Państwowy Instytut Geologiczny
Państwowy Instytut Badawczy

Państwowa służba geologiczna
Państwowa służba hydrogeologiczna

EZ-240-65/2016/ 361 /16/PP

Warszawa, dnia 31.10. 2016 r.

Wykonawcy

Dotyczy postępowania o udzielenie zamówienia publicznego na: dostawę oprogramowania do zarządzania tożsamością użytkowników systemów PSG i PSH wraz z dostosowaniem systemów dziedzinowych – zakup nowych licencji (migracja licencji oprogramowania) wraz z wdrożeniem (usługa).
Sygn. postępowania: EZ-240-65/2016

ZMIANA TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Działając na podstawie **art. 38 ust. 4** ustawy Prawo zamówień publicznych, Zamawiający zmienia treść Specyfikacji Istotnych Warunków Zamówienia.

Zmianie ulega treść załącznika nr 1 do SIWZ – opis przedmiotu zamówienia.

Zamawiający dokonuje zmiany w zakresie szczegółowego opisu przedmiotu zamówienia, pkt 1 Migracja posiadanych licencji (strona 20 SIWZ).

Zmiana dotyczy zapisu:

„Oprogramowanie będzie objęte 12 miesięczną asystą techniczną na poziomie Software Update License &Support. W skład usługi wchodzić będzie 10 dni pracy inżyniera będącego pracownikiem producenta oprogramowania, który będzie świadczył usługi zaawansowanej asysty technicznej (tunning i optymalizacja wykorzystania oprogramowania, doradztwo wdrożeniowe i architektoniczne)."

Zamawiający dokonuje zmiany na:

„Oprogramowanie będzie objęte 12 miesięczną asystą techniczną na poziomie Software Update License &Support. W skład usługi wchodzić będzie 10 dni pracy **kwartalnie** inżyniera będącego pracownikiem producenta oprogramowania, który będzie świadczył usługi zaawansowanej asysty technicznej (tunning i optymalizacja wykorzystania oprogramowania, doradztwo wdrożeniowe i architektoniczne).
Rozwiązywanie błędów powinno być realizowane w ramach asysty technicznej, natomiast dodatkowe dni muszą dotyczyć konsultingu producenta (wsparcia wdrożenia)."

W załączeniu przekazujemy aktualną treść załącznik nr 1 do SIWZ – opis przedmiotu zamówienia.

Pozostałe postanowienia SIWZ pozostają bez zmian.

Powyższe zmiany należy uwzględnić przy składaniu ofert.

ZASTĘPCA DYREKTORA
Państwowego Instytutu Geologicznego
Państwowego Instytutu Badawczego
DYREKTOR ds. GEOINFORMACJI
dr Tomasz Nateca

Załącznik nr 1 do SIWZ

Przedmiotem zamówienia jest: dostawa oprogramowania do zarządzania tożsamością użytkowników systemów PSG i PSH wraz z dostosowaniem systemów dziedzinowych – zakup nowych licencji (migracja licencji oprogramowania) wraz z wdrożeniem (usługa)

Opis przedmiotu zamówienia

Przedmiotem zamówienia obejmuje:

1) Usługę migracji posiadanych przez Zamawiającego licencji Oracle Identity&Access Management Suite do pakietu Enterprise Information Security Suite zgodnie z zasadami producenta wraz z roczną usługą asysty technicznej.
2) Usługę wdrożeniową dostarczonego oprogramowania.
3) Przeprowadzenie warsztatów

Zgodnie z art. 29 ustawy PZP Zamawiający **dopuszcza składanie ofert równoważnych**. Ilekroć w niniejszej SIWZ przedmiot zamówienia został określony przez wskazanie znaków towarowych, patentów, pochodzenia itp. Intencją Zamawiającego było przedstawienie „typu" towaru spełniającego wymagania Zamawiającego. W związku z tym dopuszczalne jest zaoferowanie przez Wykonawcę rozwiązania równoważnego, które zagwarantuje nie gorsze normy, parametry i standardy techniczno-jakościowe oraz funkcjonalne. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest zobowiązany wykazać w złożonej ofercie, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego.
W przypadku złożenia oferty równoważnej, wykonawca ma obowiązek wykazania zgodności produktów, poprzez porównanie parametrów oferowanych technologii z parametrami przedmiotu zamówienia.

Szczegółowy opis przedmiotu zamówienia

1. Migracja posiadanych licencji.

Przedmiotem zamówienia jest migracja posiadanych przez Zamawiającego licencji oprogramowania Oracle Identity&Access Management Suite do 2 licencji pakietu Enterprise Information Security Suite lub do oprogramowania równoważnego, wraz z 12 miesięczną usługą wsparcia na poziomie Software Update License &Support lub z usługą wsparcia równoważną, zgodnie z zasadami producenta.

Lista posiadanego przez Zamawiającego oprogramowania Oracle jest następująca:

Nazwa licencji	Liczba	Metryka
Identity And Access Management Suite	500	non employee user
Identity And Access Management Suite	200	employee user

Aktualnie powyższe oprogramowanie jest częścią środowiska Zamawiającego. W środowisku tym działa szereg aplikacji, w tym służące jako repozytorium tożsamości, aplikacje służące do obsługi

procesu udzielania i przechowywania uprawnień. Repozytorium danych dla tych aplikacji stanowi baza Oracle Database Enterprise Edition.

Zamawiający oczekuje migracji powyższych licencji do następujących:

Nazwa licencji	Liczba	Metryka
Oracle Enterprise Information Security Suite	2	processor

1) Wymagania dla licencji równoważnych

Zakup licencji oprogramowania wraz ze wsparciem technicznym, o których mowa powyżej jest uzupełnieniem stanu licencyjnego dla systemów już posiadanych przez Zamawiającego, działających w oparciu o oprogramowanie Oracle. Dopuszcza się oferowanie produktów równoważnych. Równoważności dotyczy zakupu licencji oprogramowania, oraz usługi wsparcia technicznego. Równoważność oznacza, że:

a) Minimalne warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja każdego z produktów wymienionych w przedmiocie zamówienia.
b) Nabycie oprogramowania równoważnego pozwala na legalne użytkowanie posiadanych przez Zamawiającego licencji oprogramowania Oracle.
c) Nabycie oprogramowania równoważnego nie powoduje powstania żadnych dodatkowych kosztów związanych z używaniem przez Zamawiającego licencji oprogramowania Oracle.
d) W efekcie zakupu Zamawiający przestanie być użytkownikiem pakietu Identity&Access Management Suite oraz nie będzie ponosił kosztów asysty technicznej do tych licencji.
e) Minimalna funkcjonalność oprogramowania równoważnego musi być porównywalna z funkcjonalnością oprogramowania, o którym mowa w przedmiocie zamówienia.
f) Oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać z oprogramowaniem Oracle posiadanym przez Zamawiającego (tj.: Oracle Database Enterprise Edition; Oracle WebLogic Server Standard Edition; Oracle SOA Suite for Oracle Middleware; Oracle Unified Business Process Management Suite).
g) Oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo – programowego Zamawiającego.
h) Oprogramowanie równoważne musi w pełni współpracować z systemami już eksploatowanymi przez Zamawiającego.
i) Oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienność produktu z produktem Oracle.
j) Warunki i zakres usługi wsparcia dla oprogramowania równoważnego nie mogą być gorsze niż usługa wsparcia określona w przedmiocie zamówienia.

Wykonawca oferujący produkt równoważny musi wykazać spełnienie wszystkich warunków opisanych powyżej, a także zobowiązać się do:

a) Dokonania wspólnie z Zamawiającym instalacji, przeniesienia danych, oraz testowania oprogramowania równoważnego w środowisku sprzętowo-programowym Zamawiającego, zapewniającą równoległą współpracę w czasie rzeczywistym z systemami posiadanymi przez Zamawiającego.
b) W przypadku, gdy oferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współpracować ze sprzętem i oprogramowaniem Zamawiającego i/lub

spowoduje zakłócenia w funkcjonowaniu środowiska sprzętowo- programowego Zamawiającego, Wykonawca pokryje wszelkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo – programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo – programowego Zamawiającego, również po odinstalowaniu oprogramowania równoważnego.

c) W przypadku wystąpienia zdarzenia opisanego w lit. b) Zamawiający ma prawo odstąpić od Umowy.

2) *Funkcjonalnie oprogramowanie równoważne musi spełniać następujące wymagania:*

- System zarządzania tożsamością musi umożliwiać wnioskowanie o uprawnienia w taki sposób, aby w przypadku konfliktu uprawnień ostrzegał wnioskującego o takiej niezgodności.
- System zarządzania tożsamością musi umożliwiać przypisywanie właściciela informacji (tzw. business owner lub data owner) do wybranego uprawnienia (uprawnienie rozumiane jest jako dostęp do informacji).
- System zarządzania tożsamością musi umożliwiać przypisanie klasyfikacji (np. tajne) do wybranego uprawnienia.
- System zarządzania tożsamością musi umożliwiać przypisanie określonego ryzyka (np. wysokie) do wybranego uprawnienia, odwzorowując w ten sposób ryzyka opisane w procesie analizy ryzyka. Określenie ryzyka powinno być odpowiednio wyeksponowane w konsoli zarządzającej, np. poprzez kolory.
- System zarządzania tożsamością musi umożliwiać opisanie każdego uprawnienia językiem opisowym, zrozumiałym dla odbiorów biznesowych, nie technicznych.
- System zarządzania tożsamością musi umożliwiać przegląd wszystkich skonfigurowanych uprawnień w dowolnym systemie gdzie pracownik ma konto. Niezbędna jest pełna informacja dotycząca pracownika w obszarze jego ról, zagregowanych uprawnień, przypisanych kont w istniejących systemach i aplikacjach, wraz z ich nazwami.
- System zarządzania tożsamością musi umożliwiać właścicielowi danych (tzw. data owner) weryfikację dostępu do informacji, za które jest odpowiedzialny. Właściciel informacji musi mieć możliwość zablokowania dostępu wybranych użytkowników do zasobów, za które jest odpowiedzialny.
- System zarządzania tożsamością musi umożliwiać właścicielowi dowolnej struktury biznesowej (np. kierownikowi określonego pionu) na dokładną analizę i weryfikację uprawnień nadanych jego pracownikom.
- System zarządzania tożsamością musi umożliwiać weryfikację uprawnień (tzw. certyfikację) w oparciu o ryzyka (tj. najpierw weryfikować uprawnienia z kategorii najwyższych ryzyk).
- System zarządzanie tożsamością musi umożliwiać właścicielowi dowolnej struktury biznesowej (np. kierownikowi określonego pionu) na czasową akceptację uprawnienia dla dowolnego pracownika. Z chwilą, gdy określony czas minie, uprawnienie to powinno zostać automatycznie odebrane.
- System zarządzania tożsamością musi umożliwiać właścicielowi dowolnej struktury biznesowej (np. kierownikowi określonego pionu) na łatwą weryfikację uprawnień nadanych jego pracownikom. System musi pokazywać role nadane pracownikowi, ich ilość, wszystkie konta nadane pracownikowi oraz umożliwić dokładną analizę zarówno ról i uprawnień.

- System zarządzania tożsamością musi umożliwiać eksport wyników procesu certyfikacji do pliku w popularnych formatach, tj. pdf lub xlsx.
- System zarządzania tożsamością musi umożliwiać właścicielowi dowolnej struktury biznesowej, właścicielowi danych, łatwą weryfikację ryzyk związanych z informacją (uprawnienia), rolą (rola biznesowa), kontami zarządzanymi, oraz sumarycznego ryzyka szacowanego dla użytkownika.
- System zarządzania tożsamością musi umożliwiać stworzenie ról biznesowych (stanowiskowych) opisujących piastowane stanowisko w firmie. Rola biznesowa, powinna zawierać inne role (np. techniczne), opisujące przydział uprawnień w systemach czy aplikacjach stosowanych przez zamawiającego.
- System zarządzania tożsamością musi umożliwiać analizy statystyczne uprawnień, np. poprzez techniki maningowe, tak aby możliwe było zdefiniowanie najlepszego zestawu ról, zawierającej określone uprawnienia.
- System zarządzania tożsamością musi umożliwiać ustawienie dowolnego procentu wspólnych uprawnień dla wybranej grupy użytkowników, a następnie przypisać taki zestaw uprawnień do określonej roli.
- System zarządzania tożsamością musi umożliwiać zaimportowanie istniejącego i stosowanego zestawu ról i uprawnień, a następnie umożliwić porównanie ról, tak aby możliwe było określenie efektywności stosowanego modelu ról.
- System zarządzania tożsamością musi umożliwiać przypisanie właściciela do dowolnej roli biznesowej, tak aby stworzenie czy modyfikacja roli były przez niego weryfikowane w specjalnym procesie akceptacyjnym.
- System zarządzania tożsamością musi umożliwiać określenie specjalnych reguł dotyczących ról, tak aby przy spełnieniu określonych warunków (np. pracownik otrzymuje rolę serwisową przy założeniu, że jego przełożonym jest kierownik sekcji serwisu IT), przydział roli następował automatycznie
- System zarządzania tożsamością musi udostępniać mechanizm wersjonowania ról, tak aby możliwe było przeanalizowanie zmian w dowolnym czasie wstecz, oraz aby możliwy był powrót konfiguracyjny do dowolnej roli wstecz.
- System zarządzania tożsamością musi udostępniać mechanizm porównywania dowolnych wersji ról, tak aby możliwa była dokładna weryfikacja różnic między obecnie stosowaną wersją roli, a dowolną historyczną.
- System zarządzania tożsamością musi udostępniać mechanizm przypisania roli do dowolnej struktury (np. organizacyjnej), tak, aby występowanie roli było związane ze ściśle określonym miejscem w hierarchii (np. organizacyjnej).
- W przypadku zmiany organizacyjnej, zmiany przełożonego, dla dowolnego pracownika, system zarządzania tożsamością musi wykonać proces weryfikacji uprawnień (certyfikacji) oraz wykonać pełny audyt w obszarze uprawnień, tak, aby można było precyzyjnie kontrolować wpływ zmiany na dotychczasowy model uprawnień.
- System zarządzania tożsamością powinien umożliwić właścicielowi roli bądź właścicielowi informacji, definiowanie procesów akceptacyjnych w przypadku zdarzeń typu: dowolna zmiana w roli (biznesowej oraz technicznej), stworzenie nowej roli (biznesowej oraz technicznej).
- Repozytorium systemu zarządzania tożsamością musi umożliwiać odebranie uprawnień dla konta administratora bazy (konto z pełnymi uprawnieniami) oraz umożliwiać rozdysponowanie tych uprawnień do innych kont. Centralne repozytorium systemu zarządzania tożsamością powinno posiadać wewnętrzne mechanizmy ograniczania konta administratora bazy w taki sposób, aby rozdysponowanie tych uprawnień do innych kont umożliwiało pełne zarzadzanie repozytorium jednak z koniecznością wykorzystania kilku kont.

- Repozytorium systemu zarządzania tożsamością musi wspierać utrzymanie spójności danych, poprzez możliwość definicji więzów integralności w strukturze repozytorium.
- Repozytorium systemu zarządzania tożsamością musi wspierać możliwość łatwego transferu danych z instancji produkcyjnej do instancji testowych oraz deweloperskich, w celu wykonania testów oraz dewelopmentu w oparciu o reprezentatywny wolumen danych.
- Repozytorium musi wspierać możliwość określenia w procesie transferu, które dane zostaną poddane anonimizacji. Proces anonimizacji musi zachować spójność danych.
- Repozytorium systemu zarządzania tożsamością musi umożliwiać przechowywanie danych w formacie blob (np. zdjęcia pracowników, zewnętrzne dokumenty zaimportowane do repozytorium w ramach procesu wnioskowania o uprawnienia etc.)
- Repozytorium systemu zarządzania tożsamością musi umożliwiać szyfrowanie wszystkich lub wybranych danych, zarówno w trakcie transmisji jak i zapisu na dysk.
- Repozytorium systemu zarządzania tożsamością musi się znajdować w relacyjnej bazie danych. System zarządzania tożsamością komunikując się ze swoim repozytorium musi bezpośrednio sięgać do danych, znajdujących się w relacyjnej bazie danych.
- System zarządzania tożsamością musi być zbudowany i wdrożony z wykorzystaniem najlepszych praktyk odnośnie bezpieczeństwa dostępu do danych. Rozumianych, jako zapewnienie niezawodności poprzez architekturę HA, poufności poprzez realizację wymogów szyfrowanego dostępu i zapisu na dysk w repozytorium tożsamości, jak również integralności na poziomie zastosowanego repozytorium tożsamości.
- System zarządzania tożsamością musi pozwolić na reprezentację firmy, jako hierarchicznej struktury organizacyjnej.
- System musi umożliwiać przypisanie pracownika do kilku organizacji jednocześnie.
- System musi udostępniać możliwość utworzenia i uruchomienia procesu automatycznej synchronizacji struktury organizacyjnej, na podstawie wskazanego źródła (np. system HR, ekstrakt w postaci pliku CSV).
- System musi pozwalać prezentować tożsamości w ramach innych struktur niż organizacyjna (np. projektowa, raportowa, aplikacyjna).
- System zarządzania tożsamością musi umożliwiać definiowanie reguł wykluczających szansę jednoczesnego nadania użytkownikowi kolidujących ze sobą uprawnień (SoD).
- System zarządzania tożsamością musi dostarczać mechanizm pozwalający zidentyfikować naruszenia zdefiniowanych reguł SoD.
- System zarządzania tożsamością musi umożliwiać integrację z dedykowanymi zewnętrznymi systemami do zarządzania rolami.
- Przez integrację rozumiana jest, co najmniej możliwość importu danych o uprawnieniach, z repozytorium systemu zarządzania tożsamością do systemu zarządzania rolami oraz możliwość eksportu definicji ról i przypisania użytkowników do ról, z systemu zarządzania rolami do systemu zarządzania tożsamością.
- Interfejs wnioskowania w systemie zarządzania tożsamością (składanie, obsługa, przeglądanie historii etc.) musi być dostępny w całości w języku polskim.
- System zarządzania tożsamością musi wspierać zarządzanie kontami serwisowymi, umożliwiając ich obsługę na innych zasadach niż konta użytkowników, np. nie blokowanie kont wraz z blokadą tożsamości, do której przypisane jest dane konto serwisowe.
- System zarządzania tożsamością musi umożliwiać definiowanie reguł i polityk audytowych pozwalających przeskanować repozytorium tożsamości w poszukiwaniu określonych sytuacji, stanowiących potencjalne ryzyko naruszenia zasad bezpieczeństwa.

- System zarządzania tożsamością musi umożliwiać zdefiniowanie procesu cyklicznego skanowania repozytorium tożsamości, z użyciem przygotowanych wcześniej polityk audytowych.
- System zarządzania tożsamością musi udostępniać możliwość zdefiniowania poziomów ryzyka związanych z poszczególnymi zagrożeniami identyfikowanymi przez reguły (np. poziom ryzyka wysoki, średni, niski).
- System zarządzania tożsamością musi umożliwiać proces obsługi znalezionych naruszeń zdefiniowanych polityk audytowych, poprzez umożliwienie czasowej, bądź stałej akceptacji ryzyka (uzasadnione odstępstwo od reguł) lub zamknięcie incydentu.
- System zarządzania tożsamością musi umożliwiać zdefiniowanie procedur minimalizacji wykrytego ryzyka, w postaci procedury prezentowanej w raporcie audytowym.
- System zarządzania tożsamością musi umożliwiać zdefiniowanie osoby odpowiedzialnej za rozwiązanie założonego incydentu, przez proces skanujący repozytorium tożsamości.

Oprogramowanie będzie objęte 12 miesięczną asystą techniczną na poziomie Software Update License &Support. W skład usługi wchodzić będzie 10 dni pracy kwartalnie inżyniera będącego pracownikiem producenta oprogramowania, który będzie świadczył usługi zaawansowanej asysty technicznej (tunning i optymalizacja wykorzystania oprogramowania, doradztwo wdrożeniowe i architektoniczne). Rozwiązywanie błędów powinno być realizowane w ramach asysty technicznej, natomiast dodatkowe dni muszą dotyczyć konsultingu producenta (wsparcia wdrożenia).

2. Usługa wdrożeniowa dostarczonego oprogramowania.

Zamawiający będzie zlecał prace w zakresie instalacji i konfiguracji dostarczonego oprogramowania, zgodnie z warunkami określonymi w § 3 Załącznika nr 2 do SIWZ – Istotne postanowienia umowy, w maksymalnym wymiarze 150 dni roboczych (1 dzień roboczy rozumiany jest jako 8 godzin roboczych).

3. Warsztaty

Wykonawca zobowiązany jest przeprowadzić warsztaty:

1. Wykonawca zobowiązany jest do przeprowadzenia Warsztatów dla użytkowników podstawowych oraz administratorów z dostarczonego oprogramowania.
2. Warsztaty powinny być specyficzne dla każdej z grup oprogramowania.
3. Warsztaty dla użytkowników podstawowych Wykonawca zobowiązany jest przeprowadzić dla grupy 8 osób Zamawiającego. Warsztat powinny obejmować podstawy z modelowania i implementacji procesów w dostarczonym oprogramowaniu.
4. Warsztaty dla administratorów Wykonawca zobowiązany jest przeprowadzić dla grupy 5 osób Zamawiającego. Warsztat powinny obejmować podstawy administrowania zakupionym oprogramowaniem.
5. Czas trwania warsztatów dla użytkowników podstawowych oraz administratorów nie może być krótszy niż jeden dzień (8 godzin) na grupę użytkowników podstawowych oraz jeden dzień (8 godzin) na grupę administratorów. Warsztaty dla grupy użytkowników podstawowych oraz grupy administratorów nie mogą odbywać się w tym samym terminie.
6. Zakres warsztatów użytkowników podstawowych z oprogramowania musi umożliwiać użytkownikom samodzielną pracę z właściwym wykorzystaniem podstawowych funkcjonalności oprogramowania.
7. Zakres warsztatów z administrowania oprogramowaniem musi umożliwiać administratorom zapoznanie się z podstawowymi funkcjami w zakresie administrowania oprogramowaniem.

8. Szczegółowy zakres, terminy oraz materiały warsztatowe muszą być uzgodnione z Zamawiającym w planie szkoleń.

9. Sale i sprzęt do szkoleń, wraz z cateringiem zapewnia Wykonawca.

10. Po zakończeniu warsztatów Wykonawca zobowiązany jest do sporządzenia raportu.