



CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel.: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Załącznik nr 3 do Opisu Przedmiotu Zamówienia

SPECYFIKACJA WYMAGAŃ OGÓLNYCH DLA PLATFORMY P1



**INNOWACYJNA
GOSPODARKA**
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka „Dotacje na innowacje – inwestujemy w naszą przyszłość”



SPIS TREŚCI

Wymagania ogólne.....	3
Interfejs użytkownika.....	3
Bezpieczeństwo	5
Dostępność.....	7
Skalowalność.....	8
Standardy	9
Wydajność	11
Wymagania dot. architektury	11
Ogólne wymagania funkcjonalne	13





Wymagania ogólne

Sekcja zawiera wymagania, które ze względu na swoją naturę odnoszą się do wszystkich lub większości podsystemów. Wymagania takie nie są katalogowane przy poszczególnych podsystemach, lecz zostały ujęte w niniejszej sekcji.

W zakresie wymagań jakościowych dla systemu P1 powinny być spełnione wymagania normy PN-ISO/IEC 25000:2008, Tytuł: Inżynieria oprogramowania -- Wymagania jakości i ocena produktów programowych (SQuaRE) - Przewodnik po SQuaRE.

Interfejs użytkownika

Wymaganie	Opis wymagania
WYM.OPZ.GUI.NFN.01 Interfejs przeglądarkowy	Interfejs użytkownika zrealizowany zostanie jako zestaw aplikacji serwerowych prezentujących dane w przeglądarce po stronie klienta
WYM.OPZ.GUI.NFN.02 Wersje przeglądarek	<p>Do testów aplikacji dla Usługobiorców i Usługodawców wykorzystane będą te przeglądarki, które w okresie 3 tyg. przed rozpoczęciem testów wewnętrznych danego produktu będą posiadały minimum 2% udziału w rynku oraz w przypadku braku przekroczenia progu 2% bądź przekroczenia go tylko przez jedną przeglądarkę z rodziny (gdzie rodziną jest MSIE, Firefox, Chrome, Opera, Safari) - dwie najpopularniejsze wersje z danej rodziny przeglądarki. Do testów wykorzystane będą również najnowsze wersje z każdej rodziny przeglądarek, których udział rynku został oszacowany poniżej poziomu 2% a data wydania nowej wersji przeglądarki przekracza miesiąc czasu.</p> <p>Wykonawca w okresie 3 tyg. przed rozpoczęciem testów wewnętrznych danego produktu prześle Zamawiającemu informację o zestawieniu przeglądarek, którą następnie umieści w Planie Testów.</p> <p>Do testów aplikacji dla innych niż powyżej wskazanych interesariuszy wykorzystane będą te przeglądarki, które w okresie 3 tyg. przed rozpoczęciem testów wewnętrznych danego produktu będą posiadały minimum 3% udziału w rynku oraz w przypadku braku przekroczenia progu 3% bądź przekroczenia go tylko przez jedną przeglądarkę z rodziny (gdzie rodziną jest MSIE, Firefox, Chrome, Opera, Safari) - dwie najpopularniejsze wersje z danej rodziny przeglądarki. Do testów wykorzystane będą również najnowsze wersje z każdej rodziny przeglądarek, których udział rynku został oszacowany poniżej poziomu 3% a data wydania nowej wersji przeglądarki przekracza miesiąc czasu.</p> <p>Wykonawca w okresie 3 tyg. przed rozpoczęciem testów wewnętrznych danego produktu prześle Zamawiającemu informację o zestawieniu przeglądarek, którą następnie umieści w Planie Testów.</p> <p>Jeżeli wersja przeglądarki nie jest już wspierana przez producenta, to nie wchodzi w</p>



**CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA**

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel.: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Wymaganie	Opis wymagania
	<p>zakres testów niezależnie od tego, w jakim przedziale procentowym się mieści. Powinna zostać dodana adnotacja w planie testów wykluczająca nie wspierane wersje</p> <p>Wymagania obowiązują dla przeglądarek działających pod kontrolą wspieranych wersji systemu operacyjnego MS Windows. W zakresie przeglądarki Safari do testów wykorzystywana będzie najnowsza jej wersja. W stosunku do konsol administracyjnych dopuszczalna jest obsługa tylko przeglądarek Firefox i Chrome. Zamawiający dopuści w stosunku do narzędzi webowych typu COTS również stosowanie przeglądarek zalecanych przez producenta danego oprogramowania. Ewentualne odstępstwa wymagać będą każdorazowego uzgodnienia z Zamawiającym.</p>
WYM.OPZ.GUI.NFN.03 Dobre praktyki projektowania	Interfejs użytkownika będzie zaprojektowany w zgodzie z powszechnie przyjętymi standardami i szeroko pojętymi dobrymi praktykami w dziedzinie konstruowania intuicyjnego interfejsu użytkownika.
WYM.OPZ.GUI.NFN.04 Dostęp dla osób niepełnosprawnych	Dokumenty jak i cała treść prezentowana przez interfejs powinna być czytelna, również dla użytkowników niedowidzących. Interfejs ogólnodostępnej części serwisu (w tym przeznaczona dla zarejestrowanych użytkowników – przedstawicieli podmiotów i osób fizycznych), z wyłączeniem konsol administracyjnych, w zakresie dostępności dla ludzi niepełnosprawnych powinien być zgodny z wytycznymi organizacji W3C [“Web Content Accessibility Guidelines 1.0”, W3C Recommendation 5-May-1999] na poziomie „pojedyncze A”. http://www.w3.org/TR/1999/WAI-WEBCONTENT-19990505/
WYM.OPZ.GUI.NFN.05 Standard rozdzielczości	Interfejs użytkownika będzie dostosowany do ekranów o rozdzielczości przynajmniej 1024x768. Wyjątkiem będą moduły wspierające urządzenia mobilne, które będą korzystać z rozdzielczości natywnej dla danego rozwiązania.
WYM.OPZ.GUI.NFN.06 Standard kodowania znaków	System będzie w warstwie prezentacyjnej posługiwać się standardem kodowania znaków UTF-8.
WYM.OPZ.GUI.NFN.07 Praca w wielu okienkach	System musi umożliwiać użytkownikowi pracę w kilku oknach aplikacji równocześnie, przy czym wystarczające jest wtedy jednokrotne zalogowanie do systemu.
WYM.OPZ.GUI.NFN.08 Urządzenia mobilne	<p>Rozwiązanie musi zapewniać wsparcie dla urządzeń mobilnych. Musi wspierać urządzenia mobilne pracujące pod kontrolą co najmniej następujących systemów operacyjnych – o ile będą one używane w czasie wdrażania systemu P1:</p> <ul style="list-style-type: none">- Android,- bada-OS,- BlackBerry OS,- iOS,- Windows Mobile,- Symbian. <p>Wymaganie nie dotyczy konsol administracyjnych.</p>



Wymaganie	Opis wymagania
WYM.OPZ.GUI.NFN.09 Interfejs graficzny do monitoringu	Podsystem musi posiadać zestaw graficznych narzędzi administracyjnych, umożliwiających monitoring poszczególnych warstw systemu: <ul style="list-style-type: none">- warstwy bazy danych- warstwy aplikacji i narzędzi.- analizy planów zapytań i optymalizacji, "wąskich gardeł systemu", obciążenia procesora, ilości operacji IO, wykorzystania pozostałych zasobów sprzętowych i programowych.

Bezpieczeństwo

Wymaganie	Opis wymagania
WYM.OPZ.BEZ.NFN.01 Ochrona dostępu	System musi zapewnić pełną ochronę przed nieuprawnionym dostępem osób i systemów do danych. W szczególności wszystkie podsystemy spełniać muszą wymogi Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych (Dz.U. 2004, nr 100, poz. 1024).
WYM.OPZ.BEZ.NFN.02 Ochrona danych osobowych	Wszystkie podsystemy muszą spełniać wymogi ustawy o ochronie danych osobowych.
WYM.OPZ.BEZ.NFN.03 Komunikacja z systemami zewnętrznymi	Komunikacja z systemami zewnętrznymi musi być szyfrowana.
WYM.OPZ.BEZ.NFN.04 Normy	System w zakresie bezpieczeństwa danych spełniać będzie wymogi normy PN-EN ISO 27799:2010: "Informatyka w ochronie zdrowia - Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002" oraz innych norm dotyczących bezpieczeństwa systemów informatycznych: <ul style="list-style-type: none">• CR 13694:1999• CR 14301:2002• CR 14302:2002• EN 12251:2004• EN 13606-4:2009• ENV 13608-1:2003• ENV 13608-2:2003• ENV 13608-3:2003• ISO/IEC 27001:2005• ISO/IEC 27002:2005• ISO/IEC 27003:2010• ISO/IEC 27004:2009





Wymaganie	Opis wymagania
	<ul style="list-style-type: none">• ISO/IEC 27005:2011• ISO/IEC 27006:2009• ISO/IEC FDIS 27034• ISO/TR 21548:2010• ISO/TS 21547:2010 lub innych, które je zastępują albo aktualizują.
WYM.OPZ.BEZ.NFN.05 Ograniczenie dostępu administracyjnego	Administracyjny dostęp do elementów systemu nieobjęty funkcjami kontroli dostępu zapewnianymi przez mechanizmy uwierzytelniania i autoryzacji samego systemu (np. bezpośredni dostęp do tabel bazy danych) możliwy będzie wyłącznie z wybranych, wskazanych przez Zamawiającego lokalizacji i maszyn.
WYM.OPZ.BEZ.NFN.06 DMZ	Serwery służące komunikacji z systemami oraz użytkownikami zewnętrznymi muszą się znajdować w DMZ.
WYM.OPZ.BEZ.NFN.07 Dostęp do danych osobowych	Dostęp użytkownika do danych osobowych lub wrażliwych będzie wymagał uwierzytelnienia.
WYM.OPZ.BEZ.NFN.08 Dokumentowanie przetwarzania danych osobowych	System spełniać będzie wymogi Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. w sprawie dokumentacji przetwarzania danych osobowych.
WYM.OPZ.BEZ.NFN.09 Wykorzystanie usług identyfikacji i uwierzytelniania	System wykorzystywać będzie usługi identyfikacji i uwierzytelniania systemu P2, a zatem spełniać będzie wszystkie zdefiniowane tam reguły i standardy.
WYM.OPZ.BEZ.NFN.10 Szyfrowanie danych zastrzeżonych	Wszystkie dane zastrzeżone (dane osobowe, indywidualne dane medyczne) w bazach danych przechowywane będą w sposób zaszyfrowany.
WYM.OPZ.BEZ.NFN.11 Blokowanie nieaktywnej sesji	System blokować będzie sesje użytkowników po ustalonym konfiguracyjnie czasie nieaktywności.
WYM.OPZ.BEZ.NFN.12 Certyfikowany podpis przesyłanego kodu	Kod wysyłany przez system i wykonywany po stronie klienta musi być podpisany cyfrowo poprzez certyfikat wystawiony przez renomowane centrum autoryzacyjne.
WYM.OPZ.BEZ.NFN.13 Poziom kontroli dostępu do danych	Serwery systemu muszą podlegać ochronie przed nieuprawnionym dostępem do danych na poziomie uprawnień systemu operacyjnego.
WYM.OPZ.BEZ.NFN.14 Zabezpieczenie typu IPS	System będzie chroniony przez zabezpieczenia typu IPS.





Wymaganie	Opis wymagania
WYM.OPZ.BEZ.NFN.15 Zabezpieczenie antywirusowe	Zarówno serwery jak i pozostałe komputery podłączone do sieci systemu P1 (np. końcówki administratorskie) muszą być zabezpieczone aktualizowanym na bieżąco oprogramowaniem antywirusowym o ile takowe oprogramowanie jest dostępne na daną platformę.
WYM.OPZ.BEZ.NFN.16 Kopia zapasowa	Podsystem musi umożliwiać odtworzenie danych na podstawie kopii zapasowej, w szczególności musi umożliwiać: - wykonywanie kopii zapasowych danych w trakcie pracy systemu, - odtworzenie danych.

Dostępność

Wymaganie	Opis wymagania
WYM.OPZ.DOS.NFN.01 Ciągłość pracy	System musi pracować w trybie 24x7.
WYM.OPZ.DOS.NFN.02 Minimalna dostępność	Dostępność systemu liczona w cyklu rocznym nie może być niższa niż 99,8%, co oznacza maksymalny czas niedostępności (awarii) systemu 17 godzin 31 minut 48 sekund w ww. okresie.
WYM.OPZ.DOS.NFN.04 Lokalizacje	Architektura Systemu musi umożliwiać posadowienie Systemu w dwóch lokalizacjach: - Centralnym Ośrodku Przetwarzania Danych (COPD), - Zapasowym Ośrodku Przetwarzania Danych (ZOPD).
WYM.OPZ.DOS.NFN.05 Przełączenie między lokalizacjami	Przełączenie przetwarzania z COPD na ZOPD i odwrotnie musi być możliwe bez utraty integralności danych oraz bez konieczności dokonywania migracji.
WYM.OPZ.DOS.NFN.06 Czas przełączenia między lokalizacjami	Konfiguracja systemu musi umożliwiać przełączenie ośrodków w czasie nie dłuższym niż 120 minut. Procedura przełączania musi ograniczać do minimum konieczność wpisywania danych przez Administratora. Dopuszcza się jedynie podawanie danych uwierzytelniających i wykonywanie wcześniej przygotowanych skryptów.
WYM.OPZ.DOS.NFN.07 Redundancja	System musi być zbudowany z elementów redundantnych zapewniających automatyczne przejście funkcji elementu, który uległ awarii. Takie przejście musi być niewidoczne dla aktorów korzystających z systemu. Elementy redundantne w ramach aktywnego ośrodka muszą być wykorzystywane przy normalnym działaniu systemu do obsługiwanie części obciążenia.
WYM.OPZ.DOS.NFN.08 Monitorowanie	System musi być wyposażony w mechanizmy monitorujące, ułatwiające wykrywanie potencjalnych źródeł awarii





Wymaganie	Opis wymagania
WYM.OPZ.DOS.NFN.09 Wielodostęp	System musi umożliwiać wielu użytkownikom równoległy dostęp do tych samych danych lub obszarów funkcjonalnych bez utraty integralności danych
WYM.OPZ.DOS.NFN.10 Wznawianie pracy po awarii	System musi udostępniać mechanizmy wznawiające pracę systemu po awarii. W szczególności musi być możliwe selektywne uruchamianie zleceń z kolejki oraz samych kolejek.
WYM.OPZ.DOS.NFN.11 Wpływ awarii	System musi zapewniać, że awaria jednego elementu nie powoduje niedostępności usługi, a jedynie spadek wydajności. Warunek ten nie musi zostać spełniony, jeżeli awarii ulega ostatni element danego typu.
WYM.OPZ.DOS.NFN.12 Wykorzystanie elementów dublujących	Elementy dublujące muszą być wykorzystywane przy normalnym działaniu systemu do obsługiwanie części obciążenia.
WYM.OPZ.DOS.NFN.13 Współpraca z monitoringiem zewnętrznym	System musi posiadać możliwość współpracy z zewnętrznym narzędziem monitorującym poziom usług. Narzędzie to zostanie zdefiniowane w ramach zamówienia na ITS.

Skalowalność

Wymaganie	Opis wymagania
WYM.OPZ.SKA.NFN.01 Liniowość skalowania	System musi zapewnić możliwość, zbliżonego do liniowego, skalowania poziomego, względem: <ul style="list-style-type: none">- maksymalnego wolumenu obsługiwanych operacji w jednostce czasu,- ilości przetwarzanych i zgromadzonych danych,- liczby jednocześnie pracujących użytkowników.
WYM.OPZ.SKA.NFN.02 Skalowalność bez zmian w kodzie	System musi zapewniać możliwość skalowalności poprzez dodawanie kolejnych węzłów w poszczególnych warstwach (scale out) oraz jedynie instalację oprogramowania i zmiany parametrów konfiguracyjnych, bez konieczności zmian kodu oprogramowania.
WYM.OPZ.SKA.NFN.03 Klastrowanie	Architektura rozwiązania musi umożliwiać skalowanie rozwiązania poprzez tworzenie logicznych klastrów serwerów na poziomie: <ul style="list-style-type: none">- serwerów WWW- serwerów aplikacyjnych- serwerów baz danych
WYM.OPZ.SKA.NFN.04 Skalowalność zasobów sprzętowych	Zasoby sprzętowe dostarczone w ramach systemu muszą umożliwiać rozbudowę poprzez dodawanie kolejnych elementów, np. dodatkowej pamięci, dodatkowych dysków, procesorów itp.





Wymaganie	Opis wymagania
WYM.OPZ.SKA.NFN.05 Skalowalność bez wpływu na użytkowników	Operacje rozszerzania systemu o kolejne serwery lub inne elementy nie mogą wymagać zatrzymania systemu lub spadku jego wydajności zauważalnego przez aktorów systemu.
WYM.OPZ.SKA.NFN.06 Load-balancing	Architektura rozwiązania musi umożliwiać wykorzystanie mechanizmu równoważenia obciążenia (load balancing) przy zastosowaniu więcej niż 1 serwera
WYM.OPZ.SKA.NFN.07 Skalowalność bezpieczeństwa	Mechanizmy bezpieczeństwa muszą zapewniać możliwość rozwoju i skalowania w przyszłości, wraz z rozwojem usług realizowanych przez P1.

Standardy

Wymaganie	Opis wymagania
WYM.OPZ.STA.NFN.01 Neutralność technologiczna	System P1 będzie wykonany przy zachowaniu zasady neutralności technologicznej, bazującej na stosowaniu otwartych standardów (w ich aktualnej wersji) wszędzie tam, gdzie są one dostępne, a ich zastosowanie jest uzasadnione ekonomicznie. Warunki, jakie powinien spełniać standard otwarty, określają zalecenia zawarte w European Interoperability Framework (EIF) w wersji 2.0.
WYM.OPZ.STA.NFN.02 SOAP	System musi zapewnić wsparcie dla standardu przesyłania komunikatów SOAP z załącznikami (z kodowaniem komunikatów: "document/literal") w wersji 1.1 lub wyższej (http://www.w3.org/TR/soap/)
WYM.OPZ.STA.NFN.03 Protokoły transportowe	System P1 musi umożliwiać przesyłanie komunikatów na poziomie protokołów transportowych: HTTP, HTTPS, JMS, MTOM, SMTP
WYM.OPZ.STA.NFN.04 WSDL	Do opisu struktury i semantyki serwisu sieciowego (web service) musi zostać wykorzystany standard WSDL w wersji 1.X lub wyższej (http://www.w3.org/TR/wsdl20/)
WYM.OPZ.STA.NFN.05 UDDI	Do zbudowania rejestru usług będzie zastosowany standard UDDI w wersji 3.X lub wyższej (http://www.oasis-open.org/committees/uddi-spec/doc/tcpspecs.htm)
WYM.OPZ.STA.NFN.06 MTOM	Do optymalizacji transportu danych w oparciu o protokół SOAP i technologię usług sieciowych będzie zastosowany standard MTOM (www.w3.org/TR/soap12-mtom)
WYM.OPZ.STA.NFN.07 Standardy web service	System musi być zgodny z następującymi standardami w zakresie udostępnianych przez niego usług (web service): <ul style="list-style-type: none">- WS-I Basic Profile w wersji 1.0 lub wyższej,- WS-Policy w wersji 1.5 lub wyższej,





Wymaganie	Opis wymagania
	- WS-Security w wersji 1.0 lub wyższej, - WS-Addressing.
WYM.OPZ.STA.NFN.08 XML Schema	Do opisu struktur danych składowanych w formacie XML należy stosować standard XML Schema (http://www.w3.org/XML/Schema)
WYM.OPZ.STA.NFN.09 XACML	Podsystemy P1 muszą zapewnić wsparcie dla standardu polityki kontroli dostępu XACML w minimalnej wersji 1.0.
WYM.OPZ.STA.NFN.10 SAML	Podsystemy P1 muszą zapewnić wsparcie dla standardu zarządzania tożsamością SAML w minimalnej wersji 2.0.
WYM.OPZ.STA.NFN.11 Dane medyczne	Komunikacji między systemami, dotycząca danych medycznych, musi wykorzystywać standardy opracowane przez IHE.
WYM.OPZ.STA.NFN.12 Słowniki medyczne	Interoperacyjność oraz spójność danych słownikowych musi zostać zapewniona poprzez zastosowanie, co najmniej, ustrukturyzowanych klasyfikacji ICD-9, ICD-10, ICF, ICHI, ICNP, ICPC-2, ICECI, SNOMED, ATC w wersjach zatwierdzonych przez odpowiednie organizacje.
WYM.OPZ.STA.NFN.13 Opis świadczeń zdrowotnych i procedur medycznych	W celu zapewnienia interoperacyjności spójność opisu świadczeń zdrowotnych oraz opisu procedury medycznej muszą zostać zastosowane standardy: ICD-9 oraz ICD-10 w ich aktualnych wersjach.
WYM.OPZ.STA.NFN.14 Nieobrazowe dane medyczne	Komunikacja z platformą P1 w zakresie transferu nieobrazowych danych medycznych będzie realizowana w oparciu o standardy HL7 (w wersji 2.x oraz 3) oraz CEN 13606 (w aktualnej wersji).
WYM.OPZ.STA.NFN.15 Dane obrazowe	System P1 musi umożliwiać gromadzenie i przekazywanie informacji o miejscu przechowywania danych obrazowych (zgodnych ze standardem DICOM w jego aktualnej wersji).
WYM.OPZ.STA.NFN.16 Leki	Opis leków i środków farmaceutycznych będzie zrealizowany przy użyciu: ATC – klasyfikacji anatomiczno-terapeutyczno-chemicznej.
WYM.OPZ.STA.NFN.17 Badania laboratoryjne	Do przesyłu wyników badań laboratoryjnych zostanie wykorzystany standard LOINC w jego aktualnej wersji.
WYM.OPZ.STA.NFN.18 J2EE	Komunikacja musi odbywać się w oparciu o serwery aplikacyjne implementujące specyfikację J2EE, bądź inne otwarte technologie





Wymaganie	Opis wymagania
WYM.OPZ.STA.NFN.19 PKI	Wykorzystanie certyfikatów klucza publicznego musi uwzględniać: <ul style="list-style-type: none">• PKCS#1 - RSA Encryption Standard Version 1.5• PKCS#7 - Cryptographic Message Syntax Version 1.5• PKCS#10 – Certification Request Syntax Standard, version 1.7.• PKCS#11 - Cryptographic Token Interface Standard, version 2.01.• PKCS#12 - Personal Information Exchange Syntax Standard, version 1.0• RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Wydajność

Wymaganie	Opis wymagania
WYM.OPZ.WYD.NFN.01 Wolumetria	System będzie umożliwiał przesyłanie jednocześnie co najmniej: <ul style="list-style-type: none">- 1000 komunikatów/sek. o wielkości 1KB,- 500 komunikatów/sek. o wielkości 4KB,- 200 komunikatów/sek. o wielkości 16KB,- 20 komunikatów/sek. o wielkości 64KB.
WYM.OPZ.WYD.NFN.02 Optymalizacja funkcjonalności krytycznych	Dostawca zobowiązuje się w porozumieniu z pozostałymi dostawcami optymalizować wydajność wszystkich funkcjonalności z położeniem nacisku na funkcjonalności krytyczne wskazane przez zamawiającego.
WYM.OPZ.WYD.NFN.03 Optymalizacja w wyniku testów	Dostawca zobowiązuje się dokonać niezbędnej optymalizacji systemu w przypadku wykrycia i wskazania przez zamawiającego na etapie testów funkcjonalności realizowanej z niewystarczającą wydajnością.
WYM.OPZ.WYD.NFN.04 Optymalizacja algorytmów	Dostawca dołoży wszelkich starań, by zastosowane przez niego algorytmy były optymalne z punktu widzenia wydajności, zajętości pamięci, zajętości przestrzeni dyskowej oraz ilości informacji przesyłanej przez sieć.
WYM.OPZ.WYD.NFN.05 Jednoczesna praca wielu użytkowników	Podsystem będzie umożliwiał jednoczesną pracę co najmniej 500 000 użytkowników (aktywnych sesji). Portal Publikacyjny musi umożliwiać obsługę co najmniej 500 000 użytkowników.
WYM.OPZ.WYD.NFN.06 Wydajność	Przy pełnym obciążeniu zakładaną liczbą aktywnych sesji system musi zapewniać czas załadowania strony pomniejszony o czas oczekiwania na dane z bazy danych oraz opóźnienia na łączu klient-serwer o wartości nie większej niż 2 sekundy.

Wymagania dot. architektury

Wymaganie	Opis wymagania
-----------	----------------





Wymaganie	Opis wymagania
WYM.OPZ.ARC.NFN.01 Zmiany architektury	Architektura Systemu P1 musi zapewniać elastyczność i możliwość łatwego dostosowania w przypadku zmian w organizacji systemu ochrony zdrowia (w tym zmian w modelu finansowania świadczeń ze środków publicznych) oraz innych zmian (legislacyjnych, zmian w otoczeniu projektu, w systemach interesariuszy). Założenia te muszą zostać odzwierciedlone w rozbudowanych możliwościach konfiguracyjnych rozwiązania (np. możliwość dołączenia nowego płatnika).
WYM.OPZ.ARC.NFN.02 Zmiany zakresu danych	Zastosowane rozwiązania Systemu P1 muszą umożliwiać zmiany zakresu gromadzonych danych (zarówno osobowych, jak i medycznych).
WYM.OPZ.ARC.NFN.03 Organizacja informacji	System P1 musi pozwalać na taką organizację informacji, która pozwoli na ograniczenie redundancji danych oraz umożliwi wykorzystanie danych dostępnych w ramach procesów biznesowych, ograniczając powtarzanie ich wprowadzanie.
WYM.OPZ.ARC.NFN.04 SOA	Architektura Systemu P1 musi zostać zaprojektowana i zrealizowana z wykorzystaniem architektury zorientowanej na usługi (SOA). Podstawowym założeniem architektury P1 musi być udostępnienie funkcjonalności Systemu w postaci interoperacyjnych usług, które będą mogły być dalej wykorzystywane i grupowane w postaci procesów biznesowych.
WYM.OPZ.ARC.NFN.05 Udostępnianie usług	Wszystkie usługi Systemu P1 udostępniane na zewnątrz muszą być udostępniane za pomocą szyny usług (zewnętrznej).
WYM.OPZ.ARC.NFN.06 Komunikacja wewnątrz P1	Interfejsy pomiędzy systemami wchodzącymi w skład systemu P1 muszą być zrealizowane za pośrednictwem szyny usług (wewnętrznej). Odstępstwa od tej reguły są dopuszczalne jedynie ze względów wydajnościowych lub technologicznych. Każde takie odstępstwo musi zostać na etapie projektowania zaakceptowane przez Zamawiającego.
WYM.OPZ.ARC.NFN.07 Ograniczenie zmian w rejestrach źródłowych	Architektura Systemu P1 musi zostać zaprojektowana w sposób, który ograniczy do minimum konieczność zmian w rejestrach źródłowych.
WYM.OPZ.ARC.NFN.08 Buforowanie danych	Architektura Systemu P1 musi zapewnić możliwość buforowania danych do czasu zapisania i wysłania ich po powtórny nawiązaniu łączności w przypadku problemów z połączeniem.
WYM.OPZ.ARC.NFN.09 Technologia szyny usług	Technologia wybrana do realizacji szyny usług musi umożliwiać efektywne zarządzanie: <ul style="list-style-type: none">- wspieranymi procesami,- integralnością dostarczanych narzędzi,- repozytorium usług (w tym edycji zarejestrowanych usług i zarządzania nimi),- katalogiem usług standardowych.- monitorowaniem aktywności.
WYM.OPZ.ARC.NFN.10 Komunikacja z systemami	System P1, a w szczególności komponenty architektury aplikacji, zapewnią komunikację pomiędzy Systemem P1 a systemami zewnętrznymi. W szczególności architektura aplikacji uwzględni współpracę z projektem P2





Wymaganie	Opis wymagania
zewnętrznymi	„Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych”, w ramach którego wytworzone zostaną między innymi elementy podsystemu zarządzania zabezpieczeniami i prywatnością.
WYM.OPZ.ARC.NFN.11 Tryb synchroniczny i asynchroniczny	Architektura rozwiązania musi umożliwić komunikację z systemami zewnętrznymi w zakresie wykorzystania i udostępniania wystandaryzowanych usług udostępnianych przez szynę usług poprzez wymianę komunikatów w trybie: - synchronicznym (komunikaty wymieniane w czasie rzeczywistym) - asynchronicznym.
WYM.OPZ.ARC.NFN.12 API	System P1 musi udostępniać interfejs programistyczny aplikacji (API): - dla udostępniania i wymiany danych - do wszystkich funkcji systemu.
WYM.OPZ.ARC.NFN.13 Standard definicji procesów	Architektura platformy SIOZ musi umożliwiać realizację procesów zdefiniowanych w standardzie BPMN/BPEL/XPDL.
WYM.OPZ.ARC.NFN.14 SCA	Architektura systemu P1 musi być zgodna z modelem SCA.
WYM.OPZ.ARC.NFN.15 Ładowanie danych do hurtowni danych	Szyna usług ESB w zakresie ładowania danych do hurtowni danych powinna zapewnić możliwość zasilania hurtowni danych danymi pochodzącymi z przepływów danych realizowanych na potrzeby innych systemów dziedzinowych. W przypadku gdy jedynym odbiorcą danych z systemów transakcyjnych jest hurtownia danych - dotyczy to szczególnie danych ładowanych masowo - nie jest wymagane, aby szyna usług ESB pośredniczyła w transferze danych.
WYM.OPZ.ARC.NFN.16 Zarządzanie fizycznym rozłożeniem danych	Podsystem powinien posiadać mechanizmy zarządzające optymalnym rozłożeniem danych na dyskach, w celu uzyskania lepszej wydajności rozwiązania.
WYM.OPZ.ARC.NFN.17 Replikacja między ośrodkami przetwarzania	Architektura musi uwzględniać replikację danych pomiędzy COPD a ZOPD, tak aby dane które trafią na platformę zostały zapisane w dwóch ośrodkach przetwarzania danych. Replikacja danych pomiędzy ośrodkami przetwarzania danych odbywa się na poziomie aplikacji lub bazy danych. Realizowana jest ona w sposób asynchroniczny.

Ogólne wymagania funkcjonalne

Wymaganie	Opis wymagania
WYM.OPZ.O.FN.1 Backup i archiwizacja	System musi zapewnić mechanizmy dokonywania backupu i archiwizacji plików wykonywalnych, kodu, danych oraz logów.



**CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA**

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel.: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Wymaganie	Opis wymagania
WYM.OPZ.O.FN.1.1 Przesyłanie plików backupu	System musi udostępniać funkcjonalność przesyłania plików backupu do Systemu Administracji - Administracja
WYM.OPZ.O.FN.2 Monitorowanie podsystemów	Podsystemy muszą udostępniać usługi pozwalające na wstrzymanie lub wznowienie pracy danego podsystemu oraz zwracające raport o aktualnym stanie danego podsystemu. System administracji pozwala na ujednoliconą prezentację tych raportów.
WYM.OPZ.O.FN.3 Bezpieczne usuwanie danych	Podsystemy muszą zapewnić mechanizmy bezpiecznego usuwania danych wrażliwych.
WYM.OPZ.O.FN.4 Korelacja zdarzeń medycznych	Wszystkie zdarzenia medyczne muszą być skorelowane z usługobiorcą, którego dotyczą, usługodawcą oraz personelem medycznym, który brał udział w obsłudze usługobiorcy.
WYM.OPZ.O.FN.5 Obsługa słowników	Podsystemy Systemu P1 muszą mieć możliwość zasilania słownikami (z wykorzystaniem Szyny Usług) z podsystemu SOR-S. Musi być zapewnione wsparcie dla słowników wynikających z przepisów prawa, w tym minimum dla słowników zawartych w systemie SRK.



**INNOWACYJNA
GOSPODARKA**
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO



Projekt współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Innowacyjna Gospodarka „Dotacje na innowacje – inwestujemy w naszą przyszłość”