

**Załącznik nr 3 do Protokołu dialogu technicznego z dnia 17.11.2020 r. Komisji
Przetargowej Grupy Zakupowej eCareMed**

Koncepcja budowy sieci wymiany informacji – 11 zestawów

Uproszczony przebieg procesów platformy rozproszonej

ZSI wytwarza dokumentację medyczną w tym EDM. BOSK (Bramka do Oprogramowania Serwera Komunikacyjnego) komunikuje się z ZSI (Zintegrowany System Informacyjny) i przekazuje dane do i z OSK (Oprogramowanie Serwera Komunikacyjnego). OSK działa w jednolitej sieci wymiany informacji umożliwiającej stworzenie rozproszonej platformy sieciowej opartej o internet oraz zaawansowane rozwiązania typu „każdy z każdym”. Komunikacja prowadzona będzie zgodnie z HL7 CDA, dane obrazowe przekazywane będą w standardzie DICOM. OSK komunikuje się z: ZSI poprzez BOSK, systemem P1 zgodnie z unikalnym OID (rejestr węzłów prowadzony przez CEZ), innymi jednostkami zdrowia oraz z pacjentem. OSK zapewni świadczenie e-usług na poziomie regionalnym.

1. Warstwa transportu.

Zamawiający wymaga dostarczenia rozwiązania technologicznego zapewniającego bezpieczną komunikację pomiędzy oddziałami uczestniczącymi w projekcie wymiany informacji o stanie zdrowia pacjentów.

Wymagane jest, aby wszystkie komponenty w zakresie sprzętu (hardware) jak i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,
- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili otwarcia zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dotykowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywania problemów technicznych,

Przedmiotowe rozwiązanie musi składać się z następujących elementów:

- urządzenia brzegowe (routery lub firewalle) zapewniające możliwość podłączenia środowiska serwerowego w lokalizacji do sieci rozległej,

Przedmiotowe rozwiązanie musi zapewniać możliwość wykorzystania dowolnego typu łącz sieciowych opartych o protokół IP a w szczególności:

- Internet,
- MPLS,

- Linie dzierżawione,

w celu realizacji połączeń pomiędzy lokalizacjami w trybie „każdy z każdym” (full mesh). Przedmiotowe połączenia muszą być szyfrowane z wykorzystaniem protokołów co najmniej TLS, DTLS czy IPsec. Nie dopuszcza się rozwiązań opartych wyłącznie o protokoły SSL.

Rozwiązanie musi zapewniać monitoring, telemetrię jak i możliwość konfiguracji parametrów jakościowych transmisji aktywnych połączeń.

Wymaga się aby dostępne były urządzenia brzegowe dedykowane obsłudze ruchu sieciowego w zakresie od 100 Mbps do 1 Gbps co pozwoli na instalację odpowiednich urządzeń, dostosowanych do potrzeb poszczególnych lokalizacji (uczestniczących w projekcie) bez konieczności ponoszenia nieuzasadnionych wydatków.

Urządzenia brzegowe (routery lub firewalle) muszą spełniać następujące kryteria:

- wydajność dla transmisji ruchu szyfrowanego IPsec (AES-256, SHA256) min. 1 Gbps,
- jeśli kwestia wydajności wiąże się z stosowną licencją Zamawiający wymaga zapewnienia minimum 100 Mbps dla ruchu szyfrowanego na początkowym etapie projektu,
- min. 4 interfejsy gigabitethernet,
- obsługa technologii agregacji linków w wykorzystaniem co najmniej protokołu LACP,
- dostęp do urządzenia poprzez webgui, ssh oraz „serial console”,
- możliwość wylistowania aktywnej konfiguracji urządzenia z poziomu ssh i wyeksportowanie w postaci pliku tekstowego,
- wsparcie dla protokołów routingu statycznego jak i dynamicznego (co najmniej OSPF, BGP)
- obsługa wirtualnych tablic routingu, osobnej dla prefixów warstwy połączeń fizycznych jak i osobnej dla połączeń logicznych dedykowanych transmisji danych produkcyjnych,
- wsparcie dla technologii kryptograficznej w oparciu o TLS, DTLS, IPsec,
- wsparcie dla mechanizmów QoS umożliwiających priorytetyzację ruchu dla poszczególnych klas,
- możliwość rozpoznawania ruchu na poziomie aplikacji i definiowania na ich podstawie polityk QoS ,

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refurbished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

2. Warstwa bezpieczeństwa.

Zamawiający wymaga dostarczenia rozwiązania technologicznego zapewniającego mechanizmy bezpieczeństwa w ruchu sieciowym pomiędzy poszczególnymi segmentami środowiska serwerowego jak i od strony użytkownika końcowego. Opisywane rozwiązanie jest dedykowane dla pojedynczej lokalizacji biorącej udział w projekcie.

Wymagane jest aby wszystkie komponenty w zakresie sprzętu (hardware) jak i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,
- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili otwarcia zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dodatkowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie prawa do aktualizacji sygnatur AntyMalware oraz IPS (intrusion protection),
- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywania problemów technicznych,

Przedmiotowe rozwiązanie musi składać się z następujących elementów:

- Zestaw urządzeń klasy NGFW (Next Generation Firewall) złożony z co najmniej dwóch jednostek mogących pracować w układzie co najmniej Active-Standby,
- Stosownych licencji jak i subskrypcji zapewniających realizację niżej wymienionych funkcjonalności.

oraz spełniać poniższe kryteria:

- co najmniej 10 interfejsów gigabitethernet z czego min 4 definiowane poprzez SFP. Interfejsy 10G z obsługą 1G są na równi traktowane z 1G.
- możliwość definiowania interfejsów logicznych w użyciu technologii vlan tagging oraz interfejsów zagregowanych w wykorzystaniem protokołu LACP,
- minimalna wydajność systemu to 1 Gbps dla ruchu z włączoną obsługą mechanizmów firewall, IPS, Application Control, Antimalware Protection oraz aktywnym logowaniem ruchu,
- minimum 100 000 sesji jednoczesnych,
- minimum 10 000 nowych sesji na sekundę,

- możliwość zdefiniowania wirtualnych systemów (min.4) będących logicznymi instancjami firewall'a,
- możliwość zdefiniowania min. 4 odrębnych tablic routingu,
- obsługa protokołów routingu dynamicznego co najmniej OSPF, BGP,
- obsługa protokołów IPSec, TLS,
- wsparcie dla Network Address Translation,
- możliwość zdefiniowania co najmniej 2 000 polityk bezpieczeństwa,
- możliwość logowania ruchu przechodzącego przez firewall w postaci – otwarcie, zamknięcie sesji, ilość danych przesłana w jedną i drugą stronę, akcja - permit/deny/drop/reject, widok źródła, destynacji, interfejsów (zone) źródłowych, docelowych, protokołów/portów, aplikacji
- możliwość definiowania polityk bezpieczeństwa z użyciem:
 - kont użytkowników, strefa bezpieczeństwa, podsieć jako warunki źródłowe
 - aplikacja, strefa bezpieczeństwa, podsieć, protokół/port jako warunki docelowe,
 - mechanizmy bezpieczeństwa w postaci inspekcji antymalwarowej przesyłanych plików,
 - mechanizmy bezpieczeństwa w postaci inspekcji oraz przeciwdziałaniu włamaniom (IPS),

System do kolekcji oraz archiwizacji logów z ruchu sieciowego przechodzącego przez firewallo powinien być zrealizowany jako dedykowane urządzenie (tzw. appliance) dla każdej z lokalizacji uczestniczących w projekcie. System powinien zapewniać obsługę i wykrywanie zagrożeń oraz reagowanie na incydenty związane z zagrożeniem bezpieczeństwa w zakresie sieci komputerowej oraz systemów OSK i BOSK.

Dopuszcza się realizację kolektora logów w wersji centralnej (jednego dla wszystkich lokalizacji) jednakże w tym wypadku wymagana jest architektura wysokiej dostępności.

Centralny kolektor logów musi być uruchomiony jako tzw. appliance (w DC w trybie kolokacji) lub jako maszyny wirtualne do uruchomienia na infrastrukturze zapewnionej przez Wykonawcę w DC na terenie Polski w trybie as-a-service. Zamawiający nie dopuszcza wersji chmurowej (tzw. Public Cloud) dla Centralnego Kolektora Logów.

Wykonawca musi zapewnić urządzenia warstwy transportu, bezpieczeństwa jako redundantnych połączeń do sieci Internet (min. 1Gbps) do dodatkowego węzła w przedmiotowym DC.

Wymaga się, aby przedmiotowy system umożliwiał kolekcję logów z ruchu sieciowego (traffic log) na okres co najmniej 12 miesięcy. Rozwiązanie musi oferować graficzny interfejs użytkownika oferujący podgląd bieżących logów, wyszukiwanie przynajmniej na podstawie kryteriów takich jak:

- source/destination IP
- source/destination port
- action deny/permit

- security policy
- application
- przedział czasowy
- interfejs

oraz tworzenie raportów czy statystyk.

Wszystkie powyższe komponenty muszą pochodzić od jednego producenta i być objęte jego wsparciem technicznym.

Z uwagi na konieczność zachowania powtarzalności oraz spójności konfiguracji (na etapie eksploatacji) przedmiotowych urządzeń wymaga się, aby zapewniony został również Centralny System Zarządzania oferujący przynajmniej następujące funkcje:

- możliwość konfigurowania poszczególnych urządzeń z użyciem wspólnej bazy obiektów (adresy, sieci, usługi, aplikacje),
- wersjonowanie konfiguracji,
- przydzielanie administratorom uprawnień do poszczególnych urządzeń,
- rejestrowanie zmian w konfiguracji urządzeń,
- możliwość backup pojedynczych urządzeń oraz zdefiniowanych grup urządzeń

Centralny System Zarządzania musi być zrealizowany jako dedykowane urządzenia do instalacji w zapewnionym przez Wykonawcę DC na terenie Polski w trybie kolokacji. Wymaga się zapewnienia wysokiej dostępności w przypadku rozwiązania bazującego na urządzeniach fizycznych. Alternatywą jest uruchomienie jako maszyny wirtualne na infrastrukturze zapewnionej przez Wykonawcę w DC na terenie Polski w trybie as-a-service.

Wykonawca musi zapewnić urządzenia warstwy transportu, bezpieczeństwa jak i redundantnych połączeń do sieci Internet (min. 1Gbps) do dodatkowego węzła w przedmiotowym DC.

Zamawiający nie dopuszcza wersji chmurowej (tzw. Public Cloud) dla Centralnego Systemu Zarządzania.

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refurbished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

3. Warstwa dostępowa dla podmiotów trzecich.

Zamawiający wymaga dostarczenia i wdrożenia rozwiązania klasy WAF (Web Application Firewall) odpowiedzialnego za ochrony aplikacji webowej udostępniającej dane podmiotom trzecim (nieuczestniczącym bezpośrednio w projekcie) za pośrednictwem sieci Internet.

Niniejsze rozwiązanie ma być dostarczone jako dedykowany sprzęt (tzw. appliance) wraz z stosownymi licencjami oraz subskrypcjami (jeśli wymagane) na okres min. 5 lat dla realizacji niżej wymienionych funkcjonalności:

- Wsparcie dla min. 5 serwerów obsługiwanych przez WAF (tzw. backend)
- Wydajność min. 50 Mbps,
- Wydajność transakcji HTTPS/SSL – min. 1000/sek,
- Autentykacja dla dostępu administracyjnego co najmniej poprzez LDAP,
- Możliwość definiowania różnych poziomów dostępu dla administratorów,
- SSL offloading,
- Możliwość pracy w układzie active/standby, active/active
- Detekcja i ochrona przed automatycznymi atakami (BOT),
- Możliwość definiowania granularnych białych list
- Analiza ruchu i ochrona przed atakami typu odmowa usługi (DOS)
- Maskowanie danych identyfikacyjnych backend serwerów poprzez blokowanie odpowiedzi typu „kod błędu”, „http header”, „return code” itd.,
- Mechanizmy ochrony przed atakami OWASP top 10,
- Monitoring „życia” backend serwera poprzez cykliczne wysyłanie żądań do aplikacji, pakiety icmp,
- Analiza i raportowanie w zakresie ataków z listy OWASP top 10,
- Możliwość integracji z zewnętrznymi systemami poprzez REST API oparte na standardach JSON,
- Inspekcja danych wychodzących pod kątem wycieku danych (tzw. DLP) z możliwością usuwania czy maskowania wrażliwych danych (w oparciu o zdefiniowane wzorce), logowanie oraz raportowanie zaistniałych zdarzeń w tego obszaru.
- Obsługa uwierzytelnienia w oparciu o następujące metody:
 - SAML v2 dla „web based single-sign-on (SSO),
 - Weryfikacja certyfikatu klienta,
 - Integracja z Active Directory, LDAP, Active Directory Federation Services,
 - Współpraca z systemami podwójnego uwierzytelnienia (tzw. Two-Factor-Authentication” takimi jak RSA Secure ID czy DUO Security).
- Możliwość eksportu logów (client request, admin access, firewall traffic log) poprzez protokół syslog oraz FTP,

Wymagane jest, aby wszystkie komponenty w zakresie sprzętu (hardware) jak i oprogramowania (software) przedmiotowego rozwiązania pochodziły od jednego producenta i były objęte wsparciem technicznym producenta na okres min 60 m-cy od daty odbioru, zapewniającym:

- przyjmowanie zgłoszeń serwisowych w trybie 24x7,
- wymianę uszkodzonych podzespołów/urządzeń na nowe w czasie nie dłuższym niż na następny dzień roboczy licząc od chwili otwarcia zgłoszenia serwisowego, dostawa musi być wykonana do miejsca instalacji sprzętu (w różnych lokalizacjach na terenie województwa śląskiego), bez ponoszenia jakichkolwiek dotykowych opłat przez Zamawiającego,
- zapewnienie prawa do aktualizacji oprogramowania w okresie trwania wsparcia,
- zapewnienie wsparcia technicznego ze strony producenta w zakresie rozwiązywania problemów technicznych,

Zamawiający dopuszcza rozwiązanie centralne dla niniejszego systemu jako:

- Układ urządzeń (tzw. appliance) w układzie wysokiej dostępności do jako dedykowane urządzenia do instalacji w zapewnionym przez Wykonawcę DC na terenie Polski w trybie kolokacji lub
- jako maszyny wirtualne do uruchomienia na infrastrukturze zapewnionej przez Wykonawcę w DC na terenie Polski w trybie as-a-service.

W takiej sytuacji Wykonawca musi zapewnić urządzenia warstwy transportu jak i bezpieczeństwa do dodatkowego węzła w przedmiotowym DC.

Rozwiązanie centralne musi charakteryzować się minimalną wydajnością:

- Wsparcie dla min. 50 serwerów obsługiwanych przez WAF (tzw. backend),
- Wydajność min. 500 Mbps,
- Wydajność transakcji HTTPS/SSL – min. 10000/sek.

Wymaga się aby „Warstwa dostępowa dla podmiotów trzecich” nie była zrealizowana za pomocą tych samych rozwiązań co Warstwa Transportowa czy Bezpieczeństwa.

Wszystkie komponenty przedmiotowego rozwiązania muszą pochodzić z oficjalnego kanału dystrybucyjnego na terytorium Polski. Urządzenia muszą być nowe, nie używane w innych projektach, nie dopuszcza się urządzeń po renowacji (refurbished).

Licencje na oprogramowanie dostarczone w ramach niniejszego rozwiązania muszą być zarejestrowane na Zamawiającego.

Urządzenia muszą być dostosowane do zasilania napięciem przemiennym 230V, 50Hz. Kable zasilające muszą być przystosowane do powszechnie używanych w Polsce gniazd zasilających.

4. Wymagania dla Wykonawcy.

Wykonawca jest zobowiązany:

- Dostarczyć wszystkie wymaganych komponentów zarówno sprzętowych jak i programowych do miejsca instalacji,
- Wykonać konfigurację rozwiązania tak aby zapewnić minimalny, wymagany poziom funkcjonalności zdefiniowany przez Koordynatora Projektu ze strony Zamawiającego,
- Opracować dokumentację rozwiązania zawierającą schematy sieci w ujęciu L2 oraz L3, opis kluczowych komponentów rozwiązania oraz zestaw procedur utrzymaniowych,
- Przeprowadzić instruktaż personelu technicznego Zamawiającego (od 6 do 12 osób) z zakresu obsługi rozwiązania,
- Zapewnić wsparcie techniczne w trakcie pierwszego roku po przekazaniu rozwiązania Zamawiającemu w wymiarze co najmniej 40 roboczogodzin w ujęciu miesięcznym, szczególnie w zakresie implementacji zmian w konfiguracji oraz rozwiązywaniu problemów eksploatacyjnych,
- Zapewnić wsparcie techniczne w pozostałym okresie w wymiarze co najmniej 8 roboczogodzin w ujęciu miesięcznym, szczególnie w zakresie implementacji zmian w konfiguracji oraz rozwiązywaniu problemów eksploatacyjnych.

5. Zamawiający zapewnia

1. Przygotowanie odpowiedniej ilości przestrzeni/Ilości „U” w już istniejących bądź nowych szafach serwerowych na planowane rozwiązania sprzętowe.
2. Zapewnienie odpowiednich parametrów działania planowanego do implementacji sprzętu:
 - a. Zasilanie – zalecane zasilanie dwutorowe gdzie utrzymanie poprzez zasilacz awaryjny UPS typu online każdego toru to min 2 godziny z monitoringiem SNMP,
 - b. Zapewnienie odpowiednich warunków klimatycznych dla planowanego sprzętu tzn. chłodzenie oraz właściwa wilgotność w pomieszczeniu. Zaleca się system klimatyzacji redundantnej,
 - c. Monitorowanie warunków środowiskowych wraz z powiadomieniem SNMP i GSM tj. temperatura, wilgotność, zanieczyszczenie, dym itp.,
 - d. Implementację zapewnienie rozwiązań bezpieczeństwa takich jak System Kontroli Dostępu, Sygnalizacji Włamania i Napadu, monitoring wizyjny CCTV, systemu gaszenia gazem w pomieszczeniu celem zapewnienia poprawnego,
 - e. Zapewnić odpowiednie mechanizmy oraz rozwiązania zapewniające komunikację części wspólnej projektu eCareMed z wewnętrzną infrastrukturą tj. odpowiednie okablowanie miedziane oraz światłowodowe, odpowiednie porty na przełącznikach a jeżeli istnieje taka konieczność to również wkładki światłowodowe lub kable typu DAC o odpowiedniej przepustowości.