L.P.	**NAZWA SPRZĘTU** Minimalne parametry wymagane przez Zamawiającego	**Liczba sztuk**	**OPIS TECHNICZNY OFEROWANEGO SPRZĘTU** Należy wskazać wszystkie elementy składowe oferowanego sprzętu w odniesieniu do kolumny z lewej strony	**INDEX**
1	**SYSTEM UWIERZYTELNIANIA, AUTORYZACJI I KONTROLI DOSTĘPU** **1. ARCHITEKTURA SYSTEMU:** Dostarczony system uwierzytelniania musi zapewniać wszystkie wymienione poniżej funkcje. Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników i ich uwierzytelnianiem. Dla zapewnienia bezpieczeństwa inwestycji i szybkiego wsparcia technicznego ze strony dostawcy wymaga się, aby wszystkie funkcje oraz zastosowane technologie pochodziły od jednego producenta. **2. SYSTEM OPERACYJNY:** Dla zapewnienia wysokiej sprawności i skuteczności działania systemu urządzenie musi pracować w oparciu o dedykowany, wzmocniony (hardenend) system operacyjny wzmocniony z punktu widzenia bezpieczeństwa. **3. PARAMETRY FIZYCZNE SYSTEMU:** System musi zapewniać obsługę nielimitowanej licencyjnie liczby wirtualnych procesorów, maksymalnie 1TB pamięci operacyjnej, 4 wirtualne interfejsy sieciowe oraz obsługę powierzchni dyskowej - minimum 16 TB. Możliwość uruchomienia na platformie VMware ESXi / ESX 3.5 / 4.0 / 4.1 / 5.0 / 5.5 / 6.0.	1		

	4. WYMAGANIA OGÓLNE: System powinien pozwalać na nie mniej niż: • zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki, bez konieczności stosowania zewnętrzej konsoli zarządzającej • możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active -Active w celu zwiększenia niezawodności • odpytywanie o stan urządzenia w oparciu o protokół SNMP (v1, v2, v3) oraz wykorzystanie SNMP Trap celem monitorowania (nie mniej niż): - obciążenia procesor(a/ów) - wykorzystania pamięci - informacji o osiąganiu granicznej liczby użytkowników - informacji o osiąganiu granicznej liczby grup użytkowników - informacji o osiąganiu granicznej liczby uwierzytelnionych użytkowników - przekroczeniu ilości uwierzytelnień - przekroczeniu ilości błędnych uwierzytelnień • graficzną reprezentację statusu uwierzytelnień • logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia i nazwy użytkownika: - lokalnie - zdalnie w oparciu o protokół syslog • aktualizację systemu operacyjnego z poziomu graficznego interfejsu zarządzającego (GUI) • tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) - również w oparciu o harmonogram w cyklu godzinowym, dziennym, tygodniowym lub miesięcznym wraz z określaniem godzin i minut			

	- rzeczona kopia bezpieczeństwa może również być również zapisywana przy pomocy protokołó FTP/SFTP • konfigurację captive portal **5. WYMAGANIA FUNKCJONALNE – UWIERZYTELNIANIE:** Celem realizacji funkcji uwierzytelniających, system powinien wspierać nie mniej niż: • lokalną, wbudowaną bazę użytkowników wraz z możliwością wykonywania nie mniej niż następujących akcji na użytkowniku: tworzenie, przypisanie tokena i zarządzanie nim, blokowanie konta (locking), usuwanie • przechowywanie następujących informacji o użytkowniku: nazwa (username), imię/nazwisko, adres email, numer telefonu komórkowego, numer telefonu, adres, kraj, stan/województwo • możliwość przechowywania przynajmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników • możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV • konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie: - poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych) - czasu życia hasła - możliwości ponownego użycia tych samych haseł • konfigurowalną politykę blokowania kont: - w oparciu o ilość nieudanych logowań - czas blokowania - okres nieaktywności po którym konto jest blokowane • możliwość odzyskiwania haseł: - z wykorzystaniem adresu email - z wykorzystaniem pytania pomocniczego • uruchomienie portalu do samodzielnej rejestracji			

	użytkowników - opcjonalnie tworzenie ich kont może wymagać akceptacji administratora - wymagana jest również opcja tworzenie kont bez ingerencji administratora • obsługę protokołu RADIUS zgodną z RFC - wbudowany serwer RADIUS - konfiguracja serwera pozwala na ograniczenie dostępu tylko do wskazanych urządzeń NAS - integrację z zewnętrznymi serwerami RADIUS • obsługę protokołu LDAP - wbudowany serwer LDAP - możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP) • obsługę SAML - Identity Provider (IdP) proxy • realizacje funkcjonalności SSO (Single Sign On) w oparciu o: - integrację z Active Directory również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny - dedykowaną aplikację na stację robocze z systemem Windows - RADIUS - informacje uzyskiwane poprzez protokół syslog - dedykowany portal **6. WYMAGANIA FUNKCJONALNE - UWIERZYTELNIANIE DWUSKŁADNIKOWE:** Realizując uwierzytelnianie dwuskładnikowe, system musi spełniać nie mniej niż: • obsługę dla tokenów sprzętowych (hardware): - ich działanie musi być realizowane w oparciu o protokół OATH wraz ze wsparciem dla TOTP oraz HOTP - wspomniane tokeny muszą pochodzić od tego samego			

	producenta co system uwierzytelniania • wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile • dla tokenów na system iOS i Android wymaga się: - aktywacji z centralnego systemu uwierzytelniania (seed provisioning) - możliwości konfiguracji ilości generowanych cyfr (6 lub 8) - generowania kodu (cyfr) co 30 lub 60 sekund - możliwości dezaktywacji tokena oraz jego reinstalacji (przeniesienia na inne urządzenie mobilne) - ochrony dostępu poprzez konfigurowalny kod PIN - aktywacji w oparciu o kod QR • możliwość dostarczenia kodu (wskazania tokena) poprzez: - email (wygaśnięcie kodu w czasie 10-3600 sekund) - SMS (wygaśnięcie kodu w czasie 10-3600 sekund) *konfiguracja bramki SMS w oparciu o HTTP/S i/lub SMTP • w przypadku tokenów programowych możliwość wykorzystania notyfikacji push przychodzących na urządzenie mobilne i zawierających szczegóły dotyczące żądania logowania (nazwa użytkownika, serwer/usługa docelowa, adres IP, data i godzina, rodzaj i wersja przeglądarki) w celu zaakceptowania ich jednym "kliknięciem" • możliwość integracji z logowaniem do systemu Windows • wsparcie dla API **7. WYMAGANIA FUNKCJONALNE - 802.1X:** System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki: • dla sieci bezprzewodowych wymagane są następujące protokoły:			

	- PEAP - EAP-TTLS - EAP-TLS - EAP-GTC • wsparcie dla uwierzytelniania w oparciu o adres MAC (MAC based authentication) • zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTL, TLS EAP • możliwość samodzielnej rejestracji urządzeń przez użytkowników celem uwierzytelniania z wykorzystaniem certyfikatów **8. WYMAGANIA FUNKCJONALNE - ZARZĄDZANIE CERTYFIKATAMI:** System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż: • własne, samodzielne CA (Certificate Authority) • CA pośredniczące (intermediary CA) • ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego • możliwość pobrania wygenerowanych certyfikatów • możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP • możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP • możliwość generowania certyfikatów typu wildcard • realizacja CRL (Certificate Revocation List) • wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560) **9. PARAMETRY WYDAJNOŚCIOWE I LICENCYJNE:** System musi obsługiwać co najmniej:			

	• uwierzytelnianie dla min 4000 użytkowników lokalnych • uwierzytelnianie dla min 4000 użytkowników zdalnych • min 8000 tokenów (uwierzytelnianie dwuskładnikowe) • min 1200 klientów protokołu RADIUS (urządzeń NAS) • 400 grup • 200 certyfikatów głównych (CA) • min 5000 certyfikatów użytkowników **10. ZARZĄDZANIE:** System udostępnia: • Graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS **11. OGÓLNE WYMAGANIA DLA PRZEDMIOTU ZAMÓWIENIA:** • Dla opisanego w ramach Przedmiotu Zamówienia Systemu wymagane jest zapewnienie przez Wykonawcę gwarancji i opieki technicznej (serwisu i wsparcia technicznego) przez cały okres trwania umowy Usługi gwarancyjne, opieka techniczna. • Wymaga się aby dostawa obejmowała również serwis producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7. • W przypadku nowych Podsystemów Wykonawca musi uwzględnić w kosztach realizacji: Dostawę, instalację, podłączenie, uruchomienie dostarczanych dostarczonego rozwiązania - W przypadku rozwiązań wirtualnych, opisanych w części przedmiotu zamówienia, koszty urządzeń oraz licencji związanych z wirtualizacją wdrażanych podsystemów. - Wszystkie dodatkowe licencje dotyczące uruchomienia i działania Podsystemu – w tym te na współpracujących			

	urządzeniach/Podsystemach, - Zaimplementowanie ustawień i polityk z dotychczasowych podsystemów, które zastąpią nowe podsystemy. - Konfigurację i integrację z innymi powiązanymi Podsystemami Zamawiającego. **13. WARUNKI WDROŻENIA I FAZY RELIZACYJNEJ:** Warunki wdrożenia i fazy realizacyjnej: • Zamawiający przewiduje etapową realizację prac z odbiorem po uruchomieniu dostarczonego rozwiązania. • Wdrożenie nowego rozwiązania powiązane być musi z integracją z podsystemami, z których już korzysta zamawiający oraz przeniesieniem dotychczasowych funkcjonalności, ustawień polityk na nowe rozwiązanie (2FA, przeniesienie Fortitokenów, Network Policy Server, Microsoft PKI) • Wykonawca zobowiązany jest do przedstawienia niezwłocznie po podpisaniu umowy planowanego harmonogramu prac i planu migracji do nowych podsystemów, aby: - Zapewnić w maksymalnym stopniu ciągłość działalności statutowej Zamawiającego. - Minimalizować uciążliwość prac poprzez wcześniejsze uzgadnianie z Zamawiającym terminów (dni, godzin) ich realizacji (w ramach przyjętego harmonogramu). Harmonogram musi zostać zatwierdzony przez Zamawiającego. • Inżynierowie wykonujący prace wdrożeniowe muszą posiadać odpowiednie kwalifikacje potwierdzone certyfikatami producentów instalowanych produktów. • Odbiór końcowy przeprowadzone będą po wykonaniu testów akceptacyjnych i zakończeniu ich pozytywnym wynikiem,			

	14. DOKUMENTACJA POWYKONAWCZA: Wymagania dotyczące dokumentacji powykonawczej: • Dokumentacja powykonawcza dotycząca nowych systemów powinna zawierać dokładny opis dostarczonego rozwiązania oraz niezbędne schematy i instrukcje - ostateczne wersje (wraz z komentarzami) plików konfiguracyjnych / backupu urządzeń i oprogramowania. • Kody na opisach i schematach w dokumentacji powykonawczej muszą być zgodne z faktycznymi oznaczeniami na etykietach urządzeń i połączeń. • W trakcie odbioru końcowego Wykonawca przekaże Zamawiającemu 1 egzemplarz dokumentacji powykonawczej w wersji papierowej i 1 egzemplarz w wersji elektronicznej.			