Załącznik nr 1 do Zapytania

Identyfikator CeZ: 19514

Opis Przedmiotu Zamówienia

1. Przedmiot zamówienia.

1.1. Przedmiotem zamówienia jest **Zakup systemu zarządzania dostępem do sieci NAC.**

1.2. Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu NAC (Network Access Control) (zwanego dalej Systemem) wraz z oprogramowaniem, niezbędnymi licencjami oraz świadczeniu usługi gwarancji dla wdrożonego systemu. System ma być dostarczony w modelu „on premise" czyli musi być zainstalowany na infrastrukturze Zamawiającego.

1.3. W szczególności przedmiot zamówienia obejmuje:

1.3.1. Dostarczenie niezbędnych licencji wieczystych typu virtual appliance lub software appliance.

1.3.2. Dostarczenie najnowszej wersji Systemu.

1.3.3. Świadczenie usług gwarancyjnych producenta oprogramowania przez okres 24 miesięcy od daty podpisania Protokołu odbioru.

1.4. Systemem zostanie objęte środowisko Zamawiającego składające się z:

1.4.1. 900 jednoczesnych unikatowych operacji uwierzytelniania do sieci Zamawiającego.

1.4.2. Sumarycznie 900 monitorowanych agentowo hostów.

1.5. Zamawiający przewiduje możliwość udzielenia zamówienia opcjonalnego w zakresie objęcia Systemem dodatkowych stacji roboczych opartych o system operacyjny z rodziny MS Windows/macOS w wymiarze do 100 sztuk względem wymagań zawartych łącznie w pkt 1.4.1 oraz 1.4.2.

1.6. Stos technologiczny wykorzystywany w środowisku sieciowym Zamawiającego:

1.6.1. Firewall Fortigate.

1.6.2. System logowania, analizy i raportowania FortiAnalyzer.

1.6.3. Klient łączenia się do sieci VPN – Forti Client VPN.

2. Harmonogram realizacji przedmiotu zamówienia:

Przedmiot zamówienia zostanie zrealizowany w terminie nie dłuższym niż 40 Dni Roboczych, liczonym od dnia zawarcia Umowy, w podziale na niżej określone etapy:

Etap I – Opracowanie harmonogramu wdrożenia.

W ramach realizacji etapu Wykonawca:

2.1. W terminie do 3 Dni Roboczych od daty podpisania umowy, przygotuje i przedstawi Zamawiającemu harmonogram wdrożenia Systemu.

2.2. Przygotuje opis niezbędnych prac w celu wdrożenia Systemu wraz ze wskazaniem podziału obowiązków pomiędzy Zamawiającego i Wykonawcę w modelu RACI.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

2.3. Przedstawi listę pracowników Wykonawcy odpowiedzialnych za wykonanie poszczególnych etapów zgodnie z przedstawionym wykazem podziału obowiązków w w/w formacie RACI wraz z danymi teleadresowymi minimalnie numer telefonu komórkowego, adres email.

2.4. Opracuje scenariusze testowe Systemu:

2.4.1. Scenariusze testowe muszą zawierać propozycje testów wydajnościowych, funkcjonalnych i bezpieczeństwa.

2.4.2. Scenariusze testowe będą przygotowane przez Wykonawcę i wymagają zatwierdzenia przez Zamawiającego.

Etap II - Analiza przedwdrożeniowa.

W ramach realizacji etapu Wykonawca:

2.5. Wykona analizę infrastruktury informatycznej Zamawiającego, która zostanie objęta Systemem, potrzeb użytkownika i wymagań funkcjonalnych odnośnie konfiguracji Sytemu, której wynikiem będzie plan wdrożenia Systemu u Zamawiającego.

2.6. Przygotuje i przedstawi Zamawiającemu Projekt techniczny Systemu (architektura Systemu) określający:

2.6.1. Wykaz oprogramowania i licencji niezbędnych do poprawnej pracy Systemu.

2.6.2. Wymogi takie jak ilość urządzeń fizycznych/maszyn wraz z dokładnymi parametrami jak vCPU, vRAM, vHDD wirtualnych wymaganych dla wszystkich składowych Systemu.

2.7. Uzgodni z Zamawiającym polityki/reguły bezpieczeństwa Systemu oraz ich wdrożenie.

2.8. Dostarczy oprogramowanie i licencje niezbędne do poprawnej pracy Systemu.

Etap III – Wdrożenie, konfiguracja i testy Systemu.

W ramach realizacji etapu Wykonawca:

2.9. Wdroży w infrastrukturze Zamawiającego System zgodnie z zaakceptowanym harmonogramem, planem wdrożenia Systemu oraz Projektem technicznym Systemu z uwzględnieniem analizy przedwdrożeniowej oraz warunkami opisanymi w pkt 3 OPZ.

2.10. Wykona pełną konfigurację i parametryzację Systemu zgodnie z Projektem technicznym będącym wynikiem analizy przedwdrożeniowej.

2.11. Przeprowadzi testy akceptacyjne.

2.12. Dostarczy Dokumentację powykonawczą dla Zamawiającego.

2.13. Przeprowadzi instruktaż dla użytkowników Systemu zgodnie z warunkami opisanymi w pkt. 6.

3. Wdrożenie Systemu.

W ramach realizacji Etapu III, Wykonawca dokona wdrożenia Systemu , rozumianego jako:

3.1. Instalacja Systemu zgodna z planem wdrożenia na udostępnionym przez Zamawiającego środowisku opisanym w pkt 1.4 OPZ. Szczegóły systemowe zostaną przekazane Wykonawcy po podpisaniu umowy.

3.2. Przygotowanie konfiguracji Systemu zgodnie z projektem technicznym Systemu oraz wdrożenie polityk bezpieczeństwa odzwierciedlających obecnie posiadaną konfigurację i wiedzę o aktualnych zagrożeniach.

3.3. Skonfigurowanie logowania zdarzeń na Systemie i umożliwienia zapisywania ich na zewnętrznym serwerze logowania udostępnionym przez Zamawiającego (możliwość zapisywania/eksportu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

logów w co najmniej trzech z wymienionych formatów: Syslog/Syslog CSV/SNMP trap/ Syslog Command Event Format (CEF)/EventLog).

3.4. Przeprowadzenie testów wydajnościowych, funkcjonalnych i bezpieczeństwa zainstalowanego Systemu, zgodnie z opracowanymi w pkt 2.4 OPZ scenariuszami, z udziałem Zamawiającego. Wynikiem testów będzie raport potwierdzający spełnienie zawartych w pkt 4.3 Obligatoryjnych funkcjonalności Systemu. Raport potwierdzony zostanie przez obie strony.

3.5. Przygotowanie i dostarczenie Dokumentacji powykonawczej oraz dokumentacji użytkownika (administratora/operatora) systemu. Dokumentacja powinna zawierać architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów akceptacyjnych i funkcjonalnych rozwiązania, opis konfiguracji systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora systemu.

3.6. Za pełne wdrożenie Systemu uznaje się instalację systemu, przeprowadzenie z wynikiem pozytywnym testów akceptacyjnych, funkcjonalnych i bezpieczeństwa, integracja z systemem logowania zdarzeń Zamawiającego, dostarczenie kompletu dokumentacji, przeprowadzenie instruktażu opisanego w pkt 6, obustronne podpisanie Protokołu odbioru.

4. Wymagania minimalne dla Systemu NAC:

4.1. **Architektura Systemu.**

4.1.1. System musi współpracować z urządzeniami wielu producentów (tzw. multi vendor).

4.1.2. W przypadku dostarczenia Systemu jako maszyny wirtualnej muszą być wspierane środowiska Hyper-V oraz Vmware.

4.1.3. System musi wspierać możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive w celu zwiększenia niezawodności.

4.1.4. System musi oferować pracę w trybie out-of-band, tj. realizować wszystkie wymagane funkcje bez konieczności analizy ruchu sieciowego (na porcie SPAN, inline).

4.1.5. Jeżeli System będzie instalowany jako oprogramowanie na systemie operacyjnym należy dostarczyć produkt, który będzie mógł być zainstalowany na jednym z systemów operacyjnych: Windows Server 2012+, CentOS, RHEL.

4.1.6. System musi być w pełni zarządzalny z jednej konsoli przez graficzny interfejs www, należy dostarczyć rozwiązanie obsługiwane za pośrednictwem popularnych przeglądarek internetowych (Chrome, MS Edge, Firefox) w aktualnych wersji na dzień składania oferty.

4.1.7. Konsola zarządzania musi umożliwiać dostęp szyfrowany z pomocą protokołu co najmniej TLS 1.2.

4.1.8. Agent Systemu dla stacji końcowej powinien działać na systemach operacyjnych obsługiwanych przez Zamawiającego (Microsoft Windows 8.1, Windows 10, Microsoft Server 2012 i nowszych, macOS oraz Linux (RHEL/CentOS/Debian)).

4.1.9. System powinien chronić zarządzane punkty końcowe działające w systemach połączonych, systemach rozproszonych i niezależnych środowiskach.

4.1.10. Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania.

4.1.11. Elementy zarządzające i analityczne Systemu muszą być skalowane w celu obsługi co najmniej 10 000 jednoczesnych unikatowych autoryzacji do sieci w ciągu doby.

4.1.12. Praca Systemu musi pozwalać na działanie bez dostępu do Internetu.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.1.13. Wymagana jest możliwość wykorzystania mechanizmy proxy do komunikacji z Internetem.

4.1.14. W przypadku braku dostępu do Internetu System zarządzający ma mieć możliwość aktualizacji za pomocą ręcznej aktualizacji.

4.1.15. System musi umożliwiać elastyczną rozbudowę poprzez dodawanie licencji w przypadku wzrostu liczby obsługiwanych urządzeń w sieci.

4.1.16. Licencja na jednoczesne unikatowe uwierzytelniania ma być zwalniana po rozłączeniu urządzenia końcowego.

4.2. **Zarządzanie Systemem.**

4.2.1. System musi umożliwiać tworzenie indywidualnych kont dla każdego użytkownika/administratora Systemu.

4.2.2. System musi pozwalać na ustalenie silnej polityki haseł. Silna polityka haseł może być realizowana lokalnie przez System lub z pomocą zewnętrznych systemów np.: Active Directory.

4.2.3. System musi umożliwiać konfigurowanie zakresu uprawnień w Systemie z wykorzystaniem predefiniowanych ról wewnętrznych – zarządzanie RBA (Role based Access) - np. dostęp tylko do raportów, administrator systemu, analityk itp.).

4.2.4. System powinien się integrować z zewnętrznym repozytorium użytkowników (LDAP lub RADIUS) w zakresie uwierzytelnienia do Systemu oraz kontroli dostępu na bazie zdefiniowanych ról. Dopuszcza się rozwiązanie używające wewnętrznego mechanizmu uwierzytelniania do Systemu.

4.2.5. System musi mieć możliwość definiowania raportów i alertów z wykorzystaniem danych zbieranych przez system.

4.2.6. System musi mieć wbudowany panel sterowania (Dashboard) z predefiniowaną zawartością dostosowaną do potrzeb określonej roli co najmniej analityka, kierownika zespołu, dyrektora bezpieczeństwa. Dashboard powinien umożliwiać schodzenie do szczegółu poszczególnych elementów od poziomu informacji podstawowych.

4.2.7. System musi posiadać panel administracyjny, przedstawiający szczegółowy obraz stanu zabezpieczeń podłączonych lub próbujących się podłączyć urządzeń końcowych.

4.2.8. Konsola zarządzania systemu musi być dostępna co najmniej w angielskiej wersji językowej.

4.3. **Obligatoryjne funkcjonalności Systemu.**

4.3.1. System musi posiadać funkcjonalność aktywnego zapobiegania dostępu do sieci nieautoryzowanych użytkowników oraz urządzeń końcowych.

4.3.2. System musi umożliwiać uwierzytelnienie użytkowników i urządzeń podłączanych do sieci lokalnej LAN i sieci bezprzewodowej WLAN z wykorzystaniem:

4.3.2.1. standardu 802.1X

4.3.2.2. adresu MAC urządzenia

4.3.2.3. formularza webowego (captive portal) z wykorzystaniem LDAP lub przy pomocy loginu i hasła z lokalnej bazy danych użytkowników w Systemie

4.3.3. System musi obsługiwać uwierzytelnianie w oparciu o: wbudowany serwer RADIUS, zewnętrzny serwer Radius, protokół LDAP, jak również w oparciu o wewnętrzną bazę użytkowników i urządzeń.

4.3.4. System musi obsługiwać autoryzację w oparciu o adresy MAC definiowane w wewnętrznej bazie z wykorzystaniem protokołu RADIUS.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.5. System musi zapewniać automatyczne wykrywanie urządzeń końcowych i śledzenie ich położenia poprzez identyfikowanie nowych adresów MAC i IP, nowych sesji uwierzytelniających (802.1X, wykorzystujące przeglądarkę internetową, LDAP) lub żądania RADIUS pochodzących z przełączników dostępowych. W ramach postępowania muszą zostać dostarczone wszystkie niezbędne elementy, które umożliwią realizację powyższej funkcji we wszystkich lokalizacjach i segmentach sieci.

4.3.6. System musi aktywnie zapobiegać przed dostępem do sieci nieautoryzowanych użytkowników, zagrożonych urządzeń końcowych i innych niechronionych urządzeń. Dla tak zdefiniowanych urządzeń końcowych muszą być zapewnione mechanizmy automatycznej kwarantanny oraz blokowania.

4.3.7. System musi umożliwiać synchronizację danych (tożsamości, jednostki organizacyjne, konta administracyjne) z minimum systemów zewnętrznych:

4.3.7.1. Microsoft Active Directory

4.3.7.2. Radius

4.3.7.3. LDAP

4.3.8. System musi umożliwiać dodawania rozpoznanych urządzeń do grup systemowych.

4.3.9. System na podstawie rodzaju rozpoznanego urządzenia musi umożliwiać różnicowanie poziomu dostępu.

4.3.10. System musi posiadać możliwość raportowania podłączonych tożsamości, urządzeń końcowych podłączonych do sieci, min. Tożsamość, adresadres MAC, nazwa urządzenia końcowego HOSTNAME, port, SSID, urządzenie sieciowe, informacja o autoryzacji oraz przydzielony VLAN z przydzielonym adresem IP.

4.3.11. System musi zapewniać scentralizowane zarządzanie z pomocą panelu zarządzania urządzeniami sieciowymi. Zarządzanie musi dopuszczać możliwość zarządzania agentowo jak i bez-agentowo.

4.3.12. System musi podejmować decyzję o przyłączeniu urządzeń końcowych do sieci poprzez ocenę ich zgodności ze zdefiniowanymi wymaganiami. Ocena zgodności musi być realizowana zarówno bez dedykowanego agenta instalowanego na stacji końcowej (za pomocą metod takich jak: WinRM, WMI) jak i z użyciem agenta.

4.3.13. System musi umożliwiać monitorowanie urządzeń sieciowych za pomocą protokołu min. SNMP.

4.3.14. Funkcjonalność zarządzania urządzeniami sieciowymi w zakresie monitoringu oraz konfiguracji ustawień portu z zakresu:

4.3.14.1. VLAN

4.3.14.2. Autoryzacja

4.3.14.3. Status

4.3.14.4. Opis

4.3.15. System musi obsługiwać możliwość automatycznego egzekwowania zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej.

4.3.16. System musi posiadać funkcjonalność automatycznego wyszukiwania urządzeń sieciowych w wybranych podsieciach minimum za pomocą protokołu SNMP w wersji 1, 2c oraz 3.

4.3.17. System musi posiadać mechanizm automatyzacji wg harmonogramu z możliwością symulacji działania, min:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.17.1. Włączenie wskazanych portów urządzeń sieciowych.
4.3.17.2. Wyłączenie wskazanych portów urządzeń sieciowych.
4.3.17.3. Wykonania komend na wskazanych urządzeniach sieciowych.
4.3.17.4. Dodanie znalezionych urządzeń sieciowych we wskazanych podsieciach z możliwością sklonowania (automatycznego lub ręcznego) konfiguracji z podanego urządzenia sieciowego wg podanych parametrów jak: parametry dostępowe SNMP w wersji 1, 2c, 3, producenta, modelu urządzenia.

4.3.18. System musi posiadać wbudowany Captive Portal do obsługi logowania się do sieci oraz rejestracji tożsamości i urządzeń końcowych (BYOD).

4.3.19. Captive Portal musi umożliwiać rejestracje gości potwierdzanych przez konta typu sponsor lub inne konta z delegowanymi uprawnieniami.

4.3.20. Captive Portal musi umożliwiać logowanie za pomocą kont lokalnych oraz Microsoft Active Directory.

4.3.21. System musi oferować wsparcie dla linków akceptacyjnych generowanych z portalu sponsorskiego.

4.3.22. System musi oferować możliwość powiązania z bramką SMS celem wysyłania PIN-ów weryfikacyjnych. Wymagana jest obsługa PIN-ów składających się ze znaków alfanumerycznych i znaków specjalnych.

4.3.23. System musi umożliwiać przyznanie dostępu czasowego dla gości.

4.3.24. System musi umożliwiać dopasowanie wyglądu portalu logowania gościnnego, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.

4.3.25. System powinien posiadać mechanizm integracji z systemami zewnętrznymi za pomocą jednej z metod Syslog, SNMP Trap, Rest API, w celu wykrywania anomalii, blokowania dostępu do sieci, rozłączania tożsamości/urządzenia końcowego, co najmniej:
4.3.25.1. Cisco
4.3.25.2. Fortinet
4.3.25.3. ESET
4.3.25.4. RSA

4.3.26. System powinien posiadać mechanizm rozłączania dostępu do sieci z poziomu interfejsu aplikacji z możliwością określenia dodania tożsamości, urządzenia końcowego, mac adresu do kwarantanny.

4.3.27. System musi posiadać dedykowanego agenta min dla systemu Windows, Mac OS, Linux w celu profilowania urządzeń końcowych.

4.3.28. System musi posiadać funkcję automatycznego profilowania urządzeń nie posiadających agenta 802.1x (suplikanta) na podstawie: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic i przyznawania dostępu do sieci na podstawie zdefiniowanych polityk dostępu do sieci.

4.3.29. System musi umożliwiać rozpoznawanie rodzaju urządzeń podłączonych do sieci lokalnej LAN i sieci bezprzewodowej WLAN poprzez analizę informacji pochodzących z co najmniej następujących źródeł: DHCP, Network Scan (NMAP), HTTP/HTTPS, SNMP, SSH, TCP, Telnet, UDP, ONVIF, WMI, OUI producenta, WinRM, WMI, Location, Agent, IP Range, Network Traffic.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.30. System musi umożliwiać współpracę z agentem instalowanym na systemie końcowym, który zapewni sprawdzenie systemu końcowego pod kątem zgodności z polityką bezpieczeństwa w tym:
- 4.3.30.1. Weryfikacja wersji agenta.
- 4.3.30.2. Weryfikacja wersji systemu operacyjnego.
- 4.3.30.3. Weryfikacja poprawek do systemu operacyjnego.
- 4.3.30.4. Weryfikacja usługi Windows Update.
- 4.3.30.5. Weryfikacja czy włączony jest firewall.
- 4.3.30.6. Weryfikacja czy jest uruchomiony system antywirusowy i aktualna baza sygnatur.
- 4.3.30.7. Weryfikacja czy urządzenie końcowe jest podłączone do domeny Microsoft Active Directory.
- 4.3.30.8. Weryfikacja czy na dysku znajdują się pliki wskazane przez administratora.
- 4.3.30.9. Weryfikacja czy w systemie są uruchomione procesy wskazane przez administratora.
- 4.3.30.10. Weryfikacja czy w systemie są wpisy w rejestrze wskazane przez administratora wg klucza, a także pod kątem:
  - 4.3.30.10.1. Wartości klucza rejestru.
  - 4.3.30.10.2. Typu wartości: Number, String, Version.

4.3.31. System musi posiadać przełączanie VLANów na określonych portach urządzeń sieciowych.

4.3.32. System musi posiadać możliwość wysyłania komunikatów do użytkowników min za pomocą agenta i Captive Portal.

4.3.33. System musi wspierać protokoły uwierzytelniania RADIUS oraz RADIUS Proxy dla zewnętrznego serwera RADIUS.

4.3.34. System musi obsługiwać uwierzytelnianie w oparciu o następujące protokoły:
- 4.3.34.1. Radius MAC
- 4.3.34.2. 802.1X
- 4.3.34.3. TTLS/PAP
- 4.3.34.4. TTLS/MSCHAPv2
- 4.3.34.5. PEAP/MSCHAPv2
- 4.3.34.6. TLS
- 4.3.34.7. FAST

4.3.35. System musi umożliwiać uwierzytelnianie 802.1X urządzeń końcowych i tożsamości.

4.3.36. System musi umożliwiać tworzenie polityk uwierzytelniania opartych o złożone reguły:
- 4.3.36.1. Tożsamość/Urządzenie końcowe.
- 4.3.36.2. Grupa tożsamości/urządzeń końcowych.
- 4.3.36.3. Parametry urządzeń końcowych, min: system operacyjny, wersja.
- 4.3.36.4. Atrybuty Active Directory.
- 4.3.36.5. Jednostka organizacyjna tożsamości/urządzeń końcowych.
- 4.3.36.6. Urządzenia sieciowe sieci przewodowej, bezprzewodowej.
- 4.3.36.7. Grupy urządzeń sieciowych.
- 4.3.36.8. Porty urządzeń sieciowych.
- 4.3.36.9. Grupy portów urządzeń sieciowych.
- 4.3.36.10. Jednostka organizacyjna portów.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.36.11. Punkty dostępowe (AP) i/lub nazwa sieci bezprzewodowej (SSID).

4.3.36.12. Metoda autoryzacji.

4.3.37. System musi umożliwiać przypisywanie sieci VLAN i/lub atrybutów RADIUS zwrotnych VSA podczas etapu autoryzacji, np.: ACL, Quality of Service, co najmniej następujących producentów:

4.3.37.1. Cisco Networks

4.3.37.2. Aruba Networks

4.3.37.3. Hewlett Packard Enterprise

4.3.37.4. Juniper Networks

4.3.38. System musi wspierać funkcjonalność IP-to-ID Mapping, polegającą na łączeniu tożsamości, adresu IP, adresu MAC.

4.3.39. System musi wspierać funkcjonalność auto rejestracji, polegającą na łączeniu tożsamości, urządzenia końcowego, adresu MAC podczas etapu autoryzacji, minimum za pomocą mechanizmów SNMP, DHCP, NMAP, WMI.

4.3.40. System musi posiadać lokalną bazę tożsamości, tworzoną w oparciu o pojedynczą tożsamość i/lub w postaci zbiorczego pliku w formacie CSV.

4.3.41. System musi posiadać lokalną bazę urządzeń końcowych, tworzoną w oparciu o pojedynczy obiekt i/lub w postaci zbiorczego pliku w formacie CSV.

4.3.42. System musi umożliwiać konfigurację czasu ważności hasła dla tożsamości gościnnych w dniach.

4.3.43. System musi posiadać wewnętrzną bazę urządzeń. Baza musi umożliwiać wprowadzanie danych poprzez import danych, wprowadzanie danych z poziomu Systemu lub z wykorzystaniem API.

4.3.44. System musi wspierać uwierzytelnienie urządzeń końcowych na podstawie zawartych w lokalnej bazie adresów MAC.

4.3.45. System musi wykorzystywać informacje zawarte w bazie urządzeń końcowych dla potrzeb procesów wykrywania, oceniania, kwarantanny, korygowania oraz autoryzacji.

4.3.46. System musi pozwalać na weryfikację zalogowanego urządzenia końcowego IoT (Internet of Things) minimum za pomocą mechanizmów SNMP, DHCP, NMAP, Agenta oraz wywołania akcji: powiadomienie administratorów i/lub zablokowanie i rozłączenie sesji.

4.3.47. Raportowanie i monitoring. System musi umożliwiać generowanie raportów oraz monitoring przynajmniej następujących parametrów:

4.3.47.1. System musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń).

4.3.47.2. System musi mieć możliwość generowania szczegółowego wykazu urządzeń podłączonych do sieci, zorganizowanego według typu urządzenia końcowego.

4.3.47.3. System musi rejestrować dane o atrybutach urządzeń końcowych i raportować zmiany w atrybutach np. przydział do VLAN-u, przyznany adres IP, klasyfikacja urządzenia w Systemie.

4.3.47.4. System musi zapewniać dane historyczne o zmianach stanu konfiguracji portów dostępowych.

4.3.47.5. System musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania i procesem podłączanych urządzeń. Dane muszą być przechowywane i dostępne do analizy przez co najmniej 12 miesięcy.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.3.47.6. System musi oferować możliwość tworzenia własnych szablonów raportów.

4.3.47.7. System musi umożliwiać logowanie do zewnętrznych serwerów logowania z wykorzystaniem Syslog.

4.3.47.8. System musi umożliwiać konfigurację generowanych alarmów i zautomatyzowanych akcji w oparciu o zdarzenia wewnętrzne np. w przypadku stwierdzenia zagrożenia na stacji, zablokowanie jej i powiadomienie administratora.

4.3.47.9. System musi umożliwiać podgląd tożsamości, urządzeń końcowych zalogowanych do sieci w czasie rzeczywistym z podziałem wg urządzeń sieciowych, kontrolerów wifi.

4.3.48. System powinien logować i przetrzymywać we własnej bazie danych co najmniej następujące informacje:

4.3.48.1. adresy MAC przełączników, urządzeń końcowych i dostępowych,

4.3.48.2. adresy IP ww. urządzeń,

4.3.48.3. identyfikatory i nazwy portów przełączników określające porty na przełącznikach i urządzeniach dostępowych do których podłączane są urządzenia końcowe,

4.3.48.4. stan skanowania - wyniki skanowania urządzenia końcowego i jego ocena w oparciu o skanowanie przeprowadzone przy pomocy dostępnych w rozwiązaniu agentów,

4.3.48.5. informacje o użytkownikach,

4.3.48.6. nazwa użytkownika do którego przypisany jest urządzenie końcowe,

4.3.48.7. nazwa zalogowanego użytkownika na urządzeniu końcowym, jeśli wykonywana jest na nim autoryzacja,

4.3.48.8. profil/rola jak została przydzielona urządzeniu końcowemu przez System,

4.3.48.9. data zarejestrowania urządzenia końcowego w Systemie,

4.3.48.10. data ostatniego logowania urządzenia końcowego w sieci lub/i podłączenia.

4.3.49. System musi umożliwiać wykonywanie na urządzeniach sieciowych skryptów CLI, które są elementem polityk bezpieczeństwa.

4.3.50. Alertowanie

4.3.50.1. System musi umożliwiać generowanie alarmów systemowych w sytuacjach krytycznych za pomocą:

4.3.50.1.1. wiadomości e-mail,

4.3.50.1.2. Syslog.

4.4. **Dodatkowe funkcjonalności Systemu.**

4.4.1. Wszystkie komponenty Systemu na stacji monitorowanej powinny mieć możliwość automatycznego wdrażania i konfiguracji w oparciu o predefiniowane reguły zarządzania.

4.4.2. System powinien obsługiwać automatyczny transfer logów z agentów w celu archiwizacji.

4.4.3. Wymagana jest możliwość wykorzystania mechanizmy proxy do komunikacji z Internetem.

4.4.4. System musi umożliwiać personalizację wyglądu interfejsu zarządzania, w tym co najmniej zmianę logo strony logowania, zmianę koloru tła i czcionek, treści, grafiki.

4.4.5. Monitoring autoryzacji:

4.4.5.1. Autoryzacje zaakceptowane w ciągu ostatnich 30 dni.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.4.5.2. Autoryzacje odrzucone w ciągu ostatnich 30 dni.

4.4.5.3. Obciążenie serwera autoryzacji.

4.4.5.4. Ostatnie 100 zdarzeń autoryzacji.

4.4.6. Monitoring dla zdarzeń systemowych:

4.4.6.1. Ostatnie 100 zdarzeń systemowych.

4.4.7. Monitoring dla tożsamości:

4.4.7.1. Podział tożsamości ze względu na typ konta.

4.4.7.2. Podział tożsamości ze względu na tożsamości aktywne i nieaktywne.

4.4.7.3. Podział tożsamości ze względu na konta, które straciły ważność.

4.4.7.4. Wykorzystanie kont gościnnych z dostępem czasowym.

4.4.8. Monitoring dla urządzeń końcowych:

4.4.8.1. Podział urządzeń ze względu na ich status.

4.4.8.2. Podział urządzeń ze względu na ich typ.

4.4.8.3. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.

4.4.9. Monitoring dla urządzeń sieciowych:

4.4.9.1. Podział urządzeń ze względu na urządzenia aktywne i nieaktywne.

4.4.9.2. Podział urządzeń ze względu na ich typ.

4.4.10. Raport stanu systemu z poziomu konsoli CLI min. obciążenie procesora, pamięci, przestrzeni dyskowej, działania usług.

5. Gwarancja

5.1 Zapisy ogólne

5.1.1. Wykonawca udziela Zamawiającemu Gwarancji na:

5.1.1.1. Wdrożony System.

5.1.1.2. Oprogramowanie.

5.1.2. Wykonawca oświadcza, że Oprogramowanie przez niego dostarczone objęte jest gwarancją producenta.

5.1.3. Wykonawca udziela gwarancji na elementy wymienione w pkt 1.1-1.3, która obowiązuje przez okres 24 miesięcy od daty podpisania Protokołu odbioru, wskazanego w Umowie.

5.1.4. Wykonawca zobowiązany jest w okresie realizacji Umowy do usuwania Błędów elementów wymienionych w pkt 1.1-1.3 na zasadach opisanych w niniejszym załączniku.

5.1.5. Zakres świadczeń w ramach Gwarancji obejmuje:

5.1.5.1. usuwanie Błędów elementów wymienionych w pkt 1.1-1.3 zgodnie z Czasami Reakcji, Czasami Naprawy, Czas Propozycji Rozwiązania i dla poszczególnych kategorii Błędów,

5.1.5.2. dostarczanie nowych wersji Oprogramowania,

5.1.5.3. aktualizację Dokumentacji w przypadku wprowadzania zmian w Systemie lub Oprogramowaniu w wyniku naprawy Błędu, w terminie 5 Dni Roboczych od dnia naprawy.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.1.6. Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych z wykorzystaniem Systemu.

5.1.7. W ramach świadczenia przez Wykonawcę usług w ramach Gwarancji, Wykonawca zobowiązany jest do umożliwienia osobom wskazanym przez Zamawiającego obserwacji prac Wykonawcy.

5.1.8. W przypadku wykrycia przez Zamawiającego Błędu, Zamawiający dokona kwalifikacji zgłoszenia (Błąd Krytyczny/Błąd Zwykły) według własnego uznania na podstawie zdefiniowanych kryteriów. Zgłoszenie zawierać będzie posiadane przez Zamawiającego informacje na temat nieprawidłowego działania Systemu istotne w ocenie Zamawiającego dla zdiagnozowania i usunięcia nieprawidłowości w działaniu Systemu.

5.1.9. Formalne potwierdzenie Zgłoszenia stanowi przesłanie przez Zamawiającego do Wykonawcy informacji o wystąpieniu Błędu i opisie jego symptomów.

5.1.10. Wykonawca zobowiązuje się rejestrować zgłaszane Błędy wykorzystując rozwiązania umożliwiające raportowanie Zgłoszeń - w tym Czas Reakcji, Czas Propozycji Rozwiązania oraz Czas Naprawy.

5.1.11. Wykonawca będzie przyjmował Zgłoszenia przez cały czas, tj. w systemie 8:00-16:00 Dni Robocze.

5.1.12. Wykonawca będzie przyjmował Zgłoszenia przekazywane w jeden z następujących sposobów:

5.1.12.1. za pomocą aplikacji serwisowej (interfejsu serwisowego),

5.1.12.2. przez przesłanie Zgłoszenia pocztą elektroniczną na adres: ……@.....

5.1.13. W razie otrzymania przez Wykonawcę Zgłoszenia lub w razie uzyskania przez Wykonawcę wiedzy o wystąpieniu Błędu z innego źródła niż Zgłoszenie, Wykonawca zobowiązany będzie do podjęcia działań zmierzających do usunięcia Błędu.

5.1.14. Jeżeli Zamawiający nie wie o istnieniu Błędu, Wykonawca poinformuje w ciągu 24 godzin, Zamawiającego o jego wystąpieniu.

5.1.15. Jeżeli Wada została wykryta przez Wykonawcę, Wykonawca nada jej odpowiednią wstępną kategorię (Błąd Krytyczny / Błąd Zwykły). W ciągu 2 godzin od powiadomienia przez Wykonawcę Zamawiający ma prawo zmienić kategorię Błędu.

5.1.16. Ostatecznie o klasyfikacji kategorii Błędu (Błąd Krytyczny / Błąd Zwykły) decyduje Zamawiający.

5.1.17. Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia odpowiednim wpisem we własnej aplikacji serwisowej (dotyczy to również Zgłoszeń składanych pocztą elektroniczną) oraz o nadaniu indywidualnego identyfikatora zgłoszenia. Chwila potwierdzenia przyjęcia Zgłoszenia nie ma wpływu na Czas Reakcji, Czas Propozycji Rozwiązania, Czas Naprawy. Wykonawca jest zobowiązany do udostępnienia Zamawiającemu własnej aplikacji serwisowej w zakresie przeglądania Zgłoszeń związanych z realizacją Umowy.

5.1.18. Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Systemu, którego dotyczy Zgłoszenie nie jest spowodowane Błędem, za który odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest:

5.1.18.1. wskazać przyczynę nieprawidłowego działania poprzez wskazanie elementu, który ją powoduje,

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.1.18.2. udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o Systemie lub Oprogramowaniu potrzebnych do przywrócenia pełnej funkcjonalności.

5.1.19. Po przeprowadzeniu Naprawy, Wykonawca zgłosi ją do odbioru poprzez przekazanie informacji :

5.1.19.1. za pomocą aplikacji serwisowej (interfejsu serwisowego),

5.1.19.2. przez przesłanie pocztą elektroniczną na adres: ……@.....

5.1.20. Po weryfikacji dokonania Naprawy, przedstawiciel Zamawiającego niezwłocznie potwierdzi w systemie lub drogą elektroniczną skuteczność lub nieskuteczność Naprawy. Data i godzina rejestracji w systemie lub wysłania maila przez przedstawiciela Zamawiającego jest datą i godziną wykonania usługi Naprawy.

5.1.21. W przypadku stwierdzenia dokonania skutecznej Naprawy Wykonawca zamyka Zgłoszenie i potwierdza jego wykonanie poprzez „zamknięcie" zgłoszenia w aplikacji serwisowej.

5.1.22. Naprawa, co do której Wykonawca poinformował o jej wykonaniu, a która została odrzucona przez przedstawiciela Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd nadal występuje, trwa do czasu jej skutecznego wykonania.

5.1.23. Wykonawca zobowiązany jest do prowadzenia ewidencji otwartych i zamkniętych Zgłoszeń, obejmującej w szczególności opis stanu realizacji danej Naprawy. Powyższe dane dostępne są cały czas dla Zamawiającego za pośrednictwem aplikacji serwisowej.

5.1.24. Wraz z dokonaniem Naprawy Wykonawca zobowiązany jest opracować i przekazać Zamawiającemu odpowiednie Dokumenty, o ile zachodzi taka potrzeba.

5.1.25. Jeżeli Wykonawca nie dokona Naprawy Błędu w określonym terminie to Zamawiający może według swojego uznania:

5.1.25.1. zawiadamiając uprzednio Wykonawcę usunąć Błąd we własnym zakresie lub powierzyć jej usunięcie innym podmiotom trzecim na ryzyko i koszt Wykonawcy, co nie spowoduje utraty przysługujących Zamawiającemu uprawnień z tytułu Gwarancji – przy czym koszty poniesione przez Zamawiającego przy usunięciu Błędu mogą być potrącone z wynagrodzenia przysługującego Wykonawcy lub z zabezpieczenia należytego wykonania przedmiotu Umowy, na co Wykonawca wyraża zgodę lub

5.1.25.2. obciążyć Wykonawcę karą umowną.

5.1.26. Jeżeli w trakcie realizacji zobowiązań z tytułu Gwarancji dojdzie do wprowadzenia zmian w Dokumentach, wówczas do przejścia autorskich praw majątkowych do zmienionych Dokumentów stosuje się odpowiednio postanowienia Umowy, w zakresie Dokumentów będących wynikiem zmian. W zakresie Oprogramowania lub jego dokumentacji, ich producent z chwilą wykonania zobowiązań z tytułu gwarancji udziela licencji na zasadach określonych w Umowie.

5.1.27. W uzasadnionych przypadkach Strony mogą podjąć decyzję o wydłużeniu Czasu Naprawy.

5.2. Warunki Gwarancji dla Oprogramowania

5.2.1.Gwarancją objęta jest całość dostarczonego Oprogramowania.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.2.2. Wykonawca zapewni elektroniczny dostęp do informacji na temat dostarczonego Oprogramowania oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania.

5.2.3. W przypadku Oprogramowania:

5.2.3.1. Wykonawca zapewnia Zamawiającemu dostarczanie aktualizacji, nowych wersji oraz zmian Oprogramowania/ opracowanych przez producentów w okresie gwarancji. Wykonawca zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim na zasadach określonych w niniejszym załączniku oraz Umowie.

5.2.3.2. Aktualizację Oprogramowania, w szczególności dostarczania i instalacji nowych wersji Oprogramowania systemowego i Oprogramowania, dostarczania i instalacji wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych.

5.2.3.3. Informuje o najlepszych praktykach i zasadach postępowania.

5.3. Poziomy SLA dla Oprogramowania/Systemu

Kategoria Błędu (priorytety)	**Czas Reakcji** (od momentu zgłoszenia)	**Czas Propozycji Rozwiązania** (od momentu potwierdzenia)	**Czas Naprawy** (od momentu zgłoszenia)
Błąd Zwykły	1 Dzień Roboczy	1 Dzień Roboczy	3 Dni Robocze
Błąd Krytyczny	2 godziny	12 godzin	24 godziny

5.3.1. Zgłoszenie o zwykłym priorytecie (Błąd Zwykły) - w zakresie błędów związanych z Oprogramowaniem/Systemem z czasem reakcji maksymalnie 1 Dzień Roboczy od chwili zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 1 Dni Roboczy od dnia potwierdzenia zwrotnego przyjęcia zgłoszenia (przez Dni Robocze rozumie się dni od poniedziałku do piątku w godzinach 8:00-16:00, z wyjątkiem dni ustawowo wolnych od pracy i dni wolnych od pracy u Zamawiającego). Rozwiązanie problemu o priorytecie zwykłym przez Wykonawcę nastąpi w terminie nie przekraczającym 3 Dni Robocze od zgłoszenia Błędu Zwykłego.

5.3.2. Zgłoszenie o krytycznym priorytecie (Błąd Krytyczny) - obejmujące pomoc przy wykryciu na serwerach produkcyjnych błędów krytycznych, konfiguracji Oprogramowania z czasem reakcji maksymalnie 2 godziny od chwili zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 12 godzin od momentu potwierdzenia zwrotnego przyjęcia zgłoszenia. Rozwiązanie problemu o priorytecie krytycznym przez Wykonawcę nastąpi w terminie nie przekraczającym 24 godziny od momentu zgłoszenia Błędu Krytycznego.

6. Instruktaż dla pracowników Zamawiającego

Wykonawca przeprowadzi instruktaż dla nie więcej niż 10 pracowników Zamawiającego, który przygotuje wskazanych pracowników do samodzielnego konfigurowania Systemu, operowania Systemem z poziomu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

administratora, użytkownika oraz wykorzystywania Systemu skonfigurowanego w specyficznej infrastrukturze Zamawiającego, w szczególności do samodzielnej konfiguracji Systemu.

6.1. Instruktaż zostanie przeprowadzony [w języku polskim] przez osoby będące trenerami producenta lub Wykonawcy oraz posiadające kwalifikacje i umiejętności potwierdzone certyfikatem producenta oferowanego Systemu.

6.2. Lista uczestników instruktażu zostanie ustalona drogą mailową z Wykonawcą po podpisaniu umowy.

6.3. Instruktaż zostanie zorganizowany w czasie trwania wdrożenia Systemu opisanego w pkt 3.

6.4. Termin przeprowadzenia instruktażu zostanie ustalony pomiędzy Zamawiającym a Wykonawcą.

6.5. Instruktaż będzie realizowany w Dni Robocze w godzinach 8:00-16:00 w siedzibie Zamawiającego lub zdalnie za zgodą Zamawiającego. Instruktaż może się odbyć w postaci zdalnego spotkania o ile zostaną spełnione wszystkie wymagania instruktażu.

6.6. Instruktaż będzie trwał minimum 2 Dni Robocze (łącznie minimum 16 godzin zegarowych).

6.7. Harmonogramy zajęć zostaną ustalone drogą mailową z Zamawiającym.

6.8. Wykonawca musi posiadać autoryzację producenta Systemu w zakresie prowadzenia instruktażu z wdrożonego u Zamawiającego Systemu.

6.9. Dla uczestników instruktażu Wykonawca przygotuje środowisko testowe z zainstalowaną wersją Systemu tożsamą dla wdrożonego u Zamawiającego Systemu pozwalające na zapoznanie się, z elementami interfejsu graficznego oraz wykonanie ćwiczeń w warunkach możliwie zbliżonych do realnych.

6.10. Wykonawca zapewni dla każdego uczestnika wersję elektroniczną materiałów dydaktycznych zawierających streszczenie/omówienie wszystkich zagadnień zawartych w programie instruktażu oraz prezentacje wykorzystane podczas instruktażu.

6.11. Jeśli na potrzeby realizacji instruktażu powstaną materiały edukacyjne będące utworami w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych będą one w ramach wynagrodzenia przewidzianego w Umowie udostępnione na licencji zapewniającej licencjobiorcy – Zamawiającemu prawo do wykorzystywania utworów zgodnie z ich przeznaczeniem na czas nieokreślony.

6.12. Zakres tematyczny instruktażu będzie zawierał się w niniejszych obszarach:

- 6.12.1. Architektura produktu.
- 6.12.2. Poruszanie się po interfejsie użytkownika.
- 6.12.3. Planowanie wdrożenia systemu wraz z architekturą systemu.
- 6.12.4. Instalacja konsoli zarządzania i agentów na stacjach końcowych.
- 6.12.5. Konfiguracja reguł filtrujących/analizujących dla dedykowanego systemu końcowego.
- 6.12.6. Wykonanie przykładowych scenariuszy:
  - 6.12.6.1. Konfigurowanie nowych polityk dostępu.
  - 6.12.6.2. Konfigurowanie nowych polityk weryfikacji zgodności stacji końcowych.
  - 6.12.6.3. Konfigurację wysyłania logów do systemu klasy SIEM.
- 6.12.7. Monitorowanie działania systemu.
- 6.12.8. Automatyzacja zadań w tym definiowanie alertów w odpowiedzi na wykryte zdarzenia.
- 6.12.9. Manualne uruchamianie zadań.
- 6.12.10. Analiza i raportowanie wyników.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

6.12.11. Konfiguracja zadań/reakcji na zdarzenia.
6.12.12. Zarządzanie użytkownikami i rolami.

Sporządził: Jeremi Olechnowicz

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706