Gołdap, dn. 10.09.2026 r.

OR.272.6.2026

ZAPYTANIE OFERTOWE

W związku z realizacją projektu pn. ***„Podniesienie poziomu cyberbezpieczeństwa jednostek organizacyjnych Powiatu Gołdapskiego”*** dofinansowanego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Priorytet II Zaawansowane usługi cyfrowe w ramach działania 2.2 Wzmocnienie krajowego systemu cyberbezpieczeństwa z Europejskiego Funduszu Rozwoju Regionalnego dotyczącego realizacji projektu grantowego „Cyberbezpieczny samorząd”, zwracam się z prośbą o przedstawienie oferty na **wdrożenie systemu uwierzytelniania wieloskładnikowego (MFA) oraz systemu PAM w Starostwie Powiatowym w Gołdapi w ramach projektu pn.: „Podniesienie poziomu cyberbezpieczeństwa jednostek organizacyjnych Powiatu Gołdapskiego”**

Opis przedmiot zamówienia

Wymagania w zakresie systemu uwierzytelniania wieloskładnikowego (MFA):

a) Przedmiotem zamówienia jest dostawa Oprogramowania wraz z udzieleniem lub zapewnieniem udzielenia licencji przez Wykonawcę Systemu służącego do uwierzytelniania wieloskładnikowego.
b) Oferowany System musi istnieć na rynku co najmniej przez okres 3 lat oraz posiadać wsparcie techniczne w języku polskim.
c) Producentem Systemu musi być podmiot posiadający siedzibę w Unii Europejskiej.
d) W ramach przedmiotu zamówienia Wykonawca zobowiązuje się udzielić lub zapewnić udzielenie wszelkich licencji wymaganych do prawidłowego działania Systemu, jako całości, jak i poszczególnych jego elementów, dla maksymalnie 15 użytkowników, na okres min 12 miesięcy, oraz dostarczyć Oprogramowanie niezbędne do uruchomienia Systemu.

I. Wymagania ogólne

a) System musi zawierać konsolę administracyjną dostępną z poziomu przeglądarki internetowej umożliwiającą administratorowi jego konfigurację oraz zarządzanie.
b) Dostęp do konsoli administracyjnej systemu musi być chroniony uwierzytelnianiem wieloskładnikowym, z możliwością ograniczenia konieczności potwierdzania żądania uwierzytelnienia wieloskładnikowego czynnikiem niepodatnym na ataki phishingowe (np. kluczem sprzętowym typu FIDO2/U2F).
c) System musi umożliwiać samodzielną rejestrację i zarządzanie uwierzytelniaczami (tokenami uwierzytelniającymi) przez użytkowników.
d) System musi umożliwiać w konsoli administracyjnej rejestrację przez administratora uwierzytelniaczy w postaci sprzętowych kluczy typu FIDO2/U2F dla określonych użytkowników. System musi również umożliwiać zarządzanie zarejestrowanymi uwierzytelniaczami tego typu oraz wyświetlanie szczegółowych informacji na ich temat, w tym adresu IP, z którego dokonano rejestracji, AAGUID, algorytmu COSE oraz licznika podpisów.
e) System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez zareagowanie na spersonalizowane powiadomienie wysyłane na urządzenie mobilne użytkownika (mobilne systemy operacyjne iOS, Android oraz Harmony OS).
f) System musi umożliwiać potwierdzenie żądania uwierzytelnienia wieloskładnikowego poprzez wpisanie kodu jednorazowego pochodzącego z dowolnej aplikacji generującej kody jednorazowe zgodnie ze standardem TOTP (RFC 6238). Przykładami takich aplikacji są Microsoft Authenticator oraz Google Authenticator.
g) System musi umożliwiać potwierdzenie żądania uwierzytelniania wieloskładnikowego poprzez wpisanie kodu jednorazowego wysłanego na numer telefonu użytkownika w postaci wiadomości SMS.
h) System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego poprzez kliknięcie w link wysłany na numer telefonu użytkownika w postaci wiadomości SMS.
i) System musi umożliwiać zebranie zgody użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na numer telefonu użytkownika.

j) System musi umożliwiać wyświetlanie w konsoli administracyjnej informacji o udzielonej zgodzie od użytkownika na wysyłkę wiadomości uwierzytelniających poprzez SMS na wskazany numer telefonu.
k) System musi wspierać możliwość potwierdzenia żądania uwierzytelnienia wieloskładnikowego przy pomocy mobilnej aplikacji uwierzytelniającej, do której dostęp może być zabezpieczony przy pomocy blokady biometrycznej w postaci odcisku palca lub skanu twarzy, jeśli urządzenie mobilne użytkownika posiada taką techniczną możliwość.
l) System musi wspierać możliwość potwierdzenia żądania uwierzytelniania wieloskładnikowego poprzez zareagowanie na połączenie telefoniczne nawiązane przez System na stacjonarny lub mobilny numer telefonu użytkownika.
m) System musi umożliwiać zakładanie kont administratorów mających dostęp do konsoli administracyjnej wraz z przypisaniem im roli stosownej do zakresu obowiązków danego administratora.
n) System musi umożliwiać identyfikowanie użytkowników po aliasach.
o) System musi umożliwiać udzielanie dostępu do określonych chronionych rozwiązań informatycznych tylko wybranym grupom użytkowników.
p) System musi wygaszać sesję administratora w konsoli administracyjnej w przypadku nieaktywności administratora.
q) System musi umożliwiać przeszukiwanie list zarejestrowanych przez użytkowników numerów telefonów oraz kluczy sprzętowych.
r) System musi zapewnić reguły lub polityki zarządzania żądaniami uwierzytelnienia użytkowników w oparciu o zdefiniowane parametry, co najmniej takie jak: grupa, chroniony zasób oraz adres IP użytkownika.
s) System powinien umożliwiać przypisywanie różnych reguł lub polityk indywidualnie do każdej chronionej aplikacji, w zależności od przynależności użytkownika do określonej grupy użytkowników.
t) System musi umożliwiać wygenerowanie tymczasowego kodu dostępowego dla wskazanego użytkownika w przypadku niedostępności uwierzytelniacza, np. zagubienia klucza uwierzytelniającego.
u) System musi zapewnić logowanie żądań uwierzytelniania użytkowników. System musi umożliwiać pobieranie logów w formacie CSV lub poprzez API.
v) System musi zapewnić logowanie zdarzeń związanych z obsługą Systemu (wprowadzanie zmian w konfiguracji i politykach, logowanie działań administratorów). System musi umożliwiać pobieranie logów w formacie CSV lub poprzez API.
w) System musi posiadać API (pol.: Interfejs Programowania Aplikacji) umożliwiające zarządzanie co najmniej użytkownikami oraz pobieranie logów.
x) System musi zapewnić interfejs użytkownika dokonującego uwierzytelniania do chronionych aplikacji w j. polskim.

II. Wymagane integracje

a) System musi zapewniać możliwość uruchomienia uwierzytelniania wieloskładnikowego dla rozwiązań uwierzytelniających użytkowników ze źródeł Active Directory (LDAP, LDAPS) i RADIUS.
b) System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows 7 i nowszymi wersjami, oraz do serwerów z systemem operacyjnym Microsoft Windows Server 2008 R2 i nowszymi wersjami. W przypadku braku połączenia z Internetem musi być możliwe wykonanie uwierzytelnienia wieloskładnikowego przynajmniej w postaci jednorazowego hasła (One-Time Password, OTP).
c) System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy pomocy sprzętowego klucza zgodnego ze standardem FIDO2 dla logowania do stacji roboczych z systemem operacyjnym Microsoft Windows, oraz poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server.
d) System musi zapewniać możliwość wykonywania uwierzytelniania wieloskładnikowego przy użyciu karty RFID dla logowania do stacji roboczych z

systemem operacyjnym Microsoft Windows oraz dla logowania poprzez RDP do serwerów z systemem operacyjnym Microsoft Windows Server.

e) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla technologii: Microsoft Outlook Web App (OWA), Microsoft Remote Desktop Gateway/Web Access/Web Client/Web Feed oraz Microsoft Active Directory Federation Services (AD FS).
f) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń przez protokół Remote Desktop Protocol (RDP).
g) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla połączeń SSH do systemów Linux.
h) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do rozwiązań VPN w oparciu o protokoły RADIUS i LDAP.
i) System musi umożliwiać wykonywanie uwierzytelniania wieloskładnikowego dla dostępu do urządzeń sieciowych (routery, switche, zapory sieciowe) w oparciu o protokoły RADIUS i LDAP.
j) System musi umożliwiać integrację z oprogramowaniem własnym poprzez zastosowanie Software Development Kit (SDK), np. dla oprogramowania .NET, Java, PHP, które umożliwi wykonywanie uwierzytelniania wieloskładnikowego w tym oprogramowaniu.
k) System musi umożliwiać jednostronną synchronizację użytkowników ze źródeł Microsoft Active Directory, OpenLDAP oraz Microsoft Entra ID.

l) Wymagania dotyczące wdrożenia

m) Wykonawca, w ramach wdrożenia dokona instalacji I konfiguracji niezbędnych komponentów ofertowanego rozwiązania.
n) Wykonawca dokona integracji oferowanego rozwiązania ze źródłem tożsamości Zamawiającego.
o) Wykonawca wdroży technologię MFA minimum dla stacji roboczych i serwerów Windows oraz połączeń VPN.
p) Wykonawca przeprowadzi analizę możliwości integracji rozwiązań ze stosu technologicznego Zamawiającego.
q) Wykonawca przeprowadzi szkolenie wprowadzające z rozwiązania MFA dla działu IT.
r) Wykonawca dostarczy materiał instruktażowy (wideo) dla pracowników Zamawiającego w kontekście procedury logowania z aktywną technologię MFA.

<u>Wymagania w zakresie systemu PAM:</u>

1. Wymagania związane z rozwiązaniem centralnego zarządzania sesjami administracyjnymi (PAM):
1.1. System operacyjny będący bazą dla rozwiązania PAM powinien być na licencji Open Source.
1.2. Platformą sprzętowa dla rozwiązania nadzorującego sesje administracyjne jest w sieci Zamawiającego wirtualna maszyna w środowisku Hyper-V.
1.3. Architektura rozwiązania PAM powinna bazować na komponentach o licencjonowaniu Open.
1.4. Zamawiający na wyżej wymieniony cel planuje przeznaczyć maszynę wirtualną o parametrach procesor (CPU) 8 rdzeni, pamięć RAM 16 GB oraz dysk twardy (HDD) 200GB.
1.5. Tworzenie użytkowników w systemie nadzorującym sesje administracyjne może odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
1.6. System zarządzania sesjami administracyjnymi powinien pozwalać na zdefiniowanie minimum 100 obiektów do których połączenie może być nadzorowane.
1.7. System zarządzania sesjami administracyjnymi powinien ofertować minimum możliwość nadzorowania sesji w protokole RDP oraz SSH.
1.8. System zarządzania sesjami administracyjnymi powinien umożliwiać tworzenie polityk dostępu dla poszczególnych użytkowników oraz grup użytkowników w kontekście zasad połączenia do poszczególnych obiektów zdefiniowanych w systemie.
1.9. System zarządzania sesjami administracyjnymi powinien pozwalać na zdefiniowanie czasu przechowywania zapisu każdej sesji. Zamawiający wymaga minimum rocznej retencji danych.
1.10. System zarządzania sesjami administracyjnymi powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają naruszenia w zakresie trwających

sesji administracyjnych, np. wydanie polecenia „reboot" lub „shutdown" w sesji administracyjnej dla połączenia SSH.
1.11. System zarządzania sesjami administracyjnymi powinien pozwalać na połączenie administratora Zamawiającego do trwającej sesji użytkownika systemu w celu nadzoru/podglądu trwającej sesji.
1.12. System zarządzania sesjami administracyjnymi powinien pozwalać na awaryjne zakończenie trwającej sesji przez Administratora Zamawiającego.
1.13. Rozwiązanie powinno integrować się technologią MFA wdrożonym w ramach zamówinia.
2. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania zarządzania sesjami administracyjnymi:
2.1. Instalacja systemu operacyjnego na wybranym przez Zamawiającego maszynie wirtualnej.
2.2. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracja parametrów podstawowej pracy wdrażanego rozwiązania.
2.3. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyów prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
2.4. Integracja rozwiązania z centralnym źródłem tożsamości (Active Directory), wykonanie synchronizacji wskazanych przez Zamawiającego kont wraz z nadaniem odpowiednich uprawnienie, w tym Administrator oraz Użytkownik. 2.5. Integracja rozwiązania z rozwiązaniem MFA, które jest dostarczone przez Wykonawcę.
2.6. Zdefiniowanie, po konsultacji z Zamawiającym obiektów docelowych (assetów), do których będą realizowane połączenia w ramach wdrożonego systemu PAM.
2.7. Zdefiniowanie reguł połączenie dla poszczególnych użytkowników i grup użytkowników zgodnie z omówioną w czasie wdrożenie koncepcją Zamawiającego.
2.8. Test działania rozwiązania i wykonanie próbnych sesji administracyjnych dla każdego ze zdefiniowanych obiektów.
2.9. Wprowadzenie pracowników działu IT do obsługi wdrożonego systemu.
2.10. Wykonanie dokumentacji powdrożeniowej.
3. Gwarancja i asysta techniczne:
3.1. Zamawiający wymaga, aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił bezpłatne wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
3.2. Zamawiający wymaga, aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył bezpłatnie asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
3.3. Zamawiający wymaga, aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
3.4. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.

1. Miejsce wdrożenia: Starostwo Powiatowe w Gołdapi, ul. Krótka 1, 19-500 Gołdap

2. Termin realizacji zamówienia: do 25 września 2026 r.

I. Tryb udzielenia zamówienia

1. Zamówienie poniżej progu stosowania ustawy Prawo zamówień publicznych – art. 2 ust. 1 pkt. 1 ustawy Prawa zamówień publicznych (t.j. Dz. U z 2024 r. poz. 1320 z późn. zm.)

2. Postępowanie prowadzone jest w języku polskim.

3. Postepowanie jest zgodne z Regulaminem udzielania zamówień publicznych, których wartość nie przekracza kwoty 170 tys. zł netto oraz z Katalogiem wydatków kwalifikowalnych II Priorytetu Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

II. Termin i sposób składania ofert

1. Wszelkie koszty związane z przygotowaniem oferty ponosi Wykonawca.

2. Do oferty – Załącznik nr 1 - należy dołączyć:

   a) klauzulę informacyjną z art. 13 RODO stosowana w celu związanym z zapytaniem ofertowym – zgodnie z załącznikiem nr 1 do Zapytania ofertowego,

   b) oświadczenia o braku podstaw wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego – treść w załączniku nr 1 do Zapytania ofertowego,

   c) upoważnienie do podpisania oferty lub dokumenty, z których wynika umocowanie do podpisania oferty przez osobę podpisującą – jeżeli dotyczy.

3. Oferta cenowa sporządzona zostanie zgodnie z załączonym formularzem oferty, który stanowi Załącznik nr1 do niniejszego zapytania.

4. Cena podana w ofercie musi uwzględniać wszelkie zobowiązania związane z realizacją przedmiotu zamówienia, wynikające z zapisów Zapytania ofertowego i załączników do zapytania oraz obejmować wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.

5. Przyjmuje się, iż Wykonawca dokładnie zapoznał się z zapisami zapytania ofertowego wskazującymi specyfikację przedmiotu zamówienia.

6. Termin złożenia oferty: do dnia 14.09.2026 r. do godz. 13.00

7. Miejsce i sposób składania ofert:

   a. Oferta ma być sporządzona w języku polskim pod rygorem nieważności.

   b. Ofertę podpisuje osoba uprawniona do składania oświadczeń woli w imieniu Wykonawcy. Upoważnienie do podpisania oferty powinno być dołączone do oferty, o ile nie wynika z innych dokumentów dołączonych do oferty.

   c. Oferty należy składać na formularzu ofertowym wraz z wymaganymi załącznikami za pośrednictwem poczty elektronicznej na adres lukasz.debowski@powiatgoldap.pl.

   d. Dokumenty składające się na ofertę muszą być złożone jako dokument w postaci elektronicznej podpisany podpisem kwalifikowalnym, zaufanym lub osobistym.

III. Ocena ofert

1. Kryterium oceny ofert – cena 100%.

2. W celu zapewnienia porównywalności wszystkich ofert, Zamawiający zastrzega sobie prawo do skontaktowania się z Wykonawcą w celu uzupełnienia lub doprecyzowania przesłanych dokumentów.

3. W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień oraz uzupełnień dotyczących treści złożonej oferty.

4. Zamawiający zastrzega sobie prawo do unieważnienia postępowania bez dokonania wyboru żadnej z ofert, bez podania przyczyny, na każdym etapie prowadzonego postępowania. Z tytułu

unieważnienia postępowania, Wykonawcy nie przysługuje żadne roszczenie wobec Zamawiającego.

5. Jeżeli Wykonawca, którego oferta została wybrana, uchyli się od zawarcia umowy, Zamawiający może wybrać ofertę najkorzystniejszą spośród pozostałych ofert, bez przeprowadzenia ich ponownej oceny.

IV. Pozostałe

1. Podstawę do wystawienia faktury będzie stanowiło wykonanie przedmiotu zlecenia zgodnie z informacjami przekazanymi Wykonawcy potwierdzone protokołem odbioru podpisanym przez Zamawiającego i Wykonawcę. Wynagrodzenie płatne będzie w terminie 14 dni od daty otrzymania, tj. od daty przydzielenia im numerów KSeF.

2. W przypadku awarii KSeF Wykonawca wystawi faktury elektroniczne w rozumieniu przepisów ustawy z dnia 11 marca 2004 roku o podatku od towarów i usług za usługi świadczone na rzecz Zamawiającego – zgodnie z procedurami przewidzianymi w przepisach dotyczących KSeF (ustawa z dnia 29 października 2021 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw – Dz. U. z 2021r., poz. 2076 i Rozporządzenie Ministra Finansów z dnia 27 grudnia 2021 r w sprawie korzystania z Krajowego Systemu e-Faktur (Dz. U. z 2021r., poz. 2481 z późn. zm.).

3. Za termin zapłaty przyjmuje się datę prawidłowo dokonanego obciążenia rachunku bankowego Zleceniodawcy.

Signed by /
Podpisano przez:

Marzanna Marianna Wardziejewska

Date / Data: 2026-09-11 09:18