**Nr sprawy: O.253.18.2024 Załącznik nr 1 do SWZ**

**FORMULARZ OPIS PRZEDMIOTU ZAMÓWIENIA**

**Dotyczy : Dostawa systemu uwierzytelniania, autoryzacji i kontroli dostępu.**

**Wymagania i informacje Zamawiającego:**

1. Specyfikowane przez Zamawiającego wymagania oraz parametry techniczne określające przedmiot zamówienia są warunkami minimalnymi, których spełniania Zamawiający będzie oczekiwał. Zamawiający dopuszcza składanie ofert równoważnych na podstawie art. 99 ust. 5 ustawy Pzp., traktując postawione wymagania oraz parametry techniczne określające przedmiot zamówienia jako warunki minimalne, których spełnienia Zamawiający będzie oczekiwał w zakresie parametrów i funkcjonalności oferowanego Systemu. Równoważność będzie oceniania w stosunku do wszystkich opisanych parametrów i funkcjonalności Systemu. W przypadku zastosowania rozwiązań równoważnych, Wykonawca bierze na siebie nakłady związane z dostosowaniem tych rozwiązań do konfiguracji systemów i usług, które posiada Zamawiający a o których mowa w dalszej części opisu przedmiotu zamówienia.
2. Sposób wypełnienia rubryki „C”. \*
3. Wykonawca składając ofertę, słowem „TAK” potwierdza, że oferuje system spełniający wymagania Zamawiającego w odniesieniu do każdego ze specyfikowanych parametrów. W przypadku zaproponowania przez Wykonawcę rozwiązań równoważnych lub lepszych, Wykonawca musi się posłużyć słowem „TAK” i opisać zaproponowane rozwiązanie. Oferty bez jednoznacznie wpisanych deklaracji, będą podlegały odrzuceniu na podstawie art. 226 ust. 1 pkt. 5. Ustawy Pzp.
4. UWAGA! Jeśli Zamawiający określił parametry jako minimalny lub maksymalny, Wykonawca zobowiązany jest oprócz słowa „TAK” lub „NIE”, wpisać dokładnie oferowany parametr. W innym przypadku oferta będzie podlegała odrzuceniu na podstawie art. 226 ust. 1 pkt. 5. Ustawy Pzp.
5. Wykonawca wypełnia tabelę i składa podpis pod tabelą.

Przedmiotem zamówienia jest dostarczenie, instalacja, konfiguracja oraz wdrożenie systemu służącego do centralnego zarządzania tożsamością, uwierzytelnianiem oraz kontrolą dostępu użytkowników.

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Opis przedmiotu zamówienia wraz z opisem wymaganych parametrów** | **Oferta wykonawcy**  **TAK/NIE** |
| **A** | **B** | **C** |
| **1.** | **Parametry systemu**  System musi obsługiwać co najmniej: | |
| 1.1 | System musi być dostarczony w formie rozwiązania sprzętowego, Zamawiający wyklucza dostarczenia systemu w formie usługi chmurowej lub w formie maszyny wirtualnej; |  |
| 1.2 | System musi posiadać co najmniej 4 interfejsy GbE RJ45; |  |
| 1.3 | System musi posiadać co najmniej dwa dyski twarde o pojemności minimum 1TB każdy; |  |
| 1.4 | System musi umożliwiać zamontowanie go w 19” szafie rack, maksymalna wysokość urządzenia 1U; |  |
| 1.5 | Uwierzytelnianie dla minimum 1500 użytkowników lokalnych i zdalnych; |  |
| 1.6 | System musi umożliwiać rozbudowę do 2000 tokenów mobilnych dla uwierzytelniania dwuskładnikowego; |  |
| 1.7 | Minimum 300 klientów protokołu RADIUS; |  |
| 1.8 | Możliwość zdefiniowania co najmniej 100 grup użytkowników; |  |
| 1.9 | Minimum 10 lokalnych centrów certyfikacji (CA); |  |
| 1.10 | Możliwość wygenerowania co najmniej 5 tys. certyfikatów dla użytkowników; |  |
| 1.11 | Uwierzytelnianie dla co najmniej 1500 użytkowników w oparciu o dedykowaną aplikację (agenta), umożliwiającą po jej zainstalowaniu na stacji roboczej z systemem Windows 10/11, aktualizowanie informacji o aktualnie zalogowanym w ramach infrastruktury AD użytkowniku. |  |
| 2. | W ramach postępowania wymaganym jest dostarczenie bezterminowych licencji na min. 50 tokenów mobilnych/programowych oraz bezterminowych licencji dla min. 1500 użytkowników SSO. |  |
| 3. | Serwis producenta przez okres 12 miesięcy, upoważniający do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. |  |
| **4.** | **Wymagania ogólne**  System musi zapewniać nie mniej niż: | |
| 4.1 | Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności; |  |
| 4.2 | Graficzną reprezentację statusu uwierzytelnionych użytkowników; |  |
| 4.3 | Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:  a) Lokalnie;  b) Zdalnie w oparciu o protokół Syslog. |  |
| **5.** | **Wymagania funkcjonalne – uwierzytelnianie**  Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż: | |
| 5.1 | Lokalną, wbudowaną bazę użytkowników; |  |
| 5.2 | Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj; |  |
| 5.3 | Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników; |  |
| 5.4 | Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV; |  |
| 5.5 | Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:   1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych); 2. czasu ważności hasła; |  |
| 5.6 | Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:   1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych); 2. czasu ważności hasła; |  |
| 5.7 | Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:   1. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych); 2. czasu ważności hasła; |  |
| 5.8 | Konfigurowalną politykę blokowania kont, która będzie uwzględniać:   1. ilość nieudanych logowań; 2. czas blokowania konta; 3. okres nieaktywności, po którym konto jest blokowane; |  |
| 5.9 | Możliwość odzyskiwania haseł:   1. z wykorzystaniem adresu email; 2. z wykorzystaniem pytania pomocniczego; |  |
| 5.10 | Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:   1. wbudowany serwer RADIUS; 2. integrację z zewnętrznymi serwerami RADIUS – praca jako klient; |  |
| 5.11 | Obsługę protokołu LDAP, w tym zakresie system musi oferować:   1. wbudowany serwer LDAP; 2. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP); |  |
| 5.12 | Obsługę protokołu SAML - Identity Provider (IdP) proxy; |  |
| 5.13 | Realizację funkcji SSO (Single Sign On) w oparciu o:   1. integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny; 2. dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows; 3. kontekst użytkownika przesyłany z serwera RADIUS; 4. informacje uzyskiwane poprzez protokół Syslog; |  |
| **6.** | **Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe musi zapewniać nie mniej niż:** | |
| 6.1 | System realizuje uwierzytelnianie dwuskładnikowe; |  |
| 6.2 | Obsługę dla tokenów sprzętowych (hardware):   1. tokeny muszą pochodzić od tego samego producenta co system uwierzytelniania; |  |
| 6.3 | Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android; |  |
| 6.4 | Dla tokenów na system iOS i Android wymaga się:   1. aktywacji z centralnego systemu uwierzytelniania (seed provisioning); 2. możliwości konfiguracji ilości generowanych cyfr; 3. generowania kodu (cyfr) co 30 lub 60 sekund; 4. możliwości dezaktywacji tokenu oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne); 5. ochrony dostępu poprzez konfigurowalny kod PIN; |  |
| 7. | **System musi umożliwiać integrację z logowaniem do systemu Windows.** |  |
| **8.** | **Wymagania funkcjonalne – 802.1x**  **System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:** | |
| 8.1 | System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x |  |
| 8.2 | Obsługa co najmniej poniższych protokołów EAP:  PEAP;  EAP-TTLS;  EAP-TLS;  EAP-GTC; |  |
| 8.3 | Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication); |  |
| 8.4 | Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS; |  |
| **9.** | **Wymagania funkcjonalne – zarządzanie certyfikatami**  **System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:** | |
| 9.1 | Obsługa wbudowanego CA (Certificate Authority); |  |
| 9.2 | Obsługa CA pośredniczących (Intermediate CA); |  |
| 9.3 | Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego; |  |
| 9.4 | Możliwość pobrania wygenerowanych certyfikatów; |  |
| 9.5 | Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP; |  |
| 9.6 | Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP; |  |
| 9.7 | Możliwość generowania certyfikatów typu wildcard; |  |
| 9.8 | Realizacja CRL (Certificate Revocation List); |  |
| 9.9 | Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560); |  |
| **10.** | **Zarządzanie** | |
| 10.1 | Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki; |  |
| 10.2 | System musi udostępniać graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS; |  |
| 10.3 | Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć; |  |
| 10.4 | System musi posiadać możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych; |  |
| **11.** | **Funkcjonalności konieczne do działania z systemami posiadanymi przez Zamawiającego:** | |
| 11.1 | System musi być zgodny z systemem FortiAnalyzer, celem logowania, korelacji i analizy informacji, koniecznych do utrzymania spójności działania systemów posiadanych przez Zamawiającego, a tym samym zapewnienia spójności utrzymywania bezpieczeństwa; |  |
| 11.2 | System musi być zgodny z systemem FortiGate, celem wymiany danych o autentykacji i autoryzacji użytkowników znajdujących się w sieci, potrzebnych to utrzymania spójności działania systemów posiadanych przez Zamawiającego, a tym samym zapewnienia spójności utrzymywania bezpieczeństwa. System musi zapewnić dostarczenie informacji o użytkownikach i zdarzeniach w sieci, z ich udziałem (zalogowaniem, wylogowaniem, adres IP) do środowiska zawierającego UTM FortiGate posiadanego przez Zamawiającego, umożliwiając budowę polityk w oparciu o tożsamość użytkownika, ustalaną na bieżąco z przekazanych danych; |  |
| 11.3 | System musi być gotowy do wdrożenia i integracji z innymi elementami i urządzeniami, odpowiadającymi za bezpieczeństwo infrastruktury, posiadanymi przez Zamawiającego, takimi jak FortiGate, FortiAnalyzer, FortiClient EMS, FortiMail, FortiClient, FrotiWeb oraz działać w oparciu o dane wymieniane między tymi systemami, za pomocą ich wbudowanej funkcjonalności – Secure Fabric, umożliwiającej automatyczne reagowanie na wykryte zagrożenia. Musi posiadać możliwość automatyzacji wymiany danych o użytkownikach w czasie rzeczywistym z systemem FortiClient EMS, FortiClient oraz FortiGate posiadanym przez Zamawiającego; |  |
| **12.** | **Wdrożenie systemu musi objąć co najmniej:** | |
| 12.1 | Integrację wdrażanego Systemu z systemem FortiGate, FortiAnalyzer oraz FortiClient EMS; |  |
| 12.2 | Przygotowanie konfiguracji Systemu właściwej dla integracji z posiadanymi przez Zamawiającego systemami FortiGate, FortiAnalyzer oraz FortiClient EMS; |  |
| 12.3 | Przygotowanie powdrożeniowej dokumentacji technicznej oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis konfiguracji Systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz Word; |  |
| **13.** | **Warsztaty powdrożeniowe** | |
| 13.1 | Zakres warsztatów powinien obejmować co najmniej:   1. Omówienie funkcji wdrażanego Systemu; 2. Omówienie działania mechanizmu identyfikacji oraz autentykacji użytkownika; 3. Omówienie konfiguracji mechanizmów identyfikacji oraz autentykacji użytkownika; 4. Omówienie zarządzania użytkownikami, politykami MDA oraz SSO; 5. Omówienie integracji Systemu z systemami FortiGate oraz FortiAnalyzer; 6. Omówienie tworzenia kopii zapasowej Systemu i odtwarzania w razie awarii; |  |
| 13.2 | 1. Czas trwania warsztatów: co najmniej 16 godzin, podzielonych na min. 4 spotkania; 2. Zajęcia muszą być przeprowadzone w języku polskim; 3. Warsztaty musza się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00; 4. Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim; |  |

**Uwaga! Dokument należy wypełnić i podpisać zgodnie z zapisami SWZ**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Opatrzyć kwalifikowanym podpisem elektronicznym,

podpisem zaufanym lub podpisem osobistym