ZP/UR/124/2014 Załącznik nr 1.1 do SIWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA
(parametry i wymagania minimalne)

Przedmiotem zamówienia jest dostawa fabrycznie nowego, nie używanego różnego sprzętu komputerowego i sieciowego wraz z montażem, instalacją, konfiguracją, uruchomieniem i wdrożeniem w celu rozbudowy sieci LAN w ramach projektu „Przyrodniczo – Medyczne Centrum Badań Innowacyjnych"

Termin realizacji: do 4 miesięcy od daty podpisania umowy

Miejsce realizacji: Uniwersytet Rzeszowski, Rzeszów, ul. Warzywna, Przyrodniczo - Medyczne Centrum Badań Innowacyjnych.

Wymagania ogólne dot. gwarancji i serwisu sprzętu:

1. Zamawiający wymaga udzielenia **co najmniej 60 miesięcy gwarancji** na dostarczone urządzenia i ich elementy, czyli całość przedmiotu zamówienia licząc od dnia podpisania przez strony protokołu odbioru końcowego (po oddaniu przedmiotu zamówienia do eksploatacji – tj. po zainstalowania, wdrożeniu, uruchomieniu i przetestowaniu przedmiotu zamówienia).
2. Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady powstałe z przyczyn tkwiących w przedmiocie zamówienia w chwili dokonania odbioru przez zamawiającego jak i wszelkie inne wady fizyczne, powstałe z przyczyn, za które wykonawca ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w ciągu terminu obowiązywania gwarancji.
3. Czas reakcji pracownika serwisu na zgłoszoną awarię wynosi: **nie dłużej niż 24 godziny** w godzinach od 8:00 do 17:00 w dni robocze, (przez czas reakcji rozumiany jest przyjęcie zgłoszenia i wizyta pracownika w miejscu instalacji)
4. Naprawa gwarancyjna będzie wykonana:
   a) w przypadku awarii w terminie nie **dłuższym niż 5 dni roboczych** od zgłoszenia awarii, chyba że Strony w oparciu o stosowny protokół konieczności wzajemnie podpisany uzgodnią dłuższy czas naprawy. (Awaria − stan niesprawności uniemożliwiający użytkowanie, występujący nagle i powodujący niewłaściwe działanie lub całkowite unieruchomienie).
   b) w przypadku usterki w terminie **nie dłuższym niż 14 dni roboczych** licząc od dnia przyjęcia zgłoszenia przez serwis (faxem lub e-mailem), chyba że Strony w oparciu o stosowny protokół konieczności wzajemnie podpisany uzgodnią dłuższy czas naprawy (Usterka - uszkodzenie lub błędne działanie utrudniające użytkowanie ale nie ograniczające funkcjonalności).
5. W przypadku trzykrotnej awarii tego samego elementu wykonawca zobowiązany jest do wymiany wadliwego elementu na nowy w terminie 30 dni od dnia zawiadomienia przez Zamawiającego faksem lub mailem, że dany element wykazuje wady.
6. W przypadku gdy wykonawca nie zastosuje się do powyższych punktów zamawiający jest uprawniony do usunięcia wad samodzielnie lub w drodze zlecenia naprawy na ryzyko i koszt wykonawcy zachowując przy tym inne uprawnienia przysługujące mu na podstawie umowy, w szczególności związanych z uprawnieniami z tytułu gwarancji i rękojmi.

Wymagania dodatkowe:

1. Oferowany sprzęt musi być fabrycznie nowy i nie używany.

2. Zamawiający wymaga aby oferowany sprzęt pochodził z oficjalnego i legalnego kanału dystrybucyjnego.
3. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta, że dostarczony sprzęt pochodził z oficjalnego i legalnego kanału dystrybucyjnego.
4. Wykonawca przed odbiorem przedmiotu zamówienia dostarczy potwierdzenie producenta, że zastosowane moduły światłowodowe SFP/SFP+ są kompatybilne z urządzeniami aktywnymi dostarczonego przedmiotu zamówienia.

Pozycja nr 1: Dostawa fabrycznie nowego, nie używanego różnego sprzętu komputerowego i sieciowego wraz z montażem, instalacją, konfiguracją, uruchomieniem i wdrożeniem

Pozycja nr 2: Konieczne do wykonania roboty instalacyjne związane z podłączeniem ułożeniem kabli strukturalnych i montaż gniazd

Opis minimalnych wymagań dotyczących pozycji nr 1:

1. Urządzenia aktywne do sieci LAN (przełączniki)

1.1. Rdzeń sieci LAN

1. W ramach rozbudowy istniejącej sieci LAN UR należy dostarczyć fabrycznie nowy, nie używany następujący sprzęt oraz wykonać jego montaż, instalację, konfigurację i uruchomienie zgodnie z poniższymi wymogami

1.1.1. Przełącznik rdzeniowy

Przełącznik rdzeniowy ma zostać wyposażony w następującą moduły/porty:

- Przełącznik modularny, umożliwiający minimum instalację dwóch modułów zarządzających oraz co najmniej sześciu kart rozszerzeń
- Minimum dwa moduły zarządzające o wydajności nie mniejszej niż 380Gbps każdy, wyposażone w pamięci typu FLASH o pojemności nie mniejszej niż 256MB
- Minimum dwa zasilacze o mocy nie mniejszej niż 2800W każdy z nich, zapewniający redundancję w przypadku awarii jednego z nich
- Przełącznik należy wyposażyć w karty tak aby posiadał on następujące ilości portów:
    - Minimum 192 porty 10/100/1000Base-T z PoE+
    - Minimum 10 portów światłowodowych umożliwiających wykonanie połączeń 10Gbps po łączach światłowodowych wielo i jedno modowych
    - Minimum 24 porty umożliwiające wykonanie połączeń światłowodowych 1Gbps
- Przełącznik należy wyposażyć w moduły:
    - Minimum 2 moduły światłowodowe 10Gbps jednomodowe na odległość do minimum 10km
    - Minimum 8 modułów światłowodowych 10Gbps wielomodowych na odległość do minimum 300m
    - Minimum 12 portów światłowodowych 1Gbps wielomodowych na odległość do minimum 300m

Przełącznik rdzeniowy ma zostać dołączony do istniejącej sieci na UR oraz ma zapewnić:

- możliwość dołączenia i współpracy przełącznika rdzeniowego z istniejącym, działającym klastrem (urządzenia fizyczne połączone w jeden wirtualny switch) na Uniwersytecie Rzeszowskim. Urządzenia muszą być łączone z wykorzystaniem standardowych połączeń ethernet 10Gbps, które wykorzystuje działający klaster na UR,
- wsparcie co najmniej dla Jumbo Frames na portach 10Gbps oraz portach 1000Base-T,
- możliwość uruchomienia standardowych protokołów co najmniej VRRP, IS-IS, OSPF, BGP-4,
- możliwość obsłużenia co najmniej tablicy adresów MAC o wielkości min. 500000 pozycji
- wydajność przełącznika min. 480 milonów pps,

- przepustowość przełącznika min. 760 Gbps,
- wsparcie dla rozwiązania dynamicznej rejestracji w sieciach VLAN np. GVRP.

1.1.2. Konfiguracja przełącznika rdzeniowego

W ramach rozbudowy istniejącej sieci LAN UR należy:

- W pomieszczeniu BD1 zamontować przełącznik rdzeniowy wraz z dostarczanym wyposażeniem (zasilacze, karty, moduły światłowodowe itp.…)
- Wykonać połączenie pomiędzy przełącznikiem rdzeniowym, a przełącznikiem (działającym klastrem przełączników na Uniwersytecie Rzeszowskim) umieszczonych w rdzeniu sieci LAN (dwie serwerownie połączone linkiem światłowodowym jednomodowym), połączenie 2x10Gbp po światłowodzie jednomodowym (należy również skonfigurować istniejące przełączniki rdzeniowe w rdzeniu sieci)
- Wykonać konfigurację przełącznika rdzeniowego zgodnie z wymogami opisanymi poniżej.

W ramach instalacji przełącznika rdzeniowego w sieci należy również dostarczyć niezbędne elementy do prawidłowego montażu dostarczanych elementów jak również dostarczyć niezbędne okablowanie (patchcord-y miedziane i światłowodowe) niezbędne do wykonania połączeń pomiędzy przełącznikami.

Przełącznik rdzeniowy należy podłączyć zagregowanym linkiem 2x10Gbps do istniejącego działającego klastra UR (po jednym linku 10Gbps do każdego z nodów klastra). Do wykonania tego połączenia należy również dostarczyć moduły 10Gbps SFP+ do posiadanych przełączników wchodzących w skład działającego klastra (Zamawiający posiada jeszcze wolne porty 10Gbps na przełącznikach w każdym z nodów klastra).

1.2. Obsługa punktów dostępowych

W ramach rozbudowy istniejącej sieci LAN UR należy dostarczyć następujący sprzęt oraz wykonać jego konfiguracje zgodnie z poniższymi wymogami.

1.2.1.Wykaz przełączników dostępowych

Należy dostarczyć przełączniki wraz z wyposażeniem spełniające wymagania:

Przełącznik: „sw_dost_typ_1”:

- Przełącznik wyposażony w minimum 20 portów 10/100/1000BaseT
- Możliwość zasilania PoE 802.3af na wszystkich portach 1000Base-T
- Przełącznik wyposażony w minimum 4 dodatkowe combo 10/100/1000BaseT lub SFP Gigabit
- Przełącznik wyposażony w min. 2 sloty na moduły umożliwiające montaż dodatkowych portów w wariantach:
    - minimum 2 porty SFP+
    - minimum 2 porty SFP
    - minimum 2 porty CX4
    - minimum 2 porty XFP
- Przełącznik musi umożliwiać łączenie urządzeń w stos działający jako jeden wirtualny przełącznik. Urządzenia muszą być łączone w ramach stosu z wykorzystaniem standardowych połączeń ethernet 10Gbps.
- Przełącznik musi być wyposażony w minimum 128MB pamięci RAM i minimum 16MB pamięci FLASH
- Wydajność przełącznika nie mniejsza niż 107 milionów pps
- Przepustowość przełącznika nie mniejsza niż 144Gbps
- Możliwość zarządzania co najmniej przez:
    - Telnet
    - Stronę WEB
    - Dedykowaną aplikację producenta
- Tablica adresów MAC o wielkości min. 16k pozycji
- Obsługa co najmniej ramek Jumbo
- Wsparcie dla IGMP Snooping per VLAN
- Obsługa sieci IEEE 802.1Q VLAN – min. 4094 sieci VLAN

- Możliwość konfiguracji statycznego routingu co najmniej dla adresów IPv4 i IPv6
- Możliwość przypisania pakietów do Voice VLAN'u z wykorzystaniem mapowania zakresów MAC
- Możliwość przypisania do wielu sieci VLAN taggowanych, jak i do wielu sieci VLAN nie-taggowanych
- Funkcja Root Guard umożliwiająca ochronę co najmniej sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
- BPDU Guard – funkcja umożliwiająca wyłączenie portu w momencie odebrania na tym porcie ramek BDPU
- Możliwość włączenia protokołu sFlow
- Możliwość uruchomienia i konfiguracji parametrów balansowania ruchu dla dedykowanych połączeń wirtualizacyjnych Ethernet co najmniej 10 Gb/s, przełączników pracujących w stosie

Przełącznik: „sw_dost_typ_2"

- Przełącznik wyposażony w minimum 44 portów 10/100/1000BaseT
- Możliwość zasilania PoE 802.3af na wszystkich portach 1000Base-T
- Przełącznik wyposażony w minimum 4 dodatkowe combo 10/100/1000BaseT lub SFP Gigabit
- Przełącznik wyposażony w min. 2 sloty na moduły umożliwiające montaż dodatkowych portów w wariantach:
    - minimum 2 porty SFP+
    - minimum 2 porty SFP
    - minimum 2 porty CX4
    - minimum 2 porty XFP
- Przełącznik musi umożliwiać łączenie urządzeń w stos działający jako jeden wirtualny przełącznik. Urządzenia muszą być łączone w ramach stosu z wykorzystaniem standardowych połączeń ethernet 10Gbps.
- Przełącznik musi umożliwiać tworzenie stosu z minimum 4 urządzeń
- Przełącznik musi być wyposażony w minimum 128MB pamięci RAM i minimum 16MB pamięci FLASH
- Wydajność przełącznika nie mniejsza niż 140 milionów pps
- Przepustowość przełącznika nie mniejsza niż 190Gbps
- Możliwość zarządzania co najmniej przez:
    - Telnet
    - Stronę WEB
    - Dedykowaną aplikację producenta
- Tablica adresów MAC o wielkości min. 16k pozycji
- Obsługa co najmniej ramek Jumbo
- Wsparcie dla IGMP Snooping per VLAN
- Obsługa sieci IEEE 802.1Q VLAN – min. 4094 sieci VLAN
- Możliwość konfiguracji statycznego routingu co najmniej dla adresów IPv4 i IPv6
- Możliwość przypisania co najmniej pakietów do Voice VLAN'u z wykorzystaniem mapowania zakresów MAC
- Możliwość przypisania do wielu sieci VLAN taggowanych, jak i do wielu sieci VLAN nie-taggowanych
- Funkcja Root Guard umożliwiająca co najmniej ochronę sieci przed wprowadzeniem do sieci urządzenia, które może przejąć rolę przełącznika Root dla protokołu Spanning Tree
- BPDU Guard – funkcja umożliwiająca wyłączenie portu w momencie odebrania na tym porcie ramek BDPU
- Możliwość włączenia co najmniej protokołu sFlow
- Możliwość konfiguracji parametrów balansowania ruchu dla dedykowanych połączeń wirtualizacyjnych Ethernet co najmniej 10 Gb/s, przełączników pracujących w stosie

Zestawienie ilościowe przełączników dostępowych do każdego z punktów dystrybucyjnych, które należy dostarczyć zostało wyspecyfikowane w poniższej tabeli :

Pkt. dystrybucyjny	Ilość sw_dost_typ_1	Ilość sw_dost_typ_2	Przełączniki połączone w stos
FD01	0	2	TAK
FD02	1	0	NIE
FD1	0	4	TAK
FD3	0	2	TAK
FD4	0	6	TAK
BD2	0	8	TAK
Dodatkowe (obsługa dodatkowych portów)	0	2	TAK
Suma	**1**	**24**	

Powyższe zestawienie nie uwzględnia modułów i/lub kabli służących do połączenia urządzeń w stos/klaster. Moduły i kable te należy również dostarczyć. Sposób łącznia przełączników w stos został opisany poniżej.
Przełącznik rdzeniowy i przełączniki dostępowe muszą wykorzystywać tą samą technologię łączenia urządzeń w stos/klaster.
Dostarczone moduły światłowodowe SFP/SFP+ do przełączników dostępowych i rdzeniowego muszą być kompatybilne oraz nie powodujące problemów serwisowych i gwarancyjnych.
Uwaga:
Każdy z przełączników opisanych w powyższej tabeli jako „**Dodatkowe**” należy również wyposażyć w:

- Kartę i kabel umożliwiający tworzenie stosu
- Kartę z portami min. 2x 10Gbps SFP+
- Moduł min. 1Gbps do wykonania połączenia na światłowodzie wielomodowym do 300m
- Moduł min. 10Gbps SFP+ do wykonywania połączeń po światłowodzie wielomodowym

1.2.2. Podłączenie przełączników dostępowych w punktach dystrybucyjnych

W każdym z punktów dystrybucyjnych należy zainstalować przełączniku i skonfigurować je zgodnie z wymogami.
Przełączniki zlokalizowane w jednym punkcie dystrybucyjnym należy łączyć w stos/klaster (urządzenia mają być widoczne jako jeden przełącznik). Przełączniki pracujące w stosie muszą posiadać co najmniej jedno połączenie co najmniej 10Gbps i jedno połączenie co najmniej 1Gbps do przełącznika rdzeniowego. W przypadku gdy liczba urządzeń w pojedynczym punkcie dystrybucyjnym przekracza ilość urządzeń jaka może wchodzić w skład stosu należy stworzyć dwa lub więcej stosów łącząc każdy ze stosów z przełącznikiem korowym jednym linkami co najmniej 10Gbps. Dodatkowo jeden ze stosów należy podłączyć linkiem co najmniej 1Gbps z przełącznikiem korowym oraz oba stosy należy połączyć ze sobą linkiem 1Gbps(Zamawiający posiada światłowód wielomodowy, 6-cio włóknowy pomiędzy każdym z punktów dystrybucyjnych, a punktem głównym).
Konfiguracja klastra/stosu musi zostać wykonane po linkach co najmniej 10Gbps oraz z każdego z przełączników muszą być wykonane co najmniej dwa połączenia 10Gbps do pozostałych nodów klastra/stosu(tzw. ring).

1.2.3. Konfiguracja połączeń punktów dystrybucyjnych z przełącznikiem korowym

Wszystkie połączenia pomiędzy przełącznikami/stosem przełączników należy skonfigurować w typ trunk i przepuszczać wszystkie dostępne vlan-y na danym przełączniku.

1.3. Konfiguracja sieci

Ze względu na rozbudowę sieci LAN należy skonfigurować urządzenia i systemy według następującego opisu.

1.3.1. VLAN i adresacja

W celu zapewnienia dostępów do sieci należy skonfigurować następujące rodzaje vlan-ów(ilość vlanów, ich adresacja, ID oraz nazwa zostaną ustalone z Zamawiającym przed przystąpieniem do prac konfiguracyjnych, liczba nowych vlan-ów nie będzie jednak przekraczała 30):

- Vlan „zarządzający”, służyć ma adresacji urządzeń sieciowych w celu zapewnienia zdalnego dostępu do nich oraz możliwości ich monitorowania
- Vlany „pracownicze”, służyć mają dostępowi pracowników URZ do zasobów udostępnianych w sieci oraz Internetu
- Vlan „gościnny”, służyć ma dostępowi osób z poza URZ do dostępu do Internetu
- Vlany „pracownie”, służyć mają wyodrębnieniu sieci do obsługi sali pracowni(pomieszczeń laboratoryjnych)

1.3.2. Routing

Dla wszystkich nowo konfigurowanych sieci LAN należy skonfigurować routing według następujących zasad:

- Sieć „zarządzająca” ma być doprowadzona do firewall-a(bramą domyślną dla tej sieci ma być adres firewall-a), ruch do/z sieci ma być ograniczony za pomocą odpowiednich reguł do ruchu niezbędnego do zarządzania/monitorowania urządzeń
- Sieci „pracownicze” należy routować na przełączniku rdzeniowym(bramą domyślną dla tych sieci ma być adres IP odpowiedniego vlan-u skonfigurowany na przełączniku – istniejącym klastrze)
- Sieć „gościnna” ma być doprowadzona do firewall-a(bramą domyślną dla tej sieci ma być adres firewall-a), ruch z sieci do Internetu ma być ograniczony za pomocą odpowiednich reguł do ruchu umożliwiającego korzystania z poczty, stron WWW dla gości URZ. Ruch do/z innych sieci powinien być zablokowany i logowany.
- Sieci „pracownie” mają być doprowadzona do firewall-a(bramą domyślną dla tych sieci ma być adres firewall-a), ruch do/z sieci ma być ograniczony za pomocą odpowiednich reguł do ruchu niezbędnego do zarządzania i dostępu do Internetu

Należy również dokonać rekonfiguracji istniejących przełączników rdzeniowych i firewalli na UR w celu zapewnienia prawidłowego działania nowo tworzonych sieci np. routingu, tak aby z nowo definiowanych sieci zapewniły dostęp do udostępnianych zasobów centralnych (serwerów i systemów) tak jak w innych budynkach UR oraz Internetu.

1.3.3. Konfiguracja parametrów i portów przełącznika

Każdy z nowo dostarczonych przełączników należy skonfigurować w taki sposób, aby były spełnione następujące założenia działania sieci LAN, które funkcjonują na UR:

- Propagacja vlan-ów pomiędzy przełącznikami ma odbywać się z wykorzystaniem protokołu co najmniej GVRP
- Uruchomienie protokołu co najmniej LLDP na każdym z przełączników, w celu rozpoznawania podłączonych urządzeń
- Uruchomienie protokołu co najmniej MSTP w celu automatycznej rekonfiguracji połączeniami pomiędzy przełącznikami w przypadku awarii połączeń podstawowych
- Konfiguracja protokołów służących do zdalnego zarządzania przełącznikami co najmniej:
    - Ssh
    - https
    - SNMP
- Zabezpieczenie wszystkich portów dostępowych z wykorzystaniem co najmniej następujących mechanizmów (zabezpieczenie portów dostępowych może różnic się dla każdego z rodzajów vlan-ów do jakich będzie przypisany port):
    - Wszystkie porty dostępowe mają być skonfigurowane w trybie „access”
    - Port-security, tylko jeden adres MAC może pojawić się na porcie, w przypadku wykrycia większej liczby adresów MAC port powinien wyłączyć się automatycznie. Adresy MAC nie mają być zapamiętywane w konfiguracji urządzenia.
    - W przypadku wykrycia pakietów BPDU na porcie, port powinien zostać zablokowany tzw. „BPDU Protecion”.
    - Zabezpieczenie przed negocjacją root-a w protokole STP na każdym z portów dostępowych tzw. Root Guard
    - ochrona przed wpięciem nieautoryzowanego serwera DHCP, zablokowanie możliwości wysyłania adresów IP z urządzeń podłączonych do portów dostępowych,

- Zablokowanie możliwości używania na wyznaczonych portach dostępowych adresów statycznych. Użytkownicy podpięci do sieci mogą wykorzystywać jedynie adresy przyznane przez serwer DHCP.
- Zabezpieczenie przed nadmiernym ruchem broadcast-owym na portach dostępowych, w przypadku przekroczenia zdefiniowanych progów, ruch powinien być ograniczony lub port powinien zostać wyłączony.

- Należy skonfigurować protokół SNMP w celu monitoringu/zarządzania przełącznikami, ruch SNMP należy ograniczyć wyłącznie z/do serwerów monitorujących sieć i urządzenia
- Czas na przełącznikach należy synchronizować z serwerem czasu wskazanym przez zamawiającego

1.4. Konfiguracja serwera DHCP

Dla nowo powstałych sieci LAN w ramach wdrożenia należy dokonać rekonfiguracji posiadanego serwera DHCP. Na serwerze należy skonfigurować dodatkowe pule adresów dla poszczególnych vlan-ów, z których adresy IP będą przydzielane użytkownikom jako rozszerzenie istniejącej spójnej sieci UR.

Szczegóły adresacji sieci, zakres adresów DHCP, adres bramy domyślnej dla każdej z sieci, adresy IP serwerów DNS i innych parametrów niezbędnych do prawidłowego działania zostaną określone z Zamawiającym przed przystąpieniem do konfiguracji według tabeli:

Vlan_ID,	Adresacja sieci	Nazwa puli	Zakres adresów IP	Brama domyślna	Serwery DNS	Dodatkowe opcje

Wykonawca musi również skonfigurować wszystkie urządzenia pośrednie, aby zapytania z sieci trafiały do odpowiedniego serwera DHCP.

1.5. Rekonfiguracja Firewall-a

W ramach projektu należy dokonać rekonfiguracji posiadanego firewall-a(klaster) jako rozszerzenie spójnej ochrony sieci UR. Rekonfiguracja w szczególności będzie dotyczyć:

- Stworzenie dodatkowych wirtualnych interfejsów dla odpowiednich vlan-ów.
- Konfiguracji reguł dostępowych dla każdej z nowo powstałych sieci LAN, ograniczając ruch do niezbędnego (reguły musza być analogiczne jak dla innych sieci aby tworzyły wspólny system zabezpieczeń dla całego UR)
- Uruchomienie ochrony IPS, antywirusowej, URL filteringu dla nowo definiowanych sieci LAN w ramach jednego kompleksowego zabezpieczenia UR.
- Konfiguracja routingu dla nowo definiowanych sieci, które musza współpracować z posiadanymi innymi działającymi sieciami na UR i tworzyć integralna spójną sieć.

1.6. Konfiguracja systemu monitoringu

Nowy dostarczony sprzęt ma być monitorowany jednym z wybranym sposobów:

- nowo dostarczane przełączniki mają posiadać oprogramowanie, które zapewni monitoring/zarządzanie co najmniej w zakresie, które posiadane oprogramowanie IMC działające na UR oraz ma zostać zintegrowane z posiadanym oprogramowaniem IMC, które pozwali na centralne zarządzanie istniejącą i nowo dostarczaną infrastrukturą z zachowaniem uruchomionych już funkcjonalności.
- wykonanie integracji bezpośrednio z oprogramowaniem IMC, które UR posiada (Wykonawca wykorzysta posiadane oprogramowanie działające na UR).

Wymagania dodatkowe:

Dostarczone moduły muszą być kompatybilne oraz nie powodujące problemów serwisowych i gwarancyjnych.

2. Komputer stacjonarny do prezentacji informacji

2.1. Komputer stacjonarny do prezentacji informacji (Kiosk informacyjny) wyposażony w klawiaturę metalową, o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne szt. 6 o poniższych minimalnych parametrach:

Element	Opis wymagań minimalnych	
Obudowa	• konstrukcja wykonana z blachy stalowej • monitor odchylony od pionu pod kątem 45 stopni (+/- 5 stopni) • dostęp serwisowy realizowany od tyłu kiosku przez drzwi uchylne stalowe, zamykane zamkiem. • podstawa kiosku dwuwarstwowa stalowa, malowana proszkowo • kolorystyka dopasowana do wymagań Zamawiającego • wymagana możliwość demontażu (wymiany) wszystkich elementów poszycia kiosku bez użycia elektronarzędzi. • podświetlane logo (każdy komputer/terminal zostanie w pełni spersonalizowany poprzez polakierowanie na dowolny, wskazany przez Zamawiającego, kolor z palety, jak również umieszczenie na nim elementów identyfikacji wizualnej w formie podświetlanego logo zgodne z wymogami Zamawiającego – księga znaku). Personalizacja zostanie uzgodniona z oferentem.	
Monitor	monitor dotykowy - przekątna monitora min : 21"	
Jednostka sterująca kioskiem	Procesor	• Procesor zgodny z architekturą x64
	Pamięć RAM	• Minimum 4 GB; z możliwością rozbudowy do min. 32 GB, min. 2 wolne złącza dla rozszerzeń pamięci
	Dysk twardy	• Min. 320GB, min. 32MB Cache,
	Karta dźwiękowa	• zintegrowana
	Porty I/O	• minimum 8 portów USB min. 2.0
	Karta sieciowa	• Zintegrowana • minimum 10/100/1000 MBit/s
	Karta graficzna	• Karta graficzna zintegrowana, z możliwością dynamicznego przydzielania pamięci.
Wyposażenie dodatkowe	• wrzutnik monet • Głośniki • Czytnik kart stykowych (smartcard) zamontowany z przodu Kiosku • Klawiatura o wzmocnionej konstrukcji odpornej na uszkodzenia mechaniczne z manipulatorem kulkowym	
Zasilanie	• 230V, 50 Hz,	
Certyfikaty i dokumenty	• Deklaracja zgodności CE	

Do oferty należy dołączyć projekt (wizualizację) komputera stacjonarnego do prezentacji informacji.

a) Parametry funkcjonującego u Zamawiającego Systemu Kiosków Informacyjnych

Dostarczone kioski informacyjne należy zintegrować z istniejącym i działającym u Zamawiającego Systemem Kiosków Informacyjnych o poniższych parametrach:

System Kiosków Informacyjnych – tzw. „Infomatów" – tworzą:

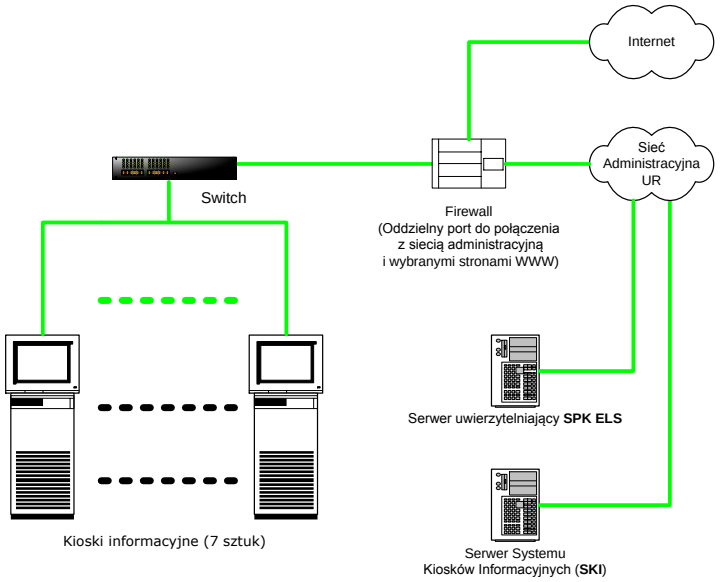
- serwer aplikacji zwany dalej serwerem Systemu Kiosków Informacyjnych (serwer SKI);
- kioski informacyjne

Serwer Systemu Kiosków Informacyjnych (SKI) znajduje się w chronionej sieci administracyjnej UR. Serwer SKI musi nawiązywać połączenia z serwerem uwierzytelniającym ELS (znajdującym się

wewnątrz sieci administracyjnej UR) oraz z wybranymi witrynami zewnętrznymi (sieć Internet i Intranet). Infomaty znajdują się w odrębnej sieci Infomatów oddzielonej od sieci Administracyjnej poprzez firewall.

Kioski Informacyjne, które zostaną dostarczone muszą współpracować z posiadanym przez Zamawiającego Systemem Elektronicznej Legitymacji Studenckiej (SELS), Systemem Elektronicznej Legitymacji Doktoranta oraz Systemem Elektronicznej Karty Pracowniczej .

Dostarczone Kioski Informacyjne muszą umożliwiać zapis, odczyt, wykorzystanie kodu PIN zapisanego w strukturach funkcjonujących u Zamawiającego kart ELS, ELD, EKP do uwierzytelniania.
Oprogramowanie Kiosku musi przygotować ELS, ELD i EKP do obsługi PKI w kioskach informacyjnych.
Oprogramowanie Kiosku umożliwi zalogowanie się użytkownika przy pomocy certyfikatu (PKI).
Oprogramowanie Kiosku musi mieć możliwość obsługi Bezobsługowego Centrum Wydruku - BCW (m.in. ładowanie impulsów na karty ELS, ELD, EKP)



Rys. Schemat ideowy Systemu Kiosków Informacyjnych

b) Oprogramowanie do nowych dostarczanych kiosków informacyjnych:

1	Kiosk informacyjny musi posiadać sterowniki do obsługi czytnika kart elektronicznych zgodnych z normą ISO/IEC 7816 lub równoważną oraz standardem PC/S.C. lub równoważnym, a w szczególności legitymacji ELS o specyfikacji zgodnej z rozporządzeniem Ministerstwa Szkolnictwa Wyższego - Dziennik Ustaw z dnia 8 grudnia 2006 r. (Nr 224, poz. 1634) Rozporządzenie wydano na podstawie art. 192 ust. 1 ustawy z dnia 27 lipca 2005 r. -Prawo o szkolnictwie wyższym.
2	Kiosk informacyjny musi autoryzować i uwierzytelniać użytkownika na podstawie danych zapisanych w specjalnej, przewidzianej do tego strukturze danych przechowywanej na legitymacji ELS lub przy pomocy logowania z hasłem, umożliwiające dostęp do stron zawierających dane osobiste, które mogą pochodzić z innych systemów uczelnianych (np. systemu dziekanatowego lub bibliotecznego).
3	Kiosk informacyjny musi obsługiwać procesorowe karty serwisowe, umożliwiające konfigurację serwisu informacyjnego kiosku przy pomocy stron WWW.
	Powłoka użytkownika (shell) oprogramowania kiosku musi być wykonana

	w postaci aplikacji wykonanej w technologii „cienkiego klienta", współpracująca z dedykowaną bazą danych, umożliwiającą tworzenie kont użytkowników i zarządzanie ich uprawnieniami, przechowywanie indywidualnej konfiguracji kiosków, itp.
	Inne funkcje oprogramowania kiosku informacyjnego
5	Autoryzacja użytkownika musi odbywać się na podstawie legitymacji ELS z kodem PIN lub w oparciu o login i hasło. Niedopuszczalne jest autoryzowanie użytkownika na podstawie jedynie numeru numeru seryjnego karty ELS. W przypadku braku karty ELS w czytniku Infokiosku lub gdy użytkownik nie zalogował się za pośrednictwem Infokiosku wymagane jest ograniczenie dostępu użytkownika jedynie do: - strony głównej (wraz z podstronami); - rozkładów jazdy PKP, PKS, etc.; - innych witryn włączanych sukcesywnie przez administratora ze strony Zamawiającego do grupy witryn nie wymagających autoryzowanego dostępu. Oprogramowanie musi także mieć możliwość zastosowania struktury PKI (Infrastruktury Klucza Publicznego) do uwierzytelniania.
6	Kiosk informacyjny musi zapewnić automatyczne wylogowanie użytkownika (przejście do strony głównej systemu) w przypadku: - wyjęcia karty ELS z czytnika; - utraty połączenia z serwerem kiosków informacyjnych (wyświetlenie stosownego komunikatu dla użytkownika); - przekroczenia limitu czasu bezczynności (określanego przez administratora systemu w zakresie od 1 minuty do 60 minut z krokiem 1 minuta).
7	Kiosk informacyjny musi pozwalać na cykliczne odświeżanie konfiguracji programowej urządzenia, rozumiane jako zdalne załadowanie parametrów konfiguracyjnych dla przeglądarki internetowej działającej na kiosku w charakterze klienta.
8	Kiosk informacyjny musi pozwalać na ochronę kiosku poprzez restrykcje systemowe (blokowanie możliwości uruchamiania wskazanych aplikacji).
9	Kiosk informacyjny musi pozwalać na obsługę klawiatury ekranowej dostosowanej do ekranów dotykowych (duże przyciski), umożliwiającej jedynie wprowadzanie tekstów, z zablokowaną możliwością wykonywania funkcji sterujących (skrótów klawiszowych).
10	Kiosk informacyjny musi pozwalać na aktywowanie klawiatury ekranowej poprzez ustawienie kursora w polu edycji lub poprzez wywołanie dedykowanym przyciskiem.
11	Kiosk informacyjny musi pozwalać na obsługę modułów bezpieczeństwa
12	Kiosk informacyjny musi pozwalać na zapisywanie danych na kartach procesorowych, które są zabezpieczone kluczami 3DES (również kluczami zdywersyfikowanymi 3DES). Powinno także pozwalać na poszerzanie funkcjonalności karty poprzez tworzenie dodatkowych struktur danych na karcie.
13	Kiosk informacyjny musi pozwalać na przechowywanie kluczy 3DES w bezpiecznym magazynie chronionym.
System operacyjny infokiosku	
Platforma	Infokiosk musi mieć zainstalowany 64 bitowy system operacyjny. System operacyjny (klasy PC) musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek; Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu; 1. Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet

	(niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW; 2. Internetowa aktualizacja zapewniona w języku polskim; 3. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6; 4. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe; 5. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi) 6. Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer 7. Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 8. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu; 9. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 10. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 11. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 12. Funkcje związane z obsługą komputerów typu TABLET PC, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 13. Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się" głosu użytkownika. 14. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 15. Wbudowany system pomocy w języku polskim; 16. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących); 17. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji; 18. Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny; 19. Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509; 20. Wsparcie dla logowania przy pomocy smartcard; 21. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji; 22. System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk; 23. Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 – możliwość uruchomienia aplikacji działających we wskazanych środowiskach; 24. Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń; 25. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem; 26. Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz

	z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową; 27. Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację; 28. Graficzne środowisko instalacji i konfiguracji; 29. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe; 30. Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe 31. Udostępnianie modemu; 32. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej; 33. Możliwość przywracania plików systemowych; 34. System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.) 35. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).

c) Dostawa, instalacja, montaż, szkolenie

W ramach dostawy należy:

- wykonać montaż kiosków w miejscu wskazanym przez Zamawiającego
- wykonać instalację urządzeń wraz z infrastrukturą potrzebną do ich uruchomienia (kable połączeniowe i zasilające, podłączenie do istniejących PEL)
- wykonać instalację i konfigurację oprogramowania systemowego i oprogramowanie zarządzająco - sterującego
- przeprowadzić bezpłatnie szkolenie w zakresie obsługi urządzenia i zainstalowanego oprogramowania dla administratorów
- przygotować instrukcję obsługi dotyczącą eksploatacji kiosku i postępowania w przypadku awarii, instrukcja musi być wydana w języku polskim
- przygotować instrukcję dotyczącą konfiguracji oprogramowania, instrukcja musi być wydana w języku polskim
- umożliwić dokonywanie zmian konfiguracji przez Zamawiającego

2.2. Komputer stacjonarny do prezentacji informacji (Info TV) szt. 1 o poniższych minimalnych parametrach:

- **Monitor o parametrach nie gorszych niż:**

- przekątna ekranu min. 55 cali
- technologia podświetlania LED
- czas reakcji matrycy: max. 8ms (grey-to-grey)
- rozdzielczość obrazu co najmniej 1920 x 1080 pikseli, FullHD
- głośniki
- kąt widzenia poziomy min. 178 stopni
- kąt widzenia pionowy min. 178 stopni
- złącza co najmniej: HDMI, DVI-D, D-Sub, 1 x RJ-45, USB 2.0, AV
- montaż na ścianie
- możliwość zabezpieczenia (Kensington)

-kabel HDMI do podłączenia z serwerem

-możliwość zdefiniowania czasu pracy monitora w zakresie godzinnym w ciągu wybranych dni tygodnia

-zestaw montażowy umożliwiającym pochylenie w pionie i w poziomie min. 15 stopni.

- **Serwer pod instalację aplikacji wraz z serwerowym systemem operacyjnym o parametrach nie gorszych niż:**

PŁYTA GŁÓWNA: obsługująca poniższy procesor
PROCESOR: Procesor osiągający wynik co najmniej 5000 pkt. w teście procesorów w kategorii PassMark CPU Mark, według wyników opublikowanych na stronie http://www.cpubenchmark.net w dniu 09.09.2014r. W przypadku użycia przez Wykonawcę innych testów wydajności Zamawiający zastrzega sobie, iż w celu sprawdzenia poprawności przeprowadzonych testów Wykonawca musi dostarczyć Zamawiającemu oprogramowanie testujące, testowany zestaw oraz dokładne opisy użytych testów wraz z wynikami w terminie nie dłuższym niż 3 dni od otrzymania zawiadomienia od Zamawiającego.
· PAMIĘĆ: min. 8 GB,
· DYSK: min. 320GB, 16MB cache,
· Zintegrowana karta sieciowa co najmniej 10/100/1000
· Karta graficzna: min. 512 MB, wymagane złącza zewnętrzne: min. 1xVGA, min. 1xDVI-I, min. 1xHDMI
· OBUDOWA: Desktop lub SFF
· Klawiatura
· Mysz optyczna,
· Zestaw montażowy dający możliwość naściennego lub podsufitowego montażu serwera,
· Serwerowy system operacyjny o min. wymaganiach:
Licencja na oprogramowanie musi być przypisana do każdego procesora fizycznego na serwerze. Liczba rdzeni procesorów i ilość pamięci nie mogą mieć wpływu na liczbę wymaganych licencji. Licencja musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym i dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji.
Serwerowy system operacyjny (SSO) typ I musi posiadać następujące, wbudowane cechy:

1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym
2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny.
3. Możliwość budowania klastrów składających się z co najmniej 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych.
4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading.
9. Wbudowane wsparcie instalacji i pracy na wolumenach, które:
    a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
    b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
    c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,
    d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.

11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        i. Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,
        ii. Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,
        iii. Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.
    c. Zdalna dystrybucja oprogramowania na stacje robocze.
    d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:
        i. Dystrybucję certyfikatów poprzez http
        ii. Konsolidację CA dla wielu lasów domeny,
        iii. Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.
    f. Szyfrowanie plików i folderów.
    g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
    h. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
    i. Serwis udostępniania stron WWW.
    j. Wsparcie dla protokołu IP w wersji 6 (IPv6),
    k. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach
    z systemem Windows,
    l. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla:

i. Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,
ii. Obsługi ramek typu jumbo frames dla maszyn wirtualnych.
iii. Obsługi 4-KB sektorów dysków
iv. Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra
v. Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API.
vi. Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model)

23. Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
27. Możliwość zarządzania co najmniej przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
28. Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

b) Dostawa, instalacja, montaż:
Wymagania wdrożeniowe
Wykonawca będzie zobowiązany do wykonania następujących prac wdrożeniowych:
- instalacja serwera pod instalację aplikacji wraz z monitorem oraz z infrastrukturą potrzebną do jego uruchomienia (kable połączeniowe, zasilające, itp.).

3. Rozbudowa sieć bezprzewodowej

Punkty dostępowe – sztuk 32 o parametrach:
- wspierające technologię transmisji danych z wykorzystaniem min. standardów a/g/n
- być dostarczone z elementami umożliwiającymi jego prawidłowy montaż na ścianie/sufit
- muszą być wyposażone w zintegrowane anteny co najmniej:
  - 2.4 GHz, Gain 4 dBi, internal Omni, horizontal beamwidth 360°
  - 5 GHz, Gain 3 dBi, internal Omni, horizontal beamwidth 360°
- Posiadać interfejsy co najmniej:
  - 10/100/1000BASE-T autosensing (RJ-45)
  - Zarządzający port konsoli (RJ-45)
- Być wyposażony w wskaźnik/diodę informujący co najmniej:
  - Statusie bootowania
  - Statusie podłączenia do kontrolera,
  - Statusie pracy
- Pracować w temperaturze co najmniej od 0 do 40 stopni C
- Być wyposażone w min. 128 MB DRAM i min. 32 MB flash
- Posiadać możliwość zasilania co najmniej:
  - Portu przełącznika działającego w technologii 802.3af
  - Z modułu Power Injector
  - Z zasilacza
- Wspierać prędkości pracy co najmniej:
  - 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps
  - 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps
  - Do 300Mbps dla technologii “802.11n”
- Być zgodne ze standardami bezpieczeństwa co najmniej:
  - UL 60950-1

    - CAN/CSA-C22.2 No. 60950-1
    - UL 2043
    - IEC 60950-1
    - EN 60950-1
- Zgodność ze standardami radiowymi co najmniej:
    - FCC Part 15.247, 15.407
    - EN 300.328, EN 301.893 (Europe)
    - EMI and susceptibility (Class B)
    - FCC Part 15.107 and 15.109
    - EN 301.489-1 and -17 (Europe)
- Zgodność ze standardami IEEE co najmniej:
    - IEEE 802.11a/b/g, IEEE 802.11n 2.0, IEEE 802.11h, IEEE 802.11d
- Zgodność ze standardami bezpieczeństwa sieci bezprzewodowych co najmniej:
    - 802.11i, Wi-Fi Protected Access 2 (WPA2), WPA
    - 802.1X
    - Advanced Encryption Standards (AES), Temporal Key Integrity Protocol (TKIP)
- Wspierać standard EAP, co najmniej:
    - Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
    - EAP-Tunneled TLS (TTLS) or Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2)
    - Protected EAP (PEAP) v0 or EAP-MSCHAPv2
    - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
    - PEAPv1 or EAP-Generic Token Card (GTC)

Dostarczane punkty dostępowe muszą być wspierane i zarządzane z posiadanego przez Zamawiającego kontrolera.
Obecnie wykorzystywany jest kontrolery:

- Producent: Cisco
- Modele z serii 4400 oraz 5508

Dodatkowo w celu podłączenia nowo dostarczonych punktów dostępowych do istniejącego kontrolera Cisco 4400 z obsługą 100 Access-Point-ów należy dostarczyć roczne wsparcie producenta urządzenia świadczone w reżimie 8 godzin, 5 dni w tygodni z czasem reakcji w następnym dniu roboczym od zgłoszenia awarii.
W ramach zadania należy rozbudować sieć bezprzewodową o dostarczone elementy oraz dokonać rekonfiguracji sieci zgodnie z wymogami opisanymi poniżej.
Zamawiający będzie mógł bezpośrednio i samodzielnie ściągać ze strony producenta aktualizacje oprogramowania oraz zgłaszać awarie na stronie producenta.
Punkty dostępowe należy podłączyć do sieci LAN, do vlanu wskazanego przez Zamawiającego, w którym funkcjonują istniejące punkty dostępowe w innych budynkach. Należy wykonać konfigurację portów dostępowych przełączników do których będą podpinane urządzenia, jak również podłączyć punkty dostępowe do posiadanych przez UR kontrolerów. Efektem końcowym wykonywanych prac w zakresie podłączenia i konfiguracji punktów dostępowych ma być rozgłaszana sieć dostępowa ("eduroam") pozwalająca uzyskać pełną funkcjonalność dostępną na innych budynkach UR.

Konfiguracja sieci bezprzewodowej
W ramach konfiguracji należy wykonać następujące zadania:

- Wykonać aktualizacje istniejących kontrolerów do najnowszej dostępnej wersji oprogramowania z zachowaniem pełnej funkcjonalności obecnie wykorzystywanej.
- Dokonać konfiguracji dostarczonych punktów dostępowych aby uzyskać funkcjonalności dokładnie takie same jak na obecnie posiadanych i działających punktach dostępowych, w szczególności:

- Wykonać integracje z systemem personalizacji legitymacji studenckich i pracowniczych użytkowanym przez Zamawiającego polegającą na automatycznym zakładaniu kont i haseł do autoryzacji w dostępie do sieci bezprzewodowej
- Stworzenie sieci dostępowych, które będą kompatybilne i zapewniające bezproblemową współpracę z działającymi na innych obiektach Uniwersytetu Rzeszowskiego sieciami umożliwiającymi obsługę pracowników i studentów w zakresie dostępu do udostępnionych zasobów sieciowych jak i Internetu
- Wszystkie nowo instalowane punkty dostępowe należy podłączyć do kontrolera, na AP-tach skonfigurować statyczne adresy obu kontrolerów w celu szybkiego przełączenia w przypadku awarii jednego z kontrolerów.

4. Zasilacz awaryjny sztuk 10 spełniający poniższe wymagania:

Moc pozorna min. 5000 VA
Moc rzeczywista min. 4500 W
Współczynnik mocy min. 0,9
Czas przełączenia na baterię max. bez zwłoki
Możliwość pracy równoległej
Liczba, typ gniazd wyjściowych: co najmniej 8 x Gniazdo IEC w tym 2 grupy po 4 x IEC C13 zdalnie sterowane, 2 gniazda IEC C19 16A + listwa zaciskowa wejście/wyjście
Typ gniazda wejściowego co najmniej: zaciski
Czas podtrzymania dla 100% obciążenia dla pf=0,9 min. 3,5 min
Czas podtrzymania przy 50% obciążenia dla pf=0,9 min. 11 min
Możliwość dodania co najmniej 12 dodatkowych modułów baterii. W celu wydłużenia czasu podtrzymania do min. 240 minut dla 100% obciążenia przy pf=0,9
Napięcie znamionowe: 230 V / 200/208/220/240 V
Częstotliwość znamionowa min. w zakresie 50/60 Hz autodetekcja
Tolerancja częstotliwości min. w zakresie 40 – 70 Hz
Sinusoidalny kształt napięcia
Napięcie znamionowe wyjściowe 230 V (domyślnie) / 200/208/220/240 V
Zakres zmian napięcia +/-1% napięcia nominalnego
Częstotliwość wyjściowa 50/60 Hz +/-0,5%
Współczynnik szczytu min. 3:1
Baterie wymieniane przez użytkownika "na gorąco"
Ochrona przed przeładowaniem
Ochrona przed głębokim rozładowaniem
Okresowy automatyczny test baterii
System nieciągłego ładowania baterii. Zdolność zwarciowa 90 A
Zimny start
Baterie wewnętrzne o pojemności co najmniej15 x 5 Ah/12V
Czas ładowania baterii do poziomy 90% do max. 1,5 godziny do 90% pojemności użytkowej
Interfejs komunikacyjny co najmniej:

- USB
- RS232 DB-9
- slot na kartę sieciową

Wyświetlacz dostarczający informacji co najmniej: stanie pracy urządzenia, stanie obciążenia, zdarzeniach, pomiarach i ustawieniach.
Przyciski sterowania co najmniej, Wskaźniki stanu: min. trubu online, trybu bateryjnego, trybu bypasas, usterki, Sygnalizator akustyczny (sygnały akustyczne: Awaria, Niski stan naładowania baterii, Przeciążenie, Serwis)
Przyciski sterujące i wskaźniki co najmniej:

- Przycisk anulowania
- Przyciski funkcyjne (przewijanie w górę i w dół)
- Przycisk Enter (potwierdzający)
- Przycisk ON/OFF załączenia i wyłączenia
- Wskaźniki trybu online, trybu baterii, trybu bypass, usterki

Obudowa uniwersalna Tower/Rack (max. 3U)

Wyposażenie co najmniej:

- zestaw do montażu w szafie Rack
- karta SNMP
- kabel RS232
- kabel USB
- oprogramowanie do zarządzania UPS-em na płycie CD lub nośniku USB
- uchwyty kablowe
- podstawki do montażu pionowego (wieża)
- instrukcja obsługi

Dołączone oprogramowanie do bezpiecznego zamykania systemów operacyjnych używanych przez Zmawiającego przy wyczerpaniu baterii (minimum: Windows: 2000, XP, 2003, Vista, Server 2008, 7; Linux, VMware ESX;). Oprogramowanie pozwalające na integrację z platformą wirtualizacyjną Vmware: vCenter Server, którą posiada (wykorzystuje) Zamawiający. Dostarczane urządzenie ma być wyposażone w możliwość komunikacji z zabezpieczanymi przez nie systemami komputerowymi, serwerami z wykorzystaniem portu co najmniej USB lub RS232 lub systemu komunikacji sieciowej Ethernet.
Obejście elektroniczne, automatyczne i mechaniczne.
Możliwość montażu ręcznego obejścia serwisowego

Oferowane UPS-y należy zamontować, podłączyć i skonfigurować według wskazań Zamawiającego.

Opis minimalnych wymagań dotyczących pozycji nr 2:

1. Wykonawca w ramach realizacji przedmiotu zamówienia zobowiązany jest do wykonania koniecznych robót instalacyjnych w szczególności:
   a) związanych z ułożeniem kabli strukturalnych
   b) związanych z montażem gniazd RJ-45
2. Ułożeniu kabli strukturalnych i montażu gniazd mogą towarzyszyć roboty dodatkowe tj. przebicia przez ściany, ułożenie kanałów kablowych dwukomorowych umożliwiających zabudowę na nich gniazd 2xRJ-45, wykonanie drobnych prac malarskich po wykonaniu robót budowlanych.
3. Należy przewidzieć ułożenie i zarobienie kabli oraz zamocowanie i przyłączenie do szaf dystrybucyjnych
4. W przypadku niewystarczającej ilości miejsc w istniejących szafach dystrybucyjnych należy przewidzieć możliwość rozbudowy szaf poprzez dobudowę nowych szaf do już istniejących. Na załączonych rysunkach od 28 do 36 oraz 6 przedstawiono lokalizację gniazd RJ-45.
5. Dodatkowe wymagania:
   a) Załączony przedmiar stanowi materiał pomocniczy. Przed przystąpieniem do przetargu zaleca się wykonanie wizji lokalnej przez Wykonawcę.
   b) Wykonawca opracuje dokumentację powykonawczą w 4 egzemplarzach.