

Projekt Infrastruktury

Ministerstwo Sprawiedliwości

Spis treści

WYKAZ SKRÓTÓW	4
1. WSTĘP	7
2. WYMAGANIA	8
2.1 KLUCZOWE WYMAGANIA NIEFUNKCJONALNE MAJĄCE WPŁYW NA INFRASTRUKTURĘ	8
2.1.1 Użyteczność (ang. usability)	8
2.1.2 Niezawodność (ang. reliability)	8
2.1.2.1 NF2.1 Wysoka dostępność (ang. high availability)	8
2.1.2.2 NF2.3 Zapewnienie ciągłości działania (ang. business continuity)	9
2.1.3 Wydajność (ang. Performance)	9
2.1.3.1 NF3.1 Wymagania na wydajność (przepustowość i szybkość reakcji)	9
2.1.3.2 NF3.2 Wymagania na pasmo sieci WAN	10
2.1.3.3 NF3.3 Wymaganie na zasoby dyskowe	10
2.1.4 Zarządzalność (ang. Supportability)	10
2.1.4.1 NF4.3 Monitorowanie infrastruktury technicznej	10
2.1.4.2 NF4.4 Zarządzanie infrastrukturą techniczną	11
2.1.4.3 NF4.5a Monitorowanie Platformy Aplikacyjnej	11
2.1.5 Bezpieczeństwo (ang. Security)	11
2.1.5.1 NF5.1 Rozliczalność (ang. accountability)	11
2.1.5.2 NF5.2 Integralność (ang. integrity)	12
2.1.5.3 NF5.3 Poufność (ang. confidentiality)	12
2.2 WŁAŚCIWOŚCI SYSTEMU REALIZUJĄCE WYMAGANIA	12
2.2.1 Użyteczność (ang. usability)	12
2.2.2 Niezawodność (ang. reliability)	13
2.2.2.1 Architektura systemu wspierająca redundancję krytycznych komponentów	13
2.2.2.2 Klaster HA bazy danych	13
2.2.2.3 System Backup-u	13
2.2.2.4 Ośrodek Zapasowy	14
2.2.2.5 Niezależne Środowisko Testowe	14
2.2.3 Wydajność	15
2.2.3.1 Architektura trójwarstwowa systemu	15
2.2.3.2 Skalowalność systemu	16
2.2.3.3 Dystrybucja obciążenia na serwery aplikacyjne	18
2.2.3.4 Odpowiednie zasoby obliczeniowe	18
2.2.3.5 FT3.3 Odpowiednie zasoby dyskowe	19
2.2.3.6 FT3.3a WAN o odpowiednim paśmie	19
2.2.3.7 FT3.3b Użycie proxy http	21
2.2.3.8 FT3.4 SAN i macierze dyskowe.	21
2.2.4 Zarządzalność (ang. Supportability)	22
2.2.4.1 FT4.3 Lokalny w OZI System Monitorowania infrastruktury	22
2.2.4.2 FT4.4a Scentralizowany system monitorowania i zarządzania platformą aplikacyjną	22
2.2.4.3 FT4.4b Scentralizowane usługi sieciowe	22
2.2.4.4 FT4.5 Wirtualizacja platformy aplikacyjnej	23
2.2.5 Bezpieczeństwo (ang. Security)	23
2.2.5.1 FT5.1c Synchronizacja czasu w oparciu o protokół NTP	23

2.2.5.2	FT5.1 Uwierzytelnianie użytkowników w centralnym Active Directory	24
2.2.5.3	FT5.2b Kontrola ruchu sieciowego	24
2.2.5.4	FT5.3 Szyfrowanie komunikacji między użytkownikiem a OZI	25
2.2.5.5	FT5.7 Zarządzanie logami systemowymi	25
3.	MODEL KOMPONENTOWY SYSTEMU	27
3.1	MODEL KOMPONENTOWY NIEZALEŻNY OD TECHNOLOGII (PIM)	27
3.1.1	System SIWPM	29
3.1.1.1	Podsystem SIWPM	29
3.1.1.2	Podsystem Konfiguracja	31
3.1.1.3	Podsystem ESB	32
3.1.1.4	Podsystem Raporty	33
3.1.2	Podsystemy Infrastrukturalne	33
3.1.2.1	Podsystem Backup	33
3.1.2.2	Podsystem lokalnego monitorowania infrastruktury	33
3.1.2.3	Podsystem zarządzania logami systemowymi	33
3.1.3	Podsystemy Pomocnicze	34
3.1.3.1	Podsystem IDM	34
3.1.3.2	Podsystem eMail	35
3.1.3.3	Usługi sieciowe	35
3.2	MODEL ROZMIESZCZENIA	35
3.2.1	Decyzje projektowe	35
3.2.1.1	Przypisanie apelacji do OZI	37

Wykaz skrótów

Skrót	Termin angielski	Znaczenie
AD	Active Directory	(Serwis katalogowy Windows) Usługi katalogowe w środowisku MS Windows lub inne rozwiązanie równoważne
CC	Cell Console	Agent oprogramowania Data Protector zawierający interfejs GUI i CLI do komunikacji użytkownika z komórką
CIFS	Common Internet File System	Sieciowy system plików w środowisku MS Windows lub inne rozwiązanie równoważne
CLI	Command Line Interface	Zestaw poleceń do komunikacji z aplikacją poprzez interpreter poleceń lub w trybie wsadowym
CM	Cell Manager	Menadżer komórki Data Protector. Grupa procesów odpowiedzialnych za funkcje zarządzania pracą komórki
CMMDB	Centralized Media Management Database	Opcjonalny element komórki Data Protector występujący w konfiguracjach rozproszonych pod zarządem MoM (Manager of Managers), zawierający centralne informacje o wszystkich nośnikach kilku komórek
CSRV	Cell Server	Serwer komórki Data Protector. Pojęcie określa serwer, na którym pracuje menadżer komórki (CM)
D2D	Disk-to-Disk	Technologia backupu danych na urządzenia dyskowe
D2D2T	Disk-to-Disk-to-Tape	Technologia backupu danych na urządzenia dyskowe i w drugim etapie z urządzenia dyskowego na taśmy
DA	Disk Agent	Agent dyskowy Data Protector. Proces odpowiedzialny za odczyt/zapis danych dyskowych i komunikację z agentem urządzenia (MA)
DC	Domain Controller	Komputer z oprogramowaniem Windows Server, zarządzający kontami użytkowników, ich uwierzytelnianiem, dostępem do zasobów sieciowych (wpuszcza się rozwiązanie równoważne)
DHCP	Dynamic Host Configuration Protocol	Protokół przypisujący adresy IP do komputerów i urządzeń sieciowych
DNS	Domain Name System	Standard serwisu sieciowego rozwiązujący nazwy na adresy IP i odwrotnie
DP	Data Protector	Nazwa oprogramowania zarządzającego systemem backupów
DRC	Disaster Recovery Center	Zapasowy ośrodek przetwarzania danych
FC	Fibre Channel	Kanał komunikacyjny o nominalnej szybkości 1 Gb/s, 2Gb/s, 4Gb/s, 8Gb/s lub 16Gb/s
FE	Fast Ethernet	Kanał komunikacyjny o nominalnej szybkości

		100Mb/s
FS	File Server	Serwer plików
GE	Gigabit Ethernet	Kanał komunikacyjny o nominalnej szybkości 1Gb/s
GUI	Graphical User Interface	Interfejs graficzny służący do komunikacji z aplikacją
HA	High Availability	Wysoka dostępność. Termin dotyczy usług dostarczanych przez grona serwerów
HTTP	Hyper Text Transfer Protocol	Protokół komunikacyjny używany w Internecie
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer	Bezpieczny protokół używany w Internecie
IDB	Internal Database	Wewnętrzna baza danych aplikacji Data Protector
IDM	Identity Mgmt System	System zarządzania tożsamością.
IDS	Intrusion Detection System	System wykrywania włamań
IP	Internet Protocol	Podstawowy protokół transmisji danych, zapewniający przesyłanie informacji pomiędzy sieciami
IPSec	IP Security Protocol	Bezpieczna (szyfrowana) odmiana protokołu IP
IS	Installation Server	W komórce Data Protector serwer zawierający oprogramowanie instalacyjne DP i odpowiadający za jego dystrybucję
KVM	KVM switch – Keyboard Video Mouse	Urządzenie umożliwiające podłączenie do jednego zestawu klawiatury, myszy oraz monitora, dwóch lub większej liczby komputerów
LAN	Local Area Network	Komputerowa sieć transmisji lokalnej
LTO	Linear Tape Open	Otwarty standard liniowego zapisu na taśmach ½ calowych
LUN	Logical Unit	Wydzielona w procesie konfiguracji macierzy dyskowej zewnętrzna logiczna jednostka przestrzeni, widziana przez dołączony do macierzy serwer
MA	Media Agent	Agent urządzenia Data Protector. Proces odpowiedzialny za odczyt/zapis danych taśmowych i komunikację z agentem dyskowym (DA)
MoM	Manager of Managers	Menadżer menadżerów komórek Data Protector. Grupa procesów odpowiedzialnych za funkcje zarządzania pracą kilku komórek w architekturze rozproszonej
MPIO	Multipath I/O	Oprogramowanie zarządzające dostępem wielościeżkowym do dysków logicznych w macierzy dyskowej
NAS	Network Attached Storage	System dyskowy podłączony do sieci komputerowej udostępniający pliki poprzez protokoły CIFS i NFS
NFS	Network File System	Sieciowy system plików w środowisku UNIX
NTP	Network Time Protocol	Protokół sieciowy do synchronizacji czasu

PDU	Power Distribution Unit	System rozprowadzenia zasilania w szafach serwerowych
QoS	Quality of Service	Usługa sieciowa realizująca zapewnienie zadanego poziomu usług sieciowych
POZI	Podstawowy Ośrodek Zarządzania Informacją	
RPO	Recovery Point Objective	Zdefiniowany maksymalny okres czasu, z którego dane mogą być utracone w wyniku awarii
RTO	Recovery Time Objective	Zdefiniowany maksymalny czas uruchomienia aplikacji po awarii
SAN	Storage Area Network	Sieć do łączenia serwerów, pamięci masowych i bibliotek taśmowych
SLA	Service Level Agreement	Umowa gwarantująca określony poziom usług
SNMP	Simple Network Management Protocol	Protokół sieciowy do podstawowego monitorowania i zarządzania urządzeniami sieciowymi
SSH	Secure Shell	Protokół zdalnej sesji (szyfrowany) umożliwiający komunikację ze zdalnym komputerem
SSL	Secure Socket Layer	Protokół zapewniający prywatność i wiarygodność pomiędzy dwoma aplikacjami
UPS	Uninterruptible Power Supply	Zasilacz awaryjny, zasilacz bezprzerwowy, zasilacz UPS. Urządzenie lub system, którego funkcją jest nieprzerwane zasilanie innych urządzeń elektrycznych lub elektronicznych
VLAN	Virtual LAN	Sieć wirtualna w sieci LAN
VSS	Volume Shadow Copy Service	Serwis systemu Windows Server lub innego umożliwiający wykonywanie kopii migawkowych wolumenów dyskowych (lub rozwiązanie równoważne)
VTL	Virtual Tape Library	Urządzenie dyskowe z oprogramowaniem emulującym bibliotekę taśmową
WAN	Wide Area Network	Komputerowa sieć transmisji rozległej
ZDB	Zero Downtime Backup	Proces składowania danych wykonywany bez zatrzymywania backupowanej aplikacji
ZOZI	Zapasowy Ośrodek Zarządzania Informacją	

1. Wstęp

Niniejszy dokument zawiera Projekt Infrastruktury systemu SIWPM.

Odbiorcami dokumentu są:

- Architekci Systemu Zamawiającego oraz Wykonawcy
- Architekt Infrastruktury Zamawiającego

2. Wymagania

Wymagania zostały opracowane przede wszystkim na podstawie dokumentu Architektura Systemu.

2.1 Kluczowe wymagania niefunkcjonalne mające wpływ na infrastrukturę.

2.1.1 Użyteczność (ang. usability)

W tym obszarze nie zidentyfikowano wymagań, które miałyby wpływ na infrastrukturę.

2.1.2 Niezawodność (ang. reliability)

2.1.2.1 NF2.1 Wysoka dostępność (ang. high availability)

ID	Źródło wymagań	Rodzaj wymagania	Priorytet	
NF1.10		Niefunkcjonalne	Konieczne	
Nazwa	NF2.1 Wysoka Dostępność (ang. high availability)			
Treść	<p>Zastosowane rozwiązania technologiczne muszą gwarantować dla użytkowników wewnętrznych dostępność warstwy programowo-technicznej na poziomie 99,73% mierzonego w czasie tzw. business hours.</p> <p>SIWPM OZI jest dostępne 24/7 (za wyjątkiem planowanych przerw serwisowych, które nie powinny być dłuższe niż 3 godziny) w 99,73% czasu.</p>			
Komentarz	<p>Na podstawie notatki „Parametry niezawodnościowe dla Systemu Informatycznego Wspomagającego Procesy Merytoryczne (SIWPM)”.</p> <ol style="list-style-type: none">1) Najwyższy poziom dostępności systemu jest wymagany w dni robocze w godzinach urzędowania sądów t.j od 7.00 do 18.00.2) W dni wolne od pracy jest pożądane by system funkcjonował, jednak nie musi być objęty równie wysokimi wymaganiami niezawodnościowymi3) Środowiska testowe, developerskie i szkoleniowe nie muszą być objęte rozwiązaniem niezawodnościowym4) Maksymalny czas niedostępności systemu (RTO) ustalono na 24 godziny w dni robocze. Oznacza to, iż<ol style="list-style-type: none">a) Sumaryczna niedostępność systemu nie powinna przekroczyć 24 godzin w ciągu dwóch miesięcy.b) Planowane przerwy technologiczne (w tym okna serwisowe) powinny			

	<p>być wyznaczane poza godzinami (i dniami) urzędowania sądów.</p> <p>c) . Użytkownicy powinni być informowani o planowanych przerwach (w tym okienkach serwisowych) w dostępności systemu również poza godzinami urzędowania sądów.</p> <p>1. Ustalono, iż utrata danych nie może przekraczać 4 godzin wstecz od momentu awarii czyli parametr RPO dla systemu SIWPM wynosi 4 godziny.</p>
--	--

2.1.2.2 NF2.3 Zapewnienie ciągłości działania (ang. business continuity)

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF2.3		Niefunkcjonalne	Konieczne	
Nazwa	NF2.3 Zapewnienie ciągłości działania (ang. business continuity)			
Treść	Zapewnienie ciągłości działania systemu SIWPM w sytuacji awaryjnego lub planowanego wyłączenia OZI.			
Komentarz	Architektura Systemu musi być zaprojektowana z uwzględnieniem zarówno ośrodka podstawowego jak i zapasowego. Ośrodki podstawowy i zapasowy są geograficznie odseparowane. Dla zapewnienia ciągłości działania Systemu w razie awarii ośrodka podstawowego pracę musi przejąć ośrodek zapasowy.			

2.1.3 Wydajność (ang. Performance)

2.1.3.1 NF3.1 Wymagania na wydajność (przepustowość i szybkość reakcji)

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF3.1		Niefunkcjonalne	Konieczne	
Nazwa	NF3.1 Wymagania na wydajność (przepustowość i szybkość reakcji)			
Treść	<p>Dostarczone przez Wykonawcę moduły wewnętrzne Systemu muszą działać prawidłowo przy jednoczesnym zalogowaniu 6000 użytkowników per OZI.</p> <p>95% żądań zostanie zrealizowanych w czasie krótszym niż 5s. W przypadku raportowania, na etapie analizy określone będą maksymalne czasy przetwarzania raportów.</p>			

Komentarz	
-----------	--

2.1.3.2 NF3.2 Wymagania na pasmo sieci WAN

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF3.2	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF3.2 Wymagania na pasmo sieci WAN			
Treść	<p>Estymacja wymagań na pasmo sieci WAN:</p> <ul style="list-style-type: none"> • Pomiędzy sądami a OZI • Pomiędzy różnymi OZI (zakłada się replikację danych alfanumerycznych z Ośrodków Regionalnych do Ośrodka Centralnego) • Pomiędzy OZI a DRC (Ośrodek Zapasowy) w przypadku replikacji danych 			
Komentarz				

2.1.3.3 NF3.3 Wymaganie na zasoby dyskowe

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF3.3	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF3.3 Wymaganie na zasoby dyskowe			
Treść	<ul style="list-style-type: none"> • Środowisko Produkcyjne powinno zawierać dane wszystkich nie zakończonych prawomocnie spraw, spraw co do których nie złożono wniosku kasacyjnego oraz spraw zakończonych w bieżącym roku.. • Środowisko Archiwalne powinno zawierać dane spraw do czasu ich brakowania w rozumieniu przepisów o archiwizacji 			
Komentarz				

2.1.4 Zarządzalność (ang. Supportability)

2.1.4.1 NF4.3 Monitorowanie infrastruktury technicznej

ID	Źródło	Rodzaj wymagania	Priorytet	
----	--------	------------------	-----------	--

	wymagania			
NF4.3	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF4.3 Monitorowanie i zarządzanie infrastrukturą techniczną			
Treść	System musi być wyposażony w mechanizm centralnego i lokalnego (w danym OZI) monitorowania infrastruktury technicznej.			
Komentarz				

2.1.4.2 NF4.4 Zarządzanie infrastrukturą techniczną

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF4.4	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF4.4 Zarządzanie infrastrukturą techniczną			
Treść	System musi być wyposażony w mechanizm centralnego zarządzania infrastrukturą techniczną.			
Komentarz				

2.1.4.3 NF4.5a Monitorowanie Platformy Aplikacyjnej

ID	Źródło wymagania	Rodzaj wymagania	Priorytet	
NF4.5	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF4.5 Monitorowanie i zarządzanie Platformą Aplikacyjną			
Treść	System musi być wyposażony w mechanizm centralnego zarządzania Platformą Aplikacyjną (systemy operacyjne, bazy danych, serwery aplikacyjne, systemy raportowe, itd.,)			
Komentarz				

2.1.5 Bezpieczeństwo (ang. Security)

2.1.5.1 NF5.1 Rozliczalność (ang. accountability)

ID	Źródło	Rodzaj wymagania	Priorytet	
----	--------	------------------	-----------	--

	wymagania			
NF5.1	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF5.1 Rozliczalność (ang. accountability)			
Treść	System musi być w stanie jednoznacznie przypisać każdą operację wykonaną w systemie użytkownikowi, który ją wykonał..			
Komentarz				

2.1.5.2 NF5.2 Integralność (ang. integrity)

ID	Źródło wymagań	Rodzaj wymagania	Priorytet	
NF5.2	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	NF5.2 Integralność (ang. integrity)			
Treść	System realizuje swoją zamierzoną funkcję w nienaruszalny sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.			
Komentarz				

2.1.5.3 NF5.3 Poufność (ang. confidentiality)

ID	Źródło wymagań	Rodzaj wymagania	Priorytet	
NF5.3	Ustalenia	Niefunkcjonalne	Pożądane	
Nazwa	NF5.3 Poufność (ang. confidentiality)			
Treść	Dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom.			
Komentarz				

2.2 Właściwości systemu realizujące wymagania

2.2.1 Użyteczność (ang. usability)

W tym obszarze nie zidentyfikowano właściwości, które miałyby wpływ na infrastrukturę.

2.2.2 Niezawodność (ang. reliability)

2.2.2.1 Architektura systemu wspierająca redundancję krytycznych komponentów

ID	Źródło	Rodzaj właściwości	Priorytet	
FT2.1	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT2.1 Architektura systemu wspierająca redundancję krytycznych komponentów			
Treść	Najważniejszą właściwością systemu adresującą wymaganie wysokiej dostępności jest redundancja krytycznych dla działania systemu komponentów składających się na system na wszystkich poziomach zaczynając od redundancji na poziomie infrastruktury lokalizacyjnej, sprzętowej a kończąc na redundancji komponentów programowych. Dzięki redundancji awaria pojedynczych krytycznych dla działania systemu komponentów nie powoduje przerwy w działaniu systemu.			
Realizacja wymagań	NF2.1 Wysoka Dostępność (ang. high availability)			
Komentarz				

2.2.2.2 Klaster HA bazy danych

ID	Źródło	Rodzaj właściwości	Priorytet	
FT2.1b	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	Klaster HA bazy danych			
Treść	Baza danych zainstalowana w trybie klastra HA.			
Realizacja wymagań	NF2.1 Wysoka Dostępność (ang. high availability)			
Komentarz				

2.2.2.3 System Backup-u

ID	Źródło	Rodzaj właściwości	Priorytet	
----	--------	--------------------	-----------	--

FT2.2	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	System Backup-u			
Treść	Zastosowanie aplikacji Data Protector jako systemu backup-u i odtwarzania danych.			
Realizacja wymagań	NF2.2 Odtwarzalność (ang. Recoverability)			

2.2.2.4 Ośrodek Zapasowy

ID	Źródło	Rodzaj właściwości	Priorytet	
FT2.3	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	Ośrodek Zapasowy			
Treść	Powstanie jeden zintegrowany DRC (Ośrodek Zapasowy) dla wszystkich OZI			
Realizacja wymagań	NF2.3 Zapewnienie ciągłości działania (ang. business continuity)			
Komentarz				

2.2.2.5 Niezależne Środowisko Testowe

ID	Źródło	Rodzaj właściwości	Priorytet	
FT2.6	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	Środowisko Testowe			
Treść	Niezależne od produkcyjnego Środowisko Testowe.			
Realizacja wymagań	NF2.1 Wysoka dostępność systemu			
Komentarz	Niezależne od produkcyjnego Środowisko Testowe powinno mieć topologię podobną do Środowiska Produkcyjnego.			

2.2.3 Wydajność

2.2.3.1 Architektura trójwarstwowa systemu

ID	Źródło	Rodzaj właściwości	Priorytet	
FT3.1a	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	Architektura trójwarstwowa			
Treść	<div><p>cmp Architektura trójwarstwowa</p><pre>graph TD; subgraph WP [Warstwa Prezentacji]; AU[Aplikacja Użytkownika]; end; subgraph WA [Warstwa Aplikacji]; WPo[Warstwa Pośrednia]; end; subgraph WD [Warstwa Danych]; BD[Baza Danych]; end; AU --> WPo; WPo --> BD;</pre><p><i>Rysunek 1 - Trójwarstwowa architektura</i></p><p>Warstwa Prezentacji jest odpowiedzialna za następującą funkcjonalność:</p></div>			

	<ul style="list-style-type: none"> • Prezentacja danych • Wstępna walidacja wprowadzanych danych • Wstępna kontrola uprawnień (ukrywanie funkcji do których użytkownik nie ma uprawnień) • Komunikacja z warstwą aplikacji. <p>Warstwa aplikacji jest odpowiedzialna za następującą funkcjonalność:</p> <ul style="list-style-type: none"> • Uwierzytelnienie i autoryzacja operacji użytkowników • Zarejestrowanie śladu rewizyjnego • Pośrednictwo w dostępie do warstwy persystencji (między innymi multipleksacja połączeń do bazy danych – obsługa puli połączeń) • Realizacja pozostałej logiki biznesowej <p>Warstwa persystencji odpowiedzialna jest za:</p> <ul style="list-style-type: none"> • zarządzanie danymi, • ich trwałość, • integralność, • i zwracanie odpowiedzi na zapytania.
Realizacja wymagań	NF3.1 Wymagania na wydajność
Komentarz	

2.2.3.2 Skalowalność systemu

ID	Źródło	Rodzaj właściwości	Priorytet	
FT3.1	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT3.1 Skalowalność systemu			
Treść	Najważniejszą właściwością systemu adresująca wymagania wysokiej wydajności jest jego skalowalność.			
Realizacja	NF3.1 Wymagania na wydajność			

wymagań	
Komentarz	<p>W systemie zbudowanym w architekturze trójwarstwowej, warstwa prezentacji i aplikacji skaluje się horyzontalnie, (czyli wzrasta jej przepustowość przez dodanie nowych węzłów, które ją przetwarzają).</p> <p>Warstwa pośrednia jest obsługiwana przez serwery aplikacyjne w OZI i może w sposób niemal nieograniczony być skalowana horyzontalnie (przez dodawanie nowych serwerów aplikacyjnych).</p> <p>Warstwa persystencji skaluje się tylko wertykalnie, skalowalność można uzyskać poprzez podział systemu tak, że każda apelacja jest obsługiwana przez niezależny system (w tym w szczególności przez niezależną bazę danych), można bazę danych obsługującą daną apelację przenieść na inny serwer. Sposób rozmieszczenia węzłów klastrów niezawodnościowych baz danych na krzyż ilustruje poniższy model.</p> <div data-bbox="346 786 1396 1568"> <p>deployment Krzyżowe rozmieszczenie węzłów klastrów niezawodnościowych bazy danych</p> <pre> graph LR subgraph Node1 [Node1] direction TB A1[«executionEnvironment» Apelacja 1 - Aktywny węzeł RDBMS] A2[«executionEnvironment» Apelacja 2 - Pasywny węzeł RDBMS] end subgraph Node2 [Node2] direction TB A1P[«executionEnvironment» Apelacja1 - Pasywny Serwer RDBMS] A2A[«executionEnvironment» Apelacja 2 - Aktywny węzeł RDBMS] end A1 --- HA1[Klaster HA] --- A1P A2 --- HA2[Klaster HA] --- A2A </pre> </div> <p>Rysunek 2- Krzyżowe rozmieszczenie węzłów klastrów niezawodnościowych bazy danych</p>

2.2.3.3 Dystrybucja obciążenia na serwery aplikacyjne

ID	Źródło	Rodzaj właściwości	Priorytet	
FT3.1b	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	Dystrybucja obciążenia na serwery aplikacyjne			
Treść	Do dystrybucji obciążenia na serwery aplikacyjne użyty zostanie sprzętowy Load Balancer.			
Realizacja wymagań	NF3.1 Wymagania na wydajność			
Komentarz	Należy skonfigurować tzw. Przyklejanie sesji ssl (na wypadek gdyby użyty mail być protokół https).			

2.2.3.4 Odpowiednie zasoby obliczeniowe

ID	Źródło	Rodzaj wymagania	Priorytet	
FT3.2	Ustalenia	Niefunkcjonalne	Konieczne	
Nazwa	Odpowiednie zasoby obliczeniowe			
Realizacja wymagań	NF3.1 Wymagania na zasoby obliczeniowe			
Treść	Najwłaściwszym sposobem przybliżenia tych wymagań jest wykonanie testów obciążeniowych na pilocie technicznym (pilot obsługujący uproszczoną, wąską funkcjonalność w docelowej architekturze i technologii) na infrastrukturze podobnej do docelowej. Tylko empiryczne pomiary są w stanie dać miarodajne liczby wskazujące jak wiele symulowanych równoległych użytkowników i z jaką responsywnością, dany system na danej infrastrukturze jest w stanie obsłużyć.			
Komentarz				

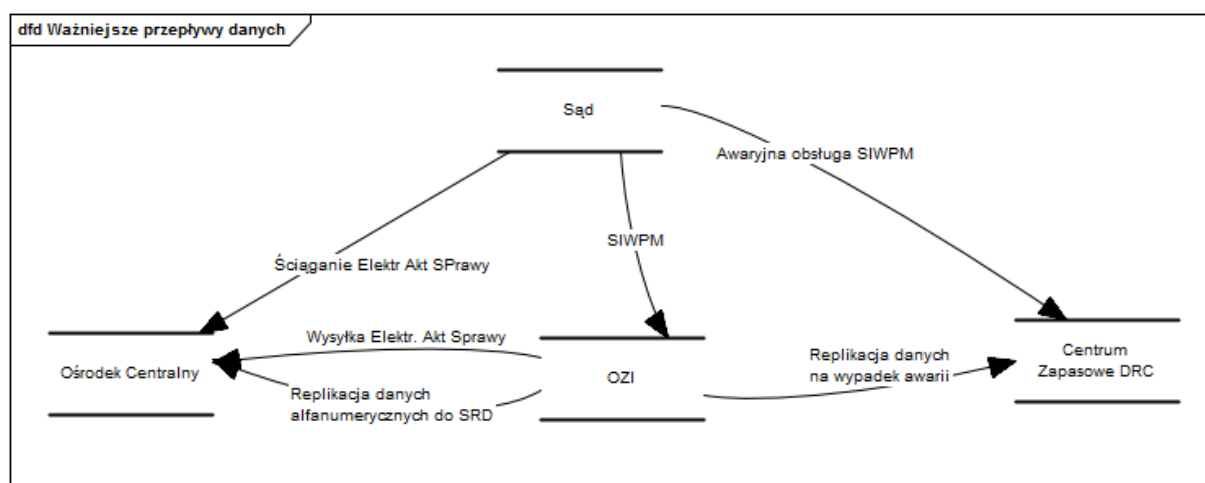
2.2.3.5 FT3.3 Odpowiednie zasoby dyskowe

Sumaryczna ilość danych Prod	9,8	TB
Ilość OZI	4	
Ilość danych Prod w OZI	2,4	TB
Ile lat przechowywać dane w Archiwum	15	
Sumaryczna ilość danych Archiwum	48,9	TB
Wymagana przestrzeń dla Archiwum OZI	12,2	TB

Szczegółowy opis analizy wolumetrycznej jest w załączniku SIWPM - Projekt Infrastruktury - Zał.1 - Analiza Wolumetryczna - v1.6

2.2.3.6 FT3.3a WAN o odpowiednim paśmie

Szczegółowy opis analizy wolumetrycznej jest w załączniku SIWPM - Projekt Infrastruktury - Zał.1 - Analiza Wolumetryczna - v1.6.



Rysunek 3 - Ważniejsze przepływy danych

Sąd – Ośrodek Centralny	Ściąganie w nocy z serwera pocztowego Elektronicznych Akt Sprawy, które pozwolą przeprowadzić rozprawę w przypadku niedostępności systemu.
Sąd – OZI	Wymiana danych w trakcie standardowej pracy systemu SIWPM

Sąd DRC	Wymiana danych w trakcie awaryjnej pracy systemu SIWPM
OZI – Ośrodek Centralny	Nocna wysyłka Elektronicznych Akt Sprawy na serwer pocztowy. Ciągła replikacja danych alfanumerycznych z regionalnych baz SIWPM do SRD (Skonsolidowanej Repliki Danych).
OZI – DRC	Replikacja danych na wypadek awarii

2.2.3.6.1 Sąd

Szacunkowe zapotrzebowanie w szczycie na pasmo komunikacyjne na użytkownika (pracownika):

- Dane ściągane (Download) – 30Kb/s/użytkownika
- Dane wysyłane (Upload) – 3Kb/s/użytkownika

2.2.3.6.2 OZI

Szacunkowa ilość użytkowników obsługiwana przez OZI	10 000	
Szacunkowe wymaganie na pasmo komunikacyjne na ściągnięcie danych do OZI	30	Mb/s
Szacunkowe wymaganie na pasmo komunikacyjne na wysyłanie danych z OZI	300	Mb/s

2.2.3.6.3 Ośrodek Centralny

Wymagane pasmo ściągnięcia danych alfanumerycznych do Ośrodka Centralnego	1	Mb/s
---	---	------

2.2.3.6.4 Ośrodek Zapasowy

Pasmo na replikację danych z OZI do DRC	4	Mb/s
---	---	------

Widać, że szacunkowe pasmo wymagane do replikacji jest do zaniedbania wobec wymagań, jakie stawia komunikacja z sądami. Ponieważ Ośrodek Zapasowy zastępuje awaryjnie OZI musi posiadać pasmo komunikacyjne takie jak OZI.

2.2.3.7 FT3.3b Użycie proxy http

ID	Źródło	Rodzaj właściwości	Priorytet	
FT3.3	Ustalenia	Niefunkcjonalne	Pożądana	
Nazwa	FT3.3b Użycie proxy http			
Treść	Użycie serwera proxy http w sądach pozwoli zoptymalizować ruch w sieci WAN. W szczególności ma to znaczenie w przypadku dystrybucji nowych wersji aplikacji użytkownika (która może być duża i bez proxy http może się długo ładować) oraz często odczytywanych dokumentów. Warunkiem efektywnego użycia http proxy jest użycie nieszyfrowanego protokołu http w warstwie aplikacyjnej. Aby jednak zapewnić poufność komunikacji przez WAN pomiędzy sądem a OZI należy tę komunikację szyfrować między routerami w sądzie i OZI za pomocą protokołu IPSec.			
Realizacja wymagań	NF3.2 Wymagania na pasmo sieci WAN			
Komentarz	SIWPM nie stawia tutaj żadnych specjalnych wymagań (proxy http w trybie forward). Może to być: SQUID, Apache z mod_proxy, IIS skonfigurowany jako proxy, w końcu także Microsoft Forefront Threat Management Gateway (Forefront TMG), dawniej znany jako Microsoft Internet Security and Acceleration Server (ISA Server).			

2.2.3.8 FT3.4 SAN i macierze dyskowe.

ID	Źródło	Rodzaj właściwości	Priorytet	
FT3.4	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT3.4 SAN i macierze dyskowe			
Realizacja wymagań	NF3.3 Wymaganie na zasoby dyskowe			
Treść	<p>System składowania danych oparty o:</p> <ul style="list-style-type: none">• Wysokowydajne macierze dyskowe DAS (Direct-attached storage) dla danych produkcyjnych• Sieciowe pamięci masowe NAS (Network-attached storage) o mniejszej wydajności, ale o większej pojemności dla danych archiwalnych			

Komentarz	
-----------	--

2.2.4 Zarządzalność (ang. Supportability)

2.2.4.1 FT4.3 Lokalny w OZI System Monitorowania infrastruktury

ID	Źródło	Rodzaj właściwości	Priorytet	
FT4.3	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT 4.3 Lokalny w OZI System Monitorowania infrastruktury			
Treść	Zostanie użyty w każdym OZI System Monitorowania infrastruktury			
Realizacja wymagań	NF4.3 Monitorowanie i zarządzanie infrastrukturą techniczną			
Komentarz				

2.2.4.2 FT4.4a Scentralizowany system monitorowania i zarządzania platformą aplikacyjną

ID	Źródło	Rodzaj właściwości	Priorytet	
FT4.4a	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT4.4a System Monitorowania i zarządzania platform aplikacyjną			
Treść	Do centralnego zarządzania i monitorowania platformy aplikacyjnej (system operacyjny, bazy danych, serwery aplikacyjne) użyty zostanie.....			
Realizacja wymagań	NF4.4 Monitorowanie i zarządzanie Platformą Aplikacyjną			
Komentarz	Należy zapewnić dostęp systemu do maszyn wirtualnych w każdym OZI.			

2.2.4.3 FT4.4b Scentralizowane usługi sieciowe

ID	Źródło	Rodzaj właściwości	Priorytet	
FT4.4a	Ustalenia	Niefunkcjonalne	Konieczna	

Nazwa	FT4.4b Scentralizowane usługi sieciowe <ul style="list-style-type: none"> • NTP • DNS • DHCP
Treść	
Realizacja wymagań	NF4.3 Monitorowanie i zarządzanie infrastrukturą techniczną
Komentarz	Należy zapewnić dostęp maszyn wirtualnych w każdym OZI do w/w usług sieciowych.

2.2.4.4 FT4.5 Wirtualizacja platformy aplikacyjnej

ID	Źródło	Rodzaj właściwości	Priorytet	
FT4.5	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT4.5 Wirtualizacja platformy aplikacyjnej			
Treść	Platforma aplikacyjna zostanie zwirtualizowana			
Realizacja wymagań	NF4.4 Zarządzanie Platformą Aplikacyjną			
Komentarz				

2.2.5 Bezpieczeństwo (ang. Security)

2.2.5.1 FT5.1c Synchronizacja czasu w oparciu o protokół NTP

ID	Źródło	Rodzaj właściwości	Priorytet	
FT5.1c	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT5.1c Synchronizacja czasu w oparciu o protokół NTP			
Treść	Czasy systemowe serwerów będą synchronizowane za pomocą protokołu NTP z ustalonym źródłem czasu..			
Realizacja	NF5.1 Rozliczalność (ang. accountability)			

wymagań	
Komentarz	

2.2.5.2 FT5.1 Uwierzytelnianie użytkowników w centralnym Active Directory

ID	Źródło	Rodzaj właściwości	Priorytet	
FT5.1	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT5.1 Uwierzytelnianie użytkowników w centralnym Active Directory			
Treść	Użytkownicy SIWPM będą się uwierzytelniać w oparciu o centralny zewnętrzny system IDM (ang Identity Mgmt) MS Active Directory			
Realizacja wymagań	NF5.2 Integralność (ang. integrity) NF5.1 Rozliczalność (ang. accountability)			
Komentarz	W MS AD rejestrowane będą dane związane z uwierzytelnieniem takie jak nazwa konta, hasło, ewentualnie certyfikat X509v3. Konto następnie będzie musiało być zarejestrowane w SIWPM i tam przypisane mu będą role definiujące uprawnienia związane z kontem. Możliwości definiowania polityki haseł będą takie jakie oferuje produkt MS AD. SIWPM wymusi (i umożliwi) okresową zmianę hasła użytkownikowi.			

2.2.5.3 FT5.2b Kontrola ruchu sieciowego

ID	Źródło	Rodzaj właściwości	Priorytet	
FT5.2b	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT5.2b Kontrola ruchu sieciowego			
Treść	Zastosowany zostanie system wykrywania i zapobiegania włamaniom (ang. Intrusion Detection System, Intrusion Prevention System) Ruch sieciowy będzie kontrolowany za pomocą firewall-i na wejściu do OZI i przy dostępie do baz danych.			

Realizacja wymagań	NF5.2 Integralność (ang. integrity)
Komentarz	

2.2.5.4 FT5.3 Szyfrowanie komunikacji między użytkownikiem a OZI

ID	Źródło	Rodzaj właściwości	Priorytet	
FT5.3	Ustalenia	Niefunkcjonalne	Konieczna	
Nazwa	FT5.3 Szyfrowanie komunikacji między użytkownikiem a OZI			
Treść	Komunikacja między sądem a OZI będzie szyfrowana w warstwie aplikacyjnej za pomocą protokołu https (oprócz szyfrowania komunikacji między ruterami w sądzie i w OZI). Tylko aplikacja użytkownika będzie dostępna po http (aby wykorzystać http proxy i wyeliminować jej wielokrotne ściągnięcie przez WAN z OZI do sądu. Aby zapewnić jej integralność należy Aplikację Użytkownika podpisywać. Aby aplikacja kliencka weryfikowała ten podpis należy zainstalować na stacji użytkownika certyfikat			
Realizacja wymagań	NF5.3 Poufność			
Komentarz	Szyfrowanie komunikacji w warstwie aplikacyjnej powoduje, że wyeliminowana zostaje optymalizacja wykorzystania pasma sieci WAN przy pomocy serwera http proxy. Ponieważ aplikacja pracuje w sieci wewnętrznej można rozważyć wyłączenie szyfrowania komunikacji w warstwie aplikacyjnej (ssl). W takiej sytuacji http proxy pracujący w trybie forward optymalizuje komunikację między sądem a OZI a w szczególności wielokrotne ściągnięcie tych samych dokumentów. i pozostawić vpn między routerami w sądach i OZI (wtedy http proxy może zostać w pełni wykorzystane do optymalizacji ruchu sieciowego).			

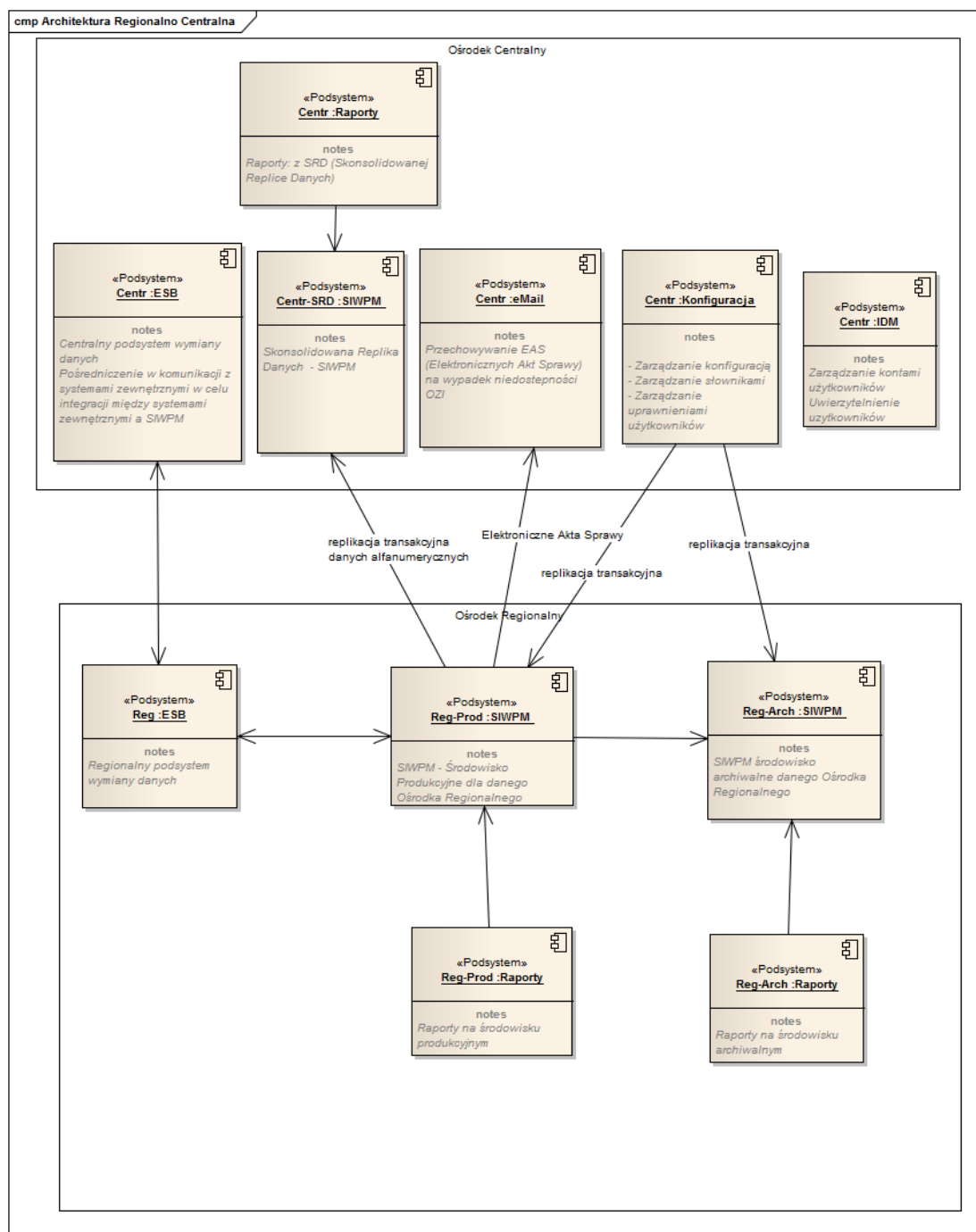
2.2.5.5 FT5.7 Zarządzanie logami systemowymi

ID	Źródło	Rodzaj właściwości	Priorytet	
FT5.7	Ustalenia	Niefunkcjonalne	Pożądana	
Nazwa	FT5.7 Zarządzanie logami systemowymi			

Treść	Jest to realizacja wymagania kontraktowego. Wykonawca musi dostarczyć mechanizm(y) uniemożliwiające nieuprawnionym użytkownikom edycję i usuwanie plików zawierających logi zdarzeń systemowych oraz chroniące przed możliwością ich przepełnienia.
Realizacja wymagań	NF5.2 Integralność (ang. integrity)
Komentarz	

3. Model Komponentowy systemu

3.1 Model komponentowy niezależny od technologii (PIM)



Rysunek 4 – Architektura Regionalno-Centralna

System SIWPM zostanie zbudowany w wariacie Regionalno-Centralnym.

Ośrodek Regionalny to oprogramowania obsługujący jedną lub wiele apelacji. Nie należy go mylić z infrastrukturą OZI, na której jest rozlokowany.

Ośrodek Centralny to oprogramowanie obsługujące funkcjonalność centralną systemu.

W Ośrodku Regionalnym odbywa się:

- przetwarzanie danych produkcyjnych pojedynczej apelacji,
- przechowywanie danych archiwalnych pojedynczej apelacji
- lokalne raportowanie pojedynczej apelacji

W Ośrodku Centralnym odbywa się:

- zarządzanie konfiguracją,
która następnie jest replikowana do Ośrodków Regionalnych
- zarządzanie użytkownikami,
- wymiana danych między ośrodkami regionalnymi i integracja z systemami zewnętrznymi
- i raportowanie na danych skonsolidowanych,
które powstają przez replikację danych z centrów regionalnych.

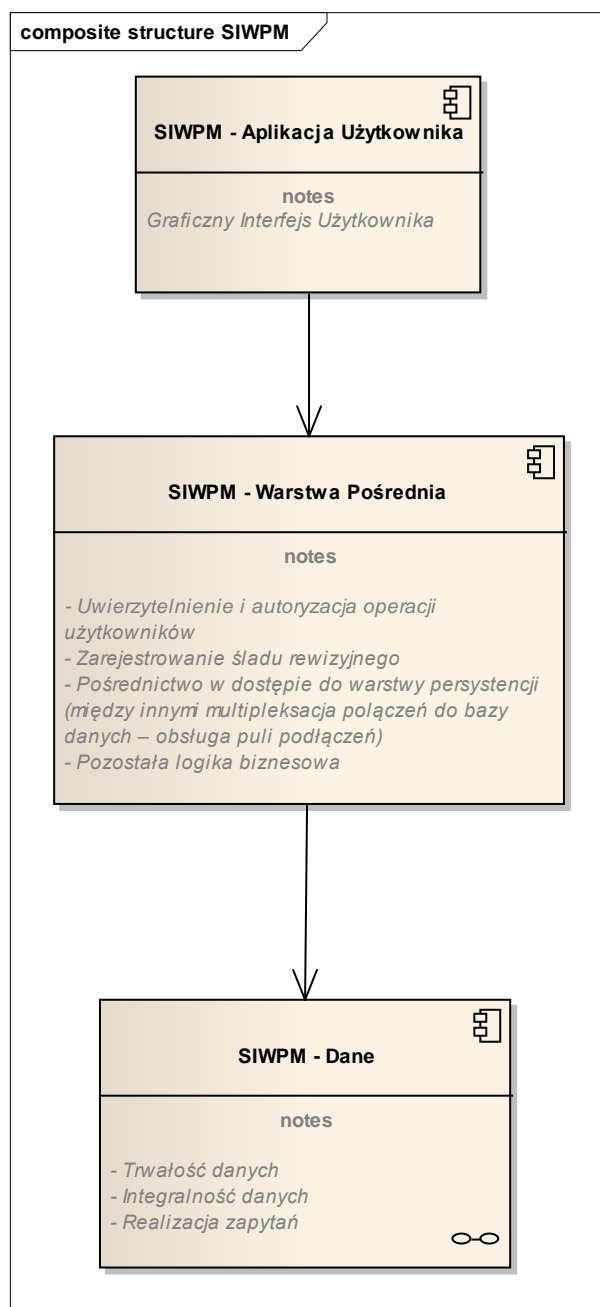
W Ośrodkach Regionalnych oprócz systemów pomocniczych (np. Reg:ESB) każda apelacja będzie obsługiwana przez własne dedykowane podsystemy:

- Produkcyjne
 - Reg-Prod:SIWPM
Środowisko Produkcyjne dla danego Ośrodka Regionalnego
 - Reg-Prod:Raporty
Raporty na środowisku produkcyjnym
- Archiwalne:
 - Reg-Arch:SIWPM
SIWPM środowisko archiwalne danego Ośrodka Regionalnego
 - Reg-Arch:Raporty
Raporty na środowisku archiwalnym

Aktualnie Ośrodek Regionalny obsługuje jedną apelację, aby można było ją przenieść do innego OZI. Jednakże Oprogramowanie SIWPM musi być gotowe na to, aby w przyszłości Ośrodki Regionalne mogły obsługiwać wiele apelacji (docelowo, aby można było system scentralizować).

3.1.1 System SIWPM

3.1.1.1 Podsystem SIWPM



Rysunek 5 – SIWPM

Podstawowy podsystem odpowiedzialny za przetwarzanie danych i dokumentów.

Podsystem zbudowany jest w architekturze trójwarstwowej i składa się z:

- Aplikacji Użytkownika, która dostarcza graficzny interfejs użytkownika.
- Warstwy Pośredniej, która jest odpowiedzialna za:

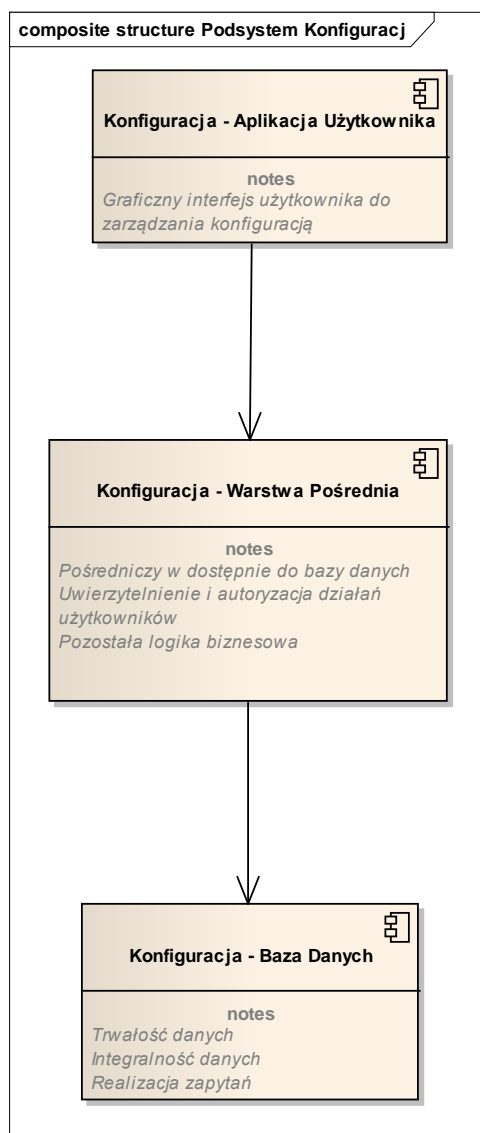
- Uwierzytelnienie i autoryzację operacji użytkowników
- Zarejestrowanie śladu rewizyjnego
- Pośrednictwo w dostępie do warstwy persystencji (między innymi multipleksacja połączeń do bazy danych – obsługa puli połączeń)
- Realizację pozostałej logiki biznesowej
- Warstwy persystencji która składa się osobnych baz danych:
 - SIWPM – Dane Alfanymericzne - baza danych alfanumerycznych
Opcjonalnie (gdyby wystąpiły problemy z wydajnością) można replikować transakcyjnie kopię danych alfanumerycznych do osobnej bazy danych dla celów raportowych
 - SIWPM – Dokumenty - Baza dokumentów (do rozważenia zastosowanie narzędzia ECM)

W przypadku problemów z wydajnością należy rozważyć koncepcję, w której odczyty lub raporty w aplikacji realizowane byłyby na innej bazie danych (np. replice) niż baza transakcyjna do zapisu. Częścią podsystemu będzie **Ślad Rewizyjny**, który jest odpowiedzialny za gromadzenie, przechowywanie i przeglądanie rejestru czynności wykonywanych przez użytkowników lub przez system (np. w wyniku integracji). Powinny być rejestrowane wszystkie zmiany (nawet te dokonane przez system) tak, aby możliwe było ich prześledzenie na wybranym rekordzie danej encji.

Podsystem SIWPM występuje w następujących postaciach:

- SRD:SIWPM – **tylko do odczytu Skonsolidowana Replika Danych (SRD) alfanumerycznych** ze wszystkich Ośrodków Regionalnych. SRD:SIWPM tworzona będzie za pomocą replikacji transakcyjnej ze wszystkich Ośrodków Regionalnych. SRD:SIWPM umożliwi:
 - Raportowanie skonsolidowane
 - Kwerendę skonsolidowanych danych alfanumerycznych
- Reg-Prod: SIWPM – podstawowy podsystem produkcyjny w danym Ośrodku Regionalnym.
- Reg-Arch: SIWPM – podsystem dla danych archiwalnych w danym Ośrodku Regionalnym.

3.1.1.2 Podsystem Konfiguracja



Rysunek 6 – Podsystem Konfiguracja – model komponentowy

Podsystem odpowiedzialny za:

- Zarządzanie konfiguracją SIWPM.
- Zarządzanie słownikami.
- Zarządzanie uprawnieniami użytkowników (ale nie za autoryzację, ta jest wykonywana w systemach docelowych np. w SIWPM).

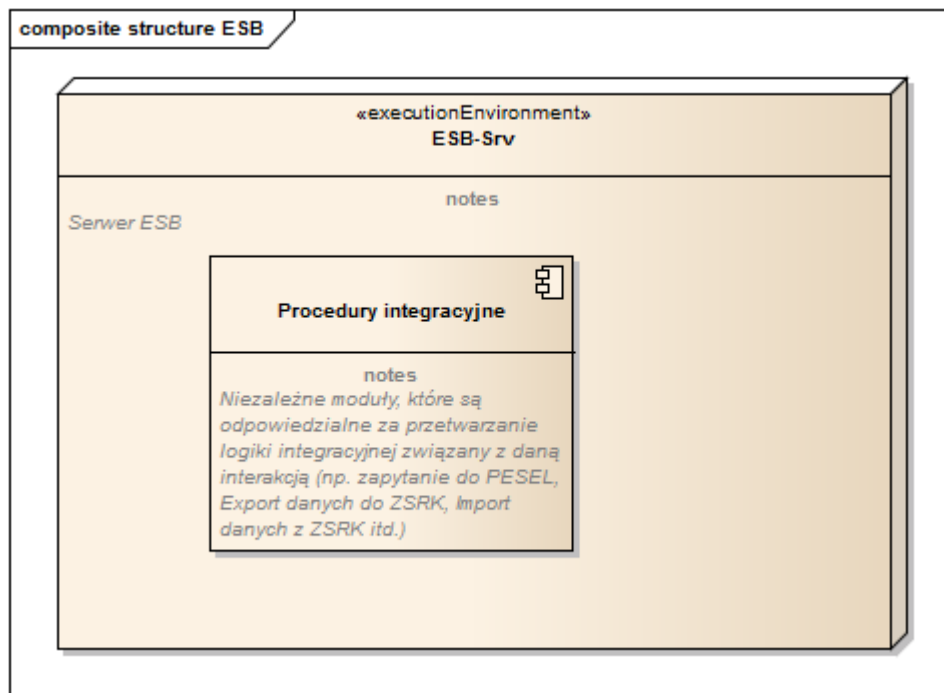
Podsystem zbudowany jest w architekturze trójwarstwowej.

Podsystem Konfiguracja zbudowany będzie w architekturze trójwarstwowej. Będzie posiadał dedykowaną bazę danych, warstwę dostępową do bazy danych oraz aplikację użytkownika do zarządzania i przeglądania konfiguracji.

Podsystem Konfiguracja występuje w następujących postaciach:

- Centralna: Konfiguracja, w którym zarządza się: parametrami konfiguracji, słownikami, uprawnieniami.
- Zawartość bazy danych konfiguracji zostanie zreplikowana do bazy operacyjnej alfanumerycznej podsystemu SIWPM.

3.1.1.3 Podsystem ESB



Rysunek 7 – ESB – model komponentowy

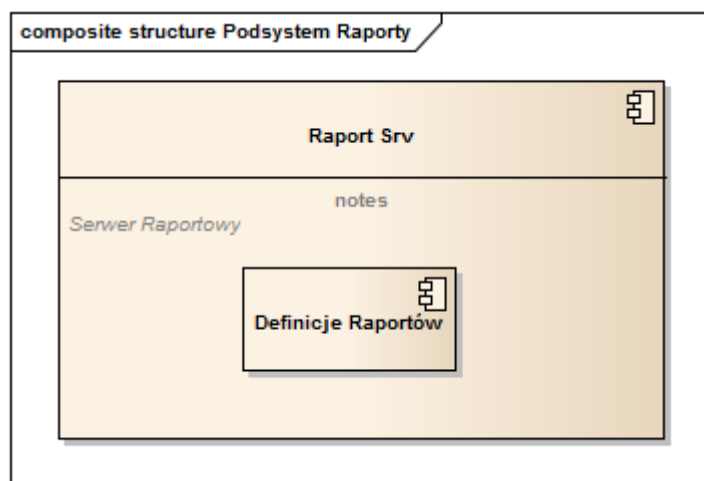
Podsystem odpowiedzialny za:

- Pośredniczenie w komunikacji z innymi systemami zewnętrznymi.
- Pośredniczenie w komunikacji między różnymi instancjami systemu SIWPM obsługującymi różne Ośrodki Regionalne (często rozmieszczone w różnych OZI).
- Uwierzytelnienie komunikujących się z SIWPM innych systemów.
- Autoryzację (kontrolę uprawnień) operacji wykonywanych przez systemy zewnętrzne.
- Wykonanie logiki związanej z integracją.
- Zapewnienie rozliczalności procesu wymiany danych przez prowadzenie śladu rewizyjnego.
- Zapewnienie niezawodności.

Podsystem będzie mieć budowę modułową – każdy rodzaj interakcji z danym zewnętrznym systemem jest obsługiwany przez oddzielną procedurę.

Integracja systemu SIWPM z innymi systemami będzie wykonywana na poziomie centralnym..

3.1.1.4 Podsystem Raporty



Rysunek 8 – Podsystem Raporty – model komponentowy

Podsystem odpowiedzialny za tworzenie raportów.

Podsystem występuje w następujących postaciach:

- Centralny:Raporty
Raporty w Ośrodku Centralnym:
- Reg-Prod:Raporty
Raporty na regionalnym środowisku produkcyjnym
- Reg-Arch:Raporty -
Raporty na regionalnym środowisku archiwalnym

3.1.2 Podsystemy Infrastrukturalne

3.1.2.1 Podsystem Backup

Podsystem Backup jest odpowiedzialny za wykonywanie kopii zapasowych danych w danym OZI..

3.1.2.2 Podsystem lokalnego monitorowania infrastruktury

Podsystem jest odpowiedzialny za monitorowanie infrastruktury technicznej w danym OZI.

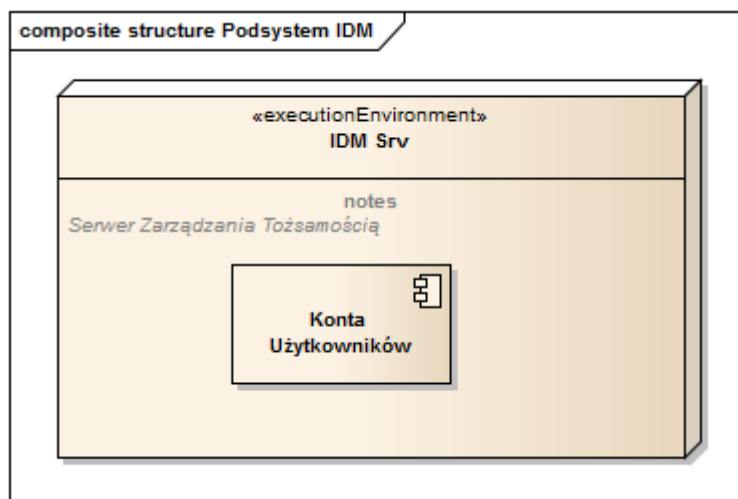
3.1.2.3 Podsystem zarządzania logami systemowymi

Podsystem jest odpowiedzialny zarządzanie logami systemowymi i ochronę ich zawartości przed nadpisaniem wynikającym z roatcji.

3.1.3 Podsystemy Pomocnicze

Podsystemy, których implementacja jest w zakresie innych projektów a z którymi SIWPM się zintegruje.

3.1.3.1 Podsystem IDM

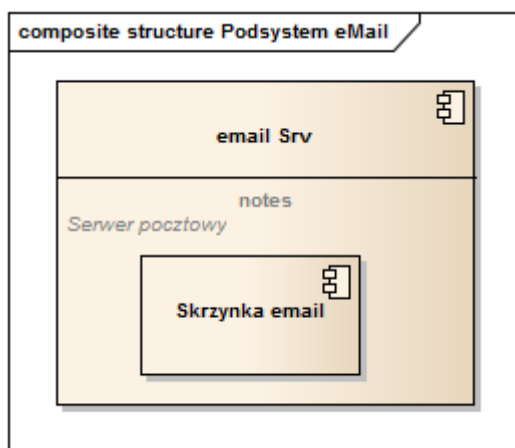


Rysunek 9 – Podsystem IDM – model komponentowy

Podsystem odpowiedzialny za:

- zarządzanie (tworzenie, modyfikowanie, przechowywanie) kontami użytkowników
- uwierzytelnianie użytkowników (weryfikacja i potwierdzenie zgłaszanej przez dany podmiot identyfikacji). Podsystem IDM nie jest odpowiedzialny za zarządzanie uprawnieniami (ta jest dokonywana w podsystemie Centralna Konfiguracja) i za autoryzację (kontrola uprawnień) operacji (ta jest dokonywana w systemach docelowych np. w SIWPM).

3.1.3.2 Podsystem eMail



Rysunek 10 – Podsystem eMail – model komponentowy

Podsystem odpowiedzialny za zarządzanie i udostępnianie skrzynek poczty elektronicznej. Skrzynki te mają służyć przede wszystkim do przechowywania i udostępniania EAS (Elektronicznych Akt Sprawy). Mogą także służyć do przechowywania i udostępniania powiadomień. EAS będą automatycznie generowane i wysyłane na skrzynki dedykowane dla każdego wydziału przy każdym sądzie zarządzane w podsystemie eMail.

3.1.3.3 Usługi sieciowe

Podsystem DNS

Podsystem odpowiedzialny za translację nazw na adresy IP.

Podsystem NTP

Podsystem odpowiedzialny za udostępnianie czasu.

3.2 Model rozmieszczenia

3.2.1 Decyzje projektowe

Ośrodek Centralny zostanie rozmieszczony w

Ośrodek Zapasowy oraz Środowiska Pomocnicze (Testowe, Szkoleniowe) zostaną umieszczone w OZI

Podsystem Centralnego Monitorowania i Zarządzania zostanie umieszczony w Ośrodku Zapasowym (podsystem nie jest krytyczny dla działania SIWPM).

Na macierzy dyskowej trzymane będą tylko pliki z bazami danych. Ponieważ obrazy maszyn wirtualnych nie zawierają żadnych istotnych danych (za wyjątkiem logów systemowych archiwizowanych przez podsystem zarządzania logami), będą trzymane na lokalnych dyskach maszyn fizycznych i nie będą replikowane do Ośrodka Zapasowego. Należy zapewnić aktualność maszyn

wirtualnych w Ośrodku Zapasowym za pomocą procedur administracyjnych. Aby ułatwić zarządzanie maszynami wirtualnymi z warstwą pośrednią SIWPM będą one ujednolicone i będą zawierać konfigurację, która umożliwi obsługę dowolnej apelacji.

3.2.1.1 Przypisanie apelacji do OZI

OZI	Apelacja	Liczba osób	Razem
Elbląg	Białystok	2 248	10 249
	Gdańsk	4 872	
	Warszawa	3 129	
Krosno	Kraków	3 792	8 863
	Rzeszów	1 640	
	Lublin	3 431	
Słupsk	Poznań	3 080	8 829
	Szczecin	2 480	
	Łódź	3 269	
Siedlce	Ośrodek Zapasowy Środ Pomocnicze Centralnego Monitorowania i Zarządzania		
Wrocław	Katowice	4 810	8 936
	Wrocław	4 126	
	Ośrodek Centralny		