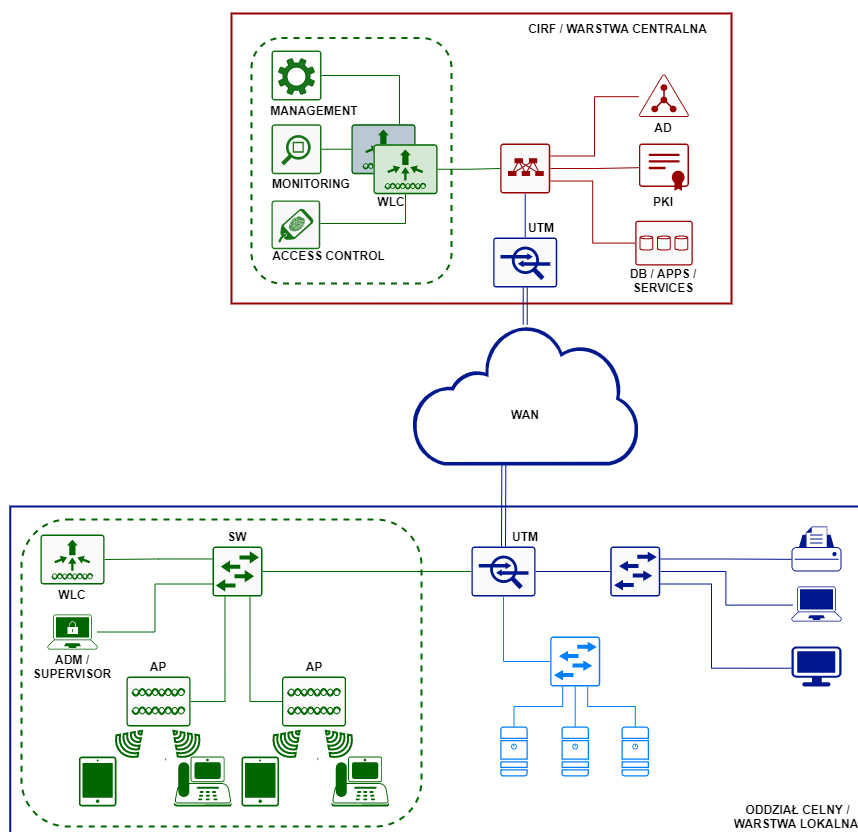


Minimalne wymagania techniczne dotyczące zastosowanych urządzeń sieci Wi-Fi:

- Wszystkie urządzenia, w tym Kontrolery, AP, Switche muszą pochodzić od jednego producenta i pracować jako spójny, zintegrowany system
- Wszystkie proponowane urządzenia muszą być dopuszczone do sprzedaży na terytorium RP.
- Sieć WLAN może mieć tylko jeden punkt styku z istniejącą siecią LAN/WAN poprzez istniejące w jednostkach zarządzania dostępowe (UTM).
- Na potrzeby sieci WLAN należy zaprojektować dedykowaną sieć LAN z własnymi zarządzalnymi przełącznikami sieciowymi i ewentualnymi punktami dystrybucyjnymi.
- Wszystkie usługi będą realizowane w formie on premises.
- Systemy monitorowania, zarządzania i potwierdzania tożsamości/ kontroli dostępu należy zaplanować w formie dedykowanego przez producenta urządzenia.



Rys. Przewidywana koncepcja budowanej sieci Wi-Fi.

Kontrolery Sieci Bezprzewodowej

- Kontrolery centralne pracujące w klastrze HA replikujące konfiguracje na kontrolery lokalne, zarządzające aktualizacjami i stanowiące punkt dystrybucji licencji w lokalizacjach.
- Zarządzanie optymalizacją RF - centralny plan rozłożenia kanałów sieci bezprzewodowej oraz mocy jej nadawania dla całej sieci bezprzewodowej uwzględniając wszystkie kontrolery podrzędne.
- Kontrolery lokalne we wszystkich lokalizacjach, zarządzające asocjacją i terminującą sesje klientów, sterujące ruchem w sieci i konfiguracją punktów dostępowych.
- Obsługa Wi-Fi 6 (802.11ax), WPA3 i Enhanced Open
- Usługa QOS – pozwalająca na zapewnienie właściwych priorytetów różnym rodzajom transmisji danych.
- Interfejsy sieciowe kontrolerów:
 - Minimum 2 porty 10GBASE-X ze stykiem definiowanym przez SFP+
 - Minimum 2 porty gigabitowe w standardzie 10/100/1000BaseT
- Bezstratny roaming pomiędzy AP wspierający ciągłość połączeń VOIP.
- Kontroler musi posiadać funkcję systemu WIDS/ WIPS.
- Kontrolery centralne mogą zostać zastąpione przez dedykowany system oferujący podobne funkcje.
- Wymagana jest możliwość rozbudowy sieci WLAN o dodatkowe punkty dostępowe (wewnętrzne i zewnętrzne) bez konieczności wymiany kontrolerów o minimum 30 % wszystkich urządzeń w każdej z lokalizacji.
- Kontrolery lokalne i centralne należy zaplanować w formie dedykowanego przez producenta urządzenia.

Access Point:

- Wszystkie zewnętrzne AP muszą spełniać warunki eksploatacyjne dotyczące temperatur w zakresie -30 do 40C oraz posiadać klasę szczelności minimum IP55. Nie dopuszcza się montowania dodatkowych obudów dla punktów dostępowych.
- AP wewnętrzne montowane na ścianach lub suficie, warunki eksploatacyjne w zakresie temperatur 5 do 45 st. C.
- Dopuszczalny montaż anten dedykowanych przez producenta do AP z zachowaniem parametrów eksploatacyjnych w zakresie klasy szczelności i temperatur użytkowania.
- Urządzenia w standardzie 802.11AX z zachowaniem kompatybilności wstecznej dla 802.11 a/b/g/n/ac.
- Technologia transmisji minimum 2x2:2 MIMO w pasmach 2,4 GHz i 5 GHz Podstawową częstotliwością pracy nadajników będzie 5GHz .
- Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe.
- Nie może zostać zastosowana technologia typu *Mesch*.
- W przypadku AP z interfejsem miedzianym należy zastosować zasilanie za pośrednictwem PoE.
- W przypadku AP z interfejsem światłowodowym niezbędne jest zaprojektowane dedykowanej sieci zasilającej

Minimalne wymagania dot. zabezpieczeń sieci:

- Autoryzacja, uwierzytelnianie, rozliczanie za pomocą dedykowanego centralnego serwera AAA (Authentication, Authorization, Accounting).
- Połączenia sieciowe pomiędzy urządzeniami końcowymi, a AP muszą być szyfrowane za pomocą standardów WPA2 oraz WPA3.

- Uwierzytelnianie urządzeń sieciowych musi odbywać się za pomocą protokołu 802.1x.
- Potwierdzenie tożsamości suplikanta, przesłanie decyzji o dopuszczeniu bądź odrzuceniu podłączanego urządzenia, wygenerowanie kluczy szyfrujących, tworzenie i egzekwowanie zasad dostępu urządzeń końcowych do sieci za pomocą dedykowanego centralnego systemu.
- Centralny system musi umożliwiać hierarchiczne zarządzanie urządzeniami (administrator centralny, administrator regionalny).
- Autentykacja urządzeń na podstawie certyfikatów PKI Zamawiającego oraz na podstawie MAB (w przypadku braku możliwości instalacji suplikanta).
- Autentykacja użytkownika będzie odbywała się za pomocą usługi Active Directory
- Centralny system musi posiadać interfejs do konfigurowania oraz przeglądania polityk sieciowych.

System monitorowania:

- Musi zostać zaimplementowany dedykowany centralny system monitorujący stan wszystkich urządzeń sieciowych.
- Funkcjonalność zbierania informacji, logów o czynnościach jakie wykonał użytkownik, na urządzeniach (np. kontrolery, AP i przełączniki).
- System musi zapewniać wielopoziomowy dostęp do informacji diagnostycznych z podziałem na monitorowane lokalizacje i grupy lokalizacji.
- System powinien zapisywać historię wykonanych poleceń/czynności administratora
- Dedykowany system raportowania.

Zarządzanie systemem sieci Wi-Fi:

- Zarządzanie, wprowadzanie polityk bezpieczeństwa za pomocą dedykowanego interfejsu (np. przypisanie podłączanych urządzeń do odpowiedniego vlan-u).
- Umożliwia konfigurację grupową lub tworzenie szablonów konfiguracji elementów systemu
- Zapewnić wielopoziomowy dostęp do zarządzanych urządzeń z podziałem na zarządzanie centralne oraz lokalne.
- Funkcjonalność zarządzania posiadanymi licencjami.
- Zarządzanie vlanami tzw. dynamic VLAN – jaki vlan ma dostać urządzenie.

Infrastruktura sieci WLAN oraz integracja z obecną infrastrukturą LAN/WAN

- Nowoprojektowana sieć WLAN nie może korzystać z infrastruktury pasywnej i aktywnej znajdującej się w wymienionych lokalizacjach.
- Zamawiający dopuszcza wykorzystanie istniejącej kanalizacji teletechnicznej i tras kablowych oraz szaf dystrybucyjnych pod warunkiem, że są one drożne i pozostanie w nich co najmniej **25 %** zapasu na przyszłe instalacje. Kanalizacja teletechniczna istnieje w okolicach budynków, pawilonach odpraw oraz w miejscach instalacji AP istniejących sieci Wi-Fi, jednak Zamawiający nie gwarantuje jej drożności.
- Zamawiający zgadza się na wykorzystanie istniejącej infrastruktury po wcześniejszym uzgodnieniu. Zamawiający nie posiada aktualnej dokumentacji określającej zajętość i drożność istniejącej kanalizacji teletechnicznej. Średnio zajętość kanalizacji szacuje się na 50%, lecz część kanałów może nie umożliwiać wprowadzenia dodatkowych linii kablowych.
- Bardziej szczegółowe dane na temat istniejącej kanalizacji teletechnicznej (na etapie projektowania) można uzyskać w Zakładach Obsługi Przejść Granicznych.
- W przypadku braku możliwości wykorzystania istniejącej infrastruktury wykonawca musi wykonać nowe ciągi kablowe w terenie, który może obejmować tereny zielone, drogi (w tym

przeznaczone dla ruchu towarowego) i chodniki brukowe, drogi asfaltowe, konstrukcje betonowe (np. perony), konstrukcje stalowe i drewniane. W nowej kanalizacji teletechnicznej konieczne jest zastosowanie rur wzmocnionych HDPE lub równoważnych. Elementy kanalizacji teletechnicznej muszą zostać dobrane tak by zapewnić co najmniej 30% rezerwy na dodatkowe okablowanie.

- W przypadku braku możliwości zamocowania AP na istniejących konstrukcjach wykonawca musi przewidzieć dedykowane maszty.
- Pozostałe okablowanie zewnętrzne należy prowadzić w metalowych i zamykanych korytach elektroinstalacyjnych lub rurkach elektroinstalacyjnych.
- Prowadzenie kabli wewnątrz istniejących budynków należy wykonać w sposób estetyczny z wykorzystaniem istniejącej infrastruktury prowadzenia okablowania tj. koryt kablowych umieszczonych w sufitach podwieszanych lub natynkowych. W przypadku braku takiej możliwości, dopuszcza się zastosowanie kanałów i listew elektroinstalacyjnych.
- Całą infrastrukturę WLAN należy zasilać z istniejącej w lokalizacji sieci zasilania rezerwowanego (agregat), a jeśli taka istnieje to z sieci zasilania gwarantowanego (UPS).