**ARCHITEKTURA REFERENCYJNA**

**ŚRODOWISKA IT**

**CPD MF**

## Cel dokumentu

Niniejszy dokument opisuje **architekturę referencyjną środowiska IT CPD MF*.*** Dokument przedstawia architekturę w docelowym środowisku informatycznym CPD MF. Zastosowano tu w szerokim zakresie standaryzację komponentów składowych architektury poprzez definicję bloków architektonicznych oraz ujednolicone podejście do graficznego przedstawiania wszystkich systemów, zarówno infrastrukturalnych jak i biznesowych.

## Odbiorcy dokumentu

Niniejszy dokument jest przeznaczony dla osób biorących udział w realizacji zadań związanych z dostarczeniem Platformy Aplikacyjnej dla ***systemów biznesowych uruchamianych na infrastrukturze teleinformatycznej CPD MF***. Jest podstawą do realizacji zamówień produktowych, budowy Platformy Aplikacyjnej oraz migracji systemów biznesowych do środowiska IT CPD MF. Opisane bloki mogą być również wykorzystywane do budowy Platformy Aplikacyjnej systemów infrastrukturalnych zainstalowanych w CPD MF.

# Zakres i zasięg architektury referencyjnej

**Zakres**

Zakres architektury referencyjnej odnosi się do wszystkich Systemów projektowanych, wdrażanych lub funkcjonujących w środowisku CPD MF. W środowisku CPD MF działają lub będą działać systemy infrastrukturalne oraz systemy biznesowe. Systemy infrastrukturalne obejmują rozwiązania w zakresie:

* komunikacji LAN
* komunikacji WAN
* komunikacji SAN
* replikacji i zabezpieczenia danych
* usług katalogowych
* kopii zapasowych danych
* archiwizowania danych
* deduplikacji danych
* zabezpieczenia antywirusowego
* dystrybucji oprogramowania
* infrastruktury klucza publicznego
* usług terminalowych
* kryptograficznej ochrony informacji
* rejestrowania i monitorowania zdarzeń
* zarządzania tożsamością cyfrową
* zarządzania infrastrukturą
* monitorowania i zarządzania usługami
* wsparcia usług
* budowy bazy konfiguracji obiektów IT

Środowisko systemów infrastrukturalnych i biznesowych jest definiowane poprzez bloki architektoniczne, które są głównymi składnikami Systemów uruchamianych w CPD MF.

W poniższej tabeli zdefiniowano główne obszary rozwiązań architektonicznych.

| **Lp** | **Nazwa obszaru** | **Opis obszaru** |
| --- | --- | --- |
|  | Warstwy systemów | W ramach architektury środowisk IT w CPD MF wyróżnione są 4 warstwy w modelu warstwowym systemów:* proxy
* aplikacyjna
* bazodanowa
* zasobów danych

Dla każdej z warstw systemów zdefiniowane są bloki architektoniczne używane do budowy dowolnych Systemów w CPD MF.   |
|  | Bloki architektoniczne | Bloki architektoniczne do budowy systemów składają się z następujących komponentów:* platformy sprzętowej
* środowiska wirtualizacyjnego
* systemu operacyjnego
* platformy aplikacyjnej

Zdefiniowano dwa rodzaje bloków:* typu IaaS
* typu PaaS

Bloki architektoniczne typu IaaS zawierają platformę sprzętową - jako bloki fizyczne - i platformę wirtualizacyjną - jako bloki wirtualne. Bloki typu PaaS, oprócz platformy sprzętowej i platformy wirtualizacyjnej, zawierają system operacyjny lub system operacyjny i platformę aplikacyjną, czyli środowisko do uruchamiania aplikacji. Bloki typu IaaS są podstawą do tworzenia usług typu IaaS, a bloki typu PaaS są używane do usług typu PaaS. Oprócz bloków architektonicznych do budowy systemów informatycznych zdefiniowane są bloki architektoniczne przeznaczone do tworzenia infrastruktury komunikacyjnej w zakresie LAN, WAN, SAN.   |
|  | Klasy systemów | Każdy System, osadzony w środowisku IT CPD MF, podlega klasyfikacji zgodnie ze „Standardem określenia klasy systemu informatycznego w resorcie finansów”. Głównymi parametrami określającymi klasę systemu są :* RTO – całkowity dopuszczalny czas przywrócenia Systemu do ponownego działania po wystąpieniu awarii
* RPO - aktualność danych po wystąpieniu awarii
* dostępność – całkowity dopuszczalny czas niedostępności Systemu w ciągu całego roku

Zgodnie z tym standardem Systemy mogą należeć do jednej z następujących klas:* Klasa I
* Klasa II
* Klasa III
* Klasa IV

Klasa I systemu jest najwyższą klasą pod względem RTO, RPO i parametru dostępności. |
|  | Klasy bezpieczeństwa systemów | Każdy System, osadzony w środowisku IT CPD MF, podlega klasyfikacji zgodnie ze „Standardem określenia klasy bezpieczeństwa systemu informatycznego w resorcie finansów”. Głównymi cechami określającymi klasę bezpieczeństwa systemu są :* mechanizmy ochrony kryptograficznej
* mechanizmy uwierzytelniania i autoryzacji użytkowników
* stopień odseparowania zasobów systemu od innych zasobów
* mechanizmy rejestrowania, monitorowania i audytu zdarzeń
* mechanizmy ochrony przed oprogramowaniem złośliwym
* czy jest dostępny zdalnie
* czy ma zabezpieczony styk systemu z innymi sieciami

Zgodnie z tym standardem Systemy mogą należeć do jednej z następujących klas:* Klasa B3
* Klasa B2
* Klasa B1
* Klasa BX

Klasa B1 systemu jest najwyższą klasą bezpieczeństwa systemu pod względem wymienionych cech. Natomiast klasa BX jest klasą bezpieczeństwa dla systemów całkowicie odseparowanych od środowiska IT. Do klasy BX należą systemy, które nie współdzielą żadnej infrastruktury z innymi systemami. Zasilanie tych systemów w dane następuje za pomocą nośników przenaszalnych, np. taśm magnetycznych, dysków magnetycznych, płyt CD-ROM i DVD lub innych mediów. Udostępnianie z tych systemów danych dla innych systemów odbywa się również drogą nośników przenaszalnych. Klasyfikacja systemów pod względem bezpieczeństwa narzuca na systemy infrastrukturalne i systemy biznesowe wymagania, które powinny być spełnione poprzez odpowiednio zaprojektowane i wdrożone zabezpieczenia na poziomie infrastruktury oraz platformy aplikacyjnej.  |
|  | Relacje między warstwami systemów | W ramach modelu warstwowego komunikacja między warstwami proxy, aplikacyjną i bazodanową realizowana jest poprzez struktury LAN w ten sposób, że pomiędzy poszczególnymi warstwami są definiowane odpowiednie podsieci VLAN. Te podsieci jednocześnie izolują ruch komunikacyjny obiektów systemów działających w danej warstwie. Zdefiniowane i uruchomione podsieci VLAN są wykorzystywane przez wiele systemów. Ruch sieciowy między warstwami systemów jest izolowany. W przypadkach koniecznych jest możliwa realizacja połączeń między podsieciami VLAN poprzez firewalle lub routery.  |
|  | Komunikacja między ośrodkami OP w CPD MF  | W skład CPD MF wchodzą następujące Ośrodki Przetwarzania:* OP Radom
* OP Warszawa
* OP Warszawa 2

Każdy z tych ośrodków posiada połączenie do sieci intranetowej resortu finansów przez sieć operatorską MPLS.  |
|  | Komunikacja z użytkownikami sieci WAN | Komunikacja użytkowników resortu finansów z ośrodkami CPD MF odbywa się poprzez sieć operatorską MPLS. W OP Radom, OP Warszawa i OP Warszawa 2 wymagane są instalacje routerów w układach redundantnych i o odpowiednio skalowalnej przepustowości.  |
|  | Komunikacja między CPD MF i urzędami administracji publicznej oraz innymi użytkownikami instytucjonalnymi  | Komunikacja między użytkownikami instytucjonalnymi a ośrodkami CPD MF odbywa się poprzez dedykowane struktury komunikacyjne w ramach rozwiązań bramki ekstranetowej. To wyjście komunikacyjne wymaga instalacji dedykowanych routerów, firewalli, IPS i UTM. W ramach tej struktury są dostępne sieci DMZ, wykorzystywane do instalacji dedykowanych urządzeń lub serwerów wymaganych w połączeniach z konkretnymi użytkownikami.  |
|  | Komunikacja z użytkownikami sieci Internet  | Komunikacja z użytkownikami sieci Internet odbywa się poprzez bramkę do Internetu. Bramka do Internetu wymaga budowy opartej na dedykowanych routerach, firewallach i systemach IPS. W ramach tej struktury dostępne są farmy serwerów proxy wymaganych w obsłudze użytkowników zewnętrznych oraz systemów biznesowych. Bramka służy również do dostępu dla użytkowników będących pracownikami resortu finansów (tylko dla OP\_W), do środowisk IT resortu poprzez kanały VPN (po przejściu procesu autoryzacji i uwierzytelnienia). Bramka internetowa składa się m.in. z serwerów DNS i komponentów systemu poczty elektronicznej. W ramach konfiguracji urządzeń w bramce realizowane jest filtrowanie ruchu zgodnie z przyjętą polityką i zasadami użytkowania tego medium w resorcie finansów.  |

Tabela 1 Główne obszary architektury CPD MF

**Zasięg**

Architektura referencyjna obejmuje Ośrodki Przetwarzania, wchodzące w skład CPD MF. Architektura IT, dostępna w każdym z tych Ośrodków jest jednolita. Z punktu widzenia administracji i użytkowania wszystkie Ośrodki stanowią jedną logiczną całość.

Komponenty systemów infrastrukturalnych powinny być zainstalowane w OP Radom, OP Warszawa i OP Warszawa 2. Niektóre z tych systemów są zintegrowane z systemami działającymi w resorcie finansów, bądź ich infrastruktura została rozszerzona do innych lokalizacji poza wymienione Ośrodki Przetwarzania. Takie rozszerzenie rozwiązań wynika ze względów technicznych lub ograniczeń w szybkości migracji do architektury centralnej istniejących systemów.

Systemy biznesowe, bądź ich wybrane komponenty, mogą być instalowane w ośrodkach wchodzących w skład CPD MF.

# Architektura referencyjna CPD MF

## Wstęp do architektury

Architektura systemów IT może być opisywana w różnych perspektywach. W wielu metodykach opis architektury głównie dotyczy:

* perspektywy biznesowej
* perspektywy funkcjonalnej lub systemów informatycznych
* perspektywy technologicznej
* perspektywy implementacyjnej.

W niektórych opisach architektur, np. w metodyce TOGAF, występują tylko 3 pierwsze perspektywy. Wszystkie wymienione perspektywy są związane ze sobą odpowiednimi relacjami racjonalnych przesłanek i reguł, które tworzą konstrukcyjnie logiczną całość. W każdej metodyce kluczową rolę odgrywa perspektywa biznesowa. W odniesieniu do niej tworzone są odpowiednie relacje, zawierające postulaty, wnioski i przesłanki, aby przejść do następnych perspektyw.

Ze szczegółowych opisów perspektyw architektur są tworzone modele architektoniczne, które zwykle stają się podstawą budowy środowisk IT z dobrze zdefiniowanymi technologiami informatycznymi oraz określonymi ograniczeniami ich zakresu stosowalności.

## Model warstwowy systemu

Do budowy środowiska IT w CPD MF został przyjęty czterowarstwowy model ogólny systemów. Uzasadnieniem dla tego modelu jest charakter środowiska IT, które będzie budowane w Ośrodkach Przetwarzania CPD MF. Głównymi składowymi obecnie budowanych systemów biznesowych są następujące warstwy:

* warstwa proxy
* warstwa aplikacyjna
* warstwa bazodanowa
* warstwa zasobów danych.

Wszystkie te warstwy odgrywają ważną rolę w modelach środowiska IT chmur obliczeniowych, ponieważ są one przedmiotem oferty w katalogach usług związanych z ofertą dla klientów. W przypadku CPD MF Klientem jest DB1/MF, DS/MF, IU/MF i, w rezultacie, cały resort finansów.

W każdej warstwie modelu są dostępne zasoby infrastrukturalne w formie bloków architektonicznych. Bloki architektoniczne umieszczone w 3 pierwszych warstwach charakteryzują się:

* platformą sprzętową
* metodą wirtualizacji
* systemem operacyjnym
* platformą aplikacyjną.

Natomiast dla warstwy zasobów danych istotnymi parametrami są:

* Pojemność danych
* Szybkość dostępu do danych
* Sposób zabezpieczenia danych
	+ typ RAIDu
	+ replika wewnętrzna w macierzy
	+ replika w zewnętrznej macierzy.

Ponadto te zasoby infrastrukturalne należą do różnych klas systemów, co oznacza, że bloki architektoniczne typu IaaS lub PaaS, jako obiekty wirtualne zbudowane na bazie serwerów fizycznych, mogą działać w ramach różnych systemów o różnych klasach. To samo dotyczy systemów operacyjnych obiektów wirtualnych. W szczególności na jednym serwerze fizycznym może działać wiele serwerów wirtualnych z różnymi systemami operacyjnymi. Zasoby danych są udostępniane różnym systemom o innych klasach w jednym typie macierzy dyskowych (uniwersalnych), w których są zainstalowane dyski o różnych szybkościach dostępności. Macierze dyskowe są wyposażone w oprogramowanie, które optymalizuje wykorzystanie dostępnej przestrzeni dyskowej pod względem intensywności operacji I/O na zdefiniowanych obszarach, np. na poziomie LUN, plików lub bloków. Takie podejście do wykorzystywania zasobów infrastrukturalnych nie determinuje ich przynależności do określonej klasy systemów. Natomiast sposób budowy poszczególnych systemów wraz z zastosowaniem odpowiednich mechanizmów (klastry i farmy w pierwszych trzech warstwach oraz replikacja danych w warstwie czwartej) wspiera wartości parametrów RTO, RPO i dostępność, definiowane dla każdej klasy systemu.

## Sieć LAN

Całe środowisko CPD MF jest połączone siecią LAN. W tabeli poniżej został podany podział sieci LAN na grupy podsieci VLAN, które pełnią określone funkcje komunikacyjne. Każda grupa składa się z wielu podsieci VLAN.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Funkcjonalne grupy VLAN-ów** | **Opis** |
| 1 | INTERIEn | podsieci podłączeniowe do Internetu w Węźle Bramki Internet |
| 2 | FWIEn | podsieci zewnętrzne w Węźle Bramki Internet |
| 3 | DMZIEn | podsieci wewnętrzne DMZ w Węźle Bramki Internet |
| 4 | VPROXYIEn | podsieci serwisów wirtualnych w Węźle Bramki Internet |
| 5 | VPROXYIE\_OUTn | podsieci w Węźle Bramki Internet dedykowane do komunikacji wewnętrznej intranetowej  |
| 6 | EXTNETn | podsieci podłączeniowe do WAN-u w Węźle Bramki Użytkowników Instytucjonalnych (UI) |
| 7 | FWEXTn | podsieci zewnętrzne w Węźle Bramki EXTRANET |
| 8 | DMZEXTn | podsieci wewnętrzne DMZ w Węźle Bramki EXTRANET |
| 9 | VPROXYWANn | podsieci serwisów wirtualnych w Węźle Bramki WAN |
| 10 | VPROXYWAN\_OUTn | podsieci w Węźle Bramki WAN dedykowane do komunikacji wewnętrznej intranetowej |
| 11 | WANn | podsieci podłączeniowe do WAN-u w Węźle Dostępowym WAN |
| 12 | FWWANn | podsieci zewnętrzne w Węźle Dostępowym WAN |
| 13 | SynWDn | podsieci techniczne na potrzeby synchronizacji Zapór Sieciowych i Urządzeń Równoważących Obciążenie (FW/LB) w Węzłach Bramki i Intranet |
| 14 | PROXYn | podsieci wewnętrzne w Węźle Bramki Internetowej i WAN dla fizycznych serwerów |
| 15 | TRANZn | podsieci tranzytowe |
| 16 | VAPPn | podsieci dla wirtualnych serwisów aplikacyjnych |
| 17 | APPn | podsieci dla serwerów aplikacyjnych |
| 18 | DBn | podsieci dla ‘BackEnd-owych’ serwerów bazodanowych |
| 19 | BACKUPn | podsieci dla wykonywania kopii zapasowych (Backup) |
| 20 | SVMOTIONn | podsieci dla komunikacji między obiektami wirtualnymi oraz przeznaczone do przenoszenia obieków wirtualnych między różnymi maszynami fizycznymi  |
| 21 | SynLANn | podsieci techniczne na potrzeby synchronizacji Zapór Sieciowych i Urządzeń Równoważących Obciążenie (FW/LB) w Węzłach Dystrybucyjnych |
| 22 | HBn | podsieci grupowania serwerów |
| 23 | MGMTn | podsieci dla systemów zarządzania |

Tabela 3 Podział zestawów VLAN-ów na grupy funkcjonalne

## Budowa bloków architektonicznych

Budowa bloków architektonicznych jest oparta na platformie sprzętowej. Następnie sprzęt poddaje się wirtualizacji – tak dalece, jak to jest możliwe i uzasadnione rachunkiem ekonomicznym. W ten sposób uzyskuje się bloki typu IaaS (ang. Infrastructure as a Service). Potem, już jako obiekty logiczne środowiska, są one wyposażane w system operacyjny i ten sposób uzyskuje się bloki typu PaaS (ang. Platform as a Service – tylko z systemem operacyjnym).

W kolejnym kroku dokonuje się wyboru i instalacji dodatkowych komponentów platformy aplikacyjnej (środowisko wykonywania aplikacji) dla bloków typu PaaS albo instalacji aplikacji. Po uformowaniu takich bloków środowisko jest gotowe do udostępnienia ich klientom.

W ramach optymalizacji wykorzystania zasobów infrastrukturalnych bloki architektoniczne budowane są w środowisku wirtualnym.

**W przypadku, gdy producent środowiska wykonywania aplikacji wyróżnia wirtualizację kontrolowaną przez system operacyjny (np. VmWare, Hyper-V) tzw. „soft partitioning” i nie dopuszcza licencjonowania w trybie tylko na rdzenie przydzielone do bloku architektonicznego wymagane jest dostarczenie licencji wraz z opcjami środowiska wykonywania aplikacji na cały serwer fizyczny (wszystkie procesory).**

**Do wyliczenia wymaganej liczby licencji należy założyć, że jeden serwer fizyczny wyposażony jest w 36 rdzeni fizycznych.**

## Opisy bloków architektonicznych

W niniejszym dokumencie określone zostały bloki architektoniczne typu IaaS oraz bloki architektoniczne urządzeń sieciowych LAN, WAN, zapór sieciowych, urządzeń odpowiadających za inspekcję ruchu (IPS), urządzeń równoważących ruch sieciowy oraz urządzeń DWDM udostępnianych jako usługa od operatora telekomunikacyjnego.

Bloki architektoniczne typu PaaS, które są wykorzystywane głównie w systemach biznesowych, zostały opisane w dokumencie „Usługi i bloki architektoniczne wspierające budowę systemów biznesowych w CPD MF”.

Wszystkie opisy bloków typu IaaS i PaaS zawierają, przedstawione w formie matryc, dopuszczalne wartości charakterystycznych parametrów. Opis każdego bloku typu IaaS zawiera listę komponentów, które zostały użyte w tekście opisu bloków architektonicznych.

## Opisy bloków architektonicznych typu IaaS

Na poziomie bloków typu IaaS – urządzenia fizyczne lub platforma wirtualizacyjna – wsparcie dla klas bezpieczeństwa systemów występuje tylko na poziomie podstawowym B3 lub BX (fizyczna separacja zasobów). Nie działają tu żadne mechanizmy związane z systemem operacyjnym, a tym bardziej oddziaływania międzysystemowe, które głównie decydują o określaniu klasy bezpieczeństwa systemów. W tym ujęciu wyjątek stanowią bloki routerów i zapór sieciowych, które, ze względu na możliwość zastosowania odpowiedniego oprogramowania, mogą wspierać ochronę kryptograficzną przesyłanych danych w sieciach zewnętrznych poprzez np. rozwiązania VPN.

Bloki typu IaaS są podstawowym elementem budowy systemów i przez wzbogacanie o platformę aplikacyjną nabierają cech bloków typu PaaS. Ze względu na swoją złożoność bloki te wspierają w większym stopniu klasy bezpieczeństwa systemów informatycznych.

## Wsparcie dla klas bezpieczeństwa

Wsparcie bloków dla klas bezpieczeństwa w kontekście poszczególnych kategorii, opisanych w definicji klas bezpieczeństwa zostało zawarte w załączniku D.

Każdy blok architektoniczny może być stosowany w systemach klasy BX pod warunkiem fizycznego odseparowania komponentów wykorzystanych w tym bloku od komponentów innych systemów.

Załącznik D zawiera tabelę z nazwami grup i poszczególnymi nazwami opisanych bloków architektonicznych. Dla oznaczania poziomu wsparcia dla klas systemów i klas bezpieczeństwa systemów w zbiorczej tabeli zostały użyte znaki „+” oznaczające, że dany blok architektoniczny posiada taką konstrukcję i cechuje się parametrami, które spełniają wymagania danej klasy systemu.

W załączniku A opisane zostały kolejno bloki architektoniczne typu IaaS wymienione w powyższej tabeli. Opis każdego bloku ma taką samą strukturę i składa się z:

* tabeli informacyjnej bloku architektonicznego
	+ identyfikatora bloku,
	+ nazwy bloku,
	+ rodzaju bloku,
	+ wsparcia dla klas systemów,
	+ wsparcia dla klas bezpieczeństwa systemów,
* historii zmian,
* celu dokumentu,
* atrybutów bloku architektonicznego,
* ograniczeń na wartości atrybutów,
* wsparcia dla klas bezpieczeństwa (szczegółowego),
* komponentów bloku architektonicznego,
* diagramu realizacji,

W tabelach opisujących ograniczenia na wartości atrybutów bloku oraz w tabelach wsparcia dla klas bezpieczeństwa bloków architektonicznych użyto słowa „TAK” w przypadku pełnego wsparcia przez konstrukcję i parametry bloku dla danej klasy bezpieczeństwa systemu. Brak wsparcia został oznaczony znakiem „-”.

Każdy blok architektoniczny może być wykorzystany do budowy systemu o wyższej klasie bezpieczeństwa niż on sam wspiera. W takim przypadku potrzebne są dodatkowe komponenty systemu, które podniosą klasę bezpieczeństwa systemu, np. oprogramowanie szyfrujące na serwerach aplikacyjnych lub zapora sieciowa dla serwera, na którym znajdują się wrażliwe zasoby danych.

# Architektura referencyjna systemów realizujących usługi biznesowe

Niniejszy sekcja opisuje bloki architektoniczne wspierające budowę systemów biznesowych.Zastosowano tu w szerokim zakresie standaryzację komponentów składowych architektury poprzez definicję bloków architektonicznych, zarówno infrastrukturalnych jak i aplikacyjnych, dla realizacji systemów biznesowych.

Architektura referencyjna zlokalizowanych w CPD MF systemów biznesowych resortu finansów określa, że są one budowane z wykorzystaniem dedykowanych dla konkretnego systemu informatycznego zestandaryzowanych elementów, nazywanych blokami architektonicznymi. Jedna instancja bloku architektonicznego może być wykorzystywana wyłącznie przez jedno środowisko jednego systemu informatycznego. Ta zasada nie dotyczy złożonych usług dostępowych typu proxy. Dla instancji tych usług dopuszcza się relacje typu wiele do wielu co oznacza, że każda z instancji może zawierać wiele bloków proxy i każdy blok proxy może wchodzić w skład wielu instancji usługi proxy.

Pozostałe usługi informatyczne, niezbędne do prawidłowego działania bloków architektonicznych oraz osadzonych w nich komponentów aplikacyjnych, są zapewniane przez współdzielone systemy infrastrukturalne.

Zarówno bloki architektoniczne, jak i współdzielone usługi teleinformatyczne świadczone przez systemy infrastrukturalne, są dostarczane przez CPD MF zgodnie z modelem usługowym i Katalogiem Usług (Rysunek 1).



Rysunek 1 Przykład Usług Platformy Aplikacyjnej CPD MF

W kolejnych załącznikach opisano wymagania w stosunku do funkcjonalności oraz architektury tych bloków, uwzględniające obowiązujące w resorcie finansów standardy klasyfikacji systemów oraz klasyfikacji bezpieczeństwa systemów.

Bloki architektoniczne, zgodnie z charakterem świadczonych przez nie usług, zostały podzielone na następujące kategorie:

* Bloki proxy, służące do budowy usług dostępowych,
* Bloki serwerów aplikacji, stanowiące środowisko uruchomieniowe komponentów aplikacyjnych,
* Bloki bazodanowe, zapewniające usługi zarządzania danymi z wykorzystaniem silników relacyjnych baz danych,
* Bloki świadczące usługi na poziomie systemu operacyjnego, umożliwiające stosowanie technologii niedostępnych w pozostałych blokach.

W przypadku zaistnienia potrzeby zmian, proces modyfikacji funkcjonalności lub architektury opisanych bloków oraz dodawania nowych bloków i wycofywania bloków z eksploatacji jest realizowany przez CPD MF zgodnie z zasadami opisanymi w obowiązującym procesie zarządzania architekturą CPD MF.

Potrzeba wprowadzenia takich zmian może wynikać zarówno z konieczności uwzględnienia wymagań systemów biznesowych, jak i zmian standardów obowiązujących w resorcie finansów, czy też w wyniku działania Procesu Zarządzania Problemami.

Każda instancja opisanych bloków architektonicznych powstaje na podstawie utrzymywanego przez CPD MF Projektu Technicznego, opisującego sposób instalacji i konfiguracji komponentów wchodzących w skład danego bloku architektonicznego. Dla każdego bloku CPD MF utrzymuje, oprócz dokumentacji projektowej i testowej, również dokumentację eksploatacyjną. Opisane powyżej dokumenty powstają zgodnie z obowiązującymi w CPD MF standardami dokumentacji i są utrzymywane zgodnie z obowiązującymi w nim procesami - zarówno procesami ITIL, jak i procesem zarządzania architekturą CPD MF.

Na diagramie poniżej przedstawiony został uproszczony model logiczny systemu udostępniającego swoje usługi w Internecie i Intranecie resortu finansów. Dostęp do tych usług mają zarówno użytkownicy końcowi, jak i inne systemy zlokalizowane poza CPD MF. Usługi dostępowe CPD MF umożliwiają zarówno udostępnienie usług świadczonych przez komponenty aplikacyjne systemu, jak i dostęp komponentów aplikacyjnych systemu do systemów zlokalizowanych poza CPD MF.



Rysunek 2 Model logiczny systemu realizujacego funkcje biznesowe

Opisywany system informatyczny składa się z bazy danych DB, dwóch komponentów aplikacyjnych AP1 i AP2, oraz dwóch komponentów pośredniczących, pozwalających na bezpieczne udostępnienie aplikacji w Internecie i Intranecie resortu finansów.

Realizacja fizyczna systemu zgodnego z przedstawioną na diagramie architekturą logiczną, w sposób zgodny z architekturą referencyjną, polegałaby na:

* osadzeniu bazy danych DB w bloku bazodanowym, zapewniającym wymagany silnik bazy relacyjnej,
* osadzeniu komponentów aplikacyjnych AP1 i AP2, w blokach aplikacyjnych zapewniających wymagany serwer aplikacyjny np. w technologii JEE,
* udostępnieniu komponentów aplikacyjnych AP1 i AP2 w sieciach zewnętrznych z wykorzystaniem opisanych w dokumencie usług dostępowych.

Dostarczenie wymaganych przez system bloków architektonicznych, zapewnienie pomiędzy nimi komunikacji oraz skonfigurowanie usług dostępowych zgodnie z wymaganiami wynikającymi z klasy bezpieczeństwa systemu wchodzi w zakres obowiązków CPD MF. Zapewnienie komunikacji pomiędzy blokiem aplikacyjnym i bazodanowym obejmuje skonfigurowanie w serwerze aplikacyjnym puli połączeń do bazy danych.

Konfiguracja usług dostępowych obejmuje wymaganą konfigurację zapór ogniowych CPD MF i, jeśli to wynika z wymagań klasy bezpieczeństwa systemu, odpowiednie skonfigurowanie sond monitorujących komunikację. Sposób separacji, logiczny lub fizyczny, pomiędzy blokami architektonicznymi należącymi do różnych systemów wynika z klasyfikacji bezpieczeństwa systemów informatycznych, w których skład wchodzą.

CPD MF administruje blokami architektonicznymi od momentu dostarczenia zamówionych bloków użytkownikowi do momentu ich wycofania z eksploatacji. W czasie eksploatacji bloku świadczy użytkownikowi usługi zgodnie zakresem opisanym dla każdego z bloków w Katalogu Usług. Usługi utrzymaniowe zapewniane przez CPD MF obejmują również zabezpieczanie konfiguracji i/lub danych kopiami bezpieczeństwa oraz instalację wymaganych poprawek systemowych (ang. patches) dla wszystkich komponentów wchodzących w skład bloku.

Wszelkie zmiany konfiguracyjne w komponentach wchodzących w skład bloku architektonicznego realizowane są wyłącznie przez CPD MF. Zmiany mogą być wprowadzane na wniosek użytkownika bloku lub samodzielnie w przypadku konieczności rozwiązania incydentu lub problemu. Zmiana wprowadzona przez CPD MF bez uzgodnienia z użytkownikiem bloku architektonicznego nie może pogorszyć parametrów usług świadczonych przez ten blok poniżej wartości uzgodnionych na etapie jego zamawiania.

Osadzenie w blokach architektonicznych i skonfigurowanie komponentów aplikacyjnych systemu informatycznego, osadzenie w bloku architektonicznym bazy danych oraz administrowanie systemem informatycznym na poziomie aplikacyjnym pozostaje w zakresie obowiązków użytkownika usług CPD MF.

# Załączniki

Załącznik A – Bloki architektoniczne środowiska teleinformatycznego

Załącznik B – Standardy parametrów oprogramowania infrastrukturalnego

Załącznik C – Standardy parametrów technicznych urządzeń teleinformatycznych

Załącznik D – Wsparcie dla klas bezpieczeństwa i systemów informatycznych

Załącznik E – Standardy proceduralne i dokumentacyjne