

OPIS RZEDMIOTU ZAMÓWIENIA

DOTYCZY CZĘŚCI NR 1

Dostawa skanerów samoobsługowych do czytelní

Przedmiotem zamówienia jest dostawa wraz z usługą instalacji 3 sztuk samoobsługowych skanerów dzielowych dla czytelników.

Wposażenie:

3 skanery samoobsługowe o następujących parametrach:

- Obszar skanowania umożliwiający skanowanie w pełni rozłożonych dokumentów w formacie A3+. Możliwość skanowania obiektów o grubości nie mniejszej niż 100 mm.
- Rozdzielczość optyczna minimum 300 dpi x 300 dpi na całym obszarze skanowania.
- Lampa skanera: nie może emitować promieniowania UV ani IR, musi być zintegrowana w obudowie skanera. Lampa musi włączać się jedynie w czasie skanowania oświetlając tylko skanowany fragment obiektu. Lampa musi być oddalona minimum 15 cm od skanowanego obiektu.
- Szybkość skanowania: maksymalnie 3 sekundy w rozdzielczości optycznej 300 dpi w kolorze, dla dokumentów o maksymalnym rozmiarze. Skaner musi jednocześnie skanować i zapisywać pliki.
- Głębia koloru: minimum 42-bit w kolorze, 14-bit w odcieniach szarości oraz 1-bit dla trybu czarno-białego.
- Wposażenie skanera: skaner musi być wyposażony w ruchome w pionie szalki, dostosowujące się do grubości grzbietu skanowanego dokumentu.
- Obsługa i ergonomia: skaner nie może być wyposażony w szybę dociskową ograniczającą ergonomię pracy, skanowanie musi odbywać się bez mechanicznego spłaszczania dokumentów. W celu maksymalnego uproszczenia procesu skanowania cała obsługa skanera (w tym podgląd skanów, wykonywanie korekt, zmiana obszaru skanowania, obracanie dokumentów itp.) musi odbywać się za pomocą zintegrowanego, wbudowanego w skaner komputera sterującego działającego pod kontrolą systemu Windows, wyposażonego w panel dotykowy o wielkości minimalnej 11".
- Oprogramowanie: oprogramowanie skanera musi być dostarczone w pełnej wersji (nie są dopuszczalne wersje testowe i działające przez określony okres czasu), stanowiąc integralną część skanera. Oprogramowanie musi umożliwiać obróbkę graficzną zeskanowanego dokumentu (prostowanie stron, korekta łuku książki, usuwanie odbić itp.). Oprogramowanie musi automatycznie wykrywać format dokumentu, wykonywać korektę geometrii skanu, usuwać obiekty obce w obrębie dokumentu, automatycznie ustawiać balans bieli i ostrość. Musi być możliwa zdalna diagnostyka i kalibracja skanera za pośrednictwem sieci LAN/Internetu bez konieczności podłączania dodatkowych urządzeń. Oprogramowanie musi umożliwiać zapis plików na pamięć USB, wysyłkę na e-mail, skanowanie do formatów co najmniej: jpeg, tiff i pdf. Program musi posiadać co najmniej polską i angielską wersję językową.
- Złącza: skaner musi posiadać port USB 2.0 do podłączania pamięci USB (pendrive) oraz port Gigabit Ethernet RJ45.
- Konstrukcja skanera: skaner musi posiadać zwartą konstrukcję i wymiary maksymalne 900 mm (szerokość) i 700 mm (głębokość) oraz wagę maksymalną 30 kg umożliwiającą łatwe przenoszenie go w inne miejsce oraz umożliwiającą umieszczenie go na meblach posiadanych przez zamawiającego.
- Certyfikaty: skaner musi posiadać certyfikat CE oraz spełniać normę Energy Star.

Usługi:

- Usługa instalacji (wdrożenia) skanerów.

Warunki realizacji:

- Czas realizacji zadania: do 4 tygodni od daty podpisania umowy.
- Urządzenia muszą być objęte minimum 36-miesięczną gwarancją producenta.
- Wykonawca musi być autoryzowanym przedstawicielem producenta urządzeń.

DOTYCZY CZĘŚCI NR 2

Dostawa wyświetlaczy (telewizorów) LCD 75-82"

Przedmiotem zamówienia jest dostawa 2 sztuk wyświetlaczy (telewizorów) LCD o przekątnej 75-82" z wyposażeniem

Wyposażenie:

Wyświetlacz (telewizor) 2 sztuki o następujących parametrach:

- Przekątna ekranu: minimalna 75" – maksymalna 82".
- Typ ekranu: prosty.
- Rozdzielczość ekranu: 4K UHD (3840x2160 pikseli).
- Podświetlenie matrycy: LED.
- Obsługa technologii HLG oraz HDR10/HDR10+.
- Wbudowany system dźwięku przestrzennego, minimalna moc wbudowanych głośników 2 x 10W.
- Obsługa Smart TV.
- Obsługa WiFi.
- Wbudowana przeglądarka internetowa.
- Możliwość nagrywania na pendrive USB.
- Wbudowany system Android TV ze wsparciem dla Chromecast (Googlecast).
- Minimalna liczba złączy HDMI: 3 szt.
- Minimalna liczba złączy USB: 3 szt.
- Złącze Ethernet RJ45.
- Tuner TV: DVB-T2, DVB-S2, DVB-C, analogowy.

Dodatkowe wyposażenie:

- 2 stojaki wolnostojące umożliwiające przesuwanie na kółkach o parametrach adekwatnych do oferowanych wyświetlaczy.

Warunki realizacji:

- Czas realizacji zadania: do 4 tygodni od daty podpisania umowy.
- Gwarancja na całe wyposażenie minimum 24 miesiące.

DOTYCZY CZĘŚCI NR 3

Dostawa infrastruktury sieci dla sieci WiFi 802.11ac (przełącznik, punkty dostępowe) wraz z wdrożeniem

Przedmiotem zadania jest dostawa infrastruktury dla sieci WiFi 802.11ac składającej się z przełącznika, punktów dostępowych oraz niezbędnych akcesoriów wraz z usługą wdrożenia.

Wyposażenie:

Kontroler sieci bezprzewodowej z pakietem licencji pozwalającym na obsługę 22 punktów dostępowych posiadający następujące właściwości:

- Architektura: kontroler fizyczny lub wirtualny z możliwością uruchomienia w środowisku VMware vSphere. W wypadku, w którym oprogramowanie kontrolera wirtualnego wymaga uruchomienia w maszynie wirtualnej wyposażonej w płatny system operacyjny – musi ono zostać dostarczone z licencjami na ten system.
- Wysoka dostępność: możliwość pracy w klastrze active-active z balansowaniem rozłożenia podłączonych punktów dostępowych. Awaria pojedynczego urządzenia w klastrze nie może mieć wpływu na ruch z urządzeń klienckich WiFi, ani powodować degradacji usługi WiFi (np. konieczności ponownej autentykacji i asocjacji). Kontroler musi zapewniać wysoką odporność na awarie usług dla klientów – w przypadku awarii kontrolera (nawet w trybie pojedynczym) usługa pracy w sieci WiFi nie zostanie przerwana dla podłączonych użytkowników, ani nie zostanie utracona możliwość podłączania się nowych użytkowników. Dotyczy to sieci WiFi bez autentykacji, z autentykacją WPA2 Personal, dla sieci z captive portalem (z katalogiem użytkowników przechowywanych na serwerze zewnętrznym), dla sieci z autentykacją i

uwierzytelnianiem WPA2 Enterprise (z katalogiem użytkowników przechowywanych na serwerze zewnętrznym).

- Licencje: dostarczone z kontrolerem licencje muszą pozwalać na obsługę minimum 22 punktów dostępowych i umożliwiać w przyszłości rozbudowę systemu o kolejne punkty dostępowe (min. 1000 AP dla pojedynczego kontrolera oraz 3000 AP dla klastra kontrolerów).
- Liczba sesji: kontroler musi pozwalać na obsługę minimum 24000 aktywnych użytkowników sieci bezprzewodowej.
- Ilość sieci WiFi: kontroler musi umożliwiać skonfigurowanie minimum 2000 niezależnych sieci WLAN (SSID) dla zapewnienia separacji usług w sieci bezprzewodowej.
- Adresacja IP: kontroler musi obsługiwać adresację IPv4 oraz móc pracować w trybie dual-stack (IPv4/IPv6).
- Obsługa ruchu sieciowego: kontroler musi umożliwiać przesyłanie ruchu bezpośrednio z punktów dostępowych zgodnie z regułami sieci przewodowej L2/L3, bez konieczności tunelowania ruchu przez kontroler.
- Tryb multitenant: kontroler musi wspierać tryb multitenant umożliwiający definiowanie osobnych uprawnień administracyjnych dla poszczególnych tenantów, uruchamiania dla nich poszczególnych usług typu dostęp gościnny lub hotspot, definiowania osobnych grup/stref AP wraz z granulacją wersji oprogramowania (w wypadku gdy w sieci pracują grupy AP, które nie są już obsługiwane przez nowe wersje oprogramowania), wyporu kanałów i ich szerokości jakie są dostępne dla grup AP, osobne raportowanie dla poszczególnych tenantów.
- Jakość usług: kontroler musi obsługiwać protokół 802.11e (WMM) w celu zapewnienia odpowiedniej jakości usług (QoS).
- Bezpieczeństwo: kontroler musi umożliwiać blokowanie użytkowników w wypadku jeśli ręcznie zmienili adres IP otrzymany z serwera DHCP. Musi być możliwe tworzenie list kontroli dostępu dla warstwy L2/3/4 z możliwością zaawansowanego filtrowania ruchu bezpośrednio na AP. Musi być możliwość stosowania różnych list kontroli dostępu dla poszczególnych WLAN.
- Detekcja aplikacji i użytkowników: kontroler musi rozpoznawać i raportować wykorzystywane aplikacje w rozbiciu per user, per AP, per SSID oraz umożliwiać ich blokowanie. Musi być możliwa identyfikacja zarówno użytkowników jak i typu urządzenia/systemu operacyjnego użytkownika sieci WiFi wraz z możliwością przypisania na tej podstawie odpowiedniej polityki dostępu (VLAN, limity prędkości itp.). Rozpoznawanie, kontrola i monitorowanie aplikacji musi być realizowane w oparciu o silnik deep-packet inspection. System musi oferować listę dostępnych aplikacji i umożliwiać zdefiniowanie aplikacji opisanych ręcznie co najmniej na podstawie numeru portu i rodzaju protokołu. Dla skategoryzowanych aplikacji musi być możliwość aktualizacji sygnatur aplikacji. Aktualizacja sygnatur musi wchodzić w zakres wsparcia technicznego, którym objęte jest wyposażenie.
- Detekcja obcych AP: kontroler musi umożliwiać wykrywanie i raportowanie obcych AP (Rogue AP) w postaci alarmów oraz powiadomień e-mail.
- Kontroler musi oferować API RESTful/JSON umożliwiające budowanie własnych aplikacji do zarządzania i monitorowania kontrolera i AP, dostępny w publicznym dokumencie opisującym sposób komunikacji.
- Raportowanie i monitorowanie: kontroler musi umożliwiać zbieranie informacji na temat uruchomionych sieci WiFi, podłączonych AP oraz podłączonych urządzeń klienckich WiFi. W tym umożliwiać monitorowanie parametrów pracy AP oraz umożliwiać porównanie tych parametrów do innych zdefiniowanych w grupie AP. Monitorowanie parametrów radiowych musi umożliwiać definiowanie warunków krytycznych punktu dostępowego powyżej którego przekroczeniu punkt dostępowy jest oznaczany odpowiednim statusem. Dla punktów dostępowych musi być konieczność zdefiniowania następujących parametrów pracy punktu dostępowego: opóźnienie na interfejsie radiowym, użycie kanału radiowego, liczba prób połączeń niezakończona sukcesem. Wbudowany analityczny system musi automatycznie prowadzić ranking punktów dostępowych wraz z historycznymi wartościami przez co znacząco usprawniony jest proces izolowania problemu i określenia zakresu problemu, który może degradować jakość pracy sieci WiFi. Musi być możliwe monitorowanie i tworzenie raportów dot. parametrów kontrolera co najmniej: użycie procesora, użycie pamięci, ilość ruchu typu management. Raportowanie powinno obejmować minimum 30 dni wstecz. Restart kontrolera nie może powodować utraty zebranych danych i raportów. Ponadto musi być możliwy podgląd informacji statystycznych dot. podłączonych urządzeń do 3 dni wstecz w tym możliwość dokładnego określenia czasu podłączenia się do danego SSID, BSSID, przydzielonego adresu IP, liczby wysłanych i odebranych danych. Dopuszcza się spełnienie powyższego warunku poprzez dostawę zewnętrznego systemu raportującego wraz z niezbędnym sprzętem, licencjami, wsparciem producenta (nie krótszym od wsparcia na oferowane rozwiązanie WiFi) oraz wdrożeniem takiego systemu.
- Zdalne logi: kontroler musi móc korzystać z serwera syslog logując zdalnie informacje na temat sesji podłączonych urządzeń zawierających co najmniej: MAC address urządzenia klienckiego, przydzielony adres IP klienta, adres IP przeznaczenia, rodzaj protokołu, MAC address AP, do którego podłączony był klient.
- Wsparcie RADIUS: w przypadku korzystania z kontrolera jako klienta NAS dla RADIUS musi być możliwość określenia sposobu przedstawiania się kontrolera w usłudze RADIUS z wykorzystaniem co najmniej BSSID WLAN i adresu MAC AP.
- Wsparcie VLAN: kontroler musi obsługiwać protokół 802.1Q i umożliwiać ustawianie osobnego VLAN-u dla każdej sieci WLAN oraz nadrzędne przydzielanie użytkownika do odpowiedniego VLAN-u zgodnie z odpowiedzią serwera RADIUS, pozwalając na pełną separację ruchu.
- Zarządzanie sieciami WLAN, równoważenie obciążenia AP: kontroler musi umożliwiać ukrywanie poszczególnych sieci WLAN (SSID), uruchamianie i włączanie ich w oparciu o harmonogram z godzinową lub większą granulacją, ograniczanie prędkości przesyłu danych od klientów dla każdego z WLAN osobno dla pobieranych i wysyłanych danych, ograniczenie maksymalnej ilości użytkowników podłączonych do

poszczególnych sieci WLAN (client admission - w podziale na każdy AP w zależności od liczby podłączonych urządzeń, wykorzystania pasma radiowego, średniej przepustowości dla urządzenia), przenoszenie klientów pomiędzy pasmami radiowymi danego AP (z możliwością zdefiniowania obciążenia pasma w zależności od ilości klientów), automatyczne równoważenie obciążenia AP przez klientów sieci radiowej, izolację sieci radiowej (zapobieganie możliwości komunikowania się klientów w obrębie tej samej sieci WLAN) uruchamianą osobno dla każdej zdefiniowanej sieci WLAN.

- Wsparcie pozostałych standardów: kontroler musi oferować pełne wsparcie dla standardów 802.11r, 802.11k, 802.11w MFP, możliwość mapowania ustawień QoS User Priority/Class of Service protokołu 802.1p na wartości DSCP, obsługiwać VLAN pooling oraz Proxy ARP.
- Automatyczne wykrywanie kontrolera przez AP: kontroler musi być automatycznie wykrywany przez punkty dostępowe w warstwie L2 i L3. W przypadku warstwy L3 kontroler musi być wykrywany co najmniej z wykorzystaniem opcji 43 serwera DHCP, zapytanie DNS lub przez ręczne zdefiniowanie go na poziomie AP.
- Automatyczna aktualizacja oprogramowania AP: kontroler musi zapewniać automatyczny upgrade firmware-u AP z wykorzystaniem bezpiecznego połączenia (SSL, IPSEC itp.).
- Zapobieganie zakłóceniom: kontroler musi w sposób dynamiczny zarządzać częstotliwościami radiowymi oraz mocą wszystkich AP oraz optymalizować dobór kanałów AP w czasie rzeczywistym.
- Sieć mesh: kontroler musi oferować możliwość konfiguracji sieci mesh pozwalając na podłączanie AP bez wykorzystania sieci przewodowej do innego AP. Topologia sieci powinna być optymalizowana automatycznie tak by zapewniać najlepszą przepustowość i przywrócenie pracy systemu w wypadku awarii. Sieć mesh w wypadku awarii danego uplinku radiowego powinna kontynuować działanie poprzez przełączenie się na alternatywny, sąsiadujący uplink.
- Autentykacja i szyfrowanie ruchu: kontroler musi zapewniać pełne wsparcie dla następujących mechanizmów zabezpieczania połączeń radiowych: WEP, WPA-TKIP, WPA2-AES, 802.11i, WPA2 Enterprise (autentykacja z wykorzystaniem zewnętrznych serwerów AAA – co najmniej Active Directory, LDAP, LDAP SSL, RADIUS, lokalna baza użytkowników w kontrolerze), WPA2 Personal, wsparcie dla Captive Portal, WISPr, standardu HotSpot 2.0 (Wi-Fi Certified Passpoint), obsługę sieci Guest WLAN (autoryzacja za pomocą generowanych ticketów dostępowych – wymagana jest możliwość dostarczania ich przez SMS, e-mail oraz możliwość wydrukowania). Wbudowana baza kont gościnnych musi umożliwiać wygenerowanie co najmniej 10000 takich kont.
- Zarządzanie kontrolerem: dostęp do zarządzania kontrolerem musi być realizowany w oparciu o bezpieczne protokoły (np. ssh, https), z możliwością wyłączenia protokołów niezabezpieczonych (np. telnet, http) jeśli są wspierane. Ruch zarządzający między kontrolerem a AP musi być zabezpieczony. Kontroler musi posiadać wbudowaną funkcję generowania ruchu w celu diagnostyki łączności i pomiaru przepływności między kontrolerem a podłączonymi AP. Kontroler musi wspierać protokół SNMPv3.
- Mapy sieci radiowej: kontroler musi umożliwiać graficzną prezentację rozmieszczenia punktów dostępowych w oparciu o wbudowane mapy (dopuszcza się rozwiązanie prezentujące rozmieszczenie AP w oparciu o mapy zewnętrznego dostawcy np. Google Maps) oraz możliwość zdefiniowania własnych map. Prezentowane na mapach informacje muszą zawierać co najmniej następujące informacje o prezentowanych AP: nazwa, adres IP, kanał radiowy, liczba podłączonych klientów, opóźnienie interfejsu radiowego, wykorzystanie interfejsu radiowego, liczba prób połączeń zakończonych niepowodzeniem.
- Zarządzanie przełącznikami: kontroler musi umożliwiać zarządzanie przełącznikami sieciowymi z poziomu interfejsu GUI kontrolera (jeśli urządzenia pochodzą od tego samego producenta).

Punkty dostępowe (AP) do instalacji wewnątrz budynków – 22 szt. posiadające następujące właściwości:

- Tryby pracy: AP muszą wspierać tryb pracy standalone (zarządzanie musi być możliwe za pomocą SSH i przeglądarki internetowej), pod kontrolą zewnętrznego kontrolera WiFi, jako samodzielny kontroler sieci WiFi umożliwiając zarządzanie grupą do 20 AP i obsługę klientów 802.11a/b/g/n/ac.
- Obsługa standardów i szybkości transmisji: AP muszą obsługiwać standardy 802.11a (6, 9, 12, 18, 24, 36, 48, 54 Mbps), 802.11b (1, 2, 5.5, 11 Mbps), 802.11d, 802.11g (6, 9, 12, 18, 24, 36, 48, 54 Mbps), 802.11n (6,5-300 Mbps), 802.11ac (6,5 – 867 Mbps).
- Optymalizacja wydajności: AP muszą automatycznie wybierać najlepszy kanał pracy w oparciu o rzeczywistą przepustowość (pojemność) kanałów dla pasm 2,4 GHz i 5 GHz oraz wspierać standard 802.11h i umożliwiać przenoszenie urządzeń klienckich na optymalny kanał. AP muszą wspierać mechanizm Airtime Fairness.
- Liczba klientów: AP muszą wspierać możliwość podłączenia minimum 400 klientów.
- Analiza widma: AP muszą posiadać wbudowane wsparcie dla analizy spektrum widma.
- Liczba sieci WLAN: AP muszą umożliwiać zdefiniowanie co najmniej 16 BSSID z własnymi politykami dostępu i regułami QoS.
- Pasma: AP muszą zapewniać równoczesną pracę w paśmie 2,4 GHz oraz 5 GHz (dual-band).
- Moduły radiowe, anteny: AP muszą posiadać wbudowane, zintegrowane anteny ze wzmocnieniem minimum 3 dBi dla pasma 5 GHz. Minimalna czułość modułu odbiorczego 2,4 GHz oraz 5 GHz -95 dBm. Maksymalna zagregowana moc nadawania dla 2,4 GHz oraz 5 GHz 24 dBm.
- Tryb MIMO: AP muszą umożliwiać pracę co najmniej w trybie MIMO 2x2:2.
- Tryb routera: AP muszą umożliwiać pracę w trybie routera ze wsparciem dla NAT i DHCP.
- Zasilanie: przez PoE lub zasilacz sieciowy.
- Porty sieciowe: 2 porty RJ45, auto MDX, co najmniej jeden z możliwością zasilania przez PoE, automatyczne wykrywanie prędkości połączenia 10/100/1000 Mbps.
- Wsparcie dla BLE: AP muszą posiadać port USB umożliwiający obsługę sensorów standardu BLE lub posiadać wbudowaną obsługę BLE.

- Zabezpieczenie fizyczne: gniazdo linki zabezpieczającej przed kradzieżą.
- Wsparcie dla pozostałych standardów i technologii: AP muszą ponadto wspierać następujące standardy i technologie: VLAN 802.1q, Tx SU beamformer (802.11ac TxBF), Tx DL MU-MIMO, Rx MCS 8-9 (256-QAM), Rx A-MPDU, Rx A-MSDU, Low Density Parity Check coding, 802.1x dla portu Ethernet w trybie suplikanta i autentykatora, 802.11e/WMM (nie mniej jak 4 kolejki QoS per klient), Multicast IP video streaming, 802.3at PoE, 802.3af PoE,
- Sieć typu Mesh: AP muszą wspierać pracę w sieci o topologii Mesh.
- Sposób montażu: AP muszą posiadać niezbędne akcesoria umożliwiające montaż na różnych typach powierzchni i wyposażenia, w tym co najmniej: lite otynkowane powierzchnie ceglane/betonowe (np. za pomocą kołków), sufity podwieszane.

Przełącznik sieciowy – 1 szt. o parametrach:

- Zarządzalny przełącznik sieciowy warstwy L3, co najmniej 12 portów RJ45 Gigabit Ethernet ze wsparciem PoE/PoE+ w tym co najmniej 2 porty RJ45 uplink Gigabit Ethernet i co najmniej 2 porty uplink/stacking 1/10 Gigabit Ethernet SFP/SFP+. Budżet PoE minimum 120W. Wsparcie dla VLAN, Spanning Tree, IGMP snooping, 802.11x, LACP. Minimalna przepustowość przełączania (pojemność przełącznika) 60 Gbps. Wysokość przełącznika 1U, uchwyty do montażu w szafie rack 19”.

Usługi:

- Usługa instalacji (wdrożenia) systemu złożonego z powyższego wyposażenia.
- W przypadku jeśli AP powinny być montowane w pozycji poziomej (pod sufitami) wykonawca w ramach wdrożenia dociągnie do każdego z nich okablowanie sieciowe połączone z gniazdem sieciowym. Okablowanie musi być umieszczone w możliwie cienkim i nie rzucającym się w oczy korytku sieciowym. Maksymalna szacowana odległość od gniazda sieciowego do AP – 10 m. Zamawiający nie przewiduje konieczności kucia i wiercenia w ścianach w celu przeprowadzenia instalacji sieciowej. Przed złożeniem oferty możliwa i wskazana jest wizja lokalna.

Warunki realizacji:

- Czas realizacji zadania: do 4 tygodni od daty podpisania umowy.
- Urządzenia muszą być objęte minimum 36-miesięczną gwarancją i wsparciem obejmującym aktualizacje oprogramowania i pomoc techniczną.
- Wszystkie urządzenia muszą pochodzić od tego samego producenta i być objęte pojedynczym kontraktem na opiekę serwisową.
- Dostarczany sprzęt musi pochodzić z autoryzowanego kanału sprzedaży na terenie Polski/UE,
- Osoba odpowiedzialna za wdrożenie musi posiadać certyfikat producenta urządzeń.

