Krajowe Centrum
Monitorowania
Ratownictwa Medycznego

Lotnicze Pogotowie Ratunkowe

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

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

ZAŁĄCZNIK NR 2 DO SIWZ

Opis przedmiotu zamówienia

Wdrożenie sieci SDN w centrach przetwarzania danych Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego (SWD PRM) w związku z realizacją zadania rozbudowy SWD PRM do wersji 2.0

Spis treści

Lotnicze Pogotowie Ratunkowe
ul. Księżycowa 5
01-934 Warszawa
tel. (22) 22-99-931/932
fax. (22) 22-99-933

NIP: 522-25-48-391
KRS: 0000144355
www.kcmrm.pl
e-mail: centrala@lpr.com.pl

1. Słowniki i skróty

Dla potrzeb niniejszego opracowania przyjmuje się następujące definicje skrótów i pojęć:

Skrót/pojęcie	Definicja
Awaria	Oznacza Awarię Krytyczną i/lub Awarię Niekrytyczną i/lub Awarię Zwykłą.
Awaria Krytyczna	Oznacza brak działania środowiska produkcyjnego Systemu, praca nie może być kontynuowana, 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 Projekcie Technicznym nie działa; 3. System w zakresie Funkcjonalności Krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę, tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji; 4. Wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: 1) uwierzytelnianie; 2) niezaprzeczalność; 3) poufność; 4) integralność; 5) dostępność; 6) rozliczalność. 5. wszelkie awarie związane z bezpieczeństwem dostępu do Systemu (w tym nieautoryzowanym dostępem do danych).
Awaria Niekrytyczna	Utrudnia działanie Systemu w środowisku produkcyjnym w zakresie Funkcjonalności Krytycznej i uniemożliwia działanie Systemu w zakresie pozostałych funkcjonalności. W tym kontekście „*utrudnia*” oznacza istnienie sposobu jego obejścia, stosując przygotowane przez Wykonawcę procedury

Skrót/pojęcie	Definicja
	tudzież procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu gwarancji (co może mieć wpływ na wygodę w użytkowaniu Systemu lub wymagać procedur ręcznych). „*Uniemożliwia*" oznacza brak możliwości jego obejścia.
Awaria Zwykła	Wszelkie awarie niebędące Awarią Krytyczną lub Awarią Niekrytyczną.
BIiŁ KGP	Biuro Informatyki i Łączności Komendy Głównej Policji – administrator sieci OST 112.
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, za wyjątkiem dni ustawowo wolnych od pracy, w godz. od 08:00 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, w szczególności Projekt Technicznydokumentacja powykonawcza, dokumentacja eksploatacyjna dokumentacja powstała w wyniku realizacji wymagań odbioru przedmiotu zamówienia, dokumenty robocze wytworzone przez Wykonawcę w ramach realizacji Umowy.
Funkcjonalność Krytyczna	Cechy funkcjonalne Systemu umożliwiające realizację operacji krytycznych z punktu widzenia działania SWD PRM i innych podsystemów działających na jego rzecz.
Incydent Serwisowy	Oznacza zgłoszenie do Wykonawcy przez Zamawiającego lub osoby wskazanej przez Zamawiającego, w trybie 24/7, nieprawidłowości w działaniu Systemu. Wykonawca zobowiązany jest do rejestracji zgłoszenia oraz usuwania Awarii i usterek lub dostarczenia procedur obejścia, powodujących przywrócenie działania Systemu i rozwiązania zgłoszenia.
Informacje	Należy przez to rozumieć informacje, o których mowa w art. 78 ust. 3 ustawy z dnia 16 lipca 2004 r., Prawo telekomunikacyjne (t. j. Dz.U. z 2019 r., poz. 2460, z późn. zm.).
KCMRM	Krajowe Centrum Monitorowania Ratownictwa Medycznego.

Skrót/pojęcie	Definicja
Lokalizacja/ Lokalizacje	Oznacza wskazane przez Zamawiającego lokalizacje na terenie RP określone w przedmiocie niniejszego zamówienia. Zamówienie będzie realizowane w następujących lokalizacjach: dwóch lokalizacjach stacjonarnie: Ośrodku Przetwarzania Danych w Warszawie oraz w Radomiu oraz w lokalizacjach zdalnych opisanych w OPZ. Bliższe dane adresowe zostaną przekazane po podpisaniu Umowy.
Modernizacja/ Rozbudowa	Doposażenie istniejącej infrastruktury SWD PRM w nowy system mocy obliczeniowej na potrzeby migracji SWD PRM na nową infrastrukturę.
Oprogramowanie/	Oznacza oprogramowanie standardowe powszechnie dostępne i eksploatowane na dzień złożenia oferty, będące przedmiotem dostaw w ramach realizacji niniejszego przedmiotu zamówienia, którego producentem jest Wykonawca lub podmiot trzeci.
Projekt Techniczny	Element Dokumentacji opisujący sposób wykonania, wdrożenia i właściwości zrealizowanego rozwiązania sieciowego.
PZP (Plan Zarządzania Projektem)	Element Dokumentacji definiujący organizację procesy, narzędzia i techniki dobrane w celu skutecznej i efektywnej realizacji przedmiotu Umowy, zawierający, co najmniej: szczegółowy opis zadań realizowanych w ramach etapów, harmonogram, plan komunikacji, szczegółowe procedury rejestracji zgłoszenia i obsługi Awarii oraz Incydentów Serwisowych realizowanych w ramach serwisu gwarancyjnego.
POK	Podstawowy Ośrodek Krajowy.
SWD PRM	System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego.
ZOK	Zapasowy Ośrodek Krajowy.
SLA	Service Level Agreement, poziom dostępności usług.
System	Infrastruktura składająca się z Urządzeń i Oprogramowania dostarczana w ramach realizacji niniejszego postępowania oraz infrastruktura i rozwiązania bezpośrednio

Skrót/pojęcie	Definicja
	wykorzystujące funkcjonowanie sieci zmodernizowanej w ramach niniejszego postępowania.
System Mocy Obliczeniowej	Infrastruktura sprzętowa (serwery, macierze dyskowe) dostarczana oraz uruchamiana w dwóch Lokalizacjach Zamawiającego na potrzeby modernizacji infrastruktury sprzętowej dla potrzeb SWD PRM.
Umowa	Umowa zawarta pomiędzy Wykonawcą a Zamawiającym na potrzeby realizacji niniejszego przedmiotu zamówienia.
Urządzenia	Sprzęt teleinformatyczny wraz z niezbędnym wyposażeniem i Oprogramowaniem oraz odnoszącą się do nich dokumentacją techniczną producenta, w tym również okablowanie strukturalne, będące przedmiotem niniejszego zamówienia.
Usługa Serwisu Gwarancyjnego	Usługa świadczona w ramach gwarancji udzielonej przez Wykonawcę, polegająca na zapewnieniu przez Wykonawcę poprawności i ciągłości prawidłowego działania Systemu oraz jego poszczególnych komponentów, w szczególności usuwanie Awarii.
Wykonawca	Podmiot realizujący zamówienie.
Zamawiający	Lotnicze Pogotowie Ratunkowe.

2. Wstęp

Celem Zamawiającego jest optymalizacja wykorzystania sieci OST 112 poprzez uruchomienie jednej sieci SDN w dwóch odległych ośrodkach centrum przetwarzania danych w związku z realizacją zadania rozbudowy SWD PRM do wersji 2.0 Środowisko sieciowe powinno być wykonane przy użyciu najnowocześniejszych standardów budowy sieci zdefiniowanej programowo (SDN) umożliwiając integrację systemów posiadanych przez Zamawiającego.

Zamawiający wymaga dostarczenia poniżej wyspecyfikowanych komponentów lub komponentów spełniających opisane warunki równoważności, wdrożenie rozwiązania oraz migrację obecnej infrastruktury na utworzone środowisko sieciowe.

Środowisko przełączania L2/L3 powinno mieć cechy scentralizowanego serwerowego środowiska sieciowego opartego o model SDN – „*Software Defined Networking*" składającego się z dwóch podstawowych obszarów sprzętowo - programowych pełniących odrębne funkcje:

1) **centralnego kontrolera SDN** – obszaru zarządzającego siecią fizyczną oraz warstwą logiczną i zapewniającego konfigurowanie usług transportowych i bezpieczeństwa (m. in. segmentacji) w oparciu o modelowanie polityk dla aplikacji;
2) **infrastruktury sieciowej** – w postaci przełączników 10/25/40/100 Gigabit Ethernet tworzących sieć o architekturze fabric - obszaru realizującego przełączanie, transport sieciowy i znajdujących się pod kontrolą komponentu zarządzającego SDN, czyli przełączników rdzeniowych [SPINE], przełączników dostępowych [LEAF], przełączników w zdalnych lokalizacjach [Remote LEAF].

W ramach postępowania Wykonawca wdroży rozwiązanie opisane w opisie Przedmiotu Zamówienia (dalej OPZ) oraz **zintegruje je z posiadanym rozwiązaniem HyperFlex**. Zamawiający posiada 2 ośrodki krajowe (POK i ZOK) bazujące na rozwiązaniu HyperFlex tworzące w każdym z nich niezależny klaster HCI. W każdym z ośrodków znajdują się obecnie 11 serwerów fizycznych które są zwirtualizowane w technologii Vmware vSphere 6.7 i tworzą pojedynczy klaster. W ramach infrastruktury IT działającej na potrzeby SWD PRM wykorzystywane są dwa ośrodki krajowe przetwarzania danych oddalone od siebie o około 100 km. Ośrodki podłączone są do sieci WAN OST112 łączem o przepustowości 10 Gbps. W ramach RTT pomiędzy systemami w lokalizacjach poprzez sieć WAN uzyskiwane czasy to 4 ms. Połączenie pomiędzy ośrodkami jest realizowane w warstwie trzeciej (L3) Dodatkowo Zamawiający posiada połączenie w warstwie drugiej (L2) opartej o 2 linki 1 GB połączone w jeden etherchannel.

Dodatkowo Zamawiający posiada 2 ośrodki wyniesione które będą uczestniczyły w projekcie posiadające 3 serwery oraz macierz dyskową w każdym na których zostało skonfigurowane lokalne środowisko Vmware 6.7 essential plus. Ośrodki te są podłączone w ramach sieci OST112 w następujący sposób:

1) **Ośrodek Backupowy** łącze L2 do ośrodka POK – 2 linki 1 GB każdy działające w etherchannel;
2) **Ośrodek KCMRM** – 2 niezależne link L3 do sieci OST112.

Zamawiający posiada aktualną dokumentację wdrożonych rozwiązań serwerowych.

W ramach postępowania Wykonawca dodatkowo wykona **czynności opisane w pkt 9.** które są niezbędne do pełnego uruchomienia SDN w ramach wykorzystywanej sieci OST112. Wszelkie

czynności modyfikujące sieć OST112 muszą być zaakceptowane przez Zamawiającego oraz przez administratora sieci OST 112 którym jest BIiŁ KGP.

Przed przystąpieniem do modyfikacji na urządzeniach sieci OST112 Wykonawca musi przedstawić projekt techniczny oraz szczegółowy plan modyfikacji wraz z oceną skutków modyfikacji oraz zagrożeniami ich wdrożenia.

Opisane w pkt 9 modyfikacje mogą być wykonane jedynie w przypadku akceptacji ich przez Zamawiającego. Wszelkie prace prowadzące do niedostępności sieci OST w jakimkolwiek punkcie sieci będą zgłaszane przed wdrożeniem modyfikacji a czas ich realizacji uzgodniony przez strony.

W ramach postępowania Wykonawca dostarczy dodatkowe licencje do routerów ISR 4461 wymienione w Opisie Przedmiotu Zamówienia oraz **wykona ich aktualizację**.

Realizacja przedmiotu zamówienia nastąpi nie później niż do dnia 20 grudnia 2020 roku.

3. Wymagania ogólne

Jeżeli w OPZ użyto do opisania przedmiotu zamówienia oznaczeń lub parametrów wskazujących konkretnego producenta, konkretny produkt lub wskazano znaki towarowe, patenty, normy, standardy, aprobaty techniczne lub pochodzenie urządzeń, Zamawiający dopuszcza zastosowanie produktów równoważnych, przez które należy rozumieć produkty o parametrach nie gorszych od przedstawionych w OPZ oraz posiadający równoważne funkcje i parametry co produkt opisany w OPZ. W takim wypadku do oferty należy załączyć dokładny opis oferowanych produktów, z którego jasno wynikać będzie zachowanie warunków równoważności.

Wszystkie Urządzenia dostarczone w ramach realizacji przedmiotu zamówienia muszą spełniać poniższe warunki:

1) muszą być dostarczone jako fabrycznie nowe, nie używane w innych projektach oraz nie starsze niż 4 miesiące od daty produkcji;
2) muszą pochodzić z oficjalnego kanału dystrybucji na Polskę lub Unię Europejską dla danego producenta;
3) dostarczane systemy operacyjne muszą być wersją najnowszą proponowaną przez producenta rozwiązania, spełniającą warunki zawarte w OPZ;
4) zarówno Urządzenia jak i ich elementy składowe wraz z systemami operacyjnymi oraz aplikacjami nie mogą znajdować się na aktualnej, na czas składania ofert, liście elementów producenta przewidzianych do wycofania z produkcji, sprzedaży lub serwisowania;

5) Urządzenia muszą być objęte co najmniej 36 miesięcznym serwisem świadczonym pięć dni w tygodniu o ile szczegółowy opis zadania nie mówi inaczej;
6) wszelkie koszty dostawy przedmiotu zamówienia pokryje Wykonawca (wyładunek i transport do miejsca wyznaczonego przez Zamawiającego);
7) Zamawiający wymaga, by dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej (tzn. opublikowanej przez producenta nie wcześniej niż 6 miesięcy) na dzień poprzedzający dzień składania ofert – lub w wersji sugerowanej przez producenta rozwiązania;
8) dodatkowo, jeśli wyraźnie nie wskazano należy uznać, że wszystkie Urządzenia muszą być dostarczone wraz z niezbędnym do instalacji okablowaniem.

Dodatkowo na potrzebę wdrożenie sieci SDN Zamawiający, zapewni zgodnie z obowiązującymi wymogami w tym zakresie pomieszczenia serwerowni posiadające odpowiednie warunki techniczne takie jak: metraż, nośność stropów, zasilanie gwarantowane, klimatyzację, dostęp do sieci OST 112 oraz obejściowe drogi komunikacji. Na etapie Projektu Technicznego Zamawiający przekaże szczegółowe wymagania co do przygotowania dokumentacji wymaganej przez administratora serwerowni w tym:

1) projekt techniczny zawierający bilans mocy urządzeń;
2) schematy połączeń i zabezpieczeń prądowych;
3) dokumentację wykonawczą i powykonawczą.

4. Dostawa Urządzeń komponentu sieciowego

4.1 Centralny Kontroler SDN

Zamawiający wymaga dostarczenia poniżej wyspecyfikowanych elementów dla rozwiązania komponentu scentralizowanego kontrolera SDN:

Lp.	Part Number	Description	Ilość
1.	APIC-CLUSTER-M3	APIC Cluster - Medium Configurations (Up to 1200 Edge Ports)	1
2.	CON-PSRT-APICCLM3	PRTNR SS 8X5XNBD APIC Cluster - Medium Configurations (Up	1

3.	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Upto 1200 Edge Ports)	1
4.	APIC-DK9-4.2	APIC Base Software Release 4.2	1
5.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
6.	APIC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	1
7.	APIC-PSU1-770W	770W power supply for USC C-Series	2
8.	APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	1
9.	APIC-MR-X16G1RS-H	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v	6
10.	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	1
11.	APIC-SD400G123X-EP	400GB 2.5in Enterprise Performance 12G SAS SSD(3X endurance)	1
12.	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	1
13.	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	2
14.	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	2
15.	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Upto 1200 Edge Ports)	1
16.	APIC-DK9-4.2	APIC Base Software Release 4.2	1
17.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
18.	APIC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	1
19.	APIC-PSU1-770W	770W power supply for USC C-Series	2
20.	APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	1
21.	APIC-MR-X16G1RS-H	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v	6
22.	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	1

23.	APIC-SD400G123X-EP	400GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	1
24.	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	1
25.	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	2
26.	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	2
27.	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Upto 1200 Edge Ports)	1
28.	APIC-DK9-4.2	APIC Base Software Release 4.2	1
29.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
30.	APIC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	1
31.	APIC-PSU1-770W	770W power supply for USC C-Series	2
32.	APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	1
33.	APIC-MR-X16G1RS-H	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v	6
34.	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	1
35.	APIC-SD400G123X-EP	400GB 2.5in Enterprise Performance 12G SAS SSD(3X endurance)	1
36.	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	1
37.	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	2
38.	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	2
39.	APIC-M3	APIC Appliance - Medium Configuration (Upto 1200 EdgePorts)	1
40.	CON-PSRT-APICM3	PRTNR SS 8X5XNBD APIC Appliance - Medium Configuration (Up	1
41.	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Upto 1200 Edge Ports)	1

42.	APIC-DK9-4.2	APIC Base Software Release 4.2	1
43.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	2
44.	APIC-PCIE-C25Q-04	Cisco UCS VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	1
45.	APIC-PSU1-770W	770W power supply for USC C-Series	2
46.	APIC-USBFLSHB-16GB	UCS Servers 16GB Flash USB Drive	1
47.	APIC-MR-X16G1RS-H	16GB DDR4-2666-MHz RDIMM/PC4-21300/single rank/x4/1.2v	6
48.	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	1
49.	APIC-SD400G123X-EP	400GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	1
50.	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	1
51.	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	2
52.	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	2

Lub dostarczenia rozwiązania równoważnego spełniającego niżej opisane wymagania:

Szczegółowe wymagania i oczekiwana funkcjonalność rozwiązania w obszarze centralnego kontrolera SDN:

Kod wymagania	Opis wymagania
C2.1.a_1	Kontroler SDN jest zrealizowany w oparciu o dedykowaną warstwę sprzętową i programową. Implementacja kontrolera w formie zwirtualizowanej i współdzielącej z innymi aplikacjami platformę obliczeniową nie jest dozwolona.
C2.1.a_2	Kontroler SDN zrealizowany jest redundantnie zarówno w warstwie sprzętowej jak i programowej tak aby zapewnić spójne działanie środowiska i możliwość modyfikacji konfiguracji po ewentualnej utracie jednej z instancji.

C2.1.a_3	Dodatkowo Zamawiający wymaga dodatkowego kontrolera pełniącego rolę cold standby.
C2.1.a_4	Utrata wszystkich instancji kontrolera SDN nie wpływa na działanie infrastruktury sieciowej w zakresie istniejącej konfiguracji (nie dotyczy to zmian lub np. podłączania nowych urządzeń).
C2.1.a_5	Komponent zarządzający kontrolera SDN jest wyposażony w minimum: 1) minimum 96 GB DRAM (w układzie 6 x 16 GB) nie gorsze niż DDR4@2666MHz; 2) pamięć typu flash USB minimum 16 GB i moduł typu TPM (Trusted Platform Module); 3) pamięć dyskowa typu SSD o pojemności minimum 400GB o wielkości 2,5"; 4) dodatkowa pamięć dyskowa w postaci dwóch napędów dyskowych o szybkości obrotowej talerzy 7,2 K i pojemności minimum 1 TB każdy pracujących na kontrolerze RAID (RAID 0/1) typu 12G; 5) dedykowana karta sieciowa (nie gorsza niż PCI-E 16x Gen-2) z nie mniej niż 4 interfejsy typu Small Form-Factor Pluggable (SFP+) o przepustowości nie mniejszej niż 10 Gbps każdy typu CNA; 6) urządzenie musi pochodzić od tego samego producenta co urządzenia typu SPINE i LEAF; 7) obudowa serwerowa o wysokości nie większej niż 1, umożliwiająca montaż nie mniej niż 8 napędów dyskowych 2,5", wyposażona w nie mniej niż 2 zasilacze pracujące w konfiguracji redundantnej; 8) połączenie kontrolerów z urządzeniami typu „LEAF" musi odbywać się za pomocą portów 10 GE; 9) co najmniej dwa procesory (każdy o wydajności o wydajności nie gorszej niż: 305 w kategorii CINT2006 Rates_Baseline dla konfiguracji 2 procesorowej (wg spec.org) o łącznej liczbie rdzeni nie mniejszej niż 12.
C2.1.a_6	Komunikacja między kontrolerem SDN i elementami infrastruktury sieciowej (fabric) jest możliwa w trybie in-band, niewymagającym użycia dedykowanych interfejsów na przełącznikach wchodzących w skład architektury.
C2.1.a_7	Kontroler SDN obsługuje wyłącznie ruch związany z zarządzaniem i monitorowaniem infrastruktury sieciowej (control plane), nie zajmuje się przełączaniem ruchu (data plane).

C2.1.a_8	Kontroler SDN umożliwia zarządzanie infrastrukturą sieciową dołączającą co najmniej 300 fizycznych serwerów dwuprocesorowych.
C2.1.a_9	Kontroler SDN umożliwia zarządzanie infrastrukturą wirtualną złożoną z co najmniej 1200 maszyn wirtualnych VM.
C2.1.a_10	Umożliwia automatyzację konfiguracji zarządzanej sieci w oparciu o model sieciowych polityk grupowych powiązanych z aplikacjami.
C2.1.a_11	Polityka definiowana na kontrolerze opisuje model działania aplikacji w oparciu o relacje pomiędzy punktami styku elementów aplikacji z siecią. W przykładowym modelu trójwarstwowym aplikacji oznacza to: 1) zdefiniowanie warstw aplikacji takich jak np.: web, aplikacyjna i bazodanowa (Web, App, DB), złożonych z grup fizycznych i wirtualnych serwerów; 2) określenie punktów styku takich jak VLAN, interfejs serwerów (fizyczne lub wirtualna port-grupa), adresy IP (IPv4 oraz IPv6) – dla danej warstwy aplikacji; 3) zdefiniowanie przydziału serwera wirtualnego do danej warstwy aplikacyjnej na bazie jego atrybutów – nazwa maszyny VM, id maszyny VM, nazwa systemu operacyjnego, typ hypervisora, tag; 4) zdefiniowanie i szczegółowe skonfigurowanie usług zewnętrznych realizowanych dla warstw 4-7 (model ISO OSI) takich jak load-balancing, content switch, firewall, itp. Istnieje możliwość dołączenia powyższych urządzeń usługowych do portu brzegowego infrastruktury sieciowej. Mechanizm przekierowania ruchu do tych urządzeń oraz reguły dla nich zdefiniowane są integralną częścią polityki sieciowej (aplikacyjnej) w ramach „fabric"; 5) możliwość zdefiniowania relacji pomiędzy warstwami aplikacyjnymi jako wzajemnie udostępnianych i konsumowanych zasobów, definicja warstw (grup serwerów) opiera się o fizyczne i wirtualne punkty styku a sama relacja obejmuje usługi L4-7 (firewall/balansowanie ruchu itp).
C2.1.a_12	Umożliwia zintegrowanie usług zewnętrznych poprzez zapewnienie szczegółowej konfiguracji i mechanizmu przekierowania ruchu dla warstw 4-7 dla następujących urządzeń: 1) Loadbalancer F5; 2) Loadbalancer Citrix; 3) Loadbalancer Avi Networks;

	4) Firewall Cisco ASA; 5) Firewal Palo Alto; 6) Firewall Checkpoint.
C2.1.a_13	Umożliwia zintegrowanie usług zewnętrznych zarówno dla urządzeń fizycznych jak i wirtualnych.
C2.1.a_14	Umożliwia wydzielanie izolowanych wirtualnych środowisk sieciowych SDN wraz z dedykowanymi zespołami administratorów i prawami dostępu dla 100 takich środowisk (multitenant).
C2.1.a_15	Dla izolowanych środowisk sieciowych SDN umożliwia implementację funkcjonalności dedykowanej bramy wyjściowej L2/L3 oraz dedykowanych usług zewnętrznych realizowanych dla warstw 4-7.
C2.1.a_16	Umożliwia tworzenie wirtualnych instancji sieciowych umożliwiających nakładanie się adresacji IP w wielu zaimplementowanych równocześnie instancjach (VRF) w ilości min. 10 instancji VRF na wirtualne środowisko.
C2.1.a_17	Umożliwia tworzenie segmentów sieci L2 w oparciu o technologię VXLAN.
C2.1.a_18	Umożliwia jednoczesne konfigurowanie sieci dla środowisk złożonych z: 1) serwerów fizycznych; 2) serwerów wirtualnych realizowanych w oparciu o VMWare vSphere i VMware vCenter; 3) serwerów wirtualnych realizowanych w oparciu o Microsoft Hyper-V i Microsoft SystemCenter VMM; 4) serwerów wirtualnych realizowanych w oparciu o RedHat KVM i OVS (Open vSwitch) w środowisku OpenStack; 5) kontenerów wirtualnych realizowanych min. w środowiskach Kubernetes oraz Openshift.
C2.1.a_19	Umożliwia monitorowanie i diagnostykę sieciową dla uruchamianych środowisk w oparciu o następujące mechanizmy: 1) prezentację sprawności środowiska w formie SLA dla danego środowiska sieciowego oraz modelu polityk aplikacyjnych w skali bezwzględnej (np. 1-100); 2) prezentowanie bieżącej i historycznej statystyki ruchu dla danego środowiska sieciowego, zdefiniowanych warstw aplikacji oraz interfejsów fizycznych;

	3) prezentację historycznych danych nt. sprawności (SLA) środowiska; 4) pomiar ruchu na portach wejściowych i wyjściowych infrastruktury sieciowej (fabric) dla środowisk uruchamianych w oparciu o model polityk aplikacyjnych; 5) diagnostykę ścieżki (traceroute) między dowolną parą portów fizycznych bądź wirtualnych wchodzących w skład infrastruktury; 6) monitorowanie i raportowanie ilości wykorzystanych i dostępnych zasobów wchodzących w skład infrastruktury; 7) zbieranie, agregowanie i interpretowanie zdarzeń (events) i problemów (faults) w ramach infrastruktury sieciowej (fabric); 8) monitorowanie ruchu poprzez kopiowanie (mirroring) ruchu dla wybranych warstw aplikacyjnych.
C2.1.a_20	Umożliwia automatyczną detekcję topologii oraz inwentarza infrastruktury sieciowej (fabric).
C2.1.a_21	Implementuje centralne repozytorium oprogramowania (firmware) dla infrastruktury sieciowej (fabric).
C2.1.a_22	Implementuje centralny mechanizm aktualizacji oprogramowania (firmware) dla infrastruktury sieciowej (fabric).
C2.1.a_23	Umożliwia zachowywanie (snapshot) i odtwarzanie (rollback) dla całości konfiguracji infrastruktury sieciowej (fabric).
C2.1.a_24	Udostępnia następujące interfejsy zarządzające: 1) GUI (http/https); 2) CLI (linia komend konsoli); 3) Plugin dla OpenStack umożliwiający integrację na poziomie Neutron ML2.
C2.1.a_25	Udostępnia następujące mechanizmy programowania: 1) REST API ze wsparciem dla formatów JSON lub XML. Możliwość konfiguracji infrastruktury bezpośrednio poprzez HTTP (p.. z wykorzystaniem Postman REST Client); 2) Python lub JavaScript SDK; 3) Powszechnie dostępny model obiektowy dla struktur logicznych i sprzętowych wchodzących w sklad infrastruktury sieciowej (fabric).
C2.1.a_26	Udostępnia autoryzację dostępu użytkowników w oparciu o mechanizmy:

	1) Lokalną definicję; 2) RADIUS; 3) TACACS+; 4) LDAP; 5) Dual Factor Authentication.
C2.1.a_27	Umożliwia synchronizację całej infrastruktury sieciowej (fabric) w oparciu o znacznik czasu przesyłany w protokole NTP.

4.2 Szczegółowe wymagania i oczekiwana funkcjonalność rozwiązania w obszarze fabric:

Kod wymagania	Opis wymagania
C2.1.b_1.	Zamawiający wymaga aby komponent przełączania L2/L3 umożliwiał programowe definiowanie sieci zgodnie z wymaganiami aplikacji i systemów uruchamianych w dostępnej mocy obliczeniowej.
C2.1.b_2.	Komponent ten musi być utworzony w oparciu o przełączniki 10/25/40/100 GigabitEthernet zorganizowane w dwustopniowej nieblokowalnej architekturze rdzeń-brzeg określanej jako fabric (przełączniki w topologii grubego drzewa) do którego podłączone mają być fizyczne urządzenia wchodzące w skład komponentu mocy obliczeniowej (serwery, serwery blade z/poprzez urządzenia zarządzania nimi).
C2.1.b_3.	Topologia grubego drzewa musi być rozumiana jako dwuwarstwowy układ przełączników sieciowych (warstwa SPINE i warstwa LEAF), gdzie każdy przełącznik LEAF podłączony jest do każdego przełącznika SPINE, a inne urządzenia podłączone są do przełączników LEAF. Przełączniki typu SPINE nie są połączone między sobą, przełączniki typu LEAF nie są połączone między sobą. Utworzona topologia ma zapewniać taki stan komunikacji pomiędzy urządzeniami podłączonymi do przełączników LEAF, że ruch będzie się odbywać maksymalnie przez 3 urządzenia (LEAF-SPINE-LEAF).
C2.1.b_4.	Urządzenia typu „LEAF" muszą być podłączone w sposób redundantny z urządzeniami typu „SPINE" połączeniami co najmniej 40Gigabit Ethernet – tzn. min. 1x40GE dotyczy połączeń do pojedynczego węzła typu „spine".
C2.1.b_5.	Dostawca musi zapewnić niezbędne okablowanie typu Twinax 40 Gigabit Ethernet do realizacji połączeń „LEAF" do „SPINE".
C2.1.b_6.	Powyższa architektura nazywana fabryką musi być zarządzana przez dedykowaną infrastrukturą sprzętowo-programową (zbudowaną z pełną niezawodnością), która będzie w stanie zaprogramować sieć w infrastrukturze mocy obliczeniowej i przełączania L2/L3 na potrzeby i zgodnie z wymaganiami aplikacji. Fabryka musi mieć możliwość budowania logicznych sieci dla konkretnych aplikacji z uwzględnieniem ich logicznej separacji.

C2.1.b_7.	Fabryka (sprzętowa architektura) musi posiadać wbudowany sprzętowy mechanizm telemetrii pozwalający na równoczesne śledzenie ilości ruchu, strat, opóźnień oraz parametrów „jitter" dla co najmniej 300 przepływów definiowanych jako ruch pomiędzy dwoma punktami styku. Opisane funkcjonalności muszą być dostępne poprzez GUI jak i interfejs aplikacyjny oparty o RestAPI.
C2.1.b_8.	Zarządzanie konfiguracją fabryki musi być realizowane w modelu „policy-based". Dla każdej aplikacji dla której konfigurowana jest sieć w fabryce musi być możliwość zdefiniowania oddzielnych polityk. Wymagane jest aby domyślna polityka komunikacji w całej fabryce była typu „deny all" (niedozwolony ruch pomiędzy punktami końcowymi). Powyższe oznacza, że jakiekolwiek urządzenia podłączone do fabryki nie mogą się komunikować ze sobą bez wprowadzenia odpowiedniej polityki przez kontroler fabryki.
C2.1.b_9.	Nowe urządzenia podłączone do fabryki (elementy fabryki) muszą być automatycznie rozpoznawane, konfigurowane (po zaakceptowaniu ich w kontrolerze) i aktualizowane co do wersji oprogramowania/firmware.
C2.1.b_10.	Fabryka musi obsługiwać co najmniej 10 niezależnych wirtualnych fabryk dostarczających funkcjonalność logicznej separacji fabryki, również pod kątem zarządzania (z separacją zasobów i użytkowników oraz osobnymi prawami dostępu).
C2.1.b_11.	Wszystkie połączenia między warstwą brzegową i rdzeniową w ramach fabric implementowane są jako 40GE o pełnej wydajności (wirespeed).
C2.1.b_12.	Wymaga się aby fabryka dostarczała podane niżej funkcjonalności (część z nich ma znaczenie na portach brzegowych fabryki – na styku z urządzeniami do niej podłączonymi opartymi o klasyczną technologie Ethernet/IP): 1) Trunking IEEE 802.1Q VLAN; 2) Wsparcie dla 4096 identyfikatorów VLAN; 3) IEEE 802.1w lub kompatybilny; 4) Spanning Tree PortFast lub odpowiadający; 5) Internet Group Management Protocol (IGMP) Versions 2, 3; 6) Funkcjonalności polegające na terminowaniu pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach; 7) Link Aggregation Control Protocol (LACP): IEEE 802.3ad; 8) Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);

	9) Ramki Pause (IEEE 802.3x); 10) Sprzętowe przełączanie pakietów w warstwie L3 w modelu „anycast" – na wszystkich węzłach typu „LEAF"; 11) Routing w oparciu o trasy statyczne; 12) Urządzenie musi umożliwiać rozbudowę o funkcjonalności warstwy L3 – OSPF, VRF, BGP, dla protokołów IPv4 oraz IPv6; 13) Obsługa łącznie minimum 64000 prefixów oraz wpisów hosta w tablicy routingu; 14) Wsparcie dla minimum 20000 tras multicastowych; 15) Wsparcie dla minimum 1000 wpisów VRF; 16) Wsparcie dla minimum 100 wirtualnych przełączników (wirtualnych fabryk) dostarczających funkcjonalność logicznej separacji fabryki, również pod kątem zarządzania; 17) Wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP); 18) Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list; 19) Policy Based Routing (na bazie np. ACL).
C2.1.b_13.	Rozwiązanie musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci(QoS): 1) Layer 2 IEEE 802.1p (CoS); 2) Klasyfikacja QoS w oparciu o listy (ACL / Access Control List) – w warstwach 2, 3, 4; 3) Kolejkowanie na wyjściu w oparciu o CoS; 4) Bezwzględne (strict-priority) kolejkowanie na wyjściu; 5) Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm równoważny.
C2.1.b_14.	Rozwiązanie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci: 1) Wejściowe ACL (standardowe oraz rozszerzone); 2) Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu;

	3) Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); 4) ACL oparte o VLAN-y (VACL); 5) ACL oparte o porty (PACL).
C2.1.b_15.	Wymagania dotyczące zarządzania i zabezpieczenia: 1) Port zarządzający 100/1000 Mbps; 2) Port konsoli CLI; 3) Zarządzanie In-band; 4) SSHv2; 5) Authentication, authorization, and accounting (AAA); 6) RADIUS; 7) Syslog; 8) SNMP v1, v2, v3; 9) Role-Based Access Control RBAC; 10) Network Time Protocol (NTP); 11) Diagnostyka procesu BOOT; 12) Wsparcie dla Puppet 1.0.
C2.1.b_16.	Implementacja następujących protokołów i mechanizmów L2: 1) sprzętowe wsparcie dla VXLAN Bridging i VXLAN Routing w oparciu o sprzętowy VTEP; 2) definiowanie domen rozgłoszeniowych L2 z opcjonalną możliwością eliminacji ruchu rozgłoszeniowego dla mechanizmów ARP/GARP, Unknown Unicast; 3) eliminacja ruchu rozgłoszeniowego dla mechanizmów ARP i Unknown Unicast poprzez lokalizację w oparciu o bazę adresową L2/L3; 4) dołączanie urządzeń zewnętrznych (serwerów, modułów, przełączników) poprzez zagregowaną wiązkę połączeń LACP 802.3ad do dwóch przełączników brzegowych (multi link aggregation, virtual port channel, itp.); 5) pełna mobilność serwera fizycznego i wirtualnego w domenie L2; 6) definiowanie zewnętrznych połączeń w domenie L2; 7) mechanizm eliminacji pętli na przełącznikach brzegowych w fabric;
C2.1.b_17.	Implementacja następujących protokołów i mechanizmów L3:

	1) IPv4 Unicast i Multicast; 2) przesyłanie IPv6 Unicast; 3) niezależne sieci prywatne (VRF) z duplikacją adresacji IP; 4) protokoły routingu eBGP, iBGP, OSPF dla IPv4 i IPv6; 5) routing statyczny dla IPv4 i IPv6; 6) przełączanie ruchu pomiędzy parą podsieci IP (SVI) realizowane sprzętowo w modelu IP Anycast w ramach fabric tj. na każdym przełączniku brzegowym, niezależnie od ilości przełączników brzegowych w fabric; 7) pełna mobilność serwera fizycznego i wirtualnego w domenie L3; 8) interfejsy i subinterfejsy L3 (per VLAN) na portach fizycznych przełączników brzegowych; 9) definiowanie zewnętrznych połączeń w domenie L3.
C2.1.b_18.	Implementacja następujących mechanizmów optymalizacji ruchu: 1) Load-balancing pakietów dostosowany do różnych warunków przesyłania (natłoku) w ramach środowiska; 2) priorytetyzacja połączeń.
C2.1.b_19.	Zamawiający wymaga rozciągnięcia pojedynczej topologii fabric na dwie oddzielne lokalizacje leżące od siebie w odległości co najmniej 100 km.
C2.1.b_20.	Zamawiający wymaga rozciągnięcia funkcjonalności komponentu scentralizowanego przełączania L2/L3 według modelu SDN na 3 wyniesione lokalizacje.

5. Infrastruktura sieciowa

5.1Przełączniki typu SPINE

Zamawiający wymaga dostarczenia przynajmniej dwóch urządzeń rdzeniowych warstwy „SPINE" per Ośrodek Krajowy w poniższym ukompletowaniu:

Lp.	Part Number	Description	Ilość
1.	N9K-C9332C	Nexus 9K ACI & NX-OS Spine, 32p 40/100G & 2p 10G	4
2.	CON-PSRT-N9KC9332	PRTNR SS 8X5XNBD Nexus 9K ACI NX-OS Spine, 32p 40/100G	4
3.	MODE-ACI-SPINE	Dummy PID for mode selection	4
4.	ACI-N9KDK9-15.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 15.0	4
5.	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
6.	NXA-PAC-1100W-PE2	Nexus AC 1100W PSU – Port Side Exhaust	8
7.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	8
8.	NXA-FAN-35CFM-PE	Nexus Fan, 35CFM, port side exhaust airflow	20

lub dostarczenie urządzeń równoważnych spełniających poniższe wymagania:

Kod wymagania	Opis wymagania
C3.1_1.	Przełącznik musi posiadać min. 32 porty 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps na pojedynczej parze okablowania multi-mode (do 100m).
C3.1_2.	Przełącznik musi posiadać dodatkowo min. 2 porty 1/10GE SFP+.

C3.1_3.	Parametry wydajnościowe: 1) prędkość przełączania minimum 6.4Tbps full duplex; 2) urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.
C3.1_4.	Przełącznik musi posiadać następującą funkcjonalność dla warstwy L2: 1) Trunking IEEE 802.1Q VLAN; 2) wsparcie dla min. 3000 sieci VLAN; 3) wsparcie sprzętowe dla 90 tysięcy adresów MAC; 4) IEEE 802.1w Rapid Spanning Tree (RST); 5) IEEE 802.1s Multiple Spanning Tree (MST); 6) zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU); 7) Internet Group Management Protocol (IGMP) Versions 2, 3; 8) terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach; 9) Link Aggregation Control Protocol (LACP): IEEE 802.3ad; 10) ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); 11) funkcjonalność izolowania portów znajdujących się w tym samym VLAN; 12) wsparcie sprzętowe dla tunelowania QinQ i QinVNI.
C3.1_5.	Przełącznik musi posiadać następującą funkcjonalność dla warstwy L3: 1) sprzętowe przełączanie pakietów w warstwie L3; 2) routing w oparciu o trasy statyczne; 3) umożliwia rozbudowę poprzez licencje o funkcjonalności warstwy L3 – OSPF, BGP, IS-IS dla protokołów IPv4 oraz IPv6; 4) Policy Based Routing (PBR); 5) VRRP; 6) wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6; 7) tunele GRE; 8) wsparcie sprzętowe dla minimum 60 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP; 9) wsparcie dla VRF; 10) wybór do 16-tu jednoczesnych ścieżek o równej metryce (ECMP);

	11) wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast); 12) wsparcie dla IGMPv3 oraz MSDP; 13) wsparcie sprzętowe dla minimum 12,000 tras multicast; 14) obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (access control list). 15) Jeżeli dla wsparcia powyższych funkcjonalności wymagana jest licencja to należy ją dostarczyć wraz z urządzeniem.
C3.1_6.	Przełącznik musi wspierać następujące mechanizmy związane z funkcjonalnością VXLAN: 1) zintegrowany, sprzętowy VXLAN Bridging/Routing; 2) obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast); 3) implementacja VXLAN BGP EVPN (Ethernet VPN); 4) obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN.
C3.1_7.	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: 1) Layer 2 IEEE 802.1p (CoS) oraz DSCP; 2) klasyfikacja QoS w oparciu o listy ACL (Access Control list) dla warstwy drugiej i trzeciej (IPv4 i IPv6); 3) kolejkowanie bezwzględne (strict-priority); 4) kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection); 5) ograniczanie ruchu (policing) do zadanej przepływności; 6) dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych; 7) Protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
C3.1_8.	Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci: 1) obsługa list kontroli dostępu (ACL):

	a) ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu, b) ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), c) ACL oparte o porty (PACL); 2) DHCP Snooping; 3) ARP Inspection; 4) IP Source Guard; 5) unicast Reverse Path Forwarding (uRPF); 6) prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast; 7) przełącznik musi posiadać możliwość wsparcia enkrypcji MACsec o prędkości wire-rate na minimum 8 portach 40/100 GE.
C3.1_9.	Urządzenie musi realizować następujące funkcjonalności dotyczące zarządzania i zabezpieczenia: 1) Port zarządzający 100/1000 Mbps; 2) Port konsoli CLI; 3) Zarządzanie In-band; 4) SSHv2; 5) Authentication, Authorization, and Accounting (AAA); 6) RADIUS; 7) TACACS; 8) Syslog; 9) SNMP v1, v2, v3; 10) telemetria w oparciu o mechanizm subskrypcji (push out), zapewniając alternatywny do SNMP, szybszy mechanizm zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB; 11) Role-Based Access Control RBAC; 12) IEEE 802.1ab LLDP; 13) możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback); 14) 802.1x; 15) ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing);

	16) kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring); 17) Network Time Protocol (NTP); 18) Precision Time Protocol IEEE 1588; 19) Diagnostyka procesu BOOT; 20) Ping; 21) Traceroute.
C3.1_10.	Narzędzia programowania i zarzadzania przełącznikiem: 1) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API; 2) wbudowana powłoka Bash do zarządzania systemem Linux przełącznika; 3) wsparcie dla kontenera LXC (Linux Container) lub runC wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika; 4) interfejs programistyczny REST API wraz z upublicznionym SDK; 5) możliwość zainstalowania klienta Chef; 6) możliwość zainstalowania agenta Puppet.
C3.1_11.	Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych.
C3.1_12.	Obudowa o rozmiarach maksymalnie 2 U (rack unit), przeznaczona do montażu w szafie rackowej 19”.

5.2Przełączniki LEAF, Remote LEAF

Zamawiający wymaga dostarczenia przynajmniej dwóch urządzeń rdzeniowych warstwy „LEAF” per Ośrodek Krajowy oraz dodatkowo po dwa urządzenia warstwy „Remote LEAF” do każdej z dwóch lokalizacji wyniesionych:

Specyfikacja przełączników warstwy „LEAF”:

Lp.	Part Number	Description	Ilość
1.	N9K-C93180YC-FX	Nexus 9300 with 48p 1/10/25G, 6p 40/100G, MACsec	4
2.	CON-PSRT-N93YCFX	PRTNR SS 8X5XNBD Nexus 9300 with 48p	4
3.	ACI-N9KDK9-15.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 15.0	4
4.	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
5.	NXA-PAC-500W-PE	Nexus NEBs AC 500W PSU - Port Side Exhaut	8
6.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	8
7.	NXA-FAN-30CFM-F	Nexus Fan, 30CFM, port side exhaust airflow	16
8.	ACI-ES-XF	DCN Essential SW license for 10G+ Nexus 9K Leaf	4
9.	CON-PSBU-ACIESXF	PSS SWSS UPGRADES ACI Essential SW license for a 10/25/40G	4

Specyfikacja przełączników warstwy „Remote LEAF”:

Lp.	Part Number	Description	Ilość
1.	N9K-C93180YC-FX	Nexus 9300 with 48p 1/10/25G, 6p 40/100G, MACsec	4
2.	CON-PSRT-N93YCFX	PRTNR SS 8X5XNBD Nexus 9300 with 48p	4
3.	ACI-N9KDK9-15.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 15.0	4
4.	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	4
5.	NXA-PAC-500W-PE	Nexus NEBs AC 500W PSU - Port Side Exhaut	8
6.	CAB-9K10A-EU	Power Cord, 250VAC 10A CEE 7/7 Plug, EU	8
7.	NXA-FAN-30CFM-F	Nexus Fan, 30CFM, port side exhaust airflow	16
8.	ACI-AD-XF	DCN Advantage SW license for a 10G+ Nexus 9K Leaf	4

9.	CON-PSBU-ACIADXF	PSS SWSS UPGRADES ACI Advantage SW license for a 10/25/40G	4

Lub dostarczenie Urządzeń równoważnych spełniających poniższe wymagania:

Kod wymagania	Opis wymagania
C6.1_1.	Przełącznik posiada: 1) min. 48 portów 1/10/25GE definiowanych za pomocą wkładek SFP/SFP+ z czego każdy port może również działać jako port FC o prędkości 16/32 Gbps; 2) min. 6 portów 40/100GE definiowanych za pomocą wkładek QSFP, przy czym każdy z tych portów QSFP posiada możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100 Gbps na pojedynczej parze okablowania multi-mode (do 100m).
C6.1_2.	Parametry wydajnościowe: 1) prędkość przełączania minimum 3.6 Tbps; 2) urządzenie sprzętowo przełącza pakiety w warstwie L2 i L3.
C6.1_3.	Przełącznik posiada następującą funkcjonalność dla warstwy L2: 1) Trunking IEEE 802.1Q VLAN; 2) wparcie dla min. 3000 sieci VLAN; 3) wsparcie sprzętowe dla 250 tysięcy adresów MAC; 4) IEEE 802.1w Rapid Spanning Tree (RST); 5) IEEE 802.1s Multiple Spanning Tree (MST); 6) zabezpieczenie przeciwko incydentom w topologii Spanning Tree (min. ochrona Root-a, filtracja BPDU); 7) Internet Group Management Protocol (IGMP) Versions 2, 3; 8) terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach; 9) Link Aggregation Control Protocol (LACP): IEEE 802.3ad 10) ramki Jumbo dla wszystkich portów (minimum 9216 bajtów); 11) funkcjonalność izolowania portów znajdujących się w tym samym VLAN; 12) wsparcie sprzętowe dla tunelowania QinQ i QinVNI.
C6.1_4.	Przełącznik posiada następującą funkcjonalność dla warstwy L3:

	1) sprzętowe przełączanie pakietów w warstwie L3; 2) routing w oparciu o trasy statyczne; 3) routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6; 4) Policy Based Routing (PBR) dla IPv4 oraz IPv6; 5) VRRP v3; 6) wsparcie dla BFD (Bidirectional Forwarding Protocol) w tym zarówno dla IPv4 jak i IPv6; 7) tunele GRE; 8) wsparcie sprzętowe dla minimum 800 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP; 9) wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking); 10) wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP); 11) wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode i tryb SSM (Source Specific Multicast); 12) wsparcie dla IGMPv3 oraz MSDP; 13) wsparcie sprzętowe dla minimum 32,000 tras multicastowych; 14) obsługa minimum 2000 wejściowych oraz minimum 2000 wyjściowych wpisów dla ACL (Access Control List).
C6.1_5.	Przełącznik wspiera następujące mechanizmy związane z funkcjonalnością VXLAN: 1) zintegrowany, sprzętowy VXLAN Bridging/Routing; 2) obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP; 3) obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast); 4) implementacja VXLAN BGP EVPN (Ethernet VPN); 5) obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway (obsługą danego SVI na wszystkich VTEP w domenie VXLAN).
C6.1_6.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem jakości usług w sieci: 1) Layer 2 IEEE 802.1p (CoS) oraz DSCP;

	2) klasyfikacja QoS w oparciu o listy ACL (Access Control List) dla warstwy drugiej i trzeciej (IPv4 i IPv6); 3) kolejkowanie bezwzględne (strict-priority); 4) kolejkowanie WRR (Weighted Round-Robin) lub WRED (Weighted Random Early Detection); 5) ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych; 6) dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych; 7) protokół PFC (Priority Flow Control) IEEE 802.1Qbb.
C6.1_7.	Przełącznik wspiera następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci: 1) Obsługa list kontroli dostępu (ACL): a) ACL dla warstwy 2 w oparciu o: adresy MAC, typ protokołu, b) ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), c) ACL oparte o VLAN-y (VACL), d) ACL oparte o porty (PACL); 2) DHCP Snooping; 3) ARP Inspection; 4) IP Source Guard; 5) unicast Reverse Path Forwarding (uRPF) 6) prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast; 7) Netflow v9 (pełen); 8) przełącznik wspiera następujące funkcjonalności dla obszaru zarządzania i zabezpieczenia przełącznika: 9) port zarządzający 100/1000 Mbps; 10) port konsoli CLI; 11) zarządzanie In-band; 12) SSHv2; 13) Authentication, Authorization, and Accounting (AAA); 14) RADIUS; 15) TACACS+;

	16) Syslog; 17) SNMP v1, v2c, v3; 18) telemetria w oparciu o mechanizm subskrypcji (push out), zapewniający alternatywny do SNMP, szybszy mechanizm (min. co 30s) zbierania informacji z przełącznika poprzez protokoły gRPC lub GPB; 19) Role-Based Access Control RBAC; 20) RMON (przynajmniej grupy Events, Alarms); 21) IEEE 802.1ab LLDP; 22) możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback); 23) 802.1x; 24) ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing); 25) kopiowanie ruchu ze źródłowych fizycznych portów Ethernet, wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu (mirroring); 26) Network Time Protocol (NTP); 27) Precision Time Protocol IEEE 1588; 28) diagnostyka procesu BOOT; 29) ping; 30) Traceroute; 31) przełącznik musi posiadać możliwość wsparcia enkrypcji MACsec o prędkości wire-rate na wszystkich portach 1/10/25 GE. Jeżeli niezbędna jest licencja do działania tej funkcji to nie trzeba jej dostarczać w ramach tego postępowania.
C6.1_8.	Narzędzia programowania i zarządzania przełącznikiem: 1) Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API; 2) wbudowana powłoka Bash do zarządzania systemem Linux przełącznika; 3) wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener posiada możliwość wykorzystywania portów fizycznych przełącznika; 4) interfejs programistyczny REST API wraz z upublicznionym SDK;

	5) możliwość zainstalowania klienta Chef; 6) możliwość zainstalowania agenta Puppet; 7) wsparcie dla NETCONF i zarządzania poprzez XML; 8) wsparcie dla OpenStack Neutron ML2 plugin.
C6.1_9.	Przełącznik powinien być wyposażony w dwa zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony portów liniowych.
C6.1_10.	Obudowa o rozmiarach maksymalnie 1U, przeznaczona do montażu w szafie rackowej 19”.
C6.1_11.	Jeżeli rozwiązanie tego wymaga to przełącznik powinien być wyposażony w odpowiednie licencje bezterminowe pozwalające na pracę pod zarządzaniem rozwiązania SDN.

6. Wymagania dotyczące okablowania strukturalnego oraz infrastruktury pasywnej

1. Zamawiający wymaga dostarczenia w ramach przedmiotu zamówienia następujących modułów optycznych:

Lp.	Opis	Ilość
1.	40GBASE Active Optical Cable o długości nie mniejszej niż 25 metrów kompatybilny z urządzeniami rdzeniowymi warstwy „SPINE” oraz warstw „LEAF”.	8
2.	Moduł 1000BASE-T SFP kompatybilny z urządzeniem rdzeniowym warstwy „LEAF”.	6
3.	Moduł 10GBASE-SR SFP kompatybilny z urządzeniem rdzeniowym warstwy „LEAF”.	8
4.	Moduł konwertujący QSFP do SFP10G kompatybilny z urządzeniem rdzeniowym warstwy „SPINE”.	4
5.	Twinax 10GBASE-CU SFP+ o długości nie mniejszej niż 5 metrów kompatybilny z kontrolerami SDN.	4
6.	10GBASE Active Optical o długości nie mniejszej niż 5 metrów kompatybilny z kontrolerami SDN.	4

2. Oferowane moduły optyczne muszą pochodzić od tego samego producenta co pozostałe komponenty scentralizowanego przełączania L2/L3.

3. Dostarczenie wszystkich niezbędnych patchcordy oraz okablowania do poprawnego podłączenia oferowanych komponentów do infrastruktury Zamawiającego leży po stronie oferenta.
4. W razie wystąpienia potrzeby dołożenia szafy rack do którejkolwiek z lokalizacji, oferent musi uwzględnić w kosztach oferty taką szafę RACK jako część dostarczanego uposażenia.

Wymaganie w stosunku do szaf typu RACK:

Kod wymagania	Opis wymagania
RACK.01	Wysokość – 42 U (minimum 1990 mm).
RACK.02	Głębokość minimum 1000 mm.
RACK.03	Szerokość minimum 600 mm.
RACK.04	Drzwi przednie – perforowane, zamykane na klucz, zdejmowane (dopuszcza się drzwi dzielone).
RACK.05	Drzwi tylne – perforowane, zamykane na klucz, zdejmowane (dopuszcza się drzwi dzielone).
RACK.06	Ściany boczne – zdejmowane na zatrzaskach pełne.
RACK.07	Wentylatory – Panel wentylatorów w panelu podsufitowym.
RACK.08	Szafy muszą być wyposażone w PDU umożliwiające podłączenie wszystkich urządzeń dostarczanych w ramach przedmiotowego zamówienia wszystkimi gniazdami do dwóch niezależnych torów zasilania jednak nie mniej niż 13 gniazd C14 per tor (PDU).
RACK.09	Elementy PDU muszą być zarządzalne oraz umożliwiać zdalne włączanie/wyłączanie gniazdek.
RACK.10	Elementy PDU muszą raportować o swoim aktualnym stanie działania.
RACK.11	Szafy muszą być wyposażone w pomiar mocy pobieranej przez urządzenia, pomiar mocy per szafa.
RACK.12	Do szaf należy dostarczyć wszelkie niezbędne elementy montażowe umożliwiające złożenie szaf, oraz zamontowanie wszystkich

	dostarczonych urządzeń dostarczanych w postępowaniu w tym maskownice wolnej przestrzeni – jeżeli dotyczy.
RACK.13	Wymagania dodatkowe – Szafa powinna mieć możliwość łączenia z innymi szafami tego samego modelu.
RACK.14	Szafa musi być kompatybilna ze wszystkimi oferowanymi urządzeniami (montowanymi w szafie rack).

7. Dostawa licencji do urządzeń posiadanych przez Zamawiającego

W ramach rozbudowy posiadanego sprzętu Cisco RU 4461 series przez Zamawiającego, należy dostarczyć poniżej wyspecyfikowane licencje do urządzeń ISR 4461 w ilości wskazanej w tabeli:

Lp.	Part Number	Description	Ilość
1	FL-4460-BOOST-K9=	Booster Performance License for 4460 Series	4

8. Update oprogramowanie Vmware do wersji Enterprise Plus

W ramach rozbudowy posiadanego środowiska wirtualnego Zamawiający wymaga podniesienia wersji wykorzystywanego obecnie VMware do wersji Enterprise Plus z wersji Standard na wszystkich 22 serwerach HyperFlex. Każdy z serwerów posiada 2 procesory oraz licencje Vmware Standard ed. posiadającą aktywne wsparcie producenta. Zamawiający wymaga by wsparcie na dostarczone licencje obejmowało okres 36 miesięcy od momentu zakupu w ramach przedmiotowego postępowania.

Lp.	Part Number	Description	Ilość
1	VMW-VSS2VSP-3A=	Upgrade: vSphere 6 Std to vSphere 6 Ent Plus (3 yr Supp Req)	44
2	CON-ISV1-VS5ENTP3A	ISV 24X7 VMware vSphere 5 EPlus for 1 P,3 Yr,RQD	44

3	UCS-VMW-TERMS	Acceptance of Terms, Standalone VMW License for UCS Servers	44

9. Opis prac jakie należy wykonać

9.1 Instalacja SDN

1. Celem Zamawiającego jest uruchomienie przedmiotowych komponentów w dwóch centralnych Lokalizacjach Centrum Przetwarzania Danych zlokalizowanych w Warszawie oraz Radomiu oraz w lokalizacjach zdalnych opisanych w OPZ, dokładne dane adresowe zostaną podane po podpisaniu Umowy.
2. W ramach prac będą również prace realizowane na rzecz podmiotów udostępniających sieć WAN oraz punkty styków dla systemu SWD PRM.
3. W ramach realizacji przedmiotu zamówienia należy między innymi zrealizować poniższe zadania, jednakże nie są to wszystkie prace jakie mogą być realizowane ze względu na konieczność dostosowania sieci WAN do potrzeb instalacji zamawianych komponentów:
    a) instalacja urządzeń w szafach RACK w obu Lokalizacjach,
    b) uruchomienie urządzeń oraz dodanie ich do domeny zarządzania KCMRM (podłączenie do sieci zarządzania oraz systemów monitoringu),
    c) uruchomienie niezbędnych połączeń oraz wytworzenie infrastruktury dostępowej dla podłączenia IP Fabryki ACI do sieci WAN z niezbędnymi pracami po stronie sieci WAN oraz z wykorzystaniem urządzeń routerów będących w posiadaniu Zamawiającego,
    d) migracja infrastruktury serwerowej w tym klastrów HyperFlex na nową infrastrukturę sieciową,
    e) uruchomienie centralnego systemu zarządzania bezpieczeństwem oraz uruchomienie mechanizmów bezpieczeństwa w komponencie IP Fabric ACI oraz w dostarczanych firewallach.

Pozostałe wymagania dotyczące usług instalacyjnych i konfiguracyjnych:

Kod wymagania	Opis wymagania
WDRU.1	Usługi instalacyjne muszą obejmować w szczególności: 1) dostarczenie Urządzeń do wskazanych przez Zamawiającego Lokalizacji; 2) rozpakowanie Urządzeń oraz utylizacja/magazynowanie opakowań; 3) montaż Urządzeń w dostarczonych przez Wykonawcę szafach; 4) podłączenie Urządzeń do zapewnianych przez Zamawiającego obwodów zasilających; 5) instalacja Urządzeń zgodnie z Projektem Technicznym; 6) instalacja Oprogramowania na Urządzeniach zgodnie z Projektem Technicznym; 7) konfiguracja Urządzeń; 8) uruchomienie Urządzeń; 9) integrację z systemami wirtualizacji; 10) aktualizację obecnego środowiska Vmware w zakresie koniecznym do integracji z SDN.
WDRU.2	Usługi konfiguracyjne muszą obejmować w szczególności konfigurację Urządzeń oraz Oprogramowania zgodnie z zatwierdzonym Projektem Technicznym.
WDRU.3	Usługi testowe muszą zostać przeprowadzone zgodnie z procedurą określoną w Planie Testów Akceptacyjnych w dokumencie opracowanym przez Wykonawcę, a zaakceptowanym przez Zamawiającego.
WDRU.4	Usługi wdrożeniowe muszą obejmować w szczególności: 1) uruchomienie Systemu wirtualizacji będącego przedmiotem zamówienia w celu przeprowadzenia testów akceptacyjnych; 2) przekazania rozwiązania produkcyjnego Zamawiającemu; 3) wykonanie Dokumentacji Powykonawczej zawierającej szczegółowy opis wdrożonego rozwiązania oraz zmiany w dokumentacji projektowej uwzględniającej poprawki naniesione w trakcie wdrożenia.
WDRU.5	Zamawiający wymaga by Wykonawca w ramach instalacji w Ośrodkach Przetwarzania Danych (POK, ZOK) oraz lokalizacjach wyniesionych uzgodnił warunki uruchomienia infrastruktury z podmiotami zarządzającymi tymi ośrodkami.

9.2Konfiguracja VRF w sieci OST112

W ramach postępowania Wykonawca musi wykonać rekonfigurację węzłów PE i CE sieci OST112 oraz CSD w celu wydzielenia urządzeń sieciowych SWD PRM do nowego tworzonego VRF na potrzeby przesyłania ruchu systemu SWD PRM i systemów zależnych.

Rekonfiguracji będą podlegać lokalizacje ośrodków dyspozytorni medycznych opisane w ramach niniejszego postępowania w sumie około 50 lokalizacji dyspozytorni medycznych i Ośrodków Regionalnych systemu PRM, a także wszystkie urządzania sieciowe, których rekonfiguracja jest wymagana do wdrożenia VRF'u dedykowanego dla potrzeb systemu SWD PRM.

W ramach postępowania Wykonawca musi wykonać rekonfigurację węzłów sieci OST112 oraz CSD w celu utworzenie nowego **VRF RADIO** na potrzeby komunikacji budowanego Podsystemu Zintegrowanej Łączności SWD PRM oraz za terminowanie usług do dedykowanych 17 Ośrodków Regionalnych obejmując obecnie wykorzystywane urządzeniach sieciowe OST112.

W ramach prac rekonfiguracji podlegać będą urządzenia sieciowe oraz firewall (w niezbędnym zakresie) w celu dostarczenia VRF do wymienionych lokalizacji oraz dostępu z nich do systemów centralnych oraz podmiotów współpracujących. Rekonfiguracja obejmuje w szczególności routery CE i PE w ośrodkach krajowych, regionalnych i dyspozytorniach medycznych.

Efektem prac ma być przeniesienie obecnie działających usług wykorzystywanych przez system SWD PRM do nowo tworzonego VRF w sieci OST 112 ze wszelkimi wymaganymi połączeniami oraz uruchomionymi mechanizmami bezpieczeństwa. Dodatkowo w trakcie prac może być konieczność uruchomienia nowych urządzeń oraz dodanie ich do domeny zarzadzania OST 112 lub SWD PRM.

9.3Konfiguracja multicast w Ośrodkach Krajowych OST 112

Wykonawca w ramach postępowania wykona rekonfigurację polegającą na uruchomieniu a następnie wdrożeniu multicast we fragmencie sieci OST 112 obejmującej ośrodki krajowe w lokalizacjach Warszawa, Radom. Celem uruchomienia mCAST w sieci OST112 jest zapewnienie komunikacji dla systemów uruchomionych w centrach danych ośrodków krajowych. Zakłada się uruchomienie mCAST w relacji tych

dwóch lokalizacji połączonych siecią MPLS w ramach uruchomionego dedykowanego IP VPN MPLS. Węzły OST 112 w tych lokalizacjach są zbudowane w architekturze redundantnej i w takiej należy uruchomić mCAST na potrzeby Ośrodków Krajowych.

10. Świadczenie Usługi Serwisu Gwarancyjnego

Zamawiający wymaga świadczenia Usługi Serwisu Gwarancyjnego spełniającego poniższe wymagania:

Kod wymagania	Opis funkcjonalności
WUS.01	Na dostarczone Urządzenia Wykonawca udzieli serwisu gwarancyjnego liczonego od daty podpisania protokołu odbioru na okres co najmniej 36 miesięcy opartego na świadczeniach serwisowych producenta.
WUS.02	Usługa Serwisu Gwarancyjnego musi być realizowana w trybie 24 godziny na dobę, 7 dni w tygodniu, 365 dni w roku, naprawa lub wymiana uszkodzonego Urządzenia w ciągu 8 godzin od momentu zgłoszenia – w sytuacji wystąpienia Awarii Krytycznej.
WUS.03	Wykonawca w ramach realizacji Umowy zapewni Zamawiającemu: 1) prawo do pobierania nowych wersji i aktualizacji Oprogramowania przez okres minimum 36 miesięcy od dnia podpisania protokołu odbioru; 2) wymianę Urządzenia w przypadku zdiagnozowania Awarii Urządzenia której nie daje się usunąć a która powoduje brak możliwości jego prawidłowego funkcjonowania; 3) dostarczenie na koszt Wykonawcy sprawnego Urządzenia lub jego elementu podlegającego wymianie do miejsc a zainstalowania Urządzenia uszkodzonego w uzgodnieniu z Zamawiającym; 4) możliwość aktualizacji Oprogramowania poprzez dostęp do zasobów producenta rozwiązania; 5) dostęp do pomocy technicznej producenta; 6) nieograniczoną ilość zgłoszeń serwisowych; 7) dostęp do materiałów producenta takich jak: techniczna dokumentacja, internetowa baza wiedzy;

	8) dostęp do poprawek i uaktualnień Oprogramowania objętego usługą wsparcia oraz nowych wersji; 9) dostęp do portalu www producenta oprogramowania umożliwiającego zarządzanie posiadanymi licencjami, podniesienie lub obniżenie (jeśli producent oficjalnie wspiera poprzednie wersje) wersji Oprogramowania; 10) dostęp do rejestru licencji (dostępnego przez portal www producenta Oprogramowania/Urządzeń).
WUS.04	Wykonawca wraz z dostawą Urządzeń przekaże warunki gwarancyjne i serwisowe Urządzeń, w tym procedury zgłaszania awarii, dostępne kanały komunikacyjne z serwisem producenta. Do zamówienia muszą zostać dostarczone procedury zgłaszania Awarii w formie dokumentów drukowanych lub elektronicznych.
WUS.06	Przyjęcie do realizacji zgłoszenia powinno zostać niezwłocznie potwierdzone przez Wykonawcę, zwrotnie na adres e-mail zgłaszającego.
WUS.07	Przez usunięcie Awarii należy rozumieć przywrócenie pierwotnej funkcjonalności Urządzeń i systemu operacyjnego sprzed wystąpienia Awarii albo zaproponowanie procedury obejścia zaistniałych Awarii bez rozwiązania problemu, pod warunkiem, że na przedstawioną przez Wykonawcę propozycję Zamawiający wyrazi zgodę.
WUS.08	Wykonawca dokona usunięcia Awarii Niekrytycznej w terminie nie dłuższym niż 24 godziny od momentu zgłoszenia.
WUS.09	Wykonawca dokona usunięcia Awarii Zwykłej w terminie nie dłuższym niż 72 godziny od momentu zgłoszenia.
WUS.10	Po wymianie Urządzenia lub modułu będącego wyposażeniem tego Urządzenia lub Oprogramowania zostanie on objęty serwisem na takich samych zasadach jak wymienione Urządzenie lub moduł będący wyposażeniem tego Urządzenia lub Oprogramowania. Dla wymienionego Urządzenia okres gwarancji rozpoczyna swój bieg na nowo.
WUS.11	Wykonawca najpóźniej w ciągu 1 Dnia Roboczego, po rozwiązaniu każdego 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).
WUS.12	Do każdego dostarczonego Urządzenia Wykonawca zobowiązuje się dostarczyć kartę gwarancyjną producenta, zawierającą numer seryjny, termin i warunki ważności gwarancji. Jeśli dla danego dostarczonego Urządzenia lub Oprogramowania producent

	nie przewiduje wystawiania własnych kart gwarancyjnych, kartę taką wystawi Wykonawca. W celu ułatwienia Zamawiającemu zarządzania kartami gwarancyjnymi dopuszcza się wystawianie zbiorczych kart gwarancyjnych Wykonawcy, jednakże każdorazowo z podaniem nr seryjnych lub innych danych umożliwiających jednoznaczną identyfikację Urządzenia lub Oprogramowania, którego dotyczy gwarancja Wykonawcy. W wypadku, jeżeli postanowienia gwarancji producenta są mniej korzystne od warunków zapisanych w OPZ stosuje się zapisy OPZ.
WUS.13	W przypadku, gdy wadliwe Urządzenie uniemożliwia wykorzystanie funkcjonalności lub uniemożliwia pracę jakiegokolwiek jego podsystemu Wykonawca na czas naprawy zobowiązany jest dostarczyć, skonfigurować i uruchomić urządzenie zastępcze, o takich samych lub zbliżonych parametrach technicznych i funkcjonalnych, w sposób, który pozwoli na przywrócenie utraconych funkcjonalności Systemu lub podsystemu.
WUS.14	Usługi serwisowe, będą świadczone w miejscu użytkowania Urządzeń z możliwością naprawy w serwisie Wykonawcy, jeśli naprawa u użytkownika okaże się niemożliwa. Jeżeli naprawa odbywać się będzie poza miejscem użytkowania Urządzenia, przed zabraniem urządzenia Wykonawca zobowiązany jest wymontować i pozostawić u Zamawiającego dyski i wymienne pamięci flash. Wykonawca pokryje koszty transportu oraz koszty ewentualnego ubezpieczenia przedmiotu zamówienia do miejsca naprawy oraz jego zwrotu do Lokalizacji. W przypadku Urządzeń, dla którego jest wymagany dłuższy niż określony dla Awarii Niekrytycznej i Zwykłej czas na naprawę lub wymianę Zamawiający dopuszcza podstawienie na czas naprawy Urządzenia o nie gorszych parametrach funkcjonalnych. Naprawa w takim przypadku nie może przekroczyć 7 Dni Roboczych od momentu zgłoszenia Awarii. Po usunięciu Awarii, dyski wymienne i/lub pamięci flash z urządzenia zastępczego pozostają u Zamawiającego.
WUS.15	Elementy Urządzeń podlegające wymianie będą wymienione przez Wykonawcę na nowe, wolne od wad i o nie gorszych parametrach.
WUS.16	Wykonawca jest zobowiązany do samodzielnego dokonania naprawy/wymiany Urządzenia na swój koszt i ryzyko w Lokalizacji. Jednakże, o ile Zamawiający wyrazi uprzednią zgodę, dopuszcza się realizację świadczenia gwarancyjnego w ten sposób, że na podstawie informacji diagnostycznych przekazanych przez Zamawiającego do Wykonawcy podczas zgłoszenia Awarii, Wykonawca prześle na swój koszt zamiennik uszkodzonego Urządzenia, natomiast fizycznej wymiany uszkodzonego Urządzenia dokona odpowiednio przeszkolony przez Wykonawcę pracownik Zamawiającego,

	czyniąc to na ryzyko Wykonawcy. Jednakże taki tryb realizacji naprawy nie zwalnia Wykonawcy z obowiązku zapewnienia przywrócenia pierwotnego stanu pracy Systemu.
WUS.17	Gwarancja obejmuje między innymi: 1) wady materiałowe i konstrukcyjne, a także nie spełnienie deklarowanych przez producenta parametrów i/lub funkcji użytkowych Urządzeń i Oprogramowania; 2) naprawę wykrytych uszkodzeń, w tym wymianę uszkodzonych modułów na nowe; 3) usuwanie wykrytych usterek i Awarii w działaniu Urządzeń lub Oprogramowania.
WUS.18	W okresie gwarancji, w przypadku awarii dysku twardego lub innego nośnika danych, będzie on wymieniony przez gwaranta na nowy bez konieczności zwrotu uszkodzonego dysku twardego lub innego nośnika danych przez Zamawiającego i dokonywania ekspertyzy dysku poza siedzibą Zamawiającego.
WUS.19	Jednokrotna naprawa tego samego Urządzenia lub modułu będącego wyposażeniem tego Urządzenia w okresie gwarancji, obliguje Wykonawcę do jego wymiany na fabrycznie nowy, wolny od wad, spełniający te same parametry i zgodny funkcjonalnie z naprawianym Urządzeniem lub modułem, w terminie 14 dni od chwili ostatniego zgłoszenia w tym zakresie. Okres gwarancji na wymienione Urządzenie lub moduł biegł będzie na nowo od daty podpisania protokołu stwierdzającego tę wymianę przez Wykonawcę i Zamawiającego, przez okres udzielony przez Wykonawcę.
WUS.20	Wszystkie części zamienne do Urządzeń lub modułów muszą pochodzić z oficjalnego kanału dystrybucji.
WUS.21	Wszystkie naprawy Urządzeń oraz aktualizacje Oprogramowania muszą być wykonywane przez autoryzowany serwis producenta Urządzeń.
WUS.22	Zamawiający uprawniony jest do opóźnienia terminu rozpoczęcia usuwania Awarii przez Wykonawcę, w takim przypadku gwarantowany czas naprawy ulegnie odpowiedniemu wydłużeniu i będzie liczony względem wskazanego przez Zamawiającego terminu.
WUS.23	W przypadku zdiagnozowania błędów w używanej przez Zamawiającego wersji Oprogramowania, Wykonawca zapewni Zamawiającemu dostęp do najnowszych wersji Oprogramowania Urządzeń posiadających wsparcie producenta, pozwalających na usuniecie tych błędów na zasadach określonych w OPZ. W przypadku wykrycia błędu, dla którego brak jest w danym momencie odpowiedniej aktualizacji, Wykonawca

	dokona eskalacji zgłoszenia do producenta. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą specyfikacją korzystanie przez Zamawiającego z Oprogramowania w ramach wsparcia technicznego nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.
WUS.24	Świadczenie usług serwisowych przez Wykonawcę będzie wliczone w cenę oferty i nie będzie podstawą do roszczenia o jakiekolwiek dodatkowe wynagrodzenie z tego tytułu.
WUS.25	Zamawiający wymaga elastyczności w rozbudowie, aby była możliwość bez konieczności uzyskania zgody Wykonawcy czy producenta, rozbudowy posiadanych Urządzeń o kolejne moduły rozszerzeń. Rozbudowa nie może powodować utraty praw gwarancyjnych do istniejącej i rozszerzonej konfiguracji danego Urządzenia.
WUS.26	Stosowanie praw wynikających z udzielonej gwarancji nie wyłącza stosowania uprawnień Zamawiającego wynikających z rękojmi za wady. Zasady gwarancji i rękojmi za wady określa Umowa.

11. Wymagania w zakresie Dokumentacji

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

Kod wymagania	Opis funkcjonalności
DOK.01	Zamawiający wymaga, aby Wykonawca przygotował, zgodnie z ogólnie akceptowalnymi standardami w dziedzinie dokumentowania Dokumentację bezpośrednio związaną z przedmiotem zamówienia i dostarczył ją Zamawiającemu.
DOK.02	W ramach Projektu Technicznego Wykonawca opracuje i dostarczy następujące dokumenty: 1) szczegółowy wykaz Oprogramowania (zawierający m.in. producenta, nazwę produktu, wykaz komponentów produktu, typ produktu, typ licencji, ilość licencji, numery licencji, okres obowiązywania licencji);

	2) szczegółowy wykaz Urządzeń (zawierający m.in. producenta, nazwę produktu, szczegółowy wykaz podzespołów produktu, kategoria produktu, szczegółowy wykaz licencji produktu, typ licencji, ilość licencji, numery seryjne); 3) projekt infrastruktury fizycznej systemu; 4) projekt infrastruktury logicznej systemu.
DOK.03	Dokumentacja Powykonawcza będzie zawierać, co najmniej następujące informacje: 1) wprowadzenie opisujące cele i zakres przedmiotu zamówienia; 2) ograniczenia rozwiązania, założenia i zależności; 3) opis i specyfikację interfejsów Urządzeń; 4) opis i specyfikację interfejsów Systemu; 5) opis implementacji w środowisku Zamawiającego; 6) schematy połączeń; 7) załącznik zawierający sposoby i metody uwierzytelnienia do zasobów systemu; 8) opis rozwiązania wydajności, skalowalności i niezawodności; 9) plan przebiegu testów akceptacyjnych i sposób oszacowania, w tym propozycję raportów z testów.
DOK.04	Dokumentację eksploatacyjną, zawierającą, co najmniej procedury: administracyjne, backupu systemu, awaryjne i użytkownika, przy czym każda z procedur musi zawierać, co najmniej następujące wyszczególnione informacje: 1) procedury związane z administracją i eksploatacją; 2) procedury działania administratora dla wdrożonego Systemu; 3) procedury konserwacji wdrożonego Systemu; 4) procedury awaryjne; 5) procedury zabezpieczeń (backup'owe); 6) procedury kontroli bezpieczeństwa Systemu (Audyt); 7) procedury eskalacji zgłoszeń serwisowych. Każda z ww. procedur będzie zawierać minimum następujące informacje: 1) identyfikator i nazwa procedury; 2) rodzaj procedury;

	3) data utworzenia i zatwierdzenia oraz wersja procedury; 4) cel i zakres procedury; 5) uzasadnienie zastosowania; 6) warunki uruchomienia procedury i oczekiwany oraz możliwy rezultat jej wykonania; 7) dane osób, które opracowały procedurę, sprawdziły, zaakceptowały i zatwierdziły; 8) wzór formularza zgłoszenia Awarii 9) szczegółowy opis rezultatów; 10) możliwe niepowodzenia; 11) przebiegi alternatywne; 12) algorytm działania, jaki należy zastosować, wykonując kolejne czynności, aby osiągnąć postawiony cel, w tym z informacją o osobie, która powinna wykonać dane czynności.
DOK.05	Procedury muszą zostać zoptymalizowane pod kątem ciągłości działania usług Systemu o wysokim poziomie SLA.
DOK.06	Plan Wdrożenia – Wykonawca opracuje i dostarczy dokument zawierający zestaw procedur niezbędnych do instalacji, konfiguracji oraz uruchomienia Urządzeń i Oprogramowania w Lokalizacjach, zarówno do realizacji po stronie Zamawiającego jak i Wykonawcy. Dokument zawierać będzie: 1) informacje odnośnie Urządzeń oraz Oprogramowania dla każdej Lokalizacji, w których instalowane będą Urządzenia dla potrzeb dostarczenia Systemu, które są przedmiotem tego zamówienia; 2) opis czynności wymaganych do realizacji przez Wykonawcę w ramach wdrożenia poszczególnych komponentów Systemu; 3) harmonogram wdrożenia; 4) zestawienie ukazujące przydzielenie poszczególnych licencji do poszczególnych Urządzeń oraz systemów operacyjnych.
DOK.07	Zamawiający wymaga, aby wszystkie dokumenty tworzone w ramach realizacji przedmiotu zamówienia 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 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 rozumiane, 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.08	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, w co najmniej w 1 egzemplarzu. Zamawiający zastrzega prawo do zgłaszania uwag do Dokumentacji.
DOK.09	W przypadku kolejnych wersji Dokumentacji wymagane jest, aby Wykonawca dostarczył elektroniczne wersje Dokumentacji, które zawierają wyróżnione różnice pomiędzy kolejnymi wersjami Dokumentacji (w trybie rejestracji zmian).
DOK.10	Wykonawca do Dokumentacji dołączy wykaz zawierający szczegółowy spis Dokumentów wraz z opisem ich przeznaczenia.

12. Szczegółowe zasady odbioru przedmiotu Umowy

I. Zasady ogólne

1. Przedmiot Umowy należy dostarczyć zgodnie z zasadami i terminami wskazanymi w Umowie.
2. O przygotowaniu przedmiotu Umowy do odbioru Wykonawca powiadomi wyznaczonego w Umowie przedstawiciela Zamawiającego za pomocą wiadomości e-mail na adres e-mail wskazany w Umowie, z co najmniej trzy (3) dniowym wyprzedzeniem, podając:
   1) numer Umowy,
   2) planowaną datę przystąpienia do odbioru przedmiotu Umowy;
   3) listę Urządzeń wraz z wyposażeniem dostarczonych w ramach przedmiotu Umowy.
3. Zamawiający przystąpi do odbioru przedmiotu Umowy w ciągu trzech (3) dni roboczych od otrzymania od Wykonawcy zgłoszenia gotowości do odbioru.
4. Odbiór zostanie przeprowadzony w Lokalizacjach Zamawiającego w obecności przedstawicieli Wykonawcy w godz. 8:00-15:35.
5. Odbiór zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego i Wykonawcy:
   1) protokołu odbioru ilościowo-jakościowego, którego zakres obejmuję dostawę Urządzeń oraz Oprogramowania– którego wzór stanowi Załącznik nr 3 do Umowy,
   2) protokołu odbioru rozwiązania którego zakres obejmuje instalację i konfigurację Urządzeń oraz Oprogramowania Standardowego – którego wzór stanowi Załącznik nr 4 do Umowy.

II.Odbiór ilościowo – jakościowy

1. Celem czynności kontrolnych prowadzonych w ramach odbioru ilościowo – jakościowego jest sprawdzenie kompletności dostarczonego przedmiotu Umowy i potwierdzenie zgodności z ilością określoną w Umowie oraz sprawdzenie wszystkich wymagań funkcjonalnych i potwierdzenie zgodności ze szczegółowym opisem przedmiotu Umowy.
2. Wykonawca będzie odpowiedzialny za dostarczenie i zaprezentowanie dostarczonego przedmiotu Umowy.

3. Podstawą dokonania odbioru ilościowo – jakościowego jest przeprowadzenie z pozytywnym skutkiem sprawdzeń kompletności ukompletowania oraz poprawności działania Urządzeń dostarczanych w ramach Umowy wraz z dostarczanymi licencjami.
4. Pozytywny wynik odbioru ilościowo – jakościowego zostanie potwierdzony podpisaniem protokołu odbioru ilościowo – jakościowego, którego wzór określa Załącznik nr 3 do Umowy.

III.Odbiór Dokumentacji

1. Dokumentacja przygotowana przez Wykonawcę zgodnie z OPZ i postanowieniami Umowy, musi zostać zaakceptowana przez Zamawiającego.
2. Przedstawiciel Wykonawcy przekaże wersje elektroniczne Dokumentacji przedstawicielowi Zamawiającego w celu jej weryfikacji.
3. Dokumenty zostaną poddane weryfikacji przez Zamawiającego w terminie 2 Dni Roboczych od dnia przekazania.
4. Zamawiający ma możliwość zgłoszenia uwag do dokumentu w formie elektronicznej do Wykonawcy, które zostaną przekazane jednorazowo dla danej wersji Dokumentacji.
5. Przedstawiciel Zamawiającego przekaże uwagi przedstawicielowi po stronie Wykonawcy. Przedstawiciele stron Umowy ustalają nową datę dostarczenia poprawionej wersji Dokumentacji, nie dłuższą jednak niż 3 Dni Robocze.
6. Dla poprawionej wersji Dokumentacji procedury zostają powtórzone, przy czym okres ponownej weryfikacji Dokumentacji przez Zamawiającego wynosi 2 Dni Robocze. Weryfikacja poprawionej Dokumentacji podlegają tylko te elementy Dokumentacji, których poprawy dokonał Wykonawca.
7. Wersja zaakceptowana przez Zamawiającego zostanie dostarczona przez Wykonawcę w formie papierowej i elektronicznej.
8. Odbiór Dokumentacji zostanie potwierdzony podpisaniem przez przedstawicieli Zamawiającego oraz Wykonawcy protokołu odbioru dokumentacji, których wzory określa załącznik nr 4 do Umowy.

IV. Odbiór przedmiotu zamówienia

1. Celem odbioru jest potwierdzenie poprawnej implementacji infrastruktury programowo – sprzętowej polegającej na:
    1) Montażu Urządzeń,
    2) Zainstalowaniu w szafach RACK Zamawiającego dostarczonego sprzętu,
    3) Konfiguracja całości środowiska,
    4) Przeprowadzeniu z Przedstawicielami Zamawiającego testów akceptacyjnych.