Załącznik nr 9a do SIWZ – Opis Przedmiotu Części I zamówienia

„Zaprojektowanie, budowa, dostawa, wdrożenie, utrzymanie, serwisowanie systemów i aplikacji tworzących architekturę platform technologicznych oraz infrastruktury sprzętowej IT dla centrum danych SPNT Sp. z o.o. w ramach projektów: 1. "Przetwarzanie w chmurze dla rozwoju miast cyfrowych - faza rozwoju" - Działanie 5.1 Programu Operacyjnego Innowacyjna Gospodarka 2. „Budowa i wyposażenie I Etapu Pomerania Technopark w Szczecinie przy ul. Niemierzyńskiej - Poddziałanie 1.2.1 Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego"

Projekt „Przetwarzanie w chmurze dla rozwoju miast cyfrowych - faza rozwoju" współfinansowany jest ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka „Fundusze Europejskie - dla rozwoju innowacyjnej gospodarki"

Projekt „Budowa i wyposażenie I etapu Pomerania Technopark w Szczecinie przy ul. Niemierzyńskiej" współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego województwa zachodniopomorskiego na lata 2007-2013

Spis treści

1. Wprowadzenie

1.1. Zakres i cel dokumentu

Dokument określa szczegółowy przedmiot zamówienia, uwarunkowania biznesowe projektu budowy infrastruktury Centrum Danych Technoparku Pomerania oraz tryb dostarczenia produktów. Wraz z Umową (załącznik 8a do SIWZ) stanowi podstawę rozliczenia pracy Wykonawcy i główny dokument nadzorczy przy:

- Projektowaniu rozwiązania przez Wykonawcę przy współudziale Zamawiającego,
- Wykonaniu rozwiązania przez Wykonawcę,
- Odbieraniu rozwiązania od Wykonawcy przez Zamawiającego.

1.2. Słownik pojęć

Termin	Definicja
Analiza heurystyczna	Analiza mająca na celu określenie użyteczności strony internetowej.
Continuous Delivery	Praktyka w tworzeniu i rozwoju oprogramowania polegająca na zautomatyzowaniu i usprawnieniu procesu dostarczania oprogramowania poprzez zastosowanie m.in. zautomatyzowanych testów oraz ciągłej integracji, zapewniająca bezpieczeństwo włączenia zmian do środowiska produkcyjnego.
Continuous Integration	Praktyka w tworzeniu i rozwoju oprogramowania polegająca na częstym i regularnym włączaniu bieżących zmian w kodzie do głównego repozytorium przy zapewnieniu poprawności kompilacji.
Instancja	Wydzielony zasób chmury obliczeniowej definiowany przy pomocy ilości oraz parametrów procesora oraz wielkości przestrzeni dyskowej.
Klient	Osoba fizyczna, lub podmiot gospodarczy korzystający z Usług oferowanych przez System
Obfuskacja	Zwana również zaciemnianiem kodu, modyfikacja kodu źródłowego oprogramowania, znacząco utrudniająca jego analizę i zrozumienie.
Overbooking	Możliwość zarezerwowania sumarycznej wielkości zasobów wyższej, niż pozwalają na to fizyczne parametry Systemu.
Partner	Klient dystrybuujący Usługi oferowane przez System, dalszym podmiotom, będącymi klientami Partnera.
Platforma oprogramowania	Zbiór Podsystemów dostarczanych w ramach Projektu, realizujących określone funkcje, wraz z infrastrukturą sprzętową umożliwiając świadczenie Usług.
Podsystem	Dostarczany w ramach Projektu komponent składowy Systemu realizujący na jego rzecz określone funkcjonalności, spełniający określone w OPZ wymagania funkcjonalne i pozafunkcjonalne.
Program	Program skierowany do Partnerów, w ramach którego otrzymują możliwość

Partnerski	dokonania zakupu Usług na specjalnych warunkach cenowych.
Projekt	Przedsięwzięcie mające na celu zaprojektowanie, wytworzenie i wdrożenie Systemu
SLA	(ang. Service Level Agreement) część umowy, dotycząca utrzymania Systemu, definiująca parametry takie jak: dostępność, czas reakcji na incydent itp.
System	Platforma oprogramowania wraz z infrastrukturą sprzętową, umożliwiające wspólnie świadczenie Usług.
Usability	Parametr określający ergonomię i funkcjonalność strony internetowej, zapewniający intuicyjną nawigację, łatwy i czytelny dostęp do informacji oraz zrozumiały ich przekaz.
Usługa	Funkcjonalność Systemu w modelu chmury obliczeniowej, dostarczająca Klientom określonych i oczekiwanych korzyści.
Usługodawca	Klient oferujący własne usługi funkcjonujące w oparciu o Usługi Systemu.
VCS	System kontroli wersji, oprogramowanie służące do kontroli zmian w kodzie źródłowym oprogramowania, bądź w innych plikach (np. dokumentacji) umieszczonych we wspólnym repozytorium.

2. Ogólne uwarunkowania biznesowe Projektu oraz opis zakresu zamówienia

Szczeciński Park Naukowo-Technologicznego Sp. z o. o. (SPNT) zarządzający Technoparkiem Pomerania realizuje inwestycję rozbudowy i uruchomienia usług Technoparku Pomerania, w tym Centrum Danych, składającego się z Centrum Głównego zlokalizowanego w budowanym obiekcie F4 przy ul. Cyfrowej 4 w Szczecinie, o powierzchni komór serwerowych 602m2 oraz Centrum Zapasowego zlokalizowanego w budynku F1, przy ul. Niemierzyńskiej 17a kompleksu Technoparku Pomerania.

W wyniku realizacji projektów:

- Przetwarzanie w chmurze dla rozwoju miast cyfrowych - faza rozwoju - dofinansowanego ze środków Programu Operacyjnego Innowacyjna Gospodarka, Działanie 5.1,
- Budowa i wyposażenie I etapu Pomerania Technopark w Szczecinie przy ul. Niemierzyńskiej - dofinansowanego ze środków Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego, Działanie 1.2.1,
- Technopark Pomerania - budowa infrastruktury usługowej i społeczeństwa informacyjnego - dofinansowanego ze środków Regionalnego Programu Operacyjnego Województwa Zachodniopomorskiego, Działanie 3.1,

zostaną udostępnione nowe usługi Technoparku, w tym Usługi Centrum Danych zaprojektowane między innymi w oparciu o potrzeby i współpracę z lokalnymi firmami informatycznymi w ramach Powiązania Kooperacyjnego Cloud for Cities.

Jako główne cele biznesowe realizowanego Projektu wyróżnia się:

- Stworzenie produktów opartych o najnowsze rozwiązania w technologii chmury obliczeniowej celem maksymalizacji potencjału Centrum Danych ulokowanego w Technoparku Pomerania.
- Wzmocnienie roli Szczecińskiego Parku Naukowo-Technologicznego (SPNT), jako jednostki wspierającej przedsiębiorstwa w dziedzinie wykorzystania rozwiązań chmury obliczeniowej poprzez wdrażanie innowacyjnych rozwiązań optymalizujących koszty i podnoszących efektywność wykorzystania zasobów IT.
- Zbudowanie rozwiązań produktowych generujących przychody dla SPNT oraz poszerzające ofertę produktową Technoparku Pomerania kierowaną do firm z Powiązania Kooperacyjnego Cloud for Cities, najemców powierzchni biurowej Technoparku Pomerania oraz innych firm i organizacji, szczególnie w województwie zachodniopomorskim.
- Osiągnięcie przychodów ze sprzedaży usług centrum danych pozwalających na pokrycie kosztów eksploatacji DC w ciągu 5 lat od jego uruchomienia.
- Uruchomienie pakietu innowacyjnych usług Centrum Danych dla klientów Technoparku Pomerania w oparciu o współpracę z lokalnymi firmami IT.

W ramach realizacji Zamówienia wytworzone zostaną produkty niezbędne do uruchomienia usług Technoparku, w tym Centrum Danych, opartych o infrastrukturę sprzętową, techniczną i oprogramowanie. Usługi będą świadczone w technologii chmury obliczeniowej w modelu:

- Infrastructure-as-a-Service (IaaS),
- Platform-as-a-Service (PaaS),
- Software-as-a-Service (SaaS).

Jednym z kluczowych kanałów sprzedaży powyższych usług będzie Program Partnerski, skierowany głównie do firm informatycznych, firm programistycznych oraz konsultantów IT, którzy w ramach realizowanych projektów dla swoich klientów będą prowadzić reselling Usług IaaS i PaaS. W pierwszej kolejności będą to firmy z Klastra.IT, które już wyraziły zainteresowanie takim modelem współpracy z SPNT dostrzegając wymierne korzyści dla swoich przedsięwzięć. Otoczeniem biznesowe skupione wokół Technoparku Pomerania stanowi ważną przewagę konkurencyjną, zaś sam Program Partnerski pozwoli tę przewagę wykorzystać pod kątem generowania przychodu z Usług Centrum Danych.

2.1. Zakres zamówienia

Zakres zamówienia obejmuje dostarczenie Systemu, na który składają się: infrastruktura techniczna, infrastruktura sprzętowa IT i oprogramowanie umożliwiające wspólnie świadczenie przez SPNT usług w technologii chmury obliczeniowej.

Na całość Systemu składają się następujące komponenty:

- Infrastruktura techniczna:
    a. Infrastruktura szaf serwerowych,
    b. Systemy chłodzenia
- Infrastruktura sprzętowa IT:
    a. Infrastruktura serwerowa na potrzeby Podsystemów oprogramowania,
    b. Infrastruktura na potrzeby przechowywania danych,
    c. Infrastruktura sieciowa dla Centrum Danych,
    d. Infrastruktura sieciowa dla kompleksu biurowego Technoparku Pomerania;
- Oprogramowanie:
    a. **IaaS** - Podsystem umożliwiający dostarczenie klientowi infrastruktury informatycznej zdefiniowanej poprzez liczbę serwerów (wirtualnych bądź dedykowanych), wielkości przestrzeni dyskowej i parametrów przepustowości łącza dostępowego.
    b. **PaaS** - osadzony na IaaS Podsystem umożliwiający klientowi tworzenie aplikacji opartych o zdefiniowane: języki programowania, różne frameworki, wspierający różne typy baz danych, różne rozwiązania typu kolejkowego oraz różne systemy zarządzania i kontroli wersji.
    c. **SelfService** - realizowany przez interfejs WEB Podsystem, umożliwiający klientowi (klientom docelowym SPNT) obsługę, monitoring i zarządzanie wykupionymi usługami, zakup nowych usług, dokonywanie płatności (przy udziale Billingu), zakup usług w ramach programu partnerskiego, obsługę konta klienta i partnera, zgłaszanie problemów (przy udziale Trouble Ticketing).
    d. **Cloud API** - Podsystem stanowiący warstwę abstrakcji, który pozwoli w spójny, łatwy do wykorzystania sposób udostępnić wewnętrzne interfejsy API użytkownikom zewnętrznym.
    e. **SSO –** Podsystem umożliwiający obsługę konta klienta przez wszystkie komponenty Platformy, bez konieczności logowania się przez klienta do każdego z nich z osobna. Zapewnia zarządzanie tożsamością klienta w każdym z Podsystemów.
    f. **ESB** - Podsystem zapewniający wzajemną komunikację i integrację wszystkich elementów Platformy poprzez wspólną szynę danych.
    g. **Trouble Ticketing** - Podsystem umożliwiający tworzenie, monitorowanie i obsługę zgłoszeń dotyczących świadczonych usług. Umożliwia klientowi zgłaszanie problemów i nieprawidłowości funkcjonowania usługi, z której korzysta, oraz kontakt z dostawcą usług w zakresie płatności, problemów technicznych związanych z obsługą Systemu itp.
    h. **Billing** - Podsystem umożliwiający naliczanie, fakturowanie oraz płatności za używane przez klienta usługi w oparciu o określone jednostki rozliczeniowe (ilość procesorów, wielkość przestrzeni dyskowej, czas dostępu itp.)
    i. **Portal** - Podsystem pełniący funkcję informacyjną w zakresie oferowanych usług, aktualności, informacji technicznych. Umożliwia klientowi zapoznanie się z publikowanymi na stronie WWW informacjami dotyczącymi wspomnianych kwestii.

Portal umożliwia ponadto dostęp do Bazy Wiedzy - zawierającej elektroniczną wersję dokumentacji opracowanej przez Wykonawcę w trakcie realizacji projektu oraz Katalogu Usług pozwalającego na dostęp do osadzonych na Podsystemach IaaS i PaaS aplikacji w modelu SaaS. Portal zintegrowany zostanie z SelfService dzięki koszykowi, co umożliwi odwiedzającym składanie zamówień produktów opisanych na Portalu.

j. **Centralny system logów** – Podsystem umożliwiający m. in. wykrywanie krytycznych zdarzeń na podstawie odpowiednio zdefiniowanych reguł, zbierający kluczowe informacje o błędach i aktywności wszystkich Podsystemów.

k. NOC - tzw. Network Operating Center - zestaw Podsystemów oprogramowania umożliwiający monitoring, ewidencję i zarządzanie Systemem składający się m. in. z:

i. DCIM,

ii. Podsystem do monitoringu,

iii. Podsystem zarządzania.

Szczegółowy opis poszczególnych komponentów wraz ze szczegółowymi wymaganiami znajduje się w rozdziałach 4 i 5 niniejszego dokumentu.

W ramach dostarczenia Systemu, Wykonawca jest zobowiązany do wykonania następujących czynności:

- Wykonania analizy przedwdrożeniowej;
- Przygotowania projektu technicznego rozwiązania;
- Dostarczenia, zainstalowania oraz skonfigurowania infrastruktury sprzętowej;
- Dostarczenia, wdrożenia oraz parametryzacji komponentów oprogramowania;
- Przeprowadzenia testów Platformy zgodnie z opracowanymi i zatwierdzonymi scenariuszami testowymi oraz opracowania raportów z przeprowadzonych testów. Zakres testów obejmuje:
    a. Testy funkcjonalne,
    b. Testy integracyjne,
    c. Testy akceptacyjne,
    d. Testy bezpieczeństwa;
- Przeprowadzenia instruktaży stanowiskowych dla przedstawicieli SPNT;
- Zapewnienia asysty stanowiskowej dla przedstawicieli SPNT na etapie wdrażania oraz w okresie gwarancji (opisanej w Umowie – załącznik 8a do SIWZ);
- Przekazania SPNT pełnej dokumentacji technicznej dostarczonej infrastruktury informatycznej i oprogramowania;
- Udzielenia gwarancji w okresie wskazanym w Umowie – załącznik 8a do SIWZ.

Szczegółowy opis czynności i produktów do dostarczenia znajdują się w rozdziałach 3-6 niniejszego dokumentu oraz w Umowie (załącznik 8a do SIWZ).

2.2. Usługi

W oparciu o dostarczony System, Zamawiający będzie świadczył następujące Usługi:

2.2.1. Usługi IaaS:

Główne założenia dla usług oferowanych w modelu IaaS, to:

- **Stworzenie solidnych i stabilnych rozwiązań bazujących na doświadczeniu i najlepszych praktykach obecnych graczy rynkowych** zapewniając infrastrukturę o wysokiej dostępności (High Availability) oraz oprogramowanie pozwalające na elastyczne podążanie za trendami rynkowymi.
- **Możliwość tworzenia produktów szytych na miarę dla konkretnej grupy docelowej** – szczególnie pod kątem dostawców rozwiązań SaaS dla wybranych grup docelowych (administracja publiczna, wybrani klienci lokalnych firm IT, branża medyczna).
- **Synergia z ofertą PaaS** – oferowane rozwiązania IaaS powinny być zbudowane w taki sposób, by umożliwić łączenie z usługami PaaS działającymi w ramach Systemu.
- **Niezależność od warstwy sprzętowej** - System powinien zostać wdrożony i zoptymalizowany pod kątem zapewnienia wysokiej wydajności we współpracy ze sprzętem zaproponowanym przez Wykonawcę, natomiast sam Podsystem IaaS musi być niezależny od producenta platformy sprzętowej (wspierać wielu producentów) na każdej płaszczyźnie: obliczeniowej (compute), danych (storage) oraz sieci (network) i umożliwiać dołączenie dowolnego typu sprzętu do wdrożonego już rozwiązania.

Poniższa tabela zawiera listę usług IaaS, które będą oferowane Klientom w formie pakietów produktowych:

Nazwa	Opis	Główne funkcjonalności
Serwery dedykowane	Możliwość wynajęcia wydzielonego serwera w jednej z dostępnych konfiguracji – procesor, dysk twardy i pamięć.	• Maszyna serwerowa do wyłącznej dyspozycji klienta w oparciu o wybraną konfigurację • Możliwość samodzielnej konfiguracji serwera oraz instalacji oprogramowania przez interfejs web • Zarządzanie serwerem przez SSH i web panel • Płatność miesięczna • Zarządzanie oraz monitoring przez API
VPS	Wirtualny serwer, który umożliwia optymalne wykorzystanie infrastruktury serwerowej i zaoferowanie Klientowi rozwiązania	• Zapewnienie gwarantowanej ilości zasobów sprzętowych serwera (RAM, HDD, CPU) • Możliwość samodzielnej konfiguracji serwera oraz instalacji oprogramowania

	bardziej zaawansowanego od hostingu współdzielonego, przy niższej cenie niż serwer dedykowany.	przez web • Zarządzanie serwerem przez SSH i web panel • Płatność miesięczna • Skalowalność serwera (zmiana parametrów w panelu lub przez API) • Zarządzanie oraz monitoring przez API oraz CLI
Cloud server	W pełni elastyczny i skalowalny wirtualny serwer rozliczany tylko za okres korzystania z zasobów, co daje najbardziej efektywne zarządzanie zasobów. Umożliwia sterowanie obciążeniem oraz amortyzuje nadmiarowy ruch.	• System cloudowy konfigurowalny pod względem: a. liczby rdzeni procesora (1-32 rdzeni – 32/64 bit), b. wielkości RAM (512MB-128GB), c. HDD (dysk systemowy + dodatkowe dyski), d. systemu operacyjnego (FreeBSD/ Linux / Windows) • Opłaty za wykorzystanie zasobu naliczane co do jednostki czasu (np. godziny) - Pay-As-You-Go • Pełna skalowalność serwera • Zarządzanie oraz monitoring przez API oraz CLI
Chmura dedykowana (prywatna)	Rozwiązanie pozwalające zbudować prywatną sieć wewnątrz infrastruktury w chmurze – pozwala budować krytyczne środowiska cloudowe gwarantując całkowitą izolację i wysokie parametry SLA.	• Połączenie większej liczby serwerów dedykowanych w ramach jednej sieci prywatnej (wraz z dostępem do tej sieci przez VPN) • Połączenie większej liczby serwerów VPS w ramach jednej sieci prywatnej (wraz z dostępem do tej sieci przez VPN) • Połączenie większej liczby serwerów cloud w ramach jednej sieci prywatnej (wraz z dostępem do tej sieci przez VPN)
Blokowy cloud storage	Wydzielony obszar na dysku twardym, który pozwala na odczytywanie i zapisywanie danych w postaci bloków.	• Brak ograniczeń dla przestrzeni, transferu czy liczby Klientów podłączonych jednocześnie • Wgrywanie plików w częściach • Opcja szyfrowania danych

		• Komunikacja poprzez API
Obiektowy cloud storage	Rozwiązanie storage'owe pozwalające na zapisywanie i odczytywanie obiektów bez względu na ich rozmiar.	• Możliwość odczytu, zapisu i modyfikacji plików i obiektów o dowolnym rozmiarze przechowywanych w kontenerach • Publiczne udostępnienie zasobów • Przechowywanie danych w postaci obiektów hierarchizowanych do struktury – drzewa, listy. • Komunikacja poprzez API • Szyfrowane połączenie (SSL)
Load Balancer as a Service (LBaaS)	Skalowalne zarządzanie ruchem na żądanie - dystrybucja obciążenia pomiędzy dwa lub więcej serwerów lub sieci by zapewnić maksymalną przepustowość, zminimalizować czas odpowiedzi i uniknąć przeciążeń.	• Dedykowany statyczny adres IP • Zapewnienie High Availability dzięki tylko jednemu Load Balancerowi • Billingowanie tylko za wykorzystany czas usługi (niski Total Cost of Ownership) • Obsługa serwerów chmurowych jak i tradycyjnych (dedykowane, kolokacja)
VPN as a Service (VPNaaS)	Rozwiązanie zabezpieczające komunikację z serwerami chmurowymi i tradycyjnymi, komputerami oraz urządzeniami mobilnymi umożliwiając bezpieczny dostęp tylko dla uprawnionych użytkowników.	• Prosta instalacja i konfiguracja • Brak konieczności zarządzania sprzętem • Niezależność klientów (oprogramowania klienckiego) od systemu operacyjnego • Obsługa serwerów chmurowych jak i tradycyjnych (dedykowane, kolokacja) • Obsługa urządzeń mobilnych
Firewall as a Service (FWaaS)	Zabezpieczenie serwerów chmurowych i tradycyjnych przed zewnętrznymi zagrożeniami dzięki ochronie ruchu przychodzącego i wychodzącego w oparciu o konfiguracje reguł i polityk.	• Zarządzanie firewallem poprzez proste w użyciu web panel • Elastyczne tworzenie, zarządzanie oraz prezentacja (filtrowanie/przeszukiwanie) reguł • Analityka i dane historyczne • Obsługa serwerów chmurowych jak i tradycyjnych (dedykowane, kolokacja)

Usługi dodane w ramach IaaS

- Dodatkowe adresy IP (IPv4 oraz IPv6)
- Obsługa domen
- Obsługa certyfikatów SSL
- Monitoring infrastruktury
- Backup infrastruktury

2.2.2. Usługi PaaS

Tworzenie i zarządzanie wirtualnymi środowiskami developerskimi i produkcyjnymi z gotowymi komponentami i rozwiązaniami niewymagającymi ręcznej konfiguracji.
Zamawiający ma w szczególności na celu stworzenie przyjaznego, elastycznego, skalowalnego i bezpiecznego środowiska dla tworzenia i późniejszego hostowania aplikacji w modelu SaaS.
Główne założenia dla usług oferowanych w modelu PaaS, to:

- **Zbudowanie rozwiązania PaaS zapewniającego kompleksową ofertę pod kątem funkcjonalności, efektywności, stabilności, skalowalności i bezpieczeństwa.** Pozwoli to na wyróżnienie się na rynku polskim, który oferuje już pierwsze rozwiązania PaaS, są one jednak dalekie od szerokiego zakresu funkcjonalności i dostępności oferty wypracowanej przez liderów rynku globalnego.
- **Zaoferowanie produktów PaaS w modelu „on-demand" -** tworzenie dedykowanych konfiguracji komponentów usług zwane szablonami, których to nie ma w standardowych pakietach produktowych. Takie dedykowane szablony zawierałyby przede wszystkim nietypowe konfiguracje środowisk developerskich z wykorzystaniem starszych wersji baz danych czy języków oprogramowania. Byłyby one możliwe do wykorzystania w przyszłości przez innych klientów. Taka usługa odpowiadałaby głownie na potrzeby firm programistycznych na potrzeby budowy zaplecza developerskiego i testowego, które niejednokrotnie wymagają specyficznych konfiguracji środowiska programistycznego.
- **Modele współpracy ze środowiskiem chmurowym:**
    - Integracja z oferowanymi rozwiązaniami IaaS - Architektura PaaS musi integrować się bezpośrednio z IaaS oraz wykorzystywać infrastrukturę zarządzaną przez IaaS. Oznacza to, że PaaS wykorzystuje IaaS w celu zarządzania środowiskami systemów operacyjnych, sieci czy też warstwą danych (storage) w celu zapewnienia elastyczności, skalowalności jak i bezpieczeństwa rozwiązania.
    - Otwartość Podsystemu na przyszłe integracje z rozwiązaniami IaaS innych dostawców jak np. Amazon WS, Azure czy Oracle
- **Stworzenie materiałów promujących korzyści z wykorzystania PaaS dla developerów –** firmy korzystające z rozwiązań PaaS notują oszczędności kosztów operacyjnych instalowania, utrzymywania i rozwoju aplikacji do 50%, co wymaga dobrego zakomunikowania, by przekonać odbiorców do otwarcia się na nowe innowacyjne rozwiązania.

- **Zapewnienie wysokiej klasy wsparcia technicznego dla klientów oraz zaangażowania społeczności developerów** przyczyni się do budowania świadomości nowego produktu. Stanowi to ważny punkt wzmocnienia przekazu realnych korzyści z korzystania z rozwiązania przez samych developerów (sprzedaż przez rekomendację, dzielenie się realnymi korzyściami).

Główne funkcjonalności:

- **Środowiska developerskie** - Stworzenie rozwiązania dla firm programistycznych umożliwiającego szybkie osadzanie niezawodnych i skalowanych aplikacji w oparciu o predefiniowane środowiska developerskie złożone z wybranych komponentów: języków programowania, baz danych, frameworków i systemów operacyjnych. PaaS zintegrowany z rozwiązaniem chmurowym IaaS tworzonym w ramach Systemu. Każde środowisko jest niezależną instancją z dedykowanymi zasobami.
- **Interfejs** - Automatyczny provisioning i zarządzanie zoptymalizowanymi środowiskami aplikacyjnymi za pomocą interfejsów takich jak intuicyjny panel SelfService, API, CLI oraz przez systemy VCS (systemy kontroli wersji).
- **Automatyzacja i skalowanie** - zaawansowane mechanizmy automatyzacji komponentów (optymalizacja zasobów, skalowanie i zarządzanie konfiguracją) i systemu (replikacja baz danych, backup, load balancing, monitoring) przynoszące realne oszczędności w porównaniu do samodzielnie zarządzanej infrastruktury własnej (niwelując znaczącą cześć prac operacyjnych i tym samym obniżając koszty projektowe).
- **Billingowanie** - Klient rozliczany jest tylko za wykorzystane zasoby według jednostki czasu (np. jednej godziny).
- **PaaS on-demand** - Konfigurowanie szablonów PaaS na zamówienie – dowolna konfiguracja komponentów, szczególnie przy wykorzystaniu starszych wersji baz danych i języków oprogramowania. Zapisywanie szablonów z możliwością wykorzystania w przyszłości przez innych odbiorców.

Korzyści dla klienta

- Stworzenie warunków programistom do konfiguracji i uruchamiania bezpiecznego środowiska developerskiego w krótkim czasie (skrócenie Time to Market dla aplikacji) - automatyzacja długotrwałego i często powtarzalnego procesu uruchamiania skomplikowanych środowisk developerskich, testowych czy produkcyjnych.
- Umożliwienie developerom skupienie się tylko na zadaniach związanych bezpośrednio z pisaniem oprogramowania dzięki utrzymaniu środowisk programistycznych z uwzględnieniem czasochłonnych prac, jakimi są administracja, monitorowanie i zarządzanie aktualizacjami.
- Dostarczenie wystandaryzowanego workflow pozwalającego zwiększać efektywność i produktywność działania.
- Generowanie oszczędności kosztów operacyjnych w sferze wytwarzania oprogramowania nawet do 50%.

2.2.3. Usługi telekomunikacyjne

W kontekście umiejscowienia Szczecińskiego Parku Naukowo-Technologicznego – zarówno pod względem geograficznym, jak również w odniesieniu do charakteru tej instytucji, łączącej sferę biznesową ze sferą samorządową - niezmiernie istotny jest aspekt wykorzystania centrum danych na potrzeby integracji telekomunikacyjnej.

Nazwa	Opis
Dostawa Internetu	• na potrzeby usług świadczonych w ramach DC - IaaS, PaaS i SaaS • na potrzeby kolokacji i firm zlokalizowanych w biurach Technoparku Pomerania, • udostępnienie punktów styku na potrzeby przyłączenia się do centrów wymiany ruchu w Polsce i Europie O konkurencyjności oferty świadczyć będą parametry: oferowana przepływność, poziom opóźnień, ograniczenia pod względem ilości przesyłanych danych, poziom bezpieczeństwa i dostępności usług, jakość monitoringu CD a także ceny usług.
Szczecin Internet Exchange (SIX)	• punkt ewidencji, wymiany i zarządzania infrastrukturą światłowodową • punkt wymiany i zarządzania kanałami transmisyjnymi • punt wymiany ruchu IP poprzez protokół BGP
Usługi LIR (Lokalny Rejestr Internetowy)	Pozyskiwanie i utrzymywanie internetowych zasobów numeracyjnych: • numery systemów autonomicznych (ASN), • klasy adresowe typu provider independent, zarówno dla protokołu IPv4, jak i nowego standardu IPv6.
Kolokacja	• kolokacja sprzętu, • kolokacja sprzętu dla rozwiązań z dziedziny telemedycyny.

3. Przebieg i produkty Projektu

W ramach Projektu Wykonawca musi przeprowadzić analizę wymagań, na jej podstawie zaprojektować, wdrożyć, skonfigurować i zasilić danymi oraz treścią oprogramowanie, a także dostarczyć, skonfigurować, zintegrować i wdrożyć zaoferowany sprzęt oraz przeprowadzić wszelkie czynności niezbędne do uruchomienia produkcyjnego dostarczonego rozwiązania i rozpoczęcia świadczenia Usług przez Zamawiającego.

W ramach przeprowadzanych analiz Wykonawca powinien zidentyfikować poszczególnych aktorów i ich potrzeby (wymagania), które zostaną zrealizowane w ramach Projektu. Oznacza to, że Wykonawca w ramach opracowania Projektu Technicznego Systemu dokona szczegółowego opisu zakresu

realizacji wdrożenia Systemu oraz aspektów technicznych tego wdrożenia. Przykładowo, analiza produktów, które mają być elementem oferty Zamawiającego, powinna dać między innymi odpowiedź na pytanie, jakie metryki i reguły biznesowe będą składać się na politykę cenową produktów. Na tej podstawie Wykonawca sprecyzuje i zrealizuje odpowiednie wymagania funkcjonalne i pozafunkcjonalne Systemu, uwzględniając przy tym zapisy SIWZ i OPZ.

Należy zaznaczyć, że podział funkcjonalny, zaproponowany w niniejszym dokumencie, jest w znacznym stopniu uzależniony od architektury i zakresu funkcjonalnego komponentów oferowanych przez Wykonawcę. Aby zapewnić optymalny przebieg projektu i łatwość utrzymania wdrożonego rozwiązania, Zamawiający, na etapie akceptacji projektu technicznego, może (ale nie musi) dopuścić pewne przesunięcia zakresów funkcjonalnych między poszczególnymi Podsystemami, biorąc pod uwagę potrzeby użytkowników końcowych, użyteczność projektowanego rozwiązania, jego bezpieczeństwo, łatwość utrzymania, elastyczność i skalowalność.

3.1. Produkty Projektu

W poniższej tabeli wskazano listę produktów specjalistycznych, które powinny zostać dostarczone przez Wykonawcę w trakcie realizacji projektu.

ID	Nazwa	Opis	Etap	Dotyczy												
				Sprzęt	NOC	IaaS	PaaS	SSO	Portal	Katalog Usług	Baza Wiedzy	Trouble Ticketing	Self Service	Billing	System logów	Cloud API
P.A	**Analiza Wymagań**															
P.A.1	Słownik Projektu	Słownik, definiujący istotne pojęcia wykorzystywane w Projekcie w celu zbudowania wspólnej terminologii dla wszystkich uczestników Projektu.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.A.2	Specyfikacja Usług	Celem dokumentu jest dospecyfikowanie Usług, które będą oferowane przez Zamawiającego i zostaną skonfigurowane w ramach realizacji Projektu. Dokument musi zawierać informacje o otoczeniu rynkowym Usług (grupy docelowe produktów, konkurencja), identyfikować wszystkie stosowane na rynku parametry rozliczeń Usług, a	II	TAK	TAK	TAK	TAK		TAK	TAK	TAK		TAK	TAK		TAK

		także zawierać Usług rekomendowane do włączenia do oferty wraz z wszystkimi parametrami wymaganymi do ich implementacji.														
P.A.3	Model przypadków użycia	Model przypadków użycia, zawierający co najmniej: zidentyfikowanych aktorów, zidentyfikowane przypadki użycia, krótkie opisy przypadków użycia.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.A.4	Analiza wymagań	Dokument stanowiący wynik przeprowadzonych przez Wykonawcę prac analitycznych związanych z identyfikacją, uporządkowaniem i analizą wymagań realizowanych w Projekcie.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.A.5	Rejestr Wymagań	Rejestr wymagań, prowadzony w formie elektronicznej w ramach Podsystemu Trouble Ticketing, zawierający	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		wszystkie zidentyfikowane, atomowe wymagania funkcjonalne i pozafunkcjonalne, zapewniający pełną śledzalność wymagań od ich źródła, poprzez wytwarzanie aż do testów. Rejestr powinien zawierać zarówno wymagania przeznaczone do realizacji, jak i odrzucone. W rejestrze powinny znaleźć się też pomysły przyszłego rozwoju Systemu.														
P.A.6	Analiza procesów obsługi Klienta	Dokument przedstawiający proponowane procesy związane z obsługą Klienta, w tym procesy obsługi zgłoszeń serwisowych, procesy sprzedaży itp. Ponadto dokument powinien zawierać rekomendację	II						TAK	TAK	TAK	TAK	TAK			

		struktury organizacyjnej niezbędnej do realizacji wskazanych procesów.														
P.A.7	Analiza wymagań prawnych	Dokument specyfikujący obowiązujące przepisy prawa krajowego i międzynarodowego w zakresie świadczenia usług dla sektora rządowego, medycznego i biznesu, wraz z mapą pokrycia poszczególnych przepisów wymaganiami w Rejestrze Wymagań.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.A.8	Analiza ryzyka	Dokument specyfikujący ryzyka związane ze świadczeniem planowanych Usług, zarówno w warstwie prawnej, organizacyjnej jak i technicznej, oraz identyfikujący sposób	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		postępowania z tymi ryzykami. Dokument powinien być także źródłem wymagań do zrealizowania w ramach budowanego Systemu.														
P.A.9	Analiza dostawców usług zewnętrznych i kosztów eksploatacyjnych	Dokument ma stanowić podstawę do wyboru dostawców usług zewnętrznych niezbędnych do zrealizowania projektu, takich, jak wysyłka wiadomości SMS czy operator płatności internetowych, dostawców mediów (prąd, łącza internetowe itp.), z uwzględnieniem istniejących możliwości technicznych w lokalizacji Zamawiającego. Analiza powinna zawierać także zestawienie wszystkich kosztów operacyjnych,	II	TAK	TAK											

		włączając w to koszty osobowe (z podziałem na stanowiska).														
P.PT	**Projekt Techniczny**															
P.PT.1	Architektura ogólna	Dokument stanowiący wprowadzenie do Projektu i pozwalający szybko zorientować się w ogólnych założeniach projektu, jego kontekście, powiązaniach między poszczególnymi Podsystemami i elementami infrastruktury.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.PT.2	Architektura szczegółowa	Dokument specyfikujący architekturę Systemu. W dokumencie należy uwzględnić co najmniej: wykorzystywane technologie i wzorce projektowania architektury, powiązania Systemu z innymi systemami,	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		wewnętrzną strukturę Systemu, interfejsy wewnętrzne i zewnętrzne Systemu wraz z zakresami wymienianych danych (w powiązaniu z "Logicznym modelem danych").														
P.PT.3	Architektura sprzętowa i sieciowa (infrastruktura)	Dokument opisujący sposób wdrożenia infrastruktury sprzętowej i sieciowej.	II	TAK	TAK											
P.PT.4	Rejestr decyzji architektonicznych	Prowadzony w formie elektronicznej (w ramach Podsystemu Trouble Ticketing) rejestr, którego celem jest udokumentowanie podjętych decyzji architektonicznych.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.PT.5	Projekt sieci	Dokument zawierający szczegółowy opis sposobu konfiguracji sieci dla wszystkich węzłów i połączeń w ujęciu OSI L1-L7 (m. in. połączenia	II	TAK												

		fizyczne, realizację sieci Ethernet, adresację IP, routing i w warstwach wyższych z uwzględnieniem urządzeń UTM i LB)														
P.PT.6	Architektura Informacji	Dokument opisujący zasady tworzenia struktury informacyjnej serwisu.	II						TAK	TAK	TAK	TAK	TAK			
P.PT.7	Projekt optymalizacji na potrzeby SEO i sieci społecznościowych	Dokument opisujący sposób zapewnienia maksymalnej widoczności treści w wyszukiwarkach internetowych i sieciach społecznościowych.	II					TAK	TAK	TAK	TAK		TAK			
P.PT.8	Projekt wdrożenia	Dokument specyfikujący sposób wdrożenia produktów Projektu.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.PT.9	Projekt zabezpieczeń	Projekt zabezpieczeń specyfikujący sposób zapewnienia bezpieczeństwa Systemu, w tym co najmniej: zastosowany model uprawnień do poszczególnych funkcjonalności i	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		obiektów w Podsystemach, polityka kopii zapasowych, wytyczne do konfiguracji infrastruktury sprzętowej i sieciowej, firewalli, load balancerów, systemów operacyjnych, serwerów aplikacji, wykrywania i zapobiegania incydentom itp.														
P.PT.10	Logiczny model danych	Model danych, przedstawiający na poziomie logicznym wszystkie dane występujące w Podystemach	II		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.PT.11	Fizyczny model danych	Model danych, przedstawiający na poziomie fizycznym wszystkie dane występujące w Podsystemach	II		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.PT.12	Projekt graficzny i użyteczności Systemu	Projekt graficzny wraz z projektem usability oraz analizą heurystyczną (nazywaną czasem heurystyką, analizą	II			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		ekspercką) Projektu w celu określenia zgodności z powszechnie uznanymi zasadami usability.														
P.W	**Wytwarzanie**															
P.W.1	Standardy kodowania	Dokument, którego celem jest ustalenie sposobu prowadzenia prac programistycznych tak, by zapewnić wysoką jakość, czytelność i niezawodność tworzonego kodu, a także ciągłą integrację i automatyczne testowanie oprogramowania.	I			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.2	Scenariusze testów akceptacyjnych	Scenariusze testów akceptacyjnych, pokrywające wszystkie zrealizowane wymagania funkcjonalne i pozafunkcjonalne dotyczące oprogramowania i infrastruktury, wraz z weryfikacją	III	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		poprawności obsługi błędów.														
P.W.3	Testy jednostkowe	Zbiór testów jednostkowych, pokrywających minimum 80% kodu wytworzonego w ramach Projektu.	II			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.4	Automatyczne testy funkcjonalne	Zestaw automatycznie wykonywanych testów, pokrywających co najmniej wszystkie scenariusze testów akceptacyjnych, dla których istnieje techniczna możliwość automatyzacji.	III	TAK		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.5	Pakiety instalacyjne oprogramowania	Pakiety binarne umożliwiające zainstalowanie produktów projektu (np. rpm lub deb w przypadku Linuksa, exe lub MSI dla Windows itp.), dostarczone w formie skonfigurowanego i wdrożonego repozytorium pakietów	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		instalacyjnych oraz skonstruowane w sposób umożliwiający ich automatyczne instalowanie i aktualizowanie.														
P.W.6	Kod źródłowy oprogramowania	Pełen, zgodny z przyjętymi standardami kodowania kod źródłowy oprogramowania. Dotyczy co najmniej całego oprogramowania, co do którego następuje przekazanie praw autorskich.	V		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.7	Specyfikacja interfejsów programistycznych	Pełna specyfikacja API udostępnianego przez Podsystemy	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.8	Dokumentacja kodu źródłowego oprogramowania	Wygenerowana automatycznie dokumentacja kodu źródłowego oprogramowania, obejmująca minimum wszystkie klasy, metody, pola i funkcje wytworzone bądź zmodyfikowane w	V		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		ramach Projektu.														
P.W.9	Specyfikacja wykorzystywanych bibliotek i komponentów	Specyfikacja wszystkich bibliotek i komponentów wykorzystywanych w Projekcie wraz z informacją o sposobie licencjonowania tego komponentu.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.W.10	Licencje	Licencje na produkty przekazane w ramach realizacji Projektu.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.DP	**Dokumentacja powykonawcza**															
P.DP.1	Dokumentacja użytkownika	Dokumentacja ma na celu przedstawienie użytkownikom sposobu działania poszczególnych funkcjonalności i poprowadzenie ich krok po kroku przez najczęściej wykonywane operacje. Dokumentacja powinna być przygotowana w sposób dostosowany do ról, jakie pełnią poszczególni użytkownicy	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		(oddzielnie dla Klientów, oddzielnie dla obsługi itp.).														
P.DP.2	Dokumentacja publicznych API	Dokumentacja ma na celu opisanie, wraz z przykładami, całego API udostępnianego publicznie dla Klientów.	IV													TAK
P.DP.3	Dokumentacja Administratora	Dokumentacja ma na celu przedstawienie administratorom poszczególnych funkcjonalności Systemu.	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.DP.4	Procedury eksploatacyjne	Procedury, przedstawiające szczegółowo sposób realizacji poszczególnych zadań związanych z eksploatacją Systemu. Opis zbioru czynności eksploatacyjnych mających na celu zrealizowanie określonego zadania eksploatacyjnego np. wykonanie aktualizacji systemu operacyjnego.	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		Procedury muszą obejmować wszystkie czynności konieczne do realizowania w celu monitorowania i utrzymania dostarczonych komponentów Systemu w poprawnym działaniu i zgodności z najnowszymi wersjami.														
P.DP.5	Plan zachowania ciągłości działania	Opis sposobu zachowania ciągłości działania w sytuacjach kryzysowych, w tym plan odtworzenia Systemu po awarii.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.DP.6	Polityka bezpieczeństwa	Polityka bezpieczeństwa opracowana dla wdrażanego rozwiązania. Musi uwzględniać istniejącą politykę bezpieczeństwa SPNT.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.DP.7	Procedury przetwarzania danych osobowych	Procedury związane z przetwarzaniem danych osobowych w ramach	IV						TAK	TAK	TAK			TAK		

		świadczonych Usług.														
P.DP.8	Treści elektroniczne	Wszystkie treści niezbędne do rozpoczęcia świadczenia Usług, w tym: opisy produktów, baza wiedzy, elementy multimedialne, pomoc kontekstowa, regulaminy i szablony umów z Klientami, polityki prywatności. Treści powinny być przygotowane w języku polskim i angielskim.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.DP.9	Księga Konfiguracji	Wyciąg z konfiguracji wszystkich Podsystemów i całej infrastruktury, przedstawiający ich docelową konfigurację.	V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.T	**Testy**															
P.T.1	Plan zapewnienia jakości	Dokument, którego celem jest przedstawienie planowanej organizacji, zakresu i przebiegu procesów zapewnienia jakości	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		w projekcie.														
P.T.2	Raport z testów akceptacyjnych	Dokument zawierający informacje o przebiegu i wynikach testów akceptacyjnych.	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.T.3	Raport z testów interfejsu użytkownika	Dokument, którego celem jest przedstawienie wyników weryfikacji interfejsu użytkownika pod kątem użyteczności (usablility) i zgodności z projektem graficznym. Dokument powinien uwzględniać przeprowadzone prace mające na celu weryfikację zgodności wytworzonych Podsystemów z Projektem, a także testy przy udziale reprezentatywnej grupy użytkowników (focus group).	IV			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
P.T.4	Raport z testów bezpieczeństwa	Raport zawierający wyniki przeprowadzonych	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		testów bezpieczeństwa. Raport powinien pozwolić na ocenę, czy określone w ramach Projektu wymagania bezpieczeństwa zostały spełnione, a także zawierać wnioski i rekomendacje działań mających na celu minimalizację zidentyfikowanych ryzyk w obszarze bezpieczeństwa.														
P.T.5	Raport z testów wydajności	Raport zawierający wyniki przeprowadzonych testów wydajności. Raport powinien pozwolić na ocenę, czy określone w ramach Projektu wymagania wydajnościowe zostały spełnione oraz jakie maksymalne obciążenie może obsłużyć Rozwiązanie.	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.T.6	Raport z testów API	Raport zawierający	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		wyniki przeprowadzonych testów interfejsów programistycznych (API).														
P.T.7	Raport z testów integracyjnych	Dokument zawierający informacje o przebiegu i wynikach testów integracyjnych.	IV	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Ś.	**Środowiska**															
P.Ś.1	Środowisko developerskie	Celem środowiska developerskiego jest zapewnienie platformy dla Wykonawcy, na której będą prowadzone prace wytwórcze. Środowisko to będzie też służyć jako laboratorium dla Zamawiającego.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Ś.2	Środowisko testowe	Celem środowiska testowego jest zapewnienie niezależnej infrastruktury, przeznaczonej do przeprowadzania testów akceptacyjnych Systemu.	II	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

P.Ś.3	Środowisko integracyjne	Celem środowiska integracyjnego jest ciągłe, automatyczne integrowanie, budowanie i testowanie oprogramowania i infrastruktury, w celu zapewnienia jak najwyższej jakości wytwarzanych produktów oraz unikania błędów integracyjnych i regresji. Środowisko integracyjne powinno być wykorzystywane przez cały cykl życia poszczególnych Podsystemów, zaczynając od wczesnych etapów wytwarzania oprogramowania, a kończąc na utrzymaniu.	III	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Ś.4	Środowisko produkcyjne	Celem środowiska produkcyjnego jest świadczenie usług produkcyjnych na rzecz Klientów. Środowisko	III	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		produkcyjne powinno być przygotowane w taki sposób, by w momencie uruchomienia produkcyjnego możliwe było obsłużenie pierwszych Klientów bez wykonywania żadnych dodatkowych prac.														
P.Z.	**Zarządcze**															
P.Z.1	Rejestr Zadań	Prowadzony w formie elektronicznej, w ramach Podsystemu Trouble Ticketing, rejestr wszystkich zadań roboczych realizowanych w Projekcie, np. zadań wynikających ze spotkań projektowych, zadań programistycznych itp. Rejestr ten powiązany jest z Rejestrem Wymagań.	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Z.2	Szablony dokumentacji projektowej	Szczegółowe szablony wszystkich dokumentów	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		dostarczanych w ramach Projektu, przedstawiające zakres dokumentu i cel dokumentu, planowany spis treści dokumentu i przykładowe zapisy w dokumencie.														
P.Z.3	Proces wytwarzania oprogramowania	Ustalony na wstępnym etapie projektu dokument opisujący sposób pracy przy przygotowywaniu i wdrażaniu oprogramowania, uwzględniający mechanizmy ciągłej integracji i pełne wykorzystanie Podsystemu Trouble Ticketing. Dokument powinien ponadto zawierać wszystkie informacje niezbędne do skonfigurowania i wdrożenia Podsystemu Trouble Ticketing na potrzeby prowadzenia w nim wszystkich prac	I			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		projektowych.														
P.Z.4	Harmonogramy wykonawcze	Opracowane przez Wykonawcę w każdym etapie Projektu w oparciu o dostarczony przez Zamawiającego Harmonogram ramowy (będący załącznikiem do Umowy). Zawierający wszystkie przewidziane i uwzględnione do realizacji w danym etapie (oraz ujęte w Rejestrze Zadań) zadania wraz z terminami wykonania.	I-V	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Z.5	Strategia zarządzania ryzykiem	Określa techniki i standardy zarządzania ryzykiem, zawiera Rejestr ryzyk wraz ze wstępną identyfikacją kluczowych ryzyk Projektu, oceną ich wypływu na Projekt oraz możliwe działania zaradcze. Dokument będzie	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

		podlegał aktualizacji przez cały okres trwania Projektu.														
P.Z.6	Strategia zarządzania konfiguracją	Określa w jaki sposób i przez kogo będą kontrolowane i chronione produkty Projektu, uwzględniając wykorzystanie Systemu kontroli wersji (VCS)	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
P.Z.7	Strategia zarządzania komunikacją	Określa środki i częstotliwość komunikacji zarówno po stronie Wykonawcy jak i między Wykonawcą, a Zamawiającym, przy uwzględnieniu wykorzystania Podsystemu Trouble Ticketing oraz zasad zawartych w Umowie (załącznik 8a do SIWZ).	I	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

Zamawiający, w uzgodnieniu z Wykonawcą, może odstąpić od realizacji niektórych elementów analizy i projektu technicznego w zakresie, w którym opisują one cechy realizowane przez wdrażane w ramach Projektu oprogramowanie standardowe firm trzecich, w wersji dostępnej na rynku w dniu złożenia Oferty przez Wykonawcę.

Wykonawca jest zobowiązany zapewnić możliwość pełnego śledzenia (ang. *traceability*) wymagań. Oznacza to, że musi istnieć udokumentowana ścieżka logiczna, prowadząca od źródła danego wymagania (np. przypadek użycia, dokument, SIWZ, przepis prawa), poprzez zadania programistyczne, aż do scenariuszy testowych pozwalających na weryfikację jego poprawnej realizacji.

3.2. Dostawy sprzętu i oprogramowania

Z uwagi na różne źródła finansowania Projektu Zamawiający wymaga, aby dostawy infrastruktury sprzętowej i Podsystemów oprogramowania odbywały się zgodnie z harmonogramem ramowym będącym załącznikiem do Umowy pomiędzy Wykonawcą, a Zamawiającym. Zamawiający ustala podział dostaw pozycji infrastruktury sprzętowej (w ilościach zgodnych z zestawieniem ilościowym podanym w rozdziale 4.2) i Podsystemów oprogramowania zgodnie z poniższymi tabelami.

3.2.1. Dostawy infrastruktury sprzętowej I

Lp.	Nazwa pozycji infrastruktury sprzętowej	Termin dostawcy
1	Router brzegowy	do 01.12.2014
2	Switch szkieletowy	
3	Firewall/UTM	
4	Load balancers	
5	Rozbudowa macierzy	
6	Switch MGMT	
7	Switch MGMT – agregacja	
8	Switch dostępowy (kompleks biurowy Technoparku Pomerania)	
9	Switch dostępowy POE (kompleks biurowy Technoparku Pomerania)	
10	Switch agregujący (kompleks biurowy Technoparku Pomerania)	
11	Rozszerzenia licencji kontrolerów Wi-Fi (kompleks biurowy Technoparku Pomerania)	
12	Punkty dostępowe (AP) (kompleks biurowy Technoparku Pomerania)	
13	Konwertery, moduły (transceivers): 10GE, 40GE, 1GE	
14	Bramka SMS	

3.2.2. Dostawy infrastruktury sprzętowej II

Lp.	Nazwa pozycji infrastruktury sprzętowej	Termin dostawcy
1	Serwery: compute nodes i distributed storage nodes Serwery: zarządzające i monitorujące	do 30.04.2015
2	Macierz	
3	Switch top of rack	
4	Szafy serwerowe	
5	Moduły chłodzące	

3.2.3. Dostawy Podsystemów oprogramowania I

Lp.	Nazwa pozycji infrastruktury sprzętowej	Termin dostawcy
1	Trouble Ticketing	do 01.12.2014
2	SSO	
3	ESB	

3.2.4. Dostawy Podsystemów oprogramowania II

Lp.	Nazwa pozycji infrastruktury sprzętowej	Termin dostawcy
4	IaaS	do 18.09.2015
5	PaaS	
6	Portal	
7	Katalog Usług	
8	Baza Wiedzy	
9	SelfService	
10	Cloud API	
11	Billing	
12	NOC: DCIM	
13	NOC: Podsystem zarządzania	
14	NOC: Monitoring	
15	Centralny system logów	

3.3. Analiza wymagań prawnych

Wykonawca realizując Projekt jest zobowiązany do przeprowadzanie analizy przepisów prawa dotyczących przedmiotu zamówienia oraz dostarczania produktów Projektu i całego Systemu zgodnie ze wskazanymi przez Zamawiającego aktami prawnymi. Dostarczony przez Wykonawcę System musi spełniać następujące założenia:

- System musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi w obszarze świadczenia Usług IaaS i PaaS na potrzeby sektora medycznego.
- System musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi w obszarze świadczenia Usług IaaS i PaaS na potrzeby sektora administracji publicznej.
- System musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi w obszarze świadczenia usług IaaS i PaaS na potrzeby sektora edukacyjnego.
- System musi informować użytkownika o używaniu Cookies zgodnie z obowiązującymi przepisami prawa.
- System musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi w obszarze świadczenia usług w formie elektronicznej.

3.3.1. Lista aktów prawnych

System musi być zgodny z obowiązującym prawem, a w szczególności z następującymi przepisami prawa:

3.3.1.1. Ustawy

Lp.	Identyfikator	Nazwa	Adres publikacji
1	U.INFOR.DZIAL.PODM.PUBL.	Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.	tekst jedn.: Dz. U. 2013 r. poz. 235
2	U.OCHR.DAN.OSOB.	Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.	tekst jedn.: Dz. U. 2002 Nr 101, poz. 926 ze zm.
3	U.PODPIS.ELEKTR.	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym.	tekst jedn.: Dz.U.2002.101.926
4	U.USŁUG.ELEKTR.	Ustawa z dnia z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną	tekst jedn.: Dz.U.2013.1422
5	U.PRAWO.TELEKOM.	Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne	tekst jedn.: Dz.U.2014.243
6	U.PRAWA.PACJENTA.	Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta	tekst jedn.: Dz.U.2012.159
7	U.INFORMACJA.ZDROWIE.	Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia	tekst jedn.: Dz.U.2011.113.657
8	U.POD.VAT	Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług	Dz. U. Nr 54, poz. 535 ze zm.
9	U.ORD.POD.	Ustawa z dnia 29 sierpnia 1997 r. Ordynacja	Dz. U. z 2005 r. Nr 8, poz.

		podatkowa	60 ze zm.

3.3.1.2. Rozporządzenia

Lp.	Identyfikator	Nazwa	Adres publikacji
1	R.KRI.	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.	Dz.U.2012.526
2	R.EPUAP.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej.	Dz.U.2011.93.546
3	R.IDENT.UŻYTK.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 21 kwietnia 2011 r. w sprawie szczegółowych warunków organizacyjnych i technicznych, które powinien spełniać system teleinformatyczny służący do identyfikacji użytkowników.	Dz.U.2011.93.545
4	R.TESTY.AKCEPT.	Rozporządzenie Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania.	Dz.U.2005.217.1836
5	R.DANE.OSOBOWE	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.	Dz.U.2004.100.1024
6	R.DOKUM.MEDYCZNA.	Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania.	Dz.U.2014.177
7	R.KRI.ZDROWIE.	Rozporządzenie Ministra Zdrowia z dnia 14 sierpnia 2013 r. w sprawie minimalnych	tekst jedn.: Dz.U.2014.177

		wymagań dla niektórych systemów teleinformatycznych funkcjonujących w ramach systemu informacji w ochronie zdrowia.	
8	R.IDENTYF.LEKARZE	Rozporządzenie Ministra Zdrowia z dnia 11 kwietnia 2013 r. w sprawie sposobu identyfikacji usługobiorców, pracowników medycznych i usługodawców oraz sposobu i trybu przekazywania przez usługodawców informacji o pracownikach medycznych udzielających świadczeń opieki zdrowotnej.	tekst jedn.: Dz.U.2013.999

4. Infrastruktura

4.1. Opis ogólny

Pod względem infrastruktury Wykonawca jest zobowiązany zaprojektować, dostarczyć, wdrożyć, a następnie utrzymywać i serwisować kompletną infrastrukturę sprzętową zintegrowaną z Platformą oprogramowania, a w szczególności Podsystemem IaaS (a w konsekwencji PaaS). Dostarczona infrastruktura powinna umożliwiać zautomatyzowaną (poprzez integrację z IaaS) realizację zaplanowanych do świadczenia Usług biznesowych (opisanych w rozdziale 2) i stanowić spójny system dostarczający niezbędne zasoby i usługi na potrzeby **Centrum Głównego** oraz **Centrum Zapasowego:**

- łącza internetowe i usługi brzegu sieci, w tym:
  - terminacja ruchu L1-L3,
  - usługa firewall, IPS, ochrony przed DDoS,
  - usługi węzła IX (SIX - Szczecin Internet eXchange point),
- połączenia sieciowe i dedykowane sieci na potrzeby wszystkich węzłów sieci,
- usługi VPN na potrzeby zarządzania i zdalnego dostępu do infrastruktury,
- usługi VPN w formie VPN as a Service (VPNaaS),
- usługi Firewall na potrzeby brzegu sieci,
- usługi Firewall as a Service (FWaaS),
- usług Load Balancing (LB), w tym usług Load Balancing as a Service (LBaaS),
- zasoby powierzchni dyskowej udostępnianej w postaci rozproszonego systemu składowania danych oraz macierzy (z uwzględnieniem backupu danych i replikacji),
- zasoby mocy obliczeniowej udostępnianej w postaci węzłów obliczeniowych.

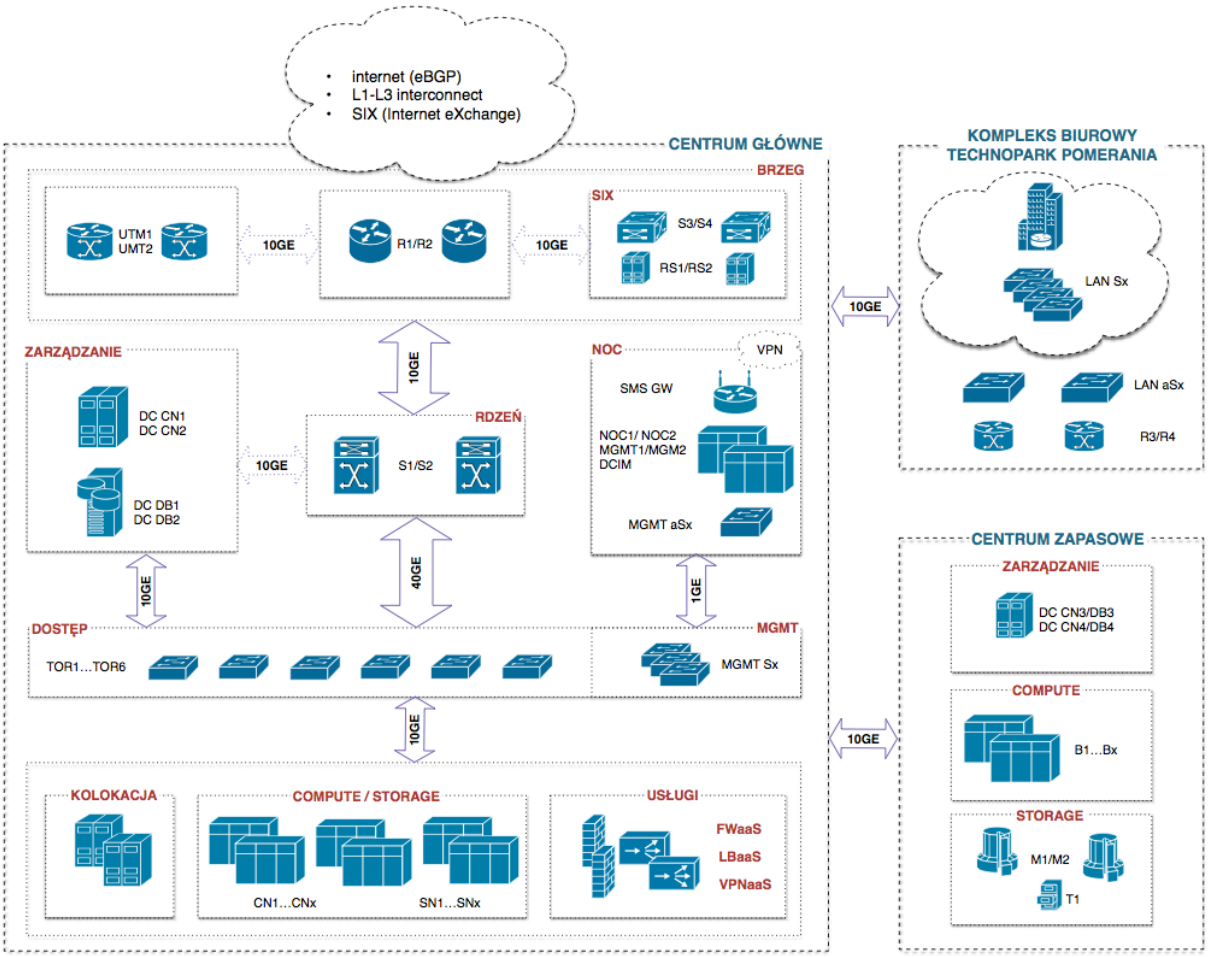
W ramach niniejszego postępowania powinna również zostać zaprojektowana, dostarczona, wdrożona, a następnie utrzymywana i serwisowana infrastruktura zapewniająca obsługę sieciową **kompleksu biurowego Technoparku Pomerania** składającego się z 4 budynków. W ramach tej infrastruktury należy:

- zapewnić agregację ruchu L2 poprzez dostawę switchy dostępowych i switchy agregujących oraz urządzeń WiFi,
- poprzez wykorzystanie urządzeń pracujących na brzegu sieci w Centrum Głównym zapewnić:
    - dostęp do Internetu,
    - usługę routingu i terminacji IP (w tym w szczególności NAT),
    - usługę firewall oraz ochronę przed atakami (IPS),
    - usługę QoS i kontroli ruchu sieciowego.

Całość dostarczanej infrastruktury powinna być zarządzana oraz monitorowana przez spójny system NOC (Network Operating Center) oraz sieć MGMT.

4.1.1. Architektura rozwiązania

Poniżej przedstawione zostały założenia do infrastruktury technicznej projektu C4C - schemat blokowy oraz opis urządzeń i rozwiązań technicznych w ramach poszczególnych warstw sieci i bloków funkcjonalnych.
Określone w ramach niniejszego rozdziału założenia (o ile nie są wskazane wprost jako wymagania w ramach OPZ) powinny stanowić przedmiot uszczegółowienia w ramach analizy i przygotowania projektu technicznego na podstawie ogólnie pojętych najlepszych praktyk i w drodze ustaleń z Zamawiającym. Pod względem jakościowym opisane poniżej założenia należy traktować jako minimalne.



Rys. 1. Architektura logiczna infrastruktury

4.1.2. Opis poszczególnych komponentów infrastruktury

4.1.2.1. Brzeg sieci

W zaplanowanej architekturze brzeg sieci stanowi ogólnie pojęty punkt styku z sieciami zewnętrznymi (w tym ogólnie pojętą siecią Internet) dla:

- obu Centrów Danych (Głównego i Zapasowego),
- kompleksu biurowego SPNT.

Integralną częścią brzegu sieci jest zespół switchy i serwerów przeznaczonych na potrzeby węzła Szczecin Internet eXchange point (tzw. SIX) oraz usług związanych z połączeniami interconnectowymi:

- połączenia z ISP,
- połączenia z innymi punktami IX w PL,
- połączenia miejską siecią metropolitalną, w tym siecią Urzędu Miasta,
- łącza światłowodowe i L2 do szpitali.

W ramach brzegu sieci może nastąpić konieczność terminacji kilku usług lub sieci zewnętrznych na jednym porcie L1.

Brzeg sieci w niniejszej architekturze należy traktować również jako dostawcę połączeń interconnectowych (L1-L3) na potrzeby usług realizowanych w ramach centrów danych i kompleksu biurowego.

Na brzegu sieci zaplanowano dwa routery (**R1/R2**) klasy operatorskiej, wyposażone w porty 10GE oraz 1GE. Najważniejszą funkcją tych urządzeń jest utrzymanie wielu sesji eBGP sieciami zewnętrznymi, w tym dostawcami łącz internetowych. Routery powinny pracować w pełnej redundancji HA (active/active) oraz powinny zostać wyposażone w redundantne zasilacze, zespoły chłodzące (wentylatory) i karty zarządzające. Pod względem funkcjonalnym urządzenia te powinny zapewniać routing IP zarówno z pozostałej części sieci jak i do niej.

W ramach brzegu sieci zaplanowany został również punkt wymiany ruchu IX (**SIX, Szczecin Internet eXchange)**, opierający się o dedykowaną infrastrukturę w postaci planowanych do zakupu w ramach niniejszego postępowania route serwerów **RS1/RS2** oraz dedykowanych switchy **S3/S4** istniejących już w obecnej infrastrukturze Zamawiającego. Switche **S3/S4** są również planowane jako główny brzeg całej sieci w warstwie L1/L2 - czyli porty bezpośredniego styku z sieciami zewnętrznymi (styki międzyoperatorskie, klienci, infrastruktura wyniesiona itp.), umożliwiające m. in. multiplikację pojedynczych łącz i połączeń na potrzeby redundantnych routerów brzegowych lub szkieletowych. Na etapie projektu technicznego należy podjąć decyzję czy na potrzeby w/w opisanych bezpośrednich styków należy również wykorzystać inne urządzenia w infrastrukturze.

W ramach uruchamiania systemu urządzeń stanowiących “Brzeg sieci” obowiązkiem Wykonawcy jest również konfiguracja i uruchomienie węzła SIX (Szczecin Internet eXchange) poprzez konfigurację istniejących switchy **S3/S4** oraz route serwerów **RS1/RS2**.

W ramach proponowanej architektury na brzegu sieci zaplanowane zostało włączenie dwóch dedykowanych urządzeń typu UTM (**UTM1/UTM2**), pracujących w trybie pełnej redundancji. Urządzenia te powinny zapewnić dostarczenie usług w postaci:

- firewall,
- system wykrywania włamań i kontroli aplikacji,
- zaawansowane wykrywanie zagrożeń z zastosowaniem analizy behawioralnej,
- terminacji IP dla kompleksu SPNT (m. in. NAT, firewall, IPS, tc, qos),
- ochrona przed atakami DDoS.

Zamawiający dopuszcza zrealizowanie usługi ochrony przed DDoS w formie odrębnego urządzenia, jeżeli architektura wdrażanych rozwiązań sprzętowych tego wymaga.

Zależnie od wybranego przez dostawcę podejścia do projektu sieci urządzenia UTM mogą również dostarczać usługi FWaaS oraz VPNaaS, przy czym preferowane przez Zamawiającego jest

wykorzystanie do tego celu instancji wirtualnych zintegrowanych z IaaS lub samej funkcjonalności IaaS (uszczegółowienie tego zagadnienia znajduje się w rozdziale **Usługi**).

4.1.2.2. Rdzeń sieci, dostęp i kolokacja

Głównym elementem sprzętowym rdzenia sieci są switche **S1/S2**, które pełnią rolę zarówno agregatora połączeń z warstwy dostępowej, jak również dostarczają magistralę dla połączeń pomiędzy wszystkimi blokami funkcjonalnymi i kluczowymi węzłami sieci. Switche te zostały zaplanowane do pracy w pełnej redundancji HA (active/active) i dla umożliwienia skutecznego zarządzania powinny być widziane przez system zarządzania jako pojedyncze urządzenie.

Istotną kwestią jest, aby switch rdzeniowy umożliwiał spójną współpracę ze switchami lub modułami switchującymi typu "top-of-rack" (dedykowanymi do poszczególnych szaf, m. in. na potrzeby kolokacji) poprzez:

- możliwość bezpośredniego przyłączenia takiego modułu do matrycy przełączającej switcha lub
- wykorzystanie podwójnych linków o przepływności min. 40GE.

Zakłada się, że obsługa zmultiplikowanych połączeń z sieci dostępowej powinna odbywać się bez konieczności stosowania protokołu STP lub podobnych rozwiązań. Ponieważ zespół switchy **S1/S2** jest kluczowym elementem całej architektury, urządzenia te powinny zostać wyposażone w redundantne zasilacze, zespoły chłodzące (wentylatory) i karty zarządzające. Dopuszczalne i rekomendowane są również urządzenia i rozwiązania umożliwiające zamykanie ruchu wschód-zachód w obrębie zespołu switchy TOR, bez pośrednictwa switchy szkieletowych.

Usługa kolokacji to z punktu widzenia doboru urządzeń sieciowych tzw. switche typu *top-of-rack* przeznaczone na potrzeby podłączania urządzeń (routery, półki blade itp) umieszczonych w innych szafach niż szafa w której zamontowany jest switch rdzeniowy.

4.1.2.3. Usługi

FWaaS (Firewall as a Service) - usługa powinna umożliwiać m. in. tworzenie i przeglądanie dedykowanych reguł firewall dla sieci najemców (tenants). Na potrzeby tej usługi dopuszcza się wykorzystanie zarówno rozwiązań opartych o maszyny wirtualne uruchamiane na compute node'ach jak również wykorzystanie integracji z urządzeniami UTM. W obu przypadkach należy zapewnić integrację z IaaS.
VPNaaS (Virtual Private Network as a Service) - usługa powinna umożliwiać tworzenie m. in. prywatnych sieci typu site-to-site VPN oraz zapewniać bezpieczny dostęp do sieci najemców (tenants) przez uprawnionych użytkowników. Na potrzeby realizacji tej usługi zalecane jest wykorzystanie funkcjonalności systemu IaaS (z wykorzystaniem zasobów compute nodes) ale dopuszczalne jest

również wykorzystanie urządzeń typu UTM. W obu przypadkach wymagana jest pełna integracja z Podsystemem IaaS.

LBaaS (Load Balancer as a Service) - w grupie węzłów sieciowych "usługi" zaplanowane zostały również urządzenia lub instancje wirtualne typu "load balancer" (**LB1/LB2**), gwarantujące zarządzanie ruchem na poziomie warstwy L3 modelu OSI i wyżej. W ramach niniejszego postępowania dopuszcza się wdrożenie zarówno rozwiązań opartych o dedykowany sprzęt jak również takich, które oparte są o rozwiązania software'owe - zwirtualizowane rozwiązania uruchomione na serwerach typu compute node (tzw. virtual appliances). Preferowane jest rozwiązanie, w którym urządzenia typu LB zostaną umieszczone na infrastrukturze wirtualizacyjnej (jako maszyny wirtualne), dzięki czemu zmniejszona zostanie różnorodność infrastruktury sprzętowej. Bez względu na fakt, czy LB1/LB2 będą stanowić dedykowane urządzenia, czy też zostaną uruchomione jako wirtualne instancje na serwerach typu compute node, w obu przypadkach zakłada się, iż urządzenia te będą wyposażone w interfejsy 10GE, przyłączone bezpośrednio do switcha rdzeniowego (lub ewentualnie poprzez switch typu TOR - zależnie od projektu technicznego).

Inżynieria ruchu w sieci powinna zostać zaplanowana w taki sposób, aby możliwe było dowolne sterowanie ruchem i kierowanie go zarówno przez urządzenia typu LB jak i z ich pominięciem. Wymagane jest również, aby obsługa zarządzania urządzeniami lub instancjami LB powinna być realizowana przez funkcjonalność urządzenia, instancji wirtualnej lub dostarczony system zarządzania - w każdym przypadku zintegrowany z IaaS.

4.1.2.4. Compute nodes i distrubuted storage nodes

Warstwa compute i storage stanowi główny moduł produkcyjny w ramach Centrum Danych, dlatego też została zaplanowana w postaci wielu spójnych pod względem cech serwerów dedykowanych jako:

- zasoby przetwarzania danych - "compute nodes" (**CN1, CN2 ... CNx)**
  oraz
- serwerów typu "storage node" **(SN1, SN2 … SNx)** wyposażonych w dyski i stanowiących rozproszony (distributed) storage stanowiący podstawę dla dostępu obiektowego i blokowego do danych,
- serwerów przeznaczonych na potrzeby zarządzania infrastrukturą,

W ramach postępowania zaplanowane do zakupu zostało kilkadziesiąt serwerów bądź modułów serwerowych, wyposażonych w min. 2 porty światłowodowe o przepływności 10GE każdy oraz dwa porty miedziane o przepływności 1GE każdy. Agregacja ruchu sieciowego z tych urządzeń powinna odbywać się w obrębie warstwy dostępowej na switchach typu top-of-rack (TOR) za pośrednictwem portów 10GE oraz 1GE. Na potrzeby zarządzania urządzenia te powinny zostać podłączone do sieci MGMT poprzez dedykowane porty oraz switche umieszczone w szafach rack.

W ramach projektu technicznego oczekiwane jest opracowanie podziału węzłów na węzły typu CN oraz SN w taki sposób, aby zasoby były wykorzystane optymalnie pod względem mocy obliczeniowej i

powierzchni oraz wykorzystania energii elektrycznej. Dopuszcza się łączenie węzłów CN oraz SN w obrębie jednego serwera fizycznego.

4.1.2.5. Serwery zarządzające i monitorujące

DC Control nodes

Serwery dedykowane na potrzeby kontroli warstwy IaaS - tzw. "DC control nodes" (**DC CN1 / DC CN2**) są zaplanowane jako niezależne moduły serwerowe zapewniające również obsługę z odpowiednią wydajnością baz danych (**DC DB1 / DC DB2**). Zakłada się sprzętową zgodność interoperacyjną z rozwiązaniem serwerowym dobranym na potrzeby serwerów typu CN/SN. W ramach realizowanej architektury odrębne serwery DC control nodes (**DC CN3/DB3** oraz **DC CN4/DB4** zostały przewidziane na potrzeby Centrum Zapasowego.

Zakłada się, że oba zestawy Control Nodes będą pracować w trybie redundantnym HA (active/active).

Zakłada się, iż ilość fizycznych maszyn niezbędnych na potrzeby DC control nodes zostanie dobrana na etapie projektu technicznego pod względem wymagań wdrażanego Podsystemu IaaS. Maszyny te powinny być wydzielone z infrastruktury produkcyjnej i w przypadku wirtualizacji zasobów działać niezależnie.

NOC, MGMT, DCIM

Dla instalacji Podsystemów oprogramowania wspierających NOC, przeznaczonych do monitoringu, systemów zarządzania i DCIM zaplanowano dedykowane serwery, analogicznie jak w przypadku rozwiązań DC control nodes - również zgodne pod względem interoperacyjnym z rozwiązaniami sprzętowymi dobranymi w ramach CN/SN - **NOC1 / NOC2, MGMT1 / MGMT2, DCIM**).

Uzupełnieniem urządzeń w ramach infrastruktury NOC jest urządzenie w postaci bramki SMS dające możliwość wysyłania powiadomień SMS niezależnie od stanu łącz dostępowych na brzegu sieci.

W celu optymalizacji w/w zasobów serwerowych dopuszcza się uruchomienie na nich systemu wirtualizacji, przy założeniu, że kluczowe Podsystemy będą pracować na odrębnych maszynach fizycznych w trybie redundantnym HA (active/active). Uruchomiony na potrzeby NOC/MGMT/DCIM system wirtualizacji nie może być częścią tego samego systemu co część produkcyjna IaaS.

Zakłada się, iż ilość fizycznych maszyn niezbędnych na potrzeby NOC, MGMT, DCIM zostanie dobrana na etapie projektu technicznego pod względem wymagań wdrażanych na nich Podsystemów oprogramowania. Maszyny te powinny być wydzielone z infrastruktury produkcyjnej i w przypadku wirtualizacji zasobów działać niezależnie.

SIX Route Servers (RS)

Na potrzeby obsługi sesji BGP w ramach węzła SIX (i planowanego połączenia z innymi centrami wymiany ruchu w Polsce) zaplanowano dedykowane serwery - analogicznie jak w przypadku rozwiązań DC control nodes - również zgodne pod względem interoperacyjnym z rozwiązaniami sprzętowymi dobranymi w ramach CN/SN - **RS1/RS2**.

Zadaniem RS1/RS2 jest utrzymywanie sesji BGP w ramach połączeń węzła Szczecin Internet eXchange. Łącznie zaplanowano 2 serwery.

4.1.2.6. Sieć MGMT

Z punktu widzenia wydzielonej sieci zarządzania (sieć MGMT) zaplanowano:

- switche **MGMT Sx** agregujące ruch z dedykowanych portów zarządzania urządzeń z poszczególnych szaf,
- switch (**MGMT aS**) umożliwiający połączenie serwerów MGMT / NOC / DCIM do sieci MGMT i agregację ruchu ze switchy **MGMT Sx**.

Na etapie projektu technicznego infrastruktury należy poddać analizie następujące kwestie:

- stworzenie niezależnego (od łączy operatorskich w ramach brzegu sieci) dostępu do sieci na potrzeby awaryjnego zarządzania poprzez wykorzystanie funkcji routera i dostępu do Internetu z wykorzystaniem sieci GSM w zaplanowanej do zakupu bramce SMS,
- stworzenie dodatkowego routera w oparciu o rozwiązania software'owe (serwer wirtualny, dystrybucja linux) wraz z niezależnym systemem VPN (rekomendowany jest OpenVPN), którego dodatkowym zadaniem będzie zapewnienie routingu pomiędzy poszczególnymi podsieciami MGMT oraz kontrolowanie dostępu.

4.1.2.7. Centrum Zapasowe

Rolę Centrum Zapasowego powinna przejąć dotychczasowa serwerownia SPNT umiejscowiona w budynku F1 przy ul. Niemierzyńskiej. Centrum Zapasowe należy zintegrować z głównym Centrum Głównym poprzez jego konfigurację jako odrębny region w infrastrukturze IaaS. W celu umożliwienia takiej integracji infrastruktura Centrum Zapasowego zostanie w ramach niniejszego postępowania wzbogacona o dedykowane węzły typu control nodes.

Aktualnie Centrum Zapasowe jest wyposażone w następującą infrastrukturę:

- compute: serwery IBM typu blade (**B1...Bx**) w obudowie rack 19U, na potrzeby środowiska wirtualizacyjnego,
- storage: macierz IBM (**M1**) obsadzona dyskami SAS, SATA, biblioteka taśmowa oraz serwery backupu z wbudowaną przestrzenią dyskową (w ramach niniejszego postępowania środowisko storage zostanie rozbudowane o dodatkową macierz, a istniejąca macierz zostanie rozbudowana o dodatkową przestrzeń).
- sieć: zbudowana na przełącznikach 1Gbps i 10Gbps, z wykorzystaniem łączenia portów w grupy i zachowaniem redundancji połączeń.

W ramach projektu technicznego całej infrastruktury należy uwzględnić integrację zasobów Centrum Zapasowego i zaplanować oraz wdrożyć taką konfigurację, aby przynajmniej dwa serwery blade

będące aktualnie na wyposażeniu Centrum Zapasowego pracowały jako część infrastruktury IaaS budowanej w ramach niniejszego postępowania. Integracja powinna również gwarantować możliwość korzystania z zasobów macierzy podłączonej do półki blade poprzez wykorzystanie iSCSI lub poprzez przekształcenie serwerów blade w storage nodes i wykorzystanie dzięki temu istniejącego połączenia fiber channel.

W ramach projektu technicznego należy również przedstawić konkretne wytyczne i plan działania w kontekście wykorzystania Centrum Zapasowego (aktualnie wskazanego lub też innego) w scenariuszach umożliwiających późniejsze rozszerzenie infrastruktury poza Szczecin, np.

- Disaster Recovery Center – zapasowe centrum komputerowo-biurowe data center, które przejmuje funkcje środowiska produkcyjnego w razie nieoczekiwanych wydarzeń i związanych z nimi przerw w działalności systemów informatycznych,
- skalowanie mocy obliczeniowej i powierzchni do innych centrów danych.

Proponowane w ramach projektu technicznego scenariusze powinny zostać przetestowane w ramach wdrożenia i będą przedmiotem scenariuszy testowych, a w konsekwencji prac odbiorowych.

4.1.2.8. Backup

Pod względem zasobów rozwiązanie backup zostało zaplanowane do realizacji poprzez:

- uzupełnienie zasobów istniejącej macierzy (**M1**) o dodatkowe dyski (łącznie około 52TB),
- dostawę, instalację i konfigurację macierzy (**M2**) (analogicznej do istniejącej) stanowiącej uzupełnienie istniejącej infrastruktury i umożliwiającej mirroring istniejącej macierzy (około 200TB)
- odpowiednią konfigurację rozproszonego systemu storage (około 800TB).

Na etapie projektu technicznego i szczegółowego planowana sposobu realizacji kopii zapasowych należy podjąć decyzję o fizycznym rozmieszczeniu macierzy dyskowych (określenie, która macierz znajdzie się w którym centrum danych).

W ramach realizowanego Projektu zaplanowano realizację backupów poprzez odpowiednie przechowywanie wzajemnych kopii zapasowych pomiędzy Centrum Głównym i Centrum Zapasowym na dostępnych systemach przechowywania danych:

- macierze (**M1, M2**),
- storage nodes (**SN1..SNx**).

Uzupełnieniem infrastruktury systemu backupów jest posiadana aktualnie przez Zamawiającego biblioteka taśmowa (**T1**).

4.1.3. Integracja z IaaS

Część infrastruktury zaangażowana w świadczenie Usług opartych o IaaS oraz PaaS powinna zostać zintegrowana w sposób umożliwiający pełną automatyzację alokacji, konfiguracji i skalowania jej zasobów. Do przykładowych usług realizowanych w ramach integracji z IaaS:

- automatyczny provisioning serwerów wirtualnych, serwerów cloud, serwerów VPS oraz dedykowanych wraz z niezbędnymi zasobami sieciowymi,
- tworzenie sieci wewnętrznej i dedykowanej na potrzeby zwirtualizowanej infrastruktury klienta,
- udostępnianie dedykowanego połączenia VPN dla zasobów udostępnionych klientowi w ramach usług (VPNaaS),
- możliwość tworzenia dedykowanych reguł firewall (FWaaS),
- automatyczne przyznawanie publicznej i niepublicznej adresacji IP (dla standardu IPv6 i IPv4),
- automatyczna konfiguracja usług load balancingu (LBaaS), w tym terminacji SSL,
- automatyczna konfiguracja mechanizmu IP failover,
- automatyczne przyznawanie zasobów w ramach storage blokowego i obiektowego.

Zakłada się, iż w ramach Projektu integracja z IaaS powinna:

- zostać przeprowadzona zgodnie z wytycznymi i dobrymi praktykami wynikającymi z wybranego rozwiązania IaaS,
- wykorzystywać moduły programistyczne dostarczone przez wybrane rozwiązanie IaaS,
- w przypadku urządzeń sieciowych stanowić integrację w oparciu o udokumentowane API lub otwarty (posiadający status open source) standard komunikacji, np. OpenFlow, OpenContrail itp. (dla SDN) lub alternatywne, otwarte mechanizmy: XMPP, XML, RADIUS itp,
- wykorzystywać mechanizmy wirtualizacji zasobów infrastruktury wbudowane w sprzęt,

W ramach integracji infrastruktury sieciowej z rozwiązaniem IaaS wskazane jest podejście wykorzystujące wytyczne wynikające z podejścia SDN (Software-Defined Networking). Mimo, iż pojęcie SDN nie zostało na obecnym etapie ustandaryzowane to każdy z wiodących dostawców sprzętu sieciowego udostępnia wytyczne dotyczące preferowanych modeli wdrożeniowych pozostających w zgodzie z technologią SDN. W ramach niniejszego postępowania wymagane jest aby:

- w ramach doboru producentów sprzętu preferować rozwiązania wspierające technologię SDN,
- stosować model integracji, który dany producent wskazuje jako zgodny z technologią SDN i wybranym systemem IaaS,
- w miarę możliwości separować płaszczyznę kontrolną (control plane) od płaszczyzny danych (data plane) oraz dostarczać interfejsy i API pozwalające na scentralizowane zarządzanie siecią, zamiast konfigurowania poszczególnych, rozproszonych urządzeń.

Nie jest dopuszczalna integracja infrastruktury z IaaS polegająca na wprowadzaniu zmian w konfiguracji urządzeń poprzez wykorzystanie tych samych interfejsów lub systemów, jakie są przeznaczone do wprowadzania zmian przez człowieka, takich jak: CLI (np. ssh, telnet) lub dedykowane dla konfiguracji manualnej systemy zarządzania. Nie jest również dopuszczalna

integracja na potrzeby konfiguracji infrastruktury oparta o protokół SNMP (wskazane jest wykorzystanie tego protokołu w trybie tylko do odczytu na potrzeby monitoringu i ewidencji).

4.1.4. Kompleks biurowy Technoparku Pomerania

4.1.4.1. Sieć LAN i dostęp do Internetu

Klientem sieci brzegowej Centrum Danych są rezydenci (firmy i pracownicy) kompleksu biurowego Technoparku Pomerania. Dostęp do Internetu, wraz z usługami dodatkowymi terminacji IP (w tym NAT) dla tych klientów jest realizowany poprzez usługi brzegu sieci (urządzenia UTM1/UTM2). Agregacja połączeń z biur będzie terminowana na switchach dostępowych **LAN Sx** i powinna zostać zrealizowana poprzez dwa dedykowane switche agregujące **LAN aSx.** Switche LAN Sx będą instalowane w budynkowych punktach dystrybucyjnych BPD-0 (3 szt.), BPD-1 (2 szt.), BPD-2 (3 szt.) oraz w piętrowych punktach dystrybucyjnych PPD 1-1 (2 szt.), PPD 1-2 (2 szt.), PPD 1-3 (2 szt.), PPD 2-1 (3 szt.), PPD 2-2 (3 szt.), PPD 2-3 (4 szt.). W każdym punkcie należy zainstalować po 1 szt. switcha dostępowego z obsługą Power over Ethernet. Switche zainstalowane w każdym punkcie mają być skonfigurowane w ramach jednego wirtualnego przełącznika. Z każdego punktu do switchy agregujących LAN **aSx** mają być zestawione dwa połączenia 10 GE (po jednym do switcha agregującego). Switche agregujące powinny być połączone w ring, oraz każdy ma być połączony z brzegiem sieci linkami 10GE.

W ramach przygotowywania projektu technicznego i wdrożenia urządzeń w sieci LAN w kompleksie biurowym Technoparku Pomerania należy dążyć do rozwiązania działającego bez konieczności wykorzystywania technologii Spanning Tree (STP) i pokrewnych. Wybór podejścia pozwalającego na uniknięcie wykorzystania rozwiązań STP powinien być dobrany w sposób zgodny z możliwościami wdrażanego sprzętu i powinien zapewniać analogiczny poziom niezawodności poprzez obsługę redundantnych połączeń.

4.1.4.2. Sieć Wi-Fi

W ramach sieci Wi-Fi Zamawiający wykorzysta posiadane dwa kontrolery Ruckus ZoneDirector 3000. W ramach rozbudowy do kontrolerów wymagany jest zakup dwóch pakietów licencji do obsługi 50 szt. AP.
Sieć Wi-Fi zaprojektowana w nowo wybudowanych budynkach przewiduje instalacje po 3 szt. AP na piętro:

- w budynku Inkubator Przedsiębiorczości: 12 szt,
- Centrum Innowacji: 12 szt,
- Cenrum Komputerowe: 9 szt,
- w budynku szkoleniowym przewiduje się instalację 10 szt.

Łącznie Zamawiający przewiduje zakup 43 szt. AP. Każdy AP będzie włączony w switch dostępowy z obsługą POE (Power over Ethernet).

4.1.5. Podsystemy oprogramowania na potrzeby NOC

Na potrzeby obsługi i monitoringu infrastruktury w ramach Centrum Zarządzania Siecią (NOC – Network Operation Control) zaplanowano wdrożenie trzech Podsystemów oprogramowania.

4.1.5.1. NOC: Monitoring i Centralny system logów

Uszczegółowienie wymagań dotyczących Podsystemu do monitoringu "NOC: Monitoring" oraz uzupełniającego jego funkcjonalność Podsystemu "Centralny system logów" znajduje się w rozdziale 5. Podsystem do monitoringu powinien charakteryzować się dużą elastycznością związaną z koniecznością wdrożenia tego rozwiązania zarówno na potrzeby monitoringu infrastruktury jak również wszystkich Podsystemów oprogramowania. Przykładem jednego z rozwiązań spełniającego taki wymóg jest system Zabbix. Uzupełnieniem Podsystemu monitoringu jest zintegrowany z nim Centralny system logów, umożliwiający m. in. wykrywanie krytycznych zdarzeń na podstawie odpowiednio zdefiniowanych reguł. Współpraca centralnego systemu logów z NOC jest tylko jednym z zadań tego Podsystemu.

4.1.5.2. NOC: Podsystem zarządzania

Przez Podsystem zarządzania rozumiany jest zbiór systemów oprogramowania umożliwiający manualną lub półautomatyczną konfigurację infrastruktury. Zakłada się, iż Podsystem zarządzania będzie opierał się o systemy oprogramowania dostarczone przez producentów poszczególnych rozwiązań sprzętowych. W ramach niniejszego postępowania zakłada się niezależność dostarczonych systemów zarządzania, jednak na poziomie dostępu, uprawnień oraz śledzenia zmian i backupu konfiguracji będzie konieczne wykonanie szeregu integracji umożliwiających spójne wykorzystywanie systemu zarządzania. Zakłada się, iż NOC: Podsystem zarządzania będą operować w ramach sieci MGMT a ich bezpośrednimi użytkownikami są administratorzy i inżynierowie sieci.

W kontekście integracji infrastruktury z Podsystemem IaaS (w ramach usług biznesowych) na potrzeby automatyzacji, przydzielania i konfigurowania zasobów sieciowych, compute i storage nie dopuszcza się wykorzystania dedykowanych (dostarczonych przez producentów) systemów zarządzania do tego celu. Uszczegółowienie wymagań dotyczących systemu zarządzania znajduje się w rozdziale 5.

4.1.5.3. NOC: DCIM

Podsystem DCIM to uzupełnienie (poprzez integrację) Podsystemu monitoringu o informacje związane z infrastrukturą pasywną, m. in. monitoring temperatury, otwarcia szaf, rozmieszczenia urządzeń. Ze względu na umiarkowaną skalę Projektu w ramach niniejszego postępowania zakłada się wdrożenie oprogramowania, które będzie umożliwiało stopniowe skalowanie i uproszczoną integrację. Uszczegółowienie wymagań dotyczących Podsystemu DCIM znajduje się w rozdziale 5. Przykładem jednego z rozwiązań spełniających te wymagania jest system OpenDCIM. W kontekście DCIM należy analizować wyłącznie założenia dla infrastruktury pasywnej (bez odniesień do koncepcji technicznej dla urządzeń aktywnych).

4.1.6. Infrastruktura pasywna

Istniejąca infrastruktura pasywna Zamawiającego opiera się o następujące rozwiązania:

4.1.6.1. Infrastruktura szaf rack

W pomieszczeniach serwerowni przewiduje się instalację szaf serwerowych jednokomorowych o wysokości 47U i podstawie 60 cm (szerokość) × 120 cm (głębokość).
Instalowane będą dwa typy szaf:

- Szafy typu 11 umożliwiające zainstalowanie w nich urządzeń o całkowitej mocy elektrycznej do 11 kVA.
- Szafy typu 22 umożliwiające zainstalowanie w nich urządzeń o całkowitej mocy elektrycznej do 22 kVA.

W szafach typu 11 i 22 zainstalowane zostaną panele 48×RJ-45/8×MRJ-21/STP/1U/S, na których zakończonych zostanie odpowiednio osiem lub cztery kable teleinformatyczne STP 25-parowe 2×MRJ-21 1000Base-T. Kable w układzie dwóch redundantnych gałęzi A/B doprowadzone zostaną do szaf serwerowych z serwerowego punktu dystrybucyjnego SPD.
W szafach typu 22 instalowane zostaną dodatkowo panele na 3 kasety MPO wyposażone w dwie kasety MPO/LC na 12 włókien OS2, na których zakończone zostaną dwa 12-włóknowe jednomodowe kable światłowodowe OS2 z wtykami MPO. Kable w układzie dwóch redundantnych gałęzi A/B doprowadzone zostaną do szaf serwerowych z serwerowego punktu dystrybucyjnego SPD.

Dodatkowo w pomieszczeniach serwerowni przewiduje się instalację szaf serwerowych wielokomorowych o wysokości 47U i podstawie 60 cm (szerokość) × 120 cm (głębokość).
Instalowane będą dwa typy szaf:

- Szafy typu 15-2 podzielone na dwie komory kolokacyjne.
- Szafy typu 15-4 podzielone na cztery komory kolokacyjne.

Oba typy szaf umożliwią zainstalowanie w nich urządzeń o całkowitej mocy elektrycznej do 15 kVA. Każda komora kolokacyjna wyposażona zostanie w drzwi chronione zamkiem na klucz. W każdej komorze szaf typu 15-4 zainstalowany zostanie jeden, a każdej komorze szaf 15-2 – dwa panele na 3 kasety MRJ-21 każdy wyposażony w dwie kasety 6×RJ45/MRJ21/STP, na których zakończone zostaną

kable teleinformatyczne STP 25-parowe 2×MRJ-21 1000Base-T. Kable w układzie dwóch redundantnych gałęzi A/B doprowadzone zostaną z serwerowego punktu dystrybucyjnego SPD.

W pierwszym etapie obiekt zostanie wyposażony w 20 szaf serwerowych.

Szczegółowy opis infrastruktury pasywnej znajduje się w dokumentacji projektowej dostępnej pod adresem: http://www.technopark-pomerania.pl/download_file/1610/1103/, która jest przedmiotem realizacji projektu „Budowa i wyposażenie I etapu Pomerania Technopark w Szczecinie przy ul. Niemierzyńskiej/Cyfrowej, kontynuacja inwestycji". Wymienione w dokumentacji urządzenia aktywne mają tylko i wyłącznie charakter poglądowy.
W ramach niniejszego postępowania, Zamawiający rozbudowuje istniejącą infrastrukturę o 4 szafy serwerowe DK TS8, zgodnie z wymaganiami szczegółowo opisanymi w rozdziale 4.3.19.

4.1.6.2. Chłodzenie

Do chłodzenia szaf serwerowych zastosowany zostanie wysokowydajny system LCP - Liquid Cooling Package firmy Rittal. Jest to wymiennik ciepła powietrze / woda, łączony szeregowo z szafami serwerowymi. Moduły LCP mogą być instalowane w zależności od zapotrzebowania na moc chłodniczą w wersji 1 moduł LCP na dwie szafy z mocą chłodnicza dla każdej szafy 12kW lub w przypadku urządzeń generujących znaczne ilości ciepła 1 moduł LCP na jedną szafę serwerową dając moc chłodniczą 24kW. System na starcie będzie wyposażony w 2 agregaty wody lodowej oraz w 12 modułów LCP.
Szczegółowy opis infrastruktury chłodzenia znajduje się w dokumentacji projektowej dostępnej pod linkiem: http://www.technopark-pomerania.pl/download_file/1622/1103/, która jest przedmiotem realizacji projektu „Budowa i wyposażenie I etapu Pomerania Technopark w Szczecinie przy ul. Niemierzyńskiej/Cyfrowej, kontynuacja inwestycji".
W ramach niniejszego postępowania, Zamawiający rozbudowuje istniejącą infrastrukturę o 2 moduły LCP T3+ EC 47U 3300235, dla chłodzenia szaf serwerowych, zgodnie z wymaganiami szczegółowo opisanymi w rozdziale 4.3.20.

4.2. Zestawienie ilościowe

Lp.	Nazwa urządzenia	Symbol	Ilość
1	Router brzegowy	R1/R2	2
2	Switch szkieletowy	S1/S2	2
3	Switch top of rack	TOR1...TOR6	6
4	Firewall/UTM	UTM1/UTM2	2
5	Load balancers	LB1/LB2	2
6	Serwery: compute nodes i distributed storage nodes	CN1...CNx SN1...SNx	64

	Serwery: zarządzające i monitorujące	NOC1/NOC2, MGMT1/MGMT2, DCIM, DC DB1/DC DB2, DC CN3/DB3DC CN4/DB4, RS1/RS2	
7	Macierz	M2	1
8	Rozbudowa macierzy	M1	1
9	Switch MGMT	MGMT Sx	6
10	Switch MGMT - agregacja	MGMT aSx	1
11	Switch dostępowy (kompleks biurowy Technoparku Pomerania)	LAN Sx	15
12	Switche dostępowy POE (kompleks biurowy Technoparku Pomerania)	LAN Sx	9
13	Switch agregujący (kompleks biurowy Technoparku Pomerania)	LAN aSx	2
14	Rozszerzenia licencji kontrolerów Wi-Fi (kompleks biurowy Technoparku Pomerania)	LAN WiFi	2
15	Punkty dostępowe (AP) (kompleks biurowy Technoparku Pomerania)	LAN AP	43
16	Konwertery, moduły (transceivers): 10GE, 40GE, 1GE	TRANS	zgodnie z projektem technicznym
17	Bramka SMS	SMS GW	1
18	Szafy serwerowe	-	4
19	Moduły chłodzące	-	2

4.3. Wymagania szczegółowe dla infrastruktury

4.3.1. Wymagania wspólne

ID wymagania	Treść wymagania
INF.WW.1	Zaprojektowana infrastruktura musi spełniać założenia opisane w rozdziale 4.1 gwarantując spełnienie wymogów jakościowych.
INF.WW.2	Zaprojektowana infrastruktura musi umożliwiać realizację celów biznesowych opisanych w rozdziale 2.
INF.WW.3	Zaprojektowana infrastruktura powinna być dobrana w sposób minimalizujący zużycie energii.
INF.WW.4	Zaprojektowana i wdrożona infrastruktura powinna zapewniać niezbędne zasoby na potrzeby wszystkich Podsystemów oprogramowania dostarczanych w ramach Projektu
INF.WW.5	Należy minimalizować ilość producentów sprzętu dobieranego w ramach infrastruktury i dążyć do jak największej jego jednorodności.
INF.WW.6	Wsparcie dla standardu IPv6 powinno być zapewnione na poziomie sprzętu i firmware na etapie realizacji Projektu
INF.WW.7	Obsługa standardu IPv6 powinna być realizowana w trybie "dual stack" (równocześnie).

INF.WW.8	Obsługa standardu IPv6 powinna być zapewniona na poziomie sieci brzegowej, szkieletowej, dostępowej i MGMT.
INF.WW.9	W odniesieniu do wymagań opisanych w OPZ oprogramowanie dostarczane w ramach infrastruktury musi być w pełni funkcjonalne i nie powinno posiadać żadnych ograniczeń licencyjnych w zakresie opisanych w OPZ wymagań dotyczących infrastruktury.
INF.WW.10	Wszystkie urządzenia w ramach dostarczonej i zintegrowanej infrastruktury powinny podlegać monitoringowi w ramach Podsystemu NOC: Monitoring, ewidencji w ramach Podsystemu DCIM oraz zarządzaniu w ramach Podsystemu NOC: Podsystem zarządzania.
INF.WW.11	Wszystkie urządzenia w ramach dostarczonej i zintegrowanej infrastruktury powinny wysyłać logi do Centralnego systemu logów.
INF.WW.12	Dostarczone w ramach infrastruktury urządzenia muszą pochodzić z oficjalnego kanału dystrybucji w Polsce.
INF.WW.13	W ramach infrastruktury nie może być pojedynczych punktów awarii poza elementami oznaczonymi jako "MGMT aSx" oraz "SMS GW".
INF.WW.14	Infrastruktura powinna zapewniać liniową skalowalność.
INF.WW.15	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać uniezależnienie od producentów rozwiązań sprzętowych.
INF.WW.16	Integracja infrastruktury z Podsystemem IaaS powinna zostać zrealizowana poprzez dedykowane moduły Podsystemu IaaS przeznaczone do obsługi poszczególnych zasobów infrastruktury, takich jak: sieć, powierzchnia dyskowa, moc obliczeniowa i pamięć RAM.
INF.WW.17	Integracja infrastruktury z Podsystemem IaaS powinna zostać zrealizowana w zgodzie z wytycznymi producenta Podsystemu lub społeczności open source związanej z danym rozwiązaniem oraz w zgodnie z dobrymi praktykami przyjętymi w ramach takiej integracji.
INF.WW.18	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczną konfigurację, alokację i skalowanie zasobów infrastruktury niezbędnych do realizacji usług dostarczanych w ramach IaaS oraz PaaS.
INF.WW.19	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyzację provisioningu nowych zasobów serwerowych.
INF.WW.20	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać skalowalność przestrzeni dyskowej do PB (Peta Bajtów) i więcej.
INF.WW.21	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać rozproszony (distributed) storage stanowiący podstawę dla dostępu obiektowego i blokowego do danych.
INF.WW.22	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczny provisioning serwerów wirtualnych, serwerów cloud, serwerów VPS, oraz dedykowanych.
INF.WW.23	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczne przyznawanie zasobów w ramach storage blokowego i obiektowego.
INF.WW.24	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczne tworzenie sieci wewnętrznej na potrzeby zwirtualizowanej infrastruktury Klienta.
INF.WW.25	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczne udostępnianie dedykowanego połączenia VPN do sieci i zasobów udostępnionych klientowi w ramach Usług.
INF.WW.26	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać możliwość

	automatycznej konfiguracji kierowania ruchu sieciowego usług Klienta przez lub z pominięciem usługi ochrony przed atakami.
INF.WW.27	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczne przyznawanie publicznej i niepublicznej adresacji IP (dla standardu IPv6 i IPv4). W przypadku standardu IPv6 funkcjonalność ta powinna być zapewniona na etapie realizacji Projektu.
INF.WW.28	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczną konfigurację usług load balancingu, w tym terminacji SSL.
INF.WW.29	Integracja infrastruktury z Podsystemem IaaS powinna zapewniać automatyczną konfigurację mechanizmu IP failover.
INF.WW.30	Wykonawca powinien dostarczyć sprzęt wraz z niezbędnym okablowaniem, dokumentacją techniczno- eksploatacyjną, certyfikatami bezpieczeństwa oraz dokumentami potwierdzającymi udzielenie Zamawiającemu gwarancji na te urządzenia.
INF.WW.31	W celu potwierdzenia, że oferowany sprzęt odpowiada wymaganiom określonym przez Zamawiającego, Wykonawca zobowiązany jest dołączyć do oferty dokumenty zawierające opis urządzeń wchodzących w skład przedmiotu zamówienia, a w szczególności dokumentacji technicznej, specyfikacji technicznej, itp., dla każdego zaoferowanego urządzenia czy oprogramowania, potwierdzającego spełnianie wymagań zamawiającego. Załączone dokumenty muszą wskazywać rzeczywiste parametry zaoferowanych urządzeń. Zamawiający wyraża zgodę, aby załączone do oferty dokumenty zostały złożone w języku angielskim.

4.3.2. Routery brzegowe

ID wymagania	**Treść wymagania**
INF.RB.1	Router brzegowy klasy operatorskiej.
INF.RB.2	Obudowa dedykowana do montażu w szafie typu rack 19''.
INF.RB.3	Architektura modularna, pozwalająca na instalację modułów w postaci: - kart liniowych, - sprzętowych redundantnych modułów zarządzających, - modułów medium transmisyjnego (transreceiverów).
INF.RB.4	Architektura wewnętrzna zapewniająca odseparowanie funkcji kontrolnych (control plane) takich jak routing, sygnalizacja, zarządzanie od obsługi ruchu użytkowego (data plane).
INF.RB.5	Rozbudowa urządzenia o dodatkowe karty interfejsów powinna odbywać się bez konieczności instalacji dodatkowej matrycy przełączającej oraz konieczności wymiany modułów zarządzających i przy zachowaniu wszystkich wymogów funkcjonalnych i wydajnościowych zawartych w niniejszej specyfikacji.
INF.RB.6	Wsparcie dla HA poprzez obsługę przełączania kart procesorowych w tryb active/active.
INF.RB.7	Minimum 4 sloty na karty liniowe (nie uwzględniając procesorowych).
INF.RB.8	Wymagana obsługa prędkości portów w urządzeniu: 10Mbps/100Mbps/1Gbps/10Gbps.
INF.RB.9	Ilość pamięci operacyjnej w kartach procesorowych: minimalnie 4GB.
INF.RB.10	Urządzenie wyposażone w następującą ilość portów światłowodowych (minimum):

	8x10Gbps i 20x1Gbps, porty muszą mieć możliwość obsługi diagnostyki modułów optycznych dostarczonych w ramach projektu; porty muszą mieć możliwość obsługi modułów światłowodowych innych producentów niż producent urządzenia z zachowaniem gwarancji na sprzęt.
INF.RB.11	Urządzenie wyposażone w min 2 zasilacze AC umożliwiające pracę urządzenia w pełnej konfiguracji (tzn. przy obsadzeniu modułami wszystkich slotów urządzenia).
INF.RB.12	Urządzenie wyposażone w min 2 karty procesorowe.
INF.RB.13	Wydajność matrycy przełączającej: minimum 75Gbps.
INF.RB.14	Wydajność przełączania pakietów: minimum 50Mpps.
INF.RB.15	Sprzętowe wsparcie dla pełnego routingu IPv4/IPv6, co najmniej: static, OSPF, IS-IS, BGP.
INF.RB.16	Wielkość tablic w sprzętowej tablicy przełączania FIB dla IPv4/IPv6: min. 1 miliona dla IPv4 i 256 tysięcy dla IPv6; podane parametry powinny być spełnione dla każdego protokołu niezależnie, również przy jednoczesnym wykorzystaniu obu protokołów; wielkość tablic RIB powinna wynosić min 2x wielkość tablic FIB dla poszczególnych protokołów.
INF.RB.17	BFD musi być obsługiwane dla IPv4/IPv6
INF.RB.18	Sprzętowa realizacja przełączania przełącznika.
INF.RB.19	Wsparcie dla MTU 9216 bajtów.
INF.RB.20	Obsługa sieci VLAN zgodna z IEEE 802.1q dla 4094 sieci VLAN jednocześnie; obsługa dowolnej translacji identyfikatorów VLAN, również w przypadku zastosowania mechanizmu Q-in-Q.
INF.RB.21	Obsługa Spanning Tree 802.1d, 802.1w, 802.1s, ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone także przy użyciu MPLS/VLPS.
INF.RB.22	Obsługa sprzętowego eksportu statystyk ruchu (eksport danych do kolektora flow); dla łącza o przepływności 1Gbps - bez próbkowania (samplingu), dla ruchu powyżej 1Gbps - możliwe wykorzystanie próbkowania (samplingu).
INF.RB.23	Wsparcie dla: PBR, VRRP.
INF.RB.24	Obsługa standardów: L2 VPN, L3 VPN, MPLS VPN, MPLS, MPLS TE, VPLS lub równoważnych.
INF.RB.25	Obsługa standardów: kolejkowanie na portach: min 8 kolejki na port, limitowanie ruchu ingress/egreess na portach/vlanach, shaping lub policing ruchu per port.
INF.RB.26	Obsługa mechanizmów kolejkowania ruchu, jego filtrowania oraz znakowania w oparciu o 802.1p, DSCP, ToS, MPLS EXP na wszystkich portach oraz dla poszczególnych sieci VLAN.
INF.RB.27	Obsługa SNMP v1/v2/v3 (informacje o MIB, np. specyfikacje OID, muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.RB.28	Obsługa oraz integracja z sieciami SDN, przynajmniej poprzez otwarty protokół.
INF.RB.29	Obsługa RADIUS/TACACS/TACACS+

4.3.3. Switche szkieletowe

ID wymagania	**Treść wymagania**
INF.SS.1	Switch szkieletowy klasy operatorskiej.
INF.SS.2	Obudowa dedykowana do montażu w szafie typu rack 19''.

INF.SS.3	Zasilanie prądem przemiennym 230V AC, wyposażone w minimum dwa redundantne zasilacze.
INF.SS.4	Architektura modularna.
INF.SS.5	Regulacja prędkości wentylatorów w zależności od temperatury wewnątrz obudowy.
INF.SS.6	Minimum 4 GB pamięci RAM.
INF.SS.7	Min. 8 slotów do obsługi kart liniowych.
INF.SS.8	Min. ilość obsługiwanych portów : 40x 1Gbps, 40x 10 Gbps, 24x 40Gbps; architektura urządzenia gotowa na obsługę min. 2x100Gbps.
INF.SS.9	Min. ilość portów zainstalowanych: 16x 40Gbps, 24x 10Gbps, 16x 1Gbps.
INF.SS.10	Redundantna praca zasilaczy - awaria jednego modułu nie może wpłynąć na pracę switcha w pełnej konfiguracji wymiana w trybie HotSwap - bez konieczności wyłączania Systemu.
INF.SS.11	Możliwość redundancji kart procesorowych - praca w trybie active/active i active/standby.
INF.SS.12	Przepustowość matrycy przełączającej min. 5 Tb/s.
INF.SS.13	Przepustowość kart liniowych min. 100 Gb/s na slot.
INF.SS.14	Sprzętowa obsługa ilości tras IPv4/IPv6: min. 128 000 dla IPv4 i 64 000 dla IPv6; podane parametry powinny być spełnione dla każdego protokołu niezależnie, również przy jednoczesnym wykorzystaniu obu protokołów.
INF.SS.15	Wszystkie porty obsługiwane z pełną prędkością łącza (wire speed).
INF.SS.16	Sprzętowa realizacja modułu przełączania.
INF.SS.17	Obsługa nie mniej niż 100 tysięcy adresów MAC na każdą kartę liniową lub nie mniej niż 1 mln. na cały przełącznik.
INF.SS.18	Obsługa ramek Jumbo (min. MTU 9000 bajtów).
INF.SS.19	Obsługa sieci VLAN zgodna z IEEE 802.1q dla 4000 sieci VLAN jednocześnie oraz Q-in-Q, możliwa dowolna translacja vlanów.
INF.SS.20	Obsługa standardu 802.3ad.
INF.SS.21	Obsługa Spanning Tree 802.1d, 802.1w, 802.1s, ramki BPDU pomiędzy sieciami VLAN muszą być przenoszone także przy użyciu MPLS/VLPS.
INF.SS.22	Sprzętowa obsługa QoS ingress/egress, możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.
INF.SS.23	Sprzętowa realizacja routingu.
INF.SS.24	Obsługiwane protokoły routingu IPv4: static, RIP, OSPF, IS-IS, BGP.
INF.SS.25	Obsługiwane protokoły routingu IPv6: static, RIP, OSPF, IS-IS, BGP.
INF.SS.26	Obsługa mechanizmu BFD.
INF.SS.27	Wymagana możliwość stworzenia klastra VRRP.
INF.SS.28	Reguły ACL w oparciu o kryteria warstw 2-4 dla ingress i egress.
INF.SS.29	Obsługa SNMP v1/v2/v3 (informacje o MIB, np. specyfikacje OID, muszą być dostępne dla Zamawiającego), CLI (minimum ssh/telnet), syslog, NTP.
INF.SS.30	Obsługa oraz integracja z sieciami SDN, integracja poprzez otwarty protokół.
INF.SS.31	Obsługa RADIUS/TACACS/TACACS+

4.3.4.Switch top of rack

ID wymagania	Treść wymagania
INF.ST.1	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.ST.2	Minimum dwa wewnętrzne zasilacze 230V AC, z redundancją zasilania.
INF.ST.3	Wyposażony w następującą ilość portów (z obsługą diagnostyki modułów): min. 40 portów 10Gbps (z czego przynajmniej 20 musi mieć obsługę modułów 1Gbps i 10Gbps zamiennie), oraz minimum 4 porty 40Gbps.
INF.ST.4	Tablica adresów MAC: min. 100000 pozycji.
INF.ST.5	Urządzenie musi się charakteryzować wydajnością "wire speed" dla funkcji przełącznika, wydajność: min. 500Gbs, przepustowość: min. 500Mpps.
INF.ST.6	Możliwość wsparcia dla pełnego routingu IPv4/IPv6, co najmniej: static, OSPF, IS-IS, BGP.
INF.ST.7	Wsparcie dla multicast routing, PIM-SM, PIM-DM.
INF.ST.8	Obsługa VRRP.
INF.ST.9	Obsługa PBR, IPv6 tunneling, BFD.
INF.ST.10	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, DHCP Snooping Trust.
INF.ST.11	Obsługa IGMP v1/v2/v3.
INF.ST.12	Obsługa 4094 jednoczesnych VLAN, translacji VLAN.
INF.ST.13	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.ST.14	Obsługa DCBX, 802.1Qbb, IEEE 802.1Qaz.
INF.ST.15	Obsługa 802.3ad.
INF.ST.16	Kontrola mac adresów w poszczególnych VLANACH.
INF.ST.17	Wsparcie dla MTU 9000 bajtów.
INF.ST.18	Możliwość obsługi BFD dla RIP, OSPF, BGP, IS-IS, VRRP, MPLS.
INF.ST.19	Funkcjonalność przełączania pakietów non-STP, zgodność z protokołem IETF TRILL lub równoważnym.
INF.ST.20	Wielkość tablic w sprzętowej tablicy przełączania FIB dla IPv4/IPv6: min. 16000 dla IPv4 i 8000 dla IPv6; podane parametry powinny być spełnione dla każdego protokołu niezależnie, również przy jednoczesnym wykorzystaniu obu protokołów.
INF.ST.21	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.
INF.ST.22	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS.
INF.ST.23	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.ST.24	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół.
INF.ST.25	Obsługa RADIUS/TACACS/TACACS+
INF.ST.26	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.ST.27	Dedykowany port do zarządzania RJ-45.

4.3.5. Firewall/UTM

ID wymagania	Treść wymagania
INF.FW.1	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U.
INF.FW.2	Obsługa portów 1Gbps i 10Gbps, urządzenie musi posiadać minimum 2 porty 10Gbps i 16 portów 1Gbps.
INF.FW.3	Zasilanie 230V AC z możliwością wymiany w czasie pracy urządzenia (tzw. hot-swap); urządzenie musi być wyposażone w minimum dwa zasilacze AC.
INF.FW.4	Minimum 3Mpps dla pakietów 64 bajtów.
INF.FW.5	Minimum 2mln jednoczesnych połączeń/sekundę.
INF.FW.6	Minimum 5Gbps dla ruchu szyfrowanego VPN.
INF.FW.7	Minimum 2Gbps dla ruchu IPS.
INF.FW.8	Sprzętowe wsparcie dla pełnego routingu IPv4/IPv6, co najmniej: static,OSPF, IS-IS, BGP.
INF.FW.9	Obsługa minimum 500 sesji BGP.
INF.FW.10	Obsługa mechanizmów QOS (policing, kolejkowanie, shaping), obsługa DSCP, IP ToS, 802.1p, WRED, obsługa tworzenia osobnych kolejek dla różnych klas ruchu.
INF.FW.11	Ochrona przed atakami DoS/DDoS realizowana sprzętowo o wydajności min. 5Gbps. Dopuszcza się realizację tego wymagania poprzez wdrożenie dedykowanego (niezależnego od UTM) urządzenia lub systemu (również działającego w trybie redundancji).
INF.FW.12	Urządzenie musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, intrusion prevention) wspomaganą sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane w atakach na sieć. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywać się w regułach polityki bezpieczeństwa. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall.
INF.FW.13	Obsługa statefull firewall dla pakietów o wielkości 64 bajty z wydajnością nie mniejszą niż 10Gbps.
INF.FW.14	System zabezpieczeń musi identyfikować próby skanowania, penetracji, włamań, ataki typu exploit, ataki destrukcyjne i destabilizujące.
INF.FW.15	Obsługa pracy w trybie HA Active-Active, tak by przełączanie pomiędzy urządzeniami odbywało się przezroczyście dla ruchu użytkowników; mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych.
INF.FW.16	Wsparcie dla VPN-IPSEC.
INF.FW.17	Obsługa IPv4, IPv6.
INF.FW.18	Obsługa SNMP v1/v2/v3 (informacje o MIB, np. specyfikacje OID, muszą być dostępne dla zamawiającego), CLI (minimum ssh/telnet), syslog, NTP.
INF.FW.19	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.

4.3.6. Load balancers

ID wymagania	Treść wymagania
INF.LB.1	Musi być urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U lub oprogramowaniem dedykowanym do wirtualizacji i przystosowanym do uruchomienia w ramach infrastruktury IaaS.
INF.LB.2	W przypadku urządzenia dedykowanego: powinno być wyposażone w porty minimum 2x 10Gbps oraz minimum 2x 1Gbps.
INF.LB.3	Minimalnie 8GB RAM.
INF.LB.4	Minimum dwa wewnętrzne zasilacze 230V AC, z redundancja zasilania.
INF.LB.5	Minimum 250GB pojemności dysku twardego.
INF.LB.6	Wsparcie load balancing dla: TCP, UDP, HTTP, HTTPS.
INF.LB.7	Minimum 2Gbps dla ruchu L4/L7.
INF.LB.8	Minimum 4 miliony jednoczesnych połączeń L4.
INF.LB.9	Zapewnienie dowolnej liczby sesji load balance na poziomie TCP, UDP, HTTP, HTTPS.
INF.LB.10	Obsługa algorytmów load balance: round robin, wagowany round robin, random losowy, najmniejsza liczba połączeń, wagowany.
INF.LB.11	Obsługa zarządzania sesją użytkownika przez adres źródłowy lub HTTP Cookie.
INF.LB.12	Obsługa zarządzania LB wraz z opcjami automatycznego podłączenia/odłączenia load balancowanych nodów powinna być realizowana przez funkcjonalność urządzenia, instancji wirtualnej lub dostarczony system zarządzania - w każdym przypadku wymagana jest integracja z IaaS.
INF.LB.13	Obsługa terminacji SSL dla One-Way SSL i Two-Way SSL.
INF.LB.14	Obsługa certyfikatów SSL dowolnego dostawcy.
INF.LB.15	Zarządzanie nagłówkami HTTP przekazywanymi do node'ów (w tym nagłówkami z polami certyfikatów SSL).
INF.LB.16	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.LB.17	Monitoring urządzenia powinien być realizowany przez dedykowane Podsystemy monitoringu Centrum Danych (np. za pomocą SNMP).

4.3.7. Serwery

ID wymagania	Treść wymagania
INF.CN.1	Architektura serwerowa, zalecany jest dobór serwerów typu "high density servers" z grupowaniem serwerów per obudowa ze wspólnym zasilaniem w celu optymalizacji zużycia energii elektrycznej.
INF.CN.2	Minimum 6 dysków hot-swap z obsługą SAS/NL-SAS/SATA/SSD dla pojedynczego node serwera.
INF.CN.3	2 porty USB.
INF.CN.4	1 port VGA.
INF.CN.5	1 slot PCI-E.
INF.CN.6	Redundantne zasilanie (per obudowa) 230V AC.

INF.CN.7	Zainstalowane 2 porty 10Gbps, wspierające sprzętowo: - 802.1q VLAN - TCP segmentation offload - IPv6 obsługa dla IP/TCP i IP/UDP receive checksum offload - wsparcie dla wirtualizacji oraz obsługa ramek jumbo o rozmiarze min.9000 bajtów.
INF.CN.8	Zainstalowane 2 porty 1Gbps miedziane.
INF.CN.9	Zainstalowany 1 port dedykowany na zarządzanie.
INF.CN.10	Zainstalowane minimum 64GB RAM 1866Mhz ECC Registered, obsługa maksimum 256GB 1866Mhz ECC Registered w jednym serwerze, sumaryczna ilość pamięci RAM w całym środowisku nie może być mniejsza niż: 3840GB.
INF.CN.11	Minimum 16 rdzeni procesora na serwer (nie uwzględniając wielowątkowości procesora, tzw. HT), taktowanie: min. 2.5Ghz na rdzeń.
INF.CN.12	Minimum 20MB last level cache per processor.
INF.CN.13	Obsługa QPI do 8GT/s.
INF.CN.14	Oferowany model procesora musi osiągać w teście CINT2006 (parametr SPECint_rate2006) wynik bazowy minimum 680 pkt. w konfiguracji minimum 2 procesory/16 rdzeni (tj. 8 rdzeni na procesor) (wynik zaproponowanego procesora musi znajdować się na stronie http://www.spec.org/cpu2006/results/rint2006.html w dniu składania ofert. Wydruk ze strony załączyć do oferty).
INF.CN.15	Ewentualna rozbudowa o dodatkowy procesor lub inny osprzęt musi odbywać się bez dodatkowych licencji.
INF.CN.16	Wsparcie dla procesora do wirtualizacji.
INF.CN.17	Minimum 46TB pojemności dysków enterprise SATA SSD (pojemność RAW, sumarycznie na wszystkich serwerach) oraz minimum 768TB pojemności dysków SATA enterprise (pojemność RAW, sumarycznie na wszystkich serwerach); rozmieszczenie położenia dysków w poszczególnych obudowach powinno zostać dobrane na etapie projektu technicznego z uwzględnieniem wybranego podejścia do rozproszonego storage; przykładowy podział: 48 serwerów w obudowach po 8 sztuk każda, wyposażonych w 2x 480GB SSD każdy oraz 16 serwerów wyposażonych w 16x 3TB SATA każdy. MTBF dla każdego z dysków zastosowanych w serwerach minimum 1.4 miliona godzin dla enterprise SATA i minimum 2 miliony godzin dla enterprise SATA SSD. Dla dysków SSD parametr TBW (Total Bytes Written) powinien wynosić min. 270TB (w rozumieniu standardów JESD218 oraz JESD 219).
INF.CN.18	Wyposażony w sprzętowy kontroler dysków z minimum 1GB pamięci, obsługujący dyski SAS, NL-SAS, SATA, SSD z obsługą RAID przynajmniej poziom 0, 1, 10, 5.
INF.CN.19	Obsługa dysków SAS/SATA/SSD dowolnego producenta, w tym możliwość użycia dysków tzw. OEM (niekoniecznie dedykowanych/markowych); wykorzystanie dysków OEM nie powinno zmniejszać programowo lub licencyjnie wydajności/przepustowości Systemu oraz nie powinno powodować utraty gwarancji.
INF.CN.20	Zarządzanie urządzeniami poprzez IPMI (Intelligent Platform Management Interface), zgodność z IPMI 2.0, KVM over LAN / KVM over IP.
INF.CN.21	Obsługa IPv4, IPv6.
INF.CN.22	Zarządzanie po dedykowanym, wbudowanym porcie Ethernet.
INF.CN.23	Obsługa interfejsu WWW dla zarządzania.

INF.CN.24	Zarządzanie serwerem przy wyłączonej maszynie, możliwe uruchomienie zdalne systemu, restart, wyłączenie, włączenie, możliwość montowania obrazu oraz instalacji systemu operacyjnego za pomocą interfejsu zarządzania.

4.3.8.Macierz

ID wymagania	Treść wymagania
INF.M2.1	Uzupełnienie istniejącej infrastruktury IBM w postaci macierzy IBM V3700 z 4 modułami rozszerzeń.
INF.M2.2	Modułowa do instalacji w standardowej szafie Rack 19”.
INF.M2.3	Dwa redundantne kontrolery udostępniające w sumie nie mniej niż 8 połączeń FC 8Gb i 4 połączenia iSCSI minimum 1Gb. RAID 0,1,5,6,10. Wymagane jest, aby architektura wewnętrzna macierzy wykorzystywała standard SAS 2.0.
INF.M2.4	Co najmniej 16GB pamięci „cache”. Pamięć „cache” przeznaczona dla procesu zapisu musi być zabezpieczona przed skutkami awarii jednego z kontrolerów.
INF.M2.5	Macierz musi obsługiwać dyski SSD (o pojemnościach 200GB i 400GB), SAS (o pojemnościach 146GB, 300GB, 600GB, 900GB) i NL-SAS lub SATA (o pojemnościach 500GB, 1TB, 2TB, 4TB) pozwalając na rozbudowę do co najmniej 120 dysków. Macierz musi obsługiwać dyski 2,5” i 3,5”. Macierz musi umożliwiać mieszanie dysków SAS, NL-SAS i SSD w ramach jednej półki dyskowej. Dostawa ma obejmować 48 dysków SATA każdy o pojemności 4TB oraz 24 dysków SSD każdy o pojemności 400GB.
INF.M2.6	Macierz musi mieć możliwość wykonywania migracji woluminów w ramach zasobów dyskowych bez zatrzymywania aplikacji z nich korzystających. Macierz musi posiadać możliwość migracji danych z zewnętrznych zasobów dyskowych.
INF.M2.7	Macierz musi obsługiwać min 50 kopii migawkowych na macierz. Licencja na tę funkcjonalność musi być zawarta w cenie. Kopie danych typu „snapshot„ muszą być wykonywane przez macierz jako pojedyncza operacja w co najmniej trzech możliwych trybach: • kopia pełna, • kopia wskaźnikowa, • przyrostowa kopia pełna. Macierz musi mieć możliwość odtworzenia zawartości woluminu logicznego z kopii typu „snapshot” bez konieczności kopiowania danych za pośrednictwem serwera.
INF.M2.8	Funkcjonalność konfigurowania woluminu dyskowego posiadającego dwie kopie fizyczne na różnych grupach dyskowych i różnego typu (np.: jedna kopia z nadalokacją druga bez). W przypadku zapisu macierz zapisuje do obu kopii synchronicznie. W przypadku odczytu czyta tylko z jednej kopii. Kiedy jedna kopia jest niedostępna macierz automatycznie korzysta tylko z dostępnej kopii a po naprawie brakującej kopii automatycznie synchronizuje dane. Wolumin mirrorowany może być przekształcony w zwykły wolumin poprzez usunięcie jednej kopii albo poprzez wyodrębnienie jednej kopii w osobny wolumin.
INF.M2.9	Funkcjonalność dynamicznej alokacji przestrzeni dyskowej większej niż jest dostępna fizycznie oraz możliwość wyłączenia tej funkcjonalności dla wybranych woluminów.

INF.M2.10	Wszystkie krytyczne komponenty takie jak: kontrolery dyskowe, pamięć „cache”, zasilacze i wentylatory muszą być zdublowane w taki sposób, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego Systemu. Brak pojedynczego punktu awarii. Wszelkie połączenia pomiędzy elementami składowymi macierzy (wszystkie ścieżki) muszą być redundantne. Wsparcie dla zasilania z dwóch niezależnych źródeł prądu poprzez nadmiarowe zasilacze typu „hot-swap”. Wentylatory typu „hot-swap”.
INF.M2.11	Interfejs zarządzający GUI, CLI nie wymagający instalacji dodatkowego oprogramowania na stacji zarządzającej. Możliwość zmiany mikrokodu bez przerywania dostępu do danych. Monitorowanie stanu pracy za pośrednictwem protokołu SNMP. Automatyzacja procesu informacji o stanie urządzenia, w tym informacji o awariach za pomocą wiadomości przesyłanych drogą elektroniczną.
INF.M2.12	Komplet wkładek FC, okablowanie zasilające, światłowodowe FC

4.3.9. Rozbudowa macierzy

ID wymagania	Treść wymagania
INF.M1.1	Dwa redundantne kontrolery udostępniające w sumie nie mniej niż 8 połączeń FC 8Gb i 2 połączenia iSCSI minimum 10Gb. RAID 0,1,5,6,10. Wymagane jest, aby architektura wewnętrzna macierzy wykorzystywała standard SAS 2.0. Rozbudowana macierz nie powinna posiadać programowych ograniczeń wydajności.
INF.M1.2	Należy doposażyć istniejącą macierz IBM V3700 poprzez rozbudowę dwóch istniejących redundantnych kontrolerów, o dodatkowe 8GB RAM cache każdy.
INF.M1.3	Obudowa modułowa do instalacji w standardowej szafie Rack 19”.
INF.M1.4	Rozbudowana macierz musi obsługiwać dyski SSD (o pojemnościach 200GB i 400GB, 800GB), SAS (o pojemnościach 146GB, 300GB, 600GB, 900GB i 1,2 TB) i NL-SAS lub SATA (o pojemnościach 500GB, 1TB, 2TB, 4TB) pozwalając na rozbudowę do co najmniej 120 dysków. Macierz musi obsługiwać dyski 2,5” i 3,5”. Macierz musi umożliwiać mieszanie dysków SAS, NL-SAS i SSD w ramach jednej półki dyskowej. Dostawa macierzy musi obejmować minimum 9TB SSD pojemności RAW oraz minimum 43TB SAS pojemności RAW.
INF.M1.5	Należy dostarczyć komplet wkładek FC, okablowanie zasilające, światłowodowe FC.

4.3.10. Switche MGMT

ID wymagania	Treść wymagania
INF.SM.1	Switch klasy operatorskiej; min. ilość urządzeń tych urządzeń powinna być zgodna z zestawieniem ilościowym; w przypadku gdy projekt techniczny wykaże większe zapotrzebowanie należy dostarczyć ilość zgodną z projektem technicznym.
INF.SM.2	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.SM.3	Minimum dwa wewnętrzne zasilacze AC, z redundancją zasilania.
INF.SM.4	Wyposażony w następującą ilość portów: min. 48 portów 10/100/1000Mbps , oraz

	minimum 4 porty 1Gbps.
INF.SM.5	Wielkość tablicy mac-adresów minimum 12000 pozycji.
INF.SM.6	Urządzenie musi być wire speed dla funkcji przełącznika, wydajność minimum 50Gbs, przepustowość minimum 50Mpps.
INF.SM.7	Obsługa IPv4/IPv6.
INF.SM.8	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, Dhcp Snooping Trust.
INF.SM.9	Obsługa 4000 jednoczesnych VLAN, translacji VLAN.
INF.SM.10	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.SM.11	Obsługa 802.3ad.
INF.SM.12	Kontrola MAC adresów w poszczególnych VLANACH, obsługa wykrywania pętli tzw. loop detection.
INF.SM.13	Wsparcie dla MTU 9000 bajtów.
INF.SM.14	Tablica routingu minimum 4000 wpisów dla IPv4 oraz 1000 wpisów dla IPv6.
INF.SM.15	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL
INF.SM.16	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS;
INF.SM.17	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring
INF.SM.18	Możliwość wyboru sposobu obsługi kolejek – Strict Priority; Weighted Round Robin;
INF.SM.19	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp
INF.SM.20	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół
INF.SM.21	Obsługa RADIUS/TACACS/TACACS+
INF.SM.22	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.SM.23	Dedykowany port do zarządzania RJ-45

4.3.11. Switche MGMT – agregacja

ID wymagania	**Treść wymagania**
INF.SMA.1	Switch klasy operatorskiej.
INF.SMA.2	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.SMA.3	Minimum dwa wewnętrzne zasilacze AC, z redundancją zasilania.
INF.SMA.4	Wyposażony w następującą ilość portów: min. 20 portów 1Gbps.
INF.SMA.5	Wielkość tablicy MAC adresów minimum 12000 pozycji.
INF.SMA.6	Urządzenie musi być wire speed dla funkcji przełącznika, wydajność minimum 20Gbs, przepustowość minimum 20Mpps.
INF.SMA.7	Obsługa IPv4/IPv6.
INF.SMA.8	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, Dhcp Snooping Trust.
INF.SMA.9	Obsługa 4000 jednoczesnych VLAN, translacji VLAN.
INF.SMA.10	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.SMA.11	Obsługa 802.3ad.

INF.SMA.12	Kontrola MAC adresów w poszczególnych VLANACH, obsługa wykrywania pętli tzw. loop detection.
INF.SMA.13	Wsparcie dla MTU 9000 bajtów.
INF.SMA.14	Tablica routingu minimum 4000 wpisów dla IPv4 oraz 1000 wpisów dla IPv6.
INF.SMA.15	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.
INF.SMA.16	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS.
INF.SMA.17	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring.
INF.SMA.18	Możliwość wyboru sposobu obsługi kolejek – Strict Priority; Weighted Round Robin.
INF.SMA.19	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.SMA.20	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół.
INF.SMA.21	Obsługa RADIUS/TACACS/TACACS+
INF.SMA.22	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.SMA.23	Dedykowany port do zarządzania RJ-45.

4.3.12. Konwertery, moduły (transceivers)

ID wymagania	Treść wymagania
INF. TRANS.1	Konwertery powinny poprawnie współpracować z portami sieciowymi do których zostaną podłączone. W przypadku konwerterów optycznych należy zależnie od wykorzystanych połączeń światłowodowych dobrać odpowiedni rodzaj (single/multi mode), moc optyczną (LX, SX, ZX) i jeżeli jest taka potrzeba wprowadzić tłumiki optyczne.
INF. TRANS.2	Ilość i rodzaj konwerterów powinny zostać dobrane w trakcie przygotowywania projektu technicznego w taki sposób aby: - spełniać założone wymogi przepływnościowe pomiędzy węzłami i warstwami sieci, - gwarantować zachowanie wymogów dostępności i redundancji, - zapewnić połączenia do istniejącej infrastruktury. Do ilości wynikającej z projektu technicznego należy doliczyć 5% każdego rodzaju konwertera.
INF. TRANS.3	Producent dostarczonych urządzeń musi dopuszczać możliwość wykorzystania modułów SFP/SFP+/QSFP/QSFP+/XFP pochodzących od innych producentów, tzn. obsługę modułów typu OEM bez utraty gwarancji czy supportu dla urządzenia.
INF. TRANS.4	Dostarczone moduły optyczne muszą wspierać diagnostykę DDM (Digital Diagnostic Monitor) lub równoważną , tzn. monitorować kluczowe parametry pracy modułu takich jak moc optyczna sygnału nadawanego, moc optyczna sygnału odbieranego, temperatura pracy, napięcie zasilania, prąd lasera i w tym zakresie funkcjonalnym muszą poprawnie współpracować z urządzeniami wyposażonymi w te moduły.

4.3.13. Bramka SMS

ID wymagania	Treść wymagania

INF.BS.1	Dedykowane urządzenie do komunikacji GSM do wysyłania wiadomości SMS.
INF.BS.2	Obsługa minimum dwóch kart SIM różnych operatorów działających na terenie Polski. Brak blokady sim-lock.
INF.BS.3	Obsługa komunikatów SMS.
INF.BS.4	Wyposażona w port minimum 2x 10/100 Mbps.
INF.BS.5	Możliwość zasilania 230V AC i/lub DC z funkcją podtrzymania bateryjnego.
INF.BS.6	Obsługa IPv4/IPv6.
INF.BS.7	Obsługa NAT oraz VPN (przynajmniej PPTP) lub równoważne.
INF.BS.8	Obsługa logowania wysłanych wiadomości SMS.
INF.BS.9	Obsługa funkcji routera przez dostęp do Internetu z sieci GSM, w celu awaryjnego dostępu do sieci.
INF.BS.10	Możliwość integracji z systemem monitoringu poprzez API (automatyzacja wysyłania komunikatów) przez dedykowany port komunikacyjny.
INF.BS.11	Dedykowany port do zarządzania.
INF.BS.12	Monitoring stanu kart SIM GSM.

4.3.14. Kompleks biurowy SPNT: switche dostępowe

ID wymagania	**Treść wymagania**
INF.SD.1	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.SD.2	Minimum dwa wewnętrzne zasilacze AC, z redundancją zasilania.
INF.SD.3	Wyposażony w następującą ilość portów: min. 48 portów 10/100/1000Mbps , oraz minimum 2 porty 10Gbps.
INF.SD.4	Możliwość zbudowania jednego wirtualnego przełącznika z 4 przełączników tego samego typu tzw. funkcja stackowania; przełącznik wirtualny powinien być widziany przez inne urządzenia sieciowe jako pojedyncze urządzenie zarówno pod kątem mechanizmów warstwy L2 jak i warstwy L3; do podłączenia przełączników jako przełącznik wirtualny, musi być wykorzystany dedykowany port, połączenie przez dedykowany port musi być połączeniem w ringu, aby zminimalizować awarie w trakcie uszkodzenia kabla/przełącznika; przepustowość portu dedykowanego do połączenia między poszczególnymi urządzeniami musi być minimum 10Gbps.
INF.SD.5	Wielkość tablicy MAC adresów minimum 12000 pozycji.
INF.SD.6	Urządzenie musi być wire speed dla funkcji przełącznika, wydajność minimum 100Gbs, przepustowość minimum 100Mpps.
INF.SD.7	Obsługa IPv4/IPv6.
INF.SD.8	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, Dhcp Snooping Trust.
INF.SD.9	Obsługa IGMP v1/v2/v3.
INF.SD.10	Obsługa 4000 jednoczesnych VLAN, translacji VLAN.
INF.SD.11	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.SD.12	Obsługa 802.1x, 802.3ad.

INF.SD.13	Kontrola MAC adresów w poszczególnych VLANACH, obsługa wykrywania pętli tzw. loop detection.
INF.SD.14	Wsparcie dla MTU 9000 bajtów.
INF.SD.15	Tablica routingu minimum 4000 wpisów dla IPv4 oraz 1000 wpisów dla IPv6.
INF.SD.16	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.
INF.SD.17	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS.
INF.SD.18	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring.
INF.SD.19	Możliwość wyboru sposobu obsługi kolejek – Strict Priority; Weighted Round Robin.
INF.SD.20	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.SD.21	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół.
INF.SD.22	Obsługa RADIUS/TACACS/TACACS+
INF.SD.23	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.SD.24	Dedykowany port do zarządzania RJ-45.

4.3.15. Kompleks biurowy SPNT: switche dostępowe POE

ID wymagania	**Treść wymagania**
INF.SDP.1	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.SDP.2	Minimum dwa wewnętrzne zasilacze AC, z redundancją zasilania.
INF.SDP.3	Wyposażony w następującą ilość portów: min. 48 portów 10/100/1000Mbps, oraz minimum 2 porty 10Gbps.
INF.SDP.4	Możliwość zbudowania jednego wirtualnego przełącznika z 4 przełączników tego samego typu tzw. funkcja stackowania; przełącznik wirtualny powinien być widziany przez inne urządzenia sieciowe jako pojedyncze urządzenie zarówno pod kątem mechanizmów warstwy L2 jak i warstwy L3; do podłączenia przełączników jako przełącznik wirtualny, musi być wykorzystany dedykowany port, połączenie przez dedykowany port musi być połączeniem w ringu, aby zminimalizować awarie w trakcie uszkodzenia kabla/przełącznika; przepustowość portu dedykowanego do połączenia miedzy poszczególnymi urządzeniami musi być minimum 10Gbps.
INF.SDP.5	Wielkość tablicy MAC adresów minimum 12000 pozycji.
INF.SDP.6	Urządzenie musi być wire speed dla funkcji przełącznika, wydajność minimum 100Gbs, przepustowość minimum 100Mpps.
INF.SDP.7	Obsługa IPv4/IPv6.
INF.SDP.8	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, Dhcp Snooping Trust.
INF.SDP.9	Obsługa IGMP v1/v2/v3.
INF.SDP.10	Obsługa 4000 jednoczesnych VLAN, translacji VLAN.
INF.SDP.11	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.SDP.12	Obsługa 802.1x, 802.3ad.

INF.SDP.13	Kontrola MAC adresów w poszczególnych VLANACH, obsługa wykrywania pętli tzw. loop detection.
INF.SDP.14	Wsparcie dla MTU 9216 bajtów.
INF.SDP.15	Tablica routingu minimum 4000 wpisów dla IPv4 oraz 1000 wpisów dla IPv6.
INF.SDP.16	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.
INF.SDP.17	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS.
INF.SDP.18	Funkcja mirroringu portów: 1 to 1 Port mirroring, Many to 1 port mirroring.
INF.SDP.19	Możliwość wyboru sposobu obsługi kolejek – Strict Priority; Weighted Round Robin.
INF.SDP.20	Wsparcie dla 802.3af, 802.3at tzw. POE/POE+, minimalnie 14W na port miedziany, przy założeniu wykorzystania wszystkich portów moc jednego zasilacza musi wynosić minimum 700W; urządzenie wówczas musi być wyposażone w dwa zasilacze każdy po 700W.
INF.SDP.21	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.SDP.22	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół.
INF.SDP.23	Obsługa RADIUS/TACACS/TACACS+
INF.SDP.24	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.SDP.25	Dedykowany port do zarządzania RJ-45.

4.3.16. Kompleks biurowy SPNT: switche agregujące

ID wymagania	**Treść wymagania**
INF.SA.1	Musi być dedykowanym urządzeniem sieciowym, przystosowanym do montażu w szafie RACK 19U, wielkość urządzenia 1U.
INF.SA.2	Minimum dwa wewnętrzne zasilacze 230V AC, z redundancją zasilania.
INF.SA.3	Wyposażony w ilość portów, z obsługą diagnostyki modułów minimum 24 porty 10Gbps.
INF.SA.4	Tablica MAC adresów minimum 32000 pozycji.
INF.SA.5	Urządzenie musi być wire speed dla funkcji przełącznika, wydajność minimum 480Gbs, przepustowość minimum 300Mpps.
INF.SA.6	Obsługa IPv4/IPv6.
INF.SA.7	Obsługa DHCP Snooping, Option 82, DHCP Relay, Option 82, Dhcp Snooping Trust.
INF.SA.8	Obsługa IGMP v1/v2/v3.
INF.SA.9	Obsługa 4000 jednoczesnych VLAN, translacji VLAN.
INF.SA.10	Obsługa Spanning Tree, 802.1d, 802.1w, 802.1s.
INF.SA.11	Obsługa 802.1x, 802.3ad.
INF.SA.12	Kontrola MAC adresów w poszczególnych VLANACH.
INF.SA.13	Wsparcie dla MTU 9000 bajtów.
INF.SA.14	Funkcjonalność przełączania pakietów non-STP.
INF.SA.15	Tablica routingu minimum 10000 wpisów dla IPv4 oraz 2000 wpisów dla IPv6.
INF.SA.16	Możliwość ograniczania pasma na porcie (globalnie) oraz możliwość ograniczenia pasma dla ruchu określonego listą ACL.

INF.SA.17	Klasyfikacja QOS po ACL, 802.1p, IP, DSCP, ToS.
INF.SA.18	Obsługa SNMP v1/v2/v3 (informacje o MIB muszą być dostępne dla zamawiającego), cli (minimum ssh/telnet), syslog, ntp.
INF.SA.19	Obsługa oraz integracja z sieciami SDN, poprzez otwarty protokół.
INF.SA.20	Obsługa RADIUS/TACACS/TACACS+
INF.SA.21	Zarządzanie przez system zarządzania i monitorowania pochodzący od tego samego producenta.
INF.SA.22	Dedykowany port do zarządzania RJ-45.

4.3.17. Kompleks biurowy SPNT: rozszerzenia licencji kontrolerów Wi-Fi

ID wymagania	Treść wymagania
INF.K.1	Wymagane 2 pakiety rozszerzenia licencji do obsługi 50 szt. Access Pointów do dwóch kontrolerów Rucus ZoneDirector 3000.

4.3.18. Kompleks biurowy SPNT: punkty dostępowe (AP)

ID wymagania	Treść wymagania
INF.AP.1	Punkt dostępowy współpracujący / w pełni kompatybilny z kontrolerem Rucus ZoneDirector 3000.
INF.AP.2	Dwa tryby pracy: samodzielny (zarzadzanie punktem odbywa się poprzez interfejs przeglądarki internetowej, telnet i SSH) oraz zarządzania przez kontroler sieci bezprzewodowej.
INF.AP.3	W trybie zarządzania przez kontroler sieci bezprzewodowej komunikacja z punktem dostępowym musi być szyfrowana.
INF.AP.4	W trybie zarządzania przez kontroler sieci bezprzewodowej punkt dostępowy może znajdować się w tej samej, lub innej podsieci IP.
INF.AP.5	Możliwość pracy jako cześć sieci kratowej (tj. „mesh") - bez podłączonego kabla Ethernet, z dynamicznym przełączeniem pomiędzy trybami i automatyczną konfiguracją.
INF.AP.6	Równoczesna praca w pasmie 2,4 GHz i 5.x GHz.
INF.AP.7	Praca w trybie MIMO 3x3:3.
INF.AP.8	Wsparcie dla metody MRC (Maximal Ratio Combining).
INF.AP.9	System musi zapewniać dostęp sygnału radiowego wokół punktu dostępowego, bez martwych pól.
INF.AP.10	System musi zapewniać maksymalne wzmocnienie 9 dBi i filtrowanie interferencji na poziomie -15dBi.
INF.AP.11	Automatyczna ochrona przed interferencjami sygnału.
INF.AP.12	Anteny wbudowane i zintegrowane z punktem dostępowym.
INF.AP.13	System antenowy musi się składać z nie mniej niż 12 elementów.
INF.AP.14	Czułość odbiornika nie mniejsza niż -101dBm.
INF.AP.15	Nie mniej niż 32 BSSID z własną polityką dostępu i regułami QoS.

INF.AP.16	Nie mniej niż 4 kolejki QoS per stacja kliencka i wsparcie standardu 802.11e.
INF.AP.17	Obsługa nie mniej niż 500 stacji, nie mniej niż 60 klientów głosowych jednocześnie.
INF.AP.18	802.11d, 802.1Q, 802.1X.
INF.AP.19	802.3af oraz 802.3at PoE.
INF.AP.20	802.11a/b/g/n.
INF.AP.21	WEP
INF.AP.22	WPA-PSK
INF.AP.23	WPA-TKIP
INF.AP.24	WPA2-AES
INF.AP.25	802.11i
INF.AP.26	IEEE 802.11n: 2.4 – 2.484 GHz i 5.15 – 5.85 GHz
INF.AP.27	IEEE 802.11a: 5.15 – 5.85 GHz
INF.AP.28	IEEE 802.11b: 2.4 – 2.484 GHz
INF.AP.29	802.11n: 6.5Mbps – 216,7Mbps (20MHz)
INF.AP.30	802.11n: 13.5Mbps – 450Mbps (40MHz)
INF.AP.31	802.11a: 54, 48, 36, 24, 18, 12, 9, 6Mbps
INF.AP.32	802.11b: 11, 5.5, 2, 1 Mbps
INF.AP.33	802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps
INF.AP.34	Zasilanie poprzez PoE lub zasilacz 12V DC
INF.AP.35	Maksymalna pobierana moc 13W.
INF.AP.36	2 porty RJ-45, auto MDX, auto-sensing 10/100/1000 Mbps, jeden z możliwością zasilania PoE.
INF.AP.37	Masa urządzenia nie większa niż 1 kg.
INF.AP.38	Praca w temperaturze 0-50C, wilgotność do 95% (bez kondensacji).
INF.AP.39	Homologacja do montażu w zamkniętych przestrzeniach UL 2043.
INF.AP.40	Montaż bez konieczności użycia zewnętrznych akcesoriów i maskownic.
INF.AP.41	Dynamicznego generowania kluczy Pre-Shared keys.
INF.AP.42	Automatycznego wyboru najlepszego kanału pracy w oparciu o realną przepustowość/pojemność kanałów dla 2,4 GHz lub 5 GHz wraz z możliwością przeniesienia klienta na optymalny kanał z wykorzystaniem standardu 802.11h.
INF.AP.43	Możliwość dobierania optymalnych kanałów transmisyjnych bez konieczności przerywania transmisji danych.
INF.AP.44	Optymalizacja wydajności sieci przy różnych prędkościach dostępowych klientów (sterowanie czasem dostępu do punktu dostępowego na podstawie okien czasowych, nie ilości przesłanych danych).
INF.AP.45	W celach diagnostycznych możliwość przechwycenia ramek 802.11/802.3 od/do klienta przesyłanych przez punkt dostępowy bez wpływu na trwającą komunikację.

4.3.19. Szafy serwerowe

ID wymagania	**Treść wymagania**
INF.SZ1	DK TS8 kompatybilna z modułami LCP T3+

INF.SZ2	Wyposażenie w wysokoszczelny szczotkowy moduł podłogi do wprowadzania kabli.
INF.SZ3	Łączniki zewnętrzne.
INF.SZ4	Uszczelki pionowe blokady strumienia powierzchni lewej i prawej strony LCP i poziom 19".
INF.SZ5	2 moduły mocy PDU 3x32A gniazda 3x 6xC13, 3x 2xC19, funkcja wł.-wył. Pojedyncze gniazdo model CW-24VYM.
INF.SZ6	2 moduł PDU - 19" z podłączeniem 32A , wyjście 4xC19 z funkcją włą-wył. Pojedyncze gniazdo.
INF.SZ7	Czujnik temperatury i wilgotności.
INF.SZ8	4 szyny poziome do prowadzenia kabli.
INF.SZ9	10 wieszaków kablowych przelotowych.
INF.SZ10	Funkcja automatycznego otwierania drzwi.

4.3.20. Moduły chłodzące

ID wymagania	Treść wymagania
INF.MC1	LCP T3+ EC 47U 3300235, dla chłodzenia szaf serwerowych DK TS8 2200x1200, o mocy chłodniczej do 30 kW.
INF.MC2	Dwa aktywne obwody chłodzenia i prądowe.
INF.MC3	Wbudowane sterowniki monitoringu i zarządzania zdalną pracą przez Rittal CMC TC.
INF.MC3	Funkcja „Auto-Load-Balancing“.
INF.MC4	Funkcja „Auto-Recovery“.
INF.MC5	Ekran dotykowy do lokalnego zarządzania i monitorowania pracą wymiennika.
INF.MC6	Funkcja automatycznego otwierania drzwi szafy serwerowej dla gaszenia pożaru w szafie oraz dla chłodzenia awaryjnego.
INF.MC7	Kolor RAL 7035.

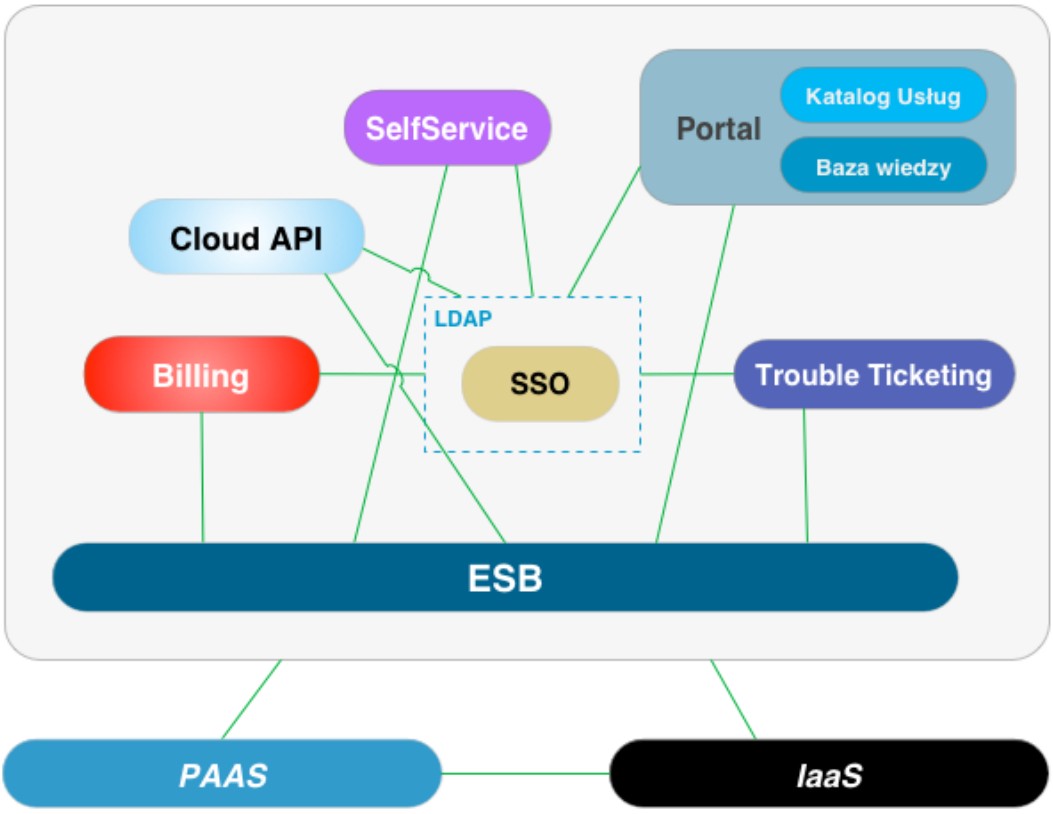
5. Platforma oprogramowania

5.1. Opis ogólny

5.1.1. Architektura logiczna Platformy oprogramowania

Opisana poniżej architektura Platformy oprogramowania została zaprojektowana w celu realizacji Usług (wspólnie z infrastrukturą sprzętową) opisanych szerzej w rozdziale 2. Podsystemy i komponenty wchodzące w jej skład będą udostępniać określone Usługi bezpośrednio dla Klientów i użytkowników, a także pełnić funkcję wspierającą.

Na poniższej ilustracji została przedstawiona architektura logiczna Platformy oprogramowania:



Rys. 2. Architektura logiczna Platformy oprogramowania

Architektura Platformy oprogramowania składa się z kilku Podsystemów. Podsystem SSO stanowi punkt rejestracji i zarządzania kontami użytkowników, a także mechanizm zapewniający pojedynczy punkt uwierzytelniania dla poszczególnych Podsystemów. W ramach Portalu użytkownicy będą mogli zapoznać się z ofertą Usług świadczonych z wykorzystaniem Systemu. W przypadku konieczności uzyskania pomocy, użytkownicy będą mogli skorzystać z Bazy Wiedzy, w której znajdą dokumentację Systemu oraz rozwiązania najczęściej występujących problemów, lub skorzystać - za pośrednictwem Podsystemu Trouble Ticketing - ze wsparcia technicznego.

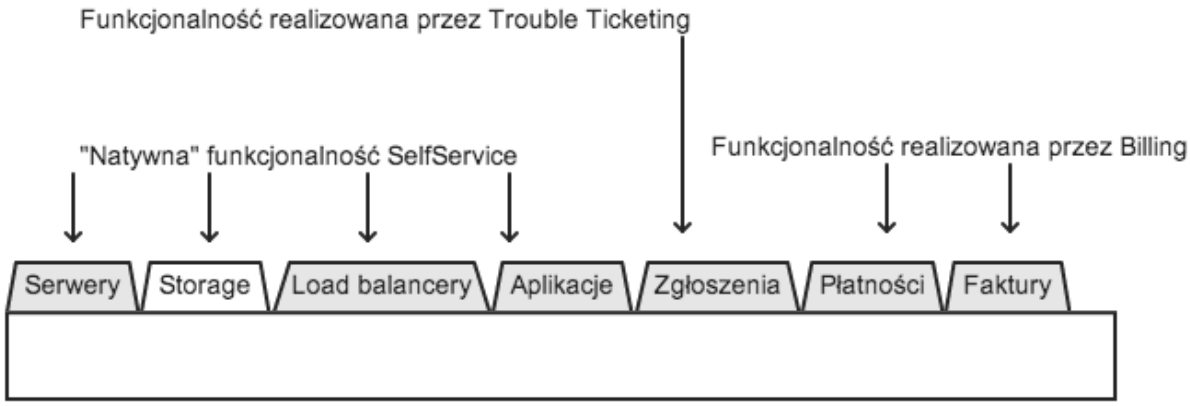
Na podstawie informacji znalezionych w Portalu użytkownicy będą mogli zakupić i skonfigurować- wykorzystując do tego celu Podsystem SelfService - Usługi świadczone przez Zamawiającego. Usługi te będą realizowane w ramach Podsystemów IaaS i PaaS, w oparciu o dostarczoną infrastrukturę sprzętową. Rozliczenie Usług będzie się odbywać w ramach Podsystemu Billing. Ponadto użytkownicy będą mogli zintegrować Platformę oprogramowania ze swoimi systemami informatycznymi przy wykorzystaniu Cloud API.

Zamawiającemu przyświeca cel wdrożenia Systemu jako produktu zapewniającego możliwość zmian i rozwoju celem adaptacji do aktualnych potrzeb rynkowych i nie traktuje niniejszej architektury (całego Systemu, czy też poszczególnych komponentów) jako zamkniętej.

5.1.2. Architektura front-end

Zamawiający sugeruje, aby został zaprojektowany wspólny i spójny interfejs użytkownika dla wszystkich Podsystemów. Pozwoli to zminimalizować liczbę wymaganych integracji pomiędzy poszczególnymi Podsystemami, a zapewnienie niezbędnych funkcjonalności będzie w takim podejściu realizowane przez "przełączanie" się do każdego z nich. Dla użytkownika nie powinno to być w jakikolwiek sposób zauważalne, jako że do każdego z Podsystemów będzie on zalogowany i autoryzowany za pomocą SSO, co bezpośrednio wpłynie na komfort i użyteczność rozwiązań.

Na poniższej ilustracji przedstawiono przykładowe wdrożenie Podsystemu SelfService, gdzie cztery pierwsze zakładki w interfejsie użytkownika to funkcjonalności realizowane przez ten Podsystem "natywnie" (za pomocą integracji z odpowiednimi API IaaS oraz PaaS). Kliknięcie w pozostałe zakładki powoduje przejście do Podsystemu zgłoszeń (Trouble Ticketing) lub Podsystemu billingowego (Billing).



Rys. 3. Przełączanie użytkownika pomiędzy funkcjonalnościami i Podsystemami na przykładzie Podsystemu SelfService

Należy zaznaczyć, że powyższy przykład jest jedynie ilustracją jednej z możliwości zbudowania Podsystemu SelfService, i zakłada, że docelowe rozwiązanie zostanie opracowane przez Wykonawcę w ramach projektu technicznego, z uwzględnieniem podjętych na etapie analizy i projektowania decyzji architektonicznych, kwestii użyteczności interfejsu użytkownika, a także możliwości łatwej modyfikacji (a nawet wymiany) każdego z Podsystemów bez istotnych zmian w pozostałych, zintegrowanych z nim Podsystemach.

5.1.3. Architektura back-end

Dla zapewnienia elastyczności oraz skalowalności Systemu został położony mocny nacisk na zapewnienie przez każdy z Podsystemów odpowiedniego API oraz na wewnętrzną integrację Podsystemów za pomocą wspólnej szyny danych ESB. Zaproponowano także podejście SSO wprowadzające centralny punkt uwierzytelniania użytkowników. Ponadto w ramach Projektu należy dostarczyć i wdrożyć centralny system logów, odpowiadający za zebranie logów systemowych

generowanych przez wszystkie Podsystemy. Centralny system logów musi dysponować interfejsem użytkownika, umożliwiającym administratorom przeglądanie, przeszukiwanie i analizowanie logów.

5.1.4. Opis i wymagania ogólne poszczególnych Podsystemów

5.1.4.1. IaaS

IaaS (*Infrastructure as a Sevice* - Infrastruktura jako usługa) - Podsystem prywatnej i publicznej chmury obliczeniowej jest fundamentem całej Platformy oprogramowania. Jest to Podsystem, za pomocą którego świadczone będą między innymi następujące Usługi:

- Serwery dedykowane
- Serwery VPS
- Serwery Cloud
- Wirtualna prywatna chmura (prywatna sieć pomiędzy usługami - Private Network as a Service)
- Blokowy cloud storage (Storage as a Service)
- Obiektowy cloud storage (Object Storage as a Service)
- Storage obrazów maszyn wirtualnych (szablony/obrazy maszyn wirtualnych)
- Load Balancer as a Service
- VPN as a Service
- Dodatkowe adresy IP (IPv4 oraz IPv6)

Szczegółowy opis funkcjonalności dla Usług świadczonych w oparciu o Podsystem IaaS znajduje się w rozdziale 2.

Z uwagi na krytyczny aspekt Podsystemu IaaS, jako że:

- za jego pośrednictwem świadczone będą Usługi dla Klienta Centrum Danych,
- w oparciu o Podsystem IaaS zbudowany zostanie Podsystem PaaS,
- Klienci świadczyć będą swoje usługi (np. aplikacje SaaS)

niezmiernie istotne jest wdrożenie **kompleksowego, dojrzałego, elastycznego (oferującego uruchamianie heterogenicznych środowisk), skalowalnego i bezpiecznego Podsystemu IaaS**.
Dzięki takiemu podejściu twórcy przyszłych rozwiązań osadzanych na Systemie będą mogli skupić się na dostarczaniu innowacyjnych rozwiązań.
Aby tak się stało, Podsystem IaaS (jak i cały System) musi umożliwić "nadążanie" za trendami rynkowymi - co w konsekwencji oznacza szybkie i łatwe możliwości zmiany lub dostosowania IaaS do nowych wymagań. **Dlatego Zamawiający wybiera podejście umożliwiające mu ciągły rozwój Systemu - a w szczególności rozwiązania IaaS**. To powoduje, że podczas prac wdrożeniowych jak i po wdrożeniu całego Systemu pożądane jest podejście *Continuous Delivery*.

Ważnym aspektem IaaS jest także uniezależnienie od warstwy sprzętowej. System zostanie wdrożony i zoptymalizowany pod kątem zapewnienia wysokiej wydajności we współpracy ze sprzętem

zaproponowanym przez Wykonawcę, natomiast sam Podsystem IaaS musi być niezależny od producenta platformy sprzętowej (wspierać wielu producentów) na każdej płaszczyźnie: obliczeniowej (compute), danych (storage) oraz sieci (network) i umożliwiać dołączenie dowolnego typu sprzętu do wdrożonego już rozwiązania.

Z uwagi na powyższe wymagania podczas wyboru (ofertowania) Podsystemu IaaS należy zwrócić szczególną uwagę na aspekty technologiczne opisane poniżej.

Hypervisor:

Warstwa compute musi wspierać jak największą liczbę hypervisorów oraz umożliwać bez modyfikacji wdrażanie kolejnych w przyszłości, tak, aby umożliwić wybór pożądanego hypervisora w zależności od potrzeb rynkowych oraz biznesowych.

Wymagane jest także, aby IaaS wspierał wirtualizację na poziomie systemu operacyjnego, co umożliwi przygotowanie Systemu do świadczenia nie tylko Usług w zakresie cloud computing, ale także w przyszłości Usług hostingowych typu shared-hosting. W oparciu o wirtualizację na poziomie systemu operacyjnego należy także uruchomić Podsystem PaaS, przy czym jako wirtualizację na poziomie systemu operacyjnego (tzw. *OS-based virtualization*) należy rozumieć rozwiązanie, w którym jądro systemu operacyjnego jest załadowane tylko raz i jest wspólne dla wszystkich uruchomionych środowisk (zwanych czasem kontenerami - ang. *container*). Technologia ta zapewnia bardzo efektywny podział na środowiska wirtualne, gdyż wirtualizacja odbywa się na poziomie systemu operacyjnego, który zamiast pojedynczego środowiska - obsługuje ich kilka, zapewniając określony poziom odseparowania między nimi.

Dzięki wykorzystaniu kontenerów dla Usług shared-hosting bądź PaaS możliwe będzie bardzo efektywne przydzielanie zasobów sprzętowych przy zachowaniu niemal natywnej wydajności serwera - oferując przy tym unikalne korzyści dla zarządzania środowiskiem wirtualnym (np. dynamiczna realokacja zasobów). Takie podejście pozwoli także na zapewnienie bezpieczeństwa i elastyczności konfiguracji Usług świadczonych poszczególnym Klientom przy bardzo niskich nakładach na obsługę, jako że nie będzie potrzeby utrzymywania wielu środowisk/systemów operacyjnych dla Usług shared-hosting i PaaS, na korzyść jednego wspólnego dla wszystkich Klientów.

Storage:

W kwestii przechowywania danych, IaaS musi zapewnić elastyczność wspieranych usług przez warstwę danych, zapewniając:

- Storage blokowy - który będzie wykorzystywany zarówno jako podstawowy storage, na którym uruchamiane są systemy operacyjne dla maszyn wirtualnych, vps czy też storage dla Usługi

shared hosting, PaaS. Kolejną Usługą przygotowaną na bazie storage blokowego ma być "storage as a service", w której ten storage będzie wykorzystywany jako dodatkowy dla wszystkich ww. Usług;

- Szyfrowany storage blokowy - przygotowując się na oferowanie różnego typu Usług, w szczególności w sektorze medycznym, należy zapewnić najwyższy poziom bezpieczeństwa danych.
- Storage obrazów/szablonów maszyn wirtualnych, szablonów kontenerów systemów operacyjnych oraz szablonów kontenerów dla instancji PaaS.

Krytyczne jest aby IaaS nie był uzależniony od wykorzystywanego rozwiązania sprzętowego, oferując modularną/pluginową budowę oraz wiele typów sterowników, a także zapewniając obsługę wielu dostawców sprzętu oraz różnorodne protokoły dostępowe (w szczególności: iSCSI, FC, RADOS Block Device).

Network:

Podobnie jak w przypadku warstwy dostępu do danych, krytyczne jest uniezależnienie IaaS od rozwiązania sprzętowego w zakresie infrastruktury sieciowej. Umożliwi to zastosowanie modularnej/pluginowej budowy oraz wykorzystania wielu typów sterowników, zapewniając obsługę wielu dostawców sprzętu sieciowego. Umożliwi to także kontrolowanie z poziomu IaaS sieci na drugiej i trzeciej warstwie modelu OSI, a także zapewni integrację warstwy sieciowej z rozwiązaniami *Software Defined Network*. Uszczegółowienie oczekiwanych sposobów integracji zostało opisane w rozdziale 4.

Warstwa sieciowa musi po zakończeniu wdrożenia oferować w szczególności następujące Usługi:

- Sieci prywatne w obrębie instancji maszyn wirtualnych cloud, vps oraz instancji aplikacji PaaS,
- Obsługa adresów publicznych IPv4 i IPv6 dla wszystkich Usług obsługiwanych przez IaaS,
- Usługa load balancerów, które będą oferowane jako Usługa dla Klientów, ale będą też wykorzystywane przez sam System,
- Obsługę oraz terminacja SSL na load balancerach,
- Zarządzanie sesją HTTP na load balancerach,
- Dowolna ilość instancji VPN: IPSEC VPN oraz SSL VPN do sieci prywatnych zarządzanych przez Usługę IaaS.

API:

Każda funkcjonalność IaaS musi być dostępna przez API, dzięki czemu możliwe będzie kompleksowe zarządzanie środowiskiem IaaS za pomocą jednolitego interfejsu API na potrzeby integracji i późniejszego rozwoju Systemu. Ponadto API IaaS będzie wchodzić w zakres przygotowywanego w ramach Projektu publicznego Cloud API, które będzie agregować i udostępniać Klientowi **pełne API**

służące do zarządzania, monitorowania oraz obsługi Systemu.

High Availability:

Wszystkie komponenty IaaS: computing, storage, networking, a także komponenty zarządzające samym Podsystemem (samo oprogramowanie zarządcze IaaS) muszą zostać zbudowane i wdrożone w trybie wysokiej dostępności (*high availability*), w celu zapewnienia nieprzerwanego działania krytycznych komponentów infrastruktury.

5.1.4.2. PaaS

Z uwagi na wymagania firm będących członkami Powiązania Kooperacyjnego Cloud for Cities w ramach projektu "Przetwarzanie w chmurze dla rozwoju miast cyfrowych - faza rozwoju" oraz szerokie działania Zamawiającego w środowisku IT, w szczególności ścisłą współpracę z firmami z KlastraIT[1] - zidentyfikowano potrzebę wdrożenia Podsystemu PaaS (*Platform as a Service*) jako kluczowego elementu Systemu oraz elementu, który może stanowić dla zainteresowanych podmiotów istotny element oszczędności czasu jak i zasobów dzięki oferowanym przez Podsystem PaaS funkcjonalnościom. Zamawiający ma w szczególności na celu stworzenie przyjaznego, elastycznego, skalowalnego i bezpiecznego środowiska dla tworzenia i późniejszego hostowania aplikacji w modelu SaaS.

Architektura PaaS musi integrować się bezpośrednio z IaaS oraz wykorzystywać infrastrukturę zarządzaną przez IaaS. Oznacza to, że PaaS wykorzystuje IaaS w celu zarządzania środowiskami systemów operacyjnych, sieci czy też warstwą danych (storage) w celu zapewnienia elastyczności, skalowalności jak i bezpieczeństwa rozwiązania.

PaaS musi zapewniać:

- Automatyzację zarządzania, skalowania (w tym możliwość auto-skalowania) i monitorowania środowiska IaaS dla serwerów aplikacyjnych oraz baz danych przeznaczonych dla aplikacji Klienta,
- Automatyczny provisioning i zarządzanie środowisk aplikacyjnych za pomocą prostych mechanizmów oraz interfejsów takich jak panel SelfService, API, CLI oraz przez systemy VCS (systemy kontroli wersji) dla Klienta,
- Automatyczny deployment aplikacji jak i baz danych na środowisku PaaS i przez udostępnione interfejsy aplikacji wskazane przez Klienta,
- Możliwość rozliczania aplikacji działających na środowisku PaaS w modelu *Pay as you go* - czyli za faktycznie wykorzystane zasoby.

[1] http://klaster.it

PaaS musi wspierać (zgodnie z wymaganiami szczegółowymi):

- Wiele języków programowania,
- Wiele bibliotek/frameworków programowania danego języka,
- Wiele serwerów aplikacyjnych dla danego języka i frameworku,
- Wiele usług bazodanowych (w tym usługi bazodanowe SQL i noSQL).

Architektura PaaS powinna w przyszłości (bez jej modyfikacji) umożliwiać rozszerzanie funkcjonalności rozwiązania o kolejne języki programowania, frameworki, systemy bazodanowe a także umożliwiać proste (za pomocą modułów/pluginów) rozszerzenie Systemu o nowe technologie, narzędzia i usługi (np. rozproszonych i asynchronicznych systemów zarządzania kolejkami zadań).

5.1.4.3. Cloud API

Wszystkie Podsystemy Platformy oprogramowania udostępniały będą kompleksowe API dla wszystkich funkcjonalności danego Podsystemu. Usługi te nie będą jednak dostosowane do wykorzystania przez użytkowników zewnętrznych. Cloud API ma stanowić warstwę abstrakcji, która pozwoli w spójny, łatwy do wykorzystania sposób udostępnić wewnętrzne interfejsy API użytkownikom zewnętrznym.

API takie powinno być przyjazne dla developerów i dobrze udokumentowane (wraz z przykładami) oraz przetestowane. Co więcej, wraz ze specyfikacją techniczną powinien zostać opublikowany zestaw testów akceptacyjnych przeznaczonych do weryfikacji poprawności działania tego API. Dzięki temu możliwe będzie zrealizowanie wymagań Rozporządzenia Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego i weryfikacji tego badania. (Dz.U. z 2005 nr 217 poz. 1836), co z kolei przełoży się na uzyskanie przewagi konkurencyjnej w przypadku Klientów z szeroko rozumianej administracji publicznej.

Aby spełnić te oczekiwania, cloud API będzie udostępniać w centralnym miejscu metody API dla użytkowników zewnętrznych Platformy oprogramowania (a zatem będzie udostępniał jeden zabezpieczony endpoint dla API), zbudowane wokół uproszczonego, spójnego modelu danych, dostosowanego do potrzeb i oczekiwań Klientów.

Ponieważ Cloud API będzie stanowić spójny interfejs API, to jeżeli Wykonawca planuje wdrożyć Podsystemy, które posiadają różne modele danych w wywołaniach API, Cloud API musi zapewnić jeden spójny model danych dla wszystkich wywołań. Podobnie wygląda kwestia w zakresie stosowanych konwencji nazewniczych, wersjonowania API itp.

Dodatkowo, jako uzupełnienie API programistycznych, należy dostarczyć zestaw narzędzi linii poleceń (CLI - *Command Line Interface*) umożliwiający wykonanie wszystkich operacji dostarczanych przez Cloud API z linii poleceń. Narzędzia te powinny być skonstruowane w sposób niezależny od platformy

systemowej i działać poprawnie pod kontrolą systemów z rodziny MS Windows, Linux i MacOS. Konieczne jest także zapewnienie możliwości automatycznego uaktualnienia zainstalowanego pakietu CLI.

5.1.4.4. SelfService

Podsystem SelfService to główny i podstawowy Podsystem oparty o interfejs WEB, umożliwiający Klientowi pełne zarządzanie wykorzystywanymi przez niego Usługami, w tym:

- Obsługę, monitoring oraz zarządzanie wykupionymi przez Klienta Usługami,
- Wykupienie oraz provisioning nowych Usług lub rezygnację z obecnych,
- Dokonanie płatności za wykupione Usługi,
- Pobranie faktur za dokonane opłaty (oraz faktur pro-forma jak i faktur korygujących),
- Pełną obsługę konta Klienta (organizacji Klienta) w ramach Platformy (zarządzanie użytkownikami, rolami, grupami, uprawnieniami) - we współpracy z Podsystemem SSO.

W związku z tym SelfService musi implementować i udostępniać Klientom wszystkie funkcjonalności udostępniane przez IaaS, PaaS i Billing w zakresie obsługi produktów i Usług wykorzystywanych przez danego Klienta w interfejsie WEB.

Poniżej wskazano najistotniejsze potrzeby użytkowników w zakresie korzystania z Podsystemu SelfService. Należy zaznaczyć, że sposób realizacji tych potrzeb może być różny dla różnych produktów; zadaniem Wykonawcy jest doprecyzowanie sposobu realizacji wskazanych potrzeb na etapie przygotowywania analizy i projektu technicznego.

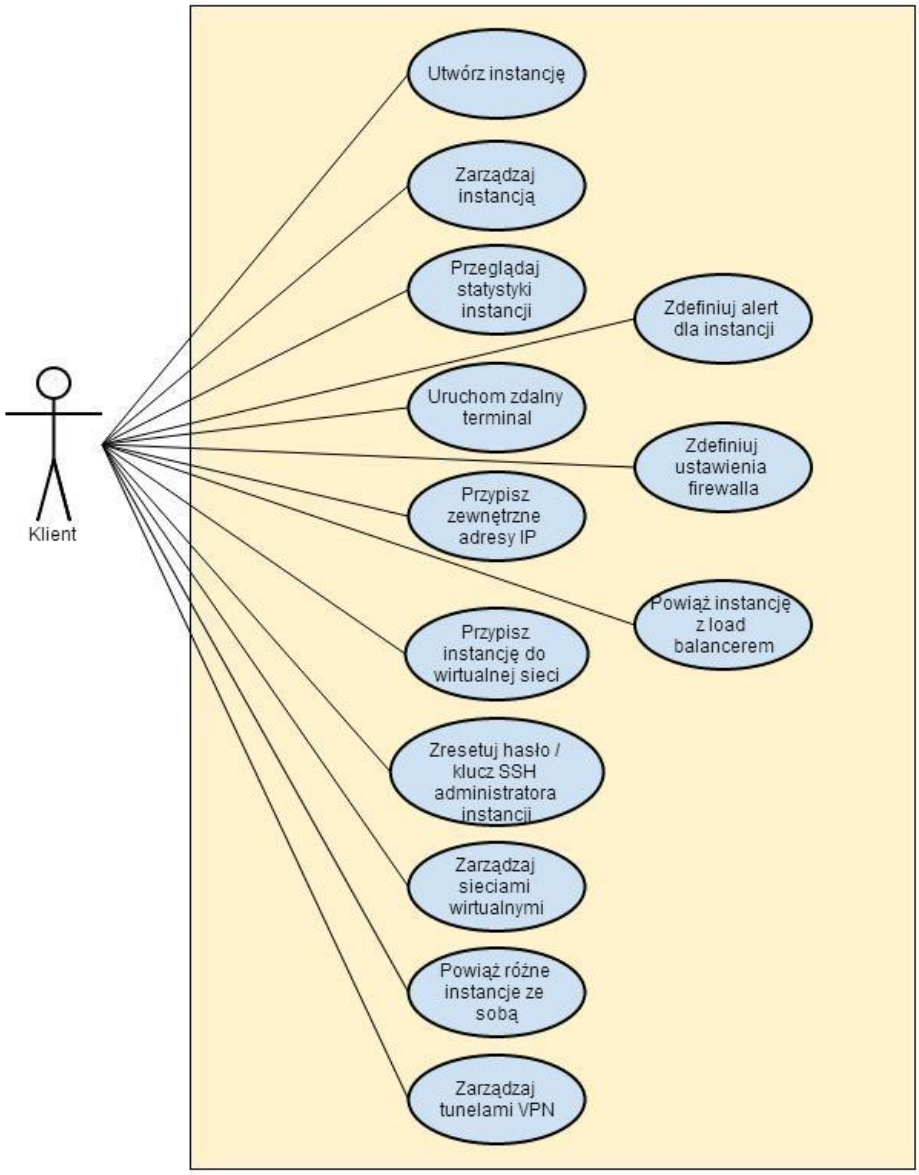


Diagram: Najistotniejsze potrzeby użytkowników w zakresie zarządzania instancjami w kontekście Podsystemu SelfService

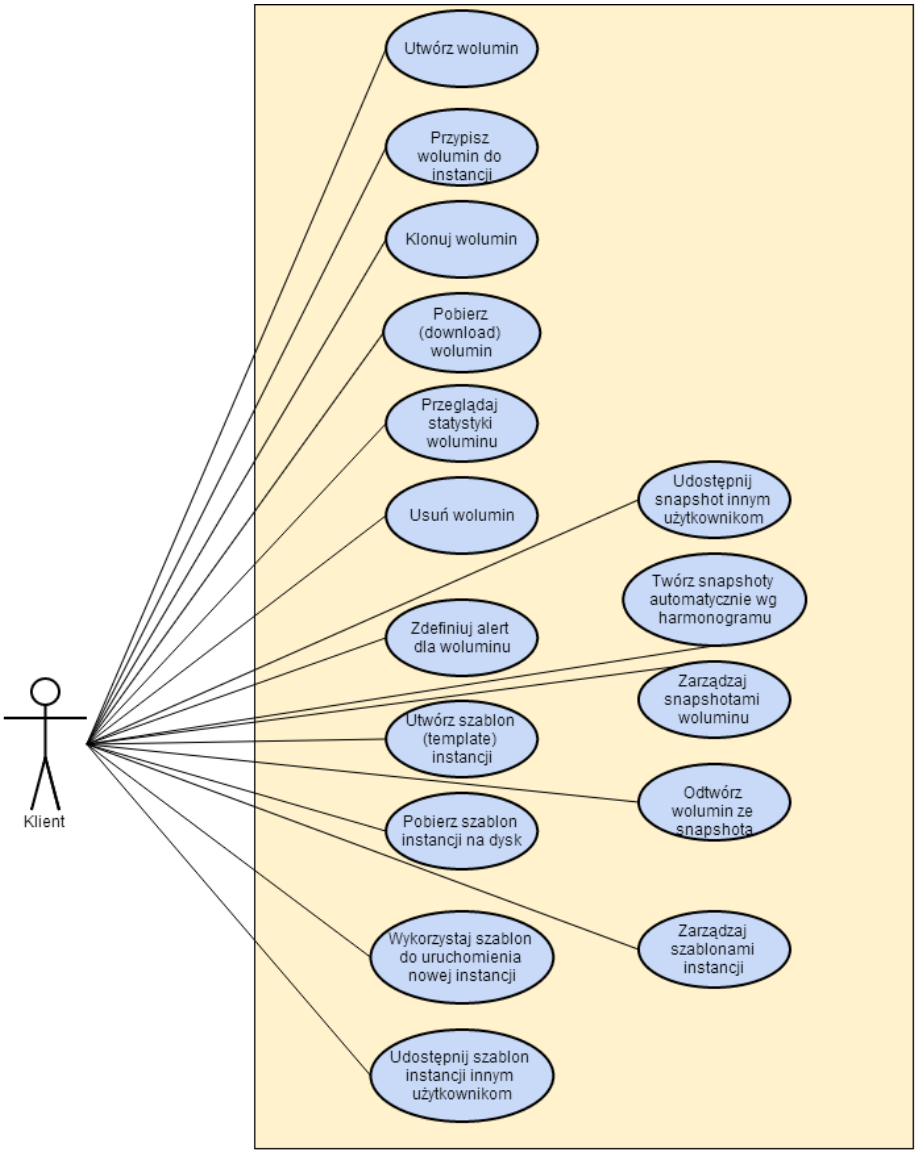


Diagram: Najistotniejsze potrzeby użytkowników w zakresie zarządzania woluminami w kontekście Podsystemu SelfService

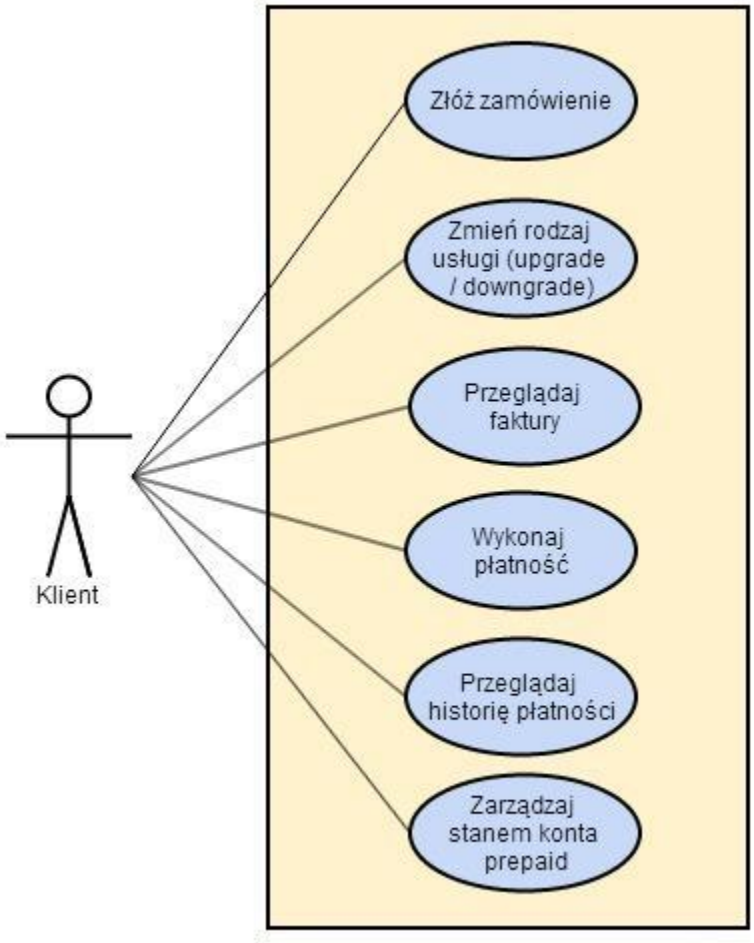


Diagram: Najistotniejsze potrzeby Klientów w zakresie finansów w kontekście Podsystemu SelfService

SelfService stanowi także centralne miejsce umożliwiające Klientowi przejście do Podsystemu Trouble Ticketing w celu obsługi zgłoszeń czy też przejście do Bazy Wiedzy w celu zapoznania się z dostępną dokumentacją.

Jako, że SelfService będzie stanowić główny punkt obsługi Klienta, krytyczny jest jego wygląd i usability, dlatego też przed rozpoczęciem wdrożenia Podsystemu Wykonawca opracuje:

1. projekt graficzny wraz z projektem usability,
2. przedstawi analizę heurystyczną (nazywaną czasem heurystyką, analizą ekspercką) projektu w celu określenia zgodności z powszechnie uznanymi zasadami usability.

W ostatniej fazie - przed samym wdrożeniem należy także przeprowadzić badania serwisu z reprezentatywną grupą użytkowników.

Należy zaznaczyć, że ostateczny sposób komunikacji między poszczególnymi Podsystemami jest uzależniony od architektury i zakresu funkcjonalnego komponentów oferowanych przez Wykonawcę. SelfService, obok Trouble Ticketing, jest Podsystemem, który jest najbardziej podatny na ewentualne różnice w tym obszarze. Stąd Zamawiający, na etapie akceptacji projektu technicznego, może

dopuścić pewne przesunięcia zakresów funkcjonalnych między poszczególnymi Podsystemami, o ile nie spowoduje to negatywnych konsekwencji z perspektywy spełnienia potrzeb użytkowników końcowych, użyteczności projektowanego rozwiązania, jego bezpieczeństwa, łatwości utrzymania, elastyczności i skalowalności.

5.1.4.5. Billing

Podsystem rozliczeniowy (Billing) powinien zapewniać elastyczne rozliczanie, płatności oraz fakturowanie wszystkich Usług oferowanych przez System, bazując na określonych atomowych jednostkach, które zostały wyznaczone do rozliczeń.

Wykonawca musi szczególnie zwrócić uwagę na fakt, iż głównymi użytkownikami Podsystemu rozliczeniowego nie będą osoby techniczne, a osoby biznesowe, dla których Billing ma być narzędziem definiowania oraz rozliczania Usług świadczonych przez System (w szczególności Usług IaaS oraz PaaS). Billing musi zatem dostarczyć wygodne oraz elastyczne narzędzia graficzne WEB (zgodne z wymaganiami), umożliwiające łatwą pracę użytkownikom nie-technicznym.

Ważnym aspektem w powyższej kwestii jest ścisła integracja Billing z IaaS oraz PaaS w celu zapewnienia nie tylko elastycznego zarządzania i rozliczania oferowanych Usług, ale także modelowania, analizy stanu obecnego oraz prognozowania wartości. Szczegóły oraz propozycje realizacji Zamawiający pozostawia Wykonawcy na etap analizy oraz przygotowania projektu technicznego.

Kolejnym istotnym aspektem dla wdrożenia Podsystemu Billing jest zwrócenie uwagi na różnorodność Usług, jakie Zamawiający planuje oferować, a które zostały opisane w rozdziale 2. Billing musi umożliwiać rozliczanie planowanych Usług w wielu modelach rozliczeniowych.

5.1.4.6. ESB

W celu zmniejszenia wzajemnego powiązania wszystkich modułów (komunikacji peer-to-peer za pomocą API) Wykonawca zobowiązany jest wdrożyć wspólną szynę danych. Komunikacja/integracja pomiędzy wszystkimi Podsystemami Platformy oprogramowania musi odbywać się poprzez szynę danych ESB - a zatem każdy Podsystem, którego architektura zakłada istnienie interfejsów w postaci API musi być dostępny z poziomu szyny usług. Oznacza to, że usługi muszą być publikowane w rejestrze szyny usług.

5.1.4.7. SSO

W budowanym Systemie niezwykle istotne jest zapewnienie spójnej warstwy zarządzania tożsamością użytkowników. Oznacza to, że jedno konto użytkownika będzie widoczne i wykorzystywane we

wszystkich Podsystemach. Co więcej, należy przyłożyć dużą wagę do użyteczności rozwiązania w zakresie uwierzytelniania - nie można dopuścić do tego, by użytkownik musiał logować się do każdego z Podsystemów oddzielnie. Jednocześnie konieczne jest umożliwienie wymuszenia dodatkowego uwierzytelnienia przed wykonaniem niektórych - istotnych z punktu widzenia bezpieczeństwa - operacji. Dlatego też jednym z elementów Projektu jest przygotowanie i dostarczenie Podsystemu SSO, który będzie adresował wymienione kwestie w spójny, łatwy w zarządzaniu i przyjazny dla użytkownika sposób.

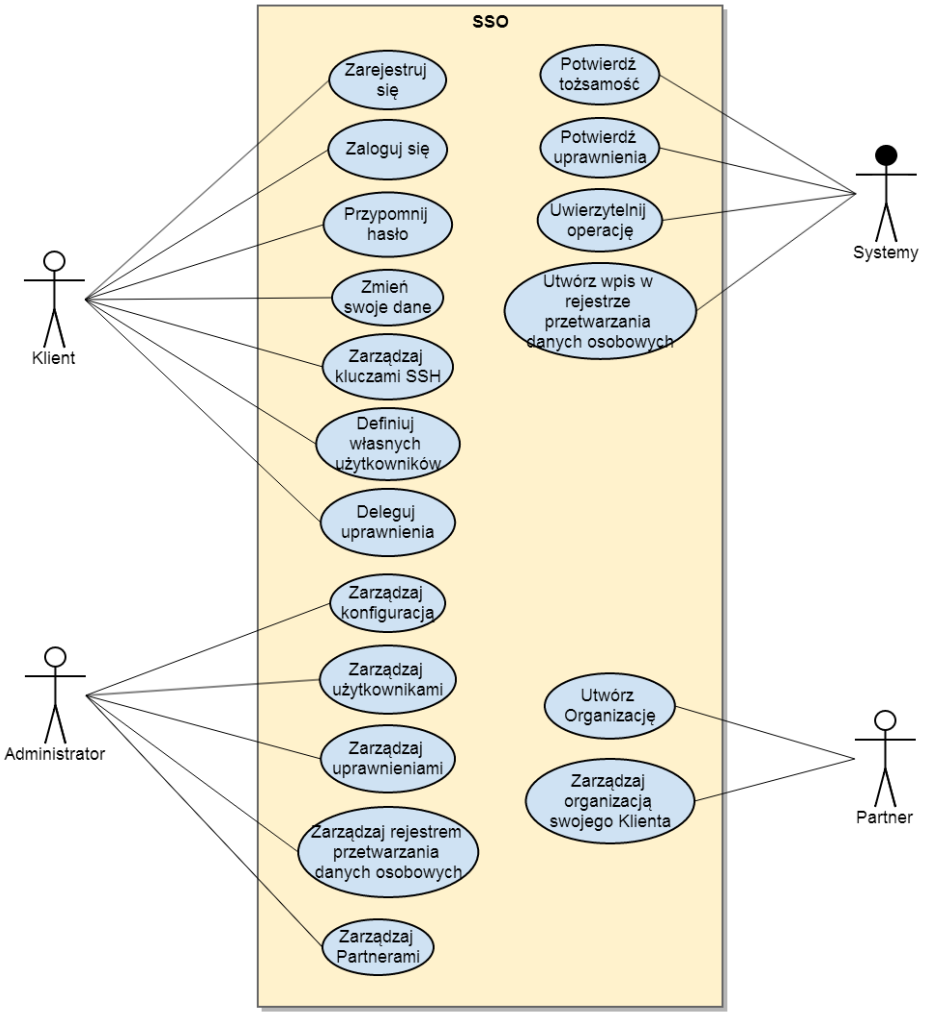


Diagram. Najistotniejsze potrzeby użytkowników w kontekście SSO

Istotnym elementem, który powinien zostać zaadresowany w kontekście Podsystemu SSO, jest uspójnienie mechanizmów zarządzania uprawnieniami w różnych, heterogenicznych Podsystemach Platformy oprogramowania, przy jednoczesnym zapewnieniu niezbędnej do realizacji potrzeb biznesowych elastyczności. Problem jest o tyle złożony, że poszczególne Podsystemy mogą mieć zupełnie inne modele uprawnień. Konieczne i wymagane jest też umożliwienie użytkownikom tworzenia innych użytkowników należących do tej samej organizacji oraz delegowania im uprawnień

do poszczególnych funkcjonalności i obiektów/zasobów. Oznacza to, że każdy użytkownik powinien móc nadać innemu użytkownikowi uprawnienia, które sam posiada. Nie wolno też zapominać o konieczności umożliwienia uprawnionym użytkownikom administrowania wszystkimi użytkownikami w danej organizacji, a także zapewnienia odpowiednich możliwości administracyjnych dla osób odpowiedzialnych za utrzymanie całości rozwiązania. Jednocześnie należy zadbać o to, by mechanizmy obsługi użytkowników i uprawnień poprawnie adresowały ryzyka bezpieczeństwa, związane z zarządzaniem użytkownikami i uprawnieniami, jak na przykład kwestię przechodniości uprawnień (to znaczy rozstrzygały, czy użytkownik może delegować dalej uprawnienia, które sam uzyskał w efekcie delegacji uprawnień).

Wdrażane rozwiązanie musi zapewnić możliwość definiowania i obsługi programów partnerskich. Mechanizmy związane z obsługą Partnerów będą bazować głównie na mechanizmach nadawania upustów, a płatności za wykorzystywane Usługi będzie ponosić Partner. Oznacza to, że z perspektywy funkcjonalnej to Partner będzie zarządzał wszystkimi zasobami; konieczne jest jednak umożliwienie mu nadania dostępu dla jego klientów do całej infrastruktury. Powinno zostać to rozwiązane poprzez umożliwienie Partnerowi definiowania nowych organizacji, w ramach których będzie miał on pełne uprawnienia administracyjne - zarówno w zakresie zarządzania użytkownikami, jak i Usługami i innymi zasobami skojarzonymi z tą organizacją. Oznacza to, że Partner będzie mógł wykonać w imieniu swojego klienta (reprezentowanego jako Organizacja) wszystkie operacje, które może wykonać ten Klient. Oczywiście niezbędne jest także zapewnienie mechanizmów, które pozwolą administratorom na modyfikację (dodanie, usunięcie) powiązań Partnerów z Organizacjami, a także klasyfikowanie Partnerów zgodnie z ich statusem (np. Klient standardowy, Partner, Złoty Partner itp.) w celu określenia przysługującego im poziomu upustów.

W związku z przetwarzaniem w ramach projektowanego rozwiązania danych osobowych, niezbędne jest odpowiednie zaadresowanie wymagań stawianych przez Ustawę o ochronie danych osobowych (wraz z aktami wykonawczymi). Oznacza to między innymi, że należy prowadzić rejestry zdarzeń związanych z przetwarzaniem tych danych, a także umożliwiać wgląd do tych rejestrów uprawnionym organom. Rejestry takie powinny wchodzić w skład Podsystemu SSO. Oczywiście pozostałe Podsystemy powinny także stosować rozwiązania techniczne i organizacyjne wynikające z przetwarzania danych osobowych i rejestrować zdarzenia w prowadzonych rejestrach. Zamawiający oczekuje, że kwestie ochrony danych osobowych (zarówno w wymiarze technicznym - poprzez wprowadzenie odpowiednich funkcjonalności i zabezpieczeń, jak i organizacyjnym) zostaną zaadresowane w przygotowanych przez Wykonawcę produktach, w szczególności w Projekcie Technicznym Systemu, opracowanych procedurach i wytycznych ich realizacji oraz polityce bezpieczeństwa.

Wszystko to sprawia, że zbudowanie Podsystemu SSO jest dość złożonym zagadnieniem, w znacznym stopniu zależnym od docelowej architektury i wykorzystywanych komponentów. W związku z tym Zamawiający oczekuje, że Wykonawca zapewni w ramach SSO spójne rozwiązanie, uwzględniające

kwestie zarządzania użytkownikami, grupami, organizacjami, rolami oraz uprawnieniami do poszczególnych funkcjonalności oraz zasobów we wszystkich Podsystemach, a jednocześnie pozwalające na wykorzystanie wszystkich cech modeli uprawnień dostarczanych przez poszczególne Podsystemy.

5.1.4.8. Portal

Jednym z głównych kanałów sprzedaży Usług IaaS i PaaS na rynku jest Internet. Podsystem Portal ma stanowić pierwszy punkt styku Internautów - potencjalnych Klientów - z ofertą świadczonych Usług i jako taki jest krytyczny dla biznesu Zamawiającego.

Najistotniejszym elementem Podsystemu Portal jest profesjonalny, nowoczesny interfejs użytkownika, zaprojektowany zgodnie z zasadami użyteczności i nastawiony na maksymalizację wyników sprzedażowych, przy jednoczesnym zachowaniu czytelności i intuicyjności interfejsu. Nie bez znaczenia jest też łatwość obsługi serwisu przez użytkowników wewnętrznych (operatorów), którzy będą odpowiadać za zarządzanie i utrzymanie serwisu WWW, tworzenie treści itp.

Klienci powinni otrzymać zbiór narzędzi, które pozwolą im zapoznać się z pełną ofertą produktową. Oznacza to, że Podsystem Portal musi dysponować mechanizmami ułatwiającymi przeszukiwanie, filtrowanie i analizowanie oferty produktowej, szacowanie kosztów Usług i składanie zamówień. Jednocześnie należy uwzględnić potrzeby poszczególnych grup docelowych, tworząc sprofilowane pod te grupy obszary Portalu.

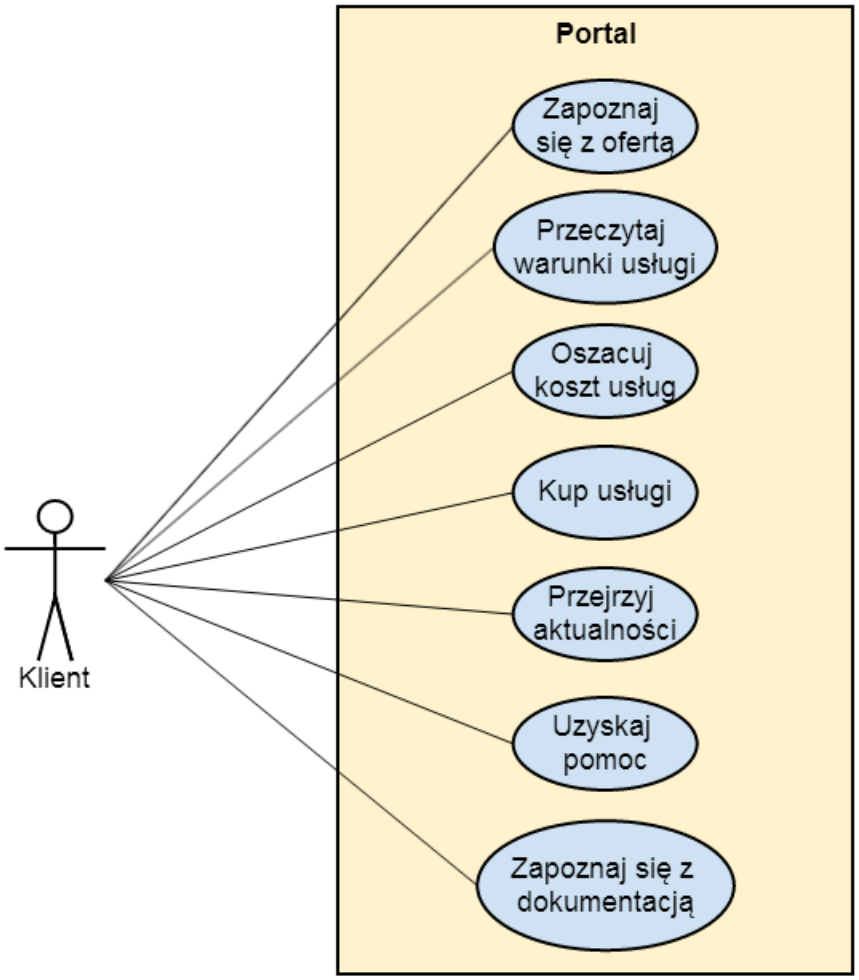


Diagram: Najistotniejsze potrzeby Klientów w kontekście Podsystemu Portal

Portal musi być zintegrowany z Podsystemami SelfService i Billing, tak, by zapewnić użytkownikowi spójny proces sprzedażowy. Szczegółowy opis tego procesu powinien być elementem przeprowadzonych przez Wykonawcę analiz i opracowania projektu technicznego, z uwzględnieniem procesów związanych z takimi elementami, jak fakturowanie czy płatności. W projekcie technicznym należy też zaproponować podział odpowiedzialności poszczególnych Podsystemów (Portal, SelfService, Billing) za realizację poszczególnych kroków procesu zakupowego, obsługę promocji i rabatów, obsługę naliczania podatków (w tym przy sprzedaży międzynarodowej) i przeliczania kursów walut, fakturowanie, określanie dostępności produktów itp.

Portal, poza obsługą sprzedaży, powinien pełnić także funkcję informacyjną, zaczynając od publikacji aktualności, poprzez udostępnianie informacji technicznych, a kończąc na umożliwieniu dostępu do Bazy Wiedzy. Ponadto powinien dysponować pełno tekstową wyszukiwarką, umożliwiającą znalezienie potrzebnych informacji zarówno w Portalu, jak i w innych Podsystemach.

Jako, że we wdrażanym rozwiązaniu istotną rolę będzie pełnić także możliwość obsługi Partnerów, Portal powinien dysponować dedykowaną sekcją przeznaczoną dla Partnerów, w ramach której będą oni mogli zapoznać się z informacjami na temat programu partnerskiego i wypełnić wniosek o przystąpienie do programu partnerskiego, wraz z akceptacją regulaminu i umowy on-line. Obsługa Podsystemu musi dysponować mechanizmami pozwalającymi taki wniosek zaakceptować albo odrzucić.

System CMS, na którym będzie bazować Portal, musi być elastyczny. Oznacza to, że musi umożliwiać definiowanie różnych rodzajów treści oraz określanie atrybutów, jakie mogą opisywać te treści. Przykładowo, dla konkretnego rodzaju treści może być konieczne dodanie atrybutu przechowującego obrazek, tekst albo liczbę. Ponadto system musi zapewniać możliwość tworzenia widoków, przedstawiających wybrane atrybuty treści w sposób posortowany lub wyfiltrowany według określonych przez administratora kryteriów. Mechanizm ten powinien także umożliwiać filtrowanie i sortowanie samym użytkownikom końcowym, by można było tworzyć przeszukiwalne i sortowalne przez tych użytkowników listy i raporty.

Przy wdrażaniu Portalu istotna jest także wygoda jego użytkowania z perspektywy osób odpowiedzialnych za jego utrzymanie. Należy tutaj zwrócić uwagę na umożliwienie wygodnego wprowadzania treści w oparciu o edytor WYSIWYG, a także na możliwość ich kategoryzowania (wg kilku niezależnych kategorii terminów) i tagowania (wg kilku niezależnych kategorii tagów). Jako “kategorie terminów” należy tutaj rozumieć zbiory zorganizowanych w strukturę drzewiastą lub płaską terminów, które można przypisywać do poszczególnych treści. Dany rodzaj treści może mieć przypisane zero lub więcej kategorii, z których użytkownik może wybrać terminy opisujące daną treść. Natomiast jako “tagowanie” należy rozumieć mechanizm opisywania treści dowolnymi słowami kluczowymi, zapewniający możliwość podpowiadania tagów podczas pisania, jeśli tagi zawierające wpisane znaki były już użyte w Podsystemie. Oczywiście istnieje potrzeba tworzenia “kategorii tagów”, funkcjonujących analogicznie do kategorii terminów.

Ponadto konieczne jest zapewnienie, że operator będzie mógł umieścić tworzone strony w odpowiednim miejscu struktury serwisu, bazując zarówno na strukturze menu, jak i kategoriach treści i tagów. Te elementy, jak również pozostałe atrybuty treści, powinny być także brane pod uwagę przy automatycznym generowaniu semantycznych adresów URL.

Istotne jest też zoptymalizowanie Podsystemu do współpracy z przeglądarkami internetowymi (SEO). Jednym z elementów wpływających na SEO jest zapewnienie, by jedna treść była widoczna tylko pod jednym adresem URL. Nie wyklucza to tworzenia dodatkowych adresów (aliasów) dla treści - w takim przypadku Podsystem powinien automatycznie przekierowywać użytkownika wykorzystującego alias do podstawowego adresu URL tej treści, wykorzystując odpowiednie mechanizmy określone w protokole HTTP (np. status 301 / 302).

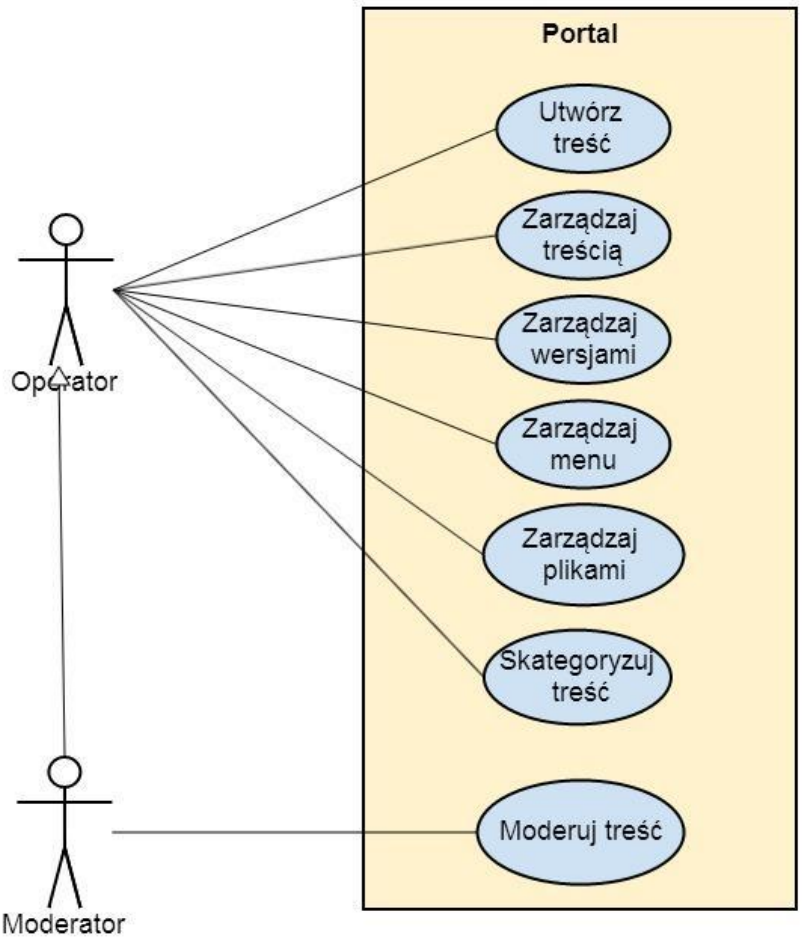


Diagram: Najistotniejsze potrzeby użytkowników wewnętrznych w kontekście Podsystemu Portal

Dużym wyzwaniem jest odpowiednia prezentacja w serwisie poszczególnych produktów. Należy uwzględnić tutaj takie kwestie, jak różne waluty i sposoby opodatkowania sprzedaży w zależności od lokalizacji Klienta, duża różnorodność świadczonych Usług i - co za tym idzie - konieczność ustalania cen według skomplikowanych kryteriów, a także możliwość uzależnienia ceny Usługi od dodatkowych parametrów, jak na przykład poziom SLA czy dodatkowe usługi zarządzania (managed hosting). Stąd istnieje konieczność kompleksowego spojrzenia na zagadnienie definiowania i publikacji produktów, z uwzględnieniem punktów styku z Podsystemami takimi jak Billing czy SelfService.

Z perspektywy Klienta niezbędne jest też przygotowanie kalkulatora umożliwiającego oszacowanie kosztów korzystania z poszczególnych Usług. Zbudowanie takiego narzędzia również wymaga współpracy Portalu z Podsystemami Billing i SelfService.

Duży wpływ na ostateczny kształt tej części Portalu będzie miała także przeprowadzona przez Wykonawcę analiza mająca na celu doprecyzowanie informacji o produktach oferowanych przez

Zamawiającego, opisanych w niniejszym OPZ. W wyniku tej analizy Wykonawca zbuduje szczegółowy katalog produktów, definiujący szczegółowo poszczególne cechy produktów wraz z ich modelami rozliczeń (billingowania), a także opracuje opisy poszczególnych produktów do opublikowania w ramach Portalu, tak, by w dniu odbioru końcowego Projektu pierwsi Klienci mogli skorzystać ze świadczonych Usług.

Przy precyzowaniu zapisów dotyczących produktów należy zwrócić uwagę na to, by Usługi IaaS i PaaS efektywnie wykorzystywały dostarczone w ramach Projektu zasoby i były dostosowane do potrzeb rynkowych. Precyzując modele rozliczeń należy uwzględnić w szczególności cechy takie, jak okresy rozliczeniowe czy łączenie Usług w pakiety, biorąc pod uwagę możliwości dostarczanego Podsystemu Billing. Założenia w tym zakresie powinny bazować na przeprowadzonym przez Wykonawcę badaniu konkurencji i potrzeb grup docelowych dla IaaS i PaaS.

W celu zapewnienia integralności i rozliczalności, a także umożliwienia dostępu do wersji archiwalnych treści, Portal powinien wersjonować wszystkie zmiany treści, a także umożliwiać porównanie dwóch wersji treści ze sobą. Z tej perspektywy istotne mogą też się okazać mechanizmy moderacji treści, pozwalające na zbudowanie dwustopniowego procesu publikacji treści (utworzenie treści, opublikowanie treści) i - w efekcie - podwyższenie jakości treści publikowanych na Portalu.

Konieczne jest zapewnienie mechanizmów obsługi wielojęzyczności treści, menu, kategorii, tagów, wyświetlanych komunikatów itp. Należy zapewnić także mechanizmy automatycznego wyboru odpowiedniej wersji językowej i waluty w zależności od użytkownika korzystającego z serwisu. Jednocześnie trzeba zadbać o to, by treści serwisu były właściwie indeksowane przez wyszukiwarki internetowe.

Duży nacisk należy położyć na zbieranie danych o zachowaniach użytkowników w ramach Portalu. Oznacza to nie tylko integrację z profesjonalną, sprawdzoną platformą do obsługi statystyk odwiedzin serwisu internetowego, ale także gromadzenie wszelkich informacji na temat zachowania użytkowników, takich, jak na przykład parametry szacowania kosztów wykorzystywane przez Klientów. Należy przy tym zadbać o ochronę prywatności użytkowników, szczególnie w kontekście *Ustawy o ochronie danych osobowych*.

Portal musi także umożliwiać efektywną komunikację z Klientem. Oznacza to, że powinien być zintegrowany z Podsystemem Trouble Ticketing w zakresie umożliwiającym efektywną komunikację z użytkownikami nieposiadającymi konta, a także dostarczać narzędzia umożliwiające budowanie ankiet czy formularzy elektronicznych.

5.1.4.9. Katalog Usług

Aby zwiększyć konkurencyjność świadczonych Usług poprzez promowanie produktów Klientów, Zamawiający zamierza uruchomić elektroniczny katalog e-usług. Klienci Zamawiającego będą mogli dodawać do katalogu informacje o świadczonych przez siebie e-usługach.

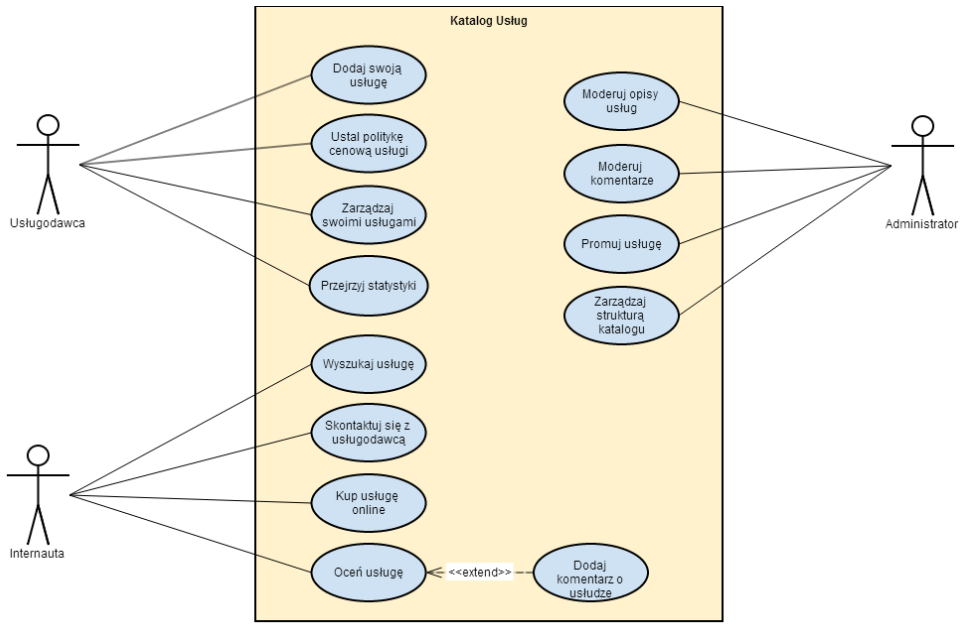


Diagram: Najistotniejsze potrzeby użytkowników w kontekście Katalogu Usług

Projektując Katalog Usług należy dokładnie przeanalizować potrzeby potencjalnych Usługodawców. Powinni mieć oni możliwość dodania i modyfikacji świadczonych przez siebie usług, definiowania dla nich polityki cenowej czy analizy statystyk dotyczących tych usług. Z kolei Internauci zainteresowani usługami powinni móc łatwo do nich dotrzeć. Oznacza to, że należy nie tylko zadbać o możliwość zbudowania elastycznej struktury katalogu, w ramach której poszczególne usługi mogą być w sposób jednoznaczny zaklasyfikowane, ale także o skutecznie działającą wyszukiwarkę usług, pozwalającą filtrować wyniki względem atrybutów opisujących poszczególne usługi. Poprawne wykonanie Katalogu Usług wymaga zatem od Wykonawcy przeprowadzenia kompleksowej analizy z perspektywy zarówno istniejących potrzeb w tym obszarze, stosowanych praktyk rynkowych, jak i użyteczności dostarczanego rozwiązania.

Niezwykle istotne jest zapewnienie odpowiedniej promocji Katalogu Usług w Internecie. Należy tutaj rozważyć kwestie optymalizacji serwisu na potrzeby wyszukiwarek internetowych czy też mechanizmy współpracy z sieciami społecznościowymi.

Jako, że Katalog Usług będzie wydzielonym, specjalizowanym bytem, zakłada się, że będzie dostępny pod innym niż Portal adresem domenowym. Niemniej jednak, oczekuje się, że będzie oparty na tym samym oprogramowaniu, co Portal, tak, by w Katalogu Usług można było skorzystać z funkcjonalności przygotowanych na potrzeby Portalu, a w Portalu - z funkcjonalności przygotowanych dla Katalogu Usług.

5.1.4.10. Baza Wiedzy

Dla potrzeb gromadzenia i zarządzania informacjami i dokumentacją zostanie przez Wykonawcę wdrożony Podsystem wyposażony w mechanizmy bazy wiedzy, przy czym należy wyróżnić Bazę Wiedzy na potrzeby wewnętrzne (dla obsługi Klienta, administratorów itp) oraz Bazę Wiedzy dla Klientów. Oznacza to, że konieczne będzie posadowienie dwóch instancji tego rozwiązania.

Baza Wiedzy powinna być narzędziem typu Wiki umożliwiającym łatwe tworzenie ustrukturyzowanych, zorganizowanych tematycznie zbiorów informacji. Kluczowe jest tutaj zapewnienie jak najłatwiejszego dostępu do zebranych informacji, ich przeszukiwania, poprawiania i uzupełniania.

Ponieważ Baza Wiedzy ma zostać wykorzystana między innymi do opublikowania całej dokumentacji użytkowej i procedur eksploatacyjnych wytworzonych w projekcie, należy zadbać o to, by wdrożona Baza Wiedzy posiadała wszystkie cechy niezbędne do osadzenia tam dużych, złożonych dokumentów, jak: generowanie spisów treści, obsługa styli akapitów, obsługa grafik i załączników, możliwość wydruku zarówno aktualnej strony jak i podstron, generowania dokumentów .pdf itp.

Bardzo istotne jest umożliwienie łatwego odnalezienia informacji zgromadzonych w Bazie Wiedzy. To od tej cechy - a także od łatwości wprowadzania informacji - zależy, czy Podsystem ten spełni swoje zadanie. Dlatego należy zapewnić wszelkie możliwe mechanizmy, by ułatwić nawigację w Podsystemie, zaczynając od zbudowania odpowiedniej struktury informacji, poprzez odpowiednie narzędzia nawigacyjne jak tagi czy narzędzia do kategoryzacji treści, aż po zaawansowane mechanizmy wyszukiwania pełno tekstowego. Nie bez znaczenia jest też właściwa współpraca z wyszukiwarkami internetowymi.

Przy wdrażaniu Bazy Wiedzy istotna jest także wygoda jej użytkowania z perspektywy osób odpowiedzialnych za jej utrzymanie. Należy tutaj zwrócić uwagę na umożliwienie wykorzystania wygodnego sposobu wprowadzania treści w oparciu o edytor WYSIWYG, a także na możliwość ich kategoryzowania (wg kilku niezależnych kategorii) i tagowania. Ponadto konieczne jest zapewnienie, że będzie można w łatwy sposób umieścić tworzone strony w odpowiednim miejscu struktury Bazy Wiedzy.

W celu zapewnienia integralności i rozliczalności, a także umożliwienia dostępu do wersji archiwalnych treści, Podsystem powinien wersjonować wszystkie zmiany treści, a także umożliwiać porównanie dwóch wersji treści ze sobą. Z tej perspektywy istotne mogą też się okazać mechanizmy moderacji treści, pozwalające na zbudowanie dwustopniowego procesu publikacji treści (utworzenie treści, opublikowanie treści) i - w efekcie - podwyższenie jakości treści publikowanych w Bazie Wiedzy.

5.1.4.11. Trouble Ticketing

Podsystem Trouble Ticketing (często także zwany Issue Ticketing, Incident Tracking, itp) służy do śledzenia i zarządzania zgłoszeniami (issues/tickets). Podsystem powinien wspierać zarówno zgłoszenia Klientów jak i zgłoszenia wewnętrzne pracowników Zamawiającego. Co więcej, Wykonawca ma wykorzystywać ten Podsystem na etapie realizacji projektu do zarządzania procesem analitycznym, projektowym, wytwórczym i wdrożeniowym. Oznacza to w szczególności, że Zamawiający wymaga iż wszystkie informacje o przebiegu tych procesów będą rejestrowane w Podsystemie Trouble Ticketing. Co więcej, analiza wymagań także powinna opierać się na tym Podsystemie, by zapewnić pełną śledzalność całego cyklu życia wymagania, od jego wprowadzenia, poprzez analizę, implementację, testy, aż po wdrożenie i późniejsze utrzymanie.

Z perspektywy Klienta korzystającego z Usług świadczonych przez Zamawiającego, Trouble Ticketing powinien umożliwiać swobodne tworzenie zgłoszeń i nadzór nad ich realizacją. Jednocześnie zgłoszenia powinny być powiązane z zasobami, których dotyczą, a także wymagać wypełnienia pól właściwych dla wybranego zasobu, tak, by utworzone zgłoszenie zawierało potrzebne do jego rozwiązania dane i nie wymagało dodatkowych ustaleń między obsługą a Klientem.

W ramach zgłoszenia musi też istnieć możliwość komunikacji między Klientem a osobą obsługującą zgłoszenie, na przykład w formie komentarzy do zgłoszenia. Klient powinien także otrzymywać powiadomienia e-mail informujące go o przebiegu realizacji zgłoszenia. Specyfikacja typów zgłoszeń, jakie może utworzyć Klient, szczegółowy zakres informacyjny i logika działania formularza zgłoszeniowego powinna zostać określona w ramach analizy i projektu technicznego.

Cała złożoność implementacji i wdrożenia Podsystemu Trouble Ticketing objawia się w momencie analizy tego Podsystemu z perspektywy użytkowników wewnętrznych. Trouble Ticketing będzie odpowiadał za zarządzanie całym wewnętrznym przepływem pracy u Zamawiającego. Wszystkie procesy biznesowe związane z obsługą Klienta, po ich opracowaniu przez zespół analityczny Wykonawcy, będą zaimplementowane w ramach Podsystemu Trouble Ticketing. Istotne jest zatem, aby - z jednej strony - Podsystem ten był sprawdzony i stabilny, a z drugiej - możliwa była jego rozbudowa, tak, by Wykonawca mógł zaimplementować wszystkie funkcjonalności niezbędne do zrealizowania zaplanowanych procesów. Sama implementacja i modyfikacja procesów biznesowych powinna być bardzo łatwa, tak, by ewentualne zmiany w tym zakresie można było łatwo wdrożyć.

Podsystem z perspektywy pracowników obsługi Klienta powinien zapewniać łatwe zapoznanie się ze zgłoszeniem, wstępną diagnostykę zgłoszenia, a także komunikowanie się w ramach zgłoszenia - zarówno w zakresie komunikacji wewnętrznej (np. z administratorem), jak i zewnętrznej (z Klientem). Cały przebieg obsługi zgłoszenia powinien być dokumentowany, a czas pracy nad zgłoszeniem raportowany przez pracowników. Istotne jest też umożliwienie oddelegowania zgłoszenia do innych pracowników, i to zarówno w sposób manualny, jak i automatyczny, na podstawie odpowiednich

reguł biznesowych.

Pracownicy obsługi Klienta powinni pobierać zgłoszenia do obsługi z kolejek zgłoszeń. Konfiguracja kolejek powinna zapewniać właściwą priorytetyzację prac z uwzględnieniem ich istotności i konieczności zachowania odpowiedniego poziomu obsługi SLA. Niezbędne jest także umożliwienie monitorowania i raportowania przypadków przekroczeń SLA oraz zbieranie i raportowanie danych statystycznych, na podstawie których kierownictwo będzie mogło wyciągać wnioski dotyczące przebiegu poszczególnych procesów. W niektórych przypadkach może być też konieczne wyznaczenie kierownika pewnego obszaru merytorycznego, który będzie odpowiadał za przydzielenie zgłoszenia do konkretnych pracowników.

Przydatnym elementem rozwiązania Trouble Ticketing jest panel kontrolny (dashboard), na którym użytkownicy mogą osadzać widgety, czyli małe aplikacje o ograniczonej funkcjonalności, które są instalowane i uruchamiane jako wydzielony blok na stronie panelu kontrolnego. Przykładami zastosowania widgetów są choćby spis wszystkich zadań przypisanych do aktualnie zalogowanego użytkownika, wyniki wyszukiwania według zdefiniowanych przez użytkownika kryteriów wyszukiwania zgłoszeń (np. zgłoszenia przeterminowane) czy też wykres prezentujący postępy prac.

Istotnym elementem wdrożenia Trouble Ticketing jest jego integracja z pozostałymi elementami rozwiązania. Chodzi o to, by pracownik obsługi Klienta z jednego miejsca miał bezpośredni dostęp do wszystkich informacji niezbędnych do pracy nad zgłoszeniem. Przykładowo, zgłoszenia dotyczące sposobu działania Usługi powinny mieć w Podsystemie Trouble Ticketing wyświetlone informacje na temat tej Usługi. Dodatkowo w interfejsie powinien znajdować się odnośnik, pozwalający pracownikowi przejść bezpośrednio do widoku odpowiedniego obiektu (Usługi, konta itp.) we właściwym Podsystemie dziedzinowym.

Aby praca ze zgłoszeniami była efektywna, konieczne jest właściwe zdefiniowanie poszczególnych ekranów, które będą wykorzystywane przez pracowników. Podsystem musi zatem umożliwiać nie tylko zdefiniowanie rodzajów zgłoszeń i atrybutów je opisujących (jak np. priorytet, stosowany do jego obsługi proces czy też dodatkowe pola danych dostępne w danym rodzaju zgłoszenia), ale także umożliwiać zaprojektowanie ekranów, które będą wyświetlane pracownikom przy przejściu między poszczególnymi statusami zgłoszenia.

Biorąc to wszystko pod uwagę a także fakt, że Podsystem Trouble Ticketing będzie konieczny już w pierwszych tygodniach projektu, Zamawiający preferuje wykorzystanie gotowego, dostępnego na rynku produktu o sprawdzonej renomie, który na dzień złożenia oferty będzie spełniać wszystkie wymagania oznaczone w niniejszym dokumencie jako obowiązujące dla pierwszej wersji Podsystemu Trouble Ticketing. Oczywiście wykorzystanie gotowego produktu nie zwalnia Wykonawcy z obowiązku dostosowania go do potrzeb i oczekiwań Zamawiającego.

5.2. Szczegółowe wymagania dla poszczególnych Podsystemów

5.2.1. Wymagania wspólne

Wszystkie wymagania zostały przedstawione w odpowiednich kategoriach, a dodatkowo dla wszystkich Podsystemów została przygotowana tabela zawierająca wymagania wspólne. W tej tabeli każde z wymagań ma zobrazowane przypisanie do poszczególnych Podsystemów w postaci wpisu "TAK" w odpowiedniej kolumnie przynależnej do danego rozwiązania. Wpis ten jednoznacznie określa, że wymaganie to musi być uwzględnione w zakresie prac i dotyczy odpowiedniego Podsystemu, co oznacza że musi być w jego przypadku zrealizowane. Analogicznie brak wpisu "TAK" jednoznacznie określa, że Podsystem nie musi, lub nawet nie jest w stanie danego wymagania realizować.

Należy zaznaczyć, że zadaniem Wykonawcy jest zrealizowanie opisanych w niniejszym dokumencie potrzeb Zamawiającego i poszczególnych użytkowników Systemu, przy jednoczesnym spełnieniu wskazanych technicznych wymagań minimalnych. Oznacza to, że wymagań tych nie należy traktować w sposób zawężający zakres Projektu.

ID wymagania	Treść wymagania	Dotyczy													
		NOC: zarządz.	NOC: monit.	NOC: DCIM	Centralny system logów	IaaS	PaaS	SSO	Portal	Katalog Usług	Baza Wiedzy	Trouble Ticketing	Self Service	Billing	Cloud API
	Wymagania prawne														
SOFT.WW.1	Na dzień odbioru, musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi, wskazanymi w OPZ rozdział 3 w obszarze świadczenia Usług w formie elektronicznej.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.2	Na dzień odbioru, musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi, wskazanymi w OPZ rozdział 3 w obszarze świadczenia Usług IaaS i PaaS na potrzeby sektora medycznego.		TAK		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.3	Na dzień odbioru, musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi, wskazanymi w OPZ rozdział 3 w obszarze świadczenia Usług IaaS i		TAK		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	PaaS na potrzeby sektora administracji publicznej.														
SOFT.WW.4	Na dzień odbioru, musi zapewnić zgodność z obowiązującymi krajowymi i międzynarodowymi regulacjami prawnymi, wskazanymi w OPZ rozdział 3 w obszarze świadczenia Usług IaaS i PaaS na potrzeby sektora edukacyjnego.		TAK		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.5	Musi informować użytkownika o używaniu Cookies zgodnie z obowiązującymi przepisami prawa.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Dobre praktyki														
SOFT.WW.6	Wszystkie decyzje Projektowe powinny być podejmowane zgodnie z dobrymi praktykami, w oparciu o normy, wytyczne, standardy i rekomendacje wydane przez uznane instytucje i za zgodą Zamawiającego, zgodnie z aktami prawnymi wskazanym w OPZ rozdział 3.														
	Stos technologiczny														
SOFT.WW.7	Podsystem musi być zrealizowany w architekturze cienkiego klienta.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

SOFT.WW.8	Wszystkie funkcje Podsystemu przeznaczone dla użytkowników (w tym klientów i administratorów) powinny być dostępne za pomocą interfejsu Web	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.9	Wszystkie funkcje Podsystemu (wszystkie wymagania funkcjonalne) powinny być dostępne za pomocą API (np.w technologii REST, SOAP itp). Konkretne technologie API zostaną ustalone na etapie opracowywania projektu technicznego.		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.10	Interfejs GUI Podsystemu musi być zrealizowany w postaci stron HTML 4.0, HTML 5 lub XHTML 1.0 lub nowszy.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.11	Podsystemy powinny wykorzystywać kodowanie znaków UTF-8		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.12	GUI Podsystemu nie może wykorzystywać technologii Adobe Flash	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.13	Podsystem nie może	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	wykorzystywać technologii Adobe Flex														
SOFT.WW.14	GUI Podsystemu nie może wykorzystywać apletów Java	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.15	GUI Podsystemu może wymagać od przeglądarki użytkownika włączonej obsługi technologii Javascript	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.16	GUI Podsystemu może wymagać od przeglądarki użytkownika włączonej obsługi Cookies	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.17	GUI Podsystemu może wymagać od przeglądarki użytkownika obsługi technologii CSS 2	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.18	GUI Podsystemu powinno być zoptymalizowane do pracy w przeglądarce Chrome (najnowsza stabilna wersja dostępna na rynku na dzień przekazania do testów akceptacyjnych)	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.19	GUI Podsystemu musi być zoptymalizowany do pracy w przeglądarce Firefox (najnowsza	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	stabilna wersja dostępna na rynku na dzień przekazania do testów akceptacyjnych)														
SOFT.WW.20	GUI Podsystemu powinno być zoptymalizowane do pracy w przeglądarce Internet Explorer w wersji 10 i nowszej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.21	GUI Podsystemu musi być zoptymalizowany do pracy w przeglądarce Safari (najnowsza stabilna wersja dostępna na rynku na dzień przekazania do testów akceptacyjnych)	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.22	GUI Podsystemu powinno być zoptymalizowane do pracy na telefonach komórkowych. Zamawiający oczekuje zweryfikowania poprawności działania dla co najmniej 5 różnych urządzeń. Lista urządzeń zostanie ustalona na etapie przygotowywania projektu technicznego.		TAK			TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.23	GUI Podsystemu powinno być		TAK	TAK		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	zoptymalizowane do pracy na tabletach. Zamawiający oczekuje zweryfikowania poprawności działania dla co najmniej 5 różnych urządzeń. Lista urządzeń zostanie ustalona na etapie przygotowywania projektu technicznego.														
SOFT.WW.24	Każda ze stron GUI Podsystemu powinna bezbłędnie przejść walidację z wykorzystaniem usług dostarczanych przez organizację w3.org, co najmniej w zakresie kodu HTML i CSS.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.25	Komunikacja HTTP powinna odbywać się po protokole szyfrowanym SSL/TLS - Zamawiający dostarczy certyfikaty SSL.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.26	Podsystem musi poprawnie obsługiwać rozszerzenie SNI (Server Name Indication) protokołu HTTPS					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.27	Wszystkie strony/podstrony GUI wytworzone w ramach danego Podsystemu				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	powinny być zrealizowane za pomocą ujednoliconego framework front-end (w obrębie danego systemu - ten sam framework nie musi być wykorzystywany we wszystkich Podsystemach)														
SOFT.WW.28	Wszystkie strony/podstrony danego Podsystemu wytworzone w ramach Projektu powinny być generowane przez szablony (templates).				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.29	Podsystemy realizujące wizualizację za pomocą wykresów, powinny w tym zakresie wykorzystywać technologie JavaScript, HTML i CSS.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.30	Każdy URL Podsystemu (strona, podstrona, adres API) musi być skonstruowany jako friendly url (clean url)		TAK	TAK				TAK	TAK	TAK	TAK		TAK		TAK
SOFT.WW.31	Każdy URL Podsystemu (strona, podstrona, adres API) musi być skonstruowany jako semantic url		TAK	TAK				TAK	TAK	TAK	TAK		TAK		TAK

SOFT.WW.32	Podsystem musi obsługiwać protokół IP w wersji 6 (IPv6).	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.33	Podsystem musi podlegać kopiom zapasowym (backup) i umożliwiać odtworzenie jego stanu sprzed awarii na podstawie tych kopii.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Tłumaczenia														
SOFT.WW.34	Podsystem musi obsługiwać wiele języków interfejsu użytkownika.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.35	Podsystem musi zawierać pełne tłumaczenie wszystkich tekstów na język polski.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.36	Podsystem musi zawierać pełne tłumaczenie wszystkich tekstów na język angielski.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.37	Podsystem musi umożliwiać dodanie tłumaczeń dla nowych języków, przy czym funkcjonalność ta nie musi być realizowana przez GUI.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.38	Podsystem musi umożliwiać modyfikację istniejących tłumaczeń, przy czym					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	funkcjonalność ta nie musi być realizowana przez GUI.														
SOFT.WW.39	Podsystem musi obsługiwać wiele walut.								TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.40	W momencie odbioru System musi obsługiwać waluty PLN, EUR, USD.								TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.41	Podsystem musi umożliwiać rozszerzanie listy obsługiwanych walut.								TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.42	Podsystem musi być w pełni zlokalizowany, w szczególności zapewniać formatowanie daty i czasu, formatowanie liczb, obsługę separatorów dziesiętnych itp. zgodnie z aktualnym językiem interfejsu.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	API każdego z Podsystemów														
SOFT.WW.43	Wszystkie funkcjonalności Podsystemu dostępne przez interfejs użytkownika muszą być także dostępne z poziomu API.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.44	Uwierzytelnianie wywołań API powinno przebiegać za pomocą integracji z					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	Podsystemem SSO.														
SOFT.WW.45	Dane w wywołaniach API powinny być przesyłane w formacie JSON lub XML.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.46	Żadna z funkcjonalności Podsystemu nie powinna być realizowana za pomocą mechanizmu IFrame (osadzania w ramkach). Jeżeli istnieje potrzeba skorzystania z innego Podsystemu należy dokonać z nim integracji za pomocą API bądź wymusić przejście do tego Podsystemu przez użytkownika. Zamawiający może wyrazić zgodę na odstępstwo od tej zasady i użycie mechanizmu IFrame, jeśli jest to niezbędne do integracji z systemami nie będącymi przedmiotem dostawy w ramach Umowy, które nie udostępniają odpowiedniego API.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Uprawnienia														
SOFT.WW.47	Platforma oprogramowania musi mieć zaimplementowany	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	model uprawnień spójny między Podsystemami, uwzględniający minimum użytkowników, grupy, organizacje i role użytkowników.														
SOFT.WW.48	Platforma oprogramowania musi zawierać spójne i łatwe w obsłudze mechanizmy zarządzania uprawnieniami z poziomu GUI.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.49	Platforma oprogramowania musi umożliwiać delegowanie uprawnień do funkcjonalności/uprawnień/zasobów między użytkownikami.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.50	Podsystem musi zapewnić mechanizm ról, agregujących uprawnienia przypisane do użytkowników bądź grup.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.51	Podsystem musi umożliwiać nadanie uprawnień do poszczególnych funkcjonalności.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.52	Podsystem musi umożliwiać nadanie uprawnień do realizacji	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	konkretnych operacji na każdym obiekcie przetwarzanym w Podsystemie (np. prawo restartu konkretnej maszyny wirtualnej, prawo edycji konkretnego użytkownika itp.)														
SOFT.WW.53	Podsystem musi umożliwiać nadawanie Partnerom uprawnień do administrowania zasobami konkretnego klienta.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Eksport danych														
SOFT.WW.54	Wszystkie operacje eksportu danych (w tym raporty) powinny umożliwiać zapisanie jego wyników w formacie XML.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.55	Wszystkie operacje eksportu danych (w tym raporty) powinny umożliwiać zapisanie jego wyników w formacie CSV poprawnie obsługiwanym przez aplikację MS Excel 2010.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.56	Wszystkie operacje eksportu danych (w tym raporty) powinny umożliwiać zapisanie		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	jego wyników w formacie PDF.														
	Utrzymanie i logi														
SOFT.WW.57	Jeżeli Podsystem działa jako usługa systemowa (deamon), musi on zapewniać skrypty startowe dla systemu operacyjnego (wskazanego przez Zamawiającego), zapewniające następujące komendy: - start - start Podsystemu, - stop - zatrzymanie Podsystemu, - status - informacje czy Podsystem działa czy też nie, - restart - restart Podsystemu, - force-stop - bezwzględne zatrzymanie wszystkich procesów Podsystemu, - check-config - weryfikacja poprawności plików konfiguracyjnych Podsystemu. W przypadku błędu należy wskazać linię oraz typ błędu, numer błędu (tak aby można było zgłaszać	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	dostawcy numery błędów i nie wymagał on dalszych informacji od Zamawiającego) oraz opis w formie zrozumiałej dla administratora.														
SOFT.WW.58	Podsystem musi zapewniać zapisywanie logów do centralnego systemu logów, dostarczanego w ramach Platformy oprogramowania, niezależnie od prowadzenia ewentualnych wewnętrznych rejestrów zdarzeń.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.59	Podsystem musi umożliwiać (w zależności od ustawień konfiguracyjnych) generowanie logów na poziomie logowania DEBUG - logi szczegółowe nt. działania Podsystemu (każdej wykonywanej operacji)	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.60	Podsystem musi umożliwiać (w zależności od ustawień konfiguracyjnych) generowanie logów na	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	poziomie logowania INFO - logi biznesowe nt. działania Podsystemu.														
SOFT.WW.61	Podsystem musi umożliwiać (w zależności od ustawień konfiguracyjnych) generowanie logów na poziomie logowania ERROR - każdy błąd jaki wystąpi w Podsystemie musi być zalogowany w trybie ERROR wraz z pełnym stacktrace błędu oraz informacją zrozumiałą dla administratora nt. błędu.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.62	Wszystkie komunikaty logów zapisywane w centralnym systemie logów muszą być w języku angielskim.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.63	Podsystem musi umożliwiać włączenie lub wyłączenie poszczególnych poziomów logowania w konfiguracji tego Podsystemu.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Instalacja, konfiguracja i uaktualnienia														
SOFT.WW.64	Instalacja bądź aktualizacja Podsystemu powinna być realizowana przez	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	pakiety systemowe systemu operacyjnego określonego jako docelowa platforma dla Podsystemu w ramach projektu technicznego														
SOFT.WW.65	Dla każdego z Podsystemów powinno być określone źródło automatycznego pobierania aktualizacji systemowych	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.66	Każdy Podsystem wymagający konfiguracji po instalacji bądź aktualizacji musi dostarczać do tego celu receptury wykorzystywanego w Rozwiązaniu mechanizmu zarządzania/orkiestracji (orchestration) - np. Ansible, SaltStack itp.		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.67	Wdrażanie konfiguracji przez mechanizm orkiestrujący powinno odbywać się przez jej pobranie z centralnego systemu kontroli wersji (VCS).				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.68	Wykonawca musi wdrożyć oprogramowanie				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	umożliwiające monitoring i zarządzanie Podsystemami (np. start, stop, restart usługi) z poziomu panelu administracyjnego.														
SOFT.WW.69	Wszystkie Podsystemy powinny zawierać mechanizmy pozwalające na raportowanie poprawności działania ich funkcji biznesowych na potrzeby mechanizmów monitoringu Usług.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.70	Każdy z Podsystemów musi dostarczać konfigurację i być zintegrowany z wdrożonym oprogramowaniem do monitoringu i zarządzania Podsystemami.		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.71	Podsystem musi zapewnić integrację z innymi Podsystemami za pomocą szyny ESB (Enterprise Service Bus).				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.72	GUI Podsystemu musi udostępniać aktualny numer wersji, historię wersji wraz z opisem	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	zmian dokonanych w każdej z wersji.														
	Wysoka dostępność														
SOFT.WW.73	Podsystemy powinny być zbudowane i wdrożone w sposób zapewniający ich wysoką dostępność, zgodnie z parametrami określonymi w Umowie.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.74	Mechanizmy wysokiej dostępności powinny być skonstruowane w sposób nie wymagający ręcznej ingerencji człowieka dla co najmniej 90% rozpatrywanych scenariuszy awarii.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Wymagania bezpieczeństwa														
SOFT.WW.75	Podsystem musi spełniać wymagania OWASP Application Security Verification Standard dla poziomu 1					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.76	Jeśli w Podsystemie są przetwarzane dane osobowe, to musi on spełniać wymagania OWASP Application Security Verification Standard dla poziomu 2					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Dokumentacja użytkowa														
SOFT.WW.77	Cała dokumentacja użytkowa powinna być	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	osadzona w ramach Podsystemu Baza Wiedzy.														
SOFT.WW.78	Cała dokumentacja użytkowa powinna zostać dostarczona do odbioru w formie eksportu z bazy wiedzy, z uwzględnieniem wymaganych przez Zamawiającego szablonów dokumentów.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.79	Cała dokumentacja przeznaczona dla użytkowników zewnętrznych powinna zostać dostarczona w języku polskim i angielskim.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.80	Cała dokumentacja przeznaczona dla użytkowników wewnętrznych powinna zostać dostarczona w języku polskim.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.81	Cała dokumentacja przeznaczona dla administratorów powinna zostać dostarczona co najmniej w języku angielskim.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.82	Podsystem musi być wyposażony w pomoc kontekstową,				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	objaśniającą sposób działania każdej strony dostępnej w ramach Podsystemu.														
	Wytwarzanie, ciągła integracja i łatwość utrzymania														
SOFT.WW.83	W przypadku, gdy Podsystem będzie bazował na gotowym produkcie komercyjnym lub open source (CMS, frameworki itp), wszystkie modyfikacje Podsystemu powinny zostać zrealizowane jako pluginy/rozszerzenia tego produktu (niedopuszczalne są modyfikacje "core'a" produktu). Wprowadzenie poprawek bezpośrednio do produktu jest dopuszczalne tylko wtedy, gdy osoba/podmiot utrzymujący dany produkt włączy tę poprawkę do głównej linii produktu. Zamawiający może, w uzasadnionych, udokumentowanych przypadkach, dopuścić wyjątki od tego	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	wymagania.														
SOFT.WW.84	Podsystem musi stosować wersjonowanie zgodnie z Semantic versioning 2.0.					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.85	Wykonawca musi zbudować środowisko integracyjne dla wszystkich Podsystemów.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.86	Testy akceptacyjne Podsystemu powinny zostać zaimplementowane przez Wykonawcę w postaci automatycznych skryptów testowych.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.87	Wprowadzenie jakichkolwiek zmian w którymkolwiek z Podsystemów powinno implikować uruchomienie procedury testów automatycznych wszystkich Podsystemów na środowisku integracyjnym.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.88	Automatyczne uruchomienie testów automatycznych może odbywać się w wyznaczonych konfiguracyjnie oknach czasowych (np. o	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	wskazanej godzinie, we wskazanym dniu tygodnia).														
SOFT.WW.89	Powinna istnieć możliwość ręcznego wymuszenia uruchomienia procedury testów automatycznych na środowisku integracyjnym w momencie wybranym przez użytkownika.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.90	W ramach procedury testów automatycznych środowisko integracyjne powinno zostać zrekonstruowane tak, by odzwierciedlało konfigurację środowiska produkcyjnego w stopniu niezbędnym do przeprowadzenia testów.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.91	W ramach procedury testów automatycznych powinny zostać uruchomione wszystkie testy akceptacyjne.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.92	W ramach procedury testów automatycznych powinny zostać uruchomione wszystkie testy jednostkowe.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.93	W ramach procedury	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	testów automatycznych powinno zostać przeprowadzone porównanie zgodności interfejsu użytkownika na środowisku produkcyjnym i integracyjnym.														
SOFT.WW.94	Procedura testów automatycznych powinna działać w sposób nie wymagający ingerencji człowieka.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.95	W przypadku wykrycia przez testy automatyczne problemów, powinny automatycznie zostać stworzone odpowiednie zgłoszenia w systemie Trouble Ticketing.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Architektura systemowa														
SOFT.WW.96	Podsystem musi uwierzytelniać użytkowników w oparciu o SSO.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.97	Podsystem zarówno w kontekście infrastruktury jak i oprogramowania musi być skalowalny w obrębie wszystkich warstw architektury (skalowalność w poziomie i pionie). W	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	Podsystemie nie mogą występować wąskie gardła stanowiące ograniczenie dla wydajności i skalowania całego Podsystemu.														
SOFT.WW.98	Podsystem może być przygotowany z gotowych Podsystemów realizujących procesy biznesowe, o ile zostaną one dostosowane do potrzeb Zamawiającego.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.99	Architektura Podsystemów musi być oparta o luźno powiązane i możliwe do wielokrotnego użycia usługi.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.100	Architektura Podsystemów musi umożliwiać dalszą jej rozbudowę bez konieczności przebudowy istniejących elementów Systemu.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.101	Podsystem musi zapewniać możliwość wymiany infrastruktury technicznej bez zmiany Podsystemów oprogramowania (w zakresie tej samej architektury sprzętu)		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

SOFT.WW.102	Podsystem musi zapewniać możliwość wprowadzania zmian w oprogramowaniu i infrastrukturze z zachowaniem ciągłości pracy całego Systemu		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.103	Podsystem musi umożliwiać korzystanie z Usług przez Klientów za pomocą interfejsów GUI niezależnie od posiadanej przez nich platformy systemowo-sprzętowej.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.104	Zamawiający wymaga wykorzystania infrastruktury sprzętowej rozwiązania opartej o technologie serwerowe oparte o architekturę x86-64	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.105	Architektura powinna zawierać komponenty wspierające diagnostykę i monitoring całego Systemu (zarówno infrastruktury jak również Podsystemów oprogramowania)				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.106	Podsystem musi być zaprojektowany w podejściu wielowarstwowym.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

SOFT.WW.107	Podsystem musi być zbudowany w oparciu o architekturę uwzględniającą takie cechy jak: - dekompozycja Podsystemu na niezależne komponenty, możliwe do oddzielnej analizy, - możliwość podmiany komponentu z dowolnej warstwy na inny, wykorzystujący ten sam protokół lub standard komunikacji, - możliwość scalenia kolejnych warstw w jedną, z zachowaniem protokołu lub standardu komunikacji, - możliwość podziału danej warstwy w wiele, z zachowaniem protokołu lub standardu komunikacji, - wydzielenie Podsystemów do zadań dedykowanych, - możliwość skalowania zasobów wykorzystywanych przez poszczególne komponenty lub warstwy,				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	- możliwość równoważenia obciążeń, - zapewnienie rozwiązań redundantnych														
SOFT.WW.108	Podsystem musi umożliwiać współbieżną pracę z zachowaniem integralności danych	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.109	Wszystkie ceny powinny być pobierane z Podsystemu Billing							TAK	TAK	TAK		TAK	TAK	TAK	TAK
SOFT.WW.110	System musi podlegać regularnemu tworzeniu kopii zapasowych (backup).	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.111	Dostarczone przez Wykonawcę rozwiązania muszą umożliwiać łączenie wszystkich elementów infrastruktury w celu zapewnienia możliwości rozbudowy wydajności Systemu bez potrzeby jego modyfikacji. Zwiększenie wydajności w przyszłości polegać powinno jedynie na rozbudowie poszczególnych warstw Systemu.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
	Front-end														
SOFT.WW.112	Interfejsy użytkowników powinny być					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	zaprojektowanie w zgodzie z zasadami RWD (Responsive Web Design)														
SOFT.WW.113	Podsystem musi wykorzystywać elementy graficzne w rozdzielczości dostosowanej do rozdzielczości i gęstości obrazu (DPI/PPI) urządzenia użytkownika.							TAK	TAK	TAK	TAK		TAK		
SOFT.WW.114	W elementach Podsystemu dostępnych dla użytkowników zewnętrznych wszelkie zasoby statyczne, będące częścią interfejsu graficznego (css,js, ikony, czcionki, obrazki interfejsu) powinny być serwowane z osobnej subdomeny (za wyjątkiem przypadków, w których nie jest to wskazane ze względów bezpieczeństwa)					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.115	Pliki javascript powinny być łączone w jeden plik i minifikowane.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.116	Pliki css powinny być łączone w jeden plik i minifikowane.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.117	Podsystem musi					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	zapewnić walidację wprowadzanych danych (np. pole NIP musi mieć określony format, itp.)														
SOFT.WW.118	Obrazy i inne elementy statyczne powinny mieć ustawiony odpowiedni czas ważności (nagłówek Expires).				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.119	Podsystemy powinny zapewniać mechanizmy umożliwiające weryfikację, czy wersja znajdująca się w cache przeglądarki i/lub serwera proxy jest aktualną wersją strony (np. nagłówek ETag)				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.120	Podsystem musi zapewnić czas wygenerowania, przesłania i zrenderowania strony dla anonimowych użytkowników na poziomie maksymalnie 3s (przy pomiarze z sieci lokalnej w siedzibie Zamawiającego).	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.121	Podsystem musi zapewnić średni czas wygenerowania, przesłania i renderowania stron dla	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK

	zalogowanych użytkowników, wykonujących typowe czynności administracyjne, na poziomie maksymalnie 4s (przy pomiarze z sieci lokalnej w siedzibie Zamawiającego).														
SOFT.WW.122	Podsystem musi zapewnić docelowe parametry wydajnościowe dla 100 użytkowników pracujących jednocześnie i 10 żądań na sekundę.	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK
SOFT.WW.123	Podsystem powinien być spójny z systemem identyfikacji wizualnej Zamawiającego.		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.124	Podsystemy powinny zapewnić spójne wizualnie interfejsy dla użytkownika końcowego (style, kolorystyka itp.)		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
	Obsługa błędów														
SOFT.WW.125	Wszelkie błędy, zarówno te leżące po stronie aplikacji (404 etc.) jak i te leżące po stronie serwera (500, 503), powinny mieć przygotowane osobne		TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	layouty, prezentujące użytkownikowi informacje o problemie oraz dane kontaktowe w celu rozwiązania problemu.														
SOFT.WW.126	Strony błędów powinny mieć wdrożone śledzenie w oparciu o wykorzystywaną w Projekcie platformę statystyk odwiedzin, aby umożliwić centralne zbieranie informacji o błędach.							TAK	TAK	TAK	TAK	TAK	TAK		
	Projekt graficzny i usability														
SOFT.WW.127	Należy przedstawić do akceptacji projekt graficzny wraz z projektem usability				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.128	Należy przedstawić do akceptacji analizę heurystyczną (nazywaną czasem heurystyką, analizą ekspercką) Projektu w celu określenia zgodności z powszechnie uznanymi zasadami usability.				TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	
SOFT.WW.129	Należy przeprowadzić badania serwisu z reprezentatywną grupą użytkowników (co najmniej 10 osób nie					TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	TAK	

	powiązanych w żaden sposób - bezpośrednio ani pośrednio - ze stronami Umowy).														

5.2.2. IaaS

ID wymagania	Treść wymagania
Wymagania ogólne	
SOFT.IAAS.1	IaaS musi być dedykowanym rozwiązaniem do budowy chmur publicznych (public clouds), prywatnych (private clouds), serwerów VPS, serwerów dedykowanych.
SOFT.IAAS.2	IaaS musi zapewniać zarządzanie oraz monitorowanie dużą (powyżej 100 000) siecią maszyn wirtualnych bądź serwerów dedykowanych.
SOFT.IAAS.3	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzania, monitoringu i skalowania maszyn wirtualnych cloud osadzonych na sprzęcie compute dla wszystkich wymaganych/wspieranych systemów operacyjnych.
SOFT.IAAS.4	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzana, monitoringu i skalowania maszyn wirtualnych VPS osadzonych na sprzęcie compute dla wszystkich wymaganych/wspieranych systemów operacyjnych.
SOFT.IAAS.5	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzana, monitoringu serwerów dedykowanych osadzonych na sprzęcie compute dla wszystkich wymaganych/wspieranych systemów operacyjnych.
SOFT.IAAS.6	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzania, monitoringu i skalowania środowiska sprzętowego "Storage" dla maszyn wirtualnych cloud, VPS.
SOFT.IAAS.7	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzania, monitoringu i skalowania środowiska sieciowego, w tym: sieci prywatnych (np. w oparciu o VLAN), adresacji prywatnej i publicznej IPv4 i IPv6 oraz sieci dostępowych VPN do usług. W przypadku protokołu IPv6 jeżeli oferowane rozwiązanie nie obsługuje na etapie składania oferty tej funkcjonalności, musi oferować ją na etapie realizacji Projektu.
SOFT.IAAS.8	W ramach wdrożenia Podsystemu IaaS muszą być zapewnione mechanizmy automatycznego provisioningu, zarządzania, monitoringu i skalowania środowiska load balancerów.
SOFT.IAAS.9	W ramach wdrożenia Podsystemu IaaS musi być zapewniona obsługa dwóch regionów: 1. "Głównego" w Centrum Danych Zamawiającego na sprzęcie dostarczonym w ramach niniejszego zamówienia (przedmiot niniejszego postępowania) oraz 2. "Zapasowego" na zakupionym, wdrożonym i rozbudowanym w ramach niniejszego zamówienia sprzęcie znajdującym się w innym budynku Zamawiającego. Ogólna specyfikacja istniejącej infrastruktury: - compute: serwery blade IBM w obudowie rack 19U, na potrzeby środowiska wirtualizacyjnego, - storage: macierz IBM obsadzona dyskami SAS, SATA, biblioteka taśmowa oraz serwery backupu z wbudowaną przestrzenią dyskową,

	- sieć: zbudowana na przełącznikach 1Gbps i 10Gbps, z wykorzystaniem łączenia portów w grupy oraz z zachowaniem redundancji połączeń. Dodatkowe uszczegółowienie realizacji tego wymagania znajduje się w rozdziale 4
SOFT.IAAS.10	IaaS musi zapewnić zarządzanie środowiskiem storage większym niż 10 petabajtów.
SOFT.IAAS.11	IaaS musi zapewnić zarządzanie oraz monitorowanie dużej (powyżej 10 000 hostów) sieci dla maszyn wirtualnych.
SOFT.IAAS.12	IaaS musi zapewnić logiczną agregację maszyn wirtualnych w grupy (inaczej strefy/zones)
SOFT.IAAS.13	IaaS musi zapewnić podział na regiony zapewniając osobną dedykowaną konfigurację dla compute, storage oraz warstwy sieci (w tym możliwość obsługi innego typu hypervisora oraz innej konfiguracji/sprzętu dla storage i sieci) dla danego regionu. Region musi zapewnić także osobny API endpoints, wspierając zarazem wspólne uwierzytelnianie użytkowników w oparciu o SSO oraz wspólny panel administracyjny dla wszystkich regionów.
SOFT.IAAS.14	IaaS musi zapewnić definiowanie domyślnego hypervisor dla maszyn wirtualnych (cloud/vps) uruchamianych w danej grupie (w danej strefie/zone).
SOFT.IAAS.15	IaaS musi zapewnić wiele organizacji (multitenant).
SOFT.IAAS.16	IaaS musi zostać skonfigurowany w trybie wysokiej dostępności (High-Availability) - w szczególności dotyczy to każdego komponentu służącego do zarządzania i monitorowania infrastruktury IaaS.
SOFT.IAAS.17	IaaS musi zapewnić pełną kontrolę każdego aspektu funkcjonalnego za pomocą API.
SOFT.IAAS.18	IaaS musi wspierać pluginy dla każdej warstwy architektury (compute, storage, network) umożliwiające rozszerzanie funkcjonalności danej warstwy.
SOFT.IAAS.19	IaaS musi zapewnić możliwość przydzielenia maszynom wirtualnym od 1 do co najmniej 128 procesorów wirtualnych.
SOFT.IAAS.20	Licencja IaaS musi zapewniać możliwość ciągłego rozwoju Systemu przez Zamawiającego (własny zespół), dopuszczalne są dwa podejścia: przekazanie kodów źródłowych do całego Podsystemu IaaS wraz z przekazaniem autorskich praw majątkowych, bądź przekazanie kodów źródłowych do całego Podsystemu IaaS wraz z licencją umożliwiającą rozwój na własne potrzeby Zamawiającego.
SOFT.IAAS.21	Kody źródłowe aplikacji muszą być przekazane w formie umożliwiającej rozwój. Kody źródłowe nie mogą być zaciemnione (nie mogą być poddane obfuskacji, z ang. obfuscation).
SOFT.IAAS.22	Wraz z kodami źródłowymi wymagane jest przekazanie dokumentacji rozwojowej, w szczególności: opis architektury logicznej rozwiązania (modułów), wymaganych i użytych bibliotek i narzędzi, sposób budowania i dystrybucji aplikacji.
SOFT.IAAS.23	IaaS musi zapewnić pełną obsługę następujących systemów operacyjnych (zarówno dla serwerów cloud, vps jak i serwerów dedykowanych): GNU Linux (w tym w szczególności: Debian GNU/Linux, RedHat Enterprise Linux, CentOS, Ubuntu, OpenSUSE, SUSE Enterprise Linux, Oracle Enterprise Linux), Microsoft Windows Server (2008, 2012 - wersje standard oraz enterprise), FreeBSD.
SOFT.IAAS.24	IaaS musi obsługiwać systemy operacyjne w najnowszej stabilnej wersji dostępnej w dniu zakończenia etapu analizy.

SOFT.IAAS.25	W ramach wdrożenia Podsystemu IaaS, Wykonawca musi przygotować obrazy dla maszyn wirtualnych (cloud/vps) oraz obrazy do instalacji serwerów dedykowanych dla wszystkich obsługiwanych systemów operacyjnych oraz umieścić je na usłudze biblioteki obrazów (image template/storage) IaaS.
SOFT.IAAS.26	IaaS musi zapewnić zautomatyzowaną instalację/uruchomienie maszyn wirtualnych (cloud/vps) czy też serwerów dedykowanych bez ingerencji administratora dla każdego wymaganego systemu operacyjnego.
SOFT.IAAS.27	IaaS musi umożliwić implementację/wdrożenie zarządzania wszystkimi funkcjonalnościami Podsystemu przez Podsystemy SelfService oraz Cloud API.
SOFT.IAAS.28	IaaS musi zapewniać pełną integrację z Podsystemem Billing oraz udostępniać w sposób zautomatyzowany (poprzez API) wszystkie dane wymagane do prawidłowego działania i spełnienia wszystkich wymagań Podsystemu Billing.
SOFT.IAAS.29	IaaS musi zapewnić możliwość obsługi wielu instancji różnych systemów operacyjnych na jednym serwerze fizycznym i musi wykorzystywać sprzętową wirtualizację zasobów.
SOFT.IAAS.30	IaaS musi być niezależne od producenta platformy sprzętowej (poprawnie współpracować ze sprzętem dostarczanym przez wielu różnych producentów).
SOFT.IAAS.31	IaaS musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągniecia maksymalnego współczynnika konsolidacji (tzw. memory overcommit).
SOFT.IAAS.32	IaaS musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej jak i parametrów samych maszyn wirtualnych (cloud/vps) jak też serwerów dedykowanych w trybie real-time.
SOFT.IAAS.33	IaaS musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
SOFT.IAAS.34	IaaS musi umożliwiać zastosowanie w serwerach fizycznych dowolnej ilości procesorów o dowolnej ilości rdzeni.
SOFT.IAAS.35	IaaS musi mieć możliwość uruchamiania fizycznych serwerów z centralnie przygotowanego obrazu poprzez protokół PXE
SOFT.IAAS.36	IaaS musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.
SOFT.IAAS.37	IaaS musi pozwalać na definiowanie wzorców (typów) serwerów wirtualnych (cloud/vps) abstrahując od parametrów serwerów, np. typ „Large”, „Medium”, itp.. Wzorce mają wyjść naprzeciw oczekiwaniu, aby użytkownicy/klienci zamawiali podobne konfiguracje maszyn, unikając dużej fragmentacji zestawianych serwerów. Definicja wzorca serwera musi uwzględniać ogólne i szczegółowe parametry, np. dla serwera: CPU lub vCPU, pamięć RAM, przestrzeń dyskowa, adresy IPv4 i IPv6, VLANy, sieci prywatne, sieci dostępowe VPN.
SOFT.IAAS.38	IaaS musi zapewnić uwierzytelnianie użytkowników w oparciu o SSO.
SOFT.IAAS.39	IaaS musi zapewnić zarządzanie uprawnieniami dla użytkowników w oparciu o SSO.
SOFT.IAAS.40	IaaS musi pozwalać na definiowanie praw dostępu do zasobów wchodzących w skład chmury dla ról/użytkowników. Definicje muszą obejmować co najmniej: dostęp do specyficznych zasobów (np. stref, sieci), maksymalne liczby poszczególnych typów zasobów (CPU, serwery, pamięć, przestrzeń dyskowa, sieci, adresy IP, VPN).

SOFT.IAAS.41	IaaS musi pozwalać na definiowanie Usług na potrzeby budowania oferty Usług zachowując pełny cykl życia Usługi: • rejestrację Usługi • autoryzację Usługi • zamawianie i akceptacja Usługi • rezerwacja zasobów • uruchamianie Usługi • modyfikacje parametrów • zarządzanie Usługami • rezygnacja z Usługi • zwalnianie zasobów.
SOFT.IAAS.42	IaaS musi pozwalać na przypisanie przygotowanych modeli kosztów do poszczególnych zasobów i ról/użytkowników.
SOFT.IAAS.43	IaaS musi umożliwiać zdefiniowanie maksymalnej ilości jednostek do wykorzystania w ramach danej Usługi (np. 10GB transferu danych dla danego serwera cloud/vps).
SOFT.IAAS.44	IaaS musi wspierać limitowanie wszystkich zasobów sprzętowych przydzielonych do danej instancji wirtualnej.
Szczegółowe wymagania dla wdrożenia warstwy/Usługi chmury obliczeniowej (compute)	
SOFT.IAAS.45	IaaS musi zapewnić wsparcie następującej listy hypervisor: Microsoft Hyper-V, Citrix XenServer, Xen, KVM, VMWware ESXi, LXC, QEMU, Docker, Baremetal (czyli kontrolę maszyny fizycznej analogicznie jak w przypadku maszyny wirtualnej).
SOFT.IAAS.46	IaaS dla następującej grupy hypervisorów musi zapewnić operacje: uruchomienia, restartu i zatrzymania: LXC, Baremetal, Docker.
SOFT.IAAS.47	IaaS dla następującej grupy hypervisorów musi zapewnić następujące operacje dla maszyny wirtualnej działającej pod kontrolą danego hypervisora: uruchomienia, restartu, zatrzymania, resize (zmiana parametrów maszyny wirtualnej), suspend, reasume: Xen, KVM, QEMU, Hyper-V, ESXi.
SOFT.IAAS.48	IaaS musi umożliwiać przenoszenia maszyn wirtualnych (cloud/vps) w czasie ich pracy (bez zatrzymania działania) pomiędzy serwerami fizycznymi (tzw. live migration), dla następujących Hypervisorów: KVM, XEN, XenServer, Hyper-V, QEMU.
SOFT.IAAS.49	IaaS musi umożliwiać instancjonowanie maszyn wirtualnych cloud/vps zapewniając automatyczne skalowanie liczby procesorów i pamięci RAM.
SOFT.IAAS.50	Instancje maszyn wirtualnych cloud/vps muszą mieć możliwość rozliczania w cyklu minutowym.
SOFT.IAAS.51	IaaS musi udostępnić dla maszyn wirtualnych (vps/cloud) zdalny tryb/system rescue czyli system awaryjnego dostępu do serwera w celu zlokalizowania i usunięcia usterek.
Szczegółowe wymagania dla wdrożenia warstwy/Usługi serwery dedykowane	
SOFT.IAAS.52	IaaS musi udostępniać w sposób zautomatyzowany zdalną konsolę zarządzania sprzętem dla klientów końcowych (użytkowników) - czyli zdalna klawiatura, ekran i mysz, które pozwalają na dostęp do ekranu klawiszy/myszy serwera za pomocą bezpiecznego połączenia.
SOFT.IAAS.53	IaaS musi udostępnić dla serwerów dedykowanych zdalny tryb/system rescue czyli system awaryjnego dostępu do serwera w celu zlokalizowania i usunięcia usterek.

SOFT.IAAS.54	IaaS musi umożliwiać zdalny restart serwera dedykowanego dla maszyn dedykowanych.
SOFT.IAAS.55	IaaS musi udostępnić możliwość zdalnego wyłączenia i ponownego uruchomienia serwera w dowolnej chwili.
SOFT.IAAS.56	IaaS dla serwerów dedykowanych musi udostępnić poza jądrem dostarczanym domyślnie na dysku twardym, możliwość uruchomienia maszyny z sieci z jądrem przygotowanym przez Zamawiającego lub Wykonawcę (uruchomienie serwera dedykowanego z innym jądrem po sieci).
Szczegółowe wymagania dla wdrożenia warstwy/Usługi danych (storage)	
SOFT.IAAS.57	IaaS musi świadczyć usługę repozytorium obrazów maszyn wirtualnych (image storage).
SOFT.IAAS.58	IaaS musi zapewnić następujące typy obrazów dyskowych: raw, vhd, vmdk, vdi, qcow2.
SOFT.IAAS.59	IaaS musi umożliwiać szyfrowanie dysków systemów wirtualnych pod jego kontrolą. Hasła powinny być nadawane przez użytkownika/klienta platformy IaaS za pomocą: dedykowanych funkcjonalności SelfService, API bądź interfejsu CLI.
SOFT.IAAS.60	Wdrożenie IaaS musi obejmować wdrożenie Usługi block storage dla Klientów (udostępnianie urządzeń blokowych rozpoznawane przez system operacyjny jako dysk).
SOFT.IAAS.61	Usługa block storage musi umożliwiać instancjonowanie przestrzeni dyskowych o rozmiarze min. 50 TB automatycznie podłączanych do systemu operacyjnego (oczywiście ograniczonych fizyczną przestrzenią dostępną przez oferowany sprzęt storage).
SOFT.IAAS.62	Usługa block storage musi umożliwiać zmianę rozmiaru (powiększanie i zmniejszanie) przestrzeni dyskowej.
SOFT.IAAS.63	IaaS musi wspierać protokoły dostępowe iSCSI, FC oraz RADOS Block Device.
SOFT.IAAS.64	Wdrożenie IaaS musi obejmować wdrożenie object storage, który musi zostać zaimplementowany z użyciem protokołu RADOS Object Storage w celu zapewnienia kompatybilności z usługą Amazon S3.
SOFT.IAAS.65	Usługa object storage musi umożliwiać zapis plików i obiektów o rozmiarze nie mniejszym niż 16TB.
SOFT.IAAS.66	Usługa object storage musi zapewniać mechanizm autoryzacji dostępu.
SOFT.IAAS.67	Transmisja obiektów z usługi object storage musi być możliwa za pomocą szyfrowanego połączenia.
Szczegółowe wymagania dla wdrożenia warstwy/Usługi sieci (networking)	
SOFT.IAAS.68	IaaS musi zapewniać tworzenie wirtualnych sieci prywatnych (wirtualna prywatna chmura) pomiędzy maszynami wirtualnymi, serwerami dedykowanymi danego klienta oraz w ramach instancji danej aplikacji PaaS - implementacja Usługi Cloud Private Network (będź inaczej Private Network as a Service).
SOFT.IAAS.69	IaaS musi zapewniać kontrolowanie sieci na warstwie drugiej modelu OSI.
SOFT.IAAS.70	IaaS musi zapewnić automatycznie nadawanie prywatnej adresacji: IPv4 oaz IPv6 oraz publicznej adresacji IPv4 oraz IPv6 dla wszystkich Usług obsługiwanych przez IaaS. W przypadku standardu IPv6 - jeżeli oferowane rozwiązanie nie obsługuje na etapie składania oferty tej funkcjonalności, musi oferować ją na etapie realizacji Projektu.
SOFT.IAAS.71	IaaS musi zapewnić usługę IP failover, polegającą na możliwości przenoszenia publicznych adresów IP między różnymi instancjami Usług.
SOFT.IAAS.72	IaaS musi zapewnić Load Balancer as a Service dla każdego Klienta. Usługa ta powinna zapewniać tworzenie dowolnej liczby instancji load balancera na poziome: TCP, UDP,

	HTTP, HTTPS oraz następujące algorytmy load balancingu: Round Robin Wagowany Round Robin (umożliwiający określenie wagi dla każdego node), Random losowy, Preferowana najmniejsza liczba połączeń - który będzie powodował kierowanie ruchu na node z najmniejszą liczbą połączeń, Wagowany najmniejsza liczba połączeń - analogiczny do preferowana najmniejsza liczba połączeń, natomiast pozwalający przypisać wagi do poszczególnych node. Usługa load balancing musi zapewniać także zarządzanie sesją użytkownika (session persistance): source IP - zarządzanie sesją za pomocą śledzenia adresu źródłowego w celu określenia node docelowego oraz HTTP Cookie - śledzenie sesji za pomocą HTTP cookies (jedynie dla HTTP load balancing). Dodatkowo musi umożliwić zarządzanie monitoringiem oraz opcjami automatycznego podłączania/odłączania load balancowanych nodów (interwał weryfikacji nodów, liczba prób, timeout).
SOFT.IAAS.73	IaaS musi zapewnić terminację SSL na load balancerach.
SOFT.IAAS.74	IaaS musi zapewnić Usługę: Firewall as a Service dla każdego Klienta. Jeżeli oferowane rozwiązanie nie obsługuje na etapie składania oferty tej funkcjonalności, musi oferować ją na etapie realizacji Projektu.
SOFT.IAAS.75	IaaS musi zapewnić możliwość konfiguracji certyfikatu SSL na poszczególnych instancjach load balancerów.
SOFT.IAAS.76	IaaS musi zapewnić Usługę: VPN as a Service (VPNaaS - VPN Site-to-Site) umożliwiającą tworzenie i zarządzanie dedykowanych sieci VPN do sieci każdego z Klientów (zarządzanych przez Klientów) za pomocą: ipsec VPN. Wykorzystana technologia musi umożliwiać połączenie się do sieci VPN darmowymi, wbudowanymi w system operacyjny bądź open source narzędziami (klientami) IPSEC dostępnymi na następujące systemy operacyjne: GNU Linux, w szczególności: Debian GNU/Linux (Wheezy i nowszy), Fedora Linux (18 i nowsza), OpenSUSE (12 lub nowszy), Ubuntu Linux (13.10 lub nowszy), Windows 7 (i nowszy), Mac OS X (10.8 i nowszy). IaaS musi zapewniać także automatyczne generowanie plików konfiguracyjnych dla wybranego narzędzia ustalonego wspólnie z Zamawiającym na etapie analizy.
SOFT.IAAS.77	IaaS musi zapewnić segmentację VLAN sieci Klienta.
SOFT.IAAS.78	Load balancery zarządzane przez IaaS muszą mieć możliwość konfigurowania przekazywanych nagłówków HTTP.
SOFT.IAAS.79	IaaS musi zapewnić możliwość zarządzania konfiguracją Two-Way SSL na load balancerach.
SOFT.IAAS.80	W przypadku włączenia usługi two-way ssl na load balancerze, IaaS musi zapewnić konfigurację przekazywania nagłówków certyfikatów SSL klienta nawiązującego połączenie (np. pola Common Name, email itd).
SOFT.IAAS.81	IaaS musi zapewniać możliwość definiowania, które z Usług (np. serwerów cloud bądź dedykowanych) mają być podłączone do load balancer.
SOFT.IAAS.82	IaaS musi zapewniać zarządzanie regułami firewall dla pojedynczego serwera cloud/vps/dedykowanego jak i całych sieci prywatnych i publicznych klienta. Jeżeli oferowane rozwiązanie nie obsługuje na etapie składania oferty tej funkcjonalności, musi oferować ją na etapie realizacji Projektu.
SOFT.IAAS.83	IaaS musi zapewnić rezerwację i przydzielanie zasobów jak również ich rozliczanie

	(zbieranie metryk udostępnianych Podsystemowi Biling): * Wirtualnych w oparciu o systemy wirtualizacji zasobów, z możliwością definicji parametrów, w tym: - vCPU – ilość - RAM – ilość - Storage - ilość wg typów storage - IOPS – ilość - Pasmo (gwarantowane, niegwarantowane) - Transfer danych - ilość - wewnątrz Usług - do sieci Internet - z sieci Internet - VLAN - ilość - Adresy IP publiczne IPv4 oraz IPv6 - ilość - Load Balancer - ilość (wraz z typami zarządzania sesji oraz terminacji SSL) - Firewall - ilość - Sieci prywatne - ilość - instancje VPN - ilość oraz typ * Fizycznych bez względu na producenta, w tym: - serwerów o zdefiniowanych parametrach - wolumenów dyskowych - wydzielonych - przydzielanych dynamicznie (integracja z storage) - Sieci prywatne - ilość - instancje VPN - ilość oraz typ - Firewall - ilość - Load Balancer - ilość (wraz z typami zarządzania sesji oraz terminacji SSL) - Adresy IP publiczne IPv4 oraz IPv6 – ilość.
Szczegółowe wymagania dla panelu administracyjnego i zarządzania przez Zamawiającego IaaS	
SOFT.IAAS.84	IaaS musi zapewnić centralny interfejs administracyjny, umożliwiający zmianę każdego parametru konfiguracyjnego za pomocą dedykowanego interfejsu WEB (cienki klient).
SOFT.IAAS.85	Interfejs administracyjny IaaS musi zapewnić funkcjonalność wersjonowania parametrów konfiguracyjnych (wartość, datę wartości, osobę/administratora, która wprowadziła wartość, unikalne ID dla zmiany, komentarz dla wprowadzonych zmian) wraz z przywracaniem wybranej wersji parametru konfiguracyjnego z poziomu panelu.
SOFT.IAAS.86	Panel administracyjny IaaS musi zapewnić możliwość zdefiniowania poziomów akceptacji wprowadzanych zmian.
SOFT.IAAS.87	Interfejs administracyjny IaaS musi zapewnić wizualizację zmian w konfiguracji, uwzględniając: - system/serwer/Usługę, której zmiana dotyczy, - datę powstania zmiany

	- osobę, która dokonała zmiany, - diff w postaci graficznej reprezentujący zmianę w stosunku do poprzednich zmian, - komentarz dot. danej zmiany. Po akceptacji zmiany musi nastąpić automatyczne wdrożenie zaakceptowanej konfiguracji za pomocą mechanizmu orkiestrującego (provisioning).
SOFT.IAAS.88	Panel administracyjny musi zapewnić mechanizm ról i uprawnień, który w szczególności musi zapewnić uprawnienia: - wprowadzanie zmian w plikach konfiguracyjnych danego zasobu IaaS, - nadawanie uprawnień do wprowadzania zmian dla całej grupy, - nadawanie uprawnień do uruchamiania danych konfiguracji na danym serwerze, usłudze, systemem - należy rozróżnić fakt wprowadzania oraz uruchamiania danych konfiguracji.
SOFT.IAAS.89	Panel administracyjny musi w trybie real-time wizualizować postęp jak i operacje (komunikaty usług wprowadzających zmiany) wykonywane podczas wprowadzanych zmian.
SOFT.IAAS.90	Interfejs administracyjny musi zapewnić powiadomienie (notyfikację) wybranych administratorów o fakcie pojawienia się konfiguracji gotowych do wdrożenia (zarządzanie grupami zgodnie z wymaganiami dla wszystkich Podsystemów odbywać będzie się przez LDAP).
SOFT.IAAS.91	Notyfikacje muszą być wysyłane na adresy email administratorów.
SOFT.IAAS.92	Treści komunikatów będą mogły być edytowane za pomocą formularza na stronie Podsystemu i muszą być zapisywane jako szablony.
SOFT.IAAS.93	Panel administracyjny musi umożliwić wyświetlanie na żywo logów wszystkich wykonywanych operacji.
SOFT.IAAS.94	Panel musi udostępniać możliwość przeszukiwania i filtrowania logów wykonywanych operacji z uwzględnieniem uprawnień do nich.
SOFT.IAAS.95	Panel administracyjny musi udostępniać możliwość rollback (przywrócenia poprzedniego stanu) - czyli uruchomienia konfiguracji, instalacji/aktualizacji poprzedniej wersji z systemu kontroli wersji.
SOFT.IAAS.96	Panel administracyjny musi umożliwiać przetestowanie wprowadzonych zmian w konfiguracji z wykorzystaniem środowiska integracyjnego zbudowanego w ramach Projektu.
SOFT.IAAS.97	Panel administracyjny musi zapewniać możliwość zarządzania i monitorowania Usług IaaS wszystkich klientów (oraz ich parametrów).

5.2.3. PaaS

ID wymagania	Treść wymagania
SOFT.PAAS.1	PaaS musi stanowić przyjazne, elastyczne, skalowalne i bezpieczne środowisko dla aplikacji SaaS.
SOFT.PAAS.2	PaaS musi zapewnić: • cykl życia aplikacji • pakiety deploymentowe (Platform Deployment Package)

	• zasoby (Resources) zgodnie ze specyfikacją Cloud Application Mangement for Platforms (https://www.oasis-open.org/committees/download.php/47278/CAMP-v1.0.pdf).
SOFT.PAAS.3	Licencja PaaS musi zapewniać możliwość ciągłego rozwoju Systemu przez Zamawiającego (własny zespół), dopuszczalne są dwa podejścia: przekazanie kodów źródłowych do całego Podsystemu PaaS wraz z przekazaniem autorskich praw majątkowych, bądź przekazanie kodów źródłowych do całego Podsystemu PaaS wraz z licencją umożliwiającą rozwój na własne potrzeby Zamawiającego.
SOFT.PAAS.4	Kody źródłowe aplikacji muszą być przekazane w formie umożliwiającej rozwój. Kody źródłowe nie mogą być zaciemnione (nie mogą być poddane obfuskacji, z ang. obfuscation).
SOFT.PAAS.5	Wraz z kodami źródłowymi wymagane jest przekazanie dokumentacji rozwojowej, w szczególności: opis architektury logicznej rozwiązania (modułów), wymaganych i użytych bibliotek i narzędzi, sposób budowania i dystrybucji aplikacji.
SOFT.PAAS.6	PaaS musi integrować się bezpośrednio z IaaS oraz wykorzystywać infrastrukturę zarządzaną przez IaaS w celu zarządzania, monitorowania oraz automatycznego skalowania środowiska IaaS.
SOFT.PAAS.7	Każda instancja aplikacji bądź bazy danych uruchamianej na Podsystemie PaaS musi działać na dedykowanym kontenerze w oparciu o wirtualizację na poziomie systemu operacyjnego GNU/Linux (właściwy system operacyjny zostanie wybrany i uzgodniony z Zamawiającym podczas etapu analizy).
SOFT.PAAS.8	PaaS musi zapewnić automatyzację zarządzania, skalowania (w tym auto-skalowanie) i monitorowania środowiska IaaS dla serwerów aplikacyjnych, baz danych przeznaczonych dla aplikacji Klienta.
SOFT.PAAS.9	PaaS musi zapewnić automatyzację zarządzania, skalowania (w tym auto-skalowanie) i monitorowania osadzonych na nim aplikacji oraz baz danych.
SOFT.PAAS.10	PaaS musi zapewnić funkcjonalność konfiguracji reguł auto-skalowania dla osadzanych aplikacji oraz baz danych.
SOFT.PAAS.11	PaaS musi zapewnić automatyczny provisioning, monitoring i zarządzanie środowisk aplikacyjnych oraz bazodanowych za pomocą Podsystemu SelfService.
SOFT.PAAS.12	PaaS musi zapewnić automatyczny provisioning, monitoring i zarządzanie środowisk aplikacyjnych oraz bazodanowych za pomocą API.
SOFT.PAAS.13	PaaS musi zapewnić automatyczny provisioning, monitoring i zarządzanie środowisk aplikacyjnych oraz bazodanowych za pomocą dedykowanej aplikacji CLI.
SOFT.PAAS.14	PaaS musi zapewnić automatyczny provisioning i zarządzanie środowisk aplikacyjnych oraz bazodanowych za pomocą systemu VCS (system kontroli wersji) GIT.
SOFT.PAAS.15	PaaS musi posiadać architekturę modułową oraz zapewnić wsparcie wielu języków programowania, w szczególności następujących języków: Java, Python, PHP. Zamawiający pisząc "zapewnić wsparcie" ma na myśli umożliwić uruchamianie, zarządzanie, monitoring oraz auto-skalowanie aplikacji napisanych w danym języku programowania.
SOFT.PAAS.16	PaaS musi zapewnić wsparcie wielu wersji danego języka oprogramowania (dana aplikacja może działać na wybranej wersji danego języka oprogramowania).
SOFT.PAAS.17	PaaS musi zapewnić wsparcie wielu wersji frameworków/bibliotek danego języka

	oprogramowania (dana aplikacja może działać na wybranej wersji danego framework/biblioteki oprogramowania).
SOFT.PAAS.18	Architektura PaaS powinna w przyszłości (bez jej modyfikacji) umożliwiać rozszerzanie funkcjonalności Podsystemu o kolejne języki programowania, frameworki, systemy bazodanowe a także umożliwiać proste (za pomocą modułów/pluginów) rozszerzenie Podsystemu o nowe technologie, narzędzia i usługi (np. rozproszonych i asynchronicznych systemów zarządzania kolejkami zadań)
SOFT.PAAS.19	Architektura PaaS musi zapewnić jego rozszerzenie o wsparcie nowych bibliotek/frameworków programowania danego języka. Zamawiający pisząc "zapewnić wsparcie" ma na myśli umożliwić uruchamianie, zarządzanie, monitoring oraz auto-skalowanie aplikacji napisanych w danym framework/bibliotece danego języku programowania.
SOFT.PAAS.20	Architektura PaaS musi zapewnić jego rozszerzenie o wsparcie nowych Usług bazodanowych (w tym usługi bazodanowe SQL i noSQL). Zamawiający pisząc "zapewnić wsparcie" ma na myśli umożliwić uruchamianie (w tym tworzenie odpowiedniej schemy oraz import wskazanych danych), zarządzanie, monitoring oraz auto-skalowanie instancji baz danych w oparciu o dany system bazodanowy oraz możliwość automatycznego konfigurowania aplikacji działającej pod kontrolą Podsystemu PaaS aby wykorzystywała daną instancję bazy danych.
SOFT.PAAS.21	Musi być dostarczona dokumentacja oraz przykład (szablon) w jaki sposób tworzyć moduły/rozszerzenia PaaS w celu zapewnienia wsparcia dla kolejnych (nie obsługiwanych jeszcze) języków programowania.
SOFT.PAAS.22	Musi być dostarczona dokumentacja oraz przykład (szablon) w jaki sposób tworzyć moduły/rozszerzenia PaaS w celu zapewnienia wsparcia przykładowego framework dla danych języków programowania.
SOFT.PAAS.23	Musi być dostarczona dokumentacja oraz przykład (szablon) w jaki sposób tworzyć moduły/rozszerzenia PaaS w celu zapewnienia wsparcia przykładowego serwera aplikacyjnego dla danego języka/framework.
SOFT.PAAS.24	Musi być dostarczona dokumentacja oraz przykład (szablon) w jaki sposób tworzyć moduły/rozszerzenia PaaS w celu zapewnienia wsparcia dla kolejnych (nie obsługiwanych jeszcze) języków systemów baz danych.
SOFT.PAAS.25	PaaS musi zapewnić wsparcie następujących frameworków języka Java: Sprint, Play!.
SOFT.PAAS.26	PaaS musi zapewnić wsparcie następujących frameworków języka Python: Django, Flask.
SOFT.PAAS.27	PaaS musi zapewnić wsparcie następujących frameworków języka PHP: CakePHP, Symphony.
SOFT.PAAS.28	PaaS musi zapewnić wsparcie następujących serwerów aplikacyjnych dla języka Java: JBoos, Tomcat.
SOFT.PAAS.29	PaaS musi zapewnić wsparcie następujących serwerów WSGI języka Python: Gunicorn, uWSGI.
SOFT.PAAS.30	PaaS musi zapewnić wsparcie następujących frameworków języka PHP: CakePHP, Symphony.
SOFT.PAAS.31	PaaS musi zapewnić wsparcie uruchamiania aplikacji języka PHP za pomocą oprogramowania: Apache2 wraz z mod_php oraz za pomocą PHP FastCGI Process

	Manager (FPM) wraz z proxy NGINX.
SOFT.PAAS.32	PaaS musi zapewnić wsparcie dla uruchamiania aplikacji języka PHP na wydzielonym koncie użytkownika, przypisanym do wirtualnego hosta (mechanizm SuExec).
SOFT.PAAS.33	PaaS musi zapewnić wsparcie następującej platformy bazodanowej SQL: PostgreSQL, MySQL.
SOFT.PAAS.34	PaaS musi zapewnić wsparcie następującej platformy bazodanowej noSQL: MongoDB.
SOFT.PAAS.35	PaaS musi zapewniać pełną automatyzację provisioningu i deploymentu aplikacji automatycznie konfigurując aplikację do działania.
SOFT.PAAS.36	PaaS musi zapewniać pełną automatyzację provisioningu i deploymentu aplikacji automatycznie konfigurując i podłączając bazę danych aplikacji oraz samą aplikację z bazą danych.
SOFT.PAAS.37	PaaS musi zapewnić pełną kontrolę każdego aspektu funkcjonalnego za pomocą API.
SOFT.PAAS.38	PaaS musi zapewniać możliwość dostarczenia metryk dla Podsystemu Biling w celu rozliczania aplikacji działających na środowisku PaaS w modelu Pay as you go - czyli za faktycznie wykorzystane zasoby (CPU, RAM, przestrzeń dyskowa, I/O, wykorzystanie (transfer) danych wyjściowych, wykorzystanie (transfer) danych wejściowych, liczba instancji, czas działania, liczba obsłużonych połączeń).
SOFT.PAAS.39	Musi być stworzona kompleksowa dokumentacja Podsystemu PaaS wraz z przykładami użycia dla każdego języka, framework oraz bazy danych.
SOFT.PAAS.40	Muszą być dostarczone szkieletowe/przykładowe aplikacje dla każdego języka i framework (w połączeniu z każdą bazą danych) w celu ułatwienia bootstrapowania nowych aplikacji.
SOFT.PAAS.41	Dokumentacja API oraz przykłady aplikacji muszą być przygotowane w języku polskim i angielskim.
SOFT.PAAS.42	PaaS musi umożliwiać zdefiniowanie w dowolnym momencie liczbę instancji danej aplikacji. Zmiana liczby instancji musi powodować automatyczne uruchomienie bądź wyłączenie danej instancji.
SOFT.PAAS.43	W przypadku zdefiniowania (automatycznie podczas skalowania bądź ręcznie) drugiej bądź kolejnej instancji danej aplikacji, musi być automatycznie podniesiona instancja load balancer'a oraz muszą być podłączone do niego wszystkie instancje aplikacji. Innym możliwym sposobem realizacji jest uruchamianie instancji load balancer od razu dla każdej nowej aplikacji a następnie podłączanie do niego kolejnych instancji aplikacji.
SOFT.PAAS.44	Musi być możliwe dostarczenie definicji uruchomienia aplikacji na środowisku PaaS (w tym bazy danych) w jednym pliku konfiguracyjnym dołączonym do źródeł aplikacji - tzw. plik Manifestu.
SOFT.PAAS.45	Podczas uruchamiania instancji aplikacji na środowisku, PaaS powinien na podstawie pliku Manifestu w sposób zautomatyzowany wykryć typ uruchamianej aplikacji (język, framework).
SOFT.PAAS.46	Plik Manifestu musi umożliwiać skonfigurowanie typu aplikacji (język oraz wersja języka, framework oraz jego wersja, sposób obsługi instancji danej aplikacji), typ bazy danych, inicjalne dane do wczytania do bazy, liczbę instancji aplikacji, liczbę instancji baz danych, sposób działania load balancera (w szczególności sesji HTTP), konfigurację SSL load balancera, nazwę domeny aplikacji, port TCP/IP (domyślnie 80).

SOFT.PAAS.47	Plik Manifestu musi być plikiem tekstowym.
SOFT.PAAS.48	Plik Manifestu musi być w jednym z formatów: YAML, JSON.
SOFT.PAAS.49	Musi być możliwość zalogowania się za pomocą SSH na kontener, na którym działa dana instancja aplikacji.
SOFT.PAAS.50	W przypadku uruchomienia więcej niż jednej instancji danej aplikacji PaaS (maksymalnie 64 instancje) musi zapewnić poprawną obsługę sesji użytkowników oraz współdzielonych zasobów (np. danych na dyskach).
SOFT.PAAS.51	W przypadku uruchomienia więcej niż jednej instancji danej aplikacji PaaS (maksymalnie 64 instancje) musi zapewnić automatyczne instancjonowanie sieci prywatnej (wirtualna prywatna chmura - private cloud network) oraz instancjonowanie dostępu do tejże sieci prywatnej za pomocą instancji VPN (instancja Usługi VPN as a Service).
Szczegółowe wymagania dla panelu administracyjnego i zarządzania przez Zamawiającego PaaS	
SOFT.PAAS.52	PaaS musi zapewnić centralny interfejs administracyjny, umożliwiający zmianę każdego parametru konfiguracyjnego za pomocą dedykowanego interfejsu WEB (cienki klient).
SOFT.PAAS.53	Interfejs administracyjny PaaS musi zapewnić funkcjonalność wersjonowania parametrów konfiguracyjnych (wartość, datę wartości, osobę/administratora, która wprowadziła wartość, unikalne ID dla zmiany, komentarz dla wprowadzonych zmian) wraz z przywracaniem wybranej wersji parametru konfiguracyjnego z poziomu panelu.
SOFT.PAAS.54	Panel administracyjny PaaS musi zapewnić możliwość zdefiniowania poziomów akceptacji wprowadzanych zmian.
SOFT.PAAS.55	Interfejs administracyjny PaaS musi zapewnić wizualizację zmian w konfiguracji, uwzględniając: - aplikację/system/serwer/Usługę, której zmiana dotyczy, - datę powstania zmiany - osobę, która dokonała zmiany, - diff w postaci graficznej reprezentujący zmianę w stosunku do poprzednich zmian, - komentarz dot. danej zmiany. Po akceptacji zmiany musi nastąpić automatyczne wdrożenie zaakceptowanej konfiguracji za pomocą mechanizmu orkiestrującego (provisioning).
SOFT.PAAS.56	Panel administracyjny musi zapewnić mechanizm ról i uprawnień, w szczególności następujące uprawnienia: - wprowadzanie zmian w plikach konfiguracyjnych danego zasobu PaaS, - nadawanie uprawnień do wprowadzania zmian dla całej grupy, - nadawanie uprawnień do uruchamiania danych konfiguracji na danym serwerze, usłudze, systemie - należy rozróżnić fakt wprowadzania oraz uruchamiania danych konfiguracji.
SOFT.PAAS.57	Panel administracyjny musi w trybie real-time wizualizować postęp jak i operacje (komunikaty usług wprowadzających zmiany) wykonywane podczas wprowadzanych zmian.
SOFT.PAAS.58	Interfejs administracyjny musi zapewnić powiadomienie (notyfikację) wybranych administratorów o fakcie pojawienia się konfiguracji gotowych do wdrożenia (zarządzanie grupami zgodnie z wymaganiami dla wszystkich Podsystemów odbywać będzie się przez LDAP).

SOFT.PAAS.59	Notyfikacje muszą być wysyłane na adresy e-mail administratorów.
SOFT.PAAS.60	Treści komunikatów będą mogły być edytowane za pomocą formularza na stronie Podsystemu i muszą być zapisywane jako szablony.
SOFT.PAAS.61	Panel administracyjny musi umożliwić wyświetlanie na żywo logów wszystkich wykonywanych operacji.
SOFT.PAAS.62	Panel musi udostępniać możliwość przeszukiwania i filtrowania logów wykonywanych operacji z uwzględnieniem uprawnień do nich.
SOFT.PAAS.63	Panel administracyjny musi udostępniać możliwość rollback (przywrócenia poprzedniego stanu) - czyli uruchomienia konfiguracji, instalacji/aktualizacji poprzedniej wersji z systemu kontroli wersji.
SOFT.PAAS.64	Panel administracyjny musi umożliwiać przetestowanie wprowadzonych zmian w konfiguracji z wykorzystaniem środowiska integracyjnego zbudowanego w ramach Projektu.
SOFT.PAAS.65	Panel administracyjny musi zapewniać możliwość zarządzania i monitorowania Usług PaaS wszystkich Klientów (oraz ich parametrów)

5.2.4. Cloud API

ID wymagania	**Treść wymagania**
SOFT.API.1	Cloud API musi zapewnić warstwę abstrakcji, która pozwoli w spójny, łatwy do wykorzystania sposób udostępnić wewnętrzne interfejsy API wszystkich Podsystemów oraz funkcjonalności wchodzących w skład Systemu dla użytkowników zewnętrznych - w szczególności musi udostępniać przez API funkcjonalności dla Klientów wszystkich Usług opartych o IaaS, PaaS, informacje nt. rozliczeń oraz faktur (Billing) oraz pełną obsługę konta Klienta (organizacji Klienta) w ramach Podsystemu (SSO).
SOFT.API.2	Cloud API musi realizować wymagania Rozporządzenia Ministra Nauki i Informatyzacji z dnia 19 października 2005 r. w sprawie testów akceptacyjnych oraz badania oprogramowania interfejsowego.
SOFT.API.3	Wymagane jest dostarczenie dokumentacji Cloud API wraz z przykładami dla każdej metody (w języku angielskim).
SOFT.API.4	Muszą być dostarczony opis wszystkich kodów oraz statusów odpowiedzi każdej metody API (w języku angielskim).
SOFT.API.5	Udostępniany endpoint API musi być zabezpieczony certyfikatem SSL (dostarczonym przez Zamawiającego).
SOFT.API.6	Cloud API powinno stanowić spójny interfejs API - a zatem, jeżeli Wykonawca planuje wdrożyć Podsystemy, które posiadają różne typy danych w wywołaniach API, Cloud API musi zapewnić jeden wybrany typ danych dla wszystkich wywołań.
SOFT.API.7	Cloud API oprócz endpointów API musi dostarczyć aplikację/narzędzie działające w linii poleceń (CLI), instalowane przez użytkownika na jego komputerze i działające na najpopularniejszych systemach operacyjnych (Linux, Windows 7 (i nowsze), Mac OS X 10.8 (i nowszy), FreeBSD), zapewniające pełną funkcjonalność Cloud API z linii poleceń (metody powinny być odwzorowane w odpowiednich argumentach i opcjach). Aplikacja taka umożliwi np. administratorom bądź developerom wykonywać operacje na platformie

	bez potrzeby integracji z API a za pomocą gotowego narzędzia, które można użyć/wykorzystać we własnych aplikacjach/skryptach. Aplikacja ta jest aplikacją CLI pozwalającą zarządzać i monitorować (jak i weryfikować rozliczenia) wszystkich Usług dostarczanych w ramach Systemu i stanowi kolejny (oprócz SelfService i API) interfejs komunikacji z platformą.
SOFT.API.8	Cloud API musi być zintegrowane z rozwiązaniem Apache DeltaCloud.
SOFT.API.9	Cloud API w przypadku obsługi klienta/użytkownika danego Partnera musi ukryć metody dot. rozliczeń, jako że rozliczenia tego typu klientów (klientów Partnerów) będą dokonywane przez tychże partnerów a nie Zamawiającego.
SOFT.API.10	Licencja Cloud API musi zapewniać możliwość ciągłego rozwoju Systemu przez Zamawiającego (własny zespół), a dopuszczalne są dwa podejścia: przekazanie kodów źródłowych do całego Podsystemu Cloud API wraz z przekazaniem autorskich praw majątkowych, bądź przekazanie kodów źródłowych do całego Podsystemu Cloud API wraz z licencją umożliwiającą rozwój na własne potrzeby Zamawiającego.
SOFT.API.11	Kody źródłowe aplikacji muszą być przekazane w formie umożliwiającej rozwój. Kody źródłowe nie mogą być zaciemnione (nie mogą być poddane obfuskacji, z ang. obfuscation).
SOFT.API.12	Wraz z kodami źródłowymi wymagane jest przekazanie dokumentacji rozwojowej, w szczególności: opis architektury logicznej rozwiązania (modułów), wymaganych i użytych bibliotek i narzędzi, sposób budowania i dystrybucji aplikacji.

5.2.5. SelfService

ID wymagania	Treść wymagania
SOFT.SS.1	SelfService musi umożliwić Klientowi kompleksowe monitorowanie (wszystkich dostępnych przez daną Usługę KPI/metryk), zarządzanie Usługami oraz ich parametrami w ramach oferty biznesowej (w szczególności Usługami IaaS: serwery dedykowane, VPS, Cloud, Storage as a Service, Firewall as a Service, Load Balancer as a Service oraz Usługami PaaS). Musi służyć Klientom jako centralna i główna aplikacja do zarządzania, rozliczania oraz monitorowania wszystkich funkcjonalności udostępnianych przez IaaS, PaaS i Billing w zakresie obsługi produktów i Usług wykorzystywanych przez danego Klienta, uwzględniając przy tym posiadane przez niego uprawnienia dostępu.
SOFT.SS.2	Licencja SelfService musi zapewniać możliwość ciągłego rozwoju Systemu przez Zamawiającego (własny zespół), a dopuszczalne są dwa podejścia: przekazanie kodów źródłowych do całego Podsystemu SelfService wraz z przekazaniem autorskich praw majątkowych, bądź przekazanie kodów źródłowych do całego Podsystemu SelfService wraz z licencją umożliwiającą rozwój na własne potrzeby Zamawiającego.
SOFT.SS.3	Kody źródłowe aplikacji muszą być przekazane w formie umożliwiającej rozwój. Kody źródłowe nie mogą być zaciemnione (nie mogą być poddane obfuskacji, z ang. obfuscation)
SOFT.SS.4	Wraz z kodami źródłowymi wymagane jest przekazanie dokumentacji rozwojowej, w szczególności: opis architektury logicznej rozwiązania (modułów), wymaganych i użytych bibliotek i narzędzi, sposób budowania i dystrybucji aplikacji.

SOFT.SS.5	SelfService musi zapewnić dla każdej Usługi oferowanej przez IaaS oraz PaaS dedykowany obszar Podsystemu (np. zakładkę) zaprojektowany w celu jak najwygodniejszej obsługi wszystkich funkcjonalności oferowanych przez Usługę.
SOFT.SS.6	SelfService musi zapewnić dla każdej z Usług dedykowaną funkcjonalność monitorowania i wizualizacji wszystkich metryk/KPI udostępnianych przez daną funkcjonalność IaaS bądź PaaS.
SOFT.SS.7	SelfService musi zapewnić dla każdej z Usług stan rozliczenia (kwotowy oraz jednostki rozliczeniowe) danej Usługi wraz z możliwością filtrowania oraz eksportowania.
SOFT.SS.8	SelfService musi zapewnić dedykowany obszar interfejsu agregujący wszystkie metryki/KPI w celu monitorowania zbiorczo stanu wszystkich Usług IaaS i PaaS. Dane powinny być wyświetlane w ujęciu tabelarycznym oraz za pomocą wykresów w ujęciu godzinnym, dniowym, tygodniowym, miesięcznym i rocznym. Musi być możliwość eksportu wyświetlanych danych.
SOFT.SS.9	SelfService musi zapewnić dedykowany obszar interfejsu użytkownika dla historii rozliczeń, płatności, faktur i umów w ramach integracji z Podsystemem Biling.
SOFT.SS.10	SelfService musi zapewnić dedykowany obszar interfejsu użytkownika umożliwiający przeglądanie, przeszukiwanie i filtrowanie logów każdej z Usług - zarówno wszystkich Usług zbiorczo jak i poszczególnych Usług osobno.
SOFT.SS.11	SelfService musi realizować kontrolę dostępu do poszczególnych funkcjonalności na podstawie roli użytkownika określonej przez SSO.
SOFT.SS.12	Zarządzanie Usługą: SelfService musi wyświetlać na bieżąco stan zleconego zadania dla Usługi (np. stworzenie serwera wirtualnego IaaS, deployment aplikacji na PaaS, itd.) za pomocą informacji w postaci procentowej zmieniającej się bez przeładowania strony (AJAX).
SOFT.SS.13	Zarządzanie Usługą: SelfService musi wyświetlać na bieżąco logi oraz wykonywane operacje zleconego zadania dla Usługi (np. stworzenie serwera wirtualnego IaaS, deployment aplikacji na PaaS, itd.) bez przeładowania strony (AJAX).
SOFT.SS.14	SelfService musi w sposób czytelny i widoczny wyświetlać wszystkie parametry danej Usługi (np. status danej Usługi, adres IPv4 i IPv6 serwera cloud, adres URL pod którym dostępna jest aplikacja PaaS po jej uruchomieniu, itp.).
SOFT.SS.15	Wszystkie krytyczne operacje wpływające na działanie Usługi muszą być (mimo zalogowania) potwierdzane hasłem zalogowanego użytkownika (jeżeli ma uprawnienie do danej operacji) lub hasłem jednorazowym - jeśli jest wykorzystywane przez danego użytkownika. Przykładem krytycznych operacji Usług jest: usunięcie Usługi, zmiana hasła root/Administratora serwera, restart działającej Usługi, itp.
SOFT.SS.16	SelfService musi implementować przeglądanie/filtrowanie i nawigację typu faceted (tzw. nawigacja fasetowa) zapewniając Klientom łatwą nawigację oraz filtrowanie Usług oraz ich parametrów.
SOFT.SS.17	SelfService musi umożliwić przypisywanie tagów do usług w celu szybszego przeglądania/filtrowania dostępnych Usług.
SOFT.SS.18	SelfService musi umożliwić zapisanie parametrów tworzonej Usługi jako szablonu, do ponownego użytku oraz umożliwić tworzenie nowych Usług z wykorzystaniem zapisanych szablonów.

SOFT.SS.19	SelfService musi udostępniać wizualizację real time logów danej Usługi bez przeładowania strony (AJAX).
SOFT.SS.20	SelfService musi zapewnić konfigurowalny mechanizm powiadomień mailowych nt. wybranych operacji na Usłudze bądź jej parametrach wraz z konfiguracją reguł powiadomień dla każdego z użytkowników osobno (np. notyfikacja email nt. restartu serwera, notyfikacja email nt. automatycznego stworzenia nowej instancji aplikacji podczas autoskalowania, itp).
SOFT.SS.21	W przypadku łączenia się Usług (np. kilka serwerów wirtualnych podłączonych do load balancera, kilka instancji aplikacji osadzonej na PaaS podłączonych do instancji bazy danych) SelfService musi zapewnić reprezentację graficzną (w postaci diagramów) wraz z reprezentacją jakie Usługi w jaki sposób są połączone.
SOFT.SS.22	SelfService musi zapewnić konfigurator (wizard) dla uruchomienia każdej z Usług, wizualizując liczbę ekranów konfiguracji/parametryzacji danej Usługi i procent zaawansowania.
SOFT.SS.23	SelfService musi zapewnić pomoc kontekstową podczas zmiany każdego z parametrów Usługi.
Wymagania dla Usług IaaS	
SOFT.SS.25	SelfService musi umożliwiać, po zakończonym provisioningu serwera (cloud/vps/dedykowanego/share-hosting), wyświetlenie za pomocą pop-up hasła dla użytkownika root (w przypadku serwerów Linux/FreeBSD) bądź administratora (dla serwerów Windows).
SOFT.SS.26	SelfService musi umożliwić zarządzanie kluczami publicznymi SSH dla wszystkich typów serwerów uwzględniając nadane uprawnienia do serwerów.
SOFT.SS.27	SelfService musi umożliwiać, po zakończonym provisioningu serwera (cloud/vps/dedykowanego/share-hosting), wysłanie na adres email użytkownika, który go stworzył hasła dla użytkownika root (w przypadku serwerów Linux) bądź administratora (dla serwerów Windows).
SOFT.SS.28	SelfService musi udostępniać terminal maszyny wirtualnej cloud/vps w przeglądarce.
SOFT.SS.29	SelfService musi udostępnić zdalną konsolę zarządzania sprzętem serwera dedykowanego w przeglądarce.
SOFT.SS.30	SelfService musi udostępnić opcję zdalnej konsoli za pomocą protokołu VNC (serwery Linux) bądź Remote Desktop Connection (serwery Windows), umożliwiając definiowanie portu oraz adresów źródłowych IP, które mają dostęp do Usługi.
Wymagania dla integracji z Podsystemem Billing oraz rozliczeń Usług	
SOFT.SS.31	SelfService musi zapewniać wyświetlanie obecnego stanu rozliczenia konta.
SOFT.SS.32	SelfService musi udostępniać wygenerowane faktury (pro-forma, faktury oraz faktury korekt) dla danego Klienta (integracja z Podsystemem Billing).
SOFT.SS.33	SelfService musi zapewniać automatyczne pobieranie płatności zgodnie ze zdefiniowanym trybem bilingowania (integracja z Podsystemem Billing).
SOFT.SS.34	SelfService musi udostępniać historię rekordów rozliczeniowych, faktur oraz płatności (integracja z Podsystemem Billing).
SOFT.SS.35	SelfService musi umożliwić płatność za pomocą integracji z Podsystemem Billing.
SOFT.SS.36	SelfService musi udostępnić historię prób pobrania płatności (jeżeli były nieudane) oraz

	czytelnie zakomunikować dlaczego Usługi/konto zostały zablokowane.
SOFT.SS.37	SelfService musi w przypadku blokady Usługi (bądź konta - czyli wszystkich Usług) w przypadku braku płatności zablokować wszystkie udostępniane funkcjonalności, oprócz: - możliwości dokonania opłaty za Usługi - możliwości pobrania faktur
Wymagania dla Usług PaaS	
SOFT.SS.38	SelfService dla każdej uruchomionej aplikacji musi zapewnić dedykowany obszar w interfejsie użytkownika (np. zakładkę).
SOFT.SS.39	SelfService dla każdej bazy danych aplikacji musi zapewnić dedykowany obszar w interfejsie użytkownika (np. zakładkę).
SOFT.SS.40	SelfService musi udostępniać możliwość tworzenia snapshotów wybranej bazy danych.
SOFT.SS.41	SelfService musi udostępniać możliwość exportu wybranej bazy danych.
SOFT.SS.42	SelfService musi udostępniać możliwość importu wybranej bazy danych.
Wymagania dla Programu Partnerskiego	
SOFT.SS.43	SelfService musi identyfikować (integracja z SSO) czy dany Klient jest Partnerem (uczestnikiem Programu Partnerskiego), klientem Partnera czy też Klientem Zamawiającego.
SOFT.SS.44	SelfService musi zapewnić Partnerom dedykowany obszar interfejsu użytkownika umożliwiający zarządzanie klientami/organizacjami/użytkownikami Partner (integracja z SSO), zarządzanie oraz monitorowanie wszystkich usług klientów Partnera.
SOFT.SS.45	SelfService musi zapewnić Partnerom dedykowany obszar interfejsu użytkownika pobieranie rekordów bilingowych każdego klienta (integracja z Billing).
SOFT.SS.46	SelfService w przypadku obsługi się klienta/użytkownika danego Partnera musi ukryć obszar rozliczeń, jako że rozliczenia tego typu klientów (klientów Partnerów) będą dokonywane przez tychże Partnerów a nie przez Zamawiającego.

5.2.6. Billing

ID wymagania	Treść wymagania
SOFT.BILL.1	Billing musi zapewniać elastyczne rozliczanie wszystkich Usług oferowanych przez System bazując na określonych atomowych jednostkach metrycznych oferowanych przez daną Usługę.
SOFT.BILL.2	Billing musi integrować się z każdym Podsystemem Platformy oprogramowania, który odpowiedzialny jest za dostarczanie Usług dla klienta w celu aktywacji/deaktywacji Usług.
SOFT.BILL.3	Billing musi umożliwić modelowanie rozliczeń na jednostkach rozliczeniowych za pomocą reguł matematycznych i logicznych w taki sposób aby umożliwić tworzenie złożonych konfiguracji modeli rozliczeniowych.
SOFT.BILL.4	Billing musi umożliwiać definiowanie produktów rozliczeniowych za pomocą reguł matematycznych i logicznych w taki sposób aby umożliwić tworzenie złożonych konfiguracji Usług.
SOFT.BILL.5	Billing musi umożliwiać grupowanie Usług w grupy Usług.
SOFT.BILL.6	Billing musi mieć modułową budowę systemu akwizycji danych (umożliwiać pobieranie danych z różnych źródeł w różnych formatach).

SOFT.BILL.7	Billing musi umożliwiać naliczanie Usług jednorazowych.
SOFT.BILL.8	Billing musi umożliwiać naliczanie Usług abonamentowych.
SOFT.BILL.9	Billing musi umożliwiać naliczanie Usług w planie taryfowym Pay-As-You-Go (za faktycznie wykorzystane zasoby).
SOFT.BILL.10	Billing musi umożliwiać wsparcie dla rozliczeń typu post-paid oraz pre-paid.
SOFT.BILL.11	Billing musi umożliwiać konfigurowanie mnożników kosztowych.
SOFT.BILL.12	Billing musi umożliwiać definiowanie okresów rozliczeniowych dla każdego Klienta indywidualnie (z dokładnością do minut).
SOFT.BILL.13	Billing wraz z Podsystemem SSO muszą zapewnić wsparcie obsługi oraz zarządzania Partnerami, w tym: umożliwiać określenie globalnej stawkę rabatów dla wszystkich Usług dla Partnera, dedykowaną stawkę rabatu dla poszczególnych Usług dla wybranego Partnera oraz zarządzanie Partnerami jak i jego klientami, w szczególności umożliwiać zmianę poziomu partnerstwa.
SOFT.BILL.14	Billing musi zapewnić generowanie, udostępnianie i przechowywanie dla Partnerów rekordów rozliczeniowych wszystkich Usług wszystkich klientów danego partnera w formacie CSV.
SOFT.BILL.15	Billing musi umożliwiać definiowanie promocji określając: czas trwania promocji; Usługi uwzględnione w promocji; typ rabatu globalnie (dla wszystkich Usług) bądź dla każdego z Usług, typy promocji to: zniżkowa (obniżenie wartości Usług) wraz z definicją wartości obniżenia: procentowa lub kwotowa - bądź typ: zwiększenie salda (czyli przypisanie wartości kwotowej dla salda); definicję dla kogo promocja jest dostępna - czy dla wszystkich klientów wg. stażu; możliwość przypisania promocji do wybranych Partnerów.
SOFT.BILL.16	Billing musi umożliwiać rozliczenie w walutach: PLN, EUR, USD - zgodnie z polskim prawem.
SOFT.BILL.17	Billing musi umożliwiać automatyczną obsługę kursów walut w oparciu o kurs NBP.
SOFT.BILL.18	Billing musi umożliwiać wsparcie dla wielu walut w tym wymagane: PLN, EUR, USD.
SOFT.BILL.19	Billing musi umożliwiać definiowanie oraz rozliczenie Usług pakietowych (połączenie kilku Usług) w modelu jednorazowym.
SOFT.BILL.20	Billing musi umożliwiać definiowanie oraz rozliczenie Usług pakietowych (połączenie kilku Usług) w modelu abonamentowym.
SOFT.BILL.21	Billing musi umożliwiać definiowanie oraz rozliczenie Usług pakietowych (połączenie kilku Usług) w modelu Pay-As-You-Go.
SOFT.BILL.22	Billing musi umożliwiać definiowanie oraz rozliczenie Usług pakietowych (połączenie kilku Usług) w modelu mieszanym (np. część produktów w modelu abonamentowym a część w modelu jednorazowym, itp).
SOFT.BILL.23	Billing musi umożliwiać automatyczne przełączanie na wyższy bądź poziom cenowy czy też pakiet na podstawie zdefiniowanych warunków.
SOFT.BILL.24	Billing musi dopuszczać Usługi, pakiety bezpłatne.
SOFT.BILL.25	Billing musi umożliwiać definiowanie oraz rozliczenie promocji do Usług łączonych.
SOFT.BILL.26	Billing musi umożliwiać ręczne oraz automatyczne fakturowanie zgodnie z prawem Polski oraz Unii Europejskiej.
SOFT.BILL.27	Billing musi umożliwiać generowanie raportów dla rozliczeń w zadanym okresie czasowym, dla zadanych Usług, w postaci tabelarycznej, wykresów oraz exportu do pliku

	CSV.
SOFT.BILL.28	Billing musi zapewnić produkty oraz konta testowe.
SOFT.BILL.29	Billing musi obsługiwać importowanie stawek/planów cenowych z plików CSV.
SOFT.BILL.30	Billing musi obsługiwać nielimitowaną ilość Usług, promocji, Klientów.
SOFT.BILL.31	Billing musi oferować wsparcie dla masowej edycji rekordów.
SOFT.BILL.32	Billing musi umożliwiać dla poszczególnych Usług określanie rozpoczęcia i daty końcowej w której Usługa jest aktywna.
SOFT.BILL.33	Billing musi oferować wsparcie dla definiowania i generowania automatycznie raportów okresowych uwzględniających co najmniej: zamówienia/odnowienia/rezygnację z Usług, płatności/rozliczenia Usług.
SOFT.BILL.34	Billing musi oferować wsparcie do automatycznej wysyłki raportów drogą e-mail.
SOFT.BILL.35	Billing musi udostępniać pełne API umożliwiającego kontrolę/konfigurację oraz dostęp do wszystkich funkcjonalności, danych rozliczeniowych oraz raportów.
SOFT.BILL.36	Billing musi zapewnić integrację z Podsystemem SSO w celu uwierzytelniania i autoryzacji do zasobów oraz identyfikacji klientów.
SOFT.BILL.37	Billing musi wspierać grupowanie klientów wg ich klasyfikacji biznesowej oraz nadawanie im parametrów rozliczeniowych (np. inne ceny na poszczególne Usługi, rabaty globalne, limity sprzedawanych Usług). Źródłem klasyfikacji biznesowej klientów jest Podsystem SSO.
SOFT.BILL.38	Billing musi oferować wsparcie dla overbookingu jako podstawy przyznawania rabatów.
SOFT.BILL.39	Billing musi oferować wsparcie dla kontrolowanego wywłaszczania (niższego priorytetu usług) jako podstawy przyznawania rabatów.
SOFT.BILL.40	Billing musi oferować wsparcie analityczne dla ustalania cen każdego zasobu rozliczeniowego w ujęciu czasowym.
SOFT.BILL.41	Billing musi umożliwić określenie sposobu migracji Usług: - downgrade - z końcem okresu rozliczeniowego lub z datą powstania zdarzenia. Pozostałe środki powinny być zaksięgowane na poczet następnego okresu rozliczeniowego - upgrade - z końcem okresu rozliczeniowego lub z datą powstania zdarzenia. Jeśli użytkownik wybierze datę powstania zdarzenia wymagane jest pobranie opłaty (różnicy).
SOFT.BILL.42	Billing musi umożliwić definicję wspieranych rodzajów płatności dla każdej Usługi.
SOFT.BILL.43	Billing musi umożliwić definiowanie czy jest okres próbny (trial) oraz jak długo trwa dla każdej Usługi (liczba dni).
SOFT.BILL.44	Billing musi umożliwiać wsparcie dla różnych formatów daty (w szczególności: DDMMYYYY, YYYYMMDD, DD-MM-YYYY, YYYY-MM-DD, DD.MM.YYYY, YYYY.MM.DD) oraz wsparcie przy czym zapisu miesiąca (MM) cyframi rzymskimi oraz arabskimi.
SOFT.BILL.45	Billing musi wspierać wiele stawek podatku VAT wraz z definicją okresu/przedziału czasowego wsparcia dla danej stawki.
SOFT.BILL.46	Billing musi umożliwiać zdefiniowanie maksymalnej ilości jednostek do wykorzystania w ramach danego produktu np. 1GB RAM, 10GB transferu danych z określeniem stawki za dalsze wykorzystanie poza limitem np. 10zł/1GB transferu.
SOFT.BILL.47	Billing musi umożliwiać określenie przedziałów cenowych za zużyty zasób np. transfer danych do 10GB koszt 10zł/GB, powyżej 8zł/GB (mnożniki kosztowe).
SOFT.BILL.48	Billing musi umożliwiać przyznawanie darmowych jednostek w danej Usłudze za

	korzystanie z innych Usług.
SOFT.BILL.49	Billing musi umożliwiać tworzenie produktów systemowych - dodane dla każdego użytkownika i konfigurowalne wspólnie dla wszystkich np. darmowy adres e-mail.
SOFT.BILL.50	Billing musi umożliwiać określenie minimalnego zużycia czasowego/jednostek w modelu Prepaid (np. naliczone z góry 1h użycia Usługi).
SOFT.BILL.51	Billing musi umożliwiać weryfikację czy stan finansowy pozwala na włączenie Usługi i na jaki okres w modelu Prepaid.
SOFT.BILL.52	Billing musi zapewnić automatyczne procesowanie ponagleń płatności wraz z powiadomieniami e-mail klientów.
SOFT.BILL.53	Billing musi umożliwiać określanie okresów karencji, po których następuje zablokowanie Usługi oraz sposobów notyfikacji e-mail wraz z ich treścią.
SOFT.BILL.54	Billing musi umożliwiać określanie ilości prób i okresów czasu po jakich następuje ponowna próba pobrania opłaty (po nieudanej próbie).
SOFT.BILL.55	Billing musi wspierać wznawianie Usług zawieszonych.
SOFT.BILL.56	Billing musi umożliwiać konfigurację szablonów e-mail (ponaglenia, podziękowania za płatność) - możliwość zdefiniowania szablonu kodem HTML z wykorzystaniem predefiniowanych atrybutów określających różne elementy konta np. imię, nazwisko, wymaganą kwotę i termin płatności.
SOFT.BILL.57	Billing musi umożliwiać obsługę płatności: karty kredytowe, przelewy tradycyjne bazujące na subkontach, płatności online. System obsługi płatności zostanie ustalony wspólnie z Zamawiającym na etapie analizy.
SOFT.BILL.58	Billing musi umożliwiać tworzenie raportu uwzględniającego: - płatności danego miesiąca, wybranego okresu - przeterminowane płatności - statystyki zużycia zasobów danego miesiąca, wybranego okresu - raporty finansowo-księgowe (uwzględnione korekty).
SOFT.BILL.59	Billing musi umożliwić wznawianie Usług - np. wyłączonych z powodu braku płatności (możliwy nowy termin początkowy okresu rozliczeniowego).
SOFT.BILL.60	Billing musi umożliwić zmniejszenie/zwiększenie ceny Usługi dla konkretnego Klienta o daną kwotę.
SOFT.BILL.61	Billing musi umożliwić ustawienie ceny Usługi dla konkretnego Klienta na daną kwotę.
SOFT.BILL.62	Billing musi umożliwiać edycję zdarzenia rozliczeniowego (źle naliczona opłata za użycie) wraz zachowaniem historii zmian oraz automatyzacją tworzenia faktur korygujących.
SOFT.BILL.63	Billing musi umożliwiać przeksięgowanie płatności na inną należność (wraz ze śledzeniem historii takowych operacji).
SOFT.BILL.64	Billing musi umożliwiać zwrot nadpłaty lub przeksięgowanie na kolejną płatność (wraz ze śledzeniem historii takowych operacji). Operacja zwrotu środków obsługiwana będzie przez system płatności ustalonym wspólnie z Zamawiającym podczas fazy analizy.
SOFT.BILL.65	Billing musi umożliwiać automatycznie naliczanie odsetek.
SOFT.BILL.66	Billing musi zapewnić migrację Usług - np. ze względu na wycofanie z oferty danej Usługi.
SOFT.BILL.67	Billing musi umożliwić wystawianie faktur (w tym faktury korygujące) i not odsetkowych (w tym faktur elektronicznych).
SOFT.BILL.68	Billing musi umożliwiać automatyczną wysyłkę faktur i not odsetkowych oraz ich wysyłkę

	na żądanie za pomocą e-mail oraz korespondencji masowej (papierowej).
SOFT.BILL.69	Billing musi umożliwiać wystawienie, przesyłanie i przechowywanie faktur w formie elektronicznej zgodnie z obowiązującymi przepisami prawa.
SOFT.BILL.70	Billing musi umożliwić generowanie oraz przechowywanie dla każdego stworzonego dokumentu (faktura, faktura korygująca, nota odsetkowa, itd) obrazu elektronicznego w postaci plików PDF.
SOFT.BILL.71	Billing musi umożliwiać udostępnianie obrazów elektronicznych faktur dla Podsystemu SelfService, który będzie udostępniał je Klientom.
SOFT.BILL.72	Billing musi umożliwić generowanie oraz przechowywanie dla każdego stworzonego dokumentu (faktura, faktura korygująca, nota odsetkowa, itd) plików umożliwiających import owych dokumentów w programie Symfonia wersja min. Premium 2014.
SOFT.BILL.73	Billing musi umożliwiać konfigurację szablonów faktur.
SOFT.BILL.74	Billing musi zapewnić definiowanie ograniczeń kwotowych i ilościowych per Klient, Usługa bądź łącznie (np. aby jeden Klient nie mógł wykupić zdefiniowanej liczby Usług - limit).
SOFT.BILL.75	Billing musi zapewnić definiowanie limitu kredytowego dla rozliczeń w modelu post-paid.
SOFT.BILL.76	Billing musi zapewnić windykację (przypomnienia, wyłączanie Usług, wznawianie Usług).
SOFT.BILL.77	Billing musi zapewnić możliwość przyszłej modyfikacji/dostosowania Podsystemu za pomocą: API oraz pluginów/modułów.
SOFT.BILL.78	Billing musi zapewnić zmienność względem: pory dnia, dnia tygodnia i dnia miesiąca.
SOFT.BILL.79	Billing musi zapewnić funkcjonalność kuponów rabatowych, które identyfikują Usługę bądź promocję oraz umożliwiają wprowadzenie ograniczeń czasowych dla kuponu oraz ograniczeń dla wykorzystania kuponu przez Klientów w zadanym stażu oraz wybranych Partnerów.
SOFT.BILL.80	Billing musi umożliwić przedstawienie raportu zasobów rozliczeniowych (wraz z przychodami) w zadanym okresie czasowym w celu określenia rentowności Usług.
SOFT.BILL.81	Billing musi umożliwiać przedstawianie powyższych raportów przekładając je na Usługi nieaktywne.

5.2.7. ESB

ID wymagania	Treść wymagania
SOFT.ESB.1	Każdy Podsystem komunikujący się po API bądź udostępniający API musi mieć zaimplementowany endpoint na ESB i komunikować się przez ESB. W uzasadnionych przypadkach Zamawiający może, na etapie opracowywania projektu technicznego, dopuścić bezpośrednią komunikację między Podsystemami.
SOFT.ESB.2	ESB musi posiadać mechanizm definiowania, implementacji, wdrażania i zarządzania usługami realizującymi dostęp do integrowanych Podsystemów.
SOFT.ESB.3	ESB zakłada istnienie usług prywatnych i publicznych. Usługi prywatne są dostępne jedynie w obrębie Systemu i nie mogą być bezpośrednio wywoływane przez Klientów Systemu.
SOFT.ESB.4	ESB musi posiadać mechanizm umożliwiający planowe i cykliczne uruchamianie usług Systemu. Zarządzanie planowanymi do uruchomienia usługami musi odbywać się w

	sposób spójny z jednego miejsca Systemu na zasadzie definiowania harmonogramu wywołań.
SOFT.ESB.5	ESB musi zapewniać funkcjonalność transformacji komunikatów i transportowania ich używając różnych protokołów: HTTP, HTTPS, JDBC, JMS, Web Services, AMQP, FTP, SSH, SOAP, REST/JSON.
SOFT.ESB.6	ESB musi zapewnić możliwość tworzenia konektorów do usług, umożliwiających łatwe podłączanie kolejnych usług w oparciu o konfigurację danego konektora.
SOFT.ESB.7	ESB musi zapewniać usługi zarówno synchroniczne jak i asynchroniczne.
SOFT.ESB.8	ESB musi zapewnić GUI WEB zapewniające funkcjonalności zarządzania oraz monitorowania rozwiązania.
SOFT.ESB.9	ESB musi dostarczać usługi translacji protokołów.
SOFT.ESB.10	ESB musi umożliwiać filtrowanie komunikatów na podstawie zawartości, przy wykorzystaniu parametrów definiowanych przez użytkownika.
SOFT.ESB.11	ESB musi umożliwiać trwałe przechowywanie komunikatów.
SOFT.ESB.12	ESB musi umożliwiać tworzenie architektury wyjątków, która może przechwytywać wyjątki, generować transakcje kompensacyjne i generować raporty o błędach.
SOFT.ESB.13	ESB musi zapewniać mechanizm transakcji XA (XA Transactions).
SOFT.ESB.14	ESB musi umożliwiać zachowanie integralności, niezaprzeczalności, poufności i autentyczności komunikacji.
SOFT.ESB.15	ESB musi zapewnić API do tworzenia nowych konektorów oraz wsparcia dla nowych nieobsługiwanych protokołów.

5.2.8.SSO

ID wymagania	Treść wymagania
Architektura i integracja z pozostałymi Podsystemami	
SOFT.SSO.1	SSO musi stanowić jedyny mechanizm uwierzytelniania dla wszystkich Podsystemów dostępnych poprzez przeglądarkę internetową.
SOFT.SSO.2	SSO jako podstawowy protokół musi wykorzystywać oAuth w wersji 2.
SOFT.SSO.3	SSO musi stanowić centralny rejestr wszystkich użytkowników wykorzystywanych w ramach Systemu.
SOFT.SSO.4	SSO musi stanowić centralny rejestr informacji o przetwarzaniu i udostępnianiu danych osobowych, wymagany przez Ustawę o ochronie danych osobowych.
SOFT.SSO.5	Podsystemy wchodzące w skład Platformy oprogramowania muszą rejestrować w SSO zdarzenia związane z przetwarzaniem danych osobowych użytkowników w zakresie określonym wytycznymi Ustawy o ochronie danych osobowych i aktów wykonawczych do tej Ustawy.
SOFT.SSO.6	SSO musi umożliwiać Podsystemom przeprowadzenie dodatkowego uwierzytelnienia użytkownika przed wykonaniem istotnych z perspektywy bezpieczeństwa operacji.
SOFT.SSO.7	SSO musi umożliwiać zdefiniowanie listy dostawców usług (Service Provider), którzy mogą korzystać z SSO jako dostawcy tożsamości (Identity Provider).

SOFT.SSO.8	SSO musi umożliwiać zarządzanie wyglądem każdej podstrony za pomocą szablonów.
SOFT.SSO.9	SSO musi być zintegrowane z bramką SMS ustaloną na etapie przygotowywania projektu technicznego.
LDAP	
SOFT.SSO.10	W skład Podsystemu SSO musi wchodzić usługa katalogowa oparta o protokół LDAP.
SOFT.SSO.11	SSO musi przechowywać wszystkie dane o użytkownikach w usłudze katalogowej LDAP.
SOFT.SSO.12	SSO musi przechowywać wszystkie informacje o zdefiniowanych organizacjach w katalogu LDAP.
SOFT.SSO.13	SSO musi przechowywać wszystkie informacje o członkostwie użytkowników w organizacji w katalogu LDAP.
SOFT.SSO.14	LDAP wchodzący w skład SSO musi zostać wdrożony w konfiguracji klastra multi-master replication.
Role i grupy	
SOFT.SSO.15	SSO musi zarządzać uprawnieniami, rolami, użytkownikami, grupami i organizacjami ze wszystkich Podsystemów.
SOFT.SSO.16	SSO musi umożliwiać definiowanie nowych ról użytkowników.
SOFT.SSO.17	SSO musi umożliwiać edycję zdefiniowanych wcześniej ról użytkowników.
SOFT.SSO.18	SSO musi umożliwiać wygodne zarządzanie powiązaniami ról z użytkownikami.
SOFT.SSO.19	SSO musi umożliwiać tworzenie grup użytkowników.
SOFT.SSO.20	SSO musi umożliwiać wygodne zarządzanie członkostwem użytkowników w grupach.
SOFT.SSO.21	SSO, w ramach procesu uwierzytelniania, musi udostępniać Podsystemom informacje o wszystkich rolach przypisanych (zarówno bezpośrednio, jak i za pośrednictwem grup) do uwierzytelnianego użytkownika.
SOFT.SSO.22	SSO musi zapewniać mechanizmy służące do oznaczania użytkowników w zależności od ich klasyfikacji biznesowej (np. "Klient", "Partner", "Złoty Partner" itp.).
Organizacje	
SOFT.SSO.23	SSO musi umożliwiać definiowanie nowych organizacji.
SOFT.SSO.24	SSO musi umożliwiać modyfikowanie nazwy organizacji.
SOFT.SSO.25	SSO musi umożliwiać definiowanie użytkowników należących do organizacji.
SOFT.SSO.26	SSO musi umożliwiać generowanie automatycznych stron logowania o adresach url typu: nazwa_organizacji.domenaplatformy.pl, które uwierzytelniają użytkowników logujących się przez taką stronę z organizacją o nazwie: nazwa_organizacji.
SOFT.SSO.27	SSO musi umożliwiać ustawienie loga dla automatycznie wygenerowanych stron logowania.
SOFT.SSO.28	SSO musi umożliwić Partnerom tworzenie organizacji dla ich klientów.
SOFT.SSO.29	SSO musi umożliwić Partnerom pełne zarządzanie organizacjami ich klientów (realizować wszystkie funkcje tak, jakby to klienci je realizowali).
Uprawnienia w ramach SSO	
SOFT.SSO.30	SSO musi umożliwiać nadanie uprawnień do każdej atomowej operacji wykonywanej w SSO.
SOFT.SSO.31	SSO musi umożliwiać nadanie uprawnień do odczytu każdego atomowego pola danych przechowywanych w SSO.
SOFT.SSO.32	SSO musi umożliwiać nadanie uprawnień do edycji każdego atomowego pola danych

	przechowywanych w SSO.
SOFT.SSO.33	SSO musi umożliwiać nadanie pojedynczego uprawnienia zezwalającego na dostęp do wszystkich organizacji zdefiniowanych w SSO.
SOFT.SSO.34	SSO musi umożliwiać nadanie uprawnienia dostępu do każdej pojedynczej organizacji zdefiniowanej w SSO.
SOFT.SSO.35	SSO musi umożliwiać nadanie uprawnienia dostępu do organizacji, do której należy dany użytkownik.
SOFT.SSO.36	SSO musi wymagać, by użytkownik wykonujący operację posiadał role, które łącznie dają mu uprawnienia do operacji i pól danych, których dotyczy operacja.
SOFT.SSO.37	SSO musi wymagać, by użytkownik wykonujący operację na koncie innym niż swoje posiadał uprawnienia dostępu do organizacji, do której należy to konto.
SOFT.SSO.38	SSO musi wyświetlać użytkownikowi tylko te pola danych, do których ma on dostęp.
SOFT.SSO.39	SSO musi umożliwiać użytkownikowi edycję tylko tych pól danych, do których ma on dostęp.
SOFT.SSO.40	SSO musi wyświetlać użytkownikowi tylko użytkowników należących do organizacji, do której ma on dostęp.
Uwierzytelnianie: hasło	
SOFT.SSO.37	SSO musi umożliwiać uwierzytelnienie użytkowników w oparciu o login i hasło.
SOFT.SSO.38	SSO musi przechowywać hasła w sposób uniemożliwiający ich odczytanie, z zastosowaniem silnej, kryptograficznie bezpiecznej funkcji skrótów oraz "soli" (salted hash).
SOFT.SSO.39	SSO musi umożliwiać użytkownikowi zmianę własnego hasła.
SOFT.SSO.40	SSO musi umożliwiać użytkownikowi posiadającemu odpowiednie uprawnienia zmianę hasła innego użytkownika.
SOFT.SSO.41	SSO powinno wyświetlać informację o sile nowego hasła podczas zmiany hasła użytkownika.
SOFT.SSO.42	SSO musi weryfikować zgodność nowego hasła podczas jego zmiany z określoną konfiguracyjnie polityką haseł.
SOFT.SSO.43	Mechanizmy określania polityki haseł w SSO powinny umożliwiać stworzenie polityki haseł odzwierciedlającej wytyczne GIODO.
SOFT.SSO.44	Mechanizmy określania polityki haseł w SSO powinny umożliwiać określenie czasu ważności haseł.
SOFT.SSO.45	SSO musi umożliwiać przypisanie różnych polityk haseł do różnych ról, grup i organizacji użytkowników.
SOFT.SSO.46	SSO musi udostępniać mechanizm resetowania hasła.
SOFT.SSO.47	Mechanizm resetowania hasła musi działać zgodnie z dobrymi praktykami rynkowymi w tym zakresie, np. zgodnie z wytycznymi OWASP Forgot Password Cheat Sheet.
SOFT.SSO.48	Mechanizm resetowania hasła musi być tak zaprojektowany, żeby zapobiegać powszechnie znanym atakom bezpieczeństwa.
Uwierzytelnianie: zewnętrzni dostawcy tożsamości	
SOFT.SSO.49	SSO musi umożliwiać rejestrację konta użytkownika z wykorzystaniem zewnętrznych dostawców tożsamości, w oparciu o protokół oAuth v2.
SOFT.SSO.50	SSO powinno automatycznie uzupełnić dane tworzonego konta danymi otrzymanymi od

	dostawcy tożsamości przy rejestracji za pomocą zewnętrznego dostawcy tożsamości.
SOFT.SSO.51	SSO powinno automatycznie uzupełnić dane rozliczeniowe danymi otrzymanymi od dostawcy tożsamości przy rejestracji za pomocą zewnętrznego dostawcy tożsamości.
SOFT.SSO.52	SSO powinno umożliwić użytkownikowi edycję automatycznie uzupełnionych danych przed ich zapisaniem przy rejestracji za pomocą zewnętrznego dostawcy tożsamości.
SOFT.SSO.53	SSO musi umożliwiać uwierzytelnianie z wykorzystaniem zewnętrznych dostawców tożsamości w oparciu o protokół oAuth v2.
SOFT.SSO.54	SSO musi obsługiwać zewnętrznego dostawcę tożsamości Facebook.
SOFT.SSO.55	SSO musi obsługiwać zewnętrznego dostawcę tożsamości Google.
SOFT.SSO.56	SSO musi obsługiwać zewnętrznego dostawcę tożsamości Windows Live.
SOFT.SSO.57	SSO musi obsługiwać zewnętrznego dostawcę tożsamości ePUAP.
SOFT.SSO.58	SSO musi umożliwiać użytkownikowi powiązanie jego konta z dowolną liczbą zewnętrznych dostawców tożsamości.
SOFT.SSO.59	SSO musi umożliwiać użytkownikowi usuwanie powiązań zewnętrznych dostawców tożsamości z jego kontem użytkownika.
SOFT.SSO.60	SSO musi umożliwiać administratorowi (na podstawie uprawnień) usuwanie powiązań zewnętrznych dostawców tożsamości z kontami użytkowników.
Uwierzytelnianie: dwustopniowe uwierzytelnianie	
SOFT.SSO.61	SSO musi umożliwiać użytkownikowi aktywację dwustopniowego uwierzytelniania.
SOFT.SSO.62	SSO musi obsługiwać dwustopniowe uwierzytelnianie w oparciu o kody SMS.
SOFT.SSO.63	SSO musi obsługiwać hasła jednorazowe oparte o algorytm HOTP (RFC 4226), w sposób kompatybilny z aplikacją Google Authenticator.
SOFT.SSO.64	SSO musi obsługiwać hasła jednorazowe oparte o algorytm TOTP (RFC 6238), w sposób kompatybilny z aplikacją Google Authenticator.
SOFT.SSO.65	SSO musi generować kody QR na potrzeby konfiguracji haseł jednorazowych.
Panel konfiguracyjny	
SOFT.SSO.66	Administrator musi dysponować panelem konfiguracyjnym, umożliwiającym modyfikację wszystkich opcji konfiguracyjnych SSO.
SOFT.SSO.67	SSO musi umożliwiać administratorowi określenie polityki haseł, definiującej reguły walidacji haseł ustawianych w SSO.
SOFT.SSO.68	SSO musi prowadzić rejestr udostępnień danych osobowych na potrzeby realizacji wymagań Ustawy o ochronie danych osobowych.
SOFT.SSO.69	SSO musi umożliwiać tworzenie wpisów w rejestrze udostępnień danych osobowych.
SOFT.SSO.70	SSO musi umożliwiać przeglądanie wpisów w rejestrze udostępnień danych osobowych.
SOFT.SSO.71	SSO musi umożliwiać oznaczanie wpisów w rejestrze udostępnień danych osobowych jako anulowanych.
Konto użytkownika	
SOFT.SSO.72	SSO musi umożliwiać użytkownikowi samodzielne utworzenie konta.
SOFT.SSO.73	SSO musi umożliwiać użytkownikowi o odpowiednich uprawnieniach utworzenie konta dla innego użytkownika.
SOFT.SSO.74	SSO musi umożliwiać wprowadzenie przy tworzeniu konta użytkownika jego danych osobowych oraz określania dla rejestrowanej organizacji czy jest to osoba fizyczna, firma z siedzibą w Unii Europejskiej bądź firma spoza Unii Europejskiej.

SOFT.SSO.75	SSO musi weryfikować europejskie numery NIP w oparciu o system VIES.
SOFT.SSO.76	SSO musi wymagać weryfikacji adresu e-mail dla konta założonego samodzielnie przez użytkownika.
SOFT.SSO.77	SSO musi wymagać weryfikacji adresu e-mail w przypadku jego samodzielnej zmiany przez użytkownika.
SOFT.SSO.78	SSO musi umożliwiać edycję danych konta użytkownika.
SOFT.SSO.79	SSO musi umożliwiać dezaktywację konta użytkownika.
SOFT.SSO.80	SSO musi umożliwiać (opcjonalnie) usunięcie danych osobowych użytkownika w momencie dezaktywacji jego konta.
SOFT.SSO.81	SSO musi umożliwiać reaktywację wcześniej dezaktywowanego konta użytkownika.
SOFT.SSO.82	SSO musi umożliwiać przeglądanie listy użytkowników.
SOFT.SSO.83	SSO musi umożliwiać filtrowanie listy użytkowników.
SOFT.SSO.84	SSO musi umożliwiać przeszukiwanie bazy użytkowników.
SOFT.SSO.85	SSO musi umożliwiać eksport danych użytkowników.
SOFT.SSO.86	SSO musi spełniać wymagania Ustawy o ochronie danych osobowych.
SOFT.SSO.87	SSO musi prowadzić rejestr wszystkich operacji wykonanych w ramach SSO.
SOFT.SSO.88	SSO musi udostępniać zalogowanemu użytkownikowi wszystkie dane, które należy mu udostępnić na podstawie Ustawy o ochronie danych osobowych.
SOFT.SSO.89	SSO musi udostępniać zalogowanemu użytkownikowi stronę umożliwiającą wgląd w jego dane zarejestrowane w SSO w zakresie wynikającym z nadanych mu uprawnień.
SOFT.SSO.90	SSO musi udostępniać zalogowanemu użytkownikowi możliwość edycji jego danych zarejestrowanych w SSO w zakresie wynikającym z nadanych mu uprawnień.
SOFT.SSO.91	SSO musi udostępniać zalogowanemu użytkownikowi możliwość podglądu rejestru zdarzeń, które dotyczą jego konta użytkownika.
SOFT.SSO.92	SSO musi udostępniać zalogowanemu użytkownikowi możliwość podglądu rejestru zdarzeń, które dotyczą jego danych osobowych.
SOFT.SSO.93	SSO musi umożliwiać zdefiniowanie terminu ważności konta użytkownika.
SOFT.SSO.94	SSO musi automatycznie dezaktywować konta, dla których upłynął termin ważności.
Konto użytkownika: klucze SSH	
SOFT.SSO.95	SSO musi umożliwiać zarejestrowanie dowolnej ilości kluczy publicznych SSH dla użytkownika.
SOFT.SSO.96	SSO musi obsługiwać klucze publiczne SSH w formacie zgodnym z aplikacją OpenSSH.
SOFT.SSO.97	SSO musi obsługiwać klucze publiczne SSH w formacie zgodnym z aplikacją PuTTY.
SOFT.SSO.98	SSO musi umożliwiać konwersję kluczy publicznych użytkownika między obsługiwanymi formatami.
SOFT.SSO.99	SSO musi przechowywać klucze publiczne użytkownika w formacie zgodnym z aplikacją OpenSSH.
SOFT.SSO.100	SSO musi przechowywać klucze publiczne użytkownika w LDAP.
SOFT.SSO.101	SSO musi umożliwiać przeglądanie listy zarejestrowanych kluczy publicznych użytkownika.
SOFT.SSO.102	SSO musi umożliwiać zmianę zarejestrowanych kluczy publicznych użytkownika.
SOFT.SSO.103	SSO musi umożliwiać usuwanie zarejestrowanych kluczy publicznych użytkownika.
SOFT.SSO.104	SSO musi umożliwiać wygenerowanie pary kluczy kryptograficznych algorytmu RSA dla użytkownika.

SOFT.SSO.105	SSO musi umożliwiać wygenerowanie pary kluczy kryptograficznych algorytmu DSA dla użytkownika.

5.2.9. Portal

ID wymagania	Treść wymagania
SOFT.P.1	Portal będzie stanowić platformę do publikacji treści związanych z działalnością Zamawiającego w obszarze IaaS i PaaS.
Zasilenie treścią	
SOFT.P.2	Projekt techniczny Portalu musi zawierać opis architektury informacji Portalu.
SOFT.P.3	Projekt techniczny Portalu musi zawierać spis wszystkich treści, które są niezbędne do rozpoczęcia świadczenia Usług przez Zamawiającego.
SOFT.P.4	Wykonawca musi przygotować wszystkie treści (teksty, uzupełniające materiały graficzne) niezbędne do rozpoczęcia świadczenia Usług przez Zamawiającego.
SOFT.P.5	Wykonawca musi przygotować regulaminy świadczenia Usług przez Zamawiającego w celu ich publikacji na Portalu.
SOFT.P.6	Wykonawca musi przygotować politykę prywatności dla Usług świadczonych przez Zamawiającego w celu ich publikacji na Portalu.
SOFT.P.7	Portal w momencie odbioru musi zawierać wszystkie treści przygotowane przez Wykonawcę.
SOFT.P.8	Portal musi udostępniać wszystkie funkcjonalności niezbędne do zasilenia go treścią opracowaną przez Wykonawcę.
SOFT.P.9	Portal musi udostępniać wszystkie funkcjonalności niezbędne do zaimplementowania docelowej architektury informacji.
SOFT.P.10	Portal musi udostępniać wszystkie funkcjonalności niezbędne do zaimplementowania opracowanego projektu graficznego.
Funkcjonalności administratora i uprawnienia	
SOFT.P.11	Portal musi umożliwić zarządzanie dostępem do treści portalu przez wielu użytkowników, zgodnie z ich uprawnieniami.
SOFT.P.12	Portal musi realizować kontrolę dostępu do poszczególnych funkcjonalności na podstawie roli użytkownika określonej przez SSO.
SOFT.P.13	Portal musi umożliwiać nadanie każdej z ról uprawnień do korzystania z poszczególnych funkcjonalności.
SOFT.P.14	Portal musi umożliwiać nadanie każdej z ról uprawnień do odczytu wybranych rodzajów treści (np. artykuł, opis Usługi).
SOFT.P.15	Portal musi umożliwiać nadanie każdej z ról uprawnień do modyfikacji wybranych rodzajów treści (np. artykuł, opis Usługi).
SOFT.P.16	Portal musi umożliwiać nadanie każdej z ról uprawnień do modyfikacji treści utworzonych przez aktualnie zalogowanego użytkownika..
SOFT.P.17	Portal musi umożliwiać nadanie każdej z ról uprawnień dostępu do konkretnych treści (np. konkretnego artykułu).
SOFT.P.18	Portal musi definiować uprawnienie określające, kto może publikować treści.
Tworzenie i zarządzanie treścią	

SOFT.P.19	Portal musi umożliwiać tworzenie treści za pomocą edytora WYSIWYG.
SOFT.P.20	Portal musi poprawnie obsługiwać wklejanie sformatowanych i ostylowanych treści (co najmniej dla treści wklejanych z programu MS Word 2010 oraz przeglądarek internetowych).
SOFT.P.21	Portal musi zapewniać wersjonowanie wszystkich stron.
SOFT.P.22	Portal musi umożliwiać przywrócenie dowolnej z poprzednich wersji danej treści.
SOFT.P.23	Portal musi umożliwiać wyświetlenie różnic między dwoma wersjami treści.
SOFT.P.24	Portal musi zapewnić mechanizm podglądu zmian przed opublikowaniem.
SOFT.P.25	Portal musi umożliwiać zapisanie treści jako wersji roboczej (nieopublikowanej).
SOFT.P.26	Portal musi umożliwiać opublikowanie wersji roboczej treści.
SOFT.P.27	Portal musi umożliwiać opublikowanie treści bez zapisywania jej jako wersji roboczej.
SOFT.P.28	Portal musi zapewniać możliwość definiowania harmonogramów publikacji (wybór daty oraz czasu (z dokładnością do minuty), o której pojawi się dana treść na portalu oraz daty i czasu (z dokładnością do minuty), o której treść zniknie z portalu.
SOFT.P.29	Portal musi zabezpieczyć użytkownika przed przypadkową utratą treści w czasie ich wprowadzania (np. w efekcie przypadkowego przeładowania lub zamknięcia okna przeglądarki).
Obsługa załączników	
SOFT.P.30	Portal musi umożliwiać definiowanie repozytoriów plików, pełniących rolę stron z plikami "do pobrania".
SOFT.P.31	Portal musi umożliwiać modyfikację nazw plików umieszczonych w repozytorium plików.
SOFT.P.32	Portal musi umożliwiać definiowanie tekstowego tytułu pliku umieszczonego w repozytorium, odrębnego od nazwy pliku.
SOFT.P.33	Portal musi umożliwiać definiowanie tekstowego opisu pliku umieszczonego w repozytorium.
SOFT.P.34	Portal musi zapewnić możliwość publikowania galerii zdjęć wraz z mechanizmami pokazu slajdów (slideshow).
SOFT.P.35	Portal musi umożliwiać dodawanie załączników (plików) do poszczególnych treści z poziomu edytora WYSIWYG.
SOFT.P.36	Portal musi umożliwiać osadzanie w treści obrazów z poziomu edytora WYSIWYG.
SOFT.P.37	Portal musi umożliwiać osadzanie w treści filmów z serwisu YouTube z poziomu edytora WYSIWYG.
SOFT.P.38	Portal musi umożliwiać osadzanie w treści filmów z serwisu Vimeo z poziomu edytora WYSIWYG.
SOFT.P.39	Portal musi umożliwiać dodanie wielu plików jednocześnie.
SOFT.P.40	Portal musi umożliwiać przeglądanie wszystkich plików umieszczonych w Portalu.
SOFT.P.41	Dla każdego pliku umieszczonego w Portalu, Portal musi zapewnić możliwość łatwego zidentyfikowania zasobu (np. treści, repozytorium plików, galerii), w którym został wykorzystany dany plik.
SOFT.P.42	Portal musi umożliwiać usuwanie wybranych plików.
Eksport danych	
SOFT.P.43	Portal musi umożliwiać masowy eksport wybranych treści do formatu CSV obsługiwanego poprawnie przez aplikację MS Excel 2010.

SOFT.P.44	Portal musi umożliwiać masowy eksport wybranych treści do formatu XML.
Adresy URL	
SOFT.P.45	Portal musi automatycznie tworzyć semantyczne adresy URL dla każdej treści.
SOFT.P.46	Portal musi umożliwiać modyfikację adresu URL, pod którym widoczna jest treść.
SOFT.P.47	Portal musi zapewnić, że każda treść jest dostępna tylko pod jednym adresem URL.
SOFT.P.48	Portal musi umożliwiać tworzenie przekierowań z jednego adresu na inny.
SOFT.P.49	Portal musi automatycznie tworzyć przekierowanie ze starego adresu na nowy po zmianie adresu URL treści.
SOFT.P.50	Portal musi zapewniać zabezpieczenie przed pętlami przekierowań (powodującymi np. błąd ERR_TOO_MANY_REDIRECTS w przeglądarce Chrome).
Kategoryzacja i tagowanie	
SOFT.P.51	Portal musi umożliwiać definiowanie wielu kategorii tagów.
SOFT.P.52	Portal musi umożliwiać powiązanie rodzaju treści z wieloma kategoriami tagów.
SOFT.P.53	Portal musi umożliwiać opisywanie treści nieograniczoną ilością tagów.
SOFT.P.54	Portal musi umożliwiać opisywanie plików w repozytorium nieograniczoną ilością tagów.
SOFT.P.55	Portal musi umożliwiać tworzenie nowych tagów poprzez wpisanie ich w trakcie tworzenia/edycji treści.
SOFT.P.56	Portal musi umożliwiać tworzenie nowych tagów poprzez wpisanie ich w trakcie tworzenia/edycji pliku w repozytorium.
SOFT.P.57	Portal musi umożliwiać tworzenie i usuwanie nowych tagów z poziomu ekranu edycji kategorii tagów.
SOFT.P.58	Portal musi umożliwiać definiowanie wielu kategorii terminów.
SOFT.P.59	Portal musi umożliwiać definiowanie wielu terminów w jednej kategorii terminów.
SOFT.P.60	Portal musi umożliwiać organizowanie terminów z jednej kategorii terminów w strukturę drzewiastą.
SOFT.P.61	Portal musi umożliwiać powiązanie rodzaju treści z wieloma kategoriami terminów.
SOFT.P.62	Portal musi umożliwiać powiązanie treści z jednym lub wieloma terminami z powiązanych kategorii terminów.
SOFT.P.63	Portal musi umożliwiać tworzenie nowych terminów w trakcie tworzenia/edycji treści.
SOFT.P.64	Portal musi umożliwiać tworzenie nowych terminów w trakcie tworzenia/edycji pliku w repozytorium.
SOFT.P.65	Portal musi umożliwiać opisywanie plików w repozytorium nieograniczoną ilością terminów.
SOFT.P.66	Portal musi umożliwiać tworzenie i usuwanie nowych terminów z poziomu ekranu edycji kategorii terminów.
Widoki	
SOFT.P.67	Portal musi umożliwiać tworzenie widoków, pozwalających na wyświetlanie na jednej stronie różnych treści.
SOFT.P.68	Portal musi umożliwiać tworzenie galerii zdjęć.
SOFT.P.69	Portal musi umożliwiać tworzenie list zawierających wybrane atrybuty treści.
SOFT.P.70	Portal musi umożliwiać tworzenie pokazów slajdów (slideshow).
Menu	
SOFT.P.71	Portal musi umożliwiać definiowanie wielu niezależnych struktur menu.

SOFT.P.72	Portal musi umożliwiać dodawanie odnośnika do treści w dowolnym miejscu menu.
SOFT.P.73	Portal musi umożliwiać aktywację / deaktywację elementów menu.
SOFT.P.74	Portal musi umożliwiać przypisanie do każdego elementu menu obrazu / ikony reprezentującej ten element menu.
SOFT.P.75	Portal musi umożliwiać przypisanie do każdego elementu menu unikalnej klasy CSS.
SOFT.P.76	Portal musi umożliwiać łatwą reorganizację struktury menu.
SOFT.P.77	Portal musi umożliwiać generowanie ścieżki do aktualnej lokalizacji ("breadcrumb") na podstawie pozycji w strukturze treści.
Wersje językowe	
SOFT.P.78	Wszystkie teksty występujące w Portalu powinny być wyświetlane w aktywnym języku.
SOFT.P.79	Portal musi umożliwiać jednoczesne stosowanie wielu mechanizmów określania aktywnego języka interfejsu użytkownika, uwzględniając określone przez administratora priorytety poszczególnych mechanizmów (jeśli mechanizm o najwyższym priorytecie wykryje język, to ten język jest stosowany; jeśli nie - przetwarzany jest kolejny mechanizm itp.).
SOFT.P.80	Portal musi zawierać mechanizm określania aktywnego języka na podstawie struktury adresu URL.
SOFT.P.81	Portal musi zawierać mechanizm określania aktywnego języka na podstawie konfiguracji przeglądarki użytkownika.
SOFT.P.82	Portal musi zawierać mechanizm określania aktywnego języka na podstawie zapisanych preferencji użytkownika (dla użytkowników zalogowanych).
SOFT.P.83	Portal musi zawierać mechanizm określania aktywnego języka na podstawie ciasteczek (cookies) i/lub sesji przeglądarki.
SOFT.P.84	Portal musi udostępniać mechanizm pozwalający użytkownikowi na przełączanie się między wersjami językowymi.
SOFT.P.85	Portal musi umożliwiać wprowadzanie tłumaczeń treści na każdy z obsługiwanych języków.
SOFT.P.86	Portal musi automatycznie wyświetlać treści w wybranym przez użytkownika języku, o ile takie tłumaczenie jest dostępne.
SOFT.P.87	Portal musi umożliwiać tłumaczenie elementów menu na każdy z obsługiwanych języków.
Komentarze	
SOFT.P.88	Portal musi umożliwić włączenie/wyłączenie opcji komentowania danej strony.
SOFT.P.89	Portal musi umożliwiać komentowanie bezpośrednio w Portalu, za pomocą platformy Facebook i Disqus (w zależności od konfiguracji zdefiniowanej przez administratora).
SOFT.P.90	Portal musi integrować się z Podsystemem SSO w celu uwierzytelniania i autoryzacji do zasobów.
SOFT.P.91	Portal musi umożliwić dodawanie plików/załączników do komentarzy.
SOFT.P.92	Portal musi umożliwiać ocenianie poszczególnych treści.
Formularze i ankiety	
SOFT.P.93	Portal musi umożliwiać tworzenie formularzy elektronicznych.
SOFT.P.94	Portal musi rejestrować wszystkie dane wprowadzane do formularzy elektronicznych.
SOFT.P.95	Portal musi umożliwiać definiowanie powiadomień e-mail wysyłanych po wypełnieniu formularza elektroniczego.

SOFT.P.96	Portal musi umożliwiać definiowanie reguł walidacji dla poszczególnych pól formularza elektroniczego.
SOFT.P.97	Portal musi umożliwiać tworzenie i wypełnianie ankiet.
SOFT.P.98	Portal musi umożliwiać dodanie do ankiety listy opcji, które mogą wybrać użytkownicy.
SOFT.P.99	Portal musi umożliwiać wypełnianie ankiet zarówno nie zalogowanym, jak i zalogowanym użytkownikom.
SOFT.P.100	Portal musi umożliwiać ograniczenie ilości głosów w ankiecie (ilości "submitów") oddawanych przez jednego użytkownika (zarówno w przypadku użytkowników zalgoowanych, jak i nie zalogowanych).
SOFT.P.101	Portal musi umożliwiać definiowanie w ankietach elementów typu: text, radio, checkbox, date, datetime, time, email, number (typy te należy rozumieć zgodnie z definicjami opisanymi w standardzie HTML 5).
SOFT.P.102	Portal, dla elementów wielokrotnego wyboru, musi umożliwiać definiowanie ilości wyborów, które może zaznaczyć użytkownik.
SOFT.P.103	Portal musi umożliwiać definiowanie reguł widoczności elementów ankiety (wyświetlanie / ukrywanie elementów na podstawie wyboru dokonanego w innych elementach ankiety).
SOFT.P.104	Portal musi umożliwiać podliczanie ilości głosów oddanych na poszczególne wartości elementów ankiety (ilość zaznaczonych checkbox'ów w danym elemencie, suma i średnia wpisanych wartości w elementach liczbowych, ilość wystąpień każdej z wprowadzonych / wybranych wartości w danym elemencie).
SOFT.P.105	Portal musi umożliwiać eksportowanie wyników ankiet.
SOFT.P.106	Portal musi umożliwiać automatyczną publikację wyników ankiet.
FAQ	
SOFT.P.107	Portal musi umożliwiać tworzenie stron z najczęściej zadawanymi pytaniami i odpowiedziami na nie (FAQ).
Forum	
SOFT.P.108	Portal musi umożliwiać stworzenie forum dyskusyjnego wsparcia dla użytkowników.
SOFT.P.109	Portal musi umożliwiać moderowanie wpisów publikowanych na forum.
SOFT.P.110	Portal musi umożliwiać tworzenie kategorii forum.
SOFT.P.111	Portal musi umożliwiać tworzenie tematów dyskusji w ramach kategorii forum.
SOFT.P.112	Wpisy na forum powinny być tworzone z wykorzystaniem edytora WYSIWYG.
Wyszukiwanie	
SOFT.P.113	Portal musi umożliwiać przeszukiwanie bazy wiedzy wraz z przeszukiwaniem załączników oraz wizualizacją (zaznaczeniem) tekstu wyszukiwanego w skrócie/cytacie podczas wyświetlania wyników. W wyświetlanych wynikach nie jest wymagane zachowanie właściwego formatowania dokumentu źródłowego.
SOFT.P.114	Portal musi umożliwiać pełno tekstowe wyszukiwanie opublikowanych treści.
SOFT.P.115	Portal w wynikach wyszukiwania powinien uwzględniać prawa dostępu zalogowanego użytkownika.
SOFT.P.116	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie PDF.
SOFT.P.117	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach

	w formacie DOC.
SOFT.P.118	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie DOCX.
SOFT.P.119	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie RTF.
SOFT.P.120	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie HTML.
SOFT.P.121	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie OpenDocument.
SOFT.P.122	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie TXT.
SOFT.P.123	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie XLS.
SOFT.P.124	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie XLSX.
SOFT.P.125	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie PPT.
SOFT.P.126	Portal musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Portalu plikach w formacie PPTX.
SOFT.P.127	Portal musi uwzględniać w wynikach wyszukiwania tylko treści publicznie dostępne.
SOFT.P.128	Portal musi uwzględniać zmiany w indeksie wyszukiwania maksymalnie w ciągu godziny od wprowadzenia zmiany w treści.
SOFT.P.129	Wyszukiwarka powinna być skonfigurowana w taki sposób, aby czas wyszukiwania bazy 100000 artykułów o wielkości średnio 10 000 znaków był liniowy i nie przekraczał 1000ms, niezależnie od formatu pliku.
SOFT.P.130	Portal musi umożliwiać filtrowanie wyników wyszukiwania za pomocą mechanizmów "facets", na podstawie zdefiniowanych atrybutów (pól) treści.
SOFT.P.131	Portal musi zaznaczać wystąpienia tekstu wyszukiwanego w skrócie/cytacie podczas wyświetlania wyników wyszukiwania.
SOFT.P.132	Mechanizmy wyszukiwania powinny poprawnie obsługiwać różne języki.
SOFT.P.133	Portal musi poprawnie obsługiwać polską fleksję w ramach mechanizmów wyszukiwania.
SOFT.P.134	Portal musi poprawnie obsługiwać angielską fleksję w ramach mechanizmów wyszukiwania.
SOFT.P.135	Portal, w ramach mechanizmów wyszukiwania, musi umożliwiać określenie wag dla poszczególnych atrybutów wyszukiwanych treści
Statystyki	
SOFT.P.136	Portal musi umożliwiać integrację z (wybraną na etapie przygotowania projektu technicznego) platformą służącą do zbierania i analizy statystyk odwiedzin.
Obsługa wielu domen	
SOFT.P.137	Portal musi umożliwiać wyświetlanie innych treści pod różnymi adresami domenowymi (mechanizm "multi-site"), przy wykorzystaniu wspólnej instancji bazy danych.
SOFT.P.138	Portal musi umożliwiać kierowanie odrębnych poddomen do fragmentów struktury Portalu

Rozszerzenia i szablony	
SOFT.P.139	Portal musi umożliwiać tworzenie rozszerzeń (pluginów, modułów) Podsystemu.
SOFT.P.140	W przypadku bazowania na istniejącym oprogramowaniu, cały kod wytworzony przez Wykonawcę w ramach Projektu musi zostać zrealizowany jako rozszerzenie (plugin, moduł itp) lub szablon do Portalu.
SOFT.P.141	Portal musi umożliwiać zainstalowanie wielu szablonów ("skórek").
SOFT.P.142	Portal musi umożliwiać wykorzystanie odrębnego szablonu w zależności od przeglądanej strony.
SOFT.P.143	Portal musi umożliwiać wykorzystanie odrębnego szablonu w zależności od pozycji strony w strukturze menu.
SOFT.P.144	Portal musi umożliwiać wykorzystanie odrębnego szablonu w zależności od roli użytkownika.
Pozostałe	
SOFT.P.145	Portal musi zawierać skuteczne zabezpieczenie wszystkich formularzy przed spamem o efektywności na poziomie co najmniej 99% (maksymalnie 1% postów może zostać niepoprawnie sklasyfikowanych), np. poprzez integrację z usługą typu Mollom
SOFT.P.146	Wszystkie funkcjonalności Portalu (w tym te związane z administracją Portalem oraz dostępem do treści Portalu) muszą być realizowane przez przeglądarkę Internetową.
SOFT.P.147	Portal musi zapewnić mechanizm cache'owania renderowanych szablonów.
SOFT.P.148	Portal musi udostępnić pełne API, pozwalające na jego kontrolę oraz konfigurację.
SEO	
SOFT.P.149	Portal musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby SEO.
SOFT.P.150	Portal musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby sieci społecznościowych (co najmniej w zakresie określonym przez standard OpenGraph i publikacje schema.org).
SOFT.P.151	Portal musi zapewniać możliwość ręcznego opisywania treści metadanymi na potrzeby SEO.
SOFT.P.152	Portal musi zapewniać możliwość ręcznego opisywania treści metadanymi na potrzeby sieci społecznościowych (co najmniej w zakresie określonym przez standard OpenGraph i publikacje schema.org).
SOFT.P.153	Portal musi automatycznie tworzyć sitemapy XML (artykuły oraz grafiki), oraz zgłaszać je po wygenerowaniu do Google.
SOFT.P.154	Portal, w ramach obsługi semantycznych adresów URL, nie musi pozwalać na indeksowanie stron w ścieżkach systemowych, lecz automatycznie przekierowywać z nich na prawidłowy, przyjazny adres, który będzie indeksowany.
Wersja dla niepełnosprawnych	
SOFT.P.155	Portal musi umożliwiać przełączenie serwisu do wersji o wysokim kontraście.
SOFT.P.156	Portal musi zapewnić standard Aria.
SOFT.P.157	Portal musi prawidłowo definiować nawigację po elementach serwisu za pomocą "tabindex".
SOFT.P.158	Portal musi ukrywać w wersji dla niepełnosprawnych zbędne elementy interfejsu, które mogłyby zaburzać pracę czytników bądź nawigację osób niepełnosprawnych po stronie.

Wersja żałobna serwisu	
SOFT.P.159	Portal musi zawierać specjalny zestaw styli dla wersji żałobnej serwisu, którą można będzie włączyć z poziomu panelu administracyjnego Podsystemu.
SOFT.P.160	Wersja żałobna Portalu powinna zmieniać także paletę kolorów dla obrazków wyświetlanych na stronie.
Obsługa procesu zakupowego	
SOFT.P.161	Portal musi zawierać funkcjonalności pozwalające na zakup Usług przez Klientów.
SOFT.P.162	Realizacja płatności elektronicznych musi odbywać się zgodnie ze standardem PCI Data Security Standard.
SOFT.P.163	Portal musi integrować się z SelfService w celu zrealizowania procesu sprzedażowego.
SOFT.P.164	Portal musi integrować się z Billingiem w celu pobierania informacji o cenach produktów.
SOFT.P.165	Portal musi zawierać mechanizmy umożliwiające Klientom oszacowanie kosztów wykorzystywanych Usług.
SOFT.P.166	Portal musi umożliwiać zapisywanie danych wprowadzanych przez Klientów w ramach szacowania kosztów Usług.
SOFT.P.167	Portal musi umożliwiać eksport zapisanych wcześniej danych wprowadzanych przez Klientów w ramach szacowania kosztów Usług do formatu CSV kompatybilnego z MS Excel 2010.

5.2.10. Katalog Usług

ID wymagania	Treść wymagania
SOFT.KU.1	Katalog Usług musi udostępniać katalog usług świadczonych przez Usługodawców.
SOFT.KU.2	Katalog Usług musi być dostępny pod odrębnym adresem domenowym od Portalu.
SOFT.KU.3	Katalog Usług musi być dostępny w dedykowanej "skórce", odrębnej od Portalu.
SOFT.KU.4	Katalog Usług musi umożliwiać wykorzystanie funkcjonalności zaimplementowanych dla Podsystemu Portal (spełniać wymagania określone dla Podsystemu Portal).
Tworzenie i zarządzanie wpisami	
SOFT.KU.5	Katalog Usług musi umożliwiać Usługodawcom wprowadzanie opisów usług do katalogu usług, wraz z załącznikami graficznymi.
SOFT.KU.6	Katalog Usług musi umożliwiać Usługodawcom modyfikację opisów usług w katalogu usług.
SOFT.KU.7	Katalog Usług musi umożliwiać Usługodawcom wycofanie usług z katalogu usług.
SOFT.KU.8	Katalog Usług musi zapewniać możliwość moderacji wpisów w katalogu usług.
SOFT.KU.9	Katalog Usług musi umożliwiać Usługodawcom definiowanie polityki cenowej dla usług.
SOFT.KU.10	Katalog Usług musi umożliwiać zapoznanie się ze statystykami dotyczącymi zdefiniowanych usług.
Przeglądanie i wyszukiwanie	
SOFT.KU.11	Katalog Usług musi udostępniać możliwość przeglądania hierarchicznej struktury katalogu usług.
SOFT.KU.12	Katalog Usług musi udostępniać możliwość klasyfikowania usług w ramach zdefiniowanych, hierarchicznych kategorii.
SOFT.KU.13	Katalog Usług musi być wyposażony w pełno tekstową wyszukiwarkę usług.

SOFT.KU.14	Wyszukiwarka powinna umożliwiać określenie wag dla poszczególnych atrybutów wyszukiwanych usług.
SOFT.KU.15	Katalog Usług musi umożliwiać filtrowanie wyników wyszukiwania za pomocą mechanizmów "facets", na podstawie zdefiniowanych atrybutów (pól) treści.
SEO	
SOFT.KU.16	Katalog Usług musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby SEO.
SOFT.KU.17	Katalog Usług musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby sieci społecznościowych.
SOFT.KU.18	Katalog Usług musi zapewniać możliwość ręcznego opisywania treści metadanymi na potrzeby SEO.
SOFT.KU.19	Katalog Usług musi zapewniać możliwość ręcznego opisywania treści metadanymi na potrzeby sieci społecznościowych.
SOFT.KU.20	Katalog Usług musi automatycznie tworzyć sitemapy XML (artykuły oraz grafiki), oraz automatycznie zgłaszać je po wygenerowaniu do wyszukiwarki Google.
SOFT.KU.21	Katalog Usług, w ramach obsługi przyjaznych adresów, nie może pozwalać na indeksowanie stron w ścieżkach systemowych; powinien automatycznie przekierowywać z nich na prawidłowy, przyjazny adres, który będzie indeksowany.
Adresy URL	
SOFT.KU.22	Katalog Usług musi automatycznie tworzyć semantyczne adresy URL dla każdej treści.
SOFT.KU.23	Katalog Usług musi umożliwiać modyfikację adresu URL, pod którym widoczna jest treść.
SOFT.KU.24	Katalog Usług musi zapewnić, że każda treść jest dostępna tylko pod jednym adresem URL.
SOFT.KU.25	Katalog Usług musi umożliwiać tworzenie przekierowań z jednego adresu na inny.
SOFT.KU.26	Po zmianie adresu URL treści Katalog Usług musi automatycznie tworzyć przekierowanie ze starego adresu na nowy.
SOFT.KU.27	Katalog Usług musi zapewniać zabezpieczenie przed pętlami przekierowań (powodującymi np. błąd ERR_TOO_MANY_REDIRECTS w przeglądarce Chrome).

5.2.11. Baza Wiedzy

ID wymagania	Treść wymagania
SOFT.BW.1	Celem Bazy Wiedzy jest zbudowanie dwóch baz wiedzy: dla Zamawiającego i dla Klientów. W ocenie Zamawiającego rozwiązaniem optymalnym byłoby zbudowanie Podsystemu na bazie rozwiązania klasy "wiki".
Zasilenie treścią	
SOFT.BW.2	Wykonawca musi przygotować wszystkie treści (teksty, uzupełniające materiały graficzne) i zasilić nimi Bazę Wiedzy w zakresie potrzebnym do rozpoczęcia świadczenia Usług przez Zamawiającego.
SOFT.BW.3	Baza Wiedzy musi udostępniać wszystkie funkcjonalności niezbędne do zasilenia go treścią opracowaną przez Wykonawcę
SOFT.BW.4	Baza Wiedzy musi udostępniać wszystkie funkcjonalności niezbędne do zaimplementowania docelowej architektury informacji.

SOFT.BW.5	Baza Wiedzy musi udostępniać wszystkie funkcjonalności niezbędne do zaimplementowania opracowanego projektu graficznego.
Funkcjonalności administratora i uprawnienia	
SOFT.BW.6	Baza Wiedzy musi realizować kontrolę dostępu do poszczególnych funkcjonalności na podstawie roli użytkownika określonej przez SSO.
SOFT.BW.7	Baza Wiedzy musi umożliwiać nadanie każdej osobie i roli uprawnień do korzystania z poszczególnych funkcjonalności.
SOFT.BW.8	Baza Wiedzy musi umożliwiać nadanie każdej osobie i roli uprawnień do odczytu wybranych części struktury bazy wiedzy.
SOFT.BW.9	Baza Wiedzy musi umożliwiać nadanie każdej osobie i roli uprawnień do modyfikacji wybranych części struktury bazy wiedzy.
SOFT.BW.10	Baza Wiedzy musi umożliwiać nadanie każdej osobie i roli uprawnień do kontroli dostępu do wybranych części struktury bazy wiedzy.
SOFT.BW.11	Baza Wiedzy musi umożliwiać nadanie każdej osobie i roli uprawnień dostępu do konkretnych treści (np. konkretnego artykułu).
Tworzenie i zarządzanie treścią	
SOFT.BW.11	Baza Wiedzy musi umożliwiać tworzenie treści za pomocą języka znaczników (ang. markup language).
SOFT.BW.12	Baza Wiedzy musi umożliwiać tworzenie treści za pomocą edytora WYSIWYG.
SOFT.BW.13	Baza Wiedzy musi poprawnie obsługiwać wklejanie sformatowanych i ostylowanych treści (co najmniej dla treści wklejanych z programu MS Word 2010 oraz przeglądarek internetowych)
SOFT.BW.14	Baza Wiedzy musi zapewniać wersjonowanie wszystkich stron.
SOFT.BW.15	Baza Wiedzy musi umożliwiać przywrócenie dowolnej z poprzednich wersji danej treści.
SOFT.BW.16	Baza Wiedzy musi umożliwiać wyświetlenie różnic między dwoma wersjami treści.
SOFT.BW.17	Baza Wiedzy musi zapewnić mechanizm podglądu zmian przed opublikowaniem.
SOFT.BW.18	Baza Wiedzy musi umożliwiać zapisanie treści jako wersji roboczej (nieopublikowanej).
SOFT.BW.19	Baza Wiedzy musi umożliwiać opublikowanie wersji roboczej treści.
SOFT.BW.20	Baza Wiedzy musi definiować uprawnienie określające, kto może publikować treści.
SOFT.BW.21	Baza Wiedzy musi zabezpieczyć użytkownika przed przypadkową utratą treści w czasie ich wprowadzania (np. w efekcie przypadkowego przeładowania lub zamknięcia okna przeglądarki).
SOFT.BW.22	Baza Wiedzy musi umożliwiać wydzielenie w strukturze bazy wiedzy artykułów dostępnych tylko dla określonych użytkowników / grup.
SOFT.BW.23	Baza Wiedzy musi umożliwiać organizację treści w bazie wiedzy w strukturę drzewiastą.
SEO	
SOFT.BW.24	Baza Wiedzy musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby SEO.
SOFT.BW.25	Baza Wiedzy musi zapewniać możliwość automatycznego opisywania treści metadanymi na potrzeby sieci społecznościowych.
SOFT.BW.26	Baza Wiedzy musi zapewniać możliwość ręcznego opisywania treści metadanymi na potrzeby SEO.
SOFT.BW.27	Baza Wiedzy musi zapewniać możliwość ręcznego opisywania treści metadanymi na

	potrzeby sieci społecznościowych.
SOFT.BW.28	Baza Wiedzy musi automatycznie tworzyć sitemapy XML (artykuły oraz grafiki), oraz zgłaszać je po wygenerowaniu do wyszukiwarki Google.
SOFT.BW.29	Baza Wiedzy w ramach obsługi semantycznych adresów URL, nie może pozwalać na indeksowanie stron w ścieżkach systemowych; powinien automatycznie przekierowywać z nich na prawidłowy, przyjazny adres, który będzie indeksowany.
Obsługa załączników	
SOFT.BW.30	Baza Wiedzy musi umożliwiać definiowanie repozytoriów plików, pełniących rolę stron z plikami "do pobrania".
SOFT.BW.31	Baza Wiedzy musi umożliwiać modyfikację nazw plików umieszczonych w repozytorium plików.
SOFT.BW.32	Baza Wiedzy musi umożliwiać definiowanie tekstowego tytułu pliku umieszczonego w repozytorium, odrębnego od nazwy pliku.
SOFT.BW.33	Baza Wiedzy musi umożliwiać definiowanie tekstowego opisu pliku umieszczonego w repozytorium.
SOFT.BW.34	Baza Wiedzy musi umożliwiać dodawanie załączników (plików) do poszczególnych treści z poziomu edytora WYSIWYG.
SOFT.BW.35	Baza Wiedzy musi umożliwiać osadzanie w treści obrazów z poziomu edytora WYSIWYG.
SOFT.BW.36	Baza Wiedzy musi umożliwiać osadzanie w treści filmów z serwisu YouTube z poziomu edytora WYSIWYG.
SOFT.BW.37	Baza Wiedzy musi umożliwiać osadzanie w treści filmów z serwisu Vimeo z poziomu edytora WYSIWYG.
SOFT.BW.38	Dla każdego pliku umieszczonego w Bazy Wiedzy, Podsystem musi zapewnić możliwość łatwego zidentyfikowania zasobu (np. artykułu, repozytorium plików), w którym został wykorzystany dany plik.
SOFT.BW.39	Baza Wiedzy musi umożliwiać usuwanie wybranych plików.
Eksport danych	
SOFT.BW.40	Baza Wiedzy musi umożliwiać eksport każdego artykułu do formatu PDF.
SOFT.BW.41	Baza Wiedzy musi umożliwiać eksport wybranego artykułu wraz z wszystkimi artykułami podrzędnymi do formatu PDF.
SOFT.BW.42	Baza Wiedzy musi umożliwiać masowy eksport wybranych treści do formatu CSV obsługiwanego poprawnie przez aplikację MS Excel.
SOFT.BW.43	Baza Wiedzy musi umożliwiać masowy eksport wybranych treści do formatu XML.
Adresy URL	
SOFT.BW.44	Baza Wiedzy musi automatycznie tworzyć semantyczne adresy URL dla każdej treści.
SOFT.BW.45	Baza Wiedzy musi umożliwiać modyfikację adresu URL, pod którym widoczna jest treść.
SOFT.BW.46	Baza Wiedzy musi zapewnić, że każda treść jest dostępna tylko pod jednym adresem URL.
SOFT.BW.47	Baza Wiedzy musi umożliwiać tworzenie przekierowań z jednego adresu na inny.
SOFT.BW.48	Baza Wiedzy musi automatycznie tworzyć przekierowanie ze starego adresu na nowy po zmianie adresu URL treści.
SOFT.BW.49	Baza Wiedzy musi zapewniać zabezpieczenie przed pętlami przekierowań (powodującymi np. błąd ERR_TOO_MANY_REDIRECTS w przeglądarce Chrome)
Kategoryzacja i tagowanie	

SOFT.BW.50	Baza Wiedzy musi umożliwiać opisywanie treści nieograniczoną ilością tagów.
SOFT.BW.51	Baza Wiedzy musi umożliwiać opisywanie plików w repozytorium nieograniczoną ilością tagów.
SOFT.BW.52	Baza Wiedzy musi umożliwiać tworzenie nowych tagów poprzez wpisanie ich w trakcie tworzenia/edycji treści.
SOFT.BW.53	Baza Wiedzy musi umożliwiać tworzenie nowych tagów poprzez wpisanie ich w trakcie tworzenia/edycji pliku w repozytorium.
SOFT.BW.54	Baza Wiedzy musi umożliwiać definiowanie wielu kategorii.
SOFT.BW.55	Baza Wiedzy musi umożliwiać definiowanie wielu terminów w jednej kategorii.
SOFT.BW.56	Baza Wiedzy musi umożliwiać organizowanie terminów z jednej kategorii w strukturę drzewiastą.
SOFT.BW.57	Baza Wiedzy musi umożliwiać powiązanie treści z jednym lub wieloma terminami.
SOFT.BW.58	Baza Wiedzy musi umożliwiać tworzenie nowych terminów w trakcie tworzenia/edycji treści.
Menu	
SOFT.BW.59	Baza Wiedzy musi umożliwiać definiowanie wielu niezależnych struktur menu.
SOFT.BW.60	Baza Wiedzy musi umożliwiać dodawanie odnośnika do treści w dowolnym miejscu menu.
SOFT.BW.61	Baza Wiedzy musi umożliwiać aktywację / deaktywację elementów menu.
SOFT.BW.62	Baza Wiedzy musi umożliwiać przypisanie do każdego elementu menu obrazu / ikony reprezentującej ten element menu.
SOFT.BW.63	Baza Wiedzy musi umożliwiać przypisanie do każdego elementu menu unikalnej klasy CSS.
SOFT.BW.64	Baza Wiedzy musi umożliwiać łatwą reorganizację struktury menu.
SOFT.BW.65	Baza Wiedzy musi umożliwiać generowanie ścieżki do aktualnej lokalizacji ("breadcrumb") na podstawie pozycji w strukturze treści.
Wersje językowe	
SOFT.BW.66	Baza Wiedzy, w momencie wdrożenia, musi obsługiwać język polski i angielski.
SOFT.BW.67	Baza Wiedzy musi umożliwiać rozszerzenie listy obsługiwanych języków o kolejne języki.
SOFT.BW.68	Wszystkie teksty występujące w Bazie Wiedzy powinny być wyświetlane w aktywnym języku.
SOFT.BW.69	Baza Wiedzy musi umożliwiać jednoczesne stosowanie wielu mechanizmów określania aktywnego języka interfejsu użytkownika, uwzględniając określone przez administratora priorytety poszczególnych mechanizmów (jeśli mechanizm o najwyższym priorytecie wykryje język, to ten język jest stosowany; jeśli nie - przetwarzany jest kolejny mechanizm itp).
SOFT.BW.70	Baza Wiedzy musi zawierać mechanizm określania aktywnego języka na podstawie struktury adresu URL.
SOFT.BW.71	Baza Wiedzy musi zawierać mechanizm określania aktywnego języka na podstawie konfiguracji przeglądarki użytkownika.
SOFT.BW.72	Baza Wiedzy musi zawierać mechanizm określania aktywnego języka na podstawie zapisanych preferencji użytkownika (dla użytkowników zalogowanych).
SOFT.BW.73	Baza Wiedzy musi zawierać mechanizm określania aktywnego języka na podstawie ciasteczek (cookies) i/lub sesji przeglądarki.
SOFT.BW.74	Baza Wiedzy musi udostępniać mechanizm pozwalający użytkownikowi na przełączanie

	się między wersjami językowymi.
SOFT.BW.75	Baza Wiedzy musi umożliwiać tłumaczenie treści na każdy z obsługiwanych języków.
SOFT.BW.76	Baza Wiedzy musi automatycznie przekierowywać użytkownika do tłumaczenia treści w aktywnym języku, o ile takie tłumaczenie jest dostępne.
SOFT.BW.77	Baza Wiedzy musi umożliwiać tłumaczenie elementów menu na każdy z obsługiwanych języków.
Komentarze	
SOFT.BW.78	Baza Wiedzy musi umożliwiać włączenie/wyłączenie opcji komentowania danej treści.
SOFT.BW.79	Baza Wiedzy musi zapewniać możliwość komentowania treści.
SOFT.BW.80	Baza Wiedzy musi umożliwiać komentowanie bezpośrednio w Podsystemie, za pomocą platformy Facebook i Disqus (w zależności od konfiguracji zdefiniowanej przez administratora)
SOFT.BW.81	Baza Wiedzy musi obsługiwać załączniki do komentarzy.
Formularze i ankiety	
SOFT.BW.82	Baza Wiedzy musi umożliwiać tworzenie formularzy elektronicznych
SOFT.BW.83	Baza Wiedzy musi rejestrować wszystkie dane wprowadzane do formularzy elektronicznych.
SOFT.BW.84	Baza Wiedzy musi umożliwiać definiowanie powiadomień e-mail wysyłanych po wypełnieniu formularza elektroniczego.
FAQ	
SOFT.BW.85	Baza Wiedzy musi umożliwiać tworzenie stron z najczęściej zadawanymi pytaniami i odpowiedziami na nie (FAQ).
Wyszukiwanie	
SOFT.BW.86	Baza Wiedzy musi umożliwiać przeszukiwanie bazy wiedzy wraz z przeszukiwaniem załączników oraz wizualizacją (zaznaczeniem) tekstu wyszukiwanego w skrócie/cytacie podczas wyświetlania wyników. W wyświetlanych wynikach nie jest wymagane zachowanie właściwego formatowania dokumentu źródłowego.
SOFT.BW.87	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie PDF.
SOFT.BW.88	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie DOC.
SOFT.BW.89	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie DOCX.
SOFT.BW.90	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie RTF.
SOFT.BW.91	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie HTML.
SOFT.BW.92	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie OpenDocument.
SOFT.BW.93	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie TXT.
SOFT.BW.94	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie XLS.

SOFT.BW.95	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie XLSX.
SOFT.BW.96	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie PPT.
SOFT.BW.97	Baza Wiedzy musi umożliwiać pełno tekstowe wyszukiwanie w zgromadzonych w Bazie Wiedzy plikach w formacie PPTX.
SOFT.BW.98	Baza Wiedzy musi uwzględniać w wynikach wyszukiwania tylko treści opublikowane.
SOFT.BW.99	Baza Wiedzy musi uwzględniać w wynikach wyszukiwania tylko treści dostępne dla aktualnego użytkownika.
SOFT.BW.100	Baza Wiedzy musi uwzględniać zmiany w indeksie wyszukiwania maksymalnie w ciągu godziny od wprowadzenia zmiany w treści.
SOFT.BW.101	Wyszukiwarka powinna być skonfigurowana w taki sposób, aby czas wyszukiwania bazy 100000 artykułów o wielkości średnio 10 000 znaków był liniowy i nie przekraczał 1000ms, niezależnie od formatu pliku.
SOFT.BW.102	Baza Wiedzy musi umożliwiać filtrowanie wyników wyszukiwania za pomocą mechanizmów "facets", na podstawie zdefiniowanych atrybutów (pól) treści.
SOFT.BW.103	Baza Wiedzy musi zaznaczać wystąpienia tekstu wyszukiwanego w skrócie/cytacie podczas wyświetlania wyników wyszukiwania.
SOFT.BW.104	Mechanizmy wyszukiwania powinny poprawnie obsługiwać różne języki.
SOFT.BW.105	Baza Wiedzy musi poprawnie obsługiwać polską fleksję w ramach mechanizmów wyszukiwania.
SOFT.BW.106	Baza Wiedzy musi poprawnie obsługiwać angielską fleksję w ramach mechanizmów wyszukiwania.
SOFT.BW.107	Baza Wiedzy w ramach mechanizmów wyszukiwania, musi umożliwiać określenie wag dla poszczególnych atrybutów wyszukiwanych treści
Statystyki	
SOFT.BW.108	Baza Wiedzy musi umożliwiać integrację z (wybraną na etapie przygotowania projektu technicznego) platformą służącą do zbierania i analizy statystyk odwiedzin.
Obsługa wielu domen	
SOFT.BW.109	Baza Wiedzy musi umożliwiać wyświetlanie innych treści pod różnymi adresami domenowymi, przy wykorzystaniu jednej bazy danych (mechanizm "multi-site")
SOFT.BW.110	Baza Wiedzy musi być posadowiony w co najmniej 2 instancjach: wewnętrznej (dla pracowników Zamawiającego) i publicznej (dla Klientów).
Rozszerzenia i szablony	
SOFT.BW.111	Baza Wiedzy musi umożliwiać tworzenie rozszerzeń (pluginów, modułów) Podsystemu.
SOFT.BW.112	W przypadku bazowania na istniejącym oprogramowaniu, cały kod wytworzony przez Wykonawcę w ramach Projektu musi zostać zrealizowany jako rozszerzenie (plugin, moduł itp) lub szablon do Podsystemu.
SOFT.BW.113	Baza Wiedzy musi umożliwiać zainstalowanie wielu szablonów ("skórek").
SOFT.BW.114	Baza Wiedzy musi umożliwiać wykorzystanie odrębnego szablonu w zależności od przeglądanej strony.
SOFT.BW.115	Baza Wiedzy musi umożliwiać wykorzystanie odrębnego szablonu w zależności od pozycji strony w strukturze menu.

SOFT.BW.116	Baza Wiedzy musi umożliwiać wykorzystanie odrębnego szablonu w zależności od roli użytkownika.
Wersja dla niepełnosprawnych	
SOFT.BW.117	Baza Wiedzy musi umożliwiać przełączenie serwisu do wersji o wysokim kontraście.
SOFT.BW.118	Baza Wiedzy musi zapewnić obsługę standardu Aria
SOFT.BW.119	Baza Wiedzy musi prawidłowo definiować nawigację po elementach serwisu za pomocą “tabindex”.
SOFT.BW.120	Baza Wiedzy musi ukrywać w wersji dla niepełnosprawnych zbędne elementy interfejsu, które mogłyby zaburzać pracę czytników bądź nawigację osób niepełnosprawnych po stronie.
Wersja żałobna serwisu	
SOFT.BW.121	Baza Wiedzy musi zawierać specjalny zestaw styli dla wersji żałobnej serwisu, którą można będzie włączyć z poziomu panelu administracyjnego Podsystemu.
SOFT.BW.122	Wersja żałobna serwisu powinna zmieniać także paletę kolorów dla obrazków wyświetlanych na stronie.
Pozostałe	
SOFT.BW.123	Baza Wiedzy musi zawierać skuteczne zabezpieczenie wszystkich formularzy przed spamem o efektywności na poziomie co najmniej 99% (maksymalnie 1% postów może zostać niepoprawnie sklasyfikowanych).
SOFT.BW.124	Wszystkie funkcjonalności Bazy Wiedzy (w tym te związane z administracją oraz dostępem do treści) muszą być realizowane przez przeglądarkę Internetową.
SOFT.BW.125	Baza Wiedzy musi zapewnić mechanizm cache’owania renderowanych szablonów.
SOFT.BW.126	Baza Wiedzy musi udostępnić pełne API, pozwalające na jego kontrolę oraz konfigurację.
SOFT.BW.127	Baza Wiedzy musi integrować się z Podsystemem SSO w celu uwierzytelniania użytkowników.

5.2.12. Trouble Ticketing

ID wymagania	Treść wymagania	Wymagane w wersji pierwszej
Analiza i projekt Trouble Ticketing		
SOFT.TT.1	Analiza w zakresie Podsystemu Trouble Ticketing powinna uwzględniać analizę procesów biznesowych związanych z obsługą zgłoszeń.	NIE
SOFT.TT.2	Analiza w zakresie Podsystemu Trouble Ticketing powinna zawierać katalog proponowanych rodzajów zgłoszeń.	NIE
SOFT.TT.3	Analiza w zakresie Podsystemu Trouble Ticketing powinna zawierać spis atrybutów (pól), właściwych dla poszczególnych rodzajów zgłoszeń.	NIE
SOFT.TT.4	Analiza w zakresie Podsystemu Trouble Ticketing powinna zawierać propozycję konfiguracji kolejek zgłoszeń.	NIE
SOFT.TT.5	Analiza w zakresie Podsystemu Trouble Ticketing powinna zawierać propozycję polityki SLA do zaimplementowania.	NIE
SOFT.TT.6	Analiza w zakresie Podsystemu Trouble Ticketing powinna zawierać	NIE

	propozycję raportów do zaimplementowania.	
SOFT.TT.7	Projekt techniczny musi zawierać projekt graficzny interfejsu użytkownika uwzględniający kwestie użyteczności (usablility).	NIE
Obsługa projektów		
SOFT.TT.8	Trouble Ticketing musi umożliwiać tworzenie projektów grupujących zgłoszenia.	TAK
SOFT.TT.9	Trouble Ticketing musi umożliwiać definiowanie nowych rodzajów zgłoszeń.	TAK
SOFT.TT.10	Trouble Ticketing musi umożliwiać określenie, które rodzaje zgłoszeń są dostępne w którym z projektów.	TAK
SOFT.TT.11	Trouble Ticketing musi umożliwiać przypisanie użytkownikom ról w ramach projektu.	TAK
SOFT.TT.12	Trouble Ticketing musi umożliwiać przypisanie uprawnień do ról w ramach projektu.	TAK
SOFT.TT.13	Trouble Ticketing musi umożliwiać przypisanie w ramach projektu konkretnego przepływu pracy (workflow) do rodzaju zgłoszenia.	TAK
SOFT.TT.14	Trouble Ticketing musi umożliwiać tworzenie projektów, w ramach których będą realizowane prace programistyczne.	TAK
SOFT.TT.15	Trouble Ticketing musi umożliwiać tworzenie projektów, w ramach których będzie realizowana obsługa zgłoszeń serwisowych użytkowników (funkcjonalność "Service Desk")	NIE
SOFT.TT.16	Trouble Ticketing musi uniemożliwiać dostęp do informacji o projekcie (w tym do zgłoszeń) użytkownikom nieposiadającym odpowiedniego uprawnienia w tym projekcie.	TAK
Tworzenie zgłoszeń		
SOFT.TT.17	Trouble Ticketing musi zapewnić możliwość uwierzytelniania użytkowników w oparciu o Podsystem SSO.	NIE
SOFT.TT.18	Trouble Ticketing musi zapewnić możliwość utworzenia nowego zgłoszenia.	TAK
SOFT.TT.19	Trouble Ticketing musi zapewnić możliwość zdefiniowania listy atrybutów (pól) dostępnych do wypełnienia na formularzu tworzenia nowego zgłoszenia.	TAK
SOFT.TT.20	Trouble Ticketing musi zapewnić możliwość podglądu statusu zgłoszenia przez użytkownika, który je utworzył.	TAK
SOFT.TT.21	Trouble Ticketing musi umożliwić dołączanie plików/załączników do zgłoszeń.	TAK
SOFT.TT.22	Trouble Ticketing musi umożliwić tworzenie powiązań między zgłoszeniami (np. duplikaty, zgłoszenia blokujące itp.)	TAK
SOFT.TT.23	Trouble Ticketing musi umożliwić tworzenie zgłoszeń podrzędnych ("podzadania").	TAK
SOFT.TT.24	Trouble Ticketing musi umożliwić opisywanie zgłoszeń z wykorzystaniem tagów.	TAK
SOFT.TT.25	Trouble Ticketing musi umożliwić definiowanie poziomów bezpieczeństwa	TAK

	zgłoszeń, umożliwiających ograniczenie zbioru użytkowników widzących dane zgłoszenie do wybranych ról projektowych.	
Komentarze		
SOFT.TT.26	Trouble Ticketing musi zapewnić możliwość tworzenia komentarzy do zgłoszenia przez twórcę zgłoszenia i pracowników obsługujących zgłoszenie.	TAK
SOFT.TT.27	Trouble Ticketing musi umożliwić ograniczenie widoczności komentarzy do wybranej roli w ramach projektu.	TAK
SOFT.TT.28	Trouble Ticketing musi umożliwiać śledzenie historii dla każdej zmiany dotyczącej zgłoszenia.	TAK
Serwis Klienta		
SOFT.TT.29	Trouble Ticketing musi zawierać wydzieloną logicznie część, przeznaczoną do obsługi użytkowników zewnętrznych (Serwis Klienta).	NIE
SOFT.TT.30	Serwis Klienta musi być wizualnie zintegrowany z Podsystemem SelfService.	NIE
SOFT.TT.31	Integracja między Serwisem Klienta a Podsystemem SelfService nie może bazować na mechanizmie IFRAME.	NIE
SOFT.TT.32	Serwis Klienta musi umożliwiać Klientom tworzenie różnych rodzajów zgłoszeń.	NIE
SOFT.TT.33	Serwis Klienta musi umożliwiać Klientom tworzenie zgłoszeń we właściwych projektach (np. "wsparcie techniczne", "wsparcie handlowe").	NIE
SOFT.TT.34	Serwis Klienta musi zapewnić w formularzu tworzenia zgłoszenia możliwość wybrania z listy obiektów (Usług, faktur, płatności) należących użytkownika tego obiektu, którego dotyczy problem.	NIE
SOFT.TT.35	Serwis Klienta musi umożliwiać Klientom wgląd w aktualny status zgłoszenia.	NIE
SOFT.TT.36	Serwis Klienta musi umożliwiać Klientom wgląd w przeznaczone dla Klientów komentarze do zgłoszenia.	NIE
SOFT.TT.37	Serwis Klienta musi umożliwiać Klientom utworzenie komentarza do zgłoszenia.	NIE
SOFT.TT.38	Serwis Klienta musi umożliwiać Klientom dodanie załącznika do zgłoszenia.	NIE
SOFT.TT.39	Serwis Klienta musi umożliwiać Klientom oznaczenie zgłoszenia jako wycofane/anulowane.	NIE
SOFT.TT.40	Serwis Klienta musi umożliwiać Klientom przeszukiwanie zgłoszeń.	NIE
SOFT.TT.41	Serwis Klienta musi umożliwiać określenie, które atrybuty (pola) zgłoszenia są widoczne dla Klienta.	NIE
SOFT.TT.42	Serwis Klienta Trouble Ticketing i Podsystem SelfService muszą być zaimplementowane i zaprojektowane graficznie w taki sposób, żeby dla użytkownika wyglądały jak elementy jednej i tej samej aplikacji.	NIE
Integracja		
SOFT.TT.43	Trouble Ticketing musi być zintegrowany z innymi Podsystemami w zakresie pobierania informacji o Usługach użytkownika.	NIE
SOFT.TT.44	Trouble Ticketing musi być zintegrowany z innymi Podsystemami w	NIE

	zakresie pobierania informacji o fakturach użytkownika.	
SOFT.TT.45	Trouble Ticketing musi być zintegrowany z Podsystemem SSO w celu uwierzytelniania użytkowników.	NIE
SOFT.TT.46	Trouble Ticketing musi udostępniać pełne API udostępniające wszystkie funkcjonalności Podsystemu (zarówno operacyjne jak i administracyjne/konfiguracyjne).	NIE
SOFT.TT.47	Trouble Ticketing musi być zintegrowany z mechanizmami obsługującymi środowisko integracyjne (continuous integration).	NIE
Przepływy pracy (workflow)		
SOFT.TT.48	Trouble Ticketing musi umożliwiać definiowanie nowych przepływów pracy (workflow).	TAK
SOFT.TT.49	Trouble Ticketing musi umożliwiać definiowanie statusów zgłoszeń dostępnych dla każdego przepływu pracy.	TAK
SOFT.TT.50	W ramach przepływu pracy Trouble Ticketing musi umożliwiać zdefiniowanie przejść między statusami zgłoszenia.	TAK
SOFT.TT.51	W ramach przepływu pracy Trouble Ticketing musi umożliwiać zdefiniowanie formularza wyświetlanego użytkownikowi przy konkretnym przejściem między statusami. Jako "zdefiniowanie formularza" należy rozumieć tutaj określenie, jakie atrybuty zgłoszenia będą wyświetlane na formularzu, wraz z możliwością określenia kolejności tych atrybutów i umieszczania ich w osobnych "zakładkach".	TAK
SOFT.TT.52	W ramach edycji przepływu pracy Trouble Ticketing musi umożliwiać określenie ról, które mogą dokonać przejścia między statusami zgłoszenia.	TAK
SOFT.TT.53	W ramach edycji przepływu pracy Trouble Ticketing musi umożliwiać automatyczne przypisanie zgłoszenia do wskazanej osoby po przejściu między statusami zgłoszenia.	TAK
SOFT.TT.54	Trouble Ticketing musi umożliwiać definiowanie i edycję przepływów pracy (workflow) z poziomu przeglądarki internetowej, bez konieczności instalacji jakichkolwiek aplikacji i dodatków na stacji użytkownika.	TAK
SOFT.TT.55	Trouble Ticketing musi umożliwiać wdrożenie zdefiniowanych przepływów pracy (workflow) z poziomu przeglądarki internetowej użytkownika.	TAK
SOFT.TT.56	Trouble Ticketing, w ramach wdrożenia nowego przepływu pracy, musi przeprowadzić migrację istniejących zgłoszeń do nowego przepływu pracy.	TAK
SOFT.TT.57	Trouble Ticketing musi umożliwiać definiowanie przepływów pracy bez prowadzenia prac programistycznych.	TAK
SOFT.TT.58	W ramach definiowania przepływów pracy Trouble Ticketing musi umożliwiać utworzenie akcji uaktualnienia wybranych atrybutów (pól) zgłoszenia.	TAK
SOFT.TT.59	W ramach definiowania przepływów pracy Trouble Ticketing musi umożliwiać utworzenie akcji wysłania informacji o zgłoszeniu w formacie JSON do zewnętrznego Podsystemu.	TAK
SOFT.TT.60	Trouble Ticketing, dla każdego zgłoszenia, musi wizualizować wykorzystywany przepływ pracy w sposób graficzny wraz z zaznaczeniem	TAK

	aktualnego statusu danego zgłoszenia.	
SOFT.TT.61	Trouble Ticketing musi umożliwić ponowne otwarcie zamkniętego wcześniej zgłoszenia.	TAK
SOFT.TT.62	Trouble Ticketing musi umożliwiać określanie kierowników obszarów merytorycznych, do których są automatycznie przypisywane nowe zgłoszenia w danym obszarze.	TAK
SOFT.TT.63	Trouble Ticketing musi umożliwić użytkownikowi przejście między statusami zgłoszenia, zgodnie z posiadanymi uprawnieniami i konfiguracją przepływu pracy.	TAK
Powiadomienia e-mail		
SOFT.TT.64	Trouble Ticketing musi wysyłać powiadomienia e-mail o zdarzeniach związanych z cyklem życia zgłoszenia.	TAK
SOFT.TT.65	Trouble Ticketing musi umożliwiać określenie w konfiguracji projektu, jakie role projektowe będą otrzymywać powiadomienia o poszczególnych zdarzeniach.	TAK
SOFT.TT.66	Trouble Ticketing musi umożliwiać "śledzenie" zgłoszeń przez użytkowników, powodujące powiadomienie ich o zdarzeniach dotyczących danego zgłoszenia niezależnie od konfiguracji powiadomień.	TAK
SOFT.TT.67	Trouble Ticketing musi umożliwiać określenie ról, do których będzie wysyłać powiadomienia o przypadkach przekroczenia SLA.	NIE
SOFT.TT.68	Trouble Ticketing musi umożliwiać grupowanie wielu powiadomień w jedną wiadomość e-mail (ang. email digest)	NIE
SOFT.TT.69	Trouble Ticketing musi umożliwiać indywidualne włączenie/wyłączenie grupowania powiadomień dla każdego użytkownika osobno.	NIE
Obsługa zgłoszeń Klientów przez użytkowników wewnętrznych		
SOFT.TT.70	Trouble Ticketing musi umożliwiać przeszukiwanie zgłoszeń.	TAK
SOFT.TT.71	Trouble Ticketing musi umożliwiać filtrowanie wyników wyszukiwania zgłoszeń według poszczególnych atrybutów (pól) zgłoszenia.	TAK
SOFT.TT.72	Trouble Ticketing musi umożliwiać zapisanie aktualnej konfiguracji wyszukiwania i filtrowania jako "zapisanych filtrów".	TAK
SOFT.TT.73	Trouble Ticketing musi umożliwiać udostępnianie "zapisanych filtrów" innym użytkownikom.	TAK
SOFT.TT.74	Trouble Ticketing musi umożliwiać definiowanie zapisanych filtrów przy wykorzystaniu języka skryptowego, umożliwiającego co najmniej: filtrowanie wg atrybutów zgłoszenia (operatory: równy, nierówny, większe, większe lub równe, mniejsze, mniejsze lub równe, należące do zbioru wartości, nienależący do zbioru wartości, zawierający tekst, niezawierający tekstu), stosowanie operatorów AND OR NOT EMPTY NULL, sortowanie według atrybutów, a także filtrowanie według historycznych wartości atrybutów (atrybut ma obecnie lub miał w przeszłości daną wartość).	TAK
SOFT.TT.75	W przypadku części Trouble Ticketing przeznaczonej dla użytkowników wewnętrznych (obsługa klienta, inżynierowie wsparcia technicznego,	NIE

	developerzy itp.), Zamawiający może - na etapie akceptacji projektu technicznego - częściowo odstąpić od wymagania zapewnienia pełnej spójności graficznej wszystkich Podsystemów.	
SOFT.TT.76	W części przeznaczonej dla użytkowników wewnętrznych Trouble Ticketing musi udostępniać konfigurowalny przez użytkownika panel kontrolny (dashboard).	TAK
SOFT.TT.77	Panel kontrolny musi umożliwiać użytkownikowi osadzanie dowolnej liczby instancji widgetów.	TAK
SOFT.TT.78	Trouble Ticketing musi udostępniać widget dla panelu kontrolnego pozwalający wyświetlać wyniki wyszukiwania zrealizowane w oparciu o zapisane wcześniej filtry	TAK
SOFT.TT.79	Trouble Ticketing musi udostępniać widget dla panelu kontrolnego pozwalający wyświetlać zgłoszenia przypisane do aktualnie zalogowanego użytkownika.	TAK
SOFT.TT.80	Trouble Ticketing musi udostępniać widget dla panelu kontrolnego pozwalający wyświetlać zawartość poszczególnych kolejek zgłoszeń.	TAK
SOFT.TT.81	Trouble Ticketing musi udostępniać widget dla panelu kontrolnego pozwalający wyświetlać wykresy obrazujące liczbę realizowanych zgłoszeń.	TAK
SOFT.TT.82	Trouble Ticketing musi umożliwiać "udostępnienie" zgłoszenia - wysłanie e-maila z linkiem do zgłoszenia do wybranego użytkownika.	TAK
SOFT.TT.83	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi prezentować użytkownikom wewnętrznym pełne informacje o usłudze, której dotyczy zgłoszenie.	NIE
SOFT.TT.84	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi prezentować użytkownikom wewnętrznym pełne informacje o fakturach za Usługę, której dotyczy zgłoszenie.	NIE
SOFT.TT.85	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi prezentować użytkownikom wewnętrznym pełne informacje o płatnościach za Usługę, której dotyczy zgłoszenie.	NIE
SOFT.TT.86	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać użytkownikom wewnętrznym możliwość wyświetlenia pełnych informacji dotyczących wszystkich Usług użytkownika, którego dotyczy zgłoszenie.	NIE
SOFT.TT.87	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać użytkownikom wewnętrznym możliwość wyświetlenia pełnych informacji dotyczących wszystkich faktur użytkownika, którego dotyczy zgłoszenie.	NIE
SOFT.TT.88	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać użytkownikom wewnętrznym możliwość wyświetlenia pełnych informacji dotyczących wszystkich płatności użytkownika, którego dotyczy zgłoszenie.	NIE
SOFT.TT.89	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać użytkownikom wewnętrznym możliwość wyświetlenia pełnych informacji dotyczących wszystkich zgłoszeń użytkownika, którego dotyczy zgłoszenie.	NIE
SOFT.TT.90	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać	NIE

	użytkownikom wewnętrznym możliwość wyświetlenia pełnych informacji dotyczących konta użytkownika, którego dotyczy zgłoszenie.	
SOFT.TT.91	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać możliwość przejścia bezpośrednio do obiektu (np. Usługi, faktury, płatności, konta użytkownika) w ramach odpowiedniego Podsystemu dziedzinowego, którego dotyczy przedmiot zgłoszenia.	NIE
SOFT.TT.92	Trouble Ticketing, przy wyświetlaniu zgłoszenia, musi udostępniać możliwość zmiany danych użytkownika zewnętrznego, który utworzył zgłoszenie.	NIE
SOFT.TT.93	Trouble Ticketing, prezentując informacje o Usługach, użytkownikach, fakturach i płatnościach, musi uwzględnić uprawnienia do tych zasobów posiadane przez aktualnie zalogowanego użytkownika.	NIE
SOFT.TT.94	Trouble Ticketing musi umożliwić przekazanie zgłoszenia do realizacji innemu użytkownikowi, o ile aktualny użytkownik ma odpowiednie uprawnienia.	TAK
Ewidencja czasu pracy		
SOFT.TT.95	Trouble Ticketing musi zapewnić ewidencjonowanie czasu poświęconego na realizację danego zgłoszenia na każdym etapie jego realizacji.	TAK
SOFT.TT.96	Trouble Ticketing musi zapewniać integrację z Podsystemem Knowledge Base, umożliwiając w łatwy sposób wskazywanie artykułów z bazy wiedzy w komentarzach zgłoszeń (wyświetlanie pełnej struktury bazy wiedzy, łatwe przeszukiwanie struktury i osadzanie automatycznie linków po wybraniu danego elementu drzewa bazy wiedzy).	NIE
Liczba użytkowników		
SOFT.TT.97	Pierwsza wersja Podsystemu Trouble Ticketing musi zapewniać możliwość pracy dla minimum 100 nazwanych użytkowników.	TAK
SOFT.TT.98	Ostateczna wersja Podsystemu Trouble Ticketing (na dzień odbioru końcowego Projektu) musi zapewniać możliwość pracy dla minimum 500 nazwanych użytkowników.	NIE
Obsługa kolejek i SLA		
SOFT.TT.99	Trouble Ticketing musi umożliwiać definiowanie kolejek zgłoszeń.	NIE
SOFT.TT.100	Trouble Ticketing musi umożliwiać określenie, z wykorzystaniem języka skryptowego, jakie zgłoszenia trafiają do poszczególnych kolejek zgłoszeń.	NIE
SOFT.TT.101	Trouble Ticketing musi umożliwiać określenie, jakie atrybuty zgłoszenia są wyświetlane w widoku kolejki zgłoszeń.	NIE
SOFT.TT.102	Trouble Ticketing musi umożliwiać pracownikowi pobranie z kolejki zgłoszenia do realizacji.	NIE
SOFT.TT.103	Trouble Ticketing musi umożliwiać definiowanie metryk SLA.	NIE
SOFT.TT.104	Trouble Ticketing musi umożliwiać określenie zdarzeń (co najmniej: utworzenie zgłoszenia, zmiana statusu, utworzenie komentarza, przypisanie zgłoszenia do użytkownika, zamknięcie zgłoszenia) rozpoczynających, wstrzymujących i kończących liczenie czasu dla danej metryki SLA.	NIE

SOFT.TT.105	Trouble Ticketing musi umożliwiać określenie zdarzeń (co najmniej: utworzenie zgłoszenia, zmiana statusu, utworzenie komentarza, przypisanie zgłoszenia do użytkownika, zamknięcie zgłoszenia), wstrzymujących (pauzujących) liczenie czasu dla danej metryki SLA.	NIE
SOFT.TT.106	Trouble Ticketing musi umożliwiać określenie zdarzeń (co najmniej: utworzenie zgłoszenia, zmiana statusu, utworzenie komentarza, przypisanie zgłoszenia do użytkownika, zamknięcie zgłoszenia) kończących liczenie czasu dla danej metryki SLA.	NIE
SOFT.TT.107	Trouble Ticketing musi umożliwiać określenie wymaganych czasów reakcji dla zgłoszeń spełniających określone kryteria (zdefiniowane z wykorzystaniem języka skryptowego).	NIE
SOFT.TT.108	Trouble Ticketing musi umożliwiać definiowanie kalendarzy określających w jakie dni i w jakich godzinach liczony jest upływ czasu reakcji.	NIE
SOFT.TT.109	Trouble Ticketing musi umożliwiać definiowanie w kalendarzach SLA dni świątecznych, w których upływ czasu reakcji nie jest liczony.	NIE

5.2.13. Centralny system logów

ID wymagania	Treść wymagania
SOFT.LOG.1	Centralny system logów musi umożliwiać zbieranie logów przesłanych za pomocą następujących formatów danych: syslog, json.
SOFT.LOG.2	Centralny system logów musi umożliwiać podłączanie (za pomocą API/modułów/pluginów) innych formatów danych wejściowych.
SOFT.LOG.3	Centralny system logów musi umożliwiać zbieranie logów zarówno z infrastruktury sprzętowej jak i Podsystemów oprogramowania.
SOFT.LOG.4	Centralny system logów musi zapewniać pełno tekstową wyszukiwarkę logów poprzez GUI oraz API z zachowaniem filtrowania, min. źródło, data, poziom alertu, treść.
SOFT.LOG.5	Centralny system logów musi zapewniać parsowanie i katalogowanie przechowywanych logów.
SOFT.LOG.6	Centralny system logów musi zapewniać archiwizację, rotację i kompresję logów.
SOFT.LOG.7	Centralny system logów musi zapewniać szybkie wyszukiwanie logów poprzez wykorzystanie mechanizmów indeksujących (np. poprzez elasticsearch).
SOFT.LOG.8	Centralny system logów musi zapewniać zarządzanie dostępem do poszczególnych źródeł logów oraz poziomów logowania.
SOFT.LOG.9	Centralny system logów musi umożliwiać eksport informacji o określonych rodzajach logów poprzez mechanizm triggeringu do Podsystemu NOC-monitoring (na potrzeby wygenerowania alarmu).
SOFT.LOG.10	Centralny system logów musi umożliwiać definiowanie reguł filtrowania logów w czasie rzeczywistym (oraz wyświetlania ich bez przeładowania strony - AJAX) oraz zapisywania tych reguł.
SOFT.LOG.11	Centralny system logów musi umożliwiać definiowanie alertów, których spełnienie spowoduje wysłanie powiadomienia e-mail do administratora.

SOFT.LOG.12	Centralny system logów musi zawierać panel kontrolny (dashboard) umożliwiający osadzanie widgetów, w których wyświetlane są logi spełniające określone kryteria wyszukiwania bądź wykresy bazujące na tych kryteriach.
SOFT.LOG.13	Centralny system logów musi umożliwiać definiowanie kryteriów wyszukiwania według poszczególnych atrybutów wpisu w logach (np. data, serwer, treść komunikatu itp.).
SOFT.LOG.14	Centralny system logów musi umożliwiać definiowanie kryteriów wyszukiwania z wykorzystaniem wyrażeń regularnych.

5.2.14. NOC: Monitoring

ID wymagania	Treść wymagania
SOFT.NOC-M.1	Oprogramowanie do monitoringu musi umożliwiać przedstawienie w formie graficznej statystyk dla wszystkich istotnych elementów sieci, takich jak: - przepustowość łącz pomiędzy poszczególnymi urządzeniami, - przepustowość łącz do operatorów, - temperaturę pracy urządzeń, - utylizację pracy urządzeń oraz komponentów w urządzeniach: - utylizacja danej karty, - wolne/zajęte miejsce na dysku, - wolna/zajęta pamięć, - wolne/zajęte przerwania, - inne, istotne z punktu widzenia szacowania obciążenia danego urządzenia. - statystykę błędów na danym porcie/karcie, - mapę połączeń wraz z procentowym zajęciem danego łącza, - statystykę zasilania urządzenia.
SOFT.NOC-M.2	Oprogramowanie do monitoringu musi umożliwiać wykrywanie sieci: - automatyczne wykrywanie urządzeń działających zgodnie z protokołem TCP/IP, - automatyczne tworzenie mapy przedstawiającej logiczną strukturę sieci, - półautomatyczne tworzenie mapy przestawiającej fizyczną strukturę sieci, - wykrywanie usług sieciowych, - automatyczna klasyfikacja urządzeń i usług (funkcja, typ, producent);
SOFT.NOC-M.3	Oprogramowanie do monitoringu musi umożliwiać budowanie konfiguracji Systemu na podstawie automatycznie wykrytych elementów sieci.
SOFT.NOC-M.4	Oprogramowanie do monitoringu musi zapewniać wsparcie dla protokołów SNMP (v2 i v3) oraz ICMP.
SOFT.NOC-M.5	Oprogramowanie do monitoringu musi zapewniać możliwość importowania własnych baz MIB SNMP do Podsystemu.
SOFT.NOC-M.6	Oprogramowanie do monitoringu musi zapewniać umożliwianie monitorowania wszystkich istotnych parametrów urządzeń poprzez możliwość tworzenia własnych wtyczek, template'ów i skryptów.
SOFT.NOC-M.7	Oprogramowanie do monitoringu musi zapewniać możliwość tworzenia tzw. liczników wirtualnych – liczników opartych o wartości liczników rzeczywistych powiązanych operacjami matematycznymi.

SOFT.NOC-M.8	Oprogramowanie do monitoringu musi zapewniać możliwość samodzielnej konfiguracji wyglądu alarmów, układu alarmów, sposobu ich reprezentacji.
SOFT.NOC-M.9	Oprogramowanie do monitoringu musi zapewniać możliwość tworzenia własnych kwerend SNMP.
SOFT.NOC-M.10	Oprogramowanie do monitoringu musi dostarczać wiele metod raportowania: - raportowanie przepływności, - raportowanie dostępności, - raportowanie czasów odpowiedzi, - raportowanie obciążenia procesorów, - raportowanie zajętości powierzchni, - raportowanie historyczne, - raportowanie w czasie rzeczywistym.
SOFT.NOC-M.11	Oprogramowanie do monitoringu musi zapewniać możliwość generowania raportów przekrojowych i skrośnych.
SOFT.NOC-M.12	Oprogramowanie do monitoringu musi zapewniać możliwość generowania raportów automatycznych, zgodnie z ustalonym terminarzem.
SOFT.NOC-M.13	Oprogramowanie do monitoringu musi zapewniać możliwość eksportowania raportów i zebranych danych do formatu CSV.
SOFT.NOC-M.14	Oprogramowanie do monitoringu musi zapewniać współpracę z relacyjną bazą danych,
SOFT.NOC-M.15	Oprogramowanie do monitoringu musi zapewniać wsparcie dla hierarchicznego modelu uprawnień.
SOFT.NOC-M.16	Oprogramowanie do monitoringu musi zapewniać współpracę z operatorem poprzez przeglądarkę WWW z możliwością stworzenia spersonalizowanej strony domowej.
SOFT.NOC-M.17	Oprogramowanie do monitoringu musi zapewniać umożliwianie graficznego przedstawienia schematu sieci, wraz umieszczeniem informacji o jej aktualnych parametrach.
SOFT.NOC-M.18	Oprogramowanie do monitoringu musi zapewniać reagowanie na określone wcześniej graniczne parametry i po ich przekroczeniu.
SOFT.NOC-M.19	Oprogramowanie do monitoringu musi zapewniać wysyłanie powiadomień - informowanie o wystąpieniu zdarzenia, wraz z określeniem poziomu alarmu: - na monitorze, - poprzez wysyłanie wiadomości e-mail, - poprzez wysyłanie wiadomości SMS (poprzez zintegrowane urządzenie dedykowane GSM).
SOFT.NOC-M.20	Oprogramowanie do monitoringu musi zapewniać możliwość wysłania powiadomień gdy zajdą określone wcześniej zdarzenia.
SOFT.NOC-M.21	Oprogramowanie do monitoringu musi zapewniać możliwość określenia użytkownika bądź grupy użytkowników, do których wysyłany jest komunikat na podstawie zdefiniowanych filtrów wysyłania powiadomień.
SOFT.NOC-M.22	Oprogramowanie do monitoringu musi zapewniać możliwość integracji z systemem paszportyzacji.
SOFT.NOC-M.23	Oprogramowanie do monitoringu musi zapewniać wsparcie dla ściany wizyjnej.
SOFT.NOC-M.24	Oprogramowanie do monitoringu musi zapewniać wsparcie dla systemu dodatków

	(wtyczek), możliwość tworzenia dodatków min. w językach: C, python, perl, bash, php, java.
SOFT.NOC-M.25	Oprogramowanie do monitoringu musi zapewniać monitorowanie sprzętu poprzez protokół IPMI.
SOFT.NOC-M.26	Oprogramowanie do monitoringu musi zapewniać możliwość obsługi map przy wykorzystaniu bibliotek D3 lub równoważnej.
SOFT.NOC-M.27	Oprogramowanie do monitoringu musi zapewniać dostęp do API, możliwość tworzenia własnych modułów do Podsystemu, personalizację Podsystemu.
SOFT.NOC-M.28	Oprogramowanie do monitoringu musi zapewniać możliwość monitorowania odseparowanych systemów poprzez serwery proxy.
SOFT.NOC-M.29	Oprogramowanie do monitoringu musi zapewniać wsparcie dla IPv6/dual stack, Podsystem musi być dostępny poprzez adresację IPv4 oraz IPv6.
SOFT.NOC-M.30	Oprogramowanie do monitoringu musi zapewniać wsparcie dla LDAP.
SOFT.NOC-M.31	Logowanie użytkowników do Podsystemu monitoringu musi zostać zrealizowane na podstawie autoryzacji z centralną bazą danych (np. LDAP), wspólną przynajmniej dla: Podsystemu monitoringu, Podsystemu zarządzania i Podsystemu DCIM.
SOFT.NOC-M.32	Oprogramowanie musi zostać zintegrowane z dedykowanym urządzeniem do wysyłania powiadomień SMS (infrastruktura: bramka SMS).
SOFT.NOC-M.33	Oprogramowanie do monitoringu musi zostać skonfigurowane do monitorowania całej infrastruktury oraz wszystkich Podsystemów oprogramowania.
SOFT.NOC-M.34	Oprogramowanie do monitoringu musi umożliwiać identyfikację każdego z urządzeń w Podsystemie NOC-DCIM (np. poprzez odnośnik).

5.2.15. NOC: Podsystem zarządzania

ID wymagania	Treść wymagania
SOFT.NOC-SZ.1	NOC: Podsystem zarządzania musi umożliwiać konfigurację, zarządzanie oraz ewidencję wszystkich urządzeń pracujących w ramach infrastruktury Centrum Danych. Podsystem może stanowić jeden spójny system zarządzania lub zbiór systemów zarządzania dostarczonych przez producentów poszczególnych urządzeń wdrożonych w ramach infrastruktury.
SOFT.NOC-SZ.2	W ramach NOC: Podsystem zarządzania dopuszcza się wdrożenie wielu rozwiązań dostarczanych przez producentów dostarczanego sprzętu, przy czym w przypadku wdrożenia kilku systemów zarządzania należy zadbać o ich spójność w zakresie bazy danych użytkowników i uprawnień (wspólna baza danych użytkowników i uprawnień) np. w oparciu o LDAP.
SOFT.NOC-SZ.3	W ramach NOC: Podsystem zarządzania wszystkie zintegrowane systemy zarządzania muszą umożliwiać śledzenie zmian w konfiguracji sprzętu który obsługują z zachowaniem spójnej informacji: kto dokonał zmiany, jaka to była zmiana i kiedy nastąpiła. Rekomendowane jest wykorzystanie systemu GIT.
SOFT.NOC-SZ.4	W ramach NOC: Podsystem zarządzania wymagane jest cykliczne realizowanie kopii zapasowej konfiguracji całej infrastruktury (kopie konfiguracji poszczególnych urządzeń).

	Kopia zapasowa konfiguracji musi być niezależna od systemów zarządzania (odtworzenie konfiguracji z takiej kopii powinno być możliwe również bez pośrednictwa systemu zarządzania)
SOFT.NOC-SZ.5	Składowe elementy NOC: Podsystem zarządzania musi być w pełni funkcjonalne w odniesieniu do wymagań i nie powinny posiadać żadnych ograniczeń wynikających z braku licencji.
SOFT.NOC-SZ.6	Każdy system zarządzania wchodzący w skład oprogramowania NOC: Podsystem zarządzania musi być dostarczony wraz systemem operacyjnym na jakim pracuje, jeśli takiego wymaga; jeśli jest wymagana dodatkowa licencja do oprogramowania zarządzającego np. licencja systemu operacyjnego, musi być ona dostarczona razem z oprogramowaniem zarządzającym.
SOFT.NOC-SZ.7	Logowanie użytkowników do NOC: Podsystem zarządzania musi zostać zrealizowane na podstawie autoryzacji z centralną bazą danych (np. LDAP), wspólną przynajmniej dla: Podsystemu monitoringu, Podsystemu zarządzania i Podsystemu DCIM.

5.2.16. NOC: DCIM

ID wymagania	**Treść wymagania**
SOFT.NOC-DCIM.1	DCIM musi zapewniać inwentaryzację sprzętu i jego identyfikację w szafach.
SOFT.NOC-DCIM.2	DCIM musi zapewniać monitoring zajętości szaf.
SOFT.NOC-DCIM.3	DCIM musi obsługiwać rezerwację miejsca w szafach.
SOFT.NOC-DCIM.4	DCIM musi zapewniać monitoring obciążenia CDU/PDU: - z pomiaru - teoretyczny
SOFT.NOC-DCIM.5	DCIM musi zapewniać śledzenie połączeń Ethernet.
SOFT.NOC-DCIM.6	DCIM musi zapewniać śledzenie połączeń elektrycznych.
SOFT.NOC-DCIM.7	DCIM musi raportować bilans cieplny.
SOFT.NOC-DCIM.8	DCIM musi zapewniać monitoring użycia portów switchy.
SOFT.NOC-DCIM.9	DCIM musi zapewniać graficzną prezentację serwerowni.
SOFT.NOC-DCIM.10	DCIM musi wspierać protokół SNMP v1/2c do monitorowania temperatury i wilgotności.
SOFT.NOC-DCIM.11	DCIM musi wspierać protokół SNMP v1/2c do monitorowania PDU/CDU.
SOFT.NOC-DCIM.12	DCIM musi być w pełni niezależne od producentów PDU/CDU/czujników.
SOFT.NOC-DCIM.13	DCIM musi wspierać raportowanie zasobów.
SOFT.NOC-DCIM.14	DCIM musi zapewniać raport kosztów pracy DC w tym: koszt miejsca, koszt energii elektrycznej.
SOFT.NOC-DCIM.15	DCIM musi zapewniać interfejs WWW.
SOFT.NOC-DCIM.16	DCIM musi zostać zintegrowane pod względem obsługi alarmów i monitoringu do Podsystemu NOC-monitoring.
SOFT.NOC-DCIM.17	DCIM musi zostać zintegrowane z istniejącą infrastrukturą pasywną Zamawiającego.
SOFT.NOC-DCIM.18	Logowanie użytkowników do DCIM musi zostać zrealizowane na podstawie autoryzacji z centralną bazą danych (np. LDAP), wspólną przynajmniej dla:

	Podsystemu monitoringu, Podsystemu zarządzania i Podsystemu DCIM.

6. Pozostałe wymagania

6.1. Instruktaże stanowiskowe

ID wymagania	Treść wymagania
INST.1	Instruktaże w zakresie użytkowania Systemu muszą obejmować obsługę całej Platformy oprogramowania w zakresie oferowanych przez nią usług.
INST.2	Instruktaże w zakresie administrowania Systemu muszą obejmować administrację całej Platformy oprogramowania jak i poszczególnych jej Podsystemów.
INST.3	Wykonawca zobowiązany jest przygotować materiały instruktażowe w wersji elektronicznej i muszą one być udostępnione w ramach Bazy Wiedzy.
INST.4	Czas trwania instruktażu w zakresie użytkowania Systemu musi wynosić, co najmniej 8 godzin zegarowych liczonych bez przerw.
INST.5	Czas trwania instruktażu w zakresie administrowania Systemu musi wynosić, co najmniej 8 godzin zegarowych liczonych bez przerw dla każdego Podsystemu oprogramowania wskazanego w rozdziałach 4.1.5 i 5.1.4.
INST.6	Szkolenia odbędą się w lokalizacji wskazanej przez Zamawiającego na terenie Szczecina – Zamawiający zapewnia salę szkoleniową.
INST.7	Wykonawca odpowiada za przygotowanie środowiska szkoleniowego, które pozwoli na przeprowadzenie instruktaży stanowiskowych.
INST.8	W instruktażach mogą uczestniczyć pracownicy Zamawiającego lub osoby z podmiotów przez niego wskazanych.
INST.9	Instruktaże w zakresie infrastruktury sprzętowej muszą być połączone z zajęciami praktycznymi (praca na sprzęcie, konfiguracja).
INST.10	Dla każdej grupy funkcjonalnej infrastruktury sprzętowej wskazanej w rozdziale 4, czas trwania instruktażu musi wynosić 8 godzin zegarowych liczonych bez przerw.