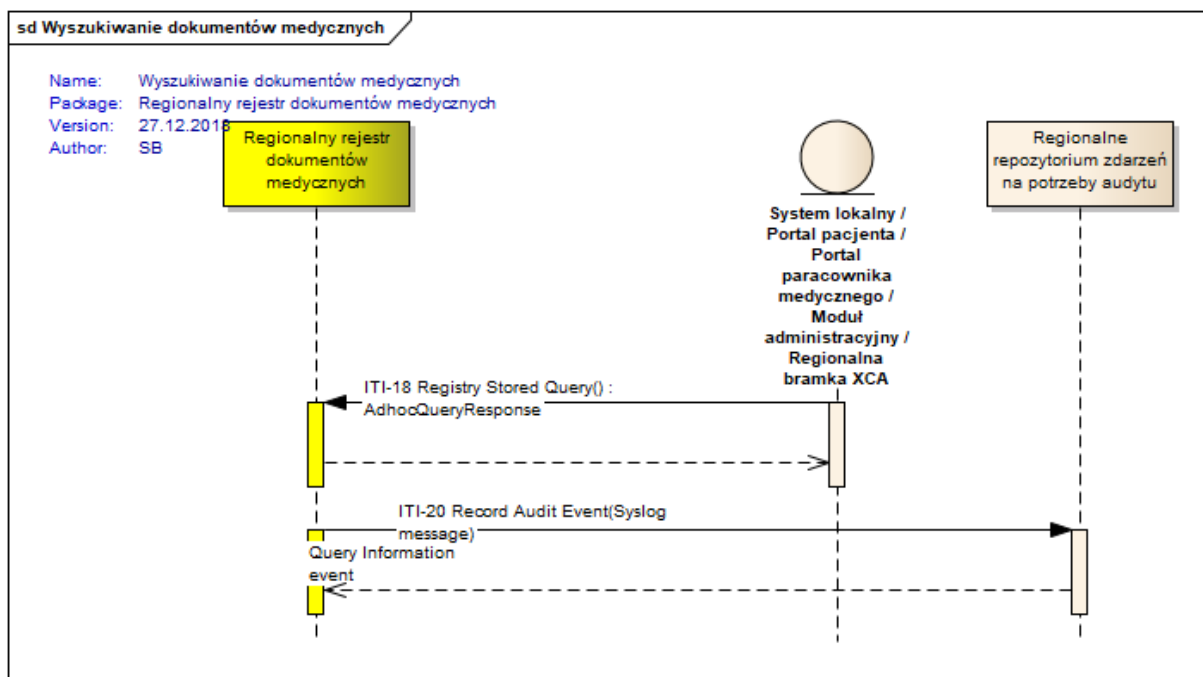
### 3.2.6.2 Transakcje



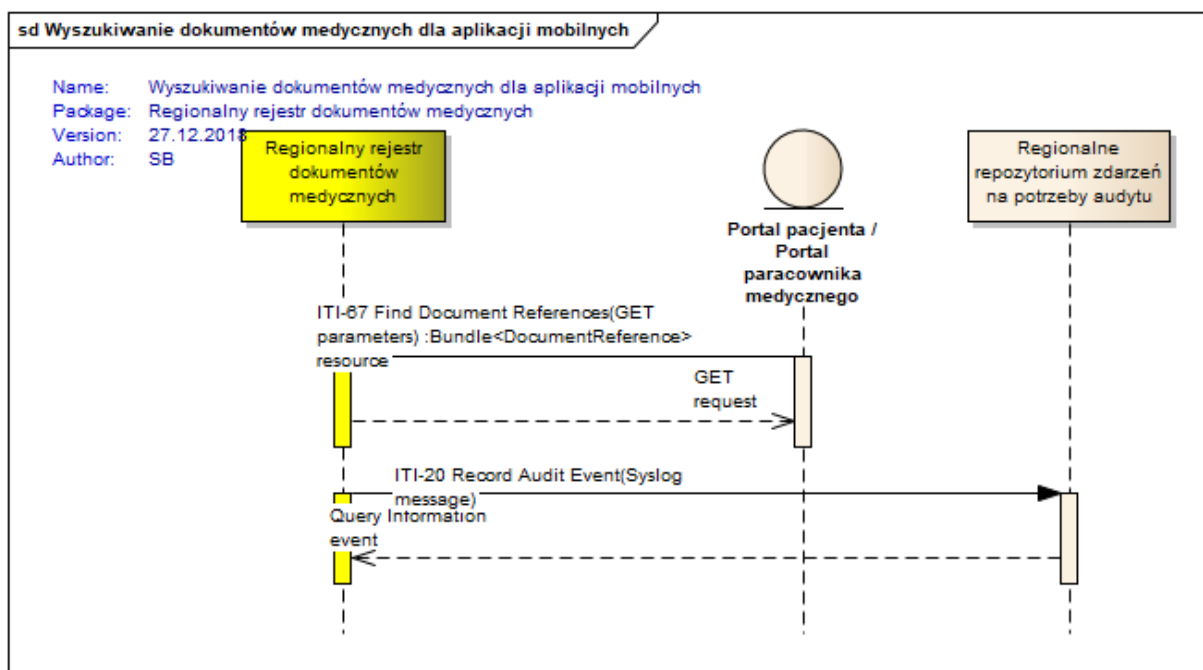
Rysunek nr 3.27 Diagram sekwencji transakcji „Rejestrowanie zbioru dokumentów medycznych”



Rysunek nr 3.28 Diagram sekwencji transakcji „Weryfikacja uprawnień do dokumentów medycznych”



Rysunek nr 3.29 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych”



Rysunek nr 3.30 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych dla aplikacji mobilnych”

### 3.3 Regionalne repozytorium dokumentów medycznych

#### 3.3.1 Wymagania funkcjonalne

**BE.RepoDM.1.** System umożliwia pobieranie dokumentów medycznych przechowywanych w repozytorium.

**BE.RepoDM.2.** System przed pobraniem dokumentu medycznego przez użytkownika weryfikuje jego uprawnienia do tego dokumentu na podstawie atrybutów dokumentu i zadeklarowanego trybu wymiany.

**BE.RepoDM.3.** System rozróżnia 5 trybów wymiany dokumentów medycznych:

- a. zapewnienia ciągłości leczenia,
- b. za zgodą pacjenta,
- c. dla pacjenta, którego dotyczy dokument;
- d. dla autora dokumentu,
- e. dostęp ratunkowy.

**BE.RepoDM.4.** Dla dokumentu medycznego zarejestrowanego w domenie krajowej, system umożliwia sprawdzenie w Platformie P1 uprawnień użytkownika pobierającego dokument.

**BE.RepoDM.5.** Dla dokumentu medycznego zarejestrowanego w domenie regionalnej, w trybie wymiany za zgodą pacjenta, system umożliwia sprawdzenie w Platformie P1 uprawnień użytkownika pobierającego dokument.

**BE.RepoDM.6.** System rejestruje tryb pobrania dokumentu, wyróżniając tryb komercyjny i niekomercyjny w przypadku udostępnienia w ramach domeny regionalnej.

**BE.RepoDM.7.** System umożliwia zapisanie dokumentu medycznego w repozytorium.

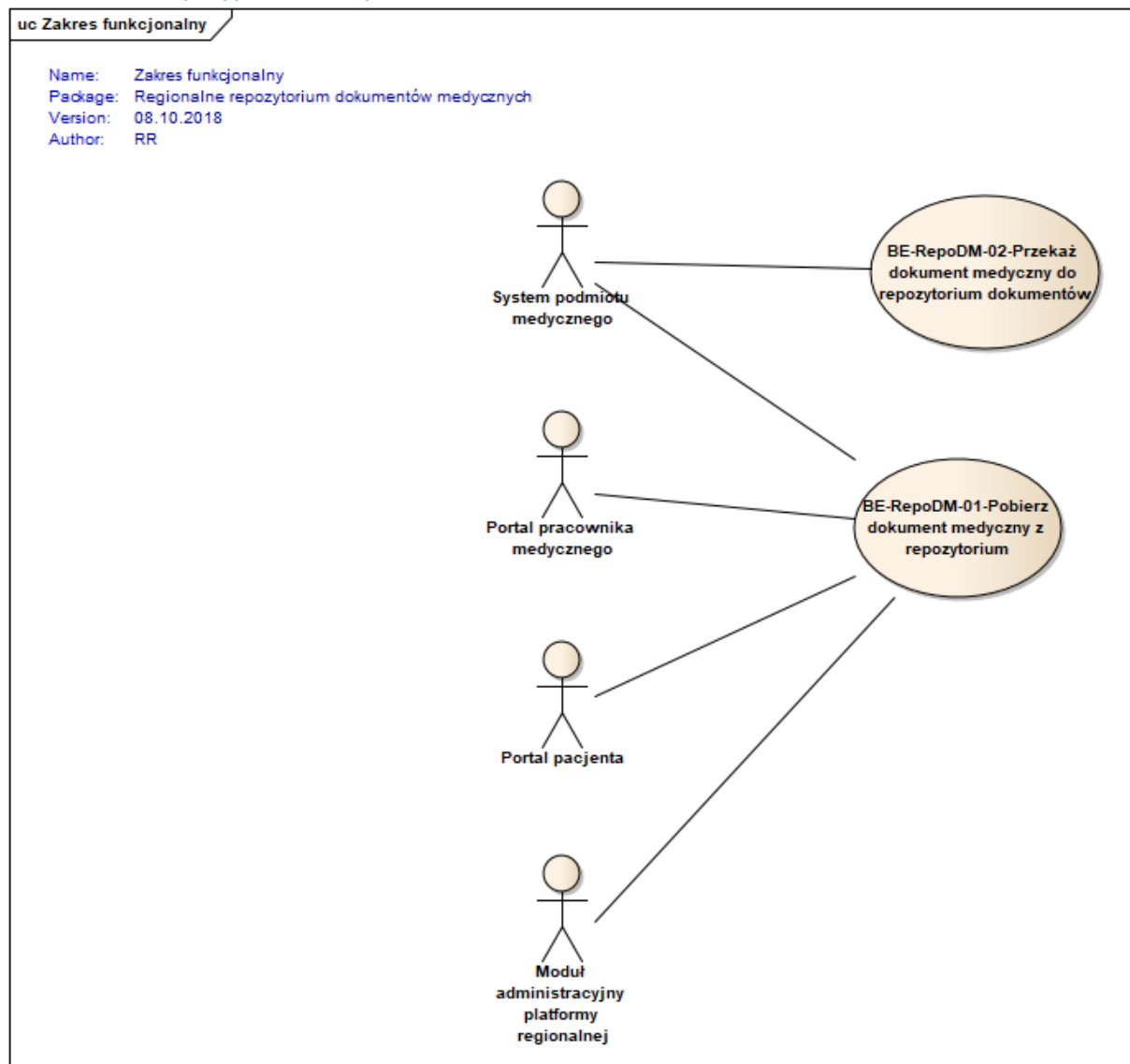
**BE.RepoDM.8.** System przekazuje każdy otrzymany dokument do walidacji przez walidator dokumentów medycznych.

**BE.RepoDM.9.** System rejestruje w rejestrze dokumentów medycznych Platformy MSIM każdy przekazywany do repozytorium dokumentów medycznych dokument, którego dotyczy rejestracja w domenie regionalnej.

**BE.RepoDM.10.** System rejestruje w rejestrze dokumentów medycznych Platformy P1 każdy przekazywany do repozytorium dokumentów medycznych dokument, którego dotyczy rejestracja w domenie krajowej.

**BE.RepoDM.11.** System przekazuje każdy otrzymany dokument do komponentu wtórnego wykorzystania danych w celu pobrania jednostkowych danych medycznych.

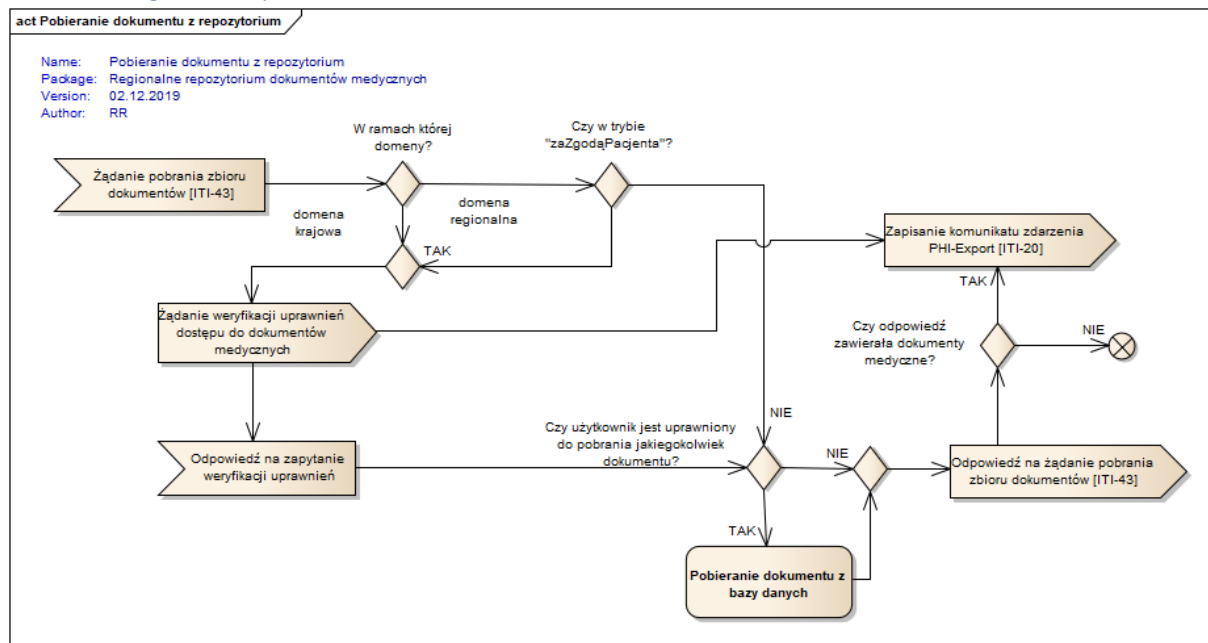
### 3.3.2 Model przypadków użycia



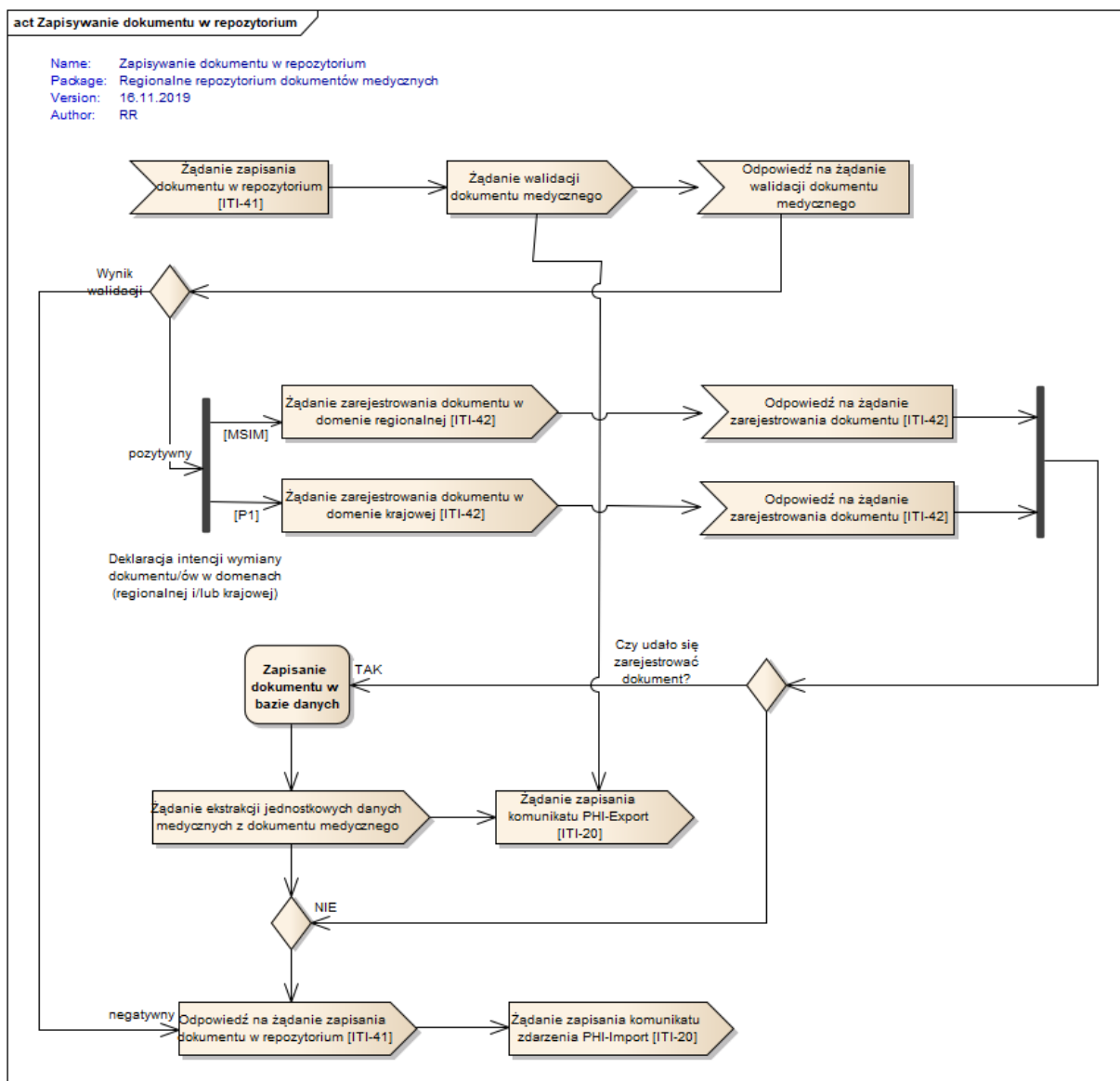
Rysunek nr 3.31 Diagram przypadków użycia obszaru „Regionalne repozytorium dokumentów medycznych”



### 3.3.3 Diagram aktywności

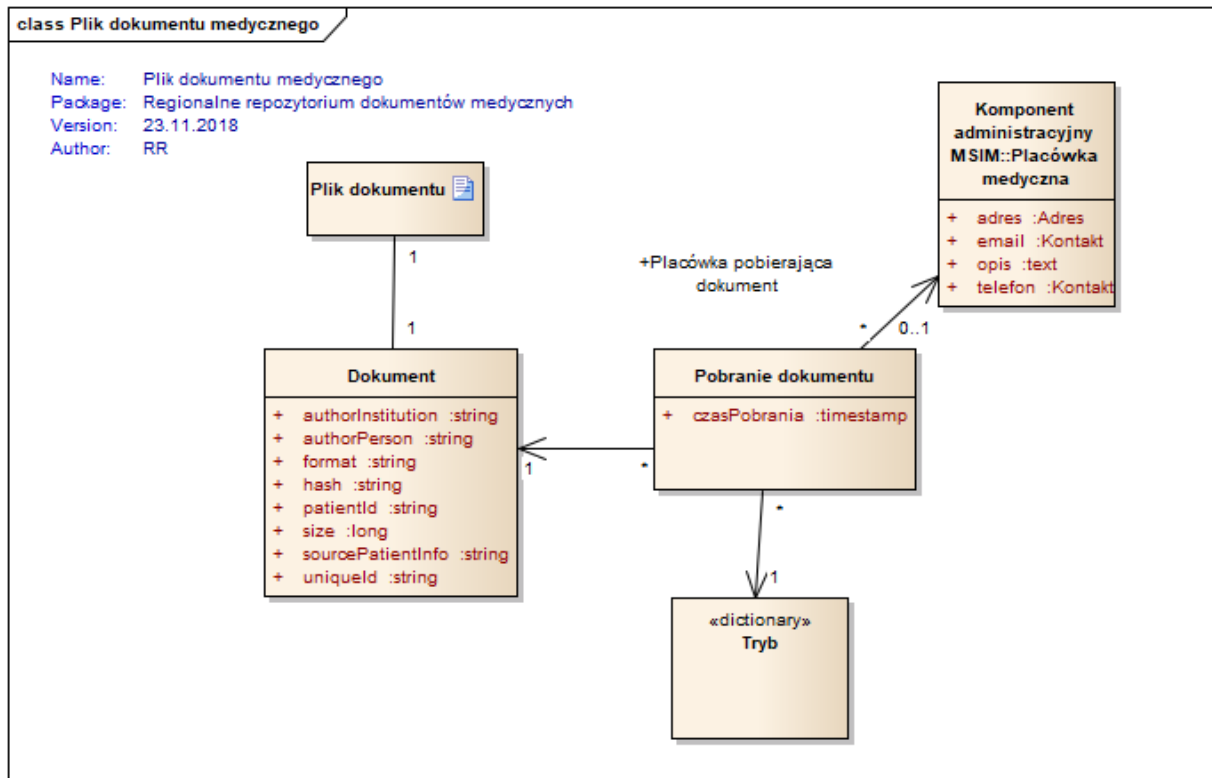


Rysunek nr 3.32 Diagram aktywności obszaru „Pobieranie dokumentu z repozytorium”

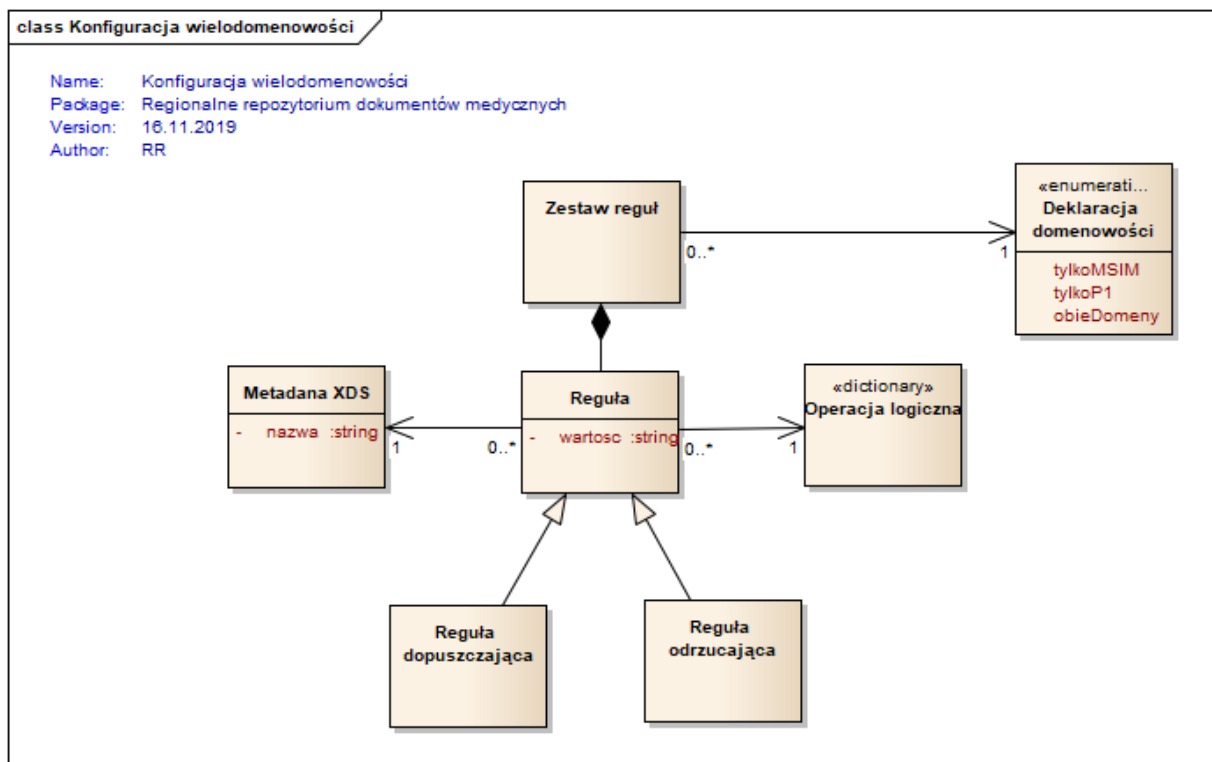


Rysunek nr 3.33 Diagram aktywności obszaru „Zapisywanie dokumentu w repozytorium”

### 3.3.4 Model danych



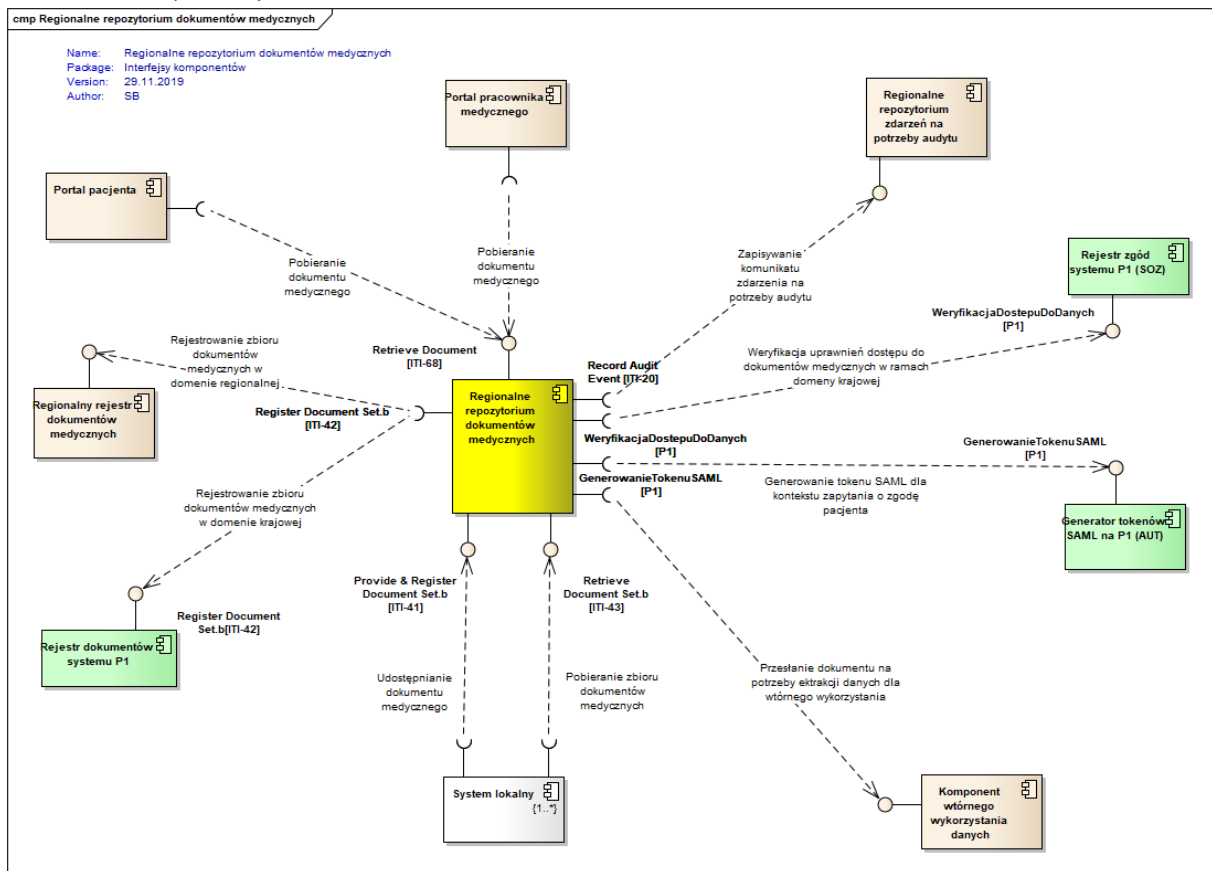
Rysunek nr 3.34 Model danych obszaru „Plik dokumentu medycznego”



Rysunek nr 3.35 Model danych obszaru "Konfiguracja wielodomenowości"

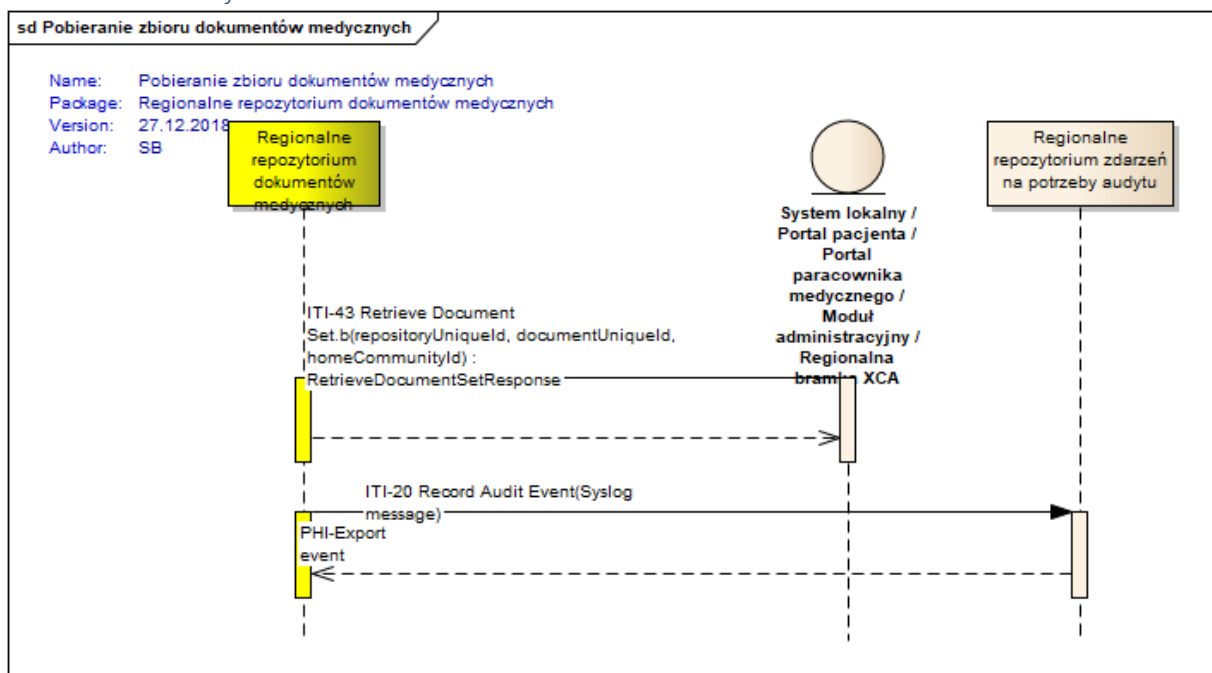
### 3.3.5 Komponenty i transakcje

#### 3.3.5.1 Komponenty

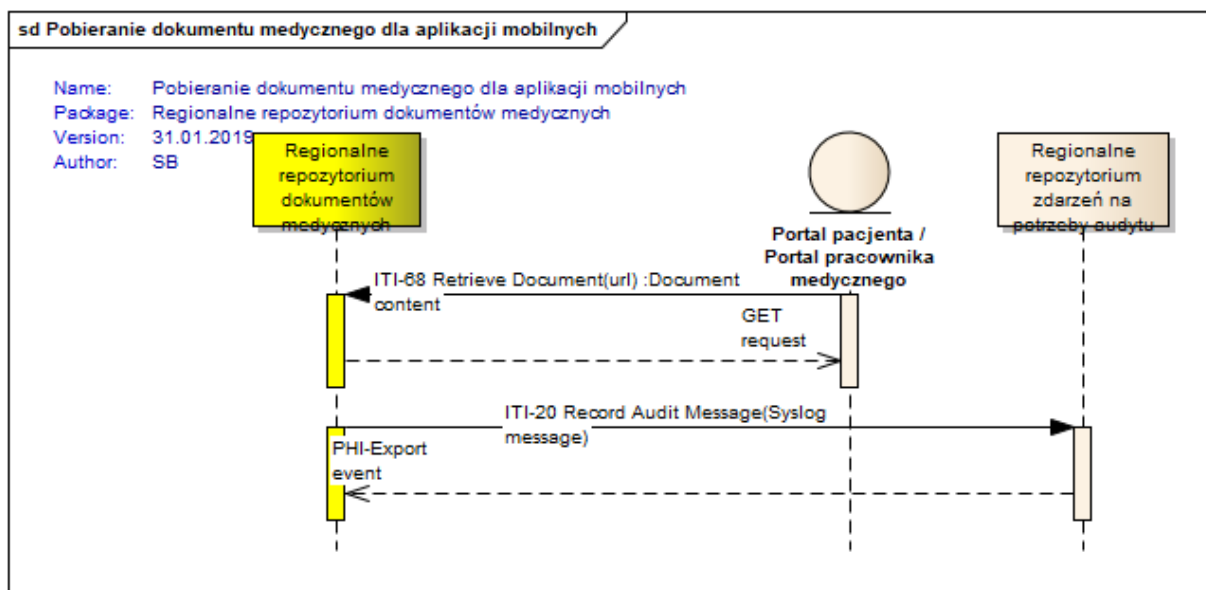


Rysunek nr 3.36 Diagram komponentów obszaru „Regionalne repozytorium dokumentów medycznych”

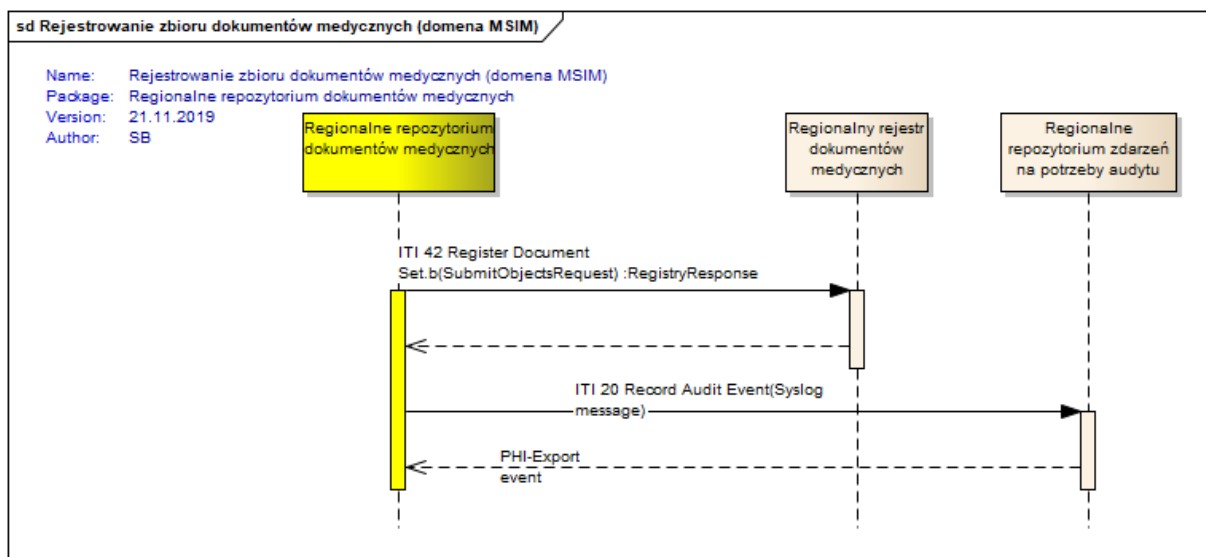
#### 3.3.5.2 Transakcje



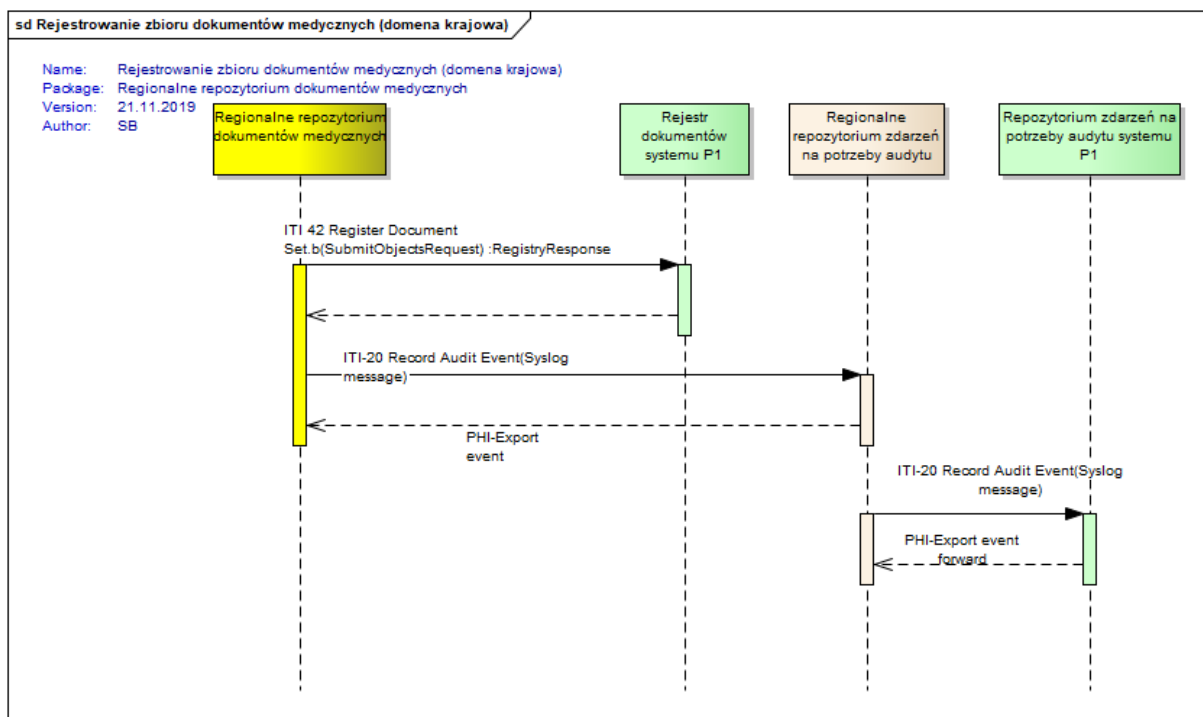
Rysunek nr 3.37 Diagram sekwencji transakcji „Pobieranie zbioru dokumentów medycznych”



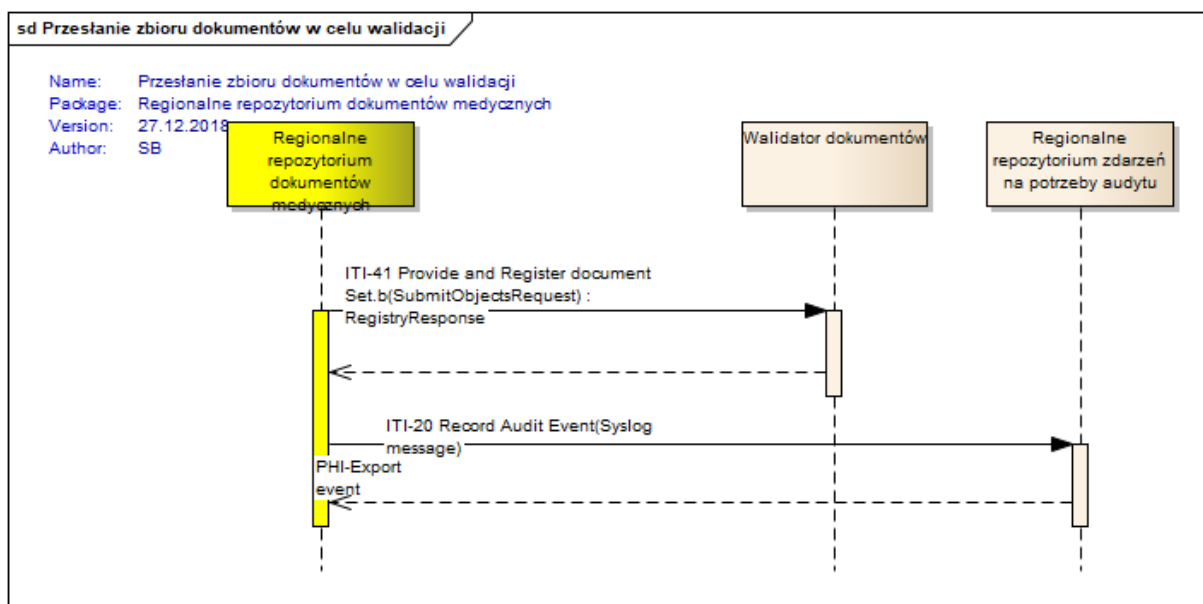
Rysunek nr 3.38 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego dla aplikacji mobilnych”



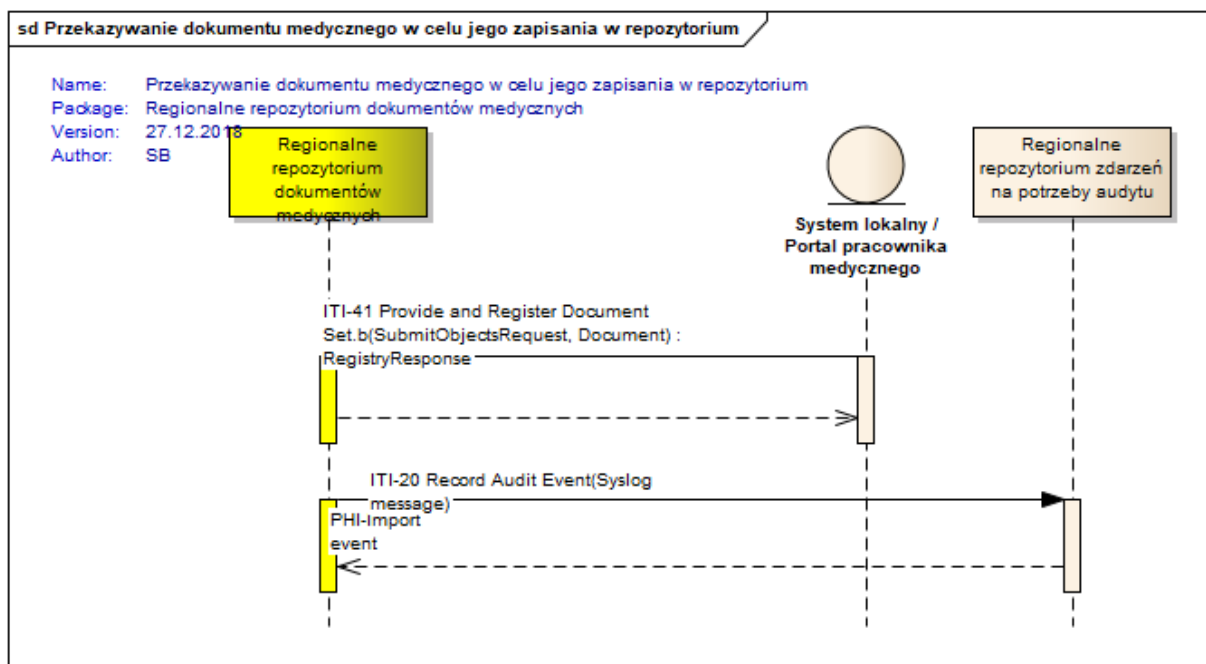
Rysunek nr 3.39 Diagram sekwencji transakcji „Rejestrowanie zbioru dokumentów medycznych (domena MSIM)”



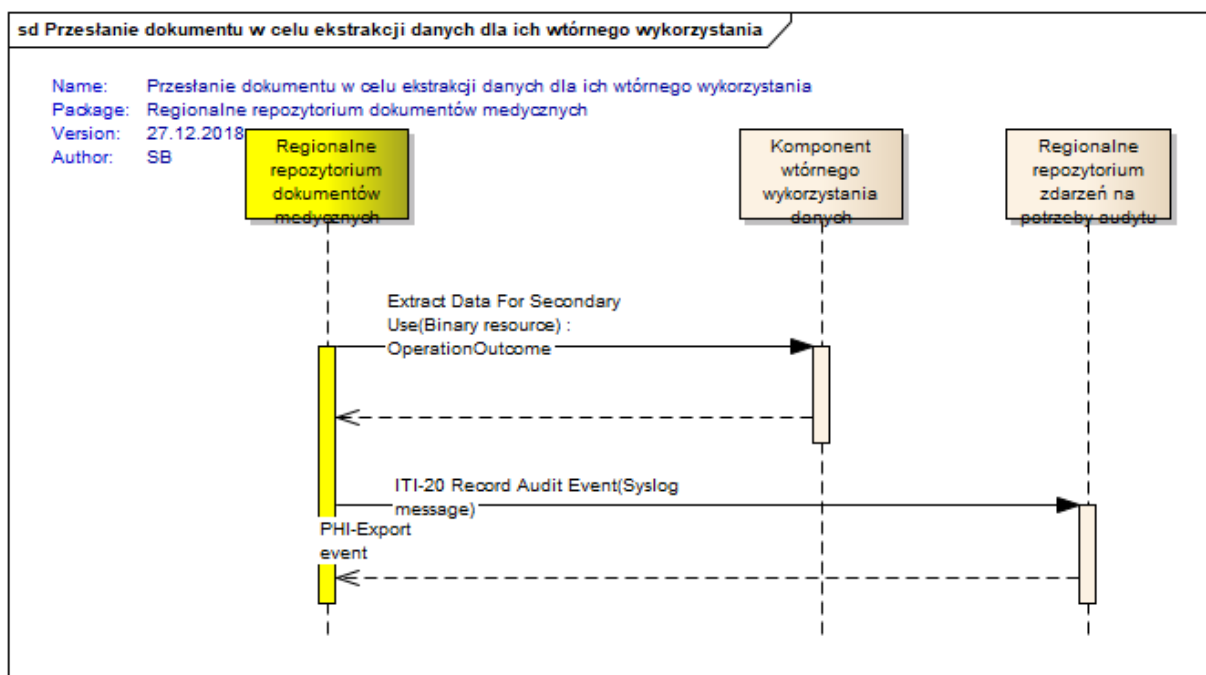
Rysunek nr 3.40 Diagram sekwencji transakcji "Rejestrowanie zbioru dokumentów medycznych (domena krajowa)"



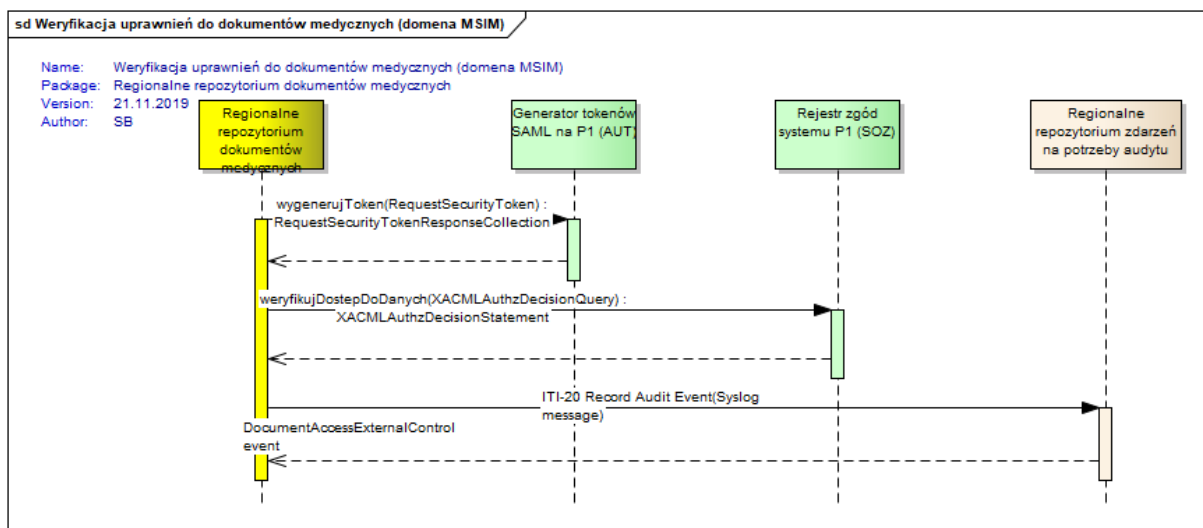
Rysunek nr 3.41 Diagram sekwencji transakcji „Przesłanie zbioru dokumentów w celu walidacji”



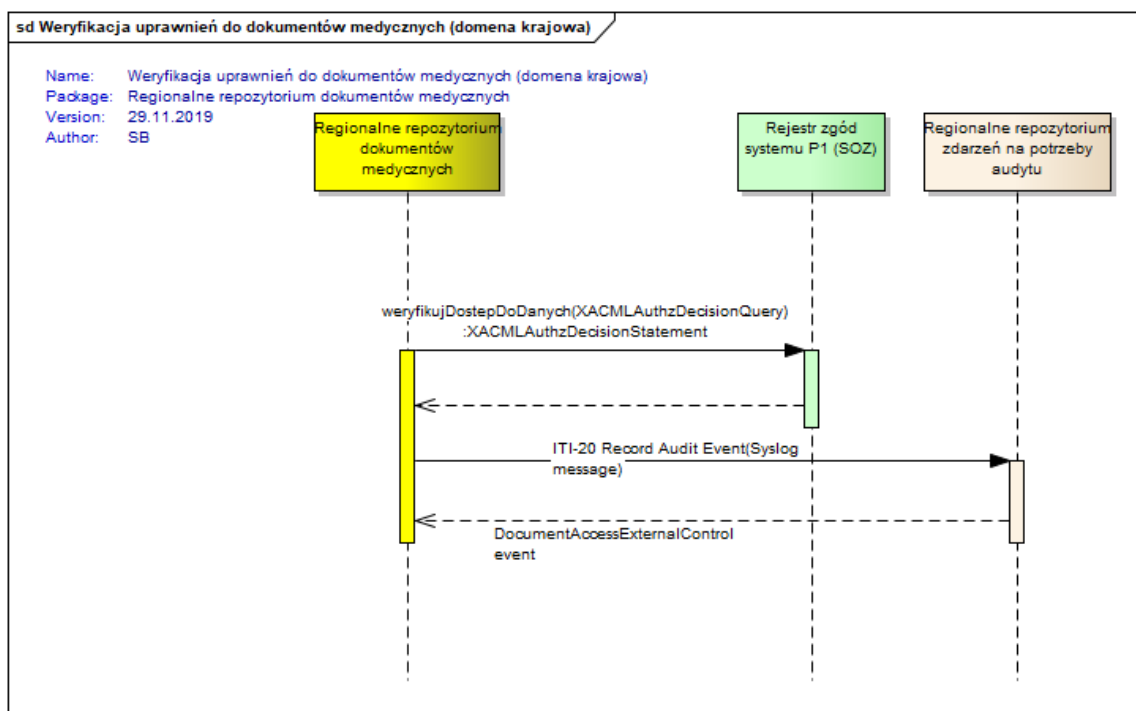
Rysunek nr 3.42 Diagram sekwencji transakcji „Przekazywanie dokumentu medycznego w celu jego zapisania w repozytorium”



Rysunek nr 3.43 Diagram sekwencji transakcji „Przesłanie dokumentu w celu ekstrakcji danych dla ich wtórnego wykorzystania”

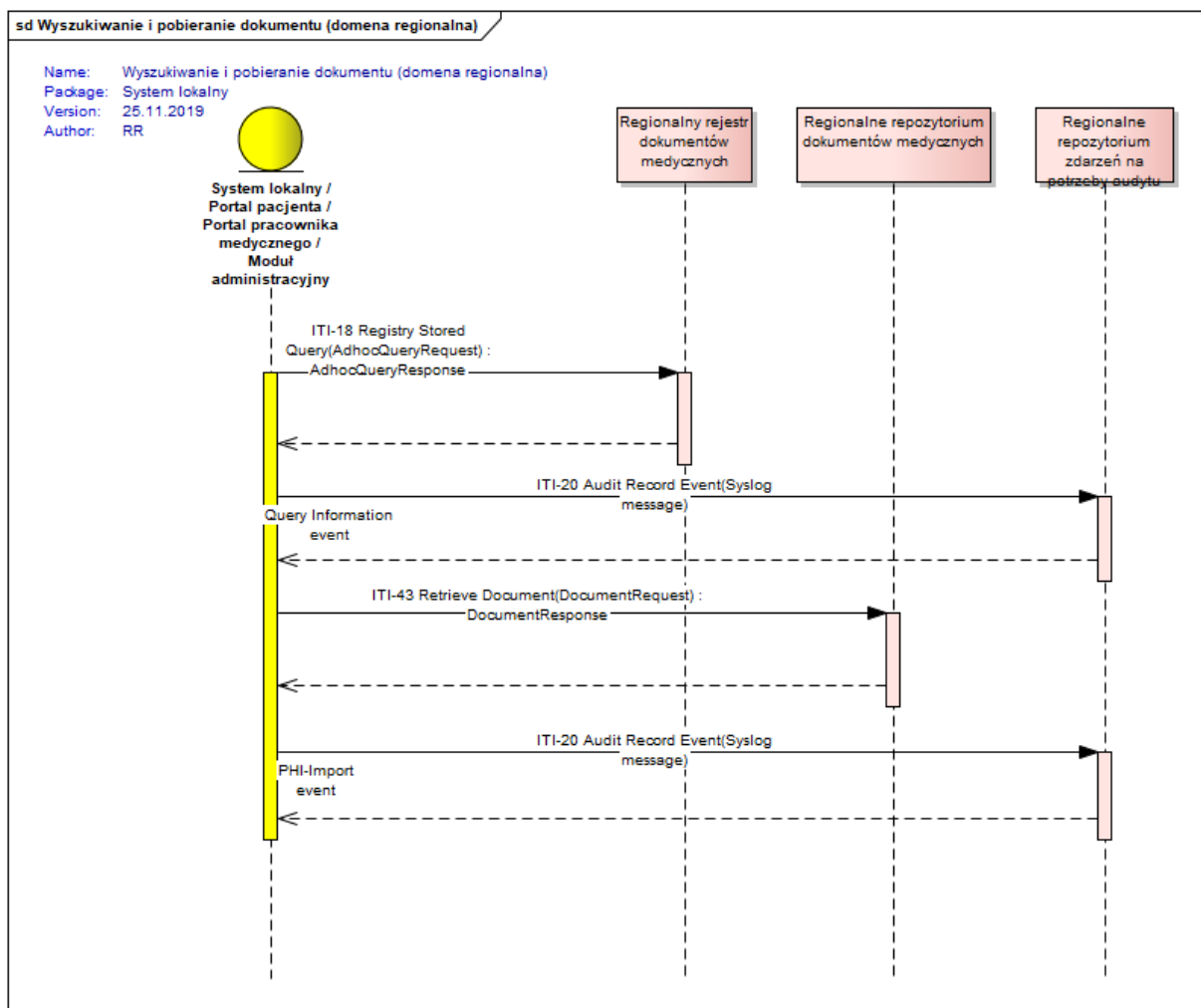


Rysunek nr 3.44 Diagram sekwencji transakcji „Weryfikacja uprawnień do dokumentów medycznych (domena MSIM)”

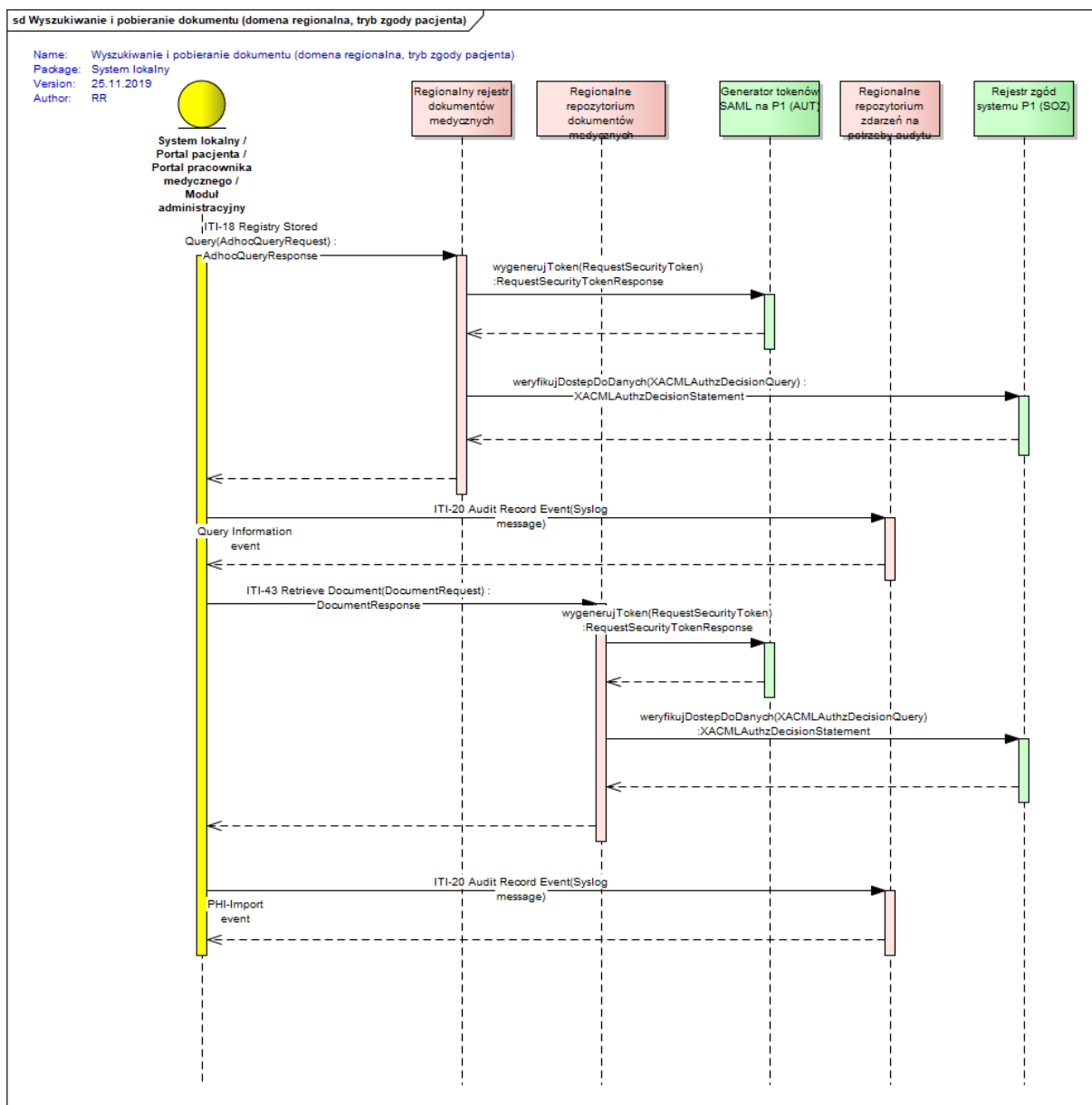


Rysunek nr 3.45 Diagram sekwencji transakcji "Weryfikacja uprawnień do dokumentów medycznych (domena MSIM)"

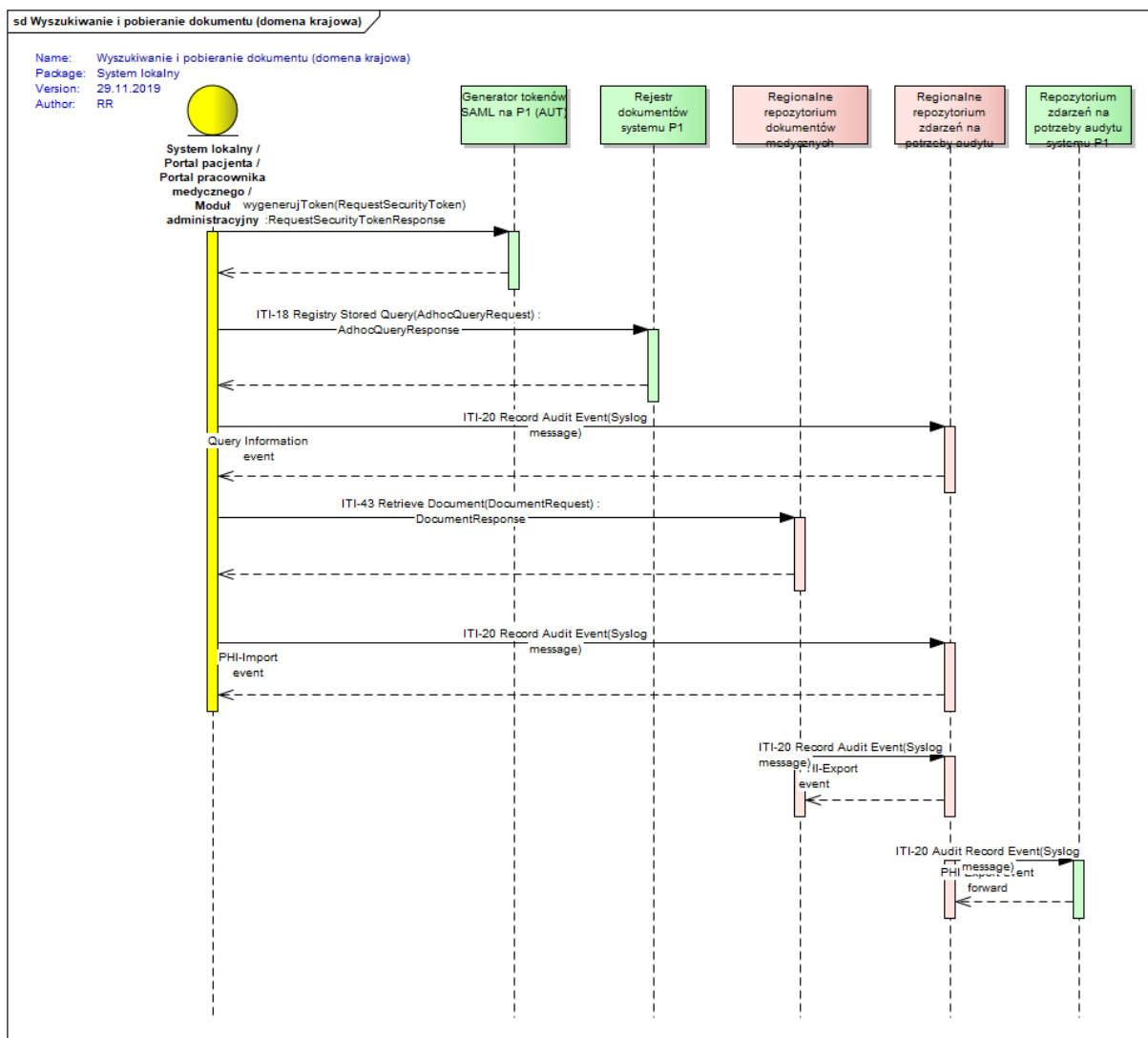




Rysunek nr 3.46 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena regionalna)"



Rysunek nr 3.47 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena regionalna, tryb zgody pacjenta)"



Rysunek nr 3.48 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena krajowa)"

### 3.4 Walidator dokumentów medycznych

#### 3.4.1 Wymagania funkcjonalne

**BE.WalDM.1.** System umożliwia weryfikację podpisu elektronicznego na dokumencie medycznym.

**BE.WalDM.2.** System obsługuje weryfikację następujących rodzajów podpisu:

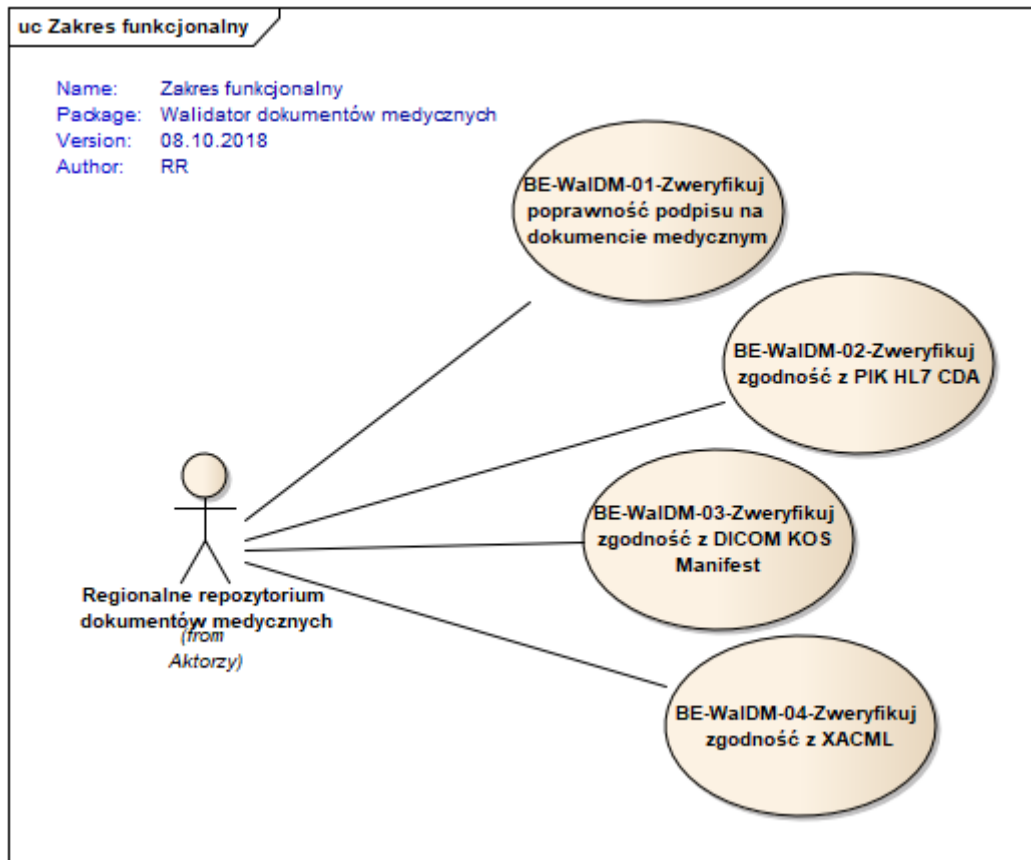
- podpis elektroniczny weryfikowany certyfikatem kwalifikowanym;
- podpis zaufany;
- podpis elektroniczny weryfikowany certyfikatem ZUS
- podpis osobisty.

**BE.WalDM.3.** System umożliwia weryfikację zgodności dokumentu medycznego z regionalną specyfikacją formatu dokumentów stanowiącą doprecyzowanie Polskiej Specyfikacji Krajowej HL7 CDA.

**BE.WalDM.4.** System umożliwia weryfikację zgodności dokumentu z DICOM.

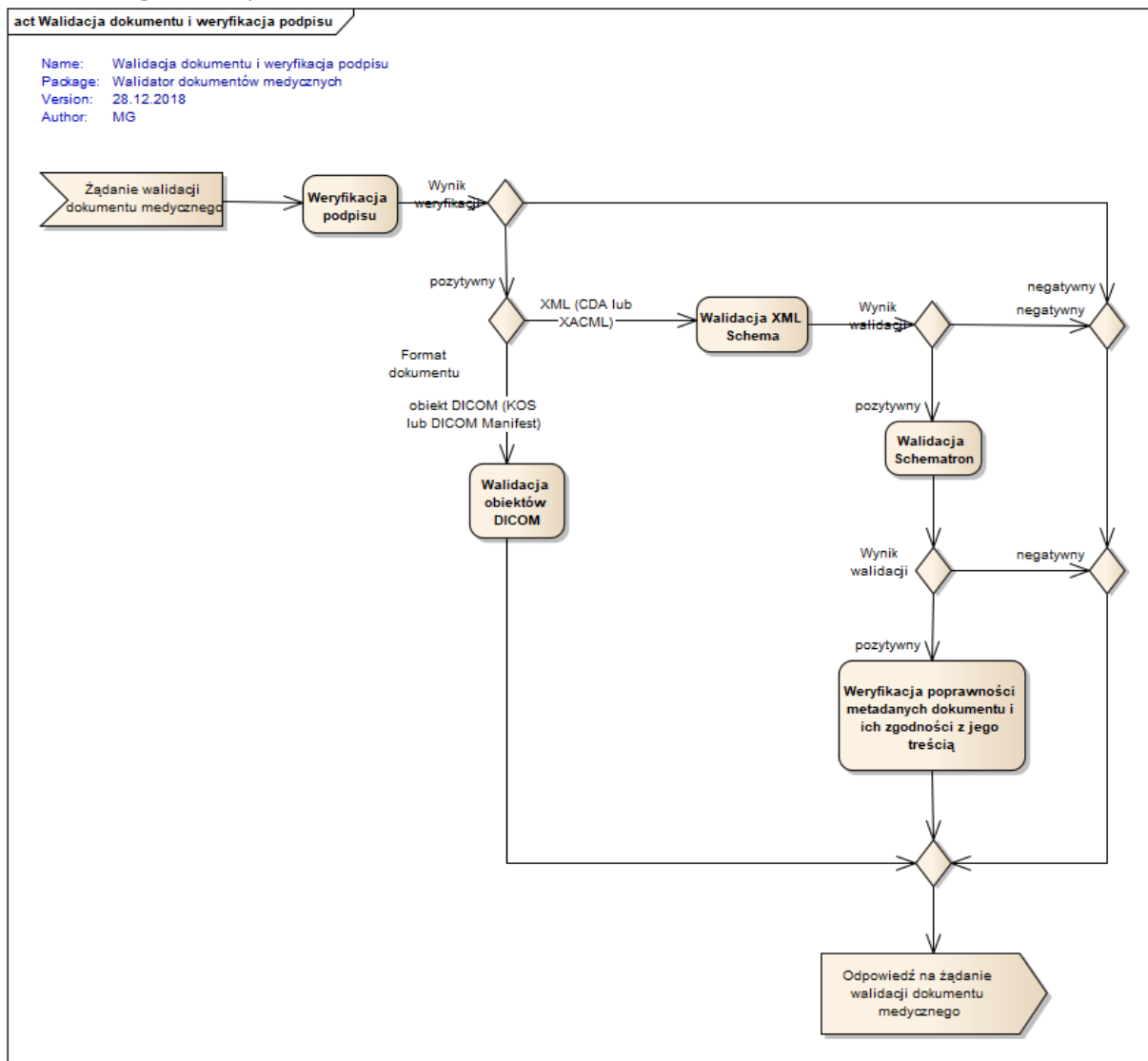
**BE.WalDM.5.** System umożliwia weryfikację zgodności dokumentu z XACML.

### 3.4.2 Model przypadków użycia



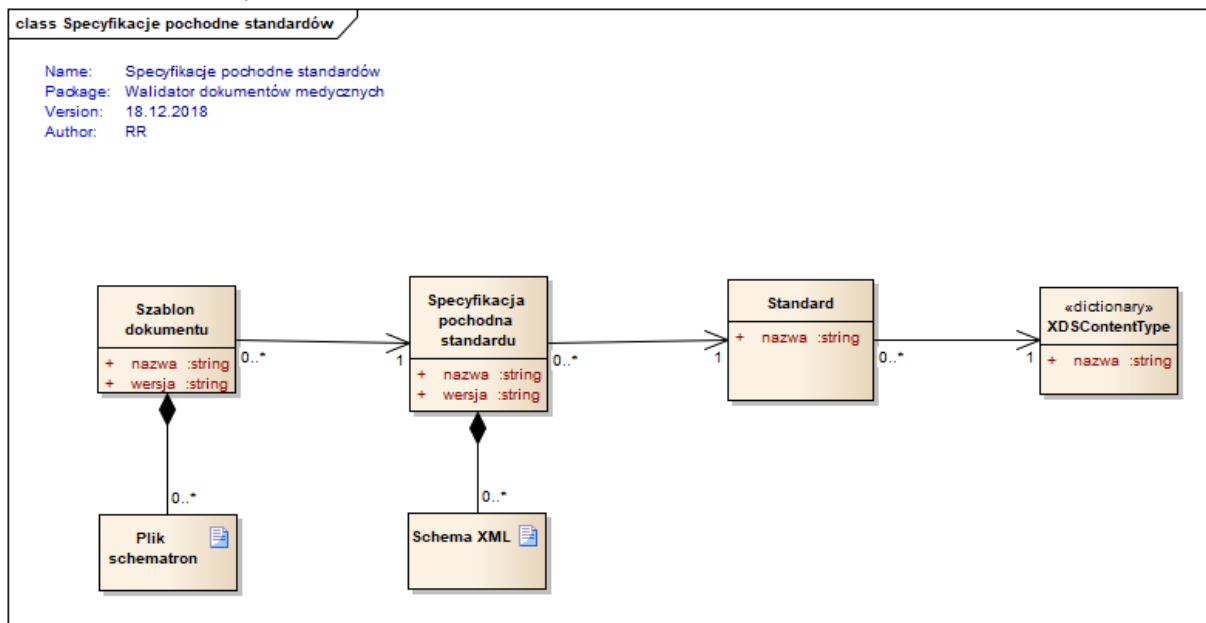
Rysunek nr 3.49 Diagram przypadków użycia obszaru „Walidator dokumentów medycznych”

### 3.4.3 Diagram aktywności



Rysunek nr 3.50 Diagram aktywności obszaru „Walidator dokumentów medycznych”

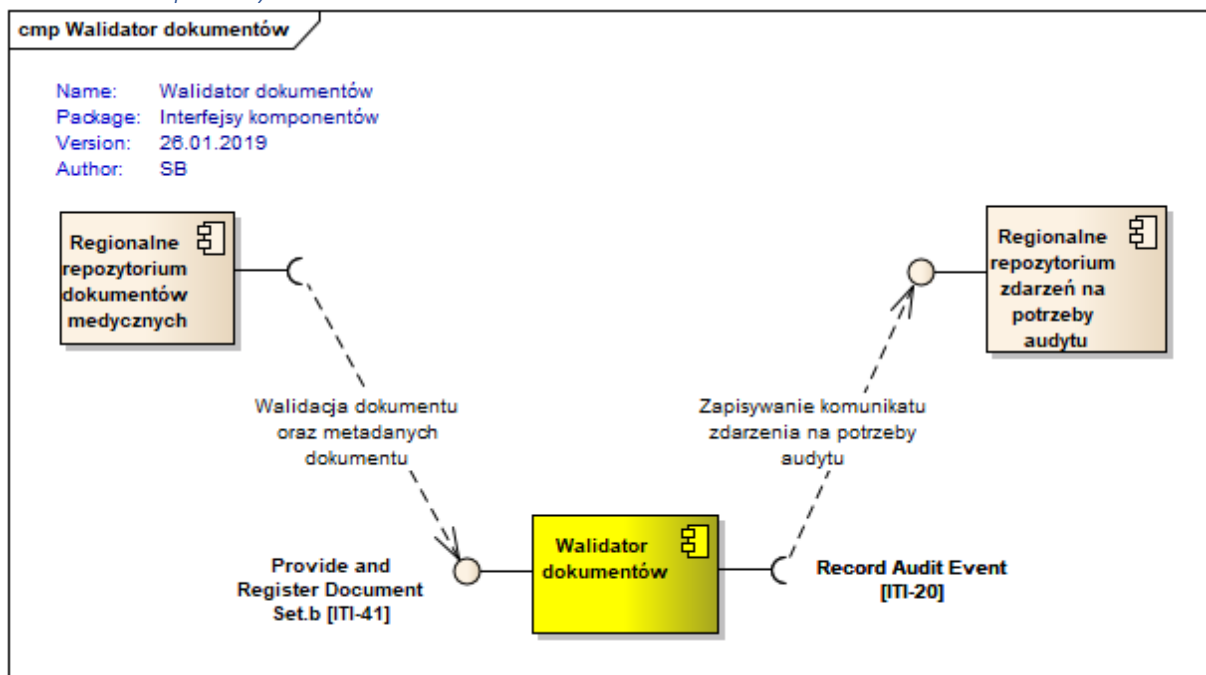
### 3.4.4 Model danych



Rysunek nr 3.51 Diagram klas obszaru "Specyfikacje pochodne standardów"

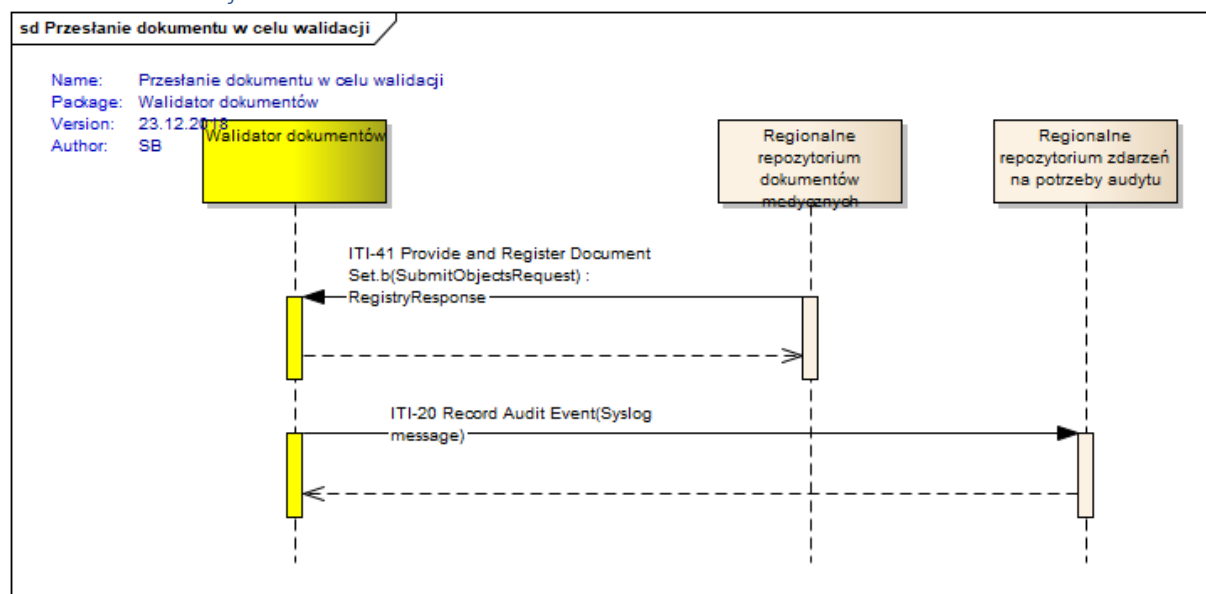
### 3.4.5 Komponenty i transakcje

#### 3.4.5.1 Komponenty



Rysunek nr 3.52 Diagram komponentów obszaru „Walidator dokumentów medycznych”

### 3.4.5.2 Transakcje



Rysunek nr 3.53 Diagram sekwencji transakcji „Przesłanie dokumentu w celu walidacji”

## 3.5 Komponent wtórnego wykorzystania danych

### 3.5.1 Wymagania funkcjonalne

**BE.KWWD.1.** System umożliwia ekstrakcję danych z dokumentów medycznych.

**BE.KWWD.2.** System umożliwia ekstrakcję danych z dokumentów przekazywanych do repozytorium regionalnego.

**BE.KWWD.3.** System nie umożliwia ekstrakcji danych z dokumentów znajdujących się tylko w lokalnych repozytoriach dokumentów medycznych.

**BE.KWWD.4.** System dokonuje wersjonowania zbiorów danych wyekstrahowanych z dokumentów medycznych przy kolejnych żądaniach ekstrakcji tych danych.

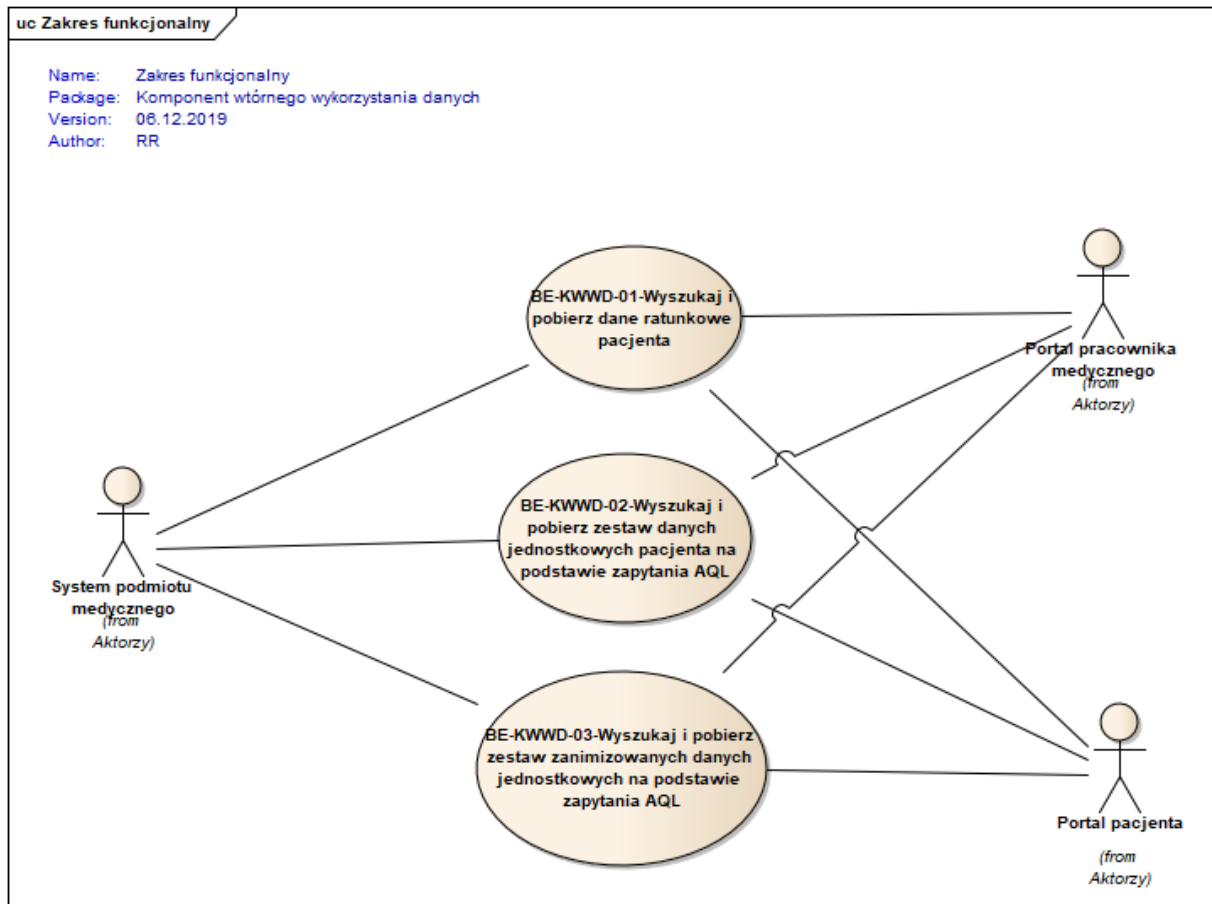
**BE.KWWD.5.** System dokonuje depersonalizacji danych wyekstrahowanych z dokumentu.

**BE.KWWD.6.** System zapisuje dane wyekstrahowane z dokumentów medycznych w strukturach zgodnych ze standardem OpenEHR jako instancje archetypów.

**BE.KWWD.7.** System umożliwia wykonywanie zapytań AQL (Archetype Query Language).

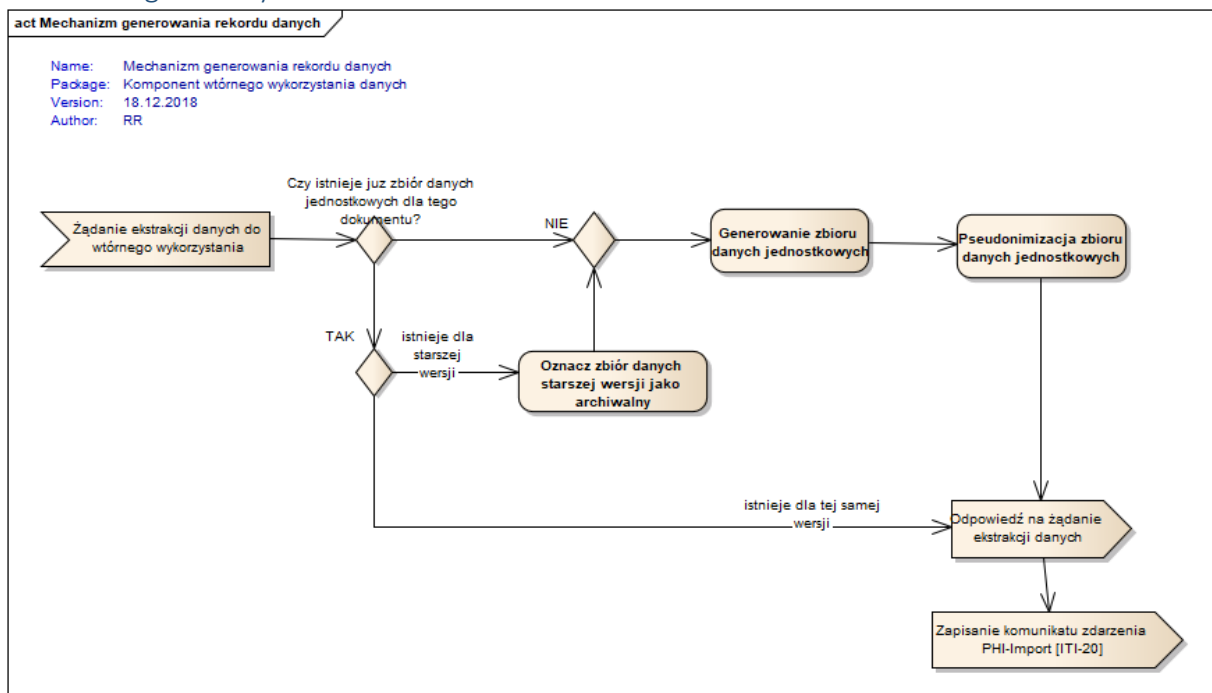
**BE.KWWD.8.** System umożliwia wykonywanie zapytań AQL w kontekście pacjenta oraz zapytań o dane zdepersonalizowane.

### 3.5.2 Model przypadków użycia



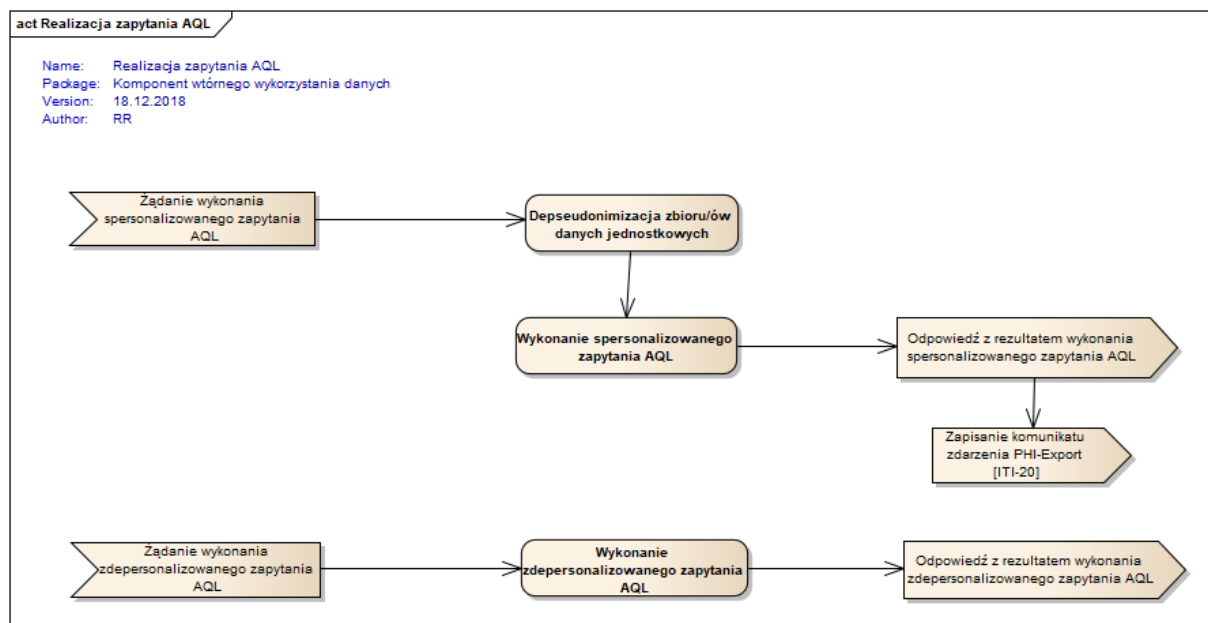
Rysunek nr 3.54 Diagram przypadków użycia obszaru „Komponent wtórnego wykorzystania danych”

### 3.5.3 Diagram aktywności



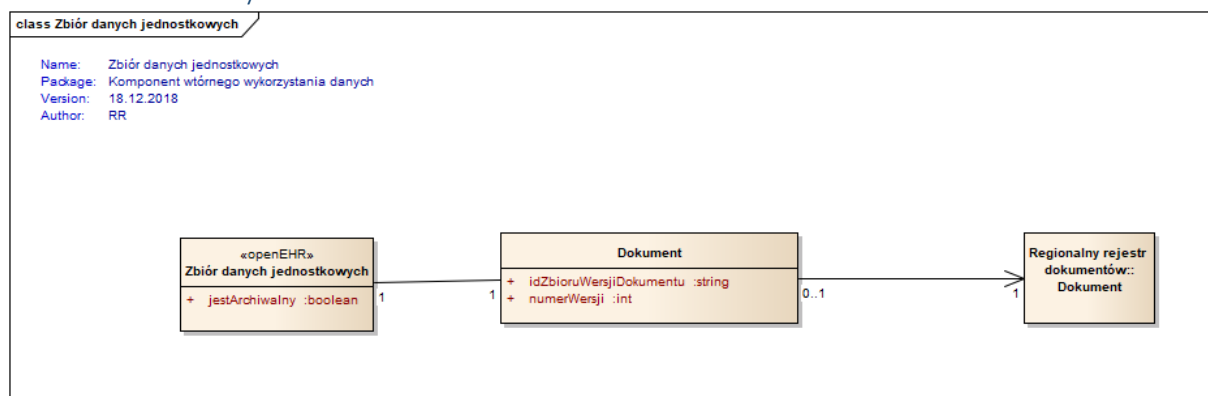
Rysunek nr 3.55 Diagram aktywności obszaru „Mechanizm generowania rekordu danych”



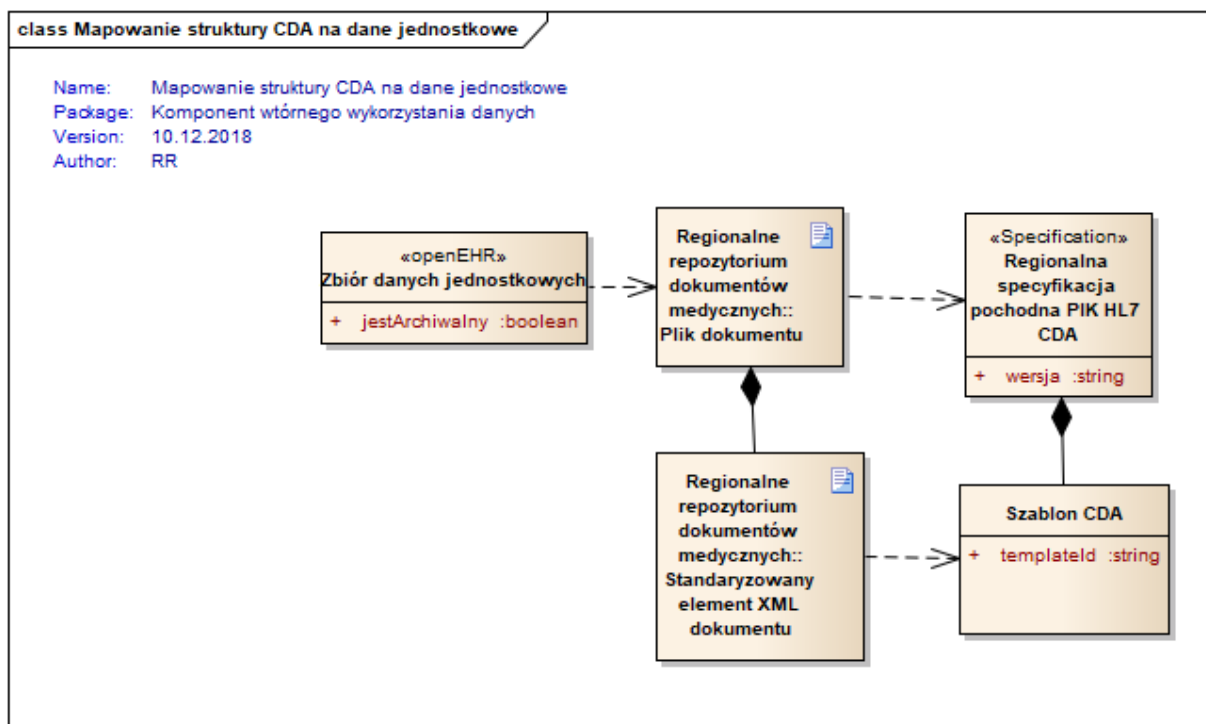


Rysunek nr 3.56 Diagram aktywności obszaru „Realizacja zapytania AQL”

### 3.5.4 Model danych



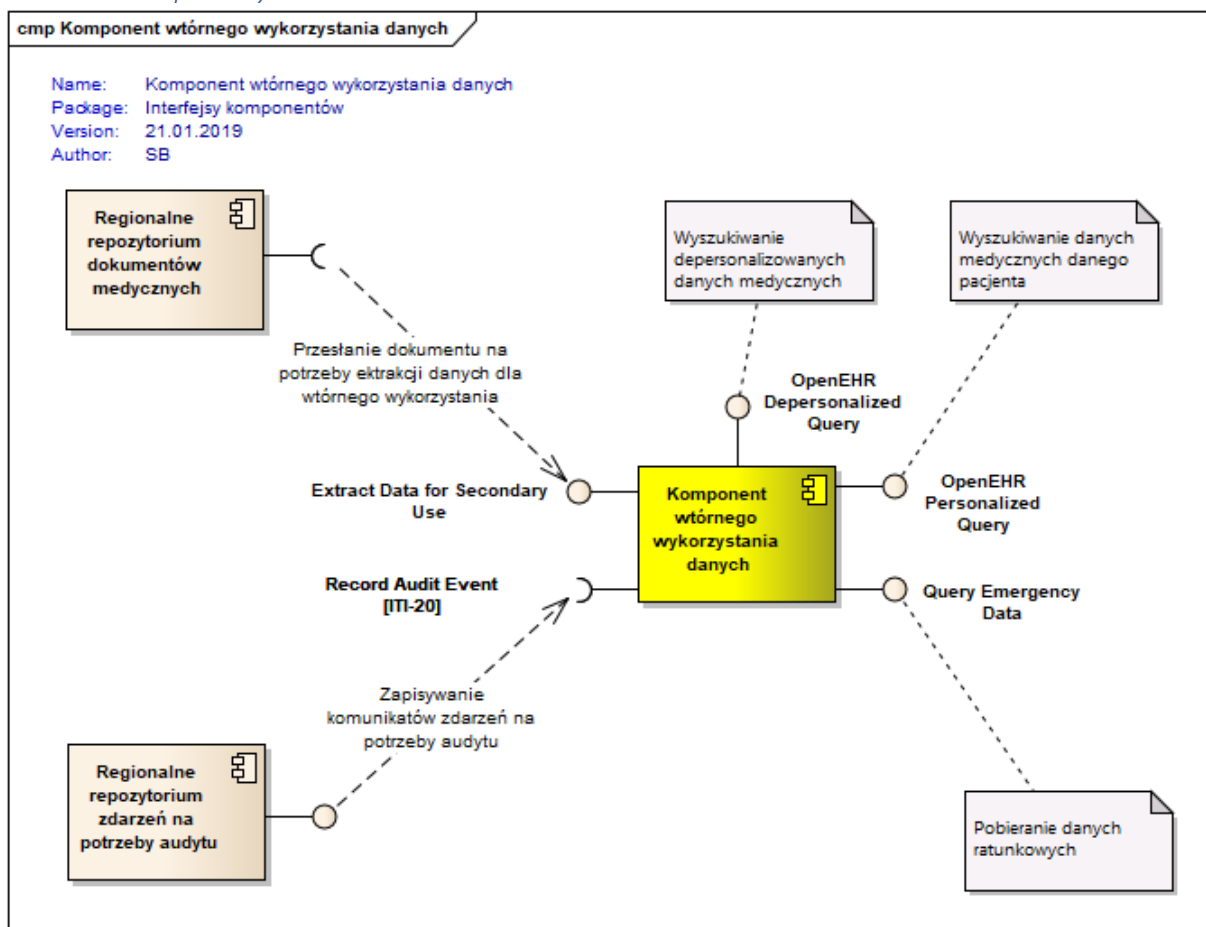
Rysunek nr 3.57 Diagram klas obszaru „Zbiór danych jednostkowych”



Rysunek nr 3.58 Diagram klas obszaru „Mapowanie struktury CDA na dane jednostkowe”

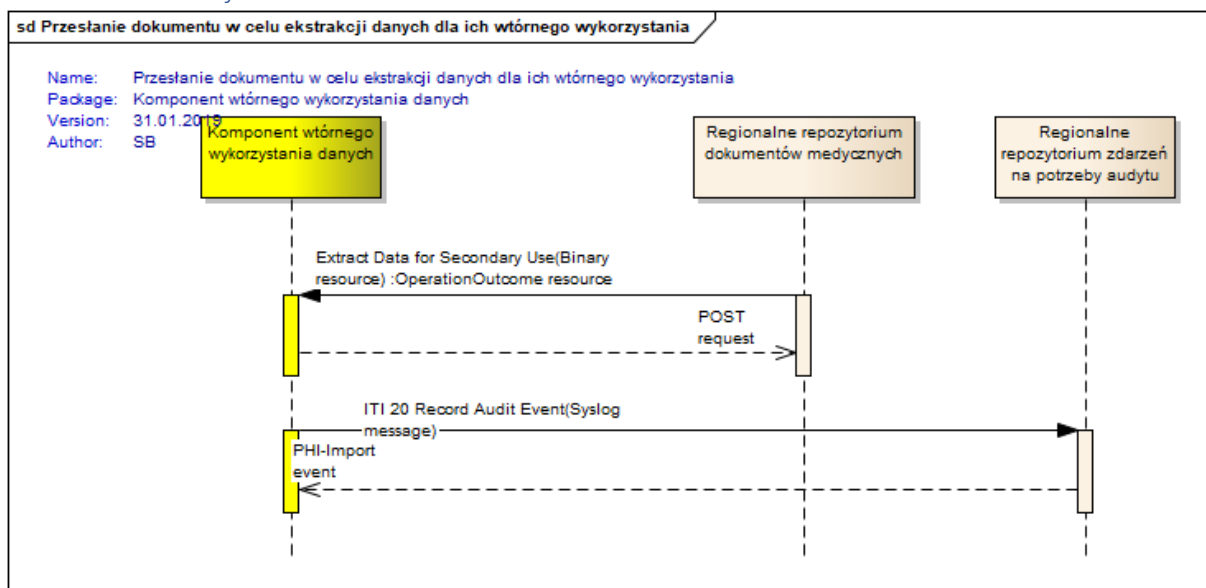
### 3.5.5 Komponenty i transakcje

#### 3.5.5.1 Komponenty

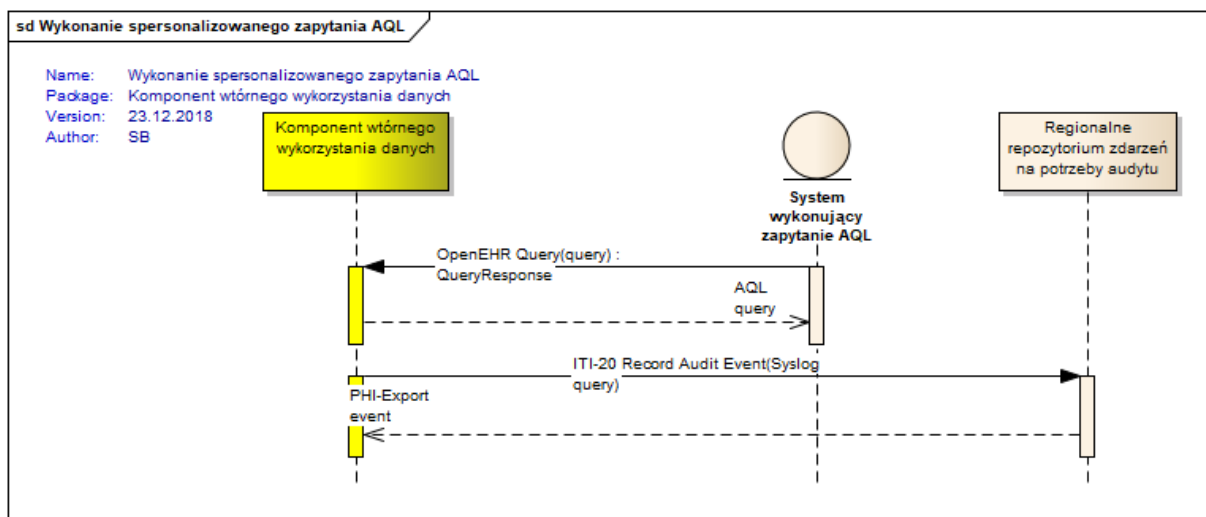


Rysunek nr 3.59 Diagram komponentów obszaru „Komponent wtórnego wykorzystania danych”

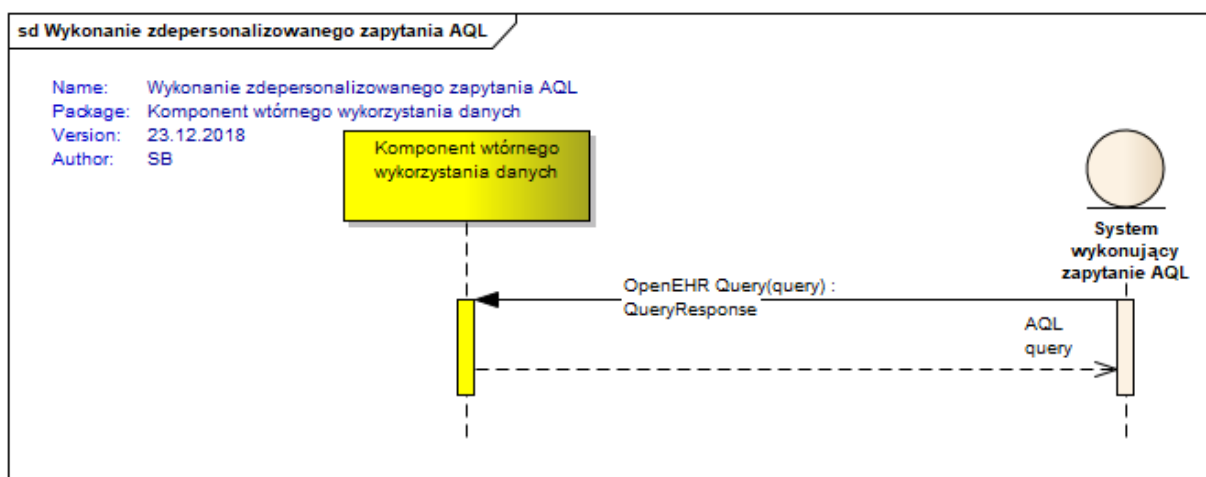
#### 3.5.5.2 Transakcje



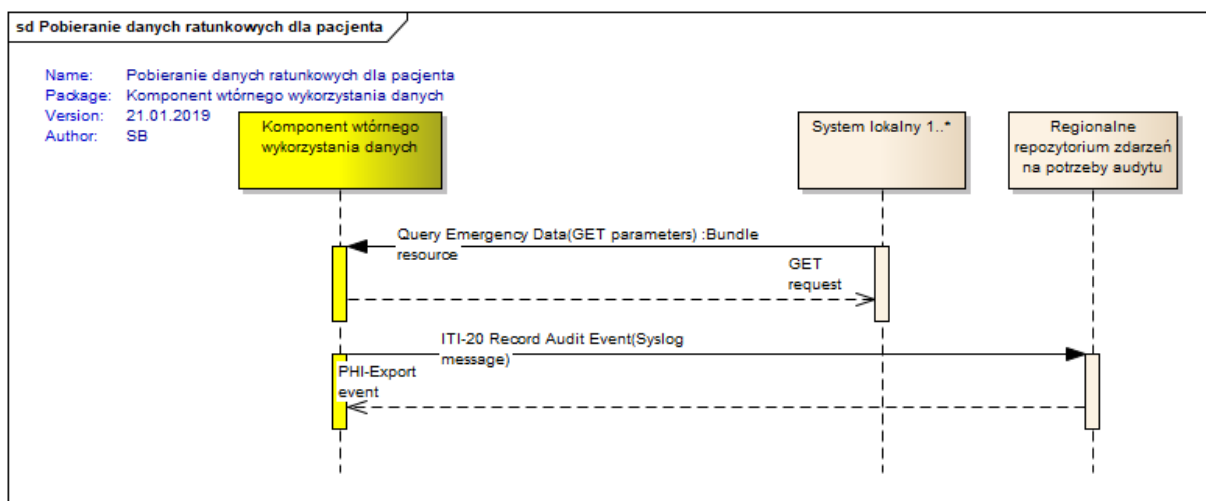
Rysunek nr 3.60 Diagram sekwencji transakcji „Przesłanie dokumentu w celu ekstrakcji danych dla ich wtórnego wykorzystania”



Rysunek nr 3.61 Diagram sekwencji transakcji „Wykonanie spersonalizowanego zapytania AQL”



Rysunek nr 3.62 Diagram sekwencji transakcji „Wykonanie zdepersonalizowanego zapytania AQL”



Rysunek nr 3.63 Diagram sekwencji transakcji „Pobieranie danych ratunkowych dla pacjenta”

## 3.6 Regionalny broker wolnych terminów i rezerwacji

### 3.6.1 Wymagania funkcjonalne

**BE.BGWW.1.** System umożliwia wyszukiwanie wolnych terminów w systemach lokalnych.

**BE.BGWW.2.** System umożliwia tworzenie rezerwacji terminów w systemach lokalnych.

**BE.BGWW.3.** System umożliwia wyszukiwanie rezerwacji terminów w systemach lokalnych.

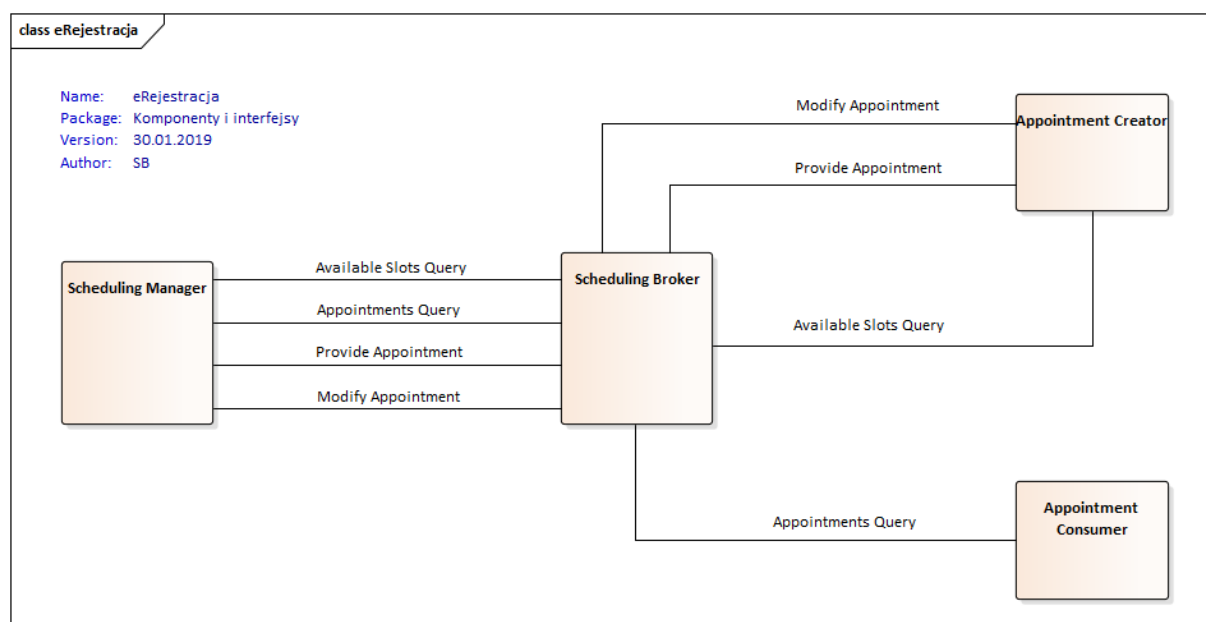
**BE.BGWW.4.** System umożliwia modyfikację rezerwacji terminów w systemach lokalnych.

**BE.BGWW.5.** System umożliwia anulowanie rezerwacji terminów w systemach lokalnych.

### 3.6.2 Model przypadków użycia

Niniejszy obszar został zamodelowany według stylu notacji używanego w dokumentacji IHE.

Przedstawione na diagramie komponenty są w istocie rolami (aktorami), które mogą być pełnione przez różne komponenty MSIM, a relacje na diagramie odzwierciedlają przypadki użycia możliwe do wywołania przez te role (aktorów).



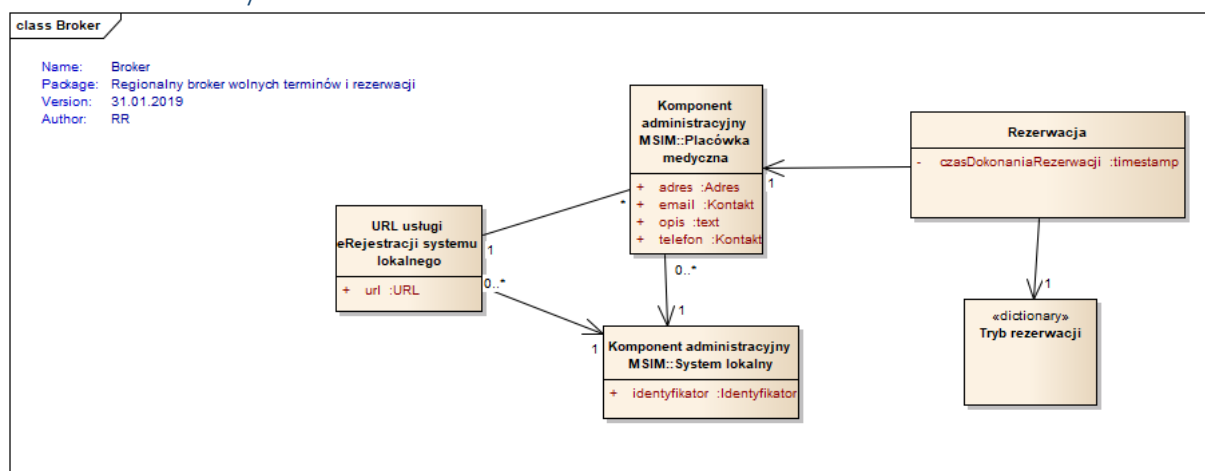
Rysunek nr 3.64 Aktorzy i transakcje obszaru „eRejestracja”

1. Scheduling Manager – system / komponent, który na podstawie wewnętrznej, złożonej konfiguracji grafików udostępnia listę wolnych terminów oraz przechowuje informacje o dokonanych rezerwacjach wolnych terminów dla danego pacjenta. System / komponent umożliwia ponadto zarządzanie dokonanymi rezerwacjami poprzez ich edycję lub anulowanie.
2. Scheduling Broker – system / komponent, który pośredniczy w komunikacji pomiędzy systemami / komponentami dostarczającymi informacji o wolnych terminach i dokonanych rezerwacjach (Scheduling Manager), a komponentami / systemami, które tworzą, zarządzają lub wyszukują dokonanych rezerwacji wolnych terminów. System / komponent przekazuje zapytanie do wielu systemów źródłowych i zwraca zbiorczą informację do systemu, który wygenerował zapytanie. Na podstawie wewnętrznej konfiguracji, system / komponent jest w stanie optymalizować wysyłanie zapytań do systemów źródłowych, eliminując te, które nie mają sensu w kontekście treści samego zapytania.

3. Appointment Creator – system / komponent, który wyszukuje wolne terminy i na tej podstawie tworzy rezerwację wolnego terminu dla danego pacjenta. System / komponent odpowiedzialny jest również za zarządzanie dokonanymi rezerwacjami – ich modyfikowaniem lub anulowaniem.
4. Appointment Consumer – system / komponent, który wyszukuje dokonanych rezerwacji dla danego pacjenta.

Systemy lokalne partnerów projektu pełnią rolę *Scheduling Manager*. Systemy lokalne pełnią również rolę *Appointment Creator* oraz *Appointment Consumer* w zakresie tworzenia, modyfikacji anulowania oraz wyszukiwania rezerwacji terminów wizyt. Komponent Regionalny broker wolnych terminów i rezerwacji odgrywa rolę *Scheduling Broker*. Aplikacje portalowe (Portal pacjenta, Portal pracownika medycznego) oraz moduł administracyjny MSIM, podobnie jest systemy lokalne, pełnią rolę *Appointment Creator* oraz *Appointment Consumer* w zakresie wyszukiwania i zarządzania rezerwacjami.

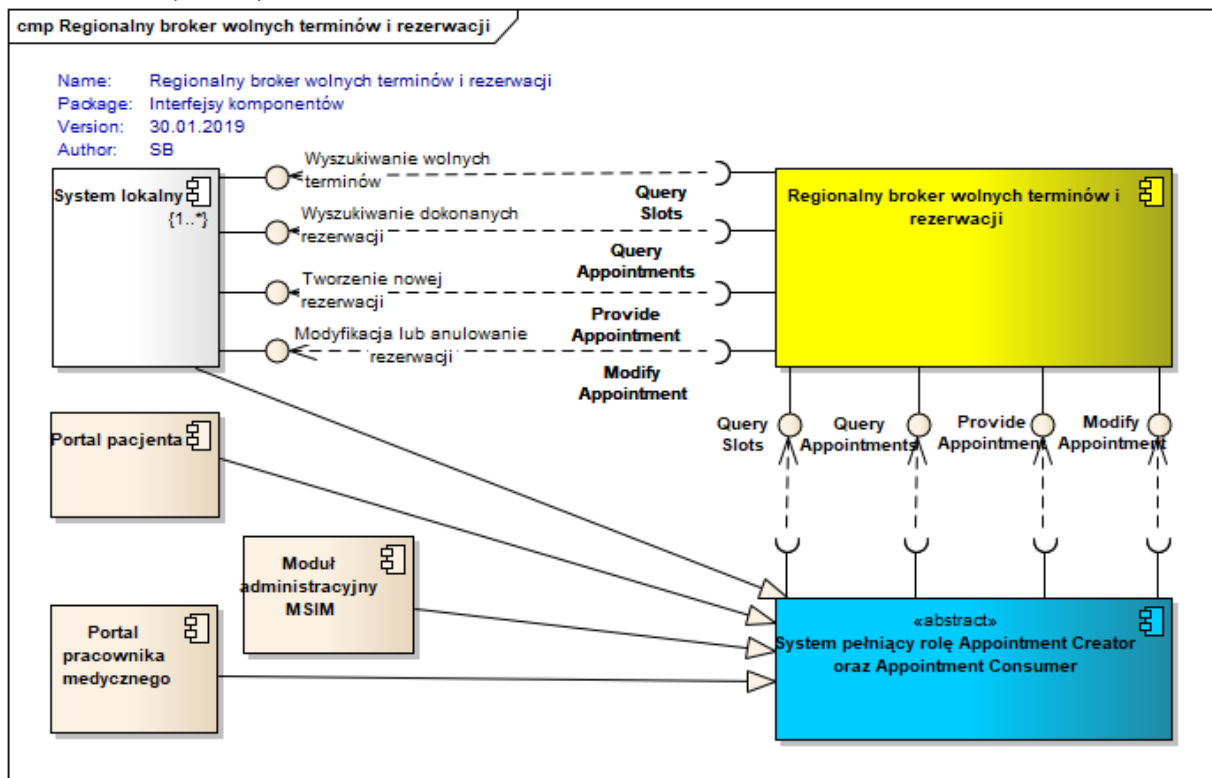
### 3.6.3 Model danych



Rysunek nr 3.65 Diagram klas obszaru „Regionalny broker wolnych terminów i rezerwacji”

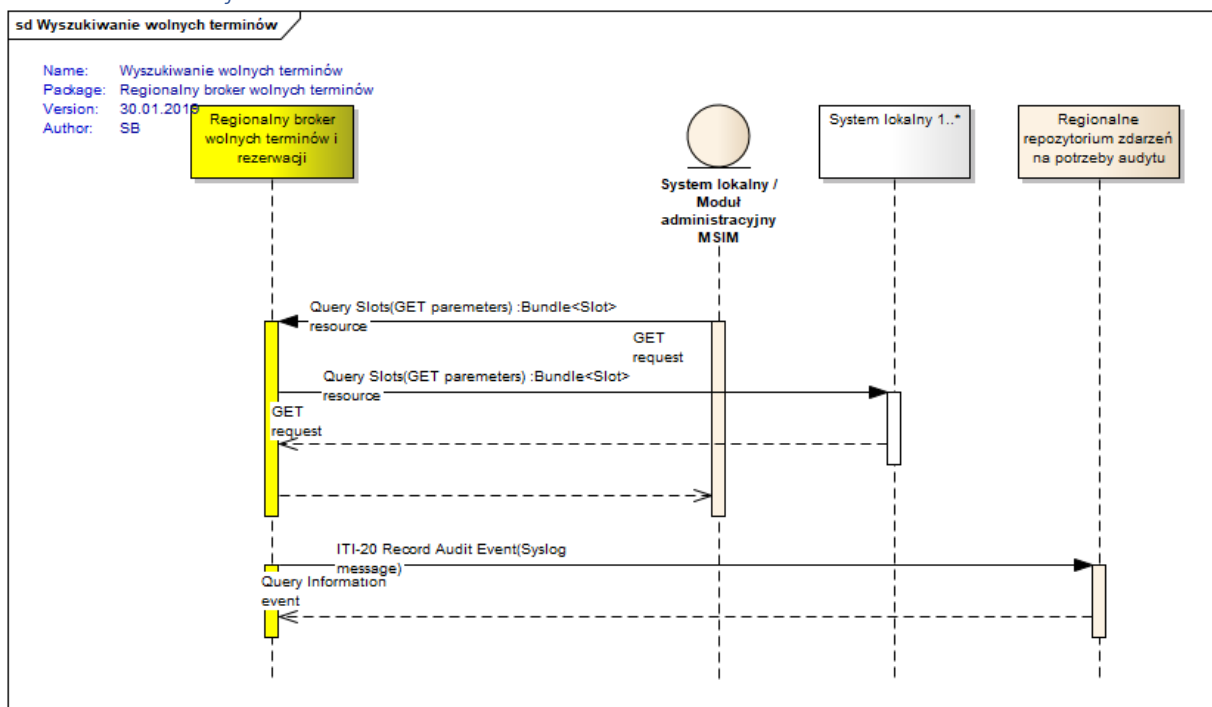
### 3.6.4 Komponenty i transakcje

#### 3.6.4.1 Komponenty

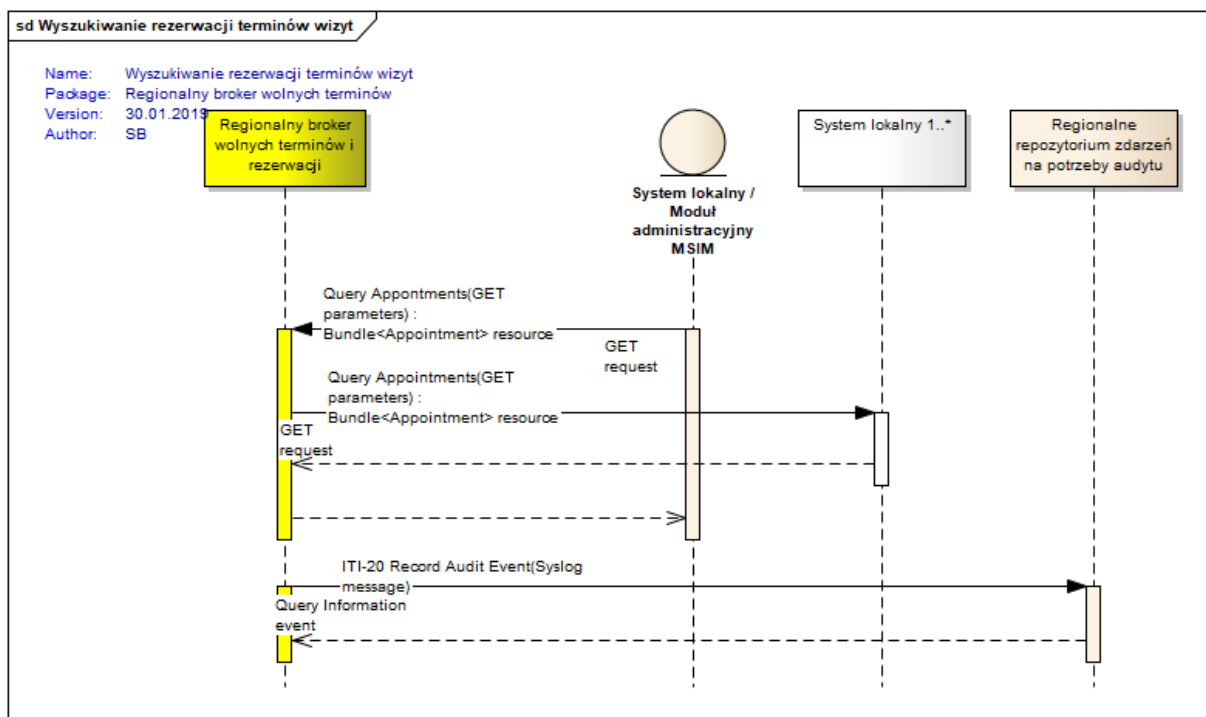


Rysunek nr 3.66 Diagram komponentów obszaru „Regionalny broker wolnych terminów i rezerwacji”

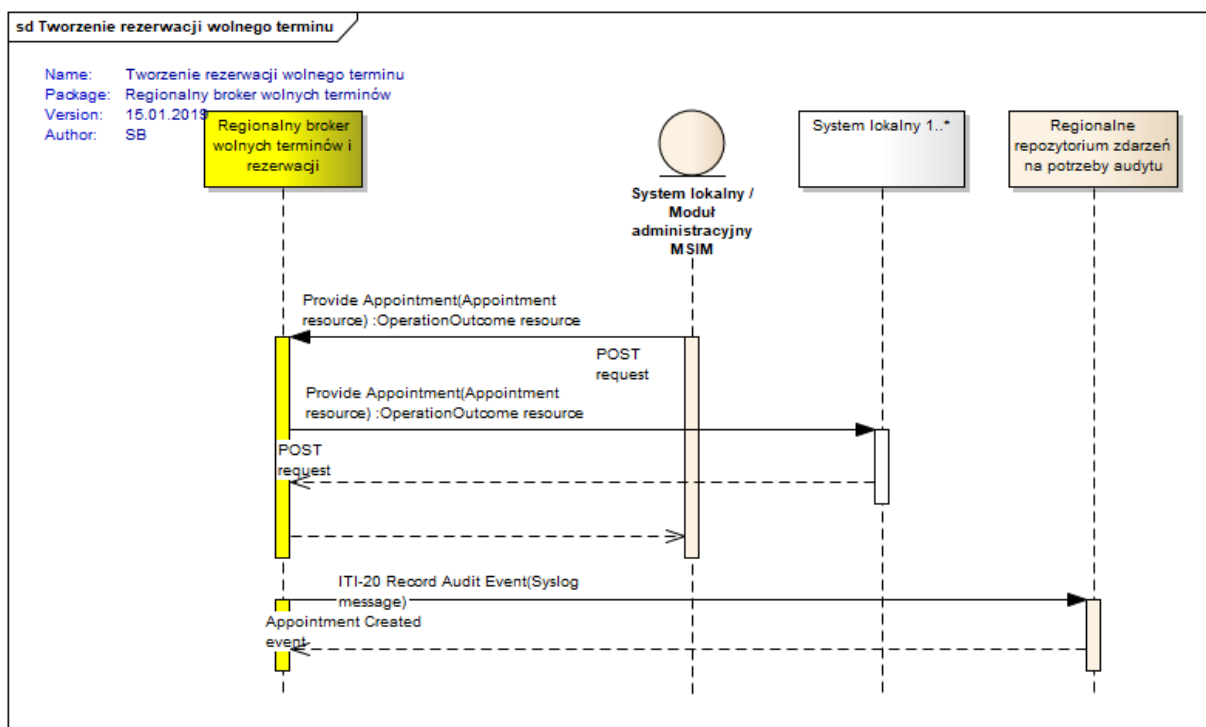
#### 3.6.4.2 Transakcje



Rysunek nr 3.67 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów”

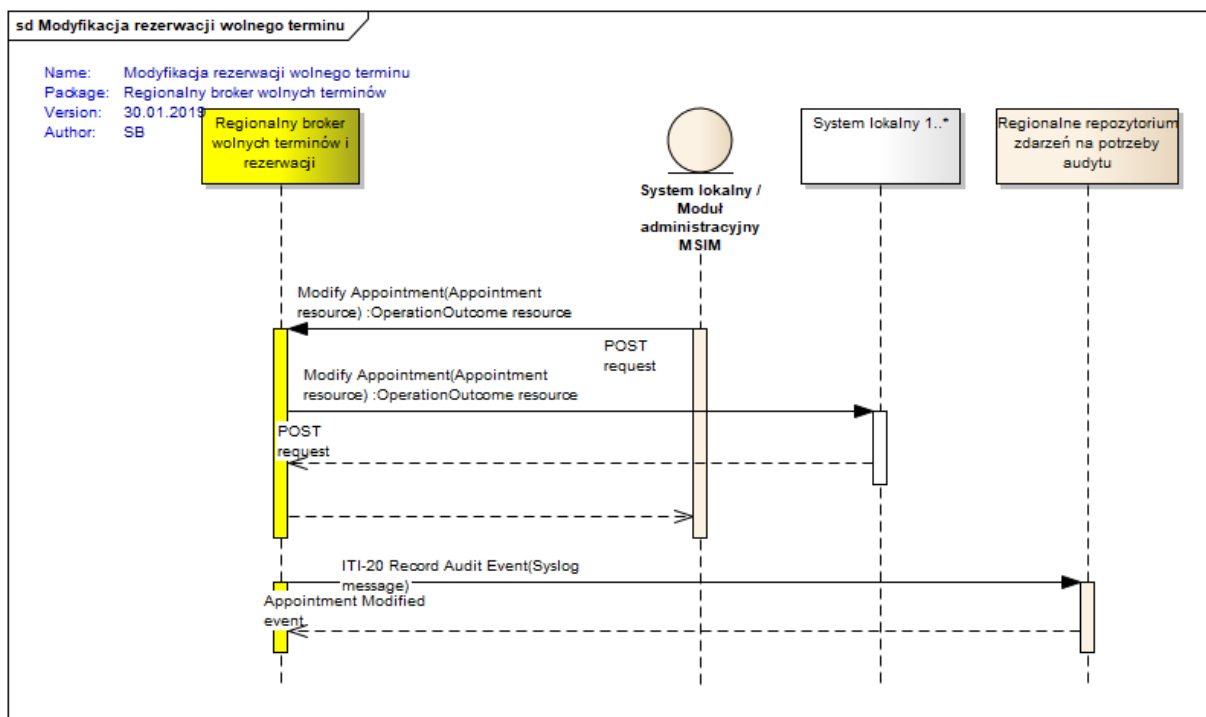


Rysunek nr 3.68 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów wizyt”

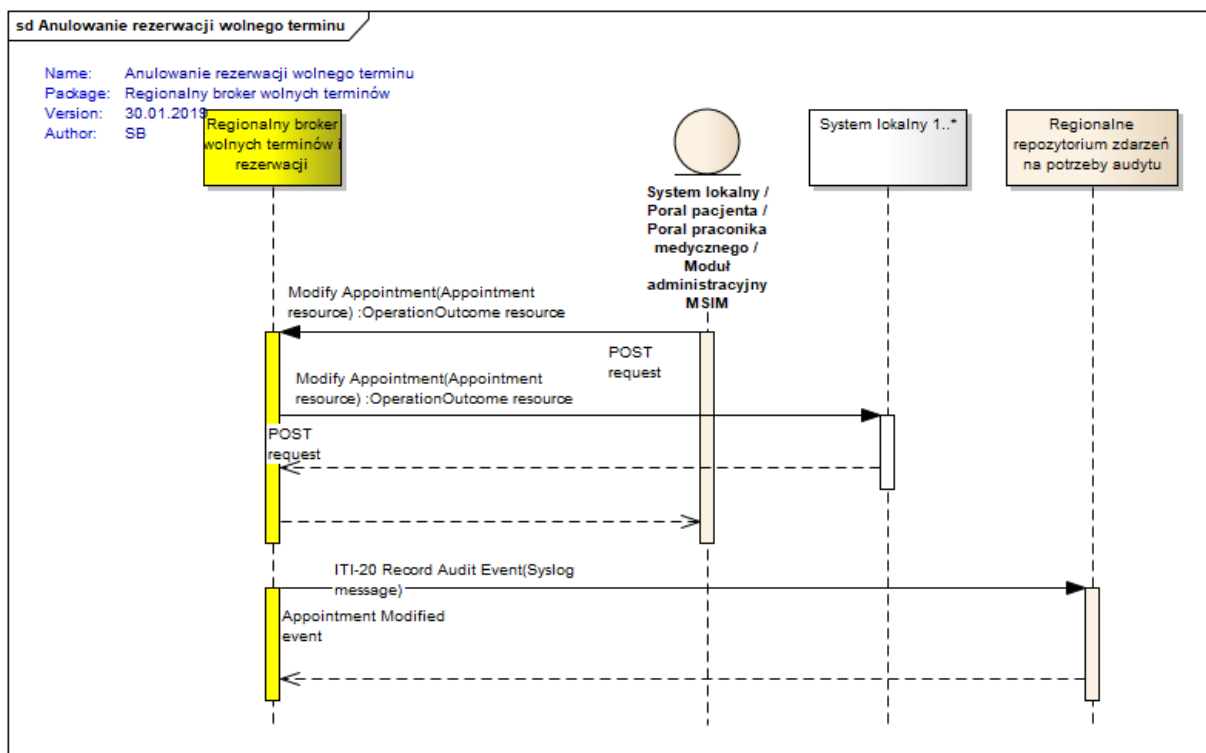


Rysunek nr 3.69 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu”





Rysunek nr 3.70 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu”



Rysunek nr 3.71 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu”

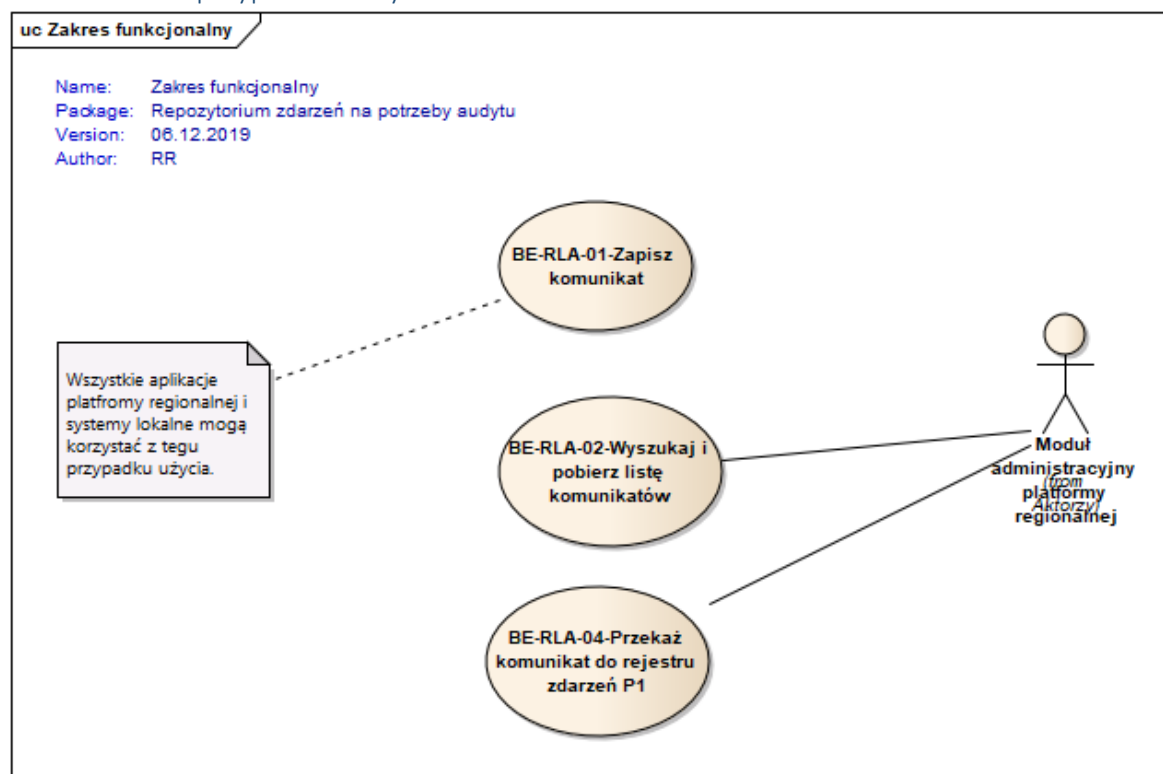
### 3.7 Regionalne repozytorium zdarzeń na potrzeby audytu

#### 3.7.1 Wymagania funkcjonalne

**BE.RLA.1.** System loguje zdarzenia błędów działania aplikacji.

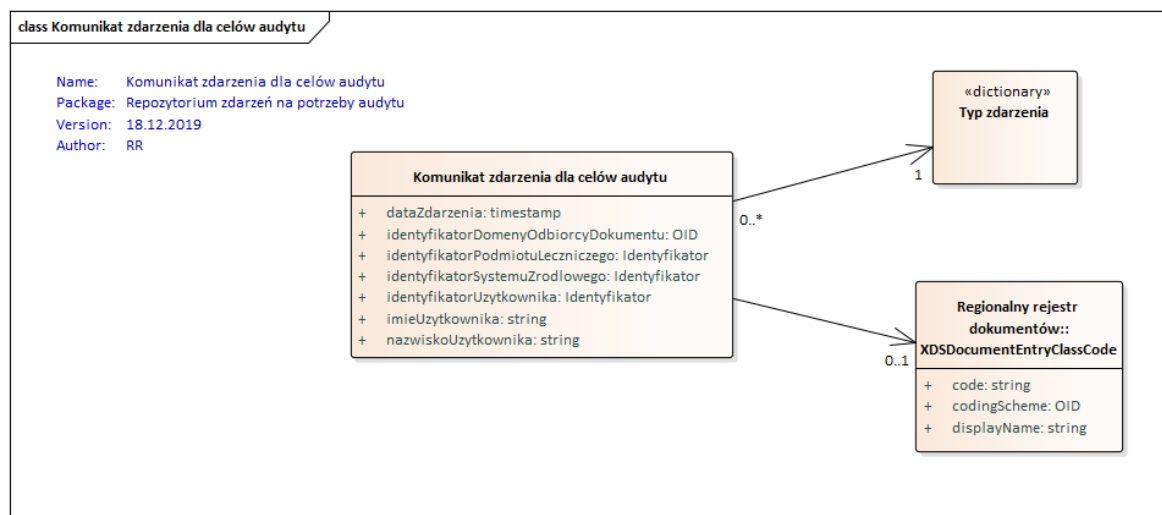
- BE.RLA.2.** System loguje zdarzenia naruszenia zasad bezpieczeństwa
- BE.RLA.3.** System loguje zdarzenia komunikacji pomiędzy komponentami w zakresie określonym przez wykorzystywane profile IHE.
- BE.RLA.4.** System loguje zdarzenia walidacji dokumentów oraz wykrytych błędów walidacji dokumentów
- BE.RLA.5.** System loguje zdarzenia otrzymania powiadomienia z systemu lokalnego z definicją grafików.
- BE.RLA.6.** System loguje zdarzenia modyfikacji zgody pacjenta.
- BE.RLA.7.** System loguje zdarzenia utworzenia nowej rezerwacji wizyty.
- BE.RLA.8.** System loguje zdarzenia modyfikacji lub anulowania dokonanej rezerwacji wizyty.
- BE.RLA.9.** System umożliwia wyszukiwanie komunikatów zdarzeń.
- BE.RLA.10.** System umożliwia przekazywanie komunikatów zdarzeń do rejestru zdarzeń Platformy P1.
- BE.RLA.11.** System umożliwia generowanie zgodnych z wymogami RODO raportów z logów zdarzeń związanych z przetwarzaniem danych osobowych.

### 3.7.2 Model przypadków użycia



Rysunek nr 3.72 Diagram przypadków użycia obszaru „Regionalne repozytorium zdarzeń na potrzeby audytu”

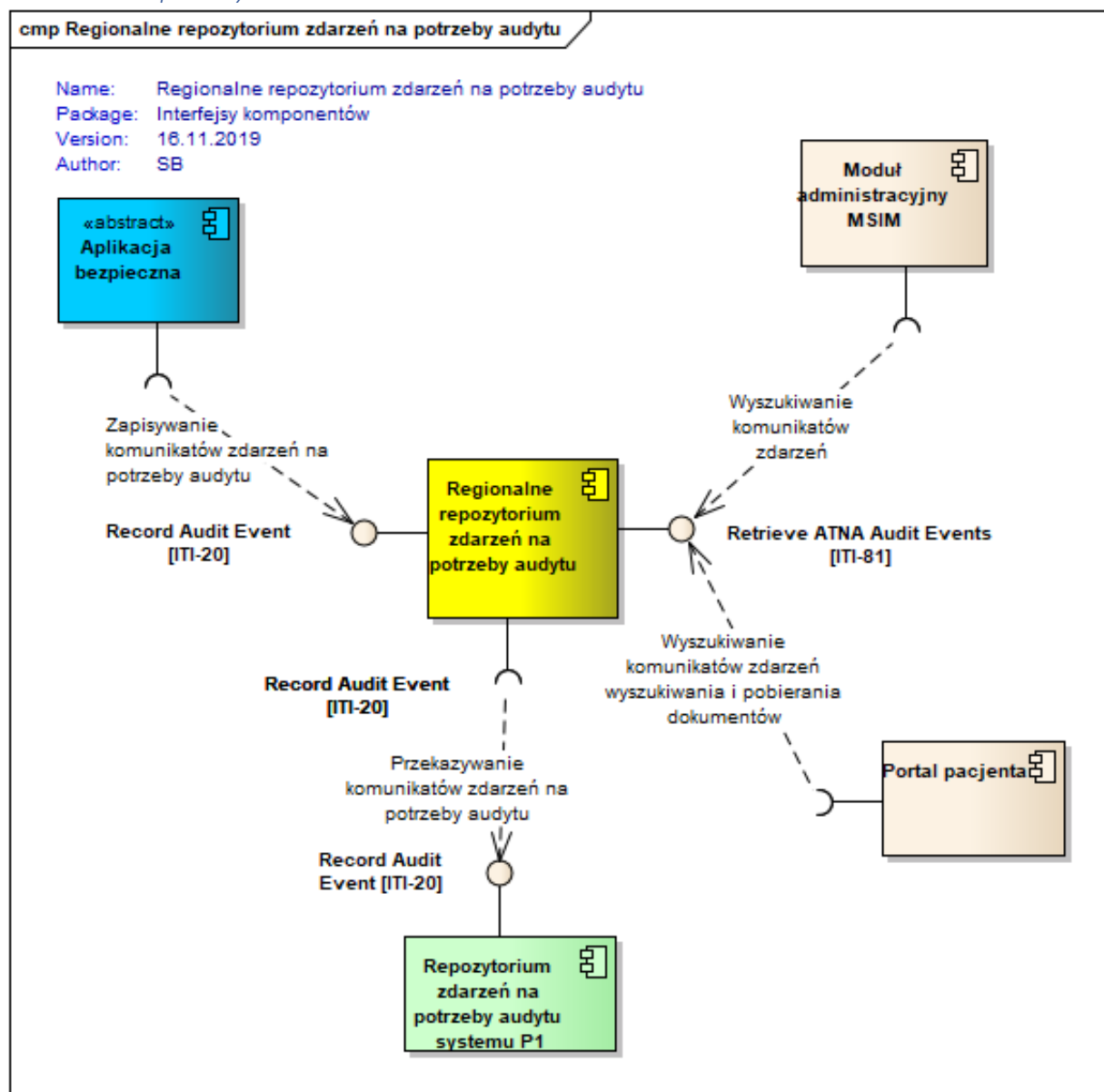
### 3.7.3 Model danych



Rysunek nr 3.73 Diagram klas obszaru „Komunikat zdarzenia dla celów audytu”

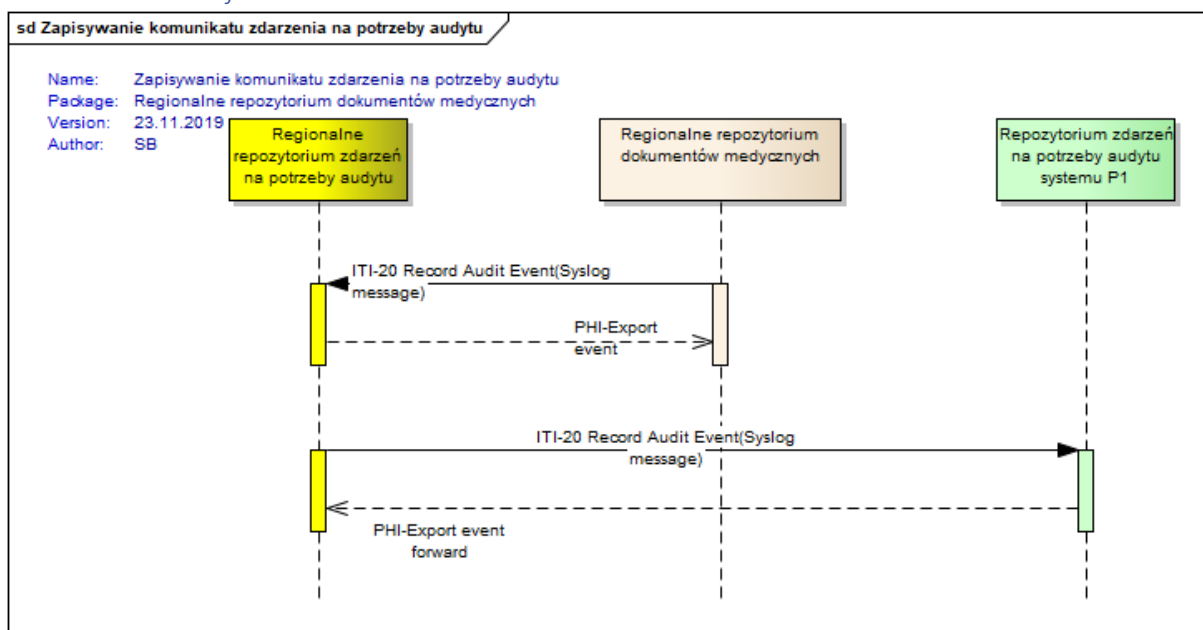
### 3.7.4 Komponenty i transakcje

#### 3.7.4.1 Komponenty

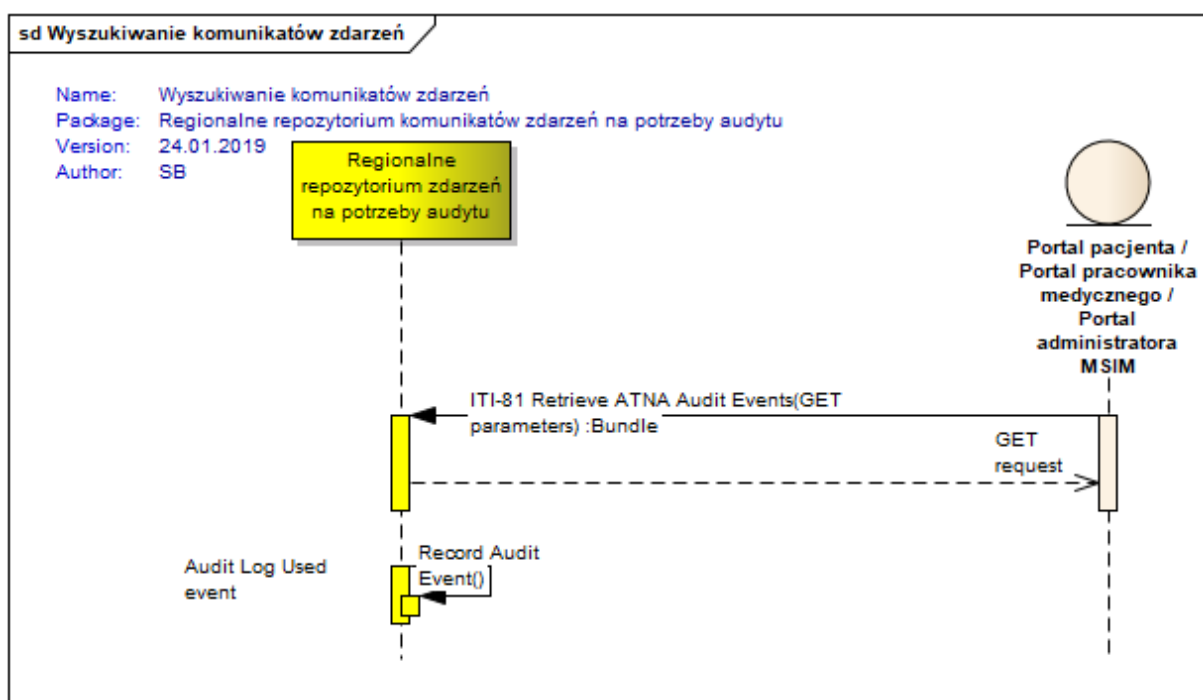


Rysunek nr 3.74 Diagram komponentów obszaru „Regionalne repozytorium zdarzeń na potrzeby audytu”

### 3.7.4.2 Transakcje



Rysunek nr 3.75 Diagram sekwencji transakcji „Zapisywanie komunikatu zdarzenia na potrzeby audytu”



Rysunek nr 3.76 Diagram sekwencji transakcji „Wyszukiwanie komunikatów zdarzeń”

## 3.8 Regionalna bramka wymiany dokumentów (bramka XCA)

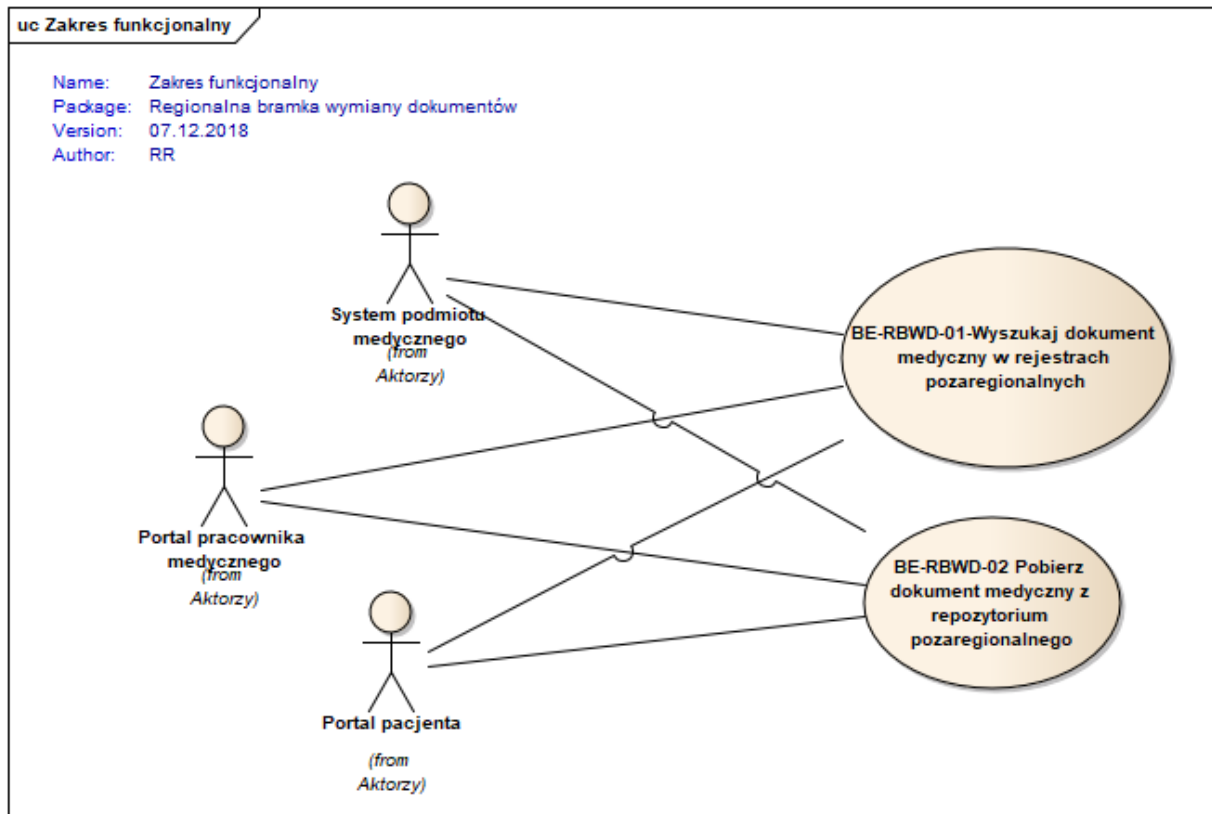
### 3.8.1 Wymagania funkcjonalne

**BE.RBWD.1.** System umożliwia wyszukiwanie dokumentów medycznych poza Platformą MSIM.

**BE.RBWD.2.** System umożliwia udostępnianie dokumentów medycznych systemom nie wchodzącym w skład Platformy MSIM.

**BE.RBWD.3.** System nie umożliwia wyszukiwania ani wymiany dokumentów poza Platformą MSIM, jeśli nie została w nim skonfigurowana żadna bramka XCA innej domeny.

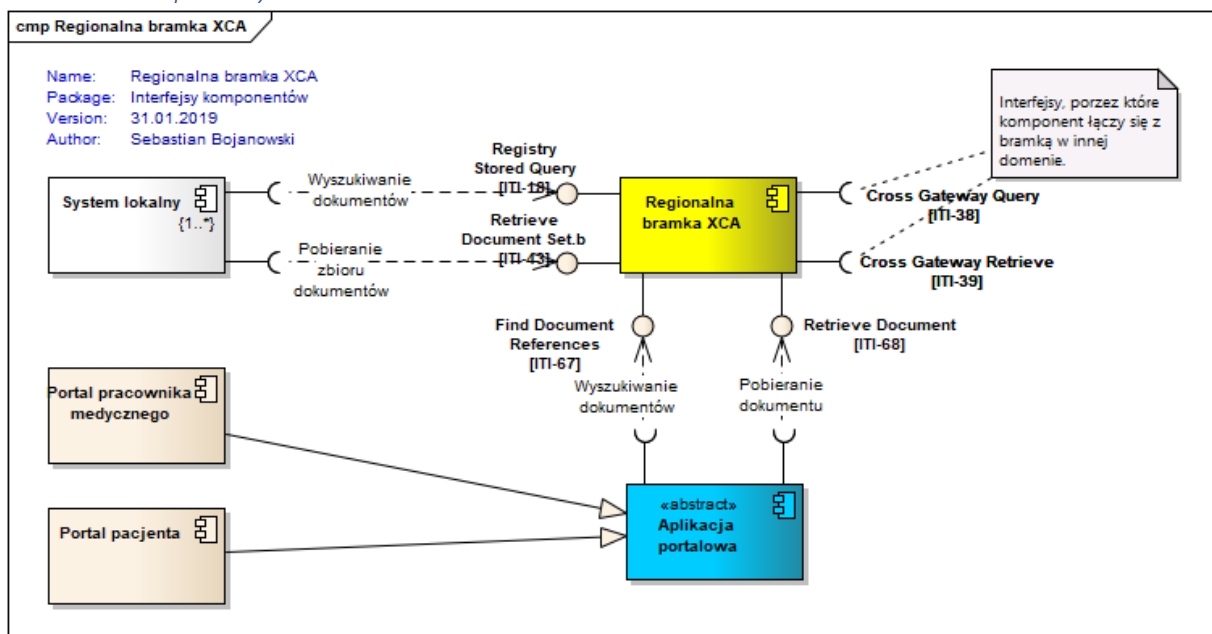
### 3.8.2 Model przypadków użycia



Rysunek nr 3.77 Diagram przypadków użycia obszaru „Regionalna bramka wymiany dokumentów”

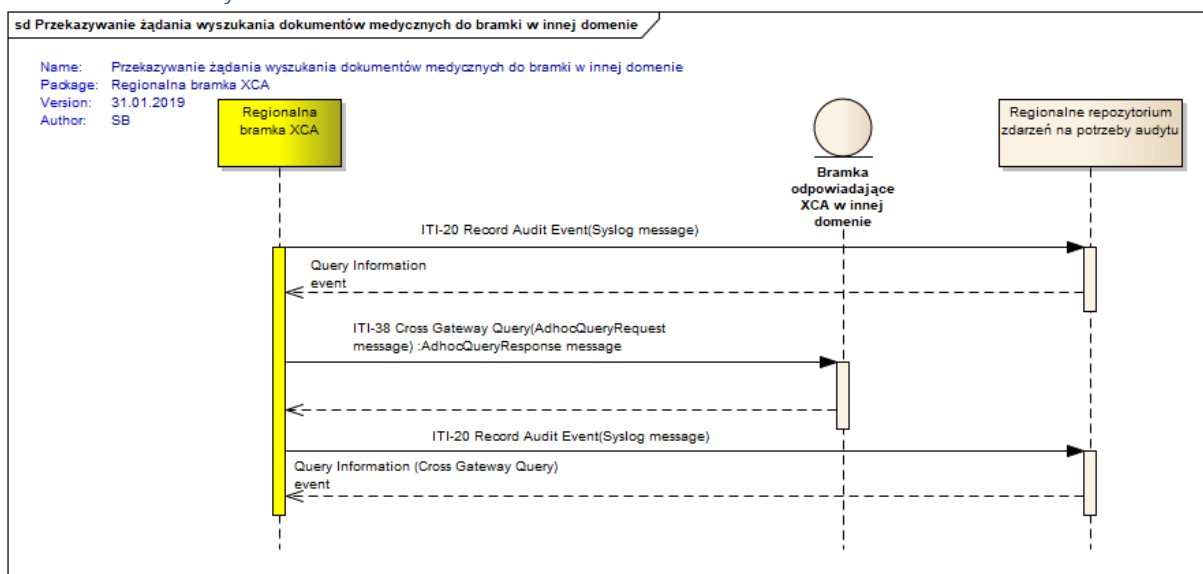
### 3.8.3 Komponenty i transakcje

#### 3.8.3.1 Komponenty

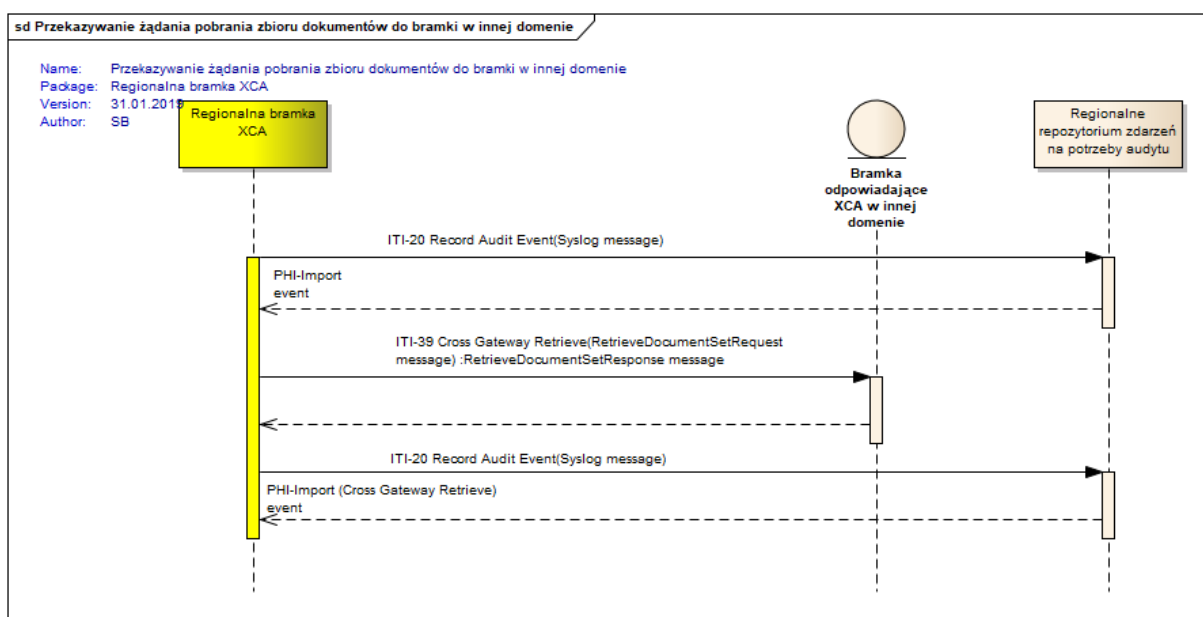


Rysunek nr 3.78 Diagram komponentów obszaru „Regionalna bramka wymiany dokumentów”

### 3.8.3.2 Transakcje



Rysunek nr 3.79 Diagram sekwencji transakcji „Przekazywanie żądania wyszukania zbioru dokumentów do bramki w innej domenie”



Rysunek nr 3.80 Diagram sekwencji transakcji „Przekazywanie żądania pobrania zbioru dokumentów do bramki w innej domenie”

## 3.9 Komponent administracyjny MSIM

### 3.9.1 Wymagania funkcjonalne

**FE.MAdm.1.** System umożliwia zarządzanie bazą systemów lokalnych i repozytoriów dokumentów.

**FE.MAdm.2.** System umożliwia zarządzanie kontami użytkowników aplikacji portalowych, przypisywanie ról i nadawanie im uprawnień.

**FE.MAdm.3.** System umożliwia zarządzanie słownikami ról i uprawnień użytkowników systemów lokalnych.

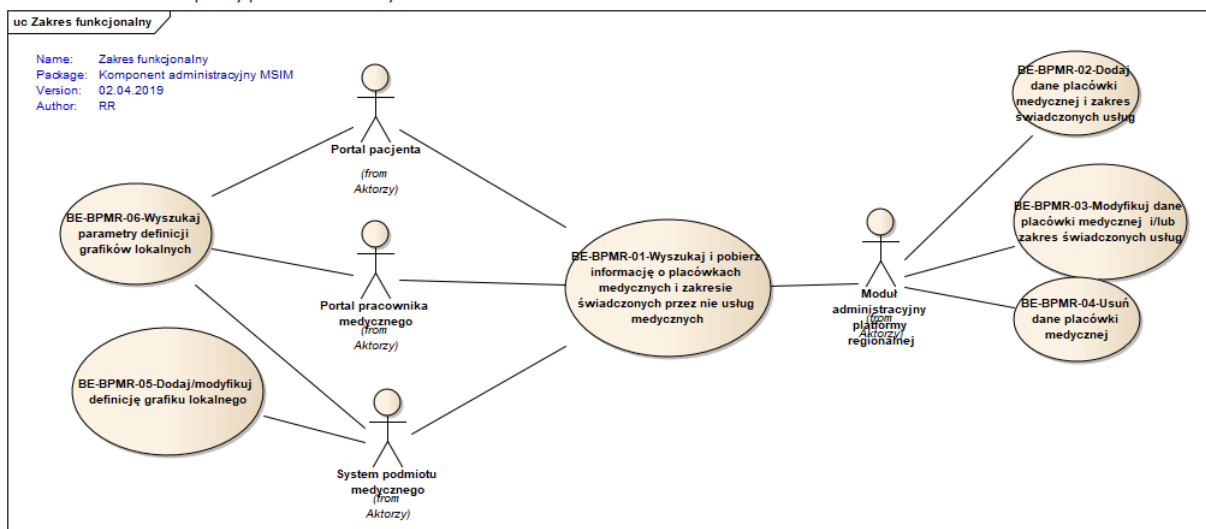
**FE.MAdm.4.** System umożliwia zarządzanie bazą pacjentów.

- FE.MAdm.5.** System umożliwia zarządzanie powiązaniem pomiędzy pacjentami, a ich przedstawicielami ustawowymi.
- FE.MAdm.6.** System umożliwia obsługę kolejki zgłoszeń problemów z danymi pacjenta.
- FE.MAdm.7.** System umożliwia kopiowanie zgłoszeń do systemu typu help desk.
- FE.MAdm.8.** System umożliwia aktualizację statusu zgłoszenia na podstawie statusu przesłanego z systemu typu help desk.
- FE.MAdm.9.** System umożliwia zarządzanie danymi o placówkach medycznych i opisach świadczonych usług.
- FE.MAdm.10.** System umożliwia wyszukiwanie i pobieranie informacji o placówkach medycznych i zakresie świadczonych przez nie usług medycznych.
- FE.MAdm.11.** System umożliwia wyszukiwanie i pobieranie informacji o pracowniku medycznym.
- FE.MAdm.12.** System umożliwia wyszukiwanie i pobieranie informacji o wolnych terminach w grafikach udostępnionych przez podmioty medyczne.
- FE.MAdm.13.** System umożliwia zarządzanie rezerwacjami wizyt dokonanymi w systemach lokalnych.
- FE.MAdm.14.** System umożliwia wyszukiwanie i pobieranie informacji o zarezerwowanych terminach wizyt.
- FE.MAdm.15.** System umożliwia wyszukiwanie dokumentów medycznych w regionalnym rejestrze dokumentów medycznych.
- FE.MAdm.16.** System umożliwia pobieranie i wyświetlanie dokumentów medycznych z repozytorium dokumentów medycznych.
- FE.MAdm.17.** System umożliwia edycję metadanych dokumentu w rejestrze regionalnym w sposób przewidziany w transakcji ITI-57, lub zbliżony.
- FE.MAdm.18.** System umożliwia usuwanie dokumentu medycznego z rejestru i repozytorium regionalnego.
- FE.MAdm.19.** System umożliwia wyszukiwanie dokumentów medycznych w pozaregionalnych rejestrach dokumentów medycznych obsługujących wymianę międzydomenową w oparciu o profil IHE XCA.
- FE.MAdm.20.** System umożliwia pobieranie i wyświetlanie dokumentów medycznych z pozaregionalnych repozytoriów dokumentów medycznych obsługujących wymianę międzydomenową w oparciu o profil IHE XCA.
- FE.MAdm.21.** System umożliwia zarządzanie słownikami terminologicznymi.
- FE.MAdm.22.** System umożliwia przeglądanie i tworzenie raportów z logów komunikatów zdarzeń na potrzeby audytu.
- FE.MAdm.23.** System realizuje funkcjonalności komponentu administracyjnego poprzez aplikację posiadającą interfejs graficzny.
- FE.MAdm.24.** System umożliwia zarządzanie zgodami pacjenta na dostęp do danych.

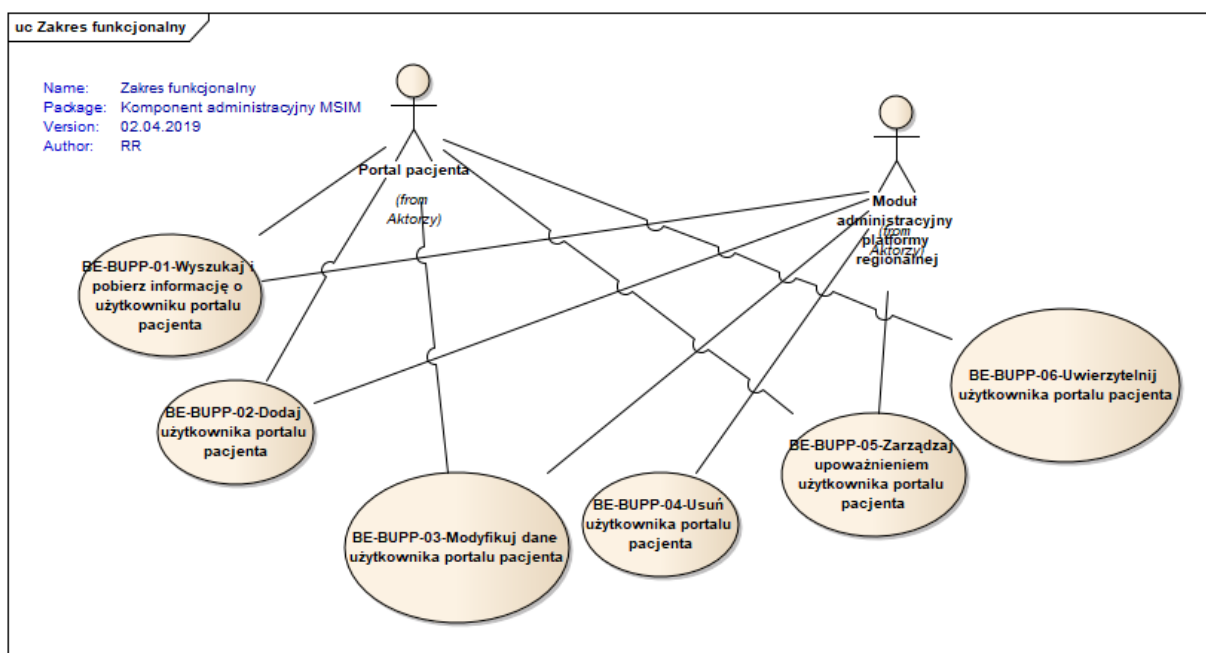


**FE.MAdm.25.** System umożliwia weryfikację zgody pacjenta na dostęp do danych.

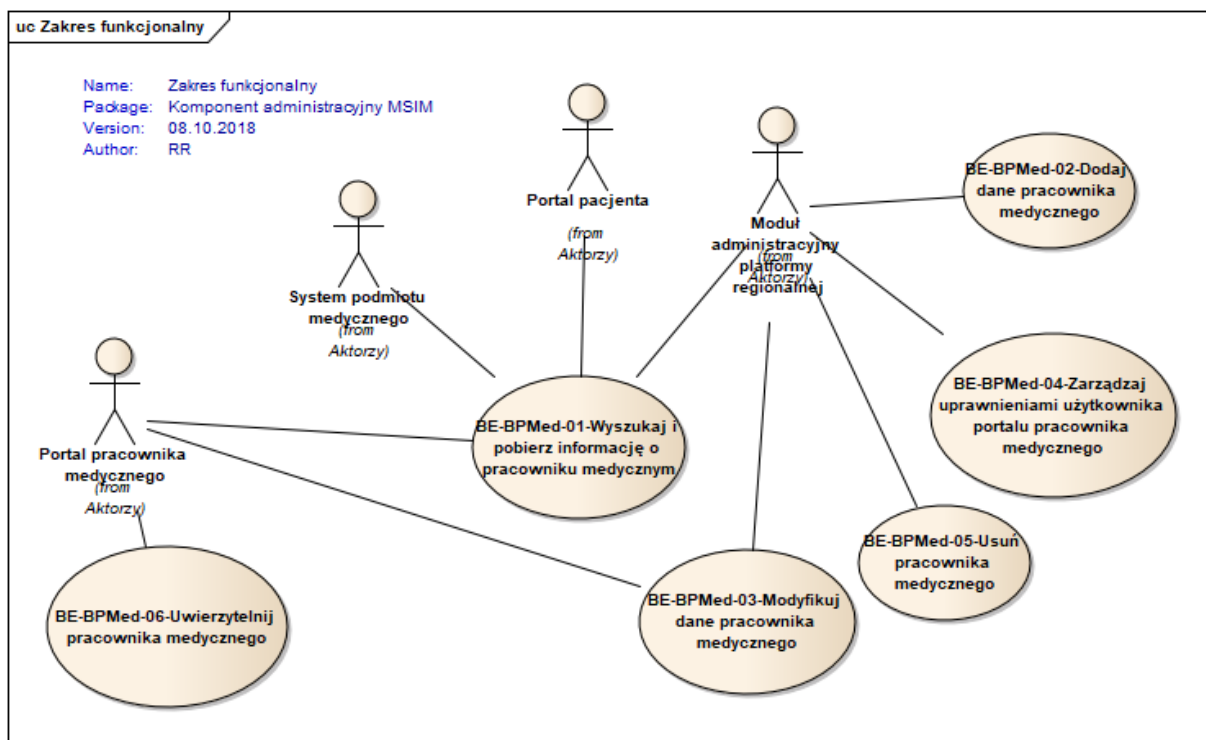
### 3.9.2 Model przypadków użycia



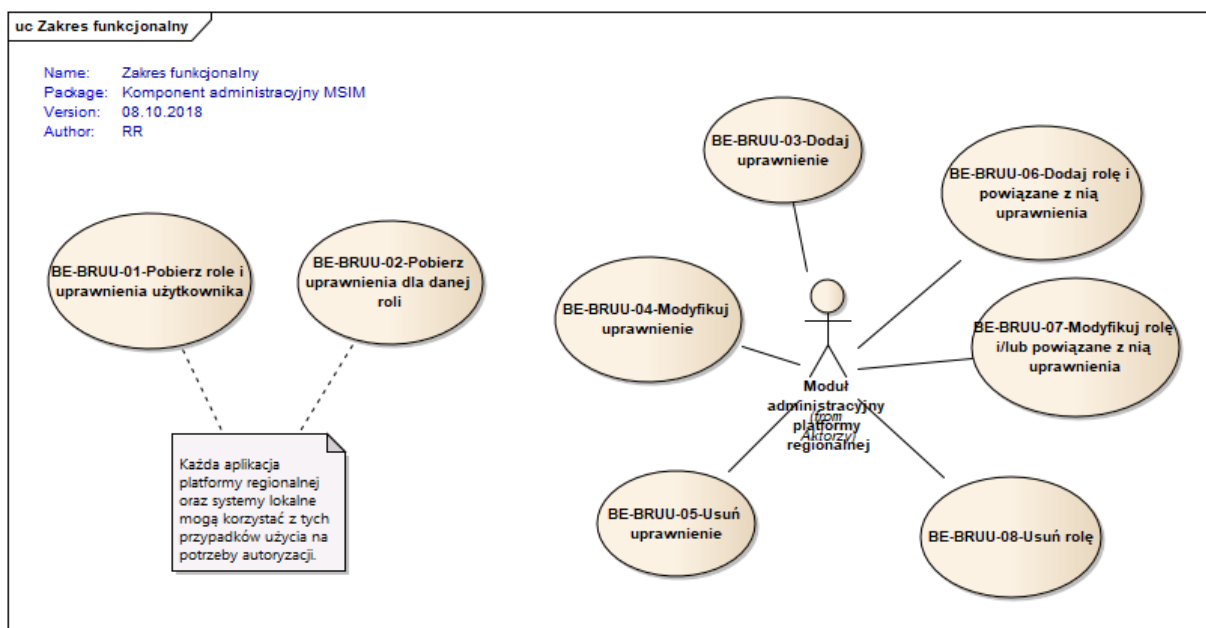
Rysunek nr 3.81 Diagram przypadków użycia obszaru „Placówki, grafiki i usługi medyczne”



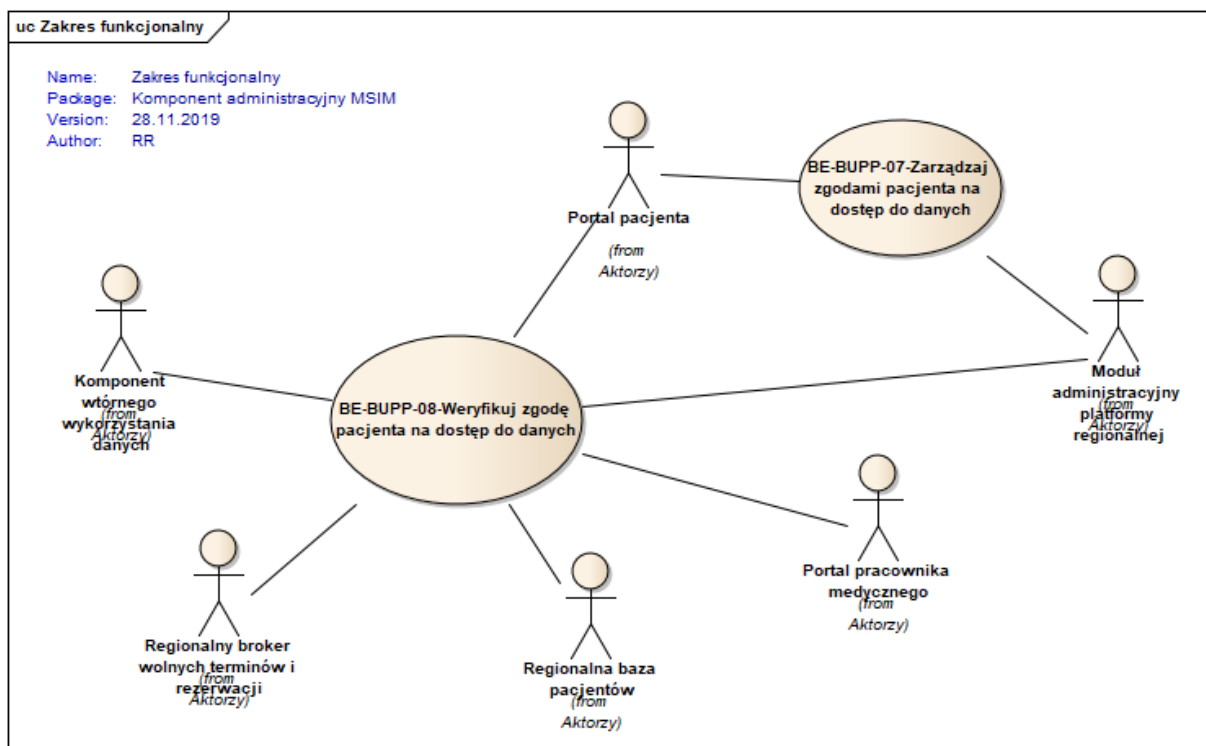
Rysunek nr 3.82 Diagram przypadków użycia obszaru „Zarządzanie użytkownikami Portalu pacjenta”



Rysunek nr 3.83 Diagram przypadków użycia obszaru „Zarządzanie użytkownikami Portalu pracownika medycznego”

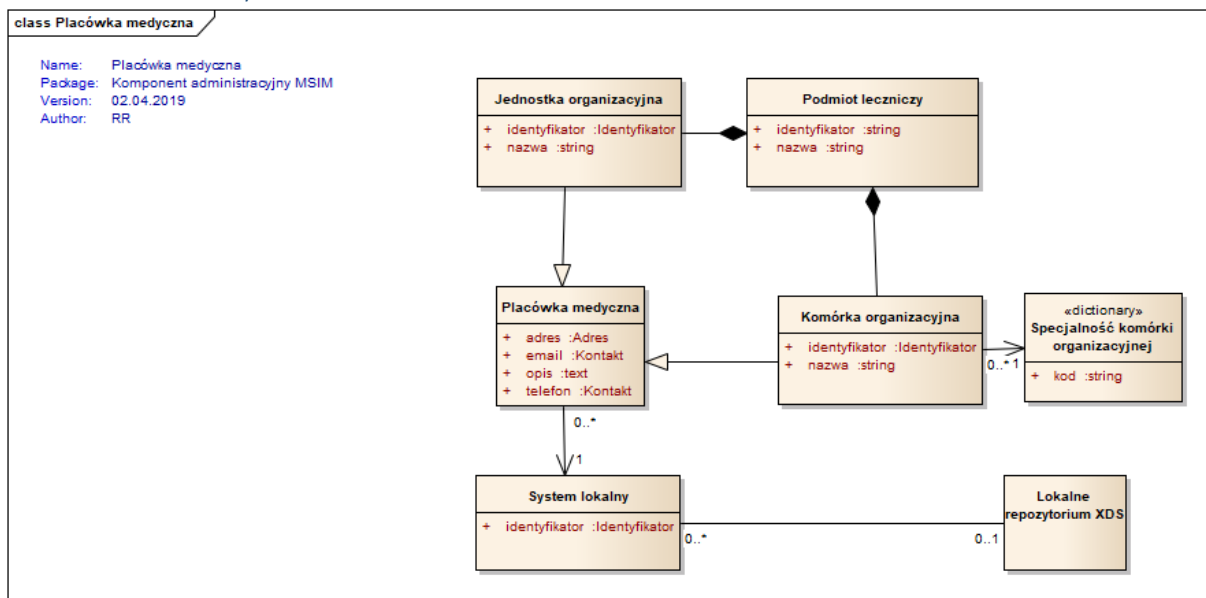


Rysunek nr 3.84 Diagram przypadków użycia obszaru „Zarządzanie rolami i uprawnieniami”

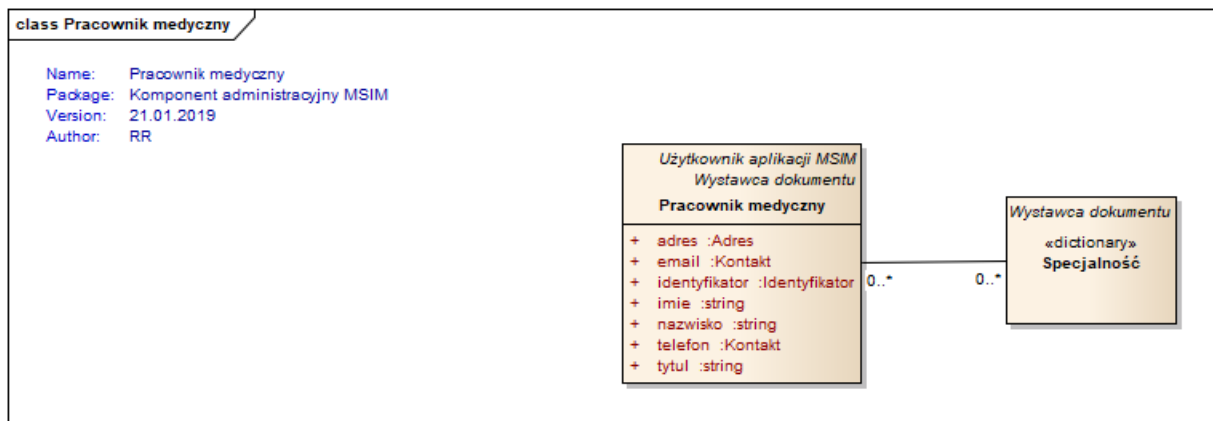


Rysunek nr 3.85 Diagram przypadków użycia obszaru "Zarządzanie zgodami pacjenta na dostęp do danych"

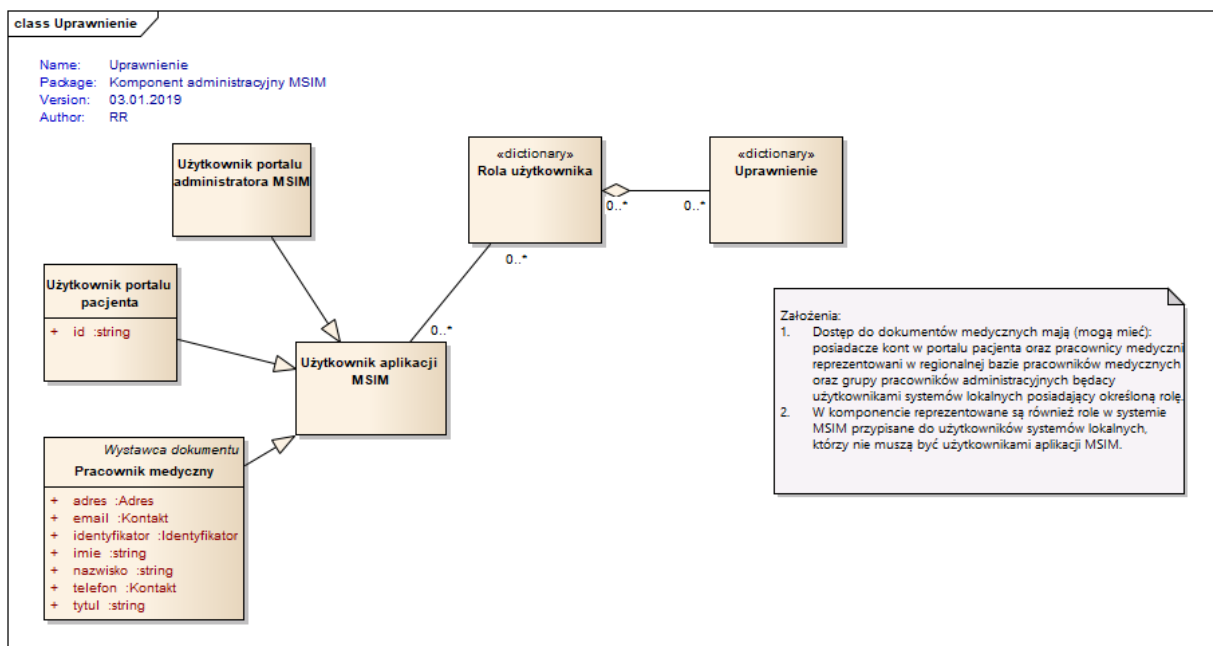
### 3.9.3 Model danych



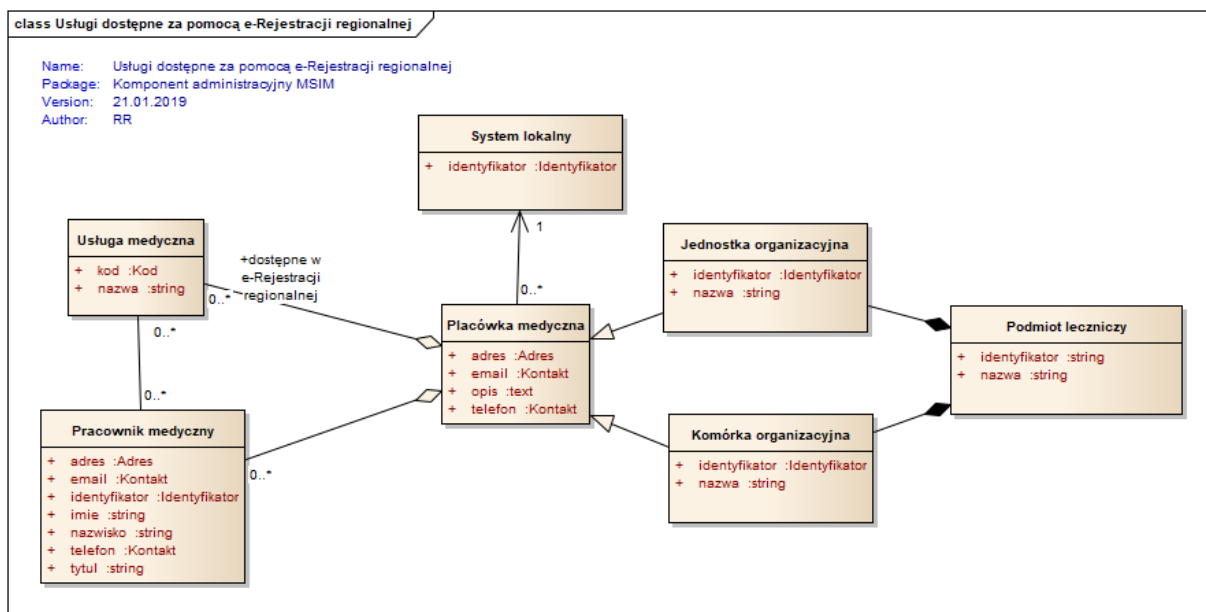
Rysunek nr 3.86 Diagram klas obszaru „Placówka medyczna”



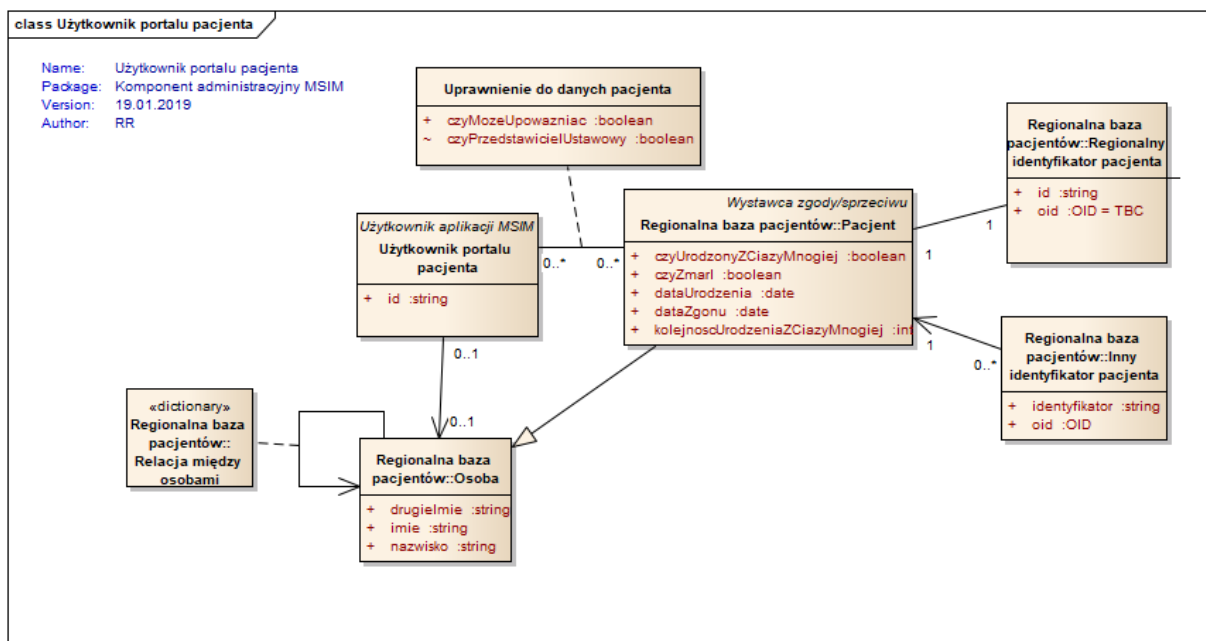
Rysunek nr 3.87 Diagram klas obszaru „Pracownik medyczny”



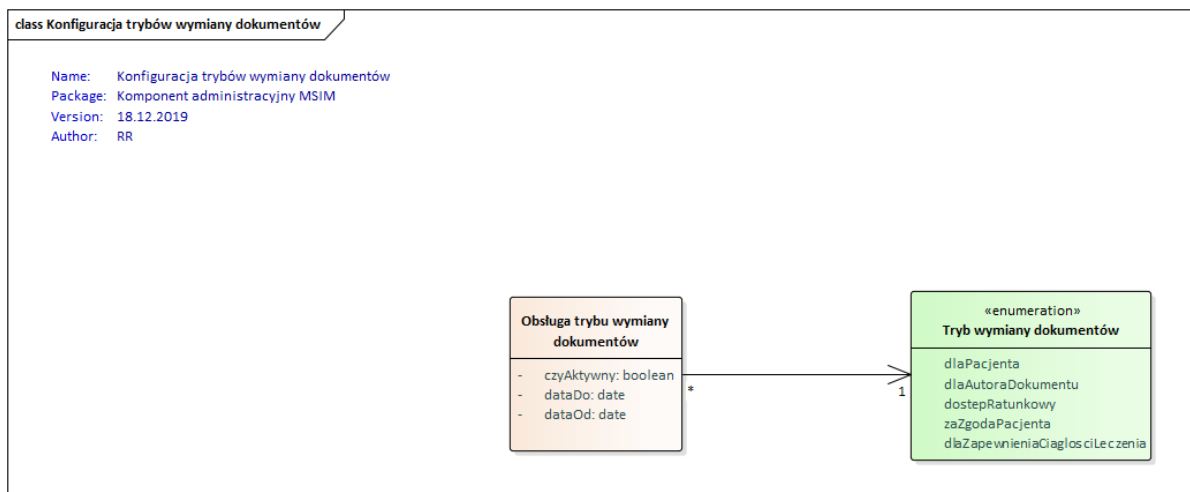
Rysunek nr 3.88 Diagram klas obszaru „Uprawnienia”



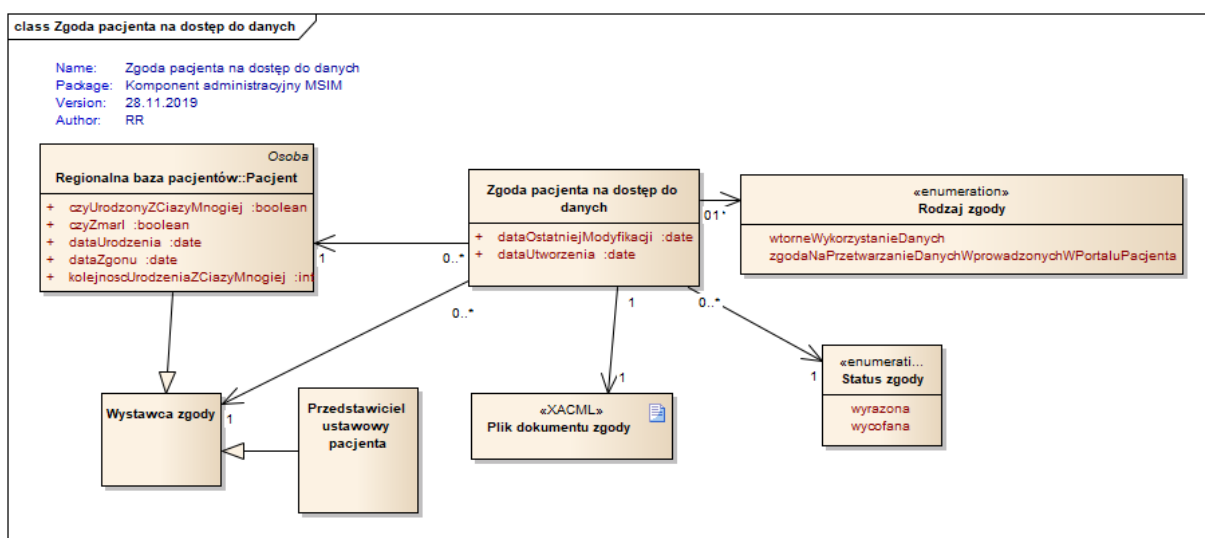
Rysunek nr 3.89 Diagram klas obszaru „Usługi dostępne za pomocą e-Rejestracji regionalnej”



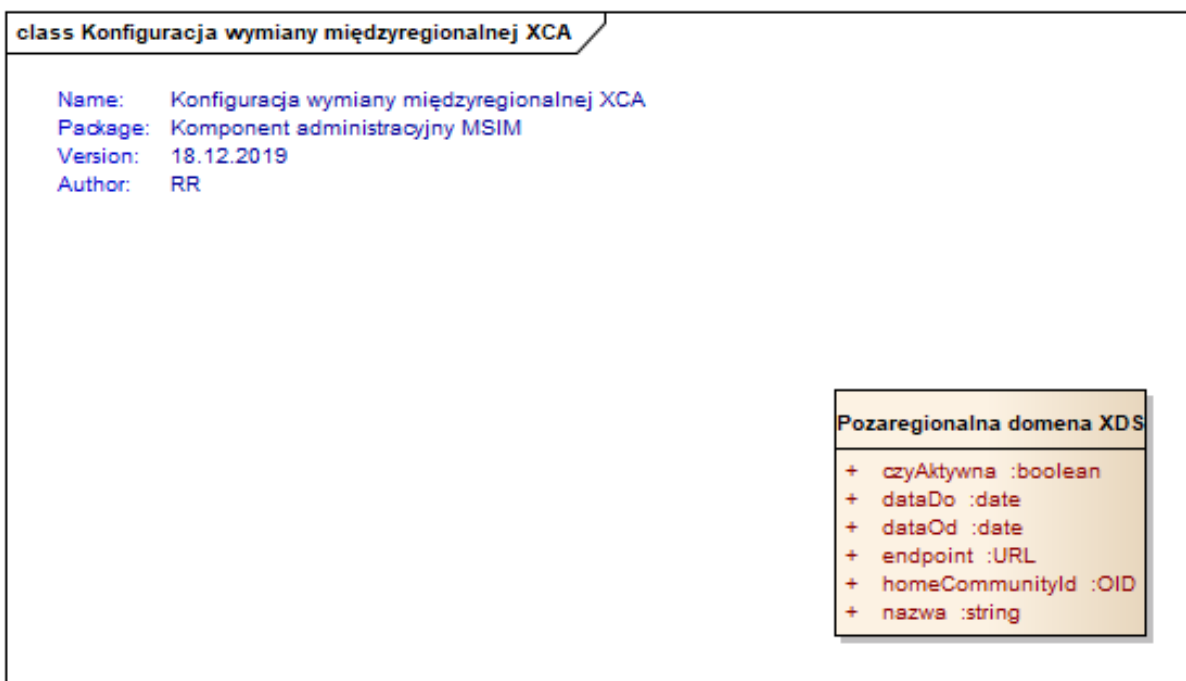
Rysunek nr 3.90 Diagram klas obszaru „Użytkownik portalu pacjenta”



Rysunek nr 3.91 Diagram klas obszaru "Konfiguracja trybów wymiany dokumentów"



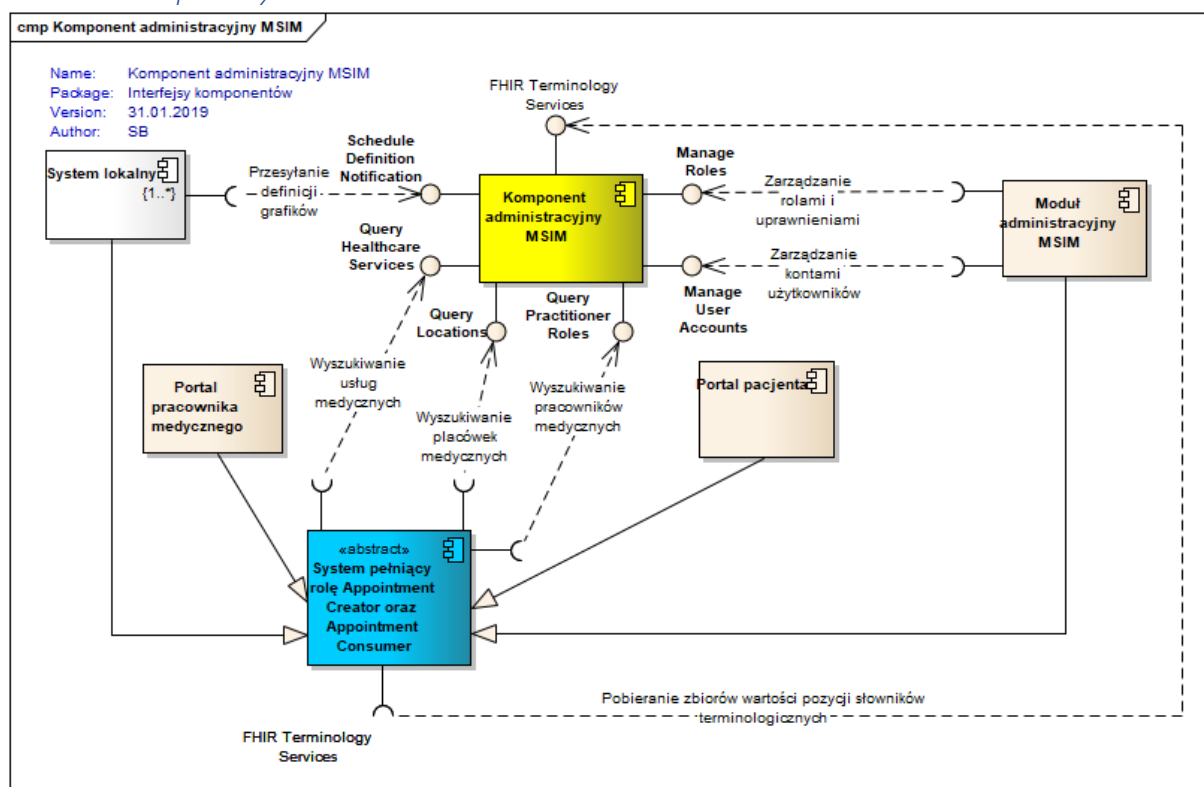
Rysunek nr 3.92 Diagram klas obszaru "Zgoda pacjenta na dostęp do danych"



Rysunek nr 3.93 Diagram klas obszaru "Konfiguracja wymiany międzyregionalnej XCA"

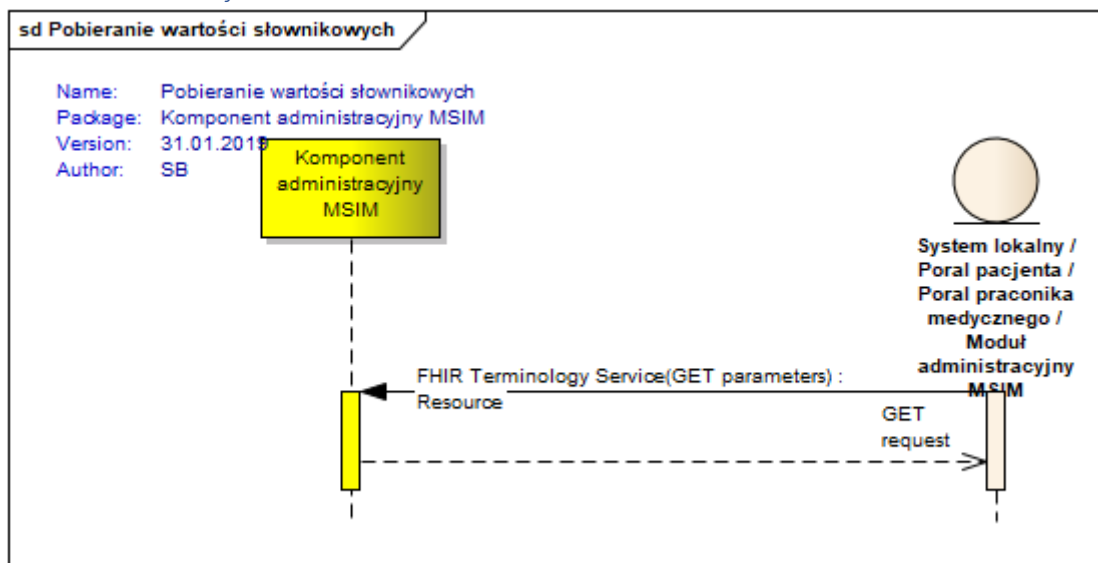
### 3.9.4 Komponenty i transakcje

#### 3.9.4.1 Komponenty

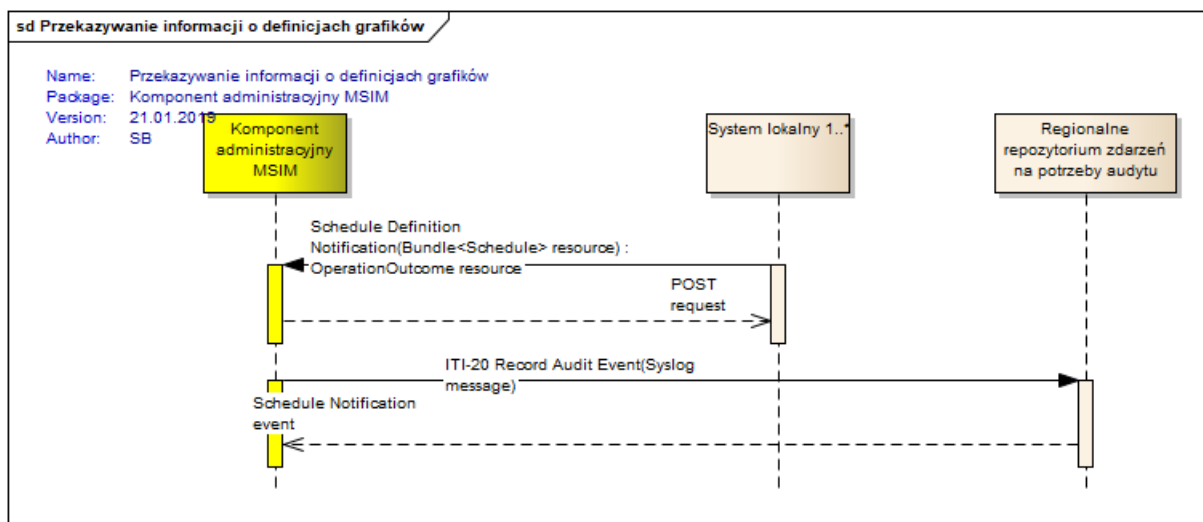


Rysunek nr 3.94 Diagram komponentów obszaru „Komponent administracyjny MSIM”

### 3.9.4.2 Transakcje

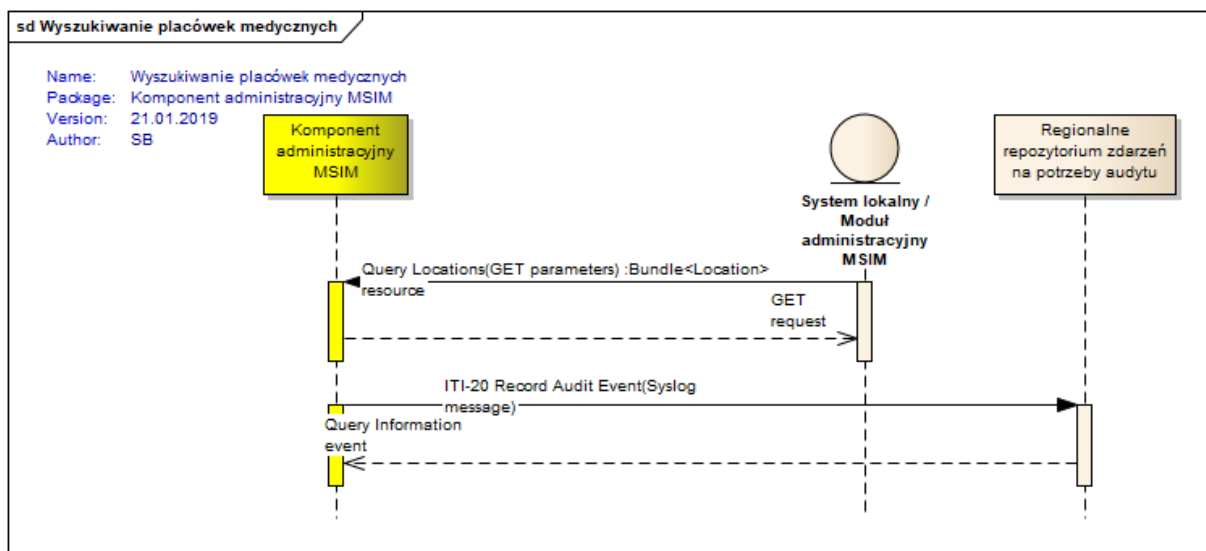


Rysunek nr 3.95 Diagram sekwencji transakcji „Pobieranie wartości słownikowych”

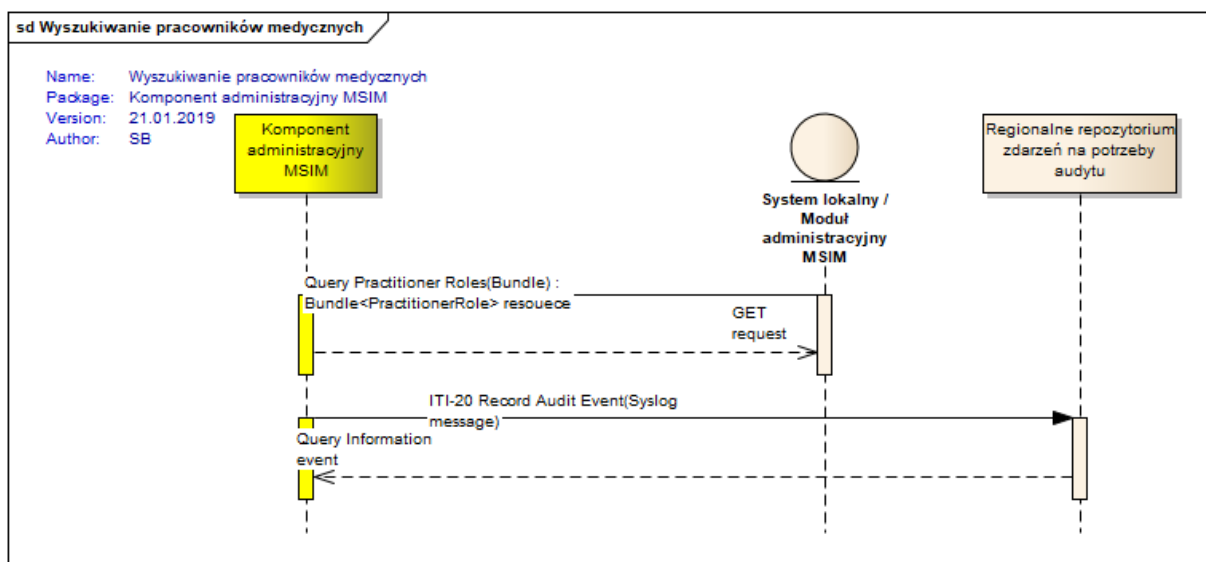


Rysunek nr 3.96 Diagram sekwencji transakcji „Przekazywanie informacji o definicjach grafików”

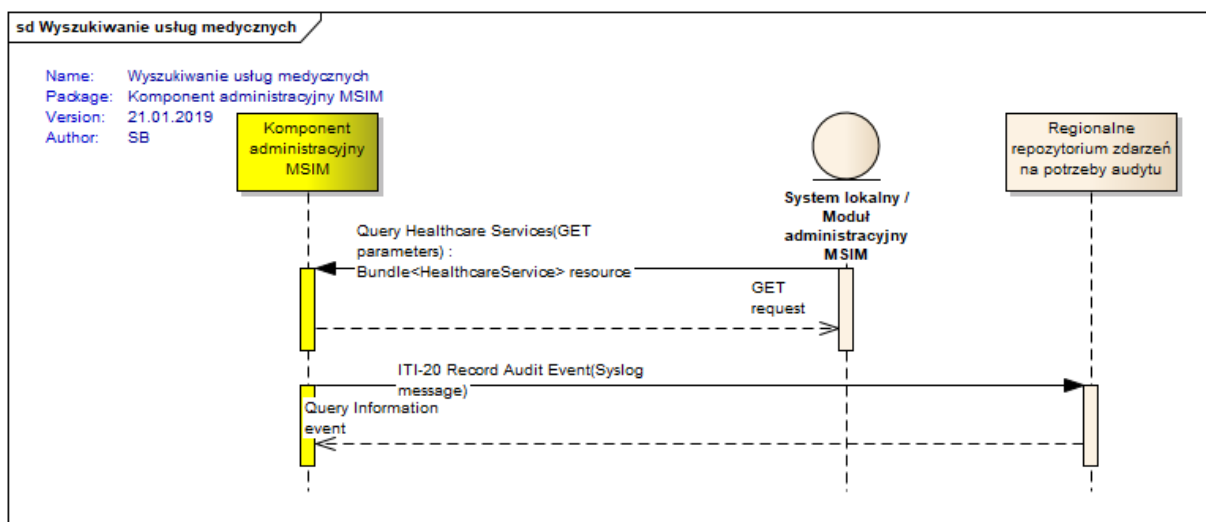




Rysunek nr 3.97 Diagram sekwencji transakcji „Wyszukiwanie placówek medycznych”



Rysunek nr 3.98 Diagram sekwencji transakcji „Wyszukiwanie pracowników medycznych”



Rysunek nr 3.99 Diagram sekwencji transakcji „Wyszukiwanie usług medycznych”

### 3.10 Wymagania нефункционаłne komponentów usługowych

#### 3.10.1 Wymagania wydajnościowe

**BE.NFun.1.** Maksymalny czas obsługi żądań w wymianie między Platformą MSIM a Partnerami nie przekracza:

1. Wyszukiwanie dokumentów medycznych: czas obsługi 2 sekundy przy obciążeniu 65 wywołań na sekundę;
2. Pobieranie dokumentów medycznych: czas obsługi 2 sekundy przy obciążeniu 65 wywołań na sekundę;
3. Przechowywanie dokumentów medycznych: czas obsługi 2 sekundy dla rozpoczęcia zapisu przy obciążeniu 135 wywołań na sekundę;
4. Przechowywanie dokumentów związanych z danymi obrazowymi: czas obsługi 2 sekundy dla rozpoczęcia przekazywania przy obciążeniu 25 wywołań na sekundę;
5. Pobieranie wolnych terminów: czas obsługi 2 sekundy przy obciążeniu 100 wywołań na sekundę;
6. Dokonywanie rezerwacji wizyt: czas obsługi 2 sekundy przy obciążeniu 100 wywołań na sekundę;
7. Zarządzanie identyfikacją pacjentów: czas obsługi 2 sekundy przy obciążeniu 150 wywołań na sekundę.

#### 3.10.2 Wymagania dotyczące skalowalności

**BE.NFun.2.** System zapewnia skalowalność pionową poprzez możliwość rozbudowy poszczególnych elementów infrastruktury techniczno-systemowej:

1. procesor, pamięć, dyski, interfejsy;
2. dodatkowe półki dyskowe, dodatkowe dyski;
3. zwiększenie zasobów dla systemu operacyjnego.

**BE.NFun.3.** System zapewnia skalowalność poziomą poprzez:

1. Możliwość rozbudowy o kolejne węzły obliczeniowe: serwery fizyczne, urządzenia sieciowe, macierze dyskowe, oprogramowanie narzędziowe, komponenty aplikacyjne;
2. Klastery wysokiej dostępności.

**BE.NFun.4.** W przypadku awarii lub aktualizacji, wyłączenie jednego z elementów nie ma wpływu na funkcjonowanie systemu.

**BE.NFun.5.** Zapewniona jest wysoka wydajność (klastery HA) – możliwość zwiększania o dodatkowe systemy, serwery aplikacyjne, bazy danych, aplikacje.

**BE.NFun.6.** Brak jest technicznych i licencyjnych ograniczeń na ilość danych gromadzonych w Systemie, zasobów infrastrukturalnych.

**BE.NFun.7.** Brak jest technicznych i licencyjnych ograniczeń na ilość procesów zaimplementowanych w Systemie.

**BE.NFun.8.** Zapewniona jest możliwość zmiany wymaganych parametrów usług i ich skalowania zgodnie z potrzebami.

**BE.NFun.9.** Zapewniona jest możliwość automatycznego skalowania mocy obliczeniowej Platformy MSIM.

#### 3.10.3 Wymagania dotyczące bezpieczeństwa i niezawodności

**BE.NFun.10.** Dostęp do danych i wymiany danych jest możliwy tylko w ramach zestawionego szyfrowanego protokołu TLS w wersji minimum 1.2.

**BE.NFun.11.** Dostęp do danych i wymiany danych może zostać zabezpieczony dodatkowo za pomocą VPN w ramach połączenia site-to-site zabezpieczonego certyfikatem i hasłem.

- BE.NFun.12.** Komunikacja między komponentami Platformy MSIM musi być szyfrowana zgodnie z założeniami profilu IHE ATNA.
- BE.NFun.13.** Wzajemne uwierzytelnienie komponentów Platformy MSIM musi być zgodne z założeniami profilu IHE ATNA.
- BE.NFun.14.** Ruch z i do Internetu musi być filtrowany i poddawany inspekcji.
- BE.NFun.15.** Wszystko co nie jest dozwolone jest zabronione.
- BE.NFun.16.** Poszczególne komponenty muszą być umieszczone w wydzielonych strefach, pomiędzy którymi ruch jest filtrowany i wykonywana jest inspekcja.
- BE.NFun.17.** Wykonywana jest cykliczna aktualizacja infrastruktury techniczno-systemowej.
- BE.NFun.18.** Wykonywany jest comiesięczny raport poprawek wydawanych przez producentów każdego ze składników infrastruktury techniczno-systemowej, wraz z rekomendacjami dotyczącymi ich wdrażania.
- BE.NFun.19.** Sesje zalogowanych użytkowników wygasają po określonym czasie.
- BE.NFun.20.** Administracja platformą w zakresie infrastruktury techniczno-systemowej jest możliwa tylko poprzez bezpieczne kanały komunikacji (VPN)
- BE.NFun.21.** Elementy infrastruktury techniczno-systemowej muszą być poddawane okresowemu tzw. utwardzaniu (ang. hardening).
- BE.NFun.22.** Utwardzanie odbywa się nie rzadziej niż co 3 miesiące.
- BE.NFun.23.** Dokumenty medyczne przechowywane w repozytorium są szyfrowane. Szyfrowanie wykonywane jest przy wykorzystaniu sprzętowych modułów kryptograficznych.
- BE.NFun.24.** Przyjmowane do repozytorium regionalnego dokumenty muszą podlegać inspekcji antywirusowej przy wykorzystaniu urządzeń typu UTM.
- BE.NFun.25.** Musi być zapewniona integralność dokumentów poprzez podpis cyfrowy przewidziany przepisami prawa w zakresie podpisywania dokumentacji medycznej.
- BE.NFun.26.** Każda interakcja komponentów MSIM między sobą oraz z systemami lokalnymi wymaga synchronizacji czasu zgodnie z założeniami profilu IHE CT.
- BE.NFun.27.** Rozliczalność zdarzeń jest zapewniona.
- BE.NFun.28.** Zdarzenia związane z przetwarzaniem danych osobowych, w szczególności pozyskaniem, wytworzeniem, dostępem (odczytem), zmianą lub usunięciem, są rejestrowane z wskazaniem osoby i okoliczności ich zaistnienia (w szczególności czasu).
- BE.NFun.29.** Zdarzenia związane z wyrażeniem lub cofnięciem zgody podmiotu danych osobowych na ich przetwarzanie, są rejestrowane z wskazaniem okoliczności ich zaistnienia (w szczególności daty i godziny, sposobu pozyskania).
- BE.NFun.30.** Dostęp do logów aplikacyjnych i systemowych zawierających dane osobowe, w szczególności adresy IP indywidualnych użytkowników, podlega rejestrowaniu z wskazaniem osoby i czasu jego zaistnienia.
- BE.NFun.31.** System musi tworzyć cyklicznie kopie zapasowe:
1. Kopie przyrostowe - minimum w cyklu dobowym
  2. Pełne kopie systemu - minimum w cyklu tygodniowym
  3. Pełny backup z kopią systemów operacyjnych - minimum w cyklu czterotygodniowym
  4. Kopie zapasowe muszą być odmiejszczawiane
- BE.NFun.32.** W momencie przystąpienia do realizacji prac wykonawczych, procedura i częstotliwość wykonywania kopii zapasowych może zostać ustalona przez Zamawiającego na innym poziomie.
- BE.NFun.33.** Przywrócenie usług do punktu w czasie sprzed awarii (RPO) wynosi 1h.
- BE.NFun.34.** Dostępność usług Platformy MSIM wynosi 99,0% w skali miesiąca.
- BE.NFun.35.** System umożliwia ciągły dostęp do danych medycznych i do dokumentów medycznych gromadzonych w Systemie co najmniej z ostatnich pięciu lat. W tym czasie dane

i dokumenty nie są archiwizowane ani poddawane działaniom, które zwiększałyby czas dostępu do nich.

**BE.NFun.36.** Logi mogą być poddawane archiwizacji.

**BE.NFun.37.** System przechowuje dane medyczne i dokumenty medyczne przez okres wymagany obowiązującymi przepisami prawa dla każdej z kategorii danych medycznych i dokumentów medycznych.

**BE.NFun.38.** System musi być zgodny z politykami bezpieczeństwa opracowywanymi w toku projektu, w tym polityką bezpieczeństwa administratora danych Platformy MSIM.

**BE.NFun.39.** System musi być zgodny z polityką kopii zapasowych Zamawiającego:

1. Testy odtworzenia wybranych elementów nie rzadziej niż raz w miesiącu;
2. Testy odtworzenia całości systemu nie rzadziej niż raz na trzy miesiące;
3. Testy podatności systemu wraz z rekomendacjami nie rzadziej niż raz w miesiącu oraz po każdej aktualizacji.

**BE.NFun.40.** System musi uniemożliwiać nieautoryzowany dostęp.

**BE.NFun.41.** Uwierzytelnienie jest wykonywane przy wykorzystaniu zaufanych dostawców tożsamości m.in. KWIE (Krajowy Węzeł Identyfikacji Elektronicznej).

**BE.NFun.42.** Uwierzytelnienie systemów pomiędzy Platformą regionalną a podmiotami medycznymi jest wykonywane przy wykorzystaniu wzajemnego uwierzytelniania (Mutual Authentication). Platforma regionalna jest dostawcą tożsamości.

**BE.NFun.43.** Interfejsy oparte o standard HL7 FHIR muszą wykorzystywać OAuth w wersji co najmniej 2.0 dla uwierzytelniania użytkowników.

**BE.NFun.44.** Dostęp do danych musi być realizowany poprzez prawa dostępu dla poszczególnych użytkowników i być rozliczalny.

**BE.NFun.45.** Uprawnienia dla użytkowników są nadawane wg zasady najmniejszego uprzywilejowania.

**BE.NFun.46.** Uprawnienia dla użytkowników są pogrupowane w role systemowe.

**BE.NFun.47.** Poszczególne komponenty systemu muszą działać niezależnie na odseparowanych węzłach. Wyłączenie jednego z komponentów z klastra wysokiej dostępności nie będzie miało wpływu na pozostałe komponenty.

**BE.NFun.48.** System musi obsługiwać awarie poszczególnych węzłów danego komponentu. Ruch musi być przekierowany na inny dostępny węzeł.

**BE.NFun.49.** Poszczególne komponenty systemu muszą być przynajmniej zdublowane w celu zapewnienia ciągłości działania.

**BE.NFun.50.** Musi być zapewniona wysoka dostępność systemu, w tym zdublowanie komponentów systemu oraz infrastruktury techniczno-systemowej (redundantne elementy wyposażenia sprzętu i zasilania, praca urządzeń w klastrze)

**BE.NFun.51.** Musi być zapewnione monitorowanie i raportowanie zasobów infrastruktury techniczno-systemowej oraz komponentów i realizowanych procesów biznesowych.

**BE.NFun.52.** System musi być wykonany w architekturze wielowarstwowej oddzielającej dane, logikę biznesową i interfejs użytkownika oraz zapewniając odpowiednie role i uprawnienia dla użytkowników.

**BE.NFun.53.** Przechowywanie i obsługa danych kryptograficznych wykonywana jest przy wykorzystaniu urządzeń HSM.

**BE.NFun.54.** Kontroli poprawności wprowadzanych danych jest realizowana przy pomocy formularzy elektronicznych.

**BE.NFun.55.** Weryfikacja poprawności wymienianych dokumentów elektronicznych odbywa się na podstawie schematów XSD i reguł schematronowych oraz weryfikacja zgodności metadanych XDS z danymi nagłówka CDA.

- BE.NFun.56.** Logowanie wszystkich zdarzeń w systemie, w tym błędów, jest zgodne z profilem IHE ATNA.
- BE.NFun.57.** Korelacja zdarzeń, w tym błędów, jest wykonywana przy wykorzystaniu rozwiązania SIEM.
- BE.NFun.58.** Komunikaty żądania (message request) i komunikaty odpowiedzi (message response) dla transakcji IHE muszą być walidowane przez odbiorcę na zgodność ze specyfikacjami IHE.
- BE.NFun.59.** Komunikaty realizowane w technologii Web Services muszą wykorzystywać SOAP w wersji 1.2.
- BE.NFun.60.** Interfejsy realizowane w technologii Web Services muszą wykorzystywać WS Security na potrzeby przekazywania informacji o uprawnieniach użytkownika zgodnie z profilem IHE XUA.
- BE.NFun.61.** Interfejsy realizowane w technologii Web Services dla transakcji IHE. muszą być zgodne z sekcją ITI TF-2x: Appendix V: Web Services for IHE Transactions
- BE.NFun.62.** System musi umożliwiać separację danych medycznych i dokumentów medycznych od danych niemiedycznych poprzez ich pseudonimizację.

## 4 Infrastruktura techniczno-systemowa

### 4.1 Wymagania ogólne

Dostarczona przez Wykonawcę infrastruktura techniczno-systemowa musi zapewnić uruchomienie i utrzymanie przez Wykonawcę następujących środowisk:

- Środowisko produkcyjne – środowisko, na którym uruchomiona zostanie produkcyjnie Platforma MSIM;
- Środowisko testów akceptacyjnych – środowisko, na którym prowadzone będą testy oprogramowania Platformy MSIM, w ramach tego środowiska Wykonawca musi zapewnić komplet narzędzi służących do realizacji zakładanych testów, w tym także narzędzia do kompilacji kodu źródłowego;
- Środowisko szkoleniowe – środowisko, na którym prowadzone będą szkolenia użytkowników Platformy MSIM;
- Środowisko ewaluacyjne – środowisko, na którym uruchomione zostanie oprogramowanie umożliwiające testowanie podmiotom zewnętrznym prawidłowości implementacji standardów i profili interoperacyjności wykorzystywanych w ramach Platformy MSIM;
- Środowisko integracyjne - środowisko, na którym uruchomione zostanie oprogramowanie umożliwiające testowanie podmiotom zewnętrznym prawidłowości komunikacji ich oprogramowania z Platformą MSIM w oparciu o interfejsy udostępniane na Platformie MSIM w warunkach bliskich wdrożeniu produkcyjnemu.

#### 4.1.1 Kolokacja

Poniżej przedstawione zostały wymagania związane z realizacją kolokacji dla Platformy MSIM w podziale na obszary.

##### **ITS.WO.1.** Lokalizacja

1. Teren, na którym zlokalizowane jest CPD (wszystkie budynki i instalacje) musi być ogrodzony z zapewnieniem bezpiecznej strefy buforowej.
2. CPD (Centrum przetwarzania danych) musi być zaprojektowane i zbudowane z właściwym przeznaczeniem (serwerownia, centrum przetwarzania danych, ośrodek przetwarzania danych, data center).
3. Na ogrodzonym Terenie, na którym zlokalizowane jest CPD, mogą znajdować się tylko budynki i instalacje bezpośrednio związane z działalnością CPD.

4. CPD musi posiadać niezależne drogi dojazdowe umożliwiające dojazd służb technicznych.

**ITS.WO.2.** Architektura i konstrukcja

1. CPD musi być położone na Terenie niezagrożonym powodzią lub podtopieniem.
2. CPD musi zapewnić dostępność dedykowanych pomieszczeń serwisowych wraz z wyposażeniem stanowisk pracy (urządzenia pomiarowe i testowe, stoły elektrostatyczne, zasilanie 230V).
3. Pomieszczenia Serwerowe i Techniczne muszą być pozbawione zbędnych instalacji stanowiących źródła zagrożeń, brak instalacji wodno-kanalizacyjnych, grzewczych).

**ITS.WO.3.** Zasilanie

1. Wymagane jest posiadanie 2 niezależnych torów zasilających NN w każdym Pomieszczeniu Serwerowym. Wszystkie tory zasilające muszą gwarantować taką samą moc maksymalną zasilania.
2. Zasilanie do Szaf musi być prowadzone pod podłogą techniczną.
3. Każdy tor zasilający w Pomieszczeniu Serwerowym musi posiadać 3 fazy.
4. Minimalna moc jednego PDU (Power Distribution Unit) wynosi 16 kW.
5. W każdej Szafie muszą być zainstalowane minimum 2 PDU (Power Distribution Unit).
6. Poziom redundancji urządzeń UPS dla każdego toru zasilającego NN z osobna wynosi 2N.
7. Zapewniony jest oddzielny, dedykowany, redundantny system zasilania gwarantowanego dla zasilania szaf klimatyzacji precyzyjnej.
8. Czas pracy każdego agregatu prądotwórczego w CPD gwarantuje zasilanie urządzeń w Pomieszczeniu Serwerowym na okres nie krótszy niż 72 godziny.

**ITS.WO.4.** System przeciwpożarowy i wentylacja

1. Pomieszczenia Serwerowe i Techniczne muszą posiadać system gaszenia gazem bezpiecznym dla sprzętu komputerowego i ludzi w postaci stałego urządzenia gaśniczego (SUG).
2. Odporność ogniowa ścian serwerowni i pomieszczenia technicznego musi wynosić min. 90 min
3. Drzwi wejściowe do serwerowni i pomieszczenia technicznego o odporności pożarowej min. EI 90
4. Pomieszczenia Serwerowe i Techniczne muszą być wyposażone w system wczesnej detekcji dymu

**ITS.WO.5.** System klimatyzacji precyzyjnej

1. Redundantny układ produkcji i dystrybucji chłodu do Pomieszczeń Serwerowych wynosi N+1.

**ITS.WO.6.** Certyfikaty

1. Dostawca Kolokacji musi posiadać certyfikację obszarów usług świadczonych na rzecz Umowy na zgodność z normami PN:EN ISO 9001:2015-10 i PN:EN ISO 27001:2014-12 lub równoważnymi.

**ITS.WO.7.** Systemy bezpieczeństwa

1. Kontrola wejścia do CPD musi odbywać się co najmniej w oparciu o dokument tożsamości.
2. Kontrola dostępu do Pomieszczeń Serwerowych i Technicznych realizowana jest w oparciu o system RFID oraz kody dostępu.
3. CPD musi posiadać System Sygnalizacji Włamania i Napadu.
4. CPD musi posiadać system telewizji przemysłowej (CCTV).
5. Dostęp całodobowy przez siedem dni w tygodniu.

**ITS.WO.8.** Sieć

1. Ilość niezależnych przyłączy światłowodowych traktowana jako niezależny rurarz/kanalizacja teletechniczna dla CPD musi wynosić co najmniej 2.
2. Każda z tras światłowodowych musi wychodzić z CPD w różnych kierunkach z wykorzystaniem niezależnej kanalizacji teletechnicznej.
3. Co najmniej 3 operatorów posiada w CPD węzeł dostępowy do sieci Internet.
4. CPD powinno być wyposażone w redundantny węzeł dostępu do sieci Internet z wykorzystaniem routerów, switchy, firewall, Intrusion Prevention System.
5. CPD musi posiadać własną publiczną adresację IP.

#### **ITS.WO.9.** Szafy

1. Kontrola dostępu do strefy realizowana w oparciu o system RFID oraz kody dostępu.
2. CPD musi zapewnić monitoring i logowanie otwarć drzwi w każdej szafie.

#### **ITS.WO.10.** BMS

1. CPD musi być wyposażone w dedykowany system Building Management System BMS.

### 4.1.2 Konfiguracja ITS

Poniższe wymagania dotyczą ogólnego sposobu realizacji warstwy ITS dla Platformy MSIM. Szczegółowe wymagania dla poszczególnych komponentów ITS zostały przedstawione w dalszej części tego rozdziału.

#### **ITS.WO.11.** Zapory ogniowe

1. Elementy infrastruktury techniczno-systemowej muszą być umieszczone w oddzielnych podsieciach.
2. Pomiędzy strefami bezpieczeństwa ruch jest limitowany i podlega inspekcji na zasadzie, że wszystko co nie jest dozwolone jest zabronione.
3. Dla każdego środowiska dedykowane muszą zostać uruchomione instancje firewall.

#### **ITS.WO.12.** Równoważnik obciążeń

1. Ruch kierowany na dane komponenty musi być równoważony.
2. Każdy balansowany komponent musi mieć dedykowany monitor weryfikujący jego status.
3. Ruch TLS musi być terminowany.

#### **ITS.WO.13.** Sieć LAN

1. Przełączniki muszą pracować w stosie.
2. Dla każdego redundantnych połączeń fizycznych musi być włączona agregacja portów na dwóch różnych przełączników LAN.
3. Agregacja portów musi być skonfigurowana z określonym protokołem wykorzystywanym przez urządzenia klienckie.
4. Konfiguracja VLAN zgodnie z wymogami na strefy sieciowe

#### **ITS.WO.14.** Sieć SAN

1. Dostęp do zasobów sieci SAN musi odbywać się na podstawie stref bezpieczeństwa (zoning).
2. Dla każdej pary target-inicjator musi być stworzona oddzielna strefa (zoning).
3. Maskowanie LUN - macierze dyskowe muszą udostępniać określone zasoby tylko dla określonych węzłów.
4. Przełączniki SAN muszą być połączone ze sobą redundantnymi linkami.

#### **ITS.WO.15.** Kopie bezpieczeństwa

1. Kopie zapasowe muszą być składowane na dwóch różnych nośnikach przechowywania danych.
2. Kopie zapasowe muszą być poddawane deduplikacji.
3. Kopie zapasowe muszą być poddawane kompresji.

4. Tygodniowe pełne kopie zapasowe muszą być odmiejszczane.
5. Kopie zapasowe muszą być szyfrowane.
6. Musi być zdefiniowana rola Administratora Kopii bezpieczeństwa. Administrator Kopii bezpieczeństwa odpowiedzialny za sprawdzanie czy kopie bezpieczeństwa są robione właściwie i czy spełniają swoje zadanie.
7. System kopii zapasowych musi wysyłać codzienne raporty ze statusem wykonanych kopii zapasowych.
8. Kopie zapasowe wybranych komponentów muszą być testowane co najmniej raz na 3 miesiące.
9. Plan kopii zapasowych musi zawierać minimum harmonogram tworzenia kopii zapasowych, zasoby jakie podlegają kopii zapasowych, okres przechowywania, typ kopii zapasowych, miejsce składowania. Plan kopii zapasowych musi być zgodny z Polityką Bezpieczeństwa Zamawiającego.

**ITS.WO.16.** Komponenty – platforma

1. Komponenty Platformy MSIM muszą pracować w odizolowanym od siebie środowisku uruchomieniowym.
2. Wykonawca dostarczy platformę umożliwiającą tworzenie, dostarczanie i uruchamianie aplikacji w zvirtualizowanym środowisku.
3. Platforma ma zapewnić możliwość wykorzystania systemu operacyjnego hosta do uruchomienia wielu instancji aplikacji gości.
4. Kod aplikacji z niezbędnym systemem plików systemu operacyjnego musi być dostarczany w jednym obrazie o ustandaryzowanej formie.
5. Zastosowane podejście projektowania rozwiązania musi zapewnić możliwość zbudowania środowiska dla wybranej aplikacji i wykorzystanie jego jako szablonu do tworzenia nowych instancji aplikacji.
6. Rozwiązanie musi zapewnić możliwość uruchomienia przygotowanych obrazów w różnych wersjach bazujących na poprzednich wersjach.
7. Rozwiązanie musi zapewnić możliwość automatyzacji budowania i dystrybuowania wersji obrazów komponentów.
8. Przyjęta architektura musi zapewnić scentralizowane zarządzanie umożliwiające uruchamianie dodatkowych węzłów ad-hoc.
9. Rozwiązanie musi zapewnić przechowywanie w centralnym repozytorium obrazów komponentów.
10. Architektura aplikacji musi być oparta o mikroserwisy, gdzie całość aplikacji tworzą luźno ze sobą połączone, współpracujące serwisy odpowiadające za fragment funkcji biznesowych całego systemu.

**ITS.WO.17.** Komponenty – orkiestracja

1. Architektura zapewnia dystrybuowanie optymalnego ruchu pomiędzy kontenerami w zależności od obciążenia.
2. Architektura zapewnia możliwość automatycznego powoływania dodatkowych kontenerów, a także automatyczną modyfikację i usuwanie.
3. Architektura zapewnia monitorowanie i logowanie statusu kontenerów.
4. Architektura zapewnia przydzielanie poszczególnym kontenerom i grupom kontenerów zasobów sprzętowych, jak i automatyczne dostosowywanie tych zasobów zgodnie z obciążeniem.
5. Architektura zapewnia automatyczną weryfikację przydzielonych zasobów i ich zmianę.



6. Architektura zapewnia automatyczną naprawę błędów poprzez naprawę, wymianę lub usuwanie kontenerów, które nie przechodzą ustawionych przez administratora testów poprawnego działania.
7. Architektura zapewnia możliwość wykonania określonych czynności w zależności od statusu kontenera np.: wykonanie restartu kontenera.
8. Architektura zapewnia automatyczne podłączanie lokalnych i chmurowych magazynów danych.
9. Architektura zapewnia wykrywanie i zarządzanie mikrouslugami.

#### 4.1.3 Wymagania ogólne dot. sprzętu

**ITS.WO.18.** Wykonawca musi dostarczyć sprzęt nowy, nieużywany, z bieżącej produkcji, wyprodukowany nie wcześniej niż 6 miesięcy przed terminem dostawy, pochodzący z autoryzowanego kanału dystrybucyjnego producenta w Polsce. Na dowód tego Wykonawca dostarczy odpowiednie oświadczenia producentów lub dystrybutorów sprzętu.

**ITS.WO.19.** Gwarancja

1. Wszystkie dostarczone urządzenia muszą posiadać gwarancję od dnia odbioru infrastruktury techniczno-systemowej do zakończenia Etapu V Umowy.
2. Gwarancja na urządzenia musi być realizowana co najmniej w Dni Robocze z wyłączeniem dni wolnych od pracy i świąt co najmniej w godzinach od 8:00 do 16:00.
3. Wymiana uszkodzonego urządzenia albo kluczowych elementów urządzenia warunkujących jego pracę musi nastąpić w miejscu instalacji (on-site) nie później niż w drugim Dniu Roboczym od zgłoszenia awarii.
4. Uszkodzone dyski objęte gwarancją muszą pozostać w dyspozycji Zamawiającego.

**ITS.WO.20.** Dla wszystkich urządzeń posiadających wbudowane oprogramowanie (firmware) lub dostarczane przez producenta oprogramowanie dedykowane (np. drivers) Wykonawca zapewnia u producenta urządzenia przez cały okres gwarancji dostęp do aktualizacji takiego oprogramowania oraz baz wiedzy lub FAQ na temat eksploatacji i/lub konfiguracji dostarczonych urządzeń (jeśli producent udostępnia takie bazy).

**ITS.WO.21.** Wykonawca musi dostarczyć niewyspecyfikowane elementy sprzętu i wyposażenia, które są niezbędne do prawidłowego funkcjonowania elementów wyspecyfikowanych i ich pracy z jak największą wydajnością. Dotyczy to w szczególności niezbędnej liczby i rodzajów przewodów połączeniowych zasilających oraz sygnałowych – w tym światłowodowych.

## 4.2 Warstwa sieciowa

### 4.2.1 Zapora ogniowa

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Siec.1.** Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.

**ITS.Siec.2.** Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Urządzenie musi posiadać rozmiar nie większy niż 2U.

**ITS.Siec.3.** System realizujący funkcję Firewall musi zapewniać możliwość pracy w jednym z trzech trybów: routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

**ITS.Siec.4.** W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

**ITS.Siec.5.** System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

**ITS.Siec.6.** W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

**ITS.Siec.7.** System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

**ITS.Siec.8.** System musi zapewniać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.

**ITS.Siec.9.** System musi zapewniać monitoring stanu realizowanych połączeń VPN.

**ITS.Siec.10.** System realizujący funkcję Firewall musi dysponować minimum:

1. 10 portami Gigabit Ethernet RJ-45.
2. 8 gniazdami SFP 1 Gbps.
3. 2 gniazdami SFP+ 10 Gbps

**ITS.Siec.11.** W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.

**ITS.Siec.12.** Należy zapewnić minimum 2 wkładki 10 Gigabit Ethernet SFP+ SR.

**ITS.Siec.13.** System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 480 GB.

**ITS.Siec.14.** System musi być wyposażony w minimum dwa redundantne zasilacze 230V AC wymieniane "na gorąco" (ang. hot swap).

**ITS.Siec.15.** Wydajność

1. W zakresie Firewall obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz 130000.000 nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall - nie mniej niż 30 Gbps.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji - nie mniej niż 5 Gbps.
4. Wydajność szyfrowania VPN IPSec - nie mniej niż 4,5 Gbps.
5. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 4,5 Gbps.

**ITS.Siec.16.** W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:

1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Analiza ruchu szyfrowanego protokołem SSL.

**ITS.Siec.17.** Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.

**ITS.Siec.18.** System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jednego oraz jeden do wielu.

**ITS.Siec.19.** W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.

- ITS.Siec.20.** System musi umożliwiać konfigurację połączeń typu IPSec VPN.
- ITS.Siec.21.** System musi umożliwiać konfigurację połączeń typu SSL VPN.
- ITS.Siec.22.** W zakresie routingu rozwiązanie powinno zapewniać obsługę:
1. Routingu statycznego.
  2. Policy Based Routingu.
  3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
- ITS.Siec.23.** System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
  2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- ITS.Siec.24.** System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- ITS.Siec.25.** Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
- ITS.Siec.26.** System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- ITS.Siec.27.** Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
- ITS.Siec.28.** System musi umożliwiać skanowanie archiwów.
- ITS.Siec.29.** Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- ITS.Siec.30.** Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- ITS.Siec.31.** Administrator systemu musi posiadać możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- ITS.Siec.32.** System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- ITS.Siec.33.** Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- ITS.Siec.34.** Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- ITS.Siec.35.** Baza powinna zawierać kategorie aplikacji z informacją o poziomie zagrożenia.
- ITS.Siec.36.** Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- ITS.Siec.37.** Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- ITS.Siec.38.** W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
- ITS.Siec.39.** Filtr WWW musi dostarczać kategorii stron zabronionych
- ITS.Siec.40.** Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- ITS.Siec.41.** System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
- ITS.Siec.42.** Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- ITS.Siec.43.** Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.

- ITS.Siec.44.** System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- ITS.Siec.45.** Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- ITS.Siec.46.** System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- ITS.Siec.47.** Musi istnieć możliwość logowania do serwera SYSLOG. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- ITS.Siec.48.** W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.
- ITS.Siec.49.** Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
- ITS.Siec.50.** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:
1. CSA lub EAL4 dla funkcji Firewall.
  2. ICSA lub NSS Labs dla funkcji IPS.
  3. ICSA dla funkcji IPSec VPN.
  4. ICSA dla funkcji SSL VPN.
  5. Wykonawca musi dostarczyć licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres od daty podpisania protokołu zdawczo-odbiorczego przez Zamawiającego do zakończenia Etapu V.

#### 4.2.2 Zapora ogniowa – zarządzanie

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

- ITS.Siec.51.** Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza.
- ITS.Siec.52.** Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Urządzenie musi posiadać rozmiar nie większy niż 2U.
- ITS.Siec.53.** System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
- ITS.Siec.54.** W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
- ITS.Siec.55.** System musi wspierać protokoły IPv4 oraz IPv6 w zakresie:
1. Firewall.
  2. Ochrony w warstwie aplikacji.
  3. Protokołów routingu dynamicznego.
- ITS.Siec.56.** W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klastery Active-Active lub Active-Passive w ramach dostarczanych urządzeń. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
- ITS.Siec.57.** System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

- ITS.Siec.58.** System musi zapewniać monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych.
- ITS.Siec.59.** System musi zapewniać monitoring stanu realizowanych połączeń VPN.
- ITS.Siec.60.** System realizujący funkcję Firewall musi dysponować minimum 6 portami Gigabit Ethernet RJ-45.
- ITS.Siec.61.** W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
- ITS.Siec.62.** System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 200 GB.
- ITS.Siec.63.** System musi być wyposażony w zasilacz 230V AC.
- ITS.Siec.64.** Wydajność
1. W zakresie Firewall'a obsługa nie mniej niż 3 mln jednoczesnych połączeń oraz min. 100000.000 nowych połączeń na sekundę.
  2. Przepustowość Stateful Firewall - nie mniej niż 2 Gbps
  3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji - nie mniej niż 1 Gbps.
  4. Wydajność szyfrowania VPN IPSec - nie mniej niż 1 Gbps.
  5. Wydajność skanowania ruchu z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 0,5 Gbps.
- ITS.Siec.65.** W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje:
1. Kontrola dostępu - zaporą ogniową klasy Stateful Inspection.
  2. Kontrola Aplikacji.
  3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
  4. Ochrona przed malware co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
  5. Ochrona przed atakami - Intrusion Prevention System.
  6. Kontrola stron WWW.
  7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP
  8. Zarządzanie pasmem (QoS, Traffic shaping).
  9. Analiza ruchu szyfrowanego protokołem SSL.
- ITS.Siec.66.** Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
- ITS.Siec.67.** System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz translację jeden do jeden oraz jeden do wielu.
- ITS.Siec.68.** W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
- ITS.Siec.69.** System musi umożliwiać konfigurację połączeń typu IPSec VPN.
- ITS.Siec.70.** System musi umożliwiać konfigurację połączeń typu SSL VPN.
- ITS.Siec.71.** W zakresie routingu rozwiązanie powinno zapewniać obsługę:
1. Routingu statycznego.
  2. Policy Based Routingu.
  3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP.
- ITS.Siec.72.** System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
1. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
  2. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
- ITS.Siec.73.** System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
- ITS.Siec.74.** Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.

- ITS.Siec.75.** System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.
- ITS.Siec.76.** Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach.
- ITS.Siec.77.** System musi umożliwiać skanowanie archiwów.
- ITS.Siec.78.** Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
- ITS.Siec.79.** Baza sygnatur ataków powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- ITS.Siec.80.** Administrator systemu musi posiadać możliwość definiowania własnych wyjątków oraz własnych sygnatur.
- ITS.Siec.81.** System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
- ITS.Siec.82.** Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
- ITS.Siec.83.** Baza Kontroli Aplikacji powinna być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
- ITS.Siec.84.** Baza powinna zawierać kategorie aplikacji z informacją o ryzyku.
- ITS.Siec.85.** Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.
- ITS.Siec.86.** Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
- ITS.Siec.87.** W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy avoidance.
- ITS.Siec.88.** Filtr WWW musi dostarczać kategorii stron zabronionych
- ITS.Siec.89.** Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
- ITS.Siec.90.** System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
- ITS.Siec.91.** Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
- ITS.Siec.92.** Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
- ITS.Siec.93.** System musi mieć wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
- ITS.Siec.94.** Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
- ITS.Siec.95.** System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
- ITS.Siec.96.** Musi istnieć możliwość logowania do serwera SYSLOG. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
- ITS.Siec.97.** W ramach logowania system musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu.

**ITS.Siec.98.** Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.

**ITS.Siec.99.** Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:

1. CSA lub EAL4 dla funkcji Firewall.
2. ICSA lub NSS Labs dla funkcji IPS.
3. ICSA dla funkcji IPSec VPN.
4. ICSA dla funkcji SSL VPN.

**ITS.Siec.100.** Wykonawca dostarcza licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: Kontrola Aplikacji, IPS, Antywirus, Antyspam, Web Filtering na okres od daty podpisania protokołu zdawczo-odbiorczego przez Zamawiającego do zakończenia Etapu V.

#### 4.2.3 Równoważnik obciążenia i WAF

Minimum 2 sztuki urządzeń, z których każde musi spełnić wymagania jak poniżej:

**ITS.Siec.101.** Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia. Urządzenie musi posiadać rozmiar nie większy niż 2U

**ITS.Siec.102.** System musi realizować co najmniej następujące funkcje:

1. Rozkład ruchu pomiędzy serwerami aplikacji Web,
2. Selektywny http caching,
3. Selektywna kompresja danych,
4. Terminowanie sesji SSL,
5. Optymalizacja i akceleracja aplikacji,
6. Ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall).

**ITS.Siec.103.** Wszystkie funkcje wymienione w specyfikacji muszą być dostępne w obrębie jednego urządzenia.

**ITS.Siec.104.** Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.

**ITS.Siec.105.** System musi posiadać co najmniej następujące metody równoważenia obciążenia:

1. Cykliczna,
2. Ważona,
3. Najmniejsza liczba połączeń,
4. Najszybsza odpowiedź serwera,
5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera.

**ITS.Siec.106.** Rozwiązanie musi pracować w trybie pełnego proxy.

**ITS.Siec.107.** Praca w trybie pełnego proxy nie może powodować degradacji wydajności rozwiązania.

**ITS.Siec.108.** Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji.

**ITS.Siec.109.** WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web. Pozytywny model bezpieczeństwa powinien kontrolować co najmniej:

1. wystąpienie URL-i, długość URL-i, zabezpieczenie przed clickjackiem dla danego URL-a,
2. typ servleta występujący pod danym url-em – format komunikacji (http form, JSON, XML, GWT),

3. przejścia pomiędzy URL-ami (servletami),
4. dopuszczalne metody http,
5. dopuszczalne cookie,
6. dopuszczalne parametry w polityce,
7. parametry dynamiczne,
8. typ/format parametrów (alfanumeryczny, integer, dynamiczny, statyczny, JSON, XML, e-mail, telefon, plik uploadowany),
9. oraz dopuszczalne parametry w danym serwlecie,
10. długość zapytań,
11. nazwy hosta,
12. wystąpień i długość parametrów (per każdy parametr),
13. wystąpień i długości nagłówków,
14. wystąpień i długości cookies,
15. oczekiwanych typów znaków per każdy parametr,
16. typów rozszerzeń plików; w tym długości URLa, requestu, query stringu, post data dla danego typu pliku,
17. URL-i podatnych na CSRF.

**ITS.Siec.110.** Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń).

**ITS.Siec.111.** Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr.

**ITS.Siec.112.** Dla każdej chronionej aplikacji internetowej urządzenie powinno umożliwiać wybór stosowanych technologii i systemu operacyjnego w celu poprawnego doboru wykorzystywanych sygnatur uwzględniając, ale nie ograniczając się do:

1. Bazy danych: ORACLE, MySQL, Microsoft SQL Server, PostgreSQL, IBM DB2,
2. System Operacyjny: Windows, Linux, UNIX,
3. Serwer WWW: Apache, Apache Tomcat, Microsoft IIS, serwerów proxy,
4. System musi posiadać co najmniej następujące interfejsy administracyjne:
  - a. GUI przy wykorzystaniu protokołu https,
  - b. Zarządzanie poprzez SSH,
  - c. Zarządzanie poprzez API REST.

**ITS.Siec.113.** Autoryzacja administratorów systemu musi bazować na rolach użytkowników.

**ITS.Siec.114.** System musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów: Cookie (hash, rewrite, custom, insert, passive):

1. Adres źródła,
2. SIP call ID,
3. Identyfikator sesji SSL,
4. Microsoft Terminal Services (RDP) – nazwa użytkownika,
5. Adres docelowy.

**ITS.Siec.115.** System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.

**ITS.Siec.116.** System musi zapewniać możliwość klonowania puli serwerów umożliwiając wysyłanie kopii ruchu do zewnętrznych systemów monitoringu lub urządzeń typu IDS/IPS.

**ITS.Siec.117.** System musi zapewniać obsługę certyfikatów z kluczami typu ECDSA wykorzystującymi krzywe eliptyczne (ECC) zarówno od strony klienta, jak i od strony puli serwerów.



- ITS.Siec.118.** Dla protokołu TLS 1.2 wymagana jest obsługa AES-GCM zarówno od strony klienta, jak i od strony puli serwerów.
- ITS.Siec.119.** System musi zapewniać obsługę certyfikatów podpisanych funkcją skrótu SHA-2 zarówno od strony klienta, jak i od strony puli serwerów.
- ITS.Siec.120.** System musi obsługiwać sieci VLAN w standardzie 802.1q.
- ITS.Siec.121.** System musi obsługiwać agregację linków w standardzie 802.1.AX (LACP).
- ITS.Siec.122.** System musi obsługiwać Jumbo Frames.
- ITS.Siec.123.** System musi świadczyć, co najmniej następujące usługi w warstwach 4-7:
1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http,
  2. Ukrywanie zasobów,
  3. Zmiana odpowiedzi serwera,
  4. Przepisywanie odpowiedzi (response rewriting),
  5. Ochrona przed atakami typu DoS/DDoS,
  6. Ochrona przed atakami typu SYN Flood,
  7. Multipleksowanie połączeń http.
- ITS.Siec.124.** System musi posiadać następujące funkcje zarządzania:
1. Obsługa protokołu SNMP v1/v2c/v3,
  2. Zewnętrzny syslog,
  3. Zbieranie danych i ich wyświetlanie,
  4. Zbieranie danych zgodnie z ustawieniami administratora,
  5. Osobna brama domyślna dla interfejsu zarządzającego,
  6. Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot),
  7. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy).
  8. Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.
- ITS.Siec.125.** System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.
- ITS.Siec.126.** System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.
- ITS.Siec.127.** System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.
- ITS.Siec.128.** System musi posiadać możliwość tworzenia klastrów wysokiej dostępności (HA) złożonych z minimum dwóch urządzeń modularnych tego samego typu. Klaster musi mieć możliwość pracy w trybie active – standby, active-active oraz klastra N+1.
- ITS.Siec.129.** Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL i stanu sesji TCP pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu.
- ITS.Siec.130.** Klaster wysokiej dostępności musi zapewniać synchronizację:
1. Konfiguracji,
  2. Stanu połączeń,
  3. Przywiązywania sesji (Session persistence).
- ITS.Siec.131.** Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu weryfikacji stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover).
- ITS.Siec.132.** Urządzenie musi być przeznaczona do montażu w szafie rack 19" i wysokości nie większa niż 1U.

**ITS.Siec.133.** System musi być wyposażony w dwa redundantne zasilacze 230V AC wymieniane "na gorąco" (ang. hot swap).

**ITS.Siec.134.** Urządzenie musi posiadać minimum 2 porty 10 Gigabit Ethernet na wkładki SFP+, oddzielny interfejs zarządzania, port konsolowy, minimum dwa porty USB.

**ITS.Siec.135.** Należy zapewnić 2 wkładki 10 Gigabit Ethernet SFP+ SR.

**ITS.Siec.136.** Sprzęt musi posiadać poniższe parametry:

1. Pamięć nie mniej niż 16GB,
2. Dysk o pojemności nie mniejszej niż 500GB,
3. Przepływność dla warstwy 4 nie mniej niż 10 Gbps,
4. Przepływność dla warstwy 7 nie mniej niż 10 Gbps,
5. Ilość jednocześnie obsługiwanych połączeń dla warstwy 4 nie mniej niż 14 000 000,
6. Ilość transakcji SSL na sekundę dla klucza o długości 2048 nie mniej niż 4 000,
7. Przepływność ruchu szyfrowanego nie mniej niż 8 Gbps,
8. Ilość połączeń na sekundę w warstwie 4 nie mniej niż 250 000,
9. Kompresja sprzętowa nie mniej niż 5 Gbps.

#### 4.2.4 Przełącznik Ethernet

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Siec.137.** Wykonawca dostarczy przełącznik stakowalny wyposażony w minimum 24 porty 10Gb.

**ITS.Siec.138.** Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco” (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne, co najmniej następujące moduły:

1. Minimum 4-portowy moduł Gigabit Ethernet z gniazdami SFP,
2. Minimum 4-portowy moduł 10Gigabit Ethernet SFP+.

**ITS.Siec.139.** Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH).

**ITS.Siec.140.** Przełącznik musi być wyposażony w 24 moduły 10Gb SFP+

**ITS.Siec.2.** Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów:

1. Przepustowość w ramach stosu min. 320Gb/s,
2. Min. 6 urządzenia w stosie,
3. Zarządzanie poprzez jeden adres IP,
4. Możliwość tworzenia połączeń cross-stack EtherChannel (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad.

**ITS.Siec.141.** Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów.

**ITS.Siec.142.** Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne.

**ITS.Siec.143.** Przełącznik musi być wyposażony w dwa zasilacze prądu zmiennego 230V AC.

**ITS.Siec.144.** Szybkość przełączania minimum 60Mpps dla pakietów 64-bajtowych.

**ITS.Siec.145.** Urządzenie musi posiadać minimum 4GB pamięci DRAM i minimum 2GB pamięci flash.

**ITS.Siec.146.** Urządzenie musi zapewnić obsługę minimum:

1. 200 sieci VLAN,
2. 32.000 adresów MAC.

**ITS.Siec.147.** Urządzenie musi zapewnić obsługę protokołu NTP.

**ITS.Siec.148.** Urządzenie musi zapewnić obsługę IGMPv1/2/3.

**ITS.Siec.149.** Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:

1. IEEE 802.1w Rapid Spanning Tree,
2. IEEE 802.1s Multi-Instance Spanning Tree.

**ITS.Siec.150.** Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.

**ITS.Siec.151.** Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:

1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
2. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN,
3. Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL,
4. Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X,
5. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
6. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
7. Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i komputera PC podłączonego za telefonem,
8. Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie w oparciu o portal www),
9. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
10. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+.

**ITS.Siec.152.** Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia).

**ITS.Siec.153.** Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:

1. Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi,
2. Implementacja co najmniej 4 kolejek dla ruchu wyjściowego dla sieci WLAN dla obsługi ruchu o różnej klasie obsługi,
3. Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek,
4. Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority),
5. Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP,
6. Kontrola sztormów dla ruchu broadcast/multicast/unicast.

**ITS.Siec.154.** Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP).

- ITS.Siec.155.** Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego.
- ITS.Siec.156.** Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm.
- ITS.Siec.157.** Dedykowany port Ethernet do zarządzania out-of-band.
- ITS.Siec.158.** Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.
- ITS.Siec.159.** Urządzenie musi zapewnić obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.
- ITS.Siec.160.** Urządzenie musi być możliwe do montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1U.
- ITS.Siec.161.** Do każdego dostarczonego modułu 10Gb SFP+ musi być dostarczony kabel światłowodowy LC-LC o długości minimum 5 metrów.

#### 4.2.5 Przełącznik Ethernet – zarządzanie

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

- ITS.Siec.162.** Wykonawca dostarczy przełącznik stakowalny wyposażony w minimum 24 porty RJ45 100/1000 (Gigabit-Ethernet). Wymagane dostarczenie 24 kabli ethernet UTP cat. 6 o długości minimum 5 metrów.
- ITS.Siec.163.** Przełącznik musi zapewniać możliwość stakowania.
- ITS.Siec.164.** Przełącznik musi być wyposażony w minimum jeden zasilacz prądu zmiennego 230V AC.
- ITS.Siec.165.** Urządzenie musi posiadać minimum 4GB pamięci DRAM i 2GB pamięci flash
- ITS.Siec.166.** Urządzenie musi zapewnić obsługę minimum:
1. 200 sieci VLAN,
  2. 32.000 adresów MAC.
- ITS.Siec.167.** Urządzenie musi zapewnić obsługę protokołu NTP.
- ITS.Siec.168.** Urządzenie musi zapewnić obsługę IGMPv1/2/3.
- ITS.Siec.169.** Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem ciągłości pracy sieci:
1. IEEE 802.1w Rapid Spanning Tree,
  2. IEEE 802.1s Multi-Instance Spanning Tree.
- ITS.Siec.170.** Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP.
- ITS.Siec.171.** Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci:
1. Wiele poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzią serwera autoryzacji (privilege-level),
  2. Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC,
  3. Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X,
  4. Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard,
  5. Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+.

**ITS.Siec.172.** Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją.

**ITS.Siec.173.** Urządzenie musi zapewnić obsługę protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6.

**ITS.Siec.174.** Urządzenie musi być możliwe do montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1U.

#### 4.2.6 Przełącznik SAN

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Siec.175.** Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s z funkcją autonegociacji prędkości.

**ITS.Siec.176.** Przełącznik FC musi mieć wysokość maksymalnie 1U oraz zapewniać techniczną możliwość montażu w szafie 19".

**ITS.Siec.177.** Przełącznik FC musi posiadać minimum 2 redundantne zasilacze typu hot-plug umożliwiające podłączenie do jednofazowego źródła zasilania 230V AC

**ITS.Siec.178.** Przełącznik FC musi posiadać minimum 48 sloty na moduły FC. Wymaga się, aby przełącznik został dostarczony z co najmniej 24 portami aktywnymi. Wszystkie wymagane funkcje muszą być dostępne dla minimum 24 portów FC przełącznika. Wszystkie aktywne porty muszą być obsadzone modułami SFP 16Gb/s SR.

**ITS.Siec.179.** Rodzaj obsługiwanych portów: E\_Port, EX\_Port, F\_Port, N\_Port, M\_Port, D\_Port.

**ITS.Siec.180.** Przełącznik FC musi mieć możliwość instalacji jednomodowych SFP umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 10 km.

**ITS.Siec.181.** Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking” uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.

**ITS.Siec.182.** Przełącznik FC musi zapewniać możliwość dynamicznego aktywowania portów za pomocą zakupionych kluczy licencyjnych.

**ITS.Siec.183.** Maksymalny dopuszczalny pobór mocy przełącznika FC to 110W przy zasilaniu zmiennoprądowym AC.

**ITS.Siec.184.** Zsumowana przepustowość przełącznika FC musi wynosić minimum 768 Gb/s ("end-to-end" w trybie full duplex).

**ITS.Siec.185.** Urządzenie musi zapewniać możliwość agregacji połączeń pomiędzy przełącznikami (trunking) na poziomie poszczególnych ramek. Wymagana jest możliwość utworzenia pojedynczego połączenia „trunk” zbudowanego z minimum ośmiu portów o prędkości 8Gb/s lub z minimum ośmiu portów o prędkości 16Gb/s. Licencja umożliwiająca wykorzystanie tej funkcjonalności jest wymagana.

**ITS.Siec.186.** Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk” oraz obsługiwać grupy połączeń „trunk” o różnych długościach.

**ITS.Siec.187.** Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu bazę danych nazw serwerów.

**ITS.Siec.188.** Przełącznik FC musi zapewniać opóźnienie przy przesyłaniu ramek FC między dowolnymi portami nie większe niż 700 ns.

**ITS.Siec.189.** Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN.

- ITS.Siec.190.** Urządzenie musi wspierać mechanizm balansowania ruchem w połączeniach wewnątrz wielodomenowych sieci fabric w oparciu OXID.
- ITS.Siec.191.** Urządzenie musi posiadać możliwość wymiany w trybie „na gorąco” minimum modułów portów Fibre Channel (SFP).
- ITS.Siec.192.** Urządzenie musi zapewnić wsparcie dla N\_Port ID Virtualization (NPIV) oraz obsługę co najmniej 255 wirtualnych urządzeń na pojedynczym porcie przełącznika.
- ITS.Siec.193.** Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla danych wchodzących dla dowolnego portu lub portów. Musi zapewnić możliwość określenia limitów niższych niż wynegocjowana prędkość portu.
- ITS.Siec.194.** Przełącznik FC musi umożliwiać kategoryzację ruchu między inicjatorem i targetem oraz przydzieleniem takiej pary urządzeń do kategorii o wysokim, średnim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi być konfigurowana za pomocą standardowych narzędzi do konfiguracji zoningu.
- ITS.Siec.195.** Przełącznik FC musi posiadać możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą jak i na niższą) w czasie pracy urządzenia, bez wymogu ponownego uruchomienia urządzeń w sieci SAN.
- ITS.Siec.196.** Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:
1. Listy Kontroli Dostępu definiujące urządzenia (przełączniki i urządzenia końcowe) uprawnione do pracy w sieci Fabric,
  2. Możliwość uwierzytelnienia (ang. authentication) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP,
  3. Możliwość uwierzytelnienia (ang. authentication) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP,
  4. Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów,
  5. Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2,
  6. Wskazanie nadrzędnych przełączników odpowiedzialnych za bezpieczeństwo w sieci typu Fabric,
  7. Konta użytkowników definiowane w środowisku RADIUS lub LDAP,
  8. Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS,
  9. Obsługa SNMP v1/v3.
- ITS.Siec.197.** Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
- ITS.Siec.198.** Przełącznik FC musi być wyposażone w następujące narzędzia diagnostyczne i mechanizmy obsługi ruchu FC:
1. logowanie zdarzeń poprzez mechanizm „syslog”,
  2. monitorowanie połączeń i „trunków”.
- ITS.Siec.199.** Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS232 oraz inband IP-over-FC.
- ITS.Siec.200.** Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S.
- ITS.Siec.201.** Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP.
- ITS.Siec.202.** Do każdego dostarczonego modułu SFP 16Gb/s SR musi być dostarczony kabel światłowodowy LC-LC o długości minimum 5 metrów.

## 4.3 Warstwa sprzętowa

### 4.3.1 Obudowa Blade

Minimum 2 sztuki urządzeń, których każde musi spełniać wymagania jak poniżej:

- ITS.Sprz.1.** Obudowa o wysokości maksymalnie 10U przystosowana do montażu w szafie rack 19". W obudowie musi być możliwość zainstalowania minimum 14 serwerów Blade oferowanego typu. System zasilania i chłodzenia obudowy musi być redundantny - zdolny do obsługi awarii minimum 2 modułów zasilaczy i wentylatorów lub awarii jednego źródła zasilania przy ciągłym dostarczeniu mocy do obudowy w pełni obsadzonej zaoferowanymi serwerami.
- ITS.Sprz.2.** Obudowa blade musi posiadać minimum 6 wnęk do instalacji modułów komunikacyjnych dla serwerów umożliwiających połączenia w technologiach: 10Gb Ethernet, Gigabit Ethernet, Fiber Channel, Infiniband.
- ITS.Sprz.3.** W obudowie muszą być zainstalowane co najmniej 2 dedykowane moduły przełączników sieciowych LAN.
- ITS.Sprz.4.** Każdy moduł sieciowy LAN musi być wyposażony w minimum 4 zewnętrzne porty 10Gb Ethernet wraz z 4 wkładkami 10 Gigabit Ethernet SFP+ SR.
- ITS.Sprz.5.** W ramach sieciowych modułów LAN musi istnieć możliwość podziału pojedynczego łącza 10Gb Ethernet do serwera na min. 4 niezależne połączenia sieciowe (każde połączenie z własnym adresem MAC) z możliwością regulacji ich przepustowości.
- ITS.Sprz.6.** W obudowie muszą być zainstalowane co najmniej 2 dedykowane moduły SAN do obsługi technologii 16Gb Fibre Channel agregujące i wyprowadzające sygnały ze wszystkich portów FC oferowanych serwerów z zachowaniem redundancji połączeń do każdego z nich.
- ITS.Sprz.7.** Każdy moduł sieciowy SAN musi być wyposażony w minimum 4 zewnętrzne porty 16Gb Fibre Channel wraz z minimum 4 odpowiednimi wkładkami 16Gb SFP+ Short Range wraz z przewodami światłowodowymi typu LC-LC o długości 3 metrów.
- ITS.Sprz.8.** Obudowa musi mieć zainstalowane min. 2 redundantne, sprzętowe moduły zarządzające z dostępem przez dedykowany interfejs sieciowy Ethernet RJ-45.
- ITS.Sprz.9.** Należy zapewnić możliwość zdalnego włączania/wyłączania/restartu niezależnie dla każdego zainstalowanego serwera.
- ITS.Sprz.10.** Należy zapewnić możliwość zdalnego udostępniania napędu DVD-ROM, na potrzeby każdego serwera z możliwością bootowania z w/w napędów.
- ITS.Sprz.11.** Należy zapewnić możliwość zdalnego zarządzania z poziomu przeglądarki internetowej, bez konieczności instalacji specyficznych komponentów programowych producenta sprzętu.
- ITS.Sprz.12.** W danym momencie musi być niezależny, równoległy dostęp do konsol tekstowych i graficznych wszystkich serwerów w ramach dostarczanej infrastruktury.
- ITS.Sprz.13.** Należy zapewnić możliwość zdalnej identyfikacji fizycznego serwera i obudowy za pomocą sygnalizatora optycznego. System zarządzania musi w sposób graficzny wizualizować stan poszczególnych elementów infrastruktury (stan normalnej pracy, uwagi, awarie). Graficzne zobrazowanie stanu infrastruktury z możliwością przejścia od widoku ogólnego do widoku szczegółowego każdego z elementów infrastruktury (architektura drill-down).
- ITS.Sprz.14.** Należy zapewnić możliwość kontroli wersji zainstalowanych sterowników/agentów na serwerach.
- ITS.Sprz.15.** Należy zapewnić możliwość przeprowadzania uaktualnień sterowników/agentów zdalnie z systemu zarządzania.
- ITS.Sprz.16.** Należy zapewnić możliwość zdalnej reakcji na zdarzenia w infrastrukturze np. poprzez automatyczne wykonywanie skryptów, możliwość automatycznego powiadamiania administratorów poprzez e-mail.



**ITS.Sprz.17.** Dostęp do aplikacji zarządzającej powinien być możliwy z serwera zarządzającego lub dowolnego innego miejsca poprzez przeglądarkę internetową (połączenie szyfrowane SSL) bez konieczności instalowania dodatkowego oprogramowania producenta serwera.

**ITS.Sprz.18.** Opieka techniczna ważna jest przez minimum cały okres gwarancji i obejmuje dostęp do najnowszych wersji firmware, sterowników, oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

**ITS.Sprz.19.** Zintegrowany z obudową moduł switcha KVM umożliwiający przyłączenie lokalne (analogowe) monitora, klawiatury i myszy.

**ITS.Sprz.20.** Oferowane urządzenie musi być fabrycznie nowe i pochodzić z autoryzowanego kanału dystrybucji producenta w Polsce

#### 4.3.2 Serwer Blade

Minimum 16 sztuk urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Sprz.21.** Co najmniej 2 procesory w architekturze x86, 64-bit, osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 173 (dla testowego serwera w konfiguracji testowej z dwoma procesorami). Wyniki testów wykorzystanych do potwierdzenia mocy obliczeniowej procesorów muszą być publikowane na stronie [www.spec.org](http://www.spec.org).

**ITS.Sprz.22.** Serwer musi być dostarczony z zainstalowaną pamięcią RAM minimum 1024 GB RAM DDR4 z korekcją błędów ECC.

**ITS.Sprz.23.** Sterownik dysków wewnętrznych SAS musi obsługiwać co najmniej RAID 0 i 1.

**ITS.Sprz.24.** Serwer musi mieć zainstalowane co najmniej dwa dyski SAS SSD, każdy minimum 200GB, typu Hot-plug o przepustowości minimum 500MB/s.

**ITS.Sprz.25.** Serwer musi być wyposażony w minimum 2 interfejsy sieciowe 10Gb Ethernet, minimum 2 interfejsy Fiber Channel 16 Gb oraz minimum 1 wewnętrzny port USB.

**ITS.Sprz.26.** Serwer musi zapewniać możliwość zdalnego dostępu do graficznego interfejsu Web karty zarządzającej (dedykowany port co najmniej 1Gb Ethernet) przez minimum dwóch administratorów jednocześnie. Zdalny dostęp musi być realizowany przez połączenie szyfrowane (SSLv3) oraz uwierzytelnianie i autoryzację użytkownika.

**ITS.Sprz.27.** Serwer musi być wyposażony w kartę zarządzającą niezależną od zainstalowanego na serwerze systemu operacyjnego. Karta zarządzająca musi umożliwić podmontowanie zdalnych wirtualnych napędów, dostęp do myszy oraz klawiatury, wsparcie dla IPv6, wsparcie dla SNMP, IPMI2.0, SSH a także integrację z Active Directory.

**ITS.Sprz.28.** Karta zarządzająca musi posiadać możliwość zdalnego monitorowania i informowania o statusie serwera (m.in. konfiguracji serwera), możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer oraz wysyłania do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.

**ITS.Sprz.29.** Wspierane systemy operacyjne minimum: Microsoft Windows 2016, RHEL, SLES, VMware vSphere 6 lub nowszy.

**ITS.Sprz.30.** Serwer musi być w pełni kompatybilny z dostarczoną obudową blade.

**ITS.Sprz.31.** Opieka techniczna ważna jest przez minimum cały okres gwarancji i obejmuje dostęp do najnowszych wersji firmware, sterowników, oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.

#### 4.3.3 Serwer RACK

Minimum 4 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Sprz.32.** Obudowa typu Rack.

**ITS.Sprz.33.** Przeznaczony do instalacji w szafie 19”.

**ITS.Sprz.34.** Maksymalna wysokość serwera 1U.



- ITS.Sprz.35.** Co najmniej 2 procesory w architekturze x86, 64-bit osiągające w testach SPECrate2017\_int\_base wynik nie gorszy niż 72 (dla testowego serwera w konfiguracji testowej z dwoma procesorami). Wyniki testu muszą być publikowane na stronie [www.spec.org](http://www.spec.org)
- ITS.Sprz.36.** Liczba zainstalowanych procesorów – minimum 2 sztuki.
- ITS.Sprz.37.** Zainstalowana pamięć RAM minimum 128GB DDR4 z korekcją błędów ECC, RDIMM.
- ITS.Sprz.38.** Zainstalowane moduły powinny umożliwić rozszerzenie pamięci RAM do pełnej obsługiwanej przez płytę główną pojemności.
- ITS.Sprz.39.** Płyta główna powinna umożliwiać obsługę minimum do 384GB pamięci RAM. Możliwość późniejszej rozbudowy do 384GB RAM przy zainstalowanej pamięci RAM minimum 128GB.
- ITS.Sprz.40.** Na płycie głównej powinno znajdować się minimum 12 slotów dla modułów pamięci, w tym minimum 2 sloty PCI-Express 3.0.
- ITS.Sprz.41.** Serwer musi być wyposażony w podsystem dyskowy zintegrowany w obudowie, podłączenie do zintegrowanego podsystemu dyskowego łączem zapewniającym transfer co najmniej 6Gb/s. Kontroler podsystemu dyskowego musi posiadać minimum 1GB pamięci cache i zapewniać obsługę zabezpieczeń co najmniej RAID 0, 1, 5, 6, 10.
- ITS.Sprz.42.** Podsystem dyskowy (zintegrowany) musi być wyposażony w minimum 2 dyski twarde 2,5", każdy o pojemności minimum 1.2TB, prędkości obrotowej minimum 10 000 obrotów na minutę, interfejsie połączeniowym SAS zapewniającym transfer min. 6Gb/s. Wszystkie dyski wchodzące w skład podsystemu dyskowego muszą być typu hot-plug tzn. z możliwością wyjęcia/włożenia podczas pracy serwera. Podsystem dyskowy musi umożliwiać instalację min. 8 dysków twardych typu hot plug.
- ITS.Sprz.43.** Serwer musi być wyposażony w następujące porty:
1. Minimum 2 porty Ethernet 1Gb/s RJ-45,
  2. Minimum 2 porty Ethernet 10Gb/s SFP+ wraz z modułami 10 Gigabit Ethernet SFP+ SR,
  3. Minimum 2 porty Fibre Channel 16Gb/s wraz z modułami SFP 16Gb/s SR.
- ITS.Sprz.44.** Serwer musi posiadać zintegrowaną kartę graficzną.
- ITS.Sprz.45.** Serwer musi posiadać minimum 2 redundantne zasilacze typu hot-plug 230V.
- ITS.Sprz.46.** System zasilania i chłodzenia musi być redundantny - zdolny do obsługi awarii 1 modułu zasilacza, wentylatora lub awarii jednego źródła zasilania przy ciągłym dostarczeniu mocy do serwera.
- ITS.Sprz.47.** Serwer musi posiadać napęd DVD-ROM.
- ITS.Sprz.48.** Karta zarządzająca umieszczona w serwerze musi zapewniać:
1. Zdalny dostęp do graficznego interfejsu Web karty zarządzającej (dedykowany port 1Gb Ethernet),
  2. Możliwość podmontowania zdalnych wirtualnych napędów,
  3. Wirtualną konsolę z dostępem do myszy, klawiatury,
  4. Możliwość zdalnego podłączenia do serwera napędu CD/DVD ROM.
- ITS.Sprz.49.** Serwer musi zapewniać wsparcie dla oprogramowania co najmniej MS Windows 2016, VMware ESXi 6.x, RHEL 7.x, SLES 11 lub nowsze.
- ITS.Sprz.50.** Serwer musi zostać dostarczony wraz z zestawem do montażu serwera w szafie rack.

#### 4.3.4 Biblioteka taśmowa

Minimum 1 urządzenie, które musi spełniać wymagania jak poniżej:

- ITS.Sprz.51.** Biblioteka musi być przystosowana do montażu w szafie 19".
- ITS.Sprz.52.** Wysokość oferowanej biblioteki taśmowej nie może przekraczać 3U.
- ITS.Sprz.53.** Biblioteka taśmowa musi być wyposażona w minimum jeden napęd LTO Ultrium-8 FC z możliwością rozbudowy do minimum 2 napędów oferowanego typu.

- ITS.Sprz.54.** Biblioteka musi posiadać minimum 32 sloty wewnętrzne na taśmy LTO Ultrium-8.
- ITS.Sprz.55.** Każdy zainstalowany napęd taśmowy musi posiadać natywny interfejs Fibre Channel 8Gb/s wraz z modułem SFP 8Gb/s SR.
- ITS.Sprz.56.** Napęd taśmowy musi posiadać prędkość transmisji danych minimum 300MB/s.
- ITS.Sprz.57.** Biblioteka musi posiadać możliwość konfiguracji, co najmniej trzech tzw. „mail slot” umożliwiających wymianę pojedynczej taśmy bez konieczności wyjmowania z biblioteki całego magazynka z taśmami.
- ITS.Sprz.58.** Wraz z każdą biblioteką musi być dostarczonych min. 50 sztuk taśm LTO Ultrium-8 RW (o pojemności pojedynczej taśmy, co najmniej 12TB - bez uwzględniania kompresji danych) wraz z etykietami oraz min. 5 sztuk taśm czyszczących.
- ITS.Sprz.59.** Biblioteka taśmowa musi posiadać możliwość zdalnego zarządzania za pośrednictwem przeglądarki internetowej.
- ITS.Sprz.60.** Biblioteka taśmowa musi być wyposażona w czytnik kodów kreskowych.
- ITS.Sprz.61.** Biblioteka musi być wyposażona w redundantne zasilacze 230V AC hot swap.
- ITS.Sprz.62.** Napędy LTO Ultrium-8 muszą posiadać wsparcie dla taśm typu WORM i sprzętową enkrypcję AES 256-bit.

#### 4.3.5 Deduplikator

Minimum 1 urządzenie, które musi spełniać wymagania jak poniżej:

- ITS.Sprz.63.** Przez urządzenie do backupu dyskowego z deduplikacją danych Zamawiający rozumie rozwiązanie charakteryzujące się jednolitą budową typu „appliance” pochodzącym od jednego producenta i realizujące wszystkie wymagane funkcjonalności. Nie dopuszcza się rozwiązania zbudowanego z niezależnych komponentów sprzętowo-programowych. Urządzenie powinno być oficjalnie dostępne w ofercie producenta przed ukazaniem się niniejszego postępowania.
- ITS.Sprz.64.** Urządzenie musi być przystosowane do montażu w szafie rack 19”.
- ITS.Sprz.65.** Urządzenie musi oferować minimum 32 TB przestrzeni użytkowej dla danych (bez deduplikacji).
- ITS.Sprz.66.** Dane przechowywane w obrębie podsystemu dyskowego urządzenia muszą być chronione za pomocą technologii RAID.
- ITS.Sprz.67.** Urządzenie musi weryfikować ewentualne przekłamanie danych w wyniku działań systemu plików / mechanizmów RAID zaimplementowanych w urządzeniu. Wymaga się, aby urządzenie sprawdzało sumy kontrolne zapisywanych fragmentów danych po przejściu danych przez system plików / mechanizmy RAID. Urządzenie musi automatycznie rozpoznawać i naprawiać błędy w locie.
- ITS.Sprz.68.** Urządzenie musi umożliwiać bezpieczne usuwanie danych zgodnie ze standardem NIST SP 800-88 poprzez mechanizm wielokrotnego nadpisania przeterminowanych danych.
- ITS.Sprz.69.** Elementy sprzętowe takie jak półki dyskowe, dyski, zasilanie muszą być zdublowane i awaria pojedynczego elementu nie może powodować utraty danych i dostępu do nich.
- ITS.Sprz.70.** Urządzenie musi posiadać minimum:
1. 4 porty FC 16 Gb/s z możliwością obsługi każdym portem FC protokołów VTL oraz deduplikacji na źródle. Każdy port wyposażony w moduł 10Gb SFP+.
  2. 4 portów Ethernet 10 Gb/s SFP z możliwością obsługi każdym portem Ethernet protokołów CIFS i NFS oraz deduplikacji na źródle. Każdy port wyposażony w moduł SFP 16Gb/s SR.
- ITS.Sprz.71.** Urządzenie musi osiągać co najmniej przepustowość 20 TB/h.
- ITS.Sprz.72.** Urządzenie nie może zmniejszać swojej wydajności w czasie przybywania kolejnych danych.

**ITS.Sprz.73.** Urządzenie musi umożliwiać jednoczesny dostęp do całej pojemności urządzenia wszystkimi poniższymi protokołami:

1. IFS, NFS i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów Ethernet,
2. VTL i deduplikacja na źródle (OST/Boost/Catalyst) dla interfejsów FC.

**ITS.Sprz.74.** Urządzenie musi posiadać obsługę mechanizmów deduplikacji dla danych otrzymywanych wszystkimi protokołami (CIFS, NFS, VTL, deduplikacja na źródle) przechowywanych w obrębie urządzenia.

**ITS.Sprz.75.** Oferowane urządzenie musi mieć możliwość emulacji napędów taśmowych LTO oraz emulacji bibliotek taśmowych.

**ITS.Sprz.76.** Proces deduplikacji musi odbywać się inline – w pamięci urządzenia, przed zapisem danych na nośnik dyskowy. Rozwiązanie nie może w żadnej fazie korzystać (w całości lub częściowo) z dodatkowego bufora na składowanie danych w postaci oryginalnej (niezdeduplikowanej).

**ITS.Sprz.77.** Wszystkie unikalne, zdeduplikowane bloki przed zapisaniem na dysk muszą być kompresowane.

**ITS.Sprz.78.** Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

**ITS.Sprz.79.** Urządzenie musi umożliwiać replikację danych do drugiego urządzenia.

1. Replikacja musi się odbywać w trybie asynchronicznym. Transmitowane muszą być tylko te fragmenty danych (bloki), które nie znajdują się na docelowym urządzeniu.
2. W przypadku wykorzystania portów Ethernet do replikacji urządzenie musi umożliwiać przyjmowanie backupów, odtwarzanie danych, przyjmowanie strumienia replikacji, wysyłanie strumienia replikacji tymi samymi portami.
3. Musi istnieć możliwość ograniczenia pasma używanego do replikacji między dwoma urządzeniami.
4. Zarządzanie całym procesem kopiowania danych oraz wszystkimi kopiami musi być możliwe z poziomu oprogramowania backupowego.
5. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

**ITS.Sprz.80.** Urządzenie musi mieć zaimplementowaną funkcjonalność wewnętrznego mechanizmu szyfrowania danych AES-256 realizowaną na poziomie urządzenia zgodnie ze standardem FIPS 140-2.

**ITS.Sprz.81.** Urządzenie musi automatycznie usuwać przeterminowane dane (bloki danych nienależące do backupów o aktualnej retencji) w procesie czyszczenia.

**ITS.Sprz.82.** Proces usuwania przeterminowanych danych (czyszczenia) nie może uniemożliwiać pracy procesów backupu i odtwarzania danych.

**ITS.Sprz.83.** Musi istnieć możliwość zdefiniowania czasu, w którym wykonywany jest proces usuwania przeterminowanych danych (czyszczenia).

**ITS.Sprz.84.** Urządzenie musi umożliwiać bezpieczne kasowanie składowanych danych zgodnych ze standardem NIST SP 800-88.

**ITS.Sprz.85.** Urządzenie musi mieć możliwość zarządzania poprzez interfejs graficzny dostępny z przeglądarki internetowej oraz poprzez linię komend (CLI) dostępną z poziomu SSH (Secure Shell). Oprogramowanie do zarządzania musi rezydować oferowanym na urządzeniu deduplikacyjnym.

**ITS.Sprz.86.** Urządzenie musi umożliwiać ustawienie powiadomień administratora o problemach w urządzeniu za pomocą poczty elektronicznej.

#### 4.3.6 Macierz dyskowa

Minimum 2 urządzenia, które muszą spełniać wymagania jak poniżej:

- ITS.Sprz.87.** Macierz dyskowa musi posiadać obudowę ze wszystkimi komponentami umożliwiającą montaż w standardowej szafie typu rack 19”.
- ITS.Sprz.88.** Wysokość macierzy oraz każdego z ekspanderów nie może być większa niż 2U.
- ITS.Sprz.89.** Macierzy musi posiadać dwa redundantne kontrolery pracujące w trybie active-active, wymienne bez przerywania pracy.
- ITS.Sprz.90.** Każda z macierzy musi posiadać możliwość skalowalności ilości obsługiwanych dysków poprzez dodanie kolejnej macierzy tego samego typu lub rozbudowę bez konieczności migracji danych, przy zachowaniu jednolitego i wspólnego zarządzania zasobami dyskowymi.
- ITS.Sprz.91.** Ekspandery macierzy muszą posiadać możliwość instalacji minimum 24 dysków 2,5-calowych.
- ITS.Sprz.92.** Macierz musi obsługiwać dyski 2,5" jak i 3,5".
- ITS.Sprz.93.** Macierz musi pozwalać na rozbudowę poprzez dołączenie dodatkowych półek dyskowych zarówno 2,5" jak i 3,5".
- ITS.Sprz.94.** Macierz musi mieć możliwość instalacji dysków SSD, SAS, NL-SAS.
- ITS.Sprz.95.** Macierz musi być wyposażona w minimum 16GB pamięci Cache na kontroler.
- ITS.Sprz.96.** Macierz musi posiadać system podtrzymania zawartości pamięci cache na wypadek awarii zasilania realizowany poprzez zapis danych z pamięci cache kontrolerów do pamięci typu flash lub równoważny zapewniający nieograniczony czas przechowywania danych.
- ITS.Sprz.97.** Macierz musi być wyposażona w minimum 64 dyski SAS min. 10k i min. 1.2TB, gdzie dla każdego dysku przepustowość wynosi minimum 500MB/s.
- ITS.Sprz.98.** Macierz wyposażona musi być w minimum 8 dysków SSD o sumarycznej przestrzeni minimum 32TB, gdzie dla każdego dysku przepustowość minimum 500MB/s.
- ITS.Sprz.99.** Macierz musi posiadać minimum 4 porty FC dla każdego kontrolera, obsadzone modułami światłowodowymi minimum SFP+ 16 Gb/s SR.
- ITS.Sprz.100.** Oferowane urządzenia musi obsługiwać poziomy RAID: 0,1,5, 6 i 10.
- ITS.Sprz.101.** Macierz musi obsługiwać protokół FC - jeśli wymagane są licencje Wykonawca dostarczy je wraz z macierzą.
- ITS.Sprz.102.** Macierz musi posiadać brak pojedynczego punktu awarii oraz musi być wyposażona w redundantne zasilanie, chłodzenie, kontrolery, dwie ścieżki dostępu do każdego dysku.
- ITS.Sprz.103.** Macierz musi być wyposażona w graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie.
- ITS.Sprz.104.** Musi istnieć możliwość bezpośredniego monitoringu stanu, w jakim w danym momencie macierz się znajduje. Dane o parametrach wydajnościowych macierzy muszą być dostępne w postaci wykresów w interfejsie GUI.
- ITS.Sprz.105.** Macierz musi posiadać funkcjonalność zarządzania całością dostępnych zasobów dyskowych, z jednej konsoli administracyjnej.
- ITS.Sprz.106.** Macierz musi posiadać interfejs zarządzający GUI, CLI oraz umożliwiać tworzenie skryptów użytkownika.
- ITS.Sprz.107.** Wymagane jest umożliwienie zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej. Zarządzanie w oparciu o użytkowników z przypisanymi uprawnieniami (rolebased). Musi istnieć możliwość bezpośredniego monitoringu stanu, w jakim w danym momencie każda z macierzy się znajduje.
- ITS.Sprz.108.** Wentylatory i zasilacze każdej macierzy w pełni nadmiarowe, z możliwością wymiany podczas pracy.

- ITS.Sprz.109.** Macierz musi umożliwiać wykonywanie aktualizacji mikrokodu macierzy w trybie online bez przerywania dostępu do zasobów dyskowych macierzy i przerywania pracy aplikacji.
- ITS.Sprz.110.** Macierz musi zapewniać funkcjonalność udostępniania przestrzeni bez konieczności fizycznego alokowania wolnego miejsca na dyskach (thin provisioning). Jeżeli funkcjonalność wymaga licencji, musi taką licencję dostarczyć dla obu macierzy w maksymalnej konfiguracji.
- ITS.Sprz.111.** Macierz musi posiadać funkcjonalność tieringu polegającą na automatycznej migracji bloków danych dysków logicznych pomiędzy różnymi typami dysków fizycznych (SSD, SAS/FC, NLSAS/SATA), w zależności od stopnia wykorzystania danego obszaru przez aplikację. Migracje muszą być wykonywane automatycznie bez udziału administratora. Migracja danych musi odbywać się bez przerywania dostępu do danych od strony hostów i aplikacji. Niezbędne jest dostarczenie licencji na całą dostarczoną pojemność obu macierzy.
- ITS.Sprz.112.** Każda z macierzy musi umożliwiać zwrot zwolnionej przestrzeni dyskowej do puli (Space reclamation).
- ITS.Sprz.113.** Macierz musi umożliwiać automatyczne rozkładanie bloków dysków logicznych pomiędzy wszystkie dostępne dyski fizyczne funkcjonujące w ramach tej samej puli/grupy dyskowej w przypadku rozszerzania dysku logicznego i dokładania dysków fizycznych.
- ITS.Sprz.114.** Macierz musi obsługiwać LUN Masking i Lun mapping. Sterowniki do obsługi wielościżkowego dostępu do wolumenów, awarii ścieżki i rozłożenia obciążenia po ścieżkach dostępu powinny być dostępne dla podłączanych systemów operacyjnych. Jeżeli zastosowanie tych sterowników wymaga licencji, musi być dostarczona dla podłączanych systemów operacyjnych i/lub podłączanych serwerów zależnie od sposobu licencjonowania.
- ITS.Sprz.115.** Macierz musi posiadać funkcjonalność zwiększania rozmiaru wolumenów.
- ITS.Sprz.116.** Macierz musi zapewniać wykonywanie kopii migawkowych.
- ITS.Sprz.117.** Macierzy musi wspierać mechanizm zdalnej replikacji z poziomu macierzy na drugą macierz.
- ITS.Sprz.118.** Oprogramowanie macierzy powinno umożliwiać monitorowanie i raportowanie.

#### 4.3.7 HSM

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

- ITS.Sprz.119.** Sprzętowy moduł kryptograficzny z wbudowanymi minimum 2 interfejsami sieciowymi Ethernet RJ45 wraz z niezbędnym oprogramowaniem, licencjami, kartami elektronicznymi dla administratorów i operatorów urządzeń oraz wsparciem producenta.
- ITS.Sprz.120.** Sieciowy, sprzętowy moduł kryptograficzny HSM certyfikowany zgodnie z FIPS 140-2 Level 3 lub ISO/IEC 15408 EAL4.
- ITS.Sprz.121.** HSM musi zapewnić ochronę przed nieuprawnionym dostępem i powinno znajdować się w bezpiecznej obudowie odpornej na nieuprawnioną ingerencję zewnętrzną nie większą niż 2U, dostosowaną do montażu w szafie stelażowej 19".
- ITS.Sprz.122.** Dostarczone urządzenie musi posiadać wszystkie niezbędne elementy (szyny, uchwyty, śruby, itp.) do zamontowania urządzenia w szafie.
- ITS.Sprz.123.** Urządzenie powinno być wyposażone w zasilanie typu hot-swap 230V.
- ITS.Sprz.124.** Moduł HSM musi posiadać minimum dwa 2 interfejsy Ethernet o szybkości 1 Gb/s.
- ITS.Sprz.125.** HSM musi być w stanie wykonać minimum 450 transakcji na sekundę, gdzie transakcja rozumiana jest jako ilość podpisów cyfrowych wykonywanych algorytmem RSA z kluczem 2048 bitowym.
- ITS.Sprz.126.** Urządzenie musi wspierać przynajmniej następujące algorytmy:
1. Kryptografia symetryczna: AES, DES, Triple DES,
  2. Kryptografia asymetryczna: RSA, ECDSA,
  3. Funkcje skrótu: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512).

**ITS.Sprz.127.** Urządzenie musi pozwalać na tworzenie kopii bezpieczeństwa materiału kryptograficznego przechowywanego w urządzeniu i na jej odtwarzanie.

1. Kopia bezpieczeństwa musi być wykonywana na dedykowane urządzenie zewnętrzne (token, moduł), który może być przechowywany np. w innej lokalizacji.
2. Rozwiązanie powinno pozwalać na wykonywanie kopii bezpieczeństwa w sposób zdalny bez konieczności asysty operatorów bezpośrednio przy urządzeniu.

**ITS.Sprz.128.** Dostarczone wraz z urządzeniem oprogramowanie musi wspierać co najmniej następujące interfejsy aplikacyjne: PKCS#11, Microsoft CryptoAPI/CNG, Java JCE, OpenSSL.

**ITS.Sprz.129.** Zarządzanie urządzeniem musi być dostępne poprzez interfejs graficzny lub komendy wiersza poleceń.

**ITS.Sprz.130.** Dostarczone licencje muszą umożliwiać pracę w konfiguracji wysokiej dostępności (dwa urządzenia w konfiguracji Active-Standby).

#### 4.3.8 Bramka SMS

Minimum 2 sztuki urządzeń, z których każde musi spełniać wymagania jak poniżej:

**ITS.Sprz.131.** Urządzenie musi być wyposażone minimum w następujące złącza: port ethernet RJ45, USB, RS-232.

**ITS.Sprz.132.** Urządzenie musi posiadać wbudowany modem minimum 3G (obsługa kart SIM).

**ITS.Sprz.133.** Urządzenie musi być dostarczone wraz z anteną dookólną 3.5dBi oraz okablowaniem umożliwiającym jej podłączenie.

**ITS.Sprz.134.** Urządzenie musi być wyposażone w zasilacz 230V.

**ITS.Sprz.135.** Urządzenie musi zapewnić realizację następujących funkcji:

1. Wysyłanie, odbiór SMS,
2. Wysyłanie SMS do pojedynczych użytkowników lub grup,
3. Wysyłanie wiadomości o konkretnej porze (harmonogram wysyłek),
4. Tworzenie i przechowywanie szablonów wiadomości,
5. Automatyczna odpowiedź na wysłane wiadomości,
6. Przekierowanie Email na SMS,
7. Przekierowanie SMS na Email,
8. Przekierowanie SMS przychodzących do zewnętrznego skryptu,
9. Interfejs HTTP API do wysyłania i odbioru wiadomości z zewnętrznych programów,
10. Interfejs webowy do zarządzania.

**ITS.Sprz.136.** Wykonawca bez odrębnego wynagrodzenia zapewnia abonament na sms w całym okresie realizacji Umowy.

#### 4.4 Warstwa oprogramowania

##### 4.4.1 Wymagania ogólne

**ITS.Opr.1.** Oprogramowanie standardowe typu COTS zostanie dostarczone wraz z prawem do uzyskiwania jego aktualizacji przez cały okres realizacji Umowy.

##### 4.4.2 Wirtualizator

**ITS.Opr.2.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi być przypisane do każdego rdzenia wszystkich procesorów fizycznych w serwerze lub do każdego procesora fizycznego w serwerze (zgodnie z modelem licencjonowania producenta), w ramach wszystkich dostarczanych serwerów (Serwery Blade)

**ITS.Opr.3.** Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.

- ITS.Opr.4.** Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
- ITS.Opr.5.** Pojedynczy klaster może się skalować do 64 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
- ITS.Opr.6.** Oprogramowanie do wirtualizacji zainstalowane na serwerze fizycznym potrafi obsłużyć i wykorzystać procesory fizyczne.
- ITS.Opr.7.** Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych 1-64 procesorowych.
- ITS.Opr.8.** Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości min. 32 TB.
- ITS.Opr.9.** Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.
- ITS.Opr.10.** Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia min. 4 TB pamięci operacyjnej RAM.
- ITS.Opr.11.** Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
- ITS.Opr.12.** Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-8 wirtualnych kart sieciowych.
- ITS.Opr.13.** Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
- ITS.Opr.14.** Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
- ITS.Opr.15.** Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade).
- ITS.Opr.16.** Rozwiązanie musi wspierać następujące systemy operacyjne: Microsoft Windows, Redhat, SuSE.
- ITS.Opr.17.** Rozwiązanie powinno posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności.
- ITS.Opr.18.** Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach).
- ITS.Opr.19.** Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
- ITS.Opr.20.** Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
- ITS.Opr.21.** Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej (hosta, maszyny wirtualnej) bez potrzeby wyłączania wirtualnych maszyn.
- ITS.Opr.22.** Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
- ITS.Opr.23.** Rozwiązanie musi mieć możliwość przenoszenia zwirtualizowanych dysków maszyn wirtualnych w czasie ich pracy pomiędzy fizycznymi zasobami dyskowymi.
- ITS.Opr.24.** Musi zostać zapewniona odpowiednia redundancja i mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez



administratora i uruchomione na nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym.

**ITS.Opr.25.** Oprogramowanie do wirtualizacji musi zapewniać mechanizm takiego zabezpieczenia wybranych przez administratora wirtualnych maszyn, aby w przypadku awarii lub niedostępności serwera fizycznego maszyny, które na nim pracowały, były bezprzerwowo dostępne na innym serwerze z zainstalowanym oprogramowaniem wirtualizacyjnym. Mechanizm ten umożliwia zabezpieczenie maszyn wirtualnych wyposażonych w minimum 2 wirtualne procesory.

**ITS.Opr.26.** System musi posiadać funkcjonalność wirtualnego przełącznika (ang. virtual switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej.

**ITS.Opr.27.** Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.

**ITS.Opr.28.** Wirtualne przełączniki muszą obsługiwać wirtualne sieci lokalne (VLAN).

**ITS.Opr.29.** Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z kilku dostępnych ścieżek.

#### 4.4.3 Oprogramowanie Kopii Zapasowych

**ITS.Opr.30.** Oprogramowanie do archiwizacji powinno współpracować z dostarczaną infrastrukturą wirtualizacji.

**ITS.Opr.31.** Rozwiązanie musi wspierać backup wszystkich systemów operacyjnych w wirtualnych maszynach, które są wspierane przez dostarczaną infrastrukturę wirtualizacji.

**ITS.Opr.32.** Rozwiązanie powinno mieć możliwość instalacji na dostarczanych systemach operacyjnych oprogramowania serwera kopii zapasowych.

**ITS.Opr.33.** Rozwiązanie powinno mieć możliwość bez agentowego tworzenia kopii zapasowych i odzyskiwania.

**ITS.Opr.34.** Rozwiązanie nie może instalować żadnych swoich komponentów (agent) w archiwizowanych maszynach wirtualnych.

**ITS.Opr.35.** Zamawiający jednocześnie dopuszcza instalację agenta w przypadku backupu maszyn fizycznych.

**ITS.Opr.36.** Rozwiązanie powinno dawać możliwość odzyskiwania całych obrazów maszyn wirtualnych z obrazów, pojedynczych plików z systemu plików znajdujących się wewnątrz wirtualnej maszyny.

**ITS.Opr.37.** Rozwiązanie powinno mieć wbudowane mechanizmy deduplikacji i kompresji archiwum w celu redukcji zajmowanej przez archiwa przestrzeni dyskowej.

**ITS.Opr.38.** Dostęp do konsoli zarządzającej musi być zapewniony za pomocą przeglądarki WWW.

**ITS.Opr.39.** Rozwiązanie powinno mieć możliwość instalacji centralnej konsoli do zarządzania większą ilością serwerów archiwizujących.

**ITS.Opr.40.** Rozwiązanie powinno mieć możliwość rozbudowy procesu archiwizacji o dowolne skrypty tworzone przez administratora i dołączane do zadań archiwizacyjnych.

**ITS.Opr.41.** Dostarczona licencja powinna umożliwić obsługę nielimitowanej ilości maszyn wirtualnych.

**ITS.Opr.42.** Oprogramowanie powinno mieć możliwość tworzenia kopii zapasowych i odzyskiwanie z migawek.

**ITS.Opr.43.** Rozwiązanie musi wspierać backup maszyn fizycznych.

**ITS.Opr.44.** Rozwiązanie powinno posiadać możliwość podłączenia do mechanizmu bibliotek taśmowych LTO6, LTO7, LTO8, nagrywania danych oraz kopii danych bezpośrednio na taśmy backupowe.



**ITS.Opr.45.** Rozwiązanie powinno posiadać możliwość integracji z dostarczonym deduplikatorem.

#### 4.4.4 SIEM

**ITS.Opr.46.** Dostarczone rozwiązanie powinno charakteryzować się następującymi parametrami:

1. Liczba obsługiwanych EPS (Events per Second) to min. 2500,
2. Liczba obsługiwanych FPM (Flows per Minute) to min. 100 000.

**ITS.Opr.47.** Korelacja zdarzeń i informacji o przepływach, wnioskowanie oraz obsługa incydentów, a także prezentacja zdarzeń w architekturze rozproszonej odbywa się na podstawie wszystkich zdarzeń i przepływów składowych niezależnie od miejsca ich kolekcji, a wyniki prezentowane są w jednej wspólnej dedykowanej konsoli.

**ITS.Opr.48.** Zarządzanie oprogramowaniem odbywa się przy użyciu przeglądarki internetowej, nie wymagane jest instalowanie żadnego dedykowanego oprogramowania klienta.

**ITS.Opr.49.** Wspierane przeglądarki internetowe to minimum:

1. Mozilla Firefox,
2. Internet Explorer.

**ITS.Opr.50.** Oprogramowanie udostępnia możliwość prezentacji statystyk i wyników działania systemu SIEM w postaci tzw. „Dashboard” czyli tablic, których wygląd w tym rozkład poszczególnych ekranów składowych daje się przystosować do potrzeb administratora czy też zalogowanego użytkownika.

**ITS.Opr.51.** Obsługiwane przez SIEM przepływy mogą pochodzić jednocześnie z:

1. NetFlow,
2. sFlow,
3. J-Flow.

**ITS.Opr.52.** Kolekcjonowanie zdarzeń, czyli logów odbywa się przynajmniej z zastosowaniem protokołów sieci TCP/IP czy innych mechanizmów jak wymienione poniżej:

1. Syslog,
2. JDBC (Java DataBase Connectivity),
3. JDBC – SiteProtector (Java DataBase Connectivity w połączeniu z oprogramowaniem zarządzania środowiskiem sond IDS/IPS IBM Site Protector),
4. SNMPv1 (Simple Network Management Protocol wersja 1),
5. SNMPv2 (Simple Network Management Protocol wersja 2),
6. SNMPv3 (Simple Network Management Protocol wersja 3),
7. Log File – cykliczne pobieranie plików i importowanie zdarzeń w nim zapisanych do bazy systemu SIEM,
8. Format W3C (Extended Log File Format).

**ITS.Opr.53.** System SIEM pozwala tworzyć wyszukiwanie logów w oparciu o kryteria wraz z możliwością dotarcia do szczegółów zdarzenia (tzw. payload czyli zawartość całego logu) oraz interwału czasowego.

**ITS.Opr.54.** System SIEM pozwala tworzyć graficznie i tekstowo prezentowaną agregację danych z wyszukiwania.

**ITS.Opr.55.** Agregację danych można w sposób interaktywny zmieniać wybierając zarówno inny interwał czasowy, za który dane są agregowane jak i wymiar agregacji.

**ITS.Opr.56.** Każde zdarzenie można otworzyć w dodatkowym oknie prezentującym wszystkie przyporządkowane i dające się przyporządkować pola w bazie danych systemu SIEM dla tego zasobu oraz payload tego zdarzenia

**ITS.Opr.57.** System SIEM umożliwia zapis zdarzeń skompresowany w bazie.

**ITS.Opr.58.** System umożliwia wyłączenie kompresji zdarzeń opisanej wyżej i włączenie zapisu w bazie całego payloadu, zgodnie z ograniczeniami producenta systemu SIEM.

- ITS.Opr.59.** System SIEM pozwala określić sposób retencji dla przechowywanych zdarzeń oraz przepływów i miejsca ich przechowywania w systemie plików rozwiązania SIEM.
- ITS.Opr.60.** Możliwe jest włączenie indeksowania zarówno dla zawartości ang. Payload każdego zdarzenia jak i przepływu. Indeksowanie to pozwala zoptymalizować operacje wyszukiwania podczas analizy logów i przepływów.
- ITS.Opr.61.** System SIEM umożliwia włączenie mechanizmu automatycznego archiwizowania danych i konfiguracji systemu SIEM do katalogu w lokalnym systemie plików i określenie retencji dla przechowywanych w ten sposób danych.
- ITS.Opr.62.** Rozwiązanie pozwala utworzyć strukturę adresacji IP używanej w poszczególnych miejscach sieci i w ten sposób określić adresacje obce. Ta struktura używana jest następnie do określenia kierunków rejestrowanych zdarzeń komunikacji i przepływów.
- ITS.Opr.63.** Rozwiązanie może być skonfigurowane w celu pobierania aktualizacji w sposób automatyczny, w zdefiniowanym przez użytkownika planie.
- ITS.Opr.64.** Rozwiązanie pozwala zdefiniować ustawienia dla uwierzytelnienia i samego działania sesji konsoli takie jak: czas wygaśnięcia sesji, maksymalna liczba nieudanych prób zalogowania i okres trwania interwału, gdy one wystąpiły, czas zablokowania konta po przekroczeniu nieudanej liczby logowań.
- ITS.Opr.65.** Rozwiązanie pozwala zdefiniować szczegółową politykę retencji dla przechowywanych danych w bazie w oparciu o wskazane wartości poszczególnych pól w bazie.
- ITS.Opr.66.** Rozwiązanie pozwala tworzyć grupy dla poszczególnych zdefiniowanych źródeł logów i następnie odwoływanie się do nich podczas tworzenia szablonów wyszukiwania.
- ITS.Opr.67.** Rozwiązanie pozwala gromadzić informację o zasobach widocznych w logach różnych systemów i gromadzonych przepływach.
- ITS.Opr.68.** Rozwiązanie pozwala na integrację z systemami zarządzania podatnościami w celu uzupełnienia informacji o zasobach o bardziej szczegółowe dane do korelacji zdarzeń w oparciu o zidentyfikowane podatności i otwarte porty.
- ITS.Opr.69.** Rozwiązanie pozwala na integrację z produktami do zarządzania podatnościami.
- ITS.Opr.70.** Rozwiązanie zawiera własną bazę adresów IP w Internecie, które rozpoznawane są jako znane źródła Malware, Botnet C&C (Command Control), a także tworzenie własnych zdalnych lub podejrzanych grup adresowych (np. adres pętli 127.0.0.1) i wyzwała incydenty, gdy system SIEM zauważy próby połączeń do tych adresów.
- ITS.Opr.71.** Rozwiązanie pozwala tworzyć reguły wykrywania, gdy aktualna sytuacja odbiega w jakiś sposób od normy w odniesieniu do zdarzeń i przepływów przy pomocy następujących mechanizmów (nie łączy się w tych regułach zdarzeń z przepływami):
1. Porównywanie wielkości odchylenia od wartości średniej przy zastosowaniu agregacji w oparciu o jeden wymiar i obserwacji innej zakumulowanej liczby różnych wartości innego wymiaru (jeden z wymiarów: adres IP źródłowy, adres IP przeznaczenia, nazwa zdarzenia, ilości zdarzeń, priorytetu zdarzeń, kategorii zdarzeń, nazwy protokołu, nazwy użytkownika) w ustalonym przedziale czasowym i jednoczesnym wskazaniu okresu (określonego datą początku i końca lub dni tygodnia i wskazanego przedziału godzin).
  2. Odchylenia przy zastosowaniu agregacji w oparciu o jeden wymiar i obserwacji innej zakumulowanej liczby różnych wartości innego wymiaru (nauczony obserwacją/próbkowaniem) (jeden z wymiarów: adres IP źródłowy, adres IP przeznaczenia, nazwa zdarzenia, ilości zdarzeń, priorytetu zdarzeń, kategorii zdarzeń, nazwy protokołu, nazwy użytkownika), a dokładnie poziomu tej zakumulowanej wartości, trendu (wzrost i spadek) oraz porównanie zakumulowanej wartości tego wymiaru do odpowiadającego mu poziomu w chwili w przeszłości. Reguły te pozwalają określić interwał czasowy (data startu i końca, albo dni o godziny w tygodniu).

3. Przekroczenie ustalonego progu pewnego wymiaru (ilości jego różnych wartości) w stosunku do innego zagregowanego parametru ze wskazaniem długości trwania interwału czasowego albo daty startu i końca, albo dni i godzin w tygodniu.

**ITS.Opr.72.** Rozwiązanie posiada przynajmniej 250 domyślnie dostępnych reguł generujących incydenty bezpieczeństwa na podstawie jednego z poniższych kryteriów, a także ich połączenia logiczne z wykorzystaniem także zaprzeczeń:

1. Reguły incydentów bazujące tylko na zdarzeniach,
2. Reguły incydentów bazujące tylko na przepływach,
3. Reguły incydentów bazujące jednocześnie na przepływach i zdarzeniach,
4. Reguły bazujące na innych incydentach.

**ITS.Opr.73.** System SIEM umożliwia przeglądanie incydentów bezpieczeństwa w odniesieniu do adresów źródłowych IP, adresów IP przeznaczenia, a także incydentów przypisanych do użytkownika, który jest aktualnie zalogowany.

**ITS.Opr.74.** Rozwiązanie umożliwia grupowanie reguł w celu otrzymania tematycznej struktury i łatwego odszukania interesującej reguły.

**ITS.Opr.75.** Dla poszczególnych incydentów prezentowane są najważniejsze informacje takie jak nazwa reguły, która go wywołała, adresy źródłowe i przeznaczenia, a także daje możliwość bezpośredniego otwarcia informacji o zdarzeniach i przepływach, które spowodowały utworzenie tego incydentu, opisanie incydentu notatkami, przypisanie danego incydentu do użytkownika systemu SIEM oraz zamknięcie incydentu.

**ITS.Opr.76.** Dla poszczególnych incydentów prezentowane są także reguły powiązane.

**ITS.Opr.77.** Możliwe jest tworzenie reguł bazujących na samych incydentach i określanie dodatkowych akcji.

**ITS.Opr.78.** Dla reguł możliwe są następujące akcje: przypisanie parametrów częściowych, na podstawie których wyliczana jest wartość priorytetu takiego zdarzenia, utworzenie incydentu prezentowanego w konsoli incydentów i dalsze nim zarządzanie, powołanie kolejnego zdarzenia, wysłanie email pod wskazany adres, wysłanie komunikatu SNMP Trap, wysłanie komunikatu do lokalnego serwera syslog, wysłanie komunikatu do zdefiniowanego serwera np. syslog, powiadomienie w konsoli.

**ITS.Opr.79.** System SIEM gromadzi informacje o działaniach administratorów w szczególności obsłudze incydentów.

**ITS.Opr.80.** Rozwiązanie pozwala tworzyć raporty w oparciu o szablony wyszukiwania wraz z określonym w nich wymiarem agregacji lub też zapisanego trendu poszczególnych wartości w czasie.

**ITS.Opr.81.** Zdefiniowane raporty mogą być generowane regularnie we wskazanym planie czasowym i wysyłane w postaci email na wskazane adresy.

**ITS.Opr.82.** Rozwiązanie pozwala tworzyć raporty w następujących formatach: PDF, HTML, RTF, XML i XLS.

#### 4.4.5 System operacyjny

**ITS.Opr.83.** Serwerowe systemy operacyjne muszą wspierać architekturę x86-64.

**ITS.Opr.84.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi być przypisane do każdego rdzenia wszystkich procesorów fizycznych w serwerze lub do każdego procesora fizycznego w serwerze (zgodnie z modelem licencjonowania producenta), w ramach wszystkich serwerów lub klastra serwerów tego samego typu.

**ITS.Opr.85.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi uprawniać do uruchamiania serwerowego systemu operacyjnego

w środowisku fizycznym i/lub nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego.

- ITS.Opr.86.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi umożliwiać pracę w trybie wysokiej dostępności.
- ITS.Opr.87.** Oprogramowanie musi umożliwiać budowanie klastrów wysokiej dostępności.
- ITS.Opr.88.** Oprogramowanie musi mieć możliwość uruchamiania na maszynach fizycznych lub w środowiskach wirtualnych.
- ITS.Opr.89.** Oprogramowanie musi posiadać wsparcie producenta dostarczanej platformy wirtualizacji.
- ITS.Opr.90.** Serwerowe systemy operacyjne muszą poprawnie współdziałać z dostarczaną platformą sprzętową.
- ITS.Opr.91.** Oprogramowanie musi umożliwiać uruchamianie pozostałych komponentów sprzętu, oprogramowania i aplikacji dostarczanych w ramach zamówienia.
- ITS.Opr.92.** Oprogramowanie musi posiadać możliwość lokalnego autoryzowania dostępu użytkowników.
- ITS.Opr.93.** Oprogramowanie musi wspierać granularny przydział uprawnień.
- ITS.Opr.94.** Oprogramowanie musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
- ITS.Opr.95.** Oprogramowanie musi stosować mechanizmy kryptograficzne do transmisji danych przesyłanych w sieciach publicznych.

#### 4.4.6 Baza Danych

- ITS.Opr.96.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi być przypisane do każdego rdzenia każdego procesora fizycznego w serwerze kasetowym lub do każdego fizycznego procesora w serwerze kasetowym (zgodnie z modelem licencjonowania producenta), w ramach wszystkich serwerów lub klastra serwerów tego samego typu zainstalowanych w obudowie lub do każdego rdzenia maszyny wirtualnej (jeśli Producent licencjonuje takie rozwiązanie).
- ITS.Opr.97.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi uprawniać do użytkowania oprogramowania bazodanowego na każdym fizycznym serwerze kasetowym, w ramach wszystkich serwerów lub klastra serwerów tego samego typu zainstalowanych w obudowie.
- ITS.Opr.98.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi umożliwiać pracę w trybie wysokiej dostępności.
- ITS.Opr.99.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi umożliwiać dostęp do danych dla nielimitowanej liczby użytkowników.
- ITS.Opr.100.** Oprogramowanie musi mieć możliwość uruchamiania na maszynach fizycznych lub w środowiskach wirtualnych.
- ITS.Opr.101.** Oprogramowanie musi być zgodne z serwerowym systemem operacyjnym i oprogramowaniem działającym na maszynach fizycznych.
- ITS.Opr.102.** Oprogramowanie musi być zgodne z serwerowym systemem operacyjnym i oprogramowaniem na maszynach wirtualnych.
- ITS.Opr.103.** Oprogramowanie musi być zgodne z dostarczaniem oprogramowaniem platformy wirtualizacji.
- ITS.Opr.104.** Oprogramowanie musi być zgodne ze standardem ANSI/ISO SQL 2003.
- ITS.Opr.105.** Oprogramowanie musi wspierać protokół JDBC 4.0.

- ITS.Opr.106.** Oprogramowanie musi zapewniać tworzenie archiwów z możliwością odzyskania utraconych danych zarówno z chwili wystąpienia awarii (możliwość odzyskiwania całości lub wybranej części bazy), jak i danych z innego, określonego punktu w czasie.
- ITS.Opr.107.** Oprogramowanie musi zapewniać realizację kopii bezpieczeństwa podczas pracy ciągłej bazy.
- ITS.Opr.108.** Oprogramowanie musi umożliwiać zarządzanie prawami użytkowników określanych poprzez przywileje systemowe (prawo do podłączenia się do bazy danych, utworzenia sesji, prawo do tworzenia tabel) oraz poprzez przywileje dostępu do obiektów aplikacji (odczyt/modyfikacja tabeli, wykonania procedury).
- ITS.Opr.109.** Oprogramowanie musi wspierać granularny przydział uprawnień.
- ITS.Opr.110.** Oprogramowanie musi mieć możliwość lokalnego rejestrowania zdarzeń bezpieczeństwa
- ITS.Opr.111.** Oprogramowanie musi umożliwiać audytowanie zmian danych na poziomie bazy danych.
- ITS.Opr.112.** Oprogramowanie musi umożliwiać audytowanie zmian danych na poziomie bazy danych.
- ITS.Opr.113.** Oprogramowanie musi umożliwiać audytowanie zmian jego konfiguracji.
- ITS.Opr.114.** Oprogramowanie musi pozwalać na wykonywanie typowych zadań administracyjnych (indeksowanie, backup, odtwarzanie danych) bez konieczności przerywania pracy systemu lub przechodzenia w tryb jednon użytkownikowy.
- ITS.Opr.115.** Oprogramowanie musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

#### 4.4.7 Baza Danych dokumentów XML

- ITS.Opr.116.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi być przypisane do każdego rdzenia każdego procesora fizycznego w serwerze kasetowym lub do każdego fizycznego procesora w serwerze kasetowym (zgodnie z modelem licencjonowania producenta), w ramach wszystkich serwerów lub klastra serwerów tego samego typu zainstalowanych w obudowie lub do każdego rdzenia maszyny wirtualnej (jeśli Producent licencjonuje takie rozwiązanie).
- ITS.Opr.117.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi uprawnian do użytkowania oprogramowania bazodanowego na każdym fizycznym serwerze kasetowym, w ramach wszystkich serwerów lub klastra serwerów tego samego typu zainstalowanych w obudowie.
- ITS.Opr.118.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi umożliwiać pracę w trybie wysokiej dostępności.
- ITS.Opr.119.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi umożliwiać dostęp do danych dla nielimitowanej liczby użytkowników.
- ITS.Opr.120.** Oprogramowanie musi zapewniać przechowywania dowolnych dokumentów XML.
- ITS.Opr.121.** Dokument XML jest podstawowym elementem przechowywanym w bazie danych i jego przetwarzanie jest realizowane w oparciu o standardy związane z XML.
- ITS.Opr.122.** Oprogramowanie musi wspierać języki zapytań zorientowane na przetwarzanie dokumentów XML.
- ITS.Opr.123.** Oprogramowanie musi wspierać języki zapytań, które działają na zbiorach dokumentów XML i konstruują dokumenty XML.
- ITS.Opr.124.** Oprogramowanie musi realizować następujące funkcjonalności:
1. Składowanie dokumentów XML,
  2. Definiowanie i przechowywanie schematów (DTD, XML Schema),

3. Obsługa zapytań (XPath, Xquery, XML-QL, Quilt),
4. Obsługa modyfikacji, wstawiania i usuwania dokumentów,
5. Obsługa interfejsów programistycznych (XML:DB API, Xquesry API for Java - XQJ, SAX, DOM, JDOM).

**ITS.Opr.125.** Oprogramowanie musi mieć możliwość uruchamiania na maszynach fizycznych lub w środowiskach wirtualnych.

**ITS.Opr.126.** Oprogramowanie musi być zgodne z serwerowym systemem operacyjnym i oprogramowaniem działającym na maszynach fizycznych.

**ITS.Opr.127.** Oprogramowanie musi być zgodne z serwerowym systemem operacyjnym i oprogramowaniem na maszynach wirtualnych.

**ITS.Opr.128.** Oprogramowanie musi być zgodne z dostarczonym oprogramowaniem platformy wirtualizacji.

**ITS.Opr.129.** Oprogramowanie musi umożliwiać tworzenie archiwów z możliwością odzyskania utraconych danych zarówno z chwili wystąpienia awarii (możliwość odzyskiwania całości lub wybranej części bazy), jak i danych z innego, określonego punktu w czasie.

**ITS.Opr.130.** Oprogramowanie musi umożliwiać tworzenie kopii bezpieczeństwa podczas pracy ciągłej bazy.

**ITS.Opr.131.** Oprogramowanie musi umożliwiać audytowanie zmian jego konfiguracji.

**ITS.Opr.132.** Oprogramowanie musi posiadać możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.

#### 4.4.8 Szyna Danych

**ITS.Opr.133.** Architektura dostarczonego rozwiązania musi być rozszerzalna, czyli musi zapewnić możliwość dodawania nowych modułów/komponentów z zachowaniem koncepcji SOA.

**ITS.Opr.134.** Architektura dostarczonego rozwiązania musi być otwarta, skalowalna, umożliwiająca łatwą rozbudowę w celu obsługi większej liczby integrowanych systemów i komunikacji.

**ITS.Opr.135.** Oprogramowanie wraz z niezbędnymi licencjami (jeżeli dostarczane oprogramowanie ich wymaga) musi uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i/lub nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego.

**ITS.Opr.136.** Rozwiązanie musi być dostarczone w architekturze HA - wysokiej dostępności - każdy komponent rozwiązania powinien być skalowalny.

**ITS.Opr.137.** Rozwiązanie powinno zawierać narzędzia klasy SOA Governance (katalog usług dla architektury SOA).

**ITS.Opr.138.** Rozwiązanie umożliwia budowanie usług agregujących (wywołujących inne usługi).

**ITS.Opr.139.** Funkcjonalności udostępnione na szynie danych w postaci usług, które są dobrze zdefiniowane poprzez kontrakt odpowiedni do użytej technologii (itp. WSDL dla usługi sieciowej, WADL dla usługi REST, itp. – stosownie do protokołu).

**ITS.Opr.140.** Implementacja usług i przepływów komunikatów zgodnych z Enterprise Integration Patterns.

**ITS.Opr.141.** Szyna usług ma obsługiwać różne rodzaje komunikatów, potrafić je transformować, odpytywać i filtrować itp.

**ITS.Opr.142.** Rozwiązanie ma zapewniać obsługę komunikatów co najmniej w formacie – XML, JSON, CSV.

**ITS.Opr.143.** Rozwiązanie ma zapewniać walidację komunikatów na podstawie schemy XSD.

**ITS.Opr.144.** Rozwiązanie ma zapewniać routing oraz filtrowanie komunikatów ze względu na zawartość i nagłówki.



**ITS.Opr.145.** Rozwiązanie ma zapewniać tworzenie adapterów integracyjnych w oparciu o protokoły HTTP/HTTPS, wywołania SOAP, REST.

**ITS.Opr.146.** Rozwiązanie ma zapewniać wsparcie komunikacji wykorzystującej technologie WebService: WSDL 1.1, SOAP 1.1, WS-Addressing, MTOM, WS-Policy, WS-Security.

#### 4.4.9 Serwer aplikacyjny

**ITS.Opr.147.** Oprogramowanie ma posiadać wbudowane wsparcie dla współdzielenia kodu (np. bibliotek) pomiędzy wieloma aplikacjami.

**ITS.Opr.148.** Biblioteki wykorzystane w oprogramowaniu powinny być instalowane w serwerze aplikacyjnym jednokrotnie i wiele aplikacji może z nich korzystać jednocześnie. Musi być zapewniona możliwość zainstalowania wielu bibliotek jednocześnie.

**ITS.Opr.149.** Oprogramowanie musi zapewniać konfigurację komponentów aplikacji webowych za pomocą odpowiedniej adnotacji.

**ITS.Opr.150.** Oprogramowanie musi mieć wbudowaną obsługę żądań HTTP w sposób asynchroniczny.

**ITS.Opr.151.** Oprogramowanie musi mieć wbudowane wsparcie dla przechowywania sesji webowych w bazie i w pamięci.

**ITS.Opr.152.** Oprogramowanie musi zapewniać możliwość przechowywania istotnych informacji dotyczących sesji użytkownika.

**ITS.Opr.153.** Oprogramowanie musi zapewniać wsparcie dla replikacji sesji w pamięci pomiędzy wieloma instancjami serwerów aplikacyjnych uruchomionych na wielu maszynach. Replikacja sesji powinna zapewniać wysoką wydajność.

**ITS.Opr.154.** Oprogramowanie musi mieć wbudowaną możliwość konfiguracji priorytetów obsługi żądań.

**ITS.Opr.155.** Oprogramowanie musi mieć wbudowaną obsługę połączeń do bazy danych z uwierzytelnieniem połączeń.

**ITS.Opr.156.** Oprogramowanie musi mieć wbudowaną obsługę transakcji rozproszonych.

**ITS.Opr.157.** Oprogramowanie musi zapewniać realizację mechanizmów bezpieczeństwa w zakresie: uwierzytelniania, kontroli dostępu, zarządzania użytkownikami, grupami i rolami, tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy.

**ITS.Opr.158.** Oprogramowanie musi umożliwiać audytowanie zdarzeń bezpieczeństwa.

**ITS.Opr.159.** Oprogramowanie musi zapewnić wsparcie dla pojedynczego logowania SSO.

#### 4.4.10 Centralny System Logów

**ITS.Opr.160.** Centralny System Logów ma zapewnić:

1. Zbieranie logów przesyłanych przez systemy operacyjne (Linux/Windows), urządzenia sieciowe oraz aplikacje,
2. Zbieranie danych przesyłanych po sieci (UDP/TCP), oprogramowanie musi rozpoznawać dane przesyłane przez syslog, ng-syslog, netflow,
3. Odbieranie, indeksowanie i przetwarzanie nielimitowanej liczby zdarzeń w ramach wydajności pojedynczego serwera, na którym pracuje.

**ITS.Opr.161.** Rozwiązanie musi mieć wbudowany mechanizm kompresji przechowywanych danych.

**ITS.Opr.162.** Rozwiązanie musi zapewnić parsowanie przesyłanych danych, w tym:

1. Rozpoznawanie formatów czasu i daty, i normalizowanie ich do jednego wspólnego formatu,
2. Konfigurowanie parsowania nieznanych formatów logów w celu umożliwienia analizy zebranych w nich informacji przez opisywane oprogramowanie.

**ITS.Opr.163.** Rozwiązanie ma zapewnić, że zbierane zdarzenia przechowywane będą przez minimum 3 miesiące i dostępne do odczytu na bieżąco.

**ITS.Opr.164.** Rozwiązanie ma zapewnić możliwość archiwizacji logów.

**ITS.Opr.165.** Rozwiązanie ma zapewnić przeszukiwanie zgromadzonych danych, a w szczególności:

1. wyszukiwanie w całym zgromadzonym przez nie zbiorze danych,
2. użycie operatorów boolowskich, wzorców, wyrażeń regularnych (REGEX) do przeszukiwania danych,
3. przeszukiwania w ograniczonym zbiorze danych (np. ze względu na zakres dat wystąpienia).

**ITS.Opr.166.** Rozwiązanie musi posiadać Interfejs obsługiwany z poziomu przeglądarki internetowej.

**ITS.Opr.167.** Rozwiązanie ma zapewnić eksport danych w minimum formatach csv i pdf.

**ITS.Opr.168.** Rozwiązanie ma umożliwić tworzenie raportów z predefiniowanych wyszukiwań w postaci tabelarycznej i graficznej.

#### 4.4.11 Antywirus

**ITS.Opr.169.** Rozwiązanie zapewnia ochronę antywirusową dla wszystkich dostarczanych przez Wykonawcę systemów operacyjnych. Wykonawca zapewnia dostęp do aktualizacji baz wirusów przez cały okres realizacji Umowy.

**ITS.Opr.170.** Ochrona antywirusowa realizowana jest na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki.

**ITS.Opr.171.** Oprogramowanie zapewnia heurystyczną technologię do wykrywania nowych, nieznanych wirusów.

**ITS.Opr.172.** Oprogramowanie zapewnia automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.

**ITS.Opr.173.** Oprogramowanie zapewnia wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „trojan”, „rootkit” oraz ataki typu 0-day.

**ITS.Opr.174.** Oprogramowanie zapewnia pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.

**ITS.Opr.175.** Oprogramowanie zapewnia wbudowaną technologię do ochrony przed rootkitami.

**ITS.Opr.176.** Oprogramowanie zapewnia wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.

**ITS.Opr.177.** Oprogramowanie zapewnia skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.

**ITS.Opr.178.** Oprogramowanie zapewnia możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „trojan” w kwarantannie.

**ITS.Opr.179.** Oprogramowanie zapewnia logowanie zdarzeń podejmowanych wobec wykrytych zagrożeń na chronionych systemach operacyjnych.

**ITS.Opr.180.** Oprogramowanie zapewnia centralną konsolę do zarządzania środowiskiem antywirusowym w tym regułami, kwarantanną, aktualizacjami, powiadomieniami.

**ITS.Opr.181.** Oprogramowanie zapewnia automatyczne powiadomienie administratora o wykrytych zagrożeniach.

**ITS.Opr.182.** Oprogramowanie zapewnia obsługę plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.



- ITS.Opr.183.** Oprogramowanie zapewnia możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.
- ITS.Opr.184.** Oprogramowanie zapewnia możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.
- ITS.Opr.185.** Oprogramowanie zapewnia możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.
- ITS.Opr.186.** Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.
- ITS.Opr.187.** Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta.
- ITS.Opr.188.** Możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na systemach operacyjnych bez dostępu do Internetu.
- ITS.Opr.189.** Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na chronionym systemie operacyjnym pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).
- ITS.Opr.190.** Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy.
- ITS.Opr.191.** Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.
- ITS.Opr.192.** Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.
- ITS.Opr.193.** Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).

#### 4.5 Wydajność

Poniżej przedstawione są prognozowane wartości obliczone na podstawie danych z szpitala średniej wielkości (w skali wszystkich szpitali będących Partnerami projektu).

##### 4.5.1 Liczba realizowanych świadczeń

	Świadczenie	Rocznie	Miesięcznie	Dziennie (pon-sob)	Dziennie (7 dni)	Na godzinę (8-15)	Na godzinę (24h)	Na minutę	Na sekundę
Dane z 1 szpitala za październik 2018	wizyt w AOS	214 320	17 860	714	n.d.	102	n.d.	1,700952381	0,028349206
	w tym: pierwszorazowych	51 000	4 250	170	n.d.	24	n.d.	0,404761905	0,006746032
	w tym: kolejnych	163 320	13 610	544	n.d.	78	n.d.	1,296190476	0,021603175
	Badań obrazowych	66 000	5 500	220	n.d.	31	n.d.	0,5238095	0,008730159
	USG	36 000	3 000	120	n.d.	17	n.d.	0,2857143	0,004761905
Dane z województwa małopols	hospitalizacji w województwie	220 000	18 333	n.d.	611	n.d.	25	0,424382716	0,007073045
	hospitalizacji w 1 szpitalu	5 789	482	19	16	3	1	0,011167966	0,000186133

Tabela nr 4.1 Liczba realizowanych świadczeń

#### 4.5.2 Prognozowane wywołania usług aplikacyjnych

Obszar	Usługa biznesowa	Usługa aplikacyjna	Standardy interoperacyjności	Wywołania usługi aplikacyjnej / sekundę	
				per Partner	całość MSIM
<b>Wymiana dokumentów medycznych</b>	Udostępnianie dokumentów medycznych	Wyszukiwanie dokumentów medycznych	XDS.b wraz z profilami towarzyszącymi	0,017733752	13,08750884
		Pobieranie dokumentów medycznych		0,017733752	13,08750884
		Przechowywanie dokumentów medycznych	n.d.	0,037265498	27,50193741
<b>Diagnostyka obrazowa</b>	Udostępnianie danych obrazowych	Pobieranie danych obrazowych	XDS.I-b z profilami towarzyszącymi	0,008866876	6,543754421
		Przechowywanie danych obrazowych		0,008730159	6,442857143
		Przechowywanie dokumentów związanych z danymi obrazowymi	n.d.	0,008730159	6,442857143
<b>eRejestracja</b>	eRejestracja	Pobieranie wolnych terminów	HL7 FHIR	0,055894309	41,25
		Dokonywanie rezerwacji wizyt		0,055894309	41,25
	Udostępnianie dokumentów medycznych	Wyszukiwanie dokumentów medycznych	XDS.b wraz z profilami towarzyszącymi	0,055894309	41,25
		Pobieranie dokumentów medycznych		0,055894309	41,25
<b>Wszystkie</b>	Zarządzanie identyfikacją pacjentów	n.d.	n.d.	0,093159807	68,75193741

Tabela nr 4.2 Prognozowane wywołania usług aplikacyjnych

#### 4.5.3 Prognozowana wolumetria danych

Nazwa parametru	Wielkość (KB)
Objętość dokumentów wytwarzanych podczas 1 świadczenia	50
Objętość logów towarzyszących 1 świadczeniu	150
<b>RAZEM: Objętość danych wytwarzanych podczas 1 świadczenia</b>	<b>200</b>

Tabela nr 4.3 Prognozowana wielkość elementów danych

	miesięcznie	rocznie
Liczba świadczeń udzielanych w 1 podmiocie	23 842	286 109
Objętość danych wytwarzanych w 1 podmiocie (KB)	4 768 491	57 221 895
Objętość danych wytwarzanych w regionalnym repozytorium MSIM (KB)	3 519 146 526	42 229 758 316
Objętość danych wytwarzanych w regionalnym repozytorium MSIM (GB)	3 356	40 273

*Tabela nr 4.4 Prognozowana wolumetria danych wytwarzanych*

	po upływie pierwszych 5 lat	po upływie kolejnych 5 lat
Objętość danych zgromadzonych w regionalnym repozytorium MSIM (KB)	211 148 791 579	422 297 583 158
Objętość danych zgromadzonych w regionalnym repozytorium MSIM (GB)	201 367	402 734

*Tabela nr 4.5 Prognozowana wolumetria danych gromadzonych*

## Wykaz rysunków

Rysunek nr 2.1 Diagram przypadków użycia obszaru „Zarządzanie danymi pacjenta” .....	9
Rysunek nr 2.2 Diagram aktywności obszaru „Zarządzanie danymi pacjenta” .....	10
Rysunek nr 2.3 Diagram klas obszaru „Zarządzanie danymi pacjenta” .....	11
Rysunek nr 2.4 Diagram klas obszaru „Zgody pacjenta na dostęp do danych” .....	11
Rysunek nr 2.5 Makieta ekranu „Dane pacjenta” .....	12
Rysunek nr 2.6 Makieta ekranu „Zgłoszenie problemu z danymi pacjenta” .....	12
Rysunek nr 2.7 Makieta ekranu „Lista upoważnionych” .....	13
Rysunek nr 2.8 Makieta ekranu „Upoważnienie innego użytkownika” .....	13
Rysunek nr 2.9 Diagram przypadków użycia obszaru „Informacje o placówkach medycznych” .....	14
Rysunek nr 2.10 Diagram klas obszaru „Informacje o placówkach medycznych” .....	14
Rysunek nr 2.11 Makieta ekranu „Lista placówek” .....	15
Rysunek nr 2.12 Makieta ekranu „Opis placówki” .....	16
Rysunek nr 2.13 Diagram przypadków użycia obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	17
Rysunek nr 2.14 Diagram aktywności obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	18
Rysunek nr 2.15 Diagram klas obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	19
Rysunek nr 2.16 Diagram komponentów obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	20
Rysunek nr 2.17 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego” .....	20
Rysunek nr 2.18 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego poza regionem” .....	21
Rysunek nr 2.19 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych” .....	21
Rysunek nr 2.20 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych poza regionem” .....	22
Rysunek nr 2.21 Diagram sekwencji transakcji „Pobieranie wartości słownikowych” .....	22
Rysunek nr 2.22 Makieta ekranu „Dokumenty medyczne pacjenta” .....	23
Rysunek nr 2.23 Makieta ekranu „Dokument medyczny” .....	24
Rysunek nr 2.24 Makieta ekranu „Podgląd opisu badania” .....	25
Rysunek nr 2.25 Makieta ekranu „Podgląd obrazu DICOM” .....	26
Rysunek nr 2.26 Diagram przypadków użycia obszaru „Informacje o udostępnieniach dokumentów” .....	26
Rysunek nr 2.27 Diagram klas obszaru „Informacje o udostępnieniach dokumentów” .....	27
Rysunek nr 2.28 Diagram komponentów obszaru „Portal pacjenta - informacje o udostępnieniach dokumentów” .....	27
Rysunek nr 2.29 Diagram sekwencji transakcji „Wyszukiwanie komunikatów zdarzeń o udostępnieniu dokumentów” .....	28
Rysunek nr 2.30 Makieta ekranu „Lista udostępnień dokumentów” .....	28
Rysunek nr 2.31 Diagram przypadków użycia obszaru „Umawianie wizyt” .....	29
Rysunek nr 2.32 Diagram aktywności obszaru „Umawianie wizyty” .....	30
Rysunek nr 2.33 Diagram klas obszaru „Umawianie wizyt” .....	31
Rysunek nr 2.34 Diagram komponentów obszaru „Portal pacjenta - umawianie wizyt” .....	31
Rysunek nr 2.35 Diagram sekwencji interakcji „Wyszukiwanie wolnych terminów” .....	32
Rysunek nr 2.36 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu” .....	32
Rysunek nr 2.37 Diagram sekwencji transakcji „Wyszukiwanie rezerwacji terminów wizyt” .....	33
Rysunek nr 2.38 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu” .....	33

Rysunek nr 2.39 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu” .....	33
Rysunek nr 2.40 Makieta ekranu „Umawianie wizyt” .....	34
Rysunek nr 2.41 Makieta ekranu „Szczegóły rezerwacji wizyty” .....	34
Rysunek nr 2.42 Makieta ekranu „Wyszukiwanie wolnych terminów” .....	35
Rysunek nr 2.43 Makieta ekranu „Nowa wizyta” .....	35
Rysunek nr 2.44 Diagram przypadków użycia uwzględniający obszar „Wyszukiwanie pacjenta” .....	36
Rysunek nr 2.45 Diagram sekwencji transakcji „Wyszukiwanie danych pacjenta” .....	37
Rysunek nr 2.46 Makieta ekranu „Wyszukiwanie pacjenta” .....	37
Rysunek nr 2.47 Makieta ekranu „Zgłoszenie problemu z danymi pacjenta” .....	38
Rysunek nr 2.48 Diagram przypadków użycia obszaru „Informacje o placówkach medycznych” .....	39
Rysunek nr 2.49 Model danych obszaru „Placówka medyczna” .....	39
Rysunek nr 2.50 Model danych obszaru „Usługi dostępne za pomocą e-Rejestracji regionalnej” .....	40
Rysunek nr 2.51 Makieta ekranu „Lista placówek” .....	40
Rysunek nr 2.52 Makieta ekranu „Opis placówki” .....	41
Rysunek nr 2.53 Diagram przypadków użycia uwzględniający obszar „Wyszukiwanie i pobieranie dokumentów medycznych” .....	43
Rysunek nr 2.54 Diagram aktywności obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	44
Rysunek nr 2.55 Diagram klas obszaru „Wyszukiwanie i pobieranie dokumentów medycznych” .....	45
Rysunek nr 2.56 Diagram sekwencji transakcji „Pobieranie wartości słownikowych” .....	46
Rysunek nr 2.57 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych pacjenta” .....	46
Rysunek nr 2.58 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych pacjenta poza regionem” .....	47
Rysunek nr 2.59 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego” .....	47
Rysunek nr 2.60 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego poza regionem” .....	48
Rysunek nr 2.61 Makieta ekranu „Dokumenty medyczne pacjenta” .....	48
Rysunek nr 2.62 Makieta ekranu „Dokument medyczny” .....	49
Rysunek nr 2.63 Makieta ekranu „Dokument medyczny dla opisu badania obrazowego” .....	50
Rysunek nr 2.64 Makieta ekranu „Przeglądarka obrazów diagnostycznych” .....	51
Rysunek nr 2.65 Diagram przypadków użycia obszaru „Digitalizacja dokumentu medycznego” .....	52
Rysunek nr 2.66 Diagram aktywności obszaru „Digitalizacja dokumentu medycznego” .....	52
Rysunek nr 2.67 Makieta ekranu „Digitalizacja dokumentu medycznego” .....	53
Rysunek nr 2.68 Makieta ekranu „Modyfikacja dokumentu digitalizowanego” .....	53
Rysunek nr 2.69 Diagram przypadków użycia obszaru „Umawianie wizyt” .....	54
Rysunek nr 2.70 Diagram aktywności obszaru „Umawianie wizyt” .....	55
Rysunek nr 2.71 Diagram klas obszaru „Umawianie wizyt” .....	56
Rysunek nr 2.72 Diagram komponentów obszaru „Umawianie wizyt” .....	56
Rysunek nr 2.73 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów” .....	57
Rysunek nr 2.74 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu” .....	57
Rysunek nr 2.75 Diagram sekwencji transakcji „Wyszukiwanie rezerwacji terminów wizyt” .....	58
Rysunek nr 2.76 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu” .....	58
Rysunek nr 2.77 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu” .....	58
Rysunek nr 2.78 Makieta ekranu „Umawianie wizyt” .....	59
Rysunek nr 2.79 Makieta ekranu „Szczegóły rezerwacji wizyty” .....	59
Rysunek nr 2.80 Makieta ekranu „Wyszukiwanie wolnych terminów” .....	60
Rysunek nr 2.81 Makieta ekranu „Nowa wizyta” .....	60
Rysunek nr 3.1 Diagram przypadków użycia obszaru „Regionalna baza pacjentów” .....	69

Rysunek nr 3.2 Diagram aktywności obszaru „Wyszukiwanie rekordu pacjenta” .....	69
Rysunek nr 3.3 Diagram aktywności obszaru „Dodawanie rekordu pacjenta” .....	70
Rysunek nr 3.4 Diagram aktywności obszaru „Modyfikacja rekordu pacjenta” .....	70
Rysunek nr 3.5 Diagram aktywności obszaru „Zgłoszenie podwójnego rekordu pacjenta” .....	71
Rysunek nr 3.6 Diagram klas obszaru „Pacjent” .....	71
Rysunek nr 3.7 Diagram klas obszaru „Zgłoszenie podwójnego rekordu pacjenta” .....	71
Rysunek nr 3.8 Diagram klas obszaru "Regionalna baza pacjentów" .....	72
Rysunek nr 3.9 Diagram sekwencji transakcji „Dodawanie rekordu pacjenta” .....	73
Rysunek nr 3.10 Diagram sekwencji transakcji „Modyfikacja rekordu pacjenta” .....	74
Rysunek nr 3.11 Diagram sekwencji transakcji „Wyszukiwanie rekordu pacjenta” .....	74
Rysunek nr 3.12 Diagram sekwencji transakcji „Wyszukiwanie rekordu pacjenta dla aplikacji mobilnych” .....	75
Rysunek nr 3.13 Diagram sekwencji transakcji „Zgłoszenie połączenia zdublowanych rekordów pacjenta” .....	75
Rysunek nr 3.14 Diagram sekwencji "Przekazywanie zbioru dokumentów do repozytorium i jego rejestracja" .....	76
Rysunek nr 3.15 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena regionalna)" .....	77
Rysunek nr 3.16 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena regionalna, tryb zgody pacjenta)" .....	78
Rysunek nr 3.17 Diagram sekwencji "Wyszukiwanie i pobieranie dokumentu (domena krajowa)" ....	79
Rysunek nr 3.18 Diagram przypadków użycia komponentu „Regionalny rejestr dokumentów” .....	80
Rysunek nr 3.19 Diagram aktywności obszaru „Wyszukiwanie dokumentów” .....	81
Rysunek nr 3.20 Diagram aktywności obszaru „Rejestrowanie dokumentów” .....	81
Rysunek nr 3.21 Diagram klas obszaru „Dokument medyczny” .....	82
Rysunek nr 3.22 Diagram klas składających się na złożoną klasę XDSDocumentEntry .....	82
Rysunek nr 3.23 Diagram klas składających się na złożoną klasę XDSSubmission Set .....	83
Rysunek nr 3.24 Diagram klas składających się na złożoną klasę XDSAuthor .....	83
Rysunek nr 3.25 Diagram klas składających się na złożoną klasę XDSSubmissionSetIntendedRecipient .....	84
Rysunek nr 3.26 Diagram komponentów obszaru „Regionalny rejestr dokumentów medycznych” ...	84
Rysunek nr 3.27 Diagram sekwencji transakcji „Rejestrowanie zbioru dokumentów medycznych” ...	85
Rysunek nr 3.28 Diagram sekwencji transakcji „Weryfikacja uprawnień do dokumentów medycznych” .....	85
Rysunek nr 3.29 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych” .....	86
Rysunek nr 3.30 Diagram sekwencji transakcji „Wyszukiwanie dokumentów medycznych dla aplikacji mobilnych” .....	86
Rysunek nr 3.31 Diagram przypadków użycia obszaru „Regionalne repozytorium dokumentów medycznych” .....	88
Rysunek nr 3.32 Diagram aktywności obszaru „Pobieranie dokumentu z repozytorium” .....	89
Rysunek nr 3.33 Diagram aktywności obszaru „Zapisywanie dokumentu w repozytorium” .....	90
Rysunek nr 3.34 Model danych obszaru „Plik dokumentu medycznego” .....	91
Rysunek nr 3.35 Model danych obszaru "Konfiguracja wielodomenowości" .....	91
Rysunek nr 3.36 Diagram komponentów obszaru „Regionalne repozytorium dokumentów medycznych” .....	92
Rysunek nr 3.37 Diagram sekwencji transakcji „Pobieranie zbioru dokumentów medycznych” .....	92
Rysunek nr 3.38 Diagram sekwencji transakcji „Pobieranie dokumentu medycznego dla aplikacji mobilnych” .....	93

Rysunek nr 3.39 Diagram sekwencji transakcji „Rejestrowanie zbioru dokumentów medycznych (domena MSIM)”	93
Rysunek nr 3.40 Diagram sekwencji transakcji "Rejestrowanie zbioru dokumentów medycznych (domena krajowa)"	94
Rysunek nr 3.41 Diagram sekwencji transakcji „Przesłanie zbioru dokumentów w celu walidacji”	94
Rysunek nr 3.42 Diagram sekwencji transakcji „Przekazywanie dokumentu medycznego w celu jego zapisania w repozytorium”	95
Rysunek nr 3.43 Diagram sekwencji transakcji „Przesłanie dokumentu w celu ekstrakcji danych dla ich wtórnego wykorzystania”	95
Rysunek nr 3.44 Diagram sekwencji transakcji „Weryfikacja uprawnień do dokumentów medycznych (domena MSIM)”	96
Rysunek nr 3.45 Diagram sekwencji transakcji "Weryfikacja uprawnień do dokumentów medycznych (domena MSIM)"	96
Rysunek nr 3.46 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena regionalna)"	97
Rysunek nr 3.47 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena regionalna, tryb zgody pacjenta)"	98
Rysunek nr 3.48 Diagram sekwencji transakcji "Wyszukiwanie i pobieranie dokumentu (domena krajowa)"	99
Rysunek nr 3.49 Diagram przypadków użycia obszaru „Walidator dokumentów medycznych”	100
Rysunek nr 3.50 Diagram aktywności obszaru „Walidator dokumentów medycznych”	101
Rysunek nr 3.51 Diagram klas obszaru "Specyfikacje pochodne standardów"	102
Rysunek nr 3.52 Diagram komponentów obszaru „Walidator dokumentów medycznych”	102
Rysunek nr 3.53 Diagram sekwencji transakcji „Przesłanie dokumentu w celu walidacji”	103
Rysunek nr 3.54 Diagram przypadków użycia obszaru „Komponent wtórnego wykorzystania danych”	104
Rysunek nr 3.55 Diagram aktywności obszaru „Mechanizm generowania rekordu danych”	104
Rysunek nr 3.56 Diagram aktywności obszaru „Realizacja zapytania AQL”	105
Rysunek nr 3.57 Diagram klas obszaru „Zbiór danych jednostkowych”	105
Rysunek nr 3.58 Diagram klas obszaru „Mapowanie struktury CDA na dane jednostkowe”	106
Rysunek nr 3.59 Diagram komponentów obszaru „Komponent wtórnego wykorzystania danych”	107
Rysunek nr 3.60 Diagram sekwencji transakcji „Przesłanie dokumentu w celu ekstrakcji danych dla ich wtórnego wykorzystania”	107
Rysunek nr 3.61 Diagram sekwencji transakcji „Wykonanie spersonalizowanego zapytania AQL”	108
Rysunek nr 3.62 Diagram sekwencji transakcji „Wykonanie zdepersonalizowanego zapytania AQL”	108
Rysunek nr 3.63 Diagram sekwencji transakcji „Pobieranie danych ratunkowych dla pacjenta”	108
Rysunek nr 3.64 Aktorzy i transakcje obszaru „eRejestracja”	109
Rysunek nr 3.65 Diagram klas obszaru „Regionalny broker wolnych terminów i rezerwacji”	110
Rysunek nr 3.66 Diagram komponentów obszaru „Regionalny broker wolnych terminów i rezerwacji”	111
Rysunek nr 3.67 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów”	111
Rysunek nr 3.68 Diagram sekwencji transakcji „Wyszukiwanie wolnych terminów wizyt”	112
Rysunek nr 3.69 Diagram sekwencji transakcji „Tworzenie rezerwacji wolnego terminu”	112
Rysunek nr 3.70 Diagram sekwencji transakcji „Modyfikacja rezerwacji wolnego terminu”	113
Rysunek nr 3.71 Diagram sekwencji transakcji „Anulowanie rezerwacji wolnego terminu”	113
Rysunek nr 3.72 Diagram przypadków użycia obszaru „Regionalne repozytorium zdarzeń na potrzeby audytu”	114
Rysunek nr 3.73 Diagram klas obszaru „Komunikat zdarzenia dla celów audytu”	115



Rysunek nr 3.74 Diagram komponentów obszaru „Regionalne repozytorium zdarzeń na potrzeby audytu” .....	116
Rysunek nr 3.75 Diagram sekwencji transakcji „Zapisywanie komunikatu zdarzenia na potrzeby audytu” .....	117
Rysunek nr 3.76 Diagram sekwencji transakcji „Wyszukiwanie komunikatów zdarzeń” .....	117
Rysunek nr 3.77 Diagram przypadków użycia obszaru „Regionalna bramka wymiany dokumentów” .....	118
Rysunek nr 3.78 Diagram komponentów obszaru „Regionalna bramka wymiany dokumentów” .....	118
Rysunek nr 3.79 Diagram sekwencji transakcji „Przekazywanie żądania wyszukania zbioru dokumentów do bramki w innej domenie” .....	119
Rysunek nr 3.80 Diagram sekwencji transakcji „Przekazywanie żądania pobrania zbioru dokumentów do bramki w innej domenie” .....	119
Rysunek nr 3.81 Diagram przypadków użycia obszaru „Placówki, grafiki i usługi medyczne” .....	121
Rysunek nr 3.82 Diagram przypadków użycia obszaru „Zarządzanie użytkownikami Portalu pacjenta” .....	121
Rysunek nr 3.83 Diagram przypadków użycia obszaru „Zarządzanie użytkownikami Portalu pracownika medycznego” .....	122
Rysunek nr 3.84 Diagram przypadków użycia obszaru „Zarządzanie rolami i uprawnieniami” .....	122
Rysunek nr 3.85 Diagram przypadków użycia obszaru „Zarządzanie zgodami pacjenta na dostęp do danych” .....	123
Rysunek nr 3.86 Diagram klas obszaru „Placówka medyczna” .....	123
Rysunek nr 3.87 Diagram klas obszaru „Pracownik medyczny” .....	124
Rysunek nr 3.88 Diagram klas obszaru „Uprawnienia” .....	124
Rysunek nr 3.89 Diagram klas obszaru „Usługi dostępne za pomocą e-Rejestracji regionalnej” .....	125
Rysunek nr 3.90 Diagram klas obszaru „Użytkownik portalu pacjenta” .....	125
Rysunek nr 3.91 Diagram klas obszaru „Konfiguracja trybów wymiany dokumentów” .....	126
Rysunek nr 3.92 Diagram klas obszaru „Zgoda pacjenta na dostęp do danych” .....	126
Rysunek nr 3.93 Diagram klas obszaru „Konfiguracja wymiany międzyregionalnej XCA” .....	127
Rysunek nr 3.94 Diagram komponentów obszaru „Komponent administracyjny MSIM” .....	127
Rysunek nr 3.95 Diagram sekwencji transakcji „Pobieranie wartości słownikowych” .....	128
Rysunek nr 3.96 Diagram sekwencji transakcji „Przekazywanie informacji o definicjach grafików” .....	128
Rysunek nr 3.97 Diagram sekwencji transakcji „Wyszukiwanie placówek medycznych” .....	129
Rysunek nr 3.98 Diagram sekwencji transakcji „Wyszukiwanie pracowników medycznych” .....	129
Rysunek nr 3.99 Diagram sekwencji transakcji „Wyszukiwanie usług medycznych” .....	129

## Wykaz tabel

Tabela nr 1.1 Definicja oznaczeń wymagań .....	8
Tabela nr 4.1 Liczba realizowanych świadczeń .....	170
Tabela nr 4.2 Prognozowane wywołania usług aplikacyjnych .....	171
Tabela nr 4.3 Prognozowana wielkość elementów danych .....	171
Tabela nr 4.4 Prognozowana wolumetria danych wytwarzanych .....	172
Tabela nr 4.5 Prognozowana wolumetria danych gromadzonych .....	172