Politechnika Poznańska
Wydział Informatyki i Zarządzania
Instytut Informatyki

Praca dyplomowa magisterska

PLATFORMA INTEGRACJI SYSTEMÓW MEDYCZNYCH OPARTA NA SOA

Stanisław Czajka, Maciej Piernik

Promotor
dr inż. Jacek Kobusiński

Poznań, 2010 r.

Tutaj przychodzi karta pracy dyplomowej;
oryginał, wstawiamy do wersji dla archiwum PP, w pozostałych kopiach wstawiamy ksero.

Spis treści

Rozdział 1

Wstęp

Współczesny system opieki zdrowotnej stanowi źródło dużej ilości danych medycznych. Dokumentacja dotycząca pacjenta składa się z danych jednocześnie dokładnych i zróżnicowanych, ale przede wszystkim niezbędnych do organizacji procesu leczenia [USTd]. Szczególnie istotna jest pod tym względem historia zdrowia i choroby pacjenta, zawierająca diagnozy lekarzy pierwszego kontaktu, wyniki badań laboratoryjnych oraz szczegółowe opisy przebiegu hospitalizacji i świadczeń ambulatoryjnych. Wspomaganie zarządzania i kontrolowanej wymiany tych informacji jest kluczowe dla sprawnego współdziałania jednostek medycznych.

Istnieje wiele złożonych szpitalnych systemów informacyjnych (*HIS*, ang. *Hospital Information System*), które pozwalają na prowadzenie *Elektronicznej Kartoteki Pacjenta* (*EHR*, ang. *Electronic Health Record*). Jednak sposoby przechowywania w nich danych są bardzo zróżnicowane. Wyraźna jest potrzeba standaryzacji modelu reprezentacji danych, aby umożliwić udostępnianie informacji w jednolity sposób oraz efektywną integrację istniejących systemów HIS. Niezbędne jest także zdefiniowanie mechanizmów komunikacji między zakładami opieki zdrowotnej, aby wymieniać i udostępniać dane w bezpieczny sposób.

Sposób przechowywania dokumentacji medycznej jest określony przez odpowiednie rozporządzenia Ministra Zdrowia [USTc, §44]. Dane te należą do szczególnie chronionych danych osobowych i powinny być składowane w miejscach ich ewidencji. Znacznie utrudnione jest tworzenie scentralizowanych repozytoriów, a potrzebne są systemy mediacyjne o rozproszonej strukturze.

Systemy takie często budowane są w architekturze zorientowanej na usługi (*SOA*, ang. *Service Oriented Architecture*). Jej założeniem jest komponowanie zbioru usług sieciowych o prostym i dobrze opisanym interfejsie. Pozwala to tworzyć złożone i rozszerzalne mechanizmy integracji, adaptowalne do indywidualnych potrzeb poszczególnych jednostek medycznych.

Cel przedsięwzięcia

Celem projektu *Platforma Integracji Systemów Medycznych oparta na SOA* jest zaprojektowanie oraz implementacja systemu, umożliwiającego integrację danych medycznych pochodzących z różnych źródeł, zgodnie z paradygmatem *SOA*.

Aplikacja będzie wykorzystywała mechanizmy lokalizacji dostępnych informacji w poszczególnych systemach informatycznych jednostek medycznych. Właściwe dane o pacjencie zostaną także podzielone na podzbiory. Będą one mogły być udostępniane przez pacjenta w sposób niezależny na określonych przez niego zasadach. Osoba żądająca dostępu będzie musiała spełnić zasady autoryzacji w celu uzyskania dostępu do określonych zbiorów danych. W efekcie powstanie rozproszone repozytorium, przechowujące dane medyczne w miejscach ich ewidencji, a zawierające wskazania do lokalizacji, w których można znaleźć informacje dotyczące poszczególnych pacjentów.

Wykonana zostanie analiza standardów reprezentacji oraz wymiany danych medycznych. Ze względu na dużą liczbę możliwych wyborów, zakłada się, że dane będą wymieniane z wykorzystaniem istniejących standardów. Z punktu widzenia technologicznego, pozwoli to na swobodne udostępnianie dokumentacji pomiędzy zakładami opieki zdrowotnej.

Tworzona platforma stanowi prototyp *Obszaru Aplikacyjnego* (*OA2-3*) w międzyuczelnianym projekcie *ITSOA* [SITf], dotyczącym współczesnych technologii informacyjnych w systemach rozproszonych. Technologie te, oparte na paradygmacie SOA, są rozwijane w celu informatyzacji procesów biznesowych i tworzenia platform usługowych. Udział w tym projekcie narzuca na przedsięwzięcie ograniczenia koncepcyjne i technologiczne, jednak z drugiej strony zwiększa szanse na stworzenie stabilnego produktu rynkowego z profesjonalnym wsparciem.

Struktura pracy

Kolejne rozdziały posiadają następującą strukturę. Drugi rozdział pracy przedstawia istniejące rozwiązania oraz analizę standardów reprezentacji i wymiany danych medycznych. W rozdziale trzecim opisano model biznesowy, a także szczegółowo wyspecyfikowano wymagania funkcjonalne i pozafunkcjonalne brane pod uwagę podczas projektowania usług. Rozdział czwarty omawia realizację techniczną projektu. Opisano w nim aspekty dotyczące architektury systemu oraz implementacji poszczególnych usług i przykładowych aplikacji. Ostatni rozdział stanowi podsumowanie wykonanej pracy oraz propozycję przyszłego rozwoju.

W ramach opisywanej pracy Stanisław Czajka wykonał analizę standardów wymiany danych medycznych oraz zaprojektował mechanizmy związane z zarządzaniem tożsamością pacjenta i bezpieczeństwem. Maciej Piernik opracował porównanie standardów reprezentacji dokumentacji medycznej oraz zaimplementował elementy systemu odpowiedzialne za obieg danych i metadanych medycznych.

Rozdział 2

Przetwarzanie danych medycznych

2.1 Istniejące rozwiązania

Najbardziej znane projekty związane z integracją danych medycznych prowadzone są na terenie USA. Rozwijają one systemy *PHR* (ang. *Personal Health Record*) i wspomagają komunikację pomiędzy usługodawcami, urządzeniami oraz pacjentami. Przede wszystkim jednak umożliwiają one pacjentom samodzielne zarządzanie ich dokumentacją medyczną, co w przeciwieństwie do zarządzania EHR przez zakłady opieki zdrowotnej nie jest ściśle opisane przez ustawy i rozporządzenia.

Do najbardziej popularnych systemów należą:

Google Health

Google Health jest usługą, która pozwala zarówno na samodzielne wprowadzanie danych, jak też ich importowanie z różnorodnych systemów, w których pacjent jest zarejestrowany. Zebrane dane pacjent może udostępniać poprzez aplikację Google oraz eksportować do innych systemów [SITd].

Microsoft Health Vault

Microsoft Health Vault to platforma stworzona przez firmę Microsoft, która pozwala na współpracę jednostek medycznych, producentów aplikacji oraz urządzeń związanych z ochroną zdrowia i fitnessem. Tak jak w usłudze Google, głównym celem projektu jest umożliwienie pacjentom organizację i udostępnianie danych medycznych [SITg].

Dossia

Projekt *Dossia* został utworzony przez grupę firm (m.in. AT&T, Intel, BP America i Walmart) i jest rozwijany jako oprogramowanie open-source. Tworzy aplikację *Personal Health Platform*, która zrzesza użytkowników indywidualnych umożliwiając zarządzanie danymi oraz pracodawców dla aktywnego uczestnictwa we wspomaganiu opieki zdrowotnej zatrudnionych [SITc].

Również w Polsce rozwijane są systemy, których celem jest wymiana danych medycznych. Najczęściej tworzone są produkty specjalizowane do wymiany wyników i opinii radiologicznych pomiędzy zakładami opieki zdrowotnej. Istnieją także systemy, w których podstawowym użytkownikiem jest pacjent. Przykładem jest wprowadzony przez Wielkopolski Oddział Wojewódzki NFZ *Zdrowotny Informator Pacjenta* [SITi]. Jest to system dedykowany dla osób ubezpieczonych w Narodowym Funduszu Zdrowia, który udostępnia informacje zgromadzone m.in. poprzez rozliczenia placówek medycznych z NFZ. Są to dane o wykonanych świadczeniach i refundowanych lekach, a także informacje związane z ubezpieczeniem oraz na temat wyboru lekarza podstawowej

opieki zdrowotnej. Nie prowadzi on jednak ewidencji danych typowo medycznych, które mogłyby być pełnym źródłem informacji np. dla lekarzy.

Brak jest rozpowszechnionych i uniwersalnych rozwiązań, których głównym celem jest udostępnianie dokumentacji medycznej pacjentowi. Wyraźna jest potrzeba stworzenia systemu spełniającego rolę uniwersalnego archiwum, niezależnego od typu dokumentacji, rodzaju zakładu opieki zdrowotnej lub ubezpieczenia pacjenta.

2.2 Standardy

Obecnie dane medyczne o pacjentach w różnych jednostkach opieki zdrowotnej przechowywane są w sposób niejednolity. Taki stan nie sprzyja integracji danych pacjenta i w efekcie poprawie opieki, co jest jednym z kluczowych zadań informatyki w medycynie. Dlatego też postanowiono ujednolicić sposób reprezentacji oraz wymiany danych medycznych o pacjentach wprowadzając *Elektroniczną Kartotekę Pacjenta*. Według definicji podanej w [Iak98] Elektroniczna Kartoteka Pacjenta, znana w skrócie jako *EHR* (ang. *Electronic Health Record*), to „cyfrowo przechowywane dane medyczne z całego życia pacjenta, mające wspomagać ciągłość opieki oraz badania naukowe, z jednoczesnym zapewnieniem ich poufności".

Do opracowania standardów EHR przystąpiło równocześnie wiele organizacji, z których każda definiuje sposób ustrukturalizowania danych medycznych pacjenta, by można je było efektywnie wymieniać i integrować. Najważniejszymi organizacjami w tej dziedzinie są *HL7* [SITe], *CEN* [SITb] oraz *ACR* [SITa] i *NEMA* [SITh], które opracowują one niezależnie trzy standardy: *HL7*, *EHRcom* oraz *DICOM*. Pomimo, iż zakresy zastosowania tych standardów oraz ich realizacja są bardzo podobne, istnieją pomiędzy nimi zasadnicze różnice, wynikające z różnych charakterów tworzących je organizacji. HL7 rozpoczynało swoją działalność na terenie Stanów Zjednoczonych, podczas gdy EHRcom jest tworzony w Europie. DICOM natomiast powstawał jako standard w dziedzinie radiologii. Szczegółowy opisy wymienionych standardów oraz podobieństwa i różnice pomiędzy nimi zostały opisane poniżej.

2.2.1 HL7

HL7 jest amerykańską organizacją zajmującą się tworzeniem międzynarodowych standardów związanych z ochroną zdrowia. Nazwa HL7 (ang. *Health Level Seven*) pochodzi od siódmej warstwy modelu ISO OSI [ISOa], której dotyczą rozwijane standardy, czyli warstwy aplikacji. Jest to najwyższa warstwa tego modelu, zajmująca się definicją protokołów komunikacji pomiędzy aplikacjami.

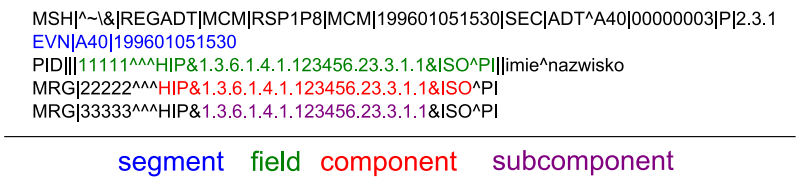
Część komunikacyjna

HL7 jest standardem elektronicznej wymiany informacji w środowiskach medycznych. Wersje 2. standardu, rozwijane od roku 1987, obejmują edycje 2.1, 2.2, 2.3, 2.3.1, 2.4, 2.5, 2.5.1, 2.6 określane razem jako 2.x. Co jest bardzo istotne dla współpracy różnych systemów informatycznych, standardy w tej wersji zachowują wsteczną kompatybilność. Wykorzystują one tekstową składnię komunikatów opierających się na hierarchicznej strukturze separatorów. Definiują grupy zdarzeń i przyporządkowanych im komunikatów związanych z wieloma aspektami funkcjonowania jednostek medycznych m.in.:

- wymianą danych o pacjencie i jego wizytach [HL799, Rozdział 3.],
- zleceniami usług medycznych [HL799, Rozdział 4.],

- rozliczeniami [HL799, Rozdział 6.],
- konsultacjami badań diagnostycznych [HL799, Rozdział 7.],
- harmonogramowaniem [HL799, Rozdział 10.],
- skierowaniami pacjentów [HL799, Rozdział 11.].

Standard ten definiuje także strukturę komunikatów: segmenty, pola oraz komponenty, a także zawarte w nich złożone lub proste typy danych. Przykładowy komunikat HL7 zaprezentowano na Rysunku 2.1 (kolorami oznaczono struktury składowe komunikatu).



Rysunek 2.1: Przykładowy komunikat HL7 v2.x.

Istnieje także standard HL7 w wersji 3, definiujący schemat XML dla komunikatów i dokumentów. Opiera się na modelu referencyjnym (*RIM*, ang. *Reference Information Model*) i definiuje nie tylko komunikaty do przesyłania danych, ale także standard ich przechowywania (*CDA*, ang. *Clinical Document Architecture*) omówiony poniżej.

HL7 CDA

HL7 CDA Release 2 [HL7], jako część standardu HL7 v3, definiuje strukturę dokumentów medycznych, która umożliwia ich łatwą wymianę w formacie XML [W3Ca]. Struktura ta wywodzi się bezpośrednio z HL7 RIM, więc zapewnia stosunkową łatwość integracji z systemami wykorzystującymi ten model.

Każdy dokument składa się z dwóch głównych części: nagłówka (*CDA Header*) oraz ciała (*CDA Body*). Nagłówek zawiera administracyjną część dokumentu, m.in.: typ, format zawartości, język i datę powstania dokumentu, dane identyfikujące pacjenta, autorów dokumentu, organizację w której dokument powstał. Ciało zawiera natomiast informacje medyczne o pacjencie, które mogą wystąpić na trzech poziomach ustrukturalizowania:

CDA Level One
: Ciało dokumentów na tym poziomie może mieć dowolny układ: od w pełni przetwarzalnego komputerowo do prostego tekstu lub nawet gotowej do wyświetlenia strony jako HTML.

CDA Level Two
: Na poziomie drugim ciała dokumentów muszą być podzielone na sekcje i do tego stopnia ustrukturalizowane, jednak nadal mogą zawierać prosty tekst wewnątrz opisów.

CDA Level Three
: Poziom trzeci wprowadza pełną zgodność z HL7 RIM do ciała dokumentu. Oznacza to, iż wszystkie informacje medyczne w nim zawarte są opisane odpowiednimi znacznikami, które umożliwiają w pełni automatycznie przetworzyć taki dokument przez komputer.

Taki podział jest bardzo dobrą cechą tego standardu, gdyż zmiany w środowiskach medycznych muszą zachodzić niezauważalnie i bardzo płynnie, z dużą wsteczną kompatybilnością. Różne poziomy dokumentów pozwalają właśnie na płynne przechodzenie od prostego tekstu do bardziej ustrukturalizowanych form reprezentacji informacji medycznej.

Ponieważ dokumenty w standardzie HL7 CDA zapisane są w formacie XML, ich strukturę można przedstawić za pomocą hierarchii znaczników. Głównym znacznikiem każdego dokumentu jest `<ClinicalDocument>`, który na początku zawiera część nagłówka, wspólną dla wszystkich poziomów. Różnice pomiędzy poszczególnymi poziomami ujawniają się dopiero w części ciała dokumentu.

Hierarchia znaczników dla dokumentu na poziomie CDA Level One przedstawiona jest na Rysunku 2.2. Ponieważ dane medyczne na tym poziomie nie są opisane żadną strukturą, mieszczą się one w całości w jednym znaczniku `<text>`, znajdującym się w ciele dokumentu.

```
<ClinicalDocument>
  <!-- NAGŁÓWEK -->
  ...
  <!-- CIAŁO -->
  <component>
    <structuredBody>
      <component>
        <section>
          <text>
            <!-- CDA LEVEL ONE -->
            <!-- ZAWARTOŚĆ MEDYCZNA -->
          </text>
        </section>
      </component>
    </structuredBody>
  </component>
</ClinicalDocument>
```

Rysunek 2.2: Hierarchia znaczników dokumentu HL7 CDA Level One.

Hierarchia znaczników w dokumentach CDA Level Two w całości zawiera się w hierarchii znaczników z dokumentów CDA Level Three, ponieważ CDA Level Three jest uzupełnieniem dla poziomu CDA Level Two. Dokument przedstawiający tę hierarchię zamieszczono na Rysunku 2.3. Zgodnie z tym rysunkiem dane medyczne podzielone są na sekcje opisane kodami z różnych słowników terminów medycznych (np. LOINC [LOI], SNOMED CT [SNO], ICD10 [ICD]). Dla dokumentów CDA Level Two w sekcji takiej znajduje się blok narracyjny, w którym mieści się tekstowy opis informacji medycznej, zgodny z podanym kodem. Dokumenty CDA Level Three posiadają dodatkowo znacznik `<entry>`, który zawiera dokładnie te same informacje, które zostały zawarte w bloku narracyjnym, jednak w pełni ustrukturalizowane i zorganizowane w hierarchię wynikającą z HL7 RIM.

Szczególnym przypadkiem dokumentów są takie, w których dane medyczne przedstawione są w innym formacie niż XML. Znacznik `<structuredBody>` jest w nich zamieniony na `<nonXMLBody>`. Zawiera on dane w dowolnym formacie (np. pliki w formacie PDF), który jest zgodny z formatem zawartości podanym w nagłówku dokumentu.

2.2.2 EHRcom

EHRcom (ang. *Electronic Healthcare Record Communication*) to standard, który jest polską oraz europejską normą [EN1], będącą cały czas w trakcie opracowywania. Obejmuje on wszystkie etapy oraz elementy niezbędne do zapewnienia w pełni funkcjonalnej Elektronicznej Kartoteki Pacjenta; od określenia modelu danych oraz sposobu ich reprezentacji, poprzez specyfikację zasad bezpieczeństwa dotyczących dostępu do poszczególnych elementów EHR, po opis sposobu wymiany informacji. Standard ten w dużej mierze opiera się na projekcie *openEHR* [ope] prowadzonym przez internetową organizację typu non-profit, której celem jest rozwijanie otwartej specyfikacji, oprogramowania oraz bazy wiedzy i zasobów dotyczących systemów informacyjnych w ochronie zdrowia [SMO].

```
<ClinicalDocument>
  <!-- NAGŁÓWEK -->
  ...
  <!-- CIAŁO -->
  <component>
    <structuredBody>
      <component>
        <section>
          <code code='KOD01' codeSystem='SŁOWNIK' />
          <text>
            <!-- CDA LEVEL TWO -->
            <!-- ZAWARTOŚĆ MEDYCZNA ZGODNA Z KODEM -->
          </text>
          <entry>
            <!-- CDA LEVEL THREE -->
            <!-- W PEŁNI USTRUKTURALIZOWANA
                 ZAWARTOŚĆ MEDYCZNA
                 ZAKODOWANA ZGODNIE Z HL7 RIM -->
          </entry>
        </section>
      </component>
      <component>
        ...
      </component>
      ...
    </structuredBody>
  </component>
</ClinicalDocument>
```

Rysunek 2.3: Hierarchia znaczników dokumentu HL7 CDA Level Two oraz CDA Level Three.

Model referencyjny EHRcom podzielony jest na kilka części, z których jedną z najważniejszych jest część *Extract*, definiująca model reprezentacji danych medycznych (ang. *Extract Reference Model*). Podobnie jak w przypadku HL7 CDA, struktura modelu EHRcom jest hierarchiczna. Została ona przedstawioną na Rysunku 2.4.

```
EHR Extract
    Folder 1
        Composition 1
            Secton 1
                Entry 1
                    Cluster 1
                        Element 1
                        Element 2
                        ...
                    Cluster 2
                    Element 3
                    ...
                Entry 2
                ...
            Section 2
            Entry 3
            ...
        Composition 2
        ...
    Folder 2
    Composition 3
    ...
```

Rysunek 2.4: Hierarchia znaczników w EHRcom.

Zgodnie z Rysunkiem 2.4 głównym elementem pakietu danych jest `EHR Extract`. Wewnątrz niego może znajdować się hierarchia folderów (`Folder`) organizująca dokumenty medyczne oznaczone elementem `Composition`. Te z kolei mogą zawierać hierarchię sekcji (`Section`) grupujących pojedyncze informacje medyczne oznaczone elementem `Entry`. Wewnątrz może znajdować się kolejna hierarchia złożona z klastrów (`Cluster`) organizujących elementy `Element` zawierające pojedynczą wartość. Wszystkie elementy modelu wraz z krotnością oraz przykładami zostały zamieszczone w Tabeli 2.1.

Tabela 2.1: Hierarchiczny model reprezentacji danych medycznych w EHRcom

Element	Krotność	Przykład
`EHR Extract`	1	
`Folder`	0..n	data, szpital, oddział, choroba
`Composition`	1..n	raport o stanie zdrowia, dokument z badania laboratoryjnego
`Section`	0..n	wywiad rodzinny, alergie, szczepienia, procedury
`Entry`	1..n	objaw, wynik badania, przypisany lek
`Cluster`	0..n	interpretacja całodobowego pomiaru ciśnienia krwi, badania USG
`Element`	1..n	poziom cholesterolu, liczba erytrocytów, tętno

2.2.3 DICOM

DICOM (ang. *Digital Imaging and Communications in Medicine*) to standard opracowywany przez ACR (ang. *American College of Radiology*) oraz NEMA (ang. *National Electrical Manufacturers Association*). Ze względu na autorów tego standardu, dotyczył on na początku dziedzin związanych z obrazowaniem medycznym, takich jak np. radiologia. Z czasem jego zakres się rozszerzał. Nadal jednak główny nacisk kładzie on na przetwarzanie obrazów.

Obecnie standard DICOM definiuje zarówno format plików jak i protokoły służące do ich wymiany. Jego rozszerzenie, *DICOM SR* (ang. *Structured Reports*), ma na celu umożliwienie wymiany wszelkiego rodzaju dokumentacji medycznej pacjenta.

Podobnie jak w przypadku dokumentów HL7 CDA omówionych w punkcie 2.2.1, zarówno dokumenty DICOM SR jak i pliki w formacie DICOM, podzielone są na część nagłówka oraz ciała. Zawartość dokumentów znajduje się w hierarchicznej strukturze opisanej kodami z różnych słowników medycznych. Standard umożliwia takie opisanie danych medycznych, aby było możliwe ich pełne automatyczne przetworzenie. Jednak w przeciwieństwie do standardu HL7 CDA, dokumenty DICOM SR przesyłane są w postaci binarnej, a nie w formacie XML.

DICOM nie jest rozpowszechnionym standardem poza dziedzinami związanymi z obrazowaniem medycznym. Jego rozszerzenie DICOM SR nie zostało i raczej nie zostanie przyjęte jako powszechny standard EHR [EAR+05].

2.2.4 Porównanie

Należy podkreślić, że w omawianym zastosowaniu wymienione standardy nie różnią się między sobą pod względem koncepcji. Prawdopodobnie każdy z nich mógłby zostać wykorzystany w opisywanym systemie, jednak istnieją pewne aspekty, które zdeterminowały wybór jednego z nich.

Wszystkie standardy mogą zawierać dane multimedialne, ale tylko DICOM SR jawnie specyfikuje sposób załączania podpisów cyfrowych. Do tego celu można jednak skorzystać z rekomendacji *XML Signature* [W3Cc], ponieważ EHRcom oraz HL7 CDA oparte są o XML.

Standardy EHRcom i HL7 CDA są bardzo podobne pod względem modelu danych medycznych. Różnią się one tym, że w EHRcom istnieje dodatkowa warstwa `Folder`, która organizuje dokumenty w hierarchiczną strukturę. Tabela 2.2 przedstawia odpowiadające sobie elementy obu modeli.

Tabela 2.2: Odpowiadające sobie elementy modelu informacji medycznej standardów EHRcom oraz HL7 CDA.

EHRcom	HL7 CDA
`Folder`	-
`Composition`	`ClinicalDocument`
`Section`	`section`
`Entry`	`entry`

Opisywane standardy nie definiują jednoznacznie sposobu wizualizacji danych. Standard HL7 CDA jako jedyny podaje jednak wskazówki dotyczące struktury oraz zakodowania informacji, aby wesprzeć proces ich ewentualnego późniejszego wyświetlania. Powszechnie dostępna jest również transformacja *XSLT* [W3Cd] dla dokumentów HL7 CDA.

W celu łatwiejszego porównania omawianych standardów zestawiono niektóre z ich cech. Wynik tego zestawienia przedstawiono w Tabeli 2.3.

Tabela 2.3: Zestawienie niektórych cech standardów reprezentacji danych medycznych.

	Wizualizacja	**Format**	**Podpis**	**Popularność**
HL7 CDA	+	XML	−	+++
EHRcom	−	XML	−	++
DICOM SR	−	binarny	+	+

Ze względu na fakt, że DICOM jest standardem w większości zorientowanym na obrazowanie medyczne oraz że środowisko skłania się bardziej w stronę dwóch pozostałych omawianych standardów, DICOM SR nie został wykorzystany w opisywanym projekcie. Poza tym, zgodnie z [USTc, §55], dokumentacja medyczna powinna być przesyłana w formacie XML, a standard DICOM SR narzuca format binarny. Ostatecznie standardem reprezentacji informacji medycznych w projekcie został HL7 CDA. Wybór taki podyktowany jest dobrym przyjęciem tego standardu przez środowisko, co jest widoczne w liczbie wdrożeń w różnych projektach na całym świecie, m.in. w Finlandii (Satakunta Macro Pilot), USA (Mayo Clinic), Kanadzie (e-Claims), Argentynie (Buenos Aires Project), Unii Europejskiej (PICNIC) etc. [Bot].

2.3 Wykorzystanie standardów

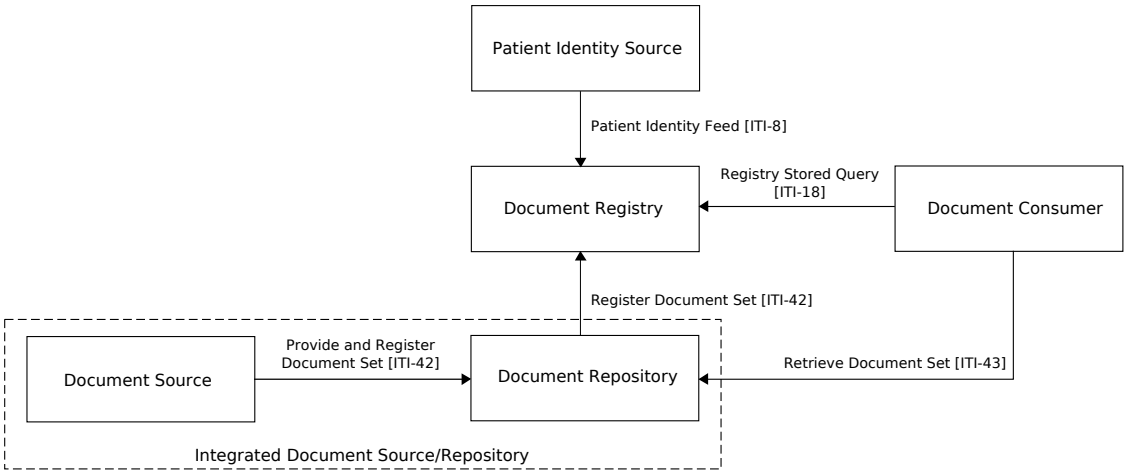
Wybór standardu dotyczącego reprezentacji danych medycznych pacjenta był problemem o rozmiarach możliwych do przedstawienia w ramach pracy dyplomowej, jednak bardzo trudne byłoby dokonanie pełnego porównania standardów komunikacyjnych na wszystkich opisywanych przez nie poziomach. Istnieje jednak inicjatywa o nazwie *IHE* (ang. *Integrating Healthcare Enterprise*) [IHE], która opracowuje wytyczne dotyczące wykorzystania różnorodnych standardów. Wskazówki te zorganizowane są w logiczne części, zwane dalej profilami, z których każda opisuje sposób realizacji ściśle określonych zadań związanych z medycyną.

2.3.1 IHE XDS

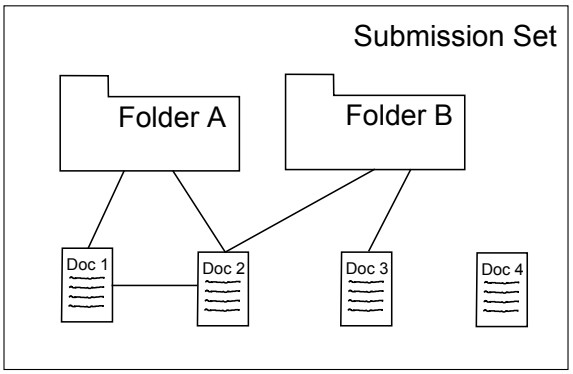
IHE XDS (ang. *Cross-Enterprise Document Sharing*) jest jednym z profili IHE, który definiuje opis systemu umożliwiającego dostęp do pełnej informacji medycznej o pacjencie. Architektura systemu pozwalającego utrzymać EHR zgodnie z założeniami IHE XDS jest zorientowana na dokumenty, które są najmniejszą jednostką wymienianej informacji medycznej. Diagram z architekturą znajduje się na Rysunku 2.5.

`Document Source` jest źródłem dokumentów i zasila nimi repozytorium (`Document Repository`) przy pomocy transakcji `Provide And Register Document Set [ITI-41]`. Te elementy systemu mogą być połączone i stanowić pojedynczy element `Integrated Document Source/Repository`. W ramach zgłoszenia dokumentów, poza ich zawartością, przesyłane są również ich metadane zorganizowane w pewną strukturę przedstawioną na Rysunku 2.6.

`Submission Set` to obiekt zawierający metadane o samym zgłoszeniu, m.in. identyfikator pacjenta, ponieważ każde zgłoszenie dokumentów dotyczy zawsze jednego pacjenta. Każde zgłoszenie może zawierać foldery (`Folder`) oraz metadane dokumentów (`Document Entry`). Foldery tworzą



Rysunek 2.5: Architektura systemu wymiany dokumentów medycznych o pacjencie według profilu IHE XDS.



Rysunek 2.6: Schemat powiązań pomiędzy poszczególnymi elementami metadanych według profilu IHE XDS.

jednopoziomową, abstrakcyjną strukturę grupującą dokumenty. Każdy dokument może należeć do wielu folderów, każdy folder natomiast może zawierać wiele dokumentów. Foldery w swojej koncepcji przypominają więc etykiety przypisywane opcjonalnie do dokumentów. Dodatkowo, dokumenty mogą zawierać powiązania między sobą. Metadane, zgłoszenia, dokumenty oraz foldery zawierają szereg atrybutów, które zostały szczegółowo opisane w [IHE09c, Rozdział 4].

Na potrzeby jednolitej wymiany przedstawionych metadanych, opisane struktury przesyłane są w formacie XML zgodnie ze standardem *ebXML* (ang. *Electronic Business using XML*) [ebX]. Jest to standard definiujący format oparty o XML, który służy do przesyłania informacji biznesowych. Dokładne przyporządkowanie wszystkich atrybutów z metadanych do struktur z tego formatu opisane jest w [IHE09c, Rozdział 4].

Zawartość zgłoszonych przez `Document Source` dokumentów zostaje zapisana lokalnie przez repozytorium. Następnie ekstrahowane są z nich metadane i zgłaszane do rejestru dokumentów (`Document Registry`) w ramach transakcji `Register Document Set [ITI-42]`. Bardzo ważne jest, iż raz zgłoszone dokumenty nie mogą zostać usunięte ani nadpisane. Jeśli do rejestru zostanie ponownie zgłoszony ten sam dokument, staje się on aktualną wersją. Wszystkie poprzednie wersje tego dokumentu są jednak utrzymywane i każda z nich zawiera odniesienie do wersji nowszej.

Po wykonaniu pełnej ścieżki zgłaszania dokumentu (od źródła do rejestru), `Document Consumer` może kierować zapytania do rejestru w celu uzyskania pożądanych informacji. Zapytania takie noszą nazwę `Stored Query` i są z góry zdefiniowane w rejestrze. Do głównych zapytań należą:

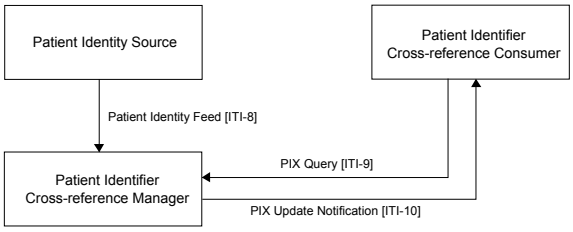
- `XDSGetFolders` - pobierające listę folderów pacjenta,
- `XDSGetFolderAndContents` - pobierające folder wraz z metadanymi o wszystkich dokumentach, które zawiera,
- `XDSGetDocuments` - pobierające metadane o konkretnych dokumentach.

`Document Consumer`, po wywołaniu na rejestrze odpowiednich zapytań w ramach transakcji `Registry Stored Query [ITI-18]` i otrzymaniu metadanych, może z nich odczytać identyfikatory oraz adresy repozytoriów, w których dokumenty się znajdują. Następnie możliwe jest wysłanie żądania dokumentów do odpowiednich repozytoriów w ramach transakcji `Retrieve Document Set [ITI-43]`.

Przedstawiona architektura jest zorientowana na wymianę dokumentów, ale równocześnie także na wymianę danych przypisanych do pojedynczego pacjenta. Dlatego też, aby zapewnić spójną identyfikację, musi istnieć źródło globalnie unikatowych identyfikatorów pacjenta informujące rejestry o nowych pacjentach lub zmianach w już istniejących. Rolę takiego źródła pełni `Patient Identity Source`, który w ramach transakcji `Patient Identity Feed [ITI-8]` przesyła informacje o zmianach jakie zachodzą w sposobie identyfikacji pacjenta.

2.3.2 IHE PIX

Kolejnym, ważnym w kontekście projektowanej platformy profilem IHE jest *PIX* (ang. *Patient Indentifier Cross-referencing*). Definiuje on elementy systemu informatycznego niezbędne do umożliwienia utrzymywania spójnych referencji do pacjentów pomiędzy różnymi domenami (ang. *Patient Identity Domain*). Obok systemów działających w jednostkach medycznych, które posiadają wspólny schemat identyfikowania pacjentów, powinny zostać zbudowane źródła identyfikatorów (`Patient Indentity Source`). Pomiędzy różnymi źródłami istnieje menedżer referencji (`Patient Identifier Cross-reference Manager`), który potrafi skojarzyć identyfikatory z różnych domen. Aby korzystać ze zbieranych informacji zdefiniowany został także aktor, którego zadaniem jest pobieranie listy identyfikatorów (`Patient Identifier Cross-reference Consumer`). Aktorów oraz interakcje między nimi prezentuje Rysunek 2.7.



Rysunek 2.7: Aktorzy i transakcje w standardzie IHE PIX.

Profil ten zakłada wykorzystanie komunikatów HL7 do wymiany informacji pomiędzy aktorami i wyróżnia następujące transakcje:

- `Patient Identity Feed [ITI-8]`. Wykorzystuje komunikaty z grupy *ADT* (ang. *Admission Discharge Transfer*) standardu HL7 w wersji 2.3.1. Pozwala na zgłaszanie podstawowych danych osobowych oraz identyfikatorów pacjentów z `Patient Identity Source` do `PIX Manager`. Wysyłanie odpowiednich komunikatów wywoływane jest zdarzeniami związanymi z modyfikacją danych pacjenta (wstawienie, zmiana, scalanie identyfikatorów).

- `PIX Query [ITI-9]`. Wykorzystuje komunikaty z grupy *QBP* (ang. *Query by parameter*) oraz z grupy *RSP* (ang. *Response*), zdefiniowane w wersji 2.5 standardu HL7. Transakcja ta

ma za zadanie umożliwić elementom `PIX Consumer` pobieranie listy identyfikatorów pacjenta z różnych domen.

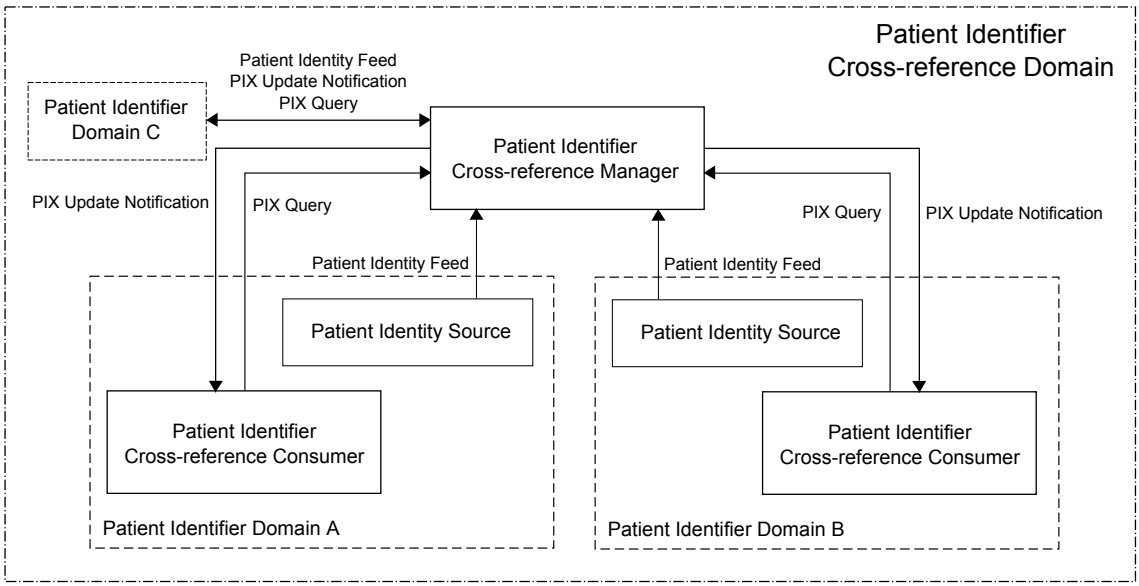
- `PIX Update Notification [ITI-10]`. Wykorzystuje komunikat `ADT^A31` (*Update Person Information*) ze standardu HL7 w wersji 2.5. Transakcja ta jest alternatywnym sposobem przekazywania danych do aktora `PIX Consumer` inicjowanym przez `PIX Manager`. Według IHE jest to opcjonalny komunikat.

Szczegóły wykorzystania poszczególnych pól i segmentów ze standardu HL7 opisuje [IHE09b, Rozdziały 3.8-3.10].

Warto zauważyć, że wykorzystywana w transakcji `[ITI-8]` wersja standardu HL7 2.3.1 nie jest najnowsza, jednak jest ona bardzo rozpowszechniona. Zgodnie z założeniem o nakładaniu jak najmniejszych wymagań na aktora `Patient Identity Source`, pozwoli to na wykorzystanie profilu IHE PIX w większej liczbie systemów informatycznych.

Istotne jest także to, że `PIX Manager` według definicji nie ma tworzyć globalnego identyfikatora pacjenta, który mógłby posłużyć jako uniwersalna referencja. Jego zadaniem jest jedynie gromadzenie informacji z różnych domen i łączenie ich w listę danych dotyczących pojedynczego pacjenta. Jednak jak opisano w [IHE09a, Rozdział 5.4] wprowadzenie dedykowanego `Master Patient Identity Source` pozwala zbudować indeks pacjentów (*eMPI*, ang. *Enterprise Master Patient Index*) tworzący takie globalne identyfikatory.

Przykładową architekturę zbudowaną zgodnie z profilem PIX zaprezentowano na Rysunku 2.8.



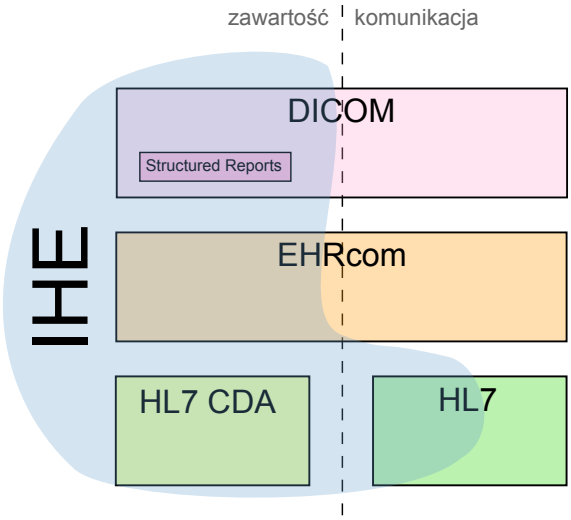
Rysunek 2.8: Przykładowe rozmieszczenie elementów IHE PIX.

2.4 Podsumowanie

Kluczową decyzją dotyczącą wyboru standardów był wybór IHE, ponieważ w jednym z profili opisuje on kompletną architekturę systemu o bardzo podobnych założeniach do prezentowanych w tej pracy, wykorzystującą różne istniejące standardy. Zastosowanymi profilami z IHE są:

- XDS - dotyczący wymiany dokumentów,
- PIX - dotyczący zarządzania identyfikatorami pacjentów.

Rysunek 2.9 pokazuje powiązania pomiędzy IHE a pozostałymi omawianymi standardami. Wyróżnienie IHE wynika z faktu, iż operuje on na wyższym poziomie abstrakcji niż pozostałe. Definiuje ramę projektową dla stworzenia kompletnego systemu EHR i wskazuje kiedy i w jaki sposób skorzystać z określonych standardów.



Rysunek 2.9: Zależności pomiędzy omawianymi standardami.

Jedynym elementem, którego nie narzuca IHE XDS jest sposób reprezentacji informacji medycznych. W tym przypadku do wyboru były trzy popularne standardy: EHRcom, HL7 CDA oraz DICOM SR. Jednak zgodnie z [USTc, §55] dane medyczne muszą być przechowywane w formacie XML, zatem standard DICOM SR został odrzucony ze względu na binarny format.

Tabela 2.2 w punkcie 2.2.4 pokazuje, iż struktura danych standardu EHRcom w odniesieniu do HL7 CDA posiada dodatkową hierarchię folderów. Struktura taka może zapewnić lepsze uporządkowanie dokumentów i tym samym ułatwić ich ewentualne wyszukiwanie. Profil IHE XDS wprowadza jednak w metadanych elementy, które mogą pełnić taką samą funkcję. Tabela 2.4 przedstawia odpowiadające sobie elementy modelu EHRcom oraz HL7 CDA uzupełnione o elementy metadanych zdefiniowane przez IHE XDS.

Tabela 2.4: Odpowiadające sobie elementy modelu informacji medycznej standardów EHRcom oraz HL7 CDA uzupełniony o IHE XDS.

EHRcom	**HL7 CDA + IHE XDS**
`EHR Extract`	`XDSSubmissionSet`
`Folder`	`XDSFolder`
`Composition`	`ClinicalDocument`
`Section`	`section/XDSFolder`
`Entry`	`entry`

Decyzja o wyborze pomiędzy EHRcom a HL7 CDA wydaje się mieć subiektywny charakter. Sam profil IHE wskazuje na dowolność wyboru pomiędzy nimi. Jednak większa liczba projektów realizowanych w oparciu o HL7 CDA na świecie oraz jego wykorzystanie w innych profilach z grupy IHE (np. Patient Care Coordination) zadecydowały, że standard ten został wybrany jako model reprezentacji danych medycznych.

Należy jednak podkreślić, iż cała architektura systemu przedstawiana w ramach IHE XDS jest całkowicie niezależna od formatu przesyłanych dokumentów. Dzięki temu dobrze zaprojektowana platforma pozwoli niskim kosztem wprowadzać inne formaty reprezentacji danych.

Rozdział 3

Projekt koncepcyjny

3.1 Model

Zgodnie z zasadami projektowania systemów informatycznych na początku prac utworzono model biznesowy. Określono aktorów oraz obiekty, a także zdefiniowano podstawowe biznesowe przypadku użycia (ang. *Business Case*).

3.1.1 Aktorzy

Pacjent

Platforma Integracji Systemów Medycznych jest nastawiona na udostępnianie danych medycznych, jednak wszelkie informacje są jednoznacznie przypisane do określonego pacjenta. W ramach systemu pacjent jest właścicielem swojej historii choroby, ma on możliwość jej przeglądania i wyłączne prawo udostępniania danych innym osobom.

Użytkownik

Pacjenci i inne osoby posiadające dostęp do danych stanowią użytkowników systemu. Szczególnym rodzajem użytkowników są lekarze identyfikowani przez numer prawa do wykonywania zawodu, którzy mogą posiadać dostęp do danych ze względu na przynależność do jednostek medycznych.

Jednostka medyczna

Źródłem danych medycznych, do których dostęp umożliwia platforma, są jednostki medyczne. Placówki służby zdrowia posiadają różnorodne oprogramowanie ewidencyjne, z którego dane będą odczytywane. Systemy informatyczne jednostek stanowią także źródło danych niezbędnych do określenia tożsamości pacjentów.

3.1.2 Obiekty

Dokument

Dane medyczne są wymieniane pomiędzy jednostkami w ustrukturalizowanej postaci, jako dokumenty. Jest to elementarna część danych, która może być przesyłana w infrastrukturze sieciowej systemu.

3.1.3 Przypadki użycia

BC1 Gromadzenie danych
Aktorzy: Jednostka medyczna
Scenariusz:

1. Jednostka zgłasza informacje o pacjentach.
2. Jednostka tworzy dokumenty.
3. Jednostka rejestruje informacje o dokumentach.
4. Jednostka udostępnia dokumenty do odczytu.

BC2 Zarządzanie i odczyt danych
Aktorzy: Pacjent, Użytkownik
Scenariusz:

1. Pacjent udziela dostępu do swoich danych.
2. Użytkownik wyszukuje dokumenty.
3. Użytkownik pobiera dokumenty.

3.2 Wymagania funkcjonalne

Podstawowym elementem projektowania każdego systemu informatycznego jest dokładnie określenie wykonywanych przez niego zadań. W kolejnych rozdziałach przedstawiono planowaną architekturę usług sieciowych, opisano dodatkowe zadania związane z rodzajem przetwarzanych danych oraz wyspecyfikowano przypadki użycia wraz z diagramami sekwencji.

3.2.1 Usługi

Na etapie planowania architektury systemu wyróżniono podstawowe moduły funkcjonalne platformy, które w kolejnych fazach projektowania zostały rozmieszczone w poszczególnych usługach. Diagram interakcji pomiędzy usługami przedstawia Rysunek 3.1.

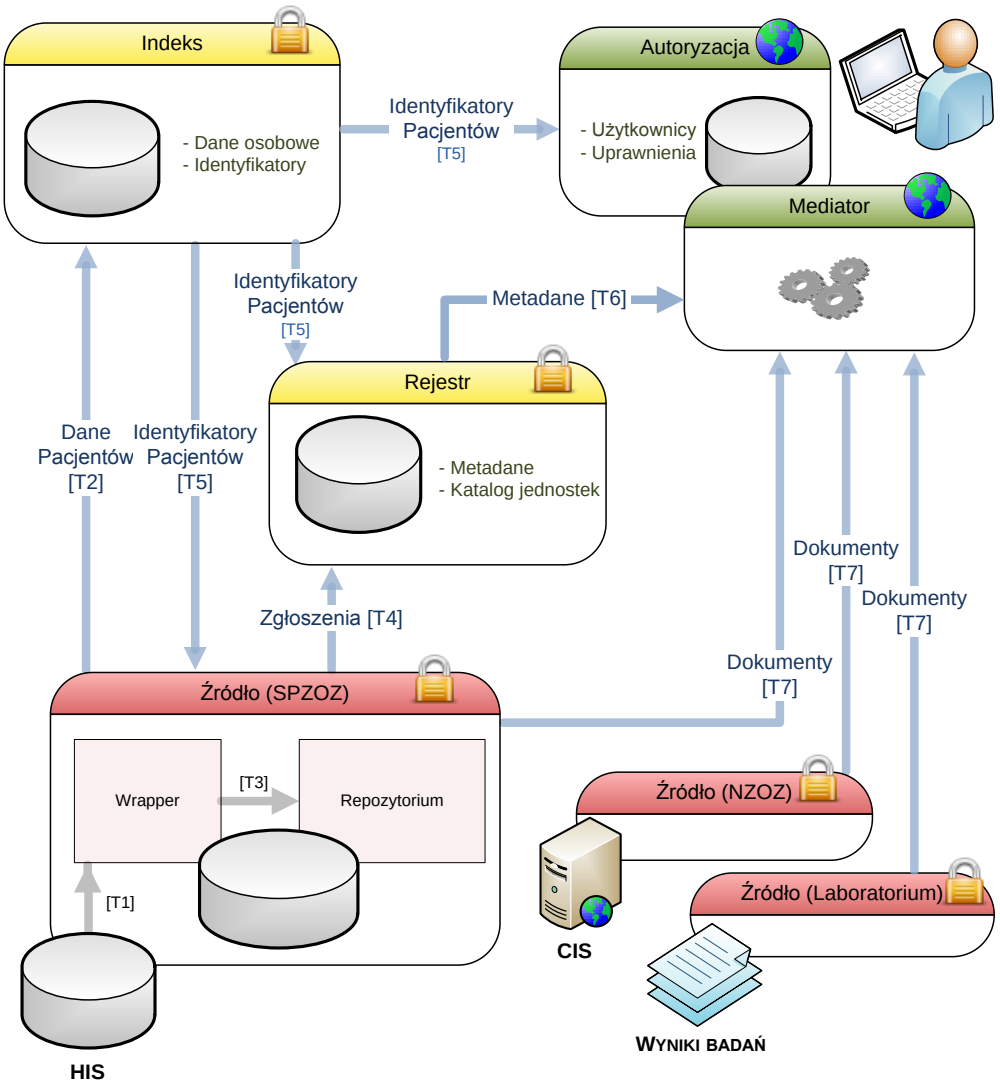
Źródło danych

Usługa źródła spełnia kilka zadań w platformie:

- zgłaszanie danych pacjentów,
- zgłaszanie dokumentów,
- udostępnianie dokumentów.

W ramach tej usługi, do pozyskania danych z jednostek medycznych wykorzystywany jest dedykowany *wrapper* (*element systemu mediacyjnego, ukrywający sposób dostępu do danych docelowych*). Jego zadaniem jest wydobycie danych z ewidencyjnego systemu informatycznego (T1) i ich zamiana na dokumenty, które stanowią najmniejszą część przesyłanych danych. Są one zgodne ze standardem HL7 CDA, a za minimalną szczegółowość przyjęto poziom drugi (punkt 2.2.1).

Dodatkowo usługa ta powinna zgłaszać nowych pacjentów do odpowiedniego indeksu platformy (T2), w celu umożliwienia ich identyfikacji pomiędzy różnymi jednostkami. Dla identyfikatorów określono symbole rozpoznawane przez platformę m.in. nr PESEL, nr i seria dowodu osobistego (szczegóły w punkcie 4.2.1). Komunikacja związana z danymi osobowymi pacjentów wykorzystuje komunikaty protokołu HL7 ADT (ang. *Admission, Discharge, Transfer*) w wersjach 2.3.1 oraz



RYSUNEK 3.1: Rodzaje usług i interakcje między nimi.

2.5. Wykorzystywane wersje standardu nie są najnowsze jednak zgodnie z [IHE09b, Rozdział 3.8] zapewni to możliwość współpracy z większą liczbą systemów informatycznych.

Jednym z głównych zadań omawianej usługi jest udostępnianie dokumentów. Jako repozytorium usługa może stale przechowywać dokumenty w dedykowanej do tego celu bazie danych lub jedynie pośredniczyć w ich pobieraniu z systemu ewidencyjnego jednostki medycznej (T3). W ramach usługi powinny być także generowane metadane przetwarzanych dokumentów i zgłaszane do usługi rejestru dokumentów (T4). Zarządzanie wymianą dokumentów wzorowane jest na profilu IHE XDS omówionym w punkcie 2.3.1.

Usługa ta w dalszych rozdziałach określana będzie jako *Źródło*.

Indeksy

Zadaniem indeksów jest zarządzanie poszczególnymi rodzajami informacji. Aktualizacja ich danych jest zapewniona przez usługi źródeł działające w jednostkach medycznych (T2, T4). Można wyróżnić dwa rodzaje indeksów ze względu na rodzaj przetwarzanych danych:

Indeks pacjentów

Indeks zarządza identyfikacją pacjentów. Jako jedyna usługa niezwiązana z pojedynczą jednostką przetwarza dane osobowe. Gromadzi m.in. identyfikatory, tak aby możliwe było przyrównanie tożsamości pacjenta z różnych jednostek, a tym samym stwierdzenie, że 2 dokumenty z różnych źródeł dotyczą tej samej osoby. Poprzez udostępnianie tych danych usługa ta zapewnia spójność identyfikacji w platformie (T5). Zarządzanie tożsamością pacjentów opracowane zostało zgodnie z profilem IHE PIX omówionym w punkcie 2.3.2.

Usługa ta w dalszych rozdziałach określana będzie jako *Indeks*.

Rejestr dokumentów

Rejestr zarządza informacjami o dokumentach. Placówki medyczne ze względu na różnorodność świadczonych usług przechowują odmienne typy danych. Rejestr zawiera informacje o dostępności poszczególnych rodzajów danych w znanych lokalizacjach. Pozwala także określić gdzie znajdują się dane pojedynczego pacjenta. Usługa ta nie przetwarza samych dokumentów, a jedynie ich metadane, które wysyłane są z usług źródła (T4) w grupach nazywanych dalej *zgłoszeniami* (ang. *Submission Set*). Sposób wymiany i przechowywania tych informacji opracowany został zgodnie z profilem IHE XDS (punkt 2.3.1).

Rejestr poprzez określanie adresów usług źródła, pełni także funkcję katalogu jednostek. Jako jedyna usługa musi posiadać informacje na temat aktualnych adresów usług sieciowych udostępniających dokumenty.

Usługa ta w dalszych rozdziałach określana będzie jako *Rejestr*.

Autoryzacja

Usługa autoryzacji zapewnia zarządzanie podstawowymi informacjami związanymi z bezpieczeństwem dostępu do danych. Dzięki tej usłudze podmiot danych powinien mieć możliwość przydzielania uprawnień wybranym użytkownikom, lekarzom lub całym zakładom opieki zdrowia. Uprawnienia mogą być przyznawane na stałe lub na określony czas, a także mogą ograniczać dostęp do danych pochodzących z określonego źródła lub do wybranego ich typu (szerszy opis znajduje się w punkcie 3.3.4).

Usługa ta w dalszych rozdziałach określana będzie jako *Autoryzacja*.

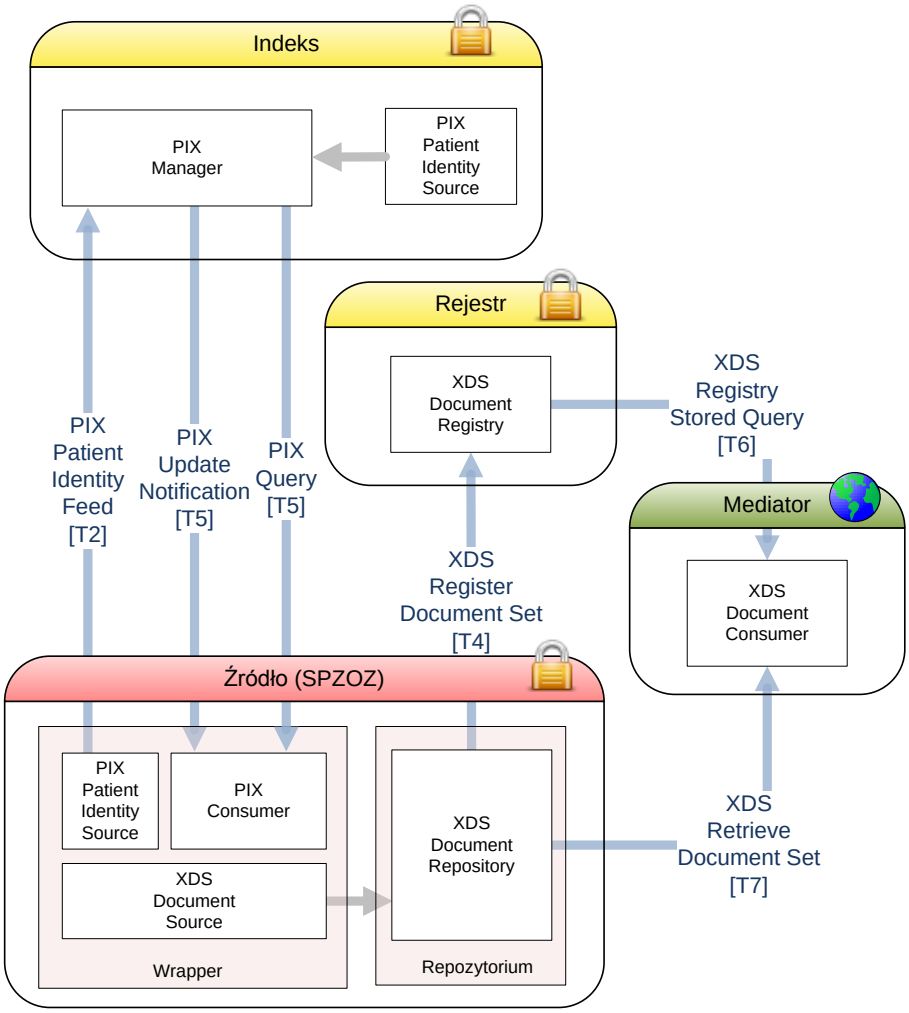
Mediator

Usługa mediatora, jako centralny element systemu mediacyjnego, powinna rozdzielać zapytanie o dane do usług źródła działających w jednostkach. Mediator wykorzystuje usługę rejestru do pozyskiwania metadanych (T6) oraz do określenia lokalizacji, z których należy pobierać dokumenty (T7). Ponadto za pomocą informacji zgromadzonych przez usługę autoryzacji i mechanizmów kontroli dostępu, usługa udostępnia wyłącznie dane, do których użytkownicy mają przyznane uprawnienia. Usługa ta stanowi główną część interfejsu platformy dostępną dla użytkownika, która będzie wykorzystywana do budowania różnorodnych aplikacji klienckich.

Usługa ta w dalszych rozdziałach określana będzie jako *Mediator*.

Rozmieszczenie usług

Można zatem wyróżnić 5 rodzajów usług: Źródło, Rejestr, Indeks, Mediator i Autoryzacja. Taki podział funkcji platformy na usługi został opracowany nie tylko ze względu na rodzaj przetwarzanych danych, ale także w celu zwiększenia możliwości rozbudowy systemu, poprawy efektywności oraz z uwagi na ograniczenia prawne i wykorzystane standardy. Rozmieszczenie aktorów zdefiniowanych w profilach IHE wśród usług prezentuje Rysunek 3.2.



Rysunek 3.2: Wykorzystywane standardy w usługach.

Usługa Źródła skupia różne części funkcjonalne platformy. Jednak jako całość przetwarza dane medyczne, które z założenia mają być przechowywane w miejscu ich ewidencji. Powinna zatem stanowić część systemu informatycznego jednostki medycznej.

Indeks pacjentów pełni krytyczną rolę w platformie. Niedostępność tej usługi nie pozwala na określenie tożsamości pacjenta w systemie, a tym samym niemożliwe jest zgłaszanie dokumentów dotyczących nowych pacjentów. W takiej sytuacji nie będzie także dostępu do jakichkolwiek danych osobowych. Jest to zatem usługa, która w docelowym środowisku pracy powinna zostać wyposażona w dodatkowe mechanizmy niezawodności.

Rejestr dokumentów pełni w systemie rolę menedżera metadanych. Grupuje także usługi Źródła, jako wspomniany wcześniej katalog jednostek. Podobnie jak Indeks pacjentów jest usługą działającą poza jednostkami medycznymi. Jednak obie usługi nie mogłyby być zintegrowane, po-

nieważ dla zapewnienia rozszerzalności platformy, Rejestrów może być wiele. Jedynym założeniem jest to, że usługa Źródła powinna być jednoznacznie przypisana do wybranego Rejestru.

Usługi Mediatora i Autoryzacji są jedynymi usługami z interfejsem dostępnym z zewnątrz platformy. Obie korzystają z uprawnień dostępu użytkowników, jednak zostały rozdzielone ze względu na różnice w przetwarzaniu danych. Autoryzacja jest prostą usługą *CRUD* (ang. *Create, Read, Update, Delete*), wykonującą krótkie operacje odczytu i zapisu na informacjach o uprawnieniach. Natomiast Mediator wykonuje czasochłonne operacje odczytu danych z innych usług w ramach platformy.

3.2.2 Dodatkowe zadania

Identyfikatory

Zadanie. Platforma wymienia pomiędzy usługami różnego rodzaju dane. Dla zachowania spójności wszystkie usługi muszą posiadać jednakowy schemat identyfikowania obiektów.

Rozwiązanie. Wykorzystano notację *ISO OID* [ISOb] (ang. *ISO Object IDentifier*), która pozwala na budowanie hierarchicznych identyfikatorów. Drzewo identyfikatorów ISO jest z założenia globalne i tak np. gałąź przydzielona dla Polski ma numer `1.2.616`.

Platforma jako całość może mieć dowolnie ustalony identyfikator ISO. Mogą zostać wykorzystane m.in. drzewa:

- `1.2.616.2` – `iso(1) member-body(2) pl(616) business(2)`
- `1.3.6.1.4.1` – `iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)`

Wybór odpowiedniego identyfikatora zależy od instytucji, która będzie zarządzać platformą w docelowym środowisku pracy i nie będzie omawiany w tej pracy.

Wybrany identyfikator drzewa stanowi prefiks dla właściwych identyfikatorów obiektów, które dalej nazywane są *UID* (ang. *Unique Identifier*). Prezentuje je Tabela 3.1. Przykłady wykorzystywanych identyfikatorów przedstawiono w Tabeli 3.2

Tabela 3.1: Rodzaje identyfikatorów ISO OID wprowadzonych w platformie.

Nazwa obiektu	**Sufiks identyfikatora**
Dokument	`document(1) source(#) instance(#)`
Pacjent	`patient(2) instance(#)`
Źródło (usługa)	`service(3) source(1) instance(#)`
Rejestr (usługa)	`service(3) registry(2) instance(#)`
Indeks (usługa)	`service(3) index(3) instance(#)`
Mediator (usługa)	`service(3) mediator(4) instance(#)`
Autoryzacja (usługa)	`service(3) authorization(5) instance(#)`
Zgłoszenie	`submission(4) instance(#)`
Folder	`folder(5) type(#)`
Folder pacjenta	`folder(5) type(#) patient(#)`
Prawo dostępu	`right(6) instance(#)`
Jednostka	`unit(7) instance(#)`

(symbol # oznacza dowolną liczbę)

Pseudonimizacja

Zadanie. W przetwarzaniu danych osobowych w rozproszonym środowisku konieczne jest wprowadzenie pseudonimizacji. Oznacza to zastąpienie nazwiska pacjenta i innych informacji mogących doprowadzić do ustalenia jego tożsamości etykietą, mająca na celu znaczące utrudnienie

Tabela 3.2: Przykłady identyfikatorów ISO OID wprowadzonych w platformie.

Nazwa obiektu	**Identyfikator**
Dokument nr 20 ze Źródła nr 4	`1.3.6.1.4.1.123456.23.1.4.20`
Pacjent nr 3	`1.3.6.1.4.1.123456.23.2.3`
Rejestr nr 4	`1.3.6.1.4.1.123456.23.3.2.4`
Folder nr 3 pacjenta nr 9	`1.3.6.1.4.1.123456.23.5.3.9`
Jednostka nr 10	`1.3.6.1.4.1.123456.23.7.10`

jego identyfikacji. Każda z usług przechowuje dane skojarzone z pacjentem, zatem utrzymanie spójności tych powiązań jest krytyczne do utrzymania poprawności i bezpieczeństwa funkcjonowania.

Rozwiązanie. Jako uniwersalny identyfikator pacjenta przyjęto omówiony wcześniej UID. Ich tworzeniem i zarządzaniem zajmuje się Indeks. Jest on zasilany danymi ze Źródeł zgodnie ze zdarzeniami opisanymi przez standard HL7. Wykorzystywane są zdarzenia:

- tworzenia pacjenta (`A01`, `A04`, `A05`),
- aktualizacji danych (`A08`),
- łączenia pacjentów (`A40`).

Pierwsze dwa zdarzenia są standardowymi operacjami, jednak łączenie pacjenta jest funkcją specyficzną dla systemów medycznych. Systemy HIS w różnych jednostkach mogą dysponować innymi rodzajami identyfikatorów danego pacjenta. Przyjmowany pacjent może być także niezidentyfikowany, w takim przypadku w rozliczeniach z NFZ, do pacjenta przypisywany jest *numer dokumentacji medycznej* [USTb]. W obu sytuacjach nie jest możliwe powiązanie danych pacjenta pochodzących z różnych źródeł.

Sytuacje takie rozwiązywane są w momencie uzupełnienia danych w systemach ewidencyjnych. Źródło wysyła wtedy do Indeksu komunikat HL7 `ADT^A40` oznaczający połączenie pacjentów. W platformie oznacza on, że jeden z identyfikatorów globalnych pacjenta przestaje być aktualny, a dane z nim związane powinny zostać przypisane do innego identyfikatora. Wszystkie usługi zostały wyposażone w mechanizmy umożliwiające aktualizacje danych w celu utrzymania ich poprawności.

Foldery

Zadanie. EHR zawiera informacje zbierane przez całe życie pacjenta. Jest więc ich bardzo dużo i mogą one pochodzić z bardzo różnych dziedzin lub etapów opieki zdrowotnej. Dlatego też dane powinny być pogrupowane w taki sposób, aby możliwy był dostęp do części z nich, pokrywającej pewien fragment informacji o zdrowiu pacjenta.

Rozwiązanie. Dokumenty, będące w omawianym systemie najmniejszą częścią przesyłanej informacji medycznej, zorganizowane są w foldery, zgodnie z profilem IHE XDS. Każdy dokument może należeć do wielu folderów, które nie tworzą hierarchii. Są więc swego rodzaju etykietami.

Zdefiniowano w systemie stały zbiór folderów wynikający z pogrupowania odpowiednich podzbiorów danych medycznych opisanego w [IHE09d]. Do każdego z nich może być przypisane wiele kodów z różnych słowników. Struktura taka zapewnia uniwersalność rozwiązania. Foldery przypisywane są do dokumentów w chwili ich zgłoszenia do źródła danych. Ponieważ minimalnym przyjętym poziomem dokumentów w standardzie HL7 CDA w systemie jest poziom drugi (punkt 3.2.1, Źródło danych), każda sekcja zawiera kod zaczerpnięty ze słownika. W chwili zgłoszenia, dokumenty przetwarzane są w poszukiwaniu kodów w sekcjach i każdy z nich zamieniany jest na odpowiedni identyfikator folderu zgodnie z przyporządkowaniem, jeśli takie istnieje. W ten sposób

foldery są spójnie i jednoznacznie identyfikowane we wszystkich usługach platformy. Przykładowe przyporządkowanie folderów do kodów słownika LOINC zaprezentowano w Tabeli 3.3.

Tabela 3.3: Przykłady przyporządkowania folderów do kodów słownika LOINC.

Nazwa folderu	UID folderu	Kod LOINC
Alergie	`1.3.6.1.4.1.123456.23.5.5`	`48765-2`
Szczepienia	`1.3.6.1.4.1.123456.23.5.8`	`11369-6`
Bieżące leki	`1.3.6.1.4.1.123456.23.5.4`	`10160-0`

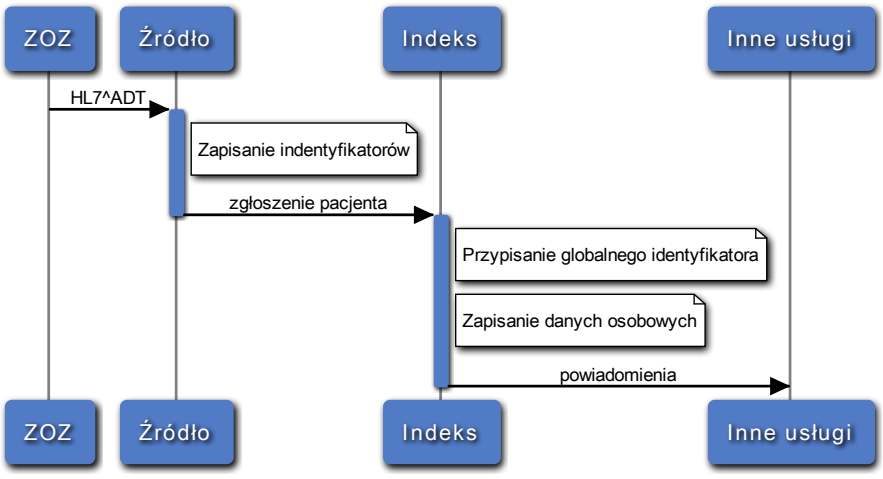
3.2.3 Przypadki użycia

Aktorami poniższych przypadków użycia są:

- Użytkownik - osoba posiadająca dostęp do danych dowolnego pacjenta, korzystająca z aplikacji klienckiej.
- Pacjent - szczególny rodzaj użytkownika, właściciel danych medycznych.
- Jednostka - placówka medyczna posiadająca informatyczny system ewidencyjny.
- Usługi - Źródło, Rejestr, Indeks, Mediator lub Autoryzacja.

UC1 Zgłaszanie pacjentów (Rysunek 3.3)
Aktorzy główni: Jednostka, Źródło, Indeks
Scenariusz:

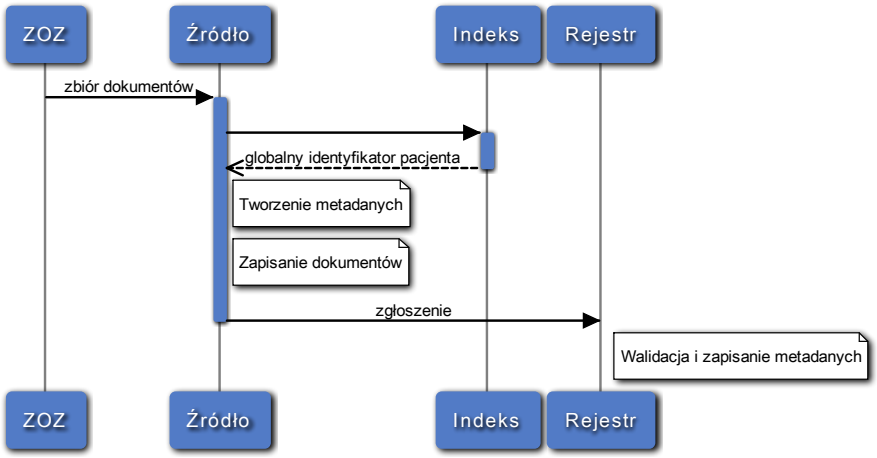
1. Jednostka zgłasza komunikat HL7 ADT.
2. Źródło zapisuje identyfikator pacjenta.
3. Źródło przesyła komunikat do Indeksu.
4. Indeks przypisuje globalny identyfikator pacjenta.
5. Indeks zapisuje przesłane dane osobowe.
6. Indeks rozsyła powiadomienia o utworzeniu lub modyfikacji danych.



Rysunek 3.3: Diagram sekwencji zgłaszania pacjentów (UC1).

UC2 Zgłaszanie dokumentów (Rysunek 3.4)
Aktorzy główni: Jednostka, Źródło, Rejestr
Aktorzy pomocniczy: Indeks
Scenariusz:

1. Jednostka zgłasza zbiór dokumentów.
2. Źródło pobiera z Indeksu globalny identyfikator pacjenta.
3. Źródło tworzy metadane dokumentów.
4. Źródło zapisuje dokumenty.
5. Źródło wysyła metadane do Rejestru.
6. Rejestr waliduje i zapamiętuje informacje o dokumentach.



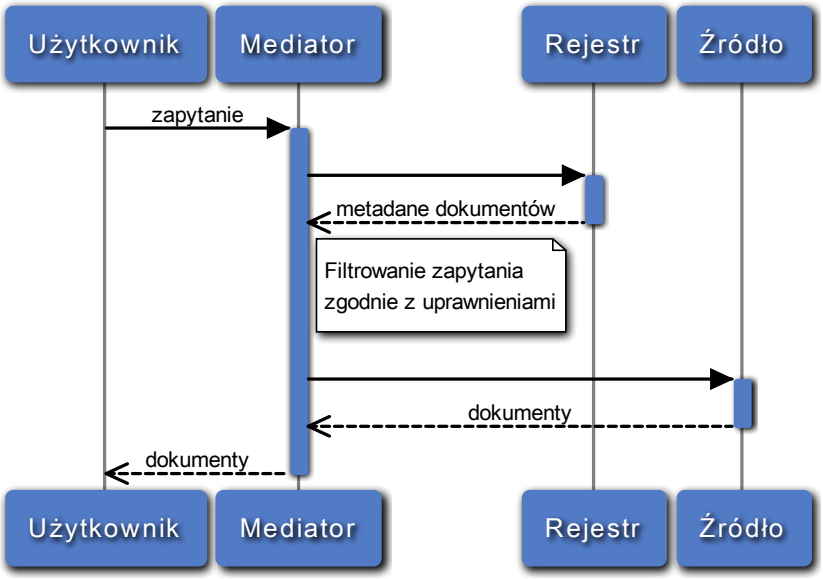
Rysunek 3.4: Diagram sekwencji zgłaszania dokumentów (UC2).

UC3 Pobieranie dokumentów (Rysunek 3.5)
Aktorzy główni: Użytkownik, Mediator
Aktorzy pomocniczy: Rejestr, Źródło
Scenariusz:

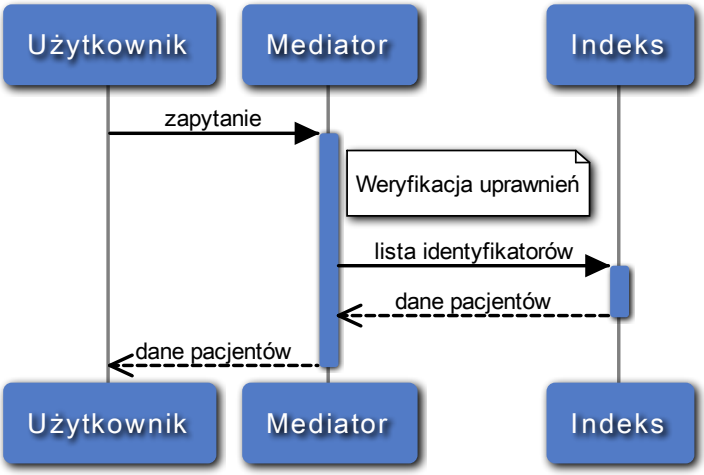
1. Użytkownik wysyła zapytanie o dokumenty do Mediatora.
2. Mediator pobiera metadane z Rejestrów.
3. Mediator filtruje zapytanie użytkownika zgodnie z uprawnieniami.
4. Mediator pobiera dokumenty ze Źródeł.

UC4 Pobieranie listy pacjentów (Rysunek 3.6)
Aktorzy główni: Użytkownik, Mediator
Aktorzy pomocniczy: Indeks
Scenariusz:

1. Użytkownik wysyła zapytanie o listę pacjentów do Mediatora.
2. Mediator określa dostęp do pacjentów zgodnie z uprawnieniami.
3. Mediator pobiera informacje o pacjentach z Indeksu lub własnych danych.



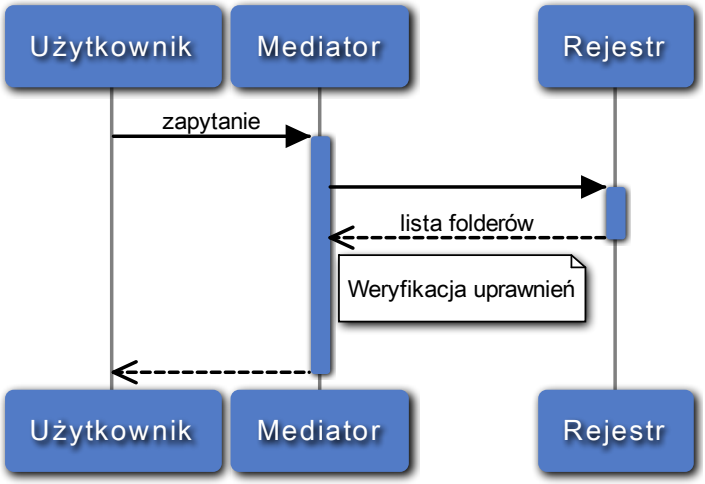
Rysunek 3.5: Diagram sekwencji pobierania dokumentów (UC3).



Rysunek 3.6: Diagram sekwencji pobierania listy pacjentów (UC4).

UC5 Pobieranie folderów pacjenta (Rysunek 3.7)
Aktorzy główni: Użytkownik, Mediator
Aktorzy pomocniczy: Rejestr
Scenariusz:

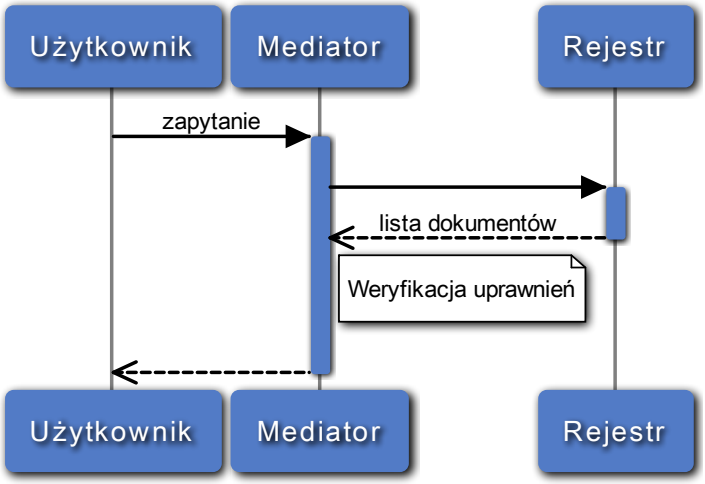
1. Użytkownik wysyła zapytanie o foldery pacjenta do Mediatora.
2. Mediator pobiera foldery pacjenta z Rejestru.
3. Mediator filtruje zapytanie użytkownika zgodnie z uprawnieniami.



Rysunek 3.7: Diagram sekwencji pobierania folderów pacjenta (UC5).

UC6 Pobieranie listy dokumentów (Rysunek 3.8)
Aktorzy główni: Użytkownik, Mediator
Aktorzy pomocniczy: Rejestr
Scenariusz:

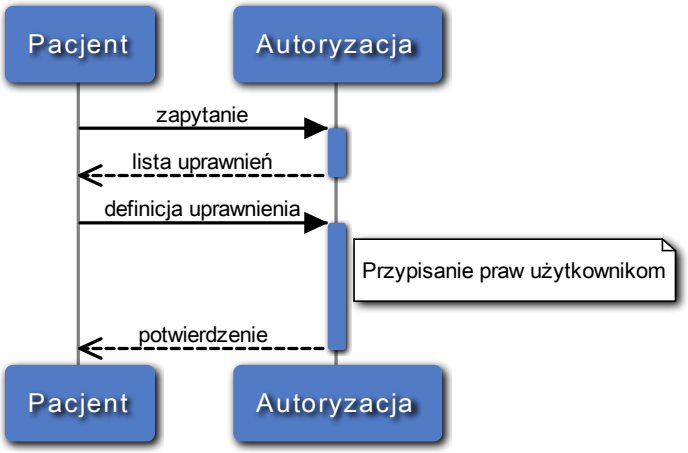
1. Użytkownik wysyła zapytanie o listę dokumentów do Mediatora.
2. Mediator pobiera listę dokumentów z Rejestru.
3. Mediator filtruje zapytanie użytkownika zgodnie z uprawnieniami.



Rysunek 3.8: Diagram sekwencji pobierania listy dokumentów (UC6).

UC7 Przydzielanie uprawnień (Rysunek 3.9)
Aktorzy główni: Pacjent, Autoryzacja
Scenariusz:

1. Pacjent pobiera uprawnienia z Autoryzacji.
2. Pacjent zgłasza Autoryzacji definicje uprawnienia.
3. Autoryzacja przypisuje uprawnienia odpowiednim użytkownikom.



Rysunek 3.9: Diagram sekwencji przydzielania uprawnień (UC7).

3.3 Wymagania pozafunkcjonalne

Wykorzystanie usług sieciowych do zbudowania złożonego procesu działającego w rozproszonym środowisku, wymusza określenie dodatkowych założeń, nie związanych bezpośrednio z jego funkcjami. Dotyczą one m.in. bezpieczeństwa, wydajności oraz sposobu opisu usług.

3.3.1 Regulacje prawne

Projekt realizowany jest z uwzględnieniem aktualnego stanu prawnego. Przeanalizowano m.in. następujące akty prawne:

- *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926, z późn.zm.)* [USTe].

  Ustawa ta dopuszcza [art. 23] przetwarzanie danych osobowych, gdy jest to niezbędne do wypełniania prawnie usprawiedliwionych celów. Dodatkowo pozwala na przetwarzanie danych wrażliwych [art. 27] w celu ochrony stanu zdrowia. Określa także podstawowe założenia dotyczące zabezpieczeń [rozdz. 5].

- *Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz.U. 2006 nr 247, poz. 1819)* [USTc].

  Dokument ten określa jednoznacznie, iż *dokumentacja wewnętrzna* powinna być przechowywana w zakładzie, w którym została sporządzona [§44 ust. 1]. Dodatkowo wymaga się [§55] w celu zachowania czytelności i standaryzacji zapisu danych, że dokumentacja elektroniczna, powinna być sporządzona w formacie XML i podpisana zgodnie z ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. nr 130, poz. 1450, z późn. zm.).

- *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. nr 100, poz. 1024)* [USTa].

  Rozporządzenie definiuje właściwości oraz warunki umożliwiające administratorowi realizację zobowiązań wobec podmiotów danych. W dokumencie tym pojęcie *ochrony danych* utożsa-

miane jest z pojęciem *bezpieczeństwa informacji*. Zgodnie z normą [PI99] przez bezpieczeństwo informacji rozumie się zachowanie: poufności, integralności, dostępności, rozliczalności, au-
tentyczności, niezaprzeczalności i niezawodności (zob. punkt 3.3.4 oraz [Oso07]).

Z uwagi na przetwarzanie danych wrażliwych oraz podłączenie platformy do publicznej sieci telekomunikacyjnej rozporządzenie wymaga stosowania zabezpieczeń na poziomie wysokim [§6].

3.3.2 Udział w projekcie ITSOA

Tworzona platforma stanowi prototyp Obszaru Aplikacyjnego w projekcie ITSOA, który realizuje badania naukowe w zakresie innowacyjnych metod i narzędzi umożliwiających praktyczne zastosowanie paradygmatu SOA w procesie tworzenia nowoczesnych rozwiązań informatycznych. Politechnika Poznańska zajmuje się częścią Obszarów Badawczych opracowujących mechanizmy związane z niezawodnością, bezpieczeństwem i zarządzaniem w środowiskach rozproszonych usług.

Założeniem opisywanego projektu jest zarówno integracja, jak i niezależność od tworzonych w ITSOA narzędzi. Platforma powinna tworzyć samodzielne środowisko usług sieciowych wyposażone we wszystkie mechanizmy pozwalające bezpiecznie realizować założone funkcje. Jednocześnie musi zostać zachowana możliwość integracji z Obszarami Badawczymi, aby w przyszłości stworzyć infrastrukturę o podwyższonej wydajności i niezawodności. Szczególnie istotne mogą być następujące Obszary Badawcze:

- **OB1-4 Detekcja awarii**. Zajmuje się wykrywaniem pojawiających się w systemie nieprawidłowości dzięki wykorzystaniu mechanizmu nazywanego rozproszonym detektorem awarii (ang. *failure detector*).
- **OB2-3 Usługa replikacji**. Pozwala na wprowadzenie wysokiej dostępności i niezawodności przez utrzymywanie wielu kopii usługi na niezależnych węzłach sieciowych, przy jednoczesnym dbaniu o ich spójność.
- **OB7-5 Języki definiowania polityki bezpieczeństwa dla SOA**. Umożliwia definiowanie i weryfikację polityki bezpieczeństwa w środowiskach SOA. Pozwala na globalną konfigurację rozproszonych komponentów w sposób zapewniający jednolity poziom bezpieczeństwa.

3.3.3 Interfejs usług

Ponieważ system opiera się na szeregu usług konieczne jest wybranie dla nich odpowiednich interfejsów. Istnieją dwa główne podejścia do tego zagadnienia: podejście z wykorzystaniem protokołu *SOAP* oraz podejście oparte na paradygmacie *REST*.

SOAP (ang. *Simple Object Access Protocol*) [W3Cb] jest to protokół specyfikujący sposób wymiany informacji pomiędzy usługami przy pomocy zdalnych wywołań procedur *RPC* (ang. *Remote Procedure Call*). Interfejs oparty o ten protokół będzie więc składał się z funkcji, które dana usługa udostępnia. Funkcje te wywoływane są przy pomocy wiadomości zapisanych w formacie XML, przesyłanych najczęściej przy pomocy metody `POST` protokołu HTTP. Podejście takie można porównać do idei programowania strukturalnego.

REST (ang. *REpresentational State Transfer*) [Fie00] opiera się przede wszystkim na zasobach oraz protokole HTTP [FGM+99]. Zasoby identyfikowane są unikatowo poprzez ich ścieżki dostępu *URI* (ang. *Uniform Resource Identifier*), a akcje na nich wywoływane są przy pomocy poleceń protokołu HTTP (`GET, PUT, POST, DELETE`). Ponieważ URI jednoznacznie identyfikuje zasób, więc odwołując się po zasób usługi zawsze powinniśmy otrzymać ten sam wynik. Taką właściwość gwarantuje bezstanowość. Usługi budowane w oparciu o REST reprezentują architekturę zorientowaną na zasoby zwaną *ROA* (ang. *Resource Oriented Architecture*). Takie podejście zasobowe można porównać do idei programowania obiektowego.

Wybór interfejsu determinuje w pewnym stopniu naturalną budowę oraz pewne cechy usług. Oczywiście nic nie stoi na przeszkodzie, aby usługa miała oba interfejsy. Jednak o ile Web Service wykonany zgodnie z paradygmatem REST dość łatwo wyposażyć w dodatkowy interfejs oparty na SOAP, o tyle działanie w przeciwną stronę może sprawić więcej problemów. Ze względu na fakt, iż niektóre operacje trudno zamodelować jako zasoby, czasami stosuje się podejście hybrydowe. Nie jest ono zgodne z paradygmatem REST, ponieważ w podejściu tym odwołanie do zasobu wywołuje funkcję.

Do głównych zalet SOAP należy jego niezależność od protokołu komunikacyjnego. Natomiast w przypadku usług REST dopuszczalny jest jedynie protokół HTTP. Najczęściej jednak oba podejścia stosują protokół HTTP. W takiej sytuacji zdecydowanie więcej korzyści czerpie z tego podejście zasobowe. Wadą jest, że SOAP wywołuje wszystkie żądania metodą `POST`, co wymusza zawieranie semantyki akcji wewnątrz samego zgłoszenia. Mogłoby to zostać z powodzeniem zrealizowane za pomocą metod HTTP, tak jak to jest w przypadku REST.

Kolejną wadą interfejsu w SOAP jest konieczność zgłaszania żądań w formie wiadomości w formacie XML. Powoduje to konieczność przesyłania dużej ilości dodatkowych informacji. W przypadku podejścia REST, żądania zgłaszane są przez wywołanie odpowiedniej metody protokołu HTTP na zadanym URI, reprezentującym zasób. W ten sposób, aby osiągnąć pożądany cel, przesyłane jest minimum informacji przy pełnym wykorzystaniu możliwości protokołu HTTP.

Ze sposobu zgłaszania żądań wynika kolejna przewaga interfejsu REST nad SOAP, a mianowicie czytelność oraz łatwość wywołania. Korzystając z interfejsu zasobowego odwołanie się do adresów usługi może być łatwe i intuicyjne. Przy dobrze zaprojektowanym interfejsie zgodnym z REST nie jest konieczna znajomość dokumentacji. Wykorzystując interfejs SOAP jest to niemożliwe do wykonania bez znajomości dokładnej specyfikacji struktury wiadomości.

Ze względu na opisaną przewagę interfejsu typu REST zostanie on wykorzystany w systemie.

3.3.4 Bezpieczeństwo

Bezpieczeństwo informacji jest jednym z najważniejszych wymagań budowanej platformy. Dokumentacja stanu zdrowia należy do szczególnie chronionych danych osobowych, dlatego konieczne są zabezpieczenia na najwyższym poziomie. Zgodnie z rozporządzeniem Ministra Zdrowia [USTc] system musi być chroniony przed zagrożeniami pochodzącymi z sieci publicznej. W szczególności musi być zapewniona kryptograficzna ochrona danych uwierzytelniających oraz kontrola działań inicjowanych z sieci publicznej.

Na podstawie norm [PS07] i [PI99] określono podstawowe cechy, które tworzona platforma musi zachować:

- **Poufność** - zapewnienie, że informacja nie jest udostępniana nieautoryzowanym podmiotom.
- **Integralność** - zapewnienie, że dane nie zostały zmienione w sposób nieautoryzowany.

- **Dostępność** - zapewnienie bycia osiągalnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
- **Rozliczalność** - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- **Autentyczność** - zapewnienie, że tożsamość podmiotu lub zasobu jest taka jak deklarowana (dotyczy użytkowników, usług i informacji).
- **Niezaprzeczalność** - brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
- **Niezawodność** - zapewnienie spójności oraz zamierzonych zachowań i skutków.

Do platformy zostaną wprowadzone odpowiednie mechanizmy w celu ograniczenia dostępu do danych. Poufność i integralność komunikacji sieciowej będzie zapewniona przez wykorzystanie certyfikatów serwera i protokołów *HTTPS* (ang. *HyperText Transfer Protocol Secure*) oraz *TLS* (ang. *Transport Layer Security*) [Res00].

Podczas korzystania z usług Mediatora i Autoryzacji, od użytkowników platformy wymagane będzie podawanie danych uwierzytelniających. Hasła użytkowników powinny być zabezpieczone także w magazynie danych usługi autoryzacji, aby dodatkowo utrudnić przejęcie danych użytkownika. Ponadto, dla możliwości kontrolowania dostępu do systemu, monitorowane będą także nieudane próby dostępu.

Ze względu na różnorodność udostępnianej przez platformę dokumentacji medycznej, dostęp do niej będzie wyposażony w elastyczny mechanizm reguł autoryzacji. Podmiot danych będzie mógł definiować reguły dostępu dla użytkowników, lekarzy lub placówek medycznych. Reguły te zawierać będą informacje o ograniczeniach:

- czasowych - daty początku i końca obowiązywania reguły,
- typu danych - folder, do którego należy dokumentacja,
- źródła danych - zakład opieki zdrowotnej, w którym utworzono dokumentację,
- powstania danych - daty określające przedział czasowy, w którym dokumentacja powstała.

Platforma zawiera zarówno usługi dostępne dla użytkownika końcowego, jak też wewnętrzne usługi, które tworzą rozproszony system mediacyjny. Dla zapewnienia bezpieczeństwa wewnętrznej komunikacji w platformie wszystkie usługi powinny uwierzytelniać się za pomocą certyfikatów klucza publicznego *X.509* [CSF+08].

Wykorzystywane standardy pozwalają na używanie mechanizmów zapewniających integralność udostępnianej w platformie dokumentacji. Standard reprezentacji danych medycznych HL7 CDA zakłada przechowywanie danych jako dokumenty XML, możliwe jest zatem wykorzystanie rekomendacji *XML Signature* [W3Cc], do ich cyfrowego podpisywania. Ponadto zasady obiegu dokumentów zawarte w IHE XDS, nie pozwalają na modyfikacje dokumentów, a jedynie na tworzenie nowych wersji (punkt 2.3.1). Zasada ta weryfikowana jest przez przechowywany w metadanych skrót *SHA1* dokumentu [EJ01].

Kontrolę nad komunikacją inicjowaną z sieci publicznej oraz niezaprzeczalność należy zapewnić poprzez wykorzystanie mechanizmów historii komunikacji. Powinny one umożliwić odtworzenie pełnej informacji na temat komunikacji sieciowej pomiędzy usługami. Podwyższoną dostępność można zapewnić przez wprowadzenie omawianych wcześniej narzędzi do replikacji i detekcji awarii tworzonych w projekcie ITSOA. Natomiast dla wysokiego poziomu niezawodności, należy wprowadzić w usługach obsługę błędów aplikacyjnych, aby nie dopuścić do utraty spójności danych i zapobiec nieoczekiwanym zachowaniom systemu.

Należy także zapewnić, aby wdrażanie i praca w docelowym środowisku odbywały się bezpiecznie. Pliki konfiguracyjne usług, zawierające kluczowe parametry związane m.in. z zabezpieczeniami powinny być szyfrowane i dostępne do edycji przez stworzoną w ramach tej pracy aplikację administracyjną.

3.3.5 Wydajność

Podobnie jak w każdym systemie informatycznym działającym na zasadzie żądań i odpowiedzi, prezentowana platforma powinna charakteryzować się wysoką wydajnością. Czas obsługi odwołań do usług powinien być minimalizowany. Wykorzystana architektura wielousługowa sprawia, że w systemie pojawia się narzut czasowy związany z komunikacją, co potencjalnie może wpływać niekorzystnie na wydajność. Dodatkowo, duże ilości danych (potencjalnie wiele dokumentów o znacznych rozmiarach) przesyłanych ze Źródła, mogą również negatywnie wpłynąć na ten wskaźnik. Aby rozwiązać ten problem może zostać zastosowanych kilka podejść.

Pierwszym z nich jest wykorzystanie metadanych o dokumentach, które mają być pobrane. Zawierają one bowiem informację o rozmiarze każdego z nich. Dzięki temu w Mediatorze może zostać podjęta ewentualna decyzja o podzieleniu żądania na mniejsze części, co jednocześnie pozwoli na szybsze zwrócenie wyników użytkownikowi. Drugim podejściem jest zastosowanie usług pośredniczących (ang. *Proxy*), które mogłyby zbierać częściowe bądź całe wyniki zapytań i w przypadku tego samego żądania mogłaby zwrócić odpowiednie dane bez ponownego wywoływania usługi.

Rozdział 4

Projekt techniczny

4.1 Architektura

Zgodnie z projektem opisanym w punkcie 3.2.1 platforma składa się z pięciu usług: Źródła, Indeksu, Rejestru, Autoryzacji i Mediatora. Każda z nich pełni oddzielną funkcję w systemie, aby umożliwić jak największą elastyczność budowanej struktury usług sieciowych. Ze względu na prostotę opisu i wykorzystania interfejsy usług są zgodne z paradygmatem REST, a wymieniane wiadomości serializowane są do formatu XML. Pozwala to tworzyć aplikacje i usługi klienckie w dowolnym środowisku programistycznym.

Poszczególne usługi zaimplementowane zostały w architekturze wielowarstwowej, aby tworzenie nowych interfejsów sieciowych lub zmiana systemu baz danych nie wymagała powielania wykonanej już pracy. Podejście takie pozwoliło zbudować moduły programistyczne, które można wykorzystać w przyszłych implementacjach. Zależności pomiędzy poszczególnymi warstwami prezentuje Rysunek 4.1.

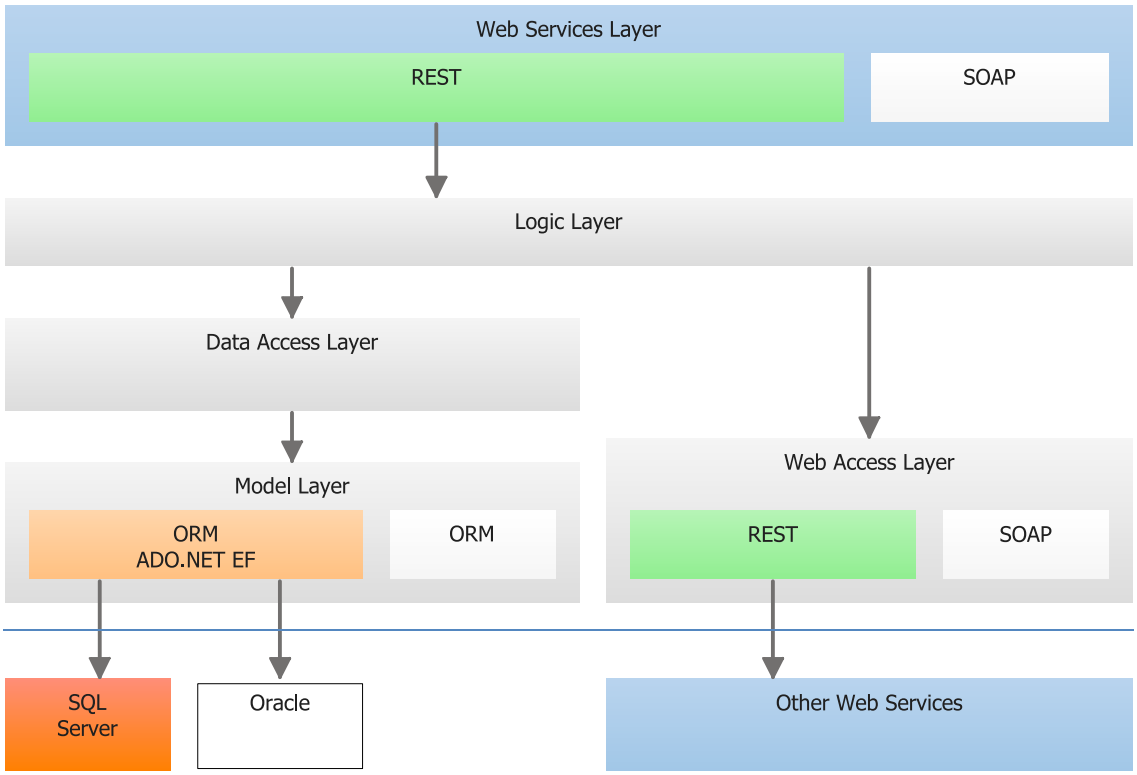
Interfejs usługi zdefiniowany jest w warstwie sieciowej (ang. *Web Service Layer*). W opisywanej pracy zachowano zgodność z paradygmatem REST, jednak zgodnie z wymaganiami projektu ITSOA, w przyszłości będą rozwijane także interfejsy zgodne z SOAP. Warstwa ta ma za zadanie przetransformować dane do postaci niezależnej od sposobu przesyłania i przekazać je do niższej warstwy logiki (ang. *Logic Layer*). Stanowi ona centralną część usługi, która poprzez odwołania do modelu lub innych usług realizuje założoną funkcjonalność.

Warstwa logiki poprzez zaprojektowane interfejsy wykorzystuje warstwy dostępowe do bazy danych oraz usług sieciowych. Dostęp do bazy danych (ang. *Data Access Layer*) pozwala na ukrycie obiektów o strukturze specyficznej dla zaprojektowanych relacji. Dodatkowym pośrednikiem jest warstwa modelu zawierająca moduł *ORM* (ang. *Object-Relational Mapping*), który pozwala automatycznie tworzyć obiekty odpowiadające schematowi encji bazy danych i uniezależnić implementację od używanego *SZBD* (*System Zarządzania Bazą Danych*).

Do interakcji z innymi usługami warstwa logiki wykorzystuje odpowiednie interfejsy, poprzez które pobiera lub wysyła dane niezależnie od interfejsu sieciowego odbiorcy. Warstwa dostępu do sieci (ang. *Web Access Layer*) może wykorzystać specyficzne implementacje klientów usług, dla protokołu SOAP lub REST, co pozostaje transparentne dla warstw wyższych.

4.2 Usługi

Poniższe rozdziały szczegółowe omówienie wszystkich usług wchodzących w skład systemu. Dla każdej z nich zostaną opisane: ogólna zasada działania i realizowane zadania, struktura zasobów oraz schemat bazy danych.



Rysunek 4.1: Architektura warstwowa systemu.

4.2.1 Źródło

W ramach tej usługi można wyróżnić 2 moduły: wrapper oraz repozytorium. Głównym zadaniem repozytorium jest przechowywanie i udostępnianie dokumentów. Wrapper natomiast tłumaczy dane pochodzące z wewnętrznych systemów jednostek medycznych na zgodne z założeniami systemu (dokumenty HL7 CDA oraz komunikaty HL7 ADT).

Wrapper - dokumenty

Jak opisano w poprzednim rozdziale (punkt 3.2.1) zadaniem wrappera jest odczytywanie danych z systemu ewidencyjnego zakładu opieki zdrowotnej. Heterogeniczność systemów HIS wymaga zdefiniowania interfejsów, które będą oprogramowywane specyficznie dla konkretnych rodzajów tych systemów. Platforma udostępnia opis takiego interfejsu, a także implementuje funkcje związane z przygotowaniem pozyskanych danych do przesłania. Przed zgłaszaniem danych ze Źródła do Rejestru, na podstawie pozyskanych przez wrapper dokumentów medycznych w formacie zgodnym z HL7 CDA tworzone są metadane, określana jest przynależność dokumentów do folderów, ustalane są referencje do istniejących pacjentów oraz wykonywane jest grupowanie do postaci zgłoszenia.

Profil IHE XDS zawiera pełny opis metadanych w [IHE09c, Rozdział 4], a także dostarcza przyporządkowanie poszczególnych elementów z dokumentów HL7 CDA opisane w [IHE09e, Rozdział 4]. Definiuje również grupy fragmentów danych składające się na Elektroniczną Kartotekę Pacjenta [IHE09d, Rozdział 6]. Pogrupowanie to zostało wykorzystane do stworzenia zbioru folderów. Ponieważ foldery muszą być przypisywane w Źródle i odczytywane w Rejestrze należy utrzymać spójność pomiędzy tymi dwoma usługami.

Podczas ekstrakcji metadanych z dokumentów tworzone jest również ich powiązanie z folderami. Aby nie narzucać jednostkom zgłaszającym dokumenty korzystania ze zdefiniowanego w systemie

zbioru folderów wprowadzony został system przyporządkowań. Każda sekcja w dokumencie HL7 CDA może zawierać dane należące do innego folderu. W dokumencie poziomu 2 (CDA Level Two) sekcje zawierają obowiązkowo kod opisujący ich zawartość, pochodzący z dowolnego medycznego słownika (np. ICD10, LOINC, SNOMED). W każdej usłudze Źródła dostarczony jest mechanizm przyporządkowywania kodu z dowolnego słownika do odpowiedniego folderu. W ten sposób każde Źródło może posiadać przyporządkowania odpowiednie dla wykorzystywanego przez ZOZ systemu informatycznego.

Wrapper - pacjenci

Wrapper jest także pośrednikiem pomiędzy systemem informatycznym jednostki a indeksem pacjentów platformy. W kodzie aplikacji poprzez zaprojektowane interfejsy możliwa jest obsługa zgłoszeń dotyczących pacjentów. Zgłoszenia te obsługiwane są jako tekstowe komunikaty standardu HL7 w wersji 2.3.1. Jak wspomniano w punkcie 3.2.2, wykorzystywane są komunikaty z grupy ADT:

- tworzenie pacjenta (A01, A04, A05),
- aktualizacja danych (A08),
- łączenie pacjentów (A40).

Są one przygotowywane po stronie Źródła i następnie przekierowywane do Indeksu. Jedyną istotną częścią ww. komunikatów jest segment *PID*, który pozwala przesłać podstawowe dane osobowe pacjentów. Wykorzystywane segmenty komunikatów ADT wymieniono w Tabeli 4.1, a kluczowe pola segmentu PID prezentuje Tabela 4.2.

Szczególnie ważne jest pole PID-3 zawierające listę identyfikatorów, z których każdy zawiera wartość, typ oraz informację o usłudze go przypisującej. W Tabeli 4.3 wyróżniono obsługiwane przez system rodzaje identyfikatorów i przypisano im symbole na podstawie [USTb, Tabela nr 7, zał. nr 3] oraz [HL799, Tabela 0203].

Tabela 4.1: Segmenty komunikatu HL7^ADT wykorzystywane w platformie.

Nazwa segmentu	**Znaczenie**	**Rozdział w [HL799]**
MSG	Nagłówek (ang. *Message Header*)	2
EVN	Typ zdarzenia (ang. *Event type*)	3
PID	Opis pacjenta (ang. *Patient identification*)	3

Tabela 4.2: Istotne pola segmentu PID wykorzystywane w platformie.

Numer	**Długość**	**Wymagany**	**Nazwa**
3	250	HL7	Patient Identifier List
5	250	HL7	Patient Name
7	26	IHE	Date/Time of Birth
8	1	IHE	Administrative Sex

Zarządzaniem tożsamością pacjentów zajmuje się Indeks i to on jest odpowiedzialny za generowanie lub przypisywanie globalnych identyfikatorów pacjenta (UID) do lokalnych identyfikatorów (PI) obowiązujących w Źródle i systemie informatycznym jednostki. Aby nie było konieczne ciągłe odpytywanie Indeksu o UID pacjenta, przy pierwszym odwołaniu do danych pacjenta, zgodnie z IHE *PIX Query* wymieniane są komunikaty `QBP^Q23` (*Get Corresponding Identifiers*) oraz `RSP^K23` (*Get Corresponding Identifiers Response*). Źródło tworzy w ten sposób własne mapowanie przypisujące UID pacjenta do jego lokalnego identyfikatora (PI).

Tabela 4.3: Istotne pola segmentu PID wykorzystywane w platformie.

Nazwa	Symbol	Źródło
Globalny identyfikator pacjenta	UID	-
Wewnętrzny unikatowy identyfikator pacjenta	PI	HL7
Nr PESEL	P	NFZ
Osobisty nr identyfikacyjny	R	NFZ
Seria i numer dowodu osobistego	D	NFZ
Seria i numer paszportu	T	NFZ
Nazwa, numer i seria innego dokumentu	I	NFZ
Numer dokumentacji medycznej	NN	NFZ

Źródło może także odbierać od Indeksu powiadomienia z informacją o łączeniu pacjentów. Informacje takie przesyłane są zgodnie z IHE `PIX Update Notification` za pomocą komunikatu `ADT^A31` (*Update Person Information*) ze standardu HL7 w wersji 2.5.

Jako część platformy zaimplementowano przykładowy moduł wrappera, który imituje szpitalny system ewidencyjny. Opiera się on na systemie plików i przechowywanych w nim dokumentach XML. Docelowo, dla prawdziwych systemów HIS mogą zostać stworzone wrappery eksportujące całe kartoteki pacjentów lub tylko wybraną część danych np. wyniki badań laboratoryjnych.

Repozytorium

Częścią Źródła jest repozytorium odpowiedzialne za wysyłanie zgłoszeń oraz udostępnianie dokumentów. Profil IHE XDS nie pozwala na operacje modyfikacji dokumentów, a jedynie na zmianę statusu dokumentu na nieaktualny (ang. *Deprecated*) oraz zgłoszenie aktualnego. Jest to warunek trudny do spełnienia ze względu na efektywność, ponieważ wymagałoby to przechowywania wszystkich zgłoszonych dokumentów w dedykowanej do tego celu bazie danych w ramach repozytorium lub utrzymywania przez system ewidencyjny jednostki danych historycznych. Wprowadzono zatem następujące tryby pracy:

- **Store** - oznacza przechowywanie każdego dokumentu zgłaszanego do repozytorium. Zapewnia pełną zgodność z profilem IHE XDS, ale jednocześnie wymaga utrzymania w repozytorium bazy danych z dużą ilością danych binarnych.

- **Cache** - oznacza przechowywanie w bazie danych repozytorium tylko tych dokumentów, które zostały chociaż raz pobrane. Tryb ten jest bardziej efektywny w zakresie zajmowanej pamięci, jednak może powodować niezgodności dokumentu pobieranego pierwszy raz z jego metadanymi, zgłoszonymi wcześniej.

- **None** - oznacza, iż dokumenty nie są przechowywane. Przy każdym żądaniu o dokumenty, repozytorium przekierowuje zapytanie do wrappera, aby pozyskać dokument z systemu ewidencyjnego.

Podstawową cechą odróżniającą repozytorium od wrappera jest postać przetwarzanego dokumentu. Wrapper zakłada, że dokumenty mają format zgodny z HL7 CDA i na tej podstawie potrafi wydobyć z nich dane. Natomiast w ramach repozytorium dokumenty przetwarzane są w postaci binarnej i udostępniane jako ciąg znaków zakodowany w formacie *Base64* [Jos06]. Umożliwia to w przyszłości rozwinięcie systemu do składowania dokumentów w dowolnym innym formacie, szczególnie obrazów wymienianych przez stacje radiologiczne.

Zasoby

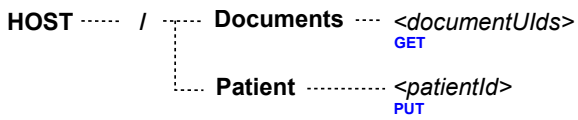
Rysunek 4.2 prezentuje schemat URI dla zasobów Źródła, opisanych poniżej.

adres URI: `/Documents/<documentUIds>`

`GET` Pobiera dokumenty o identyfikatorach podanych jako `<documentUIds>`. Realizuje transakcję `Retrieve Document Set [ITI-43]` opisaną w punkcie 2.3.1.

adres URI: `/Patient/<patientId>`

`PUT` Aktualizuje w Źródle odwzorowanie lokalnych identyfikatorów pacjenta na globalne.



Rysunek 4.2: Schemat URI dla zasobów Źródła.

Schemat bazy danych

Na Rysunku 4.3 zaprezentowano schemat bazy danych Źródła. Przedstawia on tabele oraz relacje miedzy nimi (tekstem wytłuszczonym zaznaczono także pola obowiązkowe):

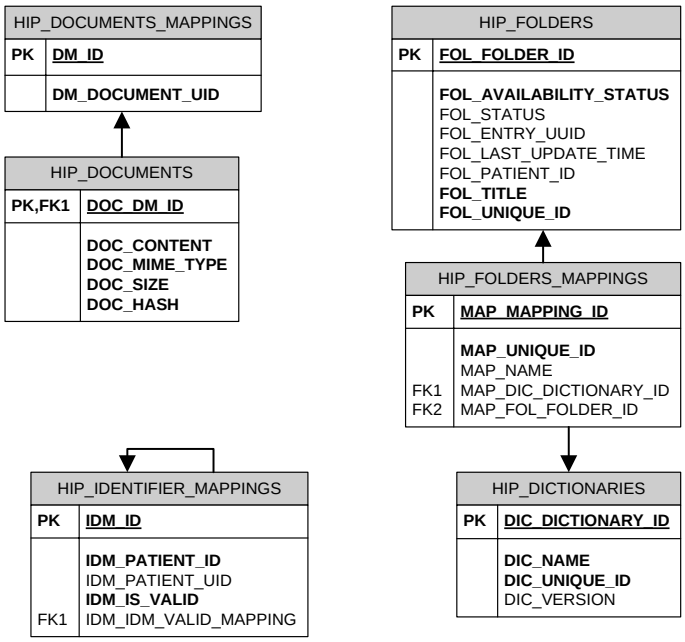
- `HIP_DOCUMENTS`
  Przechowuje zawartość dokumentów w postaci binarnej oraz podstawowe informacje o nich.
- `HIP_DOCUMENT_MAPPINGS`
  Przechowuje przypisanie dokumentu do unikatowego identyfikatora.
- `HIP_IDENTIFIER_MAPPINGS`
  Zawiera mapowanie identyfikatorów pacjentów na ich UID przydzielony przez Indeks.
- `HIP_DICTIONARIES`
  Stanowi spis słowników, z których pochodzą kody sekcji zgłaszanych dokumentów.
- `HIP_FOLDERS`
  Zawiera spis folderów wykorzystywanych w platformie.
- `HIP_FOLDERS_MAPPINGS`
  Przechowuje przyporządkowanie wartości kodów ze słowników do folderów.

4.2.2 Indeks

Głównym celem Indeksu jest zarządzanie identyfikacją pacjentów i danymi osobowymi. Tworzy on eMPI (ang. *Enterprise Master Patient Index*), łącząc aktorów `Patient Identifier Cross-reference Manager` i `Patient Identity Source` z profilu IHE PIX. Dodatkowo ustalono, że poszczególne Źródła będą stanowić osobne domeny (zob. punkt 2.3.2).

Odbierając zgłoszenia od Źródeł usługa ta gromadzi dane przesyłane w segmencie PID komunikatów HL7^ADT. W wykonanej implementacji zapamiętywane są tylko podstawowe dane:

- identyfikatory
- imię i nazwisko
- data urodzenia oraz płeć



Rysunek 4.3: Schemat bazy danych usługi źródła.

Dane te są udostępniane jedynie do wewnętrznej komunikacji, dla usług należących do platformy. Jednak najważniejszym zadaniem Indeksu jest zarządzanie tworzeniem i przypisywaniem globalnych identyfikatorów pacjentów, które są podstawowym środkiem identyfikacji pacjenta w innych usługach.

Szczegółowo rodzaje gromadzonych identyfikatorów opisano w punkcie 4.2.1. Po odebraniu od Źródła zgłoszenia z informacjami o nowym pacjencie Indeks sprawdza, czy nie istnieje już pacjent o identycznym którymkolwiek z identyfikatorów (z wyjątkiem *Numeru dokumentacji medycznej*). Gdy zostanie on znaleziony, przypisuje się jedynie przesłane identyfikatory do istniejącego pacjenta, w przeciwnym przypadku generowany jest nowy UID pacjenta zgodnie z opisem w punkcie 3.2.2.

Powiadomienia

Dla utrzymania spójności powiązań pomiędzy pacjentami a dokumentami lub prawami dostępu, ważne jest, aby usługi były powiadamiane o tworzonych identyfikatorach pacjentów lub łączeniu pacjentów. Zaimplementowano mechanizm asynchronicznego rozsyłania takich wiadomości w ramach obsługi zgłaszania komunikatów ze Źródła. Asynchroniczność w tym przypadku oznacza jedynie, że zakończenie rozsyłania tych wiadomości nie jest konieczne do zakończenia odbioru samego zgłoszenia ze Źródła. Każda wiadomość jest zapamiętywana w bazie danych i usuwana tylko w przypadku odebrania komunikatu przez usługę adresata, tak aby umożliwić retransmisję w przypadku błędów lub niedostępności usług.

Rozsyłanie powiadomień nie odbywa się zgodnie z istniejącymi standardami. Powodem takiej decyzji jest chęć maksymalnego uproszczenia implementacji odbioru tych powiadomień w innych usługach.

Zasoby

Rysunek 4.4 prezentuje schemat URI dla zasobów Indeksu, opisanych poniżej.

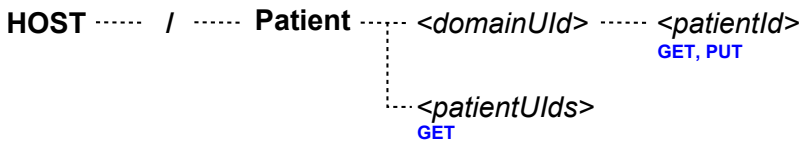
adres URI: `/Patient/<domainUId>/<patientId>`

`GET` Pobiera informacje o identyfikatorach pacjenta o identyfikatorze `<patientId>` w domenie identyfikowanej przez `<domainUId>`.

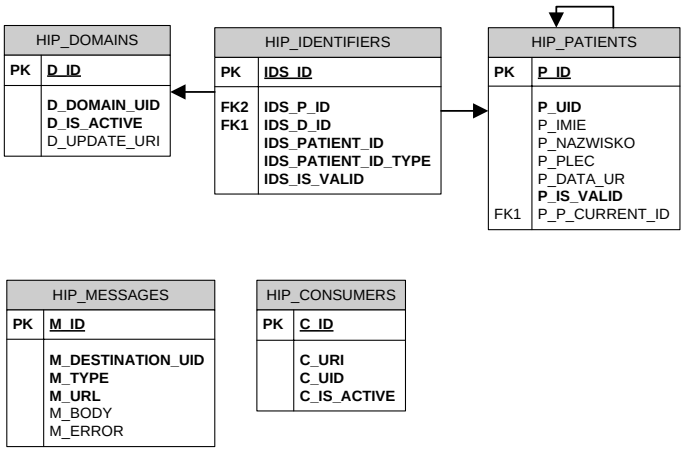
`PUT` Dostarcza informacji o identyfikatorach pacjenta. Realizuje transakcję `Patient Identity Feed [ITI-8]` opisaną w punkcie 2.3.2.

adres URI: `/Patient/<patientUIds>`

`GET` Pobiera informacje o pacjentach identyfikowanych przez identyfikatory globalne przekazane w `<patientUIds>`.



Rysunek 4.4: Struktura URI dla zasobów Indeksu.



Rysunek 4.5: Schemat bazy danych usługi Indeksu.

Schemat bazy danych

Na Rysunku 4.5 zaprezentowano schemat bazy danych Indeksu. Przedstawia on tabele oraz relacje miedzy nimi (tekstem wytłuszczonym zaznaczono także pola obowiązkowe):

- `HIP_DOMAINS`
  Przechowuje informacje o usługach Źródeł, które zgłaszają pacjentów do Indeksu.
- `HIP_PATIENTS`
  Zawiera podstawowe informacje o pacjentach.
- `HIP_IDENTIFIERS`
  Przechowuje identyfikatory pacjentów.
- `HIP_MESSAGES`
  Wykorzystywana jest do monitorowania komunikacji asynchronicznej.
- `HIP_CONSUMERS`
  Zawiera informacje o usługach, do których wysyłane są powiadomienia.

4.2.3 Rejestr

Zgodnie z opisem zawartym w IHE XDS Rejestr przechowuje zgłoszenia, foldery oraz metadane o dokumentach, przesyłane ze Źródła. Zawierają one kompletną informację potrzebną do prawidłowego realizowania wszystkich funkcji udostępnianych przez Rejestr. Na usługę tę można, pod kątem pełnionych przez nią funkcji, spojrzeć z dwóch perspektyw: od strony Źródła i Indeksu (przyjmowanie danych) oraz od strony Mediatora (odpowiadanie na zapytania o dane).

Zasilanie danymi

Źródło przesyła do Rejestru zgłoszenia zapisane zgodnie ze standardem ebXML, a ten zamienia je na odpowiednie struktury reprezentujące metadane. Na tym etapie sprawdzana jest również poprawność oraz kompletność przesyłanych danych. W przypadku, gdy zgłoszenie jest niepoprawne Rejestr informuje o tym Źródło w wiadomości zwrotnej. Źródło musi wówczas wycofać operację zapisu zgłaszanych dokumentów do bazy (w przypadku, gdy znajduje się w trybie Store).

Po wstępnym sprawdzeniu poprawności danych mogą one zostać zapisane do bazy Rejestru. Najpierw sprawdzane jest, czy zgłoszenie o tym samym identyfikatorze nie było już przesyłane – jeśli tak, jest ono odrzucane. Następnie Rejestr sprawdza, czy informacja o pacjencie, którego dotyczy zgłoszenie, istnieje – jeśli nie, tworzony jest nowy wpis. Następnie zgłoszenie wiązane jest z uzyskaną informacją o pacjencie. Warto zauważyć, iż w Rejestrze źródłem informacji o pacjentach są dokumenty – Indeks przesyła jedynie informacje dotyczące zmian w sposobie ich identyfikacji.

W kolejnym kroku, dla każdego dokumentu w zgłoszeniu poszukiwany jest w bazie dokument o tym samym identyfikatorze. Jeśli zostanie odnaleziony, wówczas oznaczany jest jako nieaktywny, a dokument ze zgłoszenia wstawiany jest jako aktywny. Ważne jest, że dla zbioru dokumentów o tych samych identyfikatorach tylko jeden z nich może być aktywny. Dodatkowo, pomiędzy każdym dokumentem a Źródłem, z którego pochodzi, wstawiane jest powiązanie. Dopiero taka informacja pozwala jednoznacznie identyfikować dokumenty, gdyż ich identyfikatory są unikatowe jedynie w obrębie Źródeł. Każdy dokument wiązany jest również z uzyskanym wcześniej pacjentem, autorem oraz zgłoszeniem.

W ostatnim kroku, dla każdego dokumentu pobierane są wszystkie połączone z nim foldery i dla każdego z nich tworzone jest wiązanie pomiędzy dokumentem, folderem oraz zgłoszeniem. Musi tak być z dwóch powodów. Po pierwsze, zgodnie z IHE XDS, w zgłoszeniu mogą być przesyłane nowe foldery. W omawianym projekcie funkcja ta nie jest wykorzystywana, gdyż zbiór folderów jest z góry zdefiniowany, ale została uwzględniona w celu utrzymania zgodności ze standardem. Podejście takie wymusza jednak utrzymanie spójności informacji o folderach pomiędzy Rejestrem a Źródłem. Drugim powodem jest możliwość przesłania w zgłoszeniu samego powiązania pomiędzy zgłoszonym już wcześniej dokumentem oraz folderem. Dodatkowo, gdy w Rejestrze po raz pierwszy pojawi się dokument w dowolnym folderze, wówczas tworzone jest mapowanie tego folderu na folder pacjenta, ponieważ zgodnie z IHE XDS foldery powinny być unikatowo przypisane do pacjentów. Dlatego też, aby zapewnić zgodność ze standardem oraz jednocześnie zdefiniować spójny zbiór folderów podjęto decyzję o takiej ich organizacji.

Pobieranie danych

Pobieranie danych z Rejestru odbywa się poprzez odwołanie do zasobu `Stored Query` z parametrem określającym zapytanie. Pula tych zapytań jest zdefiniowana przez profil IHE XDS i wymieniona w [IHE09b, Rozdział 3.18]. W omawianym projekcie wykorzystano trzy z nich:

- `GetFolders` - pobiera listę folderów pacjenta.

- `GetFolderAndContents` - pobiera foldery pacjenta oraz powiązane z nimi metadane dokumentów dla określonego w parametrze identyfikatora folderu.
- `GetDocuments` - pobiera metadane o dokumentach pacjenta wymienionych w zgłoszeniu jako lista identyfikatorów.

Ważną cechą wymienionych zapytań jest ich zorientowanie na pacjenta. Pomimo, iż dokument jest głównym obiektem Rejestru, system ma udostępniać dane należące tylko do jednego pacjenta. Dlatego każde zapytanie przyjmuje jako jeden z argumentów jego identyfikator, pomimo faktu, iż nie jest to niezbędne w celu uzyskania żądanych danych. Jest to więc element dodatkowej walidacji żądania. Jeśli identyfikator pacjenta nie zgadza się z folderem lub dokumentem, Rejestr nie zwróci żądanego zasobu.

Łączenie pacjentów

Operacja łączenia danych o dwóch różnych pacjentach jest w omawianym systemie bardzo istotna i wbrew pozorom może zachodzić dość często. Ponieważ dane o pacjencie są informacją poufną i bardzo ważną, operacja ta musi być w pełni odwracalna, by zapobiec sytuacjom, w których przez pomyłkę dane te zostałyby utracone. Aby to zapewnić procedura łączenia została zaprojektowana w sposób opisany poniżej.

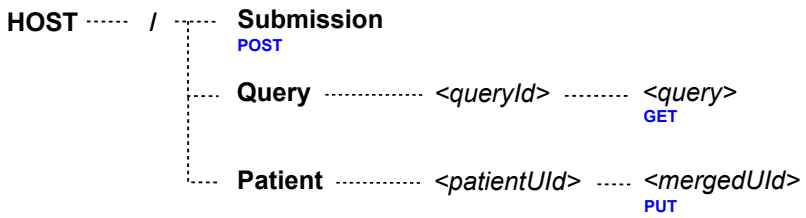
Operacja przyjmuje jako parametry wejściowe dwa unikatowe identyfikatory pacjentów, z których jeden będzie identyfikatorem połączonego pacjenta. Najpierw pobierane są więc informacje o obu pacjentach. Jeśli choćby jeden z pacjentów nie istnieje, bądź ma nieaktywny status, wówczas operacja połączenia jest anulowana. W przeciwnym przypadku tworzony jest nowy pacjent z identyfikatorem wskazanego spośród dwóch przesłanych. Za wskazanie identyfikatora, którym ma być identyfikowany pacjent po połączeniu, odpowiedzialne jest Źródło.

Kolejnym krokiem jest powiązanie danych obu pacjentów do nowego. W tym celu, dla obu pacjentów pobierane są ich dokumenty i przypisywane do nowego pacjenta. Stare powiązania pomiędzy dokumentami a pacjentami są zachowywane, aby umożliwić wycofanie tej operacji. Następnie tworzone są powiązania do folderów pacjenta. W tym wypadku dla nowego pacjenta tworzone są nowe przypisania folderów będące sumą logiczną folderów łączonych pacjentów.

Ostatnim krokiem jest ustawienie statusów łączonych pacjentów na nieaktywne a statusu nowego pacjenta na aktywny i zapisanie go do bazy danych. Takie zaprojektowanie omawianej operacji powoduje, że zawsze można odtworzyć historię wszystkich jej wywołań, ponieważ łączeni pacjenci tworzą hierarchiczną strukturę powiązań, z najnowszym pacjentem w korzeniu (na szczycie hierarchii).

Zasoby

Rysunek 4.6 prezentuje schemat URI dla zasobów Rejestru, opisanych poniżej.



Rysunek 4.6: Schemat URI dla zasobów Rejestru.

adres URI: `/Submission`

`POST` Zapisuje zgłoszenie zawierające metadane o dokumentach. Realizuje transakcję `Register Document Set [ITI-42]` opisaną w punkcie 2.3.1.

adres URI: `/Query/<queryId>/<query>`

`GET` Wywołuje zapytanie `StoredQuery` identyfikowane przez `<queryId>` z listą parametrów przekazanych jako `<query>`. Realizuje transakcję `Registry Stored Query [ITI-18]` opisaną w punkcie 2.3.1.

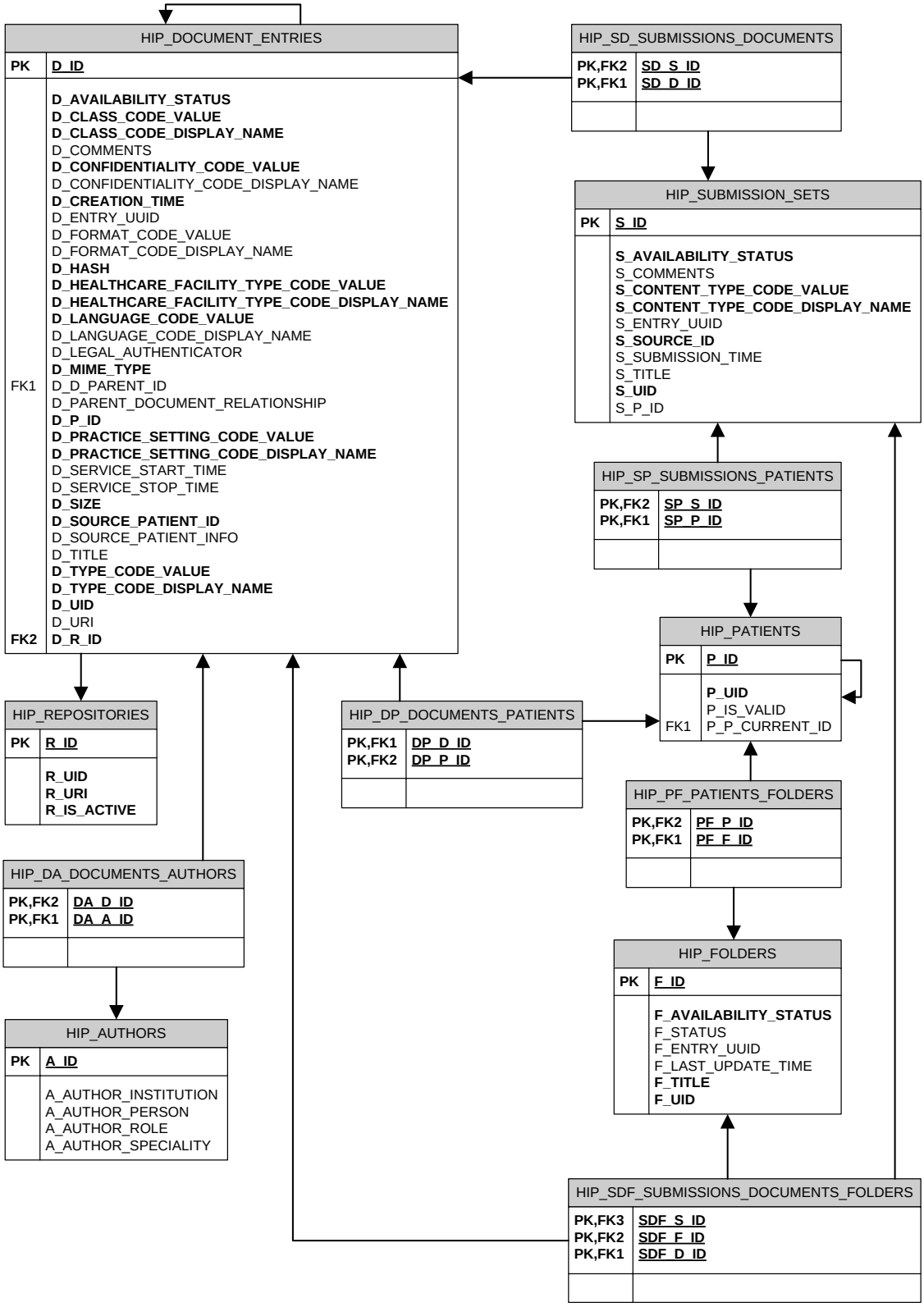
adres URI: `/Patient/<patientUId>/<mergedUId>`

`PUT` Powoduje połączenie dwóch pacjentów identyfikowanych przez `<patientUId>` oraz `<mergedUId>` w jednego pacjenta o identyfikatorze `<patientUId>`.

Schemat bazy danych

Na Rysunku 4.7 zaprezentowano schemat bazy danych Rejestru. Przedstawia on tabele oraz relacje miedzy nimi (tekstem wytłuszczonym zaznaczono także pola obowiązkowe):

- `HIP_DOCUMENT_ENTRIES`
  Przechowuje metadane, każdego zgłoszonego dokumentu.
- `HIP_REPOSITORIES`
  Stanowi katalog Źródeł, z których mogą być zgłaszane dokumenty.
- `HIP_AUTHORS`
  Zawiera spis autorów zgłaszanych dokumentów.
- `HIP_DA_DOCUMENTS_AUTHORS`
  Przechowuje powiązania dokumentów i ich autorów.
- `HIP_PATIENTS`
  Stanowi spis identyfikatorów pacjentów. Tabela ta jest wypełniana na podstawie zgłaszanych dokumentów. Jednak może być modyfikowana zgodnie z komunikatami przesyłanymi z Indeksu.
- `HIP_DP_DOCUMENTS_PATIENTS`
  Zawiera powiązania pacjentów z ich dokumentami.
- `HIP_SUBMISSION_SETS`
  Przechowuje metadane zgłoszeń.
- `HIP_SD_SUBMISSIONS_DOCUMENTS`
  Przyporządkowuje dokumenty do zgłoszeń.
- `HIP_SP_SUBMISSIONS_PATIENTS`
  Zawiera powiązania pacjentów ze zgłoszeniami.
- `HIP_FOLDERS`
  Stanowi spis rozpoznawanych w platformie folderów.
- `HIP_PF_PATIENTS_FOLDERS`
  Przechowuje informacje o dostępnych folderach, w których danym pacjent posiada dokumenty oraz ich unikatowe identyfikatory.
- `HIP_SDF_SUBMISSIONS_DOCUMENTS_FOLDERS`
  Zawiera informacje o tym, w którym zgłoszeniu zostało przesłane przyporządkowanie dokumentu do folderu.



Rysunek 4.7: Schemat bazy danych usługi Rejestru.

4.2.4 Autoryzacja

Zgodnie z opisem z punktu 3.2.1 usługa Autoryzacji powinna zarządzać dostępem do danych w systemie. W tym celu stworzony został system uprawnień przydzielanych użytkownikom, które obowiązują po jego zalogowaniu. Głównym punktem odniesienia jest pacjent, do którego informacji ma zostać przydzielone uprawnienie dla użytkownika lub jednostki medycznej. Użytkownik w systemie może (lecz nie musi) być pacjentem lub lekarzem. Lekarz z kolei może należeć do wielu jednostek medycznych. Przydzielenie prawa dla jednostki medycznej oznacza więc przydzielenie go wszystkim lekarzom jej podlegającym.

Każdy pacjent jest właścicielem swoich danych medycznych i jako taki może udzielać do nich dostępu. Dostęp ten może zostać przydzielony na czas określony bądź nieokreślony. Przedmiotem podlegającym restrykcjom dostępu są dane pacjenta. Pojedyncze uprawnienie może udzielać dostępu do wszystkich danych pacjenta lub zawężać ich zbiór poprzez specyfikację konkretnych ograniczeń. W systemie zdefiniowano trzy możliwe sposoby ograniczenia zbioru danych przez określenie:

- identyfikatora folderu,
- identyfikatora Źródła,
- przedziału czasowego, w którym dane powstały.

Pomimo zdefiniowania zbioru możliwych sposobów ograniczenia zwracanych użytkownikowi danych, bardzo łatwe jest jego rozszerzenie o dodatkowe ograniczenia. Zapewnia to regułowy sposób zapisu ograniczeń. Pojedyncza reguła może więc zawężać dane pacjenta wykorzystując kilka opisanych ograniczeń jednocześnie. Reguła ma postać ciągu znaków. Może to być stała wartość `*` oznaczająca pełen dostęp lub lista nazwanych parametrów w formacie:

`param1=wartosc1&param2=wartosc2`.

Obsługiwane parametry to: `folder`, `source`, `before`, `after` i odpowiadają one wymienionym powyżej sposobom ograniczenia dostępu do danych.

W docelowym środowisku działania ważne jest ścisłe kontrolowane dodawania powiązań pomiędzy lekarzami a jednostkami, tak aby uniemożliwić dostęp osobom nieuprawnionym. Jeszcze bardziej istotna jest procedura powiązania pacjenta z użytkownikiem platformy. Błędy lub ingerencje w te dane oznaczałyby pełen dostęp do dokumentacji pacjenta oraz możliwość dodawania uprawnień dostępu innym osobom.

Zasoby

Zasoby Autoryzacji zostały podzielone na dwie części ze względu ich dostępność. Pierwsza część jest dostępna z zewnątrz jako API platformy. Wykorzystywana jest do zbudowania w aplikacjach klienckich modułu do zarządzania uprawnieniami. Rysunek 4.8 prezentuje schemat URI dla zasobów Autoryzacji, opisanych poniżej.

Druga cześć zasobów dostępna jest tylko dla wewnętrznej komunikacji platformy, związanej ze zgłaszaniem nowych identyfikatorów pacjentów oraz informacji o ich łączeniu.

adres URI: `/User`

`GET` Pobiera informacje o zalogowanym użytkowniku.

adres URI: `/Units`

`GET` Pobiera informacje o dostępnych jednostkach medycznych.

adres URI: `/Sources`

`GET` Pobiera informacje o dostępnych Źródłach.

adres URI: `/Right`

`GET` Pobiera informacje o uprawnieniach nadanych innym użytkownikom do pacjenta związanego z bieżącym użytkownikiem.

`POST` Wstawia uprawnienie do danych pacjenta związanego z bieżącym użytkownikiem.

adres URI: `/Right/<rightUId>`

`GET` Pobiera informacje o uprawnieniu o identyfikatorze `<rightUId>`.

`PUT` Modyfikuje uprawnienie o identyfikatorze `<rightUId>`.

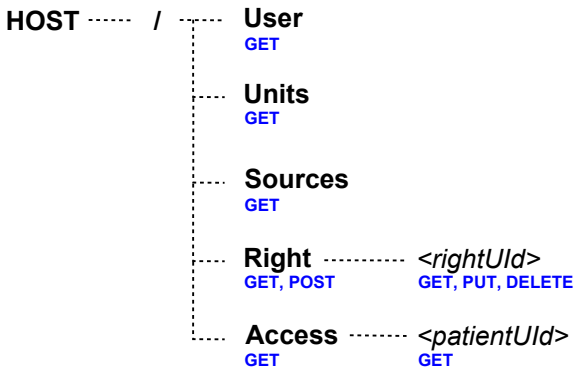
`DELETE` Usuwa uprawnienie o identyfikatorze `<rightUId>`.

adres URI: `/Access`

`GET` Pobiera informacje o uprawnieniach bieżącego użytkownika.

adres URI: `/Access/<patientUId>`

`GET` Pobiera informacje o uprawnieniach bieżącego użytkownika do pacjenta o identyfikatorze `<patientUId>`.



Rysunek 4.8: Schemat URI dla zasobów Autoryzacji.

adres URI: `/Patient/<patientUId>`

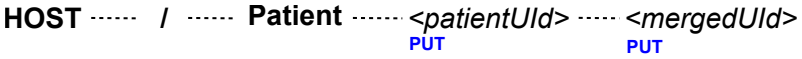
`PUT` Zgłasza nowy globalny identyfikator pacjenta.

adres URI: `/Patient/<patientUId>/<mergedUId>`

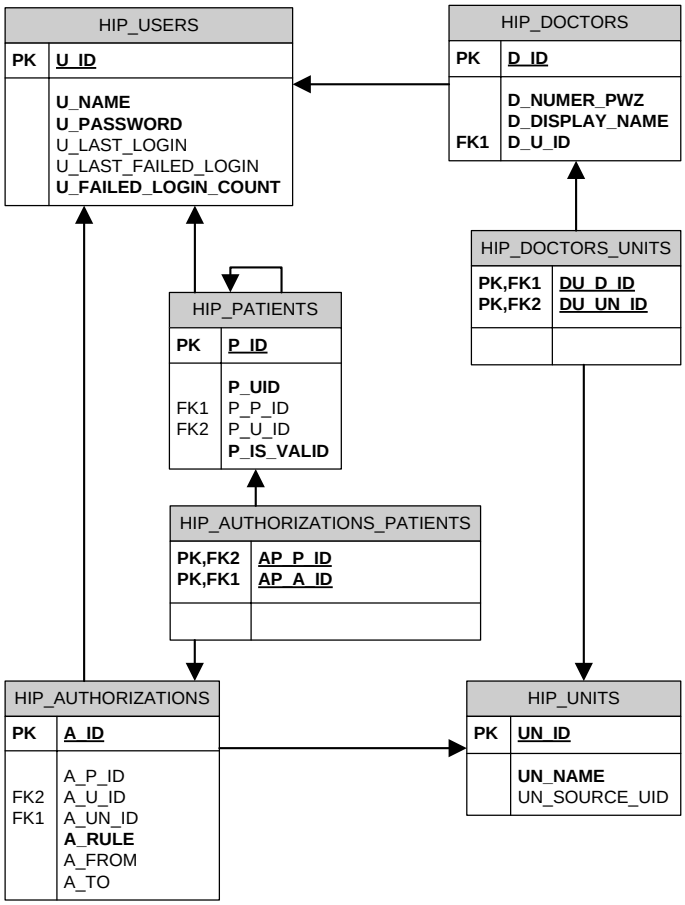
`PUT` Powoduje połączenie dwóch pacjentów identyfikowanych przez `<patientUId>` oraz `<mergedUId>` w jednego pacjenta o identyfikatorze `<patientUId>`.

Schemat bazy danych

Na Rysunku 4.10 zaprezentowano schemat bazy danych Autoryzacji. Przedstawia on tabele oraz relacje miedzy nimi (tekstem wytłuszczonym zaznaczono także pola obowiązkowe):



Rysunek 4.9: Zasoby Autoryzacji dostępne wewnątrz platformy.



Rysunek 4.10: Schemat bazy danych usługi Autoryzacji.

- `HIP_USERS`
  Zawiera dane związane z logowaniem użytkowników.
- `HIP_PATIENTS`
  Przechowuje globalne identyfikatory pacjentów.
- `HIP_DOCTORS`
  Zawiera informacje o lekarzach.
- `HIP_UNITS`
  Przechowuje informacje o jednostkach, którym można przydzielić uprawnienia.
- `HIP_DOCTORS_UNITS`
  Przyporządkowuje lekarzy do jednostek medycznych.
- `HIP_AUTHORIZATIONS`
  Zawiera dane dotyczące reguł autoryzacji.
- `HIP_AUTHORIZATIONS_PATIENTS`
  Przechowuje powiązania reguł dostępu z pacjentami, których dotyczą.

4.2.5 Mediator

Mediator jest usługą udostępniającą interfejs dla użytkownika końcowego, w pełni umożliwiający korzystanie z systemu. Zgodnie z profilem IHE XDS Mediator jest aktorem `Document Consumer`, jednak jego specyfikacja nie podlega już pod ten standard. Wiadomo jedynie, że pobiera z Rejestru metadane i na podstawie otrzymanej informacji ewentualnie pobiera ze Źródła konkretne dokumenty. Warto zauważyć, że Mediator nie zna lokalizacji Źródeł. Musi posiadać jedynie listę aktywnych Rejestrów zawierającą unikatowy identyfikator i adres.

Podstawowym zasobem Mediatora jest lista pacjentów, która może być pobrana na kilka sposobów: z bazy danych, z Indeksu lub z usługi Autoryzacji. W omawianym systemie wykorzystany został sposób pierwszy, jednak Mediator wywołuje w tym celu logikę usługi Autoryzacji, gdyż baza danych jest dla obu usług współdzielona. Zwracana lista jest ograniczona zgodnie z uprawnieniami bieżącego użytkownika.

Drugą funkcją Mediatora jest udostępnienie listy folderów danego pacjenta. Gdy odebrane zostanie takie żądanie usługa wywołuje w Rejestrze `StoredQuery` podając jako nazwę zapytania `GetFolders` oraz identyfikator pacjenta jako parametr zapytania. Odebrany wynik w formacie zgodnym z ebXML tłumaczony jest na strukturę metadanych i zwracany w takiej postaci, ponieważ Mediatora nie obowiązuje już konieczność przesyłania danych w tym standardzie.

Następnym żądaniem obsługiwanym przez Mediator jest lista metadanych o dokumentach. Przypadek ten jest bardzo podobny do żądania listy pacjentów, przy czym tym razem w Rejestrze wywoływane jest `StoredQuery` z zapytaniem `GetFolderAndContents`, które jako parametry przyjmuje opcjonalnie, poza obowiązkowym identyfikatorem pacjenta, identyfikator folderu pacjenta oraz identyfikator źródła danych. Jako wynik Mediator zwraca listę metadanych o dokumentach wraz z ich przynależnością do odpowiednich folderów, opcjonalnie przefiltrowaną po wybranym folderze lub Źródle, z którego pochodzą.

Kolejnym żądaniem, które obsługuje Mediator jest lista dokumentów. Podobnie jak przy poprzednich żądaniach, usługa wywołuje `StoredQuery` w Rejestrze, tym razem z zapytaniem `GetDocuments` przyjmującym jako parametr identyfikatory dokumentów i zwracającym listę metadanych. Następnie, dla każdego dokumentu wyciągany jest z metadanych jego identyfikator oraz adres Źródła, w którym się znajduje. Na tej podstawie, oraz wiedzy o budowie usługi, tworzony jest adres zasobu, którego żąda Mediator wywołując tym samym funkcję `RetrieveDocumentSet` z odpowiedniego Źródła. W wyniku tej operacji Mediator otrzymuje listę dokumentów w binarnym formacie i przesyła je jako wynik całej operacji w formacie XML.

Ostatnim zasobem przewidzianym w Mediatorze cała zawartość folderu. Najpierw wywoływane jest `StoredQuery GetFolderAndContents`, a następnie analogicznie jak w przypadku listy dokumentów - `RetrieveDocumentSet` do odpowiednich Źródeł. Po zebraniu wszystkich dokumentów wycinane są z nich segmenty nienależące do folderu będącego parametrem wywołania operacji. Następnie Mediator zwraca te dokumenty jako odpowiedź na żądanie.

Zasoby

Rysunek 4.11 prezentuje schemat URI dla zasobów Mediatora, opisanych poniżej.

adres URI: `/`

`GET` Pobiera listę pacjentów, do których bieżący użytkownik ma uprawnienia.

adres URI: `/<patientUId>/Folders?source=<sourceIUd>`

`GET` Pobiera foldery pacjenta o identyfikatorze `<patientUId>`. Opcjonalnie lista może być przefiltrowana po Źródle identyfikowanym `<sourceUId>`.

adres URI: `/<patientUId>/Folders/<folderUId>?source=<sourceIUd>`

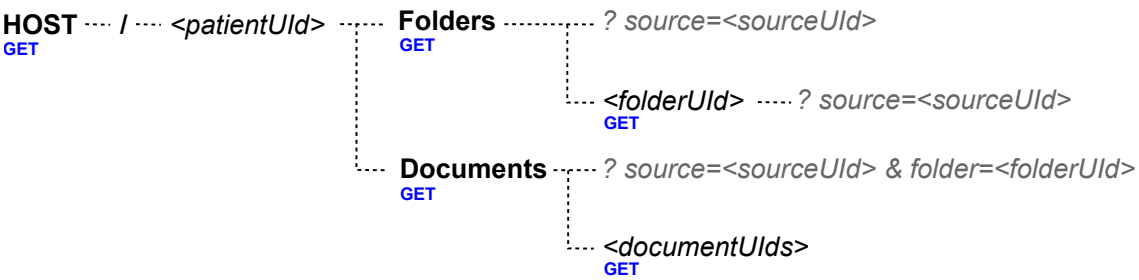
`GET` Pobiera listę metadanych dokumentów pacjenta o identyfikatorze `<patientUId>` należących do folderu identyfikowanego przez `<folderUId>`. Opcjonalnie lista może być przefiltrowana po Źródle identyfikowanym `<sourceUId>`.

adres URI: `/<patientUId>/Documents?folder=<folderUId>&source=<sourceIUd>`

`GET` Pobiera metadane dokumentów pacjenta o identyfikatorze `<patientUId>`. Opcjonalnie lista może być przefiltrowana po Źródle identyfikowanym przez `<sourceUId>` oraz po folderze identyfikowanym przez `<folderUId>`.

adres URI: `/<patientUId>/Documents/<documentUIds>`

`GET` Pobiera dokumenty wymienione identyfikatorami w `<documentUIds>` należące do pacjenta o identyfikatorze `<patientUId>`.



Rysunek 4.11: Schemat URI dla zasobów Mediatora.

4.2.6 Mechanizmy wspólne

Ustawienia

Każda usługa posiada zestaw parametrów konfiguracyjnych związanych ze swoim działaniem, bezpieczeństwem oraz dostępem do danych lub usług. Do najważniejszych ustawień należą:

- unikatowy identyfikator usługi
- identyfikatory i adresy innych usług
- rodzaj interfejsu sieciowego do obsługi komunikacji wychodzącej (REST, SOAP)
- parametry logu

- parametry historii komunikacji
- parametry zabezpieczeń

Ustawienia są przechowywane zarówno w plikach konfiguracyjnych usług jak i w bazie danych (np. w przypadku wielu usług tego samego typu uczestniczących w komunikacji). Duża liczba parametrów pozwala na dopasowanie działania platformy do potrzeb środowiska produkcyjnego lub testowego.

Szczególnie ważne są parametry związane z bezpieczeństwem. Po pierwsze, w trakcie prac programistycznych stosowanie silnych zabezpieczeń utrudniłoby wyszukiwanie błędów i szybkie testowanie działania usług. Po drugie, zgodnie z wymaganiami (punkt 3.3.2) powinna być możliwa integracja platformy z narzędziami tworzonymi w projekcie ITSOA. Dlatego wprowadzono możliwość wyłączenia mechanizmów uwierzytelniania i wymuszania korzystania z protokołu HTTPS. Dotyczy to także innych mechanizmów (log, historia komunikacji). Możliwość ich wyłączenia pozwala na użycie narzędzi zewnętrznych.

Historia komunikacji

Historia komunikacji została zaimplementowana wykorzystując mechanizm zachowań (ang. *Behavior*), który pozwala wprowadzać dodatkowe przetwarzanie przed i po obsłudze zgłoszeń przez usługę. Można ją zatem wykorzystać w prosty sposób w każdej z budowanych usług. Dzięki temu mechanizmowi możliwe jest odtworzenie pełnej ścieżki komunikacji, a tym samym możliwość retransmisji komunikatów lub wykrywania błędów.

Obsługiwana przez bazę danych historia komunikacji pozwala na zapisanie następujących informacji o komunikacji:

- data i czas żądania
- kierunek komunikacji (wychodząca, przychodząca)
- URI żądania
- metoda żądania
- treść żądania
- nagłówki żądania
- status odpowiedzi
- nagłówki odpowiedzi
- treść odpowiedzi

Ze względu na znaczące rozmiary przesyłanych komunikatów (np. w Źródle), wprowadzono parametry pozwalające na wyłączenie z historii treści i/lub nagłówków wiadomości.

Log

Wiele działań platformy wyzwalane jest automatycznie np. jako reakcja na zdarzenia w systemie informatycznym ZOZ, dlatego nie jest łatwe monitorowanie operacji wykonywanych przez usługi. Wprowadzony mechanizm logu pozwala w zdefiniowanych miejscach w kodzie logiki usług zapisywać informacje o wykonanych operacjach lub wyjątkach. Wyróżnia się trzy poziomy szczegółowości logu, zawierające różne rodzaje informacji:

- poziom *Error* - tylko komunikaty o błędach,
- poziom *Warning* - komunikaty o błędach i ostrzeżeniach,
- poziom *Information* - komunikaty o błędach, ostrzeżeniach i informacjach.

Utworzono także interfejsy umożliwiające wykorzystanie różnych sposobów przechowywania komunikatów logu. Jako przykład w platformie zaimplementowano wykorzystanie dostępnego w systemie Windows, logu zdarzeń (ang. *Event Log*).

Uwierzytelnianie

Zgodnie z wymaganiami opisanymi w punkcie 3.3.4, wewnętrzna komunikacja może być zabezpieczona uwierzytelnianiem usług za pomocą certyfikatów klucza publicznego *X.509*. Odpowiednie usługi przechowują w bazie danych powiązane informacje o identyfikatorze usługi i odcisku (ang. *thumbprint*) jej certyfikatu. Dodatkowo każda usługa w pliku konfiguracyjnym posiada parametr określający odcisk własnego certyfikatu, wykorzystywanego do komunikacji wychodzącej, a przechowywanego w repozytorium certyfikatów systemu Windows.

Komunikacja użytkownika z Mediatorem i Autoryzacją zabezpieczona jest podstawowym uwierzytelnianiem HTTP (ang. *Basic access authentication*). Poprzez aplikacje klienckie lub przeglądarkę internetową użytkownik jest zobowiązany dostarczyć nazwę użytkownika i hasło. Dla zwiększenia bezpieczeństwa, hasło dostępu jest przechowywane w bazie danych w postaci skrótu SHA1. Dodatkowo, aby chronić przed próbami odgadywania haseł wprowadzono 2 parametry:

- limit dopuszczalnych nieudanych prób logowania,
- czas blokady po przekroczeniu limitu.

Przy używaniu tej metody uwierzytelniania konieczne jest zapewnienie bezpiecznego kanału komunikacji, dlatego osobnym parametrem można wymusić korzystanie z protokołu HTTPS.

4.3 Aplikacje

W ramach projektu powstały dwie aplikacje: aplikacja administracyjna oraz przykładowa aplikacja kliencka. Pierwsza dotyczy konfiguracji działania poszczególnych usług systemu. Druga natomiast pokazuje przykładowe zastosowanie stworzonej platformy. Obie aplikacje zostały szczegółowo opisane w poniższych punktach.

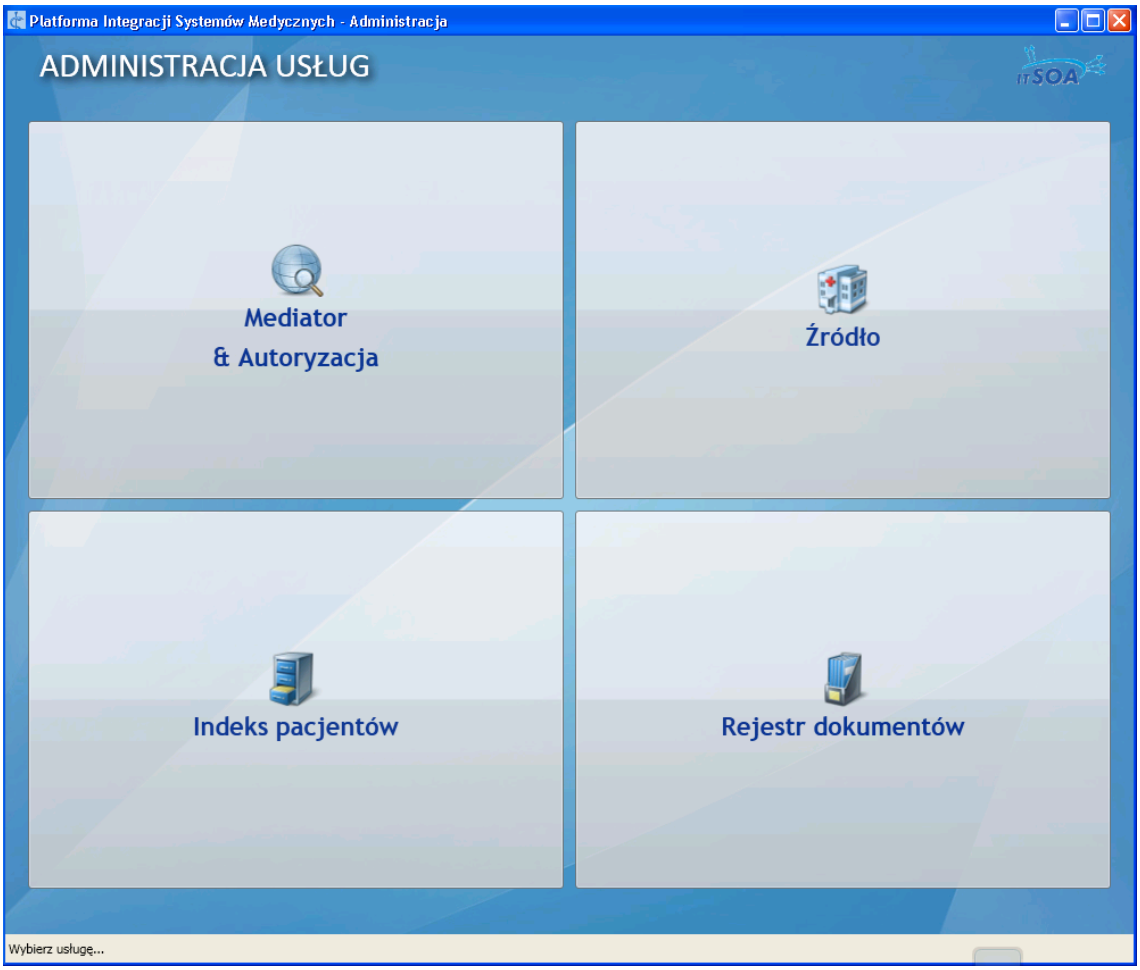
4.3.1 Aplikacja administracyjna

Wspomaganie procesu administrowania usługami jest bardzo ważne dla uniknięcia błędów w ustawieniach i ułatwienia konfigurowania i monitorowania działania platformy. W tym celu zaprojektowano aplikację, posiadającą interfejs graficzny, który wspomaga dobór ustawień oraz pozwala skonfigurować niektóre parametry środowiska związane z bezpieczeństwem.

Aplikacja posiada 4 główne widoki dla każdego rodzaju warstwy logiki usług:

- Źródło
- Repozytorium
- Indeks
- Mediator i Autoryzacja

Zgodnie z punktem 4.2.6, dostępny w systemie Windows log zdarzeń jest wykorzystywany w platformie. Wymaga to jednak odpowiedniej konfiguracji. Aplikacja administracyjna udostępnia możliwość sprawdzenia oraz wprowadzenia takiej konfiguracji. Podobnie jest z mechanizmem szyfrowania plików z parametrami, do którego system Windows udostępnia polecenia konsolowe. W stworzonej aplikacji takie ustawienia wprowadzane są przez jedno kliknięcie.



Rysunek 4.12: Aplikacja administracyjna. Ekran wyboru usługi.

Aplikacja udostępnia prosty edytor parametrów specyficznych dla danej usługi, zaszytych w pliku konfiguracyjnym. Jak zaprezentowano na Rysunku 4.13 opcje te podzielone są na 3 kategorie: ogólne, związane z bezpieczeństwem i dotyczące dostępu do danych i usług.

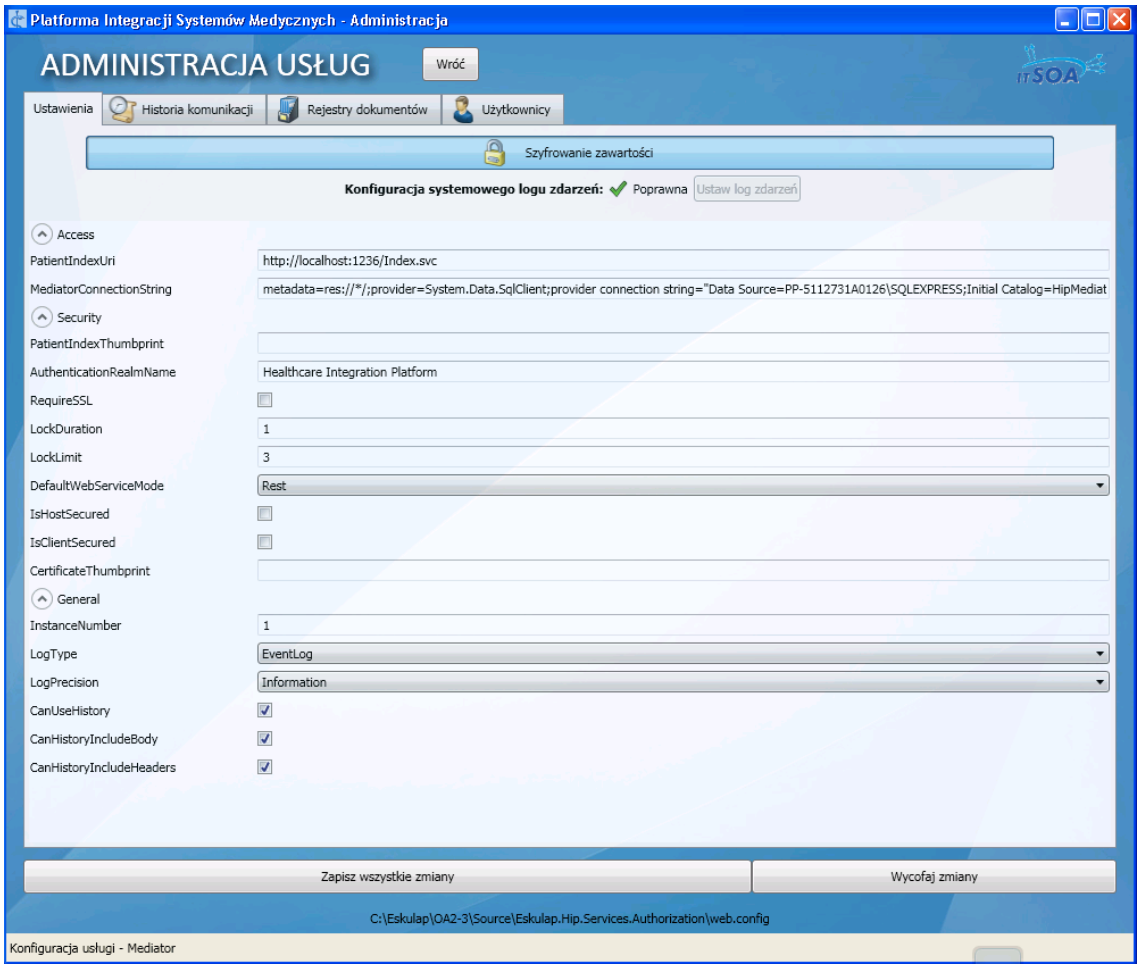
Każda usługa dysponuje mechanizmem historii komunikacji. Dodatkowo w Indeksie wprowadzono mechanizm wiadomości wysyłanych asynchronicznie, których status jest przechowywany w bazie danych. Informacje te są dostępne do odczytu w aplikacji administracyjnej (Rysunek 4.14).

Istotnym elementem są także ustawienia zapisane w bazie danych takie jak: listy usług, do których Indeks ma wysyłać powiadomienia o pacjentach lub spis użytkowników w Autoryzacji. Część z tych danych w przyszłym rozwoju będzie możliwa do automatycznego zarządzania poprzez zasoby usług sieciowych. W zaimplementowanej platformie są one jednak wprowadzane przez aplikację administracyjną.

4.3.2 Aplikacja kliencka

Weryfikacja poprawności stworzonego systemu wymagała stworzenia przykładowej aplikacji klienckiej. Jednym z założeń projektowych było takie zaplanowanie API, aby możliwe było zbudowanie serwisu w pełni wykorzystującego możliwości platformy. Z myślą o tym założeniu tworzona była usługa Mediatora udostępniająca interfejs dla aplikacji klienckich.

Zadaniem przykładowego systemu jest udostępnienie użytkownikom wygodnego dostępu do



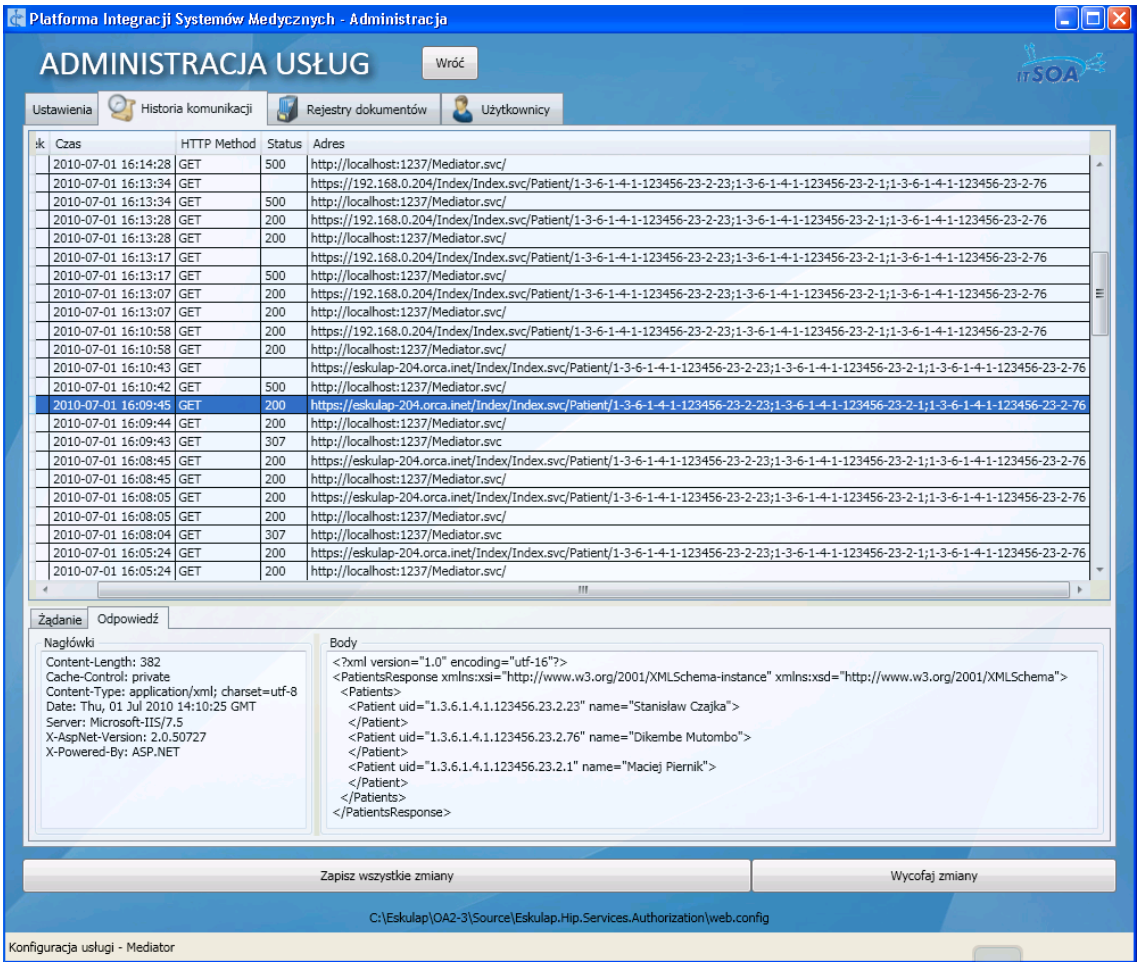
Rysunek 4.13: Aplikacja administracyjna. Edytor pliku konfiguracyjnego.

możliwie jak najpełniejszego zbioru danych medycznych pacjenta, a więc do EHR. Dostęp ten musi być oczywiście autoryzowany, a ci użytkownicy systemu, którzy są jednocześnie pacjentami mają możliwość zarządzania dostępem do swoich danych.

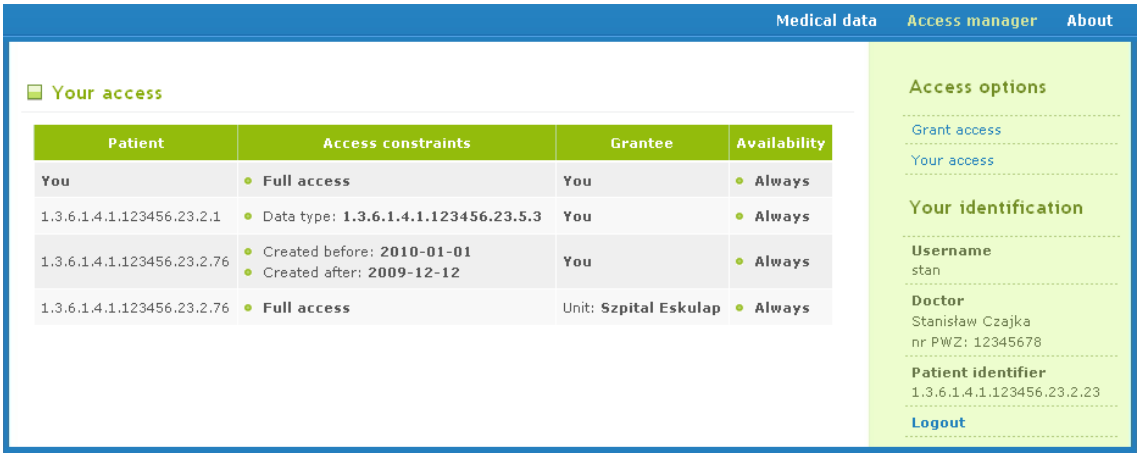
Aplikacja kliencka dzieli się na dwa moduły: moduł zarządzania dostępem do danych oraz moduł dostępu do EHR. Pierwszy z nich umożliwia wgląd w przydzielone użytkownikowi uprawnienia do danych innych pacjentów. Taka przykładowa lista uprawnień została przedstawiona na Rysunku 4.15. Poza tym pozwala on również na zarządzanie dostępem do własnych danych medycznych, pod warunkiem oczywiście, że konto użytkownika jest powiązane z pacjentem. Użytkownik może wykonywać operacje wstawienia nowego uprawnienia, usunięcia, modyfikacji lub odczytu. Przykładowy widok zarządzania uprawnieniami przedstawia Rysunek 4.16.

Część aplikacji odpowiedzialna za prezentowanie danych medycznych składa się z czterech głównych widoków. Pierwszy z nich prezentuje listę pacjentów, do danych których użytkownik ma dostęp (Rysunek 4.17).

Lista ta pobierana jest z Mediatora poprzez odwołanie do zasobu `Patients`. Pacjenci reprezentowani są swoim imieniem i nazwiskiem oraz globalnie unikatowym identyfikatorem nadanym przez system. Wybranie któregoś z pacjentów powoduje przejście do listy folderów danego pacjenta. Może ona być filtrowana przez Źródło, z którego pochodzą dokumenty wchodzące w ich skład. Lista ta pobierana jest z Mediatora poprzez odwołanie do zasobu `Folders` z identyfikatorem pacjenta oraz ewentualnym identyfikatorem Źródła. Przykład znajduje się na Rysunku 4.18.



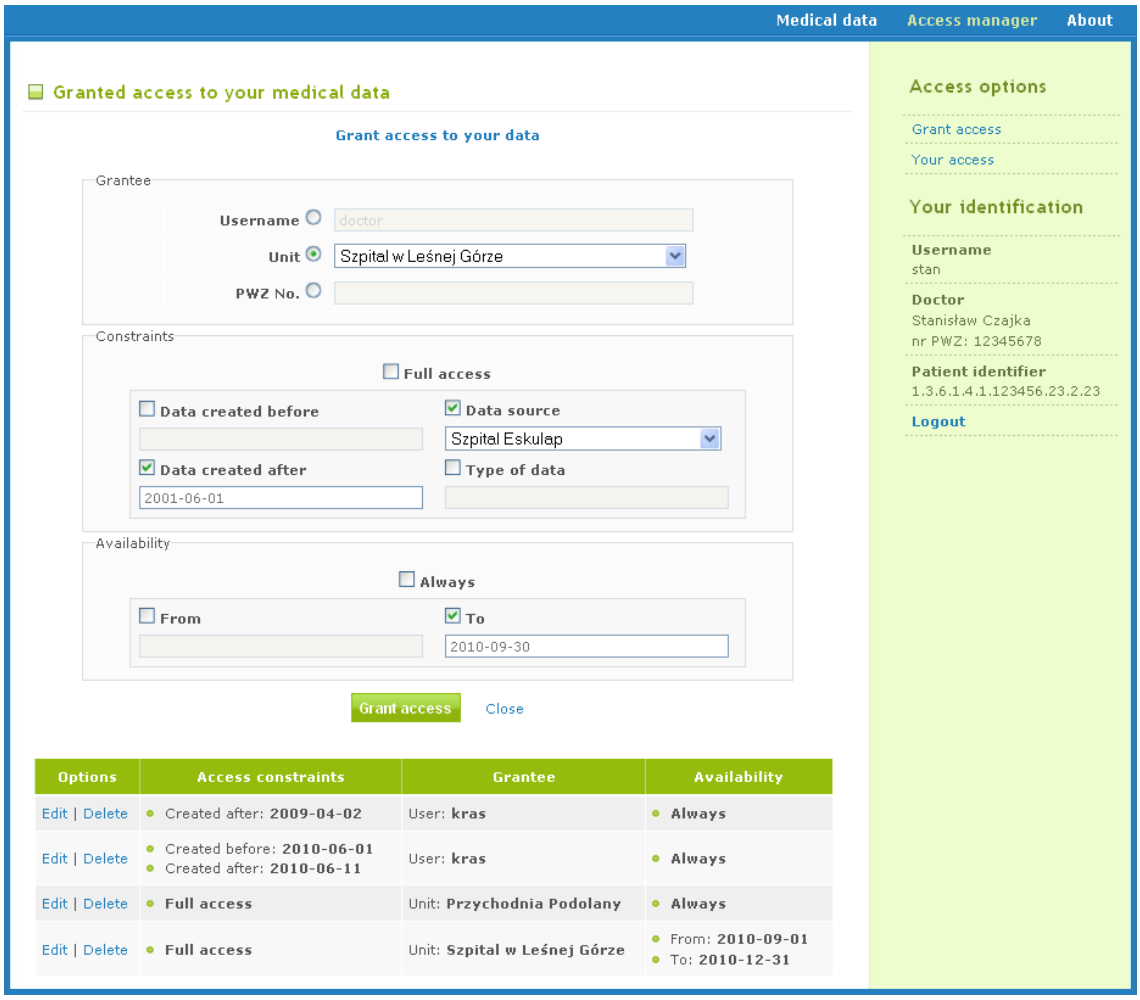
Rysunek 4.14: Aplikacja administracyjna. Podgląd historii komunikacji.



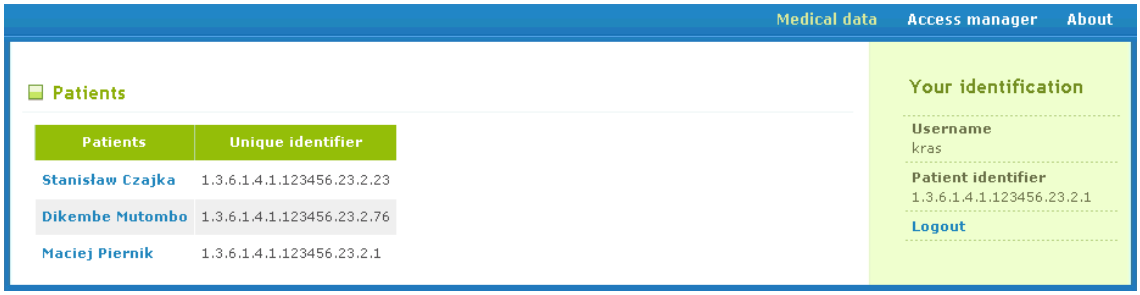
Rysunek 4.15: Lista uprawnień przydzielonych użytkownikowi do danych medycznych pacjentów.

Wybranie któregoś z folderów powoduje przejście do kolejnego widoku, jakim jest lista dokumentów pacjenta. Prezentuje ona podstawowe informacje o dokumentach, takie jak tytuł, rozmiar, datę utworzenia oraz foldery, do których należy (Rysunek 4.19).

Lista ta może być filtrowana przez konkretny folder oraz Źródło i jest uzyskiwana na skutek odwołania do zasobu `Documents` z identyfikatorem pacjenta oraz opcjonalnymi identyfikatorami

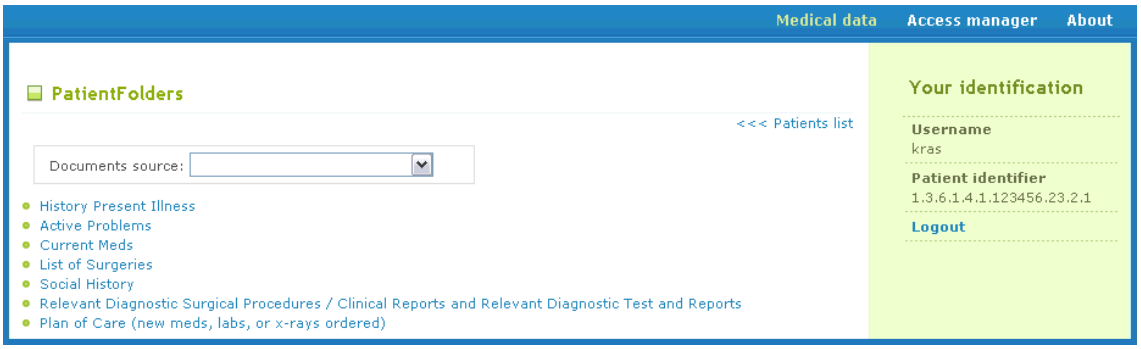


Rysunek 4.16: Widok zarządzania uprawnieniami.

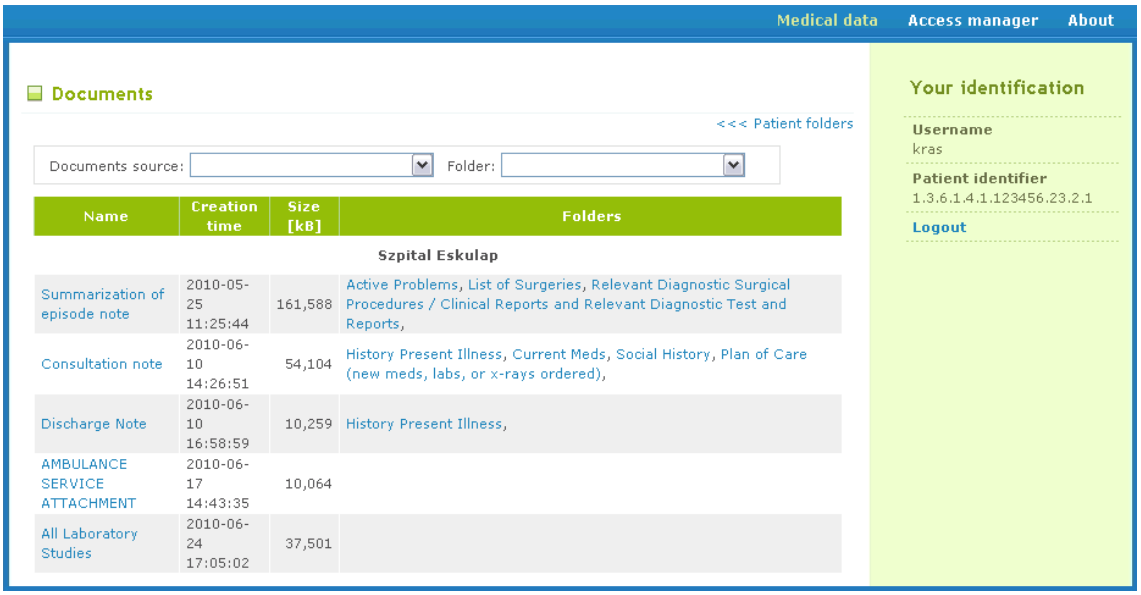


Rysunek 4.17: Lista pacjentów dostępnych dla użytkownika.

folderu i Źródła z Mediatora. Wybranie któregoś z dokumentów powoduje odwołanie do zasobu `Documents` z identyfikatorem dokumentu. W odpowiedzi aplikacja kliencka otrzymuje od Mediatora dokument XML zgodny z HL7 CDA (lub jego fragment, do którego użytkownik ma dostęp), który jest wyświetlany przy pomocy transformacji XSLT. Przykładowy fragment takiego dokumentu przedstawia Rysunek 4.20.



Rysunek 4.18: Lista folderów pacjenta.



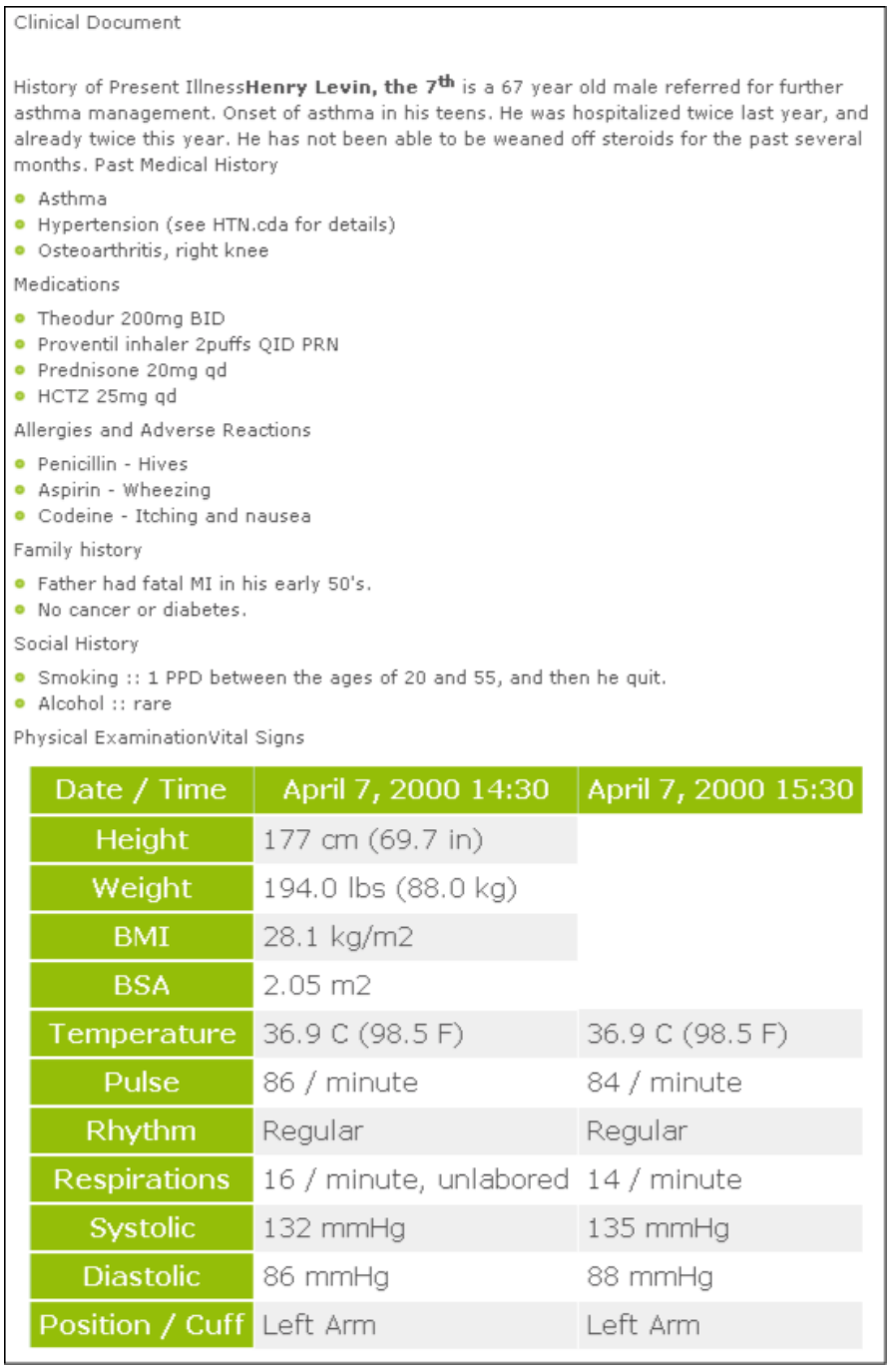
Rysunek 4.19: Lista dokumentów pacjenta.

4.4 Technologie i narzędzia

Platforma zrealizowana została na bazie .NET Framework 3.5 SP1 przy wykorzystaniu bibliotek WCF (ang. *Windows Communication Fundation*), które służą do tworzenia usług sieciowych. Dodatkowo skorzystano z pakietów WCF REST Starter Kit oraz WCF REST Contrib, które są zestawami klas dla .NET Framework oraz przydatnych narzędzi i szablonów dla Visual Studio umożliwiających tworzenie usług WCF zgodnych z paradygmatem REST. Środowiskiem programistycznym, w którym zrealizowano projekt było Visual Studio 2008 Team System, a usługi zaimplementowane zostały w języku C♯. Jako serwer bazy danych posłużył SQL Server 2008 Express, a do stworzenia mapowania encji z bazy danych na klasy w projekcie wykorzystano ADO.NET Entity Framework.

Do stworzenia aplikacji administracyjnej użyto .NET Framework w wersji 4.0 z wykorzystaniem technologii WPF (ang. *Windows Presentation Fundation*) oraz środowiska Visual Studio 2010 Express. Aplikacja kliencka została natomiast oparta o .NET Framework w wersji 3.5 SP1 i wykonano ją, podobnie jak całą platformę, również w środowisku Visual Studio 2008 Team System przy wykorzystaniu technologii ASP.NET MVC 2 oraz jQuery.

W celu przetestowania działania całego projektu wykorzystano systemy operacyjne Windows XP, Windows 7 oraz Windows Server 2008 RC 2. Usługi natomiast działały na serwerach IIS 5.1 i 7.5.



Clinical Document

History of Present Illness**Henry Levin, the 7th** is a 67 year old male referred for further asthma management. Onset of asthma in his teens. He was hospitalized twice last year, and already twice this year. He has not been able to be weaned off steroids for the past several months. Past Medical History

- Asthma
- Hypertension (see HTN.cda for details)
- Osteoarthritis, right knee

Medications

- Theodur 200mg BID
- Proventil inhaler 2puffs QID PRN
- Prednisone 20mg qd
- HCTZ 25mg qd

Allergies and Adverse Reactions

- Penicillin - Hives
- Aspirin - Wheezing
- Codeine - Itching and nausea

Family history

- Father had fatal MI in his early 50's.
- No cancer or diabetes.

Social History

- Smoking :: 1 PPD between the ages of 20 and 55, and then he quit.
- Alcohol :: rare

Physical ExaminationVital Signs

Date / Time	April 7, 2000 14:30	April 7, 2000 15:30
Height	177 cm (69.7 in)	
Weight	194.0 lbs (88.0 kg)	
BMI	28.1 kg/m2	
BSA	2.05 m2	
Temperature	36.9 C (98.5 F)	36.9 C (98.5 F)
Pulse	86 / minute	84 / minute
Rhythm	Regular	Regular
Respirations	16 / minute, unlabored	14 / minute
Systolic	132 mmHg	135 mmHg
Diastolic	86 mmHg	88 mmHg
Position / Cuff	Left Arm	Left Arm

Rysunek 4.20: Dokument w formacie HL7 CDA wyświetlony przez transformację XSLT.

Rozdział 5

Podsumowanie

Wszystkie cele projektu *Platforma Integracji Systemów Medycznych oparta na SOA* zostały zrealizowane. Przeanalizowano istniejące standardy reprezentacji i wymiany danych związanych z ochroną zdrowia, co pozwoliło zaprojektować architekturę usług sieciowych i zasady obiegu oraz integracji wewnętrznej dokumentacji medycznej. Zaimplementowano system zgodny z postawionymi wymaganiami funkcjonalnymi oraz zweryfikowano poprawność zastosowanych rozwiązań.

Analiza istniejących standardów pozwoliła wybrać z nich odpowiednie do realizacji celów projektu oraz pozytywnie zweryfikować ich użyteczność w praktycznych zastosowaniach. Wykorzystano standardy rozwijane przez różne organizacje, a należą do nich: IHE XDS, IHE PIX, HL7 CDA Release 2, HL7 v2.3.1 oraz ebXML.

Zaprojektowano elastyczną architekturę usług, umożliwiającą wgląd do Elektronicznej Kartoteki Pacjenta. Platforma stanowi rozproszone repozytorium danych, pozwalające na kontrolowane udostępnianie dokumentacji medycznej, dzięki zaprojektowanym metodom autoryzacji i mechanizmom indeksowania danych.

Zaimplementowano system o warstwowej budowie, łatwy w utrzymaniu i dający możliwość przyszłego rozwoju. Struktura projektu jest otwarta na zmiany założeń dotyczących zarówno wykorzystanych technologii, jak też wybranych standardów. Platformę stworzono przez kompozycję usług sieciowych o prostym i dobrze opisanym interfejsie zgodnym z paradygmatem REST. Zastosowano mechanizmy zapewniające ochronę danych, z uwzględnieniem aktualnego stanu prawnego.

Perspektywy rozwoju

Zbudowano działający i sprawdzony w testowych warunkach prototyp platformy usługowej. Jednak istnieje wiele obszarów, których analiza jest konieczna lub potrzebna dla jej wdrożenia w rzeczywistych warunkach pracy. Istnieją elementy funkcjonalne systemu, niezwiązane bezpośrednio z wymianą dokumentacji medycznej lub zarządzaniem pacjentami. Otwierają one możliwość rozwijania aplikacji klienckich oraz procedur związanych z administracją i nadzorem działania platformy. Należą do nich m.in.:

- zautomatyzowane zarządzanie zgłaszaniem jednostek medycznych udostępniających dane,
- kontrola zdarzeń łączenia pacjentów,
- ułatwianie tworzenia powiązań pomiędzy użytkownikami systemu a pacjentami,
- wygodne wprowadzanie informacji o lekarzach związanych z zakładami opieki zdrowotnej.

Naturalnym kierunkiem rozwoju jest integracja z innymi systemami i narzędziami informatycznymi. Do realizacji założonych celów niezbędne jest zaprojektowanie usług dostosowanych do

indywidualnych wymagań zakładów opieki zdrowotnej. Jest to konieczne ze względu na różnorodność wymienianych typów danych oraz mnogość systemów HIS.

Planowana jest także integracja z narzędziami tworzonymi w obszarach badawczych projektu ITSOA. Pozwoli to na zwiększenie bezpieczeństwa, niezawodności oraz efektywności. Szczególnie ważne dla przyszłości projektu jest ciągła poprawa wydajności platformy, aby jej wykorzystanie było wygodne dla użytkowników, a udostępnianych danych mogło być coraz więcej. Ponadto opracowanie niezależnego interfejsu usług zgodnego z protokołem SOAP pozwoli na użycie narzędzi i standardów niedostępnych dla komunikacji opracowanej na podstawie paradygmatu REST.

Platforma może stać się źródłem danych lub podstawą do zbudowania innych usług, także tych, które są tworzone w obszarach aplikacyjnych projektu ITSOA. Gromadzone dane mogą być wykorzystane w usługach związanych ze służbami ratownictwa, dla udostępniania informacji w sytuacjach zagrożenia życia. Platforma może także stanowić źródło danych dla systemów PHR. Naturalne wydaje się również kontynuowanie prac nad rozwojem aplikacji klienckich wykorzystujących różne technologie, także mobilne, aby dostęp do samych danych i zarządzania uprawnieniami był jak najłatwiejszy.

Literatura

[Bot] Oliver Johannes Bott. S-8-1 The Electronic Health Record: Standardization and Implementation.

[CSF+08] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280. http://tools.ietf.org/html/rfc5280, 2008.

[EAR+05] Marco Eichelberg, Thomas Aden, Jörg Riesmeier, Asuman Dogac, Gokce Laleci. A survey and analysis of electronic healthcare record standards. *ACM Comput. Surv.*, 37(4):277–315, 2005.

[ebX] ebXML - Enabling A Global Electronic Market. http://www.ebxml.org.

[EJ01] D. Eastlake, P. Jones. US Secure Hash Algorithm 1 (SHA1). RFC 3174. http://tools.ietf.org/html/rfc3174, 2001.

[EN1] The CEN/ISO EN13606 Information Site. http://www.en13606.eu/.

[FGM+99] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616 (Draft Standard), 1999. Updated by RFC 2817.

[Fie00] Roy Thomas Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. Praca doktorska, University of California, 2000. Chapter 5. Representational State Transfer (REST).

[HL7] HL7 Clinical Document Architecture, Release 2.0. http://healthinfo.med.dal.ca/hl7intro/CDA_R2_NormativeWebEdition/.

[HL799] Health Level Seven, Version 2.3.1. Final Standard, 1999.

[Iak98] I Iakovidis. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in europe. *Int J Med Inform*, 52(1-3):105–15, 1998.

[ICD] International Classification of Diseases (ICD). http://www.who.int/classifications/icd/en/.

[IHE] Integrating the Healthcare Enterprise. http://www.ihe.net/.

[IHE09a] IHE IT Infrastructure Technical Framework, Volume 1, Integration Profiles, 2009.

[IHE09b] IHE IT Infrastructure Technical Framework, Volume 2a, Transactions Part A, 2009.

[IHE09c] IHE IT Infrastructure Technical Framework, Volume 3, Cross-Transaction Specifications and Content Specifications, 2009.

[IHE09d] IHE Patient Care Coordination Technical Framework, Volume 1, 2009.

[IHE09e] IHE Patient Care Coordination Technical Framework, Volume 2, 2009.

[ISOa] ISO/IEC 7498-1:1994. Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.

[ISOb] ISO/IEC 9834-1:2008. Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures and top arcs of the International Object Identifier tree.

[Jos06] S. Josefsson. The Base16, Base32, and Base64 Data Encodings. RFC 4648. http://tools.ietf.org/html/rfc4648, 2006.

[LOI] Logical Observation Identifiers Names and Codes. http://loinc.org/.

[ope] openEHR - future proof and flexible EHR specifications. http://www.openehr.org/home.html.

[Oso07] Generalny Inspektor Ochrony Danych Osobowych. *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych.* Wydawnictwo Sejmowe, Warszawa 2007.

[PI99] PN-I-13335-1. Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych, PKN, 1999.

[PS07] PN-SIO/IEC-17799:2007. Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, 2007.

[Res00] E. Rescorla. HTTP Over TLS. RFC 2818. http://tools.ietf.org/html/rfc2818, 2000. Updated by RFC 5785.

[SITa] American College of Radiology. http://www.acr.org/.

[SITb] CEN - European Comittee for Standarization. http://www.cen.eu/.

[SITc] Dossia Personal Health Platform. http://www.dossia.org.

[SITd] Google Health. https://health.google.com.

[SITe] Health Level Seven International. http://www.hl7.org/.

[SITf] ITSOA. Nowe technologie informacyjne dla elektronicznej gospodarki i społeczeństwa informacyjnego oparte na paradygmacie SOA. https://www.soa.edu.pl.

[SITg] Microsoft Health Vault. http://www.healthvault.com.

[SITh] The National Electrical Manufacturers Association. http://www.nema.org/.

[SITi] ZIP - Zdrowotny Informator Pacjenta. https://zip.nfz.poznan.pl.

[SMO] Montserrat Batet Sanroma, Aida Valls Mateu, Karina Gibert Oliveras. Survey of Electronic Health Record Standards.

[SNO] Systematized Nomenclature of Medicine-Clinical Terms. http://www.ihtsdo.org/snomed-ct/.

[USTa] *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.* Dz.U. nr 100, poz. 102.

[USTb] *Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych.* Dz.U. 2008 nr 123 poz. 801.

[USTc] *Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania.* Dz.U. 2006 nr 247, poz. 1819.

[USTd] *Rozporządzenie Ministra Zdrowia z dnia 30 lipca 2001 r. w sprawie rodzajów dokumentacji medycznej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania.* Dz.U. 2001 nr 83 poz. 903.

[USTe] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.* Dz.U. 2002 nr 101, poz. 926, z późn.zm.

[W3Ca] Extensible Markup Language (XML). http://www.w3.org/XML/.

[W3Cb] SOAP Specifications. http://www.w3.org/TR/soap/.

[W3Cc] XML Signature Syntax and Processing (Second Edition). http://www.w3.org/TR/xmldsig-core/.

[W3Cd] XSL Transformations (XSLT) Version 1.0. http://www.w3.org/TR/xslt/.

Instytut Informatyki, Wydział Informatyki i Zarządzania
Politechnika Poznańska

Skład przy użyciu systemu LaTeX.

BibTeX:

```
@mastersthesis{ key,
    author = "Stanisław Czajka, Maciej Piernik",
    title = "{Platforma Integracji Systemów Medycznych Oparta na SOA}",
    school = "Poznan University of Technology",
    address = "Pozna{\'n}, Poland",
    year = "2010",
}
```