Opis Przedmiotu Zamówienia

Opis funkcjonalności rozwiązania systemu do zarządzania tożsamością.

W ramach dostarczonej usługi system musie składać się z następujących modułów i zapewnić poniższe funkcjonalności dla minimum 400 użytkowników.

1. Moduł Single Sign-On (SSO)

Wymagany jest moduł Single Sign-On oferujący zintegrowane zarządzanie dostępem z następującymi funkcjami:

* 1. Rozległa sieć integracji umożliwiająca łatwe połączenie z różnymi aplikacjami (min. 7800 gotowych integracji).
	2. Wsparcie dla protokołów komunikacji:
* SAML
* OpenID Connect
* Secure Web Authentication (SWA)
	1. Zaawansowany system wykrywania zagrożeń.
	2. Jednolite logowanie dla aplikacji chmurowych i lokalnych, zarówno na komputerach stacjonarnych, jak i urządzeniach mobilnych.
	3. Wieloczynnikowe uwierzytelnianie obejmujące:
* Pytania bezpieczeństwa
* Email jako czynnik uwierzytelniający
* Integracja z rozwiązaniami MFA firm trzecich
	1. Możliwość tworzenia polityk dostępu dla grup i aplikacji.
	2. Zaawansowane metody uwierzytelniania:
* Uwierzytelnianie RADIUS
* Uwierzytelnianie za pomocą kart PIV
	1. Funkcja odkrywania dostawcy tożsamości (IdP discovery).
	2. Uproszczone i bezpieczne logowanie bez hasła.
	3. Dostosowywanie doświadczenia użytkownika:
* Możliwość tworzenia niestandardowych adresów URL organizacji
* Konfigurowalna strona logowania
* Wsparcie dla lokalnych języków
	1. Integracje z katalogami:
* Nieograniczone integracje z Active Directory i LDAP
	1. Funkcjonalność federacji B2B:
* Możliwość łatwego łączenia tożsamości klientów, dostawców i partnerów
* Zarządzanie tożsamościami zewnętrznymi
* Bezpieczne współdzielenie dostępu z partnerami biznesowymi
	1. Raportowanie:
* Raporty w czasie rzeczywistym
* Integracja z SIEM (Security Information and Event Management)
1. Moduł Multi-factor Authentication (MFA)

Wymagany jest moduł Multi-factor Authentication zapewniający dodatkową warstwę bezpieczeństwa poprzez wykorzystanie wielu czynników uwierzytelniania:

* 1. Typy czynników:
1. Czynniki posiadania:
* OTP (One-Time Password)
* Powiadomienia push
* Logowanie bez hasła
* Email jako czynnik
* SMS
* Połączenie głosowe
* U2F (Universal 2nd Factor)
* Integracja z czynnikami firm trzecich
1. Czynniki biometryczne:
* Windows Hello
* Apple TouchID
	1. Kontekstowe zarządzanie dostępem:
1. Kontekst lokalizacji:
* Wykrywanie nowego miasta, stanu lub kraju
* Analiza nowej geolokalizacji
* Wykrywanie niemożliwych wzorców podróży
1. Kontekst urządzenia:
	* Identyfikacja nowych urządzeń
	* Rozpoznawanie zarządzanych urządzeń
	* Analiza atrybutów bezpieczeństwa urządzenia
2. Kontekst sieci:
	* Wykrywanie nowych adresów IP
	* Określone strefy IP
	* Wykrywanie anonimizatorów sieciowych
	1. Zaawansowany system wykrywania i analizy zagrożeń.
3. Moduł Universal Directory

Wymagany jest elastyczny, oparty na chmurze katalog, oferujący następujące funkcje:

* 1. Nieograniczone integracje z katalogami: Wsparcie dla Active Directory, LDAP i aplikacji.
	2. Elastyczność atrybutów:
* Nieograniczona liczba niestandardowych atrybutów i pól użytkownika
* Możliwość mapowania i transformacji atrybutów
	1. Uwierzytelnianie LDAP w chmurze: Umożliwia korzystanie z protokołu LDAP bez konieczności utrzymywania lokalnej infrastruktury.
1. Moduł Lifecycle Management

Wymagany jest moduł Lifecycle Management automatyzujący i usprawniający zarządzanie cyklem życia tożsamości użytkowników:

* 1. Integracje: - Aplikacje i katalogi
* Automatyczne przydzielanie/odbieranie uprawnień dla aplikacji z sieci integracji
* Nieograniczona liczba aplikacji z sieci integracji
* Integracja z katalogami AD lub LDAP
* Pełna synchronizacja AD dla Office 365
	1. Zarządzanie cyklem życia tożsamości:
* Dostęp do aplikacji i przydzielanie uprawnień powiązane ze stanami cyklu życia
* Tworzenie i dezaktywacja kont w aplikacjach
* Zarządzanie uprawnieniami
	1. Zarządzanie grupami:
* Odkrywanie grup
* Dopasowywanie grup
* Aktualizacje grup
	1. Automatyzacja:
* Przepływy pracy związane z autoryzacją IT
* Przepływy pracy związane z wnioskami o dostęp
	1. Raportowanie:
* Raporty w czasie rzeczywistym
* Raporty audytu dostępu
* Raporty o ostatnio odebranych uprawnieniach
	1. Dostosowywanie:
* API umożliwiające pełne dostosowanie
	1. Universal Directory:
* Konfigurowalny katalog dla użytkowników, grup i urządzeń
* Zarządzanie stanami cyklu życia
* Mapowanie i transformacja atrybutów
	1. Provisioning:
* Wbudowane standardowe mechanizmy przydzielania uprawnień (SCIM)
* SDK do lokalnego przydzielania uprawnień
	1. Zaawansowane źródła danych:
* Przydzielanie uprawnień IT sterowane przez systemy HR (np. Workday i UltiPro)
* Pobieranie danych z wybranych aplikacji z sieci integracji (np. Salesforce i GSuite)
* Pobieranie danych z aplikacji lokalnych za pomocą agenta - Pobieranie danych z katalogów CSV
1. Zakres wdrożenia rozwiązania tożsamości i dostępu
	1. Przygotowanie i planowanie
		1. Analiza istniejącej infrastruktury IT i procesów zarządzania tożsamością.
		2. Identyfikacja kluczowych interesariuszy i utworzenie zespołu projektowego
		3. Określenie celów wdrożenia i kluczowych wskaźników wydajności (KPI).
		4. Opracowanie harmonogramu wdrożenia i planu komunikacji.
		5. Przygotowanie dokumentacji projektowej, w tym planu zarządzania ryzykiem.
	2. Konfiguracja środowiska
		1. Utworzenie dedykowanego środowiska w chmurze dla rozwiązania tożsamości i dostępu.
		2. Konfiguracja połączeń sieciowych i zapewnienie odpowiednich poziomów bezpieczeństwa.
		3. Integracja z istniejącymi systemami katalogowymi (np. Active Directory, LDAP).
		4. Konfiguracja kopii zapasowych i procedur odzyskiwania po awarii.
	3. Wdrożenie modułu Single Sign-On (SSO)
		1. Konfiguracja protokołów SSO (SAML, OpenID Connect, SWA).
		2. Integracja z wybranymi aplikacjami biznesowymi (chmurowe i lokalne).
		3. Konfiguracja polityk dostępu dla różnych grup użytkowników i aplikacji.
		4. Implementacja zaawansowanego systemu wykrywania zagrożeń.
		5. Dostosowanie interfejsu użytkownika i strony logowania.
		6. Konfiguracja raportowania i integracji z SIEM.
	4. Wdrożenie modułu Multi-factor Authentication (MFA)
		1. Konfiguracja różnych metod uwierzytelniania (OTP, powiadomienia push, biometria, etc.).
		2. Konfiguracja polityk MFA dla różnych grup użytkowników i scenariuszy.
		3. Konfiguracja polityk MFA dla skonfigurowanych aplikacji.
	5. Wdrożenie modułu Universal Directory
		1. Konfiguracja struktury katalogu i schematów atrybutów.
		2. Implementacja integracji z istniejącymi katalogami (AD, LDAP).
		3. Konfiguracja mapowania i transformacji atrybutów.
		4. Ustawienie uwierzytelniania LDAP w chmurze.
	6. Wdrożenie modułu Lifecycle Management
		1. Konfiguracja automatycznego przydzielania/odbierania uprawnień dla aplikacji.
		2. Implementacja procesów zarządzania cyklem życia tożsamości.
		3. Konfiguracja zarządzania grupami i rolami.
		4. Implementacja przepływów pracy dla autoryzacji IT i wniosków o dostęp.
		5. Konfiguracja zaawansowanych źródeł danych (systemy HR, aplikacje biznesowe).
		6. Ustawienie raportowania i audytu.
	7. Integracje i dostosowania
		1. Integracja z kluczowymi aplikacjami biznesowymi.
		2. Dostosowanie interfejsów użytkownika i procesów do specyficznych wymagań organizacji
		3. Implementacja niestandardowych rozszerzeń i skryptów przy użyciu API.
	8. Testowanie i walidacja
		1. Przeprowadzenie testów funkcjonalnych dla wszystkich wdrożonych modułów.
		2. Wykonanie testów integracyjnych z istniejącymi systemami.
		3. Przeprowadzenie testów wydajnościowych i skalowalności.
		4. Walidacja zgodności z wymogami bezpieczeństwa i przepisami.
	9. Szkolenia i dokumentacja
		1. Przygotowanie dokumentacji technicznej i użytkownika.
		2. Przeprowadzenie szkoleń dla administratorów IT
		3. Przygotowanie materiałów szkoleniowych dla użytkowników końcowych.
	10. Wdrożenie produkcyjne i wsparcie
		1. Opracowanie szczegółowego planu migracji i przejścia na produkcję.
		2. Przeprowadzenie pilotażowego wdrożenia dla wybranej grupy użytkowników.
		3. Pełne wdrożenie produkcyjne rozwiązania.
		4. Zapewnienie wsparcia powdrożeniowego i rozwiązywanie problemów.
2. Wymagania w zakresie bezpieczeństwa i niezawodności
	1. Bezpieczna infrastruktura:
		1. Zgodność z najlepszymi praktykami bezpieczeństwa
		2. Wielowarstwowa architektura zabezpieczeń
		3. Szyfrowanie danych w spoczynku i w tranzycie
	2. Zgodność i certyfikacje:
		1. Zgodność *z* wymaganymi standardami branżowymi
		2. Regularne audyty bezpieczeństwa
		3. Utrzymywanie aktualnych certyfikacji
	3. Ciągłe monitorowanie i wywiad zagrożeń:
		1. System ciągłego monitorowania bezpieczeństwa
		2. Aktywne wykrywanie zagrożeń
		3. Analiza wzorców zachowań i anomalii
		4. Automatyczne powiadamianie o incydentach bezpieczeństwa
	4. Disaster Recovery (DR) i ciągłość działania:
		1. Plan odzyskiwania po awarii (DR)
		2. Procedury zapewnienia ciągłości działania - Business Continuity Plan (BCP)
		3. Regularne testy DR/BCP
		4. Określone parametry Recovery Point Objective/Recovery Time Objective
	5. Zaufane partnerstwa:
		1. Współpraca z zaufanymi dostawcami rozwiązań bezpieczeństwa
		2. Regularna weryfikacja partnerów pod kątem bezpieczeństwa
		3. Zarządzanie ryzykiem związanym z zewnętrznymi partnerami
3. Warunki wsparcia technicznego
	1. Definicje

Godziny pracy – Usługi wsparcia technicznego i utrzymania realizowane są w dni robocze, od poniedziałku do piątku, w godzinach od 8:00 do 17:00 z pominięciem świąt.

Przyjęcie zgłoszenia – przez przyjęcie zgłoszenia rozumie się mailowe potwierdzenie przez pracownika działu wsparcia lub przez system rejestracji zgłoszeń o zarejestrowaniu zgłoszenia.

Czas rozwiązania– czas w jakim Wykonawca dołoży wszelkich starań do dostarczenia Użytkownikowi rozwiązania.

* 1. Zakres świadczonego wsparcia

Usługobiorca jest uprawniony do otrzymywania wsparcia technicznego i utrzymania obejmującego obsługę telefoniczną, za pomocą poczty elektronicznej oraz systemów zdalnej pomocy, uzyskania poprawek oprogramowania i dostępu online do dokumentacji technicznej dla rozwiązań Systemu. Komponenty wsparcia technicznego i utrzymania obejmują:

1. Pomoc techniczna producenta rozwiązań
2. Dostęp do Upgrade, Update i ServicePack
3. Pomoc techniczna w języku polskim w Godzinach Pracy
4. Dostęp do polskiego portalu pomocy technicznej
5. Dostęp do polskiej bazy wiedzy
6. Telefoniczna pomoc techniczna w języku polskim
7. Mailowa pomoc techniczna w języku polskim
8. Zdalna pomoc techniczna w języku polskim
9. Obsługa zgłoszeń typu „How to”
	1. Klasyfikacja zgłoszeń

Wykonawca dołoży wszelkich starań, aby właściwie sklasyfikować i nadać priorytety obsługi dla zgłoszeń w oparciu o poniższe definicje oraz rozwiązywać je zgodnie z przyjętymi czasami.

Incydent o dotkliwości S1

Powstaje gdy oprogramowanie nie jest w stanie właściwie funkcjonować, zgodnie z opisem funkcjonalności zawartej w dokumentacji, w środowisku produkcyjnym w wyniku błędu oprogramowania oraz gdy wpływa to w sposób niekorzystny na działalność ministerstwa w całości.

Incydent o dotkliwości S2

Powstaje gdy oprogramowanie nie jest w stanie właściwie funkcjonować, zgodnie z opisem funkcjonalności zawartej w dokumentacji, w środowisku produkcyjnym w wyniku błędu oprogramowania oraz gdy wpływa na działalności ministerstwa i jednocześnie oprogramowanie częściowo działa.

Incydent o dotkliwości S3

Powstaje gdy oprogramowanie nie jest w stanie właściwie funkcjonować, zgodnie z opisem funkcjonalności zawartej w dokumentacji, w środowisku produkcyjnym w wyniku błędu oprogramowania oraz gdy nie wpływa to w istotny sposób na działalności ministerstwa.

Incydent o dotkliwości S4

To drobne usterki i problemy mające znikomy wpływ na funkcjonowanie systemu.

* 1. Czasy reakcji i przewidywane czasy rozwiązania

Wykonawca dołoży wszelkich starań, aby zapewnić terminowe rozwiązanie zgłoszeń w oparciu o przyjęte czasy reakcji i przewidywane czasy rozwiązania dla sklasyfikowanych zgłoszeń:

Incydent o dotkliwości S1 – przyjęcie zgłoszenia w ciągu 30 minut w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia 2 dni w Godzinach Pracy.

Incydent o dotkliwości S2 – przyjęcie zgłoszenia w ciągu 4 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia do 4 dni w Godzinach Pracy.

Incydent o dotkliwości S3 – przyjęcie zgłoszenia w ciągu 8 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia w ciągu 10 dni w Godzinach Pracy.

Incydent o dotkliwości S4 – przyjęcie zgłoszenia w ciągu 12 godzin w Godzinach Pracy. Przewidywany czas rozwiązania zgłoszenia przy następnej aktualizacji producenta.

Dodatkowo system musi zapewnić poniższe funkcjonalności:

1. Moduł API Access Management

System powinien\* zapewniać bezpieczne i elastyczne zarządzanie dostępem do API:

* 1. Integracje z aplikacjami i katalogami
	2. Zgodność z OAuth 2.0 i OIDC (OpenID Connect)
	3. Dynamiczna rejestracja klientów
	4. Centralne zarządzanie dostępem i autoryzacją
	5. Zarządzanie zgodą użytkownika
	6. Możliwość dostosowania zakresów (scopes) i oświadczeń (claims)
	7. Konfigurowalne serwery autoryzacji
	8. Wbudowane mechanizmy zabezpieczające dostęp do API
	9. Kontrola ruchu API
	10. Wykrywanie anomalii w wykorzystaniu API
	11. Ochrona przed atakami na API
	12. Monitorowanie i raportowanie wykorzystania API
1. Moduł Device Access

System powinien\* zapewniać moduł zapewniający bezpieczny dostęp na poziomie urządzeń:

* 1. Dla systemu Windows:
		1. MFA na pulpicie
		2. Bezhasłowe logowanie do pulpitu
		3. Samoobsługowe resetowanie hasła
	2. Dla systemu macOS:
		1. MFA na pulpicie
		2. Synchronizacja haseł pulpitu
		3. Automatyczna rejestracja FastPass
1. Moduł Privileged Access

System powinien\* zapewniać moduł pozwaljący na zarządzaniu uprzywilejowanym dostępem:

* 1. Wnioski o dostęp uprzywilejowany
	2. Just-In-Time (JIT) dostęp do infrastruktury
	3. Przechowywanie kont uprzywilejowanych
	4. Nagrywanie sesji
	5. Przechowywanie sekretów
	6. Odkrywanie i analiza uprawnień w infrastrukturze chmurowej
	7. Zarządzanie dostępem do aplikacji SaaS
1. Moduł Advanced Server Access

System powinien\* zapewniać moduł, który oferuje zaawansowane funkcje zarządzania dostępem do serwerów:

* 1. Wsparcie dla różnorodnych środowisk: AWS, Azure, GCP i infrastruktury lokalnej
	2. Kompleksowe zarządzanie cyklem życia lokalnych kont maszyn Linux i Windows
	3. Bezproblemowa integracja SSO i MFA z przepływami pracy SSH i RDP
	4. Oparty na programowalnym CA (Certificate Authority), który generuje jednorazowe certyfikaty klienta
	5. Aplikacja kliencka do lokalnych integracji SSH i RDP oraz dynamiczne powiązanie urządzeń
	6. API umożliwiające tworzenie niestandardowych przepływów uwierzytelniania i zarządzania
	7. Implementacja modelu Zero Trust dla infrastruktury chmurowej i lokalnej
	8. Ciągła weryfikacja każdego żądania dostępu
	9. Zasada najmniejszych uprawnień (Least Privilege)
	10. Dynamiczna ocena ryzyka przy każdym dostępie
1. Moduł Access Gateway

System powinien\* zapewniać moduł, który będzie oferował funkcjonalność bramy umożliwiająca bezpieczny dostęp do aplikacji:

* 1. Integracje aplikacji Okta Single Sign-on i MFA
	2. Wsparcie dla aplikacji opartych na nagłówkach
	3. Integracja z aplikacjami Kerberos/IWA
	4. Wsparcie dla lokalnych aplikacji (np. Oracle E-Business Suite, PeopleSoft, SharePoint)
	5. Możliwość integracji z niestandardowymi aplikacjami webowymi, stronami i portalami
	6. Zaawansowane polityki dla aplikacji lokalnych
	7. Możliwość konfiguracji niestandardowych zmiennych nagłówkowych
	8. Polityki autoryzacji
	9. Elastyczna infrastruktura z serwerami Access Gateway, centrami danych oraz sieciami i hostami
1. Moduł Workflows

System powinien\* zapewniać moduł, który będzie oferował automatyzacje procesów związanych z zarządzaniem dostępem i tożsamością:

* 1. Zarządzanie dostępem (Access Governance)
	2. Certyfikacja dostępu
	3. Wnioski o dostęp
	4. Raportowanie
	5. Zarządzanie cyklem życia
	6. Zaawansowane pozyskiwanie danych źródłowych
	7. Przydzielanie uprawnień SCIM
	8. Przydzielanie uprawnień OPP (On-Premises Provisioning)
1. Moduł Identity Governance

System powinien\* zapewniać moduł, który zawiera w sobie poniższe składowe, dający rozbudowane możliwości zarządzania, kontroli i raportowania dostępu do aplikacji lub systemów:

* 1. Access Governance (Zarządzanie dostępem)
		1. Centralne zarządzanie politykami dostępu
		2. Monitorowanie i egzekwowanie zasad rozdziału obowiązków (SoD)
		3. Automatyczne wykrywanie i raportowanie konfliktów dostępu
	2. Access Certification (Certyfikacja dostępu)
		1. Automatyczne kampanie certyfikacji dostępu
		2. Konfigurowalne harmonogramy i zakresy certyfikacji
		3. Intuicyjny interfejs dla recenzentów
		4. Śledzenie postępu certyfikacji w czasie rzeczywistym
	3. Access Requests (Żądania dostępu)
		1. Samoobsługowy portal do składania wniosków o dostęp
		2. Konfigurowalne przepływy pracy zatwierdzania
		3. Automatyczne przyznawanie dostępu na podstawie polityk
		4. Integracja z systemami ticketowymi
	4. Reporting (Raportowanie)
		1. Kompleksowe raporty dotyczące dostępu i uprawnień
		2. Raporty zgodności i audytu
		3. Dostosowywałne pulpity nawigacyjne
		4. Eksport danych do różnych formatów
	5. Lifecycle Management (Zarządzanie cyklem życia)
		1. Automatyzacja procesów onboardingu i offboardingu
		2. Zarządzanie zmianami ról i stanowisk
		3. Synchronizacja uprawnień między systemami
		4. Obsługa złożonych scenariuszy organizacyjnych
	6. Advanced Sourcing (Zaawansowane pozyskiwanie danych)
		1. Integracja z systemami HR jako źródłami danych
		2. Elastyczne mapowanie atrybutów
		3. Obsługa wielu źródeł danych
		4. Rozwiązywanie konfliktów danych
	7. SCIM Provisioning (Przydzielanie uprawnień SCIM)
		1. Standardowa metoda przydzielania i odbierania uprawnień
		2. Automatyczna synchronizacja użytkowników i grup
		3. Wsparcie dla wielu aplikacji zgodnych ze SCIM
		4. Redukcja ręcznej pracy administratorów
	8. OPP Provisioning (Przydzielanie uprawnień OPP)
		1. On-Premises Provisioning dla aplikacji lokalnych
		2. Bezpieczna komunikacja między chmurą a środowiskiem lokalnym
		3. Wsparcie dla starszych systemów i aplikacji niestandardowych
		4. Centralne zarządzanie tożsamościami w środowiskach hybrydowych
1. Moduł Identity Threat Protection

System powinien\* zapewniać zaawansowany moduł ochrony przed zagrożeniami związanymi z tożsamością:

* 1. Ciągła ocena ryzyka:
		1. Wykrywanie ryzyka sesji (modele ML do wykrywania przejęcia sesji)
		2. Ocena ryzyka podmiotu (ochrona przed atakami brute force i harvesting)
	2. Ochrona kontekstowa:
		1. Ochrona urządzeń i adresów IP oparta na kontekście
	3. Ciągła ewaluacja polityk:
		1. Dynamiczna, globalna ponowna ocena polityk sesji i uwierzytelniania
		2. Polityki dostępu oparte na ryzyku dla podmiotów
	4. Precyzyjna reakcja na ryzyko:
		1. MFA w czasie rzeczywistym
		2. Uniwersalne wylogowanie ze wszystkich urządzeń i wspieranych aplikacji
	5. Orkiestracja i przepływy pracy związane z bezpieczeństwem
	6. Kontekstowe egzekwowanie dostępu
	7. Obserwacja i wgląd:
		1. Raporty z badania ryzyka
		2. Pulpity nawigacyjne i widżety ryzyka bezpieczeństwa
		3. Bogate logi systemowe z uzasadnieniem ryzyka
	8. Pipeline informacji zwrotnych:
		1. Możliwość podniesienia poziomu ryzyka przez administratora (dostosowanie na podstawie zewnętrznych danych wejściowych)
		2. Informacje zwrotne i etykietowanie modelu ryzyka
		3. Masowe czyszczenie sesji

*\* System musi zapewnić realizację wskazanej funkcjonalności, natomiast funkcjonalność ta może zostać aktywowana przez Zamawiającego w drodze realizacji rozbudowy opcjonalnej*

Osoby biorące udział we wdrożeniu muszą posiadać dedykowane certyfikaty proponowanego rozwiązania:

Okta Certified Administrator (lub równoważny)

Okta Certified Professional (lub równoważny)

Workforce Identity Cloud (WIC) Presales Accreditation (lub równoważny)