Fundusze Europejskie Polska Cyfrowa

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

Warszawa, dnia 04.11.2020

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

PRZETARG NIEOGRANICZONY: KZP/08/2020

Postępowanie o udzielenie zamówienia publicznego w trybie:
PRZETARGU NIEOGRANICZONEGO

na dostawę, konfigurację i uruchomienie zestawu UTM

CPV: 32422000-7

Wartość szacunkowa zamówienia poniżej 214 000 euro.

Miejsce dostawy:

Sieć Badawcza Łukasiewicz –
Przemysłowy Instytut Automatyki i Pomiarów PIAP

Al. Jerozolimskie 202, 02-486 Warszawa

Zamawiający:

Sieć Badawcza Łukasiewicz –
Przemysłowy Instytut Automatyki i Pomiarów
PIAP
Al. Jerozolimskie 202, 02-486 Warszawa
Adres strony internetowej: www.piap.pl

I. Nazwa oraz adres Zamawiającego.

Sieć badawcza Łukasiewicz - Przemysłowy Instytut Automatyki i Pomiarów PIAP
Al. Jerozolimskie 202 02 – 486 Warszawa.

Adres strony internetowej: www.piap.pl

II. Tryb udzielenia zamówienia.

1. Niniejsze postępowanie prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 i nast. ustawy z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych zwanej dalej „ustawą PZP".
2. W zakresie nieuregulowanym niniejszą Specyfikacją Istotnych Warunków Zamówienia, zwaną dalej „SIWZ", zastosowanie mają przepisy ustawy PZP.
3. Wartości zamówienia nie przekracza równowartości kwoty określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 ustawy PZP.
4. Postępowanie prowadzone jest w wersji tradycyjnej oraz za pomocą platformy zakupowej.
5. Wejście na platformę poprzez link: https://piap.ezamawiajacy.pl/servlet/HomeServlet

Wykonawca celem skorzystania z platformy winien z odpowiednim wyprzedzeniem założyć darmowe konto na platformie.
Numer wsparcia Wykonawców: +48 22 25 72 223

III. Opis przedmiotu zamówienia.

1. Przedmiotem zamówienia jest dostawa, konfiguracja i uruchomienie zestawu UTM, wraz ze wsparciem technicznym na okres 3 lat oraz szkoleniem użytkowników systemu w zakresie określonym poniżej:

2. Wykonawca zobowiązany jest zrealizować zamówienie na zasadach i warunkach opisanych we wzorze umowy stanowiącym **Załącznik nr** 2 do SIWZ.
3. Wspólny Słownik Zamówień CPV: **32422000-7**
4. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
5. Wykonawca może złożyć ofertę na jedną albo więcej części zamówienia
6. Zamawiający nie dopuszcza możliwości składania ofert wariantowych
7. Zamawiający nie przewiduje możliwości udzielenie zamówień, o których mowa w art. 67 ust. 1 pkt 7
8. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę żadnych prac związanych z rozmieszczeniem i instalacją przedmiotu dostawy

Szczegółowy opis przedmiotu zamówienia

Specyfikacja urządzenia UTM – dane techniczne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

Funkcje modułu Firewall

1. System realizujący funkcję Firewall musi zostać dostarczony w postaci klastra pracującego w trybie Active-Passive składającego się z dwóch urządzeń.
2. Musi umożliwiać zdefiniowanie co najmniej 5 stref bezpieczeństwa (Zewnętrzna, DMZ1, DMZ2, Wewnętrzna1, Wewnętrzna2).
3. Musi umożliwiać pracę jako router (każdy port obsługuje inny adres sieci/podsieci IP) lub jako bridge (transparent mode).
4. Musi obsługiwać protokoły dynamicznego routingu: RIP v1/v2, OSPF i BGP4.
5. Musi obsługiwać Multicast routing.
6. Musi obsługiwać Policy Based routing.
7. Musi umożliwiać znakowanie QoS w oparciu o ToS (Type of Service) lub DSCP (Differentiated Service Code Point) w ramach zapewnienia jakości usług.
8. Musi obsługiwać statyczne i dynamiczne adresy IP (DHCP i PPPoE) na zewnętrznym interfejsie.
9. Musi obsługiwać DHPCv6 na zewnętrznym interfejsie.
10. Musi obsługiwać funkcję agregacji linków (802.3ad dynamic, static, active/backup).
11. Musi obsługiwać Dynamic DNS.
12. Musi obsługiwać translację adresów: statyczną, dynamiczną i 1-1.
13. Musi obsługiwać translację portów: PAT.
14. Musi obsługiwać IPSec NAT traversal.
15. Musi obsługiwać mechanizm Policy Based NAT.
16. Musi obsługiwać VLAN 802.1Q.
17. Musi zapewniać funkcję serwera DHCP (dla IPv4 i IPv6) dla wszystkich interfejsów sieciowych.
18. Musi umożliwiać pracę w trybie DHCP Relay, z jednoczesną obsługą co najmniej 3 serwerów DHCP.
19. Musi mieć możliwość obsługi zapasowego łącza typu LTE poprzez podłączenie zewnętrznego modemu USB.
20. Musi mieć możliwość automatycznego przełączania ruchu pomiędzy interfejsami zewnętrznymi w przypadku awarii jednego z nich.
21. Musi zapewniać funkcję równoważenia obciążenia pomiędzy interfejsami zewnętrznymi.

22. Musi zapewniać funkcjonalność SD-WAN w ramach automatycznej dystrybucji ruchu na podstawie jakości łącza.
23. Musi zapewniać funkcję równoważenia obciążenia w ramach połączeń do wewnętrznych serwerów.
24. Musi umożliwiać uwierzytelnianie użytkowników oraz identyfikację odpowiadającego im ruchu sieciowego.
25. Musi umożliwiać uwierzytelnianie użytkowników z wykorzystaniem: ActiveDirectory, LDAP, Radius, SecureID, VASCO oraz wewnętrznej bazy użytkowników.
26. Musi umożliwiać transparentne uwierzytelnianie użytkowników przy integracji z Active Directory.
27. Urządzenie musi posiadać co najmniej 4 mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Active Directory.
28. Co najmniej dwie metody transparentnej autoryzacji nie wymagają instalacji dedykowanego
    agenta na stacjach roboczych użytkowników.
29. Musi umożliwiać uwierzytelnianie i rozpoznawanie użytkowników korzystających z usług terminalowych Microsoft oraz Citrix.
30. Nie może ograniczać ilość urządzeń, adresów IP czy użytkowników sieci wewnętrznej.
31. Musi dostarczać mechanizmów identyfikacji urządzeń w sieci w tym co najmniej identyfikację systemu operacyjnego, otwartych portów i usług.
32. Musi zapewniać możliwość blokowania komunikacji z wybranymi krajami w zakresie poszczególnych protokołów i aplikacji.
33. Musi zapewniać możliwość blokowania komunikacji z wybranymi adresami IP, wybranymi adresami domenowymi oraz w oparciu o reputację adresów IP i/lub domen.
34. Musi posiadać mechanizmy rozpoznawania anomalii w protokołach sieciowych - dla najpopularniejszych protokołów.
35. Musi umożliwiać sterowanie przepustowością w oparciu o politykę zapory sieciowej oraz wybraną aplikację.
36. Musi dostarczać mechanizmów limitowania dostępu do sieci użytkownikom w oparciu o quoty czasowe lub transferu danych, co najmniej dla komunikacji http.
37. Musi zapewnić wsparcie implementacji polityki bezpieczeństwa w warstwie aplikacji (warstwa 7) minimum dla protokołów: HTTP, HTTPS, FTP, DNS, SMTP, POP3, IMAP, SMPTS, POP3S, IMAPS, H.323, SIP.
38. Musi zapewniać funkcjonalność Content Routing w ramach protokołu HTTP/HTTPS na podstawie co najmniej nagłówka hosta HTTP i żądania HTTP.
39. Musi zapewniać funkcjonalność TLS/SSL Offloading dla protkołu HTTPS w ramach połączeń do wewnętrznych serwerów.
40. Musi pełnić rolę bramki VPN terminującej połączenia VPN site-to-site i client-to-site.

Dostarczony system bezpieczeństwa musi zapewniać:

1. Ochronę z wykorzystaniem mechanizmów IPS.

2. Ochronę antywirusową.
3. Ochronę przed nieznanymi zagrożeniami.
4. Ochronę przed phishingiem.
5. Ochronę przed niechcianą pocztą.
6. Kontrolę wykorzystywanych aplikacji.
7. Możliwość filtrowania URL.

Parametry fizyczne systemu Firewall:
Element systemu pełniący funkcję Firewall musi dysponować :

- 8 portami 1Gb RJ45.
- System musi umożliwiać rozbudowę o dodatkowe porty: 4 x porty optyczne 10G lub
  8 x porty optyczne 1G lub 8 x porty miedziane 1G .
- Minimum 4 GB pamięci RAM.
- Minimum 2 porty USB 3.0.
- Minimum jeden port typu Console.
- Minimalna temperatura pracy urządzenia od 0 do 40 stopni Celsjusza.

Parametry wydajnościowe systemu:

- Przepustowość Firewall minimum: 19.6 Gbps.
- Przepustowość IPSec VPN nie mniejsza niż: 5.2 Gbps.
- Przepustowość skanowania antywirusowego nie mniejsza niż: 3.5 Gbps.
- Przepustowość w ramach ochrony przed atakami nie mniejsza niż: 5.7 Gbps.
- Przepustowość systemu z włączonymi mechanizmami skanowania antywirusowego, ochrony przed atakami, kontroli aplikacji minimum: 3.1 Gbps.
- Obsługa nie mniej niż: 250 tuneli IPSec site-to-site.
- Obsługa nie mniej niż: 250 tuneli client-to-site.
- Obsługa nie mniej niż: 3.800.000 jednoczesnych połączeń.
- Obsługa nie mniej niż: 82.000 nowych połączeń na sekundę.
- W ramach Firewall system musi obsługiwać minimum: 300 sieci VLAN.

W ramach ochrony przed atakami system musi zapewniać:

1. Automatyczną aktualizację bazy sygnatur IPS. Musi ona zawierać co najmniej 8000 definicji sygnatur.
2. Automatyczne blokowanie znanych źródeł ataków.
3. Ochronę przed lukami w zabezpieczeniach w aplikacjach, bazach danych, systemach operacyjnych.
4. Mechanizmy ochrony przed atakami typu DoS i DDoS co najmniej (IPsec Flood, IKE Flood, ICMP Flood, Syn Flood, UDP Flood, IP Scan, Ilość połączeń, Port Scan, IP Source Route, ARP/IP Spoofing).
5. Mechanizmy blokowania przed atakami typu: SQL Injection, Cross-Site-Scripting, Buffer OverFlow, Remote File Inclusions.

6. Mechanizm, który pozwoli generować alarmy – dla wskazanego poziomu nasilenia ataku.

W ramach kontroli antywirusowej system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o możliwość uruchomienia co najmniej 2 skanerów antywirusowych opartych na analizie sygnaturowej oraz bez sygnaturowej lokalnie lub system musi posiadać mechanizmy integracji z drugim zewnętrznym skanerem działającym lokalnie. W przypadku skanera zewnętrznego koniecznym jest dostarczenie pełnej dokumentacji przykładowego systemu oraz wykazanie w testach poprawności działania takiej integracji z zewnętrznym skanerem lokalnym.
2. Automatyczną aktualizację baz sygnatur, nie rzadziej niż co 12 godzin.
3. Mechanizmy kwarantanny e-mail dla wiadomości wskazanych przez silnik antywirusowy jako niebezpieczne.
4. Możliwość skanowania plików o rozmiarze co najmniej 20MB.
5. Możliwość zdefiniowania rozmiaru skanowanego pliku.
6. Możliwość skanowania plików w wielokrotnie skompresowanych archiwach.
7. Ilość sygnatur w ramach skanera sygnaturowego nie może być mniejsza niż 2.500.000.
8. Możliwość tworzenia wyjątków (biała lista) dla określonych adresów URL, typów plików, sygnatury pliku MD5.
9. Wykrywanie i blokowanie złośliwego oprogramowania typu: Virus, Trojan, Worms, Spyware, Rougeware, Malware.
10. Wsparcie dla głównych protokołów: HTTP, HTTPS, FTP, SMTP, POP3, IMAP, IMAPS, POP3S, SMTPS.

W ramach ochrony przed nieznanymi zagrożeniami system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję analizy behawioralnej w oparciu o platformę typu sandbox, w tym co najmniej:
   - W tym zakresie system musi pracować w trybie lokalnym lub z wykorzystaniem mechanizmów chmury (w granicach Unii Europejskiej).
   - Analizę plików pobieranych przez HTTP/HTTPS i przesyłanych pocztą elektroniczną (SMTP, POP3, IMAP) oraz plików pobieranych za pomocą protokołu FTP.
   - Ogólne oszacowanie poziomu ryzyka dla analizowanych plików i określanie różnego rodzaju akcji na ich podstawie.
   - Kwarantannę podejrzanych plików co najmniej dla protokołu SMTP.
   - Możliwość blokowania wiadomości e-mail przesyłanej protokołem SMTP zawierającej podejrzane załączniki do czasu zakończenia ich analizy.
   - Możliwość analizy plików o rozmiarze co najmniej 10MB.
   - Brak ograniczeń co do ilości analizowanych plików.

W ramach ochrony przed phishingiem system musi zapewniać:

1. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję ochrony przed phishingiem, w tym co najmniej:
   - Możliwość blokowania dostępu do spreparowanych stron.
   - Ochronę przed phishingiem niezależnie od typu połączenia, protokołu, portu.
   - Możliwość tworzenia białych/czarnych list domen, do których połączenia będą filtrowanie.
   - Notyfikację użytkownika, którego dotyczy zdarzenie - niezależnie od logów i raportów.
   - Kontrolę zapytań DNS.

W ramach kontroli antyspamowej system musi zapewniać:

1. Analizę wiadomości pocztowych w oparciu o technologię Recurrent Pattern Detection.
2. Kwarantannę wiadomości e-mail przesyłanych protokołem SMTP, wskazanych przez moduł Antyspam.
3. Możliwość oznaczania wiadomości e-mail określonych jako spam poprzez dodanie informacji do tematu wiadomości e-mail.
4. Blokowanie spamu w oparciu o język, format i zawartość wiadomości e-mail.
5. Możliwość tworzenia białych/czarnych list, w oparciu o które system zezwala lub odmawia wysyłania wiadomości e-mail dla określonych nadawców i odbiorców.
6. Możliwość usuwania złośliwego oprogramowania z wiadomości e-mail.

W ramach filtrowania zawartości URL system musi zapewniać:

1. Filtrowanie URL z wykorzystaniem baz i kategorii stron dostępnych w formie subskrypcji.
2. Baza filtra url musi zawierać co najmniej 130 kategorii stron, w tym kategorie istotne z punktu widzenia bezpieczeństwa: Command&Control, Proxy Avoidance, Bot Networks, Malicious sites, Phishing, Spyware.
3. Baza URL musi zawierać co najmniej 14.000.000 skategoryzowanych stron www.
4. Odpytywanie bazy on-line w czasie rzeczywistym.
5. Możliwość wysłania modyfikowalnej notyfikacji do użytkownika o tym dlaczego dostęp do strony www został zablokowany.
6. Możliwość uzyskania dostępu do zablokowanych stron www na podstawie grupy użytkownika lub hasła.
7. Możliwość określenia różnego rodzaju akcji dla nieskategoryzowanych stron www.
8. Możliwość tworzenia białych/czarnych list wyjątków dla filtrowania zawartości URL.
9. Możliwość określania reputacji adresu URL i na podstawie reputacji podejmowanie określonych akcji.
10. Możliwość filtrowania treści w oparciu o typy MIME.
11. Możliwość blokowania plików cookies dla określonych domen.
12. Możliwość filtrowania metod żądań i odpowiedzi protokołu HTTP.
13. Analizę treści dla protokołu https.
14. Wyłączenie inspekcji https dla wybranych kategorii stron www.

W ramach kontroli aplikacyjnej system musi zapewniać:

1. Rozpoznawanie aplikacji oraz kategorii aplikacji w oparciu o analizę ruchu a nie przez porty i protokoły.
2. Ilość rozpoznawanych aplikacji: nie mniej niż 1800, podzielonych na kategorie.
3. W ramach konkretnych aplikacji system musi umożliwiać kontrolę specyficznych akcji (np. w komunikatorach dopuszczać czat tekstowy ale blokować rozmowy głosowe, blokować wysyłanie plików).
4. Rozpoznawanie aplikacji co najmniej: Tor, CryptoAdmin, Proxy, Peer-to-peer, VoIP, MS Office 365, Gadu-gadu, Gry online.
5. Możliwość ograniczania wykorzystywanej przepustowości aplikacji lub kategorii aplikacji.

Wymagane funkcje VPN systemu:

1. Musi obsługiwać połączenia VPN site-to-site z wykorzystaniem IPSec oraz IPSec over GRE.
2. W zakresie IPSec site-to-site VPN musi współpracować z rozwiązaniami innych producentów.
3. Musi wspierać mechanizmy szyfrowania DES, 3DES, AES 128 -, 192 -, 256-bit, AES-GCM-256.
4. Musi wspierać mechanizmy uwierzytelniania: SHA-2,MD5, IKE Pre-Shared Key, certyfikaty.
5. Obsługa Dead Peer Detection (DPD).
6. Wsparcie dla IKEv1 i IKEv2.
7. Urządzenie musi obsługiwać Perfect Forward Secrecy (PFS) z wykorzystaniem algorytmów Diffie-Hellman.
8. Wsparcie dla VPN failover (wznawianie połączenia na drugim łączu w przypadku awarii głównego).
9. Musi zapewniać możliwość tworzenia wirtualnych interfejsów VPN site-to-site i przesyłania ruchu w oparciu o protokoły dynamicznego routingu.
10. Musi obsługiwać połączenia VPN client-to-site z wykorzystaniem protokołów: IPSec, SSL, L2TP, IKEv2.
11. Połączenia clinet-to-site muszą być możliwe z systemów: Windows 7, 8 i 10, MacOS, iOS i Android.
12. Dla połączeń IPSec client-to-site musi być możliwość zestawienia połączenia VPN przed zalogowaniem się użytkownika do systemu Windows.
13. Musi umożliwiać uruchomienie portalu SSL VPN, który umożliwia autoryzację w oparciu o protokoły RADIUS, LDAP, Active Directory, lokalną bazę użytkowników.
14. Portal SSL VPN musi zapewniać wsparcie dla protokołów: SSH, RDP, HTTP.
15. Portal SSL VPN musi wspierać funkcjonalność Single-Sign-On dla aplikacji webowych w oparciu o protokół SAML.

Zarządzanie

1. Elementy systemu muszą umożliwiać zarządzanie za pomocą linii poleceń (poprzez port szeregowy lub poprzez SSH) oraz za pomocą wbudowanego interfejsu www.

2. Interfejs www do zarządzania musi mieć właściwość automatycznego dopasowania rozdzielczości i czytelności podczas pracy na różnych urządzeniach.
3. Wymaga się, aby rozwiązanie wspierało instalację zdalną, bez konieczności obecności personelu technicznego w miejscu implementacji.
4. W ramach dostarczonego rozwiązania musi istnieć możliwość wyświetlenia mapy sieci wewnętrznej zawierającej szczegółowe dane na temat urządzeń (MAC, IP, System operacyjny).
5. Elementy systemu bezpieczeństwa pełniące funkcje: Firewall, VPN, Ochrona przed atakami, Kontrola Aplikacji - muszą integrować się z dedykowaną aplikacją lub platformą centralnego zarządzania instalowaną lokalnie.
6. Elementy systemu bezpieczeństwa muszą zapewniać możliwość logowania do co najmniej dwóch systemów logowania i raportowania.
7. Komunikacja do systemów logowania i raportowania musi być szyfrowana.
8. W ramach postępowania koniecznym jest dostarczenie dedykowanej aplikacji lub platformy centralnego zarządzania, logowania, raportowania.

Wymagania dotyczące systemu centralnego zarządzania, logowania, raportowania:

1. Musi zapewniać możliwość zarządzania elementami systemu jednocześnie przez wielu administratorów.
2. Musi zapewniać zarządzanie w oparciu o role przypisywane dla poszczególnych administratorów.
3. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie online
4. Musi umożliwiać edytowanie polityk bezpieczeństwa w trybie offline i aktualizację konfiguracji według zdefiniowanego harmonogramu.
5. Musi zapewniać możliwość przygotowania i edytowania konfiguracji nieaktywnego urządzenia.
6. Możliwość rozbudowy (np. w oparciu o licencję) o funkcję porównywania różnych wersji konfiguracji. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
7. Możliwość rozbudowy (np. w oparciu o licencję) o graficzną konsolę do zarządzania połączeniami VPN. W ramach postępowania muszą zostać dostarczone wszelkie niezbędne komponenty, na których można zastosować licencję w późniejszym czasie.
8. System musi umożliwiać zarządzanie bezprzewodowymi punktami dostępowymi.
9. Rozwiązanie ma umożliwiać wysyłanie alarmów przez SNMP lub e-mail.
10. System musi umożliwiać zbieranie i przechowywanie logów oraz generowanie raportów.
11. Rozwiązanie musi zapewniać narzędzie graficznej analizy logów.
12. Umożliwia przeglądanie logów ruchu w czasie rzeczywistym.
13. Rozwiązanie musi udostępniać narzędzie analizy całości ruchu.
14. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa.
15. Rozwiązanie musi posiadać zestaw predefiniowanych typów raportów.
16. Predefiniowane raporty muszą mieć możliwość dopasowania do instytucji użytkującej rozwiązanie.

17. System ma mieć możliwość generowania raportów w formacie PDF, oraz opcję eksportowania szczegółowych informacji do pliku CSV.
18. System ma być w stanie zautomatyzować generowanie raportów i mieć możliwość wysyłania ich pocztą e-mail.
19. Musi być zapewniona możliwość tworzenia raportu podsumowującego informacje zbiorcze na najwyższym poziomie szczegółowości.
20. System musi być wyposażony w konsolę umożliwiającą dostęp do szczegółowych raportów.
21. System musi mieć możliwość grupowania urządzeń, w celu tworzenia raportów i analiz zbiorczych.
22. Wymaga się, aby rozwiązanie umożliwiło kontrolę dostępu opartą na rolach, ograniczającą możliwość przeglądania raportów i urządzeń poszczególnym użytkownikom.
23. Rozwiązanie nie może narzucać ograniczeń, co do czasu przechowywania logów.

Licencje i wsparcie techniczne

1. W ramach postępowania muszą zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych i serwisów. Muszą one obejmować:
   - Ochrona przed atakami (IPS), Kontrola aplikacji, Web Filtering, Antyspam, Antywirus, Bazy reputacyjne adresów, Rozpoznawanie urządzeń pracujących w sieci, Ochrona przed nieznanymi zagrożeniami, Ochrona przed phishingiem, – na okres 3 lat.
2. System musi być objęty serwisem gwarancyjnym producenta przez okres 3 lat, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7 (świadczone telefonicznie lub poprzez portal).

IV. Termin wykonania zamówienia.

Zamawiający wymaga wykonania zamówienia (dostawy) w terminie maksymalnie 10 dni kalendarzowych od daty podpisania umowy.

V. Warunki udziału w postępowaniu.

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) nie podlegają wykluczeniu;
   2) spełniają warunki udziału w postępowaniu dotyczące:
      a) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów.
      b) sytuacji ekonomicznej lub finansowej

c) zdolności technicznej lub zawodowej.

2. Zamawiający może, na każdym etapie postępowania, uznać, że wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych wykonawcy w inne przedsięwzięcia gospodarcze wykonawcy może mieć negatywny wpływ na realizację zamówienia.
3. Spełnianie warunków poprzez poleganie na potencjale „innych podmiotów".
   1) Wykonawcy, w celu potwierdzenia spełniania warunków udziału w postępowaniu, mogą polegać na zdolnościach technicznych lub zawodowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
   2) W odniesieniu do warunków dotyczących doświadczenia, kwalifikacji zawodowych i wykształcenia osób, Wykonawcy mogą polegać na zdolnościach innych podmiotów, jeśli podmioty te zrealizują usługi, do których te zdolności są wymagane.
   3) Jeżeli zdolności techniczne lub zawodowe podmiotu, na potencjale którego Wykonawca polega, nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu, lub zachodzą wobec tych podmiotów podstawy wykluczenia, o których mowa w art. 24 ust.1 pkt. 13-22 i ust. 5 pkt.1 ustawy Pzp. Zmawiający żąda, aby Wykonawca w terminie określonym przez Zamawiającego:
   - zastąpił ten podmiot innym podmiotem lub podmiotami
   Lub
   - zobowiązał się do osobistego wykonania odpowiedniej części zamówienia, jeżeli wykaże zdolności techniczne lub zawodowe.

4. Spełnianie warunków udziału przez konsorcjum.

1) w przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum) warunki określone w pkt.V.1, 2 lit.b, c SIWZ mogą zostać spełnione przez jednego Wykonawcę lub łącznie wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

Va. Podstawy wykluczenia, o których mowa w art. 24 ust. 5 ustawy PZP.

Dodatkowo Zamawiający przewiduje wykluczenie wykonawcy:

1) w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15 maja 2015 r. – Prawo restrukturyzacyjne (Dz. U. z 2015 r. poz. 978, 1259, 1513, 1830 i 1844 oraz z 2016 r. poz. 615) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego

majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (Dz. U. z 2015 r. poz. 233, 978, 1166, 1259 i 1844 oraz z 2016 r. poz. 615);

2) który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych;

3) jeżeli wykonawca lub osoby, o których mowa w ust. 1 pkt 14, uprawnione do reprezentowania wykonawcy pozostają w relacjach określonych w art. 17 ust. 1 pkt 2–4 z:
   a) zamawiającym,
   b) osobami uprawnionymi do reprezentowania zamawiającego,
   c) członkami komisji przetargowej,
   d) osobami, które złożyły oświadczenie, o którym mowa w art. 17 ust. 2a
   – chyba że jest możliwe zapewnienie bezstronności po stronie zamawiającego w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu;
4) który, z przyczyn leżących po jego stronie, nie wykonał albo nienależycie wykonał w istotnym stopniu wcześniejszą umowę w sprawie zamówienia publicznego lub umowę koncesji, zawartą z zamawiającym, o którym mowa w art. 3 ust. 1 pkt 1–4, co doprowadziło do rozwiązania umowy lub zasądzenia odszkodowania;
5) będącego osobą fizyczną, którego prawomocnie skazano za wykroczenie przeciwko prawom pracownika lub wykroczenie przeciwko środowisku, jeżeli za jego popełnienie wymierzono karę aresztu, ograniczenia wolności lub karę grzywny nie niższą niż 3000 złotych;
6) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za wykroczenie, o którym mowa w pkt 5;
7) wobec którego wydano ostateczną decyzję administracyjną o naruszeniu obowiązków wynikających z przepisów prawa pracy, prawa ochrony środowiska lub przepisów o zabezpieczeniu społecznym, jeżeli wymierzono tą decyzją karę pieniężną nie niższą niż 3000 złotych;
8) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych, z wyjątkiem przypadku, o którym mowa w ust. 1 pkt 15, chyba że wykonawca dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności.

Fundusze Europejskie Polska Cyfrowa

Unia Europejska Europejski Fundusz Rozwoju Regionalnego

VI. Wykaz oświadczeń lub dokumentów, potwierdzających spełnianie warunków udziału w postępowaniu oraz brak podstaw wykluczenia.

1. Do oferty każdy wykonawca musi dołączyć aktualne na dzień składania ofert oświadczenie w zakresie wskazanym w załączniku **nr 2** do SIWZ Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. W przypadku złożenia oferty w postaci elektronicznej, podpisane kwalifikowanym podpisem elektronicznym.
2. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców oświadczenie o którym mowa w rozdz. VI. 1 niniejszej SIWZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Oświadczenie te ma potwierdzać spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu, brak podstaw wykluczenia.
3. Zamawiający żąda aby wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom w celu wykazania braku istnienia wobec nich podstaw wykluczenia z udziału w postępowaniu zamieszcza informacje o podwykonawcach w oświadczeniu, o którym mowa w rozdz. VI.1 niniejszej SIWZ.
4. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełnienia - w zakresie, w jakim powołuje się na ich zasoby - warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniu, o którym mowa w rozdz. VI.1 niniejszej SIWZ.
5. Zamawiający przed udzieleniem zamówienia, wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:
    a) W celu wykazania braku podstaw do wykluczenia Wykonawcy z postępowania o udzielenie zamówienia w okolicznościach, o których mowa w art. 24 ust. 5 pkt. 1 ustawy Pzp, Zamawiający żąda następujących dokumentów:
    - odpisu z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw do wykluczenia w oparciu o art. 24 ust. 5 pkt. 1 ustawy,

    UWAGA: **W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia- dokument składa każdy z Wykonawców występujących wspólnie.**

    Stosuje się art. 26 ust.6 ustawy Pzp.
6. Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP, przekaże zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia

konkurencji w postępowaniu o udzielenie Zamówienia – za pomocą poczty elektronicznej lub poprzez zakładkę :Korespondencja" na Platformie Zakupowej Zamawiającego.

7. W zakresie nie uregulowanym SIWZ, zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126)
8. Jeżeli wykonawca nie złoży oświadczenia, o którym mowa w rozdz. VI. 1. niniejszej SIWZ, oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 ustawy PZP, lub innych dokumentów niezbędnych do przeprowadzenia postępowania, oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez zamawiającego wątpliwości, zamawiający wezwie do ich złożenia, uzupełnienia poprawienia w terminie przez siebie wskazanym, chyba, że mimo ich złożenia oferta wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.

VII. Informacje o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami.

1. Wszelkie zawiadomienia, oświadczenia, wnioski oraz informacje Zamawiający oraz Wykonawcy mogą przekazywać mailem lub w poprzez Platformą, za wyjątkiem oferty, która musi być złożona za pośrednictwem Platformy, opatrzona kwalifikowanym podpisem elektronicznym lub w formie pisemnej. Zamawiający przypomina, że zgodnie z §14 ust. 4 Rozporządzenia Ministra Rozwoju z 26 lipca 2016 roku w sprawie rodzajów dokumentów jakich może żądać zamawiający (…) oświadczenia i dokumenty wymienione w rozdziale VI niniejszej SIWZ (również w przypadku ich złożenia w wyniku wezwania o którym mowa w art. 26 ust. 3 ustawy PZP) mogą być poświadczane za zgodność z oryginałem w formie pisemnej lub w formie elektronicznej.
2. W korespondencji kierowanej do Zamawiającego Wykonawca winien posługiwać się numerem sprawy określonym w SIWZ.
3. Zawiadomienia, oświadczenia, wnioski oraz informacje przekazywane przez Wykonawcę drogą elektroniczną winny być kierowane na adres: kzp@piap.lukasiewicz.gov.pl lub za pośrednictwem Platformy.
4. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ za pomocą Platformy , zakładce „Zadaj pytanie" lub mailem na adres kzp@piap.lukasiewicz.gov.pl
5. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później niż do końca dnia, w którym upływa połowa terminu składania ofert, Zamawiający udzieli wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynie po upływie terminu, o

którym mowa powyżej, lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Zamawiający zamieści wyjaśnienia na stronie internetowej, na której udostępniono SIWZ oraz na Platformie Zakupowej.

6. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w rozdz. VII. 7 niniejszej SIWZ.
7. W przypadku rozbieżności pomiędzy treścią niniejszej SIWZ, a treścią udzielonych odpowiedzi, jako obowiązującą należy przyjąć treść pisma zawierającego późniejsze oświadczenie Zamawiającego.
8. Zamawiający nie przewiduje zwołania zebrania Wykonawców.
9. Osobą uprawnioną przez Zamawiającego do porozumiewania się z Wykonawcami jest:
10. **w kwestiach formalnych: Joanna Gorzelniak- Owsiak,** joanna.gorzelniak-owsiak@piap.lukasiewicz.gov.pl; kzp@piap.lukasiewicz.gov.pl

w kwestiach merytorycznych: Marian Wrzesień
marian.wrzesien@piap.lukasiewicz.gov.pl, kzp@piap.lukasiewicz.gov.pl
Jednocześnie Zamawiający informuje, że przepisy ustawy PZP nie pozwalają na jakikolwiek inny kontakt - zarówno z Zamawiającym jak i osobami uprawnionymi do porozumiewania się z Wykonawcami - niż wskazany w niniejszym rozdziale SIWZ. Oznacza to, że Zamawiający nie będzie reagował na inne formy kontaktowania się z nim, w szczególności na kontakt telefoniczny lub/i osobisty w swojej siedzibie.

11. Ogólne zasady korzystania z Platformy:

- zgłoszenie do postępowania wymaga zalogowania Wykonawcy do Systemu na subdomenie Sieć Badawcza Łukasiewicz – Przemysłowy Instytut Automatyki i Pomiarów PIAP; **https://piap.ezamawiajacy.pl/servlet/HomeServlet** lub https://oneplace.marketplanet.pl
- Wykonawca po wybraniu opcji „przystąp do postępowania" zostanie przekierowany do strony https://oneplace.marketplanet.pl, gdzie zostanie powiadomiony o możliwości zalogowania lub do założenia bezpłatnego konta. Wykonawca zakłada konto wykonując kroki procesu rejestracyjnego; podaje adres e-mail, ustanawia hasło, następnie powtarza hasło, wpisuje kod z obrazka, akceptuje regulamin, klika polecenie „zarejestruj się".
- Rejestracja Wykonawcy trwa maksymalnie do 2 dni roboczych. W związku z tym Zamawiający zaleca Wykonawcom uwzględnienie czasu niezbędnego na rejestrację w procesie złożenia Oferty w postaci elektronicznej. Wykonawca wraz z potwierdzeniem złożenia wniosku rejestracyjnego otrzyma informacje, o możliwości przyspieszenia procedury założenia konta, wówczas należy skontaktować się pod numerem telefonu podanym w ww. potwierdzeniu.
- Po założeniu konta Wykonawca ma możliwość złożenia Oferty w postępowaniu. Komunikacja między Zamawiającym a Wykonawcami, w szczególności zawiadomienia oraz informacje, przekazywane są w formie elektronicznej za pośrednictwem Platformy Zakupowej. Za datę przekazania zaświadczeń oraz informacji przyjmuje się datę ich wysłania za pośrednictwem zakładki „Korespondencja".

12. Zamawiający informuje, iż w przypadku jakichkolwiek wątpliwości związanych z

zasadami korzystania z Platformy, Wykonawca winien skontaktować się z dostawcą rozwiązania teleinformatycznego Platformy Zakupowej **https://piap.ezamawiajacy.pl/servlet/HomeServlet** tel. +48 22 25 72 223 (infolinia dostępna w dni robocze, w godzinach 9.00-17.00) e-mail: oneplace@marketplanet.pl

13. Zamawiający zgodnie z § 4 Rozporządzenia Prezesa Rady Ministrów w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępnienia i przechowywania dokumentów elektronicznych (Dz. U. z 2017 r. poz. 1320) - zwane dalej „Rozporządzeniem" określa dopuszczalny format kwalifikowanego podpisu elektronicznego, jako:
    - dokumenty w formacie „pdf" zaleca się podpisywać formatem PAdES,
    - dopuszcza się podpisanie dokumentów w formacie innym niż „pdf", wtedy będzie wymagany oddzielny plik z podpisem. W związku z tym Wykonawca będzie zobowiązany załączyć prócz podpisanego dokumentu oddzielny plik z podpisem.
14. Zamawiający, zgodnie z § 3 ust. 3 ww. Rozporządzenia określa niezbędne wymagania sprzętowo- aplikacyjne umożliwiające pracę na Platformie Zakupowej tj.:
    - Stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s;
    - Komputer klasy PC lub MAC, o następującej konfiguracji: pamięć min 2GB Ram, procesor Intel IV 2GHZ, jeden z systemów operacyjnych - MS Windows 7 , Mac Os x 10.4, Linux, lub ich nowsze wersje;
    - Zainstalowana dowolna przeglądarka internetowa obsługująca TLS 1.2, najlepiej w najnowszej wersji w przypadku Internet Explorer minimalnie wersja 10.0;
    - Włączona obsługa JavaScript;
    - Zainstalowany program Acrobat Reader lub inny obsługujący pliki w formacie .pdf**.**
15. Zamawiający określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające prawidłowe złożenie kwalifikowanego podpisu elektronicznego:
    - Rekomendowaną przeglądarką do złożenia oferty jest MS Internet Explorer lub Firefox w wersji wpieranej przez producenta.
    - Uruchomienie oprogramowania do składania podpisu wymaga również zainstalowania Java w wersji 1.8.0_65 lub nowszej, koniecznie w wersji 32-bitowej, pozwalające na przyjmowanie przez użytkownika sesyjnych plików cookie oraz obsługującej szyfrowanie. Konieczne jest również dodanie adresu witryny platformy eZamawiający (ezamawiający.pl) do wyjątków (exception site list) w Javie. Uwaga: wymaga to uprawnień administracyjnych na komputerze.
    - Zainstaluj dedykowany komponent Szafir SDK oraz aplikację Szafir Host, który odpowiada za obsługę funkcjonalności podpisu elektronicznego w platformie eZamawiający. Rozszerzenie Szafir SDK można pobrać tutaj. Po zainstalowaniu rozszerzenia Szafir SDK oraz aplikacji Szafir Host należy przeładować bieżącą stronę.
    - Przed uruchomieniem platformy eZamawiający, w pierwszej kolejności podłącz czytnik z kartą kryptograficzną do komputera.
16. Informacje dotyczące odpowiedniego przygotowania stanowiska znajdą Państwa na

stronie:
https://oneplace.marketplanet.pl/przygotuj-stanowisko-pc-wykonujac-ponizsze-kroki

17. Zamawiający zgodnie z § 3 ust. 3 ww. Rozporządzenia, określa dopuszczalne formaty przesyłanych danych tj. plików o wielkości do 100 MB w txt, rtf, pdf ,xps, odt, ods, odp, doc, xls, ppt, docx, xlsx, pptx, csv, jpg, jpeg, tif, tiff, geotiff, png, svg, wav, mp3, avi, mpg, mpeg, mp4, m4a, mpeg4, ogg, ogv, zip, tar, gz, gzip, 7z, html, xhtml, css, xml, xsd, gml, rng, xsl, xslt, TSL, XMLsig, XAdES, CAdES, ASIC, XMLenc
18. Zamawiający zgodnie z § 3 ust. 3 ww. Rozporządzenia określa informacje na temat kodowania i czasu odbioru danych tj.:
    - Plik załączony przez Wykonawcę na Platformie Zakupowej i zapisany, widoczny jest w Systemie, jako zaszyfrowany – format kodowania UTF8. Możliwość otworzenia pliku dostępna jest dopiero po odszyfrowaniu przez Zamawiającego po upływie terminu otwarcia ofert
19. Oznaczenie czasu odbioru danych przez Platformę stanowi datę oraz dokładny czas (hh:mm:ss)
20. W przypadku wnoszenia wadium w formie poręczenia lub gwarancji:
    - W przypadku składnia Oferty w postaci elektronicznej oryginał dokumentu wadium (poręczenia lub gwarancji) opatrzonego kwalifikowanym podpisem elektronicznym osób upoważnionych do jego wystawienia, Wykonawca składa załączając na Platformie w zakładce „OFERTY" – poprzez wybranie polecenia „dodaj dokument".

VIII. Wymagania dotyczące wadium.

1. Zamawiający w niniejszym postępowaniu nie wymaga wniesienia wadium.

IX. Termin związania ofertą.

1. Wykonawca będzie związany ofertą przez okres 30 **dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert. (art. 85 ust. 5 ustawy PZP).
2. Wykonawca może przedłużyć termin związania ofertą, na czas niezbędny do zawarcia umowy, samodzielnie lub na wniosek Zamawiającego, z tym, że Zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres nie dłuższy jednak niż 60 dni.
3. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.
4. Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwie, z wniesieniem nowego wadium na przedłużony okres związania ofertą. Jeżeli przedłużenie terminu związania ofertą dokonywane jest po wyborze oferty najkorzystniejszej, obowiązek

wniesienia nowego wadium lub jego przedłużenia dotyczy jedynie Wykonawcy, którego oferta została wybrana jako najkorzystniejsza.

X. Opis sposobu przygotowywania ofert.

1. Oferta musi zawierać następujące oświadczenia i dokumenty:

   1) wypełniony **formularz ofertowy** sporządzony z wykorzystaniem wzoru stanowiącego **Załącznik nr 1** do SIWZ, zawierający w szczególności: wskazanie oferowanego przedmiotu zamówienia, łączną cenę ofertową brutto, zobowiązanie dotyczące terminu realizacji zamówienia, okresu gwarancji i warunków płatności, oświadczenie o okresie związania ofertą oraz o akceptacji wszystkich postanowień SIWZ i wzoru umowy bez zastrzeżeń, a także informację którą część zamówienia Wykonawca zamierza powierzyć podwykonawcy;
   2) oświadczenia wymienione w rozdziale VI. 1-4 niniejszej SIWZ;
2. Oferta musi być napisana w języku polskim, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką oraz podpisana przez osobę(y) upoważnioną do reprezentowania Wykonawcy na zewnątrz i zaciągania zobowiązań w wysokości odpowiadającej cenie oferty.
3. W przypadku podpisania oferty oraz poświadczenia za zgodność z oryginałem kopii dokumentów przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, należy do oferty dołączyć stosowne pełnomocnictwo w oryginale lub kopii poświadczonej notarialnie.
4. Dokumenty sporządzone w języku obcym są składane wraz z tłumaczeniem na język polski.
5. Wykonawca ma prawo złożyć tylko jedną ofertę, zawierającą jedną, jednoznacznie opisaną propozycję. Złożenie większej liczby ofert spowoduje odrzucenie wszystkich ofert złożonych przez danego Wykonawcę.
6. Treść złożonej oferty musi odpowiadać treści SIWZ.
7. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty
8. Zaleca się, aby każda zapisana strona oferty była ponumerowana kolejnymi numerami, a cała oferta wraz z załącznikami była w trwały sposób ze sobą połączona (np. zbindowaną, zszyta uniemożliwiając jej samoistną dekompletację), oraz zawierała spis treści.
9. Poprawki lub zmiany (również przy użyciu korektora) w ofercie, powinny być parafowane własnoręcznie przez osobę podpisującą ofertę.

10. Ofertę należy złożyć w zamkniętej kopercie, w siedzibie Zamawiającego i oznakować w następujący sposób:

„**Oferta - przetarg nieograniczony: ”Dostawa, konfiguracja i uruchomienie zestawu UTM”**

nie otwierać przed 19.11.2020"
NR KZP/08/2020

i opatrzyć nazwą i dokładnym adresem Wykonawcy.

lub w **przypadku składania oferty w postaci elektronicznej** - Ofertę należy złożyć na Platformie pod adresem: https://piap.ezamawiajacy.pl/servlet/HomeServlet

w zakładce „OFERTY" do dnia **19.11.2020 r. do godz. 10^{00}**

Otwarcie ofert nastąpi poprzez upublicznienie wczytanych na Platformie Ofert w dniu 19.11.2020 r. o godz. 10^{30} oraz otwarciu ofert kancelaryjnych

11. Zamawiający informuje, iż zgodnie z art. 8 w zw. z art. 96 ust. 3 ustawy PZP oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), jeśli Wykonawca w terminie składania ofert zastrzegł, że nie mogą one być udostępniane i jednocześnie wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa .
12. 1. Zamawiający zaleca, aby informacje zastrzeżone, jako tajemnica przedsiębiorstwa były przez Wykonawcę złożone w oddzielnej wewnętrznej kopercie z oznakowaniem „tajemnica przedsiębiorstwa", lub spięte (zszyte) oddzielnie od pozostałych, jawnych elementów oferty. Brak jednoznacznego wskazania, które informacje stanowią tajemnicę przedsiębiorstwa oznaczać będzie, że wszelkie oświadczenia i zaświadczenia składane w trakcie niniejszego postępowania są jawne bez zastrzeżeń.
    2. W przypadku składania oferty w postaci elektronicznej na Platformie dokumenty „stanowiące tajemnicę przedsiębiorstwa" powinny zostać załączone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Tajne". Wczytanie załącznika następuje poprzez polecenie „Dodaj"
13. Zastrzeżenie informacji, które nie stanowią tajemnicy przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji będzie traktowane, jako bezskuteczne i skutkować będzie zgodnie z uchwałą SN z 20 października 2005 (sygn. III CZP 74/05) ich odtajnieniem.
14. Zamawiający informuje, że w przypadku kiedy wykonawca otrzyma od niego wezwanie w trybie art. 90 ustawy PZP, a złożone przez niego wyjaśnienia i/lub dowody stanowić będą tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji Wykonawcy będzie przysługiwało prawo zastrzeżenia ich jako tajemnica przedsiębiorstwa. Przedmiotowe zastrzeżenie zamawiający uzna za skuteczne wyłącznie w sytuacji kiedy Wykonawca oprócz samego zastrzeżenia, jednocześnie wykaże, iż dane informacje stanowią tajemnicę przedsiębiorstwa.
15. Wykonawca może wprowadzić zmiany, poprawki, modyfikacje i uzupełnienia do złożonej oferty pod warunkiem, że Zamawiający otrzyma pisemne zawiadomienie o wprowadzeniu zmian przed terminem składania ofert. Powiadomienie o wprowadzeniu

zmian musi być złożone wg takich samych zasad, jak składana oferta tj. w kopercie odpowiednio oznakowanej napisem „ZMIANA". Koperty oznaczone „ZMIANA" zostaną otwarte przy otwieraniu oferty Wykonawcy, który wprowadził zmiany i po stwierdzeniu poprawności procedury dokonywania zmian, zostaną dołączone do oferty.
W przypadku składania oferty w postaci elektronicznej ZMIANA musi zostać dokonana poprzez Platformę zakupową

16. Wykonawca ma prawo przed upływem terminu składania ofert wycofać się z postępowania poprzez złożenie pisemnego powiadomienia, według tych samych zasad jak wprowadzanie zmian i poprawek z napisem na kopercie „WYCOFANIE". Koperty oznakowane w ten sposób będą otwierane w pierwszej kolejności po potwierdzeniu poprawności postępowania Wykonawcy oraz zgodności ze złożonymi ofertami. Koperty ofert wycofywanych nie będą otwierane.
W przypadku złożenia oferty elektronicznej Wykonawca może samodzielnie wycofać złożoną przez siebie ofertę. W tym celu w zakładce „OFERTY" należy zaznaczyć ofertę, a następnie wybrać polecenie „wycofaj ofertę".
17. Do przeliczenia na PLN wartości wskazanej w dokumentach złożonych na potwierdzenie spełniania warunków udziału w postępowaniu, wyrażonej w walutach innych niż PLN, Zamawiający przyjmie średni kurs publikowany przez Narodowy Bank Polski z dnia wszczęcia postępowania.
18. Oferta, której treść nie będzie odpowiadać treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy PZP zostanie odrzucona (art. 89 ust. 1 pkt 2 ustawy PZP). Wszelkie niejasności i wątpliwości dotyczące treści zapisów w SIWZ należy zatem wyjaśnić z Zamawiającym przed terminem składania ofert w trybie przewidzianym w rozdziale VII niniejszej SIWZ. Przepisy ustawy PZP nie przewidują negocjacji warunków udzielenia zamówienia, w tym zapisów projektu umowy, po terminie otwarcia ofert.

XI. Miejsce i termin składania i otwarcia ofert.

1. .1) Ofertę należy złożyć w siedzibie Zamawiającego Sieć Badawcza ŁUKASIEWICZ Przemysłowy Instytut Automatyki i Pomiarów PIAP, Al. Jerozolimskie 202, Kancelaria, 02- 486 Warszawa, do dnia: 19.11.2020., do godziny 10^{00} i zaadresować zgodnie z opisem przedstawionym w rozdziale X SIWZ.

lub

2) za pośrednictwem Platformy w następujący sposób:

1. wypełnienie Formularza Oferty (informacje zawarte w SIWZ),
2. dodanie w zakładce „OFERTY" dokumentów (załączników) określonych w niniejszej SIWZ, - podpisanych kwalifikowanym podpisem elektronicznym przez osoby umocowane. Czynności realizowane są poprzez wybranie polecenia „dodaj dokument" i wybranie docelowego pliku, który ma zostać wczytany.

3. Wykonawca winien opisać załącznik nazwą umożliwiającą jego identyfikację.
4. Wykonawca załączając dokument oznacza czy jest on: „Tajny" – dokument stanowi „tajemnice przedsiębiorstwa" lub opcję „Jawny" – niestanowiący tajemnicy przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 roku o zwalczaniu nieuczciwej konkurencji.
5. Złożenie oferty wraz z załącznikami następuje poprzez polecenie „Złóż ofertę".
6. Potwierdzeniem prawidłowo złożonej Oferty jest komunikat systemowy „Oferta złożona poprawie" oraz wygenerowany raport ofert z zakładki „Oferty"
7. O terminie złożenia Oferty decyduje czas pełnego przeprocesowania transakcji na Platformie.
8. Po zapisaniu, plik jest w Systemie zaszyfrowany. Jeśli Wykonawca zamieścił niewłaściwy plik, może go usunąć zaznaczając plik i klikając polecenie „usuń".

Wykonawca składa ofertę w formie zaszyfrowanej, dlatego też Oferty nie są widoczne do momentu odszyfrowania ich przez Zamawiając

2. Decydujące znaczenie dla oceny zachowania terminu składania ofert w postaci tradycyjnej ma data i godzina wpływu oferty do Zamawiającego, a nie data jej wysłania przesyłką pocztową czy kurierską. W przypadku ofert składanych poprzez Platformę Zakupową decyduje określenie czasu na Platformie - oznaczenie czasu odbioru danych przez Platformę stanowi datę oraz dokładny czas (hh:mm:ss)
3. Oferta złożona po terminie wskazanym w rozdz. XI. 1 niniejszej SIWZ zostanie zwrócona wykonawcy zgodnie z zasadami określonymi w art. 84 ust. 2 ustawy PZP.
4. Otwarcie ofert nastąpi w siedzibie Zamawiającego – bud. 3, pok. 8 , w dniu 15.09.2020., o godzinie 10^{30}.
5. Otwarcie ofert jest jawne.
6. Podczas otwarcia ofert Zamawiający odczyta informacje, o których mowa w art. 86 ust. 4 ustawy PZP.
7. Niezwłocznie po otwarciu ofert zamawiający zamieści na stronie www.piap.pl oraz na Platformie w zakładce „Dokumenty Zamówienia" w Folderze „Informacja z otwarcia ofert" Zamawiający przekaże dane określone w art. 86 ust.5 Ustawy Pzp.

XII. Opis sposobu obliczania ceny.

1. Wykonawca określa cenę realizacji zamówienia poprzez wskazanie w Formularzu ofertowym sporządzonym wg wzoru stanowiącego **Załączniki nr 1** do SIWZ łącznej ceny ofertowej brutto za realizację przedmiotu zamówienia w podziale na zadania, o których mowa w rozdziale III niniejszej SIWZ.
2. Łączna cena ofertowa brutto musi uwzględniać wszystkie koszty związane z realizacją przedmiotu zamówienia zgodnie z opisem przedmiotu zamówienia oraz wzorem umowy określonym w niniejszej SIWZ.

3. Zamawiający nie przewiduje możliwości zmian ceny ofertowej brutto
4. Ceny muszą być: podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
5. Cena oferty winna być wyrażona w złotych polskich (PLN).
6. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. W takim przypadku Wykonawca, składając ofertę, jest zobligowany poinformować zamawiającego, że wybór jego oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru , których dostawa będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

XIII. Opis kryteriów, którymi zamawiający będzie się kierował przy wyborze oferty, wraz z podaniem wag tych kryteriów i sposobu oceny ofert.

1.

a. Kryteria oceny i ich ranga w ocenie

Lp.	Kryterium	Ranga
	Cena	100 %
	RAZEM	100 %

b. Sposób obliczania wartości punktowej

Wartość punktowa poszczególnych kryteriów będzie wyliczana na podstawie następujących wzorów (po dokonaniu obliczeń zgodnie z pkt. a) :
Kryterium – K1 = 100 * najniższa z oferowanych cen/cena z ocenianej oferty.

c. Zasady wyboru oferty i udzielenia zamówienia:

- Zamawiający udzieli zamówienia Wykonawcy, którego oferta odpowiada wszystkim wymaganiom Ustawy z dnia 29.01.2004 r. Prawo zamówień publicznych, spełnia wszystkie wymagania określone w SIWZ oraz została uznana za najkorzystniejszą w oparciu o podane kryteria oceny.
- Za najkorzystniejszą zostanie uznana oferta z najniższą ceną brutto, odpowiadająca wszystkim warunkom przedstawionym w niniejszej specyfikacji.
- W przypadku oferty wykonawcy zagranicznego, w celu porównania ofert zamawiający do ceny oferty doliczy wartość podatku od towarów i usług VAT oraz wartość opłat celnych jaką będzie zobowiązany zapłacić w przypadku wyboru tej oferty.
- Jeżeli nie będzie można dokonać wyboru oferty najkorzystniejszej ze względu na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i pozostałych kryteriów oceny ofert, Zamawiający spośród tych ofert dokona wyboru oferty z niższą ceną (art. 91 ust. 4 ustawy PZP).

Zamawiający nie przewiduje przeprowadzenia dogrywki w formie aukcji elektronicznej.

XIV. Informacje o formalnościach, jakie powinny być dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego.

1. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać ze sobą dokumenty potwierdzające ich umocowanie do podpisania umowy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.
2. W przypadku wyboru oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia Zamawiający może żądać przed zawarciem umowy przedstawienia umowy regulującej współpracę tych Wykonawców. Umowa taka winna określać strony umowy, cel działania, sposób współdziałania, zakres prac przewidzianych do wykonania każdemu z nich, solidarną odpowiedzialność za wykonanie zamówienia, oznaczenie czasu trwania konsorcjum (obejmującego okres realizacji przedmiotu zamówienia, gwarancji i rękojmi), wykluczenie możliwości wypowiedzenia umowy konsorcjum przez któregokolwiek z jego członków do czasu wykonania zamówienia.
3. Zawarcie umowy nastąpi wg wzoru Zamawiającego.
4. Postanowienia ustalone we wzorze umowy nie podlegają negocjacjom.

XV. Wymagania dotyczące zabezpieczenia należytego wykonania umowy.

Zamawiający w niniejszym postępowaniu nie będzie żądał wniesienia zabezpieczenia należytego wykonania umowy.

XVI. Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego, ogólne warunki umowy albo wzór umowy, jeżeli Zamawiający wymaga od Wykonawcy, aby zawarł z nim umowę w sprawie zamówienia publicznego na takich warunkach.

Wzór umowy, stanowi **Załącznik 2** do SIWZ.

XVII. Pouczenie o środkach ochrony prawnej.

1. Każdemu Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP przysługują środki ochrony prawnej przewidziane w dziale VI ustawy PZP jak dla postępowań poniżej kwoty

określonej w przepisach wykonawczych wydanych na podstawie art. 11 ust. 8 ustawy PZP.

2. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz SIWZ przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 pkt 5 ustawy PZP.

Zamawiający oczekuje, że Wykonawcy zapoznają się dokładnie z treścią niniejszej SIWZ. Wykonawca ponosi ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów, oraz przedłożenia oferty nie odpowiadającej wymaganiom określonym przez Zamawiającego

Załączniki do SIWZ:

1. Formularz ofertowy wraz z załącznikami (oświadczenia)
2. Wzór umowy
3. Klauzula informacyjna RODO

Z A T W I E R D Z A M

Kierownik Zamawiającego lub osoba upoważniona

Klauzula informacyjna z art. 13 RODO

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest Sieć Badawcza Łukasiewicz - Przemysłowy Instytut Automatyki i Pomiarów PIAP, Al. Jerozolimskie 202, 02 – 486 Warszawa;
- inspektorem ochrony danych osobowych w Sieć Badawcza Łukasiewicz - Przemysłowym Instytucie Automatyki i Pomiarów PIAP jest Pan Maciej Wara-Wąsowski, tel. 796 239 428, email: mwarawasowski@odomg.pl;
- Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego KZP/08/2020 prowadzonym w trybie przetargu nieograniczonego;
- odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";
- Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
- obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- posiada Pani/Pan:

- na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
- na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych **;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO ***;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

- nie przysługuje Pani/Panu:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.