

Załącznik nr 3

do Ogłoszenia o Wstępnych Konsultacjach Rynkowych
Przedmiot wstępnych konsultacji rynkowych

1. Przedmiotem wstępnych konsultacji rynkowych jest zakup licencji, wdrożenie, integracja, wsparcie utrzymania systemu IAM/IDM/IGA oraz przeszkolenie administratorów.

Tabela I. Opis Usług będących Przedmiotem zamówienia

Lp.	Nazwa Usługi	Opisy Usługi
1.	Identity Lifecycle Management	Zarządzanie uprawnieniami do systemów; Procesy: Joiner, Mover, Leaver; Konta: pracownicy, współpracownicy, techniczne; Automatyzacja tworzenia, zmiany, blokowania i usuwania kont, archiwizacja.
2.	Provisioning i deprovisioning	Automatyczne nadawanie, zmiana i odbieranie uprawnień w systemach docelowych na podstawie danych z HR, ról, reguł, wniosków (wbudowanego flow) oraz decyzji właścicieli biznesowych.
3.	Integracja Active Directory i inne usługi Microsoft	Integracja z Active Directory, Microsoft Entra ID, Microsoft 365, Exchange Online, Exchange on-premise, grupami, licencjami, skrzynkami pocztowymi i usługami katalogowymi LDAP.
4.	Integracje HR, ERP i aplikacyjne	Integracja z systemem HR jako źródłem danych, ERP, Symfonia, Oracle, SQL, CSV, REST API, ITSM oraz aplikacjami niestandardowymi Zamawiającego.
5.	Role Management	Obsługa RBAC, ABAC, ról biznesowych, technicznych i dynamicznych, dziedziczenia uprawnień, modelowania ról, analizy konfliktów i reguł SoD.
6.	Access Governance	Certyfikacje i recertyfikacje okresowe, kampanie przeglądów uprawnień, raportowanie zgodności, audyt zmian oraz identyfikacja nadmiarowych i osieroconych uprawnień.
7.	Workflow i self-service	Portal użytkownika, katalog usług dostępowych, wielostopniowe akceptacje, delegacje, zastępstwa, eskalacje, powiadomienia, SLA i śledzenie statusu wniosku.

Lp.	Nazwa Usługi	Opisy Usługi
8.	Bezpieczeństwo	MFA, SSO, integracja z PAM Keycloak, SIEM/SOAR, szyfrowanie, logowanie zdarzeń, retencja, Zero Trust, identity threat detection and response.
9.	Architektura i infrastruktura	Wdrożenie on-premise, HA, DR, skalowalność, środowiska DEV/TEST/PROD, wymagania sieciowe, bazodanowe, monitoring, backup i aktualizacje.
10.	Licencje, koszty i utrzymanie	Modele licencyjne, koszty użytkowników, konektorów, środowisk, wdrożenia, migracji, supportu, rozwoju, utrzymania oraz TCO.

Cel realizacji zamówienia

Celem przyszłego zamówienia jest pozyskanie rozwiązania IAM/IDM/IGA umożliwiającego centralne, audytowalne i zautomatyzowane zarządzanie tożsamościami oraz uprawnieniami w środowisku Zamawiającego. Rozwiązanie powinno ograniczać ryzyka wynikające z ręcznego zarządzania uprawnieniami, zwiększać zgodność z wymaganiami bezpieczeństwa i regulacjami, przyspieszać obsługę wniosków dostępowych oraz zapewniać możliwość cyklicznej weryfikacji praw dostępu.

- utworzenie jednego, kontrolowanego procesu zarządzania tożsamością od zatrudnienia do zakończenia współpracy;
- zwiększenie przejrzystości i audytowalności nadawania, zmiany i odbierania uprawnień;
- ograniczenie liczby kont osieroconych, nadmiarowych uprawnień i ręcznych operacji administracyjnych;
- możliwość samodzielnej konfiguracji ścieżek akceptacji adekwatnych do wnioskowanego poziomu uprawnień;
- zapewnienie cyklicznej recertyfikacji dostępów przez właścicieli biznesowych i technicznych;
- przygotowanie organizacji do wymagań RODO, KRI, NIS2, ISO 27001 oraz praktyk Zero Trust i Identity Security.

Termin obowiązywania Umowy Ramowej

Na potrzeby WKR Zamawiający zakłada, że przyszłe zamówienie może obejmować dostawę licencji/subskrypcji, wdrożenie, integrację, migrację danych, szkolenia, dokumentację, asystę powdrożeniową, support oraz rozwój systemu przez okres wskazany w przyszłej dokumentacji zamówienia.

Okres wdrożenia	Do określenia w toku WKR; oczekiwane przedstawienie wariantów MVP, wdrożenia etapowego oraz pełnego wdrożenia produkcyjnego.
Okres utrzymania	Do konsultacji: 12, 24, 36 lub 48 miesięcy od odbioru produkcyjnego albo od zawarcia umowy.
Środowiska	Co najmniej TEST/PROD lub równoważny model zapewniający bezpieczne testowanie zmian.
Zakres usług	Analiza przedwdrożeniowa, projekt techniczny, konfiguracja, integracje, testy, szkolenia, dokumentacja, uruchomienie i wsparcie.
Rozwój systemu	Możliwość zamawiania nowych konektorów, kampanii recertyfikacyjnych, raportów, reguł ról i zmian procesowych.

Terminy dotyczące Umów Wykonawczych

Okres na jaki będą nabywane Usługi zostanie określony na etapie postępowania wykonawczego przez Jednostkę dokonującą zakupu. Okres będzie uregulowany w umowie wykonawczej.

Przewidywany maksymalny termin obowiązywania umów wykonawczych będzie wynosił 48 miesięcy od dnia ich zawarcia.

Zakres i warunki świadczenia Usług

1. Rozwiązanie i usługi muszą pochodzić bezpośrednio od Producenta lub z autoryzowanych przez Producenta kanałów dystrybucyjnych. Za autoryzowany kanał dystrybucji uznaje się podmioty, które na podstawie udokumentowanej zgody (np. umowa dystrybucyjna) Producenta odsprzedają Usługi.

2. Wykonawca, w cenie usługi, umożliwi korzystanie z najnowszych wersji rozwiązania, które będą aktualizowane w każdym momencie użytkowania po uprzednim powiadomieniu Jednostki. Aktualizacja rozwiązania musi być świadczona przez Wykonawcę w sposób automatyczny, niewymagający zaangażowania Jednostek, ani Centralnego Zamawiającego. Aktualizacja musi być dostępna dla wszystkich użytkowników. Aktualizacja nie może wpłynąć na obniżenie wymaganych minimalnych parametrów oraz zmniejszenie wydajności i dostępności.
3. Wykonawca dostarczy Jednostce wszelkie dane niezbędne do prawidłowego uruchomienia i korzystania z rozwiązania, w tym minimum instrukcję użytkownika oraz dokumentację konfiguracji.
4. Rozwiązanie i świadczone usługi, należące do przedmiotu zamówienia, muszą spełniać postanowienia wynikające z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.
5. Wymaga się, aby usługi były zgodne z:
 - a. Krajowymi Ramami Interoperacyjności,
 - b. Minimalnymi wymaganiami dla rejestrów publicznych i wymiany informacji w postaci elektronicznej,
 - c. Minimalnymi wymaganiami dla systemów teleinformatycznych,zawartymi w Rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r., na podstawie delegacji zawartej w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.
6. Wymagane jest, aby Wykonawca aktualizował rozwiązanie w przypadku zmiany przepisów prawa, którym podlegają Jednostki oraz zaleceń organów nadzorczych, przez cały okres trwania umowy wykonawczej. Aktualizacja musi zapewnić zgodność usługi z aktualnymi przepisami prawa oraz zaleceniami organów nadzorczych.
7. Wykonawca zapewni możliwość bezpłatnego korzystania z wersji testowej do celów nieprodukcyjnych, udostępniającej pełną funkcjonalność usług przez okres trwania umowy.

8. Wykonawca zapewni możliwość korzystania z rozwiązania poprzez przeglądarkę internetową z wykorzystaniem szyfrowanych kanałów komunikacji. Wymagane jest świadczenie Usług poprzez co najmniej przeglądarki: Google Chrome, Opera, Firefox, Microsoft Edge, Safari.
9. Wykonawca zapewni szyfrowanie przestrzeni dyskowych, na których będą przechowywane dane.
10. Wykonawca zapewni możliwość korzystania z Rozwiązania do zarządzania usługami, umożliwiającej administratorom konfigurację parametrów Usług przez jedną z przeglądarek internetowych wskazanych w pkt 8, z wykorzystaniem szyfrowanych kanałów komunikacji.
11. Wykonawca zapewni możliwość konfiguracji parametrów rozwiązania poprzez dedykowany interfejs programowania aplikacji z wykorzystaniem szyfrowanych kanałów komunikacji.
12. Wykonawca zapewni świadczenie pomocy technicznej w wymiarze 9 godzin dziennie w dni robocze, w godzinach pracy Jednostki, w zakresie obsługi rozwiązania, w tym wsparcie przy konfiguracji, on-boardingu, off-boardingu i rekonfiguracji. Wsparcie Producenta świadczone będzie przez cały okres obowiązywania umowy wykonawczej, w sposób zapewniający utrzymanie parametrów dostępności.
13. Rozwiązanie będzie posiadało wsparcie techniczne producenta w obszarze świadczenia usług i możliwości ich użycia, m.in. w zakresie dostarczania poprawek programistycznych i bezpieczeństwa, nowych wersji Oprogramowania, wydań uzupełniających. Wsparcie producenta świadczone będzie przez cały okres obowiązywania umowy wykonawczej w sposób zapewniający utrzymanie parametrów dostępności.
14. Wykonawca zapewni przyjmowanie zgłoszeń serwisowych dotyczących Incydentów przez całą dobę przez wszystkie dni w roku (24h/7/365) za pomocą systemu obsługi zgłoszeń serwisowych udostępnionego przez Wykonawcę lub za pośrednictwem dedykowanego adresu e-mail.
15. Wykonawca zapewni przyjmowanie zgłoszeń serwisowych dotyczących Incydentów i konsultacji bezpośrednich w wymiarze 8 godzin dziennie w dni robocze, w godzinach pracy Jednostki, za pośrednictwem dedykowanego numeru telefonu.

16. Incydenty zgłaszane przez Jednostkę za pomocą adresu e-mail lub telefonicznie będą rejestrowane przez Wykonawcę w systemie obsługi zgłoszeń, udostępnionym przez Wykonawcę, w sposób umożliwiający ich raportowanie wraz z danymi pozwalającymi m.in. na śledzenie czasu ich usunięcia.

Wymagania

1. Zakres funkcjonalny rozwiązania klasy IAM/IDM/IGA:
 - a. Dostępność mechanizmów monitorowania logów i działań użytkowników oraz pełnej rozliczalności w tym dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Jednostki, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione” oraz prób uwierzytelnienia użytkowników nieuprawnionych przy pomocy tożsamości niebędących na listach „wykradzione”.
 - b. Dostępność na żądanie wyników aktualnych audytów, w tym raportów z audytów bezpieczeństwa Rozwiązania lub deklaracji producenta, że oprogramowanie jest wolne od znanych podatności bezpieczeństwa (CVE).
 - c. Możliwość automatycznej instalacji poprawek dla oprogramowania, niewpływającej na ciągłość pracy systemu.
 - d. Możliwość integracji z Active Directory w celu wykorzystania integracji tożsamości z AD w Rozwiązaniu.
 - e. Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
 - f. Wbudowane w Platformę do zarządzania usługami mechanizmy zabezpieczające przed atakami DDoS.
 - g. Obsługa mechanizmów High Availability (HA), w tym możliwość uruchomienia przynajmniej dwóch równorzędnych ośrodków przetwarzania danych, oddalonych od siebie o co najmniej 100 km.
 - h. Wymagane rozwiązanie on-premises, działające na infrastrukturze Zamawiającego.
 - i. Gwarancja o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Jednostki.

- j. Gwarancja pobrania danych i raportów przez Jednostkę przez okres 14 dni od zakończenia świadczenia usług, w ramach ceny usług.
 - k. Gwarancja usunięcia wszystkich danych Jednostki z każdego nośnika na którym dane były przechowywane. Wykonawca powinien usunąć wszystkie dane po 14 dniach od zakończenia świadczenia usług oraz powinien umożliwić przeprowadzenie audytu tej czynności.
 - l. Gwarancję braku dostępu do danych Jednostki w usłudze, z wyłączeniem działań serwisowych wymagających każdorazowo zgody Jednostki i wykonywanych wyłącznie przez uprawnione osoby z organizacji Wykonawcy lub Producenta usługi.
2. Jeżeli nowa wersja usługi zawierać będzie bardziej restrykcyjne prawa do używania niż wersja, która była aktualna na dzień złożenia oferty, te bardziej restrykcyjne prawa do używania nie będą miały zastosowania do korzystania z tej usługi przez Jednostkę.

Wymagania związane z cyberbezpieczeństwem

1. Wymagania dotyczące Standardów Cyberbezpieczeństwa Chmur Obliczeniowych, o których mowa w Uchwale WIIP, ZUCH - Informacje (chmura.gov.pl), dla usług przetwarzania w chmurze, przedstawiono w poniższej tabeli.

Tabela II. Wymagania dotyczące Standardów Cyberbezpieczeństwa Chmur Obliczeniowych

Wymaganie	Poziomy Wymagań Bezpieczeństwa	
	SCCO1	SCCO2
Kategorie informacji	Niekontrolowane informacje nieklasyfikowane	Kontrolowane informacje urzędowe
Wymagane zabezpieczenia dla chmury obliczeniowej	Zabezpieczenia SCCO na poziomie NISKIM / UMIARKOWANYM potencjalnego wpływu na atrybuty bezpieczeństwa, zgodnie z Załącznikami nr 4 i 5 do Standardów Cyberbezpieczeństwa Chmur Obliczeniowych	Poziom SCCO1 + zabezpieczenia do ochrony informacji urzędowych, zgodnie z Załącznikami nr 4 i 5 do Standardów Cyberbezpieczeństwa Chmur Obliczeniowych

Wymaganie	Poziomy Wymagań Bezpieczeństwa	
	SCCO1	SCCO2
Centra przetwarzania danych - Jurysdykcja	Przetwarzanie dozwolone w centrach danych poza polską jurysdykcją	Przetwarzanie dozwolone w centrach danych w polskiej jurysdykcji
Dostęp do zasobów	Internet i/lub wydzielone usługi transmisji danych	Internet i/lub wydzielone łącza logiczne – wymagania Narodowych Standardów Cyberbezpieczeństwa
Separacja	Wirtualna/Logiczna DOSTĘP PUBLICZNY	Wirtualna/Logiczna Silna separacja pomiędzy organizacyjnymi zasobami publicznych chmur obliczeniowych (tenantami) oraz dedykowany kontrolowany dostęp do zasobów informacyjnych
Wymagania dla personelu	Personel dopuszczany przez dostawcę usług chmur obliczeniowych	Personel posiadający poświadczenia bezpieczeństwa osobowego na poziomie „POUFNE”

2. Dla poszczególnych usług Wykonawca zapewni spełnienie wymagań dotyczących bezpieczeństwa informacji zgodnie ze Standardami Cyberbezpieczeństwa Chmur Obliczeniowych na poziomie SCCO1 i SCCO2.

Opłaty

1. Licencje na rozwiązanie oraz usługi będą świadczone przez Wykonawcę na podstawie ustalonych opłat, w ramach podpisanej Umowy Wykonawczej.
2. W ramach Opłat zapewnione zostanie świadczenie najnowszych wersji oprogramowania i możliwość ich aktualizacji w każdym momencie użytkowania.

Zasady korzystania z usługi

1. Celem Umowy Ramowej jest określenie zasad świadczenia wybranych usług, w ramach umów wykonawczych, które zapewni Jednostkom możliwości korzystania z usług, jako całości, jak i wszystkich ich elementów i aktualizacji, w pełnym zakresie i bez dodatkowych kosztów.

2. Do usług świadczonych w ramach umów wykonawczych mają zastosowanie tzw. standardowe warunki Producenta dotyczące korzystania z usług, z zastrzeżeniem jednak, że warunki te nie mogą być sprzeczne z postanowieniami Umowy Ramowej i umowy wykonawczej. W przypadku pojawienia się sprzeczności między zapisami warunków licencyjnych Producenta a Umową Ramową lub umową wykonawczą, zapisy wyżej wskazanych umów są wiodące.
3. Wykonawca oświadcza i gwarantuje, że warunki korzystania z usług zgodnie z Umową Ramową nie będą wymagać od Jednostek ponoszenia jakichkolwiek opłat lub kosztów, które nie zostały wprost wskazane w Umowie Ramowej, na rzecz Wykonawcy, Producenta lub innych podmiotów. Wynagrodzenie z tytułu umowy wykonawczej każdorazowo obejmować będzie całość wynagrodzenia za korzystanie z usług objętych umową wykonawczą.
4. Wykonawca zapewnia, że rozwiązanie będące przedmiotem umowy wykonawczej nie będzie zawierało ograniczeń polegających na tym, że dane usługi mogą być używane wyłącznie z innym oprogramowaniem lub usługami spoza listy określonej powyżej lub, że może być wdrażane, serwisowane itp. wyłącznie przez określony podmiot lub grupę podmiotów.
5. Licencje na korzystanie z rozwiązania będą niewyłączne, nieograniczone terytorialnie i udzielone minimum na czas określony w umowie wykonawczej.
6. Aktualizacja lub zmiana wersji oprogramowania nie może powodować ograniczenia zakresu funkcjonalnego. W takim przypadku do aktualizacji lub zmienionej wersji oprogramowania stosuje się postanowienia Umowy Ramowej i umowy wykonawczej dotyczące licencji.