

Opis Przedmiotu Zamówienia

dot. CRZP/145/2021/AZP – Świadczenie wsparcia technicznego i gwarancji na usługę: Centralny Systemu Zarządzania Użytkownikami Uniwersytetu Morskiego w Gdyni (UMG)

1. Wstęp

W roku 2018 Uczelnia wdrożyła Centralny Systemu Zarządzania Użytkownikami (zwanego dalej CSZU) realizującego na bazie sprzętu oraz oprogramowania) składającego się klastra zawierającego 3 serwery firmy DELL z zainstalowanym środowiskiem wirtualizacji Windows Server 2016 Datacenter Edition oraz macierzy firmy DELL. Na bazie sprzętu uruchomiono szereg usług Microsoft niezbędnych Uczelni będących komponentami CSZU. W ciągu 3 lat eksploatacji systemu CSZU w połowie 2021 roku system CSZU został rozszerzony o usługę ADFS w celu wspierania uczelni z korzystania mechanizmów tożsamości federacyjnych, a w szczególności wykorzystania ich w programie Erasmus+/Edugain.

2. Przedmiot zamówienia

Przedmiotem Zamówienia jest świadczenie w okresie 12 miesięcy na rzecz Uniwersytetu Morskiego w Gdyni (w skrócie UMG) usługi wsparcia (na odpowiednim poziomie – SLA) reaktywnego i proaktywnego pakietu 36 godzin wraz z udzieleniem gwarancji na działanie poniżej opisanej funkcjonalności/usług CSZU:

1. Usługa zarządzania tożsamością dla około 9000 użytkowników UMG w oparciu o Active Directory firmy Microsoft z obsługą około 1000 kont pracowników oraz ok. 8000 kont studentów wraz z rozdzieloną logicznie domeną studencką i pracowniczą. Usługa katalogowa AD zapewnia redundancję oraz skalowalność jako pojedynczy las z domeną root'ową oraz dwoma poddomenami z wykorzystaniem do tego infrastruktury Active Directory pełniącej rolę usługi katalogowej (LDAP) będącej rdzeniem zarządzania tożsamościami w środowisku UMG z kontrolerami lokalnych domen, DC (domeny umg.local, pracownik.local, student.local)
2. Usługa DNS dla w/w domen,
3. Świadczenie usługi pojedynczego logowania z wykorzystaniem mechanizmów Windows Integrated Authentication w przypadku komputerów podłączonych do w/w domen Windows do zasobów środowiska domenowego Windows uczelni UMG,
4. Usługa zautomatyzowanego i cyklicznego zasilania za pomocą Microsoft Identity Manager 2016 (MIM 2016) usługi katalogowej AD obiektami użytkowników (pracowników i studentów) z określonych istniejących systemów Zamawiającego: Simple ERP oraz Simple EDU (Bazus) za pomocą narzędzi/skryptów, aplikacji oraz innych systemów. System realizuje również aktualizację zmian na obiektach już utworzonych oraz wyłączanie kont nieaktywnych użytkowników,
5. Usługa integracja z edukacyjnym środowiskiem Uczelni Microsoft365 w zakresie synchronizacji tożsamości (za pomocą usługi konektora Ad Connect) oraz obsługi uwierzytelniania i autoryzacji użytkowników do usług Office 365 wraz z weryfikacją, poprawności działania i stanu oraz bezpieczeństwa po stronie edukacyjnego tenanta Microsoft365 w zakresie: synchronizacji tożsamości, przydziału licencji użytkownikom, działania usługi Azure AD UMG oraz usług/aplikacji po stronie samego tenanta edukacyjnego Microsoft365: licencjonowanie/subskrypcje, Exchange Online, On-Drive, Sharepoint, czy też Ms-Teams,
6. Mechanizm uwierzytelniania i autoryzacji z wykorzystaniem usług federacyjnych dla aplikacji WEB, w którym jest możliwość wykorzystania uwierzytelniania za pomocą mechanizmów/protokołów WSFED, SAML 2.0 lub OAUTH. Świadczenie usługi IDP (Identity Provider) za pomocą dwóch serwerów ADFS poprzez proxy ADFS (zrealizowanego za pomocą KEMP - usługa proxy dla serwerów ADFS) w celu wspierania uczelni w programie Erasmus+/Edugain z wykorzystaniem tożsamości federacyjnych z odpowiednią konfiguracją i transformacją Claimów /atrybutów źródłowych na atrybuty wymagane przez Erasmus+/Edugain tak zwanych „Relying Party Trustów”,

7. Usługa testowego serwera z przykładową aplikacją pokazującą wykorzystanie claimów,
8. Usługa klastra MSSQL składającego się z dwóch serwerów baz danych SQL 2016,
9. Usługa Exchange Server 2016 CU 10 działającego w konfiguracji hybrydowej
10. Usługa WSUS dla celów aktualizacji dla serwerów i komputerów w sieci serwerowej,
11. Usługa serwera/jednostki certyfikującej dla PKI wraz z serwerem CDP/AIA/OCSP dla infrastruktury PKI,
12. Usługa serwery plików z wykorzystaniem DFS (Distributed File System)
13. Weryfikacji stanu i bezpieczeństwa oraz wsparcie w zakresie prawidłowej konfiguracji niezbędnych poprawek, aktualizacji odpowiednich systemów operacyjnych poszczególnych komponentów CSZU (posadowionych jako wirtualne maszyny Hyper-V z zainstalowanym zazwyczaj systemem Windows Server w środowisku Windows Datacenter 2016) oraz wykonywania niezbędnych konfiguracji oprogramowania i/lub modyfikacji dla w/w usług określonych w punktach 1-12,
14. Usługa weryfikacji i poprawności działania platformy sprzętowo-programowej składającej się klastra zawierającego 3 serwery firmy DELL (DELL R740, o numerach ST: JN188C2, JN18CC2, JN18DP2) z zainstalowanym środowiskiem wirtualizacji Windows Server 2016 Datacenter Edition oraz macierzy firmy DELL (MD3820i, ST: H4YS9Q2) udostępniającej za pomocą protokołu iSCSI na potrzeby serwerów zasoby pamięci zewnętrznej z wykorzystaniem przełączników DELL z serii S4048 TOR (Top of the Rack),

3. Zasady i realizacja wsparcia proaktywnego

Realizacja wsparcia proaktywnego świadczona będzie na zasadach zbliżonych do realizacji procesu projektowego. Oprócz wsparcia reaktywnego i świadczenia gwarancji dla w/w usług (punkty od 1 do 14) zakres świadczonych usług ma charakter otwarty i dodatkowo może obejmować w zaoferowanym pakiecie 36 godzin wsparcia poniższe usługi:

- rozbudowę systemu o nowe funkcjonalności,
- przeprowadzenie dedykowanych warsztatów lub autorskich szkoleń,
- weryfikację poprawności pracy systemu,
- omówienie aktualnych zmian w systemie,
- przedstawienie możliwości rozwoju systemu uwzględniając aktualne trendy,
- przygotowanie lub aktualizację dokumentacji systemu w związku z wykonaniem niezbędnych czynności / poprawek / rekonfiguracji / modyfikacji, które powinny zostać udokumentowane.
- Inne konsultacje związane z zakresem realizowanej umowy.

Zamawiający przedstawi specyfikację potrzeb lub wykaz zadań do realizacji, a następnie Wykonawca przygotuje oszacowanie pracochłonności zlecenia oraz możliwy termin realizacji poszczególnych zadań.

- Wycena zleconych prac w godzinach: do 3 dni roboczych.
- Gotowość do podjęcia realizacji prac: do 10 dni roboczych.
- Obsługa działań proaktywnych może być realizowana zdalnie z wykorzystaniem tunelu VPN zapewnionego przez Zamawiającego lub w siedzibie Zamawiającego.
- W przypadku wykonania prac w siedzibie Zamawiającego, Wykonawca musi mieć zapewniony dostęp do miejsca pracy pozwalającego na realizację usługi zgodnie z obowiązującymi standardami bezpieczeństwa i przepisami regulującymi stanowiska pracy.

4. Realizacja świadczenia wsparcia reaktywnego

Dla wsparcia reaktywnego i udzielonej gwarancji Zamawiający oczekuje odpowiedniego czasu reakcji i realizacji wsparcia dla CSZU zgodnie z przedstawioną klasyfikację stanu awarii:

Kategoria stanu awarii	Klasyfikacja awarii	Wymagane czasy reakcji, realizacji obsługi zgłoszonej awarii + gotowość
Stan krytyczny (priorytet I)	Obejmuje całkowite zatrzymanie pracy systemu lub bardzo poważne uszkodzenie, mające krytyczny wpływ na jego funkcjonalność	Czas reakcji: 2 godz.
		Czas realizacji: 8 godz.
		Gotowość: 7 dni w tygodniu 8:00 – 18:00
Stan ważny (priorytet II)	Awaria powodująca poważne niedogodności w pracy systemu i/lub powtarzające się zakłócenia, które mogą mieć znaczący wpływ na funkcjonalność systemu.	Czas reakcji: 2 godz.
		Czas realizacji: 16 godz.
		Gotowość: 5 dni w tygodniu 8:00 – 18:00
Stan zwykły (priorytet III)	Problem nie powodujący bezpośredniego wpływu na obniżenie funkcjonalności systemu. Ta klasa problemów obejmuje nieznaczne rozbieżności dotyczące funkcjonalności w porównaniu z opisami w dokumentacji oraz sporadyczne problemy i niedogodności.	Czas reakcji: 24 godz.
		Czas realizacji: 40 godz.
		Gotowość: 5 dni w tygodniu 8:00 – 18:00

- Zgłoszenia przyjmowane będą pocztą elektroniczną, przy pomocy zaproponowanego przez Wykonawcę systemu zgłoszeń lub telefonicznie.
 - Godziny przyjmowania zgłoszeń (Gotowość): zgodnie z priorytetem,
 - Czas reakcji na zgłoszenie: zgodnie z priorytetem,
 - W przypadku awarii wynikających z błędów systemów operacyjnych lub aplikacji producenta czas usunięcia awarii może się wydłużyć i nie jest zależny od Wykonawcy. Wykonawca doloży wszelkich starań, aby jak najszybciej usunąć tego typu awarie, zgłaszając problem do producenta i monitorując na bieżąco stan rozwiązania problemu.
 - W przypadku wszystkich awarii dopuszcza się czasowe obejścia:
 - realizujące prawie 100% funkcjonalności usługi
 - trwające nie dłużej niż 3 dni w przypadku rozwiązań możliwych do dostarczenia przez Wykonawcę lub trwające do czasu dostarczenia rozwiązania przez producenta.
 - oferujące niewielkie degradacje wydajności systemu.
 - Obsługa zgłoszonych awarii będzie realizowana zdalnie z wykorzystaniem tunelu VPN zapewnionego przez Zamawiającego. W przypadku zgłoszeń krytycznych dopuszcza się pracę Wykonawcy w Centrali Zamawiającego.
 - W przypadku wykonania prac w siedzibie Zamawiającego, Wykonawca musi mieć zapewniony dostęp do miejsca pracy pozwalającego na realizację usługi zgodnie z obowiązującymi standardami bezpieczeństwa.
- Definicje:**
- Czas reakcji: - czas liczony od momentu potwierdzenia odebrania maila lub od zgłoszenia telefonicznego
 - Czas realizacji: - czas liczony od zakończenia czasu reakcji
 - Czas usunięcia awarii: - czas przywrócenia pełnej funkcjonalności systemu CSZU

5. Warunki ogólne wsparcia technicznego

- Wykonawca zapewnia możliwość przyjmowania zgłoszeń od kilku wskazanych przez Zamawiającego pracowników,
- Wykonawca zapewnia dostarczanie raportów przedstawiających stan realizowanej usługi na życzenie Zamawiającego
- Wykonawca zapewnia dedykowanego koordynatora umowy wsparcia,
- Wykonawca nie wyznacza miesięcznych limitów wykorzystania godzin.