

OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa, instalacja i wdrożenie systemu zarządzania
dostępem uprzywilejowanym (PAM)

Część nr 2 zamówienia – Zadanie nr 6 obszaru technicznego IT wniosku o dofinansowanie

1. Informacje ogólne

Niniejszy Opis Przedmiotu Zamówienia (OPZ) określa minimalne wymagania techniczne i funkcjonalne dotyczące dostawy, instalacji, konfiguracji i wdrożenia systemu zarządzania dostępem uprzywilejowanym (PAM – Privileged Access Management) wraz z bezterminowymi licencjami dla 10 użytkowników, wsparciem technicznym producenta oraz przeprowadzeniem szkoleń dla administratorów. System obejmie ochroną konta uprzywilejowane infrastruktury teleinformatycznej wykorzystywanej przy zbiorowym zaopatrzeniu w wodę, w tym dostęp do systemów środowiska OT oraz serwerów i urządzeń sieciowych obsługujących Stację Uzdatniania Wody.

Parametr	Wartość
Przedmiot zamówienia	Dostawa, instalacja i wdrożenie systemu PAM (Privileged Access Management)
Architektura	Bezagentowa (proxy), zamknięta platforma wirtualna – pojedyncza maszyna wirtualna realizująca wszystkie funkcjonalności
Środowisko wirtualizacji	VMware vSphere/ESXi lub Microsoft Hyper-V
Licencja	Bezterminowa (wieczysta) dla co najmniej 10 użytkowników systemu PAM
Limit systemów docelowych	Brak – licencja nie może limitować liczby chronionych systemów docelowych
Wysoka dostępność	Możliwość wdrożenia drugiej instancji i klastra active-active w ramach dostarczonych licencji, bez dodatkowych opłat licencyjnych
Wsparcie techniczne	Minimum 12 miesięcy wsparcia producenta i dostępu do aktualizacji, licząc od dnia odbioru
Szkolenie	2-dniowe warsztaty dla maksymalnie 4 administratorów
Dokumentacja powykonawcza	W terminie do 14 dni od zakończenia wdrożenia

2. Zakres przedmiotu zamówienia

Przedmiotem zamówienia jest:

- Dostawa bezterminowych (wieczystych) licencji systemu PAM dla co najmniej 10 użytkowników, obejmujących co najmniej funkcjonalności: ochrony kont uprzywilejowanych, ochrony kluczy SSH, zarządzania i monitorowania sesji uprzywilejowanych, rejestrowania sesji uprzywilejowanych oraz raportowania wykorzystania kont uprzywilejowanych.
- Instalacja platformy PAM w środowisku wirtualizacji Zamawiającego oraz jej konfiguracja wstępna (sieć, certyfikaty, kopie zapasowe konfiguracji).
- Integracja z domeną Microsoft Active Directory Zamawiającego oraz konfiguracja uwierzytelniania wieloskładnikowego (MFA) dla użytkowników systemu.
- Objęcie ochroną wskazanych przez Zamawiającego kont uprzywilejowanych (serwery Windows i Linux, urządzenia sieciowe, interfejsy zarządzania serwerów, bazy danych) wraz z konfiguracją polityk dostępu, rotacji haseł i rejestrowania sesji.
- Konfiguracja audytu poleceń oraz mechanizmów akceptacji dostępu (dostęp za zgodą).
- Przeprowadzenie testów akceptacyjnych potwierdzających realizację wymagań niniejszego OPZ.
- Przeprowadzenie 2-dniowych warsztatów dla maksymalnie 4 administratorów Zamawiającego.
- Dostarczenie dokumentacji powykonawczej opisującej wykonane prace i konfigurację systemu.

3. Minimalne wymagania techniczne i funkcjonalne

Oferowany system musi spełniać łącznie wszystkie poniższe wymagania minimalne. Parametry wskazane w OPZ stanowią wymagania minimalne – Zamawiający dopuszcza zaoferowanie rozwiązania o parametrach lepszych. Niespełnienie któregośkolwiek z wymagań skutkuje odrzuceniem oferty.

3.1. Architektura

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Rozwiązanie bezagentowe	System PAM musi być rozwiązaniem bezagentowym, tj. umożliwiającym nawiązywanie sesji z wykorzystaniem serwerów proxy, bez potrzeby instalacji oprogramowania (agenta) na systemie docelowym, z obsługą uwierzytelniania wieloskładnikowego oraz wielu platform i systemów operacyjnych. System musi zabezpieczać dostęp do maszyn fizycznych, maszyn wirtualnych, sprzętu sieciowego (m.in. routery, przełączniki, zapory sieciowe), aplikacji oraz baz danych.
2	Zamknięta platforma wirtualna	System musi być dostarczany w formie zamkniętej platformy wirtualnej przygotowanej do implementacji w infrastrukturze Hyper-V lub VMware, zawierającej całość oprogramowania (system operacyjny, baza danych, aplikacja) realizującego wszystkie funkcjonalności systemu.

3	Pojedyncza maszyna wirtualna	Rozwiązanie nie może wymagać wdrożenia kolejnych komponentów jako osobnych maszyn wirtualnych lub fizycznych – do prawidłowego działania wszystkich funkcjonalności wymagana jest tylko jedna maszyna wirtualna.
4	Wysoka dostępność	Rozwiązanie musi oferować możliwość wdrożenia drugiej instancji i konfiguracji klastra typu active-active.

3.2. Licencjonowanie

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Liczba użytkowników	System PAM musi zostać dostarczony z kompletem licencji dla co najmniej 10 użytkowników, obejmujących minimum funkcjonalności: ochrona kont uprzywilejowanych, ochrona kluczy SSH, zarządzanie i monitorowanie sesji uprzywilejowanych, rejestrowanie sesji uprzywilejowanych, raportowanie wykorzystania kont uprzywilejowanych.
2	Licencja bezterminowa	Dostarczone licencje nie mogą mieć ograniczeń czasowych – muszą być udzielone bezterminowo (licencja wieczysta). Po upływie okresu wsparcia Zamawiający zachowuje prawo do bezterminowego korzystania z dostarczonej wersji systemu.
3	Brak limitu systemów docelowych	Licencje nie mogą w żaden sposób limitować liczby chronionych systemów docelowych.
4	Prywatny sejf	W ramach dostarczonych licencji użytkownicy systemu muszą posiadać możliwość korzystania z mechanizmu prywatnego sejfu haseł.
5	Wsparcie producenta	System musi być dostarczony wraz z co najmniej 12-miesięcznym wsparciem producenta i dystrybutora, obejmującym pobieranie aktualizacji przygotowanych przez producenta, licząc od dnia odbioru.

3.3. Zarządzane systemy, protokoły i narzędzia dostępu

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Zarządzane konta	System PAM musi zapewniać możliwość zarządzania w szczególności: użytkownikami systemów operacyjnych Windows i Unix/Linux; kontami domenowymi Microsoft Active Directory; kontami lokalnymi VMware ESX/ESXi; kontami na urządzeniach sieciowych różnych producentów; kontami baz danych (co najmniej Microsoft SQL, Oracle, MySQL, PostgreSQL); kontami interfejsów zarządzania serwerów (m.in. iLO, iDRAC); kontami aplikacji webowych dostępnych po HTTP/HTTPS; kontami innych systemów i urządzeń, do których dostęp odbywa się po protokołach SSH, RDP, VNC, TELNET, HTTP/HTTPS; kluczami SSH.

2	Poświadczenia Just-in-Time	System musi umożliwiać utworzenie poświadczeń typu Just-in-Time (JIT), tworzonych lub aktywowanych na czas trwania sesji.
3	Pośredniczenie w dostępie	System musi umożliwiać usługę pośredniczenia w dostępie do systemów i urządzeń dla użytkowników domenowych oraz zewnętrznych, rejestrując obsługiwane sesje, z obsługą minimum protokołów: SSH, RDP, VNC, TELNET, HTTP/HTTPS, X11.
4	Protokoły bez rejestracji sesji	System musi wspierać również protokoły bez rejestracji sesji, co najmniej: Cassandra, Elasticsearch, LDAP, LDAPS, MongoDB, MySQL, Oracle, PostgreSQL, Redis, Solr, SQL Server, Sybase, WinRM, Windows RPC, Windows SMB.
5	Narzędzia dostępu	System musi umożliwiać dostęp użytkowników do systemu docelowego następującymi narzędziami: przeglądarka internetowa, klient RDP, klient SSH/Telnet (np. PuTTY), klient serwerów bazodanowych (m.in. DBeaver).

3.4. Uwierzytelnianie i kontrola dostępu

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Mechanizmy uwierzytelniania	System musi wspierać minimum następujące mechanizmy uwierzytelniania: LDAP, RADIUS, TACACS, Active Directory, OpenID, SAML.
2	Uwierzytelnianie dwuskładnikowe	System musi zapewniać możliwość dwuskładnikowego uwierzytelniania oraz wspierać integrację z rozwiązaniami MFA opartymi o TOTP, w tym co najmniej Google Authenticator i Microsoft Authenticator.
3	Polityki oparte o role	System musi umożliwiać budowanie polityk kontroli dostępu w oparciu o role, np. na podstawie przynależności do grup AD/LDAP.
4	Polityki warunkowe	System musi umożliwiać budowanie polityk kontroli dostępu wymuszających: podanie powodu rozpoczęcia sesji; podanie powodu podglądu hasła; akceptację rozpoczęcia sesji przez innego administratora/-ów; akceptację podglądu hasła przez innego administratora/-ów; zakres godzin, dni oraz dat dostępu do poświadczeń.
5	Udostępnienie poza polityką	System musi umożliwiać czasowe udostępnienie poświadczenia użytkownikowi poza przypisaną mu polityką dostępową, z możliwością wyboru długości trwania takiego dostępu.
6	Ograniczenie dostępu do haseł	System musi ograniczać administratorowi możliwość dostępu do haseł lub ograniczać podgląd haseł uprzywilejowanych.
7	Połączenie transparentne	System musi umożliwiać transparentne połączenie do systemu docelowego, bez konieczności podawania przez użytkownika hasła konta uprzywilejowanego.

8	Rotacja haseł	System musi mieć możliwość zmiany wartości hasła na systemie docelowym zgodnie z ustawioną polityką, w tym: definiowania wymagań co do długości i złożoności hasła (małe i duże litery, cyfry, znaki specjalne); automatycznego generowania haseł w sposób pseudolosowy; generowania haseł unikalnych dla kont systemów docelowych; wymuszania automatycznej zmiany hasła po jego podglądzie.
---	----------------------	---

3.5. Monitorowanie, rejestrowanie sesji i audyt

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Sesje równoległe	System musi obsługiwać monitorowanie i ochronę kilkudziesięciu jednoczesnych połączeń od jednego użytkownika końcowego do różnych systemów, poprzez wiele lub jedno konto uprzywilejowane.
2	Podgląd sesji na żywo	System musi umożliwiać podgląd zestawionej sesji w czasie rzeczywistym oraz przerwanie i/lub zawieszenie trwającej sesji.
3	Tryb awaryjny	System musi posiadać funkcję pozwalającą na zawieszenie lub przerwanie wszystkich sesji oraz zablokowanie dostępu do samego rozwiązania w przypadku sytuacji krytycznej.
4	Audyt poleceń	System musi umożliwiać ograniczanie dostępu do systemów docelowych oraz tworzenie białych i czarnych list poleceń wykonywanych w systemie docelowym. Audyt poleceń musi umożliwiać co najmniej: zablokowanie polecenia, rozłączenie sesji po wykryciu audytowanego polecenia oraz automatyczne umieszczenie na liście blokowanych użytkowników, który próbował wykonać blokowane polecenie.
5	Rejestrowanie sesji	Nagrywanie sesji nie może mieć żadnego wpływu na wydajność systemu docelowego. System musi umożliwiać konfigurację parametrów nagrań: liczby klatek na sekundę, jakości pojedynczej klatki, formatu klatki (jpg lub png) oraz długości przechowywania nagrań, a także odtworzenie i pobranie zarejestrowanych nagrań.
6	Rejestrowanie klawiatury	System musi rejestrować znaki wprowadzane z klawiatury przez użytkownika co najmniej dla sesji SSH i RDP oraz umożliwiać szybkie przeszukiwanie zapisanych danych pod kątem wskazanych słów kluczowych.
7	Zestawy ustawień	System musi umożliwiać utworzenie oddzielnego zestawu ustawień w oparciu o: politykę dostępową, urządzenie docelowe, poświadczenie oraz adres źródłowy.
8	Logi i raportowanie	System musi posiadać log wszystkich zdarzeń systemowych oraz umożliwiać: wskazanie kont użytkowników logujących się do stacji/serwera; raportowanie wszystkich zmian wprowadzonych przez administratorów; raportowanie wszystkich logowań do

		systemu; raportowanie oparte na nietypowym źródle, czasie i długości połączenia do systemu docelowego; ograniczenie dostępu do raportów dla wskazanej grupy użytkowników lub administratorów.
9	Wizualizacja	Rozwiązanie musi posiadać graficzną wizualizację przedstawiającą status bezpieczeństwa aktywnych oraz historycznych sesji do systemów zdalnych.

3.6. Wymagania pozostałe

Lp.	Wymaganie	Opis wymagania / Parametr minimalny
1	Kanał dystrybucji	Oprogramowanie dostarczone w ramach realizacji zamówienia musi pochodzić z oficjalnego kanału dystrybucyjnego producenta na terenie Polski. W przypadku zaproponowania rozwiązania z innego kanału dystrybucji Wykonawca musi przedstawić dokument potwierdzający, że zaoferowany produkt posiada wsparcie producenta na terenie Polski.
2	Kompletność rozwiązania	System PAM musi być kompletny i pozwalać na uruchomienie minimum następujących funkcjonalności: zarządzania kontami uprzywilejowanymi w ramach organizacji, monitorowania wykorzystania kont uprzywilejowanych, nagrywania i archiwizacji sesji zdalnych oraz gwarantować skalowalność rozwiązania w przypadku dodawania nowych zasobów i usług.
3	Personalizacja	System musi umożliwiać personalizację wyglądu aplikacji, co najmniej poprzez umieszczenie logo Zamawiającego w głównym oknie aplikacji.

4. Wymagania dotyczące wdrożenia

- Wykonawca przeprowadzi instalację i konfigurację platformy PAM w środowisku wirtualizacji Zamawiającego oraz integrację z Microsoft Active Directory i skonfiguruje uwierzytelnianie wieloskładnikowe.
- Wykonawca obejmie ochroną systemu wskazane przez Zamawiającego konta uprzywilejowane wraz z konfiguracją polityk dostępu, rotacji haseł, rejestrowania sesji i audytu poleceń, oraz przeprowadzi testy akceptacyjne.
- Wykonawca przeprowadzi 2-dniowe warsztaty (po minimum 6 godzin dziennie) dla maksymalnie 4 administratorów Zamawiającego, obejmujące administrację systemem, zarządzanie politykami oraz obsługę nagrań i raportów.
- Wykonawca dostarczy dokumentację powykonawczą (opis architektury i konfiguracji, procedury administracyjne i awaryjne) w terminie do 14 dni od zakończenia wdrożenia.

5. Gwarancja i wsparcie techniczne

- Minimum 12 miesięcy wsparcia technicznego producenta i dystrybutora, licząc od dnia odbioru, z dostępem do aktualizacji i poprawek oprogramowania.
- Po upływie okresu wsparcia Zamawiający zachowuje bezterminowe prawo do korzystania z dostarczonej wersji systemu w ramach licencji wieczystej.

- Wsparcie świadczone co najmniej drogą e-mail lub przez dedykowany portal producenta/dystrybutora.

6. Warunki dostawy

- Dostarczenie kluczy licencyjnych oraz dokumentów potwierdzających udzielenie licencji bezterminowych na rzecz Zamawiającego.
- Dostarczenie dokumentacji technicznej producenta w języku polskim lub angielskim.
- Realizacja przedmiotu zamówienia w terminie określonym w umowie.