29/PNP/SW/2020 Załącznik nr 1 do SIWZ

Opis przedmiotu zamówienia

Część 1
Macierz dyskowa z dyskami SSD

Nazwa sprzętu: ……

Model: …….

Typ: ……

Producent: …….

Rok produkcji: nie starszy niż **2020** (sprzęt fabrycznie nowy nieużywany , nierekondycjonowany)

Lp	Parametr	Wymagane minimalne parametry techniczne	Parametry oferowane PODAĆ/OPISAĆ
1	**Obudowa**	Pojedynczy/podwójny kontroler z obsługą minimum 24 dysków 2,5” Hot plug 12Gbps; wewnętrzne kieszenie na dyski, sieć z opcjami rozszerzenia; Obudowa typu Rack o wysokości 2U; Obsługa pojedynczego/podwójnego kontrolera dla 2U; Procesor min. 2-rdzeniowy, taktowany częstotliwością min. 2,2 GHz; Pamięć systemowa 8GB na kontroler.	
2	**Kontroler**	Zgodność z serwerami PRIMERGY RX300 S8; Automatyczne pozycjonowanie do 3 podstawowych warstw; Obsługa RAID 0, 1, 5, 6, 10, 50. W jednej macierzy może istnieć dowolna kombinacja poziomów RAID; Maksymalnie 1024 migawki na macierz; Zgodność z dyskami SAS SSD; Szybkość transferu 12Gbps; Wspierane systemy operacyjne: Windows, Linux, Vmware.	
3	**Sieć**	Zgodność z serwerami PRIMERGY RX300 S8; Interfejs FC - 16Gb: 8 portów na macierz, iSCSI - 10Gb 8 portów SFP+ Base T, SAS – 12Gb 8 portów SAS 12 Gb; Porty wieloprotokołowe 4 porty 16Gb FC SFP+, 4 porty 10Gb iSCSI SFP+; Porty zarządzalne 2 na macierz 1Gb. Jeżeli wymagane są licencje Wykonawca dostarcza je wraz z macierzą.	
4	**Dyski**	Wymagane jest dostarczenie macierzy dyskowej posiadającej minimum 6 dysków o minimalnej łącznej pojemności 20TB i prędkości 12Gb/s.	
5	**Gwarancja**	Minimalnie 36 miesięcy gwarancji producenta, bądź partnera serwisowego legitymującego się dokumentami potwierdzającymi posiadanie stosownej autoryzacji, obejmująca serwis	

		sprzętowy oraz wsparcie dla nowych wersji oprogramowania. Gwarancja liczona jest od daty podpisania bez uwag protokołu odbioru dostawy. Gwarancja zawarta w cenie zakupionego przedmiotu. Standardowy czas przystąpienia do naprawy - początek następnego dnia roboczego od zgłoszenia awarii. Standardowy czas naprawy wynosi 1 dzień roboczy od dnia przystąpienia do naprawy. Możliwość zgłaszania awarii bez ograniczenia czasowego (24x7). Uszkodzone dyski pozostają własnością Zamawiającego. Macierz musi posiadać subskrypcje dla dostarczonego z macierzą oprogramowania oraz zapewniony dostęp do portalu serwisowego producenta umożliwiające uzyskanie dokumentacji technicznej urządzenia i systemu operacyjnego, aktualizacji firmware, bazy wiedzy przez cały okres objęcia gwarancją.	

Warunki równoważności:

- Wszystkie krytyczne komponenty macierzy takie jak: kontrolery dyskowe, pamięć cache, zasilacze i wentylatory muszą być zdublowane tak, aby awaria pojedynczego elementu nie wpływała na funkcjonowanie całego systemu. Komponenty te muszą być wymienialne w trakcie pracy macierzy.
- Graficzny interfejs dostępny przez przeglądarkę oraz interfejs tekstowy przez szyfrowane połączenie (HTTPS).
- Bezpośrednie monitorowanie stanu w jakim w danym momencie macierz się znajduje.
- Dane o parametrach utylizacji macierzy muszą być dostępne w interfejsie GUI.
- Zapewnienie możliwości tworzenia skryptów użytkownika.
- Szybkiego i łatwego przenoszenia dysków wolumenów oraz tworzenie kopii zapasowych i odtwarzanie danych za pomocą pełnej kopii.
- Możliwość zarządzania całością dostępnych zasobów dyskowych z jednej konsoli administracyjnej.
- Funkcja powiadamiania poprzez sms i / lub-e-mail.
- Funkcjonalność thin provisioning dla wszystkich wolumenów (LUN). Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy.
- Wspiera funkcję SSD-Cache dla operacji odczytu dla minimalnej pojemności - 1GB. Dostarczenie tej licencji nie jest wymagane na tym etapie postępowania.
- Funkcjonalność zwiększania rozmiaru wolumenów (LUN).
- Wykonywanie kopii migawkowych. Rozwiązanie ma automatycznie powiększać kopie migawkowe razem z przyrostem danych (tzw. delta). Jeśli wymagana jest licencja umożliwiająca wykorzystanie powyższej funkcjonalności, wykonawca dostarczy ją wraz z macierzą.
- Wspieranie mechanizmu lokalnej replikacji w ramach macierzy. Jeśli funkcja wymaga licencji należy ją dostarczyć wraz z macierzą.
- Wspieranie mechanizm zdalnej replikacji z poziomu macierzy na drugą zapasową macierz, w trybie synchronicznym oraz asynchronicznym. Licencja na powyższą funkcjonalność nie jest wymagana na tym etapie zamówienia lub Licencja na tą funkcjonalność musi być zawarta w cenie i musi obejmować zaoferowaną w ramach macierzy przestrzeń dyskową
- Oprogramowanie musi umożliwiać monitorowanie w zakresie dostarczanej macierzy dyskowej zasobów blokowych. Wymagana jest funkcjonalność monitorowania co najmniej w zakresie:

- Przestrzeni macierzy - całościowa, wolna, wykorzystywana;
- Przestrzeni macierzy j.w. z podziałem na poszczególne grupy RAID/wolumeny.

……dn……

……
podpis i pieczęć uprawnionego przedstawiciela Wykonawcy

29/PNP/SW/2020 Załącznik nr 1 do SIWZ

Część 2
Urządzenie router/firewall/VPN/UTM (2 szt. pracujące w klastrze)

Nazwa sprzętu: ……

Model: ……

Typ: ……

Producent: ……

Rok produkcji: nie starszy niż **2020** (sprzęt fabrycznie nowy nieużywany , nierekondycjonowany)

Lp	Parametr	Wymagane minimalne parametry techniczne	Parametry oferowane PODAĆ/OPISAĆ
1	**Obudowa**	Obudowa typu Rack o wysokości 1U;	
2	**Pamięć**	Co najmniej 4 GB pamięci RAM, pamięć Flash 8 GB	
3	**System operacyjny**	Urządzenie musi posiadać budowę modułową (moduły muszą działać w odseparowanych obszarach pamięci) i zapewniać całkowitą separację płaszczyzny kontrolnej od płaszczyzny przetwarzania ruchu użytkowników, m.in. moduł rutingu IP, odpowiedzialny za ustalenie tras rutingu i zarządzanie urządzenia musi być oddzielony od modułu przekazywania pakietów, odpowiedzialnego za przełączanie pakietów pomiędzy segmentami sieci obsługiwanymi przez urządzenie; System operacyjny firewalla musi śledzić stan sesji użytkowników (stateful processing), tworzyć i zarządzać tablicą stanu sesji. Musi istnieć opcja przełączenia urządzenia w tryb pracy bez śledzenia stanu sesji użytkowników, jak również wyłączenia części ruchu ze śledzenia stanu sesji.	
4	**Interfejs**	Urządzenie musi być wyposażone w nie mniej niż 8 wbudowanych interfejsy Ethernet 10/100/1000 (gotowych do użycia bez konieczności zakupu dodatkowych modułów i licencji). Urządzenie musi posiadać slot USB przeznaczony do podłączenia dodatkowego nośnika danych. Musi być dostępna opcja uruchomienia systemu operacyjnego firewalla z nośnika danych podłączonego do slotu USB na module kontrolnym. Urządzenie musi posiadać dodatkowy slot SSD na umieszczenie dysku typu SSD. Urządzenie musi być wyposażone w nie mniej niż 8 portów do zastosowania z wkładkami SFP. Uruchomienie tych portów nie może wymagać zakupu dodatkowych licencji z wyjątkiem zakupu	

		odpowiednich modułów SFP. Urządzenie musi być wyposażone w 4 sloty na dodatkowe karty z modułami interfejsów. Urządzenie musi obsługiwać co najmniej następującej rodzaje kart z modułami interfejsów: T1/E1, VDSL2 Annex A/M, Serial port, 4G/LTE.	
5	**Funkcje**	Firewall musi realizować zadania Stateful Firewall z mechanizmami ochrony przed atakami DoS, wykonując kontrolę na poziomie sieci oraz aplikacji pomiędzy nie mniej niż **64 strefami bezpieczeństwa** z wydajnością nie mniejszą niż **1 Gbps** liczoną dla ruchu IMIX. Firewall musi przetworzyć nie mniej niż **500 000 pakietów/sekundę** (dla pakietów 64-bajtowych). Firewall musi obsłużyć nie mniej niż **250 000 równoległych sesji** oraz zestawić nie mniej niż **10 000 nowych połączeń/sekundę**. Firewall musi zestawiać zabezpieczone kryptograficznie tunele VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site oraz client-to-site. IPSec VPN musi być realizowany sprzętowo. Firewall musi obsługiwać nie mniej niż 1 **000** równoległych tuneli VPN oraz ruch szyfrowany o przepustowości nie mniej niż **200 Mb/s dla ruchu IMIX**. Polityka bezpieczeństwa systemu zabezpieczeń musi uwzględnia strefy bezpieczeństwa, adresy IP klientów i serwerów, protokoły i usługi sieciowe, użytkowników aplikacji, reakcje zabezpieczeń oraz metody rejestrowania zdarzeń. Firewall musi umożliwiać zdefiniowanie nie mniej niż **2 000** reguł polityki bepieczństwa oraz nie mniej niż **64** strefy bezpieczeństwa. Firewall musi posiadać funkcję wykrywania i blokowania ataków intruzów (IPS, *intrusion prevention*) realizowaną sprzętowo. System zabezpieczeń musi identyfikować próby skanowania, penetracji i włamań, ataki typu exploit (poziomu sieci i aplikacji), ataki destrukcyjne i destabilizujące (D)DoS oraz inne techniki stosowane przez hakerów. Ustalenie blokowanych ataków (intruzów, robaków) musi odbywa się w regułach polityki bezpieczeństwa. System firewall musi realizować zadania IPS z wydajnością nie mniejszą niż **400 Mb/s** dla rekomendowanej przez producenta polityki IPS. Baza sygnatur IPS musi być utrzymywana i udostępniana przez producenta urządzenia firewall. Baza sygnatur ataków musi być aktualizowana przez producenta codziennie.	

		Tablica adresów MAC musi mieć możliwość przechowywania minimum 15000 wartości. Urządzenie musi posiadać mechanizmy priorytetyzowania i zarządzania ruchem sieciowym QoS – wygładzanie (shaping) oraz obcinanie (policing) ruchu. Mapowanie ruchu do kolejek wyjściowych musi odbywać się na podstawie DSCP, IP ToS, 802.1p, oraz parametrów z nagłówków TCP i UDP. Urządzenie musi posiadać tworzenia osobnych kolejek dla różnych klas ruchu. Urządzenie musi posiadać zaimplementowany mechanizm WRED w celu przeciwdziałania występowaniu przeciążeń w kolejkach. Firewall musi posiadać możliwość pracy w konfiguracji odpornej na awarie dla urządzeń zabezpieczeń Urządzenia zabezpieczeń w klastrze muszą funkcjonować w trybie Active-Passive z synchronizacją konfiguracji i tablicy stanu sesji. Przełączenie pomiędzy urządzeniami w klastrze HA musi się odbywać przezroczyście dla sesji ruchu użytkowników. Mechanizm ochrony przed awariami musi monitorować i wykrywać uszkodzenia elementów sprzętowych i programowych systemu zabezpieczeń oraz łączy sieciowych. Zarządzanie urządzeniem musi odbywać się za pomocą graficznej konsoli Web GUI oraz z wiersza linii poleceń (CLI) poprzez port szeregowy oraz protokoły telnet i SSH. Firewall musi posiadać możliwość zarządzania i monitorowania przez centralny system zarządzania i monitorowania pochodzący od tego samego producenta. Administratorzy muszą mieć do dyspozycji mechanizm szybkiego odtwarzania systemu i przywracania konfiguracji. W urządzeniu musi być przechowywanych nie mniej niż **5** poprzednich, kompletnych konfiguracji. Pomoc techniczna musi być świadczone są w języku polskim.	
6	**Zabezpieczenia**	**Musi posiadać wbudowany moduł kontroli antywirusowej kontrolujący pocztę elektroniczną (SMTP, POP3, IMAP), FTP oraz HTTP. Włączenie kontroli antywirusowej nie może wymagać dodatkowego serwera Kontrola antywirusowa musi być realizowana sprzętowo. Musi istnieć możliwość wyboru działania mechanizmu kontroli antywirusowej w trybie sprzętowym i programowym.** **Urządzenie zabezpieczeń musi posiadać**	

		wbudowany moduł kontroli antyspamowej działający w oparciu o mechanizm blacklist. Włączenie kontroli antyspamowej nie może wymagać dodatkowego serwera. **Urządzenie zabezpieczeń musi posiadać wbudowany moduł filtrowania stron WWW w zależności od kategorii treści stron. Włączenie filtrowania stron WWW nie może wymagać dodatkowego serwera.** **Urządzenie zabezpieczeń musi posiadać funkcję filtrowania zawartości ruchu HTTP, FTP i protokołów poczty elektronicznej (SMTP, POP3, IMAP) w celu blokowania potencjalnie szkodliwych obiektów. Urządzenie musi filtrować ruch na podstawie kryteriów obejmujących co najmniej: typy MIME, rozszerzenia plików, elementy ActiveX, Java i cookies.**	
7	**Protokoły**	Urządzenie musi obsługiwać protokoły dynamicznego rutingu: RIP, OSPF oraz BGP**. Urządzenie musi umożliwiać skonfigurowanie nie mniej niż 60 wirtualnych ruterów. Tablica rutingu powinna umożliwiać utrzymanie 1 milion wpisów routingu natomiast tablica forwardingu minimum 600 000 tras.** **Urządzenie musi posiadać możliwość uruchomienia funkcji MPLS z sygnalizacją LDP i RSVP w zakresie VPLS i L3 VPN.** **Urządzenie musi obsługiwać co najmniej 2000 sieci VLAN z tagowaniem 802.1Q. W celu zapobiegania zapętlania się ruchu w warstwie 2 firewall musi obsługiwać protokoły Spanning Tree (802.1D), Rapid STP (802.1W) oraz Multiple STP (802.1S). Urządzenie musi obsługiwać protokół LACP w celu agregowania fizycznych połączeń Ethernet.**	
8	**Gwarancja**	Minimalnie 36 miesięcy gwarancji producenta, bądź partnera serwisowego oraz opieki technicznej ważnej przez okres **trzech lat** Opieka powinna zawierać wsparcie techniczne świadczone telefonicznie oraz pocztą elektroniczną przez producenta oraz polskiego dystrybutora sprzętu, wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych. **Wsparcie powinno zawierać usługę wymiany uszkodzonego sprzętu w reżimie „następny dzień roboczy”**	

9	**Licencje**	**Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność Application Security na okres 3 lat** **Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność IPS na okres 3 lat** **Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność AntiVirus na okres 3 lat** **Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność URL Filtering na okres 3 lat** **Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność Antispam na okres 3 lat** **Urządzenie musi zostać dostarczone wraz z licencją (lub subskrypcją) na funkcjonalność Dynamic VPN na 10 jednoczesnych użytkowników na bezterminowy okres**	
11	**Wdrożenie /szkolenia**	Wymagane jest zapewnienie szkolenia z zakresu konfiguracji i zarządzania urządzenia. Szkolenie powinno być przeprowadzone dla **minimum 3 osób** w języku polskim.	

……dn……

……
podpis i pieczęć uprawnionego przedstawiciela Wykonawcy

29/PNP/SW/2020 Załącznik nr 1 do SIWZ

Część 3
Switch agregacyjny 10Gb

Nazwa sprzętu: ……

Model: ……

Typ: ……

Producent: ……

Rok produkcji: nie starszy niż **2020** (sprzęt fabrycznie nowy nieużywany , nierekondycjonowany)

Lp.	Parametr	Wymagane minimalne parametry techniczne	Parametry oferowane PODAĆ/OPISAĆ
1	**Obudowa**	Obudowa typu Rack o wysokości 1U;	
2	**Interfejs**	Przynajmniej: - 48 portów 1GbE; - 4 porty SPF+ 10 GbE; Opcjonalnie port/porty QSFP+ 40GbE; Przynajmniej 4 moduły SFP w zestawie.	
3	**Funkcje**	Maksymalna szybkość przesyłania danych powyżej: 288 Gbps; Wydajność powyżej 200 Mpps; Nadmiarowe zasilacze z możliwością wymiany na miejscu; Nadmiarowe grupy łączy trunk, które zapewniają nadmiarowość portów i upraszczają konfigurację przełącznika; Kolejki/porty QoS: 8 unicast/4 multicast; Tablica adresów MAC: przynajmniej 8 000; Funkcja MDI/MDX; Wsparcie dla bramek Jumbo Frames: 9216 b Obsługa POE.	
4	**Gwarancja**	Switch musi zostać dostarczony z co najmniej 1 rocznym wsparciem technicznym producenta obejmującym: dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (Next Business Day Advanced Hardware Replacement Services (NBD AHR)). Wsparcie techniczne musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Switch musi być objęty dożywotnią gwarancją producenta (Limited Lifetime Warranty) obejmującą dostarczenie sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (Next Business Day	

		Advanced Hardware Replacement Services (NBD AHR)). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego.	

……dn……

……
podpis i pieczęć uprawnionego przedstawiciela Wykonawcy

29/PNP/SW/2020 Załącznik nr 1 do SIWZ

Część 4
Komputer

Nazwa sprzętu: ……..

Model: ……..

Typ: ……

Rok produkcji: nie starszy niż **2020** (sprzęt fabrycznie nowy nieużywany , nierekondycjonowany)

Producent: ……..

Lp.	Parametr	Wymagane minimalne parametry techniczne	Parametry oferowane PODAĆ/OPISAĆ
1	**Procesor**	Procesor 6-rdzeniowy, 12-wątkowy, taktowany częstotliwością 3,3 GHz (4.8 GHz w trybie turbo), wyposażony w 12MB pamięć podręczną. Wyposażony w dedykowany system chłodzenia.	
2	**Pamięć RAM**	16GB, DDR4. Możliwość rozbudowy do pojemności 128GB.	
4	**Pamięć masowa**	SATA SSD, pojemność 1TB, M.2 pojemność 256GB. Możliwość montażu dysków min. 2 SATA SSD	
5	**Płyta główna**	**Moduł TPM.** **Porty i łącza** 2 x USB 2.0 w panelu frontowym, 2 x USB 3.0 w panelu frontowym, 4 x USB 3.1 generacji 1 (USB 3.0) w tylnej części obudowy, 2 x USB 3.1 generacji 2 w tylnej części obudowy, 1 x HDMI w tylnej części obudowy, 1 X RJ45 (LAN 1 GB) w tylnej części obudowy, **Wewnętrzne złącza** 6 x SATA III (6 Gb/s), 2 x M.2, 3 x PCIe 3.0 x16 3 x PCIe 3.0 x1	
6	**Karta graficzna**	Pamięć 4GB 2 x HDMI, 2 x DVI (opcjonalnie).	
7	**Zasilacz**	Wyposażone w zintegrowany system chłodzenia. Minimalna moc zasilacza wynosi 750W. Zabezpieczenie przed zbyt wysokim prądem (OCP), przeciwprzeciążeniowe (OPP), termiczne (OTP), przeciwprzepięciowe (OVP), przeciwzwarciowe (SCP), przed zbyt niskim napięciem (UVP). Typ okablowania Modularny, elementy montażowe w	

		zestawie.	
8	**Obudowa**	Obudowa dedykowana do zestawu z możliwością rozbudowy podzespołów	
9	**Wyposażenie dodatkowe**	Nagrywarka DVD, Karta sieciowa 1 x 2 porty RJ-45 1GB PCIe	
10	**Oprogramowanie**	System operacyjny w architekturze x64, umożliwiający integrację z posiadanym przez zamawiającego systemem, pozwalającym na wdrożenie jednolitej polityki bezpieczeństwa dla wszystkich komputerów w sieci, instalację oprogramowania biurowego MS Office 2019 lub równoważnych. System winien posiadać publicznie znany cykl życia przedstawiony przez producenta i dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa. System musi gwarantować współpracę z posiadanymi systemami medycznymi zamawiającego. Pakiet oprogramowania biurowego współpracujący z systemem zamawiającego, z obsługą baz danych oraz chmurowego przechowywania danych.	
11	**Gwarancja**	Gwarancja 36 miesięcy. Brak wymogu odsyłania dysku twardego - w przypadku awarii pozostaje u Zamawiającego.	

Warunki równoważności:

1. Współpraca z procesorami o architekturze x86-64.
2. Instalacja i użytkowanie aplikacji 32-bit. i 64-bit. na dostarczonym systemie operacyjnym. Obsługa 64 procesorów fizycznych oraz co najmniej 64 procesorów logicznych (wirtualnych).

.....dn.....

.....
podpis i pieczęć uprawnionego przedstawiciela Wykonawcy

29/PNP/SW/2020 Załącznik nr 1 do SIWZ

Część 5
Szyna Integracyjna - Enterprise Service Bus

Nazwa sprzętu: ……

Model: ……

Typ: ……

Producent: ……

Rok produkcji: nie starszy niż **2020** (sprzęt fabrycznie nowy nieużywany , nierekondycjonowany)

Lp.	Parametr	Wymagane minimalne parametry techniczne	Parametry oferowane PODAĆ/OPISAĆ
1	**Funkcje**	Szyna ESB musi posiadać mechanizm definiowania, implementacji, wdrażania i zarządzania usługami realizującymi dostęp do integrowanych systemów. Usługi mogą być elementarne, tworzone jako konfiguracja pewnych modułów lub posiadać większą logikę integracyjną (np. sekwencja wywołania kilku usług). Założenie istnienie usług prywatnych i publicznych. Usługi prywatne są dostępne jedynie w obrębie platformy integracyjnej i nie mogą być bezpośrednio wywoływane przez klientów systemu. Ich zadaniem jest realizowanie atomowych operacji, z których budowane są usługi publiczne. Usługi publiczne są widoczne dla klientów platformy integracyjnej poprzez: 1) punkt dostępu do usługi stanowiący adres sieciowy usług w ramach infrastruktury ESB; 2) punkt dostępu do definicji usługi (adres URL) - stanowiący adres sieciowy dokumentu WSDL opisującego usługę. Każda usługa realizuje konkretny scenariusz (proces) integracyjny. Wspólnym protokołem komunikacyjnym usług publicznych i prywatnych musi być SOAP, a protokołem transportowym HTTPS. W przypadku komunikacji asynchronicznej wspólnym protokołem transportowym musi być transport oparty o kolejki (np. JMS). Funkcjonalność tworzona w ramach szyny usług musi być udostępniana w postaci atomowych usług. Oprogramowanie szyny usług musi posiadać mechanizm umożliwiający planowe i cykliczne uruchamianie usług platformy. Zarządzanie planowanymi do uruchomienia usługami musi odbywać się w sposób spójny z jednego miejsca platformy na zasadzie definiowania harmonogramu wywołań. Szyna musi zapewniać pełne wsparcie obsługi dokumentów XML. W ramach obsługi dokumentów XML, ESB musi wspierać możliwość: 1) tworzenia i	

		parsowania komunikatów XML, 2) walidacji komunikatów na podstawie definicji XMLSchema i DTD, 3) obsługi dużych dokumentów XML (do 100MB), 4) transformacji komunikatów – dokument XML na inny dokument XML oraz pomiędzy dokumentem XML i innym formatem (w obie strony), 5) poprawnej obsługi stron kodowych obsługujących polskie znaki. W ramach obsługi protokołu SOAP i Web Services dla usług konsumowanych jak i udostępnianych ESB musi zapewniać: 1) możliwość konsumowania oraz udostępniania usług w standardzie webservices (WSDL 1.1, SOAP 1.1 i 1.2, SOAP with Attachements); 2) zgodność ze standardem WS-Security; 3) zgodność ze standardem WS-Policy; 4) wsparcie innych standardów WS określonych specyfikacjami konsorcjum OASIS (http://www.oasis-open.org); Musi dostarczać usługi transformacji komunikatów XML w modelach jeden do wielu i wiele do jednego, co najmniej przy wykorzystaniu języka XSLT 1.0 (XSL Transformations, Extensible Stylesheet Language Transformations). Musi dostarczać: usługi translacji danych; usługi translacji protokołów pozwalające na podłączanie usług według różnych protokołów. Musi zapewniać dowolne łączenie obsługiwanych protokołów między sobą i umożliwiać routing komunikatów, oparty na treści dokumentów XML i regułach biznesowych. Szyna musi umożliwiać filtrowanie komunikatów na podstawie zawartości, przy wykorzystaniu parametrów definiowanych przez użytkownika. ESB musi umożliwiać realizację procesów integracyjnych w oparciu o model synchroniczny i asynchroniczny. ESB musi umożliwiać trwałe przechowywanie komunikatów pod warunkiem, że nie prowadzi to do zbytniego obciążenia systemu. ESB musi umożliwiać tworzenie architektury wyjątków, która może przechwytywać wyjątki, generować transakcje kompensacyjne i generować raporty o błędach. Katalog raportów zostanie określony przez Wykonawcę na podstawie wyników analizy biznesowej realizowanej w ramach opracowania planu realizacji projektu. ESB musi umożliwiać odtworzenie stanu systemu sprzed awarii. Odtworzenie obejmuje całość działań, jakie trzeba wykonać aby system funkcjonował zgodnie z założeniami w szczególności: konfigurację szyny, serwera aplikacyjnego, na którym działa, systemu operacyjnego, powiązanych baz danych oraz wszystkich innych elementów systemu e-Urząd umożliwiających bezawaryjną pracę systemu.	

		Szyna ma umożliwiać nadawanie priorytetu komunikatom w warstwie transportowej (komunikacja asynchroniczna). W szczególności ESB musi obsługiwać nadawanie priorytetów komunikatom na podstawie treści komunikatu. ESB musi także umożliwiać zmianę wielkości puli wątków (per usługa) obsługujących synchroniczne żądania http. ESB musi wspierać orkiestrację usług.	
2	**Bezpieczeństwo**	Wsparcie dla co najmniej następujących standardów komunikacji: SOAP, JMS, JCA, HTTP, HTTPS, FTP, SFTP. ESB musi umożliwiać zarządzanie transakcjami w procesach biznesowych. Warstwa komunikacyjna ESB musi umożliwiać zachowanie: 1) integralności; 2) niezaprzeczalności; 3) poufności; 4) autentyczności komunikacji. Szyna musi umożliwiać raportowanie informacji o incydentach w zakresie bezpieczeństwa w szczególności nieuprawnionego logowania i informowania o incydentach na szynie. Bezpieczeństwo usług zbudowanych w oparciu o technologię Web Services musi bazować na standardzie OASIS WS-S (Web Services Security). ESB musi umożliwiać szyfrowanie i podpisywanie komunikatów XML zgodnie z obowiązującymi przepisami. ESB musi umożliwiać podpisywanie komunikatów XML zgodnie ze standardem Advanced Electronic Signature (XAdES). Minimalna długość klucza szyfrującego w przypadku zastosowania algorytmów symetrycznych musi wynosić 128 bitów, natomiast w przypadku zastosowania algorytmów asymetrycznych - 1024 bity. ESB musi umożliwiać weryfikację statusu unieważnienia certyfikatu poprzez mechanizm CRL. ESB musi umożliwiać weryfikację statusu certyfikatu poprzez mechanizm OCSP.	
3	**Integracja i komunikacja**	Możliwość integracji relacyjnych baz danych na poziomie danych i wywoływania procedur bazodanowych. ESB musi umożliwiać integrację aplikacji zbudowanych w technologiach J2EE, .Net. Szyna musi integrować się z Centrami Certyfikacji w zakresie: - weryfikacji ważności certyfikatów kwalifikowanych wystawionych przez centrum, - cyklicznej aktualizacji list CRL. Dostarczone rozwiązanie musi implementować funkcje szyny danych, tj.: komponentu pozwalającego na udostępnianie w postaci usług Web Services danych zgromadzonych w wielu bazach danych. Dostarczony moduł szyny danych musi posiadać	

		wsparcie dla minimalnie następujących baz danych: Microsoft SQL Server, Oracle, PostgreSQL. Szyna ESB musi zapewniać komunikację oraz wymianę danych także w odniesieniu do danych przestrzennych. Mają tu zastosowanie bieżące standardy opublikowane Open Geospatial Consortium (OGC) i wykorzystywane przez Wykonawcę do realizacji przedmiotu zamówienia dotyczące: OpenGIS Geographic Objects Implementation Specification GML Specification; OpenGIS Geography Markup Language (GML) Encoding Standard ver. 3.2.1; Web Coverage Processing Service schema WCS - Web Coverage Service; Web Coverage Service (WCS) Implementation Standard; OpenGIS Web Feature Service (WFS) OpenGIS Web Map Service (WMS) Implementation Specification OpenGIS Web Map Tile Service Implementation Standard (WMTS) Implementation Specification Oprogramowanie musi być zgodne ze standardami: 1) WSDL 1.1; 2) SOAP 1.2; 3) SOAP with Attachments; 4) UDDI 3.0. Szyna ESB musi zawierać przygotowana interfejsy do podłączenia systemów Zamawiającego, a w szczególności HIS, PACS Infinitt i dostarczonego systemu RIS	
4	**Wdrożenie i szkolenia**	Wykonawca zapewni wsparcie w zakresie szkolenia dla wybranych pracowników Zamawiającego (6 osób) obejmującego pełny zakres (instalację, administrację, optymalizację) dotyczący proponowanego rozwiązania Szyny Usług.	

……dn……

……
podpis i pieczęć uprawnionego przedstawiciela Wykonawcy