

**SPECYFIKACJA
ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)**

PRZETARG NIEOGRANICZONY PN.:

**„Świadczenie usług utrzymaniowych oraz
rekonfiguracyjnych dla Aplikacji Systemu
Wspomagania Dowodzenia Państwowego
Ratownictwa Medycznego (SWD PRM)”**

Zatwierdził:

Z up. Dyrektora

Z-ca DYREKTORA
ds. Ratownictwa Medycznego,
Organizacji i Planowania
Lotnicze/Podłożenie Ratunkowe

Marcin Podgórski

§ 1

NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

1. Zamawiającym jest:

Lotnicze Pogotowie Ratunkowe

Adres: ul. Księżycowa 5 01-934 Warszawa

Tel: +48 /22/ 22 99 931, Fax: +48 /22/ 22 99 933

NIP: 522-25-48-391 Regon: 016321074

http://www.lpr.com.pl e-mail:// dzp@lpr.com.pl, centrala@lpr.com.pl

2. Dni i godziny urzędowania: od poniedziałku do piątku w godzinach 8⁰⁰-15³⁵.

§ 2

TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie **przetargu nieograniczonego** na podstawie ustawy z dnia 29 stycznia 2004 r. „Prawo zamówień publicznych” (tekst jednolity Dz. U. z 2018 r. poz. 1986), zwanej dalej uPzp.
2. Postępowanie jest prowadzone zgodnie z przepisami uPzp dla postępowań, których wartość zamówienia jest równa lub przekracza kwoty określone w przepisach wydanych na podstawie art. 11 ust. 8 uPzp, tj. kwotę 144 000,00 EURO.

§ 3

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM).
2. Szczegółowy opis przedmiotu zamówienia zawarto w załączniku nr 2 do SIWZ.
3. Oznaczenie wg Wspólnego Słownika Zamówień (CPV):

72250000-2 – Usługi w zakresie konserwacji i wsparcia systemów;

72260000-5 – Usługi w zakresie oprogramowania;

72230000-6 – Usługi w zakresie rozbudowy oprogramowania.

4. W przypadku, gdyby w opisie przedmiotu zamówienia Zamawiający określił przedmiot zamówienia poprzez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów, Zamawiający dopuszcza możliwość składania ofert równoważnych. Wskazane wyżej określenie przedmiotu zamówienia ma charakter wyłącznie pomocniczy w przygotowaniu oferty i ma na celu wskazać oczekiwane standardy co do minimalnych parametrów technicznych oczekiwanych materiałów i urządzeń. Przez ofertę równoważną należy rozumieć ofertę o parametrach technicznych, wytrzymałościowych, jakościowych, wydajnościowych nie gorszych od opisu wskazanego przez Zamawiającego w opisie przedmiotu zamówienia. W związku z powyższym, Zamawiający dopuszcza możliwość zaoferowania materiałów o innych znakach towarowych, patentach lub pochodzeniu, natomiast nie o innych właściwościach i funkcjonalnościach niż określone w SIWZ. Wykonawca, powołujący się na rozwiązania równoważne stosownie do dyspozycji art. 30 ust. 5 uPzp, musi wykazać, że oferowane dostawy spełniają warunki określone przez Zamawiającego w stopniu nie gorszym. W przypadku, gdy wykonawca nie złoży w ofercie dokumentów o zastosowaniu innych materiałów i urządzeń, to rozumie się przez to, że do kalkulacji ceny oferty oraz do wykonania umowy ujęto materiały i urządzenia zaproponowane w opisie przedmiotu zamówienia.

W przypadku, gdy Zamawiający użył w opisie przedmiotu zamówienia normy, aprobaty, specyfikacje techniczne i systemy odniesienia, o których mowa w art. 30 ust. 1-3 uPzp, należy rozumieć je jako przykładowe. Zamawiający, zgodnie z art. 30 ust. 4 uPzp, dopuszcza w każdym przypadku zastosowanie rozwiązań równoważnych opisanych w treści SIWZ. Każdorazowo, gdy wskazana jest w niniejszej SIWZ norma, należy przyjąć, że w odniesieniu do niej użyto sformułowania „lub równoważne”. Wykonawca, który powołuje się na rozwiązania równoważne w stosunku do opisywanych przez Zamawiającego, jest obowiązany wykazać w złożonej ofercie, że oferowane przez niego dostawy, spełniają wymagania określone przez Zamawiającego.

§ 4

OPIS CZĘŚCI ZAMÓWIENIA

Zamawiający nie dopuszcza składanie ofert częściowych.

§ 5

INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 67 UST. 1 PKT 6 I 7 UPZP

Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 67 ust. 1 pkt 6 uPzp.

§ 6

INFORMACJA O OFERTACH WARIANTOWYCH

Zamawiający nie dopuszcza składania ofert wariantowych.

§ 7

WYKONANIE ZAMÓWIENIA PRZY UDZIALE PODWYKONAWCÓW

1. Zgodnie z przepisem art. 36a ust. 1 uPzp, Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy. Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom, i podania przez Wykonawcę firm podwykonawców
2. W przypadku niewskazania części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz niewskazania firm podwykonawców, przyjmuje się, iż przedmiot zamówienia zostanie w całości wykonany samodzielnie przez Wykonawcę.

§ 8

TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia: Wykonawca zobowiązany będzie do świadczenia usługi stanowiącej przedmiot zamówienia od dnia zawarcia umowy do 31 grudnia 2019 r.

§ 9

WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ PODSTAWY WYKLUCZENIA WYKONAWCY

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki, o których mowa w art. 22 ust. 1b uPzp, dotyczące:
 - 1) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie określa warunku w tym zakresie,
 - 2) sytuacji ekonomicznej lub finansowej – Zamawiający nie określa warunku w tym zakresie,
 - 3) zdolności technicznej lub zawodowej – Zamawiający uzna warunek za spełniony, jeżeli Wykonawca wykaże, że okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, zrealizował

dwie usługi serwisowe polegające na utrzymaniu aplikacji dla środowisk o SLA wyższym niż 90% obliczanym miesięcznie, o łącznej wartości usług nie mniejszej niż 2 000 000,00 zł (słownie: dwa miliony złotych 00/100) brutto.

W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający uzna powyższy warunek za spełniony jeżeli jeden z Wykonawców spełnia go samodzielnie.

W przypadku usług będących w trakcie realizacji warunek dotyczący wartości usługi należy odnieść do wartości części usługi zrealizowanej do upływu terminu składania ofert. Przez usługę należy rozumieć zawartą umowę.

W przypadku wskazania w wykazie większej niż dwie liczbie wykonanych przez Wykonawcę usług polegających na utrzymaniu aplikacji dla środowisk o SLA wyższym niż 90% obliczanym miesięcznie, dla spełnienia ww. warunku konieczne jest aby łączna wartość dwóch z nich wynosiła co najmniej 2 000 000,00 zł brutto.

2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy nie podlegają wykluczeniu na podstawie art. 24 ust. 1 uPzp. Zgodnie z art. 24 ust. 1 uPzp, z postępowania o udzielenie zamówienia wyklucza się:
 - 1) Wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu,
 - 2) Wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
 - a) o którym mowa w art. 165a, art. 181–188, art. 189a, art. 218–221, art. 228–230a, art. 250a, art. 258 lub art. 270–309 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (tekst jednolity Dz. U. z 2017 r. z późn. zm.) lub art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (tekst jednolity Dz. U. z 2017 r. poz. 1463 z późn. zm.),
 - b) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny,
 - c) skarbowe,
 - d) o którym mowa w art. 9 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769).
 - 3) Wykonawcę, jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 2),
 - 4) Wykonawcę, wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności,
 - 5) Wykonawcę, który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawieniu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub obiektywne i niedyskryminacyjne kryteria, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych dokumentów,
 - 6) Wykonawcę, który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd zamawiającego, mogące mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia,

- 7) Wykonawcę, który bezprawnie wpływał lub próbował wpłynąć na czynności zamawiającego lub pozyskać informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia,
 - 8) Wykonawcę, który brał udział w przygotowaniu postępowania o udzielenie zamówienia lub którego pracownik, a także osoba wykonująca pracę na podstawie umowy zlecenia, o dzieło, agencyjnej lub innej umowy o świadczenie usług, brał udział w przygotowaniu takiego postępowania, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu,
 - 9) Wykonawcę, który z innymi wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych,
 - 10) Wykonawcę będącego podmiotem zbiorowym, wobec którego sąd orzekł zakaz ubiegania się o zamówienia publiczne na podstawie ustawy z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (tekst jednolity Dz. U. z 2016 r. z późn. zm.),
 - 11) Wykonawcę, wobec którego orzeczono tytułem środka zapobiegawczego zakaz ubiegania się o zamówienia publiczne,
 - 12) Wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity z Dz. U. z 2017 r. poz. 229 z późn. zm.), złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykazą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
3. Wykluczenie Wykonawcy następuje:
- 1) w przypadkach, o których mowa w ust. 2 pkt 2) lit. a) – c) i pkt 3), gdy osoba, o której mowa w tych przepisach została skazana za przestępstwo wymienione w ust. 2 pkt 2) lit. a) – c), jeżeli nie upłynęło 5 lat od dnia uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia,
 - 2) w przypadkach, o których mowa:
 - a) w ust. 2 pkt 2) lit. d) i pkt 3), gdy osoba, o której mowa w tych przepisach, została skazana za przestępstwo wymienione w ust. 2 pkt 2) lit. d),
 - b) w ust. 2 pkt 4),– jeżeli nie upłynęły 3 lata od dnia odpowiednio uprawomocnienia się wyroku potwierdzającego zaistnienie jednej z podstaw wykluczenia, chyba że w tym wyroku został określony inny okres wykluczenia lub od dnia w którym decyzja potwierdzająca zaistnienie jednej z podstaw wykluczenia stała się ostateczna,
 - 3) w przypadkach, o których mowa w ust. 2 pkt 7) i 9), jeżeli nie upłynęły 3 lata od dnia zaistnienia zdarzenia będącego podstawą wykluczenia,
 - 4) w przypadku, o którym mowa w ust. 2 pkt 10), jeżeli nie upłynął okres, na jaki został prawomocnie orzeczony zakaz ubiegania się o zamówienia publiczne,
 - 5) w przypadku, o którym mowa w ust. 2 pkt 11), jeżeli nie upłynął okres obowiązywania zakazu ubiegania się o zamówienia publiczne.
4. Wykonawca, który podlega wykluczeniu na podstawie ust. 2 pkt 2) i 3) oraz 5) – 9) lub ust. 3, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie

dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.

5. Wykonawca nie podlega wykluczeniu, jeżeli Zamawiający, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, uzna za wystarczające dowody przedstawione na podstawie ust. 4.
6. W przypadkach, o których mowa w ust. 2 pkt 8), przed wykluczeniem Wykonawcy, Zamawiający zapewnia temu Wykonawcy możliwość udowodnienia, że jego udział w przygotowaniu postępowania o udzielenie zamówienia nie zakłóci konkurencji.
7. Zamawiający może wykluczyć Wykonawcę na każdym etapie postępowania o udzielenie zamówienia.

§ 10

WYKAZ OŚWIADCZEŃ LUB DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW DO WYKLUCZENIA

1. Wykaz oświadczeń, składanych przez Wykonawcę wraz z ofertą, w celu wstępnego potwierdzenia, że nie podlega on wykluczeniu oraz spełnia warunki udziału w postępowaniu:

- 1) Aktualny na dzień składania ofert Jednolity Europejski Dokument Zamówienia, sporządzony zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji Europejskiej, wydanym na podstawie art. 59 ust. 2 dyrektywy 2014/24/UE oraz art. 80 ust. 3 dyrektywy 2014/25/UE opatrzony kwalifikowanym podpisem elektronicznym. Wykonawca może wykorzystać w JEDZ nadal aktualne informacje zawarte w innym JEDZ, złożonym w odrębnym postępowaniu o udzielenie zamówienia.

UWAGA: Wymaga się złożenia w JEDZ jedynie ogólnego oświadczenia o spełnianiu warunków udziału w postępowaniu, zawartego w Sekcji α Cz. IV: Kryteria kwalifikacji.

- 2) Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu, składa także JEDZ-e dotyczące tych podmiotów.
- 3) W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, JEDZ składa każdy z Wykonawców wspólnie ubiegających się o zamówienie. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia w zakresie, w którym każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

2. JEDZ należy wypełnić przy wykorzystaniu systemu dostępnego poprzez następującą stronę internetową <https://ec.europa.eu/growth/tools-databases/espd/>

W tym celu należy podjąć następujące kroki:

- 1) Ze strony internetowej Zamawiającego na której udostępniony został dokument SIWZ należy pobrać plik w formacie XML o nazwie „JEDZ”,
- 2) Wejść na stronę <https://ec.europa.eu/growth/tools-databases/espd/>,
- 3) Wybrać odpowiednią wersję językową,
- 4) Wybrać opcję „Jestem Wykonawcą” (Uwaga! Powyższą opcję należy również zaznaczyć w przypadku, gdy formularz JEDZ wypełnia podmiot, na którego zasoby powołuje się Wykonawca),

5) Zaimportować pobrany wcześniej plik,

6) Wypełnić formularz,

Podpisać formularz **kwalifikowanym podpisem elektronicznym**. Zaleca się sprawdzenie poprawności podpisu poprzez program open-source „proCertum SmartSign” z aktualnymi certyfikatami.

Uwaga !!!: JEDZ należy złożyć w oryginale tj. sporządzony pod rygorem nieważności w postaci elektronicznej. Zamawiający nie dopuszcza możliwości złożenia skanu JEDZ-a opatrzonego kwalifikowanym podpisem elektronicznym.

3. Przy wypełnianiu formularza JEDZ, Wykonawca może skorzystać z instrukcji jego wypełniania, zamieszczonej przez Urząd Zamówień Publicznych na stronie internetowej pod adresem: https://www.uzp.gov.pl/_data/assets/pdf_file/0015/32415/Jednolity-Europejski-Dokument-Zamowienia-instrukcja.pdf.
4. Zamawiający, przed udzieleniem zamówienia, wezwie Wykonawcę, którego oferta została oceniona najwyżej, do złożenia w wyznaczonym, nie krótszym niż 10 dni, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów, potwierdzających okoliczności, o których mowa w art. 25 ust. 1 uPzp.
5. **Wykaz oświadczeń lub dokumentów, składanych przez Wykonawcę, którego oferta została najwyżej oceniona w postępowaniu, na wezwanie Zamawiającego w celu potwierdzenia okoliczności, o których mowa w § 9 ust. 1 SIWZ:**
 - 1) Wykaz dostaw wykonanych, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania, wymaganego poziomu SLA i podmiotów, na rzecz których usługi zostały wykonane, oraz załączeniem dowodów określających czy te usługi zostały wykonane należyte, przy czym dowodami o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego usługi były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze Wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie Wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert.
6. **Wykaz oświadczeń lub dokumentów, składanych przez Wykonawcę, którego oferta została najwyżej oceniona w postępowaniu, na wezwanie Zamawiającego w celu potwierdzenia okoliczności, o których mowa w § 9 ust. 2 SIWZ:**
 - 1) informacja z Krajowego Rejestru Karnego w zakresie określonym w § 9 ust. 2 pkt 2), 3) i 10), wystawionej nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
 - 2) oświadczenia Wykonawcy o braku wydania wobec niego prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne albo – w przypadku wydania takiego wyroku lub decyzji – dokumentów potwierdzających dokonanie płatności tych należności wraz z ewentualnymi odsetkami lub grzywnami lub zawarcie wiążącego porozumienia w sprawie spłat tych należności w zakresie określonym w § 9 ust. 2 pkt 4) SIWZ, (wzór Oświadczenia - załącznik nr 4 do SIWZ),

- 3) oświadczenia Wykonawcy o braku orzeczenia wobec niego tytułem środka zapobiegawczego zakazu ubiegania się o zamówienia publiczne w zakresie określonym w § 9 ust. 2 pkt 11) SIWZ (wzór Oświadczenia - załącznik nr 5 do SIWZ).
7. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, na wezwanie Zamawiającego - zamiast dokumentów, o których mowa w ust. 7 pkt 1) - składa informację z odpowiedniego rejestru albo - w przypadku braku takiego rejestru, - inny równoważny dokument, wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dotyczy informacja albo dokument, w zakresie określonym w § 9 ust. 2 pkt 2), 3) i 10) SIWZ.
8. Dokument, o którym mowa w ust. 8, powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
9. Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentu, o którym mowa w ust. 6 zastępuje się go dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Dokument, o którym mowa powyżej, powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
10. Wykonawca mający siedzibę na terytorium Rzeczypospolitej Polskiej, w odniesieniu do osoby mającej miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, której dotyczy dokument wskazany w ust. 6 pkt 1), składa dokument, o którym mowa w ust. 7, w zakresie określonym w § 9 ust. 2 pkt 3) i 10). Jeżeli w kraju, w którym miejsce zamieszkania ma osoba, której dokument miał dotyczyć, nie wydaje się takich dokumentów, zastępuje się go dokumentem zawierającym oświadczenie tej osoby złożonym przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na miejsce zamieszkania tej osoby. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
11. Wykonawca w stosownych sytuacjach może - w celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w § 9 ust. 1 - polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych, na zasadach określonych w art. 22a uPzp. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia.
12. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.
13. Zamawiający żąda od Wykonawcy, który polega na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a uPzp, przedstawienia w odniesieniu do tych podmiotów dokumentów wymienionych w ust. 6 pkt 1) – 3).
14. Wykonawca może wskazać oświadczenia lub dokumenty, o których mowa w ust. 7, 8, 9, 10, 11 które znajdują się w posiadaniu Zamawiającego, w celu potwierdzenia okoliczności, o których mowa w § 9 ust. 1, 2 i 3.

15. W przypadku wskazania przez Wykonawcę dostępności oświadczeń lub dokumentów, o których mowa w ust. 7, 8, 9, 10, 11, w formie elektronicznej pod określonymi adresami internetowymi ogólnodostępnych i bezpłatnych baz danych, Zamawiający pobiera samodzielnie z tych baz danych wskazane przez Wykonawcę oświadczenia lub dokumenty.
16. Oświadczenia i dokumenty, o których mowa w § 10, **z wyjątkiem JEDZ**, dotyczące Wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega Wykonawca na zasadach określonych w art. 22a uPzp oraz dotyczące podwykonawców, składane są w **oryginale tj. w postaci dokumentu elektronicznego lub w elektronicznej kopii oświadczenia poświadczonej za zgodność z oryginałem**.
17. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.
18. **Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej Zamawiającego informacji, o której mowa w art. 86 ust. 5 uPzp, przekazuje Zamawiającemu w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii oświadczenia poświadczonej za zgodność z oryginałem, oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 uPzp. Wraz ze złożeniem oświadczenia, Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia publicznego (wzór oświadczenia stanowi załącznik nr 6 do SIWZ).**
19. W zakresie nieuregulowanym w SIWZ, zastosowanie mają postanowienia Rozporządzenia Ministra Rozwoju z dnia 27 lipca 2016 r., w sprawie rodzajów dokumentów, jakich może żądać Zamawiający od Wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r. poz. 1126 ze zmianami) oraz Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych (Dz. U. z 2017r. poz. 1320 ze zmianami).

§ 11

INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ LUB DOKUMENTÓW. WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. W niniejszym postępowaniu, komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu formularzy do komunikacji udostępnionych przez miniPortal <https://miniportal.uzp.gov.pl/> i dostępnych na ePUAP <https://epuap.gov.pl/wps/portal>, oraz przy użyciu poczty elektronicznej sekretariat@lpr.com.pl lub dzp@lpr.com.pl.
2. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
3. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP.
4. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty lub wniosku oraz do komunikacji wynosi 150 MB.

5. Za datę przekazania oferty, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
6. Wykonawca składa ofertę za pośrednictwem *Formularza do złożenia, zmiany, wycofania oferty lub wniosku* dostępnego na ePUAP i udostępnionego również na miniPortalu. **Klucz publiczny niezbędny do zaszyfrowania oferty przez Wykonawcę jest dostępny dla wykonawców na miniPortalu oraz stanowi załącznik nr 8 do SIWZ.** W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.
7. **Oferta powinna być sporządzona w języku polskim, z zachowaniem postaci elektronicznej w formacie danych doc, docx i podpisana kwalifikowanym podpisem elektronicznym.** Sposób złożenia oferty, w tym zaszyfrowania oferty opisany został w Regulaminie korzystania z miniPortal. Zaleca się sprawdzenie poprawności podpisu poprzez program open-source „proCertum SmartSign” z aktualnymi certyfikatami.

Uwaga !!!: Ofertę należy złożyć w oryginale tj. sporządzonej pod rygorem nieważności w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym. Zamawiający nie dopuszcza możliwości złożenia skanu oferty opatrzonej kwalifikowanym podpisem elektronicznym.

8. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa” a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP).
9. Do oferty należy dołączyć JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
10. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem *Formularza do złożenia, zmiany, wycofania oferty lub wniosku* dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu
11. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
12. Do oferty należy dołączyć JEDZ w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
13. W postępowaniu o udzielenie zamówienia komunikacja pomiędzy Zamawiającym a Wykonawcami w szczególności składanie oświadczeń, wniosków (**innych niż oferta i JEDZ**), zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem *dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji).*
14. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem postępowania nadanym przez Zamawiającego lub/i tytułem postępowania lub/i numerem ogłoszenia TED lub/i ID postępowania.
15. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem *Formularza do komunikacji* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń

lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na wskazany w ust. 16 adres email. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie *użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych* oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie *rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia*.

16. Wykonawca może się kontaktować z Zamawiającym:
 - 1) numer telefonu: +48 (22) 22 99 931,
 - 2) adres poczty elektronicznej: sekretariat@lpr.com.pl, dzp@lpr.com.pl
17. Osobą uprawnioną do kontaktów z Wykonawcami jest:
 - 1) w sprawach merytorycznych – Pan Paweł Bąkała;
 - 2) w sprawach proceduralnych – Pan Artur Lisowski;
18. Wykonawca może zwrócić się do Zamawiającego z prośbą o wyjaśnienie treści niniejszej SIWZ. Zamawiający udzieli niezwłocznie wyjaśnień, jednak nie później niż na 6 dni przed terminem składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu składania wniosku lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku.

§ 12

WYMAGANIA DOTYCZĄCE WADIUM

1. Wykonawca jest zobowiązany wnieść wadium do dnia **5 grudnia 2018 r. do godz. 12³⁰** w wysokości **96 000,00 zł** (słownie: dziewięćdziesiąt sześć tysięcy złotych 00/100).
2. Forma wpłaty wadium:
 - 1) Wadium może być wnoszone w:
 - a) pieniądzu, płatne na konto 36 1130 1017 0020 1459 3620 0008 w banku BGK S.A.,
 - b) poleceniach bankowych lub poleceniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że polecenie kasy jest zawsze poleceniem pieniężnym,
 - c) gwarancjach bankowych,
 - d) gwarancjach ubezpieczeniowych,
 - e) poleceniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt. 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (tekst jednolity Dz. U. z 2018 r. poz. 110).
 - 2) Wadium wnoszone w pieniądzu uważa się za wniesione skutecznie wówczas, gdy przed upływem terminu określonego w § 12 ust. 1 nastąpi uznanie na rachunku Zamawiającego.
 - 3) **W przypadku wnoszenia wadium w formach niepieniężnych, Zamawiający wymaga złożenia dokumentu w formie elektronicznej na zasadach określonych w § 11 SIWZ – z zastrzeżeniem, iż będzie on podpisany kwalifikowanym podpisem elektronicznym przez Gwaranta tj. wystawcę gwarancji/polecenia.** Gwarancję/polecenie, o którym mowa w zdaniu poprzednim, należy dołączyć do oferty, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).

- 4) Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy wskazany w ust. 2 pkt 1) lit. a).
- 5) W przypadku składania przez Wykonawcę wadium w formie gwarancji lub poręczenia niepieniężnego, gwarancja lub poręczenie powinno być sporządzone zgodnie z obowiązującym prawem i winno zawierać następujące elementy:
 - a) nazwę dającego zlecenie (Wykonawcy), beneficjenta gwarancji lub poręczenia (Zamawiającego), gwaranta (banku lub instytucji ubezpieczeniowej udzielających gwarancji lub podmiotu udzielającego poręczenia) oraz wskazanie ich siedziby, nr referencyjny nadany sprawie przez Zamawiającego, nazwę zamówienia;
 - b) określenie wierzytelności, którą ma być zabezpieczona gwarancją lub poręczeniem;
 - c) kwotę gwarancji lub poręczenia;
 - d) termin ważności gwarancji lub poręczenia;
 - e) bezwarunkowe i nieodwołalne zobowiązanie gwaranta do zapłacenia kwoty gwarancji lub poręczenia na pierwsze pisemne żądanie Zamawiającego (nie później niż w ciągu 30 dni od daty zgłoszenia żądania), w przypadku zaistnienia okoliczności wymienionych w art. 46 ust. 4 a i art. 46 ust. 5 uPzp.
- 6) Zwrot bądź zatrzymanie wadium nastąpi zgodnie z art. 46 uPzp.

§ 13

TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą przez 60 dni.
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. Wykonawca (samodzielnie lub na wniosek Zamawiającego) może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy w sprawie zamówienia publicznego, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawcy o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.
4. Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą. Jeżeli przedłużenie terminu związania ofertą dokonywane jest po wyborze oferty najkorzystniejszej, obowiązek wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie Wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

§ 14

OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Oferta winna zawierać:
 - 1) wypełniony i podpisany **Formularz ofertowy (załącznik nr 1 do SIWZ)**,
 - 2) jednolite dokumenty, o których mowa w §10 ust. 1,
 - 3) dokument potwierdzający umocowanie osoby/osób podpisujących ofertę ;oraz
 - 4) w przypadku, gdy Wykonawca polega na zdolnościach lub sytuacji innych podmiotów – zobowiązanie podmiotu trzeciego, o którym mowa w § 10 ust. 12 SIWZ,
 - 5) w przypadku oferty składanej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia – oryginał pełnomocnictwa, w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym osoby upoważnionej do udzielenia pełnomocnictwa, które musi zawierać w szczególności wskazanie: oznaczenia

postępowania o zamówienie publiczne, którego dotyczy; Wykonawców ubiegających się wspólnie o udzielenie zamówienia publicznego; ustanowionego pełnomocnika oraz zakres jego umocowania.

- 6) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik - oryginał pełnomocnictwa, w formie dokumentu elektronicznego opatrzonego kwalifikowanym podpisem elektronicznym osoby upoważnionej do udzielenia pełnomocnictwa, – określający jego zakres. Pełnomocnik posługujący się pełnomocnictwem ma obowiązek złożyć - wraz pełnomocnictwem - dokument, z którego wynika uprawnienie osób, które udzieliły pełnomocnictwa, do reprezentowania Wykonawcy udzielającego pełnomocnictwa.
2. Wykonawca winien dokładnie zapoznać się ze wszystkimi zapisami SIWZ. Zaleca się, aby Wykonawca zdobył wszelkie informacje, które mogą być konieczne do przygotowania oferty oraz podpisania umowy.
3. Treść oferty musi odpowiadać treści SIWZ i być zgodna z powszechnie obowiązującymi przepisami prawa.
4. Wykonawca może złożyć tylko jedną ofertę - pod rygorem odrzucenia, z zastrzeżeniem § 4 SIWZ.
5. Zamawiający dopuszcza złożenie oferty na formularzach sporządzonych przez Wykonawcę, pod warunkiem, że ich treść, a także opis kolumn i wierszy, odpowiadać będą formularzom określonym przez Zamawiającego.
6. Wykonawca poniesie wszystkie koszty związane z przygotowaniem i złożeniem oferty.
7. W celu przeliczenia na PLN wartości i danych finansowych podanych w innych walutach, w oświadczeniach i dokumentach, których złożenia żądał Zamawiający w § 10 SIWZ, Zamawiający zastosuje średni kurs Narodowego Banku Polskiego (NBP) aktualny na dzień publikacji ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej, ogłaszany w sposób przewidziany w § 8 uchwały Zarządu NBP nr 51/2002 z dnia 23 września 2002 roku w sprawie sposobu wyliczania i ogłaszania bieżących kursów walutowych (Dz. Urz. NBP. z dnia 29 września 2002 roku z późn. zm.).

§ 15

MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT

1. Termin składania ofert upływa **dnia 5 grudnia 2018 r. o godzinie 12³⁰**.
2. Otwarcie ofert odbędzie się, w obecności Wykonawców, którzy zechcą przybyć do siedziby Zamawiającego **w dniu 5 grudnia 2018 r. o godz. 13⁰⁰**.
3. Otwarcie ofert następuje poprzez użycie aplikacji do szyfrowania ofert dostępnej na miniPortalu i dokonywane jest poprzez odszyfrowanie i otwarcie ofert za pomocą klucza prywatnego.
4. Bezpośrednio przed otwarciem ofert, Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Podczas otwarcia ofert, Zamawiający poda nazwy (firmy) oraz adresy Wykonawców, a także informacje dotyczące ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
6. Niezwłocznie po otwarciu ofert, Zamawiający zamieści na swojej stronie internetowej www.lpr.com.pl informacje, dotyczące:
 - a) kwoty, jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
 - b) firm oraz adresów Wykonawców, którzy złożyli oferty w terminie,
 - c) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.

§ 16

OPIS SPOSOBU OBLICZENIA CENY

1. Cenę oferty należy określić w złotych polskich (PLN) z dokładnością do dwóch miejsc po przecinku.
2. Ilekcć mowa o cenie, należy przez to rozumieć cenę w rozumieniu art. 3 ust. 1 pkt 1 i ust. 2 ustawy z dnia 9 maja 2014 r. o informowaniu o cenach towarów i usług (tekst jednolity Dz. U. z 2017 r. poz. 1830).
3. Cena, podana przez Wykonawcę w Formularzu ofertowym (**załącznik nr 1 do SIWZ**), musi być całkowitą ceną brutto za wykonanie zamówienia.
4. Cena powinna zawierać w sobie ewentualne upusty proponowane przez Wykonawcę.
5. Cena podana przez Wykonawcę nie będzie podlegać żadnym negocjacjom.
6. Cena podana przez Wykonawcę musi zawierać wszelkie koszty związane z realizacją zamówienia i obowiązywać będzie przez cały okres związania ofertą.
7. Wykonawca sporządzając ofertę powinien określić ceny w sposób rzetelny, tj. w taki, żeby wybór jego oferty gwarantował Zamawiającemu realizację zamówienia.
8. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający - w celu oceny takiej oferty - dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

§ 17

INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Rozliczenia, prowadzone między Zamawiającym a Wykonawcą, będą prowadzone w PLN.

§ 18

OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY

1. Kryteriami oceny ofert, ze wskazaniem procentowego znaczenia tych kryteriów, są:

Lp.	Kryterium	Ranga
1.	Cena brutto oferty	90
2.	Poziom SLA obliczany miesięcznie	10
Razem		100

Oferty zostaną ocenione za pomocą systemu punktowego, zgodnie z poniższymi kryteriami:

- 1) W kryterium nr 1 – **Cena brutto oferty**, maksymalną liczbę punktów otrzyma oferta z najniższą ceną brutto, natomiast pozostałe oferty otrzymają punkty wynikające z arytmetycznych przeliczeń, zgodnie z poniższym wzorem:

$$C = \frac{C_{\min}}{C_{ob}} \times R$$

gdzie: C – liczba punktów przyznanych Wykonawcy w kryterium Cena brutto oferty

C_{min} – najniższa zaoferowana Cena brutto oferty

C_{ob} – Cena brutto oferty zaoferowana w badanej ofercie

R – ranga

- 2) W kryterium nr 2 – Poziom SLA rozliczany miesięcznie oferty otrzymają punkty zgodnie z zaoferowanym poziomem SLA. Oferta Wykonawcy który zaoferuje:
 - a) SLA na poziomie 99,95% obliczane miesięcznie – otrzyma 0 pkt;
 - b) SLA na poziomie 99,96% obliczane miesięcznie – otrzyma 2,50 pkt;
 - c) SLA na poziomie 99,97% obliczane miesięcznie – otrzyma 5,00 pkt;
 - d) SLA na poziomie 99,98% obliczane miesięcznie – otrzyma 7,50 pkt;
 - e) SLA na poziomie 99,99% lub wyższe obliczane miesięcznie – otrzyma 10,00 pkt
2. W trakcie dokonywania obliczeń Zamawiający zaokrągli każdy z wyników do dwóch miejsc po przecinku.
3. Maksymalna ilość punktów, jaką Wykonawca może uzyskać w wyniku oceny według ww. kryteriów wynosi 100 pkt.
4. Oferta, która otrzyma najwyższą liczbę punktów, zostanie przedstawiona jako oferta najkorzystniejsza.

§ 19

INFORMACJE DOTYCZĄCE AUKCJI ELEKTRONICZNEJ

Zamawiający nie przewiduje w niniejszym postępowaniu wyboru najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej.

§ 20

INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Po wyborze najkorzystniejszej oferty, a przed zawarciem umowy, Zamawiający wezwie Wykonawcę, którego oferta została wybrana, do dopełnienia następujących formalności:
 - 1) osoby reprezentujące Wykonawcę, przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie wynika z dokumentów załączonych do oferty,
 - 2) jeżeli wybrana zostanie oferta Wykonawców występujących wspólnie, będą oni zobowiązani, przed zawarciem umowy w sprawie udzielenia zamówienia, do przedstawienia umowy regulującej współpracę tych Wykonawców,
2. Niezłożenie dokumentów, o których mowa w ust. 1 pkt 1) - 3), przez Wykonawcę, którego oferta została wybrana, w wyznaczonym przez Zamawiającego terminie przed podpisaniem umowy, Zamawiający potraktuje jako uchylanie się od zawarcia umowy w sprawie zamówienia publicznego. W takim przypadku, zgodnie z art. 94 ust. 3 uPzp, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert - bez przeprowadzania ich ponownego badania i oceny (chyba że zachodzą przesłanki unieważnienia postępowania, o których mowa w art. 93 ust. 1 uPzp).

§ 21

WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

1. Wykonawca przed podpisaniem umowy zobowiązany jest do wniesienia zabezpieczenia należytego wykonania umowy na sumę stanowiącą 10 % wartości brutto Umowy, w jednej lub kilku następujących formach (w zależności od wyboru Wykonawcy):
 - 1) pieniądzu, wpłaconym przelewem na konto: 36 1130 1017 0020 1459 3620 0008 w banku BGK S.A.
 - 2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym, że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym.
 - 3) gwarancjach bankowych.
 - 4) gwarancjach ubezpieczeniowych.
 - 5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6 ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.
2. W przypadku wnoszenia zabezpieczenia należytego wykonania umowy w formie gwarancji bankowej lub ubezpieczeniowej, gwarancja ta powinna być nieodwołalna, bezwarunkowa i płatna na pierwsze żądanie Zamawiającego. Zobowiązanie wynikające dla banku/ubezpieczyciela udzielającego takiej gwarancji pozostaje dla niego wiążące przez okres wykonywania Umowy, przedłużony o okres 30 dni.
3. Wniesienie przez Wykonawcę zabezpieczenia należytego wykonania umowy w formie weksli z poręczeniem wekslowym banku lub spółdzielczej kasy oszczędnościowo-kredytowej, ustanowienia zastawu na papierach wartościowych emitowanych przez Skarb Państwa lub jednostkę samorządu terytorialnego, ustanowienia zastawu rejestrowego na zasadach określonych w przepisach o zastawie rejestrowym i rejestrze zastawów wymaga dla swej skuteczności wcześniejszej zgody Zamawiającego.
4. W przypadku wniesienia zabezpieczenia należytego wykonania umowy w pieniądzu odpowiednia kwota powinna zostać przelana na konto Zamawiającego – wskazane w ust. 1 pkt 1) wraz z podaniem nr postępowania. Wniesienie zabezpieczenia należytego wykonania umowy jest skuteczne z chwilą uznania na rachunku Zamawiającego.
5. Kopię dowodu wniesienia zabezpieczenia należytego wykonania umowy należy przedstawić Zamawiającemu przed podpisaniem umowy. W wypadku zabezpieczenia należytego wykonania umowy w formie innej niż pieniężna Wykonawca przedstawi Zamawiającemu kopię dokumentu zabezpieczenia należytego wykonania umowy poświadczoną za zgodność z oryginałem przez Wykonawcę lub upoważnionego przedstawiciela Wykonawcy przed podpisaniem umowy. Koniecznym jest zdeponowanie oryginału dokumentu zabezpieczenia należytego wykonania umowy przed podpisaniem umowy w siedzibie Zamawiającego: Lotnicze Pogotowie Ratunkowe w Warszawie, ul. Księżycowa 5, pokój 100.

§ 22

ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Istotne postanowienia umowy dla poszczególnych zadań stanowią załączniki nr 3 do SIWZ.
2. Zgodnie z art. 144 ust. 1 uPzp, Zamawiający przewiduje możliwość dokonania istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, na warunkach i w zakresie określonym w **załącznikach nr 3 do SIWZ** – Istotne postanowienia umowy.

§ 23

POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów uPzp, przysługują środki ochrony prawnej przewidziane w Dziale VI uPzp, na zasadach i w terminach określonych dla wartości zamówienia równej lub przekraczającej kwoty, określone w przepisach wydanych na podstawie art. 11 ust. 8 uPzp.

Środkami ochrony prawnej są:

- 1) odwołanie,
- 2) skarga do sądu.

Kwestie dotyczące odwołania uregulowane są w art. 180-198 uPzp.

Na orzeczenie Krajowej Izby Odwoławczej, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Kwestie dotyczące skargi do sądu regulowane są w art. 198a-198g uPzp.

§ 24

INFORMACJE DOTYCZĄCE RODO

1. Zamawiający informuje, że na swojej stronie internetowej pod adresem: <https://www.lpr.com.pl/pl/rodo/> zamieścił Klauzulę Informacyjną o Przetwarzaniu Danych Osobowych.
2. Obowiązkiem Wykonawcy jest zapoznanie się z treścią Klauzuli oraz złożenie odpowiedniego oświadczenia zawartego w Formularzu oferty – załącznik nr 1 do SIWZ.

§ 25

ZAŁĄCZNIKI DO SIWZ

1. Formularz ofertowy – załącznik nr 1;
2. Opis przedmiotu zamówienia – załącznik nr 2;
3. Istotne postanowienia umowy – załączniki nr 3;
4. Oświadczenie Wykonawcy o braku podstaw do wykluczenia – załącznik nr 4;
5. Oświadczenie Wykonawcy o braku podstaw do wykluczenia – załącznik nr 5;
6. Informacja o przynależności wykonawcy do grupy kapitałowej – załącznik nr 6;
7. Wzór wykazu zrealizowanych usług – załącznik nr 7;
8. Klucz publiczny niezbędny do zaszyfrowania oferty – załącznik nr 8.

Radca Prawny
Marian Trzaskowski
WA-267/19

ZAŁĄCZNIK NR 1 DO SIWZ

FORMULARZ OFERTOWY

....., dnia

I. INFORMACJE O WYKONAWCY

1. Niniejsza oferta zostaje złożona przez:

.....
.....
.....
.....

adres Wykonawcy (siedziba)

NIP REGON

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy)

tel. fax

e-mail www (jeżeli posiada)

województwo powiat

w przypadku oferty wspólnej (Konsorcjum)¹:

Pełnomocnik Konsorcjum:

nazwa Wykonawcy

.....
.....

adres Wykonawcy (siedziba)

NIP REGON

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy)

tel. fax

e-mail www (jeżeli posiada)

skrzynka ePuap

województwo powiat

Uczestnik Konsorcjum:

nazwa Wykonawcy

.....
.....

¹ Należy podać nazwy i adresy wszystkich Wykonawców wskazując również Pełnomocnika

adres Wykonawcy (siedziba)

NIP REGON

Nr Krajowego Rejestru Sądowego (jeżeli dotyczy)

tel. fax

e-mail www (jeżeli posiada)

skrzynka ePuap

województwo powiat

2. Wszelką korespondencję w sprawie niniejszego postępowania należy kierować na adres:

.....
nazwa
.....

numer telefonu:

numer faksu:

adres poczty elektronicznej:

skrzynka ePuap

II. PRZEDMIOT OFERTY

Nawiązując do ogłoszenia o zamówieniu na „Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)” – nr postępowania ZP/8/X/2018, my niżej podpisani składamy ofertę w postępowaniu o zamówienie publiczne i:

1. Oferujemy wykonanie przedmiotu zamówienia w zakresie objętym w Specyfikacji Istotnych Warunków Zamówienia (SIWZ):

za cenę całkowitą brutto PLN w tym podatek VAT w wysokości %, zgodnie z poniższym formularzem cenowym:

L.p	Opis	Ilość	Cena jednostkowa brutto	Wartość ogólna brutto	VAT [%]
A	B	C	D	$E = C \times D$	F
1.	Usługi utrzymaniowe	12 miesięcy	 zł / 1 miesiąc		
2.	Usługi rekonfiguracyjne	5000 godzin	 zł / 1 godzina		
SUMA					

2. Zobowiązujemy się do zapewnienia SLA rozliczany miesięcznie na poziomie* (nie mniej 99,95%) – kryterium oceny ofert opisane w § 18 ust. 1 pkt 2 SIWZ.

* - w przypadku niewypełnienia przez Wykonawcę, Zamawiający przyjmie że Wykonawca oferuje minimalny wymagany poziom SLA – 99,95%.

3. Oświadczamy, że²:

- ☐ wybór naszej oferty nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego
☐ wybór naszej oferty prowadził będzie do powstania u Zamawiającego obowiązku podatkowego:

.....
nazwa (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do powstania obowiązku podatkowego, wartość bez kwoty podatku.

4. Oświadczamy, że zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (wraz z załącznikami stanowiącymi jej integralną część, w tym w szczególności opis przedmiotu zamówienia) oraz wyjaśnieniami i zmianami SIWZ przekazanymi przez Zamawiającego i uznajemy się za związanych określonymi w niej postanowieniami i zasadami postępowania.
5. Oświadczamy, że zapoznaliśmy się z Istotnymi postanowieniami umowy, które stanowią załącznik nr 3 do SIWZ (odpowiednio dla każdego z zadań) i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy na określonych w tym załączniku warunkach, w miejscu i terminie wyznaczonym przez Zamawiającego.
6. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO³ wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.⁴
Jednocześnie przyjmujemy do wiadomości, że szczegółowe informacje dotyczące RODO znajdują się na stronie internetowej Zamawiającego pod adresem: <https://www.lpr.com.pl/pl/rodo/>
7. Osoby uprawnione do kontaktowania się w sprawach wykonania przedmiotu umowy ze strony Wykonawcy: p., tel., e-mail

8. Oświadczamy, że powierzymy podwykonawcom część zamówienia:

Część zamówienia	Nazwa (firma) podwykonawcy

² Odpowiednie zaznaczyć

³ 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).

⁴ W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).

9. Uważamy się za związanych niniejszą ofertą na czas wskazany w Specyfikacji Istotnych Warunków Zamówienia, czyli przez okres 60 dni od upływu terminu składania ofert.

10. Wadium zostało wniesione w formie

11. Prosimy o zwrot wadium (wniesionego w pieniądzu), na zasadach określonych w art. 46 uPzp, na następujący rachunek bankowy⁵

12. Oświadczamy, że na podstawie art. 8 ust. 3 uPzp⁶:

- ☐ żadne z informacji zawartych w ofercie oraz załączonych do niej dokumentach, nie stanowią tajemnicy przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji,
- ☐ wskazane poniżej informacje zawarte w ofercie oraz załączonych do niej dokumentach, stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji i w związku z niniejszym nie mogą być one udostępniane, w szczególności innym uczestnikom postępowania.

Lp.	Oznaczenie rodzaju (nazwy) informacji	Strony w ofercie (wyrażone cyfrą)	
		od	do

Uwaga! W przypadku braku wykazania (złożenia właściwego uzasadnienia w terminie składania ofert), iż zastrzeżone dane stanowią tajemnicę przedsiębiorstwa, Zamawiający uzna, iż nie została spełniona przesłanka podjęcia niezbędnych działań w celu zachowania ich poufności i dane te staną się jawne od momentu otwarcia ofert.

13. Niniejszym potwierdzam załączenie do oferty następujących dokumentów:

(numerowany wykaz załączników wraz z tytułami)

- 1) Załącznik nr
- 2) Załącznik nr
- 3) Załącznik nr

.....
Podpis (y) Wykonawcy (ów) lub
upoważnionego(ych) przedstawiciela(li)
Wykonawcy(ów)

⁵ Jeżeli dotyczy

⁶ Niepotrzebne skreślić

ZAŁĄCZNIK NR 4 DO SIWZ

Zamawiający:

Lotnicze Pogotowie Ratunkowe

ul. Książkowa 5, 01-934 Warszawa

WYKONAWCA:

.....
(Firma, adres)

OŚWIADCZENIE WYKONAWCY

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)” (nr postępowania ZP/8/X/2018) prowadzonego przez Lotnicze Pogotowie Ratunkowe, oświadczamy, że wobec podmiotu, który reprezentujemy:

- ☐ **nie wydano** prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne.
- ☐ **wydano** prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczaniem podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne.⁷

..... (miejscowość), dnia

.....
Podpis (y) Wykonawcy (ów)
lub upoważnionego(ych) przedstawiciela(li)
Wykonawcy(ów)

⁷ Odpowiednie zaznaczyć

ZAŁĄCZNIK NR 5 DO SIWZ

Zamawiający

Lotnicze Pogotowie Ratunkowe

ul. Książkowa 5, 01-934 Warszawa

WYKONAWCA

.....
(Firma, adres)

OŚWIADCZENIE WYKONAWCY

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)” (nr postępowania ZP/8/X/2018), prowadzonego przez Lotnicze Pogotowie Ratunkowe, oświadczamy, że wobec podmiotu, który reprezentujemy, **nie orzeczono/orzeczono**⁸ tytułem środka zapobiegawczego zakazu/zakaz ubiegania się o zamówienia publiczne.

..... (miejscowość), dnia

.....
Podpis (y) Wykonawcy (ów)
lub upoważnionego(ych)
przedstawiciela(li) Wykonawcy(ów)

⁸ Niepotrzebne skreślić

ZAŁĄCZNIK NR 6 DO SIWZ

Zamawiający

Lotnicze Pogotowie Ratunkowe

ul. Księżycowa 5, 01-934 Warszawa

WYKONAWCA

.....
(Firma, adres)

INFORMACJA O PRZYNALEŻNOŚCI LUB BRAKU PRZYNALEŻNOŚCI WYKONAWCY DO GRUPY KAPITAŁOWEJ

Na podstawie art. 24 ust. 11 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych oświadczam, że: **należę / nie należę*** do tej samej grupy kapitałowej z Wykonawcami którzy złożyli odrębne oferty, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jednolity Dz. U. z 2017 r. poz. 229 z późn. zm.) w postępowaniu pn. **„Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)”** (nr postępowania ZP/8/X/2018).

....., dnia

.....
Podpis (y) Wykonawcy (ów) lub upoważnionego(ych)
przedstawiciela(li) Wykonawcy(ów)

* *niepotrzebne skreślić*

W przypadku, gdy Wykonawca **należy** do tej samej grupy kapitałowej, wraz ze złożeniem oświadczenia Wykonawca może przedstawić dowody, że powiązania z innym Wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.

ZAŁĄCZNIK NR 7 DO SIWZ

WYKAZ USŁUG

Lp.	Przedmiot zamówienia	Wartość wykonanej usługi w PLN netto **	Data wykonania zamówienia		Wymagany poziom SLA obliczany miesięcznie	Nazwa i adres odbiorcy- Zleceniodawcy
			początek (data)	zakończenie (data)		
1	2	3	4			5
1.						
2.						

Oświadczam/y* że:

poz. wykazu stanowi zdolność techniczną lub zawodową Wykonawcy składającego ofertę.

poz. wykazu jest zdolnością techniczną lub zawodową oddaną do dyspozycji przez inny/inne* podmiot/y*.

** Zgodnie z § 14 ust. 16 SIWZ: W celu przeliczenia na PLN wartości i danych finansowych podanych w innych walutach, w oświadczeniach i dokumentach, których złożenia żądał Zamawiający w § 10 SIWZ, Zamawiający zastosuje średni kurs Narodowego Banku Polskiego (NBP) aktualny na dzień publikacji ogłoszenia o zamówieniu w Dzienniku Urzędowym Unii Europejskiej, ogłaszany w sposób przewidziany w § 8 uchwały Zarządu NBP nr 51/2002 z dnia 23 września 2002 roku w sprawie sposobu wyliczania i ogłaszania bieżących kursów walutowych (Dz. Urz. NBP. z dnia 29 września 2002 roku z późn. zm.).

..... dn.

.....

Podpis (y) Wykonawcy (ów)
lub upoważnionego(ych)
przedstawiciela(i) Wykonawcy(ów)



LOTNICZE POGOTOWIE RATUNKOWE

CENTRALA

ul. Książycowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

ZAŁĄCZNIK NR 3 DO SIWZ ISTOTNE POSTANOWIENIA UMOWY

zawarta dnia r. w Warszawie, zwana dalej „Umową”, pomiędzy :

Lotniczym Pogotowiem Ratunkowym z siedzibą w Warszawie przy ul. Książycowej 5, kod 01-934 Warszawa wpisanym do Krajowego Rejestru Sądowego Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji i Publicznych Zakładów Opieki Zdrowotnej pod nr 0000144355, prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego, REGON 016321074, NIP 522-25-48-391
zwanym dalej „Zamawiającym”,
reprezentowanym przez: Dyrektora - Roberta Gałązkowskiego,

a

..... z siedzibą w przy ul., wpisaną do Rejestru Przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd ,pod numerem KRS, NIP:, REGON:,

zwanym dalej „Wykonawcą”

zwanym dalej łącznie „Stronami” lub każdą z osobna „Stroną,”

o następującej treści:

PREAMBUŁA

Niniejsza umowa zostaje zawarta w rezultacie przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na podstawie ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 roku (t.j. Dz. U. z 2018 r., poz. 1986), którego przedmiotem jest „Świadczenie usług utrzymaniowych oraz rekonfiguracyjnych dla Aplikacji Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM)”. Prawa i obowiązki wynikające z niniejszej Umowy należy interpretować w kontekście całości postępowania będącego podstawą zawarcia Umowy.

§ 1

Przedmiot Umowy

1. Przedmiotem niniejszej Umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego następujących usług:
 - 1) utrzymaniowych Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM), stanowiącego moduł Systemu Informatycznego Powiadamiania Ratunkowego,
 - 2) rekonfiguracyjnych Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM),
2. Szczegółowy Opis Przedmiotu Zamówienia stanowi Załącznik nr 1 do niniejszej Umowy.

§ 2

Termin i warunki dostawy

1. Wykonawca zobowiązany jest świadczyć usługi, o których mowa w §1 ust.1 i ust.2 w terminie od dnia podpisania niniejszej Umowy do dnia 31 grudnia 2019 roku, z zastrzeżeniem, iż w przypadku wyczerpania limitu godzin rekonfiguracyjnych, określonych w §4 ust.2 pkt 29) lit. a), Umowa w tym zakresie wygasa z dniem ich maksymalnego wykorzystania.
2. Wykonawca Zobowiązuje się wystąpić na piśmie do Zamawiającego z wnioskiem o nadanie dostępu do Systemu z wykorzystaniem OST 112 (za pośrednictwem szyfrowanego połączenia VPN) w ciągu dwóch dni roboczych od podpisania Umowy.
3. Po uzyskaniu dostępu do Systemu OST 112, Wykonawca, za pośrednictwem szyfrowanego połączenia VPN do 50 dni kalendarzowych, licząc od dnia zapewnienia przez Zamawiającego dostępu do Systemu na poziomie administracyjnym, ma obowiązek zestawzić 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 montażu 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 obsługiwać 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 MS Windows,
 - 10) Urządzenie SSL VPN musi być systemem kompletnym pochodzącym od jednego producenta. Nie dopuszcza się stosowania rozwiązań typu „open source”;
4. 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

Wynagrodzenie

1. Łączne wynagrodzenie należne Wykonawcy z tytułu należytego wykonania przedmiotu Umowy nie przekroczy kwotyzł netto (słownie: ...) plus VAT..., łącznie.....złoty brutto (słownie.....), w tym:
 - 1) maksymalne wynagrodzenie za usługi utrzymaniowe SDW PRM, o których mowa w §1 ust. 1 pkt 1, w wysokości.....;
 - 2) maksymalne wynagrodzenie za usługi rekonfiguracyjne SWD PRM, o których mowa w §1 ust. 1 pkt 2, w wysokości....., przy czym cena za 1 godzinę usługi rekonfiguracyjnej SWD PRM wynosi
2. Wynagrodzenie, o którym mowa w ust. 1 pkt 1, jest wynagrodzeniem ryczałtowym i płatne będzie raz w miesiącu w równych ratach, odpowiadających danemu miesięcznemu okresowi rozliczeniowemu, w kwocie.....(słownie...). Jeżeli okres świadczenia usług nie obejmuje pełnego miesiąca, wówczas ratę wynagrodzenia za ten okres ustala się proporcjonalnie, przyjmując, że za 1 dzień świadczenia usług Wykonawcy należy się wynagrodzenie w wysokości 1/30 kwoty wynagrodzenia określonego w zdaniu pierwszym;
3. Wynagrodzenie, o którym mowa w ust. 1 pkt 2, płatne będzie za usługi faktycznie wykonane i zatwierdzone przez Zamawiającego w drodze podpisania Protokołu Odbioru Zleceń, którego wzór stanowi Załącznik nr 4 do Umowy,
4. Wynagrodzenie, o którym mowa w ust. 1 jest ostateczne i uwzględnia wszelkie koszty i opłaty związane z wykonaniem przedmiotu Umowy, w szczególności podatek od towarów i usług oraz wynagrodzenie za przeniesienie autorskich praw majątkowych, zatem wyczerpuje w całości roszczenia Wykonawcy z tego tytułu.
5. Wynagrodzenie, o którym mowa w ust.1 pkt 1 płatne będzie w terminie 30 dni od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury VAT, wraz z podpisanym przez Strony miesięcznym Protokołem Odbioru Usług, którego wzór stanowi Załącznik nr 3 do Umowy.
6. Wynagrodzenie, o którym mowa w ust.1 pkt 2, płatne będzie w terminie 30 dni od dnia doręczenia Zamawiającemu prawidłowo wystawionej faktury VAT, wraz z podpisanym przez Strony Protokołem Odbioru Zleceń.
7. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy Wykonawcy wskazany na fakturze. Za datę zapłaty wynagrodzenia przyjmuje się datę obciążenia rachunku Zamawiającego.
8. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z realizacji umowy oraz na dokonanie jakiejkolwiek czynności prawnej skutkującej zmianą wierzyciela lub obrotem wierzytelnościami wynikającymi z umowy.

§ 4

Wykonanie przedmiotu Umowy

1. Wykonawca zobowiązany jest do wykonania przedmiotu Umowy na zasadach określonych w ust. 2, 3, 4 i 5 oraz Załączniku Nr 1 do Umowy.
2. Usługi będące przedmiotem niniejszej umowy realizowane będą w następujący sposób:
 - 1) Wykonawca w ramach usługi utrzymaniowej SWD PRM zobowiązuje się do zapewnienia czasu dostępności SWD PRM w pełnej funkcjonalności na poziomie.....nie mniejszym jednak niż % (*zgodnie z ofertą Wykonawcy jednak nie mniej niż 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;
 - 2) 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:
 - a) 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,
 - b) awarią podsystemów nie będących przedmiotem niniejszej umowy w tym:
 - centrum Certyfikatów (PKI),
 - infrastrukturą serwerową,
 - platformą wirtualizacyjną,
 - siecią w obrębie infrastruktury serwerowej,
 - UMM (Uniwersalny Moduł Mapowy)
 - PLI CBD,
 - PZŁ (Podsystem Zintegrowanej Łączności);
 - 3) Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie systemu SWD PRM, zgodnie z SLA
 - 4) Wykonawca zobowiązuje się do utrzymania SWD PRM w następującym zakresie:
 - a) usuwania Awarii mających wpływ na ciągłość działania SWD PRM lub powodujących niedostępność procesów biznesowych zdefiniowanych w Załączniku nr 1 do OPZ,
 - b) Modyfikacji Systemu SWD PRM,
 - c) optymalizacji pod względem wydajności oraz dostępności SWD PRM;
 - 5) 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:
 - a) Awaria Krytyczna,
 - b) Awaria Niekrytyczna,
 - c) Awaria Zwykła;

- 6) 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;
- 7) 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),
- 8) po Modyfikacji Oprogramowania Aplikacyjnego zostanie ono przetestowane, a po pozytywnym wyniku testów objęte serwisem na takich samych zasadach jak całość Oprogramowania Aplikacyjnego SWD PRM. Wzór formularza oceny testów stanowi Załącznik nr 2 do OPZ;
- 9) 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);
- 10) Wykonawca najpóźniej w ciągu dwóch dni roboczych 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);
- 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
- 12) Wykonawca usunie Awarię Krytyczną w terminie zapewniającym dotrzymanie świadczenia usług zgodnie z SLA;
- 13) Wykonawca usunie Awarię Niekrytyczną w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia Awarii Niekrytycznej;
- 14) Wykonawca usunie Awarię Zwykłą w terminie nie dłuższym niż 48 godzin od momentu zgłoszenia Awarii Zwykłej;
- 15) Wykonawca, w przypadku prac planowanych, zgłosi Zamawiającemu zamiar ich prowadzenia z wyprzedzeniem siedmiu dni roboczych. Potwierdzenie wyrażenia zgody lub brak zgody na wykonanie ww. prac powinno nastąpić w terminie dwóch dni roboczych;
- 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;
- 17) świadczenie usługi utrzymania obejmuje również wykonanie przez Wykonawcę wszelkich czynności związanych z przywróceniem pierwotnego stanu Systemu SWD PRM (sprzed Awarii);
- 18) Wykonawca zobowiązuje się do wykonywania obowiązków wynikających ze świadczenia usług utrzymania, o których mowa w niniejszym ustępie, w sposób zapobiegający utracie danych Zamawiającego. 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;
- 19) Zamawiający udostępni Wykonawcy, na potrzeby świadczenia usług, kody źródłowe Oprogramowania Aplikacyjnego oraz wszelką Dokumentację Systemu których jest właścicielem;
 - 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 działający po stronie Zamawiającego;
 - 21) Wykonawca zapewni miesięczne raporty ze współpracy z Zamawiającym w formie wymaganej przez Zamawiającego, w których będą omówione (przedstawione) m.in. poniższe zagadnienia:
 - a) proces usuwania Awarii zgłoszonych Wykonawcy,
 - b) datę usunięcia Awarii,
 - c) szczegółowy opis wprowadzonych zmian i przyjętych rozwiązań wraz ze wskazaniem numeru Incydentu Serwisowego zarejestrowanego w dedykowanym systemie obsługi Incydentów Serwisowych,
 - d) proces wgrywania korekt Oprogramowania,
 - e) datę wdrożenia nowej wersji Oprogramowania,
 - f) numer wersji Oprogramowania,
 - 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;
 - 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 logów SWD PRM wskazujących jednoznacznie na przyczynę Awarii lub wskazujących współpracujący podsystem, który tę Awarię generuje;
 - 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 wraz z Zamawiającym na środowisku SZK SWD PRM;
 - 25) w przypadku konieczności aktualizacji Oprogramowania Standardowego, Wykonawca jest zobowiązany dostosować Aplikację SWD PRM do nowej wersji Oprogramowania Standardowego;
 - 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

- 27) Wykonawca zobowiązuje się do prognozowania obciążenia Infrastruktury Sprzętowej oraz planowania dostępności i pojemności jej elementów, utrzymywanie planów dostępności i pojemności Infrastruktury Sprzętowej, zarządzanie ryzykiem powstania niedostępności elementów Infrastruktury Sprzętowej, która może przełożyć się na niedostępność usług świadczonych w oparciu o tę Infrastrukturę Sprzętową;
- 28) Wykonawca zobowiązuje się do podejmowania działań mających na celu zapobieganie przeciążeniu Infrastruktury Sprzętowej jeśli jest ona spowodowana aplikacją SWD PRM lub jej Modyfikacjami;
- 29) Wymagania w ramach usług rekonfiguracyjnych oraz zasad ich rozliczania są następujące:
 - a) przedmiot Umowy w zakresie rekonfiguracji będzie realizowany w okresie od dnia podpisania Umowy do wyczerpania przyjętego w Umowie limitu godzin (tj. 5000 słownie: pięć tysięcy) lub do dnia zakończenia umowy w zależności od tego, które zdarzenie nastąpi wcześniej. Wykonawcy nie przysługuje roszczenie z tytułu niewykorzystania w okresie obowiązywania Umowy maksymalnej liczby godzin rekonfiguracyjnych,
 - b) Zamawiający przekaze Wykonawcy wstępne Zlecenie określające zakres i sugerowany termin wykonania Zlecenia wraz z niezbędnymi wymogami i parametrami,
 - c) Odbiór Zleceń nastąpi w formie Protokołu Odbioru Zlecenia, podpisanego przez przedstawiciela Zamawiającego i Wykonawcy, po każdym prawidłowo wykonanym Zleceniu,
 - d) protokół Odbioru Zleceń, podpisany bez uwag będzie stanowił podstawę wystawienia faktury przez Wykonawcę i dokonania płatności przez Zamawiającego,
 - e) Wykonawca przyjmuje do wiadomości, że SWD PRM może być rozwijany o kolejne funkcjonalności i nie będzie zgłaszał z tego tytułu zastrzeżeń podczas realizacji kolejnych Zleceń. Rozwój Systemu SWD PRM będzie umożliwiał realizację kolejnych Zleceń na warunkach opisywanych każdorazowo przez Zamawiającego,
 - f) przyjmuje się, że najmniejszą możliwą wielkością Zlecenia będzie 1 godzina,
 - g) w ramach Zleceń Wykonawca wykonywać będzie prace związane z rekonfiguracjami Systemu SWD PRM zgodnie z treścią Zlecenia. Zakres wykonania prac zostanie zdefiniowany każdorazowo przez Zamawiającego,
 - h) Wykonawca realizował będzie konsultacje techniczne dotyczące SWD PRM, w ramach, których ma przedstawić wyniki analizy Zlecenia powierzonego przez Zamawiającego, sposobu rozwiązania, możliwości rozbudowy lub Modyfikacji w celu uzyskania funkcjonalności oczekiwanej przez Zamawiającego,
 - i) Wykonawca będzie dokonywał zmian usprawnień, Modyfikacji SWD PRM i Dokumentacji, wraz z przeniesieniem majątkowych praw autorskich oraz praw zależnych do zmienionego Oprogramowania Aplikacyjnego lub zmodyfikowanej Dokumentacji,
 - j) Wykonawca będzie dokonywał analizy konfiguracji serwerów aplikacyjnych systemu, oraz proponował i wdrażał rozwiązania mające na celu eliminację zidentyfikowanych błędów w celu zwiększenia wydajności SWD PRM,

- k) Wykonawca prowadził będzie analizę środowiska bazodanowego w celu optymalizacji działania oraz zwiększenia dostępności środowiska Systemu SWD PRM, oraz analizę zagrożeń jakie mogą wywołać modyfikacje SWD PRM prowadzone przez Zamawiającego w ramach innych umów,
- l) w ramach planu rozwoju Systemu – Wykonawca przeprowadzi analizę wydajnościową Systemu SWD PRM przed i po wprowadzeniu Modyfikacji,
- m) Wykonawca zobowiązany jest również do prowadzenia analizy logów Oprogramowania,
- n) Wykonawca przygotowuje rekomendacje zmian i propozycji rozwiązań dla zapewnienia odpowiedniej pojemności / dostępności Systemu wraz z implementacją rozwiązań zatwierdzonych przez Zamawiającego,
- o) na podstawie Umowy Zamawiający zleci w formie pisemnej Zlecenie wykonania Usług Rekonfiguracji w wymiarze do 5000 (słownie: pięć tysięcy) godzin,
- p) jeśli w wyniku Zleceń powstanie Modyfikacja, podlega ona takiemu SLA jak pozostała część Systemu SWD PRM,
- q) za datę przekazania przez Zamawiającego wstępnego Zlecenia uważa się dzień, w którym zostało ono wysłane do Wykonawcy (na adres e-mail), przy czym wstępne Zlecenie wysłane po godzinie 15:35 będzie traktowane przez Wykonawcę jako otrzymane (przekazane) następnego dnia roboczego o godzinie 8:00 (np. wstępne Zlecenie wysłane Wykonawcy w piątek po godzinie 15:35 będzie traktowane, jako przekazane w poniedziałek o 8:00),
- r) w terminie 3 dni roboczych od dnia przekazania wstępnego Zlecenia Wykonawca przekaże Zamawiającemu analizę Zlecenia, zawierającą: określenie szczegółowego wykazu prac (specyfikacji Zlecenia) do wykonania Zlecenia wraz z oferowanym terminem realizacji, oraz kosztorysem realizacji prac zgodnie ze specyfikacją Zlecenia, przy czym jeżeli w przypadku realizacji Zlecenia powstaną Utwory, to Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe lub ewentualne dodatkowe licencje w ramach wynagrodzenia określonego §3 ust.1.
- s) Zamawiający najpóźniej w ciągu 3 dni roboczych od otrzymania analizy Zlecenia poinformuje Wykonawcę o udzieleniu Zlecenia, w wypadku zaakceptowania warunków wskazanych, wezwie Wykonawcę do uzupełnienia lub poprawienia analizy Zlecenia w ciągu 2 dni roboczych i ponownie rozpatrzy ją zgodnie z opisaną procedurą, albo poinformuje Wykonawcę o nieudzieleniu mu Zlecenia,
- t) jeżeli w ciągu 5 dni roboczych od otrzymania analizy Zlecenia Zamawiający nie udzieli Wykonawcy odpowiedzi, przyjmuje się, że Zamawiający zrezygnował z realizacji Zlecenia. Realizacja przez Wykonawcę Zlecenia bez zatwierdzonej przez Zamawiającego analizy Zlecenia następuje w całości na koszt i ryzyko Wykonawcy,
- u) za dni robocze Strony uznają dni od poniedziałku do piątku, z wyłączeniem dni ustawowo wolnych od pracy,
- v) w przypadku, jeżeli Wykonawca nie przystąpi do realizacji Zlecenia w terminie określonym w Zleceniu i opóźnienie w przystąpieniu do realizacji Zlecenia trwa dłużej niż 5 dni roboczych, Zamawiający może odstąpić od realizacji Zlecenia w całości lub w części z przyczyn leżących po stronie Wykonawcy, bez wyznaczania Wykonawcy dodatkowego terminu w tym zakresie, naliczając z tego tytułu należne kary umowne.

Jednocześnie niezależnie od powyższego, Zamawiający zastrzega sobie prawo przekazania do wykonania Zlecenia innemu podmiotowi po cenach rynkowych na koszt Wykonawcy,

- w) W wypadku, jeżeli Wykonawca wykonuje Zlecenie w sposób nienależyty, Zamawiający wezwie Wykonawcę do zmiany sposobu wykonania Zlecenia i wyznaczy mu w tym celu termin. Po bezskutecznym upływie wyznaczonego terminu Zamawiający będzie uprawniony do odstąpienia od Zlecenia w całości albo w części lub żądania zapłaty - niezależnie od skorzystania z prawa do odstąpienia - kary umownej,
- x) odbiór poszczególnych Zleceń odbywać się będzie na podstawie podpisanego przez upoważnionych przedstawicieli Stron Protokołu Odbioru Zleceń. Zamawiający może przy odbiorze Zlecenia zgłosić uwagi lub zastrzeżenia. Uwagi lub zastrzeżenia zostaną przekazane do Wykonawcy za pośrednictwem poczty elektronicznej na adres przedstawiciela reprezentującego Wykonawcę w ramach niniejszej Umowy,
- y) w przypadku zgłoszenia przez Zamawiającego uwag lub zastrzeżeń do Zlecenia, Zamawiający wyznaczy termin na usunięcie tych uwag lub zastrzeżeń, w którym to terminie Wykonawca na własny koszt i ryzyko obowiązany jest do ich uwzględnienia w całości. W takim przypadku procedura odbioru Zleceń zostanie przeprowadzona ponownie stosownie do postanowień niniejszego ustępu. W przypadku, gdy Wykonawca nie uwzględni uwag i zastrzeżeń zgłoszonych ze strony Zamawiającego do Zlecenia w wyznaczonym terminie lub będą one uwzględnione niezgodnie z tym, co zgłosił Zamawiający, Zamawiający uprawniony będzie do odstąpienia w całości lub w części od danego Zlecenia z przyczyn leżących po stronie Wykonawcy, bez wyznaczania Wykonawcy dodatkowego terminu w tym zakresie i żądania zapłaty odszkodowania- niezależnie od ewentualnego skorzystania z prawa do odstąpienia lub kary umownej.

3. Wymagania Zamawiającego w stosunku do Wykonawcy w zakresie zarządzania przedmiotem zamówienia są następujące:

- 1) wymaga się od Wykonawcy aby organizacja przedsięwzięcia związanego z przedmiotem Umowy, procesy kierujące przedsięwzięciem, struktura i zawartość realizacji zamówienia techniki zarządzania realizacją zamówienia, 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;
- 2) w przypadku wykorzystywania przez Wykonawcę własnej metodyki zarządzania przedsięwzięciem, wymaga się, aby uwzględniała ona co najmniej następujące elementy:
 - a) 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,
 - b) analizę ryzyka przed rozpoczęciem przedsięwzięcia i zarządzanie ryzykiem w trakcie jego realizacji,
 - c) sposób zarządzania zmianami, w tym rodzaje modyfikacji (poprawki, aktualizacje, rozbudowa, udoskonalenia) oraz procedury kontroli zmian.

4. Wymagania w zakresie Rozwiązania dla Systemu muszą być zgodne z niżej wymienionymi aktami prawnymi:
 - 1) ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (t.j. Dz. U. z 2018 r., poz. 1000).
 - 2) 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);
 - 3) 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.);
 - 4) ustawa z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (t.j. Dz. U. z 2018 r., poz. 620);
 - 5) ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz. U. z 2017r., poz. 1897 z późn. zm.);
 - 6) ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (t.j. Dz. U. z 2018 r., poz. 1954);
 - 7) ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (t.j. Dz. U. z 2017r., poz. 2195, z późn. zm.);
 - 8) ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2018 r., poz. 1401);
 - 9) ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (t.j. Dz. U. z 2018r., poz. 867);
 - 10) 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.);
 - 11) Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 24 marca 2011 r. w sprawie centralnego punktu systemu centrów powiadamiania ratunkowego oraz punktów centralnych służb (Dz. U. z 2015 r., poz. 2356);
 - 12) 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
5. Wymagania Zamawiającego w zakresie przygotowania i dostarczenia Dokumentacji są następujące:
 - 1) wytworzone przez Wykonawcę procedury muszą zostać zoptymalizowane pod kątem ciągłości działania usług Systemu o wysokim poziomie SLA;
 - 2) Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedmiotu Umowy charakteryzowały się wysoką jakością, na którą będą miały wpływ, takie czynniki jak: struktura dokumentu, rozumiana jako podział danego dokumentu na rozdziały, podrozdziały i sekcje, w czytelny i zrozumiały sposób;
 - 3) wymagane jest 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;
 - 4) wymagane jest zachowanie standardów Zamawiającego w zakresie oznaczeń dokumentów wersjonowania, metryk oraz wzoru szablonu dokumentów
 - 5) przez kompletność dokumentu rozumie się pełne, bez wyraźnych, ewidentnych braków przedstawienie omawianego problemu obejmujące całość z danego zakresu rozpatrywanego zagadnienia;

- 6) spójność i niesprzeczność dokumentu rozumiane są przez 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;
- 7) cała Dokumentacja, podlegała będzie 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;
- 8) 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,
- 9) wymagane jest, aby w ramach Dokumentacji Wykonawca przekazał Zamawiającemu wszystkie dokumenty robocze wytworzone w trakcie realizacji niniejszego zamówienia, w szczególności analizy, arkusze kalkulacyjne, materiały robocze, w formacie elektronicznym, niezabezpieczonym i edytowalnym;
- 10) wszystkie Dokumenty przekazane w formie elektronicznej (pliki) muszą:
 - a) być posegregowane w folderach odpowiadających nazwą produktów oraz nazwą, wersją i podwersją przekazywanego modułu (dotyczy kodów źródłowych),
 - b) być posegregowane w folderach zgodnie ze strukturą Dokumentacji,
 - c) posiadać nazwy plików (razem ze ścieżką) krótsze niż 200 znaków;
- 11) 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);
- 12) Zamawiający udostępni Dokumentację powykonawczą oraz eksploatacyjną SWD PRM na życzenie Wykonawcy, co zostanie potwierdzone odrębnym protokołem.

§5

Podwykonawstwo

1. *Zgodnie z oświadczeniem zawartym w ofercie Wykonawca powierzy część zamówienia podwykonawcom. Zakres prac wykonywanych przez podwykonawców określa załącznik nr 5 do Umowy. / Na dzień zawarcia Umowy Wykonawca zobowiązuje się wykonać zakres rzeczowy zamówienia, objęty Umową siłami własnymi bez udziału podwykonawców.**
- * - Brzmienie uzależnione od treści oferty Wykonawcy.*
2. W trakcie realizacji Umowy Wykonawca może zgłosić Zamawiającemu zamiar powierzenia wykonania części Umowy podwykonawcom, zamiar zmiany podwykonawcy/ów lub zamiar rezygnacji z wykonania Umowy przez podwykonawcę/ów.
3. W przypadku realizacji Umowy z udziałem podwykonawców Wykonawca zobowiązuje się do koordynowania prac realizowanych przez podwykonawców.

4. Wykonawca zawiadomi Zamawiającego o wszelkich zmianach nazw lub imion i nazwisk oraz danych kontaktowych podwykonawców zaangażowanych w realizację przedmiotu Umowy.
5. Wykonawca, zlecając część lub całość prac związanych z realizacją zamówienia podwykonawcom, zobowiązany jest do przestrzegania przepisów wynikających z Kodeksu cywilnego w zakresie prawidłowej realizacji zamówienia.
6. Powierzenie wykonania części zamówienia podwykonawcom nie zwalnia Wykonawcy z odpowiedzialności za należyte wykonanie Umowy.
7. Zmiany w zakresie, o którym mowa w ust. 2 i ust. 5 wymagają aneksu do Umowy. Zapisy ust. 3-7 mają zastosowanie w przypadku realizacji zamówienia z udziałem podwykonawców.

§6

Prawa autorskie

1. Wykonawca, w ramach wynagrodzenia określonego w § 3 ust. 1, przenosi na Zamawiającego w całości autorskie prawa majątkowe do wszystkich wytworzonych w ramach realizacji przedmiotu Umowy (w tym przez Wykonawcę, jego ewentualnych podwykonawców) utworów w rozumieniu art. 1 ust. 1-2 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2018 r. poz. 1191 z późn. zm.), w tym utworów zależnych, zwanych dalej „Utworami”.
2. Przeniesienie autorskich praw majątkowych, o których mowa w ust. 1, uprawnia do nieograniczonego w czasie i przestrzeni korzystania i rozporządzania Utworami na wszystkich polach eksploatacji wymienionych w art. 50 i art. 74 ust. 4 ustawy o prawie autorskim i prawach pokrewnych, w tym do wytworzonej Dokumentacji, na następujących polach eksploatacji:
 - 1) wykorzystania bez jakichkolwiek ograniczeń,
 - 2) utrwalania i trwałego zwielokrotniania całości lub części, wytwarzania egzemplarzy Utworu dowolną (również nieznaną w chwili przeniesienia praw autorskich) techniką, w tym techniką drukarską, reprograficzną, analogową lub cyfrową, przy zastosowaniu metody zapisu magnetycznego lub optycznego lub w jakiejkolwiek innej formie,
 - 3) przekazywania, przechowywania, odtwarzania, wyświetlania, wprowadzania do pamięci komputera wraz z prawem do wykonywania modyfikacji,
 - 4) tłumaczenia, przystosowywania, zmian układu lub jakichkolwiek innych zmian,
 - 5) wprowadzania do obrotu, użyczenia lub najmu oryginału albo egzemplarzy, na których Utwór utrwalono,
 - 6) rozpowszechniania Utworów przez publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnienie Utworów w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym;
3. Przeniesienie praw autorskich, o których mowa w ust. 1, następuje wraz prawem do wykonywania i prawem do udzielenia zezwolenia na wykonywanie autorskiego prawa zależnego oraz prawem własności egzemplarzy Utworów oraz nośników, na których zostały one utrwalone.
4. Przeniesienie praw autorskich do Utworów, o których mowa w ust. 1, następuje w dniu podpisania przez obie Strony Protokołu (Protokołów) Odbioru Zleceń, o którym mowa w § 4 ust. 2 pkt 29 lit x) albo w dniu dostarczenia Zamawiającemu faktury (nie później jednak niż w dniu rozpoczęcia przez Zamawiającego korzystania z Utworu).

5. Wykonawca zapewnia, że korzystanie przez Zamawiającego z praw autorskich przeniesionych na niego (Zamawiającego) na podstawie Umowy nie będzie naruszało żadnych praw osób trzecich.
6. Wykonawca ponosi odpowiedzialność za ewentualne roszczenia osób trzecich związane z naruszeniem autorskich praw majątkowych do Utworów i zobowiązuje się do zaspokojenia wszelkich roszczeń z tym związanych.
7. Wykonawca ponosi pełną odpowiedzialność za wszelkie wady prawne Utworów wytworzonych w ramach realizacji przedmiotu Umowy.
8. Wykonawca zobowiązuje się zwolnić Zamawiającego od wszelkiej odpowiedzialności w związku z roszczeniami lub żądaniami z tytułu naruszenia praw autorskich, które to roszczenia mogłyby powstać w rezultacie wykonania przez Wykonawcę przedmiotu Umowy.
9. Jeżeli Zamawiający poinformuje Wykonawcę o jakichkolwiek roszczeniach osób trzecich zgłaszanych wobec Zamawiającego w związku z realizacją przez Wykonawcę przedmiotu Umowy, Wykonawca podejmie działania mające na celu zażegnanie sporu i poniesie w związku z tym wszelkie koszty, w tym koszty zastępstwa procesowego od chwili zgłoszenia przedmiotowego roszczenia oraz koszty ewentualnych odszkodowań. W szczególności, w razie wytoczenia przeciwko Zamawiającemu powództwa z tytułu naruszenia praw własności intelektualnej w związku z realizacją przedmiotu Umowy, Wykonawca wstąpi do postępowania w charakterze strony pozwanej.
10. W przypadku, gdy wskutek wad prawnych brak jest po stronie Zamawiającego możliwości zgodnego z prawem korzystania z Utworów, Wykonawca zobowiązany jest do niezwłocznego usunięcia na swój koszt takich wad poprzez ponowne wykonanie Utworu wolnego od wad, a w przypadku, gdy Zamawiający wyrazi na to zgodę - przedsięwzięcie innych środków zaradczych.
11. Wykonawca zobowiązuje się uzyskać od twórców Utworów powstałych w ramach Umowy zgodę na niewykonywanie przysługujących im autorskich praw osobistych do Utworów w sposób, który mógłby powodować ograniczenie w wykorzystywaniu Utworów przez Zamawiającego, jak również upoważnienia na rzecz Zamawiającego do wykonywania praw osobistych, w tym do wyrażania zgody na rozporządzanie utworami zależnymi, które mogą powstać w przyszłości.

§7

Zobowiązania Stron

1. Zamawiający zobowiązuje się do:
 - 1) współdziałania z Wykonawcą w zakresie realizacji przedmiotu Umowy;
 - 2) udzielenia Wykonawcy, w czasie realizacji przedmiotu Umowy, upoważnienia do przetwarzania danych osobowych zgromadzonych w zbiorze danych SWD PRM oraz zapewnienia Wykonawcy dostępu do informacji i dokumentów niezbędnych do wykonywania Umowy;
 - 3) zapewnienia Wykonawcy dostępu do pomieszczeń, w których będzie realizowany przedmiot Umowy.
2. Wykonawca zobowiązuje się do:
 - 1) realizacji przedmiotu Umowy terminowo, zgodnie z wymaganiami określonymi w Umowie (w tym w Załącznikach do Umowy) z należytą starannością i najlepszą wiedzą oraz zasadami profesjonalizmu zawodowego, a także powszechnie obowiązującymi przepisami;

zorganizowania usług świadczonych w ramach realizacji przedmiotu Umowy tak, aby nie kolidowały one i nie zakłócały pracy poszczególnych modułów Systemu SWD PRM, z zachowaniem wszelkich wymogów bezpieczeństwa;

- 2) nieujawniania osobom trzecim informacji technicznych, technologicznych, organizacyjnych, sprzętowych ani innych informacji pozyskanych w związku z realizacją przedmiotu Umowy, w szczególności takich jak: struktury i funkcjonalności sieci telekomunikacyjnych, rodzaj wykorzystywanych urządzeń, a także wszelkich informacji umieszczonych na urządzeniach Zamawiającego, o których Wykonawca uzyskał wiedzę lub do których uzyskał dostęp w związku z realizacją Umowy.
3. Wykonawca oświadcza, że jest odpowiedzialny względem Zamawiającego za wszelkie wady fizyczne i prawne przedmiotu Umowy.
4. Wykonawca oświadcza i zapewnia, że przysługują mu uprawnienia do zawarcia Umowy.

§ 8

Zabezpieczenie należytego wykonania Umowy

1. Celem pokrycia roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, ustala się zabezpieczenie należytego wykonania przedmiotu Umowy w wysokości 10 % wynagrodzenia brutto, tj. w kwocie zł (słownie:.....).
2. Wykonawca wnosi zabezpieczenie należytego wykonania przedmiotu Umowy najpóźniej w dniu podpisania Umowy.
3. Zabezpieczenie należytego wykonania Umowy, Wykonawca wniósł w formie
4. W przypadku niewykonania lub nienależytego wykonania Umowy, zabezpieczenie przechodzi na własność Zamawiającego i zostanie wykorzystane do pokrycia roszczeń.
5. z tytułu niewykonania lub nienależytego wykonania Umowy.
6. Zamawiający zwróci zabezpieczenie należytego wykonania Umowy Wykonawcy w terminie 30 dni od dnia wykonania przedmiotu Umowy i uznania przez Zamawiającego za należyte wykonaną.
7. W trakcie realizacji przedmiotu Umowy, Wykonawca może dokonać zmiany formy zabezpieczenia na jedną lub kilka form, o których mowa w art. 148 ust. 1 ustawy Prawo zamówień publicznych. Zmiana formy zabezpieczenia musi być dokonywana z zachowaniem ciągłości zabezpieczenia i bez zmniejszenia jego wysokości.
8. Zamawiający zwróci zabezpieczenie należytego wykonania Umowy wniesione w pieniądzu wraz z odsetkami wynikającymi z Umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek Wykonawcy.
9. Zwrot zabezpieczenia należytego wykonania Umowy nastąpi poprzez dokonanie przelewu wpłaconej na konto Wykonawcy kwoty zabezpieczenia albo poprzez zwrot oryginału dokumentu potwierdzającego wniesienie zabezpieczenia, w formie innej niż pieniężna.

§9

Kary umowne

1. Wykonawca jest odpowiedzialny za wszelkie szkody, które poniesie Zamawiający wskutek niewykonania lub nienależytego wykonania Umowy. W przypadku poniesienia przez Zamawiającego szkody przewyższającej wartość zastrzeżonej kary umownej oraz w innych

wypadkach niewykonania lub nienależytego wykonania Umowy przez Wykonawcę, Zamawiający może dochodzić odszkodowania na zasadach ogólnych wynikających z Kodeksu Cywilnego, przenoszącego wysokość zastrzeżonych kar umownych.

2. W przypadku niewykonania, bądź nienależytego wykonania przedmiotu Umowy w zakresie określonym w § 1 ust. 1 pkt 1, wynagrodzenie nie należy się, a Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 30% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 1. Przez nienależyte wykonanie przedmiotu Umowy Strony rozumieją w szczególności wykonanie niezgodnie z wymogami określonymi w § 4 ust. 2 pkt. 1) - 28), ust.3, ust.4 i ust.5 Umowy, z zastrzeżeniem szczegółowych regulacji w dalszych ustępach niniejszego paragrafu.
3. W przypadku opóźnienia w rozpoczęciu świadczenia usług utrzymaniowych SWD PRM, o których mowa w § 1 ust. 1 pkt 1, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 3% wynagrodzenia brutto określonego w § 3 ust. 1 pkt 1, za każdy rozpoczęty dzień opóźnienia.
4. W przypadku nienależytego wykonania przedmiotu Umowy w zakresie określonym w § 1 ust. 1 pkt 2, wynagrodzenie nie należy się, a Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 30% wynagrodzenia brutto określonego za dane Zlecenie. Przez nienależyte wykonanie Zlecenia Strony rozumieją w szczególności wykonanie niezgodnie z wymogami określonymi przez Zamawiającego w Zleceniu, z zastrzeżeniem szczegółowych regulacji w dalszych ustępach niniejszego paragrafu.
5. W przypadku nie wykonania danego Zlecenia, o którym mowa w §4 ust.2 pkt 29) lit. o), przez Wykonawcę, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100% wartości brutto (należnego mu wynagrodzenia z tytułu realizacji) danego Zlecenia, z zastrzeżeniem prawa Zamawiającego do zlecenia zastępczego zgodnie z §4 ust.2 pkt 38) lit. v).
6. W przypadku opóźnienia w wykonaniu Zlecenia (względem terminu wskazanego w zatwierdzonej przez Zamawiającego analizie Zlecenia) w zakresie usług rekonfiguracyjnych SWD PRM, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia brutto określonego za dane Zlecenie za każdy dzień opóźnienia.
7. W przypadku przekroczenia limitu wynikającego z dopuszczalnego poziomu SLA określonego w § 4 ust. 2 pkt 1) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,05% wynagrodzenia brutto określonego w § 3 ust. 1 za każdą rozpoczętą minutę niedostępności (ponad określony limit) Systemu SWD PRM.
8. W przypadku przekroczenia czasu usunięcia Awarii Niekrytycznej określonego w § 4 ust. 2 pkt 13), Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100zł brutto (sto złotych) za każdą rozpoczętą godzinę opóźnienia.
9. W przypadku przekroczenia czasu usunięcia Awarii Zwykłej określonego w § 4 ust. 2 pkt 14) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500 zł brutto (pięćset złotych) za każdy dzień opóźnienia.
10. W przypadku odstąpienia od Umowy, w całości lub w części z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 50 % łącznego wynagrodzenia brutto określonego w § 3 ust. 1 Umowy.
11. Zamawiający ma prawo do potrącenia naliczonych kar umownych z wynagrodzenia przysługującego Wykonawcy. Wykonawca oświadcza, że wyraża zgodę na potrącenie.
12. w rozumieniu art. 498 i 499 Kodeksu cywilnego, powstałych należności z tytułu kar umownych przewidzianych w niniejszej umowie, z przysługującego mu wynagrodzenia.

13. W celu skorzystania z uprawnień do potrącenia naliczonych kar umownych z wynagrodzenia przysługującego Wykonawcy, Zamawiający wystawi Wykonawcy notę zawierającą szczegółowe naliczenie kar umownych i w dniu wystawienia przekaże ją Wykonawcy pocztą elektroniczną na adres poczty elektronicznej podany § 4 ust. 5 oraz za pośrednictwem operatora pocztowego. Strony ustalają, iż terminem wymagalności należności z tytułu kar umownych wynikających z niniejszej Umowy jest dzień wystawienia przez Zamawiającego noty księgowej obciążającej Wykonawcę z tytułu przedmiotowych kar umownych.

§ 10

Zmiany w umowie

Zamawiający, stosownie do art. 144 ust. 1 ustawy Prawo zamówień publicznych, przewiduje możliwość dokonania zmiany zawartej Umowy, wyłącznie w zakresie dopuszczalnym przepisami ustawy Prawo zamówień publicznych, w formie pisemnego aneksu pod rygorem nieważności. Zmiany mogą nastąpić w następującym zakresie:

- 1) w przypadku zmian obowiązujących przepisów prawa, odnoszących się bezpośrednio do niniejszego zamówienia;
- 2) w przypadku gdy wystąpiła uzasadniona przyczynami technicznymi konieczność zmiany sposobu wykonania Umowy;
- 3) w przypadku gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa, w tym, w szczególności, zmiana stawki podatku od towarów i usług (VAT), przy czym zmianie ulegnie tylko stawka podatku Vat oraz wynagrodzenie brutto.
- 4) przedmiotu, terminów i sposobu wykonania Umowy spowodowanych zmianami, normach, dyrektywach, standardach lub zmianami w zakresie wiedzy technologicznej w zakresie dostosowującym postanowienia Umowy do ww. zmian. W takim przypadku wynagrodzenie Wykonawcy może zostać zmienione tylko w takim zakresie, w jakim odpowiada kosztom zwiększonym z powodu dostosowania przedmiotu Umowy do wymienionych wyżej zmian z uwzględnieniem rozsądnego zysku.

§ 11

Odstąpienie od Umowy

1. Zamawiający może odstąpić od Umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub dalsze wykonywanie Umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu.
2. Zamawiający zastrzega sobie prawo odstąpienia w całości lub w części nierealizowanej Umowy, w przypadku nie wykonania lub nienależytego wykonania Umowy ze skutkiem natychmiastowym w terminie 7 dni od powzięcia wiadomości o tych okolicznościach, między innymi w następujących okolicznościach:
 - 1) nie przystąpienia do realizacji przedmiotu Umowy, pomimo wyznaczenia przez Zamawiającego dodatkowego terminu;
 - 2) nie wywiązania się z zobowiązań określonych w szczególności w §4 ust.2-5 oraz OPZ;
 - 3) inny rodzaj nienależytego wykonania lub nie wykonania Umowy, czyniącego dalsze jej realizowanie bezprzedmiotowym.

3. W przypadku odstąpienia od Umowy przez Zamawiającego na podstawie ust. 1 i/lub ust. 2, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.
4. Skorzystanie przez Stronę z przewidzianego w Umowie prawa do odstąpienia od Umowy, z zastrzeżeniem ust. 2, w tym złożenie oświadczenia o odstąpieniu każdorazowo powinno zostać dokonane na piśmie, pod rygorem nieważności, w terminie 30 dni od powzięcia wiadomości o wystąpieniu okoliczności skutkujących odstąpieniem i zawierać uzasadnienie.

§12

Osoby upoważnione do kontaktów

1. Strony wyznaczają swoich przedstawicieli odpowiedzialnych za realizację Umowy:
 - 1) ze strony Zamawiającego:.....tel. e-mail:
 - 2) ze strony Wykonawcy:tel, e-mail:.....
2. Przedstawiciele, o których mowa w ust. 1, reprezentują Strony w sprawach bieżących uzgodnień oraz merytorycznej współpracy i koordynacji, niezbędnych dla prawidłowej realizacji Umowy, w tym podpisywania Protokołów Odbioru Zleceń.
3. Zmiana osób i danych (kontaktowych) wskazanych w ust. 1 nie wymaga sporządzania aneksu do Umowy i następuje poprzez złożenie (doręczenie) drugiej Stronie pisemnego oświadczenia.

§ 13

Siła wyższa

1. Strony nie odpowiadają za niewykonanie lub nienależyte wykonanie Umowy spowodowane siłą wyższą.
2. Siłą wyższą, w rozumieniu Umowy są zdarzenia zewnętrzne, nadzwyczajne, niezależne od Stron, których nie dało się przewidzieć przed podpisaniem Umowy, w szczególności: wojna, atak terrorystyczny, strajk, pożar, eksplozja, powódź, huragan, katastrofa naturalna.
3. Strony zobowiązują się do wzajemnego powiadamiania się o zaistnieniu zdarzenia, uniemożliwiającego wykonanie Umowy bądź przyczyniającego się do nienależytego wykonania Umowy, spowodowanego siłą wyższą, nie później niż w ciągu 2 (dwóch) dni roboczych od dnia wystąpienia takiego zdarzenia.

§ 14

Poufność

1. Strony nie mogą ujawniać informacji poufnych zawartych w Umowie, Załącznikach do Umowy czy Aneksach do Umowy, jak również informacji uzyskanych w trakcie realizacji Umowy. Zakaz nie dotyczy informacji, które strony są zobowiązane ujawnić na podstawie przepisów prawa.
2. Wykonawca, bez uprzedniej pisemnej zgody Zamawiającego, nie może bezpośrednio czy pośrednio ujawniać żadnym osobom trzecim informacji o polityce bezpieczeństwa Zamawiającego, w których posiadanie wszedł w związku z wykonywaniem Umowy. Niniejsze zobowiązanie wiąże Strony zarówno w czasie trwania Umowy, jak i w okresie 5 lat po jej rozwiązaniu lub wygaśnięciu. Za naruszenie niniejszego paragrafu Wykonawca będzie zobowiązany do naprawienia szkody na zasadach ogólnych.

3. Wykonawca oświadcza, że znany jest mu fakt, iż treść Umowy, a w szczególności przedmiot Umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (tekst jednolity Dz.U. z 2018 r., poz. 1330), która podlega udostępnianiu w trybie przedmiotowej ustawy, z zastrzeżeniem ust. 3.
4. Wykonawca jest zobowiązany, przetwarzając dane osobowe, do stosowania przy ich przetwarzaniu przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2018 r. poz. 1000).
5. Wykonawca wyraża zgodę na udostępnienie w trybie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity Dz.U. z 2018 r. poz. 1000) zawartych w umowie dotyczących go danych osobowych w zakresie obejmującym imię i nazwisko, a w przypadku prowadzenia działalności gospodarczej – również w zakresie firmy.

§ 15

Postanowienia końcowe

1. Umowa wchodzi w życie z dniem podpisania.
2. W sprawach nie uregulowanych w niniejszej Umowie stosuje się w szczególności przepisy ustawy Prawo zamówień publicznych i Kodeksu cywilnego.
3. Ewentualne spory mogące powstać w związku z Umową rozstrzygane będą przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
4. Zmiany i uzupełnienia do niniejszej Umowy wymagają zachowania formy aneksu pod rygorem nieważności.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.
6. Załącznikami do Umowy stanowiącymi jej integralną część są:
 - 1) SIWZ wraz z Opisem Przedmiotu Zamówienia – załącznik nr 1;
 - 2) oferta Wykonawcy – załącznik nr 2;
 - 3) wzór Protokołu Odbioru Usługi – załącznik nr 3;
 - 4) wzór Protokołu Odbioru Zleceń – załącznik nr 4;
 - 5) wykaz podwykonawców – załącznik nr 5 (jeżeli dotyczy).

ZAMAWIAJĄCY:

WYKONAWCA:

A. L. o. - - L.

Radiologiczny
Mariusz Trópek
Wz-2023

Zastępca Dyrektora
Lotniczego Pogotowia Ratunkowego
ds. Krajowego Centrum Monitorowania
Ratownictwa Medycznego
www.lpr.com.pl

LOTNICZE POGOTOWIE RATUNKOWE

ul. Książkowa 5, 01-934 Warszawa, tel. (22) 22-99-931/932, fax. (22) 22-99-933

Mateusz Komza



OPIS PRZEDMIOTU ZAMÓWIENIA

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

Spis treści

Wprowadzenie	3
1. Cel	3
2. Definicje	4
3. Opis rozwiązania SWD PRM	10
3.1. Architektura logiczna systemu	10
3.2. Schemat architektury logicznej środowiska PROD	10
3.3. Schemat architektury logicznej środowiska SZK	18
3.4. Schemat architektury logicznej środowiska DEV	20
3.5. Protokoły i metody wymiany danych pomiędzy serwerem i klientem w ramach SWD PRM	22
3.5.2. Inicjowanie komunikacji przez serwer	22
3.5.3. Forma komunikatu	22
3.6. Architektura bazy danych	23
3.6.4. ETL – Extract, Transform and Load	27
3.6.5. Lokalna baza danych	27
3.7. Bezpieczeństwo	27
3.7.2. Certyfikaty	28
3.7.3. Uwierzytelnianie i autoryzacja aplikacji Dyspozytora	28
3.7.5. Uwierzytelnianie i autoryzacja aplikacji mobilnej ZRM	31
3.8. Poufność	32
3.9. Integralność	32
3.10. Rozliczalność	33
3.11. Niezaprzeczalność	33
3.12. Ciągłość działania	34
3.12.1.1. Utrata połączenia sieciowego od aplikacji klienckich do OK	34
3.12.1.3. Awaria zasilania	35
3.12.3.2. Awaria macierzy dyskowej	36
3.13. Architektura fizyczna systemu	37
3.14. Oprogramowanie	39
3.14.1. Oprogramowanie serwerowe	39
3.14.2. Oprogramowanie klienckie	40
3.15. Infrastruktura klucza publicznego (PKI)	40
3.16. Ograniczenia	41
3.16.1. Wymagania na dostęp administracyjny do SWD PRM z wykorzystaniem OST 112	41
3.17. Integracja z systemami zewnętrznymi	42
3.17.1. UMM	42
3.17.2. PLI CBD	42
3.17.3. Integracja z SI CPR	42
3.17.4. Automapa	43
3.17.5. PZŁ	43
4. Usługi rekonfiguracyjne SWD PRM	43
4.1. Wymagania w zakresie usług rekonfiguracyjnych SWD PRM	43
4.2. Zakres usługi w ramach zleconych prac rekonfiguracyjnych	44
5. Usługi utrzymaniowe SWD PRM	45
6. Minimalne wymagania w zakresie zarządzania przedmiotem zamówienia	49
7. Wymagania w zakresie zgodności z przepisami prawa	50
8. WYMAGANIA W ZAKRESIE DOKUMENTACJI	52

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: a) uwierzytelnianie, b) niezaprzeczalność, c) poufność, d) integralność, e) dostępność, f) 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: a) przyjęcie zgłoszenia (w tym zgłoszenia z CPR oraz powiadomienia o zdarzeniach), b) zadysponowanie ZRM, c) przyjęcie zlecenia wyjazdu przez ZRM; 2) Monitorowanie ZRM w zakresie: status wyjazdu, lokalizacja ZRM; 3) Przejęcie obsługi zdarzeń przez inną DM. Brak funkcjonalności krytycznej wynikały 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 określony w wojewódzkim planie działania systemu Państwowe Ratownictwo Medyczne.
SD	Stanowisko dostępne 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.

¹ Z dniem 1 kwietnia 2019 r. rejon operacyjny to rejon działania dyspozytorni medycznej określony w wojewódzkim planie działania systemu Państwowe Ratownictwo Medyczne.

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. Virtual Private Network, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. 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) **SZK** – 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

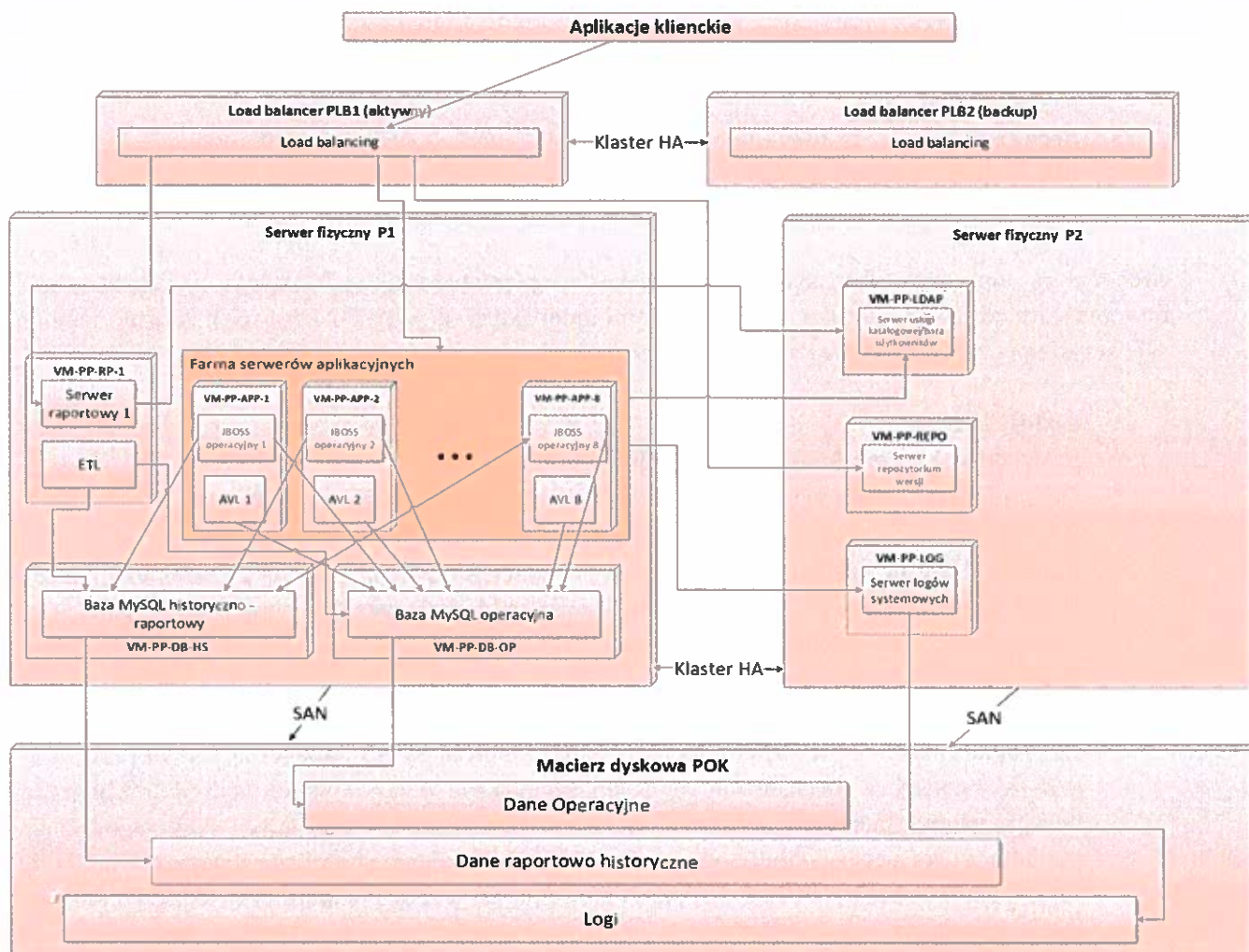
Poniższy rysunek prezentuje ogólny schemat architektury logicznej środowiska PROD dla POK. Przedstawiono na nim komponenty uwzględniające: fizyczne urządzenia (maszyny serwerowe, macierze, loadbalancery), maszyny wirtualne oraz zainstalowane na nich serwery programowe oraz bazy danych, a także połączenia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

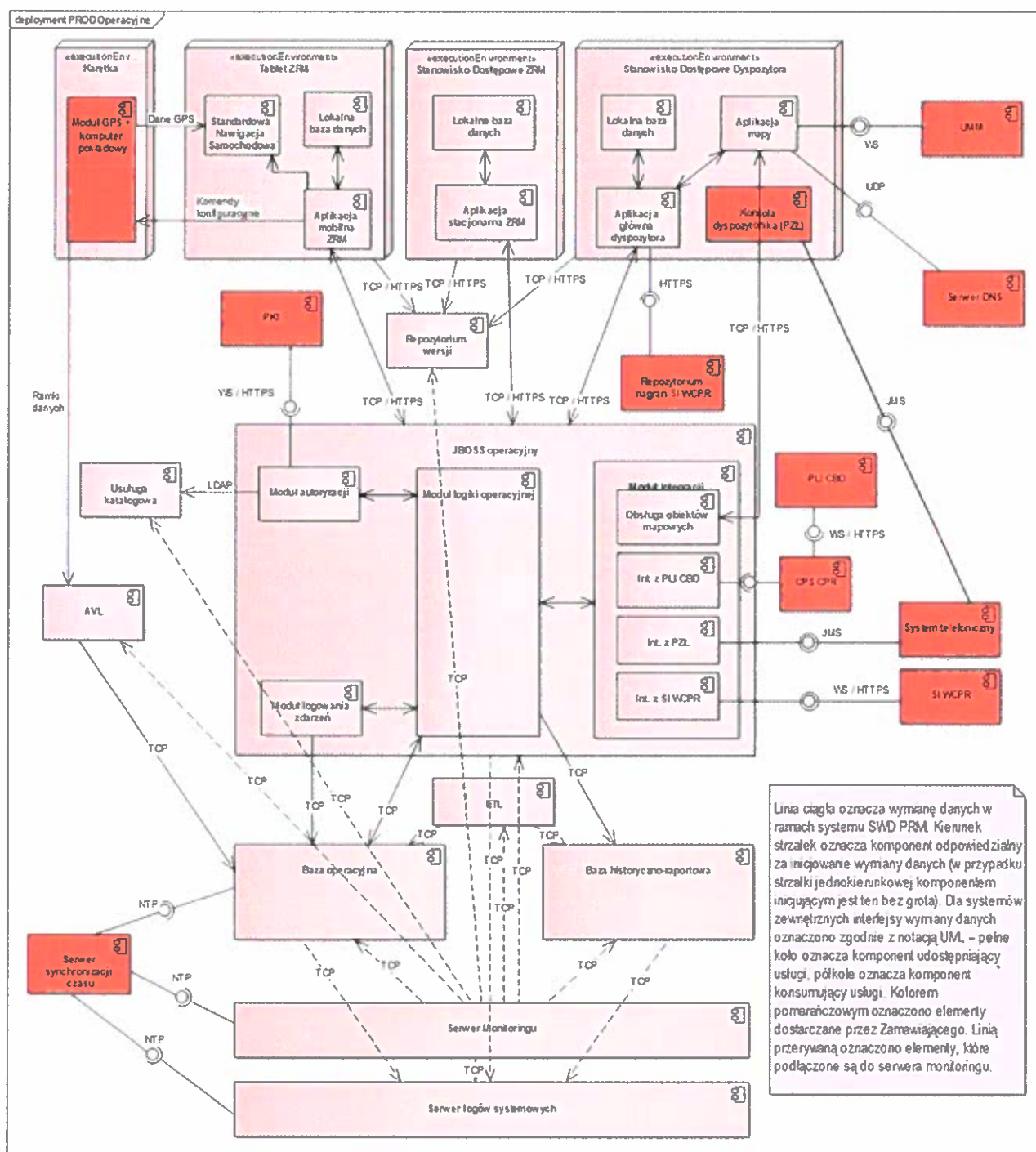
- POK aktywny (master) → ZOK pasywny (slave),
- ZOK aktywny (master) → POK pasywny (slave),
- obydwa ośrodki działające jako „aktywny – aktywny” w trybie synchronicznym.

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, półkoło 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 przesyłający do serwera AVL dane dotyczące parametrów pojazdu oraz danych dotyczących położenia geograficznego karetki. Moduł GPS przesyłał 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.

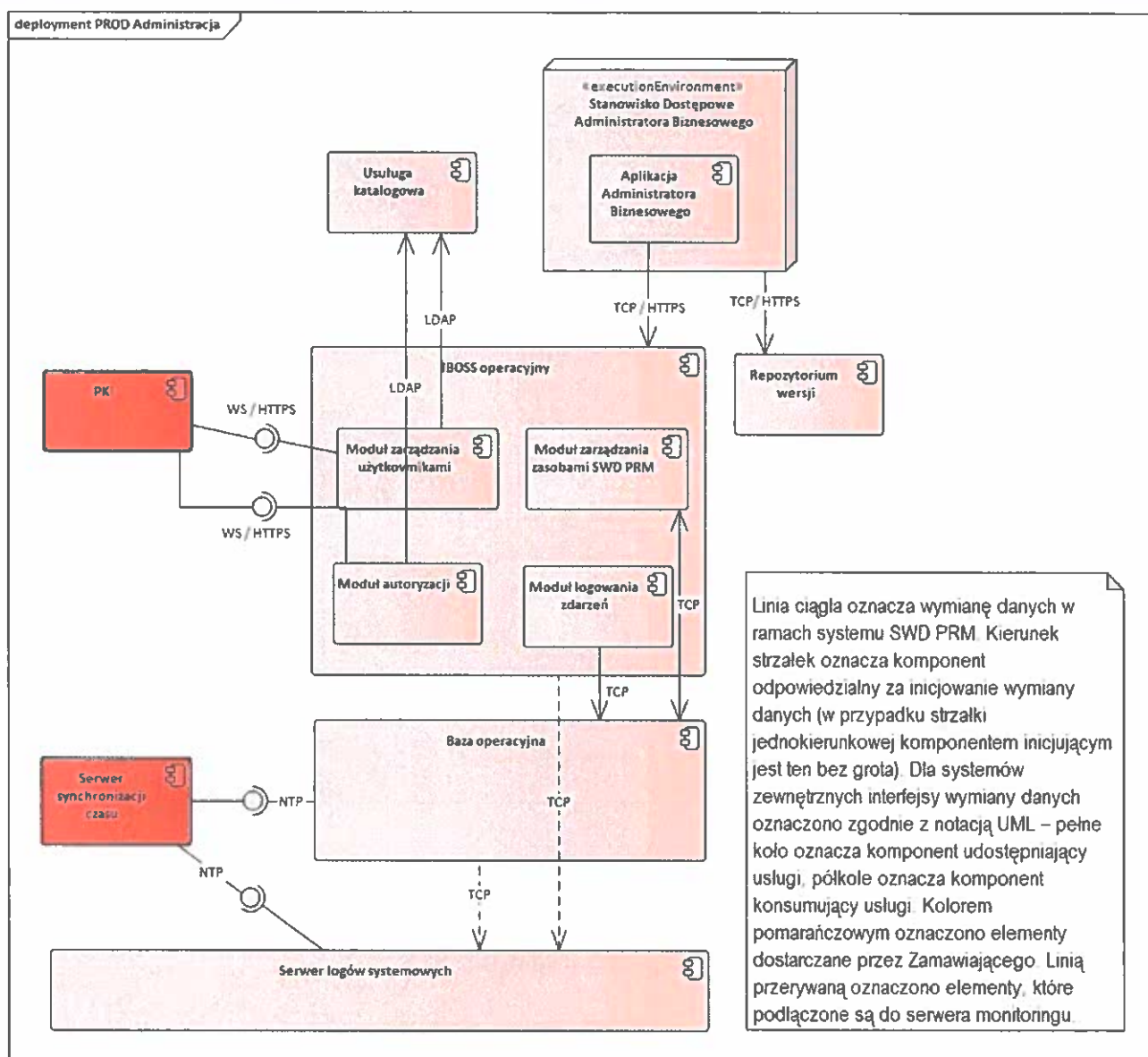
- **Moduł PKI** – moduł obsługi certyfikatów i kluczy.
- **Usługa katalogowa** – serwer LDAP służący do przechowywania danych użytkowników, ich ról, kluczy publicznych, a także do centralnego zarządzania użytkownikami Systemu.
- **Serwer synchronizacji czasu** – serwer umożliwiający synchronizację czasu 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:
 - a) 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:
 - a) Lokalna baza danych – osadzona w aplikacji, szyfrowana baza danych H2, przechowująca tymczasowe dane przed wysłaniem do OK, dane słownikowe,
 - b) Aplikacja desktopowa MS,
- **Aplikacja SD Dyspozytora (Moduł Dyspozytora i Moduł Mapy)** – uruchamiana na Stanowisku Dostępowym w Dyspozytorni, składająca się z następujących elementów:
 - a) Lokalna baza danych – osadzona w aplikacji, szyfrowana baza danych H2, przechowująca tymczasowe dane przed wysłaniem do OK, dane słownikowe,
 - b) 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,
 - c) Aplikacja mapy – aplikacja wyświetlająca dane lokalizacyjne sił i środków, miejsca zdarzenia, umożliwiającą 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:

- a) Moduł autoryzacji – odpowiedzialny za uwierzytelnianie i autoryzację użytkowników, komunikację z systemem PKI oraz usługą katalogową, zarządzanie użytkownikami i rolami.
- b) 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.



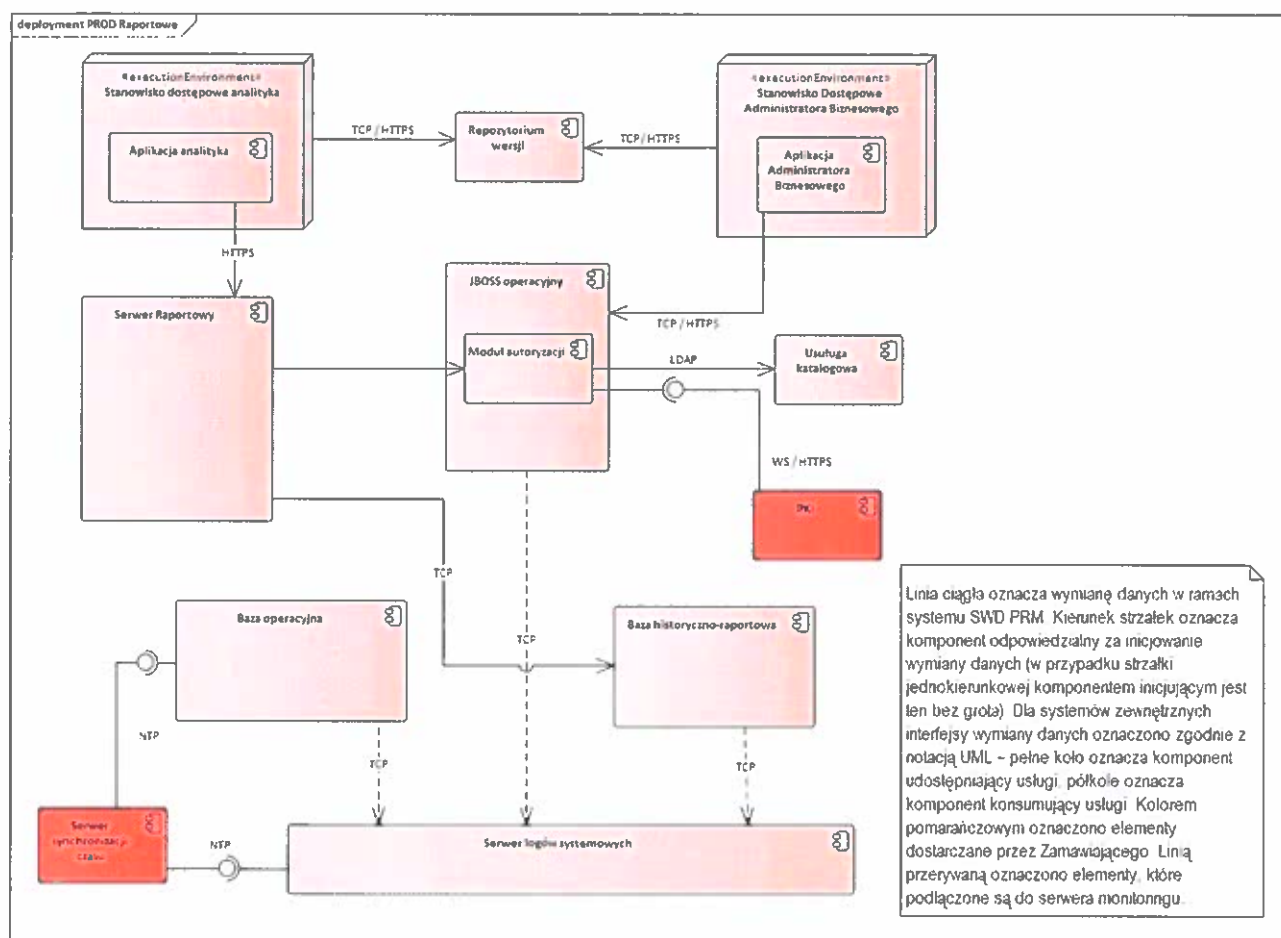
Rysunek nr 3. Architektura logiczna środowiska PROD. Działania administracyjne.

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):

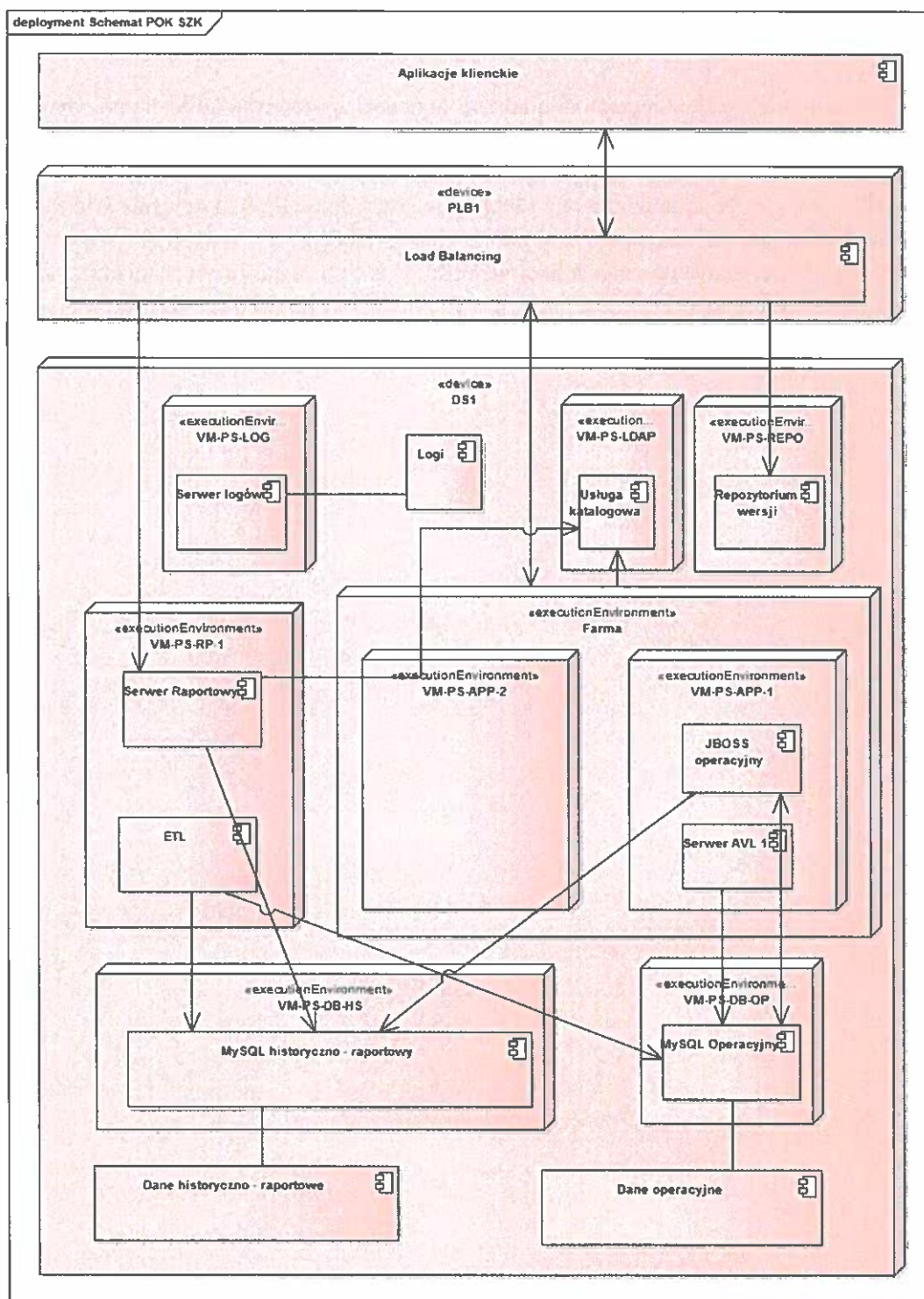
- Aplikacja Analityka (Moduł Raportowy) – aplikacja umożliwiająca tworzenie raportów, wgląd do danych statystycznych i historycznych.
- Serwer Raportowy – serwer raportów na potrzeby analityków Dysponenta.



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.

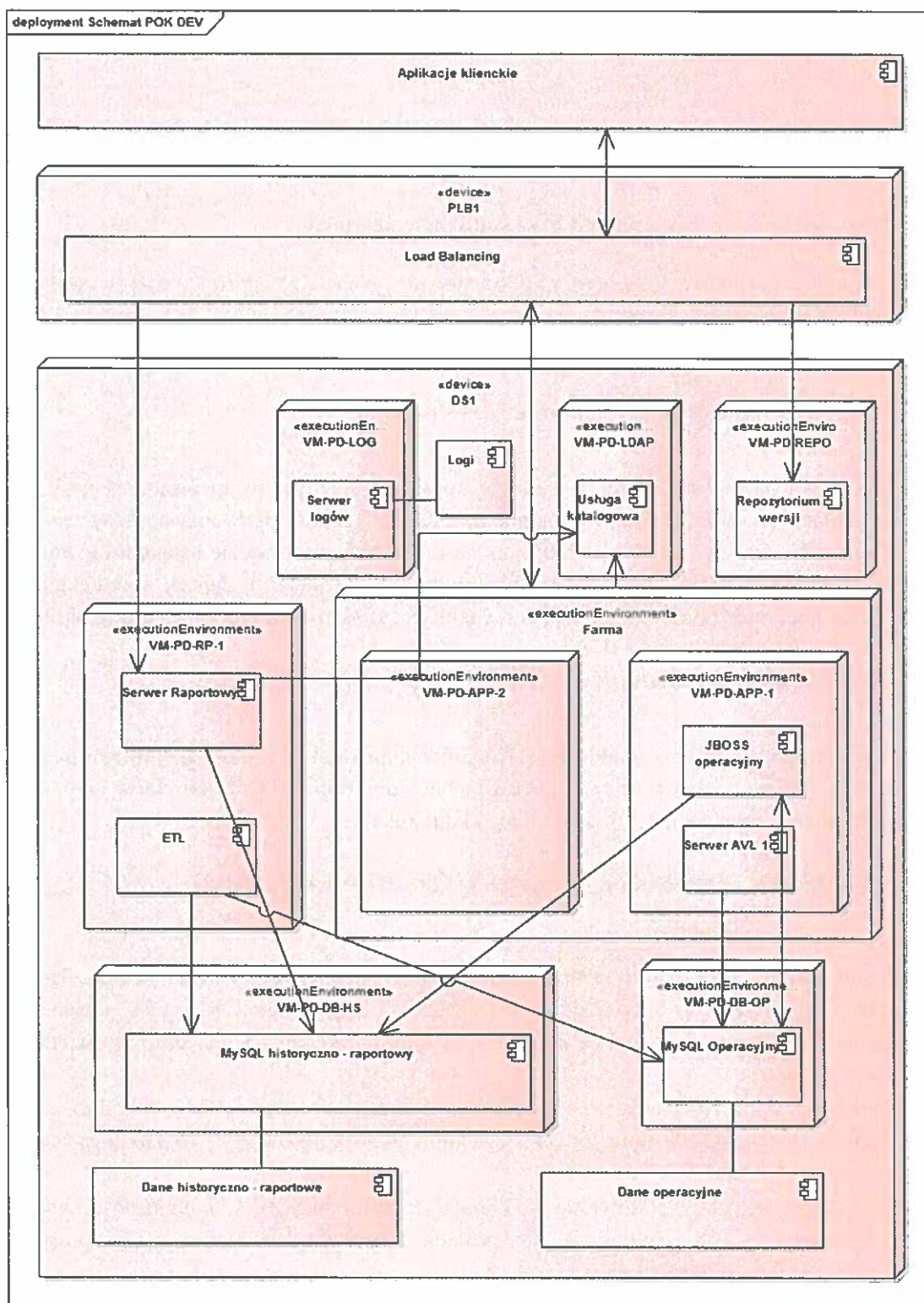


Rysunek nr 5. Diagram ogólny architektury logicznej POK dla środowiska SZK.

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:
 - a) Transakcja jest wykonywana w ośrodku A,
 - b) Polecenie wykonania transakcji jest wysyłane do ośrodka B,
 - c) Ośrodek B zapisuje transakcję do logu bazy danych na dysku,
 - d) 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.

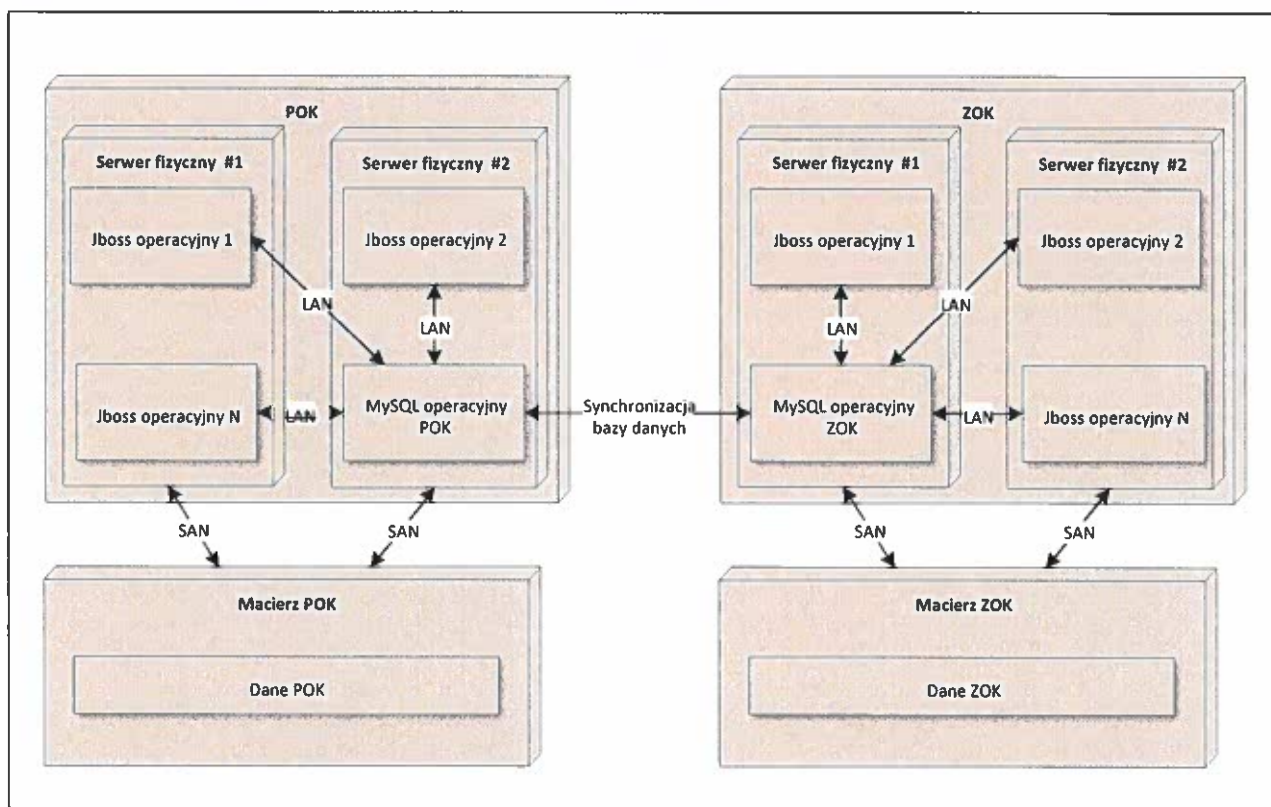
Maszyny fizyczne tworzą klastery niezawodnościowy. Maszyny wirtualne mogą być uruchamiane na dowolnym serwerze w klastrze.

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.

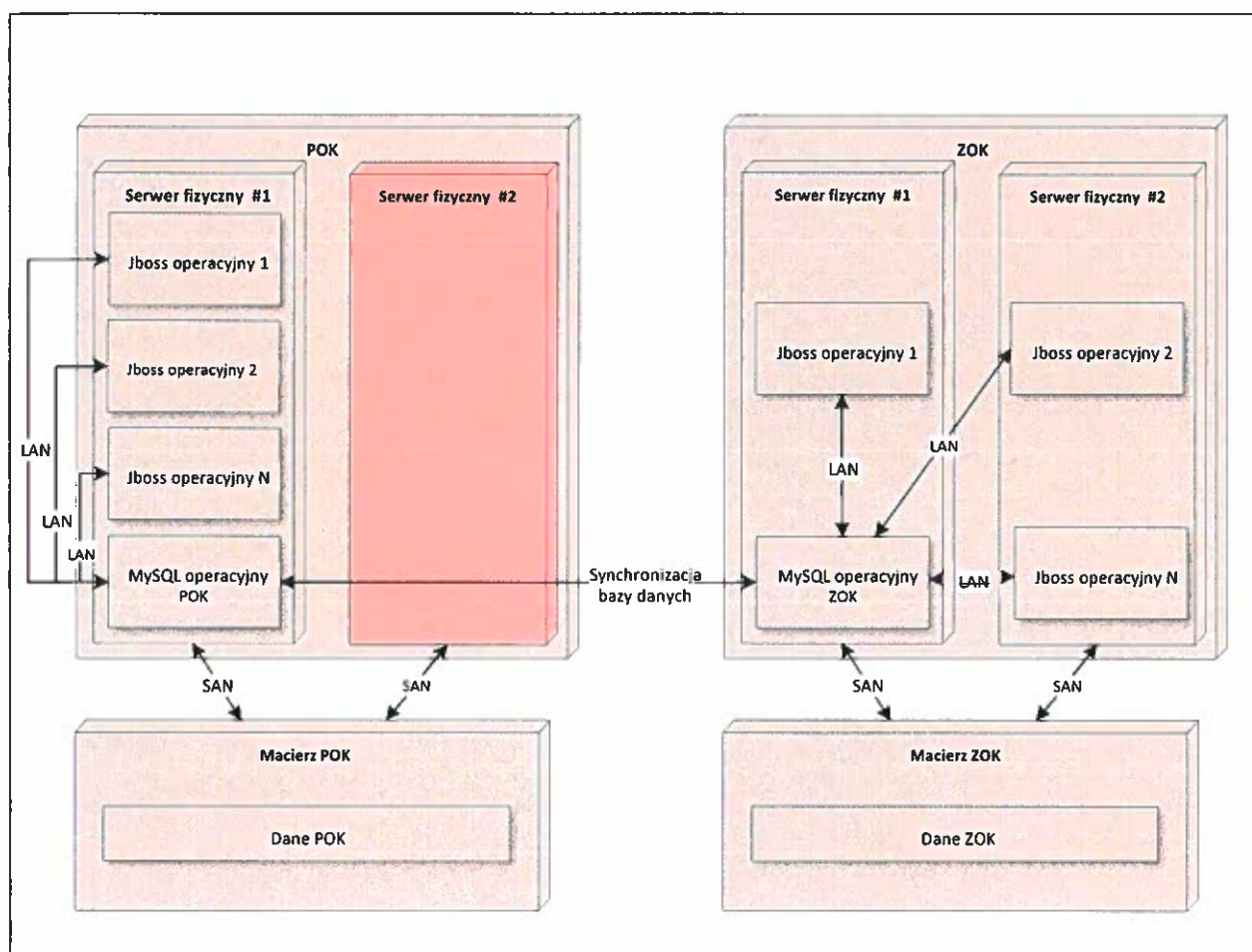
Mechanizm ten jest niezależny od mechanizmu synchronizacji baz danych między POK a ZOK.

Typowa sytuacja pracy ośrodków krajowych jest przedstawiona na poniższym rysunku.



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.



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:
 - a) Jeśli NIE, to zwraca komunikat o błędzie („Nieprawidłowy certyfikat”) -> STOP
 - b) Jeśli TAK, następuje przejście do kroku 4.
4. Serwer aplikacji weryfikuje prawidłowość i ważność certyfikatu poprzez wywołania metody/usługi weryfikacji certyfikatu w module PKI:
 - a) Jeśli weryfikacja przebiegła pomyślnie, serwer zwraca do aplikacji informację o pozytywnym wyniku uwierzytelnienia, aplikacja jest gotowa do działania.

- b) 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:
 - a) Jeśli domena zwróci błąd logowania zostaje zwrócony komunikat o błędzie -> STOP
 - b) 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:
 - a) 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.

- 4) Użytkownik chcący uzupełniać dokumentację medyczną klika na przycisk „Przejdź do trybu aktywnego” – przejście do trybu aktywnego następuje po podaniu loginu i hasła użytkownika lub włożeniu karty mikroprocesorowej do czytnika.
- 5) Po przejściu do trybu aktywnego użytkownik otrzymuje dostęp do swoich dokumentów oraz zleceń, które może uzupełniać oraz wysyłać na serwer.
- 6) 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:
 - a) 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.
 - b) 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 przyjęciem 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:
 - a) Deszyfruje hasło użytkownika kluczem prywatnym,
 - b) 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:
 - a) 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.
 - b) 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

Z uwagi 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.
 - a) Zabezpieczenie przed utratą wynikającą z uszkodzenia nośnika danych,
 - b) Zabezpieczenie przed rozmyślnym, nieautoryzowanym zniszczeniem lub zmianą danych.
- Integralność danych w procesie przesyłania ich między węzłami Systemu oraz między Systemem a systemami zewnętrznymi.

3.9.1. Integralność danych zapisanych na nośnikach danych

Integralność wszelkich danych zapisywanych na nośnikach danych w ramach OK jest zapewniona dzięki wykorzystaniu macierzy dyskowych skonfigurowanych w odpowiedni sposób. 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.

3.9.2. 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);
- 3) Aplikacja prosi o podanie hasła do certyfikatu.

- 4) 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 jak 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 przełączeni 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 włączają 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-spares. Po awarii dysku macierz odbudowuje konfigurację RAID z wykorzystaniem dysku Hot-spares 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 obsługiwane 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 wysłania 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.

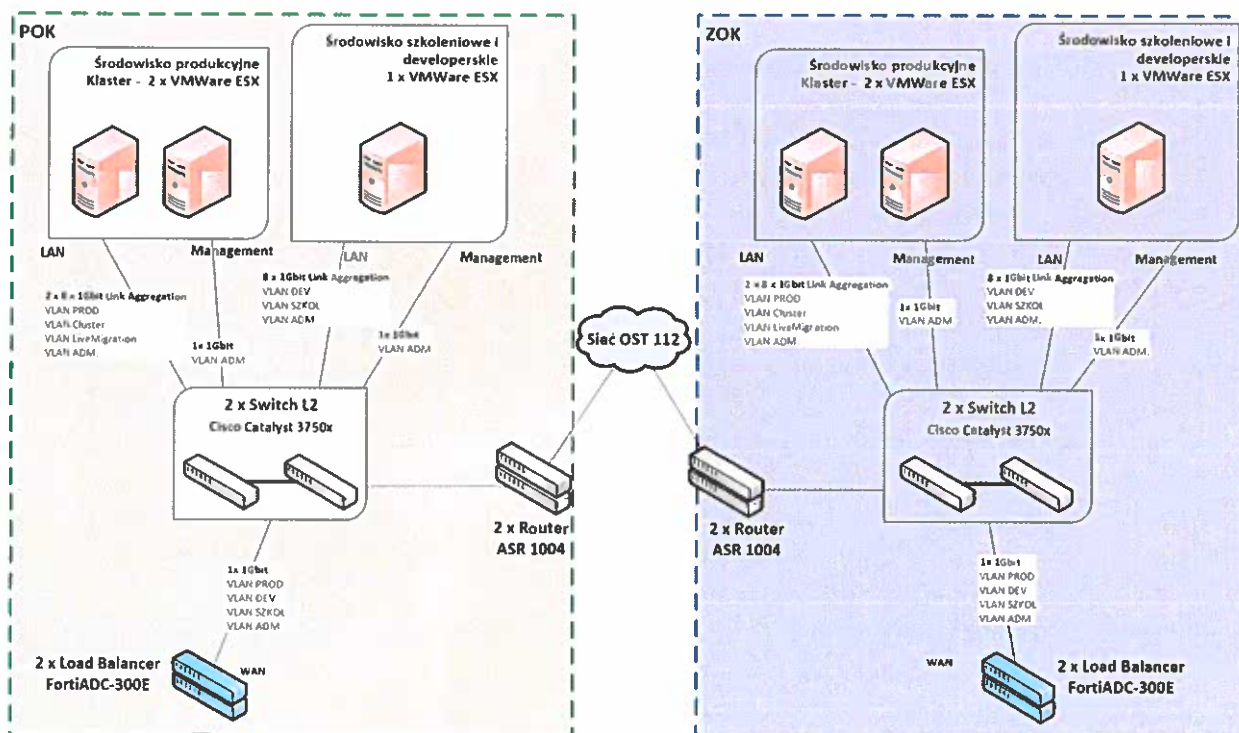
Posiadają one taką samą konfigurację sprzętową oraz są ze sobą połączone, poprzez sieć OST 112, wydzielonym łączem o przepustowości 1Gbit/s/. Połączenie do sieci OST 112 jest realizowane przez routery ASR1004 znajdujące się w osobnych szafach.

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.

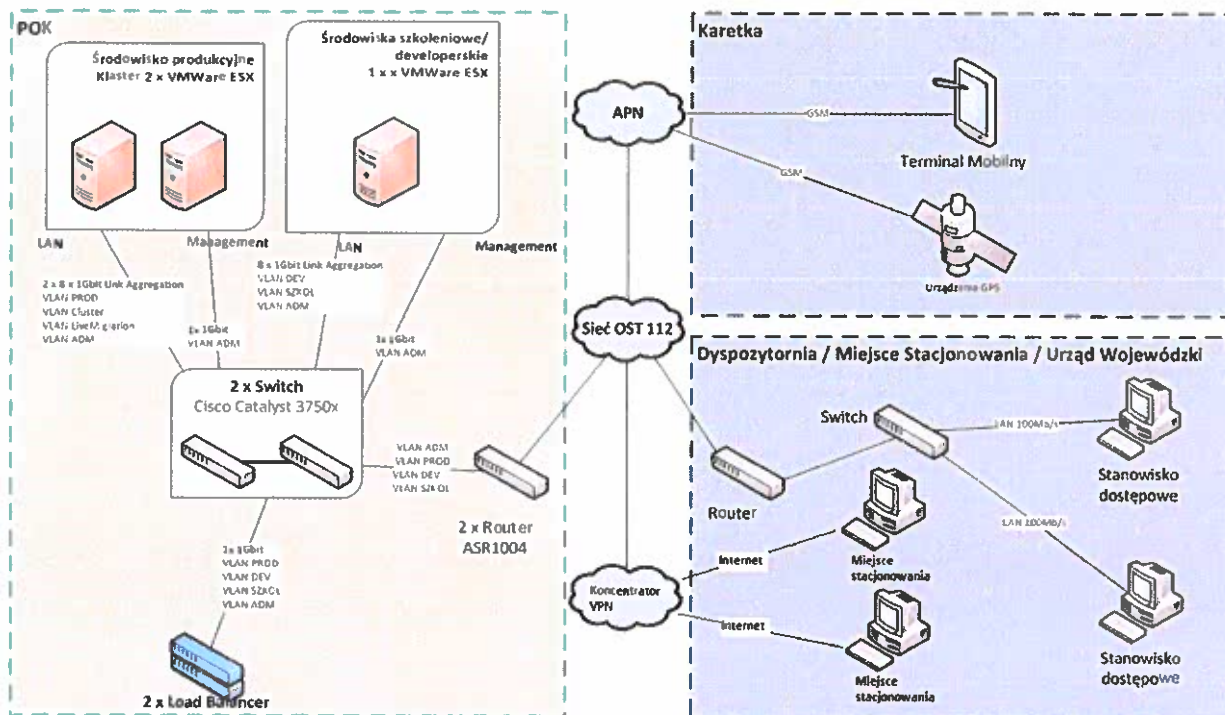
Środowisko administracyjne zawiera maszyny wirtualne wymagane do działania wszystkich środowisk oraz maszyny do zarządzania serwerami VMWare – czyli vCenter i Data Protection.



Rysunek nr 9. Schemat połączeń fizycznych systemu.

3.13.1. Stanowiska dostępne i ambulanse ZRM

Poniższy diagram przedstawia schemat architektury sprzętowej systemu SWD PRM pomiędzy pojedynczym ośrodkiem krajowym a stanowiskami dostępowymi (Stanowiska Dyspozytorskie, stanowiska ZRM w miejscach stacjonowania, stanowiska dostępne 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:
 - a) Dyspozytor,
 - b) Mobilny ZRM,
 - c) MS ZRM,
 - d) Planista,
 - e) Administrator biznesowy,
 - f) Aplikacja mapy;
- 2) 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.

Z 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 developerskie 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:

- zestawie 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 montażu 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 obsługiwać 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 IPsec 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 odebraniem 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) Awarię podsystemów nie będących przedmiotem niniejszej umowy, w tym: a) Centrum Certyfikatów (PKI), b) infrastrukturą serwerową, c) platformą wirtualizacyjną, d) siecią w obrębie infrastruktury serwerowej, e) UMM (Uniwersalny Moduł Mapowy), f) PLI CBD, g) 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 .
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: a) datę usunięcia Awarii, b) szczegółowy opis wprowadzonych zmian i przyjętych rozwiązań wraz ze wskazaniem numeru Incydentu Serwisowego zarejestrowanego w dedykowanym systemie obsługi Incydentów Serwisowych; 2) proces wgrywania korekt Oprogramowania – raport powinien zawierać co najmniej: a) datę wdrożenia nowej wersji Oprogramowania, b) numer wersji Oprogramowania, c) 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 przedstawiania 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 zamówienia, 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 2018 r., 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 powiadamiania 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 trakcie 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.

