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

Załącznik nr 6 do Opisu Przedmiotu Zamówienia

Specyfikacja wymagań dla ITS

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

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

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

SPIS TREŚCI

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

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

Wymagania dla ITS

Wymagania dla środowiska aplikacyjnego

Zamawiający wymaga, aby platforma aplikacyjna (środowisko serwera aplikacji, SA) wymagana w rozwiązaniu spełniała następujące warunki.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.001	Oprogramowanie serwera aplikacyjnego (SA) zapewni realizację odpowiedniego poziomu bezpieczeństwa w zakresie: • uwierzytelniania • kontroli dostępu • zarządzania użytkownikami, grupami i rolami • tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy • audytowania zdarzeń bezpieczeństwa • wsparcia dla pojedynczego logowania SSO
WYM.OPZ.ITS.002	Oprogramowanie (SA) zapewni zgodność ze standardami WS-* a w szczególności z WS-Security, WS-Policy.
WYM.OPZ.ITS.003	Oprogramowanie (SA) zapewni dostępność mechanizmów uwierzytelniania i szyfrowania usług takich jak: użytkownik/hasło, passphrase, weryfikacja hostów, brak uwierzytelniania, tunelowanie wywołań SSL, certyfikaty X.509
WYM.OPZ.ITS.004	Oprogramowanie (SA) będzie umożliwiało integrację w oparciu o standardy EJB 3.0 oraz Spring Framework.
WYM.OPZ.ITS.005	Oprogramowanie (SA) będzie wspierało współdzielenie kodu (np. bibliotek) pomiędzy wieloma aplikacjami (Web, EJB, Web services). Biblioteki (JAR, WAR, EAR, EJB) powinny być instalowane w serwerze aplikacyjnym jednokrotnie i wiele aplikacji powinno mieć możliwość skorzystania z nich. Oprogramowanie powinno zapewniać możliwość zainstalowania wielu wersji bibliotek równocześnie, a także możliwość konfiguracji, która wersja biblioteki będzie wykorzystywana przez aplikację. Konfiguracja powinna odbywać się w sposób deklaratywny (za pomocą deployment deskryptor'ów) – nie poprzez kopiowanie kodu bibliotek do aplikacji. Przykład – wiele implementacji JSF działających równocześnie w serwerze aplikacyjnym.
WYM.OPZ.ITS.006	Oprogramowanie (SA) musi zawierać wbudowaną obsługę żądań HTTP w sposób asynchroniczny (czyli możliwość rozdzielenia obsługi *HTTP request* i *HTTP response* na różne wątki).

Wymaganie	Opis wymagania
WYM.OPZ.ITS.007	Oprogramowanie (SA) musi wspierać przechowywanie (persistence) sesji webowych i EJB w pliku, bazie danych lub pamięci.
WYM.OPZ.ITS.008	Oprogramowanie (SA) umożliwi przechowywanie istotnych informacji dotyczących sesji użytkownika (w tym sesja http, konteksty usług typu Servlet oraz konteksty usług typu Session EJB) w zewnętrznej pamięci cache poza głównym procesem maszyny wirtualnej Java. Oprogramowanie musi umożliwiać mechanizmy klastrowania aplikacji w powyższy sposób, czyli z wykorzystaniem cache'a zewnętrznego.
WYM.OPZ.ITS.009	Oprogramowanie (SA) powinno zapewnić możliwość zaprogramowania automatycznego restartu węzła i/lub komponentu w sytuacji zawieszenia (braku odpowiedzi), pojawienia się błędów o braku pamięci lub zbyt długiego wykonywania się wątków (stuck threads).
WYM.OPZ.ITS.010	Oprogramowanie (SA) powinno zapewnić możliwość ograniczenia liczby sesji HTTP w serwerze tworzonych przez daną aplikację.
WYM.OPZ.ITS.011	Oprogramowanie (SA) powinno zawierać wbudowaną możliwość klastrowania połączeń JDBC.
WYM.OPZ.ITS.012	Oprogramowanie (SA) powinno zawierać wbudowaną możliwość klastrowania JMS (w tym automatyczne przełączanie klientów JMS w momencie failover serwerów JMS)
WYM.OPZ.ITS.013	Oprogramowanie (SA) powinno zapewnić możliwość automatycznego i ręcznego restartu (migracji) instancji serwerów aplikacyjnych na innych fizycznych maszynach w razie awarii, wraz z przeniesieniem istotnych dla przetwarzania danych (np. zawartość kolejek (np. JMS, MQSeries), logi transakcji rozproszonych JTA). Automatyczna rekonfiguracja serwerów aplikacyjnych po restarcie (zmiana adresu IP, itp.)
WYM.OPZ.ITS.014	Oprogramowanie (SA) powinno zawierać wbudowane wsparcie dla specyfikacji JSR-88 – Deployment Plan (plany wdrożeń).
WYM.OPZ.ITS.015	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę wprowadzania zmian w kodzie Java w aplikacjach na serwerze bez konieczności redeployment'u aplikacji ani restartu serwera aplikacyjnego (hot Java class swapping)
WYM.OPZ.ITS.016	Wprowadzanie zmian w konfiguracji środowiska serwerów aplikacyjnych powinno odbywać się w sposób transakcyjny (albo wszystkie zmiany zostaną poprawnie wprowadzone albo żadna zmiana nie będzie wprowadzona).
WYM.OPZ.ITS.017	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę pul połączeń do baz danych z uwierzytelnieniem połączeń. Tworzenie pul połączeń JDBC, w których jest możliwość zmapowania użytkowników serwera aplikacyjnego na użytkowników zdefiniowanych w bazie danych. Powinna być możliwość wykonania mapowania typu

Wymaganie	Opis wymagania
	„user id per connection”.
WYM.OPZ.ITS.018	Oprogramowanie (SA) powinno mieć wbudowaną obsługę zaawansowanych mechanizmów kolejkowych: grupowanie komunikatów przesyłanych do JMS z gwarancją zachowania kolejności ich przetworzenia (konsumpcji) wynikającą z kolejności ich utworzenia (produkcji).
WYM.OPZ.ITS.019	Oprogramowanie (SA) powinno zawierać opisaną w dokumentacji (wraz z przykładami) możliwość tworzenia własnych implementacji usług security: uwierzytelnienia, autoryzacji, mapowania ról, mapowania uwierzytelnień, baz danych kluczy/certyfikatów, walidacji poprawności kluczy/certyfikatów, audytowania.
WYM.OPZ.ITS.020	Oprogramowanie (SA) powinno zapewniać obsługę specyfikacji: • Java Authentication and Authorization Service (JAAS), • Java Secure Sockets Extensions (JSSE), • Java Cryptography Extensions (JCE), • Java Authorization Contract for Containers (JACC)
WYM.OPZ.ITS.021	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardów SAML 1.1, SAML 2.0 lub wyższych.
WYM.OPZ.ITS.022	Oprogramowanie (SA) powinno zawierać wbudowane API do funkcjonalności przeszukiwania i walidacji certyfikatów X.509.
WYM.OPZ.ITS.023	Oprogramowanie (SA) powinno zapewnić obsługę mechanizmów autoryzacji i mapowania ról przy użyciu standardu XACML 2.0.
WYM.OPZ.ITS.024	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardu web services WS-ReliableMessaging 1.1 i WS-ReliableMessaging Policy 1.1.
WYM.OPZ.ITS.025	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardu web services WS-Trust 1.3.
WYM.OPZ.ITS.026	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardu web services WS-SecureConversation 1.3.
WYM.OPZ.ITS.027	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardu web services WS-Security 1.1.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.028	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę standardu web services WS-SecurityPolicy 1.2.
WYM.OPZ.ITS.029	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę asynchronicznych Web services (klient Web service, po wywołaniu Web service, nie musi zatrzymać się w oczekiwaniu na odpowiedź z Web service'u. Odpowiedź jest asynchronicznie przekazywana do klienta w późniejszym czasie).
WYM.OPZ.ITS.030	Oprogramowanie (SA) powinno zawierać wbudowaną obsługę Web services, które mogą wykonywać operacje na kliencie (callback Web service).
WYM.OPZ.ITS.031	Oprogramowanie (SA) powinno zawierać wbudowany moduł do diagnostyki pracy serwera aplikacyjnego i uruchomionych w nim aplikacji. Możliwość dynamicznego dodawania poprzez konfigurację własnego kodu diagnostycznego do określonych miejsc w aplikacji i jej komponentach.

Wymagania dla Szyny Usług

Szyna usług posiada własne repozytorium służące do definicji kolejek, procedur, funkcji, komunikatów oraz parametrów transferu danych. Jest odpowiedzialna za uwierzytelnianie każdej operacji wykonywanej w ramach systemu. Szczególnie wspomaga ona komunikację pomiędzy modułem prezentacji (portalem) a resztą modułów systemu.
Szyna usług powinna posiadać możliwość przetwarzania sekwencyjnego jak i równoległego komunikatów modułów systemu, z możliwością powtórzeń operacji, których wykonanie z jakiś przyczyn nie powiodło się. W przypadku wystąpienia błędów w trakcie przetwarzania komunikatów przez szynę usług, błędy te powinny być w sposób prosty identyfikowane, poprzez przypisanie ich do: nazwa modułu, nazwa obiektu, metoda, czas wystąpienia błędu. Szyna Usług jest krytycznym elementem systemu, przerwanie jej pracy powoduje awarię całego systemu, dlatego tez wymaga się, aby posiadała ono możliwość działania w trybie „fault tolerant".

Wymaganie	Opis wymagania
WYM.OPZ.ITS.032	Oprogramowanie będzie zgodne ze standardami: • WSDL 1.x lub wyższe • SOAP 1.2 • SOAP with Attachments • UDDI 3.0
WYM.OPZ.ITS.033	Oprogramowanie umożliwi projektowanie bezstanowych procesów biznesowych.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.034	Oprogramowanie umożliwi realizację bezstanowych ale długotrwałych procesów zależnych od wielu usług – agregacja usług.
WYM.OPZ.ITS.035	Oprogramowanie umożliwi implementację wywołania innych usług wraz z translacją komunikatów.
WYM.OPZ.ITS.036	Oprogramowanie umożliwi zdefiniowanie reguł wywołania usługi.
WYM.OPZ.ITS.037	Oprogramowanie umożliwi ograniczenie wywołań usług, ochronę wydajności adapterów oraz zajętości kolejek.
WYM.OPZ.ITS.038	Oprogramowanie umożliwi implementację komunikacji bezpośredniej pomiędzy systemami dziedzinowymi na podstawie posiadanych adapterów.
WYM.OPZ.ITS.039	Oprogramowani umożliwi transformację danych, transformację komunikatów np. XPath/XSLT/XQuery.
WYM.OPZ.ITS.040	Oprogramowanie umożliwi wzbogacanie transformacji danych o warunki logiczne lub ograniczenia.
WYM.OPZ.ITS.041	Oprogramowanie będzie wspierało transformację danych poza strukturą XML np. plików tekstowych.
WYM.OPZ.ITS.042	Oprogramowanie będzie obsługiwało wiele warstw transportowych np.: JMS, HTTP, MQ, FTP, TCP.
WYM.OPZ.ITS.043	Oprogramowanie umożliwi monitorowanie poprawnej pracy usług.
WYM.OPZ.ITS.045	Oprogramowanie zapewni wsparcie w zakresie realizacji testów wydajnościowych i funkcjonalnych: zaślepki, symulatory, skrypty automatyzujące testy, konsola wywoływania ręcznego usług.
WYM.OPZ.ITS.046	Oprogramowanie będzie wspierało transformację komunikatów, na podstawie przykładowej wymiany plików XML przekazywanych transportem FTP i na podstawie zawartych w nim danych wywoływanie odpowiednich usług.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.047	Oprogramowanie będzie zawierało opis proponowanego systemu kolejkowego, możliwości w zakresie ustanawiania QoS dla: usług, kolejek, komunikatów w kolejkach.
WYM.OPZ.ITS.048	Oprogramowanie zapewni realizację odpowiedniego poziomu bezpieczeństwa w zakresie: • uwierzytelniania • kontroli dostępu • zarządzania użytkownikami, grupami i rolami • tworzenia, przechowywania i walidacji certyfikatów, haseł, kluczy • audytowania zdarzeń bezpieczeństwa • wsparcia dla pojedynczego logowania SSO
WYM.OPZ.ITS.049	Oprogramowanie zapewni zgodność ze standardami WS-* a w szczególności z WS-Security, WS-Policy.
WYM.OPZ.ITS.050	Oprogramowanie zapewni dostępność mechanizmów uwierzytelniania i szyfrowania usług np. takich jak: użytkownik/hasło, passphrase, weryfikacja hostów, brak uwierzytelniania, tunelowanie wywołań SSL, certyfikaty X.509.
WYM.OPZ.ITS.051	Oprogramowanie zapewni możliwość ograniczenia czasu wywołań dla usług oraz użycia adapterów.
WYM.OPZ.ITS.052	Oprogramowanie będzie zawierało zestawienie adapterów do systemów i standardów zewnętrznych np: NetBios, NFS, pliki lokalne, HTTP, SMTP, FTP, JMS, MQ, JDBC, EDI, Oracle, DB2.
WYM.OPZ.ITS.053	Oprogramowanie zapewni obsługę komunikatów typu np.: SOAP, XML, FTP, SMTP.
WYM.OPZ.ITS.054	Oprogramowanie zapewni obsługę komunikatów typu np.: SOAP, XML, FTP, SMTP.
WYM.OPZ.ITS.055	Oprogramowanie zapewni możliwość eksportu ustawień konfiguracyjnych i importu na innej instancji Szyny Usług.
WYM.OPZ.ITS.056	Oprogramowanie Szyny Usług będzie oparte o serwer aplikacji zgodny ze standardem JEE (Java Enterprise Edition).

Wymaganie	Opis wymagania
WYM.OPZ.ITS.057	Oprogramowanie będzie umożliwiało integrację w oparciu o standardy EJB 3.0 oraz Spring Framework.
WYM.OPZ.ITS.058	Oprogramowanie zapewni wsparcie dla replikacji sesji w pamięci pomiędzy wieloma instancjami węzłów Szyny Usług przy zapewnieniu wysokiej wydajności oraz możliwość replikacji sesji w trybie primary-secondary (czyli zarządzanie maksymalnie dwiema kopiami sesji użytkownika w klastrze).
WYM.OPZ.ITS.059	Oprogramowanie powinno mieć możliwość konfiguracji priorytetów obsługi żądań, priorytetów aplikacji i ich komponentów. Możliwość przypisywania reguł do użytkowników, aplikacji i ich komponentów (np. servlet'ów, EJB). Reguły powinny obejmować takie cechy jak: wagi (priorytety – np. % czasu procesorów gwarantowany dla aplikacji i/lub ich komponentów), czasy odpowiedzi, min/max liczba wątków, itp.
WYM.OPZ.ITS.060	Oprogramowanie powinno zawierać wbudowaną możliwość konfiguracji ochrony serwerów aplikacyjnych (i aplikacji) przed przeciążeniem. Dla przykładu: jeśli liczba żądań do serwera/aplikacji jest zbyt duża, serwer powinien przekierować nowe żądania do innych instancji w klastrze.
WYM.OPZ.ITS.061	Oprogramowanie powinno zapewnić możliwość zaprogramowania automatycznego restartu węzła i/lub komponentu w sytuacji zawieszenia (braku odpowiedzi), pojawienia się błędów o braku pamięci lub zbyt długiego wykonywania się wątków (stuck threads).
WYM.OPZ.ITS.062	Oprogramowanie powinno zawierać wbudowaną możliwość klastrowania połączeń JDBC.
WYM.OPZ.ITS.063	Oprogramowanie powinno zawierać wbudowaną możliwość klastrowania JMS (w tym automatyczne przełączanie klientów JMS w momencie failover serwerów JMS).
WYM.OPZ.ITS.064	Oprogramowanie powinno zapewnić możliwość automatycznego i ręcznego restartu (migracji) instancji serwerów aplikacyjnych na innych fizycznych maszynach w razie awarii, wraz z przeniesieniem istotnych dla przetwarzania danych (np. zawartość kolejek (np. JMS, MQSeries)), logi transakcji rozproszonych). Automatyczna rekonfiguracja serwerów aplikacyjnych po restarcie (zmiana adresu IP, itp.).
WYM.OPZ.ITS.065	Oprogramowanie powinno zawierać wbudowane wsparcie dla specyfikacji JSR-88 – Deployment Plan (plany wdrożeń).
WYM.OPZ.ITS.066	Oprogramowanie powinno zawierać wbudowaną obsługę pul połączeń do baz danych z uwierzytelnieniem połączeń. Tworzenie pul połączeń JDBC, w których jest możliwość zmapowania użytkowników serwera aplikacyjnego na użytkowników zdefiniowanych w bazie danych. Powinna być możliwość wykonania mapowania typu „user id per connection".

Wymaganie	Opis wymagania
WYM.OPZ.ITS.067	Oprogramowanie powinno mieć wbudowaną obsługę zaawansowanych mechanizmów kolejkowych: grupowanie komunikatów przesyłanych do JMS z gwarancją zachowania kolejności ich przetworzenia (konsumpcji) wynikającą z kolejności ich utworzenia (produkcji).
WYM.OPZ.ITS.068	Oprogramowanie powinno zapewnić wsparcie w zakresie wywołań i komunikacji z aplikacjami napisanych w języku innym niż JAVA np. C, .Net, C#.
WYM.OPZ.ITS.069	Oprogramowanie powinno zawierać wbudowany mechanizm automatycznej naprawy transakcji (transaction recovery) podczas restartu serwera aplikacyjnego.
WYM.OPZ.ITS.070	Oprogramowanie powinno zawierać opisaną w dokumentacji (wraz z przykładami) możliwość tworzenia własnych implementacji usług security: uwierzytelnienia, autoryzacji, mapowania ról, mapowania uwierzytelnień, baz danych kluczy/certyfikatów, walidacji poprawności kluczy/certyfikatów, audytowania.
WYM.OPZ.ITS.071	Oprogramowanie powinno zapewniać obsługę specyfikacji: • Java Authentication and Authorization Service (JAAS), • Java Secure Sockets Extensions (JSSE), • Java Cryptography Extensions (JCE), • Java Authorization Contract for Containers (JACC)
WYM.OPZ.ITS.072	Oprogramowanie powinno zawierać wbudowaną obsługę standardów SAML 1.1, SAML 2.0 lub wyższych.
WYM.OPZ.ITS.073	Oprogramowanie powinno zawierać API do funkcjonalności przeszukiwania i walidacji certyfikatów X.509.
WYM.OPZ.ITS.074	Oprogramowanie powinno zapewnić możliwość konfiguracji dynamicznego członkostwa ról, np. uwzględniającego datę i czas, zawartość wybranych elementów w komunikatach SOAP (Web services), wartość atrybutów żądań HTTP, wartość atrybutów sesji HTTP, czy parametrów metod EJB.
WYM.OPZ.ITS.075	Oprogramowanie powinno zawierać obsługę standardu Common Secure Interoperability Version 2 (CSIv2).
WYM.OPZ.ITS.076	Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-ReliableMessaging 1.1 i WS-ReliableMessaging Policy 1.1.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.077	Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-Trust 1.3.
WYM.OPZ.ITS.078	Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-SecureConversation 1.3.
WYM.OPZ.ITS.079	Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-Security 1.1.
WYM.OPZ.ITS.080	Oprogramowanie powinno zawierać wbudowaną obsługę standardu web services WS-SecurityPolicy 1.2.
WYM.OPZ.ITS.081	Oprogramowanie powinno zawierać wbudowaną obsługę asynchronicznych Web services (klient Web service, po wywołaniu Web service, nie musi zatrzymać się w oczekiwaniu na odpowiedź z Web service'u. Odpowiedź jest asynchronicznie przekazywana do klienta w późniejszym czasie).
WYM.OPZ.ITS.082	Oprogramowanie powinno zawierać wbudowaną obsługę Web services, które mogą wykonywać operacje na kliencie (callback Web service).
WYM.OPZ.ITS.083	Oprogramowanie powinno zawierać wbudowaną obsługę standardu Web Service MTOM\XOP – SOAP Message Transmission Optimization Mechanism/XML- binary Optimized Packaging.
WYM.OPZ.ITS.084	Oprogramowanie powinno zawierać wbudowane wsparcie do udostępniania Web services typu REST.
WYM.OPZ.ITS.085	Oprogramowanie powinno zawierać wsparcie dla buforowanego wywoływania Web services.
WYM.OPZ.ITS.086	Oprogramowanie powinno zawierać wbudowane wsparcie dla zewnętrznych dostawców usług kolejkowych.
WYM.OPZ.ITS.087	Oprogramowanie powinno zawierać wbudowany moduł do diagnostyki pracy serwera aplikacyjnego i uruchomionych w nim aplikacji. Możliwość dynamicznego dodawania poprzez konfigurację własnego kodu diagnostycznego do określonych miejsc w aplikacji i jej komponentach.
WYM.OPZ.ITS.088	Wykonawca zapewni odpowiednie szkolenia dla wybranych pracowników Zleceniodawcy w zakresie obejmującym pełny zakres (instalację, administrację, optymalizację oraz wykorzystywanych języków programowania) dotyczący

Wymaganie	Opis wymagania
	proponowanego rozwiązania Szyny Usług.

Wymagania dla infrastruktury cache

Zamawiający wymaga, aby infrastruktura cache (IC) spełniała następujące warunki.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.089	Oprogramowanie (IC) musi wspierać podstawowe technologie programistyczne (dostarczać API pozwalające implementować komunikację aplikacji z cache) w tym: • Java, • Technologia .NET • C/C++.
WYM.OPZ.ITS.090	Oprogramowanie (IC) musi wspierać funkcjonalność związaną z przechowywaniem sesji (persystencja sesji http, kontekstu usług typu Servlet) dla następujących kontenerów aplikacyjnych: • Tomcat 6 • IBM Websphere v7 • Oracle WebLogic Server 10.x. • Sun One Application Server 9.x / Glassfish
WYM.OPZ.ITS.091	Oprogramowanie (IC) musi zapewniać możliwość przechowywania obiektów w strukturze kolekcji (Klucz, Wartość).
WYM.OPZ.ITS.092	Oprogramowanie (IC) musi zapewniać wsparcie modelu obiektowego przechowywanych danych (model obiektowy vs. Relacyjny).
WYM.OPZ.ITS.093	Oprogramowanie (IC) musi zapewniać mechanizm śledzenia zmian w danych znajdujących się w pamięci cache.
WYM.OPZ.ITS.094	Oprogramowanie (IC) musi zapewniać możliwość stosowania / budowania własnych funkcji agregujących.
WYM.OPZ.ITS.095	Oprogramowanie (IC) musi zapewniać mechanizmy wysokiej dostępności i ochrony danych przed awariami.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.096	Oprogramowanie (IC) musi zapewniać możliwość klastrowania węzłów cache.
WYM.OPZ.ITS.097	Oprogramowanie (IC) musi zapewniać płynne dodawanie i usuwanie węzłów klastra cache.
WYM.OPZ.ITS.098	Oprogramowanie (IC) musi zapewniać przezroczystą obsługa awarii pojedynczych węzłów.
WYM.OPZ.ITS.099	Oprogramowanie (IC) mimo występowania w konfiguracji wielowęzłowej przechowującej dane nie może wymagać wspólnej przestrzeni (np. bazy danych, rejestru, itd.).
WYM.OPZ.ITS.100	Oprogramowanie (IC) musi zapewniać mechanizm cache, pomiędzy aplikacją a drugą aplikacją lub bazą danych.
WYM.OPZ.ITS.101	Oprogramowanie (IC) musi zapewniać persystencję danych cache w bazie danych.
WYM.OPZ.ITS.102	Oprogramowanie (IC) musi zapewniać możliwość budowania własnych mechanizmów integrujących IC z dowolnymi repozytoriami danych (bazy danych, katalogi, własne aplikacje udostępniające dane poprzez API).
WYM.OPZ.ITS.103	Oprogramowanie (IC) musi zapewniać mechanizm read through w komunikacji na linii aplikacja <-> cache <-> baza danych.
WYM.OPZ.ITS.104	Oprogramowanie (IC) musi zapewniać mechanizm write through w komunikacji na linii aplikacja <-> cache <-> baza danych.
WYM.OPZ.ITS.105	Mechanizm kolejkowania żądań związanych z bazą danych musi być odporny na awarie (musi być automatycznie tworzona kopia zapasowa kolejek).
WYM.OPZ.ITS.106	Oprogramowanie (IC) musi umożliwiać integrację z technologią Spring.
WYM.OPZ.ITS.107	Oprogramowanie (IC) musi umożliwiać integrację z technologią Hibernate.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.108	Oprogramowanie (IC) musi zapewniać mechanizm wyzwalaczy (ang. Triggers).
WYM.OPZ.ITS.109	Oprogramowanie (IC) musi zapewniać możliwość usuwania z pamięci kopii danych po zapisaniu ich do DataStore (np. baza danych).

Wymagania dla Centrum Certyfikacji

Niniejszy rozdział przedstawia wymagania dla Centrum Certyfikacji, stanowiącego element infrastruktury klucza publicznego wdrażanego w ramach projektu.
Centrum Certyfikacji będzie wydawało certyfikaty niekwalifikowane do następujących zastosowań: uwierzytelnianie użytkowników, uwierzytelnianie serwerów, zabezpieczenia transmisji, zabezpieczenia danych przechowywanych lokalnie, tworzenia podpisów elektronicznych.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.110	Centrum Certyfikacji musi zapewnić wystawianie certyfikatów opartych na modelu PKI (generowanie i wydawanie certyfikatów klucza publicznego X.509).
WYM.OPZ.ITS.111	Centrum Certyfikacji musi zapewnić mechanizmy zarządzania certyfikatami kluczy publicznych, w tym ich wydawanie, zawieszanie i unieważnianie.
WYM.OPZ.ITS.112	Centrum Certyfikacji musi zapewnić generowanie informacji o zmianie statusu ważności certyfikatów (np. bazę danych unieważnionych certyfikatów, listy CRL)
WYM.OPZ.ITS.113	Centrum Certyfikacji musi umożliwić dystrybucję i/lub udostępnianie informacji o statusach ważności certyfikatów i/lub prawidłowej ścieżki walidacji.
WYM.OPZ.ITS.114	Centrum Certyfikacji musi obsługiwać wydawanie certyfikatów w postaci plików w formatach DER (DER Encoded Binary X.509), PKCS #12, PKCS #7, PEM oraz na kryptograficznych kartach elektronicznych.
WYM.OPZ.ITS.115	Centrum Certyfikacji powinno być przygotowane na współpracę z innymi Urzędami Certyfikacji.
WYM.OPZ.ITS.116	Centrum Certyfikacji musi zapewnić utrzymywanie rejestru wydanych certyfikatów.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.117	Centrum Certyfikacji musi zapewnić usługę wyszukiwania certyfikatów na podstawie zadanych kryteriów.
WYM.OPZ.ITS.118	Centrum Certyfikacji musi wspierać wydawanie certyfikatów dla osób, organizacji oraz infrastruktury teleinformatycznej (tj. podsystemów i urządzeń wchodzących w skład systemu P1 - do zabezpieczania kanałów komunikacyjnych i transakcji wymienianych pomiędzy elementami systemu).
WYM.OPZ.ITS.119	Centrum Certyfikacji musi wspierać wydawanie certyfikatów dla personelu obsługującego P1 – służących do uwierzytelniania pracowników pełniących zdefiniowane role w systemie.
WYM.OPZ.ITS.120	Centrum Certyfikacji musi zapewnić tworzenie i publikowanie okresowo oraz na żądanie informacji zbiorczych o statusie certyfikatów unieważnionych i zawieszonych.
WYM.OPZ.ITS.121	Centrum Certyfikacji musi zapewnić utrzymywanie rejestru wygenerowanych list certyfikatów unieważnionych i zawieszonych
WYM.OPZ.ITS.122	Centrum Certyfikacji musi zapewnić raportowanie, w szczególności certyfikatów wydanych, aktualnych oraz unieważnionych.
WYM.OPZ.ITS.123	Centrum Certyfikacji musi obsługiwać polskie znaki diakrytyczne.
WYM.OPZ.ITS.132	Centrum Certyfikacji musi umożliwiać wydawanie certyfikatów za pośrednictwem Punktów Rejestracji. Oczekiwane jest stworzenie Centralnego Punktu Rejestracji zlokalizowanego w CSIOZ.
WYM.OPZ.ITS.133	Dostęp do aplikacji Centrum Certyfikacji musi być chronione sprzętowo – przez stosowanie kart elektronicznych.
WYM.OPZ.ITS.134	Centrum Certyfikacji nie może mieć ograniczeń co do liczby wydawanych certyfikatów.
WYM.OPZ.ITS.135	Klucze prywatne wszystkich Urzędów Certyfikacji muszą być chronione przez sprzętowe moduły kryptograficzne (ang. Hardware Security Module – HSM).
WYM.OPZ.ITS.136	Kopie zapasowe kluczy prywatnych Centrum Certyfikacji (RootCA) muszą być wykonywane z zastosowaniem podziału sekretu.

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

Wymaganie	Opis wymagania
WYM.OPZ.ITS.137	System Centrum Certyfikacji musi integrować się ze stosowanym standardem monitorowania systemów informatycznych.
WYM.OPZ.ITS.138	Wymagane jest zaprojektowanie narzędzi i procedur pozwalających na odtworzenie Centrum Certyfikacji po awarii bez utraty informacji o wydanych certyfikatach oraz zapewnienie możliwości unieważnienia certyfikatów wydanych po wykonaniu ostatniej kopii zapasowej systemu Centrum Certyfikacji.
WYM.OPZ.ITS.139	Wymagane jest zaprojektowanie dwóch niezależnych struktur Centrum Certyfikacji: główną i zapasową. Infrastruktura zapasowa przeznaczona będzie do wznowienia usług PKI w wypadku awarii głównego Centrum Certyfikacji i będzie umieszczona fizycznie w innej lokalizacji. Zapasowe Centrum Certyfikacji powinno zapewniać identyczną funkcjonalność i wydajność. Zamawiający dopuszcza minimalizację infrastruktury CC zapasowego poprzez pominięcie elementów niezawodnościowych.
WYM.OPZ.ITS.140	Urządzenia sieciowe HSM dla Centrum Certyfikacji muszą minimalnie: • udostępniać algorytm sprzętowej generacji par kluczy RSA o długości 1024/2048 bity na podstawie ciągu losowego z fizycznego źródła, • udostępniać algorytm podpisu elektronicznego funkcji skrótu SHA1, podpisu przy pomocy klucza prywatnego RSA (1024/2048 bity). • obsługiwać kryptograficzne algorytmy klucza publicznego: RSA, ElGamal, DSA, • obsługiwać symetryczne algorytmy kryptograficzne: AES, DES, Triple DES, • obsługiwać funkcje skrótu: MD2, MD5, SHA-1, SHA-2, RIPEMD-160, • posiadać wbudowany moduł RNG – fizyczny generator ciągów losowych, • posiadać antypenetracyjne zabezpieczenia zgodne z FIPS 140-2 Level 3, • posiadać wsparcie dla platform systemowych: Windows 2008 R2 / 2008 / 2003 / Windows 7 / Vista /XP, Solaris, HP-UX, AIX, Linux.
WYM.OPZ.ITS.141	Wykonawca musi zaprojektować system monitorowania podatności infrastruktury Centrum Certyfikacji. Musi on: • umożliwiać wykrywanie podatności zasobów wchodzących w skład projektowanego Centrum Certyfikacji, • skanować zdefiniowane zasoby pod kątem wykrywania podatności, • umożliwiać skanowanie zasobów w trybie sieciowym (bez lokalnego agenta), • przeprowadzać operację skanowania w poszukiwaniu podatności tylko dla architektury skanowanego systemu: np. na platformie MS Windows tylko słabości dotyczące tej platformy, • być w automatyczny sposób zasilany informacjami o nowych podatnościach, • zapewniać skalowalność dla dowolnej wielkości sieci,

Wymaganie	Opis wymagania
	• umożliwiać elastyczne definiowanie zadań skanowania w taki sposób, aby nie występowały zakłócenia normalnej pracy sieci, • umożliwiać przeprowadzenie zadań wykrywania podatności zgodnie ze zdefiniowanym harmonogramem, lub na żądanie administratora, • przedstawiać dane o wynikach skanowania w formie raportów z wyszczególnieniem podatności krytycznych oraz rekomendacjami usunięcia wykrytych podatności, • umożliwiać eksport raportów przynajmniej do formatu HTML, CSV, PDF, XML.

Wymagania dla infrastruktury sprzętowej

Niniejszy rozdział przedstawia wymagania dla infrastruktury sprzętowej projektowanej w ramach niniejszego Zamówienia. Infrastruktura umożliwiać musi funkcjonowanie podsystemów wchodzących w skład niniejszego Zamówienia.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.124 Wydajność serwera podstawowego	Każdy projektowany serwer podstawowy musi spełniać minimalne wymagania określone, w szczególności, następującymi wymaganiami.
WYM.OPZ.ITS.124.01 Wydajność serwera podstawowego - architektura procesora	Architektura procesorów serwera musi być 64-bitowa.
WYM.OPZ.ITS.124.02 Wydajność serwera podstawowego - wydajność procesora	Wydajność każdego procesora musi spełniać następujące warunki: • zgodnie ze SPEC CPU2006 (Auto Parallel=Yes, wydajność Base): CINT2006 >= 35, CFP2006 >= 41, • zgodnie ze SPEC CPU2006 Rate (Base Copies=24, wydajność Base): CINT2006 rate >= 320; CFP2006 rate >= 230.
WYM.OPZ.ITS.124.03 Wydajność serwera podstawowego - RAM	Serwer musi posiadać co najmniej 32GB RAM.
WYM.OPZ.ITS.125.01 Cechy serwera podstawowego - montaż	Serwery muszą umożliwiać montaż w szafach serwerowych lub należeć do klasy serwerów kasetowych (blade) montowanych w szafach serwerowych.
WYM.OPZ.ITS.125.02 Cechy serwera podstawowego -	Serwery muszą być wyposażone w podwójne kontrolery FibreChannel HBA 8Gb lub szybsze.

Wymaganie	Opis wymagania
FibreChannel	
WYM.OPZ.ITS.125.03 Cechy serwera podstawowego - producent	Serwery muszą pochodzić od jednego producenta.
WYM.OPZ.ITS.125.04 Cechy serwera podstawowego - komunikacja z SAN	Serwery muszą wspierać pracę z redundantnymi ścieżkami komunikacji z SAN.
WYM.OPZ.ITS.125.05 Cechy serwera podstawowego - Ethernet	Serwery muszą posiadać redundantne kontrolery sieci Ethernet 1 Gb lub szybsze.
WYM.OPZ.ITS.125.06 Cechy serwera podstawowego - dyski	Serwery muszą obsługiwać przynajmniej dwa lokalne dyski SAS 15k w trybie RAID1.
WYM.OPZ.ITS.125.07 Cechy serwera podstawowego - zasilanie	Serwery muszą być wyposażone w redundantne moduły zasilania.
WYM.OPZ.ITS.125.08 Cechy serwera podstawowego - monitorowanie	Serwery muszą umożliwić monitoring stanu poszczególnych komponentów serwera (m.in. zasilaczy, procesorów, pamięci, dysków, kontrolerów IO).
WYM.OPZ.ITS.126 Macierz SAN	W ramach Zamówienia Wykonawca zobowiązany jest do zaprojektowania macierzy SAN niezbędnych do funkcjonowania podsystemów pozostających w jego odpowiedzialności.
WYM.OPZ.ITS.126.01 Macierz SAN - FibreChannel	Macierze SAN muszą obsługiwać łącza FibreChannel. Każda macierz musi posiadać podwójny kontroler FC 8Gb lub szybszy.
WYM.OPZ.ITS.126.02 Macierz SAN - podłączenie	Macierze muszą wspierać redundantne podłączenia hostów i wielościeżkowość.
WYM.OPZ.ITS.126.03 Macierz SAN - podłączenie dysków	Macierze muszą obsługiwać konfiguracje przynajmniej RAID0, RAID1, RAID5, RAID6 oraz RAID10.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.126.04 Macierz SAN - zasilanie	Macierze muszą być wyposażone w redundantne moduły zasilania.
WYM.OPZ.ITS.126.05 Macierz SAN - replikacja	Macierze muszą umożliwiać sprzętowo lub programowo replikację danych do Zapasowego Ośrodka Przetwarzania Danych. Musi istnieć możliwość replikacji dla wybranych woluminów logicznych.
WYM.OPZ.ITS.126.06 Macierz SAN - dyski SAS	Macierze muszą obsługiwać dyski SAS.
WYM.OPZ.ITS.126.07 Macierz SAN - monitoring	Macierze muszą umożliwiać monitoring stanu macierzy i jej kluczowych komponentów (m. in. dysków, kontrolerów, zasilaczy).
WYM.OPZ.ITS.126.08 Macierz SAN - półki	Macierze muszą umożliwiać rozbudowę przynajmniej o 50% swojej pojemności.
WYM.OPZ.ITS.127.01 Połączenie serwerów i macierzy - redundancja	Połączenie musi być zrealizowane z wykorzystaniem redundantnych przełączników FibreChannel 8Gb lub szybszych.
WYM.OPZ.ITS.127.02 Połączenie serwerów i macierzy - monitoring	Przełączniki FC wykorzystane w połączeniu muszą umożliwiać monitoring statusu połączeń między serwerami a macierzą SAN.
WYM.OPZ.ITS.127.03 Połączenie serwerów i macierzy - aktywne wykorzystanie przełączników	Połączenie musi aktywnie wykorzystywać wszystkie działające przełączniki FC.
WYM.OPZ.ITS.127.04 Połączenie serwerów i macierzy - wielościeżkowość	Połączenie musi umożliwiać wielościeżkowość.
WYM.OPZ.ITS.128 Biblioteka taśmowa	W ramach Zamówienia Wykonawca zobowiązany jest do zaprojektowania bibliotek taśmowych niezbędnych do funkcjonowania podsystemów pozostających w jego odpowiedzialności.
WYM.OPZ.ITS.128.01 Biblioteka taśmowa - liczba napędów	Biblioteka taśmowa musi posiadać przynajmniej dwa napędy taśmowe. Musi istnieć możliwość dodania przynajmniej kolejnych dwóch napędów taśmowych.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.128.02 Biblioteka taśmowa - liczba taśm	Biblioteka taśmowa musi mieścić przynajmniej 48 taśm.
WYM.OPZ.ITS.128.03 Biblioteka taśmowa - szyfrowanie	Biblioteka taśmowa musi pozwalać na tworzenie zaszyfrowanych kopii zapasowych.
WYM.OPZ.ITS.128.04 Biblioteka taśmowa - standard taśm	Biblioteka taśmowa musi wspierać standard LTO-5.
WYM.OPZ.ITS.128.05 Biblioteka taśmowa - FibreChannel	Biblioteka taśmowa musi posiadać interfejs FibreChannel 8 Gb lub szybszy.
WYM.OPZ.ITS.128.06 Biblioteka taśmowa - zasilanie	Biblioteka taśmowa musi posiadać redundantne moduły zasilania.
WYM.OPZ.ITS.128.07 Biblioteka taśmowa - serwer	Biblioteka taśmowa musi być obsługiwana przez dostarczony przez producenta biblioteki taśmowej dedykowany serwer o minimalnych parametrach: • RAM 12GB z możliwością rozbudowy, • 4 rdzenie CPU z możliwością podwojenia, • redundantne kontrolery Gigabit Ethernet, • 146 GB HDD 15k SASx2 konfiguracja RAID1, • redundantne kontrolery FC HBA, • redundantne zasilanie. Serwer ten musi być niezależny od pozostałych serwerów oraz umożliwiać montaż w szafie serwerowej.
WYM.OPZ.ITS.129 Serwer do zarządzania i monitoringu	Serwery przeznaczone do zarządzania i monitorowania infrastrukturą spełniają, w szczególności, następujące minimalne wymagania: • niezależność od pozostałych serwerów, • RAM 8GB z możliwością rozbudowy, • 4 rdzeni CPU z możliwością podwojenia, • redundantne kontrolery Gigabit Ethernet, • 146 GB HDD SAS 15k x2 konfiguracja RAID1, • redundantne zasilanie, • możliwość montażu w szafie serwerowej.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.130 ZOPD	Wymaganie usunięte.
WYM.OPZ.ITS.194 Wirtualizacja	Infrastruktura musi umożliwiać wirtualizację zasobów sprzętowych, w szczególności poprzez definiowanie wirtualnych serwerów.
WYM.OPZ.ITS.194.01 Wirtualizacja - ulokowanie serwerów	Możliwa musi być obsługa wielu instancji serwerów wirtualnych na jednym serwerze fizycznym. Jednocześnie musi istnieć możliwość określenia, na których serwerach fizycznych dana maszyna wirtualna będzie uruchomiona.
WYM.OPZ.ITS.194.02 Wirtualizacja - nowe maszyny	Musi istnieć możliwość rozbudowy infrastruktury o nowe wirtualne maszyny bez spadku wydajności i dostępności pozostałych.
WYM.OPZ.ITS.194.03 Wirtualizacja - klonowanie	Musi istnieć możliwość sklonowania maszyny wirtualnej.
WYM.OPZ.ITS.194.03 Wirtualizacja - konsola graficzna	Projektowane rozwiązanie musi udostępniać graficzną konsolę administracyjną umożliwiającą zarządzanie wirtualnymi maszynami.
WYM.OPZ.ITS.194.04 Wirtualizacja - monitorowanie	Musi istnieć możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
WYM.OPZ.ITS.194.05 Wirtualizacja - kopie zapasowe	Musi istnieć możliwość wykonania kopii zapasowej wirtualnej maszyny.
WYM.OPZ.ITS.194.06 Wirtualizacja - przenoszenie maszyn	Musi istnieć możliwość przenoszenia maszyn wirtualnych między maszynami fizycznymi w czasie ich pracy.

Wymagania dla infrastruktury sieciowej

Niniejszy rozdział przedstawia wymagania dla infrastruktury sieciowej. W zakresie niniejszego Zamówienia znajduje się projekt infrastruktury umożliwiająca połączenie Szyny Usług z publicznym Internetem, integrację podsystemów P1 oraz dostęp do łącza replikacyjnego.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.142	Infrastruktura musi umożliwiać szyfrowanie danych między Systemem P1 a użytkownikami.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.143	Cała komunikacja pomiędzy COPD a ZOPD jest chroniona kryptograficznie z zapewnieniem poufności i integralność przesyłanych danych (przy jednoczesnym zapewnieniu możliwości włączania szyfrowania dla określonych usług).
WYM.OPZ.ITS.144	Infrastruktura teleinformatyczna nie może mieć pojedynczego punktu awarii (SPOF) – zapewniona jest redundancja na poziomie sprzętu i sieci.
WYM.OPZ.ITS.145	Infrastruktura udostępniająca usługi P1 w sieci Internet musi zapewnić integrację łączy internetowych (np. przy użyciu BGP) dla ograniczenia przerw dostępności.
WYM.OPZ.ITS.146	Zastosowana infrastruktura musi umożliwić podział sieci na segmenty (fizyczne i wirtualne).
WYM.OPZ.ITS.147	Architektura musi zapewnić by cały ruch sieciowy pomiędzy strefami bezpieczeństwa, z wyłączeniem replikacji pomiędzy ośrodkami przetwarzania danych, był kontrolowany przy pomocy zapór sieciowych, a także systemów wykrywania włamań oraz system antywirusowy.
WYM.OPZ.ITS.148	Zapory sieciowe (firewall) kontrolujące ruch pomiędzy segmentami sieci w ośrodkach przetwarzania danych muszą funkcjonować na dedykowanych urządzeniach (appliance) lub wykorzystywać dedykowane systemy operacyjne (secure platform) i być certyfikowane przynajmniej na poziomie ITSEC E3 lub Common Criteria EAL4, lub równoważnych.
WYM.OPZ.ITS.149	Systemy IPS w ośrodkach przetwarzania danych muszą wykorzystywać co najmniej następujące metodologie wykrywania ataków (definicje wg. Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology, Special Publication 800-94, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf): • oparte na sygnaturach (Signature-Based Detection), • oparte na anomaliach (Anomaly-Based Detection), • oparte na analizie protokołu z uwzględnieniem stanu (Stateful Protocol Analysis).
WYM.OPZ.ITS.151	Architektura musi uwzględniać stosowanie rozwiązań typu SIEM (Security Information and Event Management).
WYM.OPZ.ITS.152	Algorytmy kryptograficzne stosowane do szyfrowania i ochrony autentyczności danych elektronicznych muszą spełniać wymagania NIST opisane w dokumencie SP80-131A.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.153	Następujące grupy operacji muszą być wykonywane z wykorzystaniem osobnych urządzeń: • operacje kryptograficzne związane z zestawianiem bezpiecznych połączeń, • ochrona przy pomocy internetowych firewalli.
WYM.OPZ.ITS.154	Projektowane komponenty infrastruktury powinny zapewniać rozdzielenie funkcji obsługi technicznej systemem od administrowania uprawnieniami użytkowników (segregation of duties).
WYM.OPZ.ITS.155	Projektowana w ramach Zamówienia infrastruktura musi być dostosowana do montażu w standardowych szafach 19” typu rack o maksymalnej wysokości 42U.
WYM.OPZ.ITS.158	Zastosowana infrastruktura musi obsługiwać QoS (np. na potrzeby podniesienia priorytetu dla ruchu zarządzającego infrastrukturą).
WYM.OPZ.ITS.159	Projektowane w ramach Zamówienia urządzenia muszą mieć możliwość monitorowania ich stanu działania przy pomocy protokołu SNMP.
WYM.OPZ.ITS.160	Urządzenia sieciowe projektowane w ramach Zamówienia musza posiadać przynajmniej dwa redundantne zasilacze.
WYM.OPZ.ITS.161	Urządzenia sieciowe projektowane w ramach Zamówienia muszą mieć możliwość zdalnego ich zarządzania.
WYM.OPZ.ITS.162	Routery brzegowe projektowane w ramach Zamówienia muszą posiadać co najmniej porty Ethernet 10/100/1000BASE-T.
WYM.OPZ.ITS.163	Routery brzegowe projektowane w ramach Zamówienia muszą obsługiwać, w szczególności, protokoły: BGP, OSPF, RIP.
WYM.OPZ.ITS.164	Każdy z routerów brzegowych projektowanych w ramach Zamówienia musi pozwalać na konfigurację co najmniej 16-tu VLAN i co najmniej 16-tu stref bezpieczeństwa.
WYM.OPZ.ITS.165	Routery brzegowe muszą mieć budowę modułową.
WYM.OPZ.ITS.166	Każdy firewall internetowy projektowany w ramach Zamówienia musi mieć co najmniej porty Ethernet 10/100/1000BASE-T.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.167	Firewalle internetowe muszą mieć możliwość obsługi IPv4 oraz IPv6 zarówno dla modułu firewall jak i VPN.
WYM.OPZ.ITS.168	Każdy firewall internetowy projektowany w ramach Zamówienia musi obsługiwać co najmniej 64 VLAN.
WYM.OPZ.ITS.169	Każdy firewall internetowy musi pozwalać na konfigurację co najmniej 64 stref bezpieczeństwa.
WYM.OPZ.ITS.170	Firewalle projektowane w ramach Zamówienia muszą pozwalać co najmniej na: • automatyczne blokowanie wykrytych ataków z zewnątrz i wewnątrz systemu, • automatyczne wykrywanie zdarzeń niepożądanych, • wykrywanie ataków na podstawie analizy sygnatury ataku, • wykrywanie ataków na podstawie anomalii protokołów, • wykrywanie ataków na podstawie anomalii ruchu, • wykrywanie ataków typu backdoor, • wykrywanie ataków typu DoS, • wykrywanie ataków typu IP Spoofing, • raportowanie o wykrytych nieprawidłowościach, • rejestrowanie wszelkich operacji wykonywanych w ramach kontroli dostępu.
WYM.OPZ.ITS.171	Przełączniki sieciowe projektowane w ramach Zamówienia muszą posiadać co najmniej porty Ethernet 10/100/1000BASE-T oraz SFP.
WYM.OPZ.ITS.172	Przełączniki sieciowe projektowane w ramach Zamówienia muszą obsługiwać co najmniej 12000 MAC.
WYM.OPZ.ITS.173	Przełączniki sieciowe projektowane w ramach Zamówienia muszą obsługiwać co najmniej 4096 VLAN.
WYM.OPZ.ITS.174	Przełączniki sieciowe projektowane w ramach Zamówienia muszą posiadać funkcjonalność port mirroring.
WYM.OPZ.ITS.175	Przełączniku sieciowe muszą obsługiwać co najmniej następujące standardy i funkcjonalności: • 802.1p, • 802.1Q,

Wymaganie	Opis wymagania
	• IEEE 802.1s, • IEEE 802.1D, • IEEE 802.1w, • 802.3ad, • ACL, • SNMP.
WYM.OPZ.ITS.176	Firewalle wewnętrzne projektowane w ramach Zamówienia muszą mieć co najmniej porty Ethernet 10/100/1000BASE-T.
WYM.OPZ.ITS.177	Firewalle wewnętrzne projektowane w ramach Zamówienia muszą mieć możliwość obsługi IPv4 oraz IPv6 zarówno dla modułu firewall jak i VPN.
WYM.OPZ.ITS.178	Firewalle wewnętrzne projektowane w ramach Zamówienia muszą obsługiwać co najmniej 4096 VLAN.
WYM.OPZ.ITS.179	Firewalle wewnętrzne projektowane w ramach Zamówienia muszą pozwalać na konfigurację co najmniej 256 stref bezpieczeństwa.
WYM.OPZ.ITS.180	Infrastruktura musi uwzględniać ochronę w warstwie aplikacji zapewnioną przez firewall aplikacyjny (WAF).
WYM.OPZ.ITS.181	Firewalle aplikacyjne projektowane w ramach Zamówienia muszą posiadać co najmniej porty Ethernet 10/100/1000BASE-T.
WYM.OPZ.ITS.182	Firewalle aplikacyjne projektowane w ramach Zamówienia muszą mieć możliwość pracy w klastrze w trybie active-active.
WYM.OPZ.ITS.183	Firewalle aplikacyjne projektowane w ramach Zamówienia muszą umożliwić wykrywanie co najmniej następujących ataków: • Cross Site Scripting (XSS), • SQL Injection, • przechwytywanie sesji, • przepełnienie bufora, • Denial of Service.

Wymaganie	Opis wymagania
WYM.OPZ.ITS.184	Infrastruktura projektowana w ramach Zamówienia musi umożliwić komunikację pomiędzy ośrodkami przetwarzania danych, w szczególności, w warstwie drugiej (L2).
WYM.OPZ.ITS.185	Każde z łączy replikacyjnych będzie zakończone interfejsem Ethernet 10/100/1000BASE-T.
WYM.OPZ.ITS.186	Infrastruktura sieciowa musi umożliwiać wykorzystanie każdego z łączy replikacyjnych niezależnie. Musi istnieć możliwość automatycznego przełączenie ruchu między łączami w przypadku niedostępności jednego z nich (np. przez zastosowanie protokołów dynamicznego trasowania).
WYM.OPZ.ITS.187	Load balancery muszą posiadać co najmniej mechanizmy: • balansowania obciążenia serwerów na poziomie warstwy 4 i 7 (HTTP, HTTPS, TCP), • kompresji HTTP, • obsługi stron z błędami, • akceleracji SSL offload, • przepisywania odnośników zawartych na stronach z HTTP na HTTPS, • dodawania własnych nagłówków dla protokoły HTTP, • blokowania zapytań HTTP lub usuwanie z nich sekwencji znaków.
WYM.OPZ.ITS.188	Projektowane w ramach Zamówienia load balancery posiadają co najmniej porty Ethernet 10/100/1000BASE-T.
WYM.OPZ.ITS.189	Architektura sieciowa musi uwzględniać przynajmniej dwa redundantne łącza dla każdej z pozostałych części Projektu P1 (części II, III oraz IV przedstawionych w załączniku 1 do Opisu Przedmiotu Zamówienia).
WYM.OPZ.ITS.190	Projektowane w ramach Zamówienia przełączniki FC muszą posiadać odpowiednią liczbę portów przynajmniej o prędkości 8Gbps, umożliwiającą podłączenie serwerów, macierzy oraz bibliotek taśmowych.
WYM.OPZ.ITS.191	Projektowane w ramach Zamówienia przełączniki FC muszą posiadać moduły SFP typu hot swap.
WYM.OPZ.ITS.192	Projektowane w ramach Zamówienia przełączniki FC muszą posiadać możliwość definiowania stref bezpieczeństwa (zone).
WYM.OPZ.ITS.193	Projektowana infrastruktura musi umożliwiać współpracę z zewnętrznym systemem bezpieczeństwa.