

BST-P6/076/20/2023

Z A P Y T A N I E O I N F O R M A C J Ę

Zwracamy się do Państwa z prośbą o udzielenie informacji cenowej dotyczącej dostawy, instalacji i konfiguracji punktów dostępowych APN wraz z systemem zarządzania. Dodatkowo Zamawiający wymaga zapewnienia szkoleń z zakresu administrowania oferowanym sprzętem dla 6 administratorów Zamawiającego.

1. Szczegółowy opis przedmiotu zapytania:
 - Dostawa punktów dostępowych APN wraz z systemem zarządzania,
 - Miejsce dostawy i instalacji Urządzeń we wskazanych lokalizacjach na terenie całej Polski, zgodnie ze wskazaniem zamawiającego,
 - Wykonanie prac instalacyjno-wdrożeniowych zgodnie z wcześniej zaakceptowanym przez Zamawiającego harmonogramem,
 - Wykonanie powykonawczej dokumentacji technicznej uwzględniającej stan infrastruktury Zamawiającego w obszarze wykonywanych prac,
 - Szkolenia – Wykonawca zapewni autoryzowane szkolenia dotyczące wdrażanego rozwiązania dla minimum 6 pracowników Zamawiającego. Szkolenia muszą być zapewnione w autoryzowanym ośrodku na terenie Warszawy.

Specyfikacja**A. Ogólne wymagania dla sieci bezprzewodowej.**

1. Przedmiotem zamówienia jest rozbudowa posiadanej przez Zamawiającego sieci bezprzewodowej o nowe punkty dostępowe, poprzez dostawę urządzeń, niezbędnych licencji i oprogramowania, oraz ich instalację w miejscach i liczbie wskazanych przez Zamawiającego,
2. Zamawiający wymaga, żeby dostarczone punkty dostępowe były w pełni zarządzane z chmury producenta, ale również, aby umożliwiały adopcję i zarządzanie z lokalnego kontrolera,
3. Wykonawca zobligowany jest dostarczyć wszystkie komponenty, licencje niezbędne do poprawnego funkcjonowania rozwiązania,
4. Dostarczone przez Wykonawcę urządzenia muszą pochodzić z oficjalnego kanału dystrybucji producenta i posiadać pakiet usług gwarancyjnych producenta obejmujący użytkowników z obszaru Polski,
5. Zamawiający dopuszcza licencje czasowe w formie subskrypcji, ale na okres nie krótszy niż 5 lat,
6. Sieć bezprzewodowa, musi zapewnić skalowalność, czyli możliwość rozbudowy do minimum 2000 punktów dostępowych,
7. Sieć bezprzewodowa musi funkcjonować w oparciu o standard transmisji bezprzewodowej WLAN 802.11ax (WiFi 6), a także zapewniać kompatybilność z wcześniejszymi standardami 802.11/ac/n a/b/g,
8. W celu zapewnienia usługi bezpiecznego dostępu gościnnego musi być możliwość generowania wielu prywatnych haseł PSK w ramach jednego SSID. System musi zapewniać rozróżnienie poszczególnych użytkowników posiadających prywatne hasła PSK i zapewniać egzekwowanie różnych polityk Firewall oraz przydział do różnych sieci VLAN. Dopuszczane jest

- zapropowanie analogicznego rozwiązania usługi bezpiecznego dostępu gościnnego zapewniającego minimum:
- a. szyfrowanie WPA2/AES,
 - b. osobne konta czasowe dla gości.
9. System chmurowy musi posiadać możliwość dostarczenia wygenerowanych danych dostępu gościnnego poprzez email oraz SMS. Wymaga się, aby funkcjonalność ta była wbudowana w rozwiązanie chmurowe bez konieczności integracji z własną bramką internetową lub innym publicznym systemem wysyłania SMS,
10. Ze względu na rozproszoną infrastrukturę sieci, rozwiązanie sieci bezprzewodowej musi działać z pełną funkcjonalnością w przypadku utraty łączności z centralnym systemem zarządzania w chmurze lub lokalnym kontrolerem,
11. Funkcję warstwy kontrolnej sieci bezprzewodowej muszą pełnić punkty dostępowe. W szczególności dotyczy to funkcjonalności takich jak:
- a. automatyczny dobór mocy nadawania RF,
 - b. automatyczny dobór kanału,
 - c. Fast Secure Roaming,
 - d. Pełna obsługa SSID z 802.1x,
 - e. Captive Web Portal.
12. System powinien oferować zestaw narzędzi dla administratorów ułatwiających rozwiązywanie problemów klientów sieci WiFi w szczególności:
- a. monitoring komunikacji klienta podczas podłączania się do sieci,
 - b. możliwość uruchomienia trybu śledzenia konkretnego urządzenia w celu analizy problemów z łącznością,
 - c. automatyczne wykrywanie problemów z połączeniem do sieci WiFi,
 - d. ocenę możliwości klienta sieci bezprzewodowej odnośnie do wspieranych kanałów, szerokości kanałów, MIMO itp.
13. Wszystkie komponenty rozwiązania powinny pochodzić od jednego producenta. W celu odbioru i weryfikacji pokrycia sieci wifi, po uruchomieniu systemu Wykonawca musi przeprowadzić pomiary pokrycia i siły sygnału radiowego dla wszystkich budynków, w których dokonana zostanie instalacja punktów dostępowych i dołączyć je do dokumentacji.
14. Wykonawca zobowiązany jest do sporządzenia dokumentacji powdrożeniowej rozwiązania, która obejmie co najmniej:
- a. rozmieszczenie punktów dostępowych,
 - b. pomiar siły sygnału punktów dostępowych i przedstawienie go na mapach budynku,
 - c. przebieg, oznaczenie i pomiary wykonanych tras kablowych naniesione na podkłady budynku,
 - d. opis konfiguracji punktów dostępowych.
15. Wszystkie punkty dostępowe muszą być objęte gwarancją i wsparciem producenta na okres min. 5 lat,
16. Wymiana uszkodzonego urządzenia powinna nastąpić w przeciągu 10 dni roboczych od momentu potwierdzenia przez producent uszkodzenia sprzętowego.

B. Wymagania dla chmurowego systemu zarządzania

1. W celu zapewnienia protekcji inwestycji, system zarządzania w chmurze powinien umożliwiać adopcję i prawidłowe zarządzanie urządzeniami, zarówno najnowszymi jak i starszymi.

Zamawiający chce uniknąć w przyszłości potrzeby wymiany urządzeń w przypadku chęci rozbudowy systemu o nowe punkty dostępowe, które będą miały nowe funkcje oraz nowe wersje oprogramowania (ang. firmware),

2. Musi zapewnić możliwość wgrywania różnych wersji oprogramowania na punkty dostępowe w ramach systemu,
3. Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń,
4. Musi umożliwić określenie fizycznej lokalizacji punktów dostępowych na mapie oraz miejsca ich podłączenia do sieci,
5. Musi umożliwić monitorowanie całego systemu sieci bezprzewodowej,
6. Musi zapewnić kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieci bezprzewodowej,
7. Musi zapewnić wdrożenie scentralizowanych polityk WLAN, które można zastosować do wielu punktów dostępowych jednocześnie,
8. Musi zapewnić centralne wykonanie aktualizacji oprogramowania dla wszystkich urządzeń w systemie,
9. Musi zapewnić możliwość zaplanowania wykonania aktualizacji urządzeń w systemie,
10. Musi umożliwiać wizualizację zainstalowanych punktów dostępowych na mapach oraz planach pięter budynków. Wizualizacja musi pokazywać topologię sieciową oraz aktualny stan działania zainstalowanych punktów dostępowych,
11. Mapy pięter budynków muszą mieć, oprócz prezentacji samego rzutu piętra, możliwość obrysowania ścian i przeszkód dla sygnału radiowego, tak aby była możliwa możliwie wierna wizualizacja propagacji sygnału radiowego,
12. Musi umożliwiać wyświetlanie na planach pięter umiejscowienia wykrytych klientów,
13. Musi posiadać narzędzie do planowania radiowego w celu ustalenia miejsc montażu nowych punktów dostępowych. Planowanie musi opierać się o plany pięter budynków,
14. Musi posiadać możliwość wykonania konfiguracji dla planowanych nowych punktów dostępowych,
15. Musi zapewnić automatyczny proces rejestracji, uaktualnienia oraz konfiguracji nowych punktów dostępowych bez konieczności wykonywania działań manualnych (ang. auto provisioning),
16. System musi umożliwiać analizowanie ruchu w sieci i prezentację statystyk pod kątem używanych aplikacji oraz wolumenu danych dla każdej z aplikacji, bądź grup aplikacji,
17. Chmurowy system zarządzania musi udostępniać możliwość monitorowania, zarządzanej przez niego infrastruktury WiFi, przy użyciu dedykowanej aplikacji mobilnej, wyprodukowanej i przez producenta. Aplikacja powinna być możliwa do instalacji na urządzeniu mobilnym takim jak smartphone lub tablet z systemem operacyjnymi Apple iOS, Apple iPadOS, Android. Aplikacja mobilna musi być dostępna publicznie i za darmo na platformach Apple AppStore oraz GooglePlay,
18. Ze względu na chmurowy charakter przetwarzania danych, system zarządzania chmurowego musi posiadać certyfikat zgodności z ISO 27001, ISO 27017 oraz ISO 27701
19. System zarządzania musi być zgodny z RODO,
20. System musi umożliwiać uruchomienie podstawowej funkcjonalności WIPS (ang. Wireless Intrusion Prevention System) w zakresie:
 - a. wykrywania i usuwania wrogich punktów dostępowych (ang. rogue AP detection and termination),

- b. wykrywania wrogich klientów (ang. Rogue Client Detection),
 - c. wykrywania ataków w ilości minimum 30 różnych sygnatur ataku.
21. System musi posiadać następujące możliwości raportowania:
- a. modyfikacja, filtrowanie i tworzenie różnych zakresów urządzeń objętych raportem,
 - b. tworzenie raportów jednorazowych lub automatycznie zgodnie z zadaniem harmonogramem, w formie pdf, z opcją wysyłania ich pod wskazany adres email,
 - c. raportowanie ilości danych w ramach każdej wykrytej aplikacji,
 - d. raportowanie ilości zużytego pasma per użytkownik,
 - e. dane dla potrzeb audytów,
 - f. generowanie wykazu produktów zainstalowanych w sieci.
22. System zarządzania w chmurze musi zapewniać dostęp do API pozwalający na integrację systemu bezprzewodowego rozwiązaniami firm trzecich,
23. API musi zapewniać możliwość generowania prywatnych haseł PSK tak, aby była możliwość integracji systemu rejestracji gości na recepcji z systemem obsługi gości w ramach sieci WiFi,

C. Minimalne wymagania techniczne dla wewnętrznego punktu dostępowego sieci bezprzewodowej WiFi6.

1. Punkty dostępowe muszą pozwalać na zarządzanie z chmurowego systemu zarządzania producenta opisanego wcześniej, jak również pozwalać na współpracę z tradycyjnym kontrolerem lokalnym. Zamawiający chce w ten sposób zabezpieczyć inwestycję, przez możliwość zmiany sposobu implementacji systemu zarządzania z chmurowego na lokalny, bez konieczności wymiany punktów dostępowych,
2. Punkty dostępowe muszą być zasilane za pomocą standardu Power over Ethernet (PoE) IEEE 802.3at,
3. Muszą obsługiwać równolegle dwa pasma częstotliwości:
 - a. 5 GHz – standardy 802.11ax (WiFi6),
 - b. 2.4 GHz – standardy 802.11ax (WiFi6).
4. Punkty dostępowe muszą mieć możliwość rejestracji w centralnym systemie zarządzania, bez konieczności wykonywania konfiguracji na punkcie dostępowym niezależnie od miejsca podłączenia punktu dostępowego do sieci. Funkcjonalność ta musi działać zarówno w przypadku:
 - a. Podłączenia w dowolnym miejscu na świecie, przy zapewnieniu punktowi dostępowemu, łączności z siecią Internet – w przypadku zarządzania z chmury,
 - b. Jeśli opcjonalnie punkt dostępowy miałby być zarządzany z lokalnego kontrolera tak jak zostało to opisane w punkcie C.1. to musi mieć możliwość adopcji i zarządzania będąc podłączonym do podsieci zarządzania Zamawiającego (komunikacja w warstwie L2 ISO OSI), oraz z dowolnej innej podsieci sieci LAN Zamawiającego (komunikacja w warstwie L3 ISO OSI).
5. Muszą posiadać wbudowane minimum 2 anteny dookólne o wzmacnieniu:
 - a. minimum 2.6 dBi dla pasma 2.4 GHz,
 - b. minimum 3.6 dBi dla pasma 5 GHz.
6. Muszą posiadać obsługę standardu 802.11ax (WiFi6), oraz co najmniej 2x2:2 MIMO,
7. Min. 1 x Port 10/100/1000 Base-T RJ-45 z technologią autosensing,
8. Obsługa min. 8 SSID na radio,
9. Zintegrowany Statefull Inspection Firewall,

10. Zintegrowana funkcjonalność wykrywania i blokowania aplikacji (L7 firewall),
11. Muszą posiadać chip TPM (Trusted Platform Module) do przechowywania kluczy, haseł oraz elektronicznych certyfikatów,
12. Punkt dostępowy musi posiadać przycisk „reset”, służący do przywracania go do ustawień fabrycznych. Po dokonaniu przywrócenia do ustawień fabrycznych, punkt dostępowy musi automatycznie podłączyć się do systemu zarządzania bez konieczności ręcznego konfigurowania go,
13. Punkt dostępowy musi zapewniać możliwość uwierzytelniania go do sieci LAN z wykorzystaniem IEEE 802.1x,
14. Punkt dostępowy musi mieć możliwość montażu na suficie,
15. Zakres temperatury pracy 0-40 °C,
16. Wymagane obsługiwane standardy sieciowe min.:
 - a. IEEE 802.11a,
 - b. IEEE 802.11b,
 - c. IEEE 802.11e,
 - d. IEEE 802.11g,
 - e. IEEE 802.11i,
 - f. szyfrowanie AES/CCMP,
 - g. IEEE 802.11k,
 - h. IEEE 802.11r,
 - i. IEEE 802.11v,
 - j. IEEE 802.11n,
 - k. IEEE 802.11ac,
 - l. IEEE 802.11ax,
 - m. IEEE 802.3af,
 - n. IEEE 802.1x,
 - o. Wi-Fi Protected Access 2 (WPA2) oraz Wi-Fi Protected Access 3 (WPA3),
 - p. wsparcie dla kanałów radiowych o szerokości 20MHz, 40MHz i 80MHz,
 - q. zgodność z DFS (Dynamic Frequency Selection),
 - r. punkt dostępowy musi obsługiwać funkcję IP QoS w środowisku przewodowym i bezprzewodowym (802.1p, diffserv i policing).

D. Minimalne wymagania techniczne dla wewnętrznego punktu dostępowego sieci bezprzewodowej WiFi6E

1. Punkty dostępowe muszą pozwalać na zarządzanie z chmurowego systemu zarządzania producenta opisanego wcześniej, jak również pozwalać na współpracę z tradycyjnym kontrolerem lokalnym. Zamawiający chce w ten sposób zabezpieczyć inwestycję, przez możliwość zmiany sposobu implementacji systemu zarządzania z chmurowego na lokalny, bez konieczności wymiany punktów dostępowych,
2. Punkty dostępowe muszą być zasilane za pomocą standardu Power over Ethernet (PoE) IEEE 802.3at,
3. Muszą obsługiwać równolegle trzy pasma częstotliwości:
 - a. 6 GHz – standardy 802.11ax (WiFi6E),
 - b. 5 GHz – standardy 802.11ax (WiFi6),
 - c. 2.4 GHz – standardy 802.11ax (WiFi6),

4. Punkty dostępowe muszą mieć możliwość rejestracji w centralnym systemie zarządzania, bez konieczności wykonywania konfiguracji na punkcie dostępowym niezależnie od miejsca podłączenia punktu dostępowego do sieci. Funkcjonalność ta musi działać zarówno w przypadku:
 - c. Podłączenia w dowolnym miejscu na świecie, przy zapewnieniu punktowi dostępowemu, łączności z siecią Internet – w przypadku zarządzania z chmury,
 - d. Jeśli opcjonalnie punkt dostępowy miałby być zarządzany z lokalnego kontrolera tak jak zostało to opisane w punkcie C.1. to musi mieć możliwość adopcji i zarządzania będąc podłączonym do podsieci zarządzania Zamawiającego (komunikacja w warstwie L2 ISO OSI), oraz z dowolnej innej podsieci sieci LAN Zamawiającego (komunikacja w warstwie L3 ISO OSI).
5. Muszą posiadać wbudowane minimum 2 anteny dookólne o wzmacnieniu:
 - a. minimum 4 dBi dla pasma 6 GHz,
 - b. minimum 4 dBi dla pasma 5 GHz,
 - c. minimum 3 dBi dla pasma 2.4GHz.
6. Muszą posiadać obsługę standardu 802.11ax (WiFi6E), oraz co najmniej 2x2:2 MIMO.
7. Muszą posiadać minimum 1 port 100/1000/2500 Base-T RJ-45, oraz 1 port 10/100/1000 Base-T RJ-45 z technologią autosensing,
8. Obsługa min. 8 SSID na radio,
9. Zintegrowany Statefull Inspection Firewall,
10. Zintegrowana funkcjonalność wykrywania i blokowania aplikacji (L7 firewall),
11. Muszą posiadać chip TPM (Trusted Platform Module) do przechowywania kluczy, haseł oraz elektronicznych certyfikatów,
12. Punkt dostępowy musi posiadać przycisk „reset”, służący do przywracania go do ustawień fabrycznych. Po dokonaniu przywrócenia do ustawień fabrycznych, punkt dostępowy musi automatycznie podłączyć się do systemu zarządzania bez konieczności ręcznego konfigurowania go,
13. Punkt dostępowy musi zapewniać możliwość uwierzytelniania go do sieci LAN z wykorzystaniem IEEE 802.1x,
14. Punkt dostępowy musi mieć możliwość montażu na suficie,
15. Dopuszczalna temperatura pracy 0-50 °C,
16. Wymagane obsługiwane standardy sieciowe min.:
 - a. IEEE 802.11a,
 - b. IEEE 802.11b,
 - c. IEEE 802.11e,
 - d. IEEE 802.11g,
 - e. IEEE 802.11i,
 - f. szyfrowanie AES/CCMP,
 - g. IEEE 802.11k,
 - h. IEEE 802.11r,
 - i. IEEE 802.11v,
 - j. IEEE 802.11n,
 - k. IEEE 802.11ac,
 - l. IEEE 802.11ax,
 - m. IEEE 802.3af,
 - n. IEEE 802.1x,

- o. IEEE 802.3az,
- p. Wi-Fi Protected Access 2 (WPA2) oraz Wi-Fi Protected Access 3 (WPA3),
- q. wsparcie dla kanałów radiowych o szerokości 20MHz, 40MHz i 80MHz,
- r. zgodność z DFS (Dynamic Frequency Selection),
- s. punkt dostępowy musi obsługiwać funkcję IP QoS w środowisku przewodowym i bezprzewodowym (802.1p, diffserv i policing).

E. Zestawienie liczbowe wymaganych urządzeń

1. Wymagane jest dostarczenie 85 punktów dostępowych opisanych w punkcie C wraz z wszystkimi niezbędnymi licencjami pozwalającymi na dołączenie i zarządzanie powyższymi punktami dostępowymi w chmurowym systemie zarządzającym przez okres min. 5 lat,
2. Wymagane jest dostarczenie 6 punktów dostępowych opisanych w punkcie D wraz z wszystkimi niezbędnymi licencjami pozwalającymi na dołączenie i zarządzanie powyższymi punktami dostępowymi w chmurowym systemie zarządzającym przez okres min. 5 lat,
3. Wymagane jest, aby chmurowy system zarządzający przechowywał wszystkie zdarzenia i statystyki przez okres min. 5 lat.

Termin i sposób składania informacji cenowych

Termin składania informacji cenowych upływa w dniu **13.09.2023 r. do godz. 16.00.**

(ewentualne pytania prosimy kierować do dnia **08.09.2023 r. do godziny 16:00**).

Odpowiedź prosimy przesłać w formie e-mail na adres: **it@intercity.pl**

Formularz odpowiedzi do zapytania:

Odpowiedź powinna zawierać:

1. Podanie czasu niezbędnego na dostawę, instalację i konfigurację przedmiotu zapytaniadni
2. Uzupełnienie szacowanych kosztów zgodnie z poniższą tabelą,

L.P.	Przedmiot zapytania	Ilość	Cena jednostkowa netto (zł)	Wartość netto (zł)
1	Urządzenie dostępowe C	85		
2	Urządzenie dostępowe D	6		
3	System zarządzania	1		
4	Wsparcie Producenta – koszt miesięczny	50 miesięcy		
5	Szkolenia – koszt za 1 osobę	6 osób		
SUMA				

„PKP INTERCITY” S.A. zastrzega, że niniejsze zapytanie nie stanowi elementu jakiegokolwiek postępowania o udzielenie zamówienia, wobec czego PKP INTERCITY S.A. nie jest zobligowane do wyboru którejkolwiek oferty. Niniejsze pismo nie stanowi również oferty w rozumieniu Kodeksu Cywilnego.