ZUS | ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH

Departament Zamówień Publicznych

Warszawa, 3 grudnia 2018 r.

SYGNALISTA

Sygnalizuj nieprawidłowości w przetargu
sygnalista@zus.pl

993200/271/IN -940/2018

Informacja dla Wykonawców, biorących udział w postępowaniu

Dotyczy: postępowania o udzielenie zamówienia publicznego na **Zestawienie i utrzymanie łączy do sieci Internet w ramach Projektu „zakup usługi operatora sieci rozległej WAN KSI ZUS", część 3 z 5**, znak sprawy TZ/271/22/18.

Odpowiedzi na pytania

Stanowi: Państwo

Zamawiający informuje, że do załączników do Specyfikacji Istotnych Warunków Zamówienia (dalej: „SIWZ") w ww. postępowaniu wpłynęły wnioski o udzielenie wyjaśnień, w związku z tym Zamawiający na podstawie art. 38 ust. 2 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień Publicznych (t.j. Dz. U. z 2017 r. poz. 1579 ze zm.) – poniżej przekazuje treść zapytań wraz z wyjaśnieniami.

Pytanie nr 1

Zamawiający w odpowiedzi ma pytanie nr 44 z dnia 20.11.2018 wskazał, że *„monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mającej na celu eliminację zagrożeń muszą odbywać się **w SOC Wykonawcy zlokalizowanym na terenie Polski z obsługą w języku polskim**."* **Wnosimy o zmianę powyższej interpretacji i potwierdzenie, że** monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mającej na celu eliminację zagrożeń muszą odbywać się **w SOC Wykonawcy zlokalizowanym na terenie Polski z obsługą w języku polskim, przy czym nie wyklucza to sytuacji, że monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mające na celu eliminacje zagrożeń mogą odbywać się na terenie Unii Europejskiej.**

W przedmiotowym stanie faktycznym brak uzasadnienia merytorycznego dla wprowadzenia ograniczania w/w do terenu Polski. Jego wprowadzenie prowadzi do naruszenia uczciwej konkurencji i równego traktowania wykonawców, gdyż de facto uniemożliwia ubieganie się o udzielenie zamówienia wykonawcom mającym siedzibę na obszarze UE. Ograniczenie to prowadzi zatem do naruszenia nie tylko szeregu przepisów Pzp, ale również regulacji unijnych gwarantujących swobodny przepływ towarów i usług podmiotom w ramach UE. Jest to tym bardziej istotne, że

obecnie, z uwagi na ciągły rozwój, nawet polskie przedsiębiorstwa telekomunikacyjne montują swoje urządzenia również na terenie innych krajów, np. aby zwiększyć zasięg swojej działalności, dotrzeć do większego grona odbiorców i klientów przy zachowaniu jak największej jakości świadczonych usług. Fakt, że urządzenia mogą być zainstalowane poza terytorium Polski nie wpłynie w jakimkolwiek stopniu na ich funkcjonalność i nie przeszkodzi w należytym realizowaniu umowy.

Odpowiedź:

Zamawiający wyjaśnia, że w odpowiedzi na pytanie nr 44 z dnia 20.11.2018 r. jedynie potwierdził – zgodnie z pytaniem Wykonawcy – że monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mającej na celu eliminację zagrożeń muszą odbywać się w SOC Wykonawcy zlokalizowanym na terenie Polski z obsługą w języku polskim. Intencją Zamawiającego udzielając odpowiedzi było i jest, aby Wykonawca zapewnił ochronę każdego łącza z osobna przed atakami DDoS m.in. poprzez monitorowanie ruchu internetowego przez centrum bezpieczeństwa operatora, działające w trybie 24/7/365.

W związku z powyższym Zamawiający potwierdza, że monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mające na celu eliminacje zagrożeń mogą odbywać się na terenie Unii Europejskiej, w tym poprzez dopuszczanie lokalizacji także centrum bezpieczeństwa operatora, na terenie Unii Europejskiej. Jednocześnie Zamawiający podtrzymuje, że obsługa realizowana przez centrum bezpieczeństwa operatora ma się odbywać w języku polskim.

Pytanie nr 2

W odpowiedzi na pytanie nr 21 Zamawiający wymaga aby łącza nr 3 i 4 były utrzymywane i dostarczone przez dwóch różnych operatorach o różnych numerach AS. Czy Zamawiający wymaga aby drugi operator świadczył usługi dostępu do Internetu w całości na własnej infrastrukturze telekomunikacyjnej, czy dopuszcza możliwość dzierżawy części infrastruktury technicznej przy zachowaniu różnych numerów AS oraz punktów wymiany ruchu z innymi operatorami.

Odpowiedź:

Zamawiający wymaga aby Wykonawca doprowadził dwa punkty styku z siecią Internet, każdy z innym operatorem a tym samym z różnymi numerami AS należącymi to tych operatorów. Zamawiający nie stawia wymagań co do własności infrastruktury telekomunikacyjnej operatorów. Jednocześnie Zamawiający wskazuje, że celem powyższych wymagań jest uniknięcie pojedynczego punktu awarii (np. szkieletu sieci jednego operatora), która to awaria mogłaby mieć wpływ na działanie obydwu łączy.

Pytanie nr 3

Bardzo prosimy o potwierdzenie że jeżeli Wykonawca spełnia wymagania techniczne opisane przez Zamawiającego w odpowiedzi na pytanie nr 44 lecz jednostka w jego organizacji nosi inną nazwę niż SOC (ang. Security Operations Center) np. NOC (Network Operations Center) to czy Wykonawca może uznać, że spełnia wymagania czy dopiero jak zmieni nazwę jednostki na SOC to wymaganie będzie spełnione?

Odpowiedź:

Zamawiający wyjaśnia, że zgodnie z Załącznikiem 6 do Umowy, cz. I, pkt 7, Wykonawca jest zobowiązany do zapewnienia ochrony łączy przed atakami DDoS na następującym poziomie:

„Dla łączy z poz. 3, 4, 6, 7 oraz 8 Tabeli I z Załącznika nr 1, Wykonawca zapewni ochronę każdego łącza z osobna przed atakami DDoS, przez którą Zamawiający rozumie:

7.1. monitorowanie ruchu internetowego przez centrum zarządzania bezpieczeństwem operatora, działające w trybie 24/7/365,

7.2. wykrywanie i mitygację ataków dla warstwy modelu OSI L3-L7,

7.3. powiadamianie Zamawiającego o podejrzeniu przeprowadzonego ataku DDoS,

7.4. odparcie ataku poprzez przyjmowanie całości podejrzanego ruchu przez operatora oraz blokadę powyżej 10 Gbps,

7.5. dostarczanie w formie elektronicznej, raportów z monitorowanego ruchu, ilości ataków DDoS oraz przeprowadzanych ewentualnych mitygacji,

7.6. udostępnianie na portalu internetowym statystyk z ruchu przychodzącego i wychodzącego na łączach do Internetu, z zapewnieniem funkcjonalności:
7.6.1. synchronizacja danych w czasie nie dłuższym niż 5 minut,

7.6.2. konfiguracja wielu kont dla Zamawiającego,

7.6.3. prezentacja graficzna wolumenu przychodzącego i wychodzącego, w ujęciu bps i pps (bps - bits per second oraz pps – pacekts per second).".

Zamawiający wskazuje, że w odpowiedzi na pytanie nr 44 z dnia 20.11.2018 r. jedynie potwierdził – zgodnie z pytaniem Wykonawcy – że monitorowanie, analiza ruchu sieciowego, wykrywanie ataków oraz działania mającej na celu eliminację zagrożeń muszą odbywać się w SOC Wykonawcy zlokalizowanym na terenie Polski z obsługą w języku polskim – patrz także odpowiedź na Pytanie nr 1.

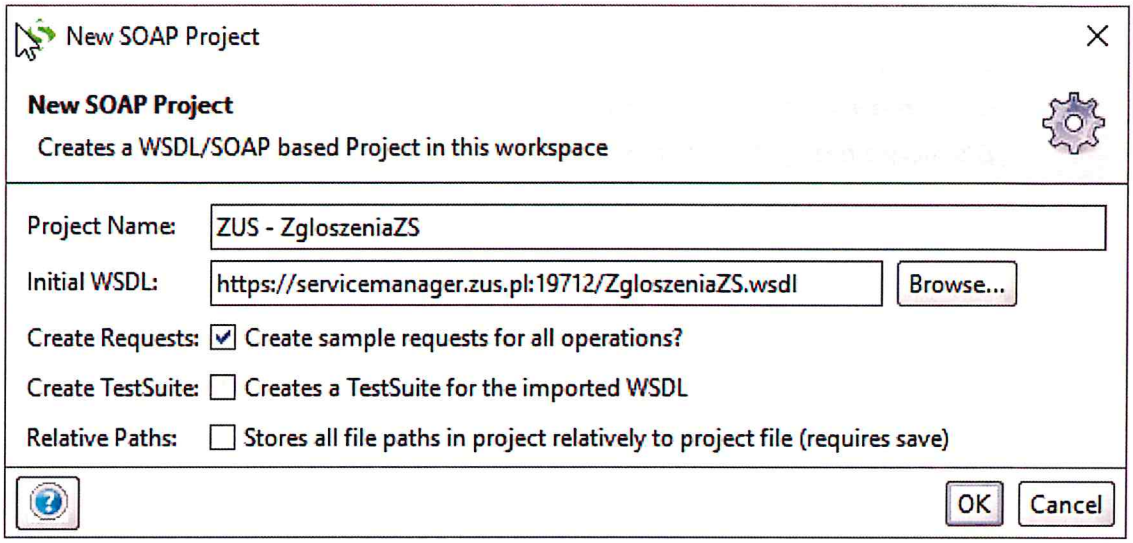
Intencją oraz wymaganiem Zamawiającego jest aby Wykonawca zapewnił ochronę każdego łącza z osobna przed atakami DDoS m.in. poprzez monitorowanie ruchu internetowe przez centrum bezpieczeństwa operatora, działające w trybie 24/7/365. Dla Zamawiającego nie ma znaczenia nazwa centrum bezpieczeństwa operatora, o ile Wykonawca zapewni bezpieczeństwo łączy zgodnie z ww. wymaganiami.

Pytanie nr 4

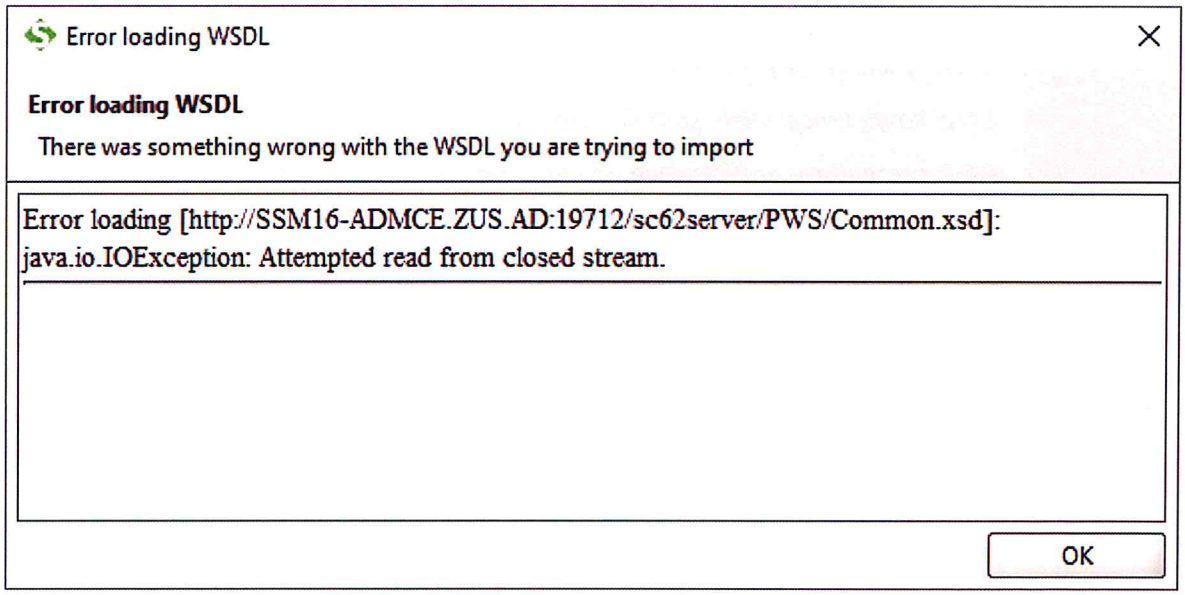
W imieniu wykonawcy zwracam się z prośbą o udzielenie odpowiedzi.
Dotychczasowe odpowiedzi udzielone przez Zamawiającego sprawiają, że wykonawcy mogą w sposób niewłaściwy zinterpretować SIWZ.

Wykonawca zwraca uwagę, że nadal występują problemy z danymi dotyczącymi opisu interfejsu do komunikacji z systemem ticketowym Zamawiającego:

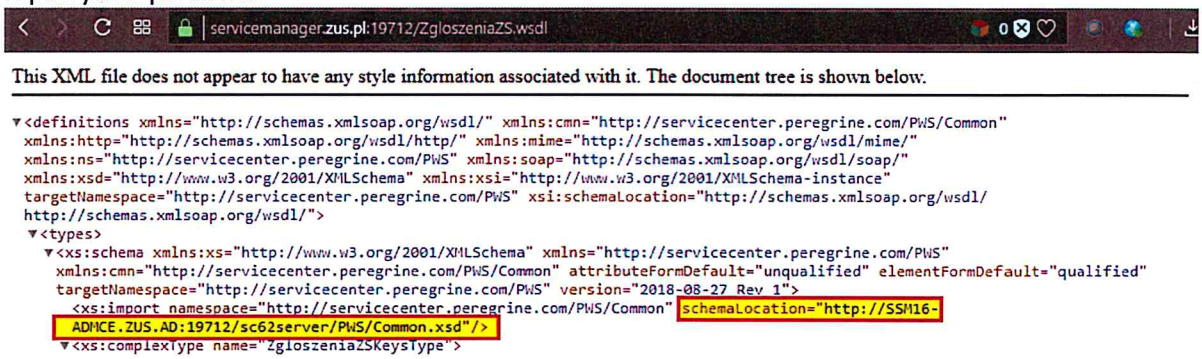
1. Próba definicji projektu w do narzędziu SoapUI dla interfejsu ZUS https://servicemanager.zus.pl:19712/ZgloszeniaZS.wsdl



2. Komunikat podczas próby utworzenia ww projektu:



3. A powyższe ponieważ



4. Plik schemy o nazwie Common.xsd (**i to wcale nie muszą być te same pliki w sensie zawartości**) https://servicemanager.zus.pl:19712/Common.xsd jest już wystawiony do Internetu, ale w dalszym ciągu definicja interfejsu do niego nie referuje, import się nie udaje, tak więc nie jest możliwa nadal weryfikacja prac po stronie Wykonawcy związana z integracją z interfejsem wyspecyfikowanym przez Zamawiającego.

Odpowiedź:

Zamawiający informuje, że pełny dostęp do webservice będzie możliwy dopiero po zawarciu umowy z wyłonionym Wykonawcą. Pełny dostęp wymaga autoryzacji przez Zamawiającego.

Informacja o zmianie terminu składania ofert

Zamawiający informuje, że dokonuje przedłużenia terminu składania ofert i wnoszenia wadium **do dnia 10.12.2018 r. do godz. 10:00.**

Miejsce składania ofert nie ulega zmianie.

Otwarcie ofert nastąpi w dniu upływu terminu składania ofert w siedzibie Zamawiającego w Warszawie, ul. Szamocka 3, 5, skrzydło C, piętro I, Departament Zamówień Publicznych, pok. 135, o godzinie 10:30.

Z poważaniem

CZŁONEK ZARZĄDU

Krzysztof Dyki

Osoba prowadząca sprawę:
Jolanta Banaszek
Główny Specjalista, Departament Zamówień Publicznych
T: +48 22 667 17 12
E: jolanta.banaszek@zus.pl