Pabianice, dnia 27.03.2020 roku

ZPK.271.18.2019

Uczestnicy
postępowania przetargowego

dotyczy: przetargu nieograniczonego pn. *„Inteligentny system transportowy – zaprojektuj i wybuduj”*

ODPOWIEDZI NA ZAPYTANIA DO TREŚCI SIWZ ORAZ MODYFIKACJA TREŚCI SIWZ

Zamawiający Miasto Pabianice, reprezentowane przez Prezydenta Miasta Pabianic, działając na podstawie art. 38 ust. 1, 1a i 2 ustawy z dnia 29.01.2004r. Prawo Zamówień Publicznych (t.j. Dz. U. z 2019 r. poz. 1843, z późn. zm.), zwanej dalej ustawą Pzp przekazuje poniżej zapytania Wykonawców do treści Specyfikacji Istotnych Warunków Zamówienia (SIWZ) wraz z wyjaśnieniami oraz działając na podstawie art. 38 ust. 4 ustawy Pzp dokonuje modyfikacji SIWZ w zakresie opisanym poniżej:

Pytanie 1:
Niniejszym informujemy Państwa, iż opis wymagań zamieszczonych w SIWZ, jednoznacznie wskazuje na konkretne, tylko jedno urządzenie, mianowicie model FG-100E firmy Fortinet. Świadczy o tym szereg zapisów, przepisanych wprost z karty katalogowej tego urządzenia (w załączeniu). Przykładowe podajemy poniżej.

Karta katalogowa
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_100E_Series.pdf

Strona 5, specyfikacja.

Wymóg PFU:
a) Przepustowość Firewall: nie mniej niż 7 Gbps – Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps
Karta katalogowa: Firewall Throughput (1518/512/64 byte UDP packets) - 7.4/7.4/4.4 Gbps

Wymóg PFU:
b) W zakresie Firewall obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę

Karta katalogowa: Concurrent Sessions (TCP)-2 Million, New Sessions/Second (TCP)- 30,000
Wymóg PFU:
c) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS)–min. 1,5 Gbps oraz Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, AC, AV - minimum 250 Mbps
Karta katalogowa: CAPWAP Throughput (1444 byte, UDP)-1.5 Gbps, SSL-VPN Throughput - 250 Mbps

d) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS - Możliwość łączenia w klaster Active-Active lub Active-Passive.
Karta katalogowa: Active / Active, Active / Passive, Clustering

Odpowiedź:
Opis przedmiotu zamówienia nie preferuje konkretnego rozwiązania. Zamawiający określił minimalne parametry wynikające z konieczności zapewnienia określonej funkcjonalności zamawianych urządzeń i zezwala na zaoferowanie urządzeń o wskazanych parametrach oraz o parametrach wyższych niż wskazane. Na rynku dostępnych jest wiele urządzeń spełniających wymagania zamawiającego.
UWAGA:
W kolejnych odpowiedziach Zamawiający dokonuje zmian w zakresie PFU i wymaganych parametrów oferowanych urządzeń.

Pytanie 2:
W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – możliwość łączenia w klaster Active-Active lub Active-Passive.
Tryb HA Active-Passive cechuje się połączeniem cech atrakcyjności cenowej i trybie niezawodnościowego. Zaproponowane rozwiązanie zostało już na etapie kreowania wymagań przewidziane z odpowiednim zapasem mocy. Dodatkowo system ma składać się z 2 urządzeń zapewniający wymagany poziom bezpieczeństwa. Prosimy Zamawiającego o dopuszczenie rozwiązania systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS w trybie Active-Passive.

Odpowiedź:
Zamawiający w Zał. nr 1 PFU podaje, iż urządzenie ma mieć „możliwość łączenia w klaster Active-Active lub Active-Passive". Zatem urządzenie musi mieć możliwość łączenia w klaster w trybie Active-Active lub Active-Passive, a nie łącznie.
Zamawiający dopuszcza urządzenie oferujące tryb Active-Passive.

Pytanie 3:
System realizujący funkcję Firewall powinien dysponować min. 16 portami Ethernet 10/100/1000 Base-TX
W niniejszym projekcie w systemie firewall będziemy implementować kilka portów, jeden lub dwa do WAN, jeden do strefy zdemilitaryzowanej, jeden do LAN. Wykorzystanych zostaną 4 porty Ethernet 10/100/1000 Base-TX. Pozostałe porty będą nie wykorzystywane. Czy Zamawiający dopuści urządzenie cechujące się atrakcyjnością cenową, posiadają 12 portów Ethernet 10/100/1000 Base-TX?

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z mniejszą ilością portów Ethernet 10/100/1000 Base-TX, tj. min 12 portów Ethernet 10/100/1000 Base-TX. Ilość nadmiarowych portów w przypadku 12 Ethernet 10/100/1000 Base-TX będzie wystarczającą i zapewnia realizację przyszłych potencjalnych potrzeb.

Tym samym zmianie ulega zapis PFU:
Było: System realizujący funkcję Firewall powinien dysponować min. 16 portami Ethernet 10/100/1000 Base-TX
Jest: System realizujący funkcję Firewall powinien dysponować min. 12 portami Ethernet 10/100/1000 Base-TX

Pytanie 4:
W zakresie Firewall obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
Czy Zamawiający zgodzi się na obniżenie parametrów jednoczesnych połączeń do 500 000 i nowych sesji do 20 000, zakładając, normalną pracę użytkowników. Założenia te uwzględniają, że podczas bardzo intensywnego wykorzystaniu swojego komputera w sieci nie powinno się mieć dużej liczby sesji jednocześnie. Równocześnie osoba chroniona urządzeniem Firewall otwierając zbyt dużo sesji w jednym momencie działa jak potencjalny atak. Liczby te w odniesieniu do ogólnej wydajności urządzenia wydają się niepotrzebnie zawyżone, powodując potrzebę zaoferowania droższego, niż stanowi na to potrzeba, rozwiązania.

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie w zakresie Firewall obsługa nie mniej niż 500 000 jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę. Proponowana wydajność urządzenia w zakresie jednoczesnych połączeń oraz nowych połączeń na sekundę, uwzględniając faktyczne potrzeby projektowe, jest w pełni wystarczająca.

Tym samym zmianie ulega zapis PFU:
Było: „W zakresie Firewall obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę".
Jest: „W zakresie Firewall obsługa nie mniej niż 500 000 jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę".

Pytanie 5:
Przepustowość Firewall: nie mniej niż 7 Gbps
Czy Zamawiający zgodzi się na obniżenie parametru przepustowości Firewall: nie mniej niż 5 Gbps, zakładając, że newralgiczne pod kątem bezpieczeństwa funkcje IPS będą nie zmienione?

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu o dopuszcza urządzenie z przepustowością Firewall nie mniejszą niż 5 Gbps.
Zmianę tego parametru, Zamawiający uzasadniania obniżeniem ilości jednoczesnych połączeń oraz nowych połączeń na sekundę.

Tym samym zmianie ulega zapis PFU:
Było: „Przepustowość Firewall: nie mniej niż 7 Gbps"
Jest: „Przepustowość Firewall: nie mniej niż 5 Gbps"

Pytanie 6:
Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps
Czy Zamawiający zgodzi się na zaoferowanie urządzenia o wydajności szyfrowania VPN IPSec: nie mniej niż 1 Gbps? Obniżenie parametru przepustowości Firewall: nie mniej niż 5 Gbps, zakładając, że newralgiczne pod kątem bezpieczeństwa funkcje IPS będą nie zmienione?

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z wydajnością szyfrowania VPN IPSec nie mniejszą niż 1 Gbps
Zmianę tego parametru, Zamawiający uzasadniania obniżeniem ilości jednoczesnych połączeń oraz nowych połączeń na sekundę.

Tym samym zmianie ulega zapis PFU:
Było: „Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps"

Jest: „Wydajność szyfrowania VPN IPSec: nie mniej niż 1 Gbps”

Pytanie 7:
Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS i Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP

Czy Zamawiający zgodzi się usunąć zapisy dotyczące ochrony przed wirusami dla protokołu IMAP? Protokół IMAP działa bezpośrednio na wiadomościach na serwerze pocztowym. Wirus powinien być wyłapany zanim trafi na serwer poprzez ochronę przed wirusami na protokole SMTP. Za pomocą protokołu IMAP użytkownik pobiera tylko nagłówki wiadomości, sama wiadomość i załączniki są pobierane na żądanie użytkownika. Wiadomości zostają są serwerze.

Odpowiedź:
Zamawiający przeanalizował celowość wymogu związanego z ochroną przed wirusami dla protokołu IMAP i odstępuje od wymogu wsparcia dla tego protokołu, przyjmując uzasadnienie podane w pytaniu.

Tym samym zmianie ulega zapis PFU:
Było:
„- Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
- Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP”
Jest:
„- Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS
- Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3”

Pytanie 8:
Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
System DLP na urządzeniu brzegowym musi rozpoznawać rodzaj dokumentu, z rozróżnieniem różnych wersji aplikacji, wyszukać ciąg znaków, które mają być zablokowane w zależności od rodzaju dokumentu. Mechanizm ten bardzo obciąża urządzenie brzegowe i nie jest bardzo skuteczny, więc sugeruje się umieszczenie tego mechanizmu na urządzeniach roboczych użytkowników. Idea ta jest realizowana przez aplikacje typu DLP na komputerze, które bardziej skutecznie realizują to wymaganie (np. oprócz zapobiegania wycieku danych poprzez pocztę czy stronę Internetową również zapobiegnie wyciekowi poprzez zasoby sieciowe, zewnętrzny nośnik pamięci jak USB czy płyta CD) i nie obciąży urządzenia brzegowego przed realizacją zadań i analizy transmisji. Czy Zamawiający zgodzi się usunąć zapisy dotyczące mechanizmu ochrony przed wyciekiem poufnej informacji (DLP) ponieważ wielu producentów rozumie, że jest to mechanizm, który powinien być konfigurowany na stacjach roboczych a nie na firewallu? DLP jest cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie, które nie wspiera mechanizmu ochrony przed wyciekiem poufnej informacji (DLP).

Tym samym zmianie ulega zapis PFU:
Było: „Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)”
Jest: Zapis „Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)” ulega wykreśleniu.

Pytanie 9:
Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

Czy Zamawiający zgodzi się usunąć zapisy dotyczące dynamicznego protokołu PIM? PIM jest cechą charakterystyczna dla routerów lub urządzenia firewall Fortigate firmy Fortinet.

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i odstępuje od wymogu wsparcia dla protokołu dynamicznego PIM. Zamawiający przeanalizował założenia i potrzeby projektowe, i zauważa, iż protokół ten nie jest niezbędny.

Tym samym zmianie ulega zapis PFU:
Było: „Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM".
Jest: „Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP".

Pytanie 10:
Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSecVPN'a, Antywirus'a, IPS'a.
Istnieje możliwość równoczesnego ustawienia w tym samym czasie dwóch trybów: Routera z funkcją NAT i transparentny, przez co nie ma potrzeby wykorzystywania wielu instancji. W ramach tej funkcjonalności jest możliwość konfigurowania Routingu, Firewall'a, IPSec VPN, Antywirus, IPS. Czy Zamawiający zgodzi się na możliwość budowy pojedynczej instancji systemów zakładając, że jest możliwość pracy urządzenia z funkcją NAT i transparentną w tym samym czasie? Instancje systemów (tj. do 10 w ramach podstawowej licencji) są cechą charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Odpowiedź:
Zamawiający dopuszcza możliwość realizacji tej usługi w sposób równoważny, tj. w sposób i na zasadach zaproponowany przez wykonawcę.

Tym samym zmianie ulega zapis PFU:
Było: „Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSecVPN'a, Antywirus'a, IPS'a".
Jest: „Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSecVPN'a, Antywirus'a, IPS'a lub możliwość budowy pojedynczej instancji systemów zakładając pracę urządzenia z funkcją NAT i transparentną w tym samym czasie".

Pytanie 11:
Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos.
Czy Zamawiający pozwoli na urządzenie, w którym system IPS pozwoli na szybszą kontrolę niż przedstawiona w wymaganiu, ale zawierającego 1500 wpisów? Analiza protokołu może być wykonywana dla poszczególnych typów ruchu sieciowego poprzez specjalne wtyczki programowe (tzw. plug-iny). Pracują w trybie kernel-mode, czyli bezpośrednio w jądrze systemu operacyjnego. Po wykryciu określonego typu ruchu (np. HTTP, FTP, SMTP, …) automatycznie uruchamiana jest odpowiednia wtyczka, która specjalizuje się w ochronie danego protokołu. Zasadnicze znaczenie ma kontekst, w jakim zostały wykryte pakiety charakterystyczne dla określonego ataku. W ten sposób sieć jest chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały. Dzięki temu mechanizmowi można wykryć ponad 10 000 różnych zagrożeń, zaś wystarczy na to tylko około 1500 wpisów. Liczba

5 000 wpisów opisanych w sposób jak w SIWZ, to cecha charakterystyczna dla urządzenia Fortigate firmy Fortinet.

Odpowiedź:

Zamawiający przychyla się do wniosku zawartego w pytaniu, dopuszcza urządzenie z bazą sygnatur ataków min 1500 wpisów z jednoczesnym dopuszczeniem realizacji tej usługi w sposób równoważny, tj. w sposób i na zasadach zaproponowany przez wykonawcę.

Tym samym zmianie ulega zapis PFU:

Było: „Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos".

Jest: „Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 1500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos".

Pytanie 12:

W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance.
Cechą charakterystyczną dla urządzenia Fortigate firmy Fortinet jest kategoryzowanie stron dla spyware, malware, spam, proxyavoidance w filtrze www. Czy Zamawiający zgodzi się na rozwiązanie, w którym ochronę z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), spam i proxyavoidance jest realizowana poprzez inną funkcjonalność znaną pod nazwą IP Reputation?

Odpowiedź:

Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza realizację tej usługi w sposób równoważny, tj. za pomocą funkcjonalności pod nazwą IP Reputation w sposób i na zasadach zaproponowanych przez wykonawcę.

Tym samym zmianie ulega zapis PFU:

Było: „W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance".

Jest: „W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance lub kategorie stron jak: spyware, malware, spam, proxyavoidance będą realizowane przez funkcjonalność pod nazwą IP Reputation".

Pytanie 13:

Czy przez gwarancję na system bezpieczeństwa, Zamawiający rozumie również aktualizację subskrypcji w przypadku systemów bezpieczeństwa w całym okresie zaoferowanej gwarancji?

Odpowiedź:

Wykonawca będzie zobowiązany do aktualizacji subskrypcji przez cały okres gwarancji.

Pytanie 14:

Z uwagi na czas, jaki upłynął od momentu opracowania PFU (czerwiec 2017) do jego publikacji (listopad 2019), oraz fakt, iż w tym okresie pojawiły się procesory nowszych generacji,

zwracamy się do Zamawiającego, o dopuszczenie procesora Procesor Intel® Xeon® Silver 4208 jako równoważnego do opisanego w PFU?
Specyfikacja w pkt. 4c podana jest pod procesor Procesor Intel® E5-2620v4, którego następcą technologicznym o identycznej liczbie rdzeni, czy taktowaniu zegara jest obecnie procesor nowej generacji, właśnie Intel® Xeon® Silver 4208.

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń, dopuszcza wdrożenie urządzeń równoważnych oraz o parametrach wyższych.

Pytanie 15:
Ponieważ w pkt. 4 wymagań, Zamawiający podaje: *„Nie mniej niż 4 dedykowane dwuprocesorowe moduły serwerowe, każdy o minimalnych wymaganiach podanych poniżej:”* a w p-pkt'ach od 4a do 4i specyfikuje wymagania minimalne dla każdego z 4 modułów serwerowych, prosimy Zamawiającego o potwierdzenie, że każdy z tych modułów serwerowych ma mieć zainstalowane 4 dyski twarde?

Odpowiedź:
Zamawiający potwierdza, iż z 4 modułów serwerowych należy wyposażyć w 4 dyski twarde zgodne z podanymi wymaganiami.

Pytanie 16:
Czy system kopii zapasowych i archiwum danych ma również obejmować archiwum obrazowane z 52 kamer systemu CCTV, w celu tworzenia kopii zapasowych serwera zapisu CCTV, który ma być uruchomiony w tej samej lokalizacji co system kopii zapasowych i archiwum danych, tj. w serwerowni kontenerowej.

Odpowiedź:
System kopii zapasowej i archiwum danych nie powinien obejmować systemu CCTV. System CCTV powinien posiadać oddzielny system archiwizacji zapisu na co najmniej 30 dni.

Pytanie 17:
Czy Zamawiający dopuści rozwiązanie posiadające 48 portów RJ45, 2 porty SFP+ oraz 2 porty SFP (z możliwością zwiększenia ich przepustowości do 10GB za pomocą dodatkowej licencji)?

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).
Zamawiający przez port SFP+ rozumie standard transmisji 10 GEth. W załączniku 1 PFU wymaga od przełącznika 2 portów SFP+ 10GEth oraz 2 slotów modułu SFP+ - czyli łącznie 4 interfejsów z przepływnością 10 GbEth oraz 1 portu SFP.
Po przeanalizowaniu założeń projektowych, Zamawiający dopuszcza przełącznik dostępowy wyposażony w ilość portów SFP+/SFP z transmisją 10GEth zaproponowaną przez wykonawcę tj. 4 porty z transmisją 10GEth i odstępuje o wymogu dodatkowego 1 portu SFP, który może być realizowany poprzez jeden z portów SFP+/SFP10GEth. Zamawiający uważa, iż zaproponowana liczba portów WAN w pełni zaspokaja potrzeby projektowe w zakresie stworzenia bezpiecznych i redundantnych połączeń sieci transmisyjnych.

Tym samym zmianie ulega zapis PFU:
Było:
„2 x Porty SFP+ 10Gigabit
1 x sloty modułu SFP
2 sloty modułu SFP+”

Jest:
„2 x Porty SFP+ 10Gigabit
2 sloty modułu SFP+/SFP 10GEth”

Pytanie 18:
Do usunięcia
- Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, ~~gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia,~~

Czy Zamawiający dopuści rozwiązanie realizujące QoS za pomocą standardowych protokołów IEEE 802.1p, DiffServ?

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).
Zamawiający określił minimalne parametry urządzeń. Dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych. Dla przypadku omówionego w pytaniu, Zamawiający uzna za równoważne realizowanie QoS za pomocą standardowych protokołów IEEE 802.1p, DiffServ, który to standard jest typowy dla przełączników sieci LAN (rozwiązań wewnętrznych).

Tym samym zmianie ulega zapis PFU:
Było: „Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia”
Jest: „Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia lub realizowany w sposób równoważny za pomocą standardowych protokołów IEEE 802.1p, DiffServ”

Pytanie 19:
Do usunięcia dla bezpieczeństwa:
~~Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet),~~
Czy Zamawiający zgodzi się na usunięcie tego zapisu. Jest to standard używany w sieciach przemysłowych, a wymóg dotyczy urządzeń w serwerowni. Jeśli nie to prośba o doprecyzowanie jakie RFC powinno minimalnie spełniać oferowane urządzenie.

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).
Poprzez „obsługę mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo”, Zamawiający rozumie mechanizm stosowany w DiffServ polegający na kolejkowaniu, kształtowaniu i ewentualnym ograniczaniu przepływu pakietów w sieci, zgodnie z polityką zdefiniowaną dla każdej klasy. W tym przypadku urządzenie musi minimalnie spełniać standard RFC-2474, RFC-2597, RFC-2598 dla aplikacji czasu rzeczywistego, takich jak np. transmisja głosu czy sygnału wideo.
W związku z powyższym, jeżeli wykonawca zaproponuje urządzenie spełniające RFC-2474, RFC-2597, RFC-2598, to Zamawiający uzna urządzenie za spełniające wymagania.

Tym samym zmianie ulega zapis PFU:
Było: „Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet)”

Jest: „Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet) lub za pomocą norm RFC min. RFC-2474, RFC-2597, RFC-2598”

Pytanie 20:
- dla przełącznika pkt B)
o dopuszczenie do zaoferowania w Straży Miejskiej przełącznika LAN do montażu w pomieszczeniach (w szafce RACK) o parametrach jak dla przełącznika LAN do Serwerowni, tyle że posiadającego 24 porty 10/100/1000 RJ45, 2 porty SFP+ oraz 2 porty SFP (z możliwością zwiększenia ich przepustowości do 10GB za pomocą dodatkowej licencji) oraz o Prędkości przekazywania pakietów na poziomie min. 95 Mpps?
Jednocześnie z uwzględnieniem pozytywnych odpowiedzi Zamawiającego do pkt. A) powyżej (pytania 2 i 3)

Odpowiedź:
Zakładamy, iż pytanie wykonawcy dotyczy przełącznika sieciowego (PFU, str. 66-67).

Zamawiający, zważywszy na potrzebę objęcia wszystkich urządzeń sieciowych LAN/WAN i Wifi wspólnym systemem kontroli dostępu do sieci, pozytywnie ustosunkowuje się do wniosku wykonawcy i dopuszcza zaoferowanie w Straży Miejskiej przełącznika sieciowego o parametrach analogicznych jak dla tego w Serwerowni MZK-CZR z jednoczesnym obniżeniem prędkości przekazywania pakietów na poziomie min. 95 Mpps. Dodatkowo uzasadnia do potrzebą montażu przełącznika sieciowego w szafce RACK, a parametry podane w PFU wskazują na przełącznik przemysłowy.

Pytanie 21:
- dla przełącznika pkt C)
o dopuszczenie przełącznika przemysłowego wyposażonego w 8 portów 10/100 RJ-45 (PoE+ 30W) oraz 4 porty SFP, w pełni zaspokajającego potrzeby transmisyjne dla wszystkich urządzeń wpiętych do niego w szafie ulicznej i poborze mocy na poziomie nie przekraczającym 15W.

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza przełącznik wyposażony w 8 portów 10/100 RJ-45 (PoE+ 30W) oraz 2 porty SFP.

Tym samym zmianie ulega zapis PFU:
Było:
„Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX z PoE (PSE) – 8
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX – 4
Porty SFP 100/1000 Base-X Auto MDI/MDIX – 2”
Jest:
„Porty RJ-45 min. 10/100 Base-T Auto MDI/MDIX z PoE (PSE) – 8
Porty SFP 100/1000 Base-X Auto MDI/MDIX – 2”

Pytanie 22:
- dla punktu dostępowego WIFI na przystankach pkt D)

o dopuszczenie urządzenia równoważnego, z uwagi na konieczność objęcia wspólnym systemem kontroli dostępu do sieci wszystkich urządzeń LAN/WLAN dostarczanych w ramach zadania, o następujących parametrach równoważności:
- musi mieć możliwość pracy niezależnej (Standalone) oraz pracy z kontrolerem WLAN;
- musi obsługiwać standard 802.11ac Wave 2
- musi posiadać dwa niezależne moduły radiowe pracujące w częstotliwościach 2,4GHz i 5GHz;
- musi posiadać moduł Bluetooth (BLE);

- obsługa 2x2 MIMO;
- musi obsługiwać 8 SSID per moduł radiowy (16 per AP);
- musi posiadać minimum 2 porty Gigabit Ethernet;
- musi posiadać funkcjonalność równomiernego dystrybuowania Klientów pomiędzy punktami dostępowymi i pasmami częstotliwościowymi;
- musi wspierać standard 802.11r Fast Roaming;
- musi wspierać mechanizm wykrywający zakłócenia i automatycznie dostosowywać do nich kanał pracy oraz moc sygnału;
- musi umożliwiać konfigurację 802.1x, 802.11i, WPA, WPA2;
- musi realizować usługi RADIUS;
- musi realizować QoS – minimum WMM, 802.1p, Diffserv i TOS;
- wbudowana widoczność i kontrola aplikacji w oparciu o DPI (Deep Packet Inspection) z możliwością tworzenia własnych sygnatur aplikacji;
- obsługa funkcjonalności rozpoznawania podłączonych urządzeń (Device Fingerprinting);
- musi mieć możliwość uruchomienia usługi Captive Portal;
- musi umożliwiać uruchomienie usługi hotspot;
- musi posiadać wbudowany IDS;
- musi umożliwiać wsparcie dla WIPS;
- musi posiadać certyfikat kompatybilności WiFi Alliance.
- musi posiadać klasę odporności IP67;
- zakres temperatur pracy -40° C do 70° C;
- ochronę wiatrową – min. 165Mph;

Odpowiedź 22:
Zamawiający przychyla się do wniosku zawartego w pytaniu (tj. konieczność objęcia wspólnym systemem kontroli dostępu do sieci wszystkich urządzeń LAN/WLAN) i dopuszcza rozwiązanie równoważne o zaproponowanych parametrach.

Tym samym zmianie ulega zapis PFU:

Było:

Porty	
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX	2
Port PoE PD	obecny na interfejsie ETH2, w pełni zgodny ze specyfikacją IEEE 802.3af Power Device, ochrona przed przeciążeniem i zwarciem, izolacja napięciowa min. 1000 VDC, izolacja obciążeniowa min. 100MΩ
Interfejs WLAN	
Tryby pracy	AP/Bridge/Repeater/AP-Client
Złącze antenowe	2xRP-SMA
Typ częstotliwości radiowej	DSSS
Modulacja IEEE802.11b	CCK, DQPSK, DBPSK

Modulacja IEEE802.11g/n	OFDM z BPSK, QPSK, 16QAM, 64QAM
Pasmo częstotliwości	Ameryka/FCC 2.412~2.462 GHz (11 kanałów), Europa CE/ETSI 2.412~2.472 Ghz (13 kanałów)
Prędkość transmisji	IEEE802.11b 1/2/5.5/11 Mbps, IEEE802.11g 6/9/12/18/24/36/48/54 Mbps, IEEE802.11n do 300Mbps
Moc nadawania	802.11b 17dBm ± 1.5dBm@11Mbps, 802.11g 16dBm ± 1.5dBm@54Mbps, 802.11gn HT20 15dBm ± 1.5dBm @MCS7, 802.11gn HT40 14dBm ± 1.5dBm @MCS7
Czułość odbiornika	802.11b -85dBm ± 2dBm@11Mbps, 802.11g -76dBm ± 2dBm@54Mbps, 802.11gn HT20 -75dBm ± 2dBm@MCS7, 802.11gn HT40 -72dBm ± 2dBm@MCS7
Bezpieczeństwo transmisji	WEP (obsługa kluczy 64-bit/128-bit), WPA / WPA2 PSK 802.11i (szyfrowanie TKIP i AES), obsługa 802.1X/RADIUS Authentication
Ochrona SSID	wyłączanie rozgłaszania SSID
Obsługa protokołów	ARP, BOOTP, DHCP, DNS, HTTPs, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP (IEEE 802.1D)
Wskaźniki LED	
Wskaźnik zasilania	LED x3 PWR 1(2) (PoE) - czerwony (zasilanie wł. / rozruch), zielony (zasilanie wł. / normalna praca)
Wskaźnik portu RJ-45 100/1000TX	2x zielony dla portu Link/Aktywność 1000Mbps, bursztynowy dla porty Link/Aktywność 100Mbps
Wskaźnik WLAN	zielony Link/Aktywność
Wskaźnik błędu	czerwony - brak połączenie Ethernet lub awaria zasilania

Złącze alarmowe	
Przekazywanie	wyjście alarmowe może przenieść 1A przy 24VDC
Zasilanie	
Wejście zasilania redundantnego	Podwójne wejście 12~48VDC na 6-pinowym złączu terminal block
Pobór mocy (typowo)	8,5W
Ochrona przeciążeniowa prądowa	obecna
Ochrona przed odwrotną polaryzacją	obecna
Charakterystyka fizyczna	
Obudowa	IP-30
Odporność na czynniki zewnętrzne	
Temperatura składowania	-40÷85°C (-40÷185°F)
Temperatura pracy	-10÷60°C (14÷140°F)
Dopuszczalna wilgotność	5%÷95% niekondensująca
Zgodność z normami/zaleceniami	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS),EN61000-4-8, EN61000-4-11

Jest:

Porty	
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX	2
Port PoE PD	obecny na interfejsie ETH2, w pełni zgodny ze specyfikacją IEEE 802.3af Power Device, ochrona przed przeciążeniem i zwarciem, izolacja napięciowa min. 1000 VDC, izolacja obciążeniowa min. 100MΩ
Interfejs WLAN	
Tryby pracy	AP/Bridge/Repeater/AP-Client

Złącze antenowe	2xRP-SMA
Typ częstotliwości radiowej	DSSS
Modulacja IEEE802.11b	CCK, DQPSK, DBPSK
Modulacja IEEE802.11g/n	OFDM z BPSK, QPSK, 16QAM, 64QAM
Pasmo częstotliwości	Ameryka/FCC 2.412~2.462 GHz (11 kanałów), Europa CE/ETSI 2.412~2.472 Ghz (13 kanałów)
Prędkość transmisji	IEEE802.11b 1/2/5.5/11 Mbps, IEEE802.11g 6/9/12/18/24/36/48/54 Mbps, IEEE802.11n do 300Mbps
Moc nadawania	802.11b 17dBm ± 1.5dBm@11Mbps, 802.11g 16dBm ± 1.5dBm@54Mbps, 802.11gn HT20 15dBm ± 1.5dBm @MCS7, 802.11gn HT40 14dBm ± 1.5dBm @MCS7
Czułość odbiornika	802.11b -85dBm ± 2dBm@11Mbps, 802.11g -76dBm ± 2dBm@54Mbps, 802.11gn HT20 -75dBm ± 2dBm@MCS7, 802.11gn HT40 -72dBm ± 2dBm@MCS7
Bezpieczeństwo transmisji	WEP (obsługa kluczy 64-bit/128-bit), WPA / WPA2 PSK 802.11i (szyfrowanie TKIP i AES), obsługa 802.1X/RADIUS Authentication
Ochrona SSID	wyłączanie rozgłaszania SSID
Obsługa protokołów	ARP, BOOTP, DHCP, DNS, HTTPs, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP (IEEE 802.1D)
Wskaźniki LED	
Wskaźnik zasilania	LED x3 PWR 1(2) (PoE) - czerwony (zasilanie wł. / rozruch), zielony (zasilanie wł. / normalna praca)

Wskaźnik portu RJ-45 100/1000TX	2x zielony dla portu Link/Aktywność 1000Mbps, bursztynowy dla porty Link/Aktywność 100Mbps
Wskaźnik WLAN	zielony Link/Aktywność
Wskaźnik błędu	czerwony - brak połączenie Ethernet lub awaria zasilania
Złącze alarmowe	
Przekazywanie	wyjście alarmowe może przenieść 1A przy 24VDC
Zasilanie	
Wejście zasilania redundantnego	Podwójne wejście 12~48VDC na 6-pinowym złączu terminal block
Pobór mocy (typowo)	8,5W
Ochrona przeciążeniowa prądowa	obecna
Ochrona przed odwrotną polaryzacją	obecna
Charakterystyka fizyczna	
Obudowa	IP-30
Odporność na czynniki zewnętrzne	
Temperatura składowania	-40÷85°C (-40÷185°F)
Temperatura pracy	-10÷60°C (14÷140°F)
Dopuszczalna wilgotność	5%÷95% niekondensująca
Zgodność z normami/zaleceniami	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS),EN61000-4-8, EN61000-4-11

Lub równoważny:
- musi mieć możliwość pracy niezależnej (Standalone) oraz pracy z kontrolerem WLAN;
- musi obsługiwać standard 802.11ac Wave 2
- musi posiadać dwa niezależne moduły radiowe pracujące w częstotliwościach 2,4GHz i 5GHz;
- musi posiadać moduł Bluetooth (BLE);
- obsługa 2x2 MIMO;
- musi obsługiwać 8 SSID per moduł radiowy (16 per AP);
- musi posiadać minimum 2 porty Gigabit Ethernet;

- musi posiadać funkcjonalność równomiernego dystrybuowania Klientów pomiędzy punktami dostępowymi i pasmami częstotliwościowymi;
- musi wspierać standard 802.11r Fast Roaming;
- musi wspierać mechanizm wykrywający zakłócenia i automatycznie dostosowywać do nich kanał pracy oraz moc sygnału;
- musi umożliwiać konfigurację 802.1x, 802.11i, WPA, WPA2;
- musi realizować usługi RADIUS;
- musi realizować QoS – minimum WMM, 802.1p, Diffserv i TOS;
- wbudowana widoczność i kontrola aplikacji w oparciu o DPI (Deep Packet Inspection) z możliwością tworzenia własnych sygnatur aplikacji;
- obsługa funkcjonalności rozpoznawania podłączonych urządzeń (Device Fingerprinting);
- musi mieć możliwość uruchomienia usługi Captive Portal;
- musi umożliwiać uruchomienie usługi hotspot;
- musi posiadać wbudowany IDS;
- musi umożliwiać wsparcie dla WIPS;
- musi posiadać certyfikat kompatybilności WiFi Alliance.
- musi posiadać klasę odporności IP67;
- zakres temperatur pracy -40° C do 70° C;
- ochronę wiatrową – min. 165Mph;

Pytanie 23:

4.5. Zamawiający informuje, że 32 nw. autobusy należy włączyć w system ITS:
4.5.1. 9 szt. autobusów Solaris Urbino 12 będących własnością MZK Pabianice Sp. z o.o., wyposażonych w autokomputery SRG3100P, nieobjęte systemem geolokalizacji GPS – należy zapewnić dla wskazanych pojazdów transmisję GPS na potrzeby systemu ITS;
4.5.2. 5 szt. autobusów Solaris Urbino 12 będących własnością Zamawiającego, wyposażonych w autokomputery SRG4000P, nieobjęte systemem geolokalizacji GPS – należy zapewnić dla wskazanych pojazdów transmisję GPS na potrzeby systemu ITS;
4.5.3. 18 szt. autobusów Solaris Urbino 12 hybrid będących własnością Zamawiającego, wyposażonych w autokomputery SRG6000P, objęte systemem geolokalizacji GPS (otwarte protokoły komunikacyjne) – należy uzyskać transmisję z zamontowanych geolokalizatorów GPS na potrzeby systemu ITS.
Czy zamawiający udostępni protokoły komunikacyjne z w/w urządzeniami? Brak interfejsów i konieczność integracji z urządzeniami konkretnego dostawcy preferuje go i przeczy uczciwej konkurencji. W przypadku braku takiej możliwości czy Zamawiający zezwoli na instalację lokalizatorów GPS?

Odpowiedź:

Zamawiający informuje, że jest w posiadaniu protokołów komunikacyjnych w autobusach ze sterownikiem SRG 6000P, służących do transmisji sygnału geolokalizacji i ma możliwość udostępnienia ich na potrzeby systemu ITS (dotyczy punktu 4.5.3 SIWZ).
Zamawiający nie wymaga integracji z urządzeniami konkretnego dostawcy i zezwoli na instalację lokalizatorów GPS.

Pytanie 24:

4.6. Wykonawca, w ramach budowy sieci transmisji danych w oparciu o linie kablowe światłowodowe, o której mowa w pkt 2.1, będzie zobowiązany również do zapewnienia możliwości podłączenia do sieci światłowodowej 5 biletomatów stacjonarnych typu BS-206, zlokalizowanych na przystankach:
4.6.1.Dworzec PKP,
4.6.2.Kilińskiego / Zamkowa,
4.6.3.Kilińskiego / SDH,
4.6.4.Jana Pawła II / szpital,
4.6.5.Grota-Roweckiego / Gryzla.

Podłączenie urządzeń do sieci światłowodowej będzie leżało w gestii producenta biletomatów – firma Mera Systemy Sp. z o.o. Zadaniem Wykonawcy będzie umożliwienie wpięcia automatów do sieci światłowodowej ITS.

Prosimy o potwierdzenie, że termin podłączenia w/w przez firmę Mera Systemy nie będzie miała wpływu na zakończenie zadania, a odpowiedzialność wykonawcy kończy się na realizacji sieci światłowodowej a nie terminowym i skutecznym włączaniu w/w urządzeń.

Odpowiedź:
Wykonawca jest zobowiązany do wykonania przyłącza światłowodowego i umożliwienie wpięcia się przez przedstawicieli firmy Mera Systemy. Podłączenie biletomatów nie jest przedmiotem zamówienia.

Pytanie 25:
4.7. Wykonawca, w ramach wdrożenia ITS, uzupełni tworzony przez siebie system o dane rozkładowe na podstawie bazy danych przekazanej przez Zamawiającego, pochodzącej z oprogramowania AGC Busman 100 lub Municom.
Czy zamawiający udostępni protokoły komunikacyjne z w/w systemami?

Odpowiedź:
MZK Pabianice Sp. z o.o. ma możliwość udostępnienia protokołów komunikacyjnych z oprogramowania MUNICOM w celu uzupełnienia tworzonego systemu ITS o dane rozkładowe z bazy programu MUNICOM. Wobec powyższego, Zamawiający udostępni wszelkie posiadane protokoły komunikacyjne.
Z bazy danych AGC Busman 100 Zamawiający udostępni natomiast tabelaryczne rozkłady jazdy wyeksportowane do arkusza kalkulacyjnego.

Pytanie 26:
4.8. Zamawiający informuje, że w ramach odrębnego projektu pn. „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów" w latach 2020 – 2021 będzie budowana sieć światłowodowa wraz z tablicami dynamicznej informacji pasażerskiej z monitoringiem wizyjnym, wzdłuż ulic Zamkowej i Warszawskiej w Pabianicach. Wykonawca będzie zobowiązany umożliwić wpięcie tablic informacji pasażerskiej i kamer CCTV, realizowanych w ramach projektu „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów" do systemu, tworzonego w ramach przedmiotowego postępowania. Powyższe oznacza, że tworzony system powinien umożliwić zarządzanie tablicami dynamicznej informacji pasażerskiej oraz kamerami monitoringu, realizowanymi zarówno w ramach niniejszego projektu, jak i projektu „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów". Zamawiający wskazuje, że połączenie obydwu sieci światłowodowych powinno nastąpić w rejonie skrzyżowania ulic Jana Kilińskiego i Zamkowej w Pabianicach.
Prosimy o doprecyzowanie. Wykonawca ma zapewnić możliwość wpięcia w system tablic i monitoringu dostawców z innego przetargu realizowanego w przyszłym roku. Biorąc pod uwagę niemożność przewidzenia jaki to będzie dostawca sugerujemy dodanie informacji, że dostawca kolejnego przetargu będzie musiał zintegrować się z protokołami komunikacyjnymi przedstawionymi przez wykonawcę aktualnego zadania.

Odpowiedź:
Wykonawca jest zobowiązany do wdrożenia systemu otwartego i będzie musiał przekazać niezbędne dane i protokoły komunikacyjne dla wpięcia tablic Wykonawcy innego zadania.

Pytanie 27:

18.1. Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert:

Lp.	Nazwa kryterium	Znaczenie kryterium (w %)
1	Cena (C)	60
2	Długość okresu gwarancji na roboty budowlane oraz zamontowane materiały i urządzenia (G), w tym:	24
2.1	na dostarczone tablice dynamicznej informacji pasażerskiej wraz z systemem ITS (GTd)	6
2.2	na system monitoringu wizyjnego (GMw)	6
2.3	na wersję portalu komunikacjapabianice.pl wraz z aplikacją mobilną (GP)	6
2.4	na wykonane roboty budowlane oraz pozostałe zamontowane urządzenia i materiały (GR)	6
3	Wsparcie operatorskie w okresie gwarancji jakości (W)	16

Z zastosowanych wzorów do obliczania kryterium gwarancji wynika, iż każdy oferent z poprawnie złożoną ofertą i minimalną gwarancją otrzymuje odpowiednio w częściach 2.1-2.4: 12 punktów.
Przykład:
a) na dostarczone tablice dynamicznej informacji pasażerskiej wraz z systemem ITS od 24 miesięcy do 60 miesięcy; OFERENCI UZYSKUJĄ OD 2.4 DO 6 PKT
b) na system monitoringu wizyjnego od 24 miesięcy do 60 miesięcy; OFERENCI UZYSKUJĄ OD 2.4 DO 6 PKT
c) na wersję portalu komunikacjapabianice.pl wraz z aplikacją mobilną od 36 miesięcy do 60 miesięcy; OFERENCI UZYSKUJĄ OD 3.6 DO 6 PKT
d) na wykonane roboty budowlane oraz pozostałe zamontowane urządzenia i materiały od 36 miesięcy do 60 miesięcy, OFERENCI UZYSKUJĄ OD 3.6 DO 6 PKT
Żaden z oferentów nie może uzyskać 0 punktów.
Łącznie różnica między minimalną a maksymalną gwarancją wyniesie 12 pkt i taką realną wartość ma owo kryterium.
Przyjmując to, w ocenie oferty punktacja wygląda następująco:
Cena – 60 pkt
Gwarancja – 12 pkt
Wsparcie operatorskie – 16 pkt
Powyższe wartości wpływają więc na wartość procentową kryterium ceny i mają się następująco:
Cena – 68,18%
Gwarancja – 13,64%
Wsparcie operatorskie – 18,18%
Zapis taki powoduje niezgodność z ustawą PZP i maksymalną wartością kryterium cenowego ocenie ofert - 60%.
Wykonawca sugeruję zmianę sposobu oceny ofert.

Odpowiedź:
Zamawiający **dokonuje modyfikacji zapisów pkt. 18.4 SIWZ** poprzez dodanie zapisu:

„W przypadku zaoferowania przez Wykonawcę długości gwarancji w wysokości 24 m-ce (dla robót wskazanych w lit. a i b) lub 36 m-cy (dla robót wskazanych w lit c i d), Zamawiający przyzna „0” zero punków”.

Pytanie 28:
Zał 1 do SIWZ:
2.2 Zadanie Nr 12 – Zakup i montaż biletomatów stacjonarnych, przyjmujących płatność gotówką i kartami płatniczymi oraz biletomatów mobilnych przyjmujących płatność kartami płatniczymi
Wykonawca prosi o potwierdzenie, że powyższy punkt w całości nie jest częścią zamówienia.

Odpowiedź:
Zadanie nr 12 nie jest objęte przedmiotem zamówienia.

Pytanie 29:
21. W ramach gwarancji Wykonawca zobowiązany jest do niezwłocznego usuwania powstałych awarii/uszkodzeń Systemu przy czym przez System rozumie się całokształt Inteligentnego Systemu Transportowego, na który składają się w szczególności; podsystem monitoringu, podsystem dynamicznej informacji pasażerskiej (w tym tablice przystankowe), portal pasażera KomunikacjaPabianice.pl wraz z aplikacją mobilną. Wszelkie awarie oraz usterki, będą usuwane przez Wykonawcę w możliwie najkrótszym terminie, tzn.:
1) w przypadku awarii Systemu:
a) czas reakcji - 6 godzin od zgłoszenia,
b) czas usunięcia - maksymalnie 12 godzin od zgłoszenia, przy czym czas reakcji i usunięcia będzie liczony w godzinach 6:00–22:00.
W przypadkach awarii, w których konieczny jest dłuższy czas jej usunięcia, Zamawiający po otrzymaniu opisu awarii i harmonogramie napraw może wrazić zgodę na wydłużenie czasu usunięcia awarii maksymalnie do 5 dni od chwili zgłoszenia.
2) w przypadku braku dostępu do infolinii:
a) czas reakcji - 4 godziny od zgłoszenia,
b) czas usunięcia - maksymalnie 12 godzin od zgłoszenia, przy czym czas reakcji i usunięcia będzie liczony w godzinach 6:00–22:00. W przypadkach awarii, w których konieczny jest dłuższy czas jej usunięcia, Zamawiający po otrzymaniu opisu awarii i harmonogramie napraw może wrazić zgodę na wydłużenie czasu usunięcia awarii maksymalnie do 2 dni od chwili zgłoszenia.
Wykonawca prosi o doprecyzowanie, czy powyższy zapis dotyczy 7 dni kalendarzowych, czy roboczych?

Odpowiedź:
Zapis dotyczy dni kalendarzowych.

Pytanie:
Wykonawca zapewni wsparcie dla Zamawiającego w postaci operatora Systemu będącego do dyspozycji Zamawiającego w godzinach 6:00 – 22:00 (przez 8 godzin), 5 dni w tygodniu przez pierwszy miesiąc gwarancji oraz w wymiarze 8 godzin dziennie (maksymalnie 40 godzin tygodniowo) przez kolejne ……. 3 miesiące od dnia odbioru przedmiotu umowy.
Wykonawca prosi o doprecyzowanie zapisu. Czy chodzi o 8 godzin następujących po sobie oraz kto decyduje, które 8 godzin z podanego zakresu operator ma być dostępny?

Odpowiedź:
Zamawiający wskazuje 8 następujących po sobie godzin w zakresie 7:00 – 15:00, przy czym dopuszcza zmianę zakresu godzinowego na inny za porozumieniem stron.

Pytanie 31:
Wykonawca w okresie gwarancji zapewni wsparcie techniczne poprzez Help Desk (infolinia, adres email) 24x7x365 i będzie zobowiązany do udzielania niezwłocznej odpowiedzi, jednak nie później niż w ciągu 24 godzin od momentu zgłoszenia zapotrzebowania.

Wykonawca prosi o doprecyzowanie zapisu i określenie jak ma on się do zapisów z Pytania numer 7 i 8.

Odpowiedź:
Wsparcie techniczne jest oddzielnym zadaniem niż operator systemu. Każde z zadań ma określone inne warunki.

Pytanie:
Wykonawca upoważnia Zamawiającego do dokonywania zmian utworu(ów) wg uznania Zamawiającego.
Wykonawca prosi o doprecyzowanie jakich utworów Zamawiający może mieć możliwość modyfikacji. Możliwość samodzielnego dokonywania zmian w oprogramowaniu sterującym ITS, informacją pasażerską, aplikacjami przez Zamawiającego może powodować nienależyte działanie systemu, jego awarie na co wykonawca nie może pozwolić, szczególnie w okresie gwarancyjnym, gdy jest odpowiedzialny za poprawne działanie systemu.

Odpowiedź:
Zamawiający informuje, że w okresie gwarancji systemu nie będzie dokonywał samodzielnych zmian w oprogramowaniu, jednak po okresie gwarancji zastrzega sobie prawo dokonywania zmian.

Pytanie 33:
Kary umowne:
3) za brak wsparcia dla Zamawiającego w postaci operatora Systemu będącego do dyspozycji zamawiającego określonego w §14 w wysokości 2.000,00 PLN za każdą godzinę braku wsparcia;
Wykonawca sugeruje by urealnić kwotę, gdyż jest niewspółmiernie wysoka.

Odpowiedź:
Zamawiający zmienia wysokość kary do kwoty 300,00 zł. Tym samym Zamawiający **dokonuje modyfikacji brzmienia załącznika nr 2a do SIWZ – Projekt umowy**, w zakresie dotyczącym opisanej zmiany.
Zamawiający publikuje ujednolicony tekst załącznika nr 2a do SIWZ – wzór umowy.

Pytanie 34:
Zapis PFU: „Dla systemów wielokamerowych, gdzie skuteczny dozór jest szczególnie istotnym mechanizm analizy obrazu w razie potrzeby alarmuje operatora, także za pośrednictwem urządzeń mobilnych. Co Zamawiający rozumie pod pojęciem „alarmowanie za pośrednictwem urządzeń mobilnych”?

Odpowiedź:
Zamawiający rezygnuje z systemu analizy obrazu, co będzie równoważne z brakiem alarmów ze strony systemu.
Tym samym zmianie ulegają zapisy PFU:

Było:
„Proponuje się system z kamerami IP z inteligentną analizą obrazu gdzie głównym celem jest zapewnienie bezpieczeństwa. VCA pozwala skupić uwagę na potencjalnie podejrzanych zdarzeniach i w razie potrzeby umożliwia proaktywne działanie. Dla systemów wielokamerowych, gdzie skuteczny dozór jest szczególnie istotny mechanizm analizy obrazu w razie potrzeby alarmuje operatora, także za pośrednictwem urządzeń mobilnych.
Całość nagranego materiału wideo powinna być usystematyzowana za pomocą metadanych w sposób umożliwiający natychmiastowe znalezienie właściwych danych przy użyciu funkcji

„wyszukiwania dowolnego materiału w materiale archiwalnym”. Dane pasujące do podanych kryteriów są natychmiast wyświetlane, przez co przeszukiwanie archiwum jest bardzo efektywne.
Aby zoptymalizować koszty całego systemu, analityka powinna być wbudowana w kamerę. Takie rozwiązanie pozwoli zoptymalizować koszty całego systemu bez ponoszenia opłat za dodatkowe oprogramowanie do analityki obrazu oraz dedykowane maszyny sprzętowe obrabiające obraz. Kamera powinna zapewniać wbudowaną analitykę z możliwością stworzenia algorytmów alarmowych min: przekroczenia linii, kierunkowość ruchu, klasyfikacja obiektu (osoba, samochód osobowy, rower/motor, samochód ciężarowy), pozostawienia obiektu, usunięcia obiektu, rozpoznanie koloru, podejrzane zachowanie, wykrycie twarzy, zmiana warunków początkowych, sabotaż, kontrola tłumu, zliczanie osób, detekcja danej trajektorii, detekcja obiektu poruszającego się w przeciwnym kierunku”.

Jest:
Ww. zapis ulega wykreśleniu.

Pytanie 35:
Czy Zamawiający dopuszcza zastosowanie dedykowanych rejestratorów sprzętowych jako urządzeń rejestrujących strumienie z kamer?

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie pod warunkiem spełnienie poniższych parametrów technicznych:

- dedykowany system operacyjny
- możliwość podłączenia i zapisu do 64 kamer 12Mpx
- obsługa formatów H.265+/H.265/H.264+/H.264/MPEG4
- obsługa kamer innych producentów oraz kamer pracujących zgodnie ze standardem ONVIF
- możliwość rejestrowanie strumieni RTSP
- przechowywanie konfiguracji kamer w pamięci rejestratora
- automatyczne zdalne odtwarzanie konfiguracji kamer w przypadku utraty ustawień
- 16 interfejsów SATA, obsługa dysków o pojemności 10TB
- Obsługa RAID0, RAID1, RAID5, RAID6, RAID10 N+1 dyski hot-swap
- System monitorowania stanu dysków HDD oraz powiadamiania aplikację nadzorczą
- Wsparcie dla algorytmów VCA
- Co najmniej 2 wyjścia HDMI, 2 wyjścia VGA (przynajmniej jedno wyjście w rozdzielczości 4K)
- Minimum 2 interfejsy sieciowe 1Gb z obsługą niezależnej pracy interfejsów, trybu rozdzielenia ruchu sieciowego oraz odporność na błędy sieci
- Minimum 3 interfejsy USB (w tym minimum jedno USB3.0)
- Minimum 16 wejść alarmowych, minimum 4 wyjścia alarmowe
- Możliwość pracy w trybie „hotspare”
- Redundantne zasilanie (co najmniej dwa zasilacze)
- Raportowanie stanów alarmowych oraz sabotażowych do aplikacji nadzorczej
- Możliwość integracji z innymi aplikacjami poprzez API/SDK

Tym samym zmianie ulega zapis PFU:

Było:

Serwer zapisu

- Parametry
- Obudowa: Rack 2U
- Procesory: 1 CPU
- Procesor (zamontowany): 1 x 2.10 GHz
- Maksymalna ilość procesorów: 2 szt.
- Pamięć (zamontowana): 8GB (1x8GB) DDR4 2133MHz
- Ilość wolnych gniazd pamięci: 11 szt.
- Maksymalna ilość dysków: 14 szt.
- Dyski Hot Swap : TAK
- Kontroler dysków: Dell Kontroler RAID SAS / SATA PERC H730 z 1GB NV cache
- Poziom Raid: 0, 1, 5, 10, 6
- Gniazda rozszerzeń:
  - Zewnętrzne porty wejścia/wyjścia:
    Szeregowy - 1
    Sieciowy - 2 RJ45
    Grafika - 2 (1 tył, 1 przód)
    USB - 5 (2 tył, 2 przód, 1 wew)
  - Interfejs sieciowy: Dwuportowa karta sieciowa Gigabit Ethernet
- Karta graficzna: 16MB (zintegrowana)
- Zainstalowany napęd: DVD-RW
- Nadmiarowość zasilania: Tak
- Zasilacze Hot Swap : TAK
- Moc zasilacza: 2x 750W (1+1)

Jest:

Serwer zapisu

- Parametry
- Obudowa: Rack 2U
- Procesory: 1 CPU
- Procesor (zamontowany): 1 x 2.10 GHz
- Maksymalna ilość procesorów: 2 szt.
- Pamięć (zamontowana): 8GB (1x8GB) DDR4 2133MHz
- Ilość wolnych gniazd pamięci: 11 szt.
- Maksymalna ilość dysków: 14 szt.
- Dyski Hot Swap : TAK
- Kontroler dysków: Dell Kontroler RAID SAS / SATA PERC H730 z 1GB NV cache
- Poziom Raid: 0, 1, 5, 10, 6
- Gniazda rozszerzeń:
  - Zewnętrzne porty wejścia/wyjścia:
    Szeregowy - 1
    Sieciowy - 2 RJ45
    Grafika - 2 (1 tył, 1 przód)
    USB - 5 (2 tył, 2 przód, 1 wew)
  - Interfejs sieciowy: Dwuportowa karta sieciowa Gigabit Ethernet
- Karta graficzna: 16MB (zintegrowana)
- Zainstalowany napęd: DVD-RW
- Nadmiarowość zasilania: Tak
- Zasilacze Hot Swap : TAK
- Moc zasilacza: 2x 750W (1+1)

LUB

Rejestrator zapisu o wymaganiach minimalnych:

- dedykowany system operacyjny
- możliwość podłączenia i zapisu do 64 kamer 12Mpx
- obsługa formatów H.265+/H.265/H.264+/H.264/MPEG4
- obsługa kamer innych producentów oraz kamer pracujących zgodnie ze standardem ONVIF
- możliwość rejestrowanie strumieni RTSP
- przechowywanie konfiguracji kamer w pamięci rejestratora
- automatyczne zdalne odtwarzanie konfiguracji kamer w przypadku utraty ustawień
- 16 interfejsów SATA, obsługa dysków o pojemności 10TB
- Obsługa RAID0, RAID1, RAID5, RAID6, RAID10 N+1 dyski hot-swap
- System monitorowania stanu dysków HDD oraz powiadamiania aplikację nadzorczą
- Wsparcie dla algorytmów VCA
- Co najmniej 2 wyjścia HDMI, 2 wyjścia VGA (przynajmniej jedno wyjście w rozdzielczości 4K)
- Minimum 2 interfejsy sieciowe 1Gb z obsługą niezależnej pracy interfejsów, trybu rozdzielenia ruchu sieciowego oraz odporność na błędy sieci
- Minimum 3 interfejsy USB (w tym minimum jedno USB3.0)
- Minimum 16 wejść alarmowych, minimum 4 wyjścia alarmowe
- Możliwość pracy w trybie „hotspare”
- Redundantne zasilanie (co najmniej dwa zasilacze)
- Raportowanie stanów alarmowych oraz sabotażowych do aplikacji nadzorczej
- Możliwość integracji z innymi aplikacjami poprzez API/SDK

Pytanie 36:
Co Zamawiający rozumie pod pojęciem „zaawansowanej listy alarmów i statystyki”?

Odpowiedź:
Zamawiający rezygnuje z systemu analizy obrazu, co będzie równoważne z brakiem alarmów ze strony systemu.

Pytanie 37:
Co Zamawiający rozumie pod pojęciem „wyszukiwanie zdarzeń w wybranym obszarze pola widzenia kamery w nagraniach archiwalnych”?

Odpowiedź:
Zamawiający rezygnuje z systemu analizy obrazu, co będzie równoważne z brakiem alarmów ze strony systemu.

Pytanie 38:
Co Zamawiający rozumie pod pojęciem „rejestracja do celów kryminalistycznych”?

Odpowiedź:
Rejestracja do celów kryminalistycznych odnosi się do wykorzystania materiału wideo przez Policję, Straż Miejską lub inne jednostki.

Pytanie 39:
Czy Zamawiający dopuszcza zastosowanie alternatywnych do „WDR – Forensic capture” algorytmów zwiększania zakresu dynamiki zapewniających podobny lub lepszy zakres dynamiki obrazu?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów, dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych oraz o wyższych parametrach.

Pytanie 40:
Czy Zamawiający dopuszcza zastosowanie kamer z nowszym standardem kodowania w stosunku do H.264 jakim jest format H.265?

Odpowiedź:
Tak

Pytanie 41:
Co Zamawiający rozumie pod pojęciem „Automatycznego adaptacyjnego sterowania przepływnością scen”?

Odpowiedź:
Jest to parametr kamer wykorzystujący automatyczne adaptacyjne sterowanie przepływnością za pomocą kodeka (może to być H.264 lub H.265)

Pytanie 42:
Co Zamawiający rozumie pod pojęciem „wyzwalacz ręczny/wirtualne wejścia sygnału”?

Odpowiedź:
Oznaczenie zdarzenia poprzez wyzwolenie ręczne lub w wyniku wejścia sygnału (np. otworzenie szafki przyłącza).

Pytanie 43:
Skoro w PFU jest mowa o kamerach stałopozycyjnych to jak Zamawiający rozumie wymóg „aktywację zintegrowanej obsługi zdarzeń poprzez funkcje PTZ”?

Odpowiedź:
Z uwagi na opisanie kamer stałopozycyjnych funkcje PTZ nie będą wymagane.

Pytanie 44:
Czy Zamawiający oczekuje, aby reakcja kamery w postaci uaktywnienia/dezaktywacji wbudowanego oświetlenia podczerwieni była powiązana ze wszystkimi zdarzeniami wymienionymi na liście na stronie 69 PFU czy tylko wybranymi?

Odpowiedź:
Uaktywnienie/dezaktywacja wbudowanego oświetlenia podczerwieni będzie zależna od natężenia światła.

Pytanie 45:
Co Zamawiający rozumie pod pojęciem „dostosowanego licznika pikseli”?

Odpowiedź:
Jest to funkcja kamery.

Pytanie 46:
Jakie dokładnie protokoły w ramach zapewnienia jakości QoS ma posiadać kamera?

Odpowiedź 46:

Kamera ma posiadać funkcje QoS.

Pytanie 47:
W związku z wycofaniem platformy Windows Phone oraz brakiem dla niej wsparcia, prosimy o rezygnację z zapisów dotyczących tego rozwiązania.

Odpowiedź:
Zamawiający rezygnuje z kompatybilności z systemem Windows Mobile.
Tym samym zmianie ulega zapis PFU:

Str. 41: Było: „Windows Phone"
Str. 42: Było: „Windows Mobile"
Jest: Ww. zapisy zostają wykreślone

Pytanie 48:
W jaki sposób Zamawiający na etapie oceny ofert chce zweryfikować poprawność złożonych ofert pod kątem zgodności zaproponowanych urządzeń/systemów z wymaganiami SIWZ/PFU?
Zamawiający podaje w SIWZ/PFU:
"Przedstawione w niniejszej dokumentacji informacje są materiałem wyjściowym dla Wykonawcy do sporządzenia własnych opracowań projektu koncepcyjnego, a następnie budowlano-wykonawczego itd.; oraz wykonania zadań wchodzących w skład kontraktu.
Zamawiający dopuszcza zmiany w stosunku do przedstawionych wymagań pod warunkiem akceptacji przez Zamawiającego rozwiązań alternatywnych oraz uzyskania przez Wykonawcę wszelkich niezbędnych uzgodnień z osobami trzecimi. Zmiany wynikać mogą z przyjętych rozwiązań branżowych i konieczności do nich dostosowania".
a) Co Zamawiający rozumie przez *„Zamawiający dopuszcza zmiany w stosunku do przedstawionych wymagań pod warunkiem akceptacji przez Zamawiającego rozwiązań alternatywnych oraz uzyskania przez Wykonawcę wszelkich niezbędnych uzgodnień z osobami trzecimi"?*
b) Czy wykonawca, który złoży ofertę, będzie mógł na etapie projektowym zawnioskować o zmiany urządzeń/ systemów, nawet w zakresie odbiegającym od wymagań minimalnych podanych aktualnie w SIWZ/PFU?
c) Podane przez Zamawiającego paramenty urządzeń/systemów wyznaczają pewien standard jakościowy, wpływają na koszty i wycenę oferty. Założenia Zamawiającego są sprecyzowane bardzo czytelnie na tym etapie poprzez właśnie podanie wymagań minimalnych w PFU.
Z uwagi, iż Zamawiający dopuszcza zastosowanie równoważnych urządzeń (podaje również *rozwiązań alternatywnych)* w takim zakresie i w taki sposób, aby zastosowane urządzenia miały parametry techniczne nie gorsze od zaprojektowanych w PFU, konieczne wydaje się zweryfikowanie zgodności ofert z SIWZ/PFU już na etapie ich złożenia i oceny.
Czy Wykonawcy zatem powinni podać podstawowe informacje nt. urządzeń/systemów uwzględnionych przez nich w ofercie, potwierdzającej zgodność z SIWZ/PFU, np. poprzez podanie producenta/ modelu urządzenia/ systemu w Formularzu Cenowym sporządzonym wg wzoru Załącznik nr 3b do SIWZ?

Odpowiedź 48:
a) Dopuszcza się rozwiązania alternatywne nie gorsze od opisanych w PFU. Jako osoby trzecie rozumie się jednostki uczestniczące w kontrakcie(Inżynier Kontraktu, Straż miejska, MZK)
b) Wykonawca może zaproponować inne, nie gorsze rozwiązanie, które będzie rozważone przez Zamawiającego. Przez rozwiązanie „nie gorsze" Zamawiający rozumie rozwiązania zachowujące wszystkie wymagania minimalne podane w PFU z możliwością zastosowania rozwiązań o parametrach wyższych.
c) Zamawiający dokonuje zmiany załącznika 3b do SIWZ – Wzór formularza ofertowego.

Pytanie 49:
Czy Zamawiający dopuści stację roboczą z procesorem z 8,25MB cache zamiast 10 MB?

Odpowiedź:
Zamawiający dopuszcza stacje robocze wyposażone w procesor z 8 MB cache.

Tym samym zmianie ulega zapis PFU:
Było:

Procesor	Procesor klasy x86, 4rdzeniowy, taktowany zegarem co najmniej 3,50GHz, pamięcią cache CPU co najmniej 10 MB, obsługujący pamięci ECC.

Jest:

Procesor	Procesor klasy x86, 4rdzeniowy, taktowany zegarem co najmniej 3,50GHz, pamięcią cache CPU co najmniej 8 MB, obsługujący pamięci ECC.

Pytanie 50:
Zamawiający określa w PFU: *„System kontroli dostępu musi umożliwiać objęcie swoim działaniem wszystkich urządzeń LAN/WLAN dostarczanych w ramach postępowania. Musi posiadać wsparcie producenta w zakresie pomocy technicznej 24x7x365 oraz aktualizacji oprogramowania na okres 24 miesięcy. Dodatkowo dostęp do bazy wiedzy producenta, która zapewnia bezpośredni dostęp np. do dokumentacji. Jeżeli w oferowanym systemie licencje są czasowe, ograniczające w jakikolwiek sposób funkcjonalność rozwiązania, Zamawiający wymaga dostarczenia licencji na okres nie mniejszy niż 5 lat”*
a) Zwracamy się do Zamawiającego o jednoznaczne potwierdzenie minimalnego okresu aktualizacji oprogramowania na System kontroli dostępu do sieci - czy jest to min. 24 miesiące, czy też 5 lat?
b) Czy Zamawiający przez gwarancję na system bezpieczeństwa (gwarancja jest kryterium poza cenowym przy ocenie ofert), rozumie również aktualizację subskrypcji w przypadku systemów bezpieczeństwa w całym okresie zaoferowanej przez wykonawcę gwarancji? W przypadku rozwiązań bezpieczeństwa, gwarancja dotyczy w reguły sprzętu. Dodatkową pozycją są tzw. kontrakty serwisowe pozwalające na aktualizację licencji security.
c) Czy System kontroli dostępu do sieci w chwili uruchomienia, w przypadku zagwarantowania wymaganej wydajności platformy sprzętowej, należy od razu dobrać tak, by tylko poprzez doposażenie platformy sprzętowej w dodatkową licencję obsługiwał on do 5000 systemów końcowych podłączonych do sieci lokalnej LAN lub sieci bezprzewodowej WLAN?

Odpowiedź:
a) Aktualizacja na okres 2 lat, licencja (jeżeli występuje) na okres 5 lat.
b) Przez okres gwarancji należy zapewnić aktualizację subskrypcji.
c) W chwili uruchomienia musi obsługiwać 1500 systemów końcowych z możliwością rozszerzenia do co najmniej 5000 po wykupie odpowiednich licencji.

Pytanie 51:
Podany w specyfikacji PFU benchmark procesora wskazuje na model Intel E5-2620v4, który aktualnie został wyparty przez rozwiązania nowej generacji procesorów Intel. Należy do nich rodzina INTEL XEON, a w tym przypadku procesor XEON Silver 4208.
W związku z powyższym prosimy Zamawiającego o umożliwienie złożenia oferty na procesorze nowej generacji, właśnie na modelu INTEL XEON Silver 4208?

Odpowiedź:

Opis przedmiotu zamówienia nie preferuje konkretnego rozwiązania. Zamawiający określił minimalne parametry wynikające z konieczności zapewnienia określonej funkcjonalności zamawianych urządzeń i zezwala na zaoferowanie urządzeń o wskazanych parametrach oraz o parametrach wyższych niż wskazane. Na rynku dostępnych jest wiele urządzeń spełniających wymagania zamawiającego.
UWAGA:

Pytanie 52:
Zwracamy się do Zamawiającego o potwierdzenie, wyposażenia każdego z 4 modułów serwerowych w 4 dyski twarde?

Odpowiedź:
Zamawiający potwierdza, iż z 4 modułów serwerowych należy wyposażyć w 4 dyski twarde zgodne z podanymi wymaganiami.

Pytanie 53:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„przepustowość Firewall: nie mniej niż 7 Gbps”
Zwracamy się do Zamawiającego o dopuszczenie urządzenia o przepustowości Firewall: nie mniej niż 5 Gbps, nie zmieniając pozostałych kluczowych funkcji IPS'a podanych w wymaganiach?

Odpowiedź:
Zgodnie z odpowiedzią nr 5, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z przepustowością Firewall nie mniejszą niż 5 Gbps.
Zmianę tego parametru, Zamawiający uzasadniania obniżeniem ilości jednoczesnych połączeń oraz nowych połączeń na sekundę.

Tym samym zmianie ulega zapis PFU:
Było: „Przepustowość Firewall: nie mniej niż 7 Gbps”
Jest: „Przepustowość Firewall: nie mniej niż 5 Gbps”

Pytanie 54:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps”
Zwracamy się do Zamawiającego o dopuszczenie urządzenia o wydajności szyfrowania VPN IPSec: nie mniej niż 1
Gbps, nie zmieniając pozostałych kluczowych funkcji IPS'a podanych w wymaganiach? W połączeniu z pozostałymi parametrami wydajnościowymi urządzenia zostanie zagwarantowana

Odpowiedź:
Zgodnie z odpowiedzią nr 6, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z wydajnością szyfrowania VPN IPSec nie mniejszą niż 1 Gbps
Zmianę tego parametru, Zamawiający uzasadniania obniżeniem ilości jednoczesnych połączeń oraz nowych połączeń na sekundę.

Tym samym zmianie ulega zapis PFU:
Było: „Wydajność szyfrowania VPN IPSec: nie mniej niż 4 Gbps”
Jest: „Wydajność szyfrowania VPN IPSec: nie mniej niż 1 Gbps”

Pytanie 55:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:

„system realizujący funkcję Firewall powinien dysponować min. 16 portami Ethernet 10/100/1000 Base-TX”
Uważamy, że przy uwzględnieniu wszystkich obecnych i przyszłych potrzeb Zamawiającego, na klastrze HA urządzeń FW zostanie zutylizowanych kilka portów Ethernet 10/100/1000 Base-TX. Jednocześnie zwracamy uwagę, że liczba 16 portów Ethernet 10/100/1000 Base-TX jest wysoce nadmiarowa.
Zwracamy się do Zamawiającego o dopuszczenie urządzenia wyposażonego w min. 12 portów Ethernet 10/100/1000 Base-TX, każde z dwóch dostarczanych w ramach klastra niezawodnościowego HA?

Odpowiedź:
Zgodnie z odpowiedzią nr 3, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z mniejszą ilością portów Ethernet 10/100/1000 Base-TX, tj. min 12 portów Ethernet 10/100/1000 Base-TX. Ilość nadmiarowych portów w przypadku 12 Ethernet 10/100/1000 Base-TX będzie wystarczającą i zapewnia realizację przyszłych potencjalnych potrzeb.

Tym samym zmianie ulega zapis PFU:
Było: „System realizujący funkcję Firewall powinien dysponować min. 16 portami Ethernet 10/100/1000 Base-TX”
Jest: „System realizujący funkcję Firewall powinien dysponować min. 12 portami Ethernet 10/100/1000 Base-TX”

Pytanie 56:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)”
Zwracamy się do Zamawiającego o dopuszczenie urządzenia, z odstąpieniem od mechanizmu ochrony przed wyciekiem poufnej informacji (DLP). Taka funkcjonalność jest realizowana na stacjach końcowych, np. komputerach, a tylko nieliczni, jak firma Fortinet, wspierają ją na zaporach ogniowych Firewall.

Odpowiedź:
Zgodnie z odpowiedzią nr 8, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie, które nie wspiera mechanizmu ochrony przed wyciekiem poufnej informacji (DLP).

Tym samym zmianie ulega zapis PFU:
Było: Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)
Jest: Zapis „Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP)” ulega wykreśleniu.

Pytanie 57:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS i kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP”
Zwracamy się do Zamawiającego o dopuszczenie urządzenia z odstąpieniem od zapisu dotyczącego protokołu IMAP, w zakresie ochrony przed wirusami i kontroli zawartości poczty. Charakterystyka protokołu IMAP dotyczy wiadomości, które już znajdują się na serwerze pocztowym, natomiast zagrożenia są przechwytywane z wykorzystaniem protokołu SMTP.

Odpowiedź:

Zgodnie z odpowiedzią nr 7, tj. Zamawiający przeanalizował celowość wymogu związanego z ochroną przed wirusami dla protokołu IMAP i odstępuje od wymogu wsparcia dla tego protokołu, przyjmując uzasadnienie podane w pytaniu.

Tym samym zmianie ulega zapis PFU:
Było:
„- Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS
- Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3, IMAP"
Jest:
„- Ochrona przed wirusami – co najmniej dla protokołów SMTP, POP3, HTTP, FTP, HTTPS
- Kontrola zawartości poczty – antyspam dla protokołów SMTP, POP3"

Pytanie 58:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„w zakresie Firewall obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę"
Zwracamy się do Zamawiającego o dopuszczenie urządzenia obsługującego nie mniej niż 500 000 jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę.
Przy skali planowanego projektu, zaproponowane nowe ilości są w zupełności wystarczające, wręcz nadmiarowe. Niepotrzebnie zawyżone wartości, bo nie wyobrażamy sobie, że liczba jednoczesnych połączeń przekroczy 500 000, podnoszą nie potrzebnie koszty systemu (nawet 2 urządzeń które zaplanowano w klastrze). Proszę pamiętać, iż z tym wiążą się koszty aktualizacji oprogramowania bezpieczeństwa w okresie gwarancji udzielonej przez oferentów, i już po nim- koszty Państwa.

Odpowiedź:
Zgodnie z odpowiedzią nr 4, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie w zakresie Firewall obsługa nie mniej niż 500 000 jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę. Proponowana wydajność urządzenia w zakresie jednoczesnych połączeń oraz nowych połączeń na sekundę, uwzględniając faktyczne potrzeby projektowe, jest w pełni wystarczająca.

Tym samym zmianie ulega zapis PFU:
Było: W zakresie Firewall obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30 tys. nowych połączeń na sekundę.
Jest: W zakresie Firewall obsługa nie mniej niż 500 000 jednoczesnych połączeń oraz 20 tys. nowych połączeń na sekundę.

Pytanie 59:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDoS"
Zwracamy się do Zamawiającego o dopuszczenie urządzenia obsługującego 1500 wpisów?
Często producenci sprzętu security, co zależy od zastosowanych technologii i nowszych generacji urządzeń, oferują wykrywanie nawet więcej niż 10 000 zagrożeń, wykorzystując zaledwie 1500 wpisów. Jednocześnie, co można znaleźć w materiałach technicznych firmy Fortinet, wartość 5000 wpisów jest charakterystyczna dla tej firmy.

Odpowiedź:

Zgodnie z odpowiedzią nr 11, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza urządzenie z bazą sygnatur ataków min 1500 wpisów z jednoczesnym dopuszczeniem realizacji tej usługi w sposób równoważny, tj. w sposób i na zasadach zaproponowany przez wykonawcę.

Tym samym zmianie ulega zapis PFU:
Było: „Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos".

Jest: „Ochrona IPS powinna opierać się co najmniej na analizie protokołów i sygnatur. Baza sygnatur ataków powinna zawierać minimum 1500 wpisów. Ponadto administrator systemu powinien mieć możliwość definiowania własnych wyjątków lub sygnatur. Dodatkowo powinna być możliwość wykrywania anomalii protokołów i ruchu stanowiących podstawową ochronę przed atakami typu DoS oraz DDos".

Pytanie 60:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„możliwość budowy min. 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall, IPSec VPN, Antywirus, IPS"
Zwracamy się do Zamawiającego o dopuszczenie urządzenia pozwalającego na uruchomienie pojedynczej instancji systemów, w której w tym samym momencie (czasie) urządzenie pracuje w trybie NAT i w trybie Transparentnym?
Na rynku oferowane są urządzenia nowej generacji, dla których jest możliwe 2 trybów: NAT i Transparentnego (dla routingu), z jednoczesnym wsparciem dla Routingu, Firewall, IPSec VPN, Antywirus, IPS dla obu trybów.
Jednocześnie, co można znaleźć w materiałach technicznych firmy Fortinet, funkcjonalność budowy oddzielnych instancji systemów bezpieczeństwa jest charakterystyczna dla tej firmy.

Odpowiedź:
Zgodnie z odpowiedzią nr 10, tj. Zamawiający dopuszcza możliwość realizacji tej usługi w sposób równoważny, tj. w sposób i na zasadach zaproponowany przez wykonawcę.

Tym samym zmianie ulega zapis PFU:
Było: „Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSecVPN'a, Antywirus'a, IPS'a".

Jest: „Możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów bezpieczeństwa w zakresie Routingu, Firewall'a, IPSecVPN'a, Antywirus'a, IPS'a. lub Możliwość budowy pojedynczej instancji systemów zakładając pracę urządzenia z funkcją NAT i transparentną w tym samym czasie".

Pytanie 61:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„w ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance"
Zwracamy się do Zamawiającego o dopuszczenie urządzenia, w którym ochrona przed malware, spam czy proxyavoidance będzie realizowana za pomocą funkcjonalności równoważnej nazywanej IP Reputation?
Określona w bardzo wąskim rozumieniu funkcjonalność, co można znaleźć w materiałach technicznych firmy Fortinet, jest charakterystyczna dla tej firmy.

Odpowiedź:
Zgodnie z odpowiedzią nr 12, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu, dopuszcza realizację tej usługi w sposób równoważny, tj. za pomocą funkcjonalności pod nazwą IP Reputation w sposób i na zasadach zaproponowanych przez wykonawcę.

Tym samym zmianie ulega zapis PFU:
Było: „W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance".

Jest: „W ramach filtra www powinny być dostępne takie kategorie stron jak: spyware, malware, spam, proxyavoidance lub kategorie stron jak: spyware, malware, spam, proxyavoidance będą realizowane przez funkcjonalność pod nazwą IP Reputation".

Pytanie 62:
Zamawiający podaje w PFU, iż oczekuje rozwiązania, którego:
„rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM"
Zwracamy się do Zamawiającego o dopuszczenie urządzenia z pominięciem zapisu dotyczącego protokołu PIM? Jednocześnie, co można znaleźć w materiałach technicznych firmy Fortinet, funkcjonalność budowy oddzielnych instancji systemów bezpieczeństwa jest charakterystyczna dla tej firmy.

Odpowiedź:
Zgodnie z odpowiedzią nr 9, tj. Zamawiający przychyla się do wniosku zawartego w pytaniu i odstępuje od wymogu wsparcia dla protokołu dynamicznego PIM. Zamawiający przeanalizował założenia i potrzeby projektowe, i zauważa, iż protokół ten nie jest niezbędny.

Tym samym zmianie ulega zapis PFU:
Było: „Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM".
Jest: „Rozwiązanie powinno zapewniać: obsługę Policy Routingu, routing statyczny, dynamiczny w oparciu o protokoły: RIPv2, OSPF, BGP".

Pytanie 63:
Czy Serwer zarządzający ścianą wizyjną w Straży Miejskiej ma być nadzorowany przez to samo oprogramowanie zarządcze, które będzie wdrożone w siedzibie MZK-CZR wraz z serwerem ściany wizyjnej MZK? W PFU, w pozycjach dotyczących Straży Miejskiej, wyspecyfikowano wyłącznie serwer ściany wizyjnej bez oprogramowania do jej zarządzania.
W przypadku, jak obecnie opisany w PFU, nie będzie możliwe zarządzanie różnymi ścianami wizyjnymi w 2 różnych lokalizacjach w sposób niezależny. Prosimy Zamawiającego o ustosunkowanie się do naszej wątpliwości, i potwierdzenie, że ściany wizyjne powinny być całkowicie niezależne i zarządzane przez właściwe służby w sposób zapewniający wykonywanie ich obowiązków, czyli każda z nich powinna posiadać taką samą funkcjonalność pozwalająca na niezależne zarządzanie.

Odpowiedź:
Zarządzanie ścianami wizyjnymi powinno być sterowane niezależnie. Jednocześnie oprogramowanie zastosowane ze sterownikiem w Straży Miejskiej musi realizować wszystkie funkcjonalności określone dla oprogramowania ściany wizyjnej w MZK-CZR.

Pytanie 64:

Czy zamiast wzmacniać ścianę pod monitory w Dyspozytorni, Zamawiający dopuszcza rozwiązanie, z dedykowanym rozwiązaniem pod ścianę wideo, stelażu stojącego na podłodze?

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.

Pytanie 65:
Czy Zamawiający zaakceptuje zmianę systemu operacyjnego procesorów ściany wizyjnej z Windows7 na Windows10.

Odpowiedź:
Tak.
Zmianie ulega zapis PFU:
Było:
„Sterownik powinien mieć architekturę serwera przemysłowego opartego o Windows 7, 64 bit, generując pulpit o rozdzielczości zgodnej z sumą natywnym rozdzielczości monitorów. Maksymalna rozdzielczość pulpitu to 32 tys. x 32 tys. pikseli".

Jest:
„Sterownik powinien mieć architekturę serwera przemysłowego opartego o Windows 7 lub 10, 64 bit, generując pulpit o rozdzielczości zgodnej z sumą natywnym rozdzielczości monitorów. Maksymalna rozdzielczość pulpitu to 32 tys. x 32 tys. pikseli"

Jednocześnie wymagania dla serwera sterującego ścianą wizyjną uzupełnia się o nw. zapis:
„Dla systemu operacyjnego dopuszcza się rozwiązanie równoważne:
Parametry równoważności:
1. Pełna polska wersja językowa interfejsu użytkownika
2. Pełna integracja z domeną Active Directory MS Windows (posiadaną przez Zamawiającego) opartą na serwerach Windows Server 2012
3. Zarządzanie komputerami poprzez Zasady Grup (GPO) Active Directory MS Windows (posiadaną przez Zamawiającego), WMI.
4. Zainstalowany system operacyjny nie wymaga aktywacji za pomocą telefonu lub Internetu.
5. Pełna obsługa ActiveX
6. Wszystkie w/w funkcjonalności nie mogą być realizowane z zastosowaniem wszelkiego rodzaju emulacji i wirtualizacji Microsoft Windows 10
7. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych".

Pytanie 66:
Czy monitory ściany wizyjnej w Straży Miejskiej powinny być również monitorami 46" dedykowanymi do budowy ścian wideo (czyli z wąską ramką), analogicznie jak w przypadku monitorów w MZK-CZR, gdzie została określona szerokość pojedynczej ramki?

Odpowiedź:
Zgodnie z istniejącą infrastrukturą, w pomieszczeniach Straży Miejskiej monitory powinny być wielkości 43" dedykowanymi do budowy ścian wideo, czyli pracującymi w trybie 24h/7. Jednocześnie w przypadku monitorów ściany wizyjnej w Straży Miejskiej dopuszcza się podświetlenie krawędziowe, co jest rozwiązaniem ogólnie przyjętym w monitorach o rozmiarach 43".

Tym samym zmianie ulega zapis PFU:

Było:

Monitory ściany wideo

Projekt obejmuje dostawę i montaż 6 monitorów

(wymagania minimalne):

Wielkość ekranu:	46”
Rodzaj Panelu:	xVA z podświetleniem bezpośrednim W-LED
Kąty widzenia:	178/178 CR 10:1
Jasność:	700cd/m2
Rozdzielczość natywna:	1920 x 1080 pikseli
Rozdzielczość maksymalna:	3840 x 2160 pikseli
Czas reakcji:	8ms
Terminarz umożliwiający zaprogramowanie godzin działania monitora:	TAK
Możliwość zamontowania na ścianie, rozstaw śrub 300 x 300 mm	TAK
Złącza:	Wejścia wideo: DVI, HDMI, Display Port (wersja 1.2), D-SUB, Wyjścia wideo: Display Port(wersja 1.2), Dodatkowe: USB
Wbudowana karta LAN z przełącznikiem sygnału	TAK, 2 x RJ-45
Możliwość pracy 24h/7:	TAK
Korekcja krzywej gamma	10 bit
Możliwość zintegrowania monitora z komputerem poprzez specjalny slot znajdujący się w obudowie monitora	TAK
Czujnik natężenia oświetlenia regulujący jasność monitora w zależności od warunków panujących w pomieszczeniu	TAK, zintegrowany zewnętrzny
Możliwość sterowania monitorem za pomocą oprogramowania dostarczonego przez producenta monitora	TAK
Możliwość zainstalowania opcjonalnych głośników	TAK

Jest:

Monitory ściany wideo

Projekt obejmuje dostawę i montaż 6 monitorów

(wymagania minimalne):

Wielkość ekranu:	43”
Rodzaj Panelu:	technologia AMVA3 z krawędziowym podświetleniem LED
Kąty widzenia:	178/178 CR 10:1
Jasność:	min. 400 cd/m2
Kontrast:	4000:1
Rozdzielczość natywna:	1920 x 1080 pikseli
Czas reakcji:	8ms
Głębokość kolorów	Min. 1.070 (10bit)
Haze Level [%]	Min. Pro (44)
Złącza:	Wejścia wideo: 1 x VGA, 1 x DisplayPort (HDCP); 3 x HDMI (HDCP); Wejścia audio: 2 x 3,5 mm jack, 1 x Interfejs DisplayPort, 3 x HDMI; Kontrola wejścia: 1 x LAN 100Mbit; 1 x Remote Control (3.5 mm jack); 1 x RS232 1 x microSD (MediaPlayer); 1 x USB 2.0 (MediaPlayer)
Głośniki	Zintegrowane (10 W + 10W)
Czujnik natężenia oświetlenia regulujący jasność monitora w zależności od warunków panujących w pomieszczeniu	TAK, zintegrowany zewnętrzny
Możliwość sterowania monitorem za pomocą oprogramowania dostarczonego przez producenta monitora	TAK, zarzadzanie wszystkimi podłączonymi monitorami z centralnej lokalizacji
Możliwość zamontowania na ścianie, rozstaw śrub 300 x 300 mm	TAK
Tryb pracy 24h/7	TAK

Pytanie 67:
Czy w pomieszczeniu Straży Miejskiej należy wykonać jakieś prace adaptacyjne/ ogólnobudowlane, związane z przygotowaniem pomieszczenia pod montaż ściany wizyjnej składającej się z 6 monitorów 46”?

Odpowiedź:
Jeżeli Wykonawca przygotował rozwiązanie wymagające wykonania prac ogólnobudowlanych to na etapie oferty należy przewidzieć takie koszty.

Pytanie 68:
Czy w pomieszczeniu Straży Miejskiej istnieje szafa teletechniczna (RACK) zapewniająca wystarczającą przestrzeń na montaż urządzeń przewidziany zadaniem i opisanych w PFU?

Odpowiedź:
Zamawiający informuje, że w pomieszczeniu Straży Miejskiej istnieje szafa teletechniczna (RACK). Na potrzeby systemu ITS Zamawiający udostępni przestrzeń do 10U.

Pytanie 69:
Czy, zgodnie z oczekiwaniami Zamawiającego, System kopii zapasowych i archiwum danych, powinien również objąć system monitoringu CCTV przystanków i krańcówek, mimo zapisu obrazów na serwerze zapisu CCTV zlokalizowanym w tym samym obiekcie co System kopii zapasowych i archiwum danych?

Odpowiedź:
System kopii zapasowej i archiwum danych nie powinien obejmować systemu CCTV. System CCTV powinien posiadać oddzielny system archiwizacji zapisu na co najmniej 30 dni.

Pytanie 70:
Zamawiający podaje, iż w ramach instalacji elektrycznych należy dostarczyć UPSy o mocy 3 i 6 kVA. Prosimy Zamawiającego o podanie wymagań minimalnych dla UPS 3kVA, który należy wdrożyć w MZK-CZR?

Odpowiedź:
UPS został opisany na stronie 67 i 68 PFU. UPS 3kVA należy dostarczyć i wdrożyć w siedzibie Straży Miejskiej.

Pytanie 71:
Zamawiający specyfikuje wymagania minimalne dla przełączników sieci aktywnej serwerowni i pom. administracyjnego. Łącznie należy wybudować 30 PELi (tj. 60 gniazdek RJ-45 sieci komputerowej) i zakończyć je na przełącznikach w szafach dystrybucyjnych nr 1 i nr 2 wyposażonych w przełączniki agregujące ruch LAN (2 x48 portów RJ-45, Base-T).
Zamawiający nie podaje wymagań dla przełącznika/przełączników sieci optycznej, do których należałoby włączyć 23 przełączniki przemysłowe obsługujące monitoring CCTV na przystankach i podpiąć do serwera zapisu CCTV.
Zwracamy się do Zamawiającego o podanie wymagań dla tych przełączników oraz potwierdzenie, że podobnie jak pozostałe urządzenia LAN/WLAN muszą być one zarządzane z tego samego systemu kontroli dostępu do sieci?

Odpowiedź:
Zamawiający, do włączenia sieci optycznej systemu kamer CCTV z 23 przystanków autobusowych, wymagana dostarczenia do serwerowni MZK-CZR przełącznika sieciowego wyposażonego w min. 24 porty SFP (10/100/1000Eth Base-X) o pozostałych wymaganiach identycznych jak wymagania dla przełączników dostępowych sieci LAN w MZK-CZR. Przełącznik ten należy dodatkowo włączyć do tego samego systemu kontroli dostępu do sieci co pozostałe wszystkie przełączniki sieciowe oraz urządzenia Wifi.

Pytanie 72:
W przypadku przełącznika sieciowego (2 szt.) do serwerowni MZK-CZR (serwerownia kontenerowa):
zwracamy się do Zamawiającego o odstąpienie od części wymogu *„Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia”* poprzez

wykreślenie zapisu *„gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia”* charakterystycznego dla sieci przemysłowych oraz przełączników dedykowanych do tych sieci. W Państwa przypadku należy wdrożyć przełączniki serwerowe, a nie przemysłowe. W przypadku sieci aktywnych, o przeznaczeniu zgodnym z Państwa potrzebami, zastosowanie w przypadku QoS mają standardy określone protokołami np. IEEE 802.1p DiffServ.

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).
Zgodnie z odpowiedzią nr 18, tj. Zamawiający określił minimalne parametry urządzeń. Dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych. Dla przypadku omówionego w pytaniu, Zamawiający uzna za równoważne realizowanie QoS za pomocą standardowych protokołów IEEE 802.1p, DiffServ, który to standard jest typowy dla przełączników sieci LAN (rozwiązań wewnętrznych).

Tym samym zmianie ulega zapis PFU:
Było: „Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia”
Jest: „Mechanizm zachowania jakości usług (QoS) pozwalający ustawiać wymagania dotyczące gwarantowanej przepływności, gwarantowanego opóźnienia i gwarantowanej fluktuacji opóźnienia lub realizowany w sposób równoważny za pomocą standardowych protokołów IEEE 802.1p, DiffServ”

Pytanie 73:
W przypadku przełącznika sieciowego (2 szt.) do serwerowni MZK-CZR (serwerownia kontenerowa):
zwracamy się do Zamawiającego o odstąpienie od części wymogu „Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet)” charakterystycznego dla sieci przemysłowych oraz przełączników dedykowanych do tych sieci. W Państwa przypadku należy wdrożyć przełączniki serwerowe, a nie przemysłowe. W przypadku parametrów związanych z funkcjami bezpieczeństwa definiuje się je poprzez normy RFC.
Prosimy Zamawiającego o podanie równoważnych RFC.

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).

Zgodnie z odpowiedzią nr 19, tj. Poprzez „obsługę mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo”, Zamawiający rozumie mechanizm stosowany w DiffServ polegający na kolejkowaniu, kształtowaniu i ewentualnym ograniczaniu przepływu pakietów w sieci, zgodnie z polityką zdefiniowaną dla każdej klasy. W tym przypadku urządzenie musi minimalnie spełniać standard RFC-2474, RFC-2597, RFC-2598 dla aplikacji czasu rzeczywistego, takich jak np. transmisja głosu czy sygnału wideo.
W związku z powyższym, jeżeli wykonawca zaproponuje urządzenie spełniające RFC-2474, RFC-2597, RFC-2598, to Zamawiający uzna urządzenie za spełniające wymagania.

Tym samym zmianie ulega zapis PFU:
Było: „Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet)”
Jest: „Obsługa mechanizmów dla usług czasu rzeczywistego typu transmisji głosu i wideo (Real Time Ethernet) lub za pomocą norm RFC min. RFC-2474, RFC-2597, RFC-2598”

Pytanie 74:
W przypadku przełącznika sieciowego (2 szt.) do serwerowni MZK-CZR (serwerownia kontenerowa):
Jednocześnie, zwracamy się do Zamawiającego o umożliwienie zaoferowania przełączników do serwerowni wyposażonych po stronie WAN w 2 porty SFP+ oraz 2 porty SFP z jedoczesnym utrzymaniem portów LAN, tj. 48 portów RJ45 10/100/1000 Base-T. Zaproponowana liczna portów WAN z nawiązką spełnia faktyczne potrzeby projektowe oraz zapewnia wszystkie możliwe standardy wysokiej dostępności urządzeń i niezawodności łączy transmisyjnych.

Odpowiedź:
Zakładamy, iż pytanie wykonawczy dotyczy przełączników sieci LAN (str. 25 PFU).
Zamawiający przez port SFP+ rozumie standard transmisji 10 GEth. W załączniku 1 PFU wymaga od przełącznika 2 portów SFP+ 10GEth oraz 2 slotów modułu SFP+ - czyli łącznie 4 interfejsów z przepływnością 10 GbEth oraz 1 portu SFP.
Po przeanalizowaniu założeń projektowych, Zamawiający dopuszcza przełącznik dostępowy wyposażony w ilość portów SFP+/SFP z transmisją 10GEth zaproponowaną przez wykonawcę tj. 4 porty z transmisją 10GEth i odstępuje o wymogu dodatkowego 1 portu SFP, który może być realizowany poprzez jeden z portów SFP+/SFP10GEth. Zamawiający uważa, iż zaproponowana liczba portów WAN w pełni zaspokaja potrzeby projektowe w zakresie stworzenia bezpiecznych i redundantnych połączeń sieci transmisyjnych.

Tym samym zmianie ulega zapis PFU:
Było:
2 x Porty SFP+ 10Gigabit
1 x sloty modułu SFP
2 sloty modułu SFP+

Jest:
2 x Porty SFP+ 10Gigabit
2 sloty modułu SFP+/SFP 10GEth

Pytanie 75:
W celu ujednolicenia sieci LAN oraz objęcia jej spójnym systemem kontroli dostępu do sieci, zwracamy się do Zamawiającego o umożliwienie zaoferowania przełącznika do Straży Miejskiej wyposażonego po stronie WAN w 2 porty SFP+ oraz 2 porty SFP z jedoczesnym utrzymaniem portów LAN, tj. 24 portów RJ45 10/100/1000 Base-T (czyli analogicznego jak w serwerowni MZK-CZR). Zaproponowana liczna portów WAN z nawiązką spełnia faktyczne potrzeby projektowe oraz zapewnia wszystkie możliwe standardy wysokiej dostępności urządzeń i niezawodności łączy transmisyjnych.
W ramach dopuszczenia proponowanego przełącznika, wnioskujemy co Zamawiającego dodatkowo o:
a) obniżenie ze 100 Mpps do 95 Mpps prędkości przekazywania pakietów (dotyczy 24 portów RJ45 10/100/1000 Base-T);
b) pozytywne ustosunkowanie się do zmian wnioskowanych powyżej, tj. z p-pkt a1) i a2) powyżej do przełączników w serwerowni MZK-CZR)

Odpowiedź:
Zakładamy, iż pytanie wykonawcy dotyczy przełącznika sieciowego (PFU, str. 66-67).

Zgodnie z odpowiedzią nr 20, Zamawiający, zważywszy na potrzebę objęcia wszystkich urządzeń sieciowych LAN/WAN i Wifi wspólnym systemem kontroli dostępu do sieci, pozytywnie ustosunkowuje się do wniosku wykonawcy i dopuszcza zaoferowanie w Straży

Miejskiej przełącznika sieciowego o parametrach analogicznych jak dla tego w Serwerowni MZK-CZR z jednoczesnym obniżeniem prędkości przekazywania pakietów na poziomie min. 95 Mpps. Dodatkowo uzasadnia do potrzebą montażu przełącznika sieciowego w szafce RACK, a parametry podane w PFU wskazują na przełącznik przemysłowy.

Pytanie 76:
W celu ujednolicenia sieci LAN oraz objęcia jej spójnym systemem kontroli dostępu do sieci, zwracamy się do Zamawiającego o:
a) dopuszczenie przełącznika przemysłowego wyposażonego w 8 portów 10/100 RJ-45 (PoE+ 30W) oraz 4 porty SFP.
Zaproponowana liczna i rodzaj portów LAN/WAN z nawiązką spełnia faktyczne bieżące i przyszłe potrzeby projektowe oraz zapewnia wszystkie możliwe standardy wysokiej dostępności urządzeń i niezawodności łączy transmisyjnych;
b) dopuszczenie przełącznika o poborze mocy nie większym niż 17W (bez zasilania dedykowanego dla PoE), co nieznacznie odbiega od podanych na sztywno 13,2W (wskazanie na rozwiązanie O-Ring).

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu i dopuszcza przełącznik wyposażony w 8 portów 10/100 RJ-45 (PoE+ 30W) oraz 2 porty SFP i jednocześnie o poborze mocy nie większym niż 17W.

Tym samym zmianie ulega zapis PFU:
Było:
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX z PoE (PSE) – 8
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX - 4
Porty SFP 100/1000 Base-X Auto MDI/MDIX – 2

Pobór mocy (typowo) – maksymalnie 13,2 W

Jest:
Porty RJ-45 min. 10/100 Base-T Auto MDI/MDIX z PoE (PSE) – 8
Porty SFP 100/1000 Base-X Auto MDI/MDIX - 2

Pobór mocy (typowo) – maksymalnie 17 W

Pytanie 77:
W celu ujednolicenia sieci LAN oraz objęcia jej spójnym systemem kontroli dostępu do sieci, zwracamy się do Zamawiającego o dopuszczenie urządzenia, które zapewni spełnienie wymagań dla publicznych sieci dostępu do Internetu określonych przez Urząd Komunikacji Elektronicznej, poprzez wprowadzenie zapisów równoważności, tj.:
urządzenie:
- wyposażone w 2 porty GEth i pracujące w trybach Autonomicznym (Standalone) oraz z Kontrolerem sieci WLAN;
- wbudowany IDS i Device Finger-Printing (rozpoznawanie podłączonych urządzeń);
- zapewniające uruchomienia usługi Portalu Gościnnego (Captive Portal);
- obsługujące min. 802.11ac WAVE 2, 2x2 MIMO oraz posiadające 2 niezależne moduły radiowe 2,4GHz i 5GHz;
- obsługujące 8 SSID na 2,4GHz i 8 SSID na 5GHz;
- wyposażone w Bluetooth (BLE);
- wykrywające zakłócenia i automatycznie dostosowujące sygnał i kanał pracy do zakłóceń;
- zapewniające konfigurację 802.1x, 802.11i, WPA, WPA2; oraz QoS w tym min. TOS, WMM, 802.1p, Diffserv;

- realizujące usługi zgodne z RADIUS oraz standard 802.11r Fast Roaming;
- umożliwiające tworzenie własnych sygnatur aplikacji, z widocznością i kontrolą aplikacji DPI (Deep Packet Inspection);
- umożliwiające wdrożenie usługi Hot-Spot WIFI ze wsparciem wsparcie dla WIPS;
- o klasie odporności IP67 i pracujące w zakresie temperatur min. -40° C do 70° C;
- zgodne z WiFi Alliance i posiadające wymagany certyfikat zgodności.

Odpowiedź:
Zamawiający przychyla się do wniosku zawartego w pytaniu (tj. konieczność objęcia wspólnym systemem kontroli dostępu do sieci wszystkich urządzeń LAN/WLAN) i dopuszcza rozwiązanie równoważne o zaproponowanych parametrach.

Tym samym zmianie ulega zapis PFU:

Było:

Porty	
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX	2
Port PoE PD	obecny na interfejsie ETH2, w pełni zgodny ze specyfikacją IEEE 802.3af Power Device, ochrona przed przeciążeniem i zwarciem, izolacja napięciowa min. 1000 VDC, izolacja obciążeniowa min. 100MΩ
Interfejs WLAN	
Tryby pracy	AP/Bridge/Repeater/AP-Client
Złącze antenowe	2xRP-SMA
Typ częstotliwości radiowej	DSSS
Modulacja IEEE802.11b	CCK, DQPSK, DBPSK
Modulacja IEEE802.11g/n	OFDM z BPSK, QPSK, 16QAM, 64QAM
Pasmo częstotliwości	Ameryka/FCC 2.412~2.462 GHz (11 kanałów), Europa CE/ETSI 2.412~2.472 Ghz (13 kanałów)
Prędkość transmisji	IEEE802.11b 1/2/5.5/11 Mbps, IEEE802.11g 6/9/12/18/24/36/48/54 Mbps, IEEE802.11n do 300Mbps
Moc nadawania	802.11b 17dBm ± 1.5dBm@11Mbps, 802.11g 16dBm ± 1.5dBm@54Mbps, 802.11gn HT20 15dBm ± 1.5dBm @MCS7, 802.11gn HT40 14dBm ± 1.5dBm @MCS7
Czułość odbiornika	802.11b -85dBm ± 2dBm@11Mbps, 802.11g -76dBm ± 2dBm@54Mbps,

	802.11gn HT20 -75dBm ± 2dBm@MCS7, 802.11gn HT40 -72dBm ± 2dBm@MCS7
Bezpieczeństwo transmisji	WEP (obsługa kluczy 64-bit/128-bit), WPA / WPA2 PSK 802.11i (szyfrowanie TKIP i AES), obsługa 802.1X/RADIUS Authentication
Ochrona SSID	wyłączanie rozgłaszania SSID
Obsługa protokołów	ARP, BOOTP, DHCP, DNS, HTTPs, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP (IEEE 802.1D)
Wskaźniki LED	
Wskaźnik zasilania	LED x3 PWR 1(2) (PoE) - czerwony (zasilanie wł. / rozruch), zielony (zasilanie wł. / normalna praca)
Wskaźnik portu RJ-45 100/1000TX	2x zielony dla portu Link/Aktywność 1000Mbps, bursztynowy dla porty Link/Aktywność 100Mbps
Wskaźnik WLAN	zielony Link/Aktywność
Wskaźnik błędu	czerwony - brak połączenie Ethernet lub awaria zasilania
Złącze alarmowe	
Przekazywanie	wyjście alarmowe może przenieść 1A przy 24VDC
Zasilanie	
Wejście zasilania redundantnego	Podwójne wejście 12~48VDC na 6-pinowym złączu terminal block
Pobór mocy (typowo)	8,5W
Ochrona przeciążeniowa prądowa	obecna
Ochrona przed odwrotną polaryzacją	obecna
Charakterystyka fizyczna	
Obudowa	IP-30

Odporność na czynniki zewnętrzne	
Temperatura składowania	-40÷85°C (-40÷185°F)
Temperatura pracy	-10÷60°C (14÷140°F)
Dopuszczalna wilgotność	5%÷95% niekondensująca
Zgodność z normami/zaleceniami	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS),EN61000-4-8, EN61000-4-11

Jest:

Porty	
Porty RJ-45 10/100/1000 Base-T(X) Auto MDI/MDIX	2
Port PoE PD	obecny na interfejsie ETH2, w pełni zgodny ze specyfikacją IEEE 802.3af Power Device, ochrona przed przeciążeniem i zwarciem, izolacja napięciowa min. 1000 VDC, izolacja obciążeniowa min. 100MΩ
Interfejs WLAN	
Tryby pracy	AP/Bridge/Repeater/AP-Client
Złącze antenowe	2xRP-SMA
Typ częstotliwości radiowej	DSSS
Modulacja IEEE802.11b	CCK, DQPSK, DBPSK
Modulacja IEEE802.11g/n	OFDM z BPSK, QPSK, 16QAM, 64QAM
Pasmo częstotliwości	Ameryka/FCC 2.412~2.462 GHz (11 kanałów), Europa CE/ETSI 2.412~2.472 Ghz (13 kanałów)
Prędkość transmisji	IEEE802.11b 1/2/5.5/11 Mbps, IEEE802.11g 6/9/12/18/24/36/48/54 Mbps, IEEE802.11n do 300Mbps

Moc nadawania	802.11b 17dBm ± 1.5dBm@11Mbps, 802.11g 16dBm ± 1.5dBm@54Mbps, 802.11gn HT20 15dBm ± 1.5dBm @MCS7, 802.11gn HT40 14dBm ± 1.5dBm @MCS7
Czułość odbiornika	802.11b -85dBm ± 2dBm@11Mbps, 802.11g -76dBm ± 2dBm@54Mbps, 802.11gn HT20 -75dBm ± 2dBm@MCS7, 802.11gn HT40 -72dBm ± 2dBm@MCS7
Bezpieczeństwo transmisji	WEP (obsługa kluczy 64-bit/128-bit), WPA / WPA2 PSK 802.11i (szyfrowanie TKIP i AES), obsługa 802.1X/RADIUS Authentication
Ochrona SSID	wyłączanie rozgłaszania SSID
Obsługa protokołów	ARP, BOOTP, DHCP, DNS, HTTPs, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, STP (IEEE 802.1D)
Wskaźniki LED	
Wskaźnik zasilania	LED x3 PWR 1(2) (PoE) - czerwony (zasilanie wł. / rozruch), zielony (zasilanie wł. / normalna praca)
Wskaźnik portu RJ-45 100/1000TX	2x zielony dla portu Link/Aktywność 1000Mbps, bursztynowy dla porty Link/Aktywność 100Mbps
Wskaźnik WLAN	zielony Link/Aktywność
Wskaźnik błędu	czerwony - brak połączenie Ethernet lub awaria zasilania
Złącze alarmowe	
Przekazywanie	wyjście alarmowe może przenieść 1A przy 24VDC
Zasilanie	
Wejście zasilania redundantnego	Podwójne wejście 12~48VDC na 6-pinowym złączu terminal block
Pobór mocy (typowo)	8,5W

Ochrona przeciążeniowa prądowa	obecna
Ochrona przed odwrotną polaryzacją	obecna
Charakterystyka fizyczna	
Obudowa	IP-30
Odporność na czynniki zewnętrzne	
Temperatura składowania	-40÷85°C (-40÷185°F)
Temperatura pracy	-10÷60°C (14÷140°F)
Dopuszczalna wilgotność	5%÷95% niekondensująca
Zgodność z normami/zaleceniami	
EMI	FCC Part 15, CISPR (EN55022) class A
EMS	EN61000-4-2 (ESD), EN61000-4-3 (RS), EN61000-4-4 (EFT), EN61000-4-5 (Surge), EN61000-4-6 (CS),EN61000-4-8, EN61000-4-11

Lub równoważny:

- musi mieć możliwość pracy niezależnej (Standalone) oraz pracy z kontrolerem WLAN;
- musi obsługiwać standard 802.11ac Wave 2
- musi posiadać dwa niezależne moduły radiowe pracujące w częstotliwościach 2,4GHz i 5GHz;
- musi posiadać moduł Bluetooth (BLE);
- obsługa 2x2 MIMO;
- musi obsługiwać 8 SSID per moduł radiowy (16 per AP);
- musi posiadać minimum 2 porty Gigabit Ethernet;
- musi posiadać funkcjonalność równomiernego dystrybuowania Klientów pomiędzy punktami dostępowymi i pasmami częstotliwościowymi;
- musi wspierać standard 802.11r Fast Roaming;
- musi wspierać mechanizm wykrywający zakłócenia i automatycznie dostosowywać do nich kanał pracy oraz moc sygnału;
- musi umożliwiać konfigurację 802.1x, 802.11i, WPA, WPA2;
- musi realizować usługi RADIUS;
- musi realizować QoS – minimum WMM, 802.1p, Diffserv i TOS;
- wbudowana widoczność i kontrola aplikacji w oparciu o DPI (Deep Packet Inspection) z możliwością tworzenia własnych sygnatur aplikacji;
- obsługa funkcjonalności rozpoznawania podłączonych urządzeń (Device Fingerprinting);
- musi mieć możliwość uruchomienia usługi Captive Portal;
- musi umożliwiać uruchomienie usługi hotspot;
- musi posiadać wbudowany IDS;
- musi umożliwiać wsparcie dla WIPS;
- musi posiadać certyfikat kompatybilności WiFi Alliance.
- musi posiadać klasę odporności IP67;
- zakres temperatur pracy -40° C do 70° C;
- ochronę wiatrową – min. 165Mph;

Pytanie 78:

Pytania do System monitoringu CCTV przystanków autobusowych i krańcówek.
Zwracamy się do Zamawiającego o udzielenie odpowiedzi do następujących pytań.
1. Zwracamy się do Zamawiającego o dopuszczenie zastosowania certyfikatu stopnia ochrony IPxx równoważnego w stosunku do stopnia ochrony NEMA X4?
2. Zwracamy się do Zamawiającego o wyjaśnienie, co rozumie przez działanie algorytmów w następujących zakresach:
a) kierunkowość ruchu (w jakiej płaszczyźnie?)
b) rozpoznanie koloru (czego? poruszającego się obiektu?)
c) podejrzane zachowanie (jak rozumieć podejrzane zachowanie?)
d) zmiana warunków początkowych (jak zdefiniowane są parametry początkowe?)
e) kontrola tłumu (kontrola w jakim zakresie?)
f) zliczanie osób (w jakim obszarze?, jakie kryteria liczenia?)
g) detekcja danej trajektorii (jak zdefiniowana jest trajektoria?, jakie kryteria?, jakie parametry?, gdzie definiowane?)
h) detekcja obiektu poruszającego się w przeciwnym kierunku (przeciwny w stosunku do czego?)
3. Czy Zamawiający oczekuje aby każda kamera realizowała wszystkie wymienione powyżej funkcje?

Odpowiedź:

1. Zamawiający dopuszcza stopień ochrony równoważny lub wyższy niż NEMA X4
2. Zamawiający rezygnuje z analityki obrazu
3. Zamawiający rezygnuje z analityki obrazu

Pytanie 79:

Zamawiający w treści projektu Umowy, pisze:
W pkt. 6 W przypadku wystąpienia wad objętych odpowiedzialnością wykonawcy z tytułu gwarancji lub rękojmi, Wykonawca zobowiązany jest do ich usunięcia w terminie 14 dni, licząc od dnia powiadomienia go o wadzie, w ramach wynagrodzenia, o którym mowa w §3, w przypadkach uzasadnionych, Zamawiający ma prawo wyznaczyć dłuższy termin usunięcia wady na wniosek wykonawcy.
Oraz
W pkt. 7 W przypadku, gdy usunięcie wady będzie trwało dłużej niż 14 dni lub ze względów technologicznych, prace powinny być wykonane w innym terminie, należy termin ten uzgodnić z Zamawiającym.
Następnie
W pkt. 21 W ramach gwarancji Wykonawca zobowiązany jest do niezwłocznego usuwania powstałych awarii/uszkodzeń Systemu przy czym przez System rozumie się całokształt Inteligentnego Systemu Transportowego, na który składają się w szczególności; podsystem monitoringu, podsystem dynamicznej informacji pasażerskiej (w tym tablice przystankowe), portal pasażera KomunikacjaPabianice.pl wraz z aplikacją mobilną. Wszelkie awarie oraz usterki, będą usuwane przez Wykonawcę w możliwie najkrótszym terminie, tzn.:
1) w przypadku awarii Systemu:
a) czas reakcji - 6 godzin od zgłoszenia,
b) czas usunięcia - maksymalnie 12 godzin od zgłoszenia, przy czym czas reakcji i usunięcia będzie liczony w godzinach 6:00–22:00. W przypadkach awarii, w których konieczny jest dłuższy czas jej usunięcia, Zamawiający po otrzymaniu opisu awarii i harmonogramie napraw może wrazić zgodę na wydłużenie czasu usunięcia awarii maksymalnie do 5 dni od chwili zgłoszenia.
2) w przypadku braku dostępu do infolinii:
a) czas reakcji - 4 godziny od zgłoszenia,

b) czas usunięcia - maksymalnie 12 godzin od zgłoszenia, przy czym czas reakcji i usunięcia będzie liczony w godzinach 6:00–22:00. W przypadkach awarii, w których konieczny jest dłuższy czas jej usunięcia, Zamawiający po otrzymaniu opisu awarii i harmonogramie napraw może wrazić zgodę na wydłużenie czasu usunięcia awarii maksymalnie do 2 dni od chwili zgłoszenia.
Przy powyższych zapisach, zwracamy się do Zamawiającego o jednoznacznie potwierdzenie warunków gwarancji dla:
a) serwerów ścian wizyjnych wraz z monitorami oraz stacji dyspozytorskich z monitorami dla MZK-CZR i Straży Miejskiej;
b) sprzętu serwerowego produkcyjnego dla aplikacji ITS i systemu backupu i archiwizacji danych wyposażenia serwerowni MZK-CZR;
c) kompletnego sprzętu sieciowego LAN/WAN i WIFI wraz z systemem kontroli dostępu do sieci oraz bezpieczeństwa sieci Firewall zastosowanego w zadaniu;
d) kamer monitoringu CCTV przystanków i krańcówek z dedykowanym serwerem zapisu;

Odpowiedź:
Wykonawca udziela gwarancji na wszystkie wbudowane urządzenia oraz systemy z czasami reakcji opisanymi w PFU.

Pytanie 80:
Dot. PFU – sieć pasywna
Zamawiający wskazuje w opisie PFU w niektórych miejscach konieczność budowy kanalizacji dwuotworowej str. 46 PFU :
….Kanalizacja dla kabla światłowodowego min. 48J powinna zostać zaprojektowana i wykonana jako kanalizacja dwuotworowa Fi 100….
Natomiast w drugim akapicie str. 46 PFU jest mowa o konieczności budowy mikrokanalizacji:
niedostatecznej ilości miejsca w pasie drogi lub innej nieruchomości, uniemożliwiającej ułożenie mikrokanalizacji zgodnie z trasą określoną w koncepcji.
Prosimy o doprecyzowanie i wskazanie jakiego typu kanalizacja jest wymagana, jeżeli jest to tańsze rozwiązanie w postaci mikrokanalizacji to prosimy o podanie przekroju wymaganego przez Zamawiającego przy tego typu kanalizacji w celu umożliwienia określenia dokładnych kosztów budowy sieci pasywnej.

Odpowiedź:
Sieć pasywna oparta będzie na zasadzie kanalizacji dwuotworowej oraz kablu światłowodowym min. 48J

Pytanie 81:
Dot.:
„2.1.3. Aplikacja mobilna oraz portal pasażera KomunikacjaPabianice.pl
Aplikacja musi być przystosowana do działania przynajmniej na systemach Android, Windows Phone, iOS.
Pytanie:
W zawiązku z zaniechaniem rozwoju środowiska Windows Phone, prosimy potwierdzenie że Zamawiający rezygnuje z tego środowiska, oraz uzna za wystarczające dostarczenie aplikacji mobilnych dla środowisk Android oraz iOS. Czołowi producenci tego typu aplikacji wspomagających pasażerów komunikacji miejskiej nie mają w podstawowej ofercie wersji oprogramowania dla środowiska Windows Phone. Dodanie tego systemu operacyjnego będzie się wiązało z dodatkowymi znacznymi kosztami oraz wydłużeniem okresu realizacji zadania w tym zakresie. Pragniemy nadmienić, iż posiadacze telefonów wyposażonych w środowisko Windows Phone będą mieli nadal możliwość skorzystania z portalu *KomunikacjaPabianice.pl* poprzez przeglądarkę internetową więc pozostawienie wymogu oddzielnej aplikacji pod ten dedykowany system jest wymaganiem nadmiarowym.

Odpowiedź:
Zamawiający rezygnuje z zapisów o systemie Windows Phone.

Pytanie 82:
Załącznik nr 1 do SIWZ, PFU str. 61 Strona 3
Prosimy Zamawiającego o rezygnację z wymagań zawartych w akapicie 3 na str. 62 PFU związanych z rozbudowaną analityką obrazu. Wymagania zawarte w wymienionym akapicie spowodują dostarczenie kamer, których koszt znacząco będzie przekraczał jednostkowy koszt wymaganych kamer wraz z systemem zarządzania CCTV co jednocześnie podniesie ofertę Wykonawcy. Jednocześnie tak rozbudowana analityka jest wykorzystywana tylko w specyficznych miejscach poddanych szczególnej ochronie, gdzie otoczenie nie jest tak dynamiczne jak w przypadku miejsc montażu tablic informacji przystankowej. W tej chwili zastosowanie dostępnych analityk w takich lokalizacjach może powodować fałszywe wzbudzenia co znacząco utrudni pracę operatora systemu i spowoduje znaczny wzrost kosztów urządzeń jak i licencji niezbędnych dla tego typu rozwiązań

Odpowiedź:
Zamawiający rezygnuje z analityki obrazu.

Pytanie 83:
SIWZ p. 4.6 – str. 6
Zamawiający wskazuje na konieczność integracji 5 biletomatów stacjonarnych produkcji MERA Systemy sp. z. o. o. Jednocześnie punkt 2.2.1. PFU wskazuje na konieczność dostarczenia i instalacji 5 biletomatów stacjonarnych. Prosimy o jednoznaczny określenie czy w ramach zadania należy dostarczyć nowe urządzenia zgodnie z PFU, czy miasto jest w posiadaniu urządzeń firmy MERA i należy je jedynie podłączyć do sieci światłowodowej zgodnie z SIWZ?

Odpowiedź:
Zadanie nie obejmuje dostarczenia biletomatów a jedynie umożliwienie ich podłączenia.

Pytanie 84:
SIWZ p. 4.8 – str. 6
Zamawiający informuje o konieczności wpięcia kamer CCTV oraz Tablic Informacji Pasażerskiej dostarczonych w ramach projektu „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów" do systemów przedmiotowego postępowania. Prosimy o udostępnienie koncepcji / projektów wykonawczych czy specyfikacji dla urządzeń jakie Wykonawca projektu „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów" jest zobowiązany dostarczyć w swoim zadaniu, w celu umożliwienia oszacowania kosztów ich włączenia do systemu dostarczonego w ramach przedmiotowego postępowania.

Odpowiedź:
Zamawiający udostępnia w załączniku specyfikację techniczną tablic informacji pasażerskiej, planowanych do ustawienia w ramach projektu pn. „Łódzki Tramwaj Metropolitalny: etap Pabianice – Ksawerów".

Pytanie 85:
SIWZ p. 4.9 – str. 9
Zgodnie z zapisami SIWZ: „W ramach niniejszego postępowania obowiązują zapisy dotyczące Zadania nr 11 oraz Zadania nr 15." Prosimy o potwierdzenie, iż opis Zadania nr 12 z PFU nie jest objęty przedmiotowym zamówieniem.

Z uwagi na wykluczające się informacje pomiędzy dokumentem SIWZ i PFU w kwestii np. biletomatów – prosimy o określenie ważności / hierarchii dokumentacji dot. przedmiotowego przetargu.

Odpowiedź:
Przedmiotowy przetarg nie obejmuje realizacji zadania 12.

Pytanie 86:
W związku z niejasną sytuacją dotyczącą lokalizacji ściany wizyjnej w siedzibie Straży Miejskiej prosimy o informację, czy Zamawiający może postawić wymaganie dotyczące zamontowania ściany wizyjnej na mobilnej konstrukcji na kółkach. Takie rozwiązanie umożliwi łatwe umiejscowienie jej w obecnie wykorzystywanym centrum monitoringu Straży Miejskiej lub nawet przemieszczenie całości układu monitorów w inne miejsce w siedzibie Straży.

Odpowiedź:
Zgodnie z istniejącą infrastrukturą, w pomieszczeniach Straży Miejskiej monitory powinny być wielkości 43" dedykowanymi do budowy ścian wideo, czyli pracującymi w trybie 24h/7. Jednocześnie w przypadku monitorów ściany wizyjnej w Straży Miejskiej dopuszcza się podświetlenie krawędziowe, co jest rozwiązaniem ogólnie przyjętym w monitorach o rozmiarach 43". Miejscem montażu monitorów przewidywanej ściany wizyjnej jest obecna powierzchnia ścienna, na której zainstalowane są monitory monitoringu wizyjnego.

Tym samym zmianie ulega zapis PFU:

Było:

Monitory ściany wideo

Projekt obejmuje dostawę i montaż 6 monitorów

(wymagania minimalne):

Wielkość ekranu:	46"
Rodzaj Panelu:	xVA z podświetleniem bezpośrednim W-LED
Kąty widzenia:	178/178 CR 10:1
Jasność:	700cd/m2
Rozdzielczość natywna:	1920 x 1080 pikseli
Rozdzielczość maksymalna:	3840 x 2160 pikseli
Czas reakcji:	8ms
Terminarz umożliwiający zaprogramowanie godzin działania monitora:	TAK
Możliwość zamontowania na ścianie, rozstaw śrub 300 x 300 mm	TAK
Złącza:	Wejścia wideo: DVI, HDMI, Display Port (wersja 1.2), D-SUB, Wyjścia wideo: Display Port(wersja 1.2), Dodatkowe: USB
Wbudowana karta LAN z przełącznikiem sygnału	TAK, 2 x RJ-45

Możliwość pracy 24h/7:	TAK
Korekcja krzywej gamma	10 bit
Możliwość zintegrowania monitora z komputerem poprzez specjalny slot znajdujący się w obudowie monitora	TAK
Czujnik natężenia oświetlenia regulujący jasność monitora w zależności od warunków panujących w pomieszczeniu	TAK, zintegrowany zewnętrzny
Możliwość sterowania monitorem za pomocą oprogramowania dostarczonego przez producenta monitora	TAK
Możliwość zainstalowania opcjonalnych głośników	TAK

Jest:

Monitory ściany wideo

Projekt obejmuje dostawę i montaż 6 monitorów

(wymagania minimalne):

Wielkość ekranu:	43”
Rodzaj Panelu:	technologia AMVA3 z krawędziowym podświetleniem LED
Kąty widzenia:	178/178 CR 10:1
Jasność:	min. 400 cd/m2
Kontrast:	4000:1
Rozdzielczość natywna:	1920 x 1080 pikseli
Czas reakcji:	8ms
Głębokość kolorów	Min. 1.070 (10bit)
Haze Level [%]	Min. Pro (44)
Złącza:	Wejścia wideo: 1 x VGA, 1 x DisplayPort (HDCP); 3 x HDMI (HDCP); Wejścia audio: 2 x 3,5 mm jack, 1 x Interfejs DisplayPort, 3 x HDMI; Kontrola wejścia: 1 x LAN 100Mbit; 1 x Remote Control (3.5 mm jack); 1 x RS232 1 x microSD (MediaPlayer); 1 x USB 2.0 (MediaPlayer)

Głośniki	Zintegrowane (10 W + 10W)
Czujnik natężenia oświetlenia regulujący jasność monitora w zależności od warunków panujących w pomieszczeniu	TAK, zintegrowany zewnętrzny
Możliwość sterowania monitorem za pomocą oprogramowania dostarczonego przez producenta monitora	TAK, zarzadzanie wszystkimi podłączonymi monitorami z centralnej lokalizacji
Możliwość zamontowania na ścianie, rozstaw śrub 300 x 300 mm	TAK
Tryb pracy 24h/7	TAK

Pytanie 87:
Jednocześnie prosimy o potwierdzenie dostępności miejsca w istniejącej szafie RACK znajdującej się w serwerowni Straży Miejskiej na montaż w niej sterownika ściany wizyjnej przewidzianego w PFU.

Odpowiedź:
Zamawiający informuje, że na potrzeby systemu ITS Zamawiający udostępni przestrzeń w istniejącej szafie RACK znajdującej się w serwerowni Straży Miejskiej do 10U.

Pytanie 88:
Prosimy o oszacowanie długości drogi kablowej pomiędzy miejscem montażu sterownika ściany wizyjnej a lokalizacją samej ściany, oraz, w przypadku akceptacji rozwiązania mobilnego (pytanie nr 1) o uwzględnienie dodatkowej rezerwy na przemieszczanie ściany w obrębie pomieszczenia, w którym stanie.

Odpowiedź:
Zamawiający nie zna rozwiązań Wykonawcy wobec czego nie jest w stanie określić długości kabli pomiędzy urządzeniami.

Pytanie 89:
Wykonanie sieci PEL w budynku MZK.
Zgodnie z danymi w opublikowanym PFU, wykonawca musi wybudować:
- min. 25 PELi w pomieszczeniach przyległego budynku administracyjnego;
- min. 5 PELi w serwerowni kontenerowej.

Każdy PEL składać się powinien z min. 2 gniazd elektrycznych i 2 gniazd RJ45. Zamawiający dopuszcza rozdzielenie gniazd elektrycznych oraz RJ-45 nie zmieniając ich minimalnej ilości.
Zwracamy się do Zamawiającego o potwierdzenie wybudowania 25 PELI w pomieszczeniach przyległego budynku administracyjnego oraz wskazanie ich potencjalnego rozmieszczenia poprzez naniesienie na istniejących planach.

Odpowiedź:
Instalacje należy wykonać zgodnie z PFU. Zadanie realizowane jest w formule „zaprojektuj i wybuduj" – w związku z tym lokalizację gniazd w serwerowni oraz pomieszczeniach przyległego budynku administracyjnego (dyspozytornia i pozostałe pomieszczenia) Zamawiający będzie uzgadniał z Wykonawcą na etapie projektowania.

Pytanie 90:

W trakcie wizji lokalnej stwierdzono, że na trasie wskazanej w PFU sieci światłowodowej, na ulicy Jana Kilińskiego, prowadzone są prace drogowe w ramach innego postępowania. Prosimy o udostepnienie dokumentacji wspomnianego projektu, w celu określenie czy nie będą występować kolizję z trasą światłowodową obecnego postępowania.

Odpowiedź:
Zamawiający nie dysponuje dokumentacją projektową wspomnianego projektu – inwestorem jest Zarząd Dróg Wojewódzkich w Łodzi, dokumentacja przetargowa jest ogólnodostępna w BIP ZDW.

Pytanie 91:
W trakcie wizji lokalnej stwierdzono, że na trasie wskazanej w PFU sieci światłowodowej, na ulicy Jana Kilińskiego, prowadzone są prace drogowe w ramach innego postępowania. Prosimy o określenie czy w ramach tych prac realizowana jest budowa kanalizacji teletechnicznej?

Odpowiedź:
Zamawiający nie dysponuje dokumentacją projektową wspomnianego projektu – inwestorem jest Zarząd Dróg Wojewódzkich w Łodzi, dokumentacja przetargowa jest ogólnodostępna w BIP ZDW.

Pytanie 92:
Jeżeli w zakresie obecnie trwających prac drogowych na ulicy Jana Kilińskiego, realizowana jest budowa kanalizacji teletechnicznej, czy Zamawiający umożliwi wykorzystanie jej w celu przeprowadzenia trasy sieci światłowodowej dla postępowania „Inteligentny system transportowy”?

Odpowiedź:
Zarządcą ulicy Jana Kilińskiego (droga wojewódzka nr 485) jest Zarząd Dróg Wojewódzkich w Łodzi.

Pytanie 93:
W trakcie wizji lokalnej stwierdzono, że na trasie wskazanej w PFU sieci światłowodowej, na ulicy Jana Kilińskiego, prowadzone są prace drogowe w ramach innego postępowania. Prosimy o wskazanie na mapie na jakich odcinkach drogi prowadzone są te prace?

Odpowiedź:
Przedmiotem inwestycji prowadzonej przez Zarząd Dróg Wojewódzkich w Łodzi jest rozbudowa drogi wojewódzkiej nr 485 klasy G od km 0+926,20 do km 3+244,81 km, tj. na odcinku od posesji Jana Kilińskiego 25 do granicy Pabianic z miejscowością Bychlew.

Pytanie 94:
W związku z obecnie trwającymi pracami drogowymi na ulicy Jana Kilińskiego, w przypadku, gdy na tym odcinku nie jest budowana kanalizacja teletechniczna lub budowana kanalizacja nie będzie mogła być wykorzystana do ułożenia sieci światłowodowej obecnego postepowania „Inteligentny system transportowy”, może istnieć konieczność zmiany przebiegu trasy sieci światłowodowej wskazanej w PFU. Czy Zamawiający dopuszcza takie rozwiązanie?

Odpowiedź 94:
Zamawiający dopuści takie rozwiązanie wyłącznie w uzasadnionych przypadkach.

Pytanie 95:
Na wizji lokalnej ustalono, że zasilanie do nowoprojektowanych elementów ITS, należałoby prowadzić z najbliższych budynków należących do Zamawiającego lub z najbliższych

spółdzielni mieszkaniowych. Zwracamy się z prośbą o wskazanie na mapie „Plan rozmieszczenia elementów ITS na terenie Miasta Pabianice – załącznik nr 1 do PFU", obiektów, z których Wykonawca może poprowadzić zasilanie do nowoprojektowanych elementów systemu ITS?. Takie informacje są niezbędne do przygotowania rzetelnej oferty.

Odpowiedź 95:

Zasilanie należy poprowadzić z przyłączy elektrycznych. Zamawiający przekazuje w załączniku warunki przyłączenia, wydane przez PGE Dystrybucja S.A.

Wyjątkiem może być lokalizacja przystanków Grota-Roweckiego / hala sportowa i Grota-Roweckiego / Kilińskiego – w tym przypadku istnieje możliwość udostępniania przyłącza energetycznego przez Miejski Ośrodek Sportu i Rekreacji – jednostkę budżetową Zamawiającego.

Poniżej przekazujemy sugerowane źródło zasilania. Ostateczna decyzja o sposobie zasilania należy do Wykonawcy.

Nr punktu	**Nazwa przystanku**	**Kierunek**	**Sugerowane źródło zasilania**
1	Dworzec PKP (dla wsiadających)	Centrum	Przyłącze biletomatu
2	Grota-Roweckiego / Bugaj	Centrum	warunki 18/WP/03208/1
3	Grota-Roweckiego / Gryzla	Centrum	Przyłącze biletomatu
4	Grota-Roweckiego / hala sportowa	Waltera-Jankego	MOSiR
5	Grota-Roweckiego / Kilińskiego	Centrum	MOSiR
6	Grota-Roweckiego / Nawrockiego	Waltera-Jankego	Przyłącze biletomatu Roweckiego / Gryzla
7	Jana Pawła II / szpital	Centrum	Przyłącze biletomatu
8	Kilińskiego / SDH	Jankego / Dworzec PKP	Przyłącze biletomatu
9	Kilińskiego / Zamkowa	Jankego / Klimkowizna	Przyłącze biletomatu
10	Nawrockiego / Gawrońska	Waltera-Jankego	warunki 18-DO/WP/03203/1
11	Nawrockiego / Mokra	Centrum	warunki 18-DO/WP/03203/1
12	Nawrockiego / Waltera-Jankego	Centrum	warunki 18-DO/WP/03198/1
13	Orla / Ewangelicka	Dworzec PKP	warunki 18-DO/WP/03224/1
14	Orla / Kilińskiego	Centrum	warunki 18-DO/WP/03224/1
15	Orla / Świętokrzyska	Centrum / Waltera	warunki 18-DO/WP/03225/1
16	Orla / Targowa	Dworzec PKP	warunki 18-DO/WP/03225/1

17	św. Jana / Partyzancka	Centrum / Dw. PKP	warunki 18-DO/WP/03232/1
18	św. Jana / ZS nr 2	Sikorskiego / PZTT / Łódź	warunki 18-DO/WP/03232/1
19	Waltera-Jankego / bl. 221	Centrum / Łódź	warunki 18-DO/WP/03197/1
20	Waltera-Jankego / bl. 243	Centrum / Łódź	warunki 18-DO/WP/03196/1
21	Waltera-Jankego - krańcówka dla wsiadających	Centrum / Łódź	przyłącze krańcówki
22	Wiejska / Łaska	Centrum	warunki 18-DO/WP/03235/1
23	Wiejska / Moniuszki	Centrum / Waltera-Jankego	warunki 18-DO/WP/03234/1

Pytanie 96:
Czy istnieje możliwość poprowadzenia zasilania do nowoprojektowanych elementów ITS z najbliższych latarni oświetleniowych?.

Odpowiedź:
Zamawiający nie wyraża zgody na poprowadzenie zasilenia do projektowanych elementów ITS z latarni oświetleniowych.

Pytanie 97:
W pkt. 2.3.3 Elementy systemu transmisji i monitoringu przystanków i biletomatów, Zamawiający określił wymagania na moduł wejść/wyjść, który ma monitorować m.in. sygnał awarii zasilacza switch'a. Co Zamawiający rozumie pod pojęciem awaria zasilacza switch'a?.

Odpowiedź:
Moduł alarmowy powinien być podłączony tak, aby wykryć awarię zasilania switch'a oraz samego switch'a (nieaktywne porty Ethernet).

Pytanie 98:
W pkt. 2.1.4. „System transmisji danych", Zamawiający piszę o konieczności zastosowania min. 2 włókien do komunikacji dla każdego urządzenia, natomiast w części „Budowa sieci światłowodowej pasywnej" jest zapis, że należy od studni kablowej do elementu ITS poprowadzić kabel min. 12 włóknowy. Zwracamy się z prośbą o ujednolicenie ilości wymaganych włókien światłowodowych.

Odpowiedź:
Zamawiający wymaga co najmniej 12 włókien, dopuszcza się wykorzystanie dwóch tych samych włókien do podłączenia kilku urządzeń z konieczności zapewnienia odporności struktury sieci na awarie.

Pytanie 99:
W PFU w Wymaganiach dla monitorów ściany wizyjnej Zamawiający zapisał, że „wymaga panelu xVA" Czy Zamawiający dopuszcza zastosowanie matrycy IPS zamiast PVA, który jest znacznie bardziej popularny i powszechnie stosowany?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Zamawiający nie dopuszcza możliwości zastosowania paneli IPS niezależnie jakiej są jasności ze względu na ich mniejszą trwałość na utrwalania obrazu oraz niższy współczynnik kontrastu, a co za tym idzie wyższy poziom jasności czerni.
Matryce xVA (w tym PVA) są dedykowane do monitorów pracujących w trybie 365 dni x24h x7 dni w tygodniu i tym samym gwarantują stałą i wymaganą jakość obrazu. Dodatkowo ściana wizyjna złożona z monitorów 46", w lokalizacji MZK-CZR służyć będzie do zobrazowania procesów związanych z systemami ITS, których znakomitą cześć stanowią ciemne tła, w których panele IPS się nie sprawdzają.

Pytanie 100:
W wymaganiach dla monitorów ściany wizyjnej Zamawiający zapisał, że „wejść wideo DVI, HDMI, Display Port (wersja 1.2) oraz wyjść Display Port (wersja 1.2)" a jednocześnie pisze, że wymaga aby do każdego monitora doprowadzać oddzielny sygnał z karty graficznej serwera sterującego oddzielnym kablem światłowodowym i to w standardzie DVI. Takie wymaganie jest nieuzasadnione ekonomicznie bowiem dzisiaj wszystkie karty graficzne mają wyjścia w standardzie Display Port 1.2 lub wyższym i umożliwiają wysterowanie każdym kanałem graficznym co najmniej sygnałów o rozdzielczości 3840x2160. Skoro monitory mają wyjścia Display Port z tzw. pętlą przejścia to uzasadnione ekonomicznie jest wykorzystanie trzech kanałów graficznych Display Port z karty graficznej i przesyłanie tych sygnałów jedynie trzema kablami światłowodowymi Display Port. W każdym kanale przesyłany byłby obraz dla dwóch monitorów tworzących grupę o łącznej, rozdzielczości 2 x 1920x1080 a każdy monitor w ramach grupy wyświetli odpowiednią część takiego obrazu. To rozwiązanie wykorzystuje stosowane powszechnie standardy Display Port. Czy Zamawiający dopuści wykorzystanie pętli przejścia w monitorach i przesyłanie sygnałów z serwera sterującego trzema kablami światłowodowymi Display Port?

Odpowiedź:
W przypadku instalacji przemysłowych nie jest wskazane mnożenie tzw. single points of failure, czyli tworzenie wrażliwych punktów systemu. Jeżeli każdy monitor otrzymuje indywidualny sygnał transmitowany oddzielnie, awaria monitora, extendera lub zasilacza extendera powoduje zanik obrazu na jednym ekranie.
Jeżeli sygnał z procesora obrazu podawany jest dla dwóch monitorów wspólnie, to w razie awarii jednego z urządzeń w kanale transmisyjnym (dzielnik obrazu monitora, extender lub zasilacz extendera) następuje zanik obrazu na dwóch ekranach.
Ze względu na utrzymanie wyższych parametrów niezawodności ściany graficznej Zamawiający utrzymuje koncepcję sześciu obrazów niezależnie generowanych przez procesor graficzny i transmitowanych do monitorów niezależnymi kanałami.

Pytanie 101:
Czy Zamawiający dopuści zastosowanie matrycy IPS w monitorach LCD?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Zamawiający nie dopuszcza możliwości zastosowania paneli IPS niezależnie jakiej są jasności ze względu na ich mniejszą trwałość na utrwalania obrazu oraz niższy współczynnik kontrastu, a co za tym idzie wyższy poziom jasności czerni.
Matryce xVA (w tym PVA) są dedykowane do monitorów pracujących w trybie 365 dni x24h x7 dni w tygodniu i tym samym gwarantują stałą i wymaganą jakość obrazu. Dodatkowo ściana wizyjna złożona z monitorów 46", w lokalizacji MZK-CZR służyć będzie do zobrazowania

procesów związanych z systemami ITS, których znakomitą cześć stanowią ciemne tła, w których panele IPS się nie sprawdzają.

Pytanie 102:
Czy Zamawiający dopuści monitory LCD z matryca IPS , której jasność wynosi 500 cd/m2. Taka jasność jest to absolutnie wystarczające nawet w bardzo jasno oświetlonej dyspozytorni.

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Zamawiający nie dopuszcza możliwości zastosowania paneli IPS niezależnie jakiej są jasności ze względu na ich mniejszą trwałość na utrwalania obrazu oraz niższy współczynnik kontrastu, a co za tym idzie wyższy poziom jasności czerni.
Matryce xVA (w tym PVA) są dedykowane do monitorów pracujących w trybie 365 dni x24h x7 dni w tygodniu i tym samym gwarantują stałą i wymaganą jakość obrazu.

Pytanie 103:
W związku z informacjami, pozyskanymi dzięki wizji lokalnej prosimy Zamawiającego o wskazanie lokalizacji dla Tablic Informacji Przystankowej, gdzie będzie można podłączyć się do budynków będących własnością miasta (jaka lokalizacja dla danego przestanku) i nie będzie konieczności budowy nowego przyłącza energetycznego od zakładu energetycznego. Informacje te są niezbędne do przygotowania rzetelnej i konkurencyjnej oferty.

Odpowiedź 103
Zasilanie należy poprowadzić z przyłączy elektrycznych. Zamawiający przekazuje w załączniku warunki przyłączenia do sieci energetycznej, wydane przez PGE Dystrybucja S.A. Wyjątkiem może być lokalizacja przystanków Grota-Roweckiego / hala sportowa i Grota-Roweckiego / Kilińskiego – w tym przypadku istnieje możliwość udostępniania przyłącza energetycznego przez Miejski Ośrodek Sportu i Rekreacji – jednostkę budżetową Zamawiającego.

Poniżej przekazujemy sugerowane źródło zasilania. Ostateczna decyzja o sposobie zasilania należy do Wykonawcy.

Nr punktu	**Nazwa przystanku**	**Kierunek**	**Sugerowane źródło zasilania**
1	Dworzec PKP (dla wsiadających)	Centrum	Przyłącze biletomatu
2	Grota-Roweckiego / Bugaj	Centrum	warunki 18/WP/03208/1
3	Grota-Roweckiego / Gryzla	Centrum	Przyłącze biletomatu
4	Grota-Roweckiego / hala sportowa	Waltera-Jankego	MOSiR
5	Grota-Roweckiego / Kilińskiego	Centrum	MOSiR
6	Grota-Roweckiego / Nawrockiego	Waltera-Jankego	Przyłącze biletomatu Roweckiego / Gryzla

7	Jana Pawła II / szpital	Centrum	Przyłącze biletomatu
8	Kilińskiego / SDH	Jankego / Dworzec PKP	Przyłącze biletomatu
9	Kilińskiego / Zamkowa	Jankego / Klimkowizna	Przyłącze biletomatu
10	Nawrockiego / Gawrońska	Waltera-Jankego	warunki 18-DO/WP/03203/1
11	Nawrockiego / Mokra	Centrum	warunki 18-DO/WP/03203/1
12	Nawrockiego / Waltera-Jankego	Centrum	warunki 18-DO/WP/03198/1
13	Orla / Ewangelicka	Dworzec PKP	warunki 18-DO/WP/03224/1
14	Orla / Kilińskiego	Centrum	warunki 18-DO/WP/03224/1
15	Orla / Świętokrzyska	Centrum / Waltera	warunki 18-DO/WP/03225/1
16	Orla / Targowa	Dworzec PKP	warunki 18-DO/WP/03225/1
17	św. Jana / Partyzancka	Centrum / Dw. PKP	warunki 18-DO/WP/03232/1
18	św. Jana / ZS nr 2	Sikorskiego / PZTT / Łódź	warunki 18-DO/WP/03232/1
19	Waltera-Jankego / bl. 221	Centrum / Łódź	warunki 18-DO/WP/03197/1
20	Waltera-Jankego / bl. 243	Centrum / Łódź	warunki 18-DO/WP/03196/1
21	Waltera-Jankego - krańcówka dla wsiadających	Centrum / Łódź	przyłącze krańcówki
22	Wiejska / Łaska	Centrum	warunki 18-DO/WP/03235/1
23	Wiejska / Moniuszki	Centrum / Waltera-Jankego	warunki 18-DO/WP/03234/1

Pytanie 104:
Prosimy o informacje czy Zamawiający posiada warunki przyłączenia do sieci energetycznej nowo budowanych Tablic Informacji Przystankowej.

Odpowiedź:
Zamawiający przekazuje w załączniku warunki przyłączenia do sieci energetycznej, wydane przez PGE Dystrybucja S.A.

Pytanie 105:
W PFU na stronie 34 w części „Wyposażenie serwerowe” w punkcie 4e Zamawiający wymaga aby serwery posiadały zainstalowane kontrolery obsługujące m.in. RAID 1E. RAID 10 posiada podobne parametry, jednak jest bardziej niezawodny i częściej spotykany w rozwiązaniach vendorów niż RAID 1E. Czy Zamawiający dopuści kontroler obsługujący RAID 10 zamiast RAID 1E?

Odpowiedź:

Zamawiający podtrzymuje zapis PFU. W przypadku zastosowania kontrolera obsługującego RAID 1E uzyskujemy lepszą wydajność serwerów co jest głównie zasługą większej liczby dysków przestrzeni storage.
Główna różnica między RAID 1E i RAID 10 polega na tym, że w przypadku RAID 1E uzyskuje się wymaganą ochronę przy użyciu mniejszej liczby dysków, co tym samym podnosi wydajność serwerów z zadaną pojemnością storage.

Pytanie 106:
W PFU na stronie 34 w części „Wyposażenie serwerowe" w punkcie 4c Zamawiający wymaga aby zainstalowane w serwerach procesory zostały wybrane na podstawie testu wydajności SPECint_rate2006. Powołując się na wyniki SPECint_rate2006 Zamawiający rezygnuje z najnowszych modeli procesorów, które nie występują w tych testach, co ograniczy wydajność zaproponowanej konfiguracji oraz może w przyszłości powodować problem z dostępnością procesora. Czy Zamawiający dopuści zainstalowanie dwóch procesorów 8-rdzeniowych w architekturze x86 osiągających w oferowanym serwerze min. 83 pkt w testach wydajności SPECrate2017_int_base?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów, dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych oraz o wyższych parametrach. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Jeżeli Wykonawca wykaże większą wydajność proponowanych urządzeń to Zamawiający zaakceptuje takie rozwiązanie.

Pytanie 107:
W PFU na stronie 35 w części „Wyposażenie serwerowe" w punkcie 4h Zamawiający wymaga aby zaoferowane serwery posiadały zintegrowaną kartę graficzną ze złączem VGA oraz 2xUSB 3.0. Jednocześnie Zamawiający specyfikuje system wysokiej gęstości upakowania, co z definicji wymusza wiele kompromisowych rozwiązań związanych z fizycznymi aspektami. Czy Zamawiający zaakceptuje dostępność portu VGA, dwóch portów USB 2.0 oraz portu szeregowego na przejściówce z modułu KVM wbudowanego w serwer oraz portu USB 3.0 wbudowanego w ten moduł?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów. Dopuszcza się zastosowanie przejściówki z modułu KVM pod warunkiem spełnienia minimalnych wymagań co do ilości i typów portów/złącz użytecznych dla każdego pojedynczego serwera.

Pytanie 108:
W PFU na stronie 34 w części „Wyposażenie serwerowe" w punkcie 4b Zamawiający wymaga aby zaoferowane serwery posiadały minimum 2 złącza PCI Express generacji 3 o prędkości x16. Jednocześnie Zamawiający specyfikuje system wysokiej gęstości upakowania, co z definicji wymusza wiele kompromisowych rozwiązań związanych z fizycznymi aspektami. Ponadto sloty PCIe x16 są rzadko wykorzystywane, głównie na potrzeby bardzo wymagających kart jak GPU. Czy Zamawiający zaakceptuje serwer wyposażony w 2 sloty PCIe 3.0 x8 low-profile lub 1 slot PCIe 3.0 x16?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów, dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych oraz o wyższych parametrach. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Dopuszcza się zaoferowanie serwera o większej ilości złącz PCI Express pod warunkiem, że co najmniej dwa z nich będą złączami PCI Express x16.

Pytanie 109:
W PFU na stronie 34 w części „Wyposażenie serwerowe” w punkcie 1 Zamawiający wymaga aby zaoferowane serwery obsługiwały minimum po 6 dysków Hot-Plug 2,5. W rozwiązaniach modularnych dyski w serwerach są przeznaczone pod instalację systemu operacyjnego dlatego też wymóg posiadania 6 dysków twardych przez serwer jest bezpodstawny. Czy zamawiający dopuści serwery, które mają możliwość instalacji min. 2 dysków twardych i dopuści rozwiązanie z 2 dyskami 2,5 cala o pojemności 1.2TB 10K SAS?

Odpowiedź:
Zamawiający określił minimalne parametry urządzeń lub systemów, dopuszcza się zaprojektowanie i wdrożenie urządzeń równoważnych oraz o wyższych parametrach. Nie dopuszcza się zastosowania urządzeń o niższych parametrach. Zamawiający nie dopuszcza serwerów, które mają możliwość instalacji min. 2 dysków twardych.
Serwery modularne zostały zaprojektowane także w innym celu niż tylko po instalację systemu operacyjnego, również pod kątem zapewnienia dedykowanych zasobów dla wszystkich komponentów systemowych ITS. Wersja modularna serwerów gwarantuje dodatkowo zintegrowane zarządzanie zasobami sprzętowymi, wyższą niezawodność platformy ITS oraz efektywność kosztową utrzymania infrastruktury sprzętowej w okresie gwarancji i trwałości projektu.

Pytanie 110:
Dotyczy tablic informacji pasażerskiej. Zamawiający w opisie funkcjonalności tablicy informacji pasażerskiej opisuje *„Możliwość prezentacji informacji pasażerskiej innych przewoźników”*. Czy Zamawiający posiada i zapewni dostęp do źródła tych informacji?

Odpowiedź:
Zarząd Dróg i Transportu w Łodzi wyraził wolę udostępniania danych niezbędnych do przekazywania danych o faktycznych godzinach odjazdów środków transportu publicznego organizowanego przez ZDiT (linia autobusowa nocna N4B) po zakończeniu okresu trwania gwarancji udzielanego przez firmę Sprint, który upływa w 2020 r.
W przypadku prezentacji informacji pasażerskiej innych przewoźników, Zamawiający będzie posługiwał się statycznym rozkładem jazdy – lub – jeżeli otrzyma źródła informacji o danych dynamicznych, przekaże je wówczas.

Pytanie 111:
Dotyczy tablic informacji pasażerskiej. Z doświadczenia producenta tablic informacji pasażerskiej wynika, że raster 5,6mm x 5,6mm to bardzo nietypowy i niestosowany w praktyce raster. Czy Zamawiający dopuszcza raster diod matryc LED w zakresie 6 mm x 6 mm przy jednoczesnej rozdzielczości 192 x 64 diod ?

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.

Pytanie 112:
Dotyczy tablic informacji pasażerskiej. Po wielu analizach stosowanych w transporcie publicznym matryc LED w warunkach zewnętrznych jasność świecenia diod LED powinna mieścić się w zakresie min 4 500–5 000 cd/m2. Czy Zamawiający dopuszcza wskazaną jasność diod?

Odpowiedź:
Zamawiający dopuszcza jasność świecenia diod LED na poziomie min. 4500 cd/m2.

Tym samym ulega zmianie zapis PFU:
Było: „Minimalna jasność świecenia diod LED – 6000cd/m^2”
Jest: „Minimalna jasność świecenia diod min. 4500cd/m^2”

Pytanie 113:
Dotyczy tablic informacji pasażerskiej. Czy w zakresie wyświetlanych kolorów Zamawiający dopuszcza kolor: bursztynowy (amber – długość emitowanej fali w zakresie 585-610 nm)?

Odpowiedź:
Zgodnie z zapisami PFU, cyt. „ilość wyświetlanych kolorów – minimum jeden (bursztynowy lub biały – do uzgodnienia z Zamawiającym), Zamawiający dopuszcza również rozwiązania z większą liczbą kolorów możliwych do skonfigurowania”. W związku z powyższym, Zamawiający dopuszcza kolor bursztynowy. Niemniej informujemy, że kolorem preferowanym jest kolor biały.

Pytanie 114:
Dotyczy tablic informacji pasażerskiej. Czy Zamawiający dopuszcza również, aby osłonę macierzy diod stanowiła zabezpieczona szyba bezpieczna laminowana z powłoką antyrefleksyjną?

Odpowiedź:
Zamawiający dopuszcza takie rozwiązanie.

Pytanie 115:
Dotyczy tablic informacji pasażerskiej. System autodiagnostyki – prosimy o doprecyzowanie jakich dokładnie parametrów oczekuje Zamawiający oraz w jakiej formie i gdzie mają być przesyłane?

Odpowiedź:
Zamawiający oczekuje informacji o ewentualnych uszkodzenia podzespołów tablicy. Wykonawca musi zapewnić funkcjonowanie takiego systemu oraz zaproponować na etapie projektu formę raportu, lokalizacja – centrum nadzoru.

Pytanie 116:
Dotyczy tablic informacji pasażerskiej. Czy Zamawiający wyraża zgodę na wykreślenie zapisu „statyczne sterowanie stałym źródłem prądu”?

Odpowiedź 116:
Zamawiający odstępuje od tego wymogu.

Tym samym ulega zmianie zapis PFU:
Było: „Wydłużona żywotność z zachowaniem dużej energooszczędności (statyczne sterowanie stałym źródłem prądu)”
Jest: Zamawiający wykreśla ww. zapis z PFU.

Pytanie 117:
Dotyczy tablic informacji pasażerskiej. W zakresie ogólnodostępnego punktu dostępowego prosimy o doprecyzowanie kto dostarczy łącze internetowe dla w/w punktów / jakie źródło internetu do tych punktów przewiduje Zamawiający?

Odpowiedź:
Wykonawca będzie odpowiedzialny za dostarczenie Internetu do punków dostępowych.

Pytanie 118:
Dotyczy tablic informacji pasażerskiej. Ile kamer w punktach tablicowych przewiduje Zamawiający?

Odpowiedź:
Co najmniej dwie kamery na punkt tablicowy.

Pytanie 119:
Zwracam się z uprzejmą prośbą o udostępnienie wszystkich wymaganych formularzy dotyczących ww. postępowania w wersji edytowalnej.

Odpowiedź:
Zamawiający udostępnia wymagane formularze dotyczące postępowania w wersji edytowalnej.

Zamawiający dokonuje także modyfikacji zapisów specyfikacji istotnych warunków zamówienia w zakresie terminu składania i otwarcia ofert oraz warunków płatności w związku z czym poniżej przedstawione zapisy SIWZ otrzymują nowe brzmienie:

W rozdziale XIV pt. SKŁADANIE I OTWARCIE OFERT, w ust. 14.2 oraz 14.3

dotychczasowy zapis:

14.2 Termin składania ofert upływa w dniu ***03.04.2020 r. o godz. 10:00.***

14.3. Otwarcie ofert nastąpi w dniu ***03.04.2020 r. o godz. 12:00*** w siedzibie: ***Urzędu Miejskiego w Pabianicach ul. Zamkowa 16, 95-200 Pabianice, pokój nr 4.***

otrzymuje nowe brzmienie:

14.2 Termin składania ofert upływa w dniu ***22.04.2020 r. o godz. 10:00.***

14.3. Otwarcie ofert nastąpi w dniu ***22.04.2020 r. o godz. 12:00*** w siedzibie: ***Urzędu Miejskiego w Pabianicach ul. Zamkowa 16, 95-200 Pabianice, pokój nr 4.***

W załączniku nr 2a do SIWZ w paragrafie 4 pt: Warunki płatności" dotychczasowy

zapis ust. 1:

"

§ 4. Warunki płatności

1. Zamawiający zapłaci wynagrodzenie Wykonawcy w częściach po zakończeniu niżej wymienionych etapow inwestycji, zgodnie z kwotami, ujętymi w Formularzu cenowym:
1) opracowanie projektu budowlanego oraz uzyskanie przez Wykonawcę wszelkich uzgodnień (w tym zatwierdzenia Zamawiającego), opinii i decyzji administracyjnych niezbędnych do rozpoczęcia prac budowlanych, przedstawienie do zatwierdzenia przez Zamawiającego projektu wykonawczego,
2) wykonanie sieci optycznej,
3) wykonanie systemu monitoringu,
4) wykonanie stacji dyspozytorskich,

5) wykonanie systemu ITS,
6) wykonanie tablic przystankowych,
7) monitoring,
8) adaptacja pomieszczeń, rozbudowa serwerowni,
9) szkolenia, kalibracja systemu, uruchomienie.

2. Podstawą wystawienia faktur częściowych będą podpisane przez wskazanego przedstawiciela Zamawiającego oraz Inżyniera Kontraktu Protokoły Odbioru Częściowego, a dla płatności końcowej Protokół Odbioru Końcowego Przedmiotu Umowy oraz ewentualne inne dokumenty wymagane Umową lub przepisami prawa, w szczególności szkice geodezyjne i dokumentacja powykonawcza. Protokół musi zostać podpisany przez Zamawiającego oraz Wykonawcę. Odbiory jednostronne przez Wykonawcę są wykluczone w każdym wypadku.

3. Warunkiem zapłaty przez Zamawiającego należnego wynagrodzenia za odebrane roboty budowlane jest przedstawienie przez Wykonawcę stosownych dowodów zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom, biorącym udział w realizacji odebranych robot budowlanych.

4. W przypadku nieprzedstawienia przez Wykonawcę wszystkich dowodów zapłaty, o których mowa powyżej, Zamawiający wstrzymuje wypłatę należnego wynagrodzenia za odebrane roboty budowlane w części równej sumie kwot wynikających z nieprzedstawionych dowodów zapłaty.

5. Wystawienie faktur częściowych następuje na kwoty wskazane w Formularzu cenowym. Faktury wystawione niezgodnie z postanowieniami Umowy, w szczególności bez wymaganych dokumentów, będą zwracane bez obowiązku płatności.

6. Faktury wystawione będą na:
– nabywcę: Miasto Pabianice, ul. Zamkowa 16, 95-200 Pabianice, NIP 731-196-27-56,
– odbiorcę: Urząd Miejski w Pabianicach, ul. Zamkowa 16, 95-200 Pabianice.

7. Środki na realizację zadania zabezpieczono w Wieloletniej Prognozie Finansowej Gminy Miejskiej Pabianice na lata 2020-2021 w ramach projektu pn. „Modernizacja i rozwój komunikacji miejskiej w Pabianicach".

8. Faktury płatne będą w terminie 30 dni, licząc od daty doręczenia Zamawiającemu prawidłowo wystawionych faktur wraz z Protokołami Odbioru Częściowego i Protokołem Odbioru Końcowego dla płatności końcowej i wszystkimi wymaganymi dokumentami, w szczególności odnoszącymi się do Podwykonawcow. Należność Wykonawcy płatna będzie w formie przelewu z rachunku Zamawiającego na rachunek Wykonawcy, wskazany na fakturze.

9. Wykonawca zobowiązuje się do umieszczania na fakturach numeru rachunku bankowego zawartego na dzień zlecenia przelewu w wykazie podmiotów, o którym mowa w art. 96b ust. 1 ustawy o podatku od towarów i usług (t.j. Dz.U. 2018 poz. 2174 z poźn.zm.). Zamawiający będzie realizował płatności wyłącznie na rachunki bankowe zawarte w rejestrze o którym mowa w zdaniu poprzednim.

10. Wykonawca ma prawo skorzystania z możliwości przekazania ustrukturyzowanej faktury elektronicznej oraz innych ustrukturyzowanych dokumentów elektronicznych na zasadach określonych w ustawie z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2018 r. poz. 2191).

11. Wykonawca nie może, bez pisemnej zgody Zamawiającego, przenieść na osobę trzecią wierzytelności wynikającej z niniejszej umowy. Potrącenie dokonane przez Wykonawcę z wierzytelnością Zamawiającego wymaga zgody Zamawiającego udzielonej na piśmie pod rygorem nieważności.

12. W razie powierzenia części Przedmiotu Umowy podwykonawcy, stosuje się zasady określone w § 7 Umowy.

13. Datą płatności jest dzień złożenia dyspozycji zapłaty z rachunku bankowego Zamawiającego."

Otrzymuje nowe brzmienie:

”

§ 1. Warunki płatności

1. Zamawiający zapłaci wynagrodzenie Wykonawcy w częściach po zakończeniu niżej wymienionych etapów inwestycji, zgodnie z kwotami, ujętymi w Formularzu cenowym:

   1) opracowanie projektu budowlanego oraz uzyskanie przez Wykonawcę wszelkich uzgodnień (w tym zatwierdzenia Zamawiającego), opinii i decyzji administracyjnych niezbędnych do rozpoczęcia prac budowlanych, przedstawienie do zatwierdzenia przez Zamawiającego projektu wykonawczego,

   2) wykonanie sieci optycznej,

   3) wykonanie kontrolera ściany graficznej,

   4) wykonanie systemu monitoringu,

   5) wykonanie stacji dyspozytorskich,

   6) wykonanie systemu ITS,

   7) wykonanie tablic przystankowych,

   8) monitoring,

   9) adaptacja pomieszczeń, rozbudowa serwerowni,

   10) szkolenia, kalibracja systemu, uruchomienie.

2. Podstawą wystawienia faktur częściowych będą podpisane przez wskazanego przedstawiciela Zamawiającego oraz Inżyniera Kontraktu Protokoły Odbioru Częściowego, a dla płatności końcowej Protokół Odbioru Końcowego Przedmiotu Umowy oraz ewentualne inne dokumenty wymagane Umową lub przepisami prawa, w szczególności szkice geodezyjne i dokumentacja powykonawcza. Protokół musi zostać podpisany przez Zamawiającego oraz Wykonawcę. Odbiory jednostronne przez Wykonawcę są wykluczone w każdym wypadku.

3. Warunkiem zapłaty przez Zamawiającego należnego wynagrodzenia za odebrane roboty budowlane jest przedstawienie przez Wykonawcę stosownych dowodów zapłaty wymagalnego wynagrodzenia podwykonawcom i dalszym podwykonawcom, biorącym udział w realizacji odebranych robót budowlanych.

4. W przypadku nieprzedstawienia przez Wykonawcę wszystkich dowodów zapłaty, o których mowa powyżej, Zamawiający wstrzymuje wypłatę należnego wynagrodzenia za odebrane roboty budowlane w części równej sumie kwot wynikających z nieprzedstawionych dowodów zapłaty.

5. Wystawienie faktur częściowych następuje na kwoty wskazane w Formularzu cenowym. Faktury wystawione niezgodnie z postanowieniami Umowy, w szczególności bez wymaganych dokumentów, będą zwracane bez obowiązku płatności.

6. Faktury wystawione będą na:

   – nabywcę: Miasto Pabianice, ul. Zamkowa 16, 95-200 Pabianice, NIP 731-196-27-56,

   – odbiorcę: Urząd Miejski w Pabianicach, ul. Zamkowa 16, 95-200 Pabianice.

7. Środki na realizację zadania zabezpieczono w Wieloletniej Prognozie Finansowej Gminy Miejskiej Pabianice na lata 2020-2021 w ramach projektu pn. „Modernizacja i rozwój komunikacji miejskiej w Pabianicach”.

8. Faktury płatne będą w terminie 30 dni, licząc od daty doręczenia Zamawiającemu prawidłowo wystawionych faktur wraz z Protokołami Odbioru Częściowego i Protokołem Odbioru Końcowego dla płatności końcowej i wszystkimi wymaganymi dokumentami, w szczególności odnoszącymi się do Podwykonawców. Należność Wykonawcy płatna będzie w formie przelewu z rachunku Zamawiającego na rachunek Wykonawcy, wskazany na fakturze.

9. Wykonawca zobowiązuje się do umieszczania na fakturach numeru rachunku bankowego zawartego na dzień zlecenia przelewu w wykazie podmiotów, o którym mowa w art. 96b ust. 1 ustawy o podatku od towarów i usług (t.j. Dz.U. 2018 poz. 2174 z późn.zm.). Zamawiający będzie realizował płatności wyłącznie na rachunki bankowe zawarte w rejestrze o którym mowa w zdaniu poprzednim.

10. Wykonawca ma prawo skorzystania z możliwości przekazania ustrukturyzowanej faktury elektronicznej oraz innych ustrukturyzowanych dokumentów elektronicznych na zasadach określonych w ustawie z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (Dz. U. z 2018 r. poz. 2191).

11. **Zamawiający, działając na podstawie art. 4. ust. 4 z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych oraz w związku z § 1 Rozporządzenia Ministra Przedsiębiorczości i Technologii z dnia 25 kwietnia 2019 r. w sprawie listy innych ustrukturyzowanych dokumentów elektronicznych, które mogą być przesyłane za pośrednictwem platformy elektronicznego fakturowania służącego do przesyłania ustrukturyzowanych faktur oraz innych ustrukturyzowanych dokumentów elektronicznych (Dz. U. z 2019 r., poz. 856), nie wyraża zgody na przesyłanie za pośrednictwem platformy innych ustrukturyzowanych dokumentów elektronicznych wskazanych w art. 2 pkt 3 tej ustawy, z wyłączeniem ustrukturyzowanej faktury elektronicznej.**

12. **Wykonawca zamierzający wysyłać ustrukturyzowane faktury elektroniczne za pośrednictwem PEF jest zobowiązany do uwzględniania czasu pracy Zamawiającego, umożliwiającego zamawiającemu terminowe wywiązanie się z zapłaty wynagrodzenia Wykonawcy. W szczególności Zamawiający informuje, że przesyłanie ustrukturyzowanych faktur elektronicznych winno nastąpić w godzinach: pn., śr., czw.: 816, wt.: 8-17, pt.: 8-15. W przypadku przesłania ustrukturyzowanej faktury elektronicznej poza godzinami pracy, w dni wolne od pracy lub święta, a także w godzinach innych niż wymienione powyżej, uznaje się, że faktura ta została doręczona w następnym dniu roboczym.**

13. Wykonawca nie może, bez pisemnej zgody Zamawiającego, przenieść na osobę trzecią wierzytelności wynikającej z niniejszej umowy. Potrącenie dokonane przez Wykonawcę z wierzytelnością Zamawiającego wymaga zgody Zamawiającego udzielonej na piśmie pod rygorem nieważności.

14. W razie powierzenia części Przedmiotu Umowy podwykonawcy, stosuje się zasady określone w § 7 Umowy.

15. Datą płatności jest dzień złożenia dyspozycji zapłaty z rachunku bankowego Zamawiającego.”

Pozostałe zapisy SIWZ nie ulegają zmianie.

Prezydent Miasta Pabianic

/-/Grzegorz Mackiewicz