



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cupt
CENTRUM UNIJNYCH
PROJEKTÓW TRANSPORTOWYCH

Załącznik nr 1 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa i wdrożenie systemu uwierzytelniania wieloskładnikowego wraz z usługą wsparcia.

I. Opis wymagań technicznych:

1. System uwierzytelnienia wieloskładnikowego (licencje/subskrypcje) musi obsługiwać co najmniej 378 użytkowników przez okres 48 miesięcy.
2. Zaoferowane rozwiązanie musi być dostarczone w formie maszyny wirtualnej „virtual appliance”, jako obraz z wbudowanym systemem operacyjnym i preinstalowanym rozwiązaniem przez producenta, do bezpośredniej instalacji w środowisku data center Zamawiającego, na platformie wirtualizacyjnej VMware ESX 7.0.
3. Rozwiązanie powinno obsługiwać użytkowników, których konta przechowywane są w:
 - Active Directory Domain Services
 - LDAP
 - Microsoft SQL Server 2016
 - lokalnym repozytorium (baza danych wbudowana w system)
4. Rozwiązanie musi obsługiwać uwierzytelnianie do systemów:
 - MS Windows 10 i 11 (również przez połączenie RDP)
 - MS Windows Server 2016, 2019, 2022 (również przez połączenie RDP)
 - Debian 11
 - Ubuntu 18
5. Rozwiązanie musi posiadać możliwość określania ról ograniczające zakres działalności użytkowników z podziałem co najmniej na role:
 - administratorzy
 - helpdesk
 - użytkownicy
6. Rozwiązanie musi posiadać mechanizm pomocy technicznej dla użytkowników w zakresie obsługi dostępnych dla nich metod uwierzytelniających, tzn.:
 - zmiany istniejących
 - dodawanie nowych
7. Zarządzanie metodami uwierzytelniającymi powinno mieć możliwość:
 - realizacji samodzielnie przez użytkowników (z opcją wyłączenia tej funkcjonalności przez administratora)
 - być realizowane przez uprawnione osoby w imieniu użytkowników, za ich wiedzą lub bez ich wiedzy



Fundusze Europejskie



Rzeczpospolita Polska

Dofinansowane przez Unię Europejską



cupt
CENTRUM UMIEJĘTNOŚCI
PROJEKTÓW TRANSPORTOWYCH

8. Rozwiązanie musi być zgodne z RODO w zakresie umożliwiającym usunięcie wszystkich informacji (danych) o użytkowniku, tzw. „zapomnij mnie”.
9. Rozwiązanie musi obsługiwać metody uwierzytelniania z wykorzystaniem dedykowanej aplikacji dostarczanej przez producenta dla Smartphone realizującej powiadomienie metodą Push i umożliwiającą potwierdzenie uwierzytelniania w aplikacji bez potrzeby wpisywania kodów i haseł jednorazowych. Aplikacja musi być dostępna na systemy Android.
10. Aplikacja musi wspierać obsługę:
 - Trusted Platform Module z certyfikatem w komputerze
 - Hasło jednorazowe wysyłane przez Email (Email OTP)
 - Hasło awaryjne ustawione przez administratora w przypadku problemu z logowaniem użytkownika
 - Biometryka odcisk palca
 - Aplikacja generująca Token software zgodny z TOTP
 - Hasło LDAP
 - OATH One Time Password
 - Własne hasło
 - PKI
 - RADIUS Klient
 - SAML Service Provider
 - Pytania i odpowiedzi
 - Zewnętrzny Identity Provider OpenID Connect, OAUTH 2.0, SAML
 - Windows Hello
 - Bluetooth eSec
11. Rozwiązanie musi umożliwiać konfigurację sekwencji uwierzytelniania:
 - składającego się z listy metod. Lista może zawierać jedną lub więcej metod.
 - sekwencje muszą być kojarzone z użytkownikami na podstawie ich przynależności do wskazanych grup z systemu AD (Active Directory)
 - każda sekwencja może być aktywna lub nieaktywna
 - sekwencja jest uznawana za spełnioną tylko wtedy, gdy wszystkie zawarte w niej metody zostały pozytywnie zrealizowane przez użytkownika
12. Rozwiązanie musi pozwolić na definiowanie scenariuszy uwierzytelnienia. Dla każdego scenariusza rozwiązanie musi pozwolić zdefiniować listę sekwencji, z których jedna musi być pomyślnie zrealizowana przez użytkownika, aby uznać proces uwierzytelnienia za skuteczny.
13. Rozwiązanie musi zapewniać możliwość budowy oraz zarządzania politykami zaawansowanego uwierzytelniania odnoszących się do następujących zdarzeń i scenariuszy w ramach logowania się do systemu operacyjnego Windows:
 - logowanie do systemu Windows w sieci lokalnej Zamawiającego z wykorzystaniem aplikacji na Smartphone (kod lub „push”)



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cupt
CENTRUM UMIEJĘTNOŚCI
PROJEKTÓW TRANSPORTOWYCH

- logowanie do systemu Windows poza siecią lokalną Zamawiającego z wykorzystaniem aplikacji na Smartphone (kod lub „push”)
 - logowania do systemu Windows bez dostępu do jakiegokolwiek sieci z wykorzystaniem aplikacji na Smartphone (kod lub „push”)
 - logowanie do systemu Windows w sieci lokalnej Zamawiającego bez dostępu do aplikacji na Smartphone
 - logowanie do systemu Windows poza siecią lokalną Zamawiającego bez dostępu do aplikacji na Smartphone
 - logowanie do aplikacji VPN Zamawiającego z wykorzystaniem aplikacji na Smartphone (kod lub „push”)
 - logowanie do aplikacji VPN Zamawiającego bez dostępu do aplikacji na Smartphone
 - Możliwość uwierzytelnienia w trybie buforowanym („cache”), tzn. po pierwszym pełnym uwierzytelnieniu, kolejne będą wymagały tylko jednej metody bez konieczności pamiętania i podawania hasła domenowego
14. Możliwość ograniczenia logowania do domeny MS AD wyłącznie dla użytkowników logujących się przy użyciu zaawansowanych metod uwierzytelniania poprzez dostarczany wraz z oprogramowaniem mechanizm instalowany po stronie kontrolera domeny.
15. Portal logowania do konsoli zaawansowanego uwierzytelniania. Oddzielnie dla grup funkcjonalnych:
- administrowanie, raportowanie i zarządzanie urządzeniami obsługującymi kody jednokrotne
 - pomoc techniczna
 - samoobsługa
16. Rozwiązanie musi zapewniać integrację oraz gotową obsługę dla:
- MS AD SSO z Kerberos
 - Obsługę i plug in do Microsoft Network Policy Server (NPS)
 - Obsługę i plug in do Microsoft Remote Desktop Gateway
 - MS AZURE
 - OFFICE 365
 - OAUTH2/ OpenID Connect
 - SAML2
17. Rozwiązanie musi zapewniać obsługę RADIUS zarówno jako serwer, jak i klient.
18. Rozwiązanie musi zapewniać obsługę aplikacji i urządzeń zintegrowanych przez Radius Server (np. VPN) przez wykorzystanie procesu uwierzytelniania, który wykorzystuje oddzielny kanał komunikacyjny od podstawowego kanału komunikacyjnego dla potwierdzenia i nawiązania wiarygodnego potwierdzenia Out-of-band (OOB).



Fundusze Europejskie



Rzeczpospolita Polska

Dofinansowane przez Unię Europejską



cupt
CENTRUM UNIJNYCH
PROJEKTÓW TRANSPORTOWYCH

19. Rozwiązanie musi zapewniać uwierzytelnianie aplikacji i urządzeń zintegrowanych przez Radius Server (np. VPN) w trybie Out-of-band (OOB) z wykorzystaniem portalu lub aplikacji i wymienionych metod:
 - Dedykowanej aplikacji dostarczanej przez producenta systemu dla Smartphone realizującej powiadomienie metodą Push i umożliwiającą potwierdzenie uwierzytelniania w aplikacji bez potrzeby wpisywania kodów i haseł jednorazowych. Aplikacja musi być dostępna na systemy Android
 - Trusted Platform Module z certyfikatem w komputerze
 - Hasło jednorazowe wysyłane przez Email (Email OTP)
 - Hasło awaryjne ustawione przez administratora w przypadku problemu z logowaniem użytkownika
 - Biometryka odcisk palca
 - Token sprzętowy zgodny HOTP
 - Aplikacja generująca Token software zgodny z TOTP
 - Hasło LDAP
 - OATH One Time Password
 - Własne hasło
 - PKI
 - Pytania i odpowiedzi
 - Windows Hello
20. Rozwiązanie musi dostarczać funkcjonalne rozszerzenie dla serwisu Microsoft IIS pozwalające na zabezpieczanie serwowanych aplikacji i zasobów bez potrzeby ich modyfikowania, czyli zapewniać dodanie dodatkowego uwierzytelniania do dowolnych aplikacji działających na tym serwerze (np. Outlook Web Access).
21. Rozwiązanie musi dostarczać mechanizm jednokrotnego logowania (Single Sign On) dla zdalnego dostępu (Remote Desktop Server).
22. Rozwiązanie powinno mieć opcjonalną możliwość aktywacji mechanizmów obsługi ryzyka związanego z uwierzytelnianiem (aktualnie niewymaganą). Poziom ryzyka system powinien oceniać na podstawie:
 - lokalizacji sieciowej użytkownika (adres IP, sieć IP)
 - czasu (bieżącego, ostatniego logowania)
 - innej zdefiniowanej w systemie
23. Czynniki oceny ryzyka powinny posiadać wagi pozwalające na globalne określenie ryzyka. Stosownie do wagi ryzyka system powinien:
 - zakończyć procedurę uwierzytelniania z wynikiem pozytywnym
 - zakończyć procedurę uwierzytelniania z wynikiem negatywnym i zablokować dostęp
 - kontynuować procedurę uwierzytelniania przez stosowanie kolejnych metod
24. Z każdą sekwencją uwierzytelniania może być związany minimalny poziom ryzyka, przy którym sekwencja będzie miała zastosowanie.



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cupt
CENTRUM UNIJNYCH
PROJEKTÓW TRANSPORTOWYCH

25. Rozwiązanie musi prezentować raporty w zakresie uwierzytelnień z podaniem użytej sekwencji:
 - udanych
 - nieudanych
 - wszystkich
 - przypisanych metod uwierzytelniania
 - podstawowe statystyki
26. Rozwiązanie musi przechowywać informacje o zdarzeniach systemowych:
 - zdarzenia systemowe prezentowane są w ramach portalu administracyjnego
 - zdarzenia systemowe powinny mieć możliwość przekazywania ich do systemów klasy SIEM
27. Rozwiązanie musi umożliwiać tworzenie kopii bezpieczeństwa pozwalające szybko przywrócić system do ustawień organizacji. Przewrócenie kopii bezpieczeństwa nie może wymagać od użytkowników generowania nowych dostępów.
 - kopia bezpieczeństwa jest wykonywana na żądanie administratora przez wybranie stosownej funkcji w portalu administracyjnym
 - kopia bezpieczeństwa jest wykonywana regularnie zgodnie z ustawionym harmonogramem bez udziału administratorów
 - kopia bezpieczeństwa jest szyfrowana
28. Rozwiązanie musi generować zestaw informacji niezbędnych do zdiagnozowania problemu przez pomoc techniczną (plik do wysłania pomocy technicznej).
29. Komunikacja z systemem (administracja i użytkownicy) powinna odbywać się przy pomocy protokołu HTTPS z możliwością zmiany certyfikatu SSL.
30. Rozwiązanie musi posiadać centralną konsolę webową dostępną przy pomocy przeglądarek internetowych:
 - Google Chrome
 - Mozilla Firefox
 - Microsoft Edge
31. Rozwiązanie musi posiadać interfejs dla użytkownika i administratora dostępny w języku polskim. Użytkownicy muszą mieć możliwość logowania się własnymi poświadczeniami.
32. Rozwiązanie musi udostępnić bezpłatnie interfejs programistyczny (REST API) w celu umożliwienia integracji z innym oprogramowaniem.

II. Prawo opcji

Zamawiający na podstawie art. 441 ust. 1 ustawy Pzp, przewiduje możliwość skorzystania przez Zamawiającego z prawa opcji. W ramach prawa opcji wymagane jest dostarczenie licencji/subskrypcji spełniających wszystkie wymagania wskazane w Rozdziale I OPZ, dla dodatkowych 30 użytkowników.



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cupt
CENTRUM UNIJNYCH
PROJEKTÓW TRANSPORTOWYCH

Zamawiający zastrzega, iż skorzystanie z prawa opcji jest jego uprawnieniem, a nie obowiązkiem, co oznacza, że Wykonawcy nie przysługuje żadne roszczenie w przypadku nieskorzystania przez Zamawiającego z tego prawa. Zamawiający zastrzega sobie prawo niewykorzystania całości lub części zamówienia objętego prawem opcji. Zamawiający może skorzystać z prawa opcji najpóźniej w terminie 42 miesięcy od dnia zawarcia Umowy.

III. Dostawa i wdrożenie

Wykonawca zapewni asystę techniczną Zamawiającemu w celu dokonania implementacji zaoferowanego rozwiązania w posiadanym przez Zamawiającego środowisku. Dodatkowo w przypadku błędnego działania środowiska po instalacji Wykonawca zobowiązany będzie na własny koszt przywrócić środowisko do stanu poprawnego funkcjonowania, a w przypadku braku takiej możliwości do stanu pierwotnego oraz dostarczenia innego rozwiązania spełniającego wymagania opisane w Rozdziale I OPZ.

IV. Gwarancja i wsparcie (maintenance)

System musi być objęty serwisem producenta przez okres 48 miesięcy, od daty dostawy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego.

1. Wykonawca udziela Zamawiającemu wsparcia na okres 48 miesięcy, od dnia podpisania protokołu odbioru.
2. Jakakolwiek wada Oprogramowania, która nastąpi w okresie trwania wsparcia, będzie przez Wykonawcę usunięta w ramach wynagrodzenia. Koszt wsparcia zawiera koszty związane z dojazdem serwisu i koszty robocizny.
3. Wykonawca zobowiązuje się do przyjmowania zgłoszeń w dni robocze w godzinach od 8.00 – 17.00.
4. Zgłoszenia będą dokonywane na wskazane numery telefonu lub adresy e-mail.
5. Obsługa zgłoszeń w ramach wsparcia będzie się odbywać w języku polskim.
6. Naprawy będą dokonywane przez Wykonawcę w dni robocze oraz w dni ustawowo wolne od pracy, w siedzibie Zamawiającego lub poprzez zdalny dostęp.
7. W przypadku ujawnienia wady (nieprawidłowości, awarii lub uszkodzenia) Oprogramowania, powstałej w okresie wsparcia, Wykonawca zobowiązany jest do usunięcia wady (naprawy) lub udzielenia wsparcia, w następujących terminach, liczonych od dnia dokonania zgłoszenia:
 - a) maksymalnie do 24 godzin od przyjęcia zgłoszenia, dla wady na Poziomie krytycznym, przy czym Poziom krytyczny oznacza, że oprogramowanie nie działa lub funkcjonalności są na poważnie obniżonym poziomie i wynikającym



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cuppt
CENTRUM UNIWERSYTETÓW
PROJEKTÓW TRANSPORTOWYCH

- z tego niekorzystnym wpływie na normalne operacje biznesowe oraz natychmiastowe obejście lub rozwiązanie nie jest dostępne. Zespół wsparcia będzie pracował nieprzerwanie do czasu usunięcia wady;
- b) maksymalnie do 48 godzin od przyjęcia zgłoszenia, dla wady na Poziomie wysokim, przy czym Poziom wysoki oznacza awarię lub obniżenie wydajności co ogranicza normalne operacje biznesowe. Te incydenty mają wpływ na czas oraz są krytyczne dla produktywności, ale nie powodują natychmiastowego zatrzymania pracy. Obejście nie jest dostępne i operacje mogą być kontynuowane w ograniczonej wydajności;
 - c) maksymalnie do 72 godzin od przyjęcia zgłoszenia dla wady na Poziomie średnim, przy czym Poziom średni oznacza drobny incydent, który można obejść bez większego wpływu dla normalnych operacji biznesowych;
 - d) maksymalnie do 10 dni roboczych od przyjęcia zgłoszenia, dla wady na Poziomie niskim, przy czym Poziom niski oznacza ogólne pytania lub problemy mające niski wpływ na działanie oprogramowania.
8. Kwalifikacja ujawnionej wady do kategorii wad, o których mowa w ust. 7, należy każdorazowo do kompetencji Zamawiającego. Zamawiający dopuszcza możliwość zmiany kategorii wady na wniosek Wykonawcy, jedynie w przypadku, gdy Wykonawca zaproponuje i zastosuje jej skuteczne obejście. Ocena skuteczności obejścia i jego przyjęcie należy do Zamawiającego.
9. W okresie wsparcia, Wykonawca zapewni Zamawiającemu usługę wsparcia technicznego w procesie aktualizacji i modyfikacji konfiguracji oferowanego Oprogramowania.
10. Prawo usługi wsparcia technicznego obejmuje:
- a) prawo do otrzymywania aktualnych wersji oprogramowania oraz publikowanych poprawek,
 - b) udzielanie konsultacji i wyjaśnień telefonicznie lub drogą poczty elektronicznej w dni robocze,
 - c) rozwiązywanie problemów w działaniu i aktualizacji oraz dostęp do składania zapytań przez stronę internetową,
 - d) internetowy dostęp do dokumentacji i bazy wiedzy oraz zdalne wsparcie, w trybie nie mniej niż 8 godzin na dobę od poniedziałku do piątku.
11. W przypadku realizacji usługi wsparcia technicznego poprzez zdalny dostęp, sesja zdalna musi odbywać się przez połączenie szyfrowane oraz pod nadzorem Zamawiającego.

V. Dokumentacja powdrożeniowa

Wykonawca zapewni i dostarczy w formacie DOC/DOCX oraz PDF dokumentację powykonawczą, która będzie:



Fundusze Europejskie



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



cupt
CENTRUM UNIJNYCH
PROJEKTÓW TRANSPORTOWYCH

- 1) sporządzona w języku polskim;
- 2) zawierać nazwę dokumentu;
- 3) zawierać metrykę dokumentu (data, numer wersji, historia zmian, autor);
- 4) zawierać spis treści;
- 5) zawierać słownik pojęć;
- 6) zawierać wszystkie elementy wdrożonego systemu wraz z adresacją i usługami;
- 7) zawierać proces instalacji i konfiguracji elementów wdrożonego systemu.

VI. Instruktaż

1. Zamawiający wymaga przeprowadzenia Instruktażu, w terminie trzech (3) miesięcy od dnia zawarcia umowy. Instruktaż musi być zrealizowany w wymiarze co najmniej 16 godzin/maksymalnie 30 godzin zegarowych dla maksymalnie 8 osób. Wykonawca zapewni możliwość aktywnego udziału uczestników w trakcie Instruktażu.
2. Instruktaż powinien zostać przeprowadzony w formie on-line.
3. Instruktaż zostanie przeprowadzony na środowisku Zamawiającego.
4. Instruktaż zostanie przeprowadzony w języku polskim.
5. Wykonawca zobowiązuje się zapewnić zrealizowanie Instruktażu w terminach wskazanych przez Zamawiającego, z co najmniej 2 tygodniowym wyprzedzeniem. Zamawiający jest uprawniony do wskazania co najmniej trzech terminów takiego Instruktażu.