NFZ
Narodowy Fundusz Zdrowia

ENIGMA

4π ANALYST

Projekt: *Usługa doradztwa eksperckiego w ramach programu wdrożenia silnych mechanizmów identyfikacji i uwierzytelniania na potrzeby systemu Rejestru Usług Medycznych II (RUM II) dla Centrali Narodowego Funduszu Zdrowia*

Architektura rozwiązania w zakresie Projektu RUM II

Wersja: *1.20*
Autor: *Zespół Wykonawcy*
Data: *23.12.2014*

4pi Sp. z o.o. 03-924 Warszawa, ul. Niekłańska 27/5, tel/fax (22) 616 33 42, www.4pi.pl
ENIGMA Systemy Ochrony Informacji Sp. z o. o., ul. Jutrzenki 116, 02-230 Warszawa, tel. 22 570 57 10, www.enigma.com.pl

SPIS TREŚCI

SPIS ILUSTRACJI

SPIS TABEL

1. WPROWADZENIE

1.1. Kontekst

Dokument niniejszy pt. „Architektura rozwiązania w zakresie Projektu RUM II" jest częścią dokumentacji, wytworzonej w toku realizacji zamówienia na „Usługa doradztwa eksperckiego w ramach programu wdrożenia silnych mechanizmów identyfikacji i uwierzytelniania na potrzeby systemu Rejestru Usług Medycznych II (RUM II) dla Centrali Narodowego Funduszu Zdrowia".

Dokument powstał w ramach Umowy zawartej w dn. 24.06.2014 pomiędzy Narodowym Funduszem Zdrowia oraz konsorcjum firm 4pi i Enigma.

1.2. Cel dokumentu

Zgodnie z Umową celem dokumentu jest: przedstawienie wysokopoziomowej architektury rozwiązania, opracowanej z uwzględnieniem standardu TOGAF.

2. ARCHITEKTURA ROZWIĄZANIA RUM II W UJĘCIU TOGAF

2.1. Odniesienie do standardu TOGAF

Poszczególne elementy w zakresie Projektu RUM II to, z punktu widzenia architektonicznego, zbiór narzędzi i usług stanowiących wspólną, nierozerwalną i zintegrowaną całość. Taki zbiór należy rozpatrywać wyłącznie w sposób holistyczny, tożsamy z podejściem do zarządzania architekturą korporacyjną. Narzędziem umożliwiającym zarządzanie, budowę i zmianę tak skomplikowanego organizmu jest metodyka zarządzania architekturą korporacyjną. Stosując najlepsze praktyki i standardy wykorzystano więc TOGAF, jako metodę podejścia do zarządzania architekturą.

Architektura korporacyjna jest zdefiniowana, jako zbiór właściwości danej korporacji (włącznie ze strukturą), które stanowią o zdolności do realizacji jej misji. W ujęciu TOGAF definicja korporacji jest zbieżna z definicją organizacji, a co za tym idzie, jako korporację[1] będziemy rozumieli: Narodowy Fundusz Zdrowia. W sposób szczególny należy podkreślić, że słowo korporacja nie odnosi się w rozumieniu metodyki wyłącznie do instytucji prywatnych a jest jedynie powszechnie stosowanym tłumaczeniem ang. „corporation". Poniżej przedstawiono główne założenia podejścia do realizacji zadań objętych metodyką.

Tworzenie architektury korporacyjnej nie jest przedsięwzięciem ściśle informatycznym, lecz złożonym zespołem działań z zakresu organizacji, zarządzania i informatyki. Tworzenie architektury korporacyjnej polega przede wszystkim na stworzeniu formalnego opisu struktury i funkcji komponentów korporacji, wzajemnych powiązań pomiędzy tymi komponentami oraz pryncypiów i wytycznych zarządzających ich tworzeniem i rozwojem w czasie.

Zgodnie z metodyką TOGAF architekturę korporacyjną można rozpatrywać na kilku poziomach.

Architektura Biznesowa ma odpowiedzieć na pytanie, w jakim celu zmieniamy architekturę informatyczną, jakie cele biznesowe chcemy osiągnąć, jakie procesy biznesowe będą wspierane, jak struktura organizacyjna organizacji będzie wspierana przez usługi i narzędzia informatyczne. Architektura biznesowa odpowiada na pytanie: DLACZEGO wdrażamy nowe rozwiązanie?

Architektura Informatyczna (Aplikacji i Danych) jest fundamentalnym aspektem budowy systemu informatycznego – pokazuje ona aplikacje, systemy, zbiory danych abstrahując od konkretnych, użytych do implementacji technologii. Odpowiada ona na pytanie: CO będzie przedmiotem wdrożenia?

Architektura Techniczna skupia się na konkretnych technologiach użytych do implementacji architektury wyższego poziomu – odpowiada ona na pytanie: JAK architektura będzie realizowana?

[1] Termin stosowany w dalszej części (zgodnie z metodyką TOGAF) w odniesieniu NFZ.

TOGAF dostarcza ramy metodyczne, tzw. Framework do wdrożenia i zarządzania architekturą korporacyjną poprzez realizację zadań wchodzących w skład TOGAF ADM (Architecture Development Method). ADM składa się z 9 faz przypominających cykl rozwoju oprogramowania, lecz tylko część etapów dotyczy oprogramowania w sposób bezpośredni. Trzy z najbardziej istotnych produktów wytworzonych w ramach ADM stanowią perspektywy architektury korporacyjnej:

- Architektura Biznesowa;
- Architektura Informatyczna (Aplikacji oraz Danych);
- Architektura Techniczna.

Standard TOGAF wykorzystany został jako metoda dojścia dla zaprojektowania architektury docelowej. Osiągnięcie przewidzianej architektury RUM II zostanie zrealizowane poprzez działania projektowe, nie jako element wdrożenia architektury korporacyjnej, wymagającej utworzenia niezależnej struktury organizacyjnej dla Architektury Korporacyjnej (EA).

Poniżej przedstawiono szczegółowo, z czego składa się każda z perspektyw architektury oraz na jakich etapach ADM są tworzone.

2.1.1. Architektura Biznesowa

Architektura biznesowa jest fragmentem EA, w którym definiuje się sposób funkcjonowania korporacji, który składa się przede wszystkim ze:

- struktury organizacyjnej;
- strategii biznesowej;
- kluczowych procesów biznesowych.

Architektura biznesowa tworzona jest przez pierwsze trzy fazy metody TOGAF ADM.

Pierwsza faza metody ADM „Przedwstępna" polega przede wszystkim na ustaleniu kontekstu biznesowego, w tym identyfikacji i konsolidacji wokół przedsięwzięcia wszystkich kluczowych interesariuszy.

W fazie drugiej „A. Wizja architektury" tworzona jest wizja koncepcji docelowej.

Wynikiem pierwszej i drugiej fazy realizacji ADM jest dokument „Założenia do uruchomienia Projektu RUM II".

Etap trzeci „B. Architektura Biznesowe" polega na właściwym opisaniu założeń docelowej Architektury Biznesowej. Na tym etapie wyłaniają się konkretne założenia i zadania do wykonania. Możliwe jest też określenie szacunków dotyczących czasu trwania poszczególnych działań i etapów przedsięwzięcia. Wynikiem realizacji kroku jest dokument „Koncepcja rozwiązań w zakresie Projektu RUM II".

Uzupełnieniem koncepcji w zakresie realizacji fazy architektury biznesowej są procesy biznesowe i zasobowe, opisane w dokumencie „Procesy w zakresie Projektu RUM II".

Dalsze etapy to właśnie rzutowanie zmian w biznesie na zmiany w IT, a więc opracowanie niezbędnego zakresu zmian Architektury Danych, Architektury Aplikacji i Architektury

Infrastruktury IT oraz implementacja i wdrożenie tych zmian. Ten fragment pracy związany jest już stricte z rozwojem narzędzi i oprogramowania.

2.1.2. Architektura Informatyczna

Na architekturę Informatyczną składają się Architektura Danych oraz Architektura Aplikacji.

Architektura Danych zawiera opis zakresu i źródeł danych niezbędnych do prawidłowej realizacji celów korporacji.

Aplikacje jedynie wspomagają zbieranie, przetwarzanie oraz przesyłanie danych, a także ich wyszukiwanie. Charakter danych oraz sposób ich przetwarzania powinny determinować sposób konstrukcji oprogramowania, które je przetwarza. Architektura Danych stanowi pomost pomiędzy Architekturą Biznesu i Architekturą IT. Architekturę danych opisano w dokumencie „Zakres danych przewidzianych do przetwarzania w Projekcie RUM II".

Architektura Aplikacji stanowi znaczną część tradycyjnie rozumianej „Architektury IT". Zawiera opis sposobu organizacji oprogramowania na poszczególne aplikacje oraz opis integracji tych aplikacji. Niniejszy dokument przedstawia Architekturę Aplikacji rozwiązań RUM II. Wskazane dokumenty oraz wymagania dla komponentów RUM II są podstawą do opracowania architektury technicznej dla każdego z komponentów i fizycznego modelu danych.

2.1.3. Architektura Techniczna

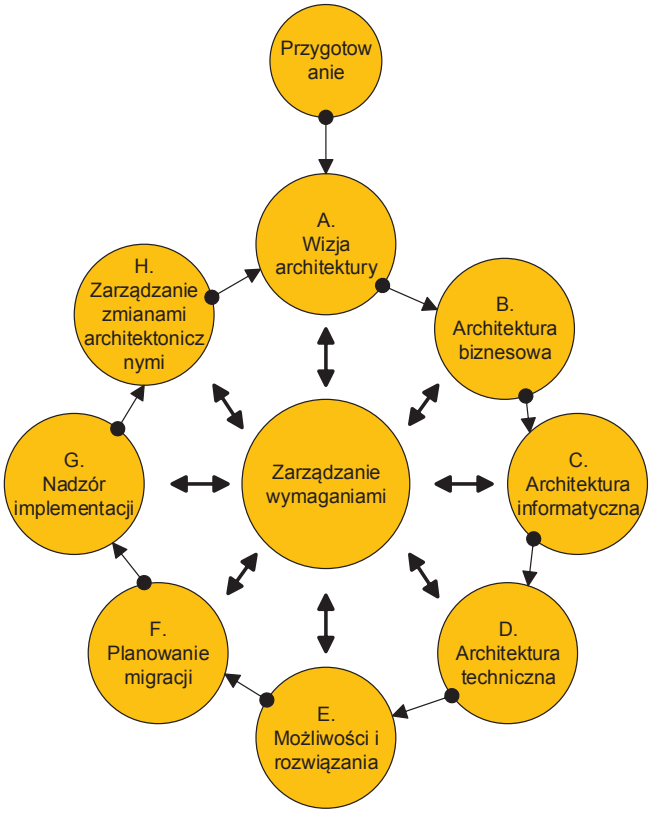
Architektura Techniczna zawiera opis elementów infrastruktury oraz użytej technologii do przetwarzania oraz teletransmisji danych. Założenia dla architektury technicznej stanowią wymagania niefunkcjonalne, opracowane w ramach specyfikacji poszczególnych komponentów architektury logicznej RUM II.

Szczegółowe założenia odnośnie architektury technicznej rozwiązania zostaną opracowane przy wykorzystaniu założeń niniejszego dokumentu oraz wymagań niefunkcjonalnych na etapie tworzenia projektu technicznego systemu przez dostawcę systemu SZUK.

2.2. Cykl ADM

Wykorzystanie ram architektonicznych TOGAF oraz cyklu ADM istotnie wpłynie na uporządkowanie realizowanych działań oraz spójność i kompletność produktów. Powyższe podejście metodyczne ma charakter generalny i dotyczy całości planowanych prac merytorycznych.

Zastosowanie metody ADM umożliwi kompleksowe podejście do wprowadzenia zmian organizacyjnych, w szczególności zapewni zgodność obszaru biznesu z IT oraz odpowiednie uporządkowanie narzędzi i systemów informatycznych. Rysunek poniżej przedstawia wszystkie fazy ADM metodyki TOGAF:



Rysunek 1. Cykl architektoniczny ADM

Należy zwrócić uwagę, że w ramach ADM część produktów podlega ciągłym rewizjom i udoskonaleniom. Np. Architektura Biznesowa tworzona w fazie B może ulec zmianom (i zazwyczaj powinna ulec zmianom) na podstawie danych uzyskanych w dalszych etapach.

Zarządzanie architekturą korporacyjną TOGAF, w zakresie Projektu RUM II, zostało wykorzystane, jako podstawowa metodyka budowy architektury rozwiązania RUM II.

W zakresie zrealizowanych prac przeprowadzono następujące etapy budowy architektury:

- Przygotowanie;
- A. Wizja architektury;
- B. Architektura biznesowa;
- C. Architektura informatyczna;
- D. Architektura techniczna.

Kolejne fazy cyklu ADM będą realizowane we współpracy z dostawcami poszczególnych zamówień realizowanych w ramach Projektu RUM II, w tym:

- E. Możliwości i rozwiązania;
- F. Planowanie migracji;
- G. Nadzór implementacji;
- H. Zarządzanie zmianami architektonicznymi.

3. ARCHITEKTURA RUM II

System RUM II ma dostarczyć narzędzia elektronicznej identyfikacji pracowników świadczeniodawców i świadczeniobiorców (pacjentów) w oparciu o karty KSM, KSA i KUZ oraz technologię PKI. Dzięki temu umożliwi uzyskanie potwierdzenia zdarzenia medycznego oraz dalszą elektronizację obiegu informacji w kolejnym obszarze ochrony zdrowia, czego efektem będą szeroko rozumiane korzyści w zakresie oszczędności środków publicznych, skrócenia procedur administracyjnych oraz udostępnienia nowych e-usług dla społeczeństwa.

3.1. Wizja architektury

Główne oczekiwania odnośnie konstrukcji rozwiązania:

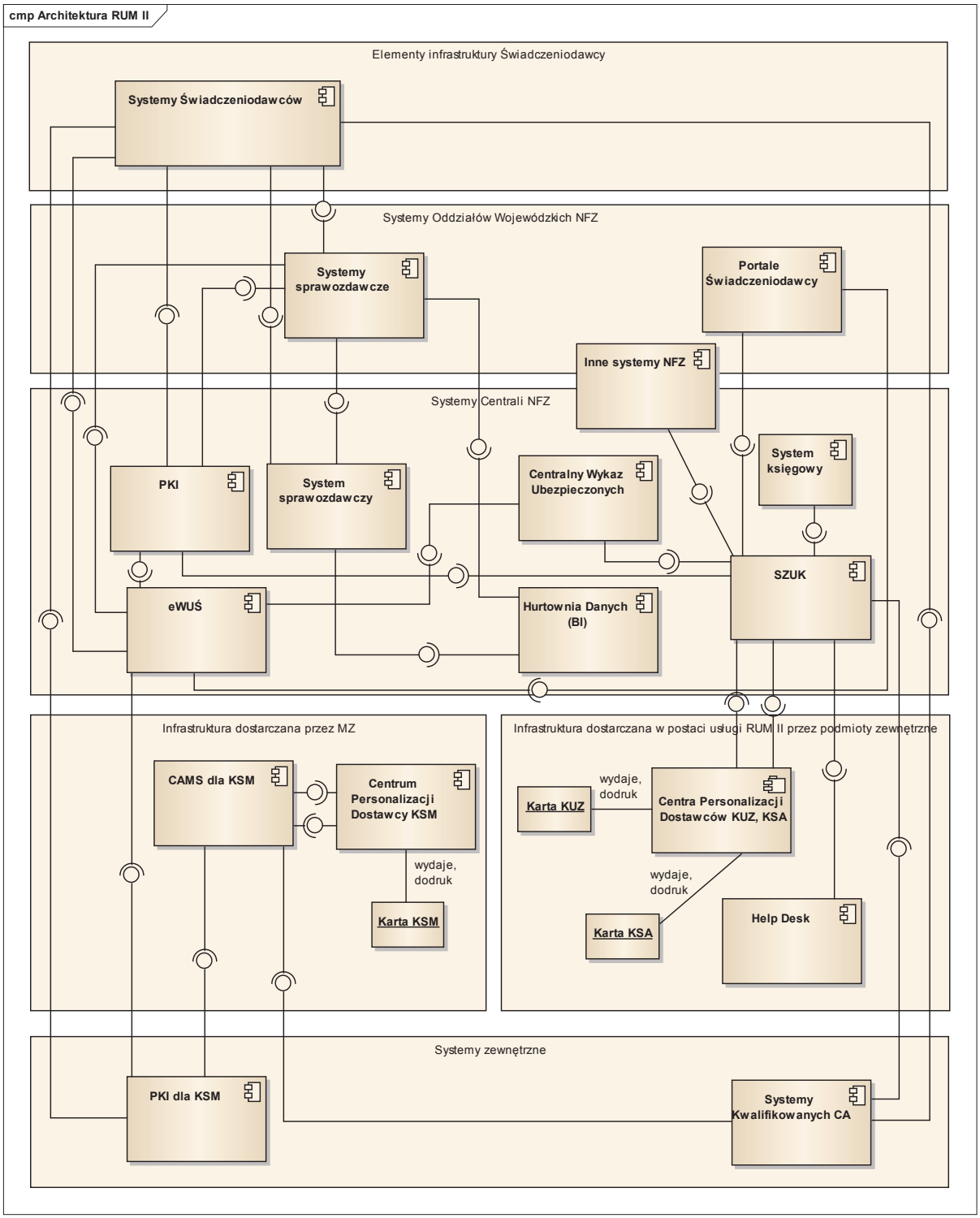
- zapewniać wysokie bezpieczeństwo danych (ochronę danych osobowych i wrażliwych przed nieupoważnionym dostępem);
- umożliwiać podstawowy zakres działania w warunkach niedostępności innych systemów, o ile nie łamie to powyższych zasad budowy architektury;
- duży wolumen przetwarzanych danych w OW i centrali NFZ (w zakresie sprawozdawczości);
- wdrażane rozwiązania będą wykorzystywać obecną infrastrukturę systemów Centrali NFZ i OW NFZ oraz innych systemów, jak również wykorzystywać infrastrukturę po stronie świadczeniodawców.

Takie uwarunkowania wymuszają określenie architektury całości rozwiązania Projektu RUM II, które zapewniać będzie określone cechy:

- modułowość konstrukcji poszczególnych komponentów zapewniająca grupowanie określonych cech rozwiązania (np. integracja, logowanie, autoryzacja) i wielokrotne ich wykorzystywanie;
- centralizacja kluczowych komponentów rozwiązania;
- standaryzacja metod współpracy systemu ze „światem zewnętrznym” – zarówno systemami informatycznymi, jak i użytkownikami;
- zgodność z filozofią tworzenia architektury opartej na usługach wg. SOA (Service Oriented Architecture);
- zastąpienie „kopiowania danych” odpowiednimi metodami dostępu do aktualnych danych źródłowych;
- umożliwiać podstawowy zakres działania poszczególnych komponentów w warunkach niedostępności innych systemów.

3.2. Architektura docelowa TO-BE

Poniżej przedstawiono diagram komponentów wysokopoziomowej architektury logicznej RUM II (w notacji UML) z powiązaniami pomiędzy nimi oraz określeniem interfejsów.



Rysunek 2. Architektura logiczna RUM II

Opis każdego z komponentów ze wskazaniem gestora systemu oraz odniesienia do zakresu niezbędnych danych przedstawiono w poniższej tabeli.

Tabela 1. Opis komponentów architektury logicznej RUM II

Komponent	Gestor Systemu	Opis komponentu
SZUK	Centrala NFZ	System Zarządzania Użytkownikami i Kartami, realizujący funkcje zarządzania wszystkimi informacjami dotyczącymi użytkowników (posiadaczy kart KUZ oraz KSA wydawanych przez NFZ), jak również „wewnętrznych" kart kryptograficznych NFZ.
CAMS dla KSM	Ministerstwo Zdrowia	System zarządzania kartami KSM, realizujący funkcje zarządzania wszystkimi informacjami dotyczącymi użytkowników kart KSM (posiadaczy kart KSM wydawanych przez MZ).
eWUŚ	Centrala NFZ	System pełni funkcje: • weryfikacji uprawnień pracownika świadczeniodawcy do korzystania z Systemu eWUŚ w kontekście danego świadczeniodawcy (wykonywane za pomocą Portalu Świadczeniodawcy) oraz PKI w zakresie uwierzytelnienia do systemu eWUŚ za pomocą karty KSA/KSM, • weryfikacji uprawnień Świadczeniobiorców do realizacji usług medycznych, system wykorzystuje dane CWU, w zakresie aktualnych uprawnień.
PKI	Centrala NFZ	System tworzenia, przechowywania, zarządzania i rozprowadzania cyfrowych certyfikatów klucza publicznego NFZ. Certyfikaty służą do weryfikacji podpisu wykonanego przy pomocy karty KUZ i KSA, jak również dostępu do danych medycznych zapisanych w KUZ.
PKI dla KSM	Ministerstwo Zdrowia	System tworzenia, przechowywania, zarządzania i rozprowadzania cyfrowych certyfikatów klucza publicznego MZ. Certyfikaty służą do weryfikacji podpisu wykonanego przy pomocy karty KSM. Alternatywą dla odrębnego PKI MZ jest wykorzystanie dla kart KSM PKI realizowanego przez NFZ, co wymaga zawarcia porozumienia pomiędzy MZ i NFZ.
Hurtownia danych	Centrala NFZ	Systemy służące do analizy danych ze sprawozdań.

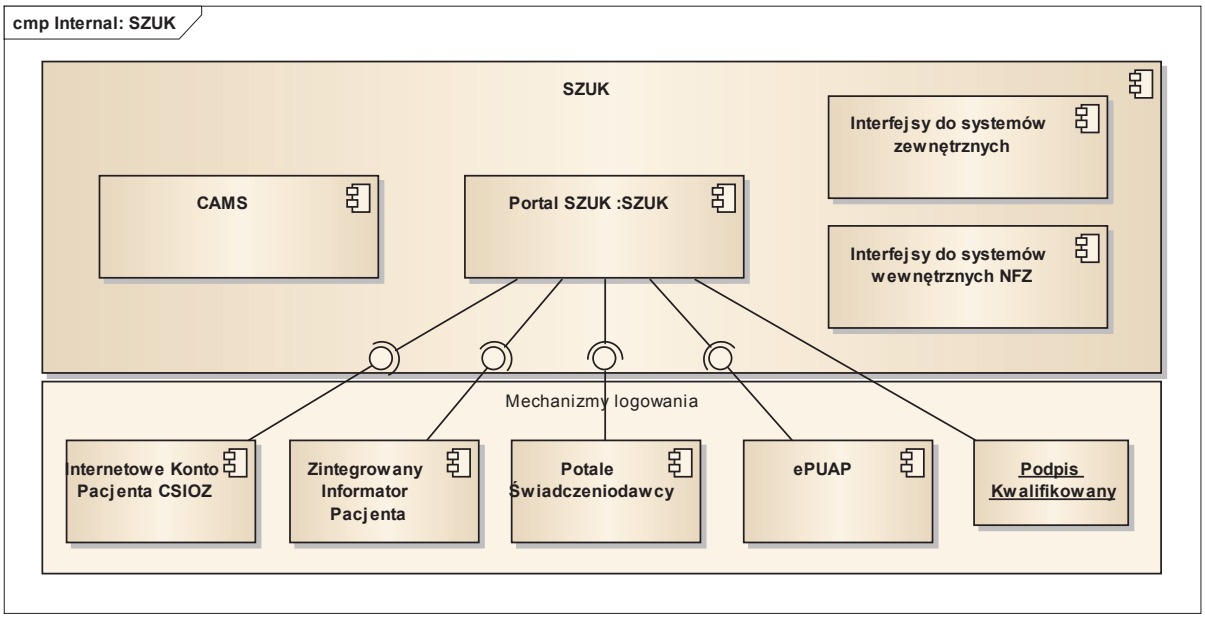
Centralny Wykaz Ubezpieczonych	Centrala NFZ	System dostarczy replikę bazy CWU w zakresie danych służących do wydawania wszystkich kart KUZ (napełnienie inicjalne systemu oraz wydanie po dacie bazowej). Replika bazy CWU będzie aktualizowana w zakresie rejestrowania nowych osób i zmian danych osób znajdujących się już w CWU..
Inne systemy NFZ	Centrala NFZ i/lub OW NFZ	Systemy dostarczające dodatkowe dane do algorytmu wyboru danych świadczeniobiorców do personalizacji i produkcji kart.
Portale Świadczeniodawców	OW NFZ	Rozproszone systemy, zlokalizowane w oddziałach NFZ. Umożliwią zasilenie danych wniosku o wydanie kart KSA. Zostaną wykorzystane, jako mechanizm logowania do SZUK.
Systemy sprawozdawcze	OW NFZ	Systemy obsługujące sprawozdawczość od świadczeniodawców do OW NFZ.
Systemy świadczeniodawców	Świadczeniodawcy	Systemy wspomagające zarządzanie realizowanymi zdarzeniami medycznymi.
Help Desk	Centrala NFZ (usługa zewnętrzna)	System wspierający zespoły świadczące wsparcie dla użytkowników kart.
Centra Personalizacji Dostawców KUZ, KSA	Dostawca (usługa zewnętrzna)	Centra Dostawców kart KUZ i KSA przeprowadzające proces personalizacji w zakresie dystrybucji inicjalnej oraz dodruków kart KUZ i KSA.
Centrum Personalizacji Dostawcy Karty KSM	Ministerstwo Zdrowia	Centrum Dostawcy karty KSM przeprowadzające proces personalizacji w zakresie dystrybucji inicjalnej oraz dodruków karty KSM.
Systemy Kwalifikowanych CA	Centra Certyfikacji Kluczy podmiotów komercyjnych	Opcjonalne wykorzystanie znacznika czasu z kwalifikowanego centrum certyfikacji kluczy oferującego taką usługę. Dla celów zwiększenia dostępności i niezawodności, w miejsce podpisów elektronicznych składanych za pomocą karty KSM lub KSA mogą zostać wykorzystane kwalifikowane podpisy elektroniczne.
System księgowy	Centrala NFZ	Księguje płatności za wydanie karty i wysyłkę. Księgowanie płatności dokonanych przelewem, gotówką oraz za pośrednictwem systemu e-płatności. Przesyła informację do SZUK o dokonaniu opłaty.

Tabela 2. Opis interfejsów architektury logicznej RUM II

Komponent źródłowy	Komponent docelowy	Opis
Centralny Wykaz Ubezpieczonych	SZUK	Import z repliki CWU danych użytkowników kart KUZ (imiona, nazwisko, PESEL, dane adresowe, przypisanie do POZ, status ubezpieczenia, informacja o zgonach).
Inne systemy NFZ	SZUK	Import danych niezbędnych do realizacji algorytmu wyboru danych świadczeniobiorców przeznaczonych do personalizacji i produkcji kart.
Portale Świadczeniodawców	SZUK	Import danych specjalistów administracyjnych do wniosku o wydanie kart KSA (imię, nazwisko, PESEL).
Portale Świadczeniodawców	eWUŚ	Weryfikacja uprawnień pracownika Świadczeniodawcy.
SZUK	Centra Personalizacji Dostawców Kart	Import danych niezbędnych do produkcji, personalizacji i dystrybucji kart KUZ, KSA.
SZUK	Help Desk	Odczyt danych o statusie karty danych dot. certyfikatów i powiązanych z nimi danych użytkownika, wymaganych dla realizacji usług wsparcia przez Help Desk.
CAMS dla KSM	Centrum Personalizacji Dostawcy Karty KSM	Import danych niezbędnych do produkcji, personalizacji i dystrybucji kart KSM.
Centra Personalizacji Dostawców Kart	SZUK	Import danych dot. produkcji i personalizacji kart KUZ, KSA.
Centrum Personalizacji Dostawcy Karty KSM	CAMS dla KSM	Import danych dot. produkcji i personalizacji kart KSM.
Centralny Wykaz Ubezpieczonych	eWUŚ	CWU udostępnia replikę, z której przesyłane są komunikaty o uprawnieniach do udzielenia świadczenia medycznego.
eWUŚ	Systemy Świadczeniodawców	Komunikaty z eWUŚ.
eWUŚ	Systemy Sprawozdawcze	Logi zapytań eWUŚ przekazywane do OW NFZ na potrzeby weryfikacji.
PKI	SZUK	Klucze, TS, OCSP, CRL
PKI	eWUŚ	Klucze, TS, OCSP, CRL.
PKI	Systemy Świadczeniodawców	Klucze, TS, OCSP, CRL.
PKI	Systemy Sprawozdawcze	Klucze, TS, OCSP, CRL.
PKI dla KSM	CAMS dla KSM	Klucze, TS, OCSP, CRL.

PKI dla KSM	eWUŚ	Klucze, TS, OCSP, CRL.
PKI dla KSM	Systemy Świadczeniodawców	Klucze, TS, OCSP, CRL.
Systemy Świadczeniodawców	Systemy Sprawozdawcze	Eksport sprawozdań świadczeniodawców do systemów NFZ.
Systemy Sprawozdawcze	Hurtownia danych (BI)	Import danych do weryfikacji sprawozdań.
Systemy Kwalifikowanych CA	SZUK	Klucze, TS, OCSP, CRL
Systemy Kwalifikowanych CA	CAMS dla KSM	Klucze, TS, OCSP, CRL
Systemy Kwalifikowanych CA	Systemy Świadczeniodawców	Klucze, TS, OCSP, CRL
System księgowy	SZUK	Komunikat o statusie płatności za kartę lub wysyłkę karty.

W uzupełnieniu do diagramu architektury przedstawiono główne komponenty wewnętrzne i mechanizmy logowania systemu SZUK. Szczegóły podział na komponenty architektury SZUK znajduje się w specyfikacji systemu SZUK.



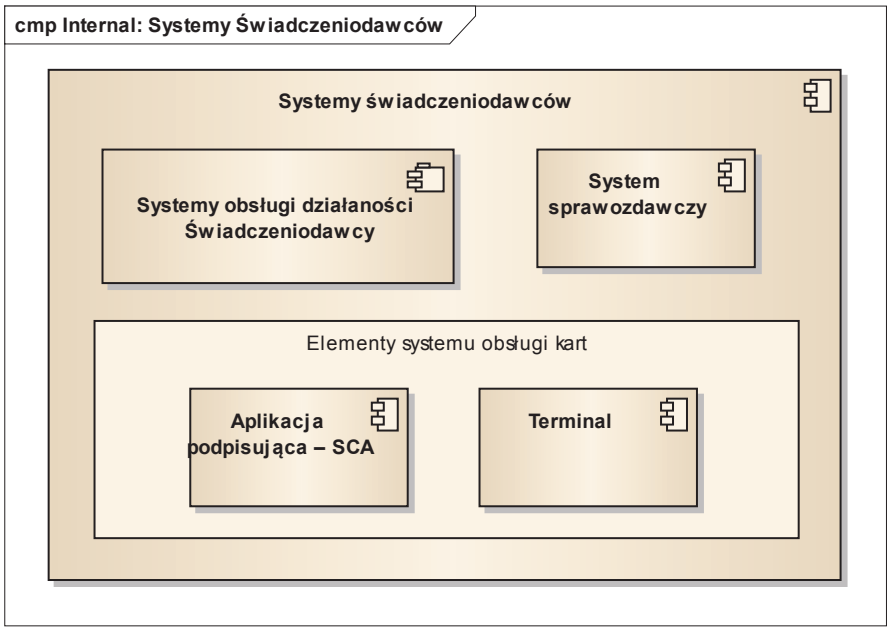
Rysunek 3. Komponenty systemu SZUK, wraz z przewidywanymi mechanizmami dostępu

Tabela 3. Opis komponentów systemu SZUK

Komponent	Gestor Systemu	Opis komponentu
Portal SZUK	Centrala NFZ	Wydzielona logiczne część systemu SZUK, służąca wymianie informacji z użytkownikami kart KUZ i KSA. Portal SZUK umożliwi złożenie wniosków o wydanie kart KUZ i KSA, uzyskanie informacji odnośnie karty, wykonanie prostych operacji na karcie.
CAMS	Centrala NFZ	Zarządzanie wydawaniem i utrzymaniem kart KUZ i KSA.
Interfejsy do systemów zewnętrznych	Centrala NFZ	Uniwersalne interfejsy dla integracji z systemami zewnętrznymi RUM II
Interfejsy do systemów wewnętrznych NFZ	Centrala NFZ	Dedykowane interfejsy do systemów wewnętrznych OW NFZ i Centrali NFZ
Zintegrowany Informator Pacjenta	Centrala NFZ	System, w którym świadczeniobiorcy widzą historię zdarzeń medycznych. Dane do logowania do ZIP będą służyły do logowania do portalu SZUK.
Portale Świadczeniodawców	OW NFZ	Rozproszone systemy, zlokalizowane w oddziałach NFZ. Zostaną wykorzystane, jako mechanizm logowania do SZUK.
Internetowe Konto Pacjenta	CSIOZ	Wykorzystany, jako mechanizm logowania do SZUK.
ePUAP	MAiC	Wykorzystany, jako mechanizm logowania do SZUK, wykorzystujący profil zaufany.
Podpis Kwalifikowany	Centra komercyjne PK	Wykorzystany, jako mechanizm logowania do SZUK, wykorzystujący kwalifikowany podpis elektroniczny.

Tabela 4. Opis interfejsów architektury logicznej RUM II

Komponent źródłowy	Komponent docelowy	Opis
Zintegrowany Informator Pacjenta	Portal SZUK	Dane do logowania do portalu
Portale Świadczeniodawców	Portal SZUK	Dane do logowania do portalu
Internetowe Konto Pacjenta	Portal SZUK	Dane do logowania do portalu
ePUAP	Portal SZUK	Dane do logowania do portalu
Podpis Kwalifikowany	Portal SZUK	Dane do logowania do portalu.



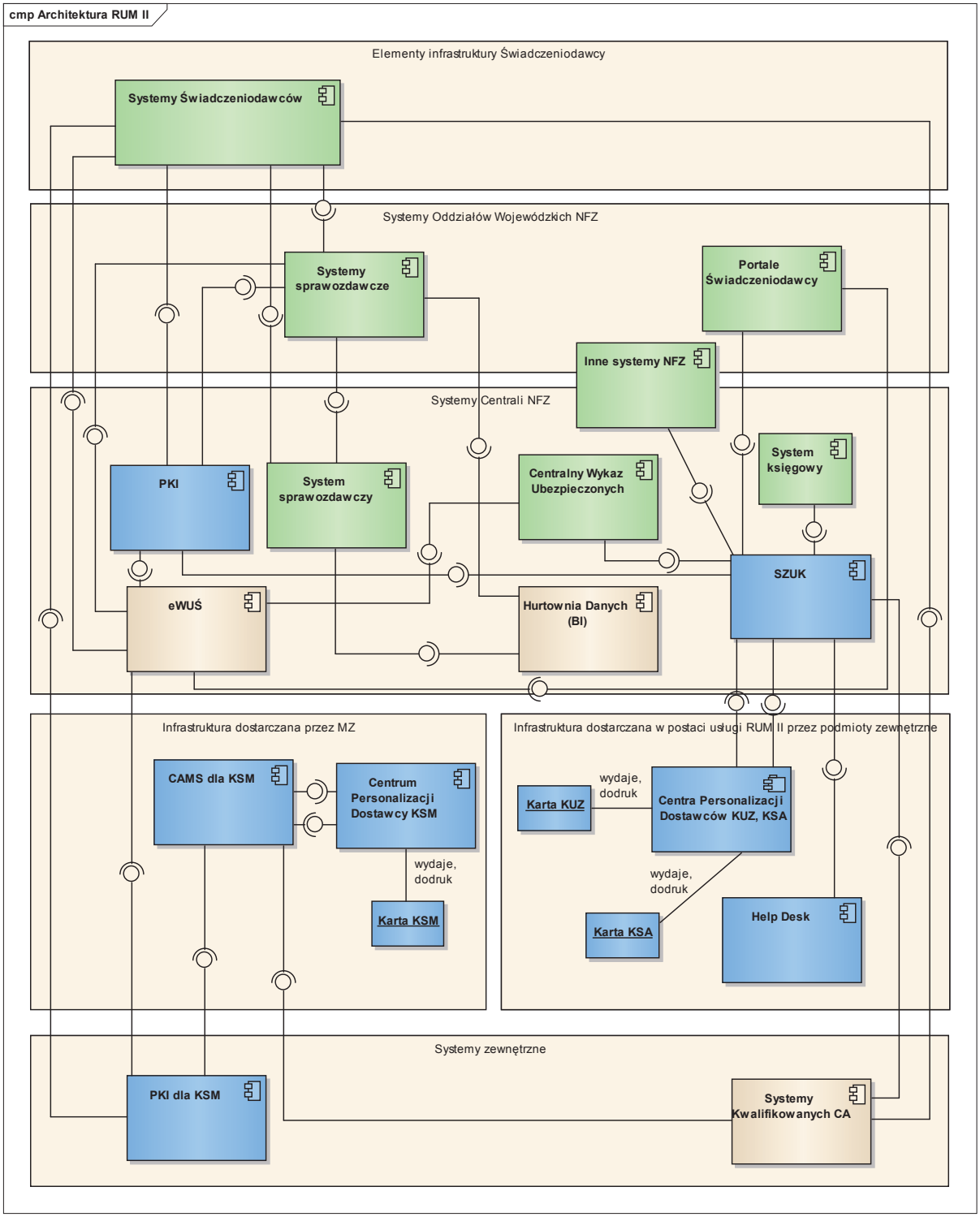
Rysunek 4. Struktura wybranych systemów Świadczeniodawcy, powiązana z wdrożeniem rozwiązań RUM II

Tabela 5. Opis komponentów systemów Świadczeniodawców

Komponent	Gestor Systemu	Opis komponentu
Systemy obsługi działalności Świadczeniodawcy	Świadczeniodawcy	Systemy wspomagające zarządzanie działalnością Świadczeniodawcy.
System sprawozdawczy	Świadczeniodawcy	System/podsystem lub element systemu Świadczeniodawcy, służący do przygotowania rekordu sprawozdawczego.
Aplikacja podpisująca – SCA	Świadczeniodawcy	Oprogramowanie podpisujące po stronie Świadczeniodawcy
Terminal	Świadczeniodawcy	Dowolny czytnik kart elektronicznych stykowych, spełniający wymagane przez NFZ parametry techniczne (w Fazie III ewentualnie czytnik „specjalny”, zapewniający znacznik czasu).

3.3. Odniesienie do obecnej architektury AS-IS

Założeniem architektury RUM II jest wpisanie w obecną architekturę systemów NFZ oraz powiązanych systemów zewnętrznych, funkcjonujących w obszarze ochrony zdrowia. Na poniższym diagramie wyszczególniono nowe komponenty, tworzone w ramach RUM II (oznaczone kolorem niebieskim) oraz obecnie istniejące komponenty wymagające modyfikacji (oznaczone kolorem zielonym).



Rysunek 5. Nowe oraz modyfikowane komponenty architektury RUM II

Tabela 6. Opis modyfikowanych komponentów w związku z wdrożeniem architektury RUM II

Komponent	Gestor Systemu	Opis zmian	Uwagi
Systemy świadczeniodawców	Świadczeniodawcy	Wymagane wdrożenie mechanizmów podpisów kartą KUZ i KSM (w 2-giej fazie) oraz wprowadzenie zmian w mechanizmach logowania za pomocą KSA i KSM.	Konieczne jest wdrożenie zmian w produktach dostawców oprogramowania dedykowanego dla Świadczeniodawców.
Centralny Wykaz Ubezpieczonych	Centrala NFZ	Wymagane wykonanie repliki bazy danych CWU, w zakresie danych koniecznych do zasilenia SZUK (realizacji procesów wydania i dystrybucji oraz utrzymania kart).	Brak.
Systemy Sprawozdawcze (OW NFZ)	Odziały NFZ	Zmiany w zakresie przetwarzania większego zakresu danych przesyłanych z systemów świadczeniodawców.	Brak.
System Sprawozdawczy (Centrala NFZ)	Centrala NFZ	Zmiany w zakresie przetwarzania większego zakresu danych przesyłanych z systemów świadczeniodawców.	Brak.
Portale Świadczeniodawcy	Oddziały NFZ	Nadawanie uprawnień dla pracownika świadczeniodawcy do korzystania z Systemu eWUŚ oraz PKI w zakresie uwierzytelnienia do systemu eWUŚ za pomocą karty KSA/KSM.	Brak.
System księgowy	Centrala NFZ	Wymagane księgowanie i obsługa płatności za wydanie i wysyłkę.	Konieczna integracja z systemem e-płatności.
Inne systemy NFZ	Centrala NFZ i/lub OW NFZ	Dostosowanie interfejsów do wymiany danych z SZUK.	Brak.

3.4. Architektury przejściowe

Z punktu widzenia architektury logicznej rozwiązań RUM II wymagane jest wdrożenie wszystkich komponentów jednocześnie dla realizacji każdej z planowanych faz (począwszy od 1 fazy).

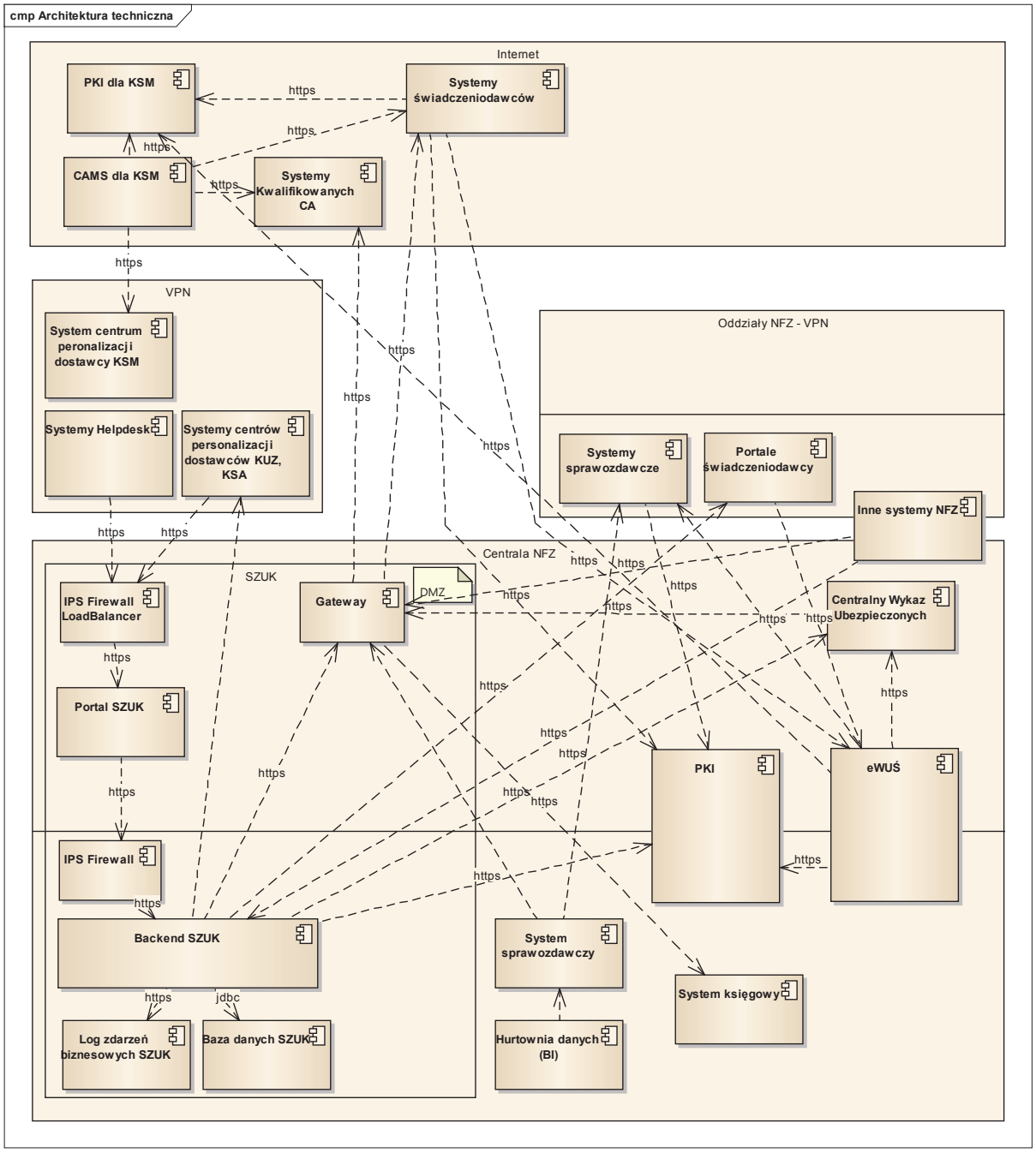
Różnica w architekturach przejściowych będzie dotyczyć liczby użytkowników systemu, zarówno w kontekście wdrożenia na danym obszarze kraju, jak również liczby świadczeniodawców, którzy wdrożą rozwiązania RUM II.

Wdrożenie obsługi kart u Świadczeniodawców, poprzedzone będzie wykonaniem modyfikacji przez dostawców oprogramowania dedykowanego dla Świadczeniodawców. W ramach pilotażowego wdrożenia rozwiązań RUM II przewidziano współpracę z wybranymi dostawcami oprogramowania.

Implementacja zmian w Systemach Świadczeniodawców będzie realizowana przyrostowo.

3.5. Perspektywa techniczna architektury

Poniżej przedstawiono diagram perspektywy technicznej wysokopoziomowej architektury RUM II (w notacji UML).



Rysunek 6 Perspektywa techniczna architektury RUM II

Przedstawiona na diagramie perspektywa techniczna architektury realizuje następujące założenia:

- Wszystkie połączenia poza połączeniem Backend SZUK i Bazy danych SZUK są szyfrowane. Proponowany protokół to https.

- W ramach Centrali NFZ wydzielono DMZ (strefę zdemilitaryzowaną), zawierającą komponenty do łączenia z niezaufaną siecią Internet.
- Wszystkie połączenia przychodzące przechodzą przez IPS (system zapobiegania intruzom), Firewall (zaporę ogniową) oraz opcjonalnie Load Balancer.
- Wszystkie połączenia wychodzące przechodzą przez Gateway (bramę).
- Dla obsługi kart KSM przez MZ przedstawiono uproszczony (w stosunku do Centrali NFZ) model, bez wskazywania wydzielonej strefy DMZ oraz mechanizmów połączeń. Założenia wymagają weryfikacji i dookreślenia przez MZ, dostarczającej kartę KSM. Dotyczy następujących komponentów i połączeń z nimi związanych: CAMS dla KSM, PKI dla KSM, System centrum personalizacji dostawcy KSM.
- Założono, że Centrala NFZ łączy się z oddziałami poprzez szyfrowany VPN (wirtualną sieć prywatną). Podobne założenie jest w stosunku do systemu Help Desk oraz Centrów Personalizacji. Sieć VPN należy skonfigurować tak, aby dawała minimalne potrzebne uprawnienia, a także mapować adresy IP na inne, aby ukryć topologię sieci.
- VPN jest zalecanym sposobem integracji dwóch serwerów z różnych sieci. Wymaga jednak dodatkowej konfiguracji i nie zawsze jest możliwy do zastosowania. Korzystanie z szyfrowanego VPN nie powoduje braku konieczności korzystania z szyfrowanego protokołu (https).
- Jeżeli któryś z systemów nie będzie połączony poprzez VPN należy założyć, że jest w sieci niezaufanej (Internet) i łączyć się z nim analogicznie poprzez Firewall/IPS w jedną stronę i Gateway (bramę) w drugą stronę.
- Analogicznie jeśli któryś z systemów wskazanych obecnie w strefie Internet będzie dostępny poprzez szyfrowany VPN – można zrezygnować z połączenie przez Firewall/IPS oraz Gateway.

3.6. Architektura bezpieczeństwa i niezawodności

3.6.1. Standaryzacja integracji – główne założenia

- Podział sieci na strefy zaufania, znaczenie ma zdalny dostęp jak i fizyczny dostęp do obiektów w danej strefie:
    - Sieć lokalna – zdefiniowana w ramach jednej szafy rackowej lub jednej serwerowni. Zakłada się, że jeśli ktoś ma fizyczny dostęp do serwerów to jest w stanie obejść większość zabezpieczeń, dlatego większy nacisk kładzie się na monitorowanie i ograniczanie fizycznego dostępu do serwerowni niż na zabezpieczenia komunikacji wewnątrz sieci. Jest to jedyna strefa, w której można uzasadnić nieszyfrowaną wymianę danych ze względów wydajnościowych. Przykładem jest dostęp serwera do bazy danych.
    - Intranet – sieć w ramach jednej organizacji lub oddziału; zabezpieczona przed dostępem z zewnątrz organizacji. Wszystkie połączenia są szyfrowane. Część funkcjonalności, które wymagane są tylko dla użytkowników wewnątrz

organizacji powinna być dostępne tylko w tej strefie (np. dedykowany portal z ustawieniami innymi niż w DMZ i niewidoczny z DMZ)

- DMZ (strefa zdemilitaryzowana) – strefa dostępna z Internetu zawierająca dodatkowe zabezpieczenia i dająca ograniczony dostęp do zasobów w Intranecie. Należy ograniczyć dostęp do zasobów Intranetu tylko do tego, co jest niezbędne. Wszystkie połączenia są szyfrowane.
- Internet – pozostała część sieci, czyli reszta świata. Zalecane jest nie zakładanie niczego na temat bezpieczeństwa tej strefy. Każdy dostęp do systemu z Internetu powinien odbywać się poprzez strefę DMZ i być ograniczony do minimum. Wszystkie połączenia są szyfrowane.

- System odwołujący się do zasobów umieszczonych w strefie Internetu musi korzystać z połączenia szyfrowanego. System musi sprawdzać czy połączył się z serwerem, którego oczekiwał. Nie wystarczy sprawdzać ważności certyfikatu serwera, należy sprawdzać czy certyfikat został wystawiony dla adresu, z którym się łączymy. W przypadkach gdy konieczne jest szczególne bezpieczeństwo można sprawdzać także skrót klucza wpisanego wcześniej, jednak wprowadza to ryzyko niedostępności gdyż klucz serwera może zostać zmieniony w dowolnym momencie i wymaga to aktualizacji konfiguracji w systemie.
- Wszystkie integracje pomiędzy systemami powinny być wykonywane poprzez zdalne wywoływanie usług udostępnianych przez systemy. Zalecane jest wykorzystanie protokołu REST po połączeniu szyfrowanym https. Ze względów wydajnościowych zalecane jest wykorzystanie formatu JSON, którego parsowanie jest dużo szybsze niż np. XML. Wszystkie wywołania modyfikujące dane powinny wykorzystywać metody POST lub PUT. Metoda GET możliwa jest jedynie dla odczytów danych.
- Wszystkie dane pochodzące od użytkowników muszą być konwertowane („escape”) zanim zostaną zaprezentowane na ekranie. Inny rodzaj konwersji wykorzystuje się dla HTML, inny dla JavaScript.
- W szczególności należy zweryfikować wszystkie zapytania do bazy danych. Wszystkie parametry zapytań muszą być przekazane do bazy jako parametry (niedozwolone jest używanie ich do bezpośredniego skonstruowania zapytania) aby uniknąć ataku SQL Injection.

3.6.2. Bezpieczeństwo systemu

- Zabezpieczenia muszą być adekwatne do wymagań. Idealnie w trakcie tworzenia wymagań powinna zostać zdefiniowana polityka bezpieczeństwa (odnosząca się do polityki bezpieczeństwa organizacji). Koszt zabezpieczeń rośnie wykładniczo. Wyprodukowanie systemu bezpieczniejszego niż jest to potrzebne powoduje lawinowy wzrost kosztów jego wytworzenia.
- Aby zwiększyć niezawodność systemu należy w trakcie jego produkcji wytworzyć automatyczne testy regresji oraz automatyczne testy integracyjne. Nie należy testować wszystkiego, a pokrycie kodu testami nie powinno przekraczać 80%. Testy

trzeba modyfikować wprowadzając zmiany, co znacznie zwiększa koszt modyfikacji systemu.

- Dla każdej strefy sieci konieczne jest zastosowanie dodatkowych zabezpieczeń sprzętowych adekwatnych do danej strefy.
    - Najlepsze efekty daje połączenie kilku różnych rodzajów zabezpieczeń.
    - Szczególną uwagę należy zwrócić na wykrycie i rejestrowanie zdarzeń bezpieczeństwa. Jest to tańsze niż pełne zapobieganie, a na niewykryte incydenty nie można zareagować.
    - Wszystkie dane wchodzące do DMZ z Internetu muszą przejść przez IPS (system zapobiegania włamaniom) oraz Firewall (zaporę sieciową). Rekomendowanym rozwiązaniem jest zastosowanie tzw. przełączników hybrydowych (ang. Hybrid switches) lub przełączników siódmej warstwy (ang. Layer Seven Switches).
    - Dodatkowe zabezpieczenia należy umieścić przed wejściem do serwera backend systemu. Jako minimum powinien tam się znaleźć dodatkowy Firewall (zapora sieciowa).
    - Rekomendowane jest zastosowanie HIDS (wykrywanie intruzów oparte na gospodarzu) na każdym serwerze systemu.

3.6.3. Bezpieczeństwo danych

- W systemie przechowywane są dane osobowe, jednak szyfrowanie danych na poziomie bazy danych spowoduje spadek wydajności. Dodatkowo nie można szyfrować danych, które będą później użyte do wyszukiwania.
- Właściwym sposobem zabezpieczenia danych przed niepowołanym dostępem będzie:
    - zabezpieczenie przed atakami SQL Injection poprzez poprawną implementację systemu.
    - ograniczenie fizycznego dostępu do serwerowni, w której znajduje się baza danych.
    - uniemożliwienie z poziomu aplikacji pobrania dużej ilości danych osobowych jednocześnie – pozwoli zminimalizować straty w przypadku próby kradzieży danych w ten sposób.
    - dodatkowe szyfrowanie danych przekazywanych centrom personalizacji – dodatkowe zabezpieczenie, gdy dane występują w dużych ilościach i są przekazywane poza system. Nie tylko połączenie, ale także plik z danymi będzie szyfrowany (jest duże prawdopodobieństwo, że centra personalizacji będą zapisywały plik na dysku po swojej stronie); należy wymusić taką konstrukcję obu systemów, aby dane nigdy nie były przechowywane w pliku w postaci jawnej (tylko deszyfrowanie na bieżąco w pamięci ulotnej).
    - logowanie dostępu do danych osobowych w dzienniku zdarzeń – każde pobranie danych osobowych powinno być rejestrowane; dużym problemem będzie zapewnienie dobrej wydajności przy implementacji tej funkcjonalności;

niezbędne jest przeprowadzenie testów wydajnościowych; należy rozważyć optymalizacje np. grupowanie zdarzeń jeśli był jednoczesny dostęp do całej grupy danych; zbieranie rejestru lokalnie i wysyłanie w skompresowanych paczkach itp. Aktualizacja takiego rejestru nie jest potrzebna natychmiast, zwykle wykorzystywana jest do analizy zdarzenia długo po zaistnieniu incydentu bezpieczeństwa.

- Implementację dziennika zdarzeń jako usługi dostępnej na osobnym serwerze – udostępnia tylko funkcje dodawania i pobierania zdarzeń; niemożliwa jest edycja i usuwanie ich bez fizycznego dostępu do serwera. To rozwiązanie może być ryzykowne z uwagi na problemy wydajnościowe. Zdarzenia wysyłane do serwera powinny to być zdarzenia biznesowe, najlepiej agregowane, a nie logi systemowe. Niezależnie zdarzenia powinny być też przechowywane lokalnie na wypadek awarii (lub celowego wyłączenia przez atakującego) sieci.

- Przechowywanie danych uwierzytelniających (login, hasło itp.):
  - system wymaga umożliwienia wielu sposobów logowania – właściwym sposobem implementacji jest delegacja żądania do systemu źródłowego. Nie zalecane jest kopiowanie danych uwierzytelniania z innych systemów – sposób uwierzytelniania (np. hasło) w systemie źródłowym może się zmienić w każdej chwili.
  - Przy przechowywaniu haseł należy bezwzględnie używać nieodwracalnej, jednokierunkowej funkcji skrótu. Rekomendowane jest użycie funkcji skrótu przeznaczonej do przechowywania haseł np. PBKDF2. Ciąg znaków (salt) powinien być losowy, idealnie generowany przez fizyczny generator liczb losowych.
  - W przypadku nieudanego uwierzytelniania należy zwrócić możliwie lakoniczny komunikat o błędzie, nie podając dokładnej przyczyny. (np. komunikat błędu nie powinien różnicować pomiędzy brakiem użytkownika, a złym hasłem).
  - Każde żądanie uwierzytelniania powinno zajmować w przybliżeniu tyle samo czasu (np. odpowiedź nie powinna być szybsza, jeśli nie znaleziono nazwy użytkownika, a wolniejsza jeśli nie zgadza się hasło).
- Zabezpieczenie danych przed utratą:
  - Baza danych musi zapewniać tworzenie kopii zapasowej w locie lub jeśli dopuszczalne jest wyłączenie systemu w nocy musi umożliwiać utworzenie kopii zapasowej w czasie planowanego wyłączenia systemu.
  - Backup bazy danych musi być zabezpieczony przed niepowołanym dostępem; przechowywany w innej fizycznej lokalizacji niż baza danych.
  - Każda wersja oprogramowania własnego działająca produkcyjnie musi mieć numer wersji, który ją identyfikuje. Musi być możliwość pobrania jej ponownie z repozytorium albo ponownego jej zbudowania ze źródeł.
  - Musi być tworzona kopia zapasowa każdego serwera systemu, aby umożliwić szybkie odtworzenie jego stanu. Idealnie wszystkie dane znajdują się w bazie

danych, więc kopie zapasowe serwerów nie muszą być chronione tak mocno jak kopie bazy danych.

- Wszystkie krytyczne elementy systemu korzystające z dysków twardych muszą korzystać z macierzy RAID skonfigurowanej zgodnie z istniejącą polityką bezpieczeństwa. Należy zwrócić uwagę ile czasu trwa odtworzenie macierzy w przypadku awarii i wymiany jednego dysku.
- Należy zapewnić zastępowalność elementów fizycznych systemów np. poprzez umowy wsparcia z firmami zewnętrznymi z gwarantowanym czasem przywrócenia serwera do działania (zgodnie z zapotrzebowaniem).
- Wszystkie elementy krytyczne dla działania systemu powinny być zdublowane (np. karty sieciowe, przełączniki sieciowe itp.).

- Integracje z systemami zewnętrznymi
  - Należy przeanalizować wymagania dla każdej integracji z systemem zewnętrznym. Szczególną uwagę zwrócić na scenariusz, gdy jeden z systemów (lub połączenie między nimi) nie działa.
  - Należy przeanalizować czasy dostępności każdego z integrowanych systemów. Systemy zintegrowane powinny w miarę możliwości mieć zdefiniowane okna serwisowe w tym samym czasie.

3.6.4. Wydajność systemu

- Aby zapewnić właściwą wydajność systemu kluczowym jest zaprojektowanie i zaimplementowanie automatycznych testów wydajnościowych na początku tworzenia systemu. Należy je uruchamiać cyklicznie w trakcie powstawania systemu, aby jak najszybciej wykryć możliwe problemy wydajnościowe. Testy należy wykonywać po zasileniu bazy danych bardzo dużą liczbą wiarygodnych danych.
- W przypadku wykrycia problemów wydajnościowych na początku powstawania systemu można rozważyć użycie rozproszonej bazy danych typu NOSQL zamiast zwykłej relacyjnej bazy danych – jest to szczególnie interesujące, ponieważ system ten bardzo dobrze skaluje się. Duże czynniki ryzyka to nieduża dojrzałość rozwiązań NOSQL oraz duża trudność w projektowaniu takich rozwiązań znacznie zwiększająca ryzyko powstania błędów w trakcie implementacji.
- Największym czynnikiem ryzyka jest komunikacja z systemami zewnętrznymi. Należy przygotować wymagania wydajnościowe dla każdej integracji i jak najszybciej wykonywać testy wydajnościowe. Istotny jest czas odpowiedzi na proste żądania (latency) oraz zbiorczy czas przetwarzania w przypadku zadań wsadowych.
- W przypadku komunikacji z systemem zewnętrznym w Internecie należy zapewnić, że oba systemy będą miały dostęp do szybkich łączy Internetowych (dokładną przepustowość można określić tylko poprzez przeprowadzenie testów wydajnościowych dla każdej integracji). Każdy z systemów powinien mieć przynajmniej dwa niezależne źródła Internetu przełączane automatycznie na wypadek awarii.

- Dla wewnętrznej wydajności systemu kluczowe znaczenie ma odległość serwera backend od jego bazy danych – najlepiej w tej samej serwerowni; oraz utworzenie właściwych indeksów w bazie danych (utworzenie zbyt dużej liczby indeksów na wszelki wypadek także spowolni system).
- Inicjalne zasilanie danych warto wykonywać przy wyłączonych indeksach i w trybie nietransakcyjnym bazy danych. (np. zasilanie wykonywać w nocy przy planowanym wyłączeniu dostępu do systemu). Takie podejście może przyspieszyć zasilanie o rząd wielkości.
- W przypadku wykrycia problemów wydajnościowych w części portalowej należy użyć większej liczby serwerów połączonych w cluster (grupę). Przed serwerami użyć przełącznik wielowarstwowy (content-switch/load balancer). Na etapie wymagań należy sprawdzić czy wybrany portal wspiera replikację sesji, aby był w stanie przełączyć użytkownika między serwerami bez utraty danych.

Koniec dokumentu