NFZ | Narodowy Fundusz Zdrowia
Śląski Oddział Wojewódzki w Katowicach

znak:WAG-II-1-2910-286/562a/KK/2011 Katowice, dnia 13 czerwca 2011 r.

**DO**

**WYKONAWCÓW**

dotyczy: **zamówienie nr 20/pn/2011** - przeprowadzenie audytu bezpieczeństwa czterech aplikacji www

Na podstawie art. 38 ust. 2 w związku z art. 38 ust. 1 pkt 3 ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych (tj. Dz.U. z 2010 r. Nr 113, poz. 759 ze zm.), przekazuję Państwu treść zapytań do Specyfikacji Istotnych Warunków Zamówienia na ***przeprowadzenie audytu bezpieczeństwa czterech aplikacji www***, jakie wpłynęły do Zamawiającego oraz udzielam wyjaśnień (odpowiedzi).

I.

**1.** Czy test mogą być w 100% przeprowadzone zdalnie (bez konieczności przyjazdu do Katowic i wykonywania prac na miejscu w Katowicach)?

Odpowiedź: Zamawiający dopuszcza wykonanie testów aplikacji zdalnie, poprzez Internet, co nie wymaga przyjazdu Wykonawcy do siedziby Śląskiego OW NFZ w Katowicach, niemniej jednak nie wyklucza go.
Obecności Wykonawcy w ww. siedzibie wymaga natomiast przegląd architektury logicznej. Ponadto, jeżeli w trakcie realizacji usługi zaistnieje potrzeba dostępu do konsoli serwera – dostęp ten będzie możliwy jedynie w siedzibie Śląskiego OW NFZ. Patrz również odpowiedź na zapytanie II.1 i II.2.
W związku z powyższym:

a) **§ 1 ust. 4 wzoru umowy** otrzymuje brzmienie:
*„4. Miejscem wykonania usługi przez Wykonawcę jest siedziba Śląskiego OW NFZ przy ul. Kossutha 13 w Katowicach. W ww. siedzibie Wykonawca dokona przeglądu architektury logicznej na podstawie dokumentacji infrastruktury oraz sieci, udostępnionej Wykonawcy przez Zamawiającego do wglądu po zawarciu umowy. Wgląd do dokumentacji możliwy będzie tylko i wyłącznie w ww. miejscu. Ponadto, jeżeli w trakcie realizacji usługi przez Wykonawcę zaistnieje potrzeba dostępu do konsoli serwera – dostęp ten będzie możliwy również jedynie w siedzibie Śląskiego OW NFZ. Zamawiający dopuszcza wykonanie testów aplikacji przez Wykonawcę zdalnie, poprzez Internet, co nie będzie wymagało przyjazdu Wykonawcy do siedziby Śląskiego OW NFZ w Katowicach."*

b) **pkt IV ppkt 2 SIWZ** otrzymuje brzmienie: *„2. Miejsce wykonania zamówienia: Katowice, ul. Kossutha 13. Szczegóły określa wzór umowy."*

**2.** Czy testowany system jest własnością NFZ?

Odpowiedź: Tak, testowany system stanowi własność NFZ.

www.nfz.gov.pl | Śląski Oddział Wojewódzki, ul. Stanisława Kossutha 13, 40-844 Katowice
tel.: 032 735 17 00, fax: 032 254 18 94, e-mail: sekretariat@nfz-katowice.pl

**3.** Czy testowany system działa na infrastrukturze, której właścicielem jest NFZ? Jeżeli testowany system działa na infrastrukturze firmy trzeciej, to czy NFZ posiada pisemną zgodę firmy trzeciej na przeprowadzenie testów?
Odpowiedź: Tak, system działa na infrastrukturze stanowiącej własność NFZ.
**4.** W jakim środowisku będą prowadzone testy systemu (testowym, przedprodukcyjnym, produkcyjnym, innym)?
Odpowiedź: Testy systemu będą prowadzone w środowisku produkcyjnym.
**5.** (....) posiada listy referencyjne z wykonanych prac. W listach referencyjnych nie ma informacji o wartości projektu. Czy dla potwierdzenia wykonania prac o określonej wartości wystarczą takie listy referencyjne oraz oświadczenie (...) o wartości projektu?
Odpowiedź: Odnośnie warunku posiadania wiedzy i doświadczenia (warunek z art. 22 ust. 1 pkt 2 pzp), Wykonawca, obok oświadczenia o spełnianiu warunku udziału w postępowaniu winien przedłożyć następujące dokumenty, zgodnie z pkt VI lit. B ppkt 3 lit. a i b SIWZ: formularz wykaz usług oraz dokumenty potwierdzające, że zamówienia wykazane w ww. formularzu zostały wykonane należycie.
W kolumnie trzeciej tabeli ww. formularza Wykonawca winien podać wartość brutto usług. Niniejsze, sprowadzając się de facto do oświadczenia Wykonawcy, będzie wystarczające dla oceny spełniania warunku dotyczącego wartości usługi (nie mniej niż 15.000,00 złotych brutto).
Nie jest zatem konieczne, aby treść dokumentu potwierdzającego należyte wykonanie usługi (np. treść referencji) zawierała w sobie informację nt. wartości usługi, zwłaszcza, że nie można z góry narzucić dokumentom wystawianym przez podmioty trzecie określonej treści.
Jak stwierdzono w wyroku KIO z dnia 19.04.2011 (KIO 700/11): *„(...) Celem referencji jest wyłącznie potwierdzenie należytego wykonania usługi, zatem nie ma konieczności wskazywania w treści referencji zarówno wartości usługi, jak i terminu jej realizacji. Informacje dotyczące wartości usługi, terminu czy zakresu wynikają z samego oświadczenia wykonawcy złożonego w treści oferty. (...). Dokument potwierdzający wykonanie usługi jest niejako dopełnieniem informacji zawartych w wykazie i nie musi dokładnie odzwierciedlać wszystkich informacji zawartych tamże - o ile bowiem i zamawiający i wykonawca biorący udział w postępowaniu mają wpływ na szczegółowość i zakres danych podanych w wykazie, to dokument potwierdzający wykonanie prac ujętych w wykazie pochodzący od osoby trzeciej jest trudny do ukształtowania pod kątem konkretnego postępowania (skonkretyzowanych wymagań zamawiającego). (...).”*
**6.** W jakim terminie NFZ oczekuje zakończenia projektu?
Odpowiedź: Termin realizacji zamówienia określa pkt IV ppkt 1 lit. a i b SIWZ.
**7.** W jakich technologiach są napisane aplikacje, które mają być testowane?
Odpowiedź: Wedle wiedzy Zamawiającego system w głównej mierze oparty jest o .NET; nie można jednak wykluczyć zastosowania przez twórcę systemu innych technologii.
**8.** Czy mogłabym otrzymać od Państwa ofertę a także załącznik w wersji edytowalnej?
Odpowiedź: Specyfikacja Istotnych Warunków Zamówienia (SIWZ) dotycząca przedmiotowego przetargu nieograniczonego - zgodnie z art. 42 ust. 1 ustawy Prawo zamówień publicznych - została udostępniona na stronie internetowej www.nfz-katowice.pl od dnia zamieszczenia ogłoszenia o zamówieniu w Biuletynie Zamówień Publicznych, w wersji pdf - zeskanowany oryginał SIWZ (z podpisem osoby zatwierdzającej SIWZ, z parafami pracowników Zamawiającego).Ten sposób udostępniania SIWZ funkcjonujący w praktyce Śląskiego OW NFZ stanowi gwarancję otrzymania przez Wykonawców dokumentów w wersji zgodnej z ich oryginalnym brzmieniem (tożsamych merytorycznie). Dokumenty - formularze wystarczy wydrukować i w miejscach do tego wyznaczonych odręcznie wypełnić; ewentualnie przeformatować wersję pdf na inną, umożliwiającą elektroniczne wypełnienie dokumentów.
W przypadku woli przepisania formularzy przez Wykonawcę (co nie jest konieczne), ewentualne ryzyko popełnienia merytorycznego błędu (niejednokrotnie decydującego o zgodności treści oferty z SIWZ) spoczywa na Wykonawcy. Udostępnianie dokumentów w formie elektronicznej pozwalającej na nieograniczoną ingerencję w treść tekstu (np. WORD), mogłoby doprowadzić do sytuacji, w których trudno byłoby udowodnić, na kim spoczywa odpowiedzialność za zmianę pierwotnego brzmienia tekstu.

Należy stwierdzić, iż w omawianym przypadku ustawowy wymóg udostępnienia SIWZ został spełniony przez Zamawiającego, a format opublikowania SIWZ nie narusza zasady równego traktowania Wykonawców; obiektywnie każdy Wykonawca jest w stanie wydrukować SIWZ ze strony internetowej Zamawiającego, a następnie przygotować i złożyć ofertę.

**II.**

**1.** W opisie przedmiotu zamówienia, w pozycji „Zakres prac audytowych", pkt 2 zapisane jest wymaganie przeprowadzenia „podstawowego audytu infrastruktury oraz sieci"

Pytanie 1: Co dokładnie Zamawiający rozumie pod pojęciem „podstawowy audyt infrastruktury oraz sieci"?

Odpowiedź: Pod pojęciem „podstawowy audyt infrastruktury oraz sieci" należy rozumieć audyt przedstawionej do wglądu dokumentacji infrastruktury oraz sieci, obejmującej swym zakresem audytowane aplikacje. Patrz odpowiedź na zapytanie II.2.

**2.** Przedmiotem zamówienia jest przeprowadzenie audytu bezpieczeństwa czterech aplikacji WWW metodą „czarnej skrzynki", tj. bez znajomości kodów źródłowych oraz bez znajomości konfiguracji aplikacji. Natomiast w dalszej części opisu przedmiotu zamówienia, w punkcie „Zakres prac audytowych" wymagane jest wykonanie przeglądu architektury logicznej (pkt 1).

Pytanie 2: W jaki sposób należy rozumieć żądanie wykonania przeglądu architektury logicznej jeżeli żadne informacje o aplikacji nie będą dostępne („czarna skrzynka")?

Odpowiedź: Przegląd architektury logicznej nastąpi na podstawie dokumentacji infrastruktury oraz sieci, udostępnionej Wykonawcy przez Zamawiającego do wglądu po zawarciu umowy. Wgląd do dokumentacji możliwy będzie tylko i wyłącznie w siedzibie Zamawiającego, a więc w miejscu wskazanym w pkt IV ppkt 2 SIWZ, które co do zasady jest miejscem wykonania zamówienia.

**3.** Pkt IV SIWZ, ppkt 2 wskazuje siedzibę zamawiającego jako miejsce wykonania usługi.

Pytanie 3: Czy wskazanie siedziby Zamawiającego jako miejsca wykonania usługi oznacza, że aplikacje podlegające testowaniu nie są dostępne z Internetu?

Odpowiedź: Aplikacje są dostępne z Internetu.

**4.** Pytanie 4: Jeżeli testowane aplikacje nie są dostępne z Internetu to jak należy rozumieć żądanie zastosowania technik „gogle hacking" (Zakres prac audytowych, pkt 4.)

Odpowiedź: patrz odpowiedź na zapytanie II.3.

**5.** Pytanie 5: Jeżeli testowane aplikacje nie są dostępne z Internetu to czy Zamawiający dopuszcza wykonanie testów aplikacji przez wykonawcą zdalnie, poprzez kanał VPN?

Odpowiedź: patrz odpowiedź na zapytanie II.3.

**6.** Pytanie 6: Jeżeli testowane aplikacje są dostępne z Internetu to czy Zamawiający dopuszcza wykonanie testów aplikacji przez wykonawcą zdalnie, poprzez Internet?

Odpowiedź: Tak, Zamawiający dopuszcza wykonanie testów aplikacji zdalnie, poprzez Internet.

**7.** Pytanie 7: Czy zamawiający udostępni oferentom wymagane wzory oświadczeń i formularzy w formie plików MS Word?

Odpowiedź: patrz odpowiedź na zapytanie I.8.

**III.**

**1.** Czy możliwe jest oszacowanie ilości formularzy aplikacji podlegających audytowi? – jesli tak prosimy o podanie ilości?

**2.** Jakiej technologii i jakiej platformy programistycznej użyto do zbudowania aplikacji?

Odpowiedź ad. 1:

| Aplikacja | Szacunkowa ilość stron | Przewidziane role |
|---|---|---|
| Apl 1 | 50 | użytkownik standardowy |
| Apl 1 | 1 | brak użytkownika |
| Apl 2 | 50 | użytkownik standardowy |
| Apl 2 | 0 | brak użytkownika |
| Apl 3 | 10 | użytkownik standardowy |
| Apl 3 | 1 | brak użytkownika |
| Apl 4 | 4 | użytkownik standardowy/ brak użytkownika |

Odpowiedź ad. 2: patrz odpowiedź na zapytanie I.7.

IV.

**1.** Dla każdej aplikacji WWW prosimy o podanie, w jakiej roli będzie występował napastnik tzn.:

a) napastnik nie posiada konta w testowanym systemie

b) napastnik posiada konto w badanym systemie o standardowych (obniżonych) uprawnieniach

c) napastnik posiada konto w badanym systemie o uprawnieniach administratora

d) ewentualne inne/jakie?

Odpowiedź: Dla każdej aplikacji należy uwzględnić dwa warianty postępowania napastnika:

I. Nie posiada konta.

II. Posiada konto o standardowych uprawnieniach.

**2.** Dla każdej aplikacji WWW i dla każdej roli w jakiej będzie występował napastnik (przedstawione powyżej) prosimy o podanie przybliżonej liczby (rząd wielkości) podstron, które będą testowane (napastnik będzie miał do nich dostęp) - np. kilka, kilkanaście, kilkadziesiąt podstron.

Odpowiedź: patrz odpowiedź na zapytanie III.1.

Udzielone odpowiedzi (wyjaśnienia), w tym wprowadzone zmiany stają się częścią SIWZ.

Zmian dokonuje się w oparciu o art. 38 ust. 4 ustawy Prawo zamówień publicznych.

Na mocy art. 38 ust. 6 ustawy, w związku z tym, iż niezbędny jest dodatkowy czas na wprowadzenie zmian w ofertach, przedłuża się termin składania ofert **do dnia 20.06.2011 r. do godz. 11.00.** Otwarcie ofert nastąpi w tym samym dniu **o godz. 11.30.**

Odpowiedniej zmianie w zakresie terminu składania i otwarcia ofert ulega pkt X lit. D (ramka) oraz pkt XI ppkt 1 i ppkt 4 SIWZ.

Wykonawca winien uwzględnić udzielone wyjaśnienia, w tym zmiany, przygotowując ofertę.

Z upoważnienia Dyrektora
Śląskiego Oddziału Wojewódzkiego
Narodowego Funduszu Zdrowia w Katowicach
ZASTĘPCA DYREKTORA
DS. EKONOMICZNO-FINANSOWYCH
Dorota Suchy

Wydziału [illegible] Gospodarczego
Śląskiego [illegible]
Narodowego [illegible] w Katowicach
NACZELNIK
Marian Ziołko

KIEROWNIK
Działu Inwestycji i Zamówień Publicznych
Śląskiego Oddziału Wojewódzkiego
Narodowego Funduszu Zdrowia w Katowicach
Tomasz Słoczkowski