

**BIURO ZAMÓWIEŃ PUBLICZNYCH**

ul. Kuźnicza 35
50-138 Wrocław
tel. +48 71 375 22 34 | +48 71 375 28 22 | +48 71 375 20 88

bzp@uwr.edu.pl | www.uwr.edu.pl

Wrocław, dnia 22.07.2025 r.

Nr postępowania: **BZP.2710.30.2025.AW**

Wykonawcy

(informacja zamieszczona na stronie
internetowej prowadzonego postępowania)

**INFORMACJA NR 1
wyjaśnienia treści SWZ**

Dotyczy: postępowania o udzielenie zamówienia publicznego prowadzonego w trybie podstawowym bez negocjacji na zadanie pn.: **„Dostawa kluczy sprzętowych wraz z wdrożeniem dla Uniwersytetu Wrocławskiego”**

Na podstawie art. 284 ust. 1, 2 i 6 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320 ze zm.) dalej jako „uPzp”, Zamawiający – Uniwersytet Wrocławski przekazuje treść zapytań wraz z wyjaśnieniami do przedmiotowego postępowania:

Pytanie nr 1:

Czy zapis punktu 1.2.4 może zostać zmieniony w taki sposób, aby warunek dotyczący dostawy u kontrahenta na kwotę nie mniejszą niż 250 000 zł brutto mógł być spełniony poprzez wykazanie większej liczby dostaw u różnych kontrahentów, których łączna wartość wynosi co najmniej 250 000 zł brutto?

Odpowiedź Zamawiającego:

Nie. Zamawiający podtrzymuje wymóg wykazania co najmniej jednej dostawy o wartości nie mniejszej niż 250 000 zł brutto. Wskazanie łącznej wartości kilku mniejszych dostaw nie spełni tego warunku.

Pytanie nr 2:

Czy oferent może rozumieć wdrożenie jako asystę techniczną. Rozumienie jako pomoc po dostarczeniu. Support dostawcy.

Odpowiedź Zamawiającego:

Nie. Zamawiający przez „wdrożenie” rozumie pełen proces obejmujący instalację, konfigurację oraz uruchomienie rozwiązania u odbiorcy. Sama asysta techniczna lub wsparcie powdrożeniowe nie jest traktowane jako równoważne wdrożeniu.

Pytanie nr 3:

Czy Zamawiający dopuszcza, aby przez „wdrożenie u kontrahenta”, o którym mowa w pkt 1.2.4, rozumieć również asystę techniczną, tj. wsparcie udzielane po dostawie, obejmujące pomoc techniczną, konsultacje lub support dostawcy, a nie wyłącznie kompleksowe wdrożenie rozumiane jako pełna instalacja, konfiguracja i uruchomienie systemu u klienta?

Odpowiedź Zamawiającego:

Nie. Wymagane jest wykazanie realizacji wdrożenia w rozumieniu pełnej instalacji, konfiguracji i uruchomienia systemu. Asysta techniczna lub wsparcie po dostawie nie spełnia tego warunku.

Pytanie nr 4:

Czy Zamawiający przewiduje wykorzystanie centralnego systemu do zarządzania cyklem życia kluczy sprzętowych (m.in. przypisanie do użytkownika, zmiana właściciela, blokowanie, unieważnianie), czy też wszystkie te operacje mają być realizowane manualnie? Czy Zamawiający oczekuje, aby taki system został dostarczony w ramach przedmiotu zamówienia?

Odpowiedź Zamawiającego:

Zamawiający przewiduje wykorzystanie posiadanego środowiska Microsoft 365 (Entra ID / Azure AD) do zarządzania cyklem życia kluczy sprzętowych (YubiKey), w tym ich przypisania, unieważniania, zmiany właściciela oraz blokowania. Operacje te mają być realizowane centralnie w ramach istniejącej infrastruktury.

Odpowiadając na pytanie w zdaniu drugim: Nie. Zamawiający posiada już system tożsamości klasy IDP (Microsoft Entra ID) i nie oczekuje dostarczenia odrębnego rozwiązania do zarządzania cyklem życia kluczy. Oczekuje natomiast integracji kluczy sprzętowych z tym systemem.

Pytanie nr 5:

Czy w ramach zarządzania bezpieczeństwem Zamawiający przewiduje możliwość zdalnego resetowania kodu PIN na kluczach użytkowników oraz stosowania centralnych polityk dotyczących jego długości, złożoności i liczby dozwolonych prób? Czy funkcjonalność ta ma zostać dostarczona przez Wykonawcę w ramach wdrożenia?

Odpowiedź Zamawiającego:

Tak. Zamawiający przewiduje stosowanie centralnych polityk bezpieczeństwa (PIN, złożoność, liczba prób) w zakresie wspieranym przez Microsoft Entra ID oraz systemy operacyjne. Reset PIN powinien być możliwy w sposób bezpieczny – zdalnie lub za pośrednictwem administracji konta.

Odpowiadając na pytanie w zdaniu drugim: Tak. Wykonawca powinien w ramach wdrożenia zapewnić konfigurację kluczy sprzętowych w taki sposób, aby spełniały wymagania bezpieczeństwa Zamawiającego, w tym polityki PIN, procedury resetu oraz integrację z systemem tożsamości.

Pytanie nr 6:

Czy Zamawiający oczekuje prowadzenia ewidencji operacji związanych z cyklem życia kluczy (np. przypisanie, unieważnienie, reset PIN) oraz generowania raportów z wykorzystania kluczy na potrzeby audytu i zgodności?

Odpowiedź Zamawiającego:

Tak. Zamawiający oczekuje, że rozwiązanie umożliwi prowadzenie ewidencji operacji związanych z kluczami sprzętowymi oraz umożliwi generowanie raportów (np. w ramach logów z Azure AD / M365) na potrzeby zgodności z RODO, NIS2 i audytów wewnętrznych.

Pytanie nr 7:

Czy Zamawiający przewiduje integrację środowiska VPN Palo Alto GlobalProtect z posiadanym systemem tożsamości klasy IDP (Microsoft Entra ID), w celu ujednolicenia procesu MFA dla użytkowników? Czy taka integracja ma zostać wykonana w ramach niniejszego zamówienia?

Odpowiedź Zamawiającego:

Tak. Zamawiający przewiduje integrację GlobalProtect z Entra ID (Azure AD), aby zapewnić spójny mechanizm MFA z wykorzystaniem kluczy sprzętowych.

Odpowiadając na pytanie w zdaniu drugim: Tak. Wykonawca powinien zapewnić konfigurację i wdrożenie integracji GlobalProtect z systemem tożsamości Zamawiającego (Entra ID), uwzględniając mechanizmy MFA i obsługę kluczy sprzętowych.

Pytanie nr 8:

Zgodnie z dokumentacją postępowania, przedmiotem zamówienia jest dostawa oraz kompleksowe wdrożenie w organizacji Zamawiającego kluczy sprzętowych YubiKey lub równoważnych, przeznaczonych do realizacji mechanizmu uwierzytelniania dwuskładnikowego (MFA), w celu zwiększenia poziomu bezpieczeństwa dostępu do zasobów informatycznych. Zakres wdrożenia obejmuje integrację kluczy z istniejącym środowiskiem Zamawiającego (Microsoft 365 oraz system VPN Palo Alto), przeprowadzenie niezbędnych konfiguracji, szkolenie administratorów, dystrybucję kluczy użytkownikom, przygotowanie dokumentacji oraz zapewnienie wsparcia technicznego.

W dokumentacji postępowania nie wskazano jednak jednoznacznie, czy Zamawiający dysponuje systemem do zarządzania cyklem życia kluczy sprzętowych, natomiast w punkcie dotyczącym Zarządzania kluczami (m.in. inwentaryzacja, przypisanie użytkownika, blokowanie, monitoring i unieważnianie kluczy) sugerowane jest istnienie takiego rozwiązania.

- 1) Czy Zamawiający obecnie dysponuje systemem do zarządzania kluczami sprzętowymi?
- 2) Jeśli tak, prosimy o wskazanie, z jakiego rozwiązania korzysta Zamawiający.
- 3) Jeśli nie, czy system do zarządzania kluczami ma zostać dostarczony i wdrożony w ramach niniejszego zamówienia?

Odpowiedź Zamawiającego:

Ad. 1) Tak. Zamawiający korzysta z posiadanego środowiska Microsoft 365 (Entra ID / Azure AD), które umożliwia centralne zarządzanie kluczami sprzętowymi zgodnymi ze standardem FIDO2/WebAuthn.

Ad. 2) Zamawiający wykorzystuje Microsoft Entra ID (dawniej Azure Active Directory) jako system tożsamości klasy IdP. Rozwiązanie to umożliwia rejestrację, przypisanie, unieważnianie oraz monitorowanie użycia kluczy sprzętowych przez użytkowników.

Ad. 3) Nie dotyczy. Zamawiający nie przewiduje dostarczania odrębnego systemu do zarządzania kluczami w ramach zamówienia. Wykonawca zobowiązany jest jednak do integracji kluczy z istniejącym systemem tożsamości (Entra ID) oraz do konfiguracji zgodnie z wymaganiami Zamawiającego.

Zgodnie z rozdz. VIII pkt 2.8 SWZ jako obowiązującą należy przyjąć treść pisma zawierającą późniejsze oświadczenie Zamawiającego.

Zamawiający informuje, że wszelkie informacje przekazywane Wykonawcom stanowią integralną część specyfikacji warunków zamówienia i dotyczą wszystkich Wykonawców biorących udział w ww. postępowaniu. Wykonawca jest zobowiązany złożyć ofertę uwzględniającą wszelkie zmiany i wyjaśnienia zawarte w Informacjach dla Wykonawców.

Przewodnicząca Komisji Przetargowej
mgr Adriana Wiaderek