

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych   
dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego**

Spis treści

[Wprowadzenie 3](#_Toc527542379)

[1. Cel 3](#_Toc527542380)

[2. Definicje 4](#_Toc527542381)

[3. Opis rozwiązania SWD PRM 10](#_Toc527542382)

[3.1. Architektura logiczna systemu 10](#_Toc527542383)

[3.2. Schemat architektury logicznej środowiska PROD 10](#_Toc527542384)

[3.3. Schemat architektury logicznej środowiska SZK 18](#_Toc527542385)

[3.4. Schemat architektury logicznej środowiska DEV 20](#_Toc527542386)

[3.5. Protokoły i metody wymiany danych pomiędzy serwerem i klientem w ramach SWD PRM 22](#_Toc527542387)

[3.5.2. Inicjowanie komunikacji przez serwer 22](#_Toc527542388)

[3.5.3. Forma komunikatu 22](#_Toc527542389)

[3.6. Architektura bazy danych 23](#_Toc527542390)

[3.6.4. ETL – Extract, Transform and Load 27](#_Toc527542391)

[3.6.5. Lokalna baza danych 27](#_Toc527542392)

[3.7. Bezpieczeństwo 27](#_Toc527542393)

[3.7.2. Certyfikaty 28](#_Toc527542394)

[3.7.3. Uwierzytelnianie i autoryzacja aplikacji Dyspozytora 28](#_Toc527542395)

[3.7.5. Uwierzytelnianie i autoryzacja aplikacji mobilnej ZRM 31](#_Toc527542396)

[3.8. Poufność 32](#_Toc527542397)

[3.9. Integralność 32](#_Toc527542398)

[3.10. Rozliczalność 33](#_Toc527542399)

[3.11. Niezaprzeczalność 33](#_Toc527542400)

[3.12. Ciągłość działania 34](#_Toc527542401)

[3.12.1.1. Utrata połączenia sieciowego od aplikacji klienckich do OK 34](#_Toc527542402)

[3.12.1.3. Awaria zasilania 35](#_Toc527542403)

[3.12.3.2. Awaria macierzy dyskowej 36](#_Toc527542404)

[3.13. Architektura fizyczna systemu 37](#_Toc527542405)

[3.14. Oprogramowanie 39](#_Toc527542406)

[3.14.1. Oprogramowanie serwerowe 39](#_Toc527542407)

[3.14.2. Oprogramowanie klienckie 40](#_Toc527542408)

[3.15. Infrastruktura klucza publicznego (PKI) 40](#_Toc527542409)

[3.16. Ograniczenia 41](#_Toc527542410)

[3.16.1. Wymagania na dostęp administracyjny do SWD PRM z wykorzystaniem OST 112 41](#_Toc527542411)

[3.17. Integracja z systemami zewnętrznymi 42](#_Toc527542412)

[3.17.1. UMM 42](#_Toc527542413)

[3.17.2. PLI CBD 42](#_Toc527542414)

[3.17.3. Integracja z SI CPR 42](#_Toc527542415)

[3.17.4. Automapa 43](#_Toc527542416)

[3.17.5. PZŁ 43](#_Toc527542417)

[4. Usługi rekonfiguracyjne SWD PRM 43](#_Toc527542418)

[4.1. Wymagania w zakresie usług rekonfiguracyjnych SWD PRM 43](#_Toc527542419)

[4.2. Zakres usługi w ramach zleconych prac rekonfiguracyjnych 44](#_Toc527542420)

[5. Usługi utrzymaniowe SWD PRM 45](#_Toc527542421)

[6. Minimalne wymagania w zakresie zarządzania przedmiotem zamówienia 49](#_Toc527542422)

[7. Wymagania w zakresie zgodności z przepisami prawa 50](#_Toc527542423)

[8. WYMAGANIA W ZAKRESIE DOKUMENTACJI 51](#_Toc527542424)

# Wprowadzenie

Przedmiotowe zamówienie dotyczy świadczenia usługi utrzymania, modyfikacji, rekonfiguracji i rozbudowy Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM).

# 1. Cel

Postępowanie ma na celu zapewnienie przez Wykonawcę wsparcia w utrzymaniu oraz rekonfiguracji Aplikacji SWD PRM.

Wykonawca w ramach usług utrzymania będzie zobowiązany do pozostawania w gotowości do dokonania analizy Awarii oraz podjęcia czynności mających na celu jej usunięcie. Wykonawca zobowiązany będzie   
w ramach Zleceń do analizy sposobu realizacji proponowanych przez Zamawiającego usprawnień, Modyfikacji, zmian rekonfiguracyjnych oraz ich implementacji w środowisku produkcyjnym, a także wdrożenia w systemie SWD PRM.

Zamawiający będzie dysponował kodami źródłowymi Aplikacji SWD PRM, i będzie miał do nich prawa autorskie po ich przekazaniu przez ministra właściwego do spraw administracji publicznej, najpóźniej w dniu   
1 stycznia 2019 r. tj. dniu rozpoczęcia realizacji zadania utrzymania SWD PRM na podstawie art. 24a ust. 4 ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2017 r. poz. 2195,   
z 2018 r. poz. 650, 1115, 1544, 1629, 1669).

# 2. Definicje

|  |  |
| --- | --- |
| **Skrót / pojęcie** | **Definicja** |
| **ACD** | (Ang. Automatic Call Distribution) mechanizm automatycznego rozdzielania rozmów przychodzących i przydzielania ich do konkretnych Użytkowników. |
| **AVL** | (Ang. Automatic Vehicle Location) Automatyczna Lokalizacja  Pojazdów. |
| **APN** | (ang. Access Point Name) urządzenia umożliwiające Użytkownikom terminali mobilnych zalogowanym do sieci komórkowych korzystanie z transmisji danych przesyłanych do/z zewnętrznych sieci (np. sieci pakietowych). |
| **Aplikacja kliencka** | Określenie klienta Aplikacji SWD PRM stanowiącej interfejs użytkownika: Aplikacja Administratora, Aplikacja Dyspozytora, Mobilny ZRM, MS ZRM, Planista, Administrator biznesowy, Aplikacja mapy. |
| **Aplikacja serwerowa** | Oprogramowanie aplikacyjne serwerów Ośrodków Krajowych. |
| **Aplikacja SWD PRM** | Aplikacja kliencka oraz Aplikacja serwerowa Systemu Wspomagania  Dowodzenia Państwowego Ratownictwa Medycznego. |
| **Awaria** | Oznacza Awarię Krytyczną i/lub Awarię Niekrytyczną i/lub Awarię  Zwykłą. |
| **Awaria Krytyczna** | Oznacza brak działania środowiska produkcyjnego Systemu, powodujący, że praca nie może być kontynuowana i operacja krytyczna dla procesu biznesowego jest niemożliwa. Awarie Krytyczne mają jedną lub więcej z poniższych cech:   1. dane biznesowe zostały uszkodzone; 2. Funkcjonalność Krytyczna udokumentowana w Dokumentacji nie działa; 3. System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4. wszelkie błędy związane z bezpieczeństwem przechowywania  i przetwarzania danych, które mogą wpłynąć na:    * 1. uwierzytelnianie,      2. niezaprzeczalność,      3. poufność,      4. integralność,      5. dostępność,      6. rozliczalność; 5. wszelkie błędy związane z bezpieczeństwem dostępu do Systemu  (w tym nieautoryzowanym dostępem do danych). |
| **Awaria Niekrytyczna** | Oznacza utrudnienie działania Systemu w środowisku produkcyjnym  w zakresie pozostałych funkcjonalności. W tym kontekście „utrudnia” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez Wykonawcę procedury, tudzież procedury przygotowane przez Zamawiającego  i zaakceptowane przez Wykonawcę w trakcie okresu utrzymania co może mieć wpływ na wygodę w użytkowaniu Systemu lub wymagać procedur ręcznych. („Uniemożliwia” oznacza brak możliwości jego obejścia). |
| **Awaria Zwykła** | Każda awaria niebędąca Awarią Krytyczną lub Awarią  Niekrytyczną. |
| **CPR** | Centrum Powiadamiania Ratunkowego. |
| **Dni Robocze** | Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 8.00 do 15:35. |
| **Dokumentacja** | Wytworzone przez Wykonawcę w ramach realizacji umowy i podlegające zatwierdzeniu przez Zamawiającego, materiały w formie papierowej, jak również informacje zapisane na innych nośnikach, w tym nośnikach elektronicznych oraz zmiany/uzupełnienia Dokumentacji posiadanej przez Zamawiającego. |
| **Dokumentacja medyczna PRM** | Karta zlecenia wyjazdu zespołu ratownictwa medycznego, karta medycznych czynności ratunkowych, księga dysponenta zespołów ratownictwa medycznego (dokumentacja zgodna z Rozporządzenie Ministra Zdrowia  z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2015r., poz. 2069) |
| **Dysponent** | Podmiot leczniczy w rozumieniu przepisów o działalności leczniczej,  w którego skład wchodzi jednostka systemu, o której mowa w art. 32 ust. 1 Ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (t.j. Dz. U z 2017 r. poz. 2195, z późn. zm.). |
| **Dyspozytor Medyczny** | Użytkownik realizujący zadania przyjmowania zgłoszeń alarmowych  z centrów powiadamiania ratunkowego, o których mowa w art. 3 ust. 2 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (t.j. Dz.U. z 2018r., poz.867), oraz powiadomień o zdarzeniach, dysponowanie zespołów ratownictwa medycznego, rejestrowanie zdarzeń medycznych, prezentację położenia geograficznego miejsca zdarzenia, pozycjonowanie zespołów ratownictwa medycznego, wykorzystujący system SWD PRM. Rola i zakres działania dyspozytora medycznego jest zdefiniowany w ustawie o Państwowym Ratownictwie Medycznym oraz Rozporządzeniu Ministra Zdrowia w sprawie ramowych procedur przyjmowania wezwań przez dyspozytora medycznego i dysponowania zespołami ratownictwa medycznego (Dz. U. z 2014 r. poz. 66). |
| **Dyspozytornia medyczna**  **(DM)** | Lokalizacja, w której znajdują się stanowiska pracy dyspozytorów medycznych. |
| **Funkcjonalność Krytyczna** | Jako funkcjonalności krytyczne uznaje się:   1. Obsługa zdarzenia – główny proces biznesowy Systemu, podzielony na podprocesy: 2. przyjęcie zgłoszenia (w tym zgłoszenia z CPR oraz powiadomienia o zdarzeniach), 3. zadysponowanie ZRM, 4. przyjęcie zlecenia wyjazdu przez ZRM; 5. Monitorowanie ZRM w zakresie: status wyjazdu, lokalizacja ZRM; 6. Przejęcie obsługi zdarzeń przez inną DM.   Brak funkcjonalności krytycznej wynikły z awarii elementów tworzących System, będących poza odpowiedzialnością Wykonawcy w ramach realizacji przedmiotu niniejszego zamówienia nie powoduje wystąpienia Awarii Krytycznej. |
| **GPS** | (Ang. Global Positioning System) system nawigacji satelitarnej. |
| **GUGiK** | Główny Urząd Geodezji i Kartografii. |
| **Incydent serwisowy** | Oznacza zgłoszenie do Wykonawcy przez Zamawiającego, Użytkowników lub osoby wskazane przez Zamawiającego realizowane w trybie 24/7, nieprawidłowości w działaniu Systemu. Wykonawca zobowiązany jest do rejestracji zgłoszenia incydentu oraz usuwania Awarii, w tym usterek, nieprawidłowości w działaniu, uszkodzeń, wad Urządzeń lub dostarczenia procedur obejścia, powodujących przywrócenie działania Systemu  i rozwiązania problemu. Incydenty niestanowiące Awarii, błędu lub usterki, nieprawidłowości w działaniu, uszkodzeń, wad Urządzeń Wykonawca przekazuje do podmiotu wskazanego przez Zamawiającego. |
| **KD** | Konsola Podsystemu Zintegrowanej Łączności. |
| **Modyfikacja** | Oznacza wyższe wersje (update/upgrade), patche i programy korekcji błędów Oprogramowania Aplikacyjnego, a także inne zmiany funkcjonalne ponad określone w przedmiocie niniejszego zamówienia, do których wykonania  i dostarczenia wraz z odnoszącą się do nich Dokumentacją, na rzecz Zamawiającego zobowiązany jest Wykonawca. |
| **MS ZRM** | Miejsce stacjonowania zespołów ratownictwa medycznego (ZRM) zdefiniowane jako miejsce wyczekiwania ZRM-u w ramach struktury Dysponenta. |
| **Odbiór** | Potwierdzenie spełnienia przez Wykonawcę całości zobowiązań określonych w Zleceniu. |
| **Oprogramowanie** | Oprogramowanie Standardowe i Oprogramowanie Aplikacyjne. |
| **Oprogramowanie Standardowe** | Oznacza oprogramowanie powszechnie dostępne i eksploatowane na dzień złożenia oferty, którego producentem jest Wykonawca lub podmiot trzeci,  w tym wyższe wersje (update/upgrade), patche i programy korekcji błędów Oprogramowania Standardowego.  Oprogramowania Standardowego wykorzystywane jest w poniższych |
|  | obszarach:   1. system operacyjny; 2. oprogramowanie bazodanowe; 3. oprogramowanie do tworzenia raportów; 4. oprogramowanie antywirusowe; 5. oprogramowanie ETL (ang. Extract, Transform and Load); 6. oprogramowanie do wirtualizacji; 7. oprogramowanie serwera aplikacyjnego; 8. oprogramowanie narzędziowe do monitorowania i diagnozy Systemu; 9. oprogramowanie do nawigacji samochodowej; 10. oprogramowanie Infrastruktury Klucza Publicznego (PKI); 11. oprogramowanie serwera konfiguracji i plików instalacyjnych dla wirtualnych maszyn działających w systemie; 12. oprogramowanie narzędziowe do monitorowania i diagnozy Systemu; 13. oprogramowanie dedykowane dla repozytorium aktualizacji Aplikacji klienckiej. |
| **Oprogramowanie Aplikacyjne** | Oznacza oprogramowanie Aplikacji SWD PRM wraz z kompletnymi kodami źródłowymi wytworzone i dostarczone w ramach realizacji poprzednich umów, do którego Zamawiający posiada majątkowe prawa autorskie oraz wskazane wyżej oprogramowanie po modyfikacjach dokonanych w ramach realizacji poprzednich umów. |
| **OST** | Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numerów alarmowych. |
| **Ośrodek Krajowy (OK)** | Centrum serwerowe w oparciu o które jest zbudowana architektura Systemu na poziomie centralnym (POK oraz ZOK). |
| **PRM** | Państwowe Ratownictwo Medyczne. |
| **Protokół Odbioru** | Dokument stanowiący potwierdzenie dokonanie Odbioru w zakresie realizacji Zleceń. |
| **PSP** | Państwowa Straż Pożarna. |
| **Rejon Operacyjny** | Obszar działania zespołu ratownictwa medycznego[[1]](#footnote-1) określony  w wojewódzkim planie działania systemu Państwowe Ratownictwo Medyczne. |
| **SD** | Stanowisko dostępowe Użytkownika. |
| **SWD** | System Wspomagania Dowodzenia klasy dyspozytorskiej „czasu rzeczywistego” wspomagający proces przyjęcia i obsługi wywołań alarmowych. |
| **SLA** | Service Level Agreement – usługa serwisowa regulująca poziom dostępności SWD PRM. |
| **PLI CBD** | Platforma Lokalizacyjno-Informacyjna z Centralną Bazą Danych, dostarczona przez Urząd Komunikacji Elektronicznej (UKE) będąca źródłem danych centralnego punktu systemu powiadamiania ratunkowego, o którym mowa w art.78 ust.4 pkt 1 ustawy z dnia 16 lipca 2004 roku Prawo telekomunikacyjne ( t.j. Dz.U z 2018 r., poz.1954) |
| **POK** | Podstawowy Ośrodek Krajowy. |
| **System** | System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego składający się z Oprogramowania Aplikacyjnego umożliwiającego przyjęcie |z centrum powiadamiania ratunkowego, o którym mowa w art. 3 ust. 2 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego, zgłoszeń alarmowych oraz powiadomień o zdarzeniach, dysponowanie zespołów ratownictwa medycznego, rejestrowanie zdarzeń medycznych, prezentację położenia geograficznego miejsca zdarzenia, pozycjonowanie zespołów ratownictwa medycznego oraz wsparcie realizacji zadań przez zespoły ratownictwa medycznego i wojewódzkiego koordynatora ratownictwa medycznego. |
| **SI PR** | System Informatyczny Powiadamiania Ratunkowego. |
| **SI CPR** | System Informatyczny Centrów Powiadamiania Ratunkowego. |
| **TM** | Terminal mobilny - przenośny komputer osobisty stanowiący element wyposażenia ambulansu ZRM. |
| **UMM** | Uniwersalny Moduł Mapowy udostępniany przez GUGiK. |
| **Urządzenia** | Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i odnoszącą się do nich dokumentacja techniczną producenta, w tym również okablowanie strukturalne i szafy rackowe oraz ich wyposażenie, będące przedmiotem niniejszego zamówienia |
| **Użytkownik** | Oznacza podmiot korzystający z Systemu. |
| **VPN** | VPN ([ang.](https://pl.wikipedia.org/wiki/J%C4%99zyk_angielski) Virtual Private Network, Wirtualna Sieć Prywatna) – [tunel,](https://pl.wikipedia.org/wiki/Tunel_(informatyka)) przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak [Internet)](https://pl.wikipedia.org/wiki/Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób [pakietów.](https://pl.wikipedia.org/wiki/Pakiet_telekomunikacyjny) Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa.  Określenie „wirtualna” oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łączy. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. |
| **Zamawiający** | Lotnicze Pogotowie Ratunkowe. |
| **Zdarzenie** | Oznacza zgłoszenie przyjęte do realizacji przez dyspozytora medycznego przekazane przez operatora numerów alarmowych do dyspozytora medycznego lub będące zainicjowanym przez dyspozytora medycznego celem dalszej obsługi np. zadysponowania ZRM. |
| **Zlecenie** | Oznacza zamówienie złożone przez Zmawiającego na wykonanie Usług Rekonfiguracji. |
| **ZOK** | Zapasowy Ośrodek Krajowy. |
| **ZRM** | Zespół ratownictwa medycznego. |

# 3. Opis rozwiązania SWD PRM

## 3.1. Architektura logiczna systemu

Ze względu na krytyczny charakter Systemu komponenty fizyczne i logiczne zostały rozproszone na dwa Ośrodki Krajowe (OK). Architektura obu Ośrodków Krajowych (POK i ZOK) została zorganizowana   
w identyczny sposób. W obu OK znajdują się środowiska: produkcyjne (PROD), szkoleniowo-testowe (SZK) oraz developerskie (DEV).

1. **PROD** – środowisko produkcyjne dedykowane pod obsługę zgłoszeń dla PRM.
2. **SZ**K – środowisko szkoleniowo-testowe dedykowane do prowadzenia szkoleń użytkowników i administratorów oraz testowania rozszerzeń systemu.
3. **DEV** – środowisko deweloperskie dedykowane do rozwoju nowych funkcjonalności systemu.

Całość ruchu sieciowego w ramach Systemu SWD PRM jest realizowana poprzez sieć OST 112. Konfiguracja ruchu sieciowego jest realizowana przez operatora sieci OST112. Połączenia sieciowe związane z obsługą stanowisk mobilnych zainstalowanych w ambulansach wymagają dostępu do sieci OST 112 i obsługiwane są przez APN zapewniany przez Zamawiającego, podłączony do punktów styku CP SPR (Centralny Punkt Systemów Powiadamiania Ratunkowego) w Warszawie i Katowicach zarządzanych przez operatora OST112.

Stanowiska w MS ZRM również wymagają dostępu do sieci OST 112. Dostęp ten realizowany jest   
z wykorzystaniem połączeń VPN na stacjach roboczych.

## 3.2. Schemat architektury logicznej środowiska PROD

## 

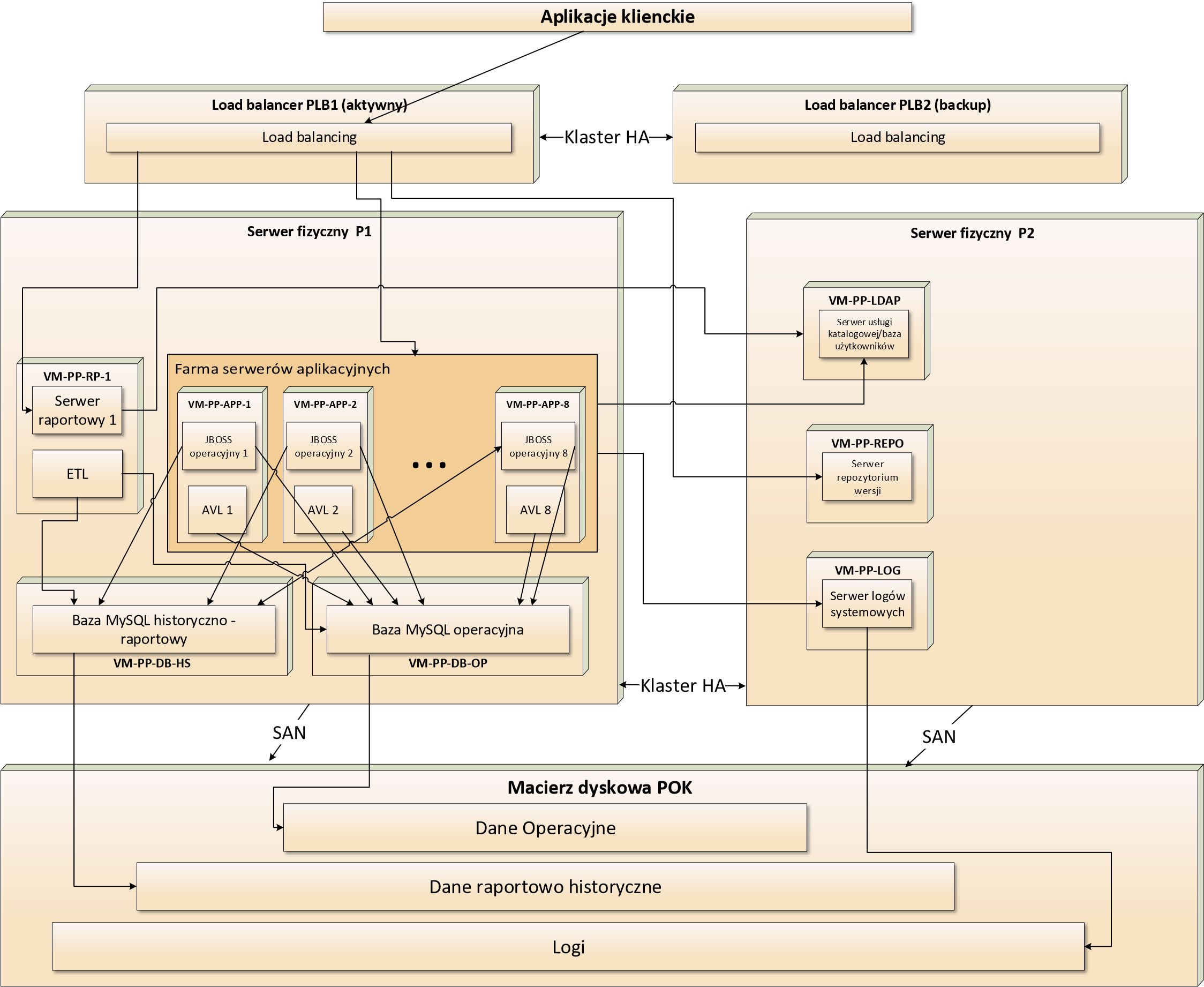
Poniższy rysunek prezentuje ogólny schemat architektury logicznej środowiska PROD dla POK. Przedstawiono na nim komponenty uwzględniające: fizyczne urządzenia (maszyny serwerowe, macierze, loadbalancery), maszyny wirtualne oraz zainstalowane na nich serwery programowe oraz bazy danych, a także połączenia (przepływ danych między komponentami).

Dla przejrzystości rysunków nie pokazano połączeń między serwerami:

1. JBOSS Operacyjny 4 – 6;
2. AVL 4 – 6;
3. Serwer raportowy 2, a bazami danych:
4. MySQL operacyjny,
5. MySQL historyczno – raportowy.

Sposób realizacji tych połączeń jest analogiczny jak w przypadku odpowiadających sobie komponentów pokazanych w ramach pierwszej maszyny fizycznej.

Zarówno w POK jak i w ZOK są uruchomione identyczne środowiska PROD.



*Rysunek nr 1. Diagram ogólny architektury logicznej POK dla środowiska PROD.*

Poniżej opisano podstawowe elementy widoczne na Rysunku 1:

* **Loadbalancery** – po dwa urządzenia na każdy OK. Loadbalancery rozkładają ruch na serwery aplikacyjne dla żądań od aplikacji klienckich oraz od innych systemów, którym SWD udostępnia interfejsy w warstwie integracji.
* **Serwer usługi katalogowej** – serwer odpowiedzialny za przechowywanie danych autoryzacyjnych użytkowników, ich ról w systemie oraz certyfikatów.
* **Serwer logów systemowych** – serwer odpowiedzialny za gromadzenie logów systemowych. Uwaga: dane umożliwiające zapewnienie rozliczalności i niezaprzeczalności działań użytkowników w ramach Systemu, a w szczególności działań administratorów systemu, są zapisywane w bazie danych.
* **Serwer raportowy** – serwer udostępniający logikę dla modułu raportowego dla analityków Dysponentów oraz mechanizmy ETL do przenoszenia danych z bazy operacyjnej do historyczno - raportowej.
* **Serwery aplikacyjne (Wildfly)** – farma serwerów aplikacji odpowiedzialnych za wykonywanie logiki biznesowej.
* **Serwery AVL** – usługi stanowiące uruchomione na serwerach aplikacyjnych JBOSS, komunikujące się z urządzeniami GPS w pojazdach w celu odbierania pozycji pojazdów i innych parametrów, zapisujące je na bieżąco w operacyjnej bazie danych.
* **Serwer MySQL operacyjny** – serwer bazy danych odpowiedzialnej za przechowywanie danych operacyjnych (danych zdarzeń / zleceń; statusów, pozycji i stanów pojazdów; danych użytkowników, itp.).
* **Serwer MySQL historyczno - raportowy** – serwer bazy danych odpowiedzialny za przechowywanie danych historycznych Systemu, a w szczególności dokumentacji medycznej, zarchiwizowanych statusów, pozycji i stanów pojazdów, zleceń wyjazdu, itp.

Architektura logiczna i fizyczna Systemu została zoptymalizowana pod kątem wydajności oraz dostępności, a także zastępowalności komponentów architektury na wypadek ich awarii. Poniżej znajduje się lista komponentów / mechanizmów odpowiedzialnych za niniejsze atrybuty Systemu.

* **Loadbalancing** – cały ruch sieciowy od aplikacji klienckich oraz systemów zewnętrznych przechodzi przez mechanizm rozkładania obciążenia.
* **Redundancja komponentów** – w ramach jednego OK uruchomione są maszyny fizyczne działające w klastrze VMware vSphere.
* **Farma serwerów aplikacyjnych** – serwery aplikacyjne (w tym AVL) są powielone w ramach farmy serwerów tak, aby zwiększyć równoczesność przetwarzania krytycznych żądań oraz zastępowalność dla modułów realizujących funkcjonalności krytyczne.
* **Baza danych** – w ramach jednego OK bazy danych są zorganizowane w klaster niezawodnościowy. W przypadku awarii bazy danych, zostanie ona automatycznie uruchomiona na drugiej maszynie fizycznej. Operacyjna baza danych synchronizowana jest między POK   
  a ZOK za pomocą mechanizmu replikacji zapewniona przez wtyczkę MySQL obsługującą dwustronną replikację semi-synchroniczną. Dane zapisywane w bazie danych POK są powielane za pomocą tego mechanizmu do bazy w ZOK i na odwrót: dane zapisywane w bazie danych ZOK są powielane do bazy w POK. Jeśli połączenie pomiędzy ośrodkami krajowymi działa poprawnie, każda transakcja bazodanowa jest wykonywana synchronicznie w obydwu bazach danych   
  w sposób opisany poniżej. Dzięki temu każda pojedyncza operacja dla aplikacji klienckich może być realizowana zarówno przez POK jak i przez ZOK. W szczególności aplikacja kliencka (na przykład Moduł dyspozytora) może wykonywać operacje z serwerem naprzemiennie – raz korzystając z POK, raz z ZOK.

Sposób pracy w trybie synchronicznym:

• Zapytanie z aplikacji klienckiej (np. Modułu dyspozytora) trafia do ośrodka krajowego A (POK lub ZOK).

* Serwer aplikacyjny w ośrodku A obsługuje zapytanie, w wyniku którego powstaje transakcja zapisu do bazy danych.
  + Baza danych w ośrodku A wykonuje transakcję zapisu w następujący sposób:
  + Transakcja jest wykonywana w ośrodku A.
  + Polecenie wykonania transakcji jest wysyłane do ośrodka B.
  + Ośrodek B zapisuje transakcję do logu bazy danych na dysku.
  + Po potwierdzeniu wykonania powyższych operacji w ośrodku A i w ośrodku B transakcja kończy się. Mamy pewność, że dane są spójne w bazach ośrodka A i B.

Dzięki podwójnemu wykorzystaniu mechanizmu replikacji semisynchronicznej, synchronizacja między ośrodkami POK i ZOK przebiega w dwu kierunkach jednocześnie:

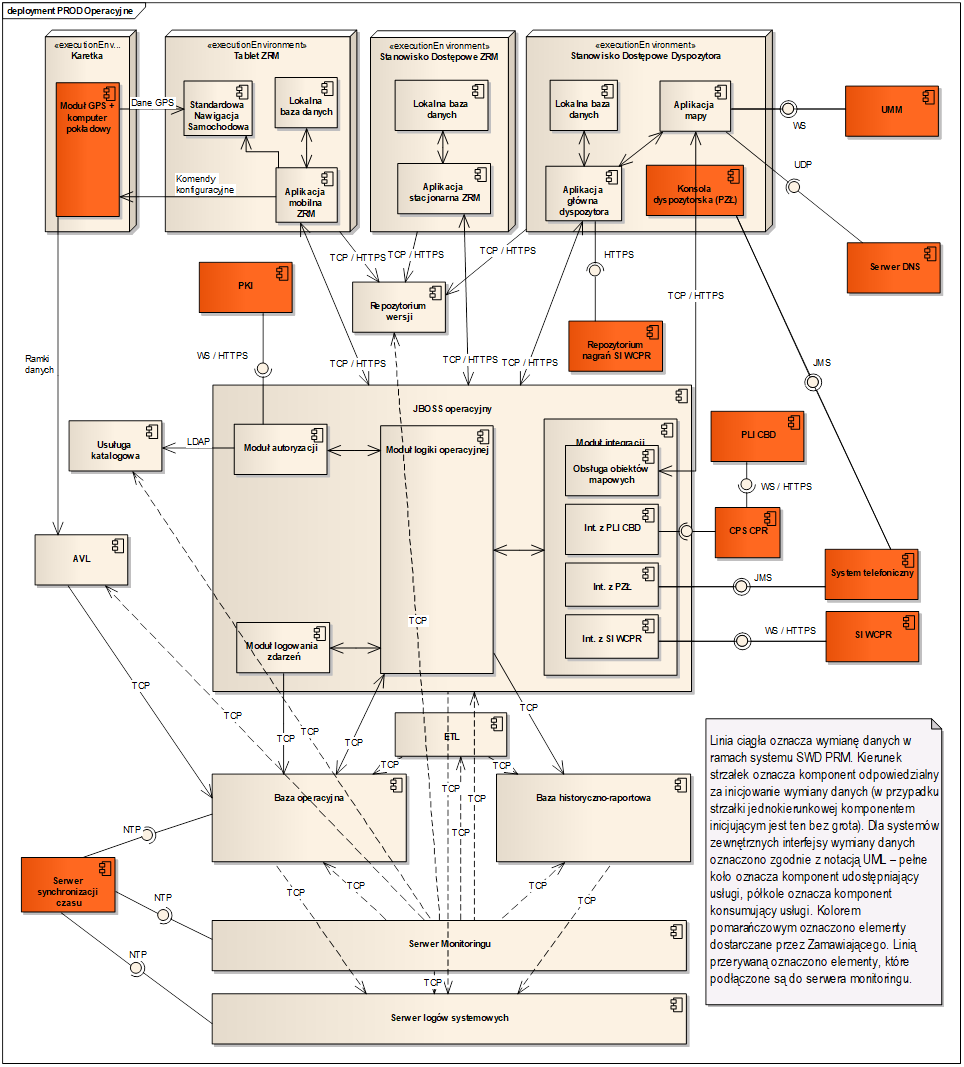
* POK aktywny (master) → ZOK pasywny (slave),
* ZOK aktywny (master) → POK pasywny (slave),
* obydwa ośrodki działające jako „aktywny – aktywny” w trybie synchronicznym.

Rysunek nr 2 prezentuje diagram architektury logicznej środowiska produkcyjnego z uwzględnieniem stanowisk dostępowych dyspozytorów medycznych, stanowisk dostępowych w miejscach stacjonowania ZRM oraz terminali mobilnych. Na diagramie pokazano jedynie komponenty odpowiedzialne za działania operacyjne. Na diagramie nie pokazano komponentów, które pracują w farmie lub trybie Stand-By. Na rysunku pokazano integrację z systemami zewnętrznymi z uwzględnieniem kierunku oraz standardu wymiany danych.

Na poniższych rysunkach przyjęto następujące oznaczenie protokołów komunikacji:

1. WS – WebService;
2. JMS - Java Messaging Service - standard asynchronicznego przesyłania komunikatów w języku programowania Java;
3. TCP - Transmission Control Protocol;
4. FTP - File Transfer Protocol;
5. LDAP - Lightweight Directory Access Protocol;
6. NTP - Network Time Protocol;
7. HTTPS - Hypertext Transfer Protocol Secure;
8. UDP - User Datagram Protocol.

Linia ciągła oznacza wymianę danych w ramach systemu SWD PRM. Kierunek strzałek oznacza komponent odpowiedzialny za inicjowanie wymiany danych (w przypadku strzałki jednokierunkowej komponentem inicjującym jest ten bez grota). Dla systemów zewnętrznych interfejsy wymiany danych oznaczono zgodnie z notacją UML – pełne koło oznacza komponent udostępniający usługi, półkole oznacza komponent konsumujący usługi. Kolorem pomarańczowym oznaczono elementy dostarczane przez Zamawiającego.



*Rysunek nr 2. Architektura logiczna środowiska PROD. Działania operacyjne.*

Moduły zewnętrzne SWD PRM:

* + **Moduł GPS i komputer pokładowy** – moduł instalowany w ambulansach przesyłające do serwera AVL dane dotyczące parametrów pojazdu oraz danych dotyczących położenia geograficznego karetki. Moduł GPS przesyłała dane dotyczące położenia zespołu ratownictwa medycznego do Standardowej nawigacji samochodowej zainstalowanej na tablecie za pomocą kabla USB podłączonego do stacji dokującej tabletu. Sterowanie modułem GPS przez Aplikację mobilną nie jest możliwe, gdyż nie zostało to technicznie umożliwione przez Dostawcę modułów GPS i terminali mobilnych.
  + **Moduł PKI** – moduł obsługi certyfikatów i kluczy.
  + **Usługa katalogowa** – serwer LDAP służący do przechowywania danych użytkowników, ich ról, kluczy publicznych, a także do centralnego zarządzania użytkownikami Systemu.
  + **Serwer synchronizacji czasu** – serwer umożliwiający synchronizację czasu dla kluczowych elementów Systemu.
  + **Konsola Dyspozytorska (PZŁ)** – konsola podsystemu zintegrowanej łączności umożliwiająca obsługę połączeń głosowych integrująca się z Systemem telefonicznym.
  + **PLI CBD** – Platforma lokalizacyjno-informacyjna z centralną bazą danych integrująca się   
    z Systemem poprzez Centralny Punkt Styku Centrum Powiadamiania Ratunkowego.
  + **SI CPR** – System Informatyczny Centrum Powiadamiania Ratunkowego.
  + **Repozytorium nagrań**– repozytorium zarchiwizowanych rozmów telefonicznych   
    w Podsystemie Zintegrowanej Łączności SICPR..
  + **UMM** – Uniwersalny moduł mapowy, umożliwiający wyświetlanie mapy oraz aktualizację danych dotyczących sił i środków.

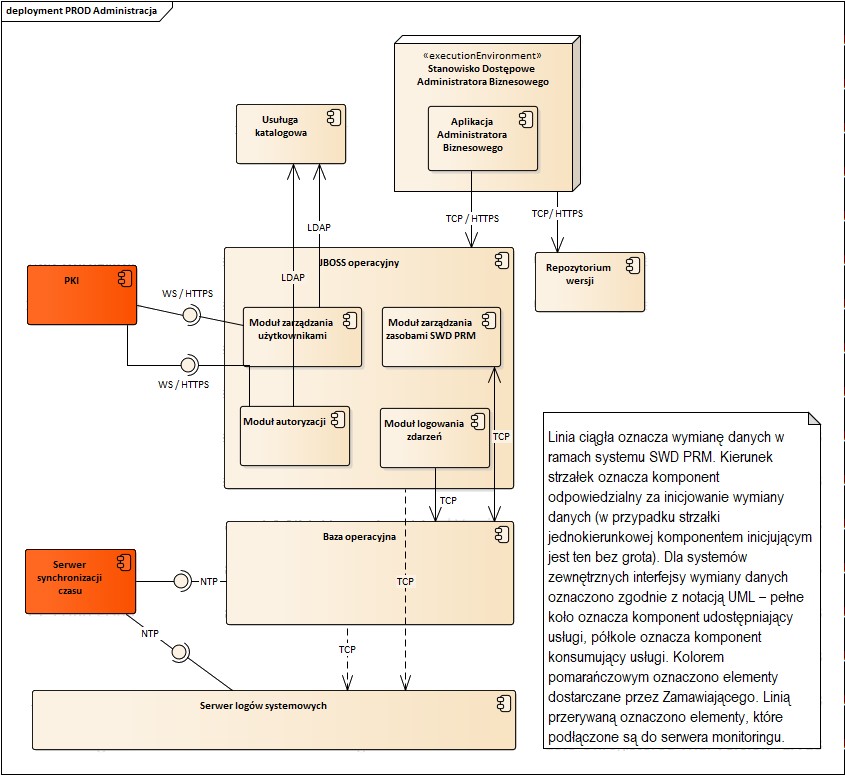
Moduły wewnętrzne:

* + **Aplikacja mobilna (Moduł Mobilny ZRM)** – uruchamiana na tablecie, składająca się   
    z następujących elementów:
    1. Lokalna baza danych – osadzona w aplikacji, szyfrowana baza danych H2, przechowująca tymczasowe dane przed wysłaniem do OK, dane słownikowe, b) Aplikacja mobilna,

c) Standardowa nawigacja samochodowa – oprogramowanie standardowe, z którym Aplikacja komunikuje się za pomocą API udostępnianego przez nawigację.

* + **Aplikacja MS ZRM (Moduł Stacjonarny ZRM)** – uruchamiana na Stanowisku Dostępowym w miejscu stacjonowania ZRM, składająca się z następujących elementów:
    1. Lokalna baza danych – osadzona w aplikacji, szyfrowana baza danych H2, przechowująca tymczasowe dane przed wysłaniem do OK, dane słownikowe,
    2. Aplikacja desktopowa MS,
* **Aplikacja SD Dyspozytora (Moduł Dyspozytora i Moduł Mapy)** – uruchamiana na Stanowisku Dostępowym w Dyspozytorni, składająca się z następujących elementów:
  1. Lokalna baza danych – osadzona w aplikacji, szyfrowana baza danych H2, przechowująca tymczasowe dane przed wysłaniem do OK, dane słownikowe,
  2. Aplikacja desktopowa Dyspozytora – ma możliwość, poprzez komunikację HTTPS, pobrania pliku nagrania głosowego, do którego hiperłącze zwracane jest poprzez komunikację między Systemem SWD PRM a SI WCPR,
  3. Aplikacja mapy – aplikacja wyświetlająca dane lokalizacyjne sił i środków, miejsca zdarzenia, umożliwiająca określenie lokalizacji zdarzenia i wzywającego na podstawie wskazania punktu na mapie. Aplikacja mapy komunikuje się poprzez proces systemu operacyjnego z Aplikacją desktopową dyspozytora.
* **Serwery AVL** – usługi serwerów JBOSS/Wildfly odbierające ramki z danymi dotyczącymi położenia pojazdu oraz jego danych z komputera pokładowego, transformujący dane i zapisujący w bazie danych.
* **JBOSS operacyjny** – działający w klastrze serwer logiki operacyjnej, składający się   
  z następujących modułów:
  1. Moduł autoryzacji – odpowiedzialny za uwierzytelnianie i autoryzację użytkowników, komunikację z systemem PKI oraz usługą katalogową, zarządzanie użytkownikami i rolami.
  2. Moduł logowania zdarzeń – odpowiedzialny za logowanie czynności wykonywanych przez użytkowników systemu w zakresie czynności operacyjnych, dostępu do danych, edycji danych, tworzenia, modyfikacji i dezaktywacji użytkowników, czasów pracy, czasów obsługi zdarzenia.
* **Baza operacyjna** – baza danych odpowiedzialna za przechowywanie danych operacyjnych (danych zdarzeń / zleceń; statusów, pozycji i stanów pojazdów; danych użytkowników, itp.). Baza operacyjna wykorzystuje mechanizm replikacji (do synchronizacji danych między POK a ZOK).
* **Baza historyczno - raportowa** – baza danych odpowiedzialna za przechowywanie danych historycznych Systemu, a w szczególności dokumentacji medycznej (przez okres 20 lat) zarchiwizowanych statusów, pozycji i stanów pojazdów, itp. (przez okres 2 lat). Baza historyczna nie jest replikowana pomiędzy POK a ZOK. Dane do instancji baz raportowych w ramach poszczególnych OK trafiają do nich (z bazy operacyjnej) cyklicznie za pomocą procesu ETL.
* **ETL** – proces odpowiedzialny za przenoszenie danych z bazy operacyjnej do bazy historyczno – raportowej.
* **Serwer monitoringu** – serwer odpowiedzialny za monitorowanie stanu i prawidłowego działania kluczowych komponentów Systemu.
* **Serwer logów systemowych** – serwer odpowiedzialny za gromadzenie logów systemowych.
* **Serwer DNS** – na potrzeby komunikacji stacji roboczych z GUGIK (dostawca map) wykorzystywane są serwery DNS z projektu SI WCPR.

**Aplikacja Administratora biznesowego (Moduł Administratora – rysunek nr 3)**  – aplikacja umożliwiająca zarządzanie konfiguracją techniczną i biznesową Systemu, zarządzanie użytkownikami, siłami i środkami, Dysponentami, DM i ZRM-ami.

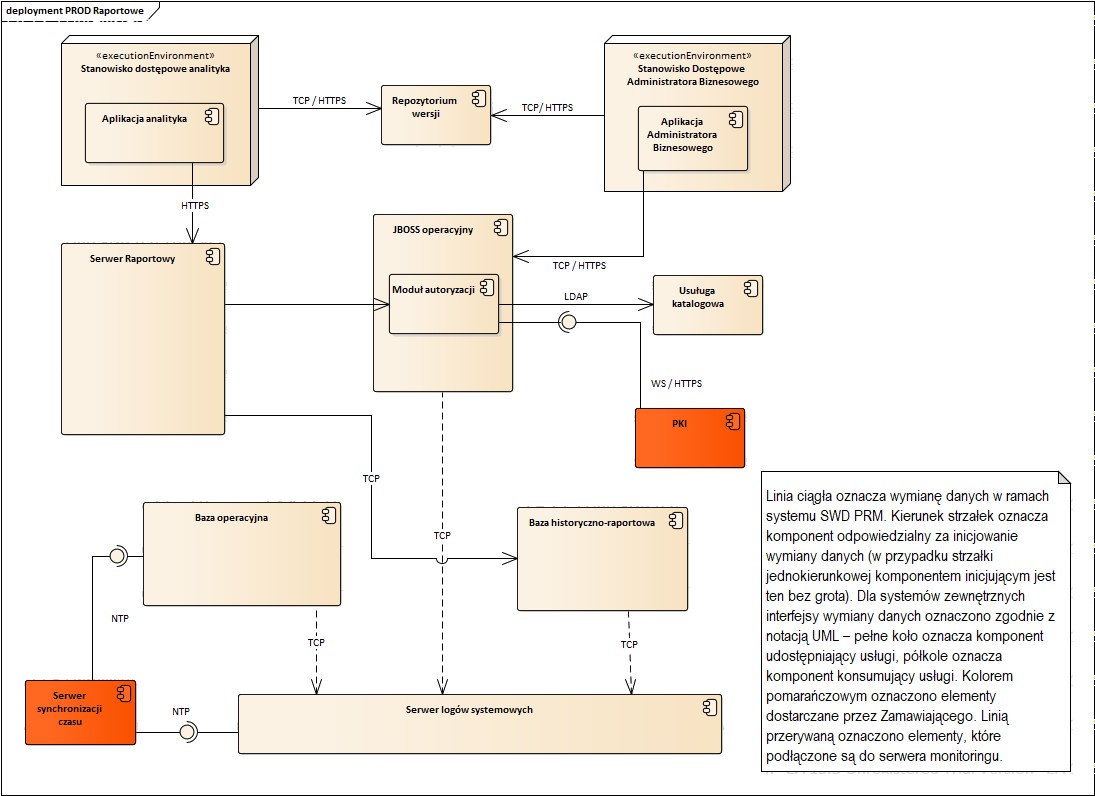


*Rysunek nr 3. Architektura logiczna środowiska PROD. Działania administracyjne.*

Rysunek nr 4 prezentuje diagram architektury logicznej środowiska produkcyjnego z uwzględnieniem stanowiska analityka raportów. Na diagramie pokazano jedynie komponenty odpowiedzialne za działania raportowe (analitycy). Na rysunku pokazano integrację z systemami zewnętrznymi z uwzględnieniem kierunku oraz standardu wymiany danych.

Poniżej opisano podstawowe elementy widoczne na tym rysunku (z pominięciem opisanych wcześniej): - moduły wewnętrzne (dostarczane lub tworzone przez Wykonawcę):

* Aplikacja Analityka (Moduł Raportowy) – aplikacja umożliwiająca tworzenie raportów, wgląd do danych statystycznych i historycznych.
* Serwer Raportowy – serwer raportów na potrzeby analityków Dysponenta.

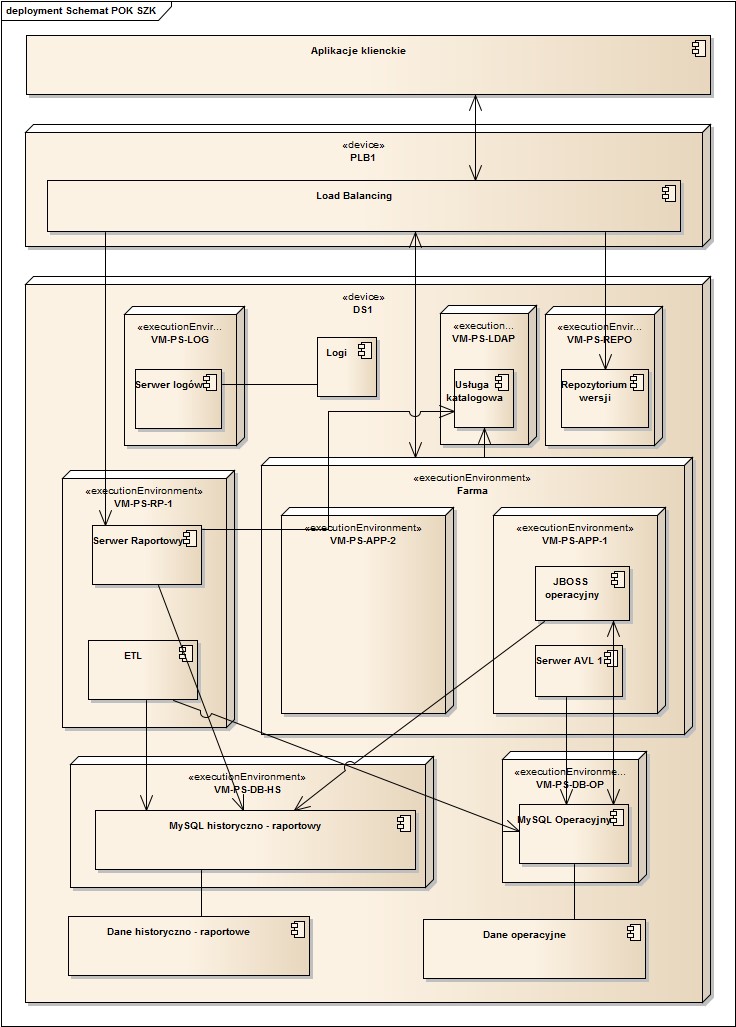


*Rysunek nr 4. Architektura logiczna środowiska PROD. Działania raportowe.*

## 3.3. Schemat architektury logicznej środowiska SZK

Rysunek nr 5 prezentuje ogólny diagram architektury logicznej środowiska SZK dla pojedynczego OK. Wszystkie wirtualne maszyny uruchomione są na jednej maszynie serwerowej (współdzielonej ze środowiskiem DEV). Dane zapisywane są na dyskach twardych maszyny serwerowej.

Zarówno w POK jak i ZOK są uruchomione identyczne środowiska SZK. Logicznie środowisko SZK odzwierciedla funkcjonalność środowiska produkcyjnego.



*Rysunek nr 5. Diagram ogólny architektury logicznej POK dla środowiska SZK.*

## 3.4. Schemat architektury logicznej środowiska DEV

Rysunek nr 6 prezentuje ogólny diagram architektury logicznej środowiska DEV dla pojedynczego OK. Wszystkie wirtualne maszyny uruchomione są na jednej maszynie serwerowej (współdzielonej ze środowiskiem SZK). Dane zapisywane są na dyskach twardych maszyny serwerowej.

Zarówno w POK jak i ZOK są uruchomione identyczne środowiska DEV. Logicznie środowisko DEV odzwierciedla funkcjonalność środowiska produkcyjnego. Dodatkowo środowisko DEV umożliwia implementowanie i testowanie nowych funkcjonalności Systemu, a także mechanizmów związanych  
z przełączaniem OK. Szczegóły dotyczące maszyn wirtualnych i fizycznych znajdują się w Dokumentacji Eksploatacyjnej.



*Rysunek nr 6. Diagram ogólny architektury logicznej POK dla środowiska DEV.*

## 3.5. Protokoły i metody wymiany danych pomiędzy serwerem i klientem w ramach SWD PRM

Wymiana danych pomiędzy serwerem a aplikacjami klienckimi jest dwukierunkowa i może być inicjowana zarówno przez aplikację klienta jak i serwer.

**3.5.1. Inicjowanie komunikacji przez aplikację kliencką**

Aplikacja klienta wywołuje metody serwera udostępniane, jako zdalne interfejsy EJB (wywołania RMI – Remote Method Invocation). Komunikacja jest zabezpieczona przez protokół SSL. Ten typ komunikacji jest synchroniczny. Z tego typu komunikacji korzystają wszystkie aplikacje klienckie.

### 3.5.2. Inicjowanie komunikacji przez serwer

Komunikacja asynchroniczna. Komunikaty są wysyłane za pośrednictwem protokołu TCP. Aby taka komunikacja mogła nastąpić, podczas uruchomienia aplikacji klienta i logowania się do systemu aplikacja klienta musi wysłać na serwer swój adres IP i numer portu, na którym będzie nasłuchiwać komunikatów serwera. Serwer powiązuje te dane z identyfikatorem użytkownika i w dalszej komunikacji przesyła komunikaty na podany adres. Komunikacja ta również jest szyfrowana za pomocą protokołu SSL.

### 3.5.3. Forma komunikatu

Z serwera przesyłane są krótkie wiadomości. Komunikatami są obiekty Javy zserializowane do postaci tablicy bajtów. Aplikacja klienta otrzymując taką tablicę deserializuje je do obiektów javy, a następnie wywołuje odpowiednią metodę do obsługi takiego komunikatu.

**3.5.4. Rodzaje komunikatów i sytuacje, w których serwer je wysyła**

Zdarzenia:

* **Komunikat o nowym zdarzeniu** – krótki komunikat zawierający identyfikator zdarzenia oraz skróconą informację o zdarzeniu: lokalizację, kategorię oraz priorytet. Obsługa takiego komunikatu sprowadza się do konieczności pobrania zdarzenia z serwera i wyświetlenie go na liście zdarzeń.
* **Zmiana danych zdarzenia** – komunikat zawierający identyfikator zdarzenia oraz mapę klucz-wartość z listą zmian w zdarzeniu. Obsługa komunikatu sprowadza się do aktualizacji wybranego zdarzenia na liście.
* **Zgłoszenie do zadysponowania** – komunikat informacyjny o konieczności wyświetlenia   
  (i pobrania – jeśli użytkownik nie posiada zgłoszenia na swojej liście) powiadomienia   
  o zgłoszeniu do zadysponowania.
* **Nowa KZW do Zdarzenia** – komunikat zawierający informację o nowej KZW dla zdarzenia – w komunikacie znajduje się id zdarzenia oraz id nowej KZW dla ZRM.
* **Aktualizacja statusu ZRM**.
* **Zmiana danych ZRM**.

KZW:

* **Aktualizacja danych KZW** – komunikat zawierający listę zmian dla KZW o podanym id.

## 3.6. Architektura bazy danych

W ramach jednego ośrodka krajowego bazy danych są podzielone na:

* **Bazę operacyjną** – odpowiedzialną za przechowywanie danych operacyjnych (danych zdarzeń/ zleceń; statusów, pozycji i stanów pojazdów; danych użytkowników, itp.).
* **Bazę historyczno – raportową** – odpowiedzialną za przechowywanie danych historycznych Systemu, a w szczególności dokumentacji medycznej (przez okres 20 lat) oraz zarchiwizowanych statusów, pozycji i stanów pojazdów (przez okres 2 lat).

**3.6.1. Synchronizacja operacyjnej bazy danych między ośrodkami krajowymi**

Synchronizacja pomiędzy bazami danych w POK i ZOK jest zapewniona przez wtyczkę MySQL obsługującą dwustronną replikację semi-synchroniczną. Dane zapisywane w bazie danych POK są powielane za pomocą tego mechanizmu do bazy w ZOK i na odwrót: dane zapisywane w bazie danych ZOK są powielane do bazy w POK.

Jeśli połączenie pomiędzy ośrodkami krajowymi działa poprawnie, każda transakcja bazodanowa jest wykonywana synchronicznie w obydwu bazach danych w sposób opisany poniżej. Dzięki temu każda pojedyncza operacja dla aplikacji klienckich może być realizowana zarówno przez POK jak i przez ZOK. W szczególności aplikacja kliencka (na przykład Moduł dyspozytora) może wykonywać operacje   
z serwerem naprzemiennie – raz korzystając z POK, raz z ZOK.

Sposób pracy w trybie synchronicznym:

* Zapytanie z aplikacji klienckiej (np. Modułu dyspozytora) trafia do ośrodka krajowego A (POK lub ZOK).
* Serwer aplikacyjny w ośrodku A obsługuje zapytanie, w wyniku którego powstaje transakcja zapisu do bazy danych.
* Baza danych w ośrodku A wykonuje transakcję zapisu w następujący sposób:
  + 1. Transakcja jest wykonywana w ośrodku A,
    2. Polecenie wykonania transakcji jest wysyłane do ośrodka B,
    3. Ośrodek B zapisuje transakcję do logu bazy danych na dysku,
    4. Po potwierdzeniu wykonania powyższych operacji w ośrodku A i w ośrodku B transakcja kończy się. Mamy pewność, że dane są spójne w bazach ośrodka A i B.

Dzięki podwójnemu wykorzystaniu mechanizmu replikacji semisynchronicznej, synchronizacja między ośrodkami POK i ZOK przebiega w dwu kierunkach jednocześnie:

* POK aktywny (master) → ZOK pasywny (slave).
* ZOK aktywny (master) → POK pasywny (slave), dzięki czemu osiągnięto cel: obydwa ośrodki działające jako „aktywny – aktywny” w trybie synchronicznym.

Część aplikacji klienckich korzysta z Podstawowego Ośrodka Krajowego (POK), a część z Zapasowego Ośrodka Krajowego (ZOK), co jest zapisane w konfiguracji poszczególnych aplikacji (dla części aplikacji podstawowym ośrodkiem jest POK a zapasowym ZOK, dla pozostałej części aplikacji podstawowym ośrodkiem jest ZOK a zapasowym POK). Każda z aplikacji monitoruje na bieżąco dostępność ośrodków. W przypadku awarii ośrodka aplikacja kliencka automatycznie przełączy się do drugiego (ustawionego   
w konfiguracji jako zapasowy). Po wykryciu dostępności podstawowego ośrodka, aplikacja automatycznie przełączy się do ośrodka podstawowego. Dzięki temu w warunkach normalnej pracy, gdy w obydwu ośrodkach są dostępne wszystkie usługi, obciążenie POK i ZOK jest równoważone. Mechanizm równoważenia obciążenia POK i ZOK zapewnia System, co jest niezauważalne dla końcowego użytkownika.

Zgodnie z twierdzeniem Erica Brewera o CAP (Consistency, Availability, Partition),

rozproszony system baz danych nie może jednocześnie zapewniać:

* spójności (C – consistency),
* dostępności (A – availability),
* odporności na podziały (P – partition).

Jednocześnie można zapewnić tylko dwie spośród trzech powyższych cech.

Architektura systemu SWD PRM zapewni dostępność (A) i odporność na podziały (P):

* System pozostaje dostępny i w pełni funkcjonalny w przypadku awarii jednego z ośrodków.
* System pozostaje dostępny i w pełni funkcjonalny w przypadku awarii łączności pomiędzy ośrodkami.

System SWD PRM nie może zapewnić spójności danych w całym systemie w tym samym momencie.   
W praktyce jednak ta spójność jest zapewniana w czasie ułamków sekund a w przypadku wystąpienia awarii zostanie zapewniona po jej usunięciu.

Jednocześnie system zapewni całkowitą spójność z punktu widzenia użytkowników pracujących w tym samym ośrodku (województwie).

**3.6.2. Mechanizm fail-over serwera operacyjnej bazy danych**

W celu zapewnienia niezawodności mechanizmu operacyjnej bazy danych, zastosowano mechanizm fail-over, którego zasadę działania pokazują rysunki umieszczone poniżej.

W każdym OK znajdują się dwie maszyny fizyczne z zainstalowanym oprogramowaniem wirtualizatora. Serwery fizyczne podłączone są do wspólnej macierzy dyskowej, na której przechowywane są dyski należące do maszyn wirtualnych.

Maszyny fizyczne tworzą klaster niezawodnościowy. Maszyny wirtualne mogą być uruchamiane na dowolnym serwerze w klastrze.

W każdym OK na klastrze wirtualizacyjnym uruchomiona jest jedna maszyna wirtualna z kopią bazy operacyjnej.

W momencie awarii maszyny fizycznej lub uruchomionej na niej maszyny wirtualnej w ramach jednego ośrodka krajowego, druga maszyna fizyczna w klastrze przejmie obsługę maszyny wirtualnej.

Mechanizm ten jest niezależny od mechanizmu synchronizacji baz danych między POK a ZOK.

Typowa sytuacja pracy ośrodków krajowych jest przedstawiona na poniższym rysunku.

**POK**

**Macierz POK**

SAN

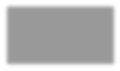


Dane POK

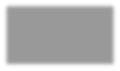
**Serwer fizyczny #1**

**Serwer fizyczny #2**

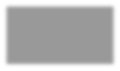
SAN



Jboss operacyjny 1

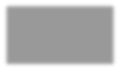


Jboss operacyjny N



Jboss operacyjny 2

LAN



MySQL operacyjny

POK

~~LAN~~

LAN

**ZOK**

**Macierz ZOK**

SAN

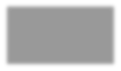


Dane ZOK

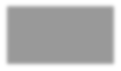
**Serwer fizyczny #1**

**Serwer fizyczny #2**

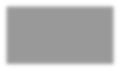
SAN



Jboss operacyjny 1

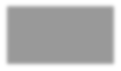


Jboss operacyjny N



Jboss operacyjny 2

LAN



MySQL operacyjny

ZOK

LAN

LAN

Synchronizacja

bazy danych

*Rysunek nr 7. Fail-over operacyjnej bazy danych. Przypadek 1.*

Na kolejnym rysunku przedstawiona jest sytuacja po awarii maszyny fizycznej, na której uruchomiona była maszyna wirtualna z operacyjną bazą danych. Obsługę tej maszyny przejęła maszyna rezerwowa.

Podczas przełączania maszyn, baza danych w ośrodku krajowym jest niedostępna, co powoduje również niedostępność serwera aplikacyjnego w tym ośrodku z punktu widzenia aplikacji klienckich. Przez ten czas usługi związane z operacyjną obsługą zgłoszeń/zdarzeń przejmuje drugi ośrodek krajowy. Przełączenia usług pozostają bez wpływu na pracę użytkowników.

**POK**

**Macierz POK**

SAN

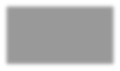


Dane POK

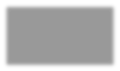
**Serwer fizyczny #1**

**Serwer fizyczny #2**

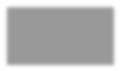
SAN



Jboss operacyjny 1

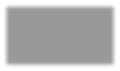


Jboss operacyjny N



Jboss operacyjny 2

LAN



MySQL operacyjny

POK

LAN

LAN

**ZOK**

**Macierz ZOK**

SAN

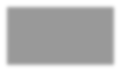


Dane ZOK

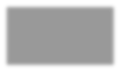
**Serwer fizyczny #1**

**Serwer fizyczny #2**

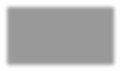
SAN



Jboss operacyjny 1

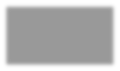


Jboss operacyjny N



Jboss operacyjny 2

LAN



MySQL operacyjny

ZOK

~~LAN~~

LAN

Synchronizacja

bazy danych

*Rysunek nr 8. Fail-over operacyjnej bazy danych. Przypadek 2.*

**3.6.3. Mechanizm fail-over połączenia sieciowego POK-ZOK**

Sytuacja utraty połączenia sieciowego POK-ZOK zostaje wykryta w przypadku braku możliwości wykonania transakcji na bazie danych w sposób synchroniczny – po przekroczeniu czasu odpowiedzi drugiego serwera.

Połączenie sieciowe POK-ZOK jest realizowane przez sieć OST 112. W przypadku awarii łącza dedykowanego dla połączenia POK-ZOK, wykorzystywane są inne łącza sieci OST 112. Zatem sytuacja, w której przerwana zostanie komunikacja POK-ZOK, a ośrodki krajowe będą mogły mimo to komunikować się ze stacjami klienckimi jest niezwykle mała prawdopodobna. Bardziej prawdopodobna jest całkowita niedostępność jednego ośrodka krajowego, która może wystąpić z wielu powodów.

W przypadku zerwania połączenia sieciowego POK-ZOK i braku możliwości przesyłania danych pomiędzy ośrodkami, replikacja semisynchroniczna przełączy się na tryb asynchroniczny. Bazy danych w POK i ZOK będą pracować niezależnie, a po odzyskaniu łączności dane zsynchronizują się. Po automatycznym „nadrobieniu” synchronizacji, replikacja ponownie wróci do trybu synchronicznego.

Poleganie na tym automatycznym mechanizmie jest zalecane tylko w przypadku krótkotrwałej awarii połączenia sieciowego – do 15 minut. W przypadku wykrycia długotrwałej awarii połączenia sieciowego zalecane jest wyłączenie serwerów aplikacyjnych JBOSS w ZOK – tak, aby wszystkie aplikacje klienckie SWDPRM pracowały tylko z POK.

### 3.6.4. ETL – Extract, Transform and Load

Mechanizm ETL służy do przenoszenia danych z bazy operacyjnej do bazy historycznoraportowej. Baza danych historyczno–raportowa zasilana jest na bieżąco poprzez jeden z równoległych procesów ETL uruchomionych na każdym serwerze operacyjnym w każdym z OK (czas kolejnych uruchomień procesu ETL jest konfigurowany podczas instalacji i domyślnie wynosi 1h). Każdy z procesów ETL pracuje na pojedynczej maszynie wirtualnej.

W przypadku awarii maszyny wirtualnej lub pojedynczego procesu ETL jego rolę przejmują pozostałe procesy ETL uruchomione w ramach tego samego OK. Po ponownym uruchomieniu uszkodzonego procesu ETL jest on automatycznie włączany do puli równolegle działających procesów. Po usunięciu awarii maszyny wirtualnej staje się ona automatycznie dostępna.

Dzięki bieżącemu zasilaniu bazy historyczno - raportowej danymi, dane te są aktualne z dokładnością do częstotliwości automatycznego uruchamiania procesu ETL. Oznacza to, że baza historyczna posiada dane sprzed najwyżej 1h (w przypadku standardowych ustawień interwału uruchamiania procesu ETL). Proces ETL jest odpowiedzialny również za usuwanie z bazy operacyjnej danych starszych niż 60 dni.   
W praktyce oznacza to, że po zakończeniu przenoszenia danych przez proces ETL dane w bazie operacyjnej i najnowsze dane w bazie historycznej są tożsame dla okresu wynoszącego 60 dni.

Szczegółowe informacje na temat logicznej budowy systemu zostały zawarte w Załączniku nr 1 do OPZ. Znajduje się tam szczegółowy opis dotyczący poszczególnych środowisk, systemów zewnętrznych,   
z którymi integruje się System oraz logicznych powiązań pomiędzy poszczególnymi komponentami.

### 3.6.5. Lokalna baza danych

Lokalna baza danych wykorzystywana jest w modułach: Dyspozytora, Mobilnym ZRM i Stacjonarnym ZRM. Użyto silnika bazy: H2, który umożliwia szyfrowanie bazy. Przy czym szyfrowana jest jedynie baza w Module Mobilnym ZRM. Wszelkie zmiany w obiektach danych (szczegóły zdarzenia, szczegóły KZW, statusy ZRM – Dyspozytor, KZW, KMCR, statusy ZRM – moduły ZRM) zapisywane są w lokalnej bazie danych w postaci zserializowanych obiektów, niezależnie od trybu pracy (off-line lub on-line).   
W przypadku pracy on-line, dane z lokalnej bazy danych są natychmiast wysyłane na serwer,   
a w przypadku pracy off-line, dane są gromadzone aż do momentu odzyskania połączenia z serwerem. Po odzyskaniu połączenia z serwerem obiekty z lokalnej bazy danych są wysyłane na serwer, który dokonuje połączenia wersji lokalnych z istniejącymi już na serwerze innymi wersjami danego obiektu.

Uwaga: zmiany zapisywane lokalnie nie są widoczne w historii dla użytkowników Systemu do momentu synchronizacji z serwerem po odzyskaniu połączenia.

## 3.7. Bezpieczeństwo

W celu dokładnego wyjaśnienia sposobu zapewnienia bezpieczeństwa w Systemie SWD PRM, poniżej opisane zostaną procesy:

* Uwierzytelniania i autoryzacji użytkowników,
* Zabezpieczenie komunikacji wewnętrznej między modułami Systemu oraz systemami zewnętrznymi,
* Sposobu wykorzystania certyfikatów aplikacji oraz użytkowników Systemu.

**3.7.1. Dane użytkowników**

Dane uwierzytelniające użytkowników są przechowywane na serwerze usługi katalogowej LDAP. Struktura danych na serwerze zawiera – oprócz danych użytkowników – listę uprawnień atomowych, pogrupowanych w role, aby można było łatwo zarządzać takimi uprawnieniami i nadawać je użytkownikom. Podczas każdej funkcji wywoływanej przez użytkownika, jest uruchamiana metoda sprawdzająca, czy użytkownik ma uprawnienia do danej części systemu. Dodatkowo na serwerze usługi katalogowej przechowywane będą informacje wiążące użytkownika z jego certyfikatem oraz informacje o stanowiskach dostępowych. Procedura uwierzytelniania stanowisk dostępowych oraz użytkowników została opisana w dalszej części tego rozdziału.

### 3.7.2. Certyfikaty

Certyfikaty wykorzystywane przez użytkowników są generowane przez centrum certyfikacji PKI.   
W przypadku próby podpisu dokumentów bądź uwierzytelnienia certyfikatem wystawionym przez inne centrum certyfikacji aplikacja zwróci błąd weryfikacji podpisu, minimalizując ryzyko nieautoryzowanego dostępu do aplikacji.

Proces logowania do poszczególnych aplikacji systemu został opisany poniżej.

### 3.7.3. Uwierzytelnianie i autoryzacja aplikacji Dyspozytora

Poniżej opisany został proces uwierzytelniania Aplikacji Dyspozytora z punktu widzenia uwierzytelniania Stanowiska Dostępowego oraz Użytkownika. Do aplikacji dyspozytora użytkownik może się zalogować za pomocą karty mikroprocesorowej lub w przypadku jej braku za pomocą loginu i hasła (tzw. Tryb warunkowy). Po zalogowaniu użytkownika do systemu jest zwrócona informacja o uprawnieniach użytkownika do części systemu. Podczas każdej czynności wykonywanej przez użytkownika aplikacja sprawdza, czy użytkownik posiada odpowiednie uprawnienia do wykonania danej czynności.

**3.7.3.1. Uwierzytelnianie Stanowiska Dostępowego**

Aby ograniczyć dostęp do danych przez aplikacje nieuwierzytelnione oraz móc zarządzać aktywnymi stanowiskami dostępowymi, aplikacja dyspozytorska w momencie uruchomienia musi uwierzytelnić się na serwerze aplikacji. Uwierzytelnienie polega na wysłaniu do serwera informacji o stanowisku   
z wykorzystaniem certyfikatu znajdującego się w każdej aplikacji dyspozytorskiej. Serwer certyfikacji weryfikuje certyfikat stanowiska na podstawie danych przechowywanych w PKI, a następnie zezwala na zalogowanie się użytkownika do aplikacji bądź informuje o błędzie.

**Wymagania początkowe:** Na każdym stanowisku dostępowym znajduje się certyfikat przechowywany w zaszyfrowanym pliku .keystore (kontener certyfikatów języka JAVA).

Klucz publiczny tego certyfikatu znajduje się na serwerze aplikacji w celu uwierzytelnienia stanowiska.

**Scenariusz uwierzytelnienia:**

1. Aplikacja zostaje uruchomiona.
2. Zostaje wysłane żądanie uwierzytelnienia do serwera aplikacji, żądanie zawiera certyfikat aplikacji.
3. Serwer aplikacji sprawdza, czy posiada certyfikat zawarty w żądaniu:
   1. Jeśli NIE, to zwraca komunikat o błędzie („Nieprawidłowy certyfikat”) -> STOP
   2. Jeśli TAK, następuje przejście do kroku 4.
4. Serwer aplikacji weryfikuje prawidłowość i ważność certyfikatu poprzez wywołania metody/usługi weryfikacji certyfikatu w module PKI:
   1. Jeśli weryfikacja przebiegła pomyślnie, serwer zwraca do aplikacji informację   
      o pozytywnym wyniku uwierzytelnienia, aplikacja jest gotowa do działania.
   2. Jeśli weryfikacja zwróciła błędy, serwer wysyła do aplikacji listę komunikatów o błędach weryfikacji (np. Certyfikat wygasł, Wystawca certyfikatu nie jest zaufany, itp.) -> STOP.

**3.7.3.2. Uwierzytelnianie Użytkownika**

Uwierzytelnienie użytkownika aplikacji dyspozytorskiej polega na wysłaniu do serwera aplikacji żądania logowania. Komunikat żądania musi być podpisany przez użytkownika za pomocą osobistego certyfikatu. Serwer aplikacji w momencie otrzymania żądania weryfikuje podpis oraz wykonuje pozostałe czynności identyfikacyjne. W przypadku poprawnego uwierzytelnienia zostaje wygenerowany identyfikator sesji użytkownika, który następnie zostaje zwrócony aplikacji dyspozytorskiej razem z informacją   
o poprawnym zalogowaniu użytkownika do systemu.

**Wymagania początkowe:** Aplikacja dyspozytorska została uruchomiona oraz jest gotowa do działania. Użytkownik umieścił swoją kartę z certyfikatem w czytniku kart mikroprocesorowych.

**Scenariusz uwierzytelnienia**

1. Użytkownik klika w przycisk „Logowanie za pomocą certyfikatu”.
2. Aplikacja prosi o podanie hasła dostępu do certyfikatu (PIN).
3. Po podaniu hasła aplikacja uzyskuje dostęp do certyfikatu i wysyła podpisane żądanie do serwera aplikacji.
4. Serwer aplikacji sprawdza podpis cyfrowy dołączony do żądania a następnie wysyła żądanie uwierzytelniania do serwera usługi katalogowej:
   1. Jeśli domena zwróci błąd logowania zostaje zwrócony komunikat o błędzie -> STOP
   2. Jeśli domena zwróci pozytywny wynik uwierzytelnienia następuje przejście do kroku 5.
5. Serwer aplikacji weryfikuje prawidłowość i ważność certyfikatu poprzez wywołania metody/usługi weryfikacji certyfikatu w module PKI:
   1. Jeśli weryfikacja przebiegła pomyślnie serwer zwraca do aplikacji informację   
      o pozytywnym wyniku uwierzytelnienia, użytkownik został zalogowany do systemu.
6. Jeśli weryfikacja zwróciła błędy, serwer wysyła do aplikacji listę komunikatów o błędach weryfikacji (np. Certyfikat wygasł, Wystawca certyfikatu nie jest zaufany itp.) -> Użytkownik nie został zalogowany do systemu.

**Scenariusz alternatywny - Dyspozytor tymczasowo nie posiada karty mikroprocesorowej.**

W takim przypadku użytkownik może zalogować się za pomocą loginu i hasła. Jednak aplikacja po zalogowaniu przejdzie w tzw. Tryb warunkowy. W tym trybie dyspozytor może wykonywać wszystkie czynności (podobnie jak za pomocą karty mikroprocesorowej). Jedyną różnicą jest brak certyfikatu osobistego, przez co wszystkie czynności wymagające podpisu elektronicznego zostają zapisane na serwerze z informacją o konieczności podpisania certyfikatem danego użytkownika. Przy kolejnym zalogowaniu użytkownika do aplikacji SWD PRM za pomocą karty mikroprocesorowej wyświetli się lista dokumentów wymagających podpisu.

W trybie warunkowym aplikacja nie blokuje możliwości wydruku Księgi Dysponenta.

Scenariusz uwierzytelniania za pomocą loginu i hasła został opisany w pkt 3.7.6. W Systemie zastosowano model logowania się użytkowników za pomocą loginu i hasła.

**3.7.4. Uwierzytelnianie i autoryzacja aplikacji desktopowej ZRM**

Logowanie do aplikacji desktopowej ZRM może zostać zrealizowane na dwa sposoby:

* Logowanie za pomocą karty mikroprocesorowej;
* Logowanie na użytkownika „ogólnego” – w przypadku, gdy kilka ZRM pracuje na jednym stanowisku dostępowym.

Mechanizm logowania za pomocą karty mikroprocesorowej wygląda identycznie jak w przypadku aplikacji dyspozytora.

Natomiast logowanie na użytkownika „ogólnego” ma zastosowanie w momencie, w którym na jednym stanowisku dostępowym musi pracować kilka ZRM. Scenariusz czynności związanych   
z uwierzytelnieniem kolejnych użytkowników aplikacji wygląda następująco:

**Scenariusz uwierzytelnienia**

1. Użytkownik klika w przycisk „Logowanie – użytkownik ogólny”.
2. Aplikacja wyświetla listę ZRM (wg grafiku), które mają pracować na tym stanowisku.
3. Użytkownicy kolejnych ZRM zgłaszają obecność oraz gotowość zespołu poprzez kliknięcie na przycisk „Zgłoś obecność” oraz włożenie swojej karty z certyfikatem do czytnika lub podaniem loginu i hasła.

Użytkownicy mogą uzupełniać swoje dokumenty oraz drukować karty zlecenia wyjazdu, a także odbierać zlecenia wyjazdu. Aby praca na jednym stanowisku dostępowym przez kilku użytkowników była bezpieczna i funkcjonalna jest wprowadzona funkcjonalność „Użytkownika aktywnego”. Wyciągnięcie karty mikroprocesorowej z czytnika w MS ZRM nie powoduje wylogowania użytkownika.

1. Użytkownik chcący uzupełniać dokumentację medyczną klika na przycisk „Przejdź do trybu aktywnego” – przejście do trybu aktywnego następuje po podaniu loginu i hasła użytkownika lub włożenia karty mikroprocesorowej do czytnika.
2. Po przejściu do trybu aktywnego użytkownik otrzymuje dostęp do swoich dokumentów oraz zleceń, które może uzupełniać oraz wysyłać na serwer.
3. W tym samym czasie w momencie nadejścia zlecenia wyjazdu dla ZRM pojawia się okno dialogowe blokując tymczasowo czynności użytkownika aktywnego. Odebranie zlecenia może odbyć się na dwa sposoby:
   1. Jeżeli zlecenie wyjazdu należy do ZRM, do którego należy użytkownik znajdujący się   
      w trybie aktywnym – odebranie zlecenia odbywa się za pomocą przycisku „Przyjmij”   
      i wykonaniu dodatkowych czynności, takich jak wydrukowanie karty zlecenia wyjazdu oraz dokumentacji medycznej pacjenta.

Czynności wykonywane dotychczas przez użytkownika zostają zapisane lokalnie,   
a użytkownik po zakończeniu obsługi zlecenia na stanowisku dostępowym (Wysłanie do serwera statusu oznaczającego wyjazd do zdarzenia) zostaje wylogowany z trybu aktywnego.

* 1. Jeżeli zlecenie wyjazdu należy do innego ZRM – odebranie zlecenia odbywa się za pomocą przycisku „Przyjmij” oraz podania loginu i hasła użytkownika lub włożenia karty   
     z certyfikatem użytkownika danego ZRM. Użytkownik ten tymczasowo przechodzi w tryb użytkownika aktywnego na czas obsługi przychodzącego zlecenia – dzięki temu może wydrukować niezbędne dokumenty oraz ustawić odpowiednie statusy. Po zakończeniu obsługi zlecenia na stanowisku dostępowym (Wysłanie do serwera statusu oznaczającego wyjazd do zdarzenia) zostaje wylogowany z trybu aktywnego. Tryb aktywny powraca do użytkownika będącego w trybie aktywnym przed przyjściem zlecenia wyjazdu.

### 3.7.5. Uwierzytelnianie i autoryzacja aplikacji mobilnej ZRM

W przypadku aplikacji mobilnej uwierzytelnienie odbywa się za pomocą loginu i hasła. Ponieważ niemożliwe jest użycie kart mikroprocesorowych, w aplikacji mobilnej nie ma możliwości podpisania dokumentów wymagających podpisu cyfrowego certyfikatem użytkownika. Z tego względu wszystkie tego typu dokumenty będą wymagały podpisu certyfikatem przez użytkownika w aplikacji desktopowej ZRM.

W aplikacji mobilnej ZRM na tablecie (z założenia bez użycia karty mikroprocesorowej) jest możliwe utworzenie Karty medycznych czynności ratunkowych, wypełnienie jej i wydrukowanie. Możliwe jest również uzupełnienie i wydrukowanie Karty zlecenia wyjazdu.

**3.7.6. Uwierzytelnianie za pomocą loginu i hasła**

W przypadku logowania za pomocą loginu i hasła proces jest dwuetapowy. W pierwszym etapie aplikacja wysyła żądanie do serwera o unikalny identyfikator, który w późniejszym etapie służy do zaszyfrowania hasła użytkownika, dzięki czemu hasło nie jest przesyłane do serwera w postaci jawnej.

Poniżej znajduje się scenariusz uwierzytelniania do aplikacji ZRM za pomocą loginu i hasła.

**Wymagania początkowe:** Aplikacja ZRM została uruchomiona oraz jest gotowa do działania. Użytkownik znajduje się na formatce logowania za pomocą loginu i hasła. **Scenariusz uwierzytelnienia**

1. Użytkownik podaje swój login i hasło.
2. Aplikacja wysyła żądanie logowania do serwera. Hasło zostaje zaszyfrowane kluczem publicznym.
3. Serwer aplikacji wykonuje kolejno:
   * 1. Deszyfruje hasło użytkownika kluczem prywatnym,
     2. Wysyła do serwera usługi katalogowej żądanie uwierzytelnienia podając login i hasło użytkownika. Logowanie odbywa się z wykorzystaniem SASL (Simple Authentication and Security Layer) w celu zabezpieczenia danych logowania.
4. Po sprawdzeniu czynności zawartych w pkt. 3:
   * 1. Jeśli weryfikacja przebiegła pomyślnie serwer wygeneruje identyfikator sesji użytkownika a następnie zwróci go do aplikacji wraz z pozytywnym wynikiem uwierzytelnienia, użytkownik został zalogowany do systemu.
     2. W przypadku, gdy którykolwiek z elementów zawartych w pkt. 3 zakończy się błędem, serwer zwróci informację o błędzie logowania -> Użytkownik nie został zalogowany do systemu.

**3.7.7. Uwierzytelnianie i autoryzacja aplikacji w trybie off-line**

W przypadku utraty połączenia z serwerem dla aplikacji dyspozytorskiej oraz aplikacji mobilnej jest możliwość pracy w trybie off-line. Podczas utraty połączenia przy obsłudze zgłoszenia użytkownik pozostaje cały czas zalogowany, dzięki czemu aplikacja zezwala na wykonanie czynności opisanych w odnośnych wymaganiach. W przypadku konieczności zalogowania się do aplikacji mobilnej bądź desktopowej ZRM użytkownicy logują się na konto ogólne.

## 3.8. Poufność

Niniejszy rozdział opisuje środki i metody zapewnienia poufności danych i transmisji w systemie SWD PRM.

**3.8.1. Poufność transmisji danych**

W celu zapewnienia poufności, komunikacja pomiędzy SWD PRM a zewnętrznymi systemami odbywa się po protokole HTTPS z wykorzystaniem certyfikatów SSL. Weryfikacja certyfikatów jest wykonywana przez mechanizmy serwera aplikacji z wykorzystaniem kontenera certyfikatów języka JAVA (Truststore), który przechowuje zaufane dla serwera aplikacji certyfikaty.

Komunikacja wewnętrznych komponentów SWD PRM wykorzystuje protokoły zabezpieczone certyfikatami SSL (w zależności od sposobu komunikacji może to być STOMP, AMQP bądź

HTTPS). Transmisja danych jest szyfrowana z użyciem klucza symetrycznego o długości 256 bitów   
(256-Bit SSL).

Dodatkowym gwarantem poufności transmisji danych jest praca wszystkich komponentów systemu   
w otoczeniu sieci OST112.

**3.8.2. Poufność dostępu do nośników danych**

Ze względu na fakt, iż tablety ZRM będą znajdować się poza fizycznym obszarem przetwarzania danych (zgodnie z § 4 pkt 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U z 2004 r., Nr.100, poz.1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych), a ponadto mogą w przypadku pracy w trybie off-line przechowywać na wewnętrznym nośniku danych dane osobowe oraz dane wrażliwe, lokalna baza danych aplikacji mobilnej jest szyfrowana, aby w przypadku dostania się urządzenia mobilnego   
w niepowołane ręce, niemożliwy był odczyt danych znajdujących się na nośniku danych.

Dane gromadzone lokalnie na stanowiskach dostępowych Dyspozytora i ZRM nie są szyfrowane, a ich poufność jest zagwarantowana na poziomie procedur i zabezpieczeń organizacyjnych opisanych   
w Polityce Bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

## 3.9. Integralność

Integralność danych Systemu SWD PRM należy rozpatrywać w dwóch aspektach:

* Integralność danych zapisanych na nośnikach danych.
  1. Zabezpieczenie przed utratą wynikającą z uszkodzenia nośnika danych,
  2. Zabezpieczenie przed rozmyślnym, nieautoryzowanym zniszczeniem lub zmianą danych.
* Integralność danych w procesie przesyłania ich między węzłami Systemu oraz między Systemem a systemami zewnętrznymi.
  + 1. **Integralność danych zapisanych na nośnikach danych**

Integralność wszelkich danych zapisywanych na nośnikach danych w ramach OK jest zapewniona dzięki wykorzystaniu macierzy dyskowych skonfigurowanych w odpowiednie poziomy Integralność danych pomiędzy ośrodkami zapewnia mechanizm replikacji operacyjnej bazy danych opisany. Integralność danych znajdujących się na SD oraz TM (w szczególności w momencie pracy off-line) może nie zostać zapewniona, ze względu na fakt, iż zarówno SD jak i TM, dostarczane przez Zamawiającego, wyposażone są w jeden dysk twardy co powoduje zwiększoną podatność SD i TM na utratę danych, wynikającą   
z uszkodzenia fizycznego nośnika danych w tych urządzeniach.

System SWD PRM odporny jest na rozmyślne, nieautoryzowane zniszczenie lub zamianę danych zgodnie.

* + 1. **Integralność danych w procesie przesyłania danych**

Integralność danych podczas przesyłania ich między węzłami Systemu zapewniona jest poprzez zabezpieczenie transmisji z użyciem klucza symetrycznego o długości 256 bitów. W przypadku komunikacji pomiędzy SWD PRM a systemami zewnętrznymi transmisja jest zabezpieczona zgodnie   
z zastosowanymi protokołami systemów zewnętrznych, jednak o poziomie nie mniejszym niż   
z wykorzystaniem protokołu TLS o długości klucza 128 bit.

## 3.10. Rozliczalność

Wszystkie operacje wykonywane przez Użytkownika, które trafiają do bazy danych, są automatycznie skojarzone z jego identyfikatorem i tak zapisane. Raz zapisana w bazie danych informacja nie jest już modyfikowana, a każda zmiana pojawi się jako nowy rekord w bazie danych.

Działania administratorów biznesowych (dodanie, dezaktywowanie, modyfikacja uprawnień użytkownika) są zapisywane w bazie danych.

Działania administratorów Systemu są logowane za pomocą mechanizmu SYSLOG.

## 3.11. Niezaprzeczalność

Właściwość niezaprzeczalności zrealizowana jest poprzez dołączanie do każdej czynności wykonywanej przez użytkownika unikalnego identyfikatora użytkownika oraz identyfikatora sesji użytkownika otrzymanego podczas zalogowania do systemu. Raz nadany identyfikator użytkownika nie może być wykorzystany po raz drugi i przypisany innemu użytkownikowi. Dzięki zapisywaniu identyfikatora użytkownika oraz identyfikatora sesji, każda operacja jest jednoznacznie powiązana z użytkownikiem.

Wszystkie operacje wykonywane przez Użytkownika, które trafiają do bazy danych, są automatycznie skojarzone z jego identyfikatorem i tak zapisane. Raz zapisana w bazie danych informacja nie jest już modyfikowana, a każda zmiana pojawi się jako nowy rekord w bazie danych.

Ze względu na konieczność zapewnienia maksymalnej szybkości działania Systemu, po poprawnym zautoryzowaniu się użytkownika w Systemie operacje zapisywane do bazy danych nie są podpisywane osobistym certyfikatem.

Wyjątkiem są pewne dokumenty, które wymagają podpisu użytkownika przed wysłaniem do serwera –   
w szczególności mowa tutaj o dokumentacji medycznej pacjenta. W tym przypadku należy wykorzystać certyfikat użytkownika. Dotyczy to operacji:

1. zamknięcia karty medycznych czynności ratunkowych;
2. modyfikacji danych (uzupełnienia) zamkniętej wcześniej karty medycznych czynności ratunkowych.

W powyższych przypadkach realizowany jest następujący scenariusz postępowania:

1. Użytkownik posiada dokument gotowy do wysłania, klika na przycisk „podpisz i wyślij” (przykładowo);
2. Aplikacja prosi o podanie hasła do certyfikatu.
3. Po wpisaniu hasła dokument zostaje podpisany oraz wysłany do serwera.

## 3.12. Ciągłość działania

W poniższym rozdziale zostaną przedstawione istotne przypadki awarii komponentów Systemu lub usług z uwzględnieniem sposobu przejęcia poszczególnych funkcji przez inne komponenty nadmiarowe. Przedstawione zostaną również podstawowe scenariusze powrotu do normalnych warunków pracy po przywróceniu działania tych komponentów.

**3.12.1. Utrata połączenia POK – ZOK**

System umożliwia bezprzerwową pracę w wypadku utraty połączenia POK-ZOK. Pracę operacyjną   
w takim przypadku przejmuje w całości ośrodek podstawowy (POK). W przypadku wykrycia braku połączenia pomiędzy POK a ZOK, ZOK oznaczany jest jako niedostępny.

Aplikacje klienckie cyklicznie odpytują o dostępność ośrodków krajowych i w przypadku wystąpienia braku połączenia (pomiędzy ośrodkami krajowymi) aplikacje klienckie podłączone do ZOK przełączają się na POK. Po odzyskaniu połączenia pomiędzy ośrodkami i zsynchronizowaniu baz danych ośrodek ZOK jest oznaczany jako dostępny i aplikacje klienckie, które domyślnie korzystają z ZOK przełączają się z powrotem na ten ośrodek.

W szczególności z POK komunikują się w pierwszej kolejności systemy zewnętrzne (SI WCPR, PZŁ). Niedostępność jednego z Ośrodków Krajowych

Całkowita niedostępność Ośrodka Krajowego może zostać wywołana przez różne zdarzenia występujące oddzielnie lub łącznie. Poniżej wymienione zostały najistotniejsze z nich.

### 3.12.1.1. Utrata połączenia sieciowego od aplikacji klienckich do OK

W poniższym scenariuszu rozpatrywany jest przypadek, gdy utrata połączenia następuje w warstwie sieciowej pomiędzy routerami brzegowymi sieci OST112, a jednym z Ośrodków Krajowych. Przy tym założeniu poszczególne elementy Systemu w tym ośrodku nadal pozostają w gotowości działania, lecz są niewidoczne przez użytkowników.

Każdy z OK jest podłączony za pomocą dwóch niezależnych urządzeń – routery Cisco ASR1004– które są podłączone do niezależnych łączy w ramach sieci OST112. Awaria jednego z łączy lub pojedynczego routera nie powoduje utraty połączenia do OK.

W przypadku awarii obu łączy równocześnie lub obu urządzeń Cisco ASR 1004 aplikacja kliencka SD   
i TM, na podstawie braku odpowiedzi, stwierdzi niedostępność usług w domyślnym OK i przełączy się na ośrodek zapasowy zgodnie ze swoją konfiguracją. Każda z aplikacji klienckich posiada predefiniowane połączenia zarówno do POK jaki i ZOK, przy czym dla części z nich domyślnym OK jest ośrodek podstawowy, a dla pozostałych ośrodek zapasowy.

Ponieważ każda operacja pomiędzy aplikacją kliencką a serwerem może być wykonana zarówno w POK jak i ZOK (w każdym momencie), przełączenie na drugi ośrodek krajowy jest niezauważalne dla użytkownika końcowego. Funkcjonalność Systemu działa w pełni.

Po przywróceniu połączenia do OK elementy systemu są w stanie pozwalającym na natychmiastowe podjęcie pracy. Powrotnie przełączenie aplikacji klienckich na ośrodek domyślny nastąpi automatycznie, bez wiedzy użytkownika. Ośrodki krajowe monitorują się wzajemnie i informują stacje klienckie   
o dostępności usług w każdym z ośrodków. W szczególności po odzyskaniu połączenia sieciowego do jednego z ośrodków krajowych informacja ta jest odnotowana przez drugi ośrodek i rozpropagowana do stacji klienckich.

W przypadku szczególnym, gdy z punktu widzenia aplikacji klienckiej oba ośrodki nie są osiągalne aplikacja może przejść w tryb off-line, w celu zabezpieczenia danych zgromadzonych w aplikacji.   
W takim przypadku użytkownik jest poinformowany o braku łączności z obydwoma ośrodkami krajowymi, aby był świadom, że wprowadzane przez niego zmiany są niewidoczne dla innych użytkowników oraz że użytkownik nie dostaje bieżących informacji z Systemu.

**3.12.1.2. Fizyczna niedostępność OK**

W przypadku fizycznej niedostępności ośrodka krajowego, przy funkcjonowaniu drugiego Ośrodka Krajowego wszyscy użytkownicy są przepięci do działającego ośrodka. System może pracować w tym stanie bez ograniczeń czasowych z zachowaniem pełnej dostępności i wydajności poszczególnych usług Systemu.

Systemy zewnętrzne wysyłające komunikaty do SWD PRM (SI CPR i PZŁ) w pierwszej kolejności komunikują się z POK. W przypadku fizycznej niedostępności POK systemy te automatycznie wysyłają komunikaty do ZOK.

Przywrócenie do działania po takiej awarii wymaga podjęcia specjalnych kroków administratora technicznego centralnego. W pierwszej kolejności przywrócenia fizycznych i logicznych zasobów niedostępnego ośrodka. W drugiej kolejności konieczne jest przywrócenie baz z kopii zapasowych.   
W przypadku niedostępności ośrodka powyżej kilku dni może wystąpić konieczność wykorzystania działań niestandardowych, takich jak przywrócenie kopii zapasowej z drugiego ośrodka lub wymuszenie pełnej synchronizacji danych z ośrodka działającego do ośrodka odtwarzanego.

### 3.12.1.3. Awaria zasilania

Niedostępność ośrodka krajowego może wystąpić w przypadku całkowitej utraty zasilania w obu obwodach zasilających doprowadzonych do każdej szafy RACK w POK lub ZOK.

Urządzenia fizyczne znajdujące się w lokalizacji OK są skonfigurowane w taki sposób, że po przywróceniu zasilania włączą się samoczynnie. Maszyny wirtualne należące do wszystkich środowisk również zostaną uruchomione automatycznie.

W przypadku szczególnym, gdy na skutek nieplanowanego zamknięcia systemu wystąpi problem   
z ponownym uruchomieniem kluczowych komponentów usługi nie są przywrócone automatycznie   
i konieczna jest interwencja administratora technicznego.

**3.12.2. Awarie komponentów logicznych**

Awarie poszczególnych komponentów logicznych mają wpływ na dostępność poszczególnych usług dla klientów końcowych.

**3.12.2.1. Niedostępność usługi w OK**

Komponentem najbliższym aplikacji klienckich są load balancery, na których można sterować dostępnością serwerów aplikacyjnych, odpowiedzialnych za obsługę poszczególnych usług.   
W szczególności możliwe jest administracyjne wyłączenie całej usługi. Podobny efekt wystąpi   
w przypadku, gdy któryś z komponentów danej usługi przestanie spełniać swoją funkcję.

Wtedy, z punktu widzenia aplikacji klienckiej usługa w danym OK również nie jest dostępna. Po wykryciu takiej sytuacji, na podstawie przekroczonego czasu odpowiedzi lub na podstawie zwróconego kodu błędu, aplikacja kliencka dokona przełączenia na ośrodek zapasowy.

Powyższe scenariusze mogą wystąpić w przypadku:

* awarii bazy danych produkcyjnej, spowodowanych np. brakiem zasobów – pamięć, cpu; zatrzymaniem procesu bazy danych);
* awarii aplikacyjnych maszyn wirtualnych.

Przerwa w działaniu tych komponentów może mieć charakter przejściowy, np. związany z przełączaniem maszyny wirtualnej pomiędzy węzłami fizycznymi klastra lub długotrwały, związany z koniecznością podjęcia działania przez administratora.

Proces serwera ETL w ramach jednego OK jest na bieżąco monitorowany. W przypadku awarii procesu, analogiczny proces zostanie uruchomiony na drugiej maszynie wirtualnej i fizycznej, przejmując rolę uszkodzonego serwera ETL.

**3.12.3. Awarie komponentów fizycznych**

Poniżej przedstawiono wpływ najistotniejszych komponentów architektury fizycznej na ciągłość działania Systemu.

**3.12.3.1. Awaria węzła w klastrze PROD**

W każdej z lokalizacji OK występują dwa serwery fizyczne obsługujące klaster wirtualizacyjny dla środowiska PROD. W przypadku awarii jednego z węzłów wszystkie maszyny wirtualne wchodzące   
w skład Systemu są uruchamiane ponownie na drugim z węzłów, uruchamiane na nowo jako zasób klastra wirtualizacyjnego. Wystąpienie takiej sytuacji musi być monitorowane w celu podjęcia działań serwisowych.

### 3.12.3.2. Awaria macierzy dyskowej

Macierz dyskowa w OK jest wyposażona w redundantne zasilacze oraz kontrolery. W przypadku awarii jednego zasilacza lub kontrolera macierz funkcjonuje poprawnie bez przerywania pracy. Naprawa jest wykonywana przez zastąpienie uszkodzonego elementu w czasie pracy macierzy i nie wymaga jej zatrzymania, a co za tym idzie nie wpływa na dostępność usług Systemu w OK. Wystąpienie takiej sytuacji musi być monitorowane w celu podjęcia działań serwisowych.

Całkowita niedostępność macierzy jest możliwa wyłączenie w przypadku awarii obu kontrolerów lub wszystkich zasilaczy, co powoduje całkowite unieruchomienie wszystkich usług w danym OK.

Innym powodem niedostępności danych na macierzy może być awaria dysków twardych. Dla zmniejszenia wpływu tego ryzyka dla każdego rodzaju dysków dostępne są dyski zapasowe, tzw. Hot-spare. Po awarii dysku macierz odbudowuje konfigurację RAID z wykorzystaniem dysku Hot-spare   
w sposób niewidoczny poza macierzą. Wystąpienie takiej sytuacji musi być monitorowane w celu podjęcia działań serwisowych.

**3.12.3.3. Awaria urządzeń sieciowych**

Urządzenia sieciowe – przełączniki sieciowe, Load balancery – są w architekturze skonfigurowane jako urządzenia z nadmiarowością. W przypadku awarii jednego z nich drugi jest w stanie zapewnić połączenia sieciowe w ramach lokalizacji. Wystąpienie takiej sytuacji musi być monitorowane w celu podjęcia działań serwisowych.

W przypadku awarii naprawa wymaga wymiany urządzenia lub modułów (zasilających lub rozszerzeń). Przywrócenie działania wymaga odtworzenia konfiguracji nowego urządzenia.

**3.12.3.4. Wpływ niedostępności OK na rozmowy telefoniczne Dyspozytora**

Przełączenie aplikacji klienckiej SD pomiędzy POK i ZOK jest obsłużone przez aplikację w sposób opisany powyżej (3.12.1.1 Utrata połączenia sieciowego od aplikacji klienckich). Powyższy mechanizm nie wymusza zmiany stanu aplikacji i nie wymusza ponownego wysyłania informacji o aktualnym zgłoszeniu do terminala telefonicznego. Dodatkowo stacja kliencka SD i terminal telefoniczny pracują   
w oddzielnych podsieciach, co dodatkowo separuje i uniezależnia te urządzenia.

## 3.13. Architektura fizyczna systemu

Fizyczna część systemu jest podzielona na dwie osobne części znajdujące się w dwóch niezależnych ośrodkach – tzw. „podstawowym” – POK i „zapasowym” - ZOK.

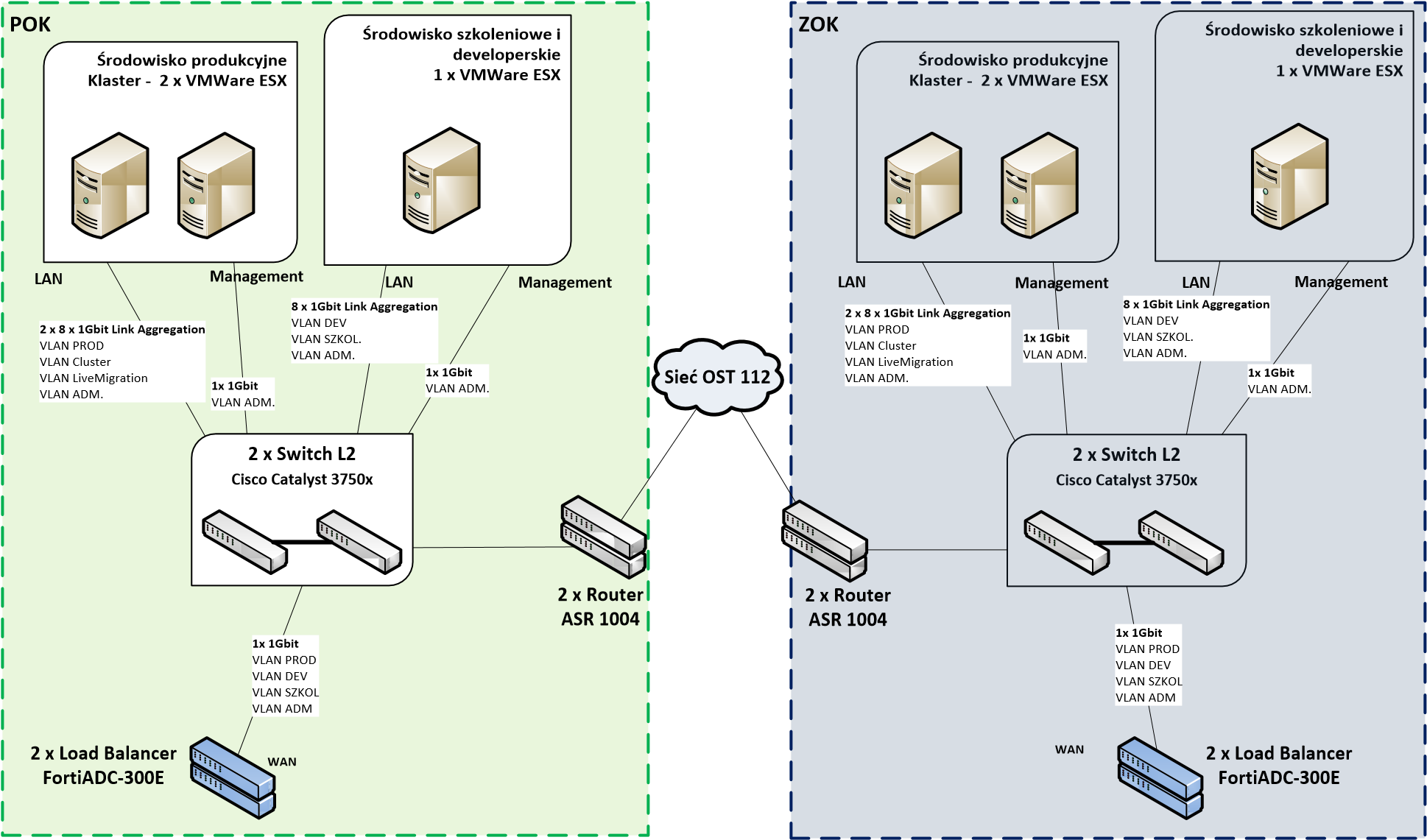
Posiadają one taką samą konfigurację sprzętową oraz są ze sobą połączone, poprzez sieć OST 112, wydzielonym łączem o przepustowości 1Gbit/s/. Połączenie do sieci OST 112 jest realizowane przez rutery ASR1004 znajdujące się w osobnych szafach.

W każdym ośrodku znajdują się:

* 2 szafy RACK zawierające serwery i urządzenia,
* macierz dyskowa,
* przełącznik KVM i konsola LCD,
* przełączniki sieciowe,
* platforma wirtualizacyjna składająca się z trzech serwerów VMWare ESX – w tym 2 działające w klastrze,
* klaster dwóch loadbalancerów.
* Urządzenie HSM

Serwery w ośrodkach mają podzielone role. Dwa z nich są skonfigurowane w klaster VMWare obsługujące środowisko produkcyjne oraz maszyny administracyjne. Pozostały serwer przeznaczony jest dla środowisk: szkoleniowego i deweloperskiego.

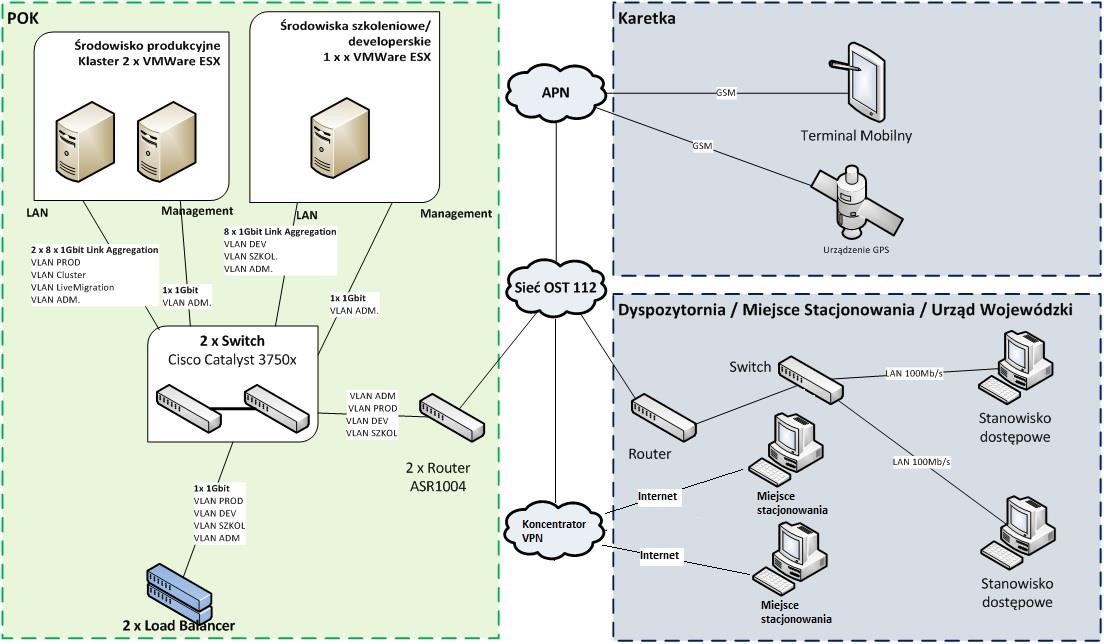
Środowisko administracyjne zawiera maszyny wirtualne wymagane do działania wszystkich środowisk oraz maszyny do zarzadzania serwerami VMWare – czyli vCenter i Data Protection.



*Rysunek nr 9. Schemat połączeń fizycznych systemu.*

**3.13.1. Stanowiska dostępowe i ambulanse ZRM**

Poniższy diagram przedstawia schemat architektury sprzętowej systemu SWD PRM pomiędzy pojedynczym ośrodkiem krajowym a stanowiskami dostępowymi (Stanowska Dyspozytorskie, stanowiska ZRM w miejscach stacjonowania, stanowiska dostępowe w urzędach wojewódzkich)   
i ambulansami ZRM.



*Rysunek nr 10. Schemat architektury sprzętowej na stanowiskach dostępowych i w ambulansach ZRM.*

## 3.14. Oprogramowanie

Zamawiający dysponuje kodami źródłowymi Oprogramowania Aplikacyjnego SWD PRM oraz jego Dokumentacją. Zamawiający jest właścicielem kodów źródłowych Oprogramowania Aplikacyjnego SWD PRM i dopuszcza ich Modyfikację przez Wykonawcę, jeśli będzie to niezbędne do realizacji niniejszego Zamówienia.

Oprogramowanie aplikacyjne SWD PRM składa się następujących elementów:

1. oprogramowanie warstwy serwera Aplikacji SWD PRM umieszczone w Ośrodkach Krajowych, z którą łączą się następujące aplikacje klienckie:
2. Dyspozytor,
3. Mobilny ZRM,
4. MS ZRM,
5. Planista,
6. Administrator biznesowy,
7. Aplikacja mapy;
8. oprogramowanie klienta Aplikacji SWD PRM działające na Stanowiskach Dyspozytorskich w Dyspozytorniach, Miejscach Stacjonowania ZRM, stanowiskach administratorskich, terminalach mobilnych dedykowanych dla ZRM.

### 3.14.1. Oprogramowanie serwerowe

Do wytworzenia oprogramowania warstwy serwera aplikacji SWD PRM działających w POK i ZOK założono wykorzystanie następujących technologii/rozwiązań:

* VMWare Essentials PLUS ESX 5.5 U1 – środowisko wirtualizacyjne zainstalowane na platformie sprzętowej dla POK i ZOK,
* CentOS 6.x x86\_64 – system operacyjny dla maszyn wirtualnych,
* WildFly 8.1.0 – serwer aplikacyjny, na którym uruchomione zostały aplikacje udostępniające usługi aplikacjom dyspozytora, zrm, administratora, planisty i mapy oraz systemowi SI WCPR,
* MySql (wersja 5.6) – serwer bazy danych, na którym przechowywane są dane operacyjne oraz historyczne systemu SWD PRM,
* Java 7 update 60 – język programowania / zbiór technologii Java,
* JAX-WS 2.2.4 – implementacja usług webowych (web service) służąca do komunikacji   
  z systemem SI WCPR,
* Quartz 2.2.1 – obsługa zadań planowanych (m.in. utrzymywanie stanu przerwy technicznej konsol telefonicznych, planowane modyfikacje danych w systemie),
* EJB 3.1 – obsługa funkcjonalności biznesowych oraz obsługa komunikatów przychodzących   
  z PZŁ,
* Hibernate 4.3 – biblioteka służąca do obsługi operacji na bazie danych oraz do odwzorowania danych bazodanowych na obiekty Java (tzw. ORM),
* Log4j – biblioteka służąca do zapisywania logów aplikacji do plików tekstowych,
* SpagoBI 5.2 – obsługa raportów,
* Apache Tomcat 7.0.47 – komponent wspierający pracę serwera raportowego zbudowanego   
  w oparciu o SpagoBI 4.2,
* Puppet 3.6 – Serwer konfiguracji i plików instalacyjnych dla wirtualnych maszyn działających   
  w systemie,

### 3.14.2. Oprogramowanie klienckie

Do wytworzenia oprogramowania aplikacji klienckich działających na Stanowiskach Dyspozytora, Miejscach Stacjonowania ZRM, stanowiskach administratorskich oraz terminalach mobilnych wykorzystano następujące technologie/rozwiązania:

* Microsoft Windows 7 Professional 64bit– System operacyjny dla stanowisk dostępowych,
* Java 7 update 67 – język programowania / zbiór technologii Java,
* JavaFx 2 – biblioteka służąca do obsługi graficznego interfejsu użytkownika,
* EJB 3.1 – wywołanie serwerowych usług biznesowych,
* Lokalna baza danych H2 – baza danych offline aplikacji oraz baza przechowująca dane lokalizacji,
* Log4j – biblioteka służąca do zapisywania logów aplikacji do plików tekstowych.

Oprogramowanie klienckie korzysta również z lokalnej relacyjnej bazy danych H2. Baza ta jest traktowana wyłącznie jako cache lokalny na wypadek utraty połączenia pomiędzy stanowiskiem klienckim a Ośrodkami Krajowymi.

Ze względu na krytyczny charakter Systemu komponenty fizyczne i logiczne zostały rozproszone na dwa Ośrodki Krajowe OK. Architektura obu Ośrodków Krajowych (POK i ZOK) została zorganizowana   
w identyczny sposób. W obu OK znajdują się środowiska: produkcyjne (PROD), szkoleniowo-testowe (SZK) oraz developerskie (DEV).

* PROD – środowisko produkcyjne dedykowane pod obsługę zgłoszeń dla PRM,
* SZK – środowisko szkoleniowo-testowe dedykowane do prowadzenia szkoleń użytkowników   
  i administratorów oraz testowania rozszerzeń systemu,
* DEV – środowisko devleoperskie dedykowane do rozwoju nowych funkcjonalności systemu.

Całość ruchu sieciowego w ramach Systemu SWD PRM jest realizowana w ramach sieci OST 112. Konfiguracja ruchu sieciowego jest realizowana przez operatora Sieci OST112.

Połączenia sieciowe związane z obsługą stanowisk mobilnych, zainstalowanych w karetkach wymagają dostępu do Sieci OST 112. W ramach Systemu obsługiwane są one przez prywatny APN (APN zapewniany jest przez Zamawiającego i jego utrzymanie nie stanowi przedmiotu umowy), podłączony do punktów styku CP SPR (Centralny Punkt System Powiadamiania Ratunkowego) w Warszawie   
i Katowicach.

## 3.15. Infrastruktura klucza publicznego (PKI)

System SWD PRM na wszystkich środowiskach używa do uwierzytelniania połączeń i użytkowników (rozumianych jako stanowiska z zainstalowaną aplikacją jak i fizyczne osoby posiadające karty mikroprocesorowe) dedykowanego modułu PKI. Zarządzanie certyfikatami

(wydawanie, odwoływanie, dystrybucja list CRL) oraz zapewnienie dostępu do modułu PKI jest obowiązkiem Zamawiającego.

W celu zapewnienia odpowiedniej poufności oraz integralności system SWD PRM wykorzystuje infrastrukturę klucza publicznego (PKI) do:

* szyfrowania transmisji danych pomiędzy stacjami klienckimi a ośrodkami POK/ZOK,
* uwierzytelniania użytkowników za pomocą kluczy przechowywanych na kartach inteligentnych (w chwili obecnej ta funkcjonalność nie jest wykorzystywana- uwierzytelnianie odbywa się za pośrednictwem loginu i hasła),
* podpisywania dokumentów.

Struktura PKI dedykowanego dla SWD PRM jest płaska- istnieje jedno centrum certyfikacji.

Infrastruktura Klucza Publicznego (PKI) dla celów zwiększenia dostępności jest zainstalowana jako rola na dedykowanej maszynie wirtualnej na której zainstalowany jest system MS Windows Server 2012 Standard. Dzięki temu możliwa jest migracja maszyny pomiędzy różnymi hostami wirtualizacji Vmware. W celu zapewnienia odpowiedniego poziomu ochrony kluczy kryptograficznych, PKI zostało zintegrowane z sprzętowymi modułami bezpieczeństwa HSM (Hardware Security Modules) marki Thales (model NH2054/nShield Connect 500+) rozproszonymi geograficznie. Na każdym z HSM zaimplementowany jest jeden wspólny dla obu ośrodków „Security World”. Oznacza to, iż informacje znajdujące się w jednym urządzeniu są zapisywane również na drugie urządzenie.

## 3.16. Ograniczenia

### 3.16.1. Wymagania na dostęp administracyjny do SWD PRM z wykorzystaniem OST 112

System pracuje w ramach sieci strukturalnej OST112, która jest siecią wewnętrzną, stworzoną na potrzeby łączności obsługi wywołań alarmowych oraz komunikacji między instytucjami odpowiedzialnymi za ratownictwo i porządek publiczny. Dostęp do sieci OST 112 zostanie zapewniony (na okres nie dłuższy niż 60 dni kalendarzowych licząc od dnia zapewnienia przez Zamawiającego dostępu do Systemu na poziomie administracyjnym) za pośrednictwem szyfrowanego połączenia VPN. Aby uzyskać dostęp Wykonawca zobowiązany jest, w ciągu 2 dni roboczych od dnia podpisania umowy, złożyć wniosek do Zamawiającego, który w imieniu Wykonawcy występuje o uzyskanie przedmiotowego dostępu do administratora sieci OST 112.

Po uzyskaniu dostępu do sieci OST112, za pośrednictwem szyfrowanego połączenia VPN Wykonawca do **50** dni kalendarzowych, licząc od dnia zapewnienia przez Zamawiającego dostępu do Systemu na poziomie administracyjnym (za pośrednictwem szyfrowanego połączenia VPN), ma obowiązek:

• zestawić łącze pomiędzy punktem styku w lokalizacji przy ul. **…………….** w

Warszawie, a miejscem świadczenia przez siebie usługi, dostarczyć, na własny koszt, do lokalizacji przy ul. ………. w Warszawie niezbędne urządzenia umożliwiające zestawienie łącza (takie jak np. router, switch, firewall).

Szczegóły techniczne dotyczące rodzaju urządzeń:

1. urządzenie SSL VPN musi posiadać co najmniej 2 porty 1 GbE;
2. urządzenie SSL VPN musi być nie większe niż 1 U i musi być przystosowane do montaży   
   w szafie RACK;
3. urządzenie SSL VPN musi umożliwić terminację VPN typu remote acces w oparciu   
   o certyfikaty i architekturę PKI;
4. urządzenie SSL VPN musi zapewnić sterowanie uprawnieniami do zasobów sieciowych   
   w oparciu o grupy;
5. urządzenie SSL VPN musi być dedykowanym urządzeniem sieciowym;
6. urządzenie SSL VPN musi obsłużyć minimalnie 50 użytkowników jednocześnie   
   z możliwością rozbudowy do min. 200;
7. urządzenie SSL VPN musi umożliwiać rozbudowę o funkcjonalność integracji   
   z zewnętrznym systemem bezpieczeństwa typu firewall poprzez protokół IF-MAP dla celów wymuszenia polityki bezpieczeństwa właściwej dla roli użytkownika systemu SSL VPN;
8. urządzenie SSL VPN musi umożliwiać sprawdzenie poziomu bezpieczeństwa urządzenia podłączającego się do systemu- min. Obecność uruchomionego oprogramowania typu firewall, antywirus, poprawki systemu Windows,
9. Klient VPN musi być dostępny min. dla systemów operacyjnych Windows, Mac OS, Apple iOS, Android, Windows Mobile;
10. urządzenie SSL VPN musi być systemem kompletnym pochodzącym od jednego producenta. Nie dopuszcza się stosowania rozwiązań typu „open source”.

Wykonawca przyjmuje do wiadomości, że w trakcie trwania umowy dostarczone przez niego urządzenia, będą administrowane przez Zamawiającego, a po zakończeniu umowy Wykonawca będzie zobowiązany do ich odbioru na własny koszt.

## 3.17. Integracja z systemami zewnętrznymi

### 3.17.1. UMM

Stanowiska, na których jest zainstalowany Moduł Dyspozytora i Moduł Mapy oraz aplikacja serwerowa, wymagają dostępu sieciowego do serwisu SDI (Geoportal), aby możliwe było użycie funkcjonalności prezentacji map numerycznych w aplikacji. Dostęp ten i zapewnienie jego jakości jest zależny od operatora sieci OST112.

Moduł mapy wykorzystuje kontrolkę UMM dostarczoną przez GUGIK, w której została zaimplementowana dodatkowa warstwa dla SWD PRM. Kontrolka została dostarczona w wersji 32bit. Kontrolka 32bit posiada ograniczenie zaalokowanej pamięci do 1,5 GB.

### 3.17.2. PLI CBD

Aplikacja serwerowa wymaga dostępu do systemu PLI CBD. Dostęp ten jest realizowany przez CP SPR, będący elementem sieci OST112 i będący poza zakresem systemu SWD PRM. Dostęp do wskazanego systemu jest zależny od operatora sieci OST112.

Format komunikacji z PLI CBD został narzucony przez system PLI CBD (interfejs jest zdefiniowany po stronie PLI CBD).

### 3.17.3. Integracja z SI CPR

Aplikacja serwerowa jest przygotowana do współpracy z systemem SI CPR. Wymiana informacji pomiędzy systemami realizowana jest za pomocą sieci OST112. Dostęp do wskazanego systemu jest zależny od operatora sieci OST112.

Format komunikacji z SI CPR został narzucony przez system SI CPR (interfejs jest zdefiniowany po stronie SI CPR i stanowi element systemu SI CPR, wspólny dla wszystkich SWD).

### 3.17.4. Automapa

W celu bieżącego nawigowania kierowcy ZRM terminal mobilny został wyposażony w oprogramowanie standardowe „Automapa”. Ze względu na brak dostępu do sieci Internet na terminalu mobilnym oprogramowanie to nie wykorzystuje bieżącej informacji o ruchu drogowym.

### 3.17.5. PZŁ

System PZŁ jest wykorzystywany do przekazywania połączeń głosowych pomiędzy służbami używającymi numerów alarmowych (112, 999, 998, 997). System pozwala na wyświetlenie informacji   
o konkretnym zdarzeniu wraz z odebranym połączeniem telefonicznym (mechanizm kojarzenia formatki).

# 4. Usługi rekonfiguracyjne SWD PRM

Zamawiający realizując zadania utrzymania i obsługi technicznej systemu SWD PRM zamierza uruchomić dodatkową formę wsparcia dla administratora Systemu, którym jest LPR w postaci możliwości zlecania Wykonawcy prac w ramach godzin rekonfiguracyjnych Systemu SWD PRM.

Przedmiotem umowy dodatkowo jest świadczenie przez Wykonawcę na rzecz Zamawiającego usługi   
w postaci zlecanych na bieżąco zadań zwanych Zleceniami. Zlecenia dotyczyć będą usprawnień, Modyfikacji, zmian rekonfiguracyjnych. Zlecenia mają na celu rozbudowę Systemu i nie mogą być formą zapewniania ciągłości pracy Systemu.

Jeśli w wyniku Zleceń powstanie Modyfikacja, podlega ona takiemu SLA jak pozostała część Systemu SWD PRM

Na podstawie Umowy Zamawiający zleci pisemnie w formie Zleceń wykonanie Usług Rekonfiguracji   
w wymiarze do **5000** (słownie: pięć tysięcy) godzin.

## 4.1. Wymagania w zakresie usług rekonfiguracyjnych SWD PRM

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| **WKR.01** | Zamawiający wymaga aby przedmiot Umowy z punktu 4 był realizowany przez Wykonawcę w okresie od dnia podpisania Umowy do wyczerpania przyjętego w Umowie limitu godzin rekonfiguracyjnych lub do dnia zakończenia umowy w zależności od tego, które zdarzenie nastąpi wcześniej. |
| **WKR.02** | Przedmiot Umowy w formie Zleceń będzie odbierany, poprzez podpisywanie Protokołu Odbioru Zlecenia przez Zamawiającego po realizacji każdego Zlecenia. |
| **WKR.03** | Protokół Odbioru Zleceń, podpisany bez uwag będzie stanowił podstawę do wystawienia faktury przez Wykonawcę i dokonania płatności przez Zamawiającego. |
| **WKR.04** | Wykonawca przyjmie do wiadomości, że SWD PRM może być rozbudowywany o kolejne funkcjonalności i nie będzie zgłaszał z tego tytułu zastrzeżeń podczas realizacji kolejnych Zleceń. Rozbudowa Systemu SWD PRM będzie umożliwiała realizację kolejnych Zleceń na warunkach opisywanych każdorazowo przez Zamawiającego. |
| **WKR.05** | Przyjmuje się, że najmniejszą możliwą wielkością Zlecenia będzie  1 godzina. |
| **WKR.06** | W ramach Zleceń Wykonawca będzie realizował prace związane  z rekonfiguracją, modyfikacją i rozbudową Systemu SWD PRM zgodnie  z treścią Zlecenia. Zakres wykonania prac zostanie zdefiniowany każdorazowo. |

## 4.2. Zakres usługi w ramach zleconych prac rekonfiguracyjnych

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| **WKZ.01** | Konsultacje techniczne w ramach, których Wykonawca ma przedstawić wyniki analizy Zlecenia powierzonego przez Zamawiającego, sposób rozwiązania, możliwości rozbudowy lub Modyfikacji w celu uzyskania funkcjonalności oczekiwanej przez Zamawiającego. |
| **WKZ.02** | Dokonywanie zmian, usprawnień, Modyfikacji SWD PRM i Dokumentacji, wraz z przeniesieniem majątkowych praw autorskich oraz praw zależnych do zmienionego Oprogramowania Aplikacyjnego lub zmodyfikowanej Dokumentacji. |
| **WKZ.03** | Analiza konfiguracji serwerów aplikacyjnych systemu, zaproponowanie  i wdrożenie rozwiązań mających na celu eliminację zidentyfikowanych błędów w celu zwiększenia wydajności SWD PRM. |
| **WKZ.04** | Analiza środowiska bazodanowego w celu optymalizacji działania oraz zwiększenia dostępności środowiska Systemu SWD PRM. |
| **WKZ.05** | Analiza zagrożeń jakie mogą wywołać modyfikacje SWD PRM prowadzone przez Zamawiającego w ramach innych umów. |
| **WKZ.06** | Plan rozbudowy Systemu – przeprowadzenie analizy wydajnościowej Systemu SWD PRM przed i po wprowadzeniu Modyfikacji. |
| **WKZ.07** | Analiza logów Oprogramowania. |
| **WKZ.08** | Przygotowywanie rekomendacji zmian i propozycji rozwiązań dla zapewnienia odpowiedniej pojemności/dostępności Systemu wraz z implementacją rozwiązań zatwierdzonych przez Zamawiającego. |

# 5. Usługi utrzymaniowe SWD PRM

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| **WUT.01** | Wykonawca zobowiązuje się do zapewnienia czasu dostępności SWD PRM w pełnej funkcjonalności na poziomie 99,95% dla Systemu (czas niedostępności w ciągu miesiąca to 21 minuty i 36 sekund). SLA będzie liczone od momentu zgłoszenia Awarii Krytycznej przez Administratora Systemu lub jego pracowników. |
| **WUT.02** | SLA Ośrodka Krajowego liczone jest jako suma czasu trwania niedostępności SWD PRM spowodowanej Awariami Krytycznymi, przy czym okna serwisowe związane z konserwacją/konfiguracją Systemu SWD PRM nie podlegają uwzględnieniu w obliczaniu SLA (termin i zakres prac realizowanych w ramach okna serwisowego wymaga uzyskania przez Wykonawcę uprzedniej akceptacji Zamawiającego).  Do czasu przestoju w dostępności Systemu nie wlicza się następujących zdarzeń:   1. Braku dostępu do urządzeń zainstalowanych w Ośrodku Krajowym, mającym wpływ na pracę SWD PRM spowodowany problemami z infrastrukturą sieciową będącą poza odpowiedzialnością Wykonawcy, chyba że wina w zakresie uzyskania dostępu leży po stronie Wykonawcy; 2. Awarią podsystemów nie będących przedmiotem niniejszej umowy, w tym: 3. Centrum Certyfikatów (PKI), 4. infrastrukturą serwerową, 5. platformą wirtualizacyjną, 6. siecią w obrębie infrastruktury serwerowej, 7. UMM (Uniwersalny Moduł Mapowy), 8. PLI CBD, 9. PZŁ (Podsystem Zintegrowanej Łączności). |
| **WUT.03** | Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie systemu SWD PRM, zgodnie z SLA. |
| **WUT.04** | Wykonawca zobowiązuje się do utrzymania SWD PRM w następującym zakresie:   1. usuwania Awarii mających wpływ na ciągłość działania SWD PRM lub powodujących niedostępność procesów biznesowych; 2. Modyfikacji Systemu SWD PRM; 3. optymalizacji pod względem wydajności oraz dostępności SWD PRM. |
| **WUT.05** | Wykonawca zapewni obsługę zgłaszanych przez Zamawiającego Incydentów w trybie ciągłym, tj. 24 godziny na dobę/7 dni w tygodniu/365 dni w roku, według następujących kategorii:   1. Awaria Krytyczna; 2. Awaria Niekrytyczna; 3. Awaria Zwykła. |

|  |  |
| --- | --- |
| **WUT.06** | W celu zarządzania Incydentami Serwisowymi Zamawiający zapewni Wykonawcy dostęp do systemu do obsługi Incydentów Serwisowych wraz  z procedurą zgłaszania Awarii. Za pomocą ww. systemu dokonywane będą zgłoszenia Incydentów Serwisowych, a także obsługa i monitorowanie realizacji Incydentów Serwisowych. |
| **WUT.07** | Wykonawca jest zobowiązany do niezwłocznego potwierdzenia otrzymania zgłoszenia Awarii, jednak nie później niż w ciągu 15 minut od otrzymania ww. zgłoszenia, zgodnie z procedurą zgłaszania Awarii (system do obsługi Incydentów Serwisowych, e-mail, telefon). |
| **WUT.08** | Po przygotowaniu przez Wykonawcę Modyfikacji Oprogramowania Aplikacyjnego, zostanie ono przetestowane na środowisku szkoleniowym. Po pozytywnym wyniku testów i wdrożeniu na produkcję, objęte serwisem na takich samych zasadach jak całość Oprogramowania Aplikacyjnego SWD PRM. Wzór formularza oceny testów stanowi Załącznik nr 2 do OPZ. |
| **WUT.09** | Usunięcie Awarii zostanie zakończone przywróceniem działania Oprogramowania sprzed powstania Awarii oraz potwierdzeniem przez Wykonawcę jej usunięcia w sposób zgodny z procedurą zgłaszania Awarii (system do obsługi Incydentów Serwisowych, email, telefon). |
| **WUT.10** | Wykonawca najpóźniej w 2 dni robocze po rozwiązaniu Incydentu Serwisowego przedstawi raport z tego Incydentu Serwisowego (prezentujący co najmniej czasy przyjęcia zgłoszenia o Incydencie Serwisowym oraz rozwiązania Incydentu Serwisowego, a także przyczyny, sposoby rozwiązania i działania zapobiegające występowaniu Incydentu Serwisowego w przyszłości). |
| **WUT.11** | Jeżeli naprawa spowoduje nieaktualność przekazanej Dokumentacji, Wykonawca dostarczy Zamawiającemu (do siedziby Zamawiającego) uaktualnioną Dokumentację w ciągu 5 dni roboczych oraz w formie elektronicznej na adres email: [ctswdprm@lpr.com.pl](mailto:ctswdprm@lpr.com.pl). |
| **WUT.12** | Wykonawca usunie Awarię Krytyczną w terminie zapewniającym dotrzymanie świadczenia usług zgodnie z SLA. |
| **WUT.13** | Wykonawca usunie Awarię Niekrytyczną w terminie nie dłuższym niż  24 godziny od momentu zgłoszenia Awarii Niekrytycznej. |
| **WUT.14** | Wykonawca usunie Awarię Zwykłą w terminie nie dłuższym niż 48 godzin od momentu zgłoszenia Awarii Zwykłej. |
| **WUT.15** | Wykonawca, w przypadku prac planowanych, zgłosi Zamawiającemu zamiar ich prowadzenia z wyprzedzeniem 7 dni roboczych. Potwierdzenie wyrażenia zgody lub brak zgody na wykonanie ww. prac powinno nastąpić w terminie  2 dni roboczych. |
| **WUT.16** | Przez usunięcie Awarii rozumie się przywrócenie funkcjonalności Systemu sprzed Awarii albo wykonanie procedury obejścia zaistniałych Awarii bez przywrócenia funkcjonalności Systemu sprzed Awarii, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję wykonania procedury obejścia Zamawiający wyrazi zgodę. |
| **WUT.17** | Świadczenie usługi utrzymania obejmuje również wykonanie przez Wykonawcę wszelkich czynności związanych z przywróceniem pierwotnego stanu Systemu SWD PRM (sprzed Awarii). |
| **WUT.18** | Wykonawca zobowiązuje się do wykonywania obowiązków wynikających ze świadczenia usług utrzymania, o których mowa w niniejszym ustępie,  w sposób zapobiegający utracie danych zawartych w Systemie.  W przypadku, gdy dokonanie usunięcia Awarii wiąże się z ryzykiem utraty danych, Wykonawca zobowiązany jest poinformować o tym Zamawiającego w celu wykonania kopii bezpieczeństwa przez Zamawiającego. Wykonawca określi także sposób wykonania kopii danych po konsultacji  z Zamawiającym, tak by zminimalizować możliwość utraty danych. |
| **WUT.19** | Zamawiający udostępni Wykonawcy, na potrzeby świadczenia usług, kody źródłowe Oprogramowania Aplikacyjnego oraz wszelką Dokumentację Systemu, których jest właścicielem. |
| **WUT.20** | W przypadku wprowadzenia przez Wykonawcę korekt Oprogramowania Aplikacyjnego, każdorazowo na wezwanie Zamawiającego, Wykonawca dostarczy Zamawiającemu zaktualizowaną wersję kodów źródłowych Oprogramowania Aplikacyjnego wraz z odnoszącą się do niego Dokumentacją. Na koniec okresu świadczenia usług utrzymania Wykonawca dostarczy Zamawiającemu zaktualizowaną wersję kodów źródłowych wraz z Dokumentacją Modyfikacji. Wykonawca użyje do tego celu systemu kontroli wersji działającego po stronie Zamawiającego. |
| **WUT.21** | Wykonawca zapewni miesięczne raporty ze współpracy z Zamawiającym  w formie wymaganej przez Zamawiającego, w których będą omówione (przedstawione) poniższe zagadnienia, w tym m.in.:   1. proces usuwania Awarii zgłoszonych Wykonawcy, spowodowanych Incydentami – raport powinien zawierać co najmniej: 2. datę usunięcia Awarii, 3. szczegółowy opis wprowadzonych zmian i przyjętych rozwiązań wraz ze wskazaniem numeru Incydentu Serwisowego zarejestrowanego w dedykowanym systemie obsługi Incydentów Serwisowych; 4. proces wgrywania korekt Oprogramowania – raport powinien zawierać co najmniej:    1. datę wdrożenia nowej wersji Oprogramowania,    2. numer wersji Oprogramowania,    3. szczegółowy opis wprowadzonych zmian i przyjętych rozwiązań wraz ze wskazaniem numeru Incydentu Serwisowego zarejestrowanego w dedykowanym systemie obsługi Incydentów Serwisowych. |
| **WUT.22** | Wykonawca zobowiązuje się do usuwania Awarii, w tym także w razie niespełnienia deklarowanych przez producenta parametrów lub funkcji użytkowych Oprogramowania wynikających z Dokumentacji określonej  w OPZ. |
| **WUT.23** | Wykonawca zobowiązuje się do usuwania wykrytych Awarii mających wpływ na ciągłość działania SWD PRM lub powodujących niedostępność procesów biznesowych zdefiniowanych w Dokumentacji. Jeśli Awaria zostanie wykryta poza obszarem objętym Umową Wykonawca zobowiązany jest do wskazania Zamawiającemu elementu generującego Awarię wraz z uzasadnieniem w postaci opisu i logów Systemu wskazujących jednoznacznie na przyczynę Awarii lub wskazujących współpracujący podsystem, który tę Awarię generuje. |
| **WUT.24** | W przypadku dokonywania aktualizacji Oprogramowania Standardowego lub modyfikacji infrastruktury sprzętowej, Wykonawca jest zobowiązany do udzielenia zaleceń i wskazania ewentualnych konsekwencji takich aktualizacji. Wykonawca zobowiązany jest także określić kompatybilność Oprogramowania Standardowego aktualizowanego przez Wykonawcę  z SWD PRM poprzez przeprowadzenie testów z Zamawiającym na środowisku SZK SWD PRM. |
| **WUT.25** | W przypadku konieczności aktualizacji Oprogramowania Standardowego, Wykonawca jest zobowiązany dostosować Aplikację  SWD PRM do nowej wersji Oprogramowania Standardowego. |
| **WUT.26** | Wykonawca zobowiązuje się do informowania Zamawiającego o aktualnym lub planowanym wykorzystaniu Infrastruktury Sprzętowej , zagrożeniach wynikających z jej ograniczeń i konieczności jej modyfikacji przez Zamawiającego. Wykonawca jest zobowiązany do przedstawia raportu  w którym wykaże wpływ planowanych Modyfikacji na Infrastrukturę oraz zalecenia jakie powinien wprowadzić Zamawiający na skutek eksploatacji SWD PRM oraz Modyfikacji. |
| **WUT.27** | Wykonawca zobowiązuje się do prognozowania obciążenia Infrastruktury Sprzętowej oraz planowania dostępności i pojemności jej elementów, utrzymywania planów dostępności i pojemności Infrastruktury Sprzętowej, zarządzania ryzykiem powstania niedostępności elementów Infrastruktury Sprzętowej, która może przełożyć się na niedostępność usług świadczonych w oparciu o tę Infrastrukturę Sprzętową. |
| **WUT.28** | Wykonawca zobowiązuje się do podejmowania działań mających na celu zapobieganie przeciążeniu Infrastruktury Sprzętowej, jeśli jest ona spowodowana aplikacją SWD PRM lub jej Modyfikacjami. |

# 6. Minimalne wymagania w zakresie zarządzania przedmiotem zamówienia

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| **WZP.01** | Wymaga się od Wykonawcy aby organizacja przedsięwzięcia związanego z przedmiotem zamówienia, procesy kierujące przedsięwzięciem, struktura i zawartość realizacji zamówienia techniki zarządzania realizacją zmówienia, zestaw elementów sterujących zarządzaniem i jakością, w tym cała tworzona Dokumentacja, zostały oparte o ogólnie znaną metodykę projektową lub własną uwzględniającą konkretne techniki, narzędzia  i notacje, a także zapewniającą osiągnięcie zamierzonych celów jakościowych przy jednoczesnej minimalizacji możliwości niepowodzenia przedsięwzięcia. |
| **WZP.02** | W przypadku wykorzystywania przez Wykonawcę własnej metodyki zarządzania przedsięwzięciem, wymaga się, aby uwzględniała ona co najmniej następujące elementy:   1. sposób zarządzania przedsięwzięciem, w tym proces kontroli postępu prac w zakresie kosztów, pracochłonności, raportowanie  o postępach w realizacji przedsięwzięcia oraz sposób zarządzania problemami w realizacji przedsięwzięcia; 2. analizę ryzyka przed rozpoczęciem przedsięwzięcia i zarządzanie ryzykiem w trakcie jego realizacji; 3. sposób zarządzania zmianami, w tym rodzaje modyfikacji (poprawki, aktualizacje, rozbudowa, udoskonalenia) oraz procedury kontroli zmian. |

# 7. Wymagania w zakresie zgodności z przepisami prawa

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis wymagania** |
| **PR.01** | Rozwiązanie dla Systemu musi być zgodne z niżej wymienionymi aktami prawnym:   * Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych  (t.j. Dz. U. z 2018 r. poz. 1000). * Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r.  w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r., poz. 2247); * Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2017 r., poz. 570 z późn. zm.); * Ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej  (t.j. Dz. U. z 2018 r., poz. 620); * Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej  (t.j. Dz. U. z 2017 r., poz. 1897 z późn. zm.); * Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne  (t.j. Dz. U. z 2018 r.,poz. 1954); * Ustawa z dnia 8 września 2006 r. o Państwowym   Ratownictwie Medycznym (t.j. Dz. U. z 2017 r., poz. 2195 z późn. zm.);   * Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym  (t.j. Dz. U. z 2018r., poz. 1401); * Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (t.j. Dz. U. z 2018 r. poz. 867); * Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia  7 marca 2002 r. w sprawie usługi powszechnej i związanych  z sieciami i usługami łączności elektronicznej praw użytkowników -dyrektywa o usłudze powszechnej (Dz.U.UE.L.2002.108.51  z późn. zm.); * Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r.  w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. z 2015 r. poz. 2069); * Rozporządzenie Ministra Spraw Wewnętrznych  i Administracji z dnia 24 marca 2011 r. w sprawie centralnego punktu systemu centrów powiadamiani ratunkowego oraz punktów centralnych służb (Dz. U. z 2015 r., poz.2356); * Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679  z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE. |

# 8. WYMAGANIA W ZAKRESIE DOKUMENTACJI

Wykonawca w ramach realizacji przedmiotu zamówienia dostarczy dokumentację spełniającą wymagania określone w poniższej tabeli.

Minimalne wymagania dla Dokumentacji:

|  |  |
| --- | --- |
| **Kod wymagania** | **Opis funkcjonalności** |
| **DOK.01** | Wytworzone przez Wykonawcę procedury muszą zostać zoptymalizowane pod kątem ciągłości działania usług Systemu o wysokim poziomie SLA. |
| **DOK.02** | Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedsięwzięcia charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak:   1. struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób; 2. zachowanie standardów, w tym notacji UML, a także sposób pisania, rozumianych jako zachowanie spójnej struktury, formy i sposobu pisania dla poszczególnych dokumentów oraz fragmentów tego samego dokumentu; 3. zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów wersjonowania, metryk oraz wzoru szablonu dokumentu; 4. kompletność dokumentu rozumiana jako pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia; 5. spójność i niesprzeczność dokumentu rozumianych jako zapewnienie wzajemnej zgodności pomiędzy wszystkimi rodzajami informacji umieszczonymi w dokumencie, jak i brak logicznych sprzeczności pomiędzy informacjami zawartymi we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu. |
| **DOK.03** | Cała Dokumentacja, podlega akceptacji Zamawiającego i zostanie dostarczona w języku polskim, w wersji elektronicznej w niezabezpieczonym/edytowalnym formacie MS Word i niezabezpieczonym formacie PDF (na płycie CD/DVD lub innym równoważnym nośniku danych) i drukowanej, co najmniej w 1 egzemplarzu (dopuszcza się inne formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe jak DWG, DXF, należy jednak dołączyć przeglądarkę obsługującą wykorzystane formaty). Diagramy UML sporządzone za pomocą narzędzi CASE muszą być dostarczone w formacie EAP. Dostarczone wykresy Gantta muszą być dostarczone w formacie MPP lub  w formacie XLS umożliwiającym import do MS Project. |
| **DOK.04** | Wymagane jest, aby w ramach Dokumentacji, Wykonawca przekazał Zamawiającemu pliki źródłowe zastosowanych w niej obrazów, w tym m.in. schematów, rysunków, topologii oraz wykresów, w formacie niezabezpieczonym i edytowalnym. |
| **DOK.05** | Wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu wszystkie dokumenty robocze wytworzone w takcie realizacji niniejszego zamówienia, w szczególności analizy, arkusze kalkulacyjne, materiały robocze, w formacie elektronicznym, niezabezpieczonym i edytowalnym. |
| **DOK.06** | Wszystkie Dokumenty przekazane w formie elektronicznej (pliki) muszą:   1. być posegregowane w folderach odpowiadających nazwą produktów oraz nazwą, wersją i podwersją przekazywanego modułu (dotyczy kodów źródłowych); 2. być posegregowane w folderach zgodnie ze strukturą Dokumentacji; 3. posiadać nazwy plików (razem ze ścieżką) krótsze niż 200 znaków. |
| **DOK.07** | W przypadku kolejnych wersji Dokumentacji wymagane jest, aby Wykonawca dostarczał elektroniczne wersje Dokumentacji, które zawierają wyróżnione różnice pomiędzy kolejnymi wersjami Dokumentacji (w trybie rejestracji zmian). |
| **DOK.08** | Zamawiający udostępni Dokumentację powykonawczą oraz eksploatacyjną SWD PRM na życzenie Wykonawcy. |

1. Z dniem 1 kwietnia 2019 r. rejon operacyjny to rejon działania dyspozytorni medycznej określony w wojewódzkim planie działania systemu Państwowe Ratownictwo Medyczne. [↑](#footnote-ref-1)