**Opis przedmiotu zamówienia (OPZ)**

1. Przedmiotem Zamówienia jest dostawa, konfiguracja i wdrożenie Systemu Silnego Uwierzytelniania (zwany również jako system wieloskładnikowego uwierzytelnienia, dalej jako System) obejmujący użytkowników systemów Zamawiającego.
2. Zakres przedmiotu obejmuje:
   1. Dostawa i konfiguracja Systemu,
   2. Dostawa i wdrożenie sprzętowych tokenów, w postaci pendrive, w liczbie 10 sztuk,
   3. Dostawa kompletnej dokumentacji m.in. konfiguracji systemu, administratora, użytkownika, drogą elektroniczną oraz poprzez wskazaną przez Wykonawcę stronę internetową,
   4. Wdrożenie Systemu,
   5. Szkolenie pracowników Zamawiającego w wymiarze minimum 8 godzin roboczych. Szkolenie powinno być prowadzone w języku polskim i powinno się odbyć w siedzibie Zamawiającego. Jeżeli nie jest to możliwe, wówczas wszelkie koszty związane z tym szkoleniem pokrywa Wykonawca.
3. Wymagania systemowe i licencyjne dla Systemu:
4. Wszystkie komponenty Systemu muszą mieć możliwość instalacji i pełne wsparcie w środowisku wirtualnym na platformach: VMware, Hyper V.
5. System musi być udostępniany przez producenta w postaci software appliance - maszyny wirtualnej z zaszytym systemem operacyjnym nie wymagającym odrębnej dostawy, posiadania odrębnych licencji, instalacji, itp. Aktualizacje i poprawki dostarczane przez producenta muszą dotyczyć całości software appliance.
6. Dostawca musi dostarczyć bezterminowe licencje dla oprogramowania Systemu dla użytkowników, obejmującą co najmniej 250 tożsamości użytkowników oraz możliwość uruchomienia oprogramowania bez ograniczenia liczby serwerów Systemu oraz bez ograniczenia liczby jednostek (fizycznych i wirtualnych) CPU w tych serwerach.
7. Wszelkie niezbędne licencje muszą być dostarczone z przedmiotem Zamówienia.
8. Dostawca zapewni możliwość dokupienia dodatkowych licencji dla tożsamości użytkowników, przynajmniej w okresie wsparcia producenta oprogramowania.
9. System musi być objęty 3 letnim wsparciem producenta oprogramowania (tzw. maintenance), które zapewnia:
   1. dostęp do poprawek;
   2. dostęp do nowych wersji oprogramowania;
   3. dostęp do portalu producenta z nośnikami i kluczami aktywacyjnymi dla oferowanego oprogramowania;
   4. wsparcie i pomoc w zakresie instalacji, aktualizacji i konfiguracji;
   5. możliwość zgłaszania problemów i awarii dla dostarczonego przez Wykonawcę Systemu do pomocy technicznej, przynajmniej w godzinach 8:00-20:00 w dni robocze, w języku polskim.
10. Opis funkcjonalny Systemu:

**Wymagania ogólne:**

| **Lp.** | **Opis wymagania** |
| --- | --- |
|  | Musi posiadać własne repozytorium tożsamości tak, aby mógł działać bez zewnętrznych źródeł danych, jeśli będzie taka konieczność. |
|  | Musi mieć możliwość podłączenia do następujących zewnętrznych repozytoriów tożsamości:   * + 1. Active Directory w trybach MS AD oraz AD LDS,     2. eDirectory,     3. dowolny LDAP zgodny z LDAP v3. |
|  | Musi dawać możliwość wybrania przez administratora atrybutu/atrybutów, które będą identyfikowały użytkownika w zewnętrznych repozytoriach tożsamości (np. AccountName, eMailAddress, Nr telefonu itp.). |
|  | Musi umożliwiać wskazanie w zewnętrznym repozytorium tożsamości obiektów reprezentujących grupy użytkowników. |
|  | Interfejs użytkownika powinien być oparty na interfejsie webowym. Interfejs webowy powinien być poprawnie obsługiwany w popularnych przeglądarkach internetowych (Firefox, Chrome, IE, Edge, Opera, Safari, itp.). |
|  | Musi zapewniać możliwość zdefiniowania oraz niezależną obsługę wielu podmiotów (ang. Multitenancy). |
|  | Rejestracja elementów uwierzytelniających użytkowników (np. urządzeń mobilnych, kart, tokenów) musi być realizowana za pośrednictwem interfejsu webowego. |
|  | Musi umożliwiać zdefiniowanie, a następnie musi wymuszać uwierzytelnianie wieloskładnikowe przy dostępie do konsoli administracyjnej Systemu. |
|  | Musi zapewniać obsługę scenariusza „zapomnianego urządzenia” uwierzytelniającego poprzez możliwość wygenerowania specjalnego, awaryjnego hasła jednorazowego. |
|  | Musi posiadać dostępny mechanizm weryfikacji, uniemożliwiający dla zdefiniowanej grupy użytkowników zalogowanie się do domeny Zamawiającego z użyciem tylko swojego konta i hasłem w sytuacji gdy użytkownik loguje się na domeny ze stacji roboczej bez zainstalowanego agenta Systemu. |
|  | Administrator Systemu musi mieć możliwość rejestracji lub wyrejestrowywania urządzeń służących do autoryzacji, bez udziału użytkownika. |
|  | Musi mieć możliwość komunikacji z siecią publiczną przez serwer Proxy. |

**Metody uwierzytelniania i integracja z systemami:**

| **Lp.** | **Opis wymagania** |
| --- | --- |
|  | Musi umożliwiać definiowanie sekwencji uwierzytelniających składających się z minimum trzech elementów. |
|  | Musi istnieć w systemie możliwość pominięcia jednej z metod w sekwencji uwierzytelniającej jeśli użytkownik dokonuje autoryzacji w określonym administracyjnie odstępie czasu od poprzedniego pełnego uwierzytelnienia. |
|  | Oprogramowanie Systemu musi zapewniać możliwość uwierzytelnienia minimum przy pomocy następujących technik i metod weryfikacji dla poniższych kategorii: |
|  | 1. Wiedza Użytkownika. Weryfikacja za pomocą:    1. hasła,    2. PIN (wprowadzany z klawiatury komputera lub przez telefon),    3. pytania bezpieczeństwa (challenge-response). 2. Sprzęt będący w posiadaniu Użytkownika. Weryfikacja z pomocą:    1. karty procesorowej PKI,    2. tokenu sprzętowego,    3. tokenu programowego,    4. urządzenia mobilnego w połączeniu z aplikacją do obsługi silnego uwierzytelnienia,    5. urządzenia mobilnego w połączeniu z SMS,    6. urządzenia z modułem Bluetooth,    7. klucza USB zgodnego z FIDO U2F,    8. karty i urządzenia zbliżeniowego RFID,    9. karty i urządzenia NFC. 3. Informacje biometryczne. Weryfikacja za pomocą:    1. odcisku palca dla urządzeń zgodnych z MS Biometric Framework,    2. rozpoznawania twarzy. |
|  | Musi posiadać scentralizowaną bazę reguł uwierzytelniających przydzielanych do użytkowników i musi posiadać możliwość definiowania łańcuchów uwierzytelniania składających się z minimum 3 metod. |
|  | Musi obsługiwać hasła jednorazowe (OTP) zarówno w trybie bazującym na upływie czasu (TOTP) jak i na zdarzeniach (HOTP) zgodnie z wymaganiami OATH. |
|  | Musi dostarczać odpowiednie oprogramowanie klienta i musi zapewniać uwierzytelnienie wieloskładnikowe dla następujących systemów operacyjnych:   * Microsoft Windows (tzw. Credential Provider), * Mac OSX, * Linux (konsola tekstowa).   Zamawiający preferuje oprogramowanie w języku polskim. |
|  | Musi umożliwiać integrację z systemami i aplikacjami poprzez dostarczane wraz z systemem środowisko SDK (zestaw API dla REST oraz OAuth). |
|  | Musi zapewnić integracją z aplikacjami Microsoft Office 365 i Azure za pośrednictwem ADFS poprzez dostarczenie odpowiedniej wtyczki (plug in). |
|  | Musi pozwalać na integrację z usługami sieciowymi przy pomocy RADIUS. |
|  | Wykonawca musi dostarczać aplikację na platformy Android, iOS zapewniającą powiadomienia typu push notifications dla weryfikacji tożsamości użytkownika z potwierdzeniem za pomocą urządzenia mobilnego. |
|  | Musi dostarczać aplikację na platformy Android, iOS zapewniającą możliwość weryfikacji tożsamości użytkownika poprzez potwierdzenie w aplikacji bez konieczności wpisywania numerów tokenu. W przypadku braku łączności pomiędzy urządzeniem, a serwerem musi być możliwość wygenerowania w aplikacji jednorazowego tokenu (software token) wykorzystania go w aplikacji do procesu potwierdzenia uwierzytelnienia przez urządzenie. |
|  | Musi zapewniać możliwość logowania się do domeny Zamawiającego na stacji roboczej w sposób nie wymagający podawania hasła przez użytkownika, a jedynie wymagane przez użytkownika jest użycie innej metody np. logujemy się do domeny tylko wykorzystując kartę dotykową lub USB 2FA. W tym wypadku system musi przechowywać w cache hasło użytkownika do domeny, które będzie przekazywane w tle. |
|  | Musi posiadać scentralizowaną bazę reguł uwierzytelniających dla użytkowników. |
|  | Musi również zapewniać obsługę i mieć możliwość wymuszenia zaawansowanego uwierzytelniania dla stacji roboczych Microsoft Windows, które nie są w domenie.  Np. komputery współpracowników lub firm zewnętrznych nie będące w domenie, którym dajemy dostęp do zasobów wewnętrznych i wymuszamy na nich zaawansowane uwierzytelnianie. |
|  | Musi zapewniać integrację z Microsoft Remote Desktop Gateway pozwalającą na wymuszenie wieloskładnikowego uwierzytelnienia podczas łączenia się do Microsoft Remote Desktop Gateway. |
|  | Musi zapewniać możliwość budowy systemu odpornego na awarie (failover) i przeciążenia (load balancing) |
|  | Musi udostępniać wtyczkę do Microsoft IIS pozwalającą na stosowanie wieloskładnikowego uwierzytelniania do aplikacji webowych działających na tym serwerze. |
|  | Musi zapewniać replikację danych pomiędzy serwerami systemu. |
|  | Musi zapewnić logowanie informacji o zdarzeniach w systemie (system logów). |
|  | Powinien być zgodny z przepisami RODO, m.in. system powinien udostępnić użytkownikowi opcję "zapomnij mnie", tzn. pozwolić na proste i kompleksowe skasowanie informacji uwierzytelniających użytkownika przechowywanych w systemie. |

**Wymagania dla Systemu, będące przedmiotem dodatkowej punktacji w kryterium oceny ofert:**

| **Lp.** | **Opis wymagania** | **Punktacja** |
| --- | --- | --- |
|  | Powinien posiadać moduł obsługiwany przez popularne przeglądarki internetowe, umożliwiający wsparcie użytkowników w procesie rejestracji lub wyrejestrowywania urządzeń do uwierzytelniania przez dział wsparcia Zamawiającego. | 10 |
|  | Powinien udostępniać opcję osobistego udziału użytkownika w procesie rejestracji lub wyrejestrowywania przez dział wsparcia urządzeń do weryfikacji tożsamości. Udział użytkownika oznacza wprowadzenie przez niego, w procesie rejestracji urządzeń, poświadczeń znanych tylko jemu. | 5 |
|  | Powinien zapewniać mechanizm Backupu | 10 |
|  | System dla metody uwierzytelniania wykorzystującej urządzenie mobilne z GPS musi zapewnić możliwość zdefiniowania w systemie za pomocą mapy obszaru geograficznego dla którego uwierzytelnianie za pomocą tego urządzenia będzie akceptowane i możliwe. Jeżeli użytkownik z urządzeniem znajduje się poza wyznaczonym obszarem na mapie system nie powinien realizować operacji 2FA (tzw. Two Factor Authentication). Administrator musi mieć możliwość zarządzania tymi ograniczeniami na poziomie pojedynczego urządzenia lub użytkownika. | 10 |
|  | Powinien posiadać wbudowany serwer RADIUS. | 5 |