ROZDZIAŁ II OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Dostawa urządzeń szyny danych ESB oraz serwerów systemu kolejkującego wraz z niezbędnymi licencjami oraz wsparciem technicznym na okres 36 miesięcy.

2. Kody CPV

1. 48820000-2 Serwery
2. 72250000-2 Usługi w zakresie konserwacji i wsparcia systemów

3. Zastosowane definicje i skróty

Nazwa / skrót	Opis
Lokalizacja	Oznacza wskazane przez Zamawiającego lokalizacje oznaczone literami: A i B, znajdujące się na terenie m.st. Warszawy (lokalizacje zostaną podane w dniu podpisania Umowy), do których Wykonawca dostarczy wymagany przez Zamawiającego sprzęt lub oprogramowanie wraz dokumentacją.
Dni Robocze	Dni od poniedziałku do piątku w godzinach od 8:00 do 16:00, z wyłączeniem dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej.
Sprzęt	Zakupione i dostarczone w ramach Umowy urządzenia wraz z wyposażeniem, oprogramowaniem wbudowanym (firmware), komponentami, akcesoriami, elementami zapewniającymi właściwą instalację i używanie Sprzętu zgodnie z przeznaczeniem.
Oprogramowanie	Oprogramowanie standardowe dostarczone w ramach Umowy (ang. Firmware).
Awaria	Stan, w którym nie jest możliwe korzystanie ze Sprzętu, w sposób zgodny z jego przeznaczeniem lub nieprawidłowe działanie Oprogramowania.
Zgłoszenie	Poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii.
Czas Obsługi	Okres od dokonania Zgłoszenia do momentu w jakim zostanie przywrócona pierwotna funkcjonalność i efektywność działania Sprzętu.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Nazwa / skrót	Opis
Czas Reakcji	Czas pomiędzy dokonaniem Zgłoszenia a uzyskaniem potwierdzenia przystąpienia do realizacji Wsparcia technicznego
Obejście	Przywrócenie działania Sprzętu, z możliwymi ograniczeniami sposobu korzystania z niego, nieuniemożliwiającymi jednak realizacji funkcji obsługiwanych przez Sprzęt. Przekazanie urządzenia zastępczego stanowi również Obejście. Obejście nie stanowi usunięcia Awarii.
API	Interfejs programistyczny aplikacji
FIFO	„First in, first out" – metoda kolejki
FTP, SFTP	Protokół do transmisji plików
GET, POST, PUT, DELETE	Metody używane przez protokół HTTP
HTTP	Hyper Text Transfer Protocol – protokół do przekazywania dokumentów hipertekstowych w sieci.
JMS	Java Message Service – API do przesyłania komunikatów pomiędzy dwoma lub więcej klientami
LDAP	*Lightweight Directory Access Protocol* - protokół przeznaczony do korzystania z usług katalogowych
MQMD	Struktura zawierająca informacje kontrolne przy przekazywaniu danych przez system kolejkowy pomiędzy aplikacjami
Proxy	Serwer pośredniczący
WMQ	IBM WebSphere MQ – oprogramowanie do przesyłania komunikatów
WS-Policy, WS-SecurityPolicy, WS-ReliableMessagingPolicy	Zbiór specyfikacji możliwości I ograniczenie bezpieczeństwa

4. Przedmiot zamówienia

1) Przedmiotem zamówienia jest wymiana istniejącej infrastruktury Zamawiającego IBM DataPower Gateway XI52 i IBM DataPower Gateway o funkcjonalności Szyny Danych ESB oraz systemu przesyłania komunikatów zrealizowanych na urządzeniach IBM MQ Appliance M2000 wraz z niezbędnymi licencjami oraz wsparciem technicznym na okres 36 miesięcy.

2) Zachowanie dotychczasowych technologii dla szyny danych (DataPower) oraz systemu przesyłania komunikatów (IBM MQ) umożliwi podłączenie nowych urządzeń i usunięcie starych

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

urządzeń bez niedostępności systemów obsługiwanych przez szynę i system przesyłania komunikatów.

3) Zmiana technologii skutkowałaby wykonaniem wielu czynności dostosowujących integrowane systemy między innymi w zakresie:
   - Konfiguracji sieciowej
   - Konfiguracji usług sieciowych
   - Zmiany metod uwierzytelniania
   - Przepisania kodów dla usług zwierających logikę biznesową
   - Testów usług (aktualnie DataPower obsługuje kilkadziesiąt tysięcy obiektów)
   - Budowania nowych kompetencji.

4) Zamawiający wymaga urządzeń o funkcjonalności szyny danych zintegrowanych z HSM, pełniących funkcję bramy dla interfejsów API w różnych formatach, zapewniających zabezpieczenie transmisji danych poprzez stosowanie bezpiecznych protokołów transmisji danych, szyfrowanie i deszyfrowanie przekazywanych treści, podpisywanie komunikatów i walidację podpisanych komunikatów. Urządzenia powinny również zapewniać możliwość uwierzytelniania użytkowników z wykorzystaniem protokołu LDAP. Ponadto urządzenia powinno zapewniać możliwość transformacji komunikatów, obsługiwać połączenia z bazami danych oraz z systemami kolejkującymi komunikaty, a także kierowanie komunikatów na podstawie treści.

5) Odnośnie urządzeń z oprogramowaniem do przesyłania komunikatów, Zamawiający wymaga, aby Oprogramowanie zapewniało gwarantowaną, bezpieczną i niezawodną wymianę informacji między aplikacjami, systemami, usługami i plikami w oparciu o przesyłania komunikatów za pośrednictwem kolejek, w sposób natywny wspierane dla urządzeń IBM DataPower Gateway XI52 i IBM DataPower Gateway.

5. Wymagania ogólne

1) Dostarczany Sprzęt musi być kompletny, tj.: mieć okablowanie oraz wszystkie inne komponenty, zapewniające właściwą instalację i użytkowanie.

2) Dostarczany Sprzęt musi być fabrycznie nowy i pochodzić z najnowszych linii produktowych.

3) Sprzęt musi być dostarczony ze wszystkimi niezbędnymi do działania i zapewnienia wymaganych funkcjonalności bezterminowymi licencjami na używanie tych funkcjonalności.

4) Wszystkie urządzenia powinny posiadać możliwość aktualizacji do najnowszej stabilnej wersji oprogramowania układowego (firmware).

5) Zamawiający może wykonywać uprawnienia z tytułu rękojmi niezależnie od uprawnień wynikających z gwarancji jakości. Zamawiający wymaga zapewnienia przez Wykonawcę, że usługi opisane w pkt 7 poniżej, świadczone będą bezpośrednio przez producenta przedmiotu zamówienia opisanego w pkt 6 poniżej (dalej określanego jako „Producent") lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta dla rynku geograficznego właściwego dla Zamawiającego lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „Partner") .

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

6) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego użytkownika jakim będzie Minister Cyfryzacji, ul. Królewska 27, 00-060 Warszawa.

7) W ramach odbioru Zamawiający dokonuje odbioru:

- ilościowego – w ramach którego weryfikuje w szczególności ilość elementów dostarczonego Sprzętu, jego kompletność, jak również zgodność dostawy z terminem realizacji Umowy;
- jakościowego – w ramach którego weryfikuje w szczególności zgodność Sprzętu z Umową i dostarczoną Dokumentacją oraz pod kątem braku uszkodzeń mechanicznych, funkcjonalnym oraz poprawności jego działania.

8) Wykonawca jest zobowiązany do przekazania w raz z dostawą Zamawiającemu zestawienia w formacie xls dostarczonego Sprzętu zawierającego informacje dotyczące miejsca dostawy, daty dostawy, typu i modelu Sprzętu, konfiguracji sprzętowej, numeru seryjnego Sprzętu, ceny jednostkowej netto, kwoty VAT oraz ceny jednostkowej brutto.

6. Wymagania szczegółowe w zakresie Urządzeń

Funkcjonalność urządzenia powinna umożliwiać ograniczenie przepustowości w oparciu o różne kryteria między innymi takie jak nazwa użytkownika, adres źródłowy.

1.1. Serwery systemu kolejkującego

Nr	Wymaganie
Wymagania ogólne	
1.	Podział wg. lokalizacji: Lokalizacja A - 2 szt. Lokalizacja B - 2 szt.
2.	System kolejkowy musi dostarczać komunikaty w trybie synchronicznym i asynchronicznym (kolejkowanie komunikatów).
3.	System kolejkowy musi gwarantować doręczenie komunikatu pomiędzy dwoma, lub wieloma aplikacjami z mechanizmem wyślij i zapomnij (ang. fire and forget).
4.	System kolejkowy musi zapewniać wsparcie dla mechanizmów publish/subscribe.
5.	System kolejkowy musi zapewniać możliwość tworzenia obiektów takich jak kolejki (ang. Queues) oraz obiekty do publikacji komunikatów (ang. Topics).
6.	System kolejkowy musi zapewniać funkcjonalność wewnętrznego kopiowania komunikatów z jednej kolejki do wielu innych.
7.	System kolejkowy musi umożliwiać komunikację systemów zewnętrznych za pomocą następujących protokołów: MQ, MQTT, AMQP, MQLight.
8.	System kolejkowy musi zapewniać wsparcie do komunikacji z następujących platform: C/C++, Java, JMS 2.0.
Wymagania bezpieczeństwa	
9.	System kolejkowy musi posiadać wbudowaną funkcjonalność szyfrowania komunikatów i ich odszyfrowywania przez odbiorców końcowych.
10.	System kolejkowy musi posiadać możliwość ustawienia na konkretnych kolejkach polityk bezpieczeństwa, które realizują: • integralność komunikatów poprzez podpis cyfrowy, • prywatność komunikatów poprzez zarówno podpis cyfrowy jak i szyfrowanie,

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

	• poufność komunikatów poprzez tylko szyfrowanie z wykorzystaniem formatu PKCS#7,
11.	Polityki bezpieczeństwa muszą być realizowane wewnętrznymi mechanizmami systemu kolejkowego bez potrzeby stosowania bibliotek kryptograficznych przez programistów tworzących aplikacje dostępowe do systemu kolejkowego.
12.	Dostęp do kolejek zabezpieczonych politykami bezpieczeństwa musi być ograniczony tylko do tych klientów (aplikacji) systemu kolejkowego, którzy zostali wyposażeni przez administratora w odpowiednie zestawy kluczy kryptograficznych.
13.	System kolejkowy musi posiadać pełne i wbudowane wsparcie protokołu SSL/TLS.
14.	System kolejkowy musi posiadać mechanizm uwierzytelniania klientów poprzez: • nazwę użytkownika i hasło, • certyfikat, • możliwość podłączenia do zewnętrznego serwera LDAP.
Wymagania na przechowywania i przetwarzanie komunikatów	
15.	System kolejkowy musi umożliwiać przechowywanie komunikatów zarówno w pamięci ulotnej (komunikaty nietrwałe) jak i w pamięci trwałej (komunikaty persystentne)
16.	System kolejkowy musi posiadać mechanizmy pozwalające na niezawodne dostarczanie komunikatów.
17.	System kolejkowy musi posiadać mechanizmy pozwalające na transakcyjne przetwarzanie komunikatów z różnych kolejek i zatwierdzanie transakcji poprzez polecenie „COMMIT” lub odrzucenie poprzez polecenie „ROLLBACK”.
18.	System kolejkowy musi posiadać możliwość użycia protokołu multicast przy komunikacji typu publish/subscribe
19.	System kolejkowy musi posiadać możliwość tworzenia połączeń między serwerami kolejkowymi hub and spoke
20.	System kolejkowy musi posiadać mechanizmy pozwalające na poprawną realizację komunikacji pomiędzy zdalnymi serwerami bez względu na warunki techniczne i aktualną dostępność aplikacji np. awarie sieci, chwilowe wyłączenie aplikacji.
Wymagania administracyjne	
21.	System kolejkowy musi posiadać: • graficzną konsolę administracyjną z dostępem przez przeglądarkę, • graficzne narzędzie administracyjne do instalacji na lokalnej maszynie administratora, • administracyjną konsolę tekstową (CLI - command line interfejs).
22.	System kolejkowy musi posiadać zestaw kolejek administracyjnych za pomocą których można sterować pracą całego systemu kolejkowego, a także odczytywać i monitorować aktualne parametry systemu.
23.	Oprogramowanie system kolejkowy musi posiadać wsparcie instalacji wszystkich komponentów na różnych systemach operacyjnych: • Windows, • Linux, • AIX, a także na dedykowanym serwerze typu Appliance z wbudowanymi zabezpieczeniami przed otwarciem.
24.	System kolejkowy musi posiadać kompatybilność między różnymi wersjami oprogramowania w ramach dostarczonego systemu kolejkującego
Wymagania wydajnościowe	
25.	Wydajność systemu kolejkowego danego producenta musi być potwierdzona publicznie dostępnymi raportami z testów wydajnościowych.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Wymagania wysokiej dostępności	
26.	System kolejkowy musi wspierać rozwiązania klastra wydajnościowego zapewniającego loadbalancing w ramach węzłów klastra - serwerów kolejkowych z takimi samymi kolejkami.
27.	System kolejkowy musi wspierać rozwiązania klastra niezawodnościowego bez dodatkowego oprogramowania firm trzecich.
28.	System kolejkowy musi posiadać konfiguracje wysokiej dostępności zarówno w formie Active-Ative jak i Active-Passive.
29.	System kolejkowy w konfiguracji wysokiej dostępności musi umożliwiać replikację komunikatów między dwoma menadżerami kolejek w sposób synchroniczny, tak aby ten sam komunikat został poprawnie zapisany na dwóch oddzielnych serwerach posiadających oddzielne zasoby dyskowe.
30.	System kolejkujący musi umożliwiać replikację komunikatów w trybie asynchronicznym.
31.	Replikacja komunikatów w trybie synchronicznym lub asynchronicznym musi odbywać się dedykowanymi do tego celu interfejsami sieciowymi o prędkości co najmniej 10Gb.
32.	Replikacja komunikatów od strony sprzętowej musi zapewniać połączenie urządzeń systemu kolejkującego w każdej z lokalizacji za pomocą dwóch niezależnych łączy sieciowych 1Gb każdy, a także trzecim łączem o prędkości minimum 10Gb.
33.	Dwa systemy kolejkowe zainstalowane na dwóch oddzielnych serwerach w trybie wysokiej wydajności muszą posiadać możliwość wystawienia jednego wspólnego adresu IP (ang. floating IP address) do połączeń z aplikacjami klienckimi.
34.	Biblioteki klienckie systemu kolejkowego muszą umożliwiać automatyczne podłączenie się do aktualnie aktywnego węzła systemu kolejkowego w trybie wysokiej dostępności.
Wymagania sprzętowe	
35.	System kolejkowy musi zostać dostarczony na serwerach o następujących parametrach: • minimum dwa procesory nie mniej niż 12-rdzeniowe z rodziny x86, 64 bitowe, umożliwiające osiągnięcie przez serwer w konfiguracji dwuprocesorowej wyniku SPECrate2017_int_base – 140 pkt. Wyniki testów serwerów zawierających procesor spełniających powyższe wymagania muszą być opublikowane i ogólnie dostępne na stronie www.spec.org. • możliwość ograniczenia liczby dostępnych rdzeni procesorów dla systemu kolejkowego, • minimum 192 GB RAM 2666 MHz DDR4 DIMMs, • minimum 3 TB użytecznej przestrzeni dyskowej z dyskami SSD z wewnętrznym systemem RAID1 (mirroring), • minimum 2 interfejsy sieciowe 1Gb Ethernet przeznaczone do połączeń administracyjnych, • minimum 8 interfejsów sieciowych 1Gb Ethernet przeznaczonych do połączeń klienckich, • minimum 6 interfejsów sieciowych 10Gb Ethernet z wkładkami SFP+, • minimum 4 interfejsy sieciowe 40Gb Ethernet z wkładkami QSFP+.
36.	Możliwość tworzenia wirtualnych interfejsów sieciowych (VLAN)
37.	Serwery sprzętowe oraz system kolejkowy muszą wspierać możliwość użycia agregacji interfejsów sieciowych (ang. Link Aggregation)
38.	Serwer sprzętowy musi posiadać wewnętrzny mechanizm zabezpieczenia przed nieautoryzowanym otwarciem obudowy.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

1.2. Szyna danych ESB

Nr	Wymaganie
1.	Podział wg. lokalizacji: Lokalizacja A - 3 szt. Lokalizacja B - 3 szt.
Wsparcie dla klienta systemu kolejkowego IBM WebSphere MQ (WMQ)	
2.	Wsparcie wykorzystywanego przez Zamawiającego protokołu WMQ (wersja 8.0.1 i wyższe) w sposób natywny i bezpośredni (bez pośrednich aplikacji, interface'sów jak JMS czy innych),
3.	Możliwość modyfikacji pól nagłówka MQMD dla komunikatów wejściowych i wyjściowych.
4.	Możliwość komunikacji one-way, jak i request-response za pomocą protokołu WMQ.
5.	Możliwość komunikacji za pomocą kolejek jak i mechanizmu publish-subscribe.
6.	Możliwość sterowanie liczbą sesji połączeń do WMQ, (od 1 do n) w szczególności wspierać przetwarzanie komunikatów z kolejki wejściowej typu FIFO oraz zachować porządek FIFO z kolejki wejściowej w kolejce wyjściowej (niezmienność kolejności komunikatów pomiędzy kolejkami wejściowymi i wyjściowymi).
7.	Wsparcie równoległego przetwarzania komunikatów (n podłączonych sesji/wątków) z kolejki wejściowej z zachowaniem porządku FIFO komunikatów z kolejki wejściowej w kolejce wyjściowej.
8.	Wsparcie podłączenia się do serwera WMQ za pomocą protokołu bezpiecznego SSL.
9.	Możliwość modyfikacji ustawień Put Message Option (PMO) oraz Get Message Option (GMO.)
10.	Możliwość podłączania się do WMQ dla wielu różnych użytkowników.
http	
11.	Możliwość blokowania odpowiednich funkcji protokołu http jak: GET, POST, PUT, DELETE.
12.	Wsparcie protokołu według standardu opisanego w RFC 2616 opublikowanego przez World Wide Web Consortium (W3C).
13.	Możliwość modyfikacji (usuwanie, modyfikację, dodawanie) pól nagłówków protokołu zarówno dla request jak i response.
14.	Możliwość wystawianie protokołu http na dowolnym porcie.
15.	Możliwość zmiany adresu URL (URL rewriting).
WebServices	
16.	Możliwość integracji z serwerami UDDI zawierającymi definicje usług.
17.	Możliwość tworzenia WebService Proxy dla istniejących WebServices'ów.
18.	Możliwość importu plików WSDL dla wystawianych poprzez Proxy WebServices'ów.
19.	Możliwość automatycznego wystawianie WSDL ze zmienionymi wartościami IP i portu.
20.	Wsparcie standardu WS-Policy.
21.	Wsparcie standardu WS-SecurityPolicy.
22.	Wsparcie standardu WS-ReliableMessagingPolicy.
Inne	
23.	Wsparcie protokołu FTP(S).
24.	Wsparcie protokołu WebSphere JMS.
25.	Wsparcie protokołu SFTP.
26.	Możliwość konwersji pomiędzy protokołami: WMQ, http, FTP, WebSphere JMS.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

27.	Wsparcie komunikacji z następującymi bazami danych za pomocą języka SQL: Oracle, DB2.
28.	Możliwość monitorowania liczby konkretnych wywołań (requestów) i tworzenia ograniczeń w jednostce czasu, w szczególności dławić ruch przekraczający zadany limit. Ograniczanie ruchu może być parametryzowane w zależności od adresów IP, dni i godzin itp.
Transformacje, parsery	
29.	Możliwość transformacji dokumentów XML za pomocą arkuszy XSLT.
30.	Posiada wbudowane parsery i walidatory przesyłanych komunikatów w formacie SOAP i JSON bez konieczności ich „ręcznego" definiowania oraz umożliwia ich transformacje.
31.	Możliwość monitorowania wystąpień ewentualnych błędów podczas przetwarzania oraz pozwala odpowiednio na nie zareagować (np. pozwala na sformatowanie odpowiedniego komunikatu o błędzie i wysłanie go wołającemu).
32.	Możliwość transformacji dokumentów w formatach innych niż XML (np. pliki płaskie, binarne, struktury z separatorami, lub struktury o ustalonej długości).
33.	Wsparcie konwersji polskich stron kodowych (Windows/Unix itp) dla przetwarzanych komunikatów.
34.	Możliwość przetworzenia jednego dużego komunikatu wejściowego posiadającego 'N' transakcji na 'N' komunikatów wyjściowych zawierających pojedyncze transakcje.
35.	Narzędzie graficzne pozwalające na budowę transformacji dowolnych formatów w dowolne za pomocą funkcjonalności Przeciągnij i Upuść (Drag&Drop).
Bezpieczeństwo	
36.	Rozwiązanie klasy Hardware Security Module (HSM).
37.	Urządzenie musi posiadać wewnętrzny mechanizm zabezpieczenia przed nieautoryzowanym otwarciem obudowy.
38.	Żadne informacje biznesowe ani przesyłane dane nie są przechowywane na urządzeniu.
39.	Posiada certyfikat EAL4 lub równoważny, potwierdzający spełnianie wymagań w zakresie bezpieczeństwa komputerów tj.: • Opracowany metodycznie, przetestowany i poddany przeglądowi. • Obejmujący analizę wspomaganą przez niskopoziomowe projektowanie modułów TOE (Cel oceny) ang. Target off Evaluation oraz podzbiór implementacji. • Obejmujący testowanie wspomagane przez niezależne wyszukiwanie oczywistych luk. • Uwzględniający kontrolę rozwoju wspieraną przez model cyklu życia, identyfikację narzędzi i automatyczne zarządzanie konfiguracją.
40.	Wsparcie standardu bezpieczeństwa WS-Security w zakresie uwierzytelnienia, autoryzacji, podpisów cyfrowych (podpisywanie i sprawdzanie podpisów), szyfrowania treści.
41.	Bezpieczne repozytorium dla certyfikatów i kluczy publicznych.
42.	Wsparcie dla kluczy RSA o długości 1024, 2028 oraz 4096.
43.	Wsparcie standardu PKCS#7 w zakresie podpisów cyfrowych (podpisywanie i weryfikacja podpisów) dla dowolnego formatu danych wejściowych (podpis może znajdować się w dowolnym miejscu komunikatu wejściowego).
44.	Wsparcie mechanizmu CRL.
45.	Wsparcie standardu SAML w wersjach: 2.0, 1.1, 1.0.
46.	Wsparcie standardu WS-Trust.
47.	Wsparcie standardu XKMS.
48.	Wsparcie standardu XML Encryption.
49.	Pozwala generować samopodpisane (ang. self-signed) zestawy klucz/certyfikat.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

50.	Możliwość określania maksymalnego rozmiaru komunikatu wejściowego w KB
51.	Możliwość walidacji dokumentów XML zgodnie z opisaną definicją XSD.
52.	Możliwość ograniczenia pobierania zewnętrznych plików XSD podczas walidacji dokumentów XML. (Np. walidacja dokumentów XML tylko dla struktur XSD znajdujących się lokalnie) w szczególności nie dopuszcza do pobierania XSD ze zdalnych serwerów http.
53.	Możliwość określenia maksymalnej ilości atrybutów dla przetwarzanego dokumentu XML i reakcję błędem na dokumenty przekraczające zapisane kryteria.
54.	Możliwość określenia maksymalnej ilości elementów dla przetwarzanego dokumentu XML i reakcji błędem na dokumenty przekraczające zapisane kryteria.
55.	Możliwość określenia rozmiaru węzła XML (node) dla dokumentu XML i reakcji błędem na dokumenty przekraczające zapisane kryteria.
56.	Zaimplementowana ochrona przed następującymi zagrożeniami spowodowanymi użyciem technologii XML: Jumbo payloads (bardzo duże dokumenty XML), Recursive elements (rekursywne elementy), MegaTags (długie nazwy elementów), XPath Injection (wstrzykiwanie wyrażeń XPath), SQL Injection (wstrzykiwanie wyrażeń SQL), Schema Poisoning, XML encapsulation (wstawianie komend systemowych w sekcję CDATA), XML Virus (załączniki SOAP z wirusami).
57.	Możliwość filtrowania dokumentów względem ustalonej treści dla dokumentów w dowolnym formacie.
58.	Możliwość automatycznego wycinania załączników SwA (SOAP with Attachements).
Routing	
59.	Możliwość sterowania przetwarzaniem (routing) na podstawie treści komunikatów wejściowych.
60.	Możliwość sterowania przetwarzaniem na podstawie wartości nagłówków protokołów wejściowych.
Wdrażanie i utrzymanie	
61.	Możliwość przenoszenie konfiguracji pomiędzy środowiskiem deweloperskim a produkcyjnym.
62.	Wsparcie protokołu SNMP.
63.	Logowanie informacji o błędach w funkcjonowaniu oraz umożliwia logowanie dowolnej treści w podziale na kategorie jak i poziom krytyczności (severity).
64.	Wsparcie protokołu SYSLOG do zapisu logów.
65.	Możliwość wysłania wiadomości email z informacją o błędach celem poinformowania administratora o ich wystąpieniu.
66.	Możliwość konfiguracji i administracji za pomocą konsoli znakowej i połączenia ssh.
67.	Możliwość konfiguracji i administracji za pomocą przeglądarki internetowej.
68.	Możliwość przydzielenia na wyłączność fizycznych (CPU/RAM) zasobów dla usługi lub grupy usług.
Realizacja i odbiór	
69.	Dostawa sprzętu oraz instalacja w serwerowni zamawiającego na terenie Warszawy.
Warunki licencjonowania i wsparcia	
70.	Licencja na sprzęt oraz oprogramowania na okres 3 lat
71.	W ramach wsparcia Zamawiającemu przysługiwać będzie prawo do dostępu do uaktualnień poprawek fabrycznie zainstalowanego oprogramowania (w ramach

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

	zakupionej wersji) udostępnianych przez producenta oraz obsługi serwisowej (nowe edycje produktów, wydania uzupełniające, aktualizacje, poprawki programistyczne).
72.	Przyjmowanie zgłoszeń w trybie 24h na dobę 7 dni w tygodniu przez 365 dni w roku.
73.	Wsparcie techniczne świadczone będzie drogą telefoniczną lub elektroniczną za pośrednictwem poczty e mail lub strony WWW.
74.	Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy.
75.	W przypadku stwierdzenia uszkodzenia dysku twardego, będzie on wymieniony przez Wykonawcę na nowy dysk twardy, wolny od wad, bez konieczności zwrotu uszkodzonego dysku twardego. Zamawiający nie dopuszcza możliwości dokonywania ekspertyzy uszkodzonego dysku twardego poza miejscem instalacji naprawianego urządzenia.
76.	Serwis gwarancyjny na dostarczony Sprzęt, realizowany będzie zgodnie z normą zarządzania jakością ISO 9001 lub równoważną. Poprzez zwrot „równoważny" Zamawiający rozumie dokument wystawiony przez uprawniony niezależny podmiot, który potwierdza spełnienie normy charakteryzującej się cechami właściwymi dla normy wymienionej przez Zamawiającego. Aktualne certyfikaty zarządzania jakością ISO 9001 lub równoważne, w zakresie co najmniej świadczenia usług serwisu i naprawy Sprzętu, Wykonawca zobowiązuje się dostarczyć Zamawiającemu przy każdej zmianie lub odnowieniu takiego certyfikatu.

7. Warunki gwarancji i wsparcia technicznego dla dostarczanego sprzętu

1) Dostarczony Sprzęt musi być objęty 36 miesięczną gwarancją producenta (która może być realizowana także przez podmioty autoryzowane przez producenta), której bieg rozpocznie się od podpisania protokołu odbioru przez Zamawiającego.

2) Wykonawca zobowiązany będzie dostarczyć Zamawiającemu, w terminie 3 Dni Roboczych od podpisania Umowy:

   - drogą elektroniczną na wskazane adresy e-mail niezbędne dane dostępowe umożliwiające skorzystanie z usług serwisu gwarancyjnego i wsparcia technicznego dla Oprogramowania,
   - do siedziby Zamawiającego, pisemne oświadczenie, w formie certyfikatu lub podobnego dokumentu, potwierdzające objęcie Oprogramowania i Sprzętu gwarancją wsparciem technicznym.

3) Obsługa serwisowa świadczona będzie w języku polskim.

4) W razie Awarii, Zamawiający będzie uprawniony do dokonywania Zgłoszeń: 24 godziny na dobę, przez 7 dni w tygodniu (również w dni ustawowo wolne od pracy) za pośrednictwem poczty elektronicznej lub telefonicznie lub przez system informatyczny.

5) Za chwilę przyjęcia Zgłoszenia uważa się chwilę dokonania Zgłoszenia za pośrednictwem jednej ze wskazanych wyżej metod.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

6) Gwarant będzie zobowiązany zapewnić usunięcie Awarii przez wykonanie wszelkich niezbędnych czynności zmierzających do usunięcia Awarii w sposób adekwatny do danej Awarii, w tym w szczególności lecz nie wyłącznie przez:
   - naprawę,
   - dostawę i zamontowanie części zamiennych,
   - zdemontowanie i złożenie w miejscu wskazanym przez Zamawiającego dotkniętych Awarią Sprzętu lub ich elementów,
   - dostarczenie poprawek, aktualizacji,
   - reinstalację, konfiguracje;
7) Gwarant będzie zobowiązany realizować usługi gwarancyjne w następujących terminach:
   - dochowania Czasu Reakcji – maksymalnie w ciągu 2 godziny od dokonania Zgłoszenia,
   - dochowania Czasu Obsługi - maksymalnie w ciągu 12 godzin od dokonania Zgłoszenia[1].
8) W razie nieusunięcia Awarii Sprzętu w terminach, o których mowa powyżej, Gwarant będzie zobowiązany zapewnić dostarczenie na czas naprawy urządzenie zastępcze, o parametrach technicznych nie gorszych od parametrów technicznych Sprzętu naprawianego (zastosowanie Obejścia).
9) W przypadku stwierdzenia uszkodzenia nośnika danych (np. dysku twardego), należy wymienić go na nowy, wolny od wad, o tych samych lub lepszych parametrach, bez zwrotu uszkodzonego dysku twardego. Nie dopuszcza się dokonywania ekspertyzy uszkodzonego nośnika poza miejscem instalacji naprawianego urządzenia. Ekspertyza nie może polegać na przeglądaniu danych na nośniku;
10) w przypadku braku możliwości naprawy Sprzętu w terminie naprawy, w miejsce Sprzętu który nie może być przez Gwaranta naprawiony, Gwarant będzie zobowiązany do dostarczenia do Lokalizacji i przekazania Zamawiającemu (bez dodatkowego wynagrodzenia) innego Sprzętu, o parametrach technicznych nie gorszych od parametrów Sprzętu uszkodzonego, a następnie świadczenia wsparcia technicznego w stosunku do tego Sprzętu przez okres gwarancji;
11) Czas Obsługi uważa się za dochowany z chwilą zgłoszenia dokonania naprawy, jeśli Awaria została faktycznie usunięta. Jeśli okaże się podczas weryfikacji usunięcia Awarii, że Awaria nie została usunięta, Czas Obsługi jest dochowany dopiero z chwilą zgłoszenia poprawki faktycznie usuwającej Awarię;
12) osoby wykonujące czynności związane z naprawą Sprzętu muszą dysponować odpowiednimi uprawnieniami i kwalifikacjami, potwierdzonymi certyfikatami wystawionymi przed producenta Urządzeń;
13) osoby biorące udział w realizacji tego zamówienia muszą posiadać wyciąg z Krajowego Rejestru Karnego oraz będą przestrzegać wewnętrznych regulaminów i zasad dotyczących pracy na terenie budynków oraz pomieszczeń, w których wykonywane są prace.

[1] Czas obsługi stanowi kryterium oceny ofert w ramach kryterium „Usunięcia Awarii”

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl