SPECYFIKACJA
ISTOTNYCH WARUNKÓW ZAMÓWIENIA
(SIWZ)

w postępowaniu o udzielenie zamówienia publicznego prowadzonym
w trybie przetargu nieograniczonego
na
modernizację infrastruktury Platformy Usług Elektronicznych (PUE)

Wartość zamówienia przekracza równowartość kwoty 135 000 EURO

Warszawa, 2016 r

SPIS TREŚCI

Rozdział I
INFORMACJE OGÓLNE

I. INFORMACJA O ZAMAWIAJĄCYM

Zamawiającym jest **Zakład Ubezpieczeń Społecznych** z siedzibą w Warszawie (01-748 Warszawa), ul. Szamocka 3, 5, tel. 22 667-17-04, faks 22 667-17-33/36.

II. TRYB UDZIELENIA ZAMÓWIENIA I WARTOŚĆ ZAMÓWIENIA

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie przetargu nieograniczonego na podstawie przepisów ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2015 r. poz. 2164, t.j.) zwanej dalej ustawą.

Wartość zamówienia:
Wartość zamówienia przekracza wyrażoną w złotych równowartość kwoty 134 000 euro, o której mowa w przepisach wydanych na podstawie art. 11 ust. 8 ustawy.

III. OFERTY CZĘŚCIOWE, WARIANTOWE

1. Oferta musi obejmować całość przedmiotu zamówienia wskazanego w Rozdziale II niniejszej Specyfikacji.
2. Każdy Wykonawca ma prawo złożyć tylko jedną ofertę.
3. Zamawiający nie dopuszcza możliwości składania ofert wariantowych w rozumieniu art. 2 pkt 7) ustawy.
4. Zamawiający nie dopuszcza składania ofert częściowych.
5. Zamawiający dopuszcza możliwość składania ofert równoważnych w zakresie i na zasadach określonych w Rozdziale II, podrozdział I, ust. 2 SIWZ oraz w załączniku nr 1 do Wzoru umowy, który stanowi Załącznik nr 2 do SIWZ.

IV. FORMA PRZEKAZYWANIA INFORMACJI, OŚWIADCZEŃ I DOKUMENTÓW W POSTĘPOWANIU ORAZ KOPII ODWOŁAŃ

1. Oświadczenia, wnioski, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują faksem lub mailem w postaci skanu dokumentu z podpisem, z uwzględnieniem ust. 2. Nr faksu Zamawiającego: 22 667 17 33/36. Adres email Zamawiającego: SekretariatDZP@zus.pl
2. Forma pisemna zastrzeżona jest dla złożenia oferty wraz z załącznikami (dotyczy również uzupełnienia oferty – art. 26 ust. 3 ustawy), w tym oświadczeń i dokumentów potwierdzających spełnianie warunków udziału w postępowaniu oraz oświadczeń i dokumentów potwierdzających spełnianie przez oferowany przedmiot zamówienia wymagań określonych przez Zamawiającego, a także zmiany lub wycofania oferty, z zastrzeżeniem specyfikacji technicznej (opisu) produktów, dla której formę określono w Załączniku A do Formularza ofertowego (Załącznik nr 1 do SWIZ).
3. Wykonawca potwierdza niezwłocznie fakt otrzymania oświadczenia, wniosku, zawiadomienia lub informacji poprzez podpisanie pierwszej strony dokumentu i jej odesłanie na faks lub email Zamawiającego.

4. Jeżeli Wykonawca przekaże oświadczenia, wnioski, zawiadomienia oraz informacje faksem/mailem i pisemnie, za datę ich złożenia przyjmuje się datę wpływu pierwszego dokumentu - dokument uważa się za złożony w terminie jeżeli jego treść dotarła do adresata przed upływem wyznaczonego terminu, z zastrzeżeniem ust. 2.
5. W przypadku wniesienia odwołania, Odwołujący przesyła kopię odwołania Zamawiającemu za pomocą faksu – wyłącznie na nr 22 667 17 33 / 36 lub drogą elektroniczną – wyłącznie na adres email: SekretariatDZP@zus.pl

V. OSOBY UPRAWNIONE DO KONTAKTÓW Z WYKONAWCAMI

Osobą uprawnioną do kontaktu z Wykonawcami jest:
imię i nazwisko: Marta Wałkuska
stanowisko służbowe: Starszy Specjalista
tel. 22 667-17-28
email: marta.walkuska@zus.pl
godziny urzędowania: 8:30 – 16:30

VI. ZAMÓWIENIE UZUPEŁNIAJĄCE

Zamawiający nie przewiduje udzielenia zamówienia uzupełniającego na przedmiot zamówienia określony w Rozdziale II niniejszej Specyfikacji.

VII. INFORMACJE DODATKOWE

1. Postępowanie, którego dotyczy niniejszy dokument oznaczone jest znakiem: **TZ/271/79/15**. Wskazane jest aby Wykonawcy we wszelkich kontaktach z Zamawiającym powoływali się na ten znak.
2. Istnieje możliwość uzyskania załączników do SIWZ niezbędnych do przygotowania oferty (Załączniki nr 1, 3, 4, 5 do SIWZ) w wersji elektronicznej, pod warunkiem przekazania Zamawiającemu prośby wraz z podaniem adresu poczty elektronicznej (email) Wykonawcy.

Rozdział II

OPIS PRZEDMIOTU ZAMÓWIENIA I TERMIN WYKONANIA

I. PRZEDMIOT ZAMÓWIENIA

1. Przedmiotem zamówienia jest **modernizacja infrastruktury Platformy Usług Elektronicznych (PUE)** poprzez zwiększenie mocy obliczeniowej oraz bezpieczeństwa przetwarzania danych, w tym dostarczenie urządzeń oraz licencji na oprogramowanie wraz z 36 miesięczną gwarancją i usługami wdrożeniowymi – zgodnie z Opisem przedmiotu zamówienia, stanowiącym załącznik nr 1 do Wzoru umowy (Załącznik nr 2 do SIWZ).
2. Wszędzie tam gdzie przedmiot zamówienia został opisany przez wskazanie znaków towarowych, patentów lub pochodzenia dopuszcza się zaoferowanie produktów równoważnych. Za produkty równoważne Zamawiający uzna produkty o nie gorszych parametrach technicznych niż produkty określone w Opisie przedmiotu zamówienia. W przypadku zaoferowania produktów równoważnych, których zastosowanie prowadzi do zmiany platformy, za produkt równoważny zostanie uznane rozwiązanie obejmujące:
   1) dostosowanie (wraz z migracją) wszystkich aplikacji pracujących w PUE oraz oprogramowania systemowo narzędziowego do prawidłowej pracy na zaoferowanym rozwiązaniu;
   2) zapewnienie nieprzerwanego, prawidłowego funkcjonowania PUE przez cały okres trwania umowy;
   3) zapewnienie mechanizmów ciągłości działania dla zaproponowanej platformy wraz z dostosowaniem wszystkich procedur eksploatacyjnych, administratorskich dla zaproponowanych rozwiązań;
   4) przeszkolenie pracowników (administratorów i operatorów) Zamawiającego z zastosowanych rozwiązań techniczno-systemowych.
3. **Kod Wspólnego Słownika Zamówienia (CPV):**

   30236000-2 – Różny sprzęt komputerowy
   48000000-8 – Pakiety oprogramowania i systemy informatyczne
   48820000-2 – Serwery
   72541000-9 – Usługi rozbudowy sprzętu komputerowego
   80510000-2 – Usługi szkolenia specjalistycznego

II. TERMIN WYKONANIA ZAMÓWIENIA, WARUNKI REALIZACJI ZAMÓWIENIA I PŁATNOŚCI

1. Termin realizacji przedmiotu zamówienia, z wyłączeniem szkoleń, o których mowa w pkt 12.8 (cz. III) Załącznika nr 1 do Wzoru umowy (stanowiącego Załącznik nr 2 do SIWZ) – do 6 miesięcy od daty zawarcia umowy.
2. Termin realizacji szkoleń, o których mowa w pkt 12.8 (cz. III) Załącznika nr 1 do Wzoru umowy (stanowiącego Załącznik nr 2 do SIWZ) – do dnia 31 grudnia 2016 roku.
3. Miejsce dostawy przedmiotu zamówienia:
   1) Szamocka 3, 01-748 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Centralnego Ośrodka Obliczeniowego (COO) w Warszawa;

2) Czerniakowska 16, 00-701 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Zapasowego Centralnego Ośrodka Obliczeniowego (ZCOO) w Warszawie.

4. Opis przedmiotu zamówienia oraz warunki realizacji zostały określone w Załączniku nr 2 do SIWZ, tj. we Wzorze umowy i jej załącznikach.
5. Szczegółowe warunki płatności wynagrodzenia za wykonanie przedmiotu zamówienia zostały określone w Załączniku nr 2 do SIWZ, tj. we Wzorze umowy.
6. Dostarczony w ramach niniejszego zamówienia sprzęt komputerowy oraz urządzenia sieciowe muszą być fabrycznie nowe i muszą pochodzić z bieżącej produkcji, tj. wyprodukowane nie wcześniej niż 6 miesięcy przed datą zawarcia umowy, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia (ang. refurbished), a także muszą być wolne od wad oraz posiadać pełen zestaw przewidzianych przez producenta właściwych nośników (np. sterowniki).
7. Oferowany sprzęt komputerowy oraz urządzenia sieciowe, jeśli jest to dla nich wymagane, muszą posiadać certyfikat CE lub deklarację zgodności CE.
8. Oferowany sprzęt komputerowy oraz urządzenia sieciowe muszą spełniać wymogi określone w Rozporządzeniu Ministra Gospodarki z dnia 8 maja 2013 r. w sprawie zasadniczych wymagań dotyczących ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz. U. z 2013 r., poz. 547).
9. Wykonawca dostarczy sprzęt komputerowy oraz urządzenia sieciowe, zgodnie z wymaganiami zawartymi w Opisie przedmiotu zamówienia, wraz z niezbędnym okablowaniem, dokumentacją techniczno-eksploatacyjną, certyfikatami bezpieczeństwa oraz dokumentami potwierdzającymi udzielenie Zamawiającemu gwarancji na te urządzenia.

Rozdział III
WYSOKOŚĆ I ZASADY WNIESIENIA WADIUM

I. WYSOKOŚĆ WADIUM

Wykonawca przystępujący do postępowania jest zobowiązany wnieść wadium w wysokości: **400 000,00 zł** (słownie złotych: czterysta tysięcy 00/100).

II. FORMA WADIUM

Wadium może być wniesione w jednej lub kilku z poniższych form:

1) pieniądzu,
2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że poręczenie kasy jest zawsze poręczeniem pieniężnym,
3) gwarancjach bankowych,
4) gwarancjach ubezpieczeniowych,
5) poręczeniach udzielonych przez podmioty, o których mowa w art. 6 b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2007 r., Nr 42, poz. 275 z późn. zm.).

III. TERMIN I MIEJSCE WNIESIENIA WADIUM

1. Wadium należy wnieść przed upływem terminu składania ofert określonego w Rozdziale VI, podrozdział I pkt 1.
2. W przypadku wnoszenia wadium w pieniądzu ustaloną kwotę należy wpłacić na rachunek bankowy Zamawiającego nr **81 1020 5590 0000 0602 9000 7017 (PKO BP S.A.).**

   Wadium winno znaleźć się na rachunku bankowym Zamawiającego przed upływem terminu składania ofert.
   Zaleca się aby na przelewie umieścić informację: **„wadium do postępowania Modernizacja infrastruktury PUE, znak sprawy: TZ/271/79/15”.**
3. W przypadku wnoszenia wadium w pozostałych dopuszczalnych formach określonych w podrozdziale II kserokopię dokumentu potwierdzającego wniesienie wadium zaleca się dołączyć do oferty, a oryginał należy złożyć w siedzibie Zamawiającego w Warszawie ul. Szamocka 3, 5 Departament Zamówień Publicznych, pok. 104 (I piętro, skrzydło „C”).
4. Z dokumentu wadium wniesionego w formie gwarancji bankowej/ubezpieczeniowej powinno wynikać jednoznacznie gwarantowanie wypłat należności w sposób nieodwołalny, bezwarunkowy i na pierwsze żądanie Zamawiającego zawierające oświadczenie o okolicznościach stanowiących podstawę do żądania wypłaty należności.
5. Wadium takie powinno obejmować cały okres związania ofertą, poczynając od daty składania ofert.
6. Nie wniesienie wadium w wymaganym terminie (także na przedłużony okres związania ofertą), wysokości lub formie skutkuje wykluczeniem Wykonawcy z postępowania.

IV. ZWROT WADIUM

1. Zamawiający zwróci wadium wszystkim Wykonawcom niezwłocznie po wyborze oferty najkorzystniejszej lub unieważnieniu postępowania, z wyjątkiem Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, z zastrzeżeniem ust. 2 podrozdziału V „Zatrzymanie Wadium”.
2. Wykonawcy, którego oferta została wybrana jako najkorzystniejsza, Zamawiający zwróci wadium niezwłocznie po zawarciu umowy w sprawie zamówienia publicznego oraz wniesieniu zabezpieczenia należytego wykonania umowy, jeżeli jego wniesienia żądano.
3. Zamawiający zwróci wadium niezwłocznie na pisemny wniosek Wykonawcy, który wycofał ofertę przed upływem terminu składania ofert.
4. Jeżeli wadium wniesiono w pieniądzu, Zamawiający zwraca je wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonym o koszty prowadzenia rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek Wykonawcy.

V. ZATRZYMANIE WADIUM

1. Wykonawca, którego oferta została wybrana, traci wadium wraz z odsetkami na rzecz Zamawiającego w sytuacjach, gdy:
   1) odmówił podpisania umowy na warunkach określonych w ofercie;
   2) nie wniósł wymaganego zabezpieczenia należytego wykonania umowy;
   3) zawarcie umowy stało się niemożliwe z przyczyn leżących po stronie Wykonawcy.

2. Zamawiający zatrzymuje wadium wraz z odsetkami, jeżeli Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 26 ust. 3 ustawy, z przyczyn leżących po jego stronie, nie złożył dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1 ustawy, pełnomocnictw, listy podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5) ustawy, lub informacji o tym, że nie należy do grupy kapitałowej, lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3) ustawy, co powodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej.

Rozdział IV
WARUNKI UDZIAŁU W POSTĘPOWANIU, OPIS SPEŁNIENIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU, OFERTA ORAZ DOKUMENTY WYMAGANE OD WYKONAWCY

I. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy spełniają warunki dotyczące:
   1) posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
   2) posiadania wiedzy i doświadczenia;
   3) dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
   4) sytuacji ekonomicznej i finansowej.
2. O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonali, a w przypadku świadczeń okresowych lub ciągłych wykonują, co najmniej **2 dostawy** odpowiadające przedmiotowi zamówienia, **każda** o wartości równej lub przekraczającej kwotę **8 000 000,00 zł brutto,** w tym co najmniej jedna z nich obejmująca swoim zakresem również wdrożenie, konfigurację dostarczonych urządzeń sieciowych, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie. Poprzez dostawę odpowiadającą przedmiotowi zamówienia należy rozumieć należycie zrealizowane dostarczenie sprzętu sieciowego, takiego jak: routery, przełączniki sieciowe, zapory sieciowe itp. W przypadku zamówień, które są w trakcie realizacji, wykonana część musi odpowiadać powyższym wymaganiom.

   W przypadku Wykonawców składających wspólną ofertę przynajmniej jeden z nich musi wykazać się spełnieniem warunku, o którym mowa powyżej. W przypadku, gdy Wykonawca polega na wiedzy i doświadczeniu innych podmiotów, to co najmniej jeden z nich powinien samodzielnie spełnić powyższy warunek udziału w postępowaniu. W przypadku, gdy Wykonawca wykaże na potwierdzenie spełnienia powyższego warunku udziału w postępowaniu, dostawy, przy realizacji których brał udział, jako członek konsorcjum, z dowodów, czy dostawy zostały wykonane lub są wykonywane należycie, powinien wynikać zakres prac wykonanych przez Wykonawcę, jako członka konsorcjum.
3. O udzielenie zamówienia ubiegać się mogą Wykonawcy, którzy nie podlegają wykluczeniu z postępowania o udzielenie zamówienia.

4. Wykonawcy mogą polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych lub ekonomicznych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków.

II. WYMOGI FORMALNE OFERTY

1. Oferta musi spełniać następujące wymogi:
   a) treść oferty musi odpowiadać treści niniejszej Specyfikacji;
   b) oferta musi zostać sporządzona w języku polskim w formie pisemnej, na maszynie do pisania, komputerze lub inną trwałą i czytelną techniką;
   c) oferta i załączone do niej oświadczenia i dokumenty, wymagane przez Zamawiającego, sporządzone przez Wykonawcę, muszą być podpisane – za podpisanie uznaje się własnoręczny podpis złożony (w sposób umożliwiający identyfikację osoby) przez osobę(-y) upoważnioną(-e) do reprezentowania Wykonawcy;
   d) poprawki lub zmiany w ofercie, muszą być dokonane w sposób czytelny, parafowane własnoręcznie przez osobę(-y) podpisującą(-e) ofertę.
2. Zaleca się, aby:
   a) każda strona oferty była parafowana przez osobę podpisującą ofertę;
   b) wszystkie strony oferty wraz z załącznikami były ponumerowane oraz połączone w sposób trwały;
   c) materiały nie wymagane przez Zamawiającego, tj. nie stanowiące oferty (druki i foldery reklamowe), były wyraźnie oznaczone i oddzielone od oferty;
   d) osoba(-y) podpisująca(-e) ofertę opatrzyła(-y) swój podpis pieczątką imienną.
3. W przypadku, gdy informacje zawarte w ofercie stanowią tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.), **Wykonawca powinien to wyraźnie zastrzec w ofercie** i odpowiednio oznaczyć zastrzeżone informacje oraz **wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa**.

   Zgodnie z art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, przez tajemnicę przedsiębiorstwa rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

   W świetle powołanego przepisu, zgodnie z wyrokiem Sądu Najwyższego z dnia 3 października 2000 r. (I CKN 304/00), określona informacja stanowi tajemnicę przedsiębiorstwa, jeżeli spełnia łącznie trzy warunki:

   1) ma charakter techniczny, technologiczny, organizacyjny przedsiębiorstwa lub posiada wartość gospodarczą,
   2) nie została ujawniona do wiadomości publicznej,
   3) podjęto w stosunku do niej niezbędne działania w celu zachowania poufności.

   Wskazane jest wyodrębnienie dokumentów zawierających zastrzeżone informacje.

   Informujemy, iż zgodnie z art. 8 ust. 3 ustawy, **Zamawiający nie będzie występował o uzupełnienie lub wyjaśnienie złożonego w ofercie zastrzeżenia tajemnicy przedsiębiorstwa oraz jego uzasadnienia**. Zamawiający oceni zastrzeżenie tajemnicy

przedsiębiorstwa oraz jego uzasadnienie. W przypadku uznania przez Zamawiającego, że Wykonawca nie wykazał w ofercie, że informacje i dokumenty stanowią tajemnicę przedsiębiorstwa, **Zamawiający uzna to zastrzeżenie za bezskuteczne.** W takim przypadku oferta będzie jawna również w zakresie nieskutecznie objętym tajemnicą przedsiębiorstwa, o czym Zamawiający poinformuje Wykonawcę.

Nie podlegają zastrzeżeniu informacje obejmujące: nazwę (firmę) oraz adres Wykonawcy, cenę oferty, termin wykonania zamówienia, okres gwarancji i warunki płatności.

III. WYMAGANE DOKUMENTY

1. Wykonawca składa wraz z ofertą następujące dokumenty i oświadczenia:

1.1. Oświadczenia i dokumenty potwierdzające spełnianie warunków udziału w postępowaniu:

1) oświadczenie potwierdzające spełnianie przez Wykonawcę warunków określonych w art. 22 ust. 1 ustawy, sporządzone wg wzoru stanowiącego Załącznik nr 3 do Specyfikacji;

2) wykaz wykonanych bądź wykonywanych dostaw na potwierdzenie warunku, o którym mowa w Rozdziale IV, podrozdział I, ust. 2 SIWZ, sporządzony wg wzoru stanowiącego Załącznik nr 5 do Specyfikacji.

3) jeżeli Wykonawca polega na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia, zdolnościach finansowych lub ekonomicznych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków, zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował tymi zasobami w trakcie realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia.

1.2. Oświadczenia i dokumenty o braku podstaw do wykluczenia z postępowania o udzielenie zamówienia:

1) oświadczenie o braku podstaw do wykluczenia z postępowania, sporządzone wg wzoru stanowiącego Załącznik nr 4 do Specyfikacji;

2) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2) ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

3) aktualne zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że Wykonawca nie zalega z opłacaniem podatków lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;

4) aktualne zaświadczenie właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że Wykonawca nie zalega z opłacaniem składek na ubezpieczenie zdrowotne i społeczne lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie

lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;

5) aktualna informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4) – 8) oraz pkt 10) i 11) ustawy, wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

6) aktualna informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9) ustawy, wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

7) lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5) ustawy lub informacja o tym, że Wykonawca nie należy do grupy kapitałowej.

1.3. Oświadczenia i dokumenty potwierdzające, że oferowany przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego dla przedmiotu zamówienia:

1) wypełniony Załącznik A do Formularza ofertowego;

2) specyfikacja techniczna (opis) produktów, które mają zostać dostarczone Zamawiającemu, na potwierdzenie spełniania warunków określonych w Załączniku A do Formularza ofertowego – w formie określonej w Załączniku A do Formularza ofertowego.

1.4. Inne wymagane oświadczenia i dokumenty:

1) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik - pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy;

2) w przypadku, gdy ofertę składają Wykonawcy ubiegający się wspólnie o udzielenie zamówienia wymagane jest załączenie dokumentu pełnomocnictwa określającego zakres umocowania pełnomocnika ustanowionego do reprezentowania ich w postępowaniu, stosownie do art. 23 ust. 2 ustawy;

3) dokument potwierdzający wniesienie wadium, jeżeli zostało wniesione w innej formie niż w pieniądzu (zaleca się dołączyć).

2. Jeżeli, w przypadku Wykonawcy mającego siedzibę na terytorium Rzeczypospolitej Polskiej, osoby, o których mowa w art. 24 ust. 1 pkt 5) - 8), pkt 10) i 11) ustawy, mają miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, Wykonawca składa w odniesieniu do nich zaświadczenie właściwego organu sądowego albo administracyjnego miejsca zamieszkania dotyczące niekaralności tych osób w zakresie określonym w art. 24 ust. 1 pkt 5)-8), pkt 10) i 11) ustawy, wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert, z tym że w przypadku gdy w miejscu zamieszkania tych osób nie wydaje się takich zaświadczeń - zastępuje się je dokumentem zawierającym oświadczenie złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego miejsca zamieszkania tych osób lub przed notariuszem.

3. Wykonawca zagraniczny

3.1. Wykonawca zagraniczny (mający siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej) zamiast dokumentów wskazanych w pkt 1.2.:

1) ppkt 2), 3), 4), 6) – składa dokument lub dokumenty, wystawione w kraju, w którym

ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że:

a) nie otwarto jego likwidacji ani nie ogłoszono upadłości – wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,

b) nie zalega z uiszczaniem podatków, opłat, składek na ubezpieczenie społeczne i zdrowotne albo że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu – wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert,

c) nie orzeczono wobec niego zakazu ubiegania się o zamówienie – wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

2) ppkt 5) - składa zaświadczenie właściwego organu sądowego lub administracyjnego miejsca zamieszkania osoby, której dokumenty dotyczą, w zakresie określonym w art. 24 ust. 1 pkt 4) – 8), pkt 10) i 11) ustawy - wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

3.2. Jeżeli w miejscu zamieszkania osoby lub w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów wskazanych w pkt 3.1. zastępuje się je dokumentem zawierającym oświadczenie, w którym określa się także osoby uprawnione do reprezentacji Wykonawcy, złożone przed właściwym organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego odpowiednio kraju miejsca zamieszkania osoby lub kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, lub notariuszem - wystawione odpowiednio w terminach określonych w pkt 3.1.

IV. ZASADY UDZIAŁU W POSTĘPOWANIU WYKONAWCÓW WYSTĘPUJĄCYCH WSPÓLNIE

1. Wykonawcy ubiegający się wspólnie o udzielenie zamówienia ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
2. Wykonawcy, o których mowa w ust. 1, składają jedną ofertę, przy czym:
   a) wymagane oświadczenia i dokumenty wskazane w podrozdziale III pkt 1.2 niniejszego Rozdziału składa każdy z Wykonawców,
   b) oświadczenie potwierdzające spełnianie warunków określonych w art. 22 ust.1 ustawy – wszyscy Wykonawcy wspólnie,
   c) pozostałe dokumenty składają wszyscy Wykonawcy wspólnie.

V. FORMA DOKUMENTÓW

1. Wymagane dokumenty powinny być złożone w formie oryginału lub kserokopii potwierdzonej za zgodność z oryginałem przez osobę uprawnioną do reprezentowania Wykonawcy.
   W przypadku zaistnienia sytuacji, o której mowa w podrozdziale III „Wymagane dokumenty" ust. 1, pkt 1.1 ppkt 3) Wykonawca zobowiązany jest przedstawić pisemne zobowiązanie w formie oryginału lub kopii potwierdzonej notarialnie.
2. Za osoby uprawnione do reprezentowania Wykonawcy uznaje się osoby upoważnione do reprezentowania firmy, wskazane we właściwym rejestrze bądź w stosownym

pełnomocnictwie, które należy załączyć do oferty w oryginale lub kopii poświadczonej za zgodność z oryginałem przez osobę udzielającą pełnomocnictwa lub poświadczone notarialnie.

3. W przypadku, gdy załączone do oferty dokumenty zostały sporządzone w języku obcym (w tym dokumenty składane przez Wykonawcę zagranicznego) niezbędne jest przedstawienie ich tłumaczenia na język polski.
4. Jeżeli złożone kserokopie dokumentów będą nieczytelne lub będą budzić wątpliwości co do ich prawdziwości, Zamawiający może żądać przedstawienia oryginału lub notarialnie poświadczonej kopii dokumentu.
5. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia oraz w przypadku innych podmiotów, na zasobach których Wykonawca polega na zasadach określonych w art. 26 ust. 2b ustawy, kopie dokumentów dotyczących odpowiednio Wykonawcy lub tych podmiotów są poświadczone za zgodność z oryginałem odpowiednio przez Wykonawcę lub te podmioty.

VI. OPAKOWANIE OFERTY

Ofertę należy złożyć w dwóch zamkniętych kopertach. Kopertę zewnętrzną należy oznaczyć w następujący sposób:

Zakład Ubezpieczeń Społecznych
Departament Zamówień Publicznych
01-748 Warszawa
ul. Szamocka 3, 5

Oferta przetargowa na
„Modernizacja infrastruktury Platformy Usług Elektronicznych (PUE)"
Postępowanie nr TZ/271/79/15

Koperta wewnętrzna musi być oznakowana w następujący sposób:

Zakład Ubezpieczeń Społecznych
„Oferta przetargowa"

i zaadresowana na adres Wykonawcy, aby można ją było odesłać bez otwierania w przypadku stwierdzenia jej opóźnienia.

VII. OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA WARUNKÓW UDZIAŁU W POSTĘPOWANIU

1. Zamawiający oceni, czy Wykonawca spełnia warunki oraz czy nie zachodzą w stosunku do Wykonawcy przesłanki wykluczenia na podstawie złożonych, przez Wykonawcę, wraz z ofertą oświadczeń i dokumentów żądanych przez Zamawiającego i określonych w Rozdziale IV SIWZ.
2. Ocena spełnienia warunków udziału w postępowaniu zostanie dokonana na zasadzie: Wykonawca – spełnia albo Wykonawca – nie spełnia poszczególnych warunków.

Rozdział V
OPIS SPOSOBU OBLICZENIA CENY OFERTY

1. Wykonawca poda cenę oferty w sposób określony w Formularzu ofertowym części II, V „Formularz cenowy" (Załącznik nr 1 do SIWZ).
2. Stawka podatku VAT jest określana zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. 2011 nr 177, poz. 1054 z późn. zm.).
3. Wszystkie wartości powinny być podane w złotych polskich. Cena oferty powinna być wyrażona cyfrowo i słownie oraz podana z dokładnością do dwóch miejsc po przecinku.
4. Cena podana w ofercie powinna zawierać wszystkie koszty Wykonawcy oraz uwzględniać inne opłaty i podatki, w tym koszty transportu, ubezpieczenia do miejsca dostawy, a także ewentualne upusty i rabaty, oraz nie może ulec zwiększeniu w czasie obowiązywania umowy z zastrzeżeniem sytuacji określonej w Rozdziale XII SIWZ.
5. **W przypadku, gdy Wykonaca złoży ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, Zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.**

Rozdział VI
INFORMACJE O MIEJSCU I TERMINIE SKŁADANIA I OTWARCIA OFERT

I. MIEJSCE l TERMIN SKŁADANIA OFERT

1. Ofertę należy złożyć w siedzibie Zamawiającego w Warszawie, ul. Szamocka 3, 5, Skrzydło „C", pok. 104, do dnia **30.05.2016 r., do godz. 12:00**
2. Oferty złożone po tym terminie zostaną zwrócone.
3. Każdy Wykonawca składający ofertę otrzyma od Zamawiającego potwierdzenie z numerem wpływu odnotowanym także na kopercie oferty.
4. Oferty przesłane faksem nie będą rozpatrywane.

II. MIEJSCE I TERMIN OTWARCIA OFERT

Otwarcie ofert nastąpi w dniu upływu terminu składania ofert w siedzibie Zamawiającego w Warszawie, ul. Szamocka 3, 5, skrzydło „C", piętro I, Departament Zamówień Publicznych, pok. 135, **o godzinie 12:30**.

III. PUBLICZNE OTWARCIE OFERT

1. Otwarcie ofert jest jawne.
2. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie danej części zamówienia.
3. Dokonując otwarcia ofert, Zamawiający poda imię i nazwisko, nazwę (firmę) i adres (siedzibę) Wykonawcy, cenę oferty, a także termin wykonania, okres gwarancji oraz warunki płatności, jeżeli ich podanie w ofercie było wymagane.

IV. TERMIN ZWIĄZANIA OFERTĄ

Wykonawca pozostaje związany złożoną ofertą przez okres 60 dni. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.

V. ZMIANA I WYCOFANIE OFERTY

1. Wykonawca może przed upływem terminu do składania ofert, zmienić lub wycofać ofertę poprzez złożenie pisemnego powiadomienia, przed upływem wyznaczonego terminu składania ofert. Powiadomienie musi być podpisane przez osobę uprawnioną do reprezentowania Wykonawcy.
2. Powiadomienie o wprowadzeniu zmian, winno zostać złożone w sposób i formie przewidzianych w niniejszej Specyfikacji dla złożenia oferty, z zastrzeżeniem, że koperta zewnętrzna będzie zawierała dodatkowe oznaczenie „ZMIANA" i zostanie podany numer wpływu z potwierdzenia, o którym mowa w podrozdziale I ust. 3 niniejszego Rozdziału.

Rozdział VII

KRYTERIA I ZASADY OCENY OFERT

I. TRYB OCENY OFERT

1. Zamawiający poprawia w ofercie:
   1) oczywiste omyłki pisarskie,
   2) oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek,
   3) inne omyłki polegające na niezgodności oferty ze Specyfikacją istotnych warunków zamówienia, nie powodujące istotnych zmian w treści oferty

   - niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona.
2. Oferta Wykonawcy, który w terminie 3 dni od dnia doręczenia zawiadomienia nie zgodził się na poprawienie omyłki, o której mowa w ust. l pkt 3), będzie podlegała odrzuceniu.

II. KRYTERIA WYBORU NAJKORZYSTNIEJSZEJ OFERTY

Przy wyborze oferty Zamawiający będzie kierował się następującymi kryteriami:

	Kryterium wyboru	**Znaczenie kryterium**
1	Cena oferty brutto (z podatkiem VAT) (C)	90%
2	Deklarowany czas obsługi zgłoszeń krytycznych (max 24 godziny) (T)	3%
3	Jednorodność sprzętu oferowanego przez Wykonawcę w ramach funkcjonalności „System bezpieczeństwa” (J)	3%
4	Przeprowadzenie szkoleń przez autoryzowany ośrodek szkoleniowy producenta (S)	4%

III. ZASADY OCENY OFERT WEDŁUG USTALONYCH KRYTERIÓW

1. Ocena ofert dokonywana będzie wg poniższych kryteriów:

1.1. **Cena oferty brutto (z podatkiem VAT) (C)**

Punktacja zostanie przydzielona według poniższego wzoru:

$$C = \frac{\text{najniższe maksymalne wynagrodzenie}}{\text{maksymalne wynagrodzenie badanej oferty}} \times 90\ \%$$

1.2. **Deklarowany czas obsługi zgłoszeń krytycznych (max 24 godziny) (T)**

Punktacja zostanie przydzielona według poniższego wzoru:

$$T = \frac{\text{najniższy maksymalny czas}}{\text{maksymalny czas badanej oferty}} \times 3\ \%$$

Wykonawca określa czas obsługi zgłoszenia krytycznego w pełnych godzinach.

W przypadku gdy Wykonawca nie określi w Formularzu ofertowym czasu obsługi zgłoszeń krytycznych Zamawiający przyjmie, że czas ten wynosi 24 godziny. W przypadku zaoferowania czasu obsługi zgłoszeń krytycznych powyżej 24 godzin, Zamawiający odrzuci ofertę na podstawie art. 89 ust. 1 pkt 2) ustawy.

1.3. **Jednorodność sprzętu oferowanego przez Wykonawcę w ramach funkcjonalności „System bezpieczeństwa" (J)**. Funkcjonalność „System bezpieczeństwa" została określona w Załączniku nr 1 do Wzoru umowy (stanowiącego Załącznik nr 2 do SIWZ), cz. III „Szczegółowy opis przedmiotu zamówienia", pkt 6.

Punktacja zostanie przydzielona wg następującej zasady:

1.3.1. zaoferowanie przez Wykonawcę sprzętu jednego producenta – 3 pkt

1.3.2. zaoferowanie przez Wykonawcę sprzętu różnych producentów – 0 pkt

1.4. **Przeprowadzenie szkoleń przez autoryzowany ośrodek szkoleniowy producenta (S)**, o których mowa w Załączniku 1 do Wzoru umowy (stanowiącego Załącznik nr 2 do SIWZ), Część III „Szczegółowy opis przedmiotu zamówienia", pkt 12.8.

Punktacja zostanie przydzielona wg następującej zasady:

Liczba zadeklarowanych przez Wykonawcę szkoleń, które zostaną przeprowadzone przez autoryzowany ośrodek szkoleniowy, określonych w pkt 12.8 (cz. III) załącznika 1 do Wzoru umowy (Załącznik nr 2 do SIWZ)	Ilość przyznanych punktów
0	0
1	0
2	0,5
3	1

4	1,5
5	2
6	2,5
7	3
8	3,5
9	4

Zamawiający zsumuje ilość zadeklarowanych przez Wykonawcę szkoleń, określoną w tabeli w pkt. 5, cz. III Formularza ofertowego, które zostaną przeprowadzone przez autoryzowany ośrodek szkoleniowy i przyzna Wykonawcy ilość punktów, zgodnie z powyższą tabelą.

2. Przyjmuje się, że 1% = 1 pkt i tak zostanie przeliczona liczba punktów.
3. Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów po zsumowaniu kryteriów C, T, J oraz S.

Ilość punktów uzyskana w kryterium Cena oferty brutto (z podatkiem VAT) (C) + ilość punktów uzyskana w kryterium Deklarowany czas obsługi zgłoszeń krytycznych (max 24 godziny) (T) + ilość punktów uzyskanych w kryterium Jednorodność sprzętu oferowanego przez Wykonawcę w ramach funkcjonalności „System bezpieczeństwa" (J) + ilość punktów uzyskana w kryterium Przeprowadzenie szkoleń przez autoryzowany ośrodek szkoleniowy producenta (S) **= łączna ilość uzyskanych punktów**

Rozdział VIII
ZABEZPIECZENIE NALEŻYTEGO WYKONANIA UMOWY

1. Wykonawca zobowiązany jest wnieść przed podpisaniem umowy zabezpieczenie należytego wykonania umowy w wysokości **10 % maksymalnego wynagrodzenia z podatkiem VAT, z tytułu świadczenia całości przedmiotu zamówienia objętego umową.**
2. Zabezpieczenie należytego wykonania umowy może być wniesione w jednej lub kilku z następujących form:
   a) pieniądzu,
   b) poręczeniu bankowym lub poręczeniu spółdzielczej kasy oszczędnościowo-kredytowej,
   c) z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym,
   d) gwarancji bankowej,
   e) gwarancji ubezpieczeniowej,
   f) poręczeniu udzielonym przez podmioty, o których mowa w art.6 b ust.5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2007 r. Nr 42, poz.275 z późn. zm.).
3. W przypadku wnoszenia zabezpieczenia należytego wykonania umowy:
   a) w pieniądzu – odpowiednią kwotę należy wpłacić na rachunek bankowy Zamawiającego nr rachunku **81 1020 5590 0000 0602 9000 7017 (PKO BP S.A.)**, a dokument potwierdzający wpłatę (pokwitowanie) należy złożyć w siedzibie

Zamawiającego w Warszawie ul. Szamocka 3, 5, skrzydło „C" piętro I, pok. 104, najpóźniej przed podpisaniem umowy;

b) w przypadku wniesienia zabezpieczenia w pozostałych dopuszczanych formach dokument zabezpieczenia należy złożyć w siedzibie Zamawiającego w Warszawie ul. Szamocka 3, 5, skrzydło „C" piętro I, pok. 104 najpóźniej przed podpisaniem umowy.

4. Z dokumentu zabezpieczenia należytego wykonania umowy wniesionego w formie gwarancji bankowej/ubezpieczeniowej powinno wynikać jednoznacznie gwarantowanie wypłat należności w sposób nieodwołalny, bezwarunkowy i na pierwsze żądanie Zamawiającego zawierające oświadczenie o okolicznościach stanowiących podstawę do żądania wypłaty należności.
5. Warunki i termin zwolnienia zabezpieczenia należytego wykonania umowy określone zostały we Wzorze umowy (Załącznik nr 2 do SIWZ).

Rozdział IX

WZÓR UMOWY

Wzór umowy określający szczegółowe warunki, na których Zamawiający zawrze umowę w sprawie udzielenia zamówienia publicznego, stanowi Załącznik nr 2 do SIWZ.

Rozdział X

POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ

Wykonawcom, a także innym osobom, których interes prawny w uzyskaniu zamówienia doznał lub może doznać uszczerbku, w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej, o których mowa w Dziale VI ustawy – Środki Ochrony Prawnej.

Rozdział XI

FORMALNOŚCI PO WYBORZE OFERT W CELU ZAWARCIA UMOWY

I. OGŁOSZENIE O WYNIKU POSTĘPOWANIA

Niezwłocznie po wyborze najkorzystniejszej oferty Zamawiający powiadomi Wykonawców, którzy złożyli oferty o:

1) wyborze najkorzystniejszej oferty podając nazwę (firmę), albo imię i nazwisko, siedzibę albo miejsce zamieszkania i adres Wykonawcy, którego ofertę wybrano, uzasadnienie jej wyboru oraz nazwy (firmy), albo imiona i nazwiska, siedziby albo miejsca zamieszkania i adresy Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację;
2) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne;
3) Wykonawcach, którzy zostali wykluczeni z postępowania podając uzasadnienie faktyczne i prawne;

4) terminie, określonym zgodnie z art. 94 ust. 1 lub ust. 2 ustawy, po którego upływie umowa w sprawie zamówienia publicznego może być zawarta.

II. WARUNKI ZAWARCIA UMOWY

1. Zamawiający wskaże termin i miejsce podpisania umowy Wykonawcy, którego oferta została wybrana w zawiadomieniu o wyborze oferty.
2. **Przed podpisaniem umowy Wykonawca, którego oferta została wybrana, zobowiązany jest do wniesienia zabezpieczenia należytego wykonania umowy na warunkach i w formie określonych w Rozdziale VIII SIWZ pod rygorem nie zawarcia umowy.**
3. Umowa zostanie zawarta w terminach, o których mowa w art. 94 ust. 1 ustawy Prawo zamówień publicznych.
4. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminów, o których mowa w ust. 3, jeżeli w postępowaniu o udzielenie zamówienia została złożona tylko jedna oferta.
5. W sprawach nieuregulowanych w niniejszej Specyfikacji istotnych warunków zamówienia mają zastosowanie przepisy ustawy – Prawo zamówień publicznych oraz przepisy Kodeksu cywilnego.

Rozdział XII

ZMIANA UMOWY

1. Zamawiający dopuszcza możliwość dokonania zmian Umowy w zakresie opisu przedmiotu zamówienia i jego cech oraz sposobu i terminu jego realizacji – jeżeli zmiany są korzystne dla Zamawiającego lub wywołane okolicznościami, których nie można było przewidzieć w momencie składania oferty.
2. Zamawiający nie dopuszcza możliwości zmiany Umowy w zakresie przeniesienia praw i obowiązków wynikających z Umowy na osoby trzecie w zakresie cesji wierzytelności.
3. Zmiana Umowy wynika z okoliczności, których nie można było przewidzieć w chwili zawarcia Umowy lub zmiany te są korzystne dla Zamawiającego.
4. Zmiana postanowień Umowy następuje w formie pisemnego aneksu pod rygorem nieważności, z zastrzeżeniem wyjątków przewidzianych w Umowie.
5. Z wnioskiem o zmianę postanowień Umowy może wystąpić zarówno Wykonawca, jak i Zamawiający.

LISTA ZAŁĄCZNIKÓW DO SIWZ

Wymienione poniżej załączniki stanowią integralną część niniejszej Specyfikacji:

Załącznik nr 1 – Formularz ofertowy,

Załącznik nr 2 – Wzór umowy,

Załącznik nr 3 – Wzór oświadczenia potwierdzającego spełnienie przez Wykonawcę warunków określonych w art. 22 ust. 1 ustawy,

Załącznik nr 4 – Wzór oświadczenia o braku podstaw do wykluczenia na podstawie art. 24 ust. 1 ustawy,

Załącznik nr 5 – Wzór wykazu wykonanych bądź wykonywanych dostaw.

Załącznik nr 1
do SIWZ TZ/271/79/15

.....
(miejscowość, data)

.....
Nazwa i adres Wykonawcy

.....
Numer faksu, adres e-mail Wykonawcy

Zakład Ubezpieczeń Społecznych
ul. Szamocka 3, 5
01-748 Warszawa
(**Zamawiający**)

OFERTA

I. PRZEDMIOT OFERTY

1. Oferujemy wykonanie zamówienia publicznego, którego przedmiotem jest **Modernizacja infrastruktury Platformy Uslug Elektronicznych (PUE)**.
2. Oferowany przedmiot zamówienia spełnia wszystkie wymagania Zamawiającego określone w SIWZ.

II. CENA OFERTY

1. Oferujemy wykonanie zamówienia za maksymalne wynagrodzenie z tytułu realizacji przedmiotu Umowy z podatkiem VAT …..…… *zł (słownie złotych: ……..*), określone w Formularzu cenowym.

   * - wypełnia Wykonawca

2. Ceny jednostkowe określone zostały w części V Oferty - Formularz cenowy, zgodnie z postanowieniami Rozdziału V SIWZ.

III. DEKLAROWANE WARUNKI REALIZACJI ZAMÓWIENIA

Deklarujemy następujące warunki realizacji zamówienia:

1. Termin realizacji przedmiotu zamówienia z wyłączeniem szkoleń, o których mowa w pkt 12.8 (cz. III) Załącznika nr 1 do Wzoru umowy (Załącznik nr 2 do SIWZ) – do 6 miesięcy od daty podpisania umowy.
2. Termin realizacji szkoleń, o których mowa w pkt 12.8 (cz. III) Załącznika nr 1 do Wzoru umowy (Załącznik nr 2 do SIWZ) – do 31 grudnia 2016 roku.
3. **Deklarujemy czas obługi zgłoszeń krytycznych w pełnych godzinach …..* godz. (**max 24 godziny**).** W przypadku gdy Wykonawca nie wpisze w ust. 3 czasu obsługi zgłoszeń krytycznych Zamawiający przyjmie, że czas ten wynosi 24 godziny. W przypadku zaoferowania czasu obsługi zgłoszeń krytycznych powyżej 24 godzin, Zamawiający odrzuci ofertę na podstawie art. 89 ust. 1 pkt 2) ustawy Pzp.

4. **Sprzęt dostarczony w ramach funkcjonalności „System bezpieczeństwa" będzie pochodził od jednego producenta ……* (**wpisać odpowiednio TAK lub NIE**).**

5. **Deklarujemy przeprowadzenie szkoleń przez autoryzowany ośrodek szkoleniowy (**wypełnić tabelę poniżej**):**

LP	Pkt OPZ	Szkolenie (zakres tematyczny):	Autoryzowany ośrodek szkoleniowy (TAK/NIE); Dane ośrodka (nazwa ośrodka, adres) *
1	12.8.1.1	Konfiguracja i zarządzanie siecią SAN	*
2	12.8.1.2	Balansowanie ruchu sieciowego	*
3	12.8.1.3	Przełączanie ruchu wewnątrz infrastruktury PUE (technologia Data Center Interconnect)	*
4	12.8.1.4.1	Zarządzanie dostarczonym systemem bezpieczeństwa - Firewall	*
5	12.8.1.4.2	Zarządzanie dostarczonym systemem bezpieczeństwa – IPS	*
6	12.8.1.4.3	Zarządzanie dostarczonym systemem bezpieczeństwa- antywirus/ antymalware	*
7	12.8.1.5	Zarządzanie i konfiguracja platformy serwerowej	*
8	12.8.1.6	Platforma wirtualizacyjna	*
9	12.8.1.7	Zarządzanie i konfiguracja macierzy	*

* wypełnia Wykonawca, w przypadku niewypełnienia któregokolwiek z punktów powyższej tabeli, Zamawiający przyjmie, że Wykonawca nie oferuje przeprowadzenia danego szkolenia przez autoryzowany ośrodek szkoleniowy

6. Miejsce dostawy przedmiotu zamówienia:
   1) Szamocka 3, 01-748 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Centralnego Ośrodka Obliczeniowego (COO) w Warszawa
   2) Czerniakowska 16, 00-701 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Zapasowego Centralnego Ośrodka Obliczeniowego (ZCOO) w Warszawie

7. Zasady rozliczeń zgodnie z Wzorem Umowy, stanowiącym Załącznik nr 2 do SIWZ.

8. Wniesienie zabezpieczenia należytego wykonania umowy w wysokości 10 % maksymalnego wynagrodzenia z podatkiem VAT, z tytułu świadczenia całości przedmiotu zamówienia objętego umową, w formie .....*

9. Podwykonawcom zamierzamy powierzyć wykonanie zamówienia w całości / części dotyczącej .....* (określić odpowiedni zakres lub pozostawić bez wypełnienia jeżeli nie dotyczy).

* wypełnia Wykonawca

IV. OŚWIADCZENIA

1. Oświadczamy, że zapoznaliśmy się ze Specyfikacją istotnych warunków zamówienia i zobowiązujemy się do stosowania i ścisłego przestrzegania warunków w niej określonych.
2. Oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w Specyfikacji istotnych warunków zamówienia, tj. 60 dni od upływu terminu składania ofert.
3. Oświadczamy, że zawarty w Specyfikacji istotnych warunków zamówienia wzór umowy został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia Umowy na warunkach określonych we wzorze, w miejscu i terminie wyznaczonym przez Zamawiającego.
4. Jesteśmy świadomi, że w przypadku nie dojścia do zawarcia Umowy z przyczyn leżących po naszej stronie wniesione wadium ulega przepadkowi na rzecz Zamawiającego.
5. Jesteśmy świadomi, że w przypadku nie złożenia z przyczyn leżących po naszej stronie, dokumentów lub oświadczeń, o których mowa w art. 25 ust. 1 ustawy, pełnomocnictw, listy podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt 5) ustawy, lub informacji o tym, że nie należymy do grupy kapitałowej, lub nie wyrazimy zgody na poprawienie omyłki, o której mowa w art. 87 ust. 2 pkt 3) ustawy, co spowoduje brak możliwości wybrania oferty złożonej jako najkorzystniejszej, wniesione wadium ulega przepadkowi na rzecz Zamawiającego.
6. Oświadczamy, że wnieśliśmy wadium w formie ..... * Zwrotu wadium należy dokonać na rachunek bankowy Wykonawcy: ..... * (*dotyczy Wykonawców, którzy wnieśli wadium w formie pieniądza*).

   * - wypełnia Wykonawca
7. Oświadczamy, że dostarczony w ramach niniejszego zamówienia sprzęt komputerowy oraz urządzenia sieciowe są fabrycznie nowe i pochodzą z bieżącej produkcji, tj. zostały wyprodukowane nie wcześniej niż 6 miesięcy przed datą zawarcia Umowy, a jednocześnie nie są urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia (ang. refurbished), a także są wolne od wad oraz posiadają pełen zestaw przewidzianych przez producenta właściwych nośników (np. sterowniki).
8. Oświadczamy, że oferowany sprzęt komputerowy oraz urządzenia sieciowe, jeśli jest to dla nich wymagane, posiadają certyfikat CE lub deklarację zgodności CE.
9. Oświadczamy, że oferowany sprzęt komputerowy oraz urządzenia sieciowe spełniają wymogi określone w Rozporządzeniu Ministra Gospodarki z dnia 8 maja 2013 r. w sprawie zasadniczych wymagań dotyczących ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz.U. z 2013 r., poz. 547).
10. W związku z art. 91 ust. 3a. ustawy Prawo zamówień publicznych oświadczamy, że wybór naszej oferty:

    1) **nie będzie** prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami dotyczącymi podatku od towarów i usług*****,

    2) **będzie** prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami dotyczącymi podatku od towarów i usług*****, w związku z tym:

    oświadczamy, że **towary/usługi***, których **dostawa/świadczenie*** będzie prowadzić do

powstania u Zamawiającego obowiązku podatkowego to:

……
(wpisać nazwę (rodzaj) towaru lub usługi / gdy nie dotyczy pozostawić bez wypełnienia)

Wartość wskazanych powyżej towarów/usług* bez podatku VAT wynosi: …… złotych.
* - *niepotrzebne skreślić*

Jeżeli Wykonawca błędnie określi powstanie u Zamawiającego obowiązku podatkowego Zamawiający zastosuje się do art. 17 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. 2011, Nr 177, poz. 1054 z późn. zm.).

V. FORMULARZ CENOWY

Lp.	Wyszczególnienie	Ilość*	Cena jednostkowa netto w PLN*	Razem wartość netto w PLN (kol. 3 x 4)	Stawka podatku VAT w %*	Wartość podatku VAT w PLN * (kol. 4 x kol.6)	Cena jednostkowa brutto w PLN* (kol. 4 + kol. 7)	Razem wartość brutto, tj z VAT w PLN (kol. 3 x kol. 8)*
1	2	3	4	5	6	7	8	9
1.	**Sprzęt:**							
1.1.1	Serwer bazodanowy- typ A							
1.1.2	Serwer aplikacyjny- typ B							
1.2.	Router brzegowy							
1.3.	Przełącznik sieciowy							
1.4.	Przełącznik do zarządzania urządzeniami MGMT							
1.5.	Urządzenie balansujące ruch sieciowy							
1.6.	System bezpieczeństwa							
1.6.1	…*							
…	…*							
1.7.	Sprzętowy moduł bezpieczeństwa							
1.8	Przełącznik SAN							
1.9	Macierz dyskowa							
1.10.	System zarządzania dostarczonymi urządzeniami							

1.10.1	…*							
…	…*							
							Wartość sprzętu razem (suma poz. 1.1 – 1.10):	
2.	**Licencje na oprogramowanie:**							
2.1	Oprogramowanie wirtualizacyjne							
2.2	Oprogramowanie wirtualizacyjne (CPU) Vmware vSphere Standard							
2.3	Oprogramowanie serwerowe dla PUE – Microsoft Windows Server 2012R2 Standard lub równoważne							
2.4	Oprogramowanie serwerowe dla PUE – Microsoft SQL Server 2008 R2 Standard lub równoważne							
2.5	Oprogramowanie serwerowe dla PUE –Red Hat Enterprise for Virtual Datacenters, Standard lub równoważne							
2.6	Red Hat Enterprise Linux Server, Standard lub równoważne							
2.7	Postgres Plus Enterprise Edition 3 Year Unlimited License Agreement lub równoważne							
2.8	Red Hat JBoss Enterprise Application Platform with Management, 64 Core Standard lub równoważne							
2.9	WebMethods lub równoważne							

2.9.1	…*							
…	…*							
							Wartość oprogramowania razem (suma poz. 2.1-2.9)	
3.	**Usługa wdrożenia i przeprowadzenia szkoleń**							
3.1.	Instalacja i konfiguracja dostarczonego sprzętu							
3.2.	Instalacja dostarczonego oprogramowania							
3.3.	Przeprowadzenie szkoleń dla 15 osób w zakresie eksploatacji i konfiguracji zmodernizowanej infrastruktury dla PUE**							
3.4.	Przeprowadzenie szkoleń, o których mowa w Części III Załącznika 1 do wzoru umowy, pkt. 12.8** o poniższej tematyce:							
3.4.1.	Konfiguracja i zarządzanie siecią SAN **							
3.4.2.	Balansowanie ruchu sieciowego**							
3.4.3.	Przełączanie ruchu wewnątrz infrastruktury PUE (technologia DCI)**							
3.4.4.	Zarządzanie dostarczonym systemem bezpieczeństwa – firewall**							
3.4.5.	Zarządzanie dostarczonym systemem bezpieczeństwa – IPS**							
3.4.6.	Zarządzanie dostarczonym systemem bezpieczeństwa- antywirus/ antymalware**							
3.4.7.	Zarządzanie i konfiguracja platformy serwerowej **							

3.4.8.	Platforma wirtualizacyjna**							
3.4.9	Zarządzanie i konfiguracja macierzy**							
							Wartość usług razem (suma poz. 3.1-3.4)	
4.	**Autorskie prawa majątkowe do dokumentacji technicznej**							
							Cena całkowita oferty brutto (1+2+3+4), tj. z VAT: (maksymalne wynagrodzenie Wykonawcy)	

* - *wypełnia Wykonawca*

** - *Zamawiający informuje, że przyjął, że wykonanie i przeprowadzenie szkolenia jest zwolnione z podatku VAT.*

Oświadczamy, że podana wyżej cena całkowita oferty brutto zawiera wszystkie koszty wynikające z realizacji Umowy, w tym koszty usług towarzyszących wykonywaniu Umowy, opłaty i podatki, jest ceną ostateczną, niepodlegającą zwiększeniu w okresie trwania Umowy.

Szczegółowa specyfikacja oferowanego rozwiązania:

Lp.	Wyszczególnienie	Typ/model/nazwa i wersja oprogramowania*	Producent*
1	2	3	4
1.	**Sprzęt:**		
1.1.1	Serwer bazodanowy- typ A		
1.1.2	Serwer aplikacyjny- typ B		
1.2.	Router brzegowy		
1.3.	Przełącznik sieciowy		
1.4.	Przełącznik do zarządzania urządzeniami MGMT		
1.5.	Urządzenie balansujące ruch sieciowy		
1.6.	System bezpieczeństwa		
16.1.	…*		
…	…*		
1.7.	Sprzętowy moduł bezpieczeństwa		
1.8	Przełącznik SAN		
1.9	Macierz dyskowa		
1.10.	System zarządzania dostarczonymi urządzeniami		
1.10.1	…*		
…	…*		
2.	**Oprogramowanie (licencje)**		
2.1.	Oprogramowanie wirtualizacyjne		
2.2	Oprogramowanie wirtualizacyjne (CPU) Vmware vSphere Standard		
2.3..	Oprogramowanie serwerowe dla PUE – Microsoft Windows Server 2012R2 Standard lub równoważne		
2.4.	Oprogramowanie serwerowe dla PUE – Microsoft SQL Server 2008 R2 Standard lub równoważne		
2.5.	Oprogramowanie serwerowe dla PUE –Red Hat Enterprise for Virtual Datacenters, Standard lub równoważne		
2.6	Red Hat Enterprise Linux Server, Standard lub równoważne		
2.7.	Postgres Plus Enterprise Edition 3 Year Unlimited License Agreement lub równoważne		
2.8.	Red Hat JBoss Enterprise Application Platform with Management, 64 Core Standard lub równoważne		
2.9.	WebMethods lub równoważne		
2.9.1	….*		
…	…*		

* - wypełnia Wykonawca

VI. ZAŁĄCZNIKI DO OFERTY

1. Wykonawca składa wraz z ofertą następujące dokumenty i oświadczenia:

   1.1. Oświadczenia i dokumenty potwierdzające spełnianie warunków udziału w postępowaniu:

   1) oświadczenie potwierdzające spełnianie przez Wykonawcę warunków określonych w art. 22 ust. 1 ustawy, sporządzone wg wzoru stanowiącego Załącznik nr 3 do Specyfikacji;

   2) wykaz wykonanych bądź wykonywanych dostaw na potwierdzenie warunku, o którym mowa w Rozdziale IV, podrozdział I, ust. 2 SIWZ, sporządzony wg wzoru stanowiącego Załącznik nr 5 do Specyfikacji.

   3) jeżeli Wykonawca polega na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia, zdolnościach finansowych lub ekonomicznych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków, zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował tymi zasobami w trakcie realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby wykonania zamówienia.

   1.2. Oświadczenia i dokumenty o braku podstaw do wykluczenia z postępowania o udzielenie zamówienia:

   1) oświadczenie o braku podstaw do wykluczenia z postępowania, sporządzone wg wzoru stanowiącego Załącznik nr 4 do Specyfikacji;

   2) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu wykazania braku podstaw do wykluczenia w oparciu o art. 24 ust. 1 pkt 2) ustawy, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

   3) aktualne zaświadczenie właściwego naczelnika urzędu skarbowego potwierdzające, że Wykonawca nie zalega z opłacaniem podatków lub zaświadczenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;

   4) aktualne zaświadczenie właściwego oddziału Zakładu Ubezpieczeń Społecznych lub Kasy Rolniczego Ubezpieczenia Społecznego potwierdzające, że Wykonawca nie zalegaz opłacaniem składek na ubezpieczenie zdrowotne i społeczne lub potwierdzenie, że uzyskał przewidziane prawem zwolnienie, odroczenie lub rozłożenie na raty zaległych płatności lub wstrzymanie w całości wykonania decyzji właściwego organu - wystawione nie wcześniej niż 3 miesiące przed upływem terminu składania ofert;

   5) aktualna informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 4) - 8) oraz pkt 10) i 11) ustawy wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

   6) aktualna informacja z Krajowego Rejestru Karnego w zakresie określonym w art. 24 ust. 1 pkt 9) ustawy wystawiona nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;

7) lista podmiotów należących do tej samej grupy kapitałowej o której mowa w art. 24 ust. 2 pkt 5) ustawy lub informacja o tym, że Wykonawca nie należy do grupy kapitałowej.

1.3. Oświadczenia i dokumenty potwierdzające, że oferowany przedmiot zamówienia odpowiada wymaganiom określonym przez Zamawiającego dla przedmiotu zamówienia:

1) wypełniony Załącznik A do Formularza ofertowego;

2) specyfikacja techniczna (opis) produktów, które mają zostać dostarczone Zamawiającemu, na potwierdzenie spełniania warunków określonych w Załączniku A do Formularza ofertowego – w formie określonej w Załączniku A do Formularza ofertowego.

1.4. Inne wymagane oświadczenia i dokumenty:

1) w przypadku, gdy Wykonawcę reprezentuje pełnomocnik - pełnomocnictwo określające jego zakres i podpisane przez osoby uprawnione do reprezentacji Wykonawcy;

2) w przypadku, gdy ofertę składają Wykonawcy ubiegający się wspólnie o udzielenie zamówienia wymagane jest załączenie dokumentu pełnomocnictwa określającego zakres umocowania pełnomocnika ustanowionego do reprezentowania ich w postępowaniu, stosownie do art. 23 ust. 2 ustawy;

3) dokument potwierdzający wniesienie wadium, jeżeli zostało wniesione w innej formie niż w pieniądzu (zaleca się dołączyć);

….....

(podpis osoby upoważnionej
do reprezentowania Wykonawcy)

Załącznik A do Formularza ofertowego

Wzór tabeli potwierdzającej spełnianie wymagań

1. Kolumna **„**Numer wymagania" oznacza numer w Załączniku nr 1 do Wzoru umowy (Załącznik nr 2 do SIWZ) – Część „Szczegółowy opis przedmiotu zamówienia" określający punkt w pełnym kontekście wraz z podpunktami jeśli istnieją.
2. W kolumnie „Spełnienie wymagania (TAK/NIE)" należy określić czy dane wymaganie jest spełnione.
3. Kolumnę „Szczegółowy opis sposobu spełnienia wymagania" należy wypełnić w sposób umożliwiający Zamawiającemu ocenę spełnienia wymagania według następujących priorytetów:
   a) Poprzez podanie tytułu dokumentu (lub dokumentów) i numer strony (lub stron), na której znajduje się opis potwierdzający spełnienie poszczególnych wymagań, w przypadku dokumentacji dostarczonej w formie papierowej. W przypadku dokumentacji dostarczonej w formie elektronicznej (np. plik PDF zamieszczony na płycie CD, DVD lub pendrive) należy podać nazwę pliku (lub plików) i numer (lub numery) stron. Format opisu miejsca w dokumentacji: nazwa dokumentu/ rozdział (pełen kontekst)/ strona/ punkt/ akapit/ tabela/ rysunek itp.)
   b) W przypadku braku jednoznacznego potwierdzenia w dokumentacji technicznej producenta możliwe jest odwołanie się do innego dokumentu technicznego (np. opis konfiguracji, architektura funkcjonalna) potwierdzającego spełnienie wymagania określonego przez Zamawiającego w Załączniku nr 1 do Wzoru umowy – Rozdział III „Szczegółowy opis przedmiotu zamówienia".
   c) Dla wymagań funkcjonalnych dopuszczalne jest opisanie sposobu realizacji danego wymagania. W szczególnym przypadku Wykonawca może opisać spełnienie wymaganego parametru technicznego poprzez podanie konkretnej wartości np.: ilość procesorów czy też pamięci RAM.

Numer wymagania	Spełnienie wymagania (TAK/NIE)*	Szczegółowy opis sposobu spełnienia wymagania*
1.1.		
1.2.		
1.2.1.		
1.2.2.		
1.2.3.		
1.2.4.		
1.2.5.		
1.2.6.		
1.3.		
1.4.		
1.5.		
1.5.1.		
1.5.2.		
1.5.3.		
1.5.4.		
1.5.5.		
1.5.6.		
1.6.		
1.6.1.		
1.6.2.		
1.6.3.		
1.6.4.		

1.6.5.		
1.6.6.		
1.7.		
1.7.1.		
1.7.2.		
1.7.3.		
2.1.		
2.2.		
2.3.		
2.4.		
2.5.		
2.6.		
2.7.		
2.8.		
2.9.		
2.10.		
2.11.		
2.12.		
2.13.		
2.14.		
2.15.		
2.16.		
2.17.		
2.18.		
2.19.		
2.20.		
2.21.		
2.22.		
2.23.		
2.24.		
2.25.		
2.26.		
2.27.		
2.28.		
2.29.		
2.30.		
2.31.		
3.1.		
3.2.		
3.3.		
3.4.		
3.5.		
3.6.		
3.7.		
3.7.1.		
3.7.2.		

3.7.3.		
3.7.4.		
3.7.5.		
3.7.6.		
3.7.7.		
3.7.8.		
3.8.		
3.8.1.		
3.8.2.		
3.8.3.		
3.8.4.		
3.8.5.		
3.8.6.		
3.8.7.		
3.9.		
3.10.		
3.11.		
3.12.		
3.13.		
3.14.		
3.15.		
3.15.1.		
3.15.2.		
3.15.3.		
3.15.4.		
3.15.5.		
3.15.6.		
4.1.		
4.2.		
4.3.		
4.4.		
4.5.		
4.6.		
4.7.		
5.1.		
5.2.		
5.3.		
5.4.		
5.5.		
5.6.		
5.7.		
5.8.		
5.9.		
5.10.		
5.11.		
5.12.		

5.12.1.		
5.12.2.		
5.12.3.		
5.12.4.		
5.12.5.		
5.12.6.		
5.13.		
5.13.1.		
5.13.2.		
5.13.3.		
5.13.4.		
5.13.5.		
5.13.6.		
5.13.7.		
5.13.8.		
5.13.9.		
5.13.10.		
5.13.11.		
5.13.12.		
5.14.		
5.14.1.		
5.14.2.		
5.14.3.		
5.14.4.		
5.14.5.		
5.14.6.		
5.14.7.		
5.14.8.		
5.14.9.		
5.14.10.		
5.14.11.		
5.14.12.		
5.14.13.		
5.14.14.		
5.14.15.		
5.14.16.		
5.14.17.		
5.14.18.		
5.14.19.		
5.14.20.		
5.14.21.		
5.15.		
5.16.		
5.17.		
5.18.		
5.19.		

5.20.		
5.21.		
5.22.		
5.23.		
5.24.		
5.25.		
5.26.		
5.27.		
5.28.		
5.29.		
5.30.		
5.31.		
5.32.		
5.33.		
5.34.		
5.35.		
5.36.		
5.37.		
5.38.		
5.39.		
5.39.14.		
5.39.15.		
6.1.		
6.1.1.		
6.1.2.		
6.1.3.		
6.1.4.		
6.1.5.		
6.1.6.		
6.2.		
6.2.1.		
6.2.2.		
6.2.3.		
6.3.		
6.3.1.		
6.3.2.		
6.3.3.		
6.3.4.		
6.3.5.		
6.3.6.		
6.3.7.		
6.4.		
6.5.		
6.6.		
6.7.		
6.7.1.		

6.7.2.		
6.7.3.		
6.7.4.		
6.7.5.		
6.7.6.		
6.7.7.		
6.7.8.		
6.7.9.		
6.7.10.		
6.7.11.		
6.7.12.		
6.7.13.		
6.7.14.		
6.7.15.		
6.7.16.		
6.7.17.		
6.7.18.		
6.7.19.		
6.7.20.		
6.7.21.		
6.7.22.		
6.7.23.		
6.7.24.		
6.7.25.		
6.7.26.		
6.7.27.		
6.7.28.		
6.7.29.		
6.7.30.		
6.7.31.		
6.7.32.		
6.7.33.		
6.7.34.		
6.7.35.		
6.7.36.		
6.7.37.		
6.7.38.		
6.7.39.		
6.7.40.		
6.7.41.		
6.7.42.		
6.7.43.		
6.7.44.		
6.7.45.		
6.7.46.		
6.7.47.		

6.7.48.		
6.7.49.		
6.7.50.		
6.7.51.		
6.7.52.		
6.7.53.		
6.7.54.		
6.7.55.		
6.7.56.		
6.7.57.		
6.7.58.		
6.7.59.		
6.7.60.		
6.7.61.		
6.7.62.		
6.7.63.		
6.7.64.		
6.7.65.		
6.8.		
6.8.1.		
6.8.2.		
6.8.3.		
6.9.		
6.9.1.		
6.9.2.		
6.10.		
6.10.1.		
6.10.2.		
6.10.3.		
6.10.4.		
6.10.5.		
6.10.6.		
6.10.7.		
6.10.8.		
6.10.9.		
6.10.10.		
6.11.		
6.11.1.		
6.11.2.		
6.11.3.		
6.11.4.		
6.11.5.		
6.11.6.		
6.11.7.		
6.11.8.		
6.11.9.		

6.11.10.		
6.11.11.		
6.11.12.		
6.11.13.		
6.11.14.		
6.12.		
6.12.1.		
6.12.2.		
7.1.		
7.2.		
7.3.		
7.4.		
7.5.		
7.6.		
7.7.		
7.8.		
7.9.		
7.10.		
7.11.		
7.12.		
7.13.		
7.14.		
7.15.		
7.16.		
7.17.		
7.18.		
7.19.		
8.1.		
8.2.		
8.3.		
8.4.		
8.5.		
8.6.		
8.7.		
8.8.		
8.9.		
8.10.		
8.11.		
8.12.		
8.13.		
8.14.		
8.15.		
8.16.		
9.1.		
9.2.		
9.3.		

9.4.		
9.5.		
9.6.		
9.7.		
9.8.		
9.9.		
9.10.		
9.11.		
9.12.		
9.13.		
9.14.		
9.15.		
9.16.		
9.17.		
9.18.		
9.19.		
9.20.		
9.21.		
9.22.		
9.23.		
9.24.		
9.25.		
9.26.		
9.27.		
9.28.		
9.29.		
9.30.		
9.31.		
9.31.1.		
9.31.2.		
9.32.		
9.33.		

* wypełnia Wykonawca

Załącznik nr 2 do SIWZ
TZ/271/79/15

UMOWA NR ……. (TZ/271/79/15)

zawarta w dniu ..... w Warszawie pomiędzy:

Zakładem Ubezpieczeń Społecznych z siedzibą w Warszawie, ul. Szamocka 3, 5 posiadającym NIP nr 521-30-17-228, REGON nr 000017756, reprezentowanym przez:

.....

zwanym dalej „**Zamawiającym”**,

a

..... z siedzibą w ..... , ul. ..... , działająca w oparciu o ....., posiadająca NIP ....., REGON ....., wysokość kapitału zakładowego ……. (jeśli dotyczy),

reprezentowaną przez:

.....

zwaną dalej: „**Wykonawcą”**,

zwanymi dalej łącznie **„Stronami**”, a każda z osobna **„Stroną”**

w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego realizowanego na podstawie ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164) została zawarta umowa (dalej: **„Umowa”**) o następującej treści:

§ 1

Przedmiot Umowy

1. Przedmiotem Umowy jest modernizacja infrastruktury dla Platformy Usług Elektronicznych (dalej „PUE”) poprzez zwiększenie mocy obliczeniowej oraz bezpieczeństwa przetwarzania danych, w tym dostarczenie sprzętu komputerowego i urządzeń sieciowych (dalej „urządzenia”) oraz udzielenie licencji/sublicencji/subskrypcji (dalej „licencje”) na oprogramowanie objęte przedmiotem Umowy (dalej „oprogramowanie”) wraz z 36 miesięczną gwarancją i usługami wdrożeniowymi oraz szkoleniowymi – zgodnie z Opisem przedmiotu zamówienia, stanowiącym Załącznik nr 1 do Umowy.
2. Wszystkie elementy będące przedmiotem Umowy, określone w ust. 1, będą ze sobą poprawnie współpracować (tzn. będą ze sobą kompatybilne) oraz będą poprawnie współpracować z istniejącą infrastrukturą Zamawiającego. Ewentualne koszty integracji elementów z istniejącą infrastrukturą Zamawiającego ponosi Wykonawca.
3. Przedmiot Umowy, o którym mowa w ust. 1, z wyłączeniem szkoleń, Wykonawca zrealizuje w dwóch lokalizacjach:
   1) Szamocka 3, 01-748 Warszawa – do tej lokalizacji dostarczane są elementy

przedmiotu Umowy przeznaczone dla Centralnego Ośrodka Obliczeniowego (dalej **„COO”**) w Warszawie,

2) Czerniakowska 16, 00-701 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu Umowy przeznaczone dla Zapasowego Centralnego Ośrodka Obliczeniowego (dalej **„ZCOO”**) w Warszawie.

§ 2
Wynagrodzenie Wykonawcy

1. Wynagrodzenie brutto, tj. z uwzględnieniem podatku od towarów i usług (VAT), należne Wykonawcy z tytułu realizacji przedmiotu Umowy nie przekroczy kwoty ……zł (słownie złotych: …….), w tym: wynagrodzenie netto …….. zł (słownie złotych……..), wartość podatku VAT …… zł (słownie złotych ……), zgodnie z Formularzem ofertowym Wykonawcy, stanowiącym Załącznik nr 2 do Umowy.
2. Ceny jednostkowe za realizację przedmiotu Umowy zawiera Formularz cenowy, określony w Załączniku nr 2 do Umowy.
3. Wynagrodzenie brutto oraz ceny jednostkowe, o których mowa w ust. 1 i 2, obejmują wszelkie koszty Wykonawcy związane z realizacją Umowy oraz nie ulegną zwiększeniu w okresie obowiązywania Umowy.

§ 3
Termin i warunki realizacji Umowy

1. Wykonawca zrealizuje przedmiot Umowy, z wyłączeniem szkoleń, o których mowa w Części III, punkt 12.8 Załącznika nr 1 do Umowy, w terminie do 6 miesięcy od dnia zawarcia Umowy.
2. Wykonawca zrealizuje usługi szkoleniowe, o których mowa w Części III, punkt 12.8 Załącznika nr 1 do Umowy, w terminie do dnia 31 grudnia 2016 roku, przy czym poszczególne szkolenia zostaną zrealizowane w terminach uzgodnionych z Zamawiającym, z uwzględnieniem § 4 ust. 2.
3. Wykonawca przedłoży uprzednio uzgodniony z Zamawiającym, w formie papierowej i elektronicznej projekt instalacji i konfiguracji urządzeń oraz oprogramowania wraz z harmonogramem czasowym dostawy oraz instalacji i konfiguracji urządzeń w terminie 14 dni kalendarzowych od dnia zawarcia Umowy, co zostanie potwierdzone podpisanym bez zastrzeżeń Protokołem cząstkowym odbioru w części B.3. (Załącznik nr 3 do Umowy). Procedura odbioru projektu została określona w pkt 9) w Załączniku nr 8 do Umowy.
4. Dostawy i wdrożenie przedmiotu Umowy nastąpią w terminie realizacji przedmiotu Umowy, o którym mowa w ust. 1, przy czym dostawy i wdrożenie mogą być rozpoczęte po podpisaniu bez zastrzeżeń przez Strony Protokołu cząstkowego odbioru, o którym mowa w ust. 3. Dostawy i wdrożenie nastąpią na zasadach i warunkach określonych w Umowie. Dostawy i wdrożenie przedmiotu Umowy w danej lokalizacji zostaną

potwierdzone każdorazowo Protokołem cząstkowym odbioru w części A, B.1., B.2. i C (Załącznik nr 3 do Umowy).

5. Wykonawca przedłoży w formie papierowej i elektronicznej egzemplarz dokumentacji technicznej rozwiązania, uzgodnionej z Zamawiającym, w terminie o którym mowa w ust. 1. Dokumentacja techniczna musi zawierać elementy wskazane w pkt 12.5 Załącznika nr 1 do Umowy. Procedura odbioru dokumentacji została określona w pkt 9) i 10) w Załączniku nr 8 do Umowy.
6. Za termin realizacji przedmiotu Umowy przyjmuje się:
   1) w zakresie określonym w ust. 1 – datę podpisania bez zastrzeżeń przez Strony – na podstawie podpisanych bez zastrzeżeń Protokołów cząstkowych odbioru, których wzór określa Załącznik nr 3 do Umowy oraz Protokołu końcowego odbioru wdrożenia, którego wzór określa Załącznik nr 4 do Umowy;
   2) w zakresie określonym w ust. 2 – datę podpisania bez zastrzeżeń przez Strony ostatniego z Protokołów przeprowadzenia szkolenia, których wzór określa Załącznik nr 12 do Umowy.
7. Wykonawca zobowiązany jest potwierdzić faksem lub emailem (faks: (22) ……., email: ……..) Zamawiającemu termin dostawy i wdrożenia przedmiotu Umowy na co najmniej 2 dni robocze Zamawiającego (za dni robocze Zamawiającego rozumie się dni od poniedziałku do piątku w godz. 8.00-15.00, z wyłączeniem świąt i dni ustawowo wolnych od pracy), przed planowaną datą dostawy i wdrożenia w danej lokalizacji. Dostawa wraz z wdrożeniem odbędzie się w dni robocze Zamawiającego. Za zgodą Zamawiającego (pisemną, email) dostawa wraz z wdrożeniem może nastąpić poza powyższymi godzinami oraz w dni wolne od pracy lub soboty.
8. Po stronie Zamawiającego osobą upoważnioną do kontaktów w zakresie realizacji Umowy jest: ……., tel. ……., faks ……., adres email: …… . Po stronie Wykonawcy osobą upoważnioną do kontaktów w zakresie realizacji Umowy jest: …… tel. ……., faks ……., adres email: ……..
9. Zamawiający ma prawo odmowy przyjęcia przedmiotu Umowy w przypadku niedotrzymania przez Wykonawcę terminu określonego w ust. 7. W takim przypadku Zamawiający wyznaczy nowy termin dostawy oraz wdrożenia, o którym powiadomi faksem lub emailem (na faks lub email Wykonawcy, o którym mowa w ust. 8) Wykonawcę, nie później niż na 2 dni robocze Zamawiającego przed tym terminem.
10. Odpowiedzialność z tytułu utraty lub uszkodzenia urządzeń i oprogramowania, będących przedmiotem Umowy, przechodzi na Zamawiającego z chwilą podpisania bez zastrzeżeń przez przedstawicieli Stron Protokołu końcowego odbioru wdrożenia, którego wzór określa Załącznik nr 4 do Umowy.
11. Szczegółowa procedura odbioru przedmiotu Umowy opisana jest w Załączniku nr 8 do Umowy.
12. Wykonawca nie może przekazać realizacji przedmiotu Umowy na osoby trzecie, gdy nie wynika to z Umowy.

§ 4

Warunki wykonania usług szkoleniowych

1. Wykonawca w ramach realizacji przedmiotu Umowy zorganizuje i przeprowadzi szkolenia w zakresie określonym w Załączniku nr 1 do Umowy.
2. Szkolenia, o których mowa w Części III, pkt 12.7 oraz pkt 12.8 Załącznika nr 1 do Umowy, zostaną przeprowadzone przez Wykonawcę w terminach uzgodnionych z Zamawiającym (pisemnie, email), z równomiernym rozłożeniem ich realizacji w czasie, z uwzględnieniem zastrzeżenia, że Zamawiający nie może skierować wszystkich osób zgłoszonych na dany temat w jednym terminie.
3. Zamawiający oświadcza, że szkolenia będące przedmiotem Umowy służą do kształcenia zawodowego pracowników Zamawiającego.
4. Szkolenia będące przedmiotem Umowy zostaną przeprowadzone w języku polskim, w salach szkoleniowych i na sprzęcie zapewnionym przez Wykonawcę na terenie Warszawy.
5. Osoby uczestniczące w szkoleniach otrzymają materiały szkoleniowe w języku polskim lub w języku angielskim, jeśli Wykonawca nie posiada materiałów w języku polskim.
6. Osoby uczestniczące w szkoleniach otrzymają zaświadczenie po ukończeniu każdego szkolenia.
7. Wykonawca w terminie co najmniej na 7 dni kalendarzowych przed rozpoczęciem każdego szkolenia, potwierdzi Zamawiającemu faksem lub emailem (faks: (22) ……., email: ……..) ustalony termin realizacji szkolenia, wskazując miejsce i godzinę rozpoczęcia szkolenia.
8. Po przeprowadzeniu każdego ze szkoleń, określonych w Załączniku nr 1 do Umowy, Wykonawca sporządzi Protokół przeprowadzenia szkolenia, według wzoru stanowiącego Załącznik nr 12 do Umowy. Zamawiający przedmiotowy protokół podpisze, bądź zgłosi zastrzeżenia w terminie 3 dni roboczych Zamawiającego od dnia otrzymania od Wykonawcy Protokołu przeprowadzenia szkolenia.
9. Realizacja cyklu szkoleń będzie następowała w dni robocze i zostanie zakończona w terminie do dnia 31 grudnia 2016 roku.

§ 5

Zasady rozliczeń

1. Płatność za wykonanie przedmiotu Umowy, z wyłączeniem szkoleń, o których mowa w Części III, pkt 12.8 Załącznika nr 1 do Umowy, zostanie dokonana przez Zamawiającego w terminie 30 dni od daty otrzymania przez Centralę Zakładu Ubezpieczeń Społecznych, sekretariat Departamentu Zarządzania Systemami Informatycznymi w Warszawie, ul. Szamocka 3, 5, prawidłowo wystawionej faktury wraz z podpisanym, bez zastrzeżeń przez Strony, Protokołem końcowego odbioru wdrożenia, którego wzór określa Załącznik nr 4 do Umowy.
2. Płatność za realizację szkoleń, o których mowa w Części III, pkt 12.8 Załącznika nr 1 do

Umowy, nastąpi z dołu w miesięcznych opłatach, za szkolenia wykonane w danym miesiącu kalendarzowym, w terminie 30 dni od daty otrzymania przez Zakład Ubezpieczeń Społecznych – Departament Zarządzania Systemami Informatycznymi, ul. Szamocka 3, 5, 01-748 Warszawa, prawidłowo wystawionej faktury wraz z podpisanymi, bez zastrzeżeń przez Strony, Protokołami przeprowadzenia szkolenia, których wzór określa Załącznik nr 12 do Umowy.

3. Płatności następować będą przelewem na rachunek bankowy Wykonawcy nr: ……..…….

   Fakturę należy wystawić zgodnie z danymi:

   NIP 521 301 72 28

   Zakład Ubezpieczeń Społecznych

   01-748 Warszawa, ul. Szamocka 3, 5

4. Za termin płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.

§ 6
Kary umowne i odstąpienie od Umowy

1. W przypadku opóźnienia terminu realizacji przedmiotu Umowy, o którym mowa w § 3 ust. 1 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% wynagrodzenia brutto za realizację przedmiotu Umowy, o którym mowa w § 2 ust. 1 Umowy, za każdy rozpoczęty kalendarzowy dzień opóźnienia.
2. W przypadku opóźnienia terminu realizacji przedmiotu Umowy, o którym mowa w § 3 ust. 1 Umowy, powyżej 21 dni kalendarzowych Zamawiający może odstąpić od Umowy, a Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20% wynagrodzenia brutto za realizację przedmiotu Umowy, o którym mowa w § 2 ust. 1 Umowy.
3. W przypadku opóźnienia któregokolwiek terminu realizacji usług szkoleniowych uzgodnionego z Zamawiającym w trybie określonym w § 4 ust. 2 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 200,00 złotych (słownie: dwieście zł 00/100) za każdy rozpoczęty dzień roboczy Zamawiającego opóźnienia, za każde opóźnione szkolenie odrębnie.
4. W przypadku odstąpienia od Umowy lub wypowiedzenia Umowy przez którąkolwiek ze Stron z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20% wynagrodzenia brutto za realizację przedmiotu Umowy, o którym mowa w § 2 ust. 1 Umowy.
5. W przypadku opóźnienia terminu przekazania uzgodnionego projektu instalacji i konfiguracji urządzeń oraz oprogramowania wraz z harmonogramem czasowym, o którym mowa w § 3 ust. 3 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1.000,00 zł (słownie złotych: jeden tysiąc 00/100) za każdy rozpoczęty kalendarzowy dzień opóźnienia.
6. W przypadku opóźnienia terminu naprawy, o którym mowa w § 7 ust. 10 pkt 2) Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15.000,00 zł (słownie złotych: piętnaście tysięcy 00/100) za każdą rozpoczętą godzinę opóźnienia.

7. W przypadku opóźnienia terminu naprawy, o którym mowa w § 7 ust. 10 pkt 1) Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1.000,00 zł (słownie złotych: jeden tysiąc 00/100) za każdą rozpoczętą godzinę opóźnienia.
8. W przypadku opóźnienia czasu reakcji, o którym mowa w § 7 ust. 11, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1.000,00 zł (słownie złotych: jeden tysiąc 00/100) za każdą rozpoczętą godzinę opóźnienia.
9. W przypadku opóźnienia terminu potwierdzenia przyjęcia zgłoszenia, o którym mowa w § 7 ust. 9 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1.000,00 zł (słownie złotych: jeden tysiąc 00/100) za każdą rozpoczętą godzinę opóźnienia.
10. W przypadku opóźnienia przez Wykonawcę terminu integracji systemu obsługi zgłoszeń Zamawiającego z systemem obsługi zgłoszeń Wykonawcy, o którym mowa w § 7 ust. 5 Umowy, lub opóźnienia terminu dostosowania systemu obsługi zgłoszeń Wykonawcy w przypadku zmiany struktur komunikatów, o którym mowa w § 7 ust. 6 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500,00 zł (słownie złotych: pięćset 00/100) za każdy rozpoczęty kalendarzowy dzień opóźnienia.
11. W przypadku opóźnienia terminu wymiany urządzenia, o którym mowa w § 7 ust. 14 lub 15 Umowy, Wykonawca zapłaci karę umowną w wysokości 2.000,00 zł (słownie złotych: dwa tysiące 00/100) za każdy rozpoczęty dzień kalendarzowy opóźnienia.
12. W przypadku opóźnienia terminów, określonych zgodnie z § 7 ust. 18 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 3.000,00 zł (słownie złotych: trzy tysiące 00/100) za każdy rozpoczęty kalendarzowy dzień opóźnienia, odrębnie dla każdego z opóźnionych terminów.
13. W przypadku naruszenia zasad bezpieczeństwa informacji, o których mowa w § 10 Umowy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5 % wynagrodzenia brutto za realizację przedmiotu Umowy, wskazanego w § 2 ust. 1 Umowy za każdy przypadek ujawnienia informacji prawnie chronionych.
14. W przypadku, gdy szkoda powstała po stronie Zamawiającego przewyższa zastrzeżone kary umowne, Zamawiający ma prawo żądać odszkodowania uzupełniającego na zasadach ogólnych.
15. Kary umowne opisane powyżej mogą ulec łączeniu z różnych tytułów.
16. Łączna odpowiedzialność Wykonawcy z tytułu kar umownych ograniczona jest do 100% wynagrodzenia brutto za realizację przedmiotu Umowy, o którym mowa w § 2 ust. 1 Umowy.
17. Każde naliczenie kar umownych zostanie udokumentowane wystawieniem i przesłaniem do Wykonawcy przez Zamawiającego noty obciążeniowej zawierającej w treści kalkulację kwot naliczonych kar umownych, z terminem płatności 14 dni od daty jej otrzymania. Zamawiający ma prawo potrącania kar umownych niezapłaconych w terminie określonym w nocie, z należnego wynagrodzenia (faktur) lub zabezpieczenia należytego wykonania Umowy, bez potrzeby uzyskania zgody Wykonawcy. W przypadku braku możliwości dokonania potrącenia z faktury lub zabezpieczenia należytego wykonania umowy lub braku wpłaty za notę przez Wykonawcę, zostanie wystawione

wezwanie do zapłaty. Brak wpłaty w odpowiedzi na wezwanie do zapłaty spowoduje wszczęcie dochodzenia należności na drodze windykacji sądowej.

§ 7
Gwarancja i rękojmia

1. Niezależnie od rękojmi za wady, Wykonawca udzieli Zamawiającemu 36 miesięcznej gwarancji na dostarczone urządzenia wraz ze wsparciem technicznym na dostarczone oprogramowanie w ramach udzielonych licencji, będących przedmiotem Umowy, począwszy od dnia podpisania bez zastrzeżeń przez przedstawicieli Stron Protokołu końcowego odbioru wdrożenia, którego wzór określa Załącznik nr 4 do Umowy, na zasadach określonych w Umowie.
2. Okres rękojmi jest równy okresowi gwarancji.
3. W ramach wsparcia technicznego, o którym mowa w ust. 1, Wykonawca zobowiązany jest udostępniać uaktualnienia oprogramowania dla dostarczonych urządzeń w ramach udzielonej licencji.
4. W dniu podpisania Umowy Zamawiający i Wykonawca wymienią adresy poczty elektronicznej i numery telefonów oraz faksów do kontaktów między Centrum Serwisowym (CS) Wykonawcy, a Centrum Zgłoszeniowym (CZ) Zamawiającego oraz wskażą osoby uprawnione do kontaktów.
5. Wykonawca w terminie 2 miesięcy od dnia zawarcia Umowy, dokona integracji systemu obsługi zgłoszeń Wykonawcy z systemem obsługi zgłoszeń Zamawiającego, co Strony potwierdzą podpisaniem Protokołu potwierdzenia integracji, według wzoru stanowiącego Załącznik nr 10 do Umowy.
6. Zamawiający zastrzega prawo do zmiany struktur komunikatów opisanych w Załączniku nr 9 do Umowy. Wykonawca jest zobowiązany do dostosowania CS do obsługi nowych mechanizmów w terminie nie przekraczającym 2 miesięcy od dnia zgłoszenia zmiany mechanizmów komunikacji przez Zamawiającego.
7. Do czasu integracji CS Wykonawcy z CZ Zamawiającego oraz w przypadku awarii CZ Zamawiającego (HP Service Manager) lub CS Wykonawcy, Zamawiający będzie dokonywać zgłoszeń oraz Strony będą wymieniać komunikaty dotyczące obsługi zgłoszeń za pośrednictwem uzgodnionych adresów mailowych, o których mowa w ust. 4, na Formularzu zgłoszenia awarii, którego wzór określa Załącznik nr 5 do Umowy. Strony zobowiązane są do niezwłocznego poinformowania o awarii swojego systemu obsługi zgłoszeń za pośrednictwem uzgodnionych adresów mailowych. W przypadku braku takiej informacji, zgłoszenia i komunikaty przesyłane przez system obsługi zgłoszeń będą uznane za dostarczone.
8. Zgłoszenia serwisowe oraz wymiana komunikatów dotyczących obsługi zgłoszeń, po integracji CS Wykonawcy z CZ Zamawiającego, będą dokonywane za pośrednictwem posiadanego przez Zamawiającego systemu HP Service Manager (lub mailowo w przypadku kanału awaryjnego). Format oraz struktura komunikatów obsługiwanych przez CZ Zamawiającego (HP Service Manager) jak również zakres informacji przekazywanych przy zgłoszeniu serwisowym opisany jest w Załączniku nr 9 do Umowy.

9. Wykonawca, nie później niż w czasie 1 godziny od momentu wysłania przez Zamawiającego zgłoszenia serwisowego, potwierdzi przyjęcie tego zgłoszenia w formie takiej, w jakiej otrzymał zgłoszenie. W przypadku braku potwierdzenia w tym czasie Zamawiający kontaktuje się z Wykonawcą w celu wyjaśnienia przyczyny braku potwierdzenia oraz ustalenia ewentualnego sposobu rejestracji zgłoszenia u Wykonawcy. Dokonanie wyjaśnień w wyniku zainicjowanego przez Zamawiającego kontaktu nie zwalnia od naliczenia kar umownych z tytułu opóźnienia terminu potwierdzenia przyjęcia zgłoszenia.
10. Przez naprawę rozumie się przywrócenie urządzenia lub funkcjonalności oprogramowania do stanu sprzed awarii, przy czym czas naprawy, to czas liczony od momentu zgłoszenia awarii do momentu przywrócenia urządzenia lub oprogramowania do stanu technicznego sprzed awarii potwierdzonym przez Zamawiającego. Czas naprawy nie może przekroczyć:
    1) 72 godzin przy zgłoszeniach o poziomie niekrytycznym,
    2) … (zgodnie z wybraną ofertą) godziny przy zgłoszeniach o poziomie (statusie) krytycznym

    od momentu zgłoszenia awarii. O poziomie zgłoszenia decyduje Zamawiający.
11. Wykonawca zobowiązany jest do dochowania czasu reakcji dla zgłoszeń ze statusem krytycznym, nie dłuższego niż 1 godzina, licząc od momentu zgłoszenia awarii przez Zamawiającego. (W przypadku zgłoszeń o statusie innym niż „Krytyczny" czas reakcji nie jest wymagany.) Czas reakcji rozumiany jest jako przesłanie do Zamawiającego wstępnego planu działań serwisowych. Dodatkowe wymagania dla zgłoszeń o statusie „Krytyczny" określone są w Załączniku nr 1 do Umowy, pkt 13 „Gwarancja (usługi serwisu gwarancyjnego)".
12. Wykonanie zgłoszenia serwisowego zostanie potwierdzone podpisaniem Formularza wykonania zgłoszenia serwisowego, którego wzór określa Załącznik nr 6 do Umowy, a następnie przesłaniem potwierdzenia do systemu obsługi zgłoszeń Zamawiającego (HP Service Manager), w którym załączony będzie skan podpisanego Formularza wykonania zgłoszenia serwisowego. Czasem wykonania zgłoszenia będzie czas z podpisanego protokołu, czas ten będzie odnotowany w systemie obsługi zgłoszeń Zamawiającego (HP Service Manager). Dopuszcza się opóźnienie w dosłaniu skanu podpisanego Formularza zrealizowania zgłoszenia serwisowego do systemu obsługi zgłoszeń Zamawiającego (HP Service Manager) do 2 dni roboczych Zamawiającego. W przypadku braku możliwości przesłania dokonania potwierdzenia zgłoszenia serwisowego przez system HP Service Manager, usługi serwisowe będą zgłaszane za pośrednictwem poczty email, z uwzględnieniem ust. 7.
13. W przypadku niemożności dokonania naprawy serwisowej w terminie określonym w ust. 10, Wykonawca, na czas naprawy, dostarczy i skonfiguruje w terminie, o którym mowa w ust. 10, urządzenie zastępcze o parametrach technicznych takich samych lub lepszych, jak urządzenie naprawiane.
14. W przypadku niemożności dokonania naprawy serwisowej urządzenia, o której mowa w ust. 10, w terminie 14 dni od momentu zgłoszenia awarii przez Zamawiającego, Wykonawca przed upływem tego terminu przekaże Zamawiającemu na własność fabrycznie nowe urządzenie o parametrach technicznych takich samych lub lepszych, jak

urządzenie uszkodzone, pod rygorem zapłaty kar umownych, o których mowa w § 6 ust. 11.

15. Wykonawca zobowiązuje się do wymiany urządzenia na fabrycznie nowe pod rygorem zapłaty kar umownych, o których mowa w § 6 ust. 11, w terminie o którym mowa w ust. 14, o parametrach technicznych takich samych lub lepszych, jak urządzenie posiadane przez Zamawiającego w przypadku, gdy po wykonaniu trzech napraw tego samego podzespołu jednego urządzenia, będzie wykazywało ono nadal wady w działaniu lub w przypadku wykonaniu trzech napraw różnych podzespołów jednego urządzenia, urządzenie nadal będzie wykazywało objawy tej samej usterki lub awarii. Nowe urządzenie powinno być wyprodukowane nie wcześniej niż 6 miesięcy przed datą zawarcia Umowy.
16. Warunki i postanowienia Umowy są nadrzędne nad warunkami zawartymi w karcie gwarancyjnej i dokumencie licencyjnym chyba, że uregulowania wynikające z karty gwarancyjnej i dokumentu licencyjnego są dla Zamawiającego korzystniejsze od postanowień Umowy. Zapisy w karcie gwarancyjnej nie mogą być sprzeczne z postanowieniami Umowy.
17. Wykonawca zobowiązuje się dokonać okresowych przeglądów konserwacyjnych zgodnie z poniższymi wymaganiami:
    1) Wymaga się wykonywania cyklicznych przeglądów systemów i konfiguracji oraz dokonywania analizy oprogramowania wbudowanego i systemowego – co najmniej raz na 3 miesiące trwania gwarancji, z zastrzeżeniem że ostatni przegląd musi odbyć się w 35 miesiącu trwania gwarancji;
    2) Wymaga się wykonania cyklicznej weryfikacji poziomu dostępności systemu – co najmniej raz na 12 miesięcy trwania gwarancji, z zastrzeżeniem że ostatnia weryfikacja musi odbyć się w 35 miesiącu trwania gwarancji;
    3) Wymaga się wykonania cyklicznej analizy warunków eksploatacyjnych – co najmniej raz na 12 miesięcy trwania gwarancji, z zastrzeżeniem że ostatnia analiza musi odbyć się w 35 miesiącu trwania gwarancji.
18. Harmonogram wykonania okresowych przeglądów konserwacyjnych, o których mowa w ust. 17, ustalony zostanie pisemnie z Zamawiającym w terminie 30 dni od daty zawarcia Umowy. Potwierdzeniem wykonania przeglądu konserwacyjnego będzie podpisanie bez zastrzeżeń przez Zamawiającego Protokołu wykonania przeglądu konserwacyjnego, którego wzór określa Załącznik nr 7 do Umowy.
19. Wszystkie nośniki danych (dysk twardy), w przypadku awarii dysków lub sprzętu zawierającego nośniki danych, pozostają u Zamawiającego.
20. Urządzenia lub ich części pozostałe po naprawie, pozostają własnością Zamawiającego.
21. Szczegółowe warunki gwarancji zostały zawarte w pkt 13 „Gwarancja (usługi serwisu gwarancyjnego)” w Załączniku nr 1 do Umowy.

§ 8
Zabezpieczenie należytego wykonania Umowy

1. Wykonawca udzielił Zamawiającemu zabezpieczenia należytego wykonania Umowy

w formie ……., w wysokości …….zł (słownie złotych: …….), tj. 10 % wynagrodzenia brutto za realizację przedmiotu Umowy, określonego w § 2 ust. 1 Umowy, ważnego od dnia zawarcia Umowy do dnia upływu okresu rękojmi, o którym mowa w § 7 ust. 2, przedłużonego o 15 dni, z uwzględnieniem ust. 3.

2. Wykonawca ma prawo zmienić formę zabezpieczenia należytego wykonania Umowy na inną przewidzianą w art. 148 ustawy Prawo zamówień publicznych zgodnie z zasadami określonymi w art. 149 tej ustawy. Zmiana ta nie powoduje konieczności zmiany Umowy.
3. Zabezpieczenie należytego wykonania Umowy będzie zwrócone Wykonawcy w następujący sposób:
   a) 70% wartości zabezpieczenia zostanie zwrócone w terminie 30 dni od dnia wykonania zamówienia i uznania przez Zamawiającego za należycie wykonane, co zostanie potwierdzone podpisaniem bez zastrzeżeń przez Strony Protokołu końcowego odbioru wdrożenia, którego wzór określa Załącznik nr 4 do Umowy,
   b) 30% wartości zabezpieczenia zostanie zatrzymane przez Zamawiającego na zabezpieczenie roszczeń z tytułu rękojmi za wady – kwota ta zostanie zwrócona w terminie 15 dni po upływie okresu rękojmi.
4. Zabezpieczenie należytego wykonania Umowy służy do pokrycia roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, a także pokrycia roszczeń z tytułu rękojmi, bez potrzeby uzyskania zgody Wykonawcy, w tym potrącania kar umownych.

§ 9
Licencje i majątkowe prawa autorskie

1. Z dniem podpisania przez Strony Protokołu cząstkowego odbioru w części B.2. (Załącznik nr 3 do Umowy) Wykonawca udziela Zamawiającemu nieodwołalnej, niewyłącznej i niezbywalnej licencji na korzystanie z oprogramowania stanowiącego przedmiot Umowy, z zastrzeżeniem możliwości wypowiedzenia licencji jedynie w przypadku rażącego naruszania przez Zamawiającego warunków licencyjnych. W ramach licencji na korzystanie z oprogramowania Zamawiający jest uprawniony do:
   1) trwałego lub czasowego zwielokrotnienia programu komputerowego w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,
   2) instalacji, uruchamiania, przechowywania i korzystania,
   3) implementacji w środowisku operacyjnym Zamawiającego,
   4) wprowadzania i przechowywania w pamięci komputerów zgodnie z dostarczonym przez Wykonawcę dokumentem licencyjnym (licence agreement),
   5) uruchamiania, wyświetlania i stosowania w celach zgodnych z dokumentacją,

6) przystosowywania, wprowadzania zmian układu lub innych zmian wyłącznie w zakresie, w jakim to przystosowywanie lub zmiany będą niezbędne do korzystania zgodnie z przeznaczeniem.

2. Wykonawca przeniesie na Zamawiającego autorskie prawa majątkowe do dokumentacji technicznej powstałej w związku z realizacją przedmiotu Umowy.
3. Wykonawca oświadcza, że od dnia wydania dokumentacji technicznej Zamawiającemu przysługiwać będą majątkowe prawa autorskie do tej dokumentacji w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych w zakresie niezbędnym do wykonania Umowy.
4. Przeniesienie autorskich praw majątkowych do dokumentacji technicznej obejmuje nieograniczone w czasie oraz nieograniczone terytorialnie korzystanie i rozporządzanie utworami na polach eksploatacji określonych w art. 50 oraz art. 74 ust. 4 ustawy o prawie autorskim i prawach pokrewnych, w tym w szczególności obejmujących:
   1) wykorzystywanie w działalności prowadzonej przez Zamawiającego bez jakichkolwiek ograniczeń,
   2) utrwalanie i zwielokrotnianie w całości lub części, wytwarzanie dowolną techniką egzemplarzy, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową, przekazywanie, przechowywanie, wyświetlanie,
   3) tłumaczenie, przystosowywanie, zmiana układu lub jakiekolwiek inne zmiany w dokumentacji technicznej,
   4) wprowadzanie do obrotu, użyczanie, najem, dzierżawa oryginału lub egzemplarzy, na których dokumentację techniczną utrwalono, upoważnianie innych osób do wykorzystywania w całości lub części dokumentacji lub jej kopii,
   5) rozpowszechnianie poprzez publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie a także publiczne udostępnienie w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym.
5. Zamawiający może wykonywać autorskie prawa majątkowe samodzielnie lub może upoważnić do tego osoby trzecie.
6. Wykonawca przenosi na Zamawiającego wyłączne prawo do wykonywania zależnych praw autorskich oraz prawo do zezwalania na wykonywanie zależnych praw autorskich do dokumentacji, o której mowa w ust. 2, w szczególności do tłumaczenia, przystosowywania, zmiany układu oraz wprowadzania innych zmian lub modyfikacji i nie będzie domagał się z tego tytułu dodatkowego wynagrodzenia.
7. Wykonawca zapewni, by posiadacze autorskich praw osobistych do dokumetacji nie wykonywali ich w stosunku do Zamawiającego.
8. Z chwilą przeniesienia autorskich praw majątkowych do dokumentacji, na Zamawiającego przechodzi prawo własności nośnika, na którym została ona utrwalona i przekazana Zamawiającemu.

9. Wykonawca zapewnia, że korzystanie przez Zamawiającego z praw autorskich i praw pokrewnych, przenoszonych na podstawie Umowy i w sposób przez nią przewidziany nie będzie naruszało żadnych praw osób trzecich.
10. Wykonawca ponosi odpowiedzialność za roszczenia osób trzecich związanych z naruszeniem autorskich praw majątkowych do utworów powstałych w wyniku realizacji Umowy i zobowiązuje się do zaspokojenia wszelkich roszczeń z tym związanych, na następujących zasadach:
    1) W zakresie dopuszczonym prawem Wykonawca podejmie obronę Zamawiającego (przystąpi do postępowania po jego stronie) w przypadku zgłoszenia przez osobę trzecią przeciwko Zamawiającemu roszczenia z tytułu naruszenia przez utwory dostarczone na podstawie Umowy chronionego know-how, patentów, praw ochronnych do wzoru użytkowego, wzoru przemysłowego, topografii układów scalonych, znaku towarowego lub praw autorskich;
    2) Jeżeli dostarczone produkty wytworzone przez Wykonawcę faktycznie naruszać będą prawa osób trzecich, Wykonawca niezwłocznie przystąpi do ich modyfikacji w sposób pozwalający na ich dalsze wykorzystywanie przez Zamawiającego bez naruszania prawa osób trzecich lub uzyska dla Zamawiającego na swój koszt odpowiednią licencję na produkty dotknięte naruszeniem a także w terminie uzgodnionym z Zamawiającym pokryje odszkodowania, które w związku z powyższymi roszczeniami osób trzecich zostały zasądzone od Zamawiającego prawomocnym wyrokiem.

§ 10
Bezpieczeństwo informacji

1. Wykonawca jest zobowiązany do zachowania w tajemnicy informacji, danych i wiedzy, bez względu na formę ich utrwalenia, stanowiących tajemnicę prawnie chronioną Zamawiającego, uzyskanych w trakcie wykonywania Umowy.
2. Wykonawca jest zobowiązany zachować w tajemnicy pozyskane od Zamawiającego informacje dotyczące rozmieszczenia i konfiguracji infrastruktury techniczno-systemowej oraz stosowanych zabezpieczeń.
3. Uzyskane przez Wykonawcę, w związku z wykonywaniem Umowy, informacje nie mogą być wykorzystane do innego celu, niż do realizacji Umowy.
4. Zobowiązanie do zachowania w tajemnicy nie dotyczy informacji, które:
    1) stały się publicznie dostępne bez naruszenia przez Wykonawcę postanowień Umowy,
    2) były znane przed otrzymaniem ich od Zamawiającego i nie były objęte zobowiązaniem do zachowania w tajemnicy wobec jakiegokolwiek podmiotu,
    3) podlegają ujawnieniu na mocy przepisów prawa.
5. W terminie 5 dni roboczych Zamawiającego od rozwiązania lub wygaśnięcia Umowy Wykonawca zobowiązany jest do zwrotu Zamawiającemu lub zniszczenia wszelkich materiałów zawierających informację stanowiącą tajemnicę prawnie chronioną

Zamawiającego, jakie otrzymał lub wytworzył w związku z wykonywaniem Umowy, za wyjątkiem jednej kopii ww. materiałów niezbędnych do ewentualnego dochodzenia roszczeń, które zostaną zniszczone z upływem terminu przedawnienia roszczeń. Wykonawca zapewni tym materiałom ochronę w stopniu co najmniej równym poziomowi ochrony, na jakim chroni własne informacje. Potwierdzenie zwrotu ww. materiałów dokumentuje się w protokole, który podpisują Zamawiający i Wykonawca. Niezwłocznie po upływie terminu przedawnienia potencjalnych roszczeń Wykonawca informuje pisemnie Zamawiającego o zniszczeniu kopii materiałów pozostawionych do ewentualnego dochodzenia roszczeń.

6. Osoby wykonujące zadania w związku z realizacją Umowy na terenie budynków, pomieszczeń lub części pomieszczeń użytkowanych przez Zamawiającego są zobowiązane do przestrzegania obowiązujących u Zamawiającego uregulowań wewnętrznych dotyczących bezpieczeństwa informacji. Wszystkie osoby biorące udział w realizacji przedmiotu Umowy zostaną poinformowane, iż przedmiotowe informacje stanowią tajemnicę prawnie chronioną Zakładu oraz zobowiązane są do zachowania ich w tajemnicy. W takim przypadku Wykonawca odpowiedzialny jest za wszelkie naruszenia dokonane przez takie osoby, włącznie z odpowiedzialnością materialną.
7. Zamawiający zastrzega sobie możliwość dochodzenia roszczeń wobec Wykonawcy, w wypadku wyrządzenia przez niego szkód Zamawiającemu lub osobom trzecim, będących wynikiem naruszenia bezpieczeństwa informacji, na zasadach określonych w Kodeksie Cywilnym.

§ 11
Powierzenie przetwarzanie danych osobowych

1. Wykonawca realizuje przetwarzanie danych osobowych jako podmiot, któremu Zamawiający, jako administrator danych, powierzył przetwarzanie danych w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135).
2. Wykonawca może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianym w Umowie.
3. Wykonawca jest zobowiązany poinformować osoby wykonujące w jego imieniu zadania związane z realizacją Umowy o obowiązkach wynikających z przepisów ustawy o ochronie danych osobowych, a w szczególności o obowiązku zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.
4. Wykonawca jest zobowiązany przekazać do Zamawiającego dane osób wykonujących w jego imieniu zadania związane z przetwarzaniem danych osobowych w ramach Umowy, w celu nadania im przez Zamawiającego stosownych upoważnień do przetwarzania danych. Wzór upoważnienia do przetwarzania danych osobowych i oświadczenia osób wykonujących w imieniu Wykonawcy zadania związane z realizacją Umowy znajduje się w Załączniku nr 11 do Umowy.
5. Osoby wykonujące w imieniu Wykonawcy zadania związane z realizacją Umowy są zobowiązane do przestrzegania uregulowań wewnętrznych aktów prawnych

Zamawiającego dotyczących bezpieczeństwa informacji, w tym w szczególności uregulowań zawartych w:

1) Polityce bezpieczeństwa informacji w Zakładzie Ubezpieczeń Społecznych;
2) Polityce bezpieczeństwa danych osobowych w Zakładzie Ubezpieczeń Społecznych;
3) Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Zakładzie Ubezpieczeń Społecznych;
4) Procedurze postępowania w sytuacji naruszenia ochrony danych osobowych w Zakładzie Ubezpieczeń Społecznych.

6. Wykonawcy zabrania się wykonywania kopii danych zawierających dane osobowe.
7. Osoby wykonujące w imieniu Wykonawcy zadania związane z realizacją Umowy są zobowiązane informować bezzwłocznie Zamawiającego o wszelkich stwierdzonych przypadkach naruszenia zasad ochrony danych osobowych lub o niewłaściwym ich przetwarzaniu.
8. W wypadku przetwarzania danych z naruszeniem przepisów o ochronie danych osobowych lub niezgodnie z Umową Wykonawca ponosi odpowiedzialność wobec Zamawiającego i wobec osób, których dotyczą przetwarzane dane osobowe, na zasadach określonych w kodeksie cywilnym.
9. W sprawach nieuregulowanych w Umowie mają zastosowanie przepisy ustawy o ochronie danych osobowych.

§ 12
Siła wyższa

1. Strony Umowy będą zwolnione z odpowiedzialności za niewypełnienie swoich zobowiązań zawartych w Umowie z powodu siły wyższej, jeżeli okoliczności zaistnienia siły wyższej będą stanowiły przeszkodę w ich wypełnieniu.
2. Siłą wyższą jest zdarzenie zewnętrzne, nie posiadające swojego źródła wewnątrz przedsiębiorstwa, niemożliwe do przewidzenia oraz niemożliwe do zapobieżenia, przy czym dotyczy to niemożliwości zapobieżenia jego szkodliwym następstwom.
3. Strona może powołać się na zaistnienie siły wyższej tylko wtedy, gdy poinformuje ona o tym pisemnie drugą stronę w ciągu 3 dni kalendarzowe od jej zaistnienia.
4. Okoliczności zaistnienia siły wyższej muszą zostać udowodnione przez stronę, która się na nie powołuje.

§ 13
Zmiany Umowy

1. Zamawiający dopuszcza możliwość dokonania zmian Umowy w zakresie opisu przedmiotu zamówienia i jego cech oraz sposobu i terminu jego realizacji – jeżeli zmiany są korzystne dla Zamawiającego lub wywołane okolicznościami, których nie można było przewidzieć w momencie składania oferty.

2. Zamawiający nie dopuszcza możliwości zmiany Umowy w zakresie przeniesienia praw i obowiązków wynikających z Umowy na osoby trzecie w zakresie cesji wierzytelności.
3. Zamawiający dopuszcza zmianę Umowy w sytuacji, gdy wynika to z okoliczności, których nie można było przewidzieć w chwili zawarcia Umowy lub zmiany te są korzystne dla Zamawiającego.
4. Zmiana postanowień Umowy wymaga formy pisemnego aneksu pod rygorem nieważności z wyłączeniem zmiany osób do kontaktu, danych teleadresowych oraz zmiany treści dokumentu stanowiącego Załącznik nr 9 do Umowy.
5. Z wnioskiem o zmianę postanowień Umowy może wystąpić zarówno Wykonawca, jak i Zamawiający.

§ 14
Postanowienia ogólne

1. Wszelkie spory mogące wyniknąć z zawarcia i wykonania Umowy, Strony poddają pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
2. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164, t.j.), Kodeksu cywilnego, ustawy z dnia 4 lutego 1994 r. – o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.) oraz inne przepisy mające związek z przedmiotem Umowy.
3. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach. W tym przypadku Wykonawca może żądać jedynie zapłaty z tytułu zrealizowanej części Umowy.
4. Zamawiający nie dopuszcza możliwości zmiany Umowy w zakresie cesji wierzytelności na osoby trzecie.
5. Załączniki do Umowy stanowią jej integralną część.
6. Umowa zostaje zawarta z chwilą podpisania jej przez Strony.
7. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla Zamawiającego oraz jeden egzemplarz dla Wykonawcy.

Wykaz załączników:

Załącznik nr 1 – Opis przedmiotu zamówienia

Załącznik nr 2 – Formularz ofertowy (*zgodnie z ofertą wybranego Wykonawcy*)

Załącznik nr 3 – Protokół cząstkowy odbioru

Załącznik nr 4 – Protokół końcowy odbioru wdrożenia

Załącznik nr 5 – Formularz zgłoszenia awarii

Załącznik nr 6 – Formularz wykonania zgłoszenia serwisowego

Załącznik nr 7 – Protokół wykonania przeglądu konserwacyjnego

Załącznik nr 8 – Szczegółowa procedura odbioru przedmiotu Umowy

Załącznik nr 9 – Komunikacja pomiędzy HP SM a systemem obsługi incydentów Wykonawcy

Załącznik nr 10 – Protokół potwierdzenia integracji

Załącznik nr 11 – Upoważnienie do przetwarzania danych osobowych

Załącznik nr 12 – Protokół przeprowadzenia szkolenia

Załącznik nr 13 – Miesięczny raport z wykonanych usług

ZAMAWIAJĄCY **WYKONAWCA**

…….. ……

Załącznik nr 1
do Umowy nr …… (TZ/271/79/15)

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Słownik pojęć

COO- Centralny Ośrodek Obliczeniowy
ZCOO- Zapasowy Centralny Ośrodek Obliczeniowy
DC- Data Center (serwerownie ZUS COO i ZCOO)
DWDM- Dense Wavelength Division Multiplexing – technika zwielokrotnienia w dziedzinie długości fali, wykorzystywana w transmisji światłowodowej
PUE- Platforma Usług Elektronicznych

Wszystkie wymagane pojemności macierzy użyte w specyfikacji odpowiadają założeniu:

- 1TB = 1024GB,
- 1GB = 1024MB,
- 1MB = 1024kB,
- 1kB = 1024B.

II. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest modernizacja infrastruktury dla PUE poprzez zwiększenie mocy obliczeniowej oraz bezpieczeństwa przetwarzania danych, w tym dostarczenie urządzeń oraz licencji na oprogramowanie wraz z 36 miesięczną gwarancją i usługami wdrożeniowymi.

2. Wszędzie tam gdzie przedmiot zamówienia został opisany przez wskazanie znaków towarowych, patentów lub pochodzenia dopuszcza się zaoferowanie produktów równoważnych. Za produkty równoważne Zamawiający uzna produkty o nie gorszych parametrach technicznych niż produkty określone w OPZ. W przypadku zaoferowania produktów równoważnych których zastosowanie prowadzi do zmiany platformy, za produkt równoważny zostanie uznane rozwiązanie obejmujące:

- dostosowanie (wraz z migracją) wszystkich aplikacji pracujących w PUE oraz oprogramowania systemowo narzędziowego do prawidłowej pracy na zaoferowanym rozwiązaniu,
- zapewnienie nieprzerwanego, prawidłowego funkcjonowania PUE przez cały okres trwania umowy,
- zapewnienie mechanizmów ciągłości działania dla zaproponowanej platformy wraz z dostosowaniem wszystkich procedur eksploatacyjnych, administratorskich dla zaproponowanych rozwiązań,
- przeszkolenie pracowników (administratorów i operatorów) Zamawiającego z zastosowanych rozwiązań techniczno-systemowych.

3. Miejsce dostawy przedmiotu zamówienia:

3.1. Szamocka 3, 01-748 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Centralnego Ośrodka Obliczeniowego (COO) w Warszawa

3.2. Czerniakowska 16, 00-701 Warszawa – do tej lokalizacji dostarczane są elementy przedmiotu zamówienia przeznaczone dla Zapasowego Centralnego Ośrodka Obliczeniowego (ZCOO) w Warszawie

4. Zestawienie elementów przedmiotu zamówienia w podziale na lokalizacje oraz poziom serwisu gwarancyjnego ujęte jest w tabelach poniżej. W przypadku nie ujęcia któregoś z elementów przedmiotu zamówienia w poniższych tabelach, Zamawiający przekaże Wykonawcy informacje o szczegółowym rozmieszczeniu elementów w ciągu 3 dni od dnia podpisania umowy.

Tabela nr 1, Zestawienie ilościowe, miejsce instalacji:

LP	KOMPONENT	ILOŚĆ	COO	ZCOO
1.	Rozbudowa mocy obliczeniowej środowiska			
	Rozbudowa mocy obliczeniowej środowiska serwerów bazodanowych- typ A (docelowo serwery fizyczne)	4	2	2
	Rozbudowa mocy obliczeniowej środowiska serwerów aplikacyjnych- typ B (docelowo serwery pod wirtualizację)	10	5	5
2.	Ruter brzegowy	4	2	2

3.	Przełącznik sieciowy	4	2	2
4.	Przełącznik do zarządzania urządzeniami MGMT	2	1	1
5.	Urządzenie balansujące ruch sieciowy	4	2	2
6.	System bezpieczeństwa	2*	1*	1*
7.	Sprzętowy moduł bezpieczeństwa	2	0	2
8.	Przełącznik SAN	4	2	2
9.	Macierz dyskowa	2	1	1
10.	System zarządzania dostarczonymi urządzeniami	1		
11.	Oprogramowanie			
	Oprogramowanie wirtualizacyjne	1**		
	Oprogramowanie serwerowe dla PUE	1**		
12.	Usługa wdrożenia i szkolenia	1		
13.	Gwarancja	1		

*- ilość urządzeń w systemie bezpieczeństwa zależy od zaproponowanego rozwiązania

**- zgodnie z zapisami punktu 11 Oprogramowanie

5. Sprzęt

5.1. Dostarczony w ramach niniejszego zamówienia sprzęt komputerowy oraz urządzenia sieciowe muszą być fabrycznie nowe i będą pochodzić z bieżącej produkcji, tj. wyprodukowane nie wcześniej, niż 6 miesięcy przed datą zawarcia umowy, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia. (ang. refurbished), a także wolne od wad oraz posiadać pełen zestaw przewidzianych przez producenta właściwych nośników (np. sterowniki).

5.2. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego.

5.3. Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument wystawiony przez producenta sprzętu lub jego oficjalnego przedstawiciela potwierdzający zarejestrowanie kontraktu serwisowego na dostarczone urządzenia i oprogramowanie. Serwis gwarancyjny musi obejmować prawo do aktualizacji wersji oprogramowania systemowego oraz oprogramowania wbudowanego (tzw. firmware) urządzeń. Wykonawca zapewni Zamawiającemu dostęp do:

5.3.1. nowych wersji oprogramowania,

5.3.2. narzędzi konfiguracyjnych i dokumentacji technicznej,

5.3.3. pomocy technicznej producentów,

5.3.4. prawo bezpośredniego zgłaszania przez Zamawiającego usterek i awarii sprzętu do Producenta.

5.4. Ze względu na pożądaną pełną kompatybilność oraz zabezpieczenie uprawnień gwarancyjnych Zamawiającego, dostarczane w ramach Zamówienia rozwiązania (urządzenia oraz karty i moduły do nich) powinny pochodzić od jednego producenta, chyba że wymagania szczegółowe stanowią inaczej. W przypadku oferowania urządzeń różnych producentów, należy dostarczyć oświadczenia ich producentów o pełnej wzajemnej kompatybilności oraz oświadczenia o współpracy autoryzowanych placówek serwisowych producentów w zakresie usuwania problemów powstających na styku rozwiązań.

5.5. Wszystkie wymagania przedstawione w niniejszym dokumencie muszą zostać spełnione w aktualnie dostępnych komercyjnie rozwiązaniach oprogramowania i sprzętu. Nie dopuszcza się możliwości, że wykonawca określi przyszłą wersję oprogramowania lub sprzętu, która będzie spełniać daną wyspecyfikowaną funkcjonalność.

5.6. Wymagane jest dostarczenie, wraz z dostawą urządzeń, szczegółowej dokumentacji technicznej producenta oferowanych produktów potwierdzającej spełnianie wymagań technicznych urządzeń będących przedmiotem zamówienia (Zamawiający dopuszcza w tym przypadku możliwość złożenia dokumentacji w języku angielskim).

5.7. W wypadku powzięcia wątpliwości co do zgodności oferowanych produktów z umową, w szczególności w zakresie legalności oprogramowania, Zamawiający jest uprawniony do:

5.7.1. zwrócenia się do producenta oferowanych produktów o potwierdzenie ich zgodności z umową (w tym także do przekazania producentowi niezbędnych danych umożliwiających weryfikację),

oraz zlecenia producentowi oferowanych produktów, lub wskazanemu przez producenta podmiotowi,

5.7.2. inspekcji produktów pod kątem ich zgodności z umową oraz ważności i zakresu uprawnień licencyjnych.

5.8. Jeżeli inspekcja, o której mowa powyżej wykaże niezgodność produktów z umową lub stwierdzi, że korzystanie z produktów narusza majątkowe prawa autorskie osób producenta, koszt inspekcji zostanie pokryty przez Wykonawcę, według rachunku przedstawionego przez podmiot wykonujący inspekcję, w kwocie nie przekraczającej 30% wartości zamówienia (ograniczenie to nie dotyczy kosztów poniesionych przez Strony w związku z inspekcją, jak np. konieczność zakupu nowego oprogramowania). Prawo zlecenia inspekcji nie ogranicza ani nie wyłącza innych uprawnień Zamawiającego, w szczególności prawa do żądania dostarczenia produktów zgodnych z umową oraz roszczeń odszkodowawczych.

5.9. Sprzęt komputerowy oraz urządzenia sieciowe, jeśli jest to dla nich wymagane, winny posiadać certyfikat CE lub deklarację zgodności CE.

5.10. Sprzęt komputerowy i urządzenia sieciowe winny spełniać wymagania Rozporządzenia Ministra Gospodarki z dnia 8 maja 2013 r. w sprawie zasadniczych wymagań dotyczących ograniczenia stosowania niektórych niebezpiecznych substancji w sprzęcie elektrycznym i elektronicznym (Dz. U. z 10 maja 2013r., poz. 547).

5.11. Wykonawca dostarczy sprzęt zgodnie z wymaganiami zawartymi w kolejnych rozdziałach niniejszego Opisu Przedmiotu Zamówienia. Wykonawca dostarczy sprzęt wraz z niezbędnym okablowaniem, dokumentacją techniczno-eksploatacyjną, certyfikatami bezpieczeństwa oraz dokumentami potwierdzającymi udzielenie Zamawiającemu gwarancji na te urządzenia.

5.12. Zamawiający zapewni infrastrukturę miejsca instalacji obejmującą:

5.12.1. miejsce na umieszczenie sprzętu,

5.12.2. dostęp do zasilania energetycznego,

5.12.3. dostęp do sieci teleinformatycznej.

5.13. Wszelkie koszty związane z dostawą do wskazanego przez Zamawiającego miejsca i wdrożenia sprzętu oraz oprogramowania ponosi Wykonawca.

6. Oprogramowanie

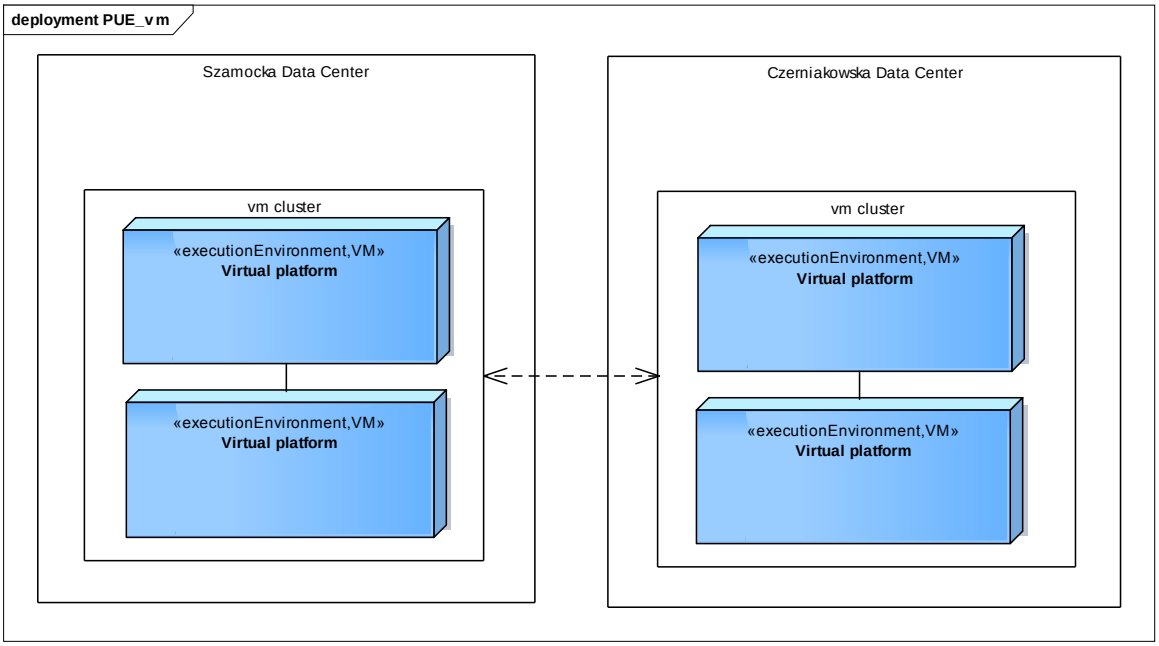
6.1. Wykonawca dostarczy oprogramowanie standardowe (oprogramowanie typu COTS - Commercial off-the-shelf – „z półki" lub oprogramowanie typu open-source) zgodnie z wymaganiami Zamawiającego. Za oprogramowanie standardowe może być uznane tylko oprogramowanie powszechnie dostępne. Wraz z oprogramowaniem standardowym Wykonawca dostarczy dokumentację dotyczącą dostarczonego oprogramowania (w tym licencje/sublicencje dla oprogramowania innego niż typu open-source). Dostarczone licencje/sublicencje nie mogą być ograniczone w czasie. Dla oprogramowania standardowego Wykonawca zapewni usługi serwisu gwarancyjnego polegające na dostarczaniu przez cały okres realizacji umowy poprawek oraz aktualizacji oprogramowania standardowego udostępnianych przez producenta.

6.2. Licencje/sublicencje nie mogą być związane z konkretnym sprzętem, powinny natomiast umożliwiać przenoszenie licencjonowanego/sublicencjonowanego oprogramowania pomiędzy poszczególnym sprzętem (nawet sprzętem zakupionym przez Zamawiającego poza niniejszym postępowaniem), przy zachowaniu ograniczeń na liczbę komputerów i procesorów, na których jest zainstalowane i uruchomione oprogramowanie standardowe, zgodnie z warunkami licencji/sublicencji.

6.3. Wykonawca zapewnia i zobowiązuje się, że zgodne z niniejszą umową korzystanie przez Zamawiającego z dostarczonych produktów nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich.

7. Usługa przebudowy środowiska

7.1. Wymaganiem zamawiającego jest aby dostarczona w ramach zamówienia platforma wirtualizacyjna, działająca na serwerach, mogła pracować w trybie zwiększonej dostępności tzn. „High availability" z uwzględnieniem dwóch ośrodków. Zgodnie z niniejszym rysunkiem poglądowym Wykonawca musi dostarczyć rozwiązanie redundantne względem pojedynczej lokalizacji, jak i dwóch serwerowni.



Rysunek nr 1

8. Główne założenia przebudowy środowiska Platformy Usług Elektronicznych:

8.1. Wirtualizacja na platformie dostarczonej w niniejszym zamówieniu.

8.2. Rozdzielenie infrastruktury na dwa ośrodki.

8.3. Wdrożenie rozwiązania wirtualizującego oraz przygotowanie serwerów wirtualizacyjnych. Wykonawca musi zainstalować i skonfigurować wszystkie komponenty zgodnie z zapisami projektu implementacyjnego.

8.4. Migracja danych z obecnej macierzy HP EVA 4400 do nowo dostarczonej macierzy w dwóch ośrodkach.

8.5. Skonfigurowanie komunikacji za pomocą DWDM i łącz Internetowych w obu ośrodkach COO i ZCOO.

8.6. Przeprojektowanie sieci w taki sposób, aby odseparować ruch produkcyjny, administracyjny oraz backupowy oraz rekonfiguracji infrastruktury sieci SAN.

8.7. Upgrade technologiczny infrastruktury sieciowej (podniesienie wydajności przynajmniej do 10Gbps)

8.8. Zwielokrotnienie i rozproszenie środowisk wraz z konieczną rekonfiguracją aplikacji portalu PUE po systemach obu centrów przetwarzania danych

8.9. Opracowanie i przygotowanie do testów rozwiązań równoważących obciążenie sieciowe

8.10. Wprowadzenie polityk bezpieczeństwa na zapory ogniowe środowiska.

8.11. Opracowanie scenariuszy zabezpieczeń wirtualizatora dla poszczególnych komponentów środowiska.

9. Aktualna konfiguracja środowiska Platformy Usług Elektronicznych

9.1. W skład tego środowiska wchodzą następujące elementy sprzętowe:

Tabela nr 2, Aktualny sprzęt w środowisku PUE

LP	Komponent	Ilość
1.	Router Cisco 7204VXR,	2
2.	Switch Cisco 3750,	6
3.	Firewalle Cisco 5540,	4
4.	Load balancery Cisco ACE 4710,	2
5.	Urządzenie szyfrujące HSM Thales nShield Connect 500	2
6.	Chassis Blade HP c7000 z serwerami HP BL460 i 685	2
7.	Macierz HP EVA 4400	1

9.2. Serwery można podzielić na dwa obszary: produkcja 19 sztuk oraz środowisko przedprodukcyjne 6 sztuk. Przedprodukcja oraz 17 z 19 serwerów działa na systemie Red Hat Enterprise Linux. Pozostałe dwa serwery PROD_BAMDB działają na systemie Windows Server 2008 i jest tam zainstalowany MS SQL 2008R2 x64 Standard.

9.3. Na serwerach jest zainstalowane oprogramowanie przedstawione w poniższym zestawieniu:

Tabela nr 3, Środowisko produkcyjne

LP	Nazwa serwera	Ilość	Core/ serwer	RAM/ serwre	Oprogramowanie
1	**ESB_B2B**	2	6	8	Red Hat Enterprise Linux 6 SoftwareAG webMethods Integration Server 8
2	**PORTAL**	3	12	16	Red Hat Enterprise Linux 6 JBoos 5
3	**APP**	2	6	8	Red Hat Enterprise Linux 6 Apache Tomcat 7
4	**PROXY**	2	12	4	Red Hat Enterprise Linux 6 Apaceh Reverse 2 Squid Cache 3
5	**VA**	1	12	24	Red Hat Enterprise Linux 6 Apache Tomcat 7 Apache HTTPD
6	**DB**	2	24	96	Red Hat Enterprise Linux 6 PostgreSQL/EnterpriseDB 9
7	**BAM**	1	12	16	Red hat Enterprise Linux 6 myWebmethods Server
8	**BAM_DB**	2	12	32	Microsoft Windows Server 2008 Standard Microsoft SQL Server 2008R2 Standard
10	**ESB_APP**	4	12	16	Red Hat Enterprise Linux 6 SoftwareAG webMethods Integration Server 8

Tabela nr 4, Środowisko przedprodukcyjne

LP	Nazwa serwera	Ilość	Core/ serwer	RAM/ serwre	Oprogramowanie
1	**DB**	2	12	32	Red Hat Enterprise Linux 6 PostgreSQL/EnterpriseDB 9
2	**ESB**	2	12	16	Red Hat Enterprise Linux 6 Red Hat Enterprise Virtualization Hypervisor SoftwareAG webMethods Integration Server 8
3	**TEST_BAM (virtual)**	1	4	4	Red Hat Enterprise Linux 6 myWebmethods Server
4	**TEST_BAM_DB (virtual)**	1	4	8	Microsoft Windows Server 2008 Microsoft SQL Server 2008R2
5	**PORTAL**	2	12	16	Red Hat Enterprise Linux 6 Red Hat Enterprise Virtualization Hypervisor JBoos 5
6	**TEST_VA (virtual)**	1	4	8	Red Hat Enterprise Linux 6 Apache Tomcat 7
7	**TEST_LB (virtual)**	1	4	4	Red Hat Enterprise Linux 6 Apache Reverse 2 Squid Cache 3
8	**TEST_APP (virtual)**	1	4	4	Red Hat Enterprise Linux 6 Aapche Tomcat 7
9	**TEST_PROXY (virtual)**	1	4	4	Red Hat Enterprise Linux 6 Apaceh Reverse 2 Squid Cache 3

Tabela nr 5, Środowisko produkcyjne – posiadane i używane licencje WebMethods

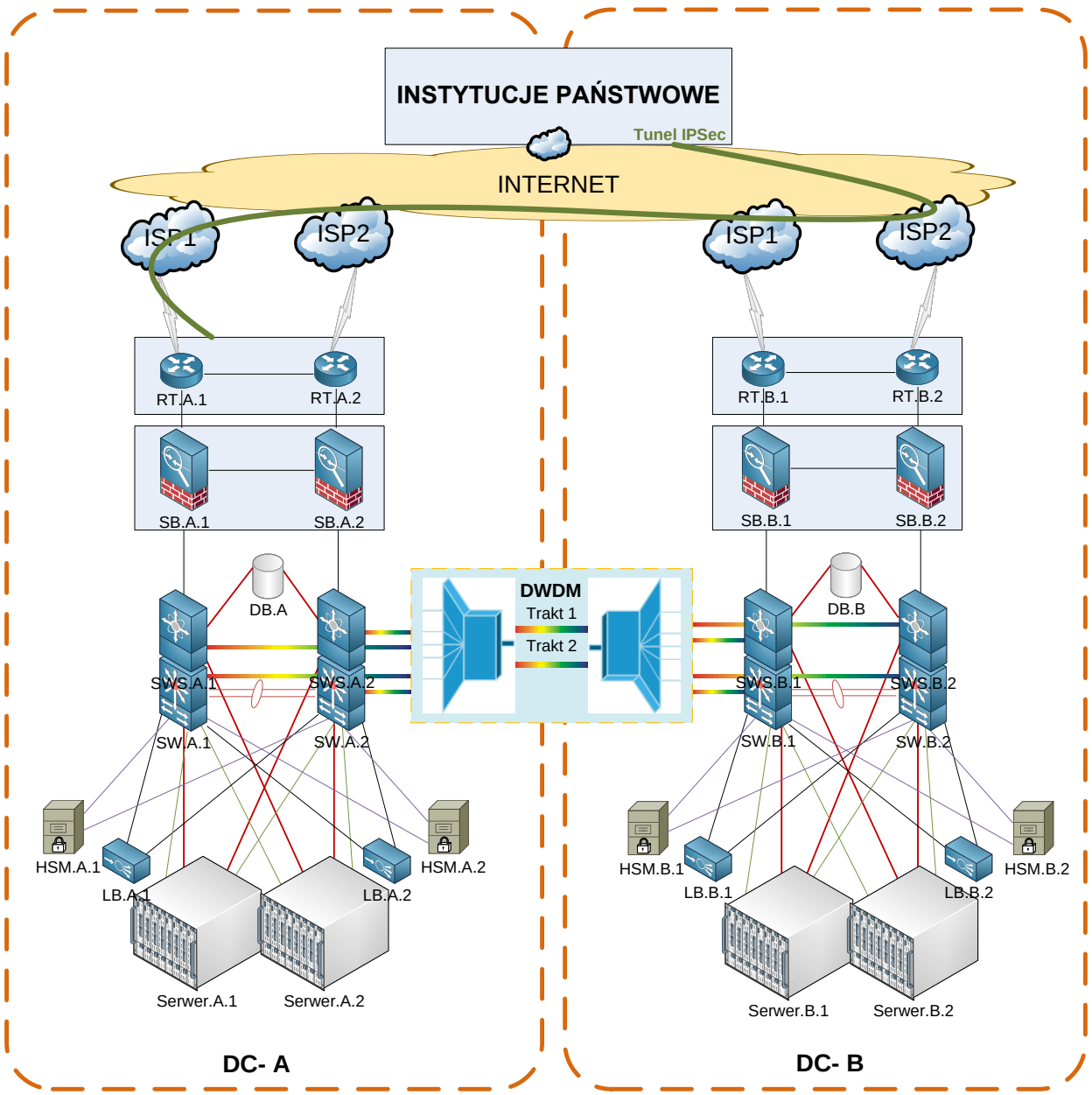
Nr	Oprogramowanie	typ procesora/ limit maszyn/ limit partycji	Nazwa serwera
1	wM Integration Platform Project (Production):	Each	PROD_ESB1..4
	- Intergation Server	-Processor Core Type A	
	- wM Broker	-Processor Core Type A	
2	Enterprise JavaBeans Adapter (Production)	32 Cores Processor Core Type A	PROD_ESB1..4
3	JDBC Adapter (Production)	32 Cores Processor Core Type A	PROD_ESB1..4
4	MQ Adapter (Production)	8 Cores Processor Core Type B	PROD_ESB1..4
5	Adapter Development Kit (Production)	Each	PROD_ESB1..4

6	Trading Networks (Production)	5 Cores Processor Core Type A	PROD_ESBB2B1..2
7	Optimize Base Engine Bundle (Production)	Each	PROD_BAM_1
8	Optimize for Infrastructure Module Bundle (Production)	Each	PROD_BAM_1
	- Optimize for Infrastructure	Each	
9	wM Reporting - Small Bundle (Production)	Each	PROD_BAM_1
10	Optimize for B2B Module Bundle (Production)	Each	PROD_BAM_1
	- Optimize for Process	Each	
	- Optimize for B2B	Each	
11	Wirtualizacja (Production)	32 Cores Processor Core Type A	PROD_xxx

Tabela nr 6, Środowisko przedprodukcyjne – posiadane i używane licencje WebMethods

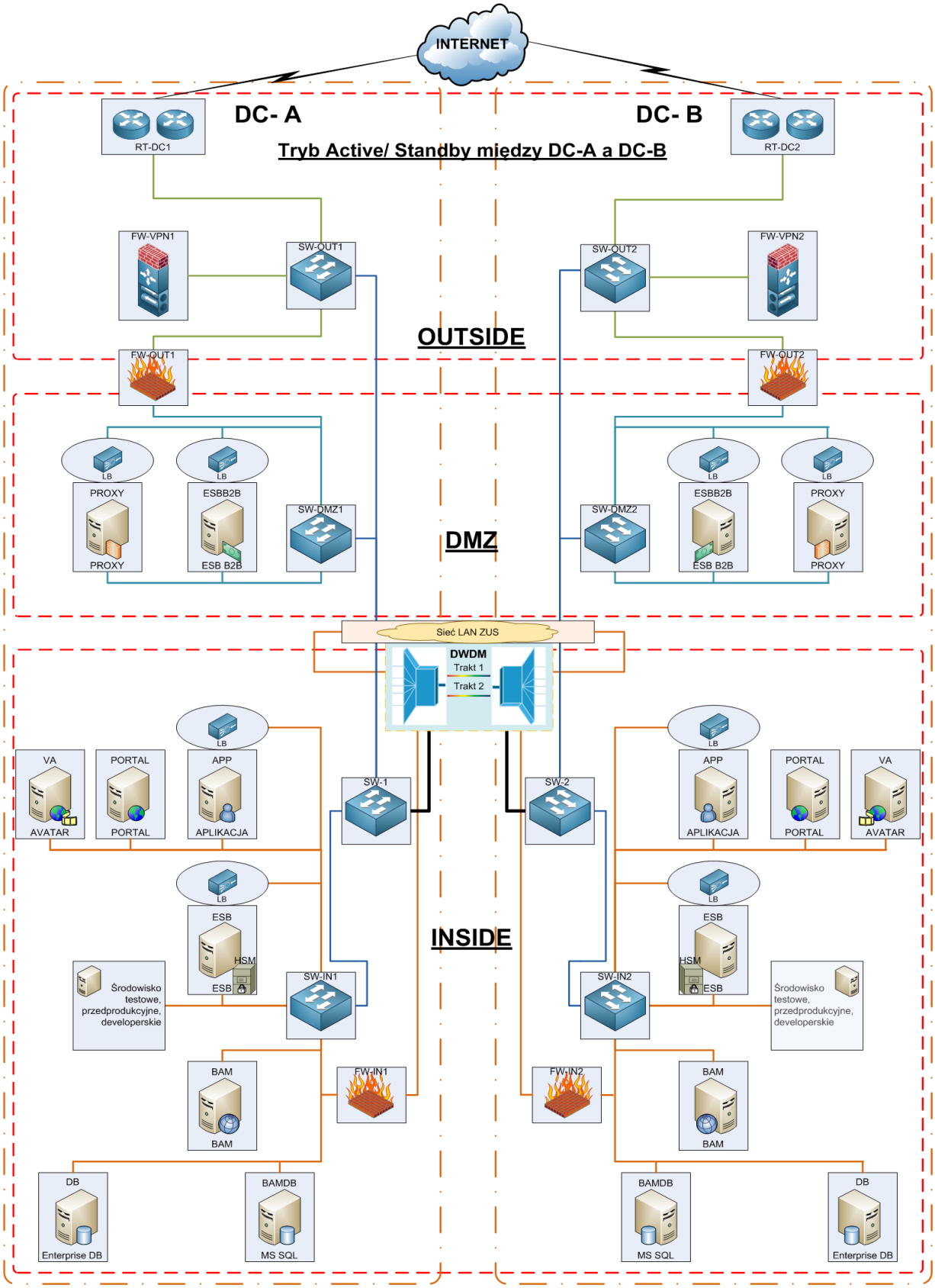
Nr	Oprogramowanie	typ procesora/ limit maszyn/ limit partycji	Nazwa serwera
1	wM Integration Platform Project (Production):	Each	TEST_ESB1..2
	- Intergation Server	-Processor Core Type A	
	- wM Broker	-Processor Core Type A	
2	Enterprise JavaBeans Adapter (Production)	8 Cores Processor Core Type A	TEST_ESB1..2
3	JDBC Adapter (Production)	8 Cores Processor Core Type A	TEST_ESB1..2
4	MQ Adapter (Production)	4 Cores Processor Core Type B	TEST_ESB1..2
5	Adapter Development Kit (Production)	Each	TEST_ESB1..2
6	Optimize Base Engine Bundle (Production)	Each	TEST_BAM
	- My webMethods Server		
	- Optimize Base Engine		
	- Broker for Optimize		
7	Optimize for Infrastructure Module Bundle (Production)	Each	TEST_BAM
	- Optimize for Infrastructure	Each	
8	Optimize for B2B Module Bundle (Production)	Each	TEST_BAM
	- Optimize for Process	Each	
	- Optimize for B2B	Each	
9	wM Reporting - Small Bundle (Production)	Each	TEST_BAM

Koncepcja docelowej konfiguracji fizycznej i logicznej środowiska Platformy Usług Elektronicznych


INSTYTUCJE PAŃSTWOWE
Tunel IPSec
INTERNET
ISP1
ISP2
ISP1
ISP2
RT.A.1
RT.A.2
RT.B.1
RT.B.2
SB.A.1
SB.A.2
SB.B.1
SB.B.2
DB.A
DB.B
DWDM
Trakt 1
Trakt 2
SWS.A.1
SWS.A.2
SWS.B.1
SWS.B.2
SW.A.1
SW.A.2
SW.B.1
SW.B.2
HSM.A.1
HSM.A.2
HSM.B.1
HSM.B.2
LB.A.1
LB.A.2
LB.B.1
LB.B.2
Serwer.A.1
Serwer.A.2
Serwer.B.1
Serwer.B.2
DC- A
DC- B

Rysunek nr 2

1)



Rysunek nr 3

III.Szczegółowy opis przedmiotu zamówienia

Wraz z poniższymi opisywanymi elementami takimi jak serwer, ruter, przełącznik itd. wymagane jest

dostarczenie standardowej szafy RACK 19” o wysokości 42U, w której to będą zamontowane dostarczone komponenty.

1. Rozbudowa mocy obliczeniowej środowiska serwerów aplikacyjno – bazodanowych – (wymagania minimalne)

1.1. System musi być kasetowym systemem serwerowym opartym o:
- 1.1.1. Obudowy serwerowe przeznaczoną do montażu w szafie RACK 19’’, zawierające gniazda rozszerzenia przewidziane do instalacji serwerów kasetowych, modułów sieciowych, zasilaczy oraz wentylatorów.
- 1.1.2. Serwery kasetowe przeznaczone do instalacji w obudowie.
- 1.1.3. Centralny system zarządzania obudowami i serwerami.

1.2. Wymaga się, aby pojedyncza obudowa serwerów kasetowych spełniała następujące wymagania:
- 1.2.1. Zainstalowane w obudowie zasilacze do obsługi minimum dwóch źródeł zasilania AC. Dla każdego źródła musi być zapewniona redundancja zasilaczy.
- 1.2.2. Zainstalowana odpowiednia ilość wentylatorów.
- 1.2.3. Możliwość wymiany „na gorąco” (hot-swap) wentylatorów oraz zasilaczy.
- 1.2.4. Wymagana jest możliwość pracy zasilaczy w trybach N+1, N+N, Grid,
- 1.2.5. Zainstalowane minimum dwa dedykowane moduły sieciowe, każdy moduł umożliwiający dołączenie dowolnego serwera kasetowego co najmniej 4 dedykowanymi wewnętrznymi interfejsami LAN 10GE ze wsparciem dla FCoE (FC over Ethernet). Dołączenie musi być realizowane w ramach obudowy (backplane), w sposób nie wymagający użycia kabli.
- 1.2.6. Łączna przepustowość połączenia obudowy do sieci zewnętrznej LAN lub systemu zarządzania musi wynosić minimum 320 Gbps.

1.3. Wymagane mechanizmy niezawodności, dostępności i łatwości serwisowania dla architektury CPU w dostarczonych serwerach:
- 1.3.1. Dostęp procesora do magistrali pamięciowej poprzez dedykowane bufory z możliwością pracy w trybach o zwiększonej niezawodności lub zwiększonej wydajności,
- 1.3.2. Możliwość obsługi awarii pojedynczego modułu DRAM w ramach bufora przy zachowaniu możliwości korekcji pojedynczych błędów bitowych i bez zakłócenia działania aplikacji/systemu operacyjnego,
- 1.3.3. Możliwość obsługi jednoczesnej awarii dwóch modułów DRAM w ramach bufora przy zachowaniu możliwości korekcji pojedynczych błędów bitowych i bez zakłócenia działania, aplikacji/systemu operacyjnego,
- 1.3.4. Identyfikacja modułów DIMM mogących stwarzać potencjalny problem,
- 1.3.5. Możliwość dodawania/wymiany modułów DRAM “na gorąco” w czasie działania aplikacji/systemu operacyjnego,
- 1.3.6. Możliwość dodawania/wymiany CPU “na gorąco” w czasie działania aplikacji/systemu operacyjnego,
- 1.3.7. Możliwość dodawania/wymiany karty PCIe “na gorąco” w czasie działania aplikacji/systemu operacyjnego,
- 1.3.8. Możliwość migracji zawartości modułu DIMM stwarzającego potencjalny problem do zapasowego modułu DIMM przy zachowaniu spójności z mechanizmem cache i bez zakłócenia działania aplikacji/systemu operacyjnego,
- 1.3.9. Możliwość przekazania lokalizacji błędu który nie mógł być skorygowany na poziomie sprzętowym do warstwy systemu operacyjnego/hypervisora.

1.4. Całość środowiska serwerowego dołączona do przełącznika SAN przynajmniej 4 x 16 GB.

1.5. Serwer kasetowy dla środowiska serwerów bazodanowych- serwer typ A- 4 sztuki. Każdy serwer musi spełniać następujące wymagania:
- 1.5.1. Musi posiadać co najmniej cztery gniazda dla procesorów,
- 1.5.2. Musi posiadać co najmniej 96 gniazd DIMM przeznaczone do instalacji modułów pamięci umożliwiających uzyskanie w maksymalnej konfiguracji 6 TB pamięci,
- 1.5.3. Musi umożliwiać instalację minimum dwóch dysków 2.5-in. SFF SAS lub 15mm SATA lub SSD wymiennych od przodu serwera hot-swap,
- 1.5.4. Musi posiadać zainstalowane minimum dwa konwergentne adaptery sieciowe zapewniające obsługę LAN/SAN (FCoE) poprzez łacznie co najmniej 8 x interfejsów 10GE.
- 1.5.5. Musi umożliwiać instalację następujących systemów operacyjnych znajdujących się na oficjalnej liście kompatybilności sprzętu w wersji nie niższej niż :

1.5.5.1. Microsoft Windows 2008 R2,
1.5.5.2. Microsoft Windows Server 2012 R2,
1.5.5.3. RedHat Enterprise Linux 64 bit,
1.5.5.4. VMWare vSphere 6.0.
1.5.6. Wymaga się dostarczenia czterech serwerów kasetowych typ A wyposażonych minimum w następujące komponenty:
1.5.6.1. 4 procesory, każdy minimum 18 rdzeni, umożliwiające osiągnięcie w teście SPECint_rate_base2006 wyniku na poziomie min. 2700 pkt. (dla dowolnego producenta serwera czteroprocesorowego),
1.5.6.2. 256 GB pamięci DRAM,
1.5.6.3. 2 x dyski HDD 2.5'' 300GB SAS 12G.
1.6. Serwer kasetowy dla środowiska serwerów aplikacyjnych - serwer typ B- 10 sztuk, Każdy serwer musi spełniać następujące wymagania:
1.6.1. Musi posiadać co najmniej cztery gniazda dla procesorów,
1.6.2. Musi posiadać co najmniej 96 gniazd DIMM przeznaczone do instalacji modułów pamięci umożliwiających uzyskanie w maksymalnej konfiguracji 6 TB pamięci,
1.6.3. Musi umożliwiać instalację minimum dwóch dysków 2.5-in. SFF SAS lub 15mm SATA lub SSD wymiennych od przodu serwera hot-swap,
1.6.4. Musi posiadać zainstalowane minimum dwa konwergentne adaptery sieciowe zapewniające obsługę LAN/SAN poprzez łącznie co najmniej 8 x interfejsów 10GE.
1.6.5. Musi umożliwiać instalację następujących systemów operacyjnych znajdujących się na oficjalnej liście kompatybilności sprzętu w wersji nie niższej niż :
1.6.5.1. Microsoft Windows 2008 R2,
1.6.5.2. Microsoft Windows Server 2012 R2,
1.6.5.3. RedHat Enterprise Linux 64 bit,
1.6.5.4. VMWare vSphere 6.0.
1.6.6. Wymaga się dostarczenia dziesięć serwerów kasetowych typ B wyposażonych minimum w następujące komponenty:
1.6.6.1. 4 procesory, każdy minimum 15 rdzeni, umożliwiające osiągnięcie w teście SPECint_rate_base2006 wyniku na poziomie min. 2300 pkt. (dla dowolnego producenta serwera czteroprocesorowego),
1.6.6.2. 512 GB pamięci DRAM,
1.6.6.3. 2 x dyski HDD 2.5'' 300GB SAS 12G.
1.7. System zarządzania serwerami kasetowymi.
1.7.1. Centralny system zarządzania wszystkimi serwerami kasetowymi musi składać się z redundantnych (podwojonych) komponentów.
1.7.2. Centralny redundantny system zarządzania serwerami musi zapewnić centralne zarządzanie wszystkimi obudowami i serwerami kasetowymi.
1.7.3. Centralny redundantny system zarządzania serwerami kasetowymi musi realizować następujące funkcjonalności:
1.7.3.1. Musi umożliwiać aktualizację firmware na serwerach stelażowych i kasetowych w następującym zakresie:
1.7.3.1.1. BIOS,
1.7.3.1.2. RAID,
1.7.3.1.3. KVM/iLO,
1.7.3.1.4. Adaptery sieciowe.
1.7.3.2. Repozytorium dla firmware serwerów kasetowych
1.7.3.3. Aktualizacja oprogramowania serwerów kasetowych musi odbywać się bez przerw w środowiska (z wyjątkiem aktualizowanego serwera).
1.7.3.4. Musi umożliwiać definicję serwera przy pomocy logicznego profilu obejmującego konfigurację serwera w zakresie sieci LAN i SAN. W zakres logicznego profilu serwerowego muszą wchodzić minimum następujące parametry:
1.7.3.4.1. adres MAC,
1.7.3.4.2. adres WWNN/WWPN,
1.7.3.4.3. sekwencja bootowania systemu,
1.7.3.4.4. ustawienia BIOS,
1.7.3.4.5. wersja BIOS/firmware,

1.7.3.4.6. lista sieci VLAN.

1.7.3.5. Musi posiadać funkcje centralnego zarządzanie adresami MAC oraz adresami WWNN/WWPN serwerów.

1.7.3.6. Musi umożliwiać przeniesienie logicznego profilu serwera między dowolną parą serwerów.

1.7.3.7. Musi umożliwiać automatyczne przeniesienie logicznego profilu z uszkodzonego serwera na zdefiniowany wcześniej przez administratora serwer zapasowy.

1.7.3.8. Musi posiadać wsparcie dla następujących mechanizmów komunikacji zewnętrznej: HTTPS, SNMP, IPMI.

1.7.3.9. Musi udostępniać zdalną konsolę KVM dla każdego z serwerów. Konsola musi być wyposażona w maksymalny możliwy zestaw funkcji i licencji przewidziany przez producenta serwerów dla oferowanego rozwiązania. Konsola musi dla każdego serwera umożliwiać minimum:

1.7.3.9.1. Autoryzacja dostępu do konsoli,

1.7.3.9.2. Zdalne włączanie, wyłączanie, restart serwera,

1.7.3.9.3. Montowanie zdalnych napędów dyskietki, CD/DVD, oraz obrazów,

1.7.3.9.4. Przeglądanie logów serwera,

1.7.3.9.5. Weryfikacja sekwencji bootowania.

1.7.3.10. Musi oferować poprzez graficzny (GUI) oraz terminalowy (CLI) interfejs użytkownika następujące funkcjonalności:

1.7.3.10.1. Lista komponentów serwera (inwentarz),

1.7.3.10.2. Wyświetlanie informacji o awariach i zdarzeniach,

1.7.3.10.3. Automatyczne powiadamianie o awarii poprzez email,

1.7.3.10.4. Archiwizacja i odtworzenie konfiguracji,

1.7.3.10.5. Zarządzanie z uwzględnieniem podziału roli użytkowników,

1.7.3.10.6. Integracja ze środowiskiem wirtualizacji serwerów,

1.7.3.10.7. Zarządzanie mocą całego środowiska poprzez podgląd maksymalnej i średniej wykorzystanej przez komponenty mocy,

1.7.3.10.8. Zarządzanie chłodzeniem całego środowiska poprzez podgląd temperatur na poszczególnych komponentach środowiska.

2. Ruter brzegowy – 4 sztuki (wymagania minimalne)

Routery dostarczone do muszą być modularne i charakteryzować się następującymi właściwościami i cechami:

2.1. Na brzegu sieci mają być routery o architekturze rozproszonej (z odseparowanym control i date plane).

2.2. Routery muszą być wyposażone w min. 6 portów przynajmniej 1GE .

2.3. Zarządzanie routerem:

2.3.1. Router musi posiadać port konsolowy do zarządzania urządzeniem,

2.3.2. Port Eth 10/100/1000 Mb/s do zarządzania out of band,

2.3.3. Zarządzanie przez protokół SSHv2 i Telnet.

2.4. Wsparcie dla protokołu NetFlow V9 lub równoważnych.

2.5. Router musi posiadać redundantny system zasilania. Wkładanie lub usuwanie modułów zasilaczy nie może w żaden sposób wpływać na pracę obciążonego routera.

2.6. Pojemność tablicy RIB oraz FIB przynajmniej 1 milion wpisów.

2.7. Pojemność pamięci RAM – minimum 8GB RAM.

2.8. Przepustowość minimum 10Gb/s.

2.9. Wydajność minimum 7 Mpps.

2.10. Wsparcie dla routingu

2.10.1. IPv4: statyczny, RIP, IS-IS, OSFP, BGP

2.10.2. IPv6: statyczny, RIPng, IS-ISv6, OSFPv3, MBGP

2.10.3. Wsparcie dla routingu multicast (PIM SM, SSM)

2.10.4. Wsparcie dla 2000 grup IGMP dla ruchu multicast.

2.11. Urządzenie musi wspierać mechanizmy Anti-DDoS dla BGP, w szczególności zgodny z RFC 5575 klient BGP Flowsepc – „Dissemination of Flow Specification Rules" sterowanie ruchem w celu uniknięcia ataku typu DDoS.

2.12. Wsparcie dla mechanizmów szybkiej zbieżności z wykorzystaniem IP FRR (IP Fast ReRoute) – programowaniem zapasowej ścieżki w tablicy FIB.

2.13. Wsparcie dla funkcjonalności BGP Best External.

2.14. Wsparcie dla 16 ścieżek o tym samym koszcie (ECMP).
2.15. Wsparcie dla funkcjonalności IP Unicast Forwarding Path Check.
2.16. Wsparcie dla protokołu VRRP lub HSRP.
2.17. Wsparcie dla funkcjonalności VRRP lub HSRP Object Tracking.
2.18. Wsparcie dla protokołu BFD z 2000 sesji.
2.19. Wsparcie dla policy routingu.
2.20. Opcjonalne wsparcie dla MPLS, VPWS, VPLS.
2.21. Wsparcie dla protokołu SNMP v1, v2, v3
2.22. Wsparcie dla Syslog.
2.23. Wsparcie dla LLDP lub CDP.
2.24. Wsparcie dla Network Time Protocol (NTP).
2.25. Obsługa protokołu IKE.
2.26. Wsparcie funkcji Secure Hash Algorithm SHA.
2.27. Możliwość tworzenie list dostępowych ACL opartych o adresy źródłowe i docelowe IP, porty źródłowe i docelowe TCP/UDP.
2.28. Skalowalność liczby ACL - 2000 / wpisów do ACL – 20000.
2.29. Wsparcie dla izolacji tablic routingu w ramach VRFów.
2.30. Wsparcie dla standardów IEEE 802.3ah i 802.1.ag wykrywanie problemów na łączu pomiędzy urządzeniami z minimalnym odstępem dla CFM: 100ms.
2.31. Wysokość do 3U.

3. Przełącznik sieciowy – 4 sztuki

Urządzenia rdzeniowe. Switche dostarczone do DC muszą być modularne i charakteryzować się następującymi właściwościami i cechami:

3.1. Urządzenie o architekturze modularnej, pozwalającej na instalację kart liniowych i redundantnych modułów zarządzająco-przełączających, urządzenie musi posiadać nie mniej niż 4 gniazda.
3.2. Urządzenie musi być oparte o w pełni rozdzielną i niezależną od warstwy przesyłania danych warstwę kontrolno-zarządzającą. Moduły kontrolno-zarządzające (Supervisory) nie mogą pośredniczyć w przesyłaniu ramek/pakietów między kartami liniowymi.
3.3. Urządzenie musi w dostarczonej konfiguracji być wyposażone w 96 gniazd SFP+ 1/10 GigabitEthernet umożliwiających instalację wkładek następującego typu: 1000BaseT, 1000BaseSX. 1000BaseLX, 10GE-SR, 10GE-LR. Wszystkie porty 10GE muszą mieć możliwość jednoczesnej pracy w trybie wirespeed (linerate) dla prędkości 10GE.
    3.3.1. Wykonawca musi dostarczyć odpowiedne wkładki SFP/ SFP+ w ilości zgodnej z zaproponowanym rozwiązaniem, zgodnie z zapisem punktu II 8.7.
    3.3.2. Zaleca się przeprowadzenie wizji lokalnej w celu dobrania i skonfigurowania wkładek i kart do DWDM oraz przełącznika, aby zapewnić komunikację za pomocą DWDM dla sieci LAN i SAN w obu ośrodkach COO i ZCOO.
    3.3.3. Resztę wolnych portów należy obsadzić wkładkami według schematu: 35% 10GE-SR, 35% 1000BaseSX, 30% 1000BaseT. Liczbę portów należy obliczyć zaokrąglając w górę zaczynając od wkładki o najwyższym priorytecie 10GE-SR następnie 1000BaseSX i 1000BaseT.
3.4. Wydajność przełączania dla pakietów przynajmniej 600 Mpps dla każdej karty liniowej.
3.5. Wydajność przełączania przynajmniej 400 Gbps dla każdej karty liniowej.
3.6. Wsparcie dla standardów IEEE 802.1Q VLAN encapsulation.
3.7. Funkcjonalności L2 i L3.
    3.7.1. Wsparcie dla protokołów STP: STP 802.1D, RSTP 802.1w, MSTP 802.1s
    3.7.2. Urządzenie musi mieć funkcjonalność łączenia dwóch przełączników fizycznych w jeden przełącznik wirtualny traktowany jako jedno urządzenie logiczne w punktu widzenia protokołów routingu LACP i Spanning Tree
    3.7.3. Dla pracy w warstwie L2 urządzenie musi umożliwiać budowę bez pętlowej topologii sieci w warstwie L2 bez wykorzystania protokołu Spanning Tree.
    3.7.4. Wsparcie dla routingu:
        3.7.4.1. IPv4 (RIPv2, OSPF, BGP),
        3.7.4.2. IPv6 (OSPF, BGP).
    3.7.5. Policy Based Routing dla IPv4 oraz IPv6,
    3.7.6. Wsparcie dla protokołu VRRP lub HSRP,

3.7.7. Wsparcie dla standardów DCB (Data Center Bridging): IEEE 802.1Qbb PFC, IEEE 802.1Qaz ETS, IEEE DCBX,

3.7.8. Wsparcie dla protokołu FCoE (w wypadku gdy funkcjonalność wymaga licencji nie jest konieczne jej dostarczenie),

3.8. Switche w obu DC muszą być połączone za pomocą technologii Data Center Interconnect (DCI) umożliwiającej:

3.8.1. Wykorzystanie dowolnej sieci IP lub połączenia optycznego dla połączenia obu DC,

3.8.2. Wsparcie dla VMWare vMotion,

3.8.3. Rozdzielenie domen STP w obu ośrodkach DC,

3.8.4. Ograniczenie propagacji adresów MAC między ośrodkami DC,

3.8.5. Możliwość obsługi co najmniej 1500 sieci VLAN,

3.8.6. Możliwosć translacji VLAN pomiędzy ośrodkami DC,

3.8.7. Mechanizm eliminacji pętli między ośrodkami DC,

3.9. Urządzenie musi być wyposażone w wirtualizację kontekstową tj. możliwość wydzielenia w nim nie mniej niż ośmiu wirtualnych kontekstów nie licząc standardowego kontekstu globalnego, konteksty muszą być w pełni logicznie odizolowane od siebie i posiadać dedykowane i niezależne zasoby takie jak fizyczne porty, sieci VLAN, tablice routingu, wraz z dedykowaną konfiguracją, administracją i przydziałem zasobów sprzętowych (CPU).

3.9.1. Jeśli funkcjonalność powyższa wymaga dostarczenia dedykowanej licencji to wymaga się jej dostarczenia dla czterech wirtualnych kontekstów nie licząc standardowego kontekstu globalnego

3.10. Bezpieczeństwo:

3.10.1. Możliwość tworzenie list dostępowych ACL opartych o adresy źródłowe i docelowe IP, porty źródłowe i docelowe TCP/UDP,

3.10.2. Urządzenie musi być odporne na ataki typu DoS takie jak SYN Flood attacks, Land attacks, Smurf attacks oraz ICMP Flood attacks,

3.10.3. Port Ethernet 10/100/1000 Base-T do zarządzania urządzeniem w trybie out-of-band,

3.11. Zarządzanie:

3.11.1. Port konsoli szeregowej,

3.11.2. Zarządzanie przez protokół SSHv2 i Telnet,

3.11.3. Wsparcie dla protokołu SNMP v1, v2, v3,

3.11.4. Wsparcie dla Syslog,

3.11.5. Wsparcie dla LLDP lub CDP,

3.12. Wsparcie dla Network Time Protocol (NTP),

3.13. Kopiowanie ruchu i przesyłanie do zdalnego odbiornika poprzez sieć IP,

3.14. Obudowa:

3.14.1. Przełącznik wyposażony w minimum 2 niezależne zasilacze 230 VAC. Wyciągnięcie jednego zasilacza nie może mieć wpływu na prace urządzenia i usług na nim uruchomionych,

3.14.2. Możliwość wymiany kart liniowych, zasilaczy i wentylatorów w trakcie pracy urządzenia bez wpływu na jego działania,

3.14.3. Redundantne wentylatory,

3.14.4. Obudowa wykonana z metalu, przystosowana do montażu w szafie 19''.

3.15. Funkcjonalności opcjonalne:

3.15.1. Możliwość uruchomienia protokołu MPLS i połączenia ośrodków DC poprzez VPLS (w wypadku gdy funkcjonalność wymaga licencji nie jest konieczne jej dostarczenie),

3.15.2. Możliwość uruchomienia szyfrowania ruchu Ethernet między ośrodkami DC z wykorzystaniem IEEE 802.1ae MacSec na przynajmniej 4 interfejsach 1/10 GE łączących ośrodki DC,

3.15.3. Możliwość uruchomienia sprzętowego load balancera dla protokołów IPv4 i IPv6 ze wsparciem dla tworzenia grup serwerów i adresów VIP, próbkowania serwerów, wyboru ruchu na podstawie protokołu/portu L4 i poprzez filtra ACL

3.15.4. Możliwość dołączania wyniesionych satelitarnych modułów liniowych, bez wykorzystania mechanizmów L2/L3

3.15.5. Wsparcie dla VXLAN i protokołu IETF BGP-EVPN

3.15.6. Interfejs REST API w oparciu o JSON/XML

4. Przełącznik do zarządzania urządzeniami MGMT – 2 sztuki

Urządzenie dedykowane dla strefy zarządzania infrastrukturą(VLAN_MGMT).

4.1. Urządzenie musi posiadać przynajmniej 24 porty Ethernet 10/100/1000 Base-T
4.2. Switch musi oferować przynajmniej routing statyczny.
4.3. Wsparcie dla routingu IPv4 i IPv6.
4.4. Możliwość tworzenie list dostępowych ACL opartych o adresy źródłowe i docelowe IP, porty źródłowe i docelowe TCP/UDP.
4.5. Zarządzanie:
  4.5.1. Port konsoli szeregowej,
  4.5.2. Wsparcie dla protokołu SNMP v1, v2, v3,
  4.5.3. Wsparcie dla Syslog,
  4.5.4. Wsparcie dla LLDP lub CDP,
  4.5.5. Zarządzanie przez protokół SSHv2 i Telnet,
4.6. Wsparcie dla Network Time Protocol (NTP),
4.7. Przełącznik wyposażony w minimum 2 niezależne zasilacze 230 VAC. Wyciągnięcie jednego zasilacza nie może mieć wpływu na pracę urządzenia i usług na nim uruchomionych.

5. Urządzenie balansujące ruch sieciowy – 4 sztuki

Urządzenia przeznaczone do balansowania ruchu w sieci. Ruch sieciowy ma być inteligentnie balansowany pomiędzy wyznaczone pule serwerów.

5.1. System musi realizować co najmniej następujące funkcje:
  5.1.1. Rozkład ruchu pomiędzy serwerami aplikacji Web,
  5.1.2. Selektywny http caching,
  5.1.3. Selektywna kompresja danych,
  5.1.4. Terminowanie sesji SSL,
  5.1.5. Filtrowanie pakietów,
  5.1.6. Optymalizacja i akceleracja aplikacji,
  5.1.7. Globalnego równoważenia obciążenia za pomocą protokołu DNS,
  5.1.8. Ochrona przed atakami na aplikacje internetowe i serwery WWW (Web Application Firewall).
5.2. Wszystkie wymienione w niniejszym dokumencie funkcje muszą być dostępne w obrębie jednego urządzenia.
5.3. Klucze prywatne zapisane na dysku urządzenia muszą być zaszyfrowane. Nie dopuszcza się rozwiązań przechowujących klucze prywatne w formie jawnej.
5.4. System musi posiadać co najmniej następujące metody równoważenia obciążenia:
  5.4.1. Cykliczna,
  5.4.2. Ważona,
  5.4.3. Najmniejsza liczba połączeń,
  5.4.4. Najszybsza odpowiedź serwera,
  5.4.5. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera,
  5.4.6. Najmniejsza liczba połączeń i najszybsza odpowiedź serwera w zdefiniowanym czasie,
  5.4.7. Dynamicznie ważona oparta na SNMP/WMI,
  5.4.8. Definiowana na podstawie grupy priorytetów dla serwerów.
5.5. Rozwiązanie musi posiadać wbudowany w system operacyjny język skryptowy, posiadający co najmniej następujące cechy:
  5.5.1. Analiza, zmiana oraz zastępowanie parametrów w nagłówku http oraz w zawartości pakietów,
  5.5.2. Obsługa protokołów: http, tcp, xml, rtsp, sip,
  5.5.3. Musi posiadać funkcję inspekcji protokołów LDAP oraz RADIUS.
5.6. Język skryptowy musi bazować na języku programowania Tool Command Language lub równoważnym, z własnymi komendami.
5.7. Musi istnieć możliwość modyfikacji metod równoważenia obciążenia pomiędzy serwerami przy wykorzystaniu wbudowanego języka skryptowego.
5.8. Producent systemu musi dostarczyć darmową, specjalizowaną aplikację do analizy poprawności składni skryptów pisanych przy wykorzystaniu języka skryptowego opisanego w punkcie 5.6. Aplikacja musi posiadać wbudowane szablony skryptów oraz funkcję automatycznego uzupełniania wpisywanych komend.
5.9. Rozwiązanie musi pracować w trybie pełnego proxy.

5.10. Rozwiązanie musi posiadać programowalny interfejs API do integracji z zewnętrznymi systemami oraz automatyzacji wykonywania operacji.
5.11. Funkcjonalność lokalnego równoważenia obciążenia:
  5.11.1. Wspierane mechanizmy równoważenia obciążenia: round robin, ważona, dynamicznie ważona (na podstawie SNMP/WMI), najmniejsza liczba połączeń, najszybsza odpowiedź, observer, predictive, grupy priorytetów, możliwość modyfikacji za pomocą języka skryptowego,
  5.11.2. Buforowanie połączeń TCP w przypadku osiągnięcia zadanej ilości sesji dla danego serwera,
  5.11.3. Obsługiwane mechanizmy monitorowania stanu serwerów: ICMP, TCP, TCP half-open, UDP, SSL, http/https, LDAP, zapytania do baz MS SQL i Oracle, FTP, SIP, SMB/CIFS, Radius, SIP, POP3, IMAP, SMTP, SNMP, SOAP, skryptowy, sprawdzanie odpowiedzi w oparciu o wyrażenia regularne,
  5.11.4. Obsługiwane mechanizmy przywiązywania sesji: cookie (hash, rewrite, custom, insert,passive), adres źródłowy, adres docelowy, SSL ID, RDP login name, JSESSIONID, SIP call ID,
  5.11.5. Wsparcie dla usług warstw 4-7: inspekcja warstwy 7, wstrzykiwanie nagłówków http, ukrywanie zasobów, zmiana odpowiedzi serwera, zaszyfrowane cookies, przepisywanie odpowiedzi, ochrona przed atakami DoS/DDoS i SYN Flood, multipleksacja zapytań HTTP, kompresja i cache'owanie http.
5.12. Optymalizacja i akceleracja aplikacji:
  5.12.1. Urządzenie musi optymalizować protokół TCP i posiadać predefiniowane profile dla następujących charakterystyk sieci:
    5.12.1.1. LAN,
    5.12.1.2. WAN,
    5.12.1.3. CELL (komórkowy),
  5.12.2. Urządzenie powinno implementować TCP proxy z mechanizmem zamykania okna w stronę serwera www w przypadku zbyt wolnego odbierania danych przez zdalnego klienta.
  5.12.3. Urządzenie musi posiadać cache i musi umożliwiać definiowania list URI w celu:
    5.12.3.1. Trwałego przetrzymywania obiektów w cache,
    5.12.3.2. Cachowania obiektów,
    5.12.3.3. Zapobieżenia cachowania obiektów.
  5.12.4. Urządzenie musi mieć możliwość włączenia ignorowania nagłówków przeglądarki dotyczących cachowania (Cache-control),
  5.12.5. Urządzenie musi wspierać multipleksacje wielu zapytań http w tej samej sesji TCP,
  5.12.6. Urządzenie musi umożliwiać kompresję zwracanej zawartości http. Użycie kompresji powinno być zależne od:
    5.12.6.1. Listy dozwolonych URI,
    5.12.6.2. Listy wykluczonych URI,
    5.12.6.3. Listy kompresowalnych Content-Type,
    5.12.6.4. Listy wykluczonych Content-Type.
5.13. Rozwiązanie musi zapewniać globalne, inteligentne sterowanie ruchem wykorzystując usługę DNS jako mechanizm rozdziału ruchu (Global Solution Load Balancing), w ramach którego zapewni:
  5.13.1. Monitorowanie stanu pracy usług korzystając z monitorów działających w warstwie sieci, transportowej oraz aplikacji modelu ISO/OSI,
  5.13.2. Rozdzielanie ruchu korzystając co najmniej z metod:
    5.13.2.1. Cykliczna,
    5.13.2.2. Ważona,
    5.13.2.3. Na podstawie adresów IP klienta usługi (topologii),
    5.13.2.4. Obciążenia serwera,
    5.13.2.5. Najmniejszej liczby połączeń,
  5.13.3. Mechanizmy utrzymywania sesji polegające na kierowaniu zapytań z lokalnego serwera dns klienta aplikacji zawsze do tego samego centrum danych i serwera aplikacji,
  5.13.4. Wbudowany w system operacyjny język skryptowy, umożliwiający analizę i zmianę parametrów w protokole DNS,
  5.13.5. Ochronę serwerów DNS z wykorzystanie DNSSEC a także na zastosowaniu list kontroli dostępu umożliwiających filtrowanie ruchu DNS bazując na typie rekordu,
  5.13.6. Możliwość pracy, jako serwer DNS obsługujący następujące rekordy: A, AAAA, A6, CNAME, DNAME, HINFO, KEY, MX, NS, NXT, PTR, SIG, SOA, SRV,
  5.13.7. Konwersja rekordów między IPv4 i IPv6,

5.13.8. Wsparcie dla usług geolokacji, możliwość przekierowania ruchu do najbliższej geograficznie lokalizacji,
5.13.9. Wybór lokalizacji na podstawie ilości urządzeń pośredniczących oraz ilości przetwarzanych danych,
5.13.10. Możliwość wysyłania zapytań dotyczących obciążenia do urządzeń firm trzecich,
5.13.11. Możliwość bezpośredniego odpytywania serwerów o obciążenie,
5.13.12. Możliwość przekierowania ruchu do innej lokalizacji po przekroczeniu zdefiniowanego progu ilości sesji.

5.14. Ochrona przed atakami na aplikacje internetowe i serwery WWW (WAF) musi zapewniać co najmniej następujące własności:
5.14.1. Weryfikacja zarówno zapytań jak i odpowiedzi http pod względem naruszeń, w przypadku wykrycia incydentu musi istnieć możliwość aktywnego blokowania ruchu,
5.14.2. Filtrowanie odpowiedzi serwera i kodów błędu, ukrycie zasobów serwera,
5.14.3. WAF musi działać w oparciu o pozytywny model bezpieczeństwa (tylko to, co znane i prawidłowe jest dozwolone), model ten tworzony jest na bazie automatycznie budowanego przez WAF profilu aplikacji Web (URLi, metod dostępu, typów plików, cookie, oczekiwanych typów znaków oraz długości zapytań),
5.14.4. Profil aplikacji web tworzony musi być na podstawie analizy ruchu sieciowego. Musi istnieć możliwość ograniczania zaufanych adresów źródłowych, z których komunikacja z aplikacją tworzyć będzie oczekiwany profil zachowania użytkowników.
5.14.5. Możliwość definiowania przepływu ruchu w obrębie aplikacji z uwzględnieniem jej logiki biznesowej,
5.14.6. Oprócz pozytywnego modelu zabezpieczeń WAF musi posiadać również funkcje identyfikacji incydentów poprzez sygnatury (negatywny model zabezpieczeń),
5.14.7. Musi istnieć możliwość selektywnego włączania/wyłączania sygnatur per parametr,
5.14.8. Musi istnieć możliwość ręcznego konfigurowania/modyfikacji reguł polityki dostępu,
5.14.9. Musi istnieć możliwość ochrony dynamicznych oraz ukrytych parametrów,
5.14.10. WAF musi posiadać funkcje analizy i odczytu CSS/XSS,
5.14.11. WAF musi posiadać możliwość walidacji XML poprzez: walidację Schema/WSDL, wybór dozwolonych metod SOAP, opis ataków na XML, rejestrację zapytań XML,
5.14.12. WAF musi posiadać mechanizmy ochrony przed atakami: SQL Injection, Cross-Site Scripting, Cross-Site Request Forgery, Session hijacking, Command Injection, Cookie/Session Poisoning, Parameter/Form Tampering, Forceful Browsing, Brute Force Login,
5.14.13. WAF musi posiadać mechanizmy ochrony przed atakami DoS ukierunkowanymi na warstwę aplikacyjną (zalewanie aplikacji web dużą ilością zapytań http),
5.14.14. WAF musi rozróżniać rzeczywistych użytkowników od automatów podczas ataku (D)DoS poprzez:
5.14.14.1. Wstrzykiwanie skryptu w przypadku wystąpienia podejrzenia ataku - w przypadku wykrycia naruszenia polityki urządzenie powinno umożliwiać zdefiniowanie odpowiedzi wysyłanej do użytkownika,
5.14.14.2. Wykorzystanie CAPTCHA.
5.14.15. Powinna istnieć możliwość doboru odpowiedzi w zależności do rodzaju naruszenia.
5.14.16. WAF musi posiadać możliwość uwzględniania w logach dotyczących incydentów informacji o uwierzytelnionym użytkowniku oraz blokowania dużej ilości incydentów wykonywanych w zdefiniowanym czasie przez jednego użytkownika.
5.14.17. W obrębie licencji WAF dostarczony musi być moduł ochrony protokołu HTTP, SMTP oraz FTP.
5.14.18. WAF musi posiadać wsparcie dla aplikacji AJAX oraz JSON.
5.14.19. WAF musi umożliwiać automatyczne budowanie polityk w oparciu o skanowanie przez zewnętrznych dostawców np. Cenzic, HP WebInspect, IBM AppScan, Qualys Guard, WhiteHat Sentinel.
5.14.20. WAF musi posiadać mechanizmy normalizacji w celu obrony przed technikami ukrywania ataku.
5.14.21. Urządzenie MUSI wspierać następujące tryby pracy:
5.14.21.1. Tryb wykrywania, logowania i blokowania ataków,
5.14.21.2. Tryb wykrywania i logowania ataków bez blokowania,
5.14.21.3. Tryb uczenia się bez blokowania,

5.14.21.4. Tryb bez wykrywania i blokowania ataków.

5.15. Rozwiązanie musi zapewniać funkcjonalność stanowej zapory sieciowej umożliwiającej kontrolę ruchu sieciowego oraz ochronę przed atakami typu DoS w warstwie 3 i 4 ISO/OSI.

5.16. System musi zapewniać ochronę DoS/DDoS przynajmniej dla protokołów HTTP/HTTPS, SIP, DNS.

5.17. Zarządzanie regułami bezpieczeństwa musi być realizowane za pomocą wbudowanego w system interfejsu graficznego.

5.18. Rozwiązanie musi chronić przed atakami typu flood, sweep, teardrop oraz smurf.

5.19. Rozwiązanie musi obsłużyć sprzętowo minimum 40 milionów SYN cookies na sekundę.

5.20. System musi posiadać co najmniej następujące interfejsy administracyjne:

5.20.1. GUI przy wykorzystaniu protokołu https,

5.20.2. Zarządzanie poprzez SSH,

5.20.3. Zarządzanie poprzez SOAP-SSL,

5.20.4. Zarządzanie poprzez API REST,

5.21. Autoryzacja administratorów systemu .musi bazować na rolach użytkowników.

5.22. System musi posiadać funkcje przywiązywania sesji (Session persistence) przy wykorzystaniu co najmniej następujących atrybutów:Cookie (hash, rewrite, custom, insert, passive).

5.22.1. Adres źródła,

5.22.2. SIP call ID,

5.22.3. Identyfikator sesji SSL,

5.22.4. Microsoft Terminal Services (RDP) – nazwa użytkownika,

5.22.5. Adres docelowy,

5.22.6. Tworzone przez administratora systemu przy wykorzystaniu języka skryptowego z punktu 5.5.

5.23. System musi posiadać funkcję sprawdzania dostępności usług (ang. health monitoring) przy wykorzystaniu co najmniej następujących metod: icmp, echo (port 7/TCP), zapytanie MS SQL, zapytanie Oracle, sprawdzanie odpowiedzi poprzez wyszukiwanie wyrażeń regularnych, TCP half-open, wykorzystanie protokołów: http, https, ftp, sip, nntp, smb, pop3, imap, smtp, ssl, radius. Dodatkowo musi istnieć możliwość wykorzystania skryptów do tworzenia złożonych monitorów sprawdzających aktywność usług.

5.24. System musi posiadać funkcję definiowania maksymalnej ilości obsługiwanych przez dany serwer połączeń, w przypadku przekroczenia zdefiniowanej wartości musi istnieć możliwość wysłania klientowi strony błędu lub przekierowania klienta na inny serwer.

5.25. System musi obsługiwać sieci VLAN w standardzie 802.1q.

5.26. System musi obsługiwać agregację linków w standardzie 802.3ad (LACP).

5.27. System musi świadczyć, co najmniej następujące usługi w warstwach 4-7:

5.27.1. Inspekcja warstwy aplikacji, w tym inspekcja nagłówka http,

5.27.2. Ukrywanie zasobów,

5.27.3. Zmiana odpowiedzi serwera,

5.27.4. Przepisywanie odpowiedzi (response rewriting),

5.27.5. Ochrona przed atakami typu DoS/DDoS,

5.27.6. Ochrona przed atakami typu SYN Flood,

5.27.7. Multipleksowanie połączeń http.

5.28. System musi posiadać następujące funkcje zarządzania siecią:

5.28.1. Obsługa protokołu SNMP v1, v2, v3,

5.28.2. Zewnętrzny syslog,

5.28.3. Zbieranie danych i ich wyświetlanie,

5.28.4. Zbieranie danych zgodnie z ustawieniami administratora,

5.28.5. Osobna brama domyślna dla interfejsu zarządzającego,

5.28.6. Wsparcie dla przynajmniej 2 wersji oprogramowania (multi-boot),

5.28.7. Zapisywanie konfiguracji (możliwość szyfrowania i eksportu kluczy),

5.28.8. Dedykowany podsystem monitorowania stanu pracy urządzenia (always on management) z funkcjami restartu, wstrzymania oraz sprzętowego resetu systemu.

5.29. System musi posiadać funkcję integracji z zewnętrznymi serwerami uwierzytelnienia użytkowników LDAP, RADIUS, TACACS.

5.30. System musi posiadać funkcję definiowania i edycji szablonów konfiguracji aplikacji. Szablony powinny służyć do optymalizacji procesu wdrażania systemu zarówno dla znanych aplikacji biznesowych, jak i własnych aplikacji klienta. W ramach opisanych szablonów musi istnieć możliwość

automatycznej kontroli poszczególnych elementów konfiguracji szablonu i zabezpieczenie ich przed modyfikacją i usunięciem.

5.31. System musi posiadać moduł analizy ruchu http. Moduł powinien zbierać następujące metryki:
- 5.31.1. Czas odpowiedzi per serwer,
- 5.31.2. Czas odpowiedzi per URI,
- 5.31.3. Ilość sesji użytkownika,
- 5.31.4. Przepustowość,
- 5.31.5. Adres źródła,
- 5.31.6. Kraj,
- 5.31.7. User Agent (wykorzystywana przez klienta aplikacja),
- 5.31.8. Metoda dostępu.

5.32. System musi posiadać funkcję walidacji certyfikatów klientów łączących się przy wykorzystaniu protokołu SSL.

5.33. Musi być dostarczony w formie klastra wysokiej dostępności (HA) złożonego z dwóch urządzeń tego samego typu pracujących w trybie active – standby z możliwością realizacji trybu active-active oraz rozbudowy do klastra N+1.

5.34. W ramach klastra musi istnieć możliwość jednoczesnego wykorzystania różnych modeli urządzeń sprzętowych oraz maszyn wirtualnych.

5.35. Klaster wysokiej dostępności musi zapewniać kopiowanie informacji o sesji SSL pomiędzy urządzeniami, aby uniknąć ponownej negocjacji po przełączeniu ruchu.

5.36. Klaster wysokiej dostępności musi zapewniać synchronizację:
- 5.36.1. Konfiguracji,
- 5.36.2. Stanu połączeń,
- 5.36.3. Przywiązywania sesji (Session persistence),

5.37. Wykrycie awarii urządzeń w klastrze odbywać się musi przy użyciu, co najmniej następujących metod:
- 5.37.1. Weryfikacja stanu pracy urządzenia poprzez analizę aktywności w sieci (Network failover),
- 5.37.2. Weryfikacji stanu pracy urządzenia poprzez interfejs szeregowy (serial failover).

5.38. Wymagana jest 3 letnia gwarancja producenta. W obrębie gwarancji zawarte musi być:
- 5.38.1. Dostęp do aktualnych wersji oprogramowania oraz dokumentacji producenta,
- 5.38.2. Sposób obsługi zgłoszeń gwarancyjnych w trybie 24x7,
- 5.38.3. Wymiana sprzętu następnego dnia roboczego po identyfikacji usterki.

5.39. System którego funkcjonalności zostały opisane powyżej musi spełniać wymogi techniczne opisane poniżej dla jednego urządzenia sieciowego:
- 5.39.1. Pamięć nie mniej niż 32GB,
- 5.39.2. Dwa dyski twarde o pojemności nie mniejszej niż 400 GB,
- 5.39.3. Przepływność:
  - 5.39.3.1. dla warstwy 4: nie mniej niż 39,5 Gbps,
  - 5.39.3.2. dla warstwy 7 nie mniej niż 19,5 Gbps,
- 5.39.4. Przepustowość wewnętrznej magistrali nie mniej niż 320 Gbps,
- 5.39.5. Ilość jednocześnie obsługiwanych połączeń nie mniej niż 24 miliony,
- 5.39.6. Ilość transakcji SSL na sekundę dla klucza o długości 2048 nie mniej niż 24 tysiące,
- 5.39.7. Ilość jednocześnie obsługiwanych połączeń SSL nie mniej niż 4 miliony,
- 5.39.8. Przepływność ruchu szyfrowanego nie mniej niż 18 Gbps,
- 5.39.9. Ilość jednoczesnych połączeń na sekundę w warstwie 4 nie mniej niż 770 tysięcy,
- 5.39.10. Kompresja sprzętowa nie mniej niż 18 Gbps,
- 5.39.11. Sprzętowa ochrona DDoS nie mniej niż 40 milionów SYN cookies na sekundę,
- 5.39.12. Nie mniej niż cztery interfejsy 10/100/1000 Base-T, nie mniej niż osiem interfejsów z możliwością obsadzenia wkładkami SFP+, oddzielny interfejs zarządzania, port konsolowy, interfejs szeregowy failover, dwa porty USB. Należy zapewnić przynajmniej 2 wkładki 10 Gigabit Ethernet SFP+ SR,
- 5.39.13. Urządzenie musi mieć panel i wyświetlacz LCD z funkcjami:
  - 5.39.13.1. ustawienia adresu IP na potrzeby zarządzania,
  - 5.39.13.2. ustawienia parametrów portu szeregowego,
  - 5.39.13.3. wyświetlania informacji o systemie
  - 5.39.13.4. wyświetlania podstawowych alarmów,
  - 5.39.13.5. możliwości restartu urządzenia,
- 5.39.14. Obudowa urządzenia:

5.39.14.1. przeznaczona do montażu w szafie rack 19”,
5.39.14.2. wysokość nie większa niż 2U,
5.39.14.3. Nie mniej niż dwa redundantne zasilacze zasilane prądem zmiennym 230V AC.
5.39.15. Urządzenia o kompatybilności elektromagnetycznej o parametrach co najmniej równoważnych z poniższymi normami:
5.39.15.1. EN 300 386 V1.5.1 (2010-10),
5.39.15.2. EN 55022:2010,
5.39.15.3. EN 61000-3-2:2006+A1:2009+A2:2009,
5.39.15.4. EN 61000-3-3:2008,
5.39.15.5. EN 55024:2010.

6. System bezpieczeństwa

6.1. Założenia dla systemu bezpieczeństwa
6.1.1. Jednym z celów modernizacji PUE jest między innymi poprawa bezpieczeństwa przetwarzanych danych i dlatego zaproponowany system bezpieczeństwa powinien obejmować szereg narzędzi w tym co najmniej:
6.1.1.1. System firewalli zewnętrznych (FW-OUT) chroniący PUE przed atakami z sieci Internet,
6.1.1.2. System firewalli wewnętrznych (FW-IN) chroniący PUE przed niepożądanym dostępem z sieci wewnętrznej,
6.1.1.3. System IPS – realizowany jako element funkcjonalności firewalla lub jako zewnętrzne, dedykowane rozwiązanie,
6.1.1.4. Sieciowy system antywirusowy/antymalware – pozwalający na wykrywanie wrogiego kodu – jako element funkcjonalności firewalla lub jako zewnętrzne, dedykowane rozwiązanie.
6.1.2. Dodatkowo dla rozwiązań IPS wymaga się zastosowania urządzeń (rodzin urządzeń) posiadających udokumentowaną, potwierdzoną niezależnymi testami skuteczność wykrywania ataków na poziomie nie gorszym niż 99% - przy czym powyższy wynik należy udokumentować raportem z przeprowadzenia testu przez niezależną od producenta instytucję specjalizującą się w dziedzinie dostarczania rozwiązań ochrony systemów komputerowych.
6.1.3. Zastosowane w projekcie platformy muszą zapewniać także odpowiednio wysoki poziom wydajności. Wszystkie funkcjonalności powinny być osiągnięte przy zastosowaniu specjalnie zaprojektowanego oprogramowania jak i dedykowanych rozwiązań sprzętowych.
6.1.4. Główną istotą systemu bezpieczeństwa jest maksymalne uproszczenie rozwiązania co oznacza, że oczekuje się ograniczenia liczby dostawców, standaryzacji urządzeń oraz integracji poszczególnych funkcjonalności.
6.1.5. Poprzez ograniczenie liczby dostawców rozumie się taką konstrukcję systemu, która pozwoli na zmniejszenie ilości potencjalnych styków pomiędzy rozwiązaniami poszczególnych producentów. Zamierzeniem tego jest chęć uniknięcia dodatkowych kosztów związanych z koniecznością korzystania z wielu systemów zarządzania, korelacją informacji pomiędzy nimi jak też kosztów związanych koniecznością izolowania i usuwania problemów na stykach pomiędzy rozwiązaniami.
6.1.6. Dla wszystkich urządzeń należy przewidzieć serwis i niezbędne subskrypcje na okres 3 lat.
6.2. Ochrona styku PUE z internetem, Ochrona styku z siecią wewnętrzną - Firewall następnej generacji, IPS, System ochrony AntiMalware.
6.2.1. Celem zamawiającego jest zbudowanie redundantnego systemu ochrony styku systemu PUE z internetem poprzez zastosowanie firewalla następnej generacji. Intencją Zamawiającego jest uzyskanie maksymalnie wysokiego poziomu bezpieczeństwa poprzez zastosowanie komponentów Firewall, IPS oraz AntiMalware. Zamawiający zakłada uruchomienie 4 urządzeń pracujących w klastrze – po 2 urządzenia dla każdej z lokalizacji. Urządzenia w klastrze powinny funkcjonować jako jeden logiczny firewall. System powinien być rozbudowywalny do 8 firewalli pracujących w jednym klastrze. Alternatywnie Zamawiający dopusza zastosowanie rozwiązań dwukrotnie bardziej wydajnych jeżeli w klastrze mogą docelowo pracować 4 urządzenia lub 4-krotnie wydajniejszych urządzeń w przypadku jeżeli pracowałyby one w modelu failover Active/Active.

6.2.2. Ochrona styku z siecią wewnętrzną realizowana będzie przez parę firewalii, przy czym wymagania dotyczące ich rozbudowy pozostają jednakowe dla wszystkich urządzeń zastosowanych w projekcie.

6.2.3. Poniżej opisane wymagania dotyczą pojedynczego urządzenia o ile może ono pracować w klastrze złożonym z 4 urządzeń. W przypadku zastosowania rozwiązania alternatywnego w trybie redundancji 1:1 należy przyjąć czterokrotnie wyższe parametry wydajnościowe dla firewalla sieciowego/NGFW/IPS/VPN (wymagania te przekładają się też na ewentualne dedykowane dodatkowe urządzenia realizujące wymagane funkcjonalności – jak jest to opisane w punkcie ”Dopuszczalne sposoby realizacji rozwiązania”.

6.3. Architektura urządzenia:

6.3.1. Urządzenie musi być dedykowaną platformą sprzętową. Nie dopuszcza się rozwiązań „serwerowych” bazujących na ogólnodostępnych na rynku podzespołach PC ogólnego przeznaczenia.

6.3.2. Urządzenie o konstrukcji modularnej pełniące funkcje ściany ogniowej (firewall) typu Statefull inspection i Application Inspection.

6.3.3. Urządzenie wyposażone w co najmniej:

6.3.3.1. 8 (osiem) interfejsów Gigabit Ethernet 10/100/1000 (RJ45),

6.3.3.2. 4 (cztery) interfejsy 10Gigabit Ethernet definiowane przez SFP+,

6.3.3.3. min dwa dedykowane interfejsy Gigabit Ethernet 10/100/1000 (RJ45) do zarządzania.

6.3.4. Urządzenie obsługuje interfejsy VLAN-IEEE 802.1q na interfejsach fizycznych, nie mniej niż 1000 sumarycznie,

6.3.5. Urządzenie wyposażone w moduł sprzętowego wsparcia szyfrowania 3DES i AES oraz licencje na szyfrowanie 3DES/AES,

6.3.6. Urządzenie posiada dedykowany dla zarządzania port konsoli,

6.3.7. Urządzenie musi być wyposażone w pamięć Flash oraz pamięć RAM dostosowaną do wymagań wydajnościowych Zamawiającego. Tym samym Zamawiający oczekuje od oferenta takiego doboru tych komponentów – zgodnie z zaleceniami producenta oferowanego rozwiązania – by spełnić wymagania Zamawiającego. W przypadku jeżeli dobrane komponenty okazałyby się niewystarczające Zamawiający będzie rościł prawo do ich uzupełnienia (bezkosztowo) w czasie obowiązywania serwisu.

6.4. Zasilanie urządzenia:

6.4.1. Urządzenie musi posiadać redundantne zasilacze umożliwiające zasilanie prądem przemiennym 230V (niedopuszczalne rozwiązania zewnętrzne)

6.5. Obudowa:

6.5.1. Urządzenie musi mieć metalową obudowę,

6.5.2. Urządzenie ma możliwość instalacji w szafie typu rack 19”,

6.5.3. Urządzenie musi być dostarczone z elementami montażowymi dla szafy rack 19”,

6.5.4. Urządzenie musi być przystosowane do pracy w zakresie temperatur 0-40 stopni Celsjusza.

6.6. Wydajność urządzenia:

6.6.1. Urządzenie musi zapewniać rzeczywistą przepustowość inspekcji dla ruchu sieciowego IP (inspekcja stanowa w warstwie 3/4 modelu OSI) nie mniej niż 4 Gb/s,

6.6.2. Urządzenie musi obsługiwać w warstwie sieciowej co najmniej 1.000.000 jednoczesnych sesji/połączeń z prędkością zestawiania 50 000 połączeń na sekundę,

6.6.3. Urządzenie musi być wyposażone w sprzętowy układ odciążający procesor urządzenia przy wykonywaniu operacji szyfrowania algorytmami DES/3DES/AES i oferować wydajność szyfrowania nie mniejszą niż 250Mbps,

6.6.4. Urządzenie musi umożliwiać równoczesną obsługę co najmniej 100 tuneli VPN wykorzystujących IPsec. Urządzenie musi umożliwiać rozbudowę o obsługę ruchu SSL VPN przy czym Zamawiający nie wymaga uwzględnienia w ofercie licencji dla tego celu,

6.6.5. Urządzenie musi zapewniać wydajność systemu z funkcjonalnością wykrywania aplikacji co najmniej 4 Gbps –odpowiednio do wydajności firewalla sieciowego,

6.6.6. Urządzenie musi zapewniać wydajność systemu IPS z przepustowością co najmniej 4Gbps przy jednoczesnym działaniu systemu klasyfikacji i rozpoznawania aplikacji (SKRA)–odpowiednio do wydajności firewalla sieciowego.

6.7. Funkcjonalność urządzenia:

6.7.1. Urządzenie musi działać pod kontrolą dedykowanego systemu operacyjnego. Nie dopuszcza się stosowania systemów operacyjnych ogólnego przeznaczenia,

6.7.2. Urządzenie pełni funkcję ściany ogniowej śledzącej stan połączeń (tzw. stateful inspection) z funkcją weryfikacji informacji charakterystycznych dla warstwy aplikacji

6.7.3. Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory,

6.7.4. Urządzenie musi posiadać możliwość uwierzytelnienia z wykorzystaniem LDAP, NTLM oraz Kerberos,

6.7.5. Urządzenie nie może posiadać ograniczenia na ilość jednocześnie pracujących użytkowników w sieci chronionej,

6.7.6. Urządzenie musi umożliwiać realizację funkcji koncentratora VPN umożliwiającego zestawianie połączeń IPSec VPN (zarówno site-to-site, jak i remote access),

6.7.7. Urządzenie musi obsługiwać protokoły IKEv1 i IKEv2,

6.7.8. Urządzenie musi obsługiwać funkcję skrótu SHA-2 o długości 256, 384 i 512 bitów,

6.7.9. Urządzenie musi obsługiwać szyfrowanie protokołem AES z kluczem 128, 192 i 256 bitów w trybie pracy Galois/Counter Mode(GCM) i Galois Message Authentication Code (GMAC),

6.7.10. Urządzenie musi obsługiwać protokół Diffiego-Hellmana w przestrzeni krzywych eliptycznych (ECDH)

6.7.11. Urządzenie musi obsługiwać protokół DSA w przestrzeni krzywych eliptycznych (ECDSA),

6.7.12. Urządzenie musi wspierać RADIUS CoA (RFC3576 i późniejsze),

6.7.13. Urządzenie posiada, zapewnianego przez producenta urządzenia i objętego jednolitym wsparciem technicznym, klienta VPN dla technologii IPSec VPN i SSL VPN,

6.7.13.1. Oprogramowanie klienta VPN (IPSec oraz SSL) ma możliwość instalacji na stacjach roboczych pracujących pod kontrolą systemów operacyjnych Windows (7, XP – wersje 32 i 64-bitowe) i Linux i umożliwia zestawienie do urządzenia połączeń VPN z komputerów osobistych PC,

6.7.13.2. Oprogramowanie klienta VPN obsługuje protokoły szyfrowania 3DES/AES,

6.7.13.3. Oprogramowanie klienta VPN umożliwia blokowanie lokalnego dostępu do Internetu podczas aktywnego połączenia klientem VPN,

6.7.14. Urządzenie ma możliwość pracy jako transparentna ściana ogniowa warstwy drugiej ISO OSI

6.7.15. Urządzenie musi umożliwiać grupowanie VLANów w transparentnym trybie pracy firewalla. Wymagana jest możliwość zdefiniowania co najmniej 8 takich grup po 4 VLANy. Każda tak zdefiniowana grupa musi umożliwiać realizację odrębnych list kontroli dostępu,

6.7.16. Urządzenie musi umożliwiać wdrożenia w scenariuszu z routingiem asymetrycznym,

6.7.17. Urządzenie obsługuje protokół NTP,

6.7.18. Urządzenie współpracuje z serwerami CA,

6.7.19. Urządzenie obsługuje funkcjonalność Network Address Translation (NAT oraz PAT) – zarówno dla ruchu wchodzącego, jak i wychodzącego. Urządzenie wspiera translację adresów (NAT) dla ruchu multicastowego,

6.7.20. Urządzenie musi wspierać mechanizm translowania adresów sieciowych NAT i translowania adresów i portów PAT w następujących wariantach: z IPv6 na IPv6, z IPv4 na IPv4, z IPv4 na IPv6,

6.7.21. Urządzenie musi umożliwiać więcej niż 32768 dynamicznych translacji PAT do pojedynczego zewnętrznego adresu IP,

6.7.22. Urządzenie musi umożliwiać konfigurację czasu ważności translacji PAT,

6.7.23. Urządzenie wykonując dynamiczne translacje PAT do puli zewnętrznych adresów IP, musi równomiernie korzystać ze wszystkich zdefiniowanych w puli adresów.

6.7.24. Urządzenie zapewnia mechanizmy redundancji w tym możliwość konfiguracji urządzeń w układ zapasowy (failover) działający w trybie wysokiej dostępności (HA) active/standby i active/active.

6.7.25. Urządzenie realizuje synchronizację tablicy połączeń pomiędzy węzłami pracującymi w trybie wysokiej dostępności HA,
6.7.26. Urządzenie zapewnia możliwość konfiguracji redundancji na poziomie interfejsów fizycznych urządzenia,
6.7.27. Urządzenie zapewnia funkcjonalność stateful failover dla ruchu VPN
6.7.28. Urządzenie posiada mechanizmy inspekcji aplikacyjnej i kontroli co najmniej następujących usług:
6.7.28.1. Hypertext Transfer Protocol (HTTP),
6.7.28.2. File Transfer Protocol (FTP),
6.7.28.3. Extended Simple Mail Transfer Protocol (ESMTP),
6.7.28.4. Domain Name System (DNS),
6.7.28.5. Simple Network Management Protocol v 1/2/3 (SNMP),
6.7.28.6. Internet Control Message Protocol (ICMP),
6.7.28.7. SQL*Net,
6.7.28.8. inspekcji protokołów dla ruchu voice/video – H.323 (włącznie z H.239), SIP, MGCP, RTSP
6.7.29. Urządzenie umożliwia zaawansowaną normalizację ruchu TCP:
6.7.29.1. poprawność pola TCP ACK(invalid-ack)
6.7.29.2. poprawność sekwencjonowania segmentów TCP (seq-past-window)
6.7.29.3. poprawność ustanawiania sesji TCP z danymi (synack-data)
6.7.29.4. limitowanie czasu oczekiwania na segmenty nie w kolejności
6.7.29.5. poprawność pola MSS (exceed-mss).
6.7.29.6. poprawność pola długości TCP
6.7.29.7. poprawność skali okna segmentów TCP non-SYN
6.7.29.8. poprawność wielkości okna TCP
6.7.30. Urządzenie musi umożliwiać zaawansowane badanie stanu każdej sesji TCP w zakresie:
6.7.30.1. sprawdzania opcji TCP, usuwania opcji TCP i odrzucania segmentów z opcjami TCP,
6.7.30.2. poprawności pola TCP ACK,
6.7.30.3. poprawności sekwencjonowania segmentów TCP (seq-past-window) ze wsparciem mechanizmów akceleracji sieci WAN wprowadzających przesunięcie numerów sekwencyjnych TCP,
6.7.30.4. weryfikacji sumy kontrolnej segmentu TCP,
6.7.30.5. weryfikacji pola TCP SACK ALLOW,
6.7.30.6. weryfikacji wielkości okna TCP,
6.7.30.7. usuwania flagi URG,
6.7.30.8. usuwania segmentów przekraczających maksymalny rozmiar (MSS),
6.7.30.9. usuwania segmentów z flagą SYN i z flagami SYN/ACK, jeśli zawierają one dane,
6.7.31. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych otwartych połączeń TCP i UDP zestawionych do hosta lub do grupy hostów.
6.7.32. Urządzenie musi umożliwiać ograniczenie maksymalnej liczby równoczesnych półotwartych połączeń TCP zestawionych do hosta lub do grupy hostów.
6.7.33. Urządzenie musi umożliwiać zresetowanie otwartego połączenia TCP, jeśli przez określony okres czasu przez połączenie nie przesyłano żadnych danych.
6.7.34. Urządzenie musi umożliwiać inspekcję ruchu HTTP w zakresie:
6.7.34.1. zgodności z formalną definicją protokołu,
6.7.34.2. ukrywania nagłówka Server w odpowiedzi http,
6.7.34.3. filtrowania dopuszczalnych metod HTTP,
6.7.34.4. filtrowania dopuszczalnych typów MIME,
6.7.34.5. filtrowania dopuszczalnych adresów URL,
6.7.35. Urządzenie musi umożliwiać inspekcję ruchu SMTP w zakresie:
6.7.35.1. zgodności z formalną definicją protokołu ESMTP,
6.7.35.2. ukrywania wiadomości powitalnej serwera,
6.7.35.3. filtrowania długości wydawanych komend,
6.7.35.4. filtrowania listy odbiorców dłuższej niż określona liczba,
6.7.35.5. filtrowania długości adresu nadawcy,
6.7.35.6. filtrowania długości pola MIME,
6.7.35.7. filtrowania dopuszczalnych typów MIME,

6.7.36. Urządzenie musi umożliwiać inspekcję ruchu DNS w zakresie:
- 6.7.36.1. zgodności z formalną definicją protokołu DNS,
- 6.7.36.2. filtrowania długości wiadomości,
- 6.7.36.3. filtrowania po typie zapytania,
- 6.7.36.4. randomizowania numeru identyfikacyjnego wiadomości,
- 6.7.36.5. weryfikacji zgodności numeru indentyfikacyjnego zapytania i odpowiedzi,
- 6.7.36.6. blokowania innych odpowiedzi niż pierwsza (ochrona przed atakiem dns spoofing i dns poisoning),

6.7.37. Urządzenie zapewnia obsługę i kontrolę protokołu ESMTP w zakresie wykrywania anomalii, śledzenia stanu protokołu oraz obsługi komend wprowadzonych wraz z protokołem ESMTP,

6.7.38. Urządzenie ma możliwość inspekcji protokołów HTTP oraz FTP na portach innych niż standardowe,

6.7.39. Urządzenie zapewnia wsparcie stosu protokołów IPv6 w tym:
- 6.7.39.1. dla list kontroli dostępu dla IPv6,
- 6.7.39.2. możliwości filtrowania ruchu IPv6 na bazie nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload,
- 6.7.39.3. wspiera inspekcję protokołu IPv6, pracując w trybie transparentnym,
- 6.7.39.4. wspiera adresację IPv6 interfejsów w scenariuszach wdrożeniowych z wysoką dostępnością (failover),
- 6.7.39.5. wspiera realizację połączeń VPN typu site-to-site opartych o minimum IKEv1 z użyciem protokołu IPv6,

6.7.40. Urządzenie umożliwia współpracę z serwerami autoryzacji w zakresie przesyłania list kontroli dostępu z serwera do urządzenia z granulacją per użytkownik.

6.7.41. Urządzenie obsługuje routing statyczny i dynamiczny (co najmniej dla protokołów RIP, OSPFv2, OSPFv3 i BGP).

6.7.42. Urządzenie pozwala na osiągnięcie wysokiej dostępności dla protokołów routingu dynamicznego (min OSPF), tzn trasy dynamiczne zawarte w tablicy routingu są synchronizowane z urządzenia active na urządzenie standby,

6.7.43. Urządzenie musi obsługiwać ruch multicastowy w zakresie wsparcia protokołu PIM, IGMP i definiowania list kontroli dostępu dla ruchu multicastowego.

6.7.44. Urządzenie musi umożliwiać konfigurację w roli serwera DHCP.

6.7.45. Urządzenie musi umożliwiać funkcję przekazywania zapytań DHCP do zewnętrznego serwera DHCP (DHCP relay) dla IPv4 i IPv6.

6.7.46. Urządzenie umożliwia zbieranie informacji o czasie (timestamp) i ilości trafień pakietów w listy kontroli dostępu (ACL).

6.7.47. Urządzenie umożliwia konfigurację globalnych reguł filtrowania ruchu, które przykładane są na wszystkie interfejsy urządzenia jednocześnie.

6.7.48. Urządzenie umożliwia konfigurację reguł NAT i ACL w oparciu o obiekty i grupy obiektów. Do grupy obiektów może należeć host, podsieć lub zakres adresów, protokół lub numer portu.

6.7.49. Listy kontroli dostępu muszą umożliwiać definiowanie reguł w oparciu o następujące podstawowe parametry:
- 6.7.49.1. źródłowy i docelowy adres IPv4,
- 6.7.49.2. źródłowy i docelowy adres IPv6,
- 6.7.49.3. źródłowy i docelowy numer portu UDP,
- 6.7.49.4. źródłowy i docelowy numer portu TCP,
- 6.7.49.5. nazwy domenowej hosta źródłowego lub docelowego,
- 6.7.49.6. nazwa użytkownika w usłudze katalogowej Microsoft Active Directory,
- 6.7.49.7. nazwa grupy w usłudze katalogowej Microsoft Active Directory,
- 6.7.49.8. czas,

6.7.50. Urządzenie nie może posiadać żadnych programowych ograniczeń na liczbę reguł dostępu jakie mogą być równocześnie wykorzystywane.

6.7.51. Urządzenie musi umożliwiać inspekcję ruchu IPv4 z wykorzystaniem nagłówków: End of Options List, No Operation, Router Alarm.

6.7.52. Urządzenie musi umożliwiać inspekcję ruchu IPv6 z wykorzystaniem nagłówków rozszerzeń: Hop-by-Hop Options, Routing (Type 0), Fragment, Destination Options, Authentication, Encapsulating Security Payload.

6.7.53. Jeśli pakiet IPv4/IPv6 został pofragmentowany, urządzenie musi odtworzyć oryginalny pakiet kontrolując przy tym kolejność fragmentów i ich integralność.

6.7.54. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby równocześnie odtwarzanych z fragmentów pakietów IPv4/IPv6 per każdy interfejs urządzenia realizujący usługę firewalla. Wymaga się, aby urządzenie umożliwiało równoczesne odtwarzanie co najmniej 30.000 pofragmentowanych pakietów.

6.7.55. Urządzenie musi umożliwiać skonfigurowanie maksymalnej dopuszczalnej liczby fragmentów w ramach jednego odtwarzanego pakietu.

6.7.56. Urządzenie musi umożliwiać skonfigurowanie maksymalnego dopuszczalnego okresu czasu, w którym musi otrzymać wszystkie fragmenty niezbędne do odtworzenia pakietu.

6.7.57. Urządzenie musi umożliwiać pominięcie stanu sesji TCP w scenariuszach wdrożeniowych z asymetrycznym przepływem ruchu.

6.7.58. Urządzenie musi wspierać Proxy dla protokołu SCEP i umożliwia zautomatyzowany proces pozyskiwania certyfikatów przez użytkowników zdalnych dla dostępu VPN.

6.7.59. Urządzenie musi wspierać użytkowników korzystających z trybu klienta VPN (IPSec oraz SSL) oraz clientless SSL VPN, w zakresie obsługi haseł w systemie Microsoft AD, bezpośrednio lub poprzez oprogramowanie pośredniczące, co najmniej dla obsługi sytuacji wygaśnięcia terminu ważności hasła w systemie Microsoft AD, umożliwiając zmianę przeterminowanego hasła.

6.7.60. Urządzenie musi obsługiwać IKE, IKE Extended Authentication (Xauth) oraz IKE Aggressive Mode. Ponadto urządzenie wspiera protokół IKEv2 (Internet Key Exchange w wersji 2) dla połączeń zdalnego dostępu VPN oraz site-to-site VPN opartych o protokół IPSec.

6.7.61. Urządzenie musi umożliwiać konfigurację wirtualnych firewalli. Wymagana jest docelowa obsługa co najmniej 100 wirtualnych firewalli, w ofercie nalezy przewidzieć obsługę 5 wirtualnych firewalli.

6.7.62. Urządzenie musi obsługiwać ramki Ethernet typu Jumbo (o rozmiarze 9216 bajtów).

6.7.63. Urządzenie musi obsługiwać ramki XOFF zgodnie z definicją standardu 802.3x.

6.7.64. Urządzenie musi umożliwiać konfigurację następujących mechanizmów zarządzania jakością przesyłania danych (Quality of Service):

6.7.64.1. Urządzenie obsługuje mechanizmy kolejkowania ruchu z obsługą kolejki absolutnego priorytetu - obsługa kolejki priorytetowej o konfigurowalnej długości per każdy interfejs urządzenia realizący usługę firewalla– pakiety umieszczone w tej kolejce zostaną obsłużone przed innymi pakietami umieszczonymi w innych kolejkach.

6.7.64.2. policing – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez odrzucanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps. Policing musi być obsługiwany dla ruchu wchodzącego i wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.

6.7.64.3. shaping – mechanizm ograniczający maksymalną przepustowość wybranych połączeń poprzez buforowanie pakietów z dopuszczeniem chwilowych odchyleń, gdy sumaryczna przepustowość strumieni danych przekroczy zadaną wartość w bps konfigurowalną z granularnością co najmniej 8kbps. Zbuforowane pakiety są wysyłane w późniejszym okresie czasu, gdy sumaryczna przepustowość strumieni danych będzie niższa niż zadana wartość w bps. Shaping musi być obsługiwany co najmniej dla ruchu wychodzącego na każdym interfejsie urządzenia realizującym usługę firewalla.

6.7.65. Urządzenie musi umożliwiać wykrywanie, raportowanie i filtrowanie ruchu typu "call-home" od zainfekowanych złośliwym oprogramowaniem hostów w sieci chronionej do sieci typu botnet. Proces filtrowania musi się opierać o globalną bazę adresów IP utrzymywaną przez producenta urządzenia. W wycenie należy przewidzieć licencję na 3 lata.

6.8. Funkcjonalność urządzenia – NGFW.

6.8.1. Urządzenie musi zapewniać funkcjonalności tzw, Next-Generation firewall w zakresie nie mniejszym niż

6.8.1.1. Możliwość konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika (Identity Firewall), integrując się ściśle z usługą katalogową Microsoft Active Directory,

6.8.1.2. Dostępność systemu automatycznego wykrywania i klasyfikacji aplikacji (Application Visibility and Control),

6.8.1.3. Dostępność systemu IPS.

6.8.2. System musi posiadać otwarte API dla współpracy z systemami zewnętrznymi w tym co najmniej z systemami SIEM,

6.8.3. System Klasyfikacji i Rozpoznawania Aplikacji (SKRA) musi:

6.8.3.1. posiadać możliwość klasyfikacji ruchu i wykrywania co najmniej 3000 aplikacji sieciowych

6.8.3.2. pozwalać na tworzenie profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego z którego korzysta użytkownik oraz wykorzystywanych usług,

6.8.3.3. pozwalać na wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji,

6.8.3.4. umożliwiać współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system SKRA oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach.

6.9. Funkcjonalność urządzenia IPS.

6.9.1. System IPS musi posiadać możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Wymagane jest by system tworzył kontekst z wykorzystaniem co najmniej poniższych parametrów:

6.9.1.1. Wiedza o użytkownikach – uwierzytelnienie,

6.9.1.2. Wiedza o urządzeniach – pasywne skanowanie ruchu,

6.9.1.3. Wiedza o urządzeniach mobilnych,

6.9.1.4. Wiedza o aplikacjach wykorzystywanych po stronie klienta,

6.9.1.5. Wiedza o podatnościach,

6.9.1.6. Wiedza o bieżących zagrożeniach,

6.9.1.7. Baza danych URL,

6.9.2. System IPS musi

6.9.2.1. Posiadać możliwość pracy w trybie in-line (wszystkie pakiety, które mają być poddane inspekcji muszą przechodzić przez system),

6.9.2.2. posiadać możliwość pracy zarówno w trybie pasywnym (IDS) jak i aktywnym (z możliwością blokowania ruchu),

6.9.2.3. posiadać możliwość wykrywania i uniemożliwiać szeroką gamę zagrożeń w tym co najmniej:

6.9.2.3.1. złośliwe oprogramowanie,

6.9.2.3.2. skanowanie sieci,

6.9.2.3.3. ataki na usługę VoIP,

6.9.2.3.4. próby przepełnienia bufora,

6.9.2.3.5. ataki na aplikacje P2P,

6.9.2.3.6. zagrożenia dnia zerowego, itp.

6.9.2.4. posiadać możliwość wykrywania modyfikacji znanych ataków (sygnatury) jak i te nowo powstałe, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna)

6.9.2.5. zapewniać co najmniej poniższe sposoby wykrywania zagrożeń

6.9.2.5.1. sygnatury ataków opartych na exploitach,

6.9.2.5.2. reguły oparte na zagrożeniach,

6.9.2.5.3. mechanizm wykrywania anomalii w protokołach,

6.9.2.5.4. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego,

6.9.2.6. mieć możliwość inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakres protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu,

6.9.2.7. posiadać mechanizm minimalizujący liczbę fałszywych alarmów jak i niewykrytych ataków (ang. false positives i false negatives),

6.9.2.8. mieć możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń,

6.9.2.9. posiadać wiele możliwości reakcji na zdarzenia takie jak:

6.9.2.9.1. tylko monitorowanie,

6.9.2.9.2. blokowanie ruchu zawierającego zagrożenia,

6.9.2.9.3. zapisywanie pakietów,

6.9.2.10. mieć możliwość detekcji ataków i zagrożeń opartych na protokole IPv6,

6.9.2.11. posiadać możliwość pasywnego zbierania informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - co najmniej powinna być zbierana,

6.9.2.11.1. informacja o systemach operacyjnych,

6.9.2.11.2. informacja o serwisach,

6.9.2.11.3. informacja o otwartych portach, aplikacjach,

6.9.2.11.4. informacja o zagrożeniach,

6.9.2.12. posiadać możliwość pasywnego gromadzenia informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych,

6.9.2.13. zapewniać możliwość pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp.

6.9.2.14. posiadać możliwość automatycznej inspekcji i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji,

6.9.2.15. zapewniać możliwość obrony przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu musi stosować najodpowiedniejszy mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego,

6.9.2.16. zapewniać mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne

6.9.2.17. zapewniać możliwość definiowania wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie,

6.9.2.18. być zarządzany poprzez system centralnego zarzadzania za pomocą szyfrowanego połączenia,

6.9.2.19. Zapewniać możliwość wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS,

6.9.2.20. Zapewniać mechanizmy automatyzacji co najmniej w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise),

6.9.2.21. Zapewniać mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa,

6.9.2.22. Posiadać możliwość wykorzystania mechanizmów obsługi ruchu asymetrycznego firewalla dla uzyskania pełnej widoczności ruchu – w szczególności musi posiadać możliwość pracy w trybie failover firewalla oraz w trybie klastrowania

6.9.2.23. failover firewalla oraz w trybie klastrowania

6.10. Funkcjonalność urządzenia - AntiMalware

6.10.1. Urządzenie musi zapewniać możliwość wykrywania i śledzenia transferu następujących kategorii plików w ruchu sieciowym:

6.10.1.1. pliki systemowe,

6.10.1.2. pliki wykonywalne,

6.10.1.3. pliki PDF,

6.10.1.4. pliki pakietu Office,

6.10.1.5. pliki skompresowane,

6.10.2. Urządzenie musi posiadać możliwość monitorowania jak i kontrolowania transferu plików w co najmniej następujących protokołach:

6.10.2.1. HTTP,

6.10.2.2. SMTP,

6.10.2.3. FTP,

6.10.2.4. IMAP,

6.10.2.5. POP3,

6.10.2.6. W danym kierunku:

6.10.2.6.1. Upload,

6.10.2.6.2. Download,

6.10.3. Urządzenie musi posiadać możliwość sprawdzania sumy kontrolnej plików widzianych w ruchu sieciowym pod kątem ich reputacji w rozwiązaniu antymalwarowym.
6.10.4. Urządzenie musi posiadać możliwość dokonania statycznej analizy struktury całego pliku pod kątem charakterystycznych elementów używanych w złośliwym oprogramowaniu.
6.10.5. Urządzenie musi posiadać możliwość współpracy z rozwiązaniem antymalwerowym pod kątem dynamicznej analizy plików (sandbox).
6.10.5.1. Urządzenie musi zapewniać możliwość wysłania pliku do dynamicznej analizy (sandboxa).
6.10.5.2. Konsola zarządzająca musi zapewniać dostarczenie co najmniej dwóch rodzajów raportów z dynamicznej analizy sandboxowej dla każdego analizowane pliku mogącego zawierać złośliwe oprogramowanie:
6.10.5.2.1. raport skrócony,
6.10.5.2.2. pełny raport.
6.10.6. Urządzenie musi zapewniać możliwość zapisania na dysk twardy kopii analizowanych plików o następujących charakterystykach:
6.10.6.1. pliki wolne od złośliwego kodu,
6.10.6.2. pliki zawierające złośliwy kod,
6.10.6.3. pliki podejrzane,
6.10.6.4. pliki o własnej, zdefiniowanej przez użytkownika kategorii,
6.10.7. Urządzenie działając w trybie inline musi zapewniać możliwość zablokowania transferu plików o następujących cechach:
6.10.7.1. Dla zdefiniowanej kategorii,
6.10.7.2. Dla zdefiniowanego rodzaju,
6.10.7.3. Dla zdefiniowanego protokołu,
6.10.7.4. Dla zdefiniowanego kierunku transferu,
6.10.7.5. zawierających malware tak aby odbiorca pliku uniknął potencjalnej infekcji.
6.10.8. Konsola zarządzająca systemu ochrony antymalware musi posiadać możliwość wglądu w zdarzenia rozwiązania antymalwerowego rezydującego na monitorowanych stacjach roboczych oraz serwerach.
6.10.9. Konsola zarządzająca musi posiadać możliwość dostarczenia szczegółowych informacji na temat statystyk monitorowanych kategorii plików.
6.10.10. Konsola zarządzająca musi posiadać możliwość wyświetlenia szczegółowej trajektorii transferu danego pliku po monitorowanej sieci oraz korelacji zdarzeń przychodzących z rozwiązania antymalware rezydującego na serwerach i stacjach roboczych.

6.11. Zarządzanie i konfiguracja
6.11.1. Urządzenie musi umożliwiać zarządzanie:
6.11.1.1. przez linię poleceń (ang. Command Line Interface) dostępną poprzez bezpośrednie połączenie do portu konsoli urządzenia i dostępną zdalnie przy pomocy protokołów telnet i SSH v2.
6.11.1.2. przez graficzny interfejs użytkownika z wykorzystaniem dedykowanej aplikacji,
6.11.1.3. programowo przez interfejs API dostępny przy pomocy protokołu https,
6.11.1.4. przez protokół SNMPv3 ze wsparciem dla integralności i poufności komunikacji,
6.11.2. Zdalnie dostępne interfejsy zarządzania muszą być dostępne w sieci IPv4 i IPv6.
6.11.3. Urządzenie dla protokołu SSH musi umożliwiać uwierzytelnienie w oparciu nazwę użytkownika i hasło oraz w oparciu o klucz publiczny.
6.11.4. Urządzenie musi umożliwiać konfigurację maksymalnej równoczesnej liczby sesji zdalnego zarządzania.
6.11.5. Urządzenie musi umożliwiać ograniczenie dostępu do zdalnie dostępnych interfejsów zarządzania tylko z wybranych adresów IPv4 i IPv6.
6.11.6. Urządzenie musi umożliwiać wyeksportowanie konfiguracji do pliku tekstowego i jej przeglądanie, analizę oraz edycję w trybie offline.
6.11.7. Urządzenie musi mieć możliwość raportowania zdarzeń przy pomocy protokołu SYSLOG. Wymagane jest wsparcie szyfrowanej transmisji wiadomości SYSLOG przy pomocy SSL/TLS.
6.11.8. Urządzenie musi wspierać eksport zdarzeń opartych o przepływy za pomocą protokołu NetFlow v9 (RFC 3954) lub równoważnym.

6.11.9. Urządzenie musi posiadać możliwość komunikacji z serwerami uwierzytelnienia i autoryzacji za pośrednictwem protokołu RADIUS lub TACACS+.
6.11.10. Dostęp do urządzenia musi być możliwy przez SSH.
6.11.11. Urządzenie musi obsługiwać protokół SNMP v 1/2/3.
6.11.12. Urządzenie musi umożliwiać edycję pliku konfiguracyjnego urządzenia w trybie off-line. Tzn. istnieje możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC. Po zapisaniu konfiguracji w pamięci nieulotnej jest możliwe uruchomienie urządzenia z nową konfiguracją.
6.11.13. Urządzenie musi umożliwiać zrzucenie obecnego stanu programu (coredump) dla potrzeb diagnostycznych.
6.11.14. Urządzenie musi umożliwiać uwierzytelnienie i konfigurację poziomu dostępu administratora w oparciu o role (ang. Role Bases Access Control) z wykorzystaniem bazy danych użytkowników zdefiniowanej lokalnie na urządzeniu lub na zewnętrznych serwerach dostępnych przy pomocy protokołów RADIUS lub TACACS+.

6.12. Dopuszczalne sposoby realizacji rozwiązania:
6.12.1. Wymaga się spełnienia następujących warunków realizacji zadania ochrony styku z internetem:
6.12.1.1. Firewalle zastosowowane do ochrony styku z PUE muszą pochodzić od jednego producenta,
6.12.1.2. Funkcjonalność firewalla sieciowego i firewall NGFW musi być realizowana na jednym urządzeniu,
6.12.1.3. Dopuszcza się zastosowanie zewnętrznych urządzeń IPS w przypadku gdy funkcjonalność IPS realizowana na urządzeniach ochrony styku z internetem byłaby innego producenta aniżeli dedykowane sondy IPS. W takim przypadku oferent zobowiązany jest do zapewnienia całościowej wymaganej funkcjonalności IPS na dostarczonych sondach. Dotyczy to także wymagań wydajnościowych. Oferent w przypadku zastosowania tego modelu zobowiązany jest:
6.12.1.3.1. do zapewnienia 2 dodatkowych portów 10Gbps w urządzeniu firewall,
6.12.1.3.2. do zastosowania urządzenia firewall o odpowiednio wyższej wydajności tj. Minimum 8 Gbps dla urządzenia pracującego w klastrze (ruch full duplex – 4 Gbps do sondy IPS z firewalla oraz 4Gbps ruchu „powrotnego”),
6.12.1.3.3. odpowiedniego wyposażenia (porty) sondy IPS umożliwiającego realizację tego zadania,
6.12.1.3.4. odpowiednio wydajnej sondy IPS – w szczególności należy dostosować,
6.12.1.3.5. do zapewnienia odpowiedniej liczby urządzeń (1:1 z firewallami) celem uzyskania niezbędnej redundancji. Niedopuszczalne jest zastosowanie mniejszej liczby urządzeń IPS niż firewalli.
6.12.1.4. Dopuszcza się zastosowanie zewnętrznych urządzeń Antivirus/AntiMalware. W takim przypadku Oferent zobowiązany jest do zapewnienia wymaganej funkcjonalności AntiMalware opisanej jako realizowanej na dedykowanych urządzeniach. Dotyczy to w szczególności wymagań wydajnościowych. Oferent zobowiązany jest do zapewnienia dodatkowych portów w urządzeniu firewall jak też odpowiedniego wyposażenia systemu antimalware umożliwiającego realizację tego zadania. Zamawiający oczekuje również, iż dostawca zapewni odpowiednią liczbę urządzeń (1:1 z firewallami) celem uzyskania niezbędnej redundancji. Zamawiający wymaga w tym przypadku również poświadczenia ze strony producentów firewalla i systemu antimalware (lub przedstawicielstw tych producentów na Polskę) potwierdzającego poprawną współpracę obu rozwiązań. Poświadczenie takie nie jest wymagane jeżeli taka współpraca opisana w oficjalnej dokumentacji producenta firewalla (jako wspierane rozwiązanie) lub w przypadku gdy oba rozwiązania pochodzą od tego samego producenta.
6.12.1.5. Dopuszcza się zastosowanie zewnętrznego urządzenia realizującego funkcjonalność VPN. W takim zakłada się że ruch VPN będzie kierowany bezpośrednio do takiego urządzenia a ruch odszyfrowany będzie przekierowywany do urządzenie Firewall. W takim przypadku oferent zobowiązany jest do zapewnienia całościowej wymaganej funkcjonalności VPN na dostarczonych urządzeniach w szczególności wymagań

wydajnościowych, przy czym nie wymaga się tutaj zwiększenia wydajności samego firewalla.

6.12.2. Dopuszcza się zastosowanie rozwiązań z maksymalnie 3 urządzeń. W skrajnym przypadku możliwe jest np. zaproponowanie całościowego rozwiązania składającego się z NGFW z VPN, systemu IPS, systemu ochrony antivirus/antimalware, z których każdy realizowany jest przez innego producenta.

7. Sprzętowy moduł bezpieczeństwa – 2 sztuki

Zamawiający w chwili obecnej posiada dwa moduły HSM Thales nShield Connect 500 pracujące w środowisku produkcyjnym. Wymaganiem Zamawiającego jest aby zaoferowany sprzęt działał z posiadanym. Zamawiający dopuszcza sytuację, w której Wykonawca zastąpi posiadane moduły innymi urządzeniami, o specyfikacji nie gorszej niż przedstawiona poniżej.

7.1. Ochrona przed nieupoważnionym dostępem.
  7.1.1. Obudowa modułu powinna być odporna na nieuprawnioną ingerencję zewnętrzną.
7.2. Brak ograniczeń na liczbę chronionych przez moduł kluczy.
7.3. Certyfikat zgodności ze standardem co najmniej FIPS 140-2 poziom 3.
7.4. Mechanizm podziału "sekretu"
  7.4.1. Ochrona kluczy prywatnych z wykorzystaniem mechanizmu podziału sekretu (K z N).
  7.4.2. Zarządzanie modułem z wykorzystaniem mechanizmu podziału sekretu (K z N).
7.5. W przypadku gdy do podziału sekretu wymagane jest wykorzystanie kart kryptograficznych (ang. smart card) wymaga się wyposażenia modułu HSM w 15 takich kart.
7.6. Możliwość obsługi wielu serwerów przez jeden moduł HSM.
7.7. Możliwość obsługi wielu aplikacji przez jeden moduł HSM.
7.8. Obsługiwane API:
  7.8.1. PKCS#11,
  7.8.2. CSP for Microsoft CryptoAPI,
  7.8.3. OpenSSL.
7.9. Możliwość ochrony klucza prywatnego RSA o długości 2048-bitów i powyżej.
7.10. Wraz z modułem musi być dostarczone oprogramowanie Cryptographic Service Provider i musi ono umożliwiać implementację komponentów odpowiedzialnych za wykonywanie podpisu elektronicznego w środowiskach:
  7.10.1. C++ kod niezarządzalny (przy wykorzystaniu interfejsu CryptoAPI 2.0).
7.11. Równoległa obsługa, przez jeden moduł HSM, wielu kompletów kluczy.
7.12. Separacja funkcji i ról administratorów zarządzających modułem HSM.
7.13. Obsługiwane systemy operacyjne:
  7.13.1. Linux w tym conajmniej RHEL 6.4 lub nowszy,
  7.13.2. MS Windows Server 2008,
  7.13.3. MS Windows Server 2012 w środowisku 32-bitowym i 64-bitowym.
7.14. Wspierane algorytmy kryptograficzne
  7.14.1. symetryczne: AES, DES, 3DES,
  7.14.2. asymetryczne: DSA, El Gamal, RSA,
  7.14.3. wymiany kluczy: Diffie-Hellman,
  7.14.4. hash: MD5, SHA-1, SHA-2.
7.15. Wydajność nie mniejsza niż 500 operacji na sekundę dla podpisu algorytmem RSA z kluczem 1024 bity.
7.16. Wykonywanie kopii zapasowych kluczy prywatnych chronionych przez HSM (w ramach bezpiecznego środowiska).
7.17. Możliwość pracy w układach wysokiej dostępności umożliwiających pełną redundantność i rozkładanie obciążenia.
7.18. Możliwość zdalnego zarządzania modułem.
7.19. Wsparcie techniczne urządzenia przez okres nie krótszy niż trzy lata z możliwością jego indywidualnego przedłużenia.

8. Przełącznik SAN – 4 sztuki

8.1. Przełącznik SAN musi być wykonany w technologii FC minimum 16 Gb/s i zapewniać możliwość pracy portów FC z prędkościami 16, 8, 4, 2 Gb/s w zależności od rodzaju zastosowanych wkładek SFP.

8.2. W przypadku obsadzenia portu FC za pomocą wkładki SFP 16Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 16, 8 lub 4 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

8.3. W przypadku obsadzenia portu FC za pomocą wkładki SFP 8Gb/s przełącznik musi umożliwiać pracę tego portu z prędkością 8, 4 lub 2 Gb/s, przy czym wybór prędkości musi być możliwy w trybie autonegocjacji.

8.4. Przełącznik SAN musi być wyposażony, w co najmniej 24 aktywne porty FC obsadzone 12 wkładkami SFP ShortWave 8Gb/s oraz 12 wkładkami SFP ShortWave 16Gb/s.

8.5. Wszystkie zaoferowane porty przełącznika SAN muszą umożliwiać działanie bez tzw. oversubscrypcji gdzie wszystkie porty w maksymalnie rozbudowanej konfiguracji przełącznika mogą pracować równocześnie z pełną prędkością 8Gb/s lub 16Gb/s w zależności do zastosowanych wkładek FC.

8.6. Całkowita przepustowość przełącznika FC dostępna dla maksymalnie rozbudowanej konfiguracji wyposażonej we wkładki 16Gb/s musi wynosić minimum 384 Gb/s end-to-end full duplex.

8.7. Rodzaj obsługiwanych portów, co najmniej: E, oraz F.

8.8. Przełącznik SAN musi mieć wysokość maksymalnie 1 RU (jednostka wysokości szafy montażowej) i szerokość 19” oraz zapewniać techniczną możliwość montażu w szafie 19”.

8.9. Przełącznik SAN powinien posiadać nadmiarowe zasilacze i wentylatory, których wymiana musi być możliwa w trybie „na gorąco” bez przerywania pracy przełącznika.

8.10. Przełącznik SAN musi mieć możliwość agregacji połączeń ISL między dwoma przełącznikami i tworzenia w ten sposób logicznych połączeń typu trunk o przepustowości minimum 128 Gb/s dla każdego logicznego połączenia. Load balancing ruchu między fizycznymi połączeniami ISL w ramach połączenia logicznego typu trunk musi być realizowany na poziomie pojedynczych ramek FC a połączenie logiczne musi zachowywać kolejność przesyłanych ramek. W wypadku gdy funkcjonalność wymaga licencji konieczne jest jej dostarczenie.

8.11. Przełącznik SAN musi realizować sprzętową obsługę zoningu (przez tzw. układ ASIC) na podstawie portów i adresów WWN.

8.12. Przełącznik SAN musi mieć możliwość wymiany i aktywacji wersji firmware’u (zarówno na wersję wyższą, jak i na niższą) w czasie pracy urządzenia i bez zakłócenia przesyłanego ruchu FC.

8.13. Przełącznik SAN musi wspierać następujące mechanizmy zwiększające poziom bezpieczeństwa:

- 8.13.1. uwierzytelnianie (autentykacja) przełączników w sieci Fabric za pomocą protokołów DH-CHAP i FCAP,
- 8.13.2. uwierzytelnianie (autentykacja) urządzeń końcowych w sieci Fabric za pomocą protokołu DH-CHAP,
- 8.13.3. szyfrowanie połączenia z konsolą administracyjną, wsparcie dla SSHv2,
- 8.13.4. definiowanie wielu kont administratorów z możliwością ograniczenia ich uprawnień za pomocą mechanizmu tzw. RBAC (Role Based Access Control),
- 8.13.5. definiowane kont administratorów w środowisku RADIUS i LDAP,
- 8.13.6. szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS,
- 8.13.7. obsługa SNMP,
- 8.13.8. IP Filter dla portu administracyjnego przełącznika,
- 8.13.9. wgrywanie nowych wersji firmware przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP,
- 8.13.10. wykonywanie kopii bezpieczeństwa konfiguracji przełącznika FC z wykorzystaniem bezpiecznych protokołów SCP oraz SFTP,

8.14. Przełącznik SAN musi mieć możliwość konfiguracji przez:

- 8.14.1. polecenia tekstowe w interfejsie znakowym konsoli terminala
- 8.14.2. przeglądarkę internetową z interfejsem graficznym

8.15. Przełącznik SAN musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, RS-232 oraz inband IP-over-FC.

8.16. Przełącznik SAN musi zapewniać wsparcie dla standardu zarządzającego SMI-S.

9. Macierz dyskowa – 2 sztuki

9.1. Przez macierz dyskową Zamawiający rozumie zestaw dysków twardych kontrolowanych przez dedykowane kontrolery macierzowe (bez dodatkowych urządzeń pośrednich, serwerów wirtualizujących itp.).

9.2. Możliwość skalowania kontrolerów macierzowych do co najmniej 4 szt. obsługujących blokowy dostęp do danych.

9.3. Wraz z macierzą wymagane jest dostarczenie standardowej szafy RACK 19" o wysokości 42U, w której macierz dyskowa będzie zamontowana.

9.4. Macierz musi posiadać min. przestrzeń użytkową 75TB, co najmniej w oparciu o min. 19TB w dyskach SSD, pozostała przestrzeń w dyskach SAS 10k rpm. Przestrzeń użytkowa skonfigurowana z poziomem ochrony RAID 5 lub wyższym. Należy przyjąć 1TB=1024GB, 1GB=1024MB, itd.

9.5. Przestrzeń dyskowa zbudowana w oparciu o dyski minimum SAS 600 GB 10k 2,5" i SSD 400 GB 2,5".

9.6. Macierz musi posiadać wydajność min. 70 000 IO/s przy parametrach: stosunek odczyty/zapisy: 70%/30%, cache hit=30%, średni response time=1 ms. Możliwość 5-krotnego skalowania ilości IO/s (przy zachowanych ww. parametrach) bez konieczności wymiany kontrolerów macierzowych.

9.7. Macierz musi posiadać możliwość rozbudowy (bez utraty danych i konieczności ich odtwarzania z backupu) do co najmniej 950 dysków, a także musi posiadać możliwość rozbudowy przestrzeni użytkowej do przynajmniej 120 TB.

9.8. Macierz musi obsługiwać dyski SSD, SAS oraz Nearline-SAS. Możliwość mieszania napędów dyskowych Nearline-SAS z napędami dyskowymi SSD oraz SAS w obrębie pojedynczej półki dyskowej.

9.9. Macierz powinna obsługiwać mechanizmy ochrony RAID: RAID0, RAID1, RAID5, RAID6 realizowane sprzętowo, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy.

9.10. Macierz powinna mieć możliwość definiowania globalnych dysków Spare lub odpowiedniej zapasowej przestrzeni dyskowej.

9.11. Macierz musi obsługiwać dyski twarde typu „Hot-Plug" z dwoma interfejsami.

9.12. Tryb pracy kontrolerów macierzowych:

9.12.1. Praca w trybie active/active dla każdego wolumenu logicznego.

9.12.2. Równoczesny, aktywny dostęp (odczyt/zapis) do każdego wolumenu logicznego ze wszystkich kontrolerów macierzy dla lepszego rozłożenia obciążenia.

9.13. Minimalna wielkość zainstalowanej pamięci Cache 192GB – z możliwością rozbudowy bez wykorzystywania zewnętrznych dysków SSD do pojemności co najmniej 384GB.

9.14. Macierz musi posiadać możliwość rozbudowy pamięci Cache o obszar zbudowany za pomocą zaoferowanych dysków SSD.

9.15. Zabezpieczenie pamięci Cache za pomocą mirrorowania pamięci Cache kontrolerów macierzowych. W przypadku awarii zasilania w celu ochrony danych zawartość pamięci Cache musi zostać trwale zapisana.

9.16. Instalacja lub uruchamianie dodatkowej funkcjonalności macierzy dyskowej nie może powodować zmniejszenia dostępnego obszaru pamięci Cache kontrolerów macierzowych.

9.17. Macierz musi posiadać, co najmniej 12 zewnętrznych interfejsów FC o nie mniejszej przepustowości niż 16Gb/s. Możliwość rozbudowy liczby zewnętrznych interfejsów FC do co najmniej 24 szt. Możliwość rozbudowy o interfejsy iSCSI i FCOE.

9.18. Zarządzanie grupami dyskowymi oraz wolumenami logicznymi:

9.18.1. Macierz musi mieć możliwość zdefiniowania co najmniej 64000 wolumenów logicznych.

9.18.2. Macierz musi mieć możliwość tworzenia wolumenów logicznych o wielkości nie mniejszej niż 16TB.

9.18.3. Możliwość dynamicznego zwiększania pojemności wolumenów logicznych oraz wielkości grup dyskowych (przez dodanie dysków) z poziomu kontrolera macierzowego bez przerywania dostępu do danych.

9.18.4. Dla każdego wolumenu logicznego możliwość określania parametrów wydajnościowych: minimum i maksimum ilości operacji IO/s, minimum i maksimum przepustowości MB/s. [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.19. Macierz musi posiadać możliwość ochrony danych w heterogenicznych środowiskach sieci SAN – maskowanie LUN.

9.20. Możliwość jednoczesnego podłączenia co najmniej 64 niezależnych systemów: VMware ESX 4/5/6, MS Windows 2008/2012, RedHat Linux 5/6/7, SUSE/SLES 10/11/12. Macierz musi wspierać

mechanizm VMware vSphere 6 Vvol. Wsparcie powinno być dostępne w ramach oferowanych licencji oprogramowania.

9.21. Macierz musi mieć możliwość obsługi wielu kanałów I/O (multipathing). Automatyczne przełączanie kanału I/O w wypadku awarii ścieżki dostępu serwerów do macierzy z utrzymaniem ciągłości dostępu do danych. Przełączanie kanałów I/O oparte o natywne mechanizmy systemów operacyjnych wspieranych przez macierz. Wymagane jest dostarczenie odpowiednich licencji do obsługi ww. funkcjonalności.

9.22. Macierz musi umożliwiać uaktualnianie oprogramowania (firmware'u) macierzy (zarówno kontrolerów, jak i dysków) bez przerywania pracy macierzy.

9.23. Wymiana elementów systemu w trybie „Hot-Swap", a w szczególności takich, jak: kontrolery, zasilacze, wentylatory.

9.24. Macierz musi być przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania.

9.25. Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Pełna redundancja macierzy, w szczególności zdublowanie kontrolerów macierzowych, zasilaczy i wentylatorów.

9.26. Zarządzanie i monitoring stanu macierzy:

9.26.1. Macierz musi umożliwiać zdalne zarządzanie macierzą oraz automatyczne informowanie centrum serwisowego o awarii.

9.26.2. Świadczenia obsługi serwisowej zgodnie z wymogami ISO .

9.26.3. Zarządzanie macierzą z poziomu interfejsu graficznego i interfejsu znakowego. Wymagane jest stałe monitorowanie stanu macierzy oraz możliwość konfigurowania jej zasobów dyskowych.

9.26.4. Monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, grup dyskowych, wolumenów logicznych, pojedynczych napędów dyskowych oraz kontrolerów.

9.26.5. Wymagana możliwość historycznej kolekcji danych wydajnościowych.

9.26.6. Wymagane jest dostarczenie odpowiedniej licencji dla opisanych funkcjonalności dla całej pojemności macierzy.

9.26.7. Dostarczenie odpowiedniej licencji dla opisanych funkcjonalności dla całej pojemności macierzy jeśli jest wymagana dla uruchomienia tych funkcjonalności.

9.27. Macierz musi mieć możliwość udostępniania zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.28. Macierz musi umożliwiać deduplikację danych wykonywaną na bieżąco (w locie) co najmniej dla warstwy dysków SSD [wymagane jest dostarczenie licencji dla tej funkcjonalności].

9.29. Migracja danych w obrębie macierzy:

9.29.1. Macierz musi umożliwiać migrację danych, bez przerywania do nich dostępu, pomiędzy różnymi warstwami technologii dyskowych: SSD, SAS, Nearline-SAS oraz różnych poziomów RAID na poziomie całych wolumenów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.29.2. Macierz musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych: SSD, SAS, Nearline-SAS na poziomie części wolumenów logicznych. Zmiany te muszą się odbywać wewnętrznymi mechanizmami macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz (SSD, SAS, Nearline-SAS) a jego części będą automatycznie, online i transparentnie dla korzystającego z tego LUNa hosta/hostów realokowane na podstawie analizy ruchu [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.30. Macierz musi umożliwiać podział macierzy na odseparowane macierze logiczne zarządzane przez dedykowanych administratorów [nie jest wymagane dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.31. Wewnętrzne kopie danych:

9.31.1. Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym

lub na jego kopii [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.31.2. Macierz musi umożliwiać, dokonywania na żądanie, pełnej fizycznej kopii danych w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Możliwość wykonania kopi w innej grupie dyskowej niż dane oryginalne [wymagane jest dostarczenie licencji dla tej funkcjonalności dla całej pojemności macierzy].

9.32. Macierz musi wspierać minimum 2000 kopii migawkowych per wolumen logiczny i minimum 16000 wszystkich kopii migawkowych.

9.33. Replikacja danych:

9.33.1. Macierz musi umożliwiać zdalną sprzętową replikację danych drugiej macierzy tego samego typu. Replikacja wykonywana na poziomie kontrolerów, bez obciążania serwerów podłączonych do macierzy. Replikacja musi być dostępna w trybie synchronicznym i asynchronicznym. Możliwość replikacji po protokole FC i IP. [wymagane jest dostarczenie licencji dla tej funkcjonalności na całą pojemność macierzy].

9.33.2. Macierz musi umożliwiać replikację zdalną w następujących trybach: „jeden do jednego", „jeden do wielu", „wiele do jednego".

9.33.3. Macierz musi umożliwiać replikację jednego wolumenu logicznego (tych samych danych) do dwóch innych, niezależnych ośrodków za pomocą replikacji synchronicznej i asynchronicznej.

10. System zarządzania dostarczonymi urządzeniami

System musi umożliwiać centralne zarządzanie dostarczonymi urządzeniami. Dostarczone rozwiązanie ma umożliwiać zarządzanie routerami, przełącznikami, firewallami i serwerami, może to być jeden lub kilka systemów.

System zarządzenia urządzeniami LAN

System musi umożliwiać centralne zarządzanie zaproponowanymi urządzeniami sieciowymi (przełączniki, routery). Wykonawca zapewni system o poniższej funkcjonalności, który będzie obsługiwał dostarczone urządzenia sieciowe.

10.1. Możliwość instalacji oprogramowania jako maszyna wirtualna (osadzana na platformie wirtualizacyjnej dostarczonej niniejszym zamówieniem) lub system może być dostarczony na dedykowanej platformie sprzętowej.

10.1.1. Preferowane jest dostarczenia oprogramowania w formie maszyny wirtualnej pracującej pod środowiskiem VMware ESXi posiadanym przez zamawiającego.

10.2. Oprogramowanie zarządzające powinno być dostarczone w najnowszej dostępnej wersji.

10.3. Dostarczona wersja musi posiadać licencje na zarządzanie dostarczonymi urządzeniami z możliwością rozbudowy o kolejne 15 urządzeń.

10.4. Wymagania funkcjonalne- system musi zapewniać:

10.4.1. zarządzanie i zbieranie statystyk z wykorzystaniem protokołu SNMP,

10.4.2. narzędzia automatycznej identyfikacji i wyszukiwania urządzeń instalowanych w sieci,

10.4.3. narzędzia prezentacji urządzeń sieciowych wraz z dynamiczną prezentacją zmiany stanu urządzenia,

10.4.4. narzędzie umożliwiające zbieranie i zapisywanie informacji o parametrach pracy zainstalowanego sprzętu,

10.4.5. wbudowane narzędzia do konfiguracji urządzeń w zakresie przynajmniej interfejsów, list kontroli dostępu, PortChannel oraz wirtualny PortChannel, VLAN 802.1Q, Private VLAN, MSTP/RSTP, HSRP, VRRP lub odpowiedniki, Port Security

10.4.6. narzędzie do zarządzania obrazami oprogramowania urządzeń,

10.4.7. zarządzanie wersjami oprogramowania urządzeń,

10.4.8. funkcje archiwizacji konfiguracji, przeglądania zmian konfiguracji, automatyzacji zbierania konfiguracji urządzeń,

10.4.9. narzędzie do konfiguracji. monitoringu i optymalizacji usług WAN (technologia VPN, polityka routingu oraz polityka QoS z podziałem na aplikacje).

10.4.10. narzędzie do generowania raportów, które mogą być uruchamiane natychmiastowo lub w określonych odstępach czasu i być przeglądane na bieżąco lub wysyłane do pliku,

10.4.11. narzędzie do zbierania alarmów pochodzących z urządzeń, kategoryzacji alarmów,

10.4.12. możliwość informowania o alarmach/incydentach przez notyfikację email.

Konsola zarządzania elementami bezpieczeństwa

Konsola musi umożliwiać centralne zarządzanie zaproponowanymi komponentami bezpieczeństwa i posiadać następującą funkcjonalność.

10.5. Funkcjonalność konsoli firewalla:

10.5.1. Zarządzanie funkcjonalnością firewall:

10.5.1.1. Centralne zarządzanie urządzeniami i licencjami (Inwentaryzację urządzeń z dokładnością do konfiguracji sprzętowej, użytego firmware oporgramowania, wersji pliku konfiguracyjnego),

10.5.1.2. Definiowanie funkcji firewalla z określeniem stref (zone) bezpieczeństwa,

10.5.1.3. Definiowanie funkcji wysokiej dostępności (failover) oraz rozłożenia ruchu (clustering) o ile dostarczone rozwiązanie może pracować w klastrze,

10.5.1.4. Definiowanie polityk firewalla z określeniem źródła, celu, service flow

10.5.2. Zarządzanie funkcjonalnością VPN:

10.5.2.1. narzędzia do konfiguracji sieci VPN,

10.5.2.2. zarządzanie sieciami VPN,

10.5.2.3. definiowanie QoS i routingu dla VPN,

10.5.3. Zbieranie i wyświetlania zdarzeń bezpieczeństwa w sieci

10.5.3.1. wsparcie dla wiadomości syslog pochodzących od ścian ogniowych,

10.5.3.2. widoki zdarzeń dla ścian ogniowych i sieci VPN,

10.5.3.3. tworzenie raportów dotyczących sytuacji w sieci,

10.6. Funkcjonalność konsoli IPS

10.6.1. Platforma zarządzająca musi być oparta na dedykowanym, uodpornionym (ang. hardened) systemie operacyjnym.

10.6.2. Platforma zarządzająca musi być centralnym punktem, z którego możliwe jest zarządzanie wszystkimi urządzeniami.

10.6.3. Platforma zarządzająca musi umożliwiać agregację wszystkich zdarzeń IDS/IPS oraz centralne monitorowanie i analizę działającą w czasie rzeczywistym.

10.6.4. Platforma zarządzająca musi być dostępna przez interfejs WEB, bez potrzeby instalacji dodatkowego oprogramowania klienckiego.

10.6.5. Konsola zarządzająca musi zapewniać interfejs, który może zostać dostosowany do wymagań użytkownika, w szczególności administrator musi posiadać możliwość definiowania widoków (dashboard), które spełniają jego indywidualne kryteria

10.6.6. Konsola zarządzająca musi mieć możliwość konfigurowania limitu powtórzeń danego zdarzenia w określonym czasie zanim zostanie wygenerowany alarm.

10.6.7. Konsola zarządzająca musi mieć możliwość automatycznej konfiguracji pobierania zestawów sygnatur na najnowsze zagrożenia i podatności. Musi istnieć możliwość informowania o zmianach w pakietach z nowymi sygnaturami/regułami.

10.6.8. Konsola zarządzające musi zapewniać zarządzanie oparte o role, gdzie każdy z użytkowników systemu może mieć różne widoki interfejsu oraz różne możliwości konfiguracyjne w zależności od roli, do której został przypisany.

10.6.9. Konsola zarządzająca musi zapewniać funkcjonalność typu harmonogram zadań umożliwiającą automatyczne uruchamianie rutynowych czynności administracyjnych takich jak kopie zapasowe, uaktualnienia, tworzenie raportów, stosowanie polityk bezpieczeństwa oraz automatyczne dostrajanie polityki IPS.

10.6.10. Konsola zarządzająca musi zapewniać więcej niż jedną predefiniowaną politykę bezpieczeństwa w celu ułatwienia wdrożenia systemu.

10.6.11. Konsola zarządzająca musi zapewniać grupowanie urządzeń i polityk w celu ułatwienia zarządzania konfiguracją.

10.6.12. Konsola zarządzająca musi zapewniać przeglądanie, włączanie oraz wyłączanie zarówno indywidualnych reguł jak i grup oraz kategorii reguł.

10.6.13. Konsola zarządzająca musi mieć możliwość przechowywania atrybutów hostów definiowanych przez użytkownika takich jak jego krytyczność tak aby ułatwić czynności monitorowania sieci.

10.6.14. Konsola zarządzająca musi pozwalać na dogłębne wykorzystanie informacji kontekstowych (takich jak informacje o konfiguracji, zachowaniu sieci i hostów) w celu poprawienia efektywności i dokładności procesu manualnej i automatycznej analizy incydentów.

10.6.15. Oferowane rozwiązanie musi dawać możliwość znaczącej redukcji nakładów operacyjnych oraz przyśpieszać reakcję na zagrożenia poprzez automatyczną priorytetyzację alarmów w oparciu o korelację zagrożeń ze skutecznością ataku na docelowego hosta.

10.6.16. Oferowane rozwiązanie musi mieć możliwość dynamicznego dostrajania systemu IDS/IPS przy zachowaniu minimalnej interwencji administratora poprzez

10.6.16.1. selekcję reguł,

10.6.16.2. zmianę konfiguracji polityki,

10.6.16.3. uaktualnianie polityki, itp.

10.6.17. Konsola zarządzająca musi zapewnić możliwość automatycznego uaktualniania reguł publikowanych przez producenta, automatyczną dystrybucję i stosowanie reguł na urządzeniach IPS.

10.6.18. Konsola zarządzająca musi zapewnić możliwość wykonywania i odtwarzania kopi zapasowych zarówno urządzeń IPS jak i platformy zarządzającej.

10.6.19. Konsola zarządzająca musi zapewnić funkcjonalność pozwalającą na zarządzanie cyklem życia incydentu, od początkowego powiadomienia poprzez odpowiedzi, aż do rozwiązania.

10.6.20. Konsola zarządzająca musi zapewnić możliwość wglądu w reguły, które wygenerowały dany incydent oraz powiązanego z nim pakietu.

10.6.21. Konsola zarządzająca musi zapewnić różne możliwości automatycznej odpowiedzi na zagrożenia – nie mniej niż:

10.6.21.1. alarmy,

10.6.21.2. rekonfiguracja zapory ogniowej,

10.6.21.3. rekonfiguracja routera.

10.6.22. Konsola zarządzająca musi zapewnić możliwość przechowywania incydentów, logów oraz innych informacji generowanych przez system zarówno w wewnętrznej bazie danych jak i posiadać możliwość udostępniania do zabezpieczonego wglądu w te informacje zewnętrznym aplikacjom raportującym w trybie ‘tyko do odczytu’.

10.6.23. Konsola zarządzająca musi zapewnić możliwość synchronizowania czasu pomiędzy wszystkimi komponentami przez protokół NTP.

10.6.24. Konsola zarządzająca musi zapewnić możliwość logowania wszystkich czynności wykonywanych przez administratora zarówno lokalnie jak i na zdalnym serwerze.

10.6.25. Rozwiązanie musi zapewniać logowanie przy użyciu zewnętrznego serwera LDAP zarówno do urządzeń IPS, jak i konsoli zarządzającej.

10.6.26. Konsola zarządzająca musi zapewnić duże możliwości generowania raportów włączając w to raporty predefiniowane oraz możliwość kompletnego dostosowania raportów do wymagań użytkownika.

10.6.27. Konsola zarządzania musi posiadać możliwość automatycznej generacji raportów

10.6.27.1. za wybrany okres (np. godzina, dzień, tydzień itp.),

10.6.27.2. dla konkretnego modułu generującego zdarzenia (np. Health (stan urządzeń),

10.6.27.3. dla przepływów ruchu - Flows (statystyki ruchu sieciowego),

10.6.27.4. Audit Log,

10.6.27.5. Compliance (polityka zgodności),

10.6.27.6. Dla wykrytych podatności,

10.6.27.7. Dla zdarzeń związanych z wykrywaniem użytkowników,

10.6.27.8. z importowania nowych paczek sygnatur/reguł, itp.).

10.6.28. Konsola zarządzająca musi posiadać możliwość generowania statystyk dostępnych przez interfejs użytkownika oraz możliwość generowania raportów w różnych formatach (html, pdf, csv) i przesyłania ich e-mailem.

10.6.29. Konsola zarządzająca musi zapewniać informowanie o zagrożeniach poprzez

10.6.29.1. wysłanie e-maila,

10.6.29.2. wyslanie trap SNMP,

10.6.29.3. przesłanie informacji do serwera Syslog,

10.6.29.4. uruchomienie skryptu użytkownika

10.6.29.5. wysłanie informacji do jednego lub kilku rozwiązań typu SIEM poprzez zaszyfrowane łącze,

10.6.30. Konsola zarządzająca musi pozwalać na monitorowanie stanu pracy wszystkich zainstalowanych urządzeń IPS.

10.6.31. Konsola zarządzająca musi posiadać możliwość kreowania i edycji polityk monitorowania stanu pracy wszystkich urządzeń: zarówno konsoli zarządzających jak i urządzeń IPS.

10.6.32. Konsola zarządzania musi pozwalać na gromadzenie logów ze wszystkich obsługiwanych sond IPS.

10.6.33. Konsola zarządzania musi posiadać zaawansowany system przeszukiwania logów pozwalający na przeprowadzanie analizy:

10.6.33.1. aktualnego stanu danego urządzenia,

10.6.33.2. podglądu historii dostępnych zasobów,

10.6.33.3. możliwość eliminacji powtarzających się alarmów (tzw. Black Listing).

10.6.34. System zarządzania musi pozwalać na tworzenie wielu polityk bezpieczeństwa zawierających różne zestawy sygnatur i przydzielania ich do segmentów zdefiniowanych na różnych urządzeniach. Powinny być dostępne dwie opcje podczas instalacji przypisanej polityki:

10.6.34.1. wysłanie polityki tylko do przypisanego urządzenia IPS,

10.6.34.2. wysłanie polityki do każdego z dostępnych urządzeń IPS,

10.6.35. Reguły wykrywające nowo ujawnione zagrożenia i luki muszą być wygenerowane przez dostawcę w przeciągu 48 godzin od ich ogłoszenia. Zamawiający uzna też rozwiązanie za spełniające wymaganie jeżeli reguły te będą wygenerowane przed dostawcę dla krytycznych zagrożeń podczas gdy regularne uaktualnienia baz sygnatur odbywać się będą nie rzadziej niż co 2 tygodnie.

10.6.36. Reguły wykrywania zagrożeń muszą mieć możliwość modyfikacji i rozszerzenia, muszą być oparte na ogólnodostępnym języku składni tak, aby użytkownicy mogli tworzyć je samodzielnie lub edytować te dostarczane przez producenta systemu.

10.6.37. Reguły dostarczone przez producenta muszą być należycie udokumentowane, z pełnymi opisami własności, pochodzenia oraz istotności blokowanych ataków i zagrożeń.

10.6.38. Konsola zarządzająca musi posiadać mechanizm konfiguracji wielkości poszczególnych baz danych w zależności od rodzaju logowanego zdarzenia wedle wymagań administratora.

10.6.39. Polityki definiowane przez konsolę zarządzającą muszą posiadać historię zmian wraz z informacją o:

10.6.39.1. Osobie/administratorze modyfikującym politykę,

10.6.39.2. Czasie modyfkacji polityki,

10.6.39.3. Informacji porównawczej danej polityki z politykami wstecznymi (definiowanymi wcześniej),

10.6.40. Konsola zarządzająca musi posiadać możliwość porównywania odrębnych polityk IPS w formie raportu.

10.6.41. Konsola zarządzająca musi posiadać możliwość eksportowania dostępnych ustawień i polityki w formie paczek konfiguracyjnych dostępnych w odrębnych plikach.

10.6.42. Konsola zarządzająca musi zapewniać tworzenie profilu ruchu sieciowego w normalnych warunkach (tzw. profil podstawowy) wykorzystując różne technologie analizy przepływów (np. NetFlow) i możliwość wykrycia odchylenia od profilu podstawowego (funkcjonalność Analizy Zachowania w Sieci - AZwS).

10.6.43. Funkcjonalność AZwS musi przedstawiać sposób wykorzystania pasma sieciowego w celu ułatwienia wykrywania przeciążeń i przestojów urządzeń sieciowych.

10.6.44. Funkcjonalność AZwS musi zapewniać możliwość gromadzenia informacji o węzłach końcowych (np. serwerach, stacjach roboczych) w celu zapewnienia korelacji ze zdarzeniami bezpieczeństwa. Korelacja ma na celu umożliwienie priorytetyzacji zdarzeń bezpieczeństwa.

10.6.45. Urządzenia sieciowe, na których uruchomiony jest system IPS muszą być zapewniać jednocześnie funkcjonalność AZwS. Funkcjonalność AZwS nie może wymagać instalacji dodatkowych urządzeń.

10.6.46. Konsola zarządzająca do system IPS musi być również wykorzystywana do zarządzania funkcjonalnością AZwS. Zarządzanie AZwS nie może wymagać instalacji dodatkowej konsoli zarządzającej.

10.6.47. Oferowane rozwiązanie musi mieć możliwość ustanawiania i wymuszania polityki zgodności jak i alarmowania w przypadku jej naruszeń w czasie rzeczywistym.

10.6.48. Oferowane rozwiązanie musi mieć możliwość wykluczania poszczególnych hostów z polityk zgodności oraz blokowania odpowiednich zdarzeń i alarmów dla tych właśnie hostów.

10.6.49. Oferowane rozwiązanie musi posiadać możliwość łatwej identyfikacji wszystkich hostów, które posiadają dany atrybut lub nie spełniają zadanych warunków polityki zgodności.
10.6.50. Całość komunikacji pomiędzy poszczególnymi komponentami systemu IPS musi być zabezpieczona protokołem kryptograficznym.
10.6.51. Platforma musi mieć możliwość uruchomienia funkcji nowej generacji zapory ogniowej, URL filtering, kontroli plików za pomocą dodatkowej licencji.
10.6.52. Konsola musi umożliwiać skonfigurowanie i utrzymanie polityki dostępu zapory ogniowej i instrumentów oraz polityk IPS.
10.6.53. Konsola musi prowadzić przegląd wszystkich zdarzeń związanych z bezpieczeństwem pod kątem analizy powłamaniowej i wczesnej prewencji włamań.
10.6.54. Konsola musi umożliwiać dostrajanie polityki bezpieczeństwa do specyfiki monitorowanych segmentów sieciowych oraz zarządzanie setkami urządzeń monitorujących.
10.6.55. Użytkownik obsługujący konsolę zarządzającą musi mieć możliwość
10.6.55.1. ustawienia i wykorzystania automatycznych rekomendacji strojenia polityki
10.6.55.2. zapobiegania zagrożeń IPS opartych na wiedzy kontekstowej o:
10.6.55.2.1. sieci,
10.6.55.2.2. użytkownikach,
10.6.55.2.3. systemach operacyjnych,
10.6.55.2.4. usługach i aplikacjach,
10.6.55.2.5. charakterystyce sesji ruchu sieciowego, które mają być chronione.
10.6.56. System zarządzania musi mieć możliwość integrowania się z rozwiązaniami firm trzecich typu Vulnerabilitity Scanner/Vulnerability Management, dostarczających dodatkowych informacji na temat luk i podatności istniejących w monitorwanych środowiskach w celu bardziej precyzyjnego szacowania skutków zagrożeń oraz automatycznego procesu strojenia polityki modułu IPS.
10.6.57. Platforma musi mieć otwarty i rozszerzalny mechanizm zapobiegania zagrożeniom oraz możliwość definiowania własnych detektorów aplikacji.
10.6.58. Rozwiązanie powinno mieć możliwość przypisywania następujących parametrów w polityce kontroli dostępu dla danych interfejsów, podsieci, vlanów i użytkowników:
10.6.58.1. dozwolone porty i protokoły,
10.6.58.2. dozwolone aplikacje według różnych kategorii,
10.6.58.3. dozwolone kategorie stron internetowych (URL filtering),
10.6.58.4. dedykowaną politykę wykrywania zagrożeń IPS dla każdej z reguł zapory ogniowej,
10.6.58.5. sposób traktowania wyspecyfikowanego ruchu w danej regule: przepuszczanie bez analizy, analiza, blokowanie ciche, blokowanie z resetowaniem sesji, blokowanie interaktywne.
10.6.59. Rozwiązanie musi zapewiać usługę dynamicznej reputacji znanych adresów IP propagujących zagrożenia w sieci Internetowej oraz możliwość definiowania własnych, zewnętrznych źródeł informacji. Adresy te powinny być blokowane jako znane zagrożenia i kategoryzowane w między innymi następujący grupy, według typu stwarzanego zagrożenia:
10.6.59.1. Attackers,
10.6.59.2. Bogon,
10.6.59.3. Bots,
10.6.59.4. CNC,
10.6.59.5. Malware,
10.6.59.6. Open_proxy,
10.6.59.7. Open_relay,
10.6.59.8. Phishing,
10.6.59.9. Tor_exit_node,
10.6.60. W ramach funkcji kategoryzacji zapytań HTTP (URL filtering) rozwiązanie musi mieć możliwość interaktywnego blokowania z resetowaniem zapytań. W ramach tej funkcji musi zostać zapewniona możliwość zdefiniowania własnej strony internetowej ostrzegającej o naruszeniu polityki kontroli dostępu i zrzuceniu zablokowanej próby połączenia.
10.6.61. Konsola zarządzające musi zapewniać obsługę zdalneucj uaktualniań, wykonywania kopii zapasowych oraz przywracania jak i funkcjonalność odinstalowywania uaktualnień bez konieczności fizycznego dostępu do urządzenia.
10.7. Wydajność i sposób realizacji konsoli zarządzania FW/IPS

10.7.1. Konsola zarządzania musi być dostępna w co najmniej dwóch postaciach pozwalających Zamawiającemu na swobodny dobór właściwego narzędzia zarządzania:
  10.7.1.1. w formie tradycyjnych urządzeń fizycznych,
  10.7.1.2. jako maszyna wirtualna przy czym w tej wersji musi posiadać tożsame funkcje z konsolą w postaci urządzenia fizycznego (nie dotyczy to funkcji wymagajacych obecności dedykowanych układów ASIC).
10.7.2. Konsola zarządzania musi zostać zaoferowana w postaci dedykowanego urządzenia wraz z oprogramowaniem,
10.7.3. Konsola zarządzania musi posiadać odpowiednią wydajność pozwalającą na obsłużenie 14 urządzeń IPS oraz docelowo na obsłużenie nie mniej niż 50 systemów/sond IPS,
10.7.4. Konsola zarządzania musi posiadać odpowiednią przestrzeń dyskową pozwalającą na gromadzenie informacji – wymagane jest zapewnienie co najmniej 1,5TB pojemności,
10.7.5. Konsola zarządzania musi pozwalać na obsłużenie minimum 50 000 hostów i 100 000 urządzeń dołączonych do sieci – zapewniając pokrycie dla całośći infrastruktury Zamawiającego
10.7.6. Konsola zarządzająca musi być przygotowana do ciągłej obsługi nie mniej niż 10 000 zdarzeń na sekundę
10.7.7. Konsola zarządzająca musi zapewniać możliwość przechowania co najmniej 50 milionów zdarzeń IPS
10.7.8. Funkcjonalności opcjonalne:
  10.7.8.1. Konsola zarządzająca z macierzą dysków z systemem RAID 5.
  10.7.8.2. Konsola zarządzająca z możliwością połączenia urządzenia z drugim takim samym w celu uzyskania klastra wysokiej dostępności.

11. Oprogramowanie

Głównym celem niniejszego postępowania jest zwiększenie bezpieczeństwa przetwarzanych danych oraz zapewnienie większej dostępności oraz skalowalności poprzez między innymi zwirtualizowanie obecnego środowiska i rozdzielenie infrastruktury na ośrodki COO i ZCOO.

Oprogramowanie wirtualizacyjne- wymagania

11.1. Warstwa wirtualizacji musi być rozwiązaniem systemowym tzn. musi być zainstalowana bezpośrednio na sprzęcie fizycznym.
11.2. Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i musi się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
11.3. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością dostępu do min. 255GB pamięci operacyjnej.
11.4. Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych w zakresie od 1- do 24-procesorowych, co 1 procesor.
11.5. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11.6. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
11.7. Rozwiązanie musi wspierać następujące systemy operacyjne: Windows XP, Windows Vista , Windows 7, Windows 10, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 R2, SLES 10, SLES9, SLES8, Ubuntu 7.04, RHEL 5, RHEL 6, RHEL7, Solaris wersja 10 dla platformy x86, NetWare 6.5, NetWare 6.0, NetWare 6.1, Debian, CentOS, FreeBSD, Asianux, SCO OpenServer, SCO Unixware.
11.8. Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji. Rozwiązanie musi zawierać mechanizmy kompresji pamięci fizycznej RAM.
11.9. Oprogramowanie do wirtualizacji musi mieć możliwość mapowania urządzeń podłączonych przez USB do maszyn wirtualnych z zachowaną możliwością przenoszenia tych maszyn pomiędzy serwerami fizycznymi.

11.10. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i usługami.
11.11. Rozwiązanie musi zapewnić możliwość monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej.
11.12. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
11.13. Oprogramowanie do wirtualizacji musi zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
11.14. Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
11.15. Oprogramowanie zarządzające musi posiadać możliwość przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi Microsoft Active Directory.
11.16. Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej z dwóch ścieżek.
11.17. Oprogramowanie do wirtualizacji musi zapewnić możliwość ograniczenia i priorytetyzowania wydajności podsystemu dyskowego, kontrolę ilości wykonywanych operacji dyskowych na poziomie pojedynczej wirtualnej maszyny i grupy maszyn.
11.18. Platforma wirtualizacyjna musi umożliwiać wykorzystanie procesorów fizycznych do 18 rdzeni na procesor.
11.19. Platforma wirtualizacyjna musi obsługiwać karty HBA o przepustowości 8GB.
11.20. Platforma wirtualizacyjna musi zapewnić możliwość startu systemu poprzez sieć SAN za pomocą protokołów FC, iSCSI i FCoE.
11.21. Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych aniżeli fizycznie zarezerwowane.
11.22. System musi umożliwiać tworzenie standardowej konfiguracji dla hostów i zautomatyzowanie zgodności dla tych konfiguracji.
11.23. System musi posiadać funkcjonalność wirtualnego przełącznika (switch) umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Przełączniki wirtualne muszą mieć możliwość konfiguracji 2040 portów.
11.24. System musi umożliwiać podłączenie wirtualnych przełączników firm trzecich.
11.25. System musi zapewniać możliwość nadawania priorytetów różnym rodzajom ruchu sieciowego (ruch generowany przez wirtualne maszyny, ruch generowany przez system do wirtualizacji)
11.26. Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi.
11.27. Rozwiązanie musi zapewnić ciągłą pracę usług. Usługi krytyczne biznesowo muszą działać bez przestoju, czas niedostępności innych usług musi nie przekraczać kilkunastu minut.
11.28. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały przełączone na inne serwery infrastruktury.
11.29. Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury.
11.30. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania.
11.31. Rozwiązanie musi zapewniać mechanizm bezpiecznego uaktualniania warstwy wirtualizacyjnej, hostowanych systemów operacyjnych (np. wgrywania patch-y) i aplikacji tak aby zminimalizować ryzyko awarii systemu na skutek wprowadzenia zamiany.
11.32. Rozwiązanie musi zapewnić możliwość szybkiego wykonywania kopii zapasowych oraz odtwarzania usług. Proces ten musi nie mieć wpływu na utylizację zasobów fizycznych infrastruktury wirtualnej.
11.33. Rozwiązanie musi umożliwiać tworzenie, testowanie i uruchamianie planów odtworzenia ośrodka przetwarzania danych po awarii, nie powodując przerwy w pracy środowiska produkcyjnego. Narzędzie musi, integrować się z istniejącymi rozwiązaniami do replikacji danych na poziomie wykorzystywanych macierzy.

11.34. Rozwiązanie musi zapewniać pracę bez przestojów dla wybranych maszyn wirtualnych, niezależnie od systemu operacyjnego oraz aplikacji, podczas awarii serwerów fizycznych, bez utraty danych i dostępności danych podczas awarii serwerów fizycznych.

11.35. Rozwiązanie musi umożliwiać dodawanie i rozszerzanie dysków wirtualnych, procesorów i pamięci RAM podczas pracy wybranych systemów.

11.36. System musi umożliwiać kontrole dostępu sieciowego do obszarów wrażliwych wirtualnego centrum danych takiego jak DMZ lub serwery z danymi wrażliwymi podlegające zgodności z przepisami PCI lub SOX w obszarze środowiska wirtualnego.

11.37. Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Pożądana jest możliwość przenoszenia usług pomiędzy serwerami fizycznymi oraz wolumenami dyskowymi, bez przerywania pracy usług.

11.38. Rozwiązanie musi umożliwiać automatyczne równoważenie obciążenia serwerów fizycznych pracujących jako platforma dla infrastruktury wirtualnej.

11.39. Rozwiązanie musi zapewnić możliwość szybkiego tworzenia i uruchamiania nowych usług wraz z ich pełną konfiguracją i preinstalowanymi narzędziami systemowymi w celu efektywnej obsługi wymagań biznesowych.

11.40. Rozwiązanie musi zapewnić mechanizm wykonywania kopii – klonów systemów operacyjnych wraz z ich pełną konfiguracją i danymi.

Oprogramowanie serwerowe dla PUE.

Realizując cel rozproszenia i zwielokrotnienia środowisk PUE, czyli środowisko produkcyjne COO i ZCOO, obszar testów składający się z środowiska testowego, przedprodukcyjnego, developerskiego o konfiguracjach nie gorszych niż obecne środowisko produkcyjne i testowe – Tabela nr 3, 4, 5, 6 należy dostarczyć oprogramowanie oraz licencje/subskrypcje które pozwolą to zrealizować. Zamawiający wymaga rozbudowy oprogramowania o dodatkowe licencje/subskrypcje posiadanych rodzajów oprogramowania zamieszczonych w poniższej tabeli.

11.41. Wymagania minimalne na oprogramowanie dla PUE celem rozproszenia i zwielokrotnienia środowisk.

Tabela nr 7 Zestawienie oprogramowania serwerowego dla PUE

LP	Nazwa licencji/ subskrypcji[1]	Ilość licencji (minimum)
1.	Oprogramowanie wirtualizacyjne (CPU)	40
2.	Oprogramowanie wirtualizacyjne (CPU) Vmware vSphere Standard[4]	16
3.	Microsoft Windows Server 2012R2 Standard z możliwością downgrade do Microsoft Windows Server 2008	4[5]
4.	Microsoft SQL Server 2014 Standard z możliwością downgrade do Microsoft SQL Server 2008 R2 Standard	4[5]
5.	Red Hat Enterprise Linux for Virtual Datacenters, Standard	20
6.	Red Hat Enterprise Linux Server, Standard	8
7.	Postgres Plus Enterprise Edition 3 Year Unlimited License Agreement	1 bez limitu na core
8.	Red Hat JBoss Enterprise Application Platform with Management, 64 Core Standard[3]	3
9.	WebMethods	różne rodzaje[2]

[1] lub oprogramowanie równoważne o funkcjonalności nie mniejszej niż oprogramowanie wymienione w tabeli.
[2] zakres zależny od rodzaju zaproponowanych procesorów na platformie serwerowej
[3] ZUS posiada subskrypcje na 96 corów
[4] ZUS posiada 16 wolnych licencji typu upgrade z Vmware vSphere Standard do Vmware vSphere Enterprise Plus
[5] licencje na nowe serwery dla środowiska produkcyjnego (ośrodek zapasowy) oraz dwa środowiska testowe

11.42. Jeśli na wyżej wymienione oprogramowanie jest ograniczenie czasowe to oferent zobowiązany jest zapewnić licencje/subskrypcje na okres 3 lat.

12. Usługa wdrożenia i szkolenia.

12.1. Wymaga się następujących usług w zakresie instalacji i konfiguracji:

12.1.1. Instalacji fizycznej sprzętu w dostarczonych szafach RACK (montaż, podłączenie zasilania, podłączenie do sieci LAN i SAN - wykonawca zapewnia okablowanie podłączeniowe oraz patchcordy).

12.1.2. Konfiguracji dostarczonego sprzętu zgodnie z wymaganiami Zamawiającego. Wykonawca musi dostarczyć odpowiedne wkładki SFP/ SFP+ w ilości zgodnej z zaproponowanym rozwiązaniem.

12.1.3. Instalacji dostarczonego oprogramowania.

12.1.4. Konfiguracja systemów operacyjnych w zakresie prawidłowego włączenia ich do aktualnie eksploatowanych środowisk Zamawiającego.

12.1.5. Instalacja i konfiguracja dostarczonego w ramach zamówienia oprogramowania narzędziowego w zakresie prawidłowego włączenia ich do aktualnie eksploatowanych środowisk Zamawiającego.

12.1.6. Wirtualizacja istniejących systemów operacyjnych wraz z aplikacją na platformę wirtualizacją dostarczoną w niniejszym postępowaniu.

12.1.7. Instalacja ma się odbywać w terminach ustalonych z Zamawiającym, a samo przełączenie z obecnego środowiska na nowy system musi odbyć się w przerwie technologicznej.

12.2. Powyższe przekłada się na następujący zestaw wymaganych usług wdrożeniowych – dla każdego z wymienionych powyżej etapów (punkty 12.1.1 do 12.1.6) wymagane jest dostarczenie projektu technicznego i implementacyjnego, przeprowadzenie wdrożenia, testy akceptacyjne, przygotowanie dokumentacji powdrożeniowej:

12.2.1. Konfiguracja maszyn wirtualnych środowisk produkcyjnych dla przygotowania pod wprowadzenie do pakietów klastra rozległego;

12.2.2. Konfigurację dodatkowych przestrzeni dyskowych, w tym również kopii wewnątrz macierzowych dla wybranych obszarów danych;

12.2.3. Rekonfiguracja środowiska klastra rozległego, wykorzystującego replikację między macierzową w tym konfiguracja replikacji między macierzowej.

12.3. Dodatkowo wymagane jest przeprowadzenie:

12.3.1. Modernizacja i rekonfiguracja sieci SAN pod kątem: podłączenia nowych portów FC,

12.3.2. Modernizacja i rekonfiguracja rozwiązania backupowego opartego o rozwiązanie posiadane przez Zamawiającego (HP Data Protector).

12.4. Wymagane jest dostarczenie / aktualizacja dokumentacji technicznej.

12.5. Utworzona dokumentacja techniczna rozwiązania musi zawierać w szczególności:

12.5.1. Projekt przedwdrożeniowy infrastruktury techniczno-systemowej.

12.5.2. Dokumentację techniczną powykonawczą modernizacji infrastruktury techniczno-systemowej.

12.5.3. Uaktualnienia innych projektów technicznych i dokumentacji w zakresie wprowadzonej zmiany – aktualizacja modelu projektowego PUE utrzymywanego w Enterprise Architect (Sparx).

12.5.4. Procedur administracyjnych (zgodnie z szablonem Zamawiającego), wraz z dodatkowymi narzędziami wspomagającymi, niezbędnych do utrzymania systemu.

12.5.5. Dokumenty będące produktami w ramach zamówienia muszą:

12.5.5.1. Posiadać określoną strukturę tzn. tworzone dokumenty będą zawierały metrykę dokumentu oraz będą podzielone na rozdziały, podrozdziały i sekcje w czytelny i przejrzysty sposób,

12.5.5.2. Posiadać spójną strukturę, formę i sposób pisania, aby nie powodowały wątpliwości interpretacyjnych,

12.5.5.3. Być kompletne tzn. stworzona dokumentacja będzie pełna, obejmująca całość z danego zakresu rozpatrywanego

12.5.5.4. Zagadnienia, bez ewidentnych braków,

12.5.5.5. Być spójne i niesprzeczne tzn. Wykonawca będzie czuwał nad zgodnością pomiędzy wszystkimi informacjami umieszczonymi w dokumencie a także nad logicznością informacji zwartych we wszystkich przekazanych dokumentach oraz we fragmentach tego samego dokumentu.

12.5.6. Zamawiający wymaga, aby stworzona dokumentacja była dostarczona zgodnie z następującymi wymaganiami:

12.5.6.1. w języku polskim, w wersji elektronicznej, w formacie Microsoft Word (na płycie CD-ROM lub DVD) i/lub drukowanej, co najmniej w 1 egzemplarzu z tym, że rodzaj wersji (elektronicznej i/lub papierowej) Zamawiający może określić osobno w stosunku do każdego z dokumentów, w przypadku wprowadzania zmian do wcześniej przekazanych bądź udostępnionych Zamawiającemu dokumentów.

12.5.6.2. Wykonawca dostarczy nowe dokumenty również w takim formacie, w którym zmiany te są wyraźnie widoczne w tekście (format Microsoft Word, w trybie rejestracji zmian).

12.5.6.3. Wykonawca przekazuje Zamawiającemu majątkowe prawa autorskie do wytworzonej dokumentacji.

12.6. Wykonawca musi przeprowadzić testy infrastruktury zgodnie z opracowanymi scenariuszami testowymi potwierdzającymi między innymi zgodność wdrożonego rozwiązania z wymaganiami opisanymi w Opisie Przedmiotu Zamówienia oraz testami sprawdzającymi poprawność konfiguracji wdrożonego rozwiązania pod względem równoważenia obciążenia sieciowego Wyniki przeprowadzonych testów muszą być potwierdzone raportami z testów.

12.7. Przeprowadzenie szkolenia do 15 osób w zakresie eksploatacji i konfiguracji zmodernizowanej infrastruktury dla PUE.

12.8. Przeprowadzenie szkoleń z każdego zakresu tematycznego wymienionego poniżej dla 3 osób. Przeprowadzenie szkoleń przez autoryzowany ośrodek szkoleniowy producenta sprzętu i/lub oprogramowania będzie dodatkowo punktowane.

12.8.1. Zakresy tematyczne szkoleń:

12.8.1.1. Konfiguracja i zarządzanie siecią SAN,

12.8.1.2. Balansowanie ruchu sieciowego,

12.8.1.3. Przełączanie ruchu wewnątrz infrastruktury PUE (technologia Data Center Interconnect),

12.8.1.4. Zarządzanie dostarczonym systemem bezpieczeństwa:

12.8.1.4.1. Firewall,

12.8.1.4.2. IPS,

12.8.1.4.3. antywirus/antymalware.

12.8.1.5. Zarządzanie i konfiguracja platformy serwerowej,

12.8.1.6. Platforma wirtualizacyjna.

12.8.1.7. Zarządzanie i konfiguracja macierzy.

12.8.2. Szkolenia muszą się odbywać w języku polskim.

13. Gwarancja (usługi serwisu gwarancyjnego)

13.1. Wymagane jest, aby usługi serwisu gwarancyjnego świadczone były przez producenta lub autoryzowanego partnera serwisowego producenta w zakresie:

13.1.1. Gwarancja na sprzęt i/lub oprogramowanie wynosi 36 miesięcy od daty podpisania bez zastrzeżeń Protokołu Odbioru.

13.1.2. Dostęp do poprawek i aktualizacji oprogramowania przez 36 miesięcy od daty Protokołu Odbioru.

13.1.3. Dostępność wsparcia serwisowego 24 godziny na dobę, 7 dni w tygodniu.

13.1.4. Rozwiązywanie problemów ze sprzętem i oprogramowaniem.

13.1.5. Dostęp do centrów kompetencyjnych Producenta.

13.1.6. Usługi serwisu gwarancyjnego świadczone w siedzibie Zamawiającego.

13.1.7. W przypadku awarii nośnika danych (dysk twardy) Zamawiający zatrzymuje uszkodzony nośnik i wymaga dostarczenia nowego nośnika od Wykonawcy.

13.1.8. Naprawa sprzętu w gwarantowanym czasie wynikającym ze statusu zgłoszenia, liczonym od momentu zgłoszenia awarii. Status zgłoszenia określa Zamawiający.

13.1.9. Natychmiastowy czas reakcji dla zgłoszeń ze statusem krytycznym, tj. nie dłuższy niż 1 godzina (Zamawiający decyduje o klasyfikacji zgłoszenia jako krytyczne). Czas reakcji rozumiany jest jako przesłanie do Zamawiającego wstępnego planu działań serwisowych.

13.1.10. Wymagany jest dedykowany zespół serwisowy po stronie Wykonawcy, składający się z minimum 5 osób w tym jednego koordynatora kontraktu serwisowego oraz minimum 4 ekspertów technicznych w zakresie oferowanych technologii.

13.1.11. Zamawiający ma prawo do konsultacji zdalnych z zespołem serwisowym bez ograniczeń w czasie trwania wsparcia serwisowego.

13.1.12. W terminie 14 dni od dnia podpisania bez zastrzeżeń protokołu odbioru wdrożenia wymagane jest przygotowanie Planu Obsługi Serwisowej opisującego procedury serwisowe i eskalacyjne, zespół serwisowy, ścieżki komunikacji serwisowej jak również harmonogram prac serwisowych.

13.1.13. Wymaga się wykonywania cyklicznych przeglądów systemów i konfiguracji oraz dokonywanie analizy oprogramowania wbudowanego i systemowego – co najmniej raz na 3 miesiące trwania gwarancji z zastrzeżeniem, że ostatni przegląd musi odbyć się w 35 miesiącu trwania gwarancji.

13.1.14. W przypadku opublikowania nowej wersji oprogramowania wbudowanego i systemowego wymaga się wykonania instalacji uaktualnień w terminach uzgodnionych z Zamawiającym.

13.1.15. Wymaga się wykonania cyklicznej weryfikacji poziomu dostępności systemu, – co najmniej raz na 12 miesięcy trwania gwarancji z zastrzeżeniem że ostatnia weryfikacja musi odbyć się w 35 miesiącu trwania gwarancji.

13.1.16. Wymaga się wykonania cyklicznej analizy warunków eksploatacyjnych, – co najmniej raz na 12 miesięcy trwania gwarancji z zastrzeżeniem że ostatnia analiza musi odbyć się w 35 miesiącu trwania gwarancji.

13.1.17. Wymaga się dostarczania miesięcznych raportów dotyczących zgłoszeń serwisowych oraz wykonanych prac serwisowych.

13.1.18. Zamawiający ma prawo do nieodpłatnych konsultacji technicznych w siedzibie Zamawiającego w wymiarze max 100 godzin w roku.

13.1.19. Usługi serwisu gwarancyjnego zgłaszane będą za pośrednictwem posiadanego przez Zamawiającego systemu HP Service Manager.

Załącznik nr 2 do Umowy ……(TZ/271/79/15)

Formularz ofertowy (*zgodnie z ofertą wybranego Wykonawcy*)

Załącznik nr 3 do Umowy ……(TZ/271/79/15)

PROTOKÓŁ CZĄSTKOWY ODBIORU

W dniu....., w lokalizacji Zamawiającego ……..., ul. ……..,
komisja w składzie:

1. .....
2. .....

na podstawie Umowy nr …….

A. dokonała odbioru urządzeń:

1. ……

(model, nr seryjny, data produkcji)

2. ……

(model, nr seryjny, data produkcji)

……

i oprogramowań:

1. ……

(producent, nazwa oprogramowania)

2. …….

(producent, nazwa oprogramowania)

……

B. Wykonawca:

B.1.- przekazał / nie przekazał* Zamawiającemu karty gwarancyjne urządzeń, o których mowa w punkcie A niniejszego protokołu w ilości ..... szt;

B.2.- przekazał / nie przekazał* Zamawiającemu dokumenty licencyjne uprawniające Zamawiającego do korzystania z oferowanego oprogramowania, o których mowa w punkcie A protokołu w ilości ..... szt.

B.3.- Wykonawca przekazał / nie przekazał* Zamawiającemu projekt instalacji i konfiguracji urządzeń oraz oprogramowania wraz z harmonogramem czasowym, w ilości ..... szt.

C. Wykonawca wykonał instalację i konfigurację/nie wykonał instalacji i konfiguracji* urządzeń i oprogramowania, będących przedmiotem Umowy.

Przedstawiciele Zamawiającego przyjęli bez zastrzeżeń* wykonanie wymienionych wyżej elementów składających się na dostawę oraz instalację i konfigurację urządzeń oraz oprogramowania będących przedmiotem Umowy / nie przyjęli* wykonania wymienionych wyżej elementów składających się na dostawę oraz instalację i konfigurację urządzeń i oprogramowania będących przedmiotem Umowy ze względu na:

.....
.....

* niepotrzebne skreślić

Przedstawiciele Zamawiającego: Przedstawiciele Wykonawcy:

....

Załącznik nr 4 do Umowy nr ……(TZ/271/79/15)

PROTOKÓŁ KOŃCOWY ODBIORU WDROŻENIA

W dniu ....., w siedzibie Zamawiającego w Warszawie, ul. …….., komisja w składzie:

1. .....
2. .....
3. .....

dokonała odbioru dostawy oraz instalacji i konfiguracji urządzeń oraz oprogramowania łącznie z dokumentami licencyjnymi, będących przedmiotem Umowy nr …….

W trakcie odbioru:

1. Stwierdzono / nie stwierdzono* wykonanie dostawy urządzeń i oprogramowania (na podstawie protokołów cząstkowych odbioru).
2. Stwierdzono / nie stwierdzono* wykonanie instalacji i konfiguracji urządzeń i oprogramowania (na podstawie Protokołów cząstkowych odbioru).
3. Wykonawca przekazał / nie przekazał* Zamawiającemu dokumentację powykonawczą, zgodnie z §3 ust. 5 Umowy, w ilości ..... szt., w formie .....
4. Wykonawca przekazał / nie przekazał * Zamawiającemu Plan Obsługi Serwisowej opisujący procedury serwisowe i eskalacyjne, zespół serwisowy, ścieżki komunikacji serwisowej jak również harmonogram prac serwisowych,

Przedstawiciele Zamawiającego przyjęli bez zastrzeżeń* wykonanie wymienionych wyżej elementów składających się na dostawę oraz instalację i konfigurację urządzeń oraz oprogramowania będących przedmiotem Umowy / nie przyjęli* wykonania wymienionych wyżej elementów składających się na dostawę oraz instalację i konfigurację urządzeń i oprogramowania będących przedmiotem Umowy ze względu na:

.....
.....
.....

Uwagi:

.....
.....
.....

* niepotrzebne skreślić

Przedstawiciele Zamawiającego: Przedstawiciele Wykonawcy:

....

Załącznik nr 5 do Umowy ……(TZ/271/79/15)

FORMULARZ ZGŁOSZENIA AWARII

Część A. Wypełnia pracownik Zamawiającego i wysyła na adres e-mail Wykonawcy

Nazwa Wykonawcy **.....**	
Data zgłoszenia __ __ __ __ _____ **(dzień miesiąc rok)**	**Czas zgłoszenia** __ __ __ __ **(godzina, minut)**
Informacja o awarii	
Status zgłoszenia problemu……	
Opis awarii, uszkodzenia lub innych nieprawidłowości:	
Imię i nazwisko osoby zgłaszającej, telefon, fax.	**Podpis osoby zgłaszającej**

Część B. Wypełnia przedstawiciel Wykonawcy ..... odsyła do Zamawiającego na adres poczty elektronicznej - .....

Zgłoszenie przyjął **.....** **Nazwisko i imię**	**Data:** __ __ ___ _____ **(dzień, miesiąc, rok)**	**Czas:** __ __ __ __ **(godzina, minut)**
Uwagi:		
Podpis osoby przyjmującej zgłoszenie **.....**		

Załącznik nr 6 do Umowy …….(TZ/271/79/15)

FORMULARZ WYKONANIA ZGŁOSZENIA SERWISOWEGO

Przyczyna interwencji:	**Data i godzina potwierdzenia otrzymania zgłoszenia:**	**Data i godzina rozpoczęcia usługi serwisowej:**
zgłoszenie z dnia: . . . . . . o godz. . . . . . numer zgłoszenia	Data:…… godz:….....	Data……. godz. . . . .

Wykonawca usługi:

imię i nazwisko: . . . . . .

tel.: . . . . tel. kom. . . . .

Opis czynności serwisowych wraz z wykazem wymienionych podzespołów:

. . . . . .
data i godz. zakończenia

. . . . . .
podpis serwisanta

Oświadczenie serwisanta o podjętych czynnościach i skuteczności usługi:

Odbiorca usługi (przedstawiciel Zamawiającego):

imię i nazwisko: . . . . . .

nazwa jednostki organizacyjnej: . . . . . .

adres: . . . . . .

tel.: . . . . . .

Oświadczenie Odbiorcy usługi - przedstawiciela Zamawiającego - o skuteczności usługi serwisowej:

Oświadczenie Odbiorcy o przyjęciu urządzenia zastępczego / nowego * (należy podać nazwę, model, datę produkcji i numer seryjny urządzenia zastępczego / nowego wraz z podaniem nazwy, modelu i numeru seryjnego urządzenia uszkodzonego).

** niepotrzebne skreślić*

. . . . . .
Ze strony Zamawiającego

. . . . . .
Ze strony Wykonawcy, data

. . . . . .
data i godzina

Załącznik nr 7 do Umowy …….(TZ/271/79/15)

Protokół wykonania przeglądu konserwacyjnego

Przegląd: **1. Systemów i konfiguracji** **2. Poziomu dostępności*** **3. Warunków eksploatacyjnych*** (niepotrzebne skreślić)	**Data i godzina rozpoczęcia Przeglądu:** . . . . . godz. . . . .
Nazwa jednostki organizacyjnej Zamawiającego oraz miejsce wykonania przeglądu: nazwa: . . . . . . adres: . . . . tel.: . . . . . fax:	
Wykonawca usługi: imię i nazwisko: . . . . . . tel.: . . . . . tel. kom.	
Opis przedmiotu przeglądu wraz z oświadczeniem serwisanta o stanie przedmiotu przeglądu: 1 2 3	
Podjęte działania, ewentualne wymienione elementy lub części: . . . . . data i godz. zakończenia	. . . . . podpis serwisanta
Odbiorca usługi (przedstawiciel Zamawiającego): imię i nazwisko: . . . . . . tel.:	
Potwierdzenie wykonania przeglądu oraz ewentualne uwagi Odbiorcy usługi: . . . . . data i godzina	. . . . . pieczątka oraz podpis odbierającego usługę

Załącznik nr 8 do Umowy ……..(TZ/271/79/15)

Szczegółowa procedura odbioru przedmiotu Umowy

1) Wykonawca musi zapewnić, że urządzenia dostarczone w ramach realizacji Umowy będą: sprzętem fabrycznie nowym, pochodzącym z bieżącej produkcji, tj. wyprodukowane nie wcześniej niż 6 miesięcy przed datą zawarcia Umowy, a jednocześnie nie będą urządzeniami, które mogły być używane w innych projektach i poddane procesowi odnowienia *(ang. refurbished),* a także muszą być wolne od wad oraz posiadać pełen zestaw przewidzianych przez producenta właściwych nośników (np. sterowniki).
2) Urządzenia zostaną dostarczone w oryginalnych opakowaniach fabrycznych; informacja o dacie produkcji urządzeń musi znaleźć się w protokole odbioru dla każdego z urządzeń (Protokół cząstkowy odbioru – Załącznik nr 3 do Umowy) wraz z jego numerem seryjnym, modelem. Zamawiający zastrzega sobie prawo do potwierdzenia dat produkcji u producentów zaoferowanego sprzętu.
3) W ramach realizacji przedmiotu Umowy Wykonawca zapewni udzielenie bezterminowych licencji na zaoferowane oprogramowanie na warunkach określonych w dokumencie licencyjnym Producenta oprogramowania, z zastrzeżeniem § 9 Umowy. Urządzenia oraz oprogramowanie wraz z licencjami będą wolne od wad fizycznych i prawnych.
4) Wykonawca oświadcza, że posiada prawo do dysponowania oprogramowaniem dostarczonym wraz z urządzeniami. Wykonawca wraz z urządzeniami przekaże dokument/y potwierdzający/e udzielenie/przekazanie bezterminowej licencji na oprogramowanie (dokument licencyjny).
5) Wszelkie dostawy, odbiory oraz wszelkie czynności związane z przekazaniem Produktów (określonych w ust. 6 poniżej) będą realizowane przez Wykonawcę w dni robocze Zamawiającego, chyba że zostanie to odmiennie ustalone przez Strony.
6) Dla dostawy urządzeń Wykonawca zobowiązany będzie dostarczyć, z wyprzedzeniem minimum 2 dni roboczych Zamawiającego informację zawierającą co najmniej:
   1) Termin dostawy,
   2) Szczegółowy wykaz dostarczanych urządzeń,
   3) Termin wdrożenia.
7) Zastosowanie procedury odbioru przedmiotu Umowy:
   1) odbiór wdrożenia następuje na mocy Protokołu końcowego odbioru wdrożenia, sporządzonego wyłącznie w formie pisemnej wg Załącznika nr 4 do Umowy,
   2) warunkiem niezbędnym końcowego odbioru wdrożenia jest bezwarunkowy odbiór wszystkich jego elementów,
   3) w przypadku potwierdzenia prawidłowości prac, Zamawiający dokona odbioru wdrożenia. Za datę odbioru uważa się datę podpisania przez Strony bez zastrzeżeń Protokołu końcowego odbioru wdrożenia, zgodnego z Załącznikiem nr 4 do Umowy,
   4) w przypadku stwierdzenia wadliwości Zamawiający przedstawi Wykonawcy uzasadnienie odmowy oraz wskaże wady, które muszą zostać usunięte wraz z terminem ich usunięcia.
8) Wynikiem przeprowadzenia odbioru wszystkich produktów będzie sporządzony i podpisany przez obie obie strony Protokół końcowy odbioru wdrożenia, stanowiący Załącznik nr 4 do Umowy.

9) Procedura odbioru dokumentacji technicznej rozwiązania (powdrożeniowej) oraz projektu instalacji i konfiguracji urządzeń oraz oprogramowania wraz z harmonogramem czasowym:
   a) Zamawiający, w terminie 2 dni roboczych Zamawiającego od otrzymania wytworzonych dokumentów, może zgłosić zastrzeżenia i uwagi do ich treści i wezwać Wykonawcę do uwzględnienia tych zastrzeżeń i uwag,
   b) Wykonawca uwzględnia uwagi i zastrzeżenia Zamawiającego, o których mowa w lit. a) lub uzasadnia odmowę ich uwzględnienia w terminie 1 dnia roboczego Zamawiającego i przekazuje Zamawiającemu kolejną – ostateczna wersję dokumentów.
10) Ostateczna wersja dokumentacji powdrożeniowej powinna zostać przekazana Zamawiającemu nie później niż w terminie, o którym mowa w § 3 ust. 1 Umowy, natomiast ostateczna wersja projektu instalacji i konfiguracji urządzeń oraz oprogramowania wraz z harmonogramem czasowym powinna zostać przekazana Zamawiającemu nie później niż w terminie 14 dni kalendarzowych od dnia zawarcia Umowy. Wprowadzanie poprawek do dokumentacji nie powoduje przedłużenia terminu realizacji przedmiotu Umowy, o którym mowa w § 3 ust. 1 Umowy. Uzgodniona dokumentacja, o której mowa w punkcie powyżej, zostanie dostarczona w formie elektronicznej w formacie Word i Pdf (na płycie CD-ROM) i papierowej – drukowanej w 1 egzemplarzu i będzie sporządzona w języku polskim.

Załącznik nr 9 do umowy nr ……(TZ/271/79/15)

STRUKTURA KOMUNIKATÓW XML WYSYŁANYCH Z HP SM I ODBIERANYCH PRZEZ HP SM W ZUS W RAMACH OBSŁUGI ZGŁOSZEŃ SERWISOWYCH

OPIS FUNKCJONALNOŚCI

W celu automatyzacji obsługi zgłoszeń serwisowych pomiędzy Zakładem Ubezpieczeń Społecznych a usługodawcami zewnętrznymi w systemie HP Service Manager (ZUS) został zaimplementowany odrębny moduł obsługi tychże zgłoszeń. Opiera on się na wymianie komunikatów mailowych, które w treści zawierają parametry zgłoszenia i statusy jego obsługi w formacie XML.

Przetwarzanie automatyczne komunikatów mailowych odbywa się bez przerw za wyjątkiem sytuacji awaryjnych i planowej przerwy technologicznej, która ma miejsce zawsze we wtorek w godzinach 18:00 – 20:00 – komunikaty przesłane do HP Service Manager w tym czasie są rejestrowane po godz. 20:00.

1. Konfiguracja komunikacji mailowej

Automatyczna komunikacja będzie przebiegała w oparciu o dedykowane dla HP SM skrzynki do **wysyłki** i **odbioru** komunikatów oraz podanego przez usługodawcę **(Dostawcę)** adresu mailowego do komunikacji.

Skrzynka wysyłającą komunikaty z HP SM do serwisu Dostawcy	Skrzynka odbierająca komunikaty zwrotne z serwisu Dostawcy
sc@zus.pl	**servicemanager@zus.pl**

Jedynym obsługiwanym **formatem wiadomości** pocztowej przesyłanych Z/DO HP SM jest w format tekstowy **(Plain Text Body)**, gdzie w treści wiadomości występuje **struktura XML** opisana w dalszej części dokumentu. Jeżeli umowa z usługodawcą przewiduje w komunikacji wymianę informacji niezbędnych do obsługi zgłoszenia (logi, zrzuty ekranu itp.) **w postaci załączników (wszystkie typy plików za wyjątkiem plików wykonywalnych *.exe) - wiadomość może posiadać załącznik o rozmiarze pliku nie przekraczającym 5MB.**

UWAGA: w treści wiadomości wystąpić może tylko struktura XML przewidziana dla komunikatu i niedozwolone są tym samym podpisy i stopki firmowe.

STRUKTURA WIADOMOŚCI

Wszystkie informacje niezbędne ido automatycznej obsługi zgłoszenia serwisowego zawarte są w treści komunikatu kodowanej w XML stąd też dla zachowania prawidłowego przetwarzania komunikatów treść wiadomości **musi spełniać wymagania poprawności dokumentu XML** (do sprawdzenia m.in. na http://www.w3.org/TR/REC-xml/ **oraz posiadać strukturę odpowiednią, dla komunikatów wychodzących/przychodzących obsługiwanych przez HP Service Manager**. Dla XML nie istnieje plik XSD**;** powiązanie znaczników XML z polami bazy danych opisano w Tabeli 1. i Tabeli 2**.**

Zgodnie ze specyfikacją dla języka XML **znaki o specjalnym znaczeniu** znajdujące się w polach opisowych komunikatu muszą być zastąpione odniesieniami XML. **Jedyne dozwolone składnie przedstawia tabela:**

Odniesienie XML	**Znak specjalny**	
&lt;	<	Mniejszy niż
&gt;	>	Większy niż
&amp;	&	Ampersand
&apos;	'	Apostrof
&quot;	"	Cudzysłów

W przypadku gdy w strukturze XML zostaną przekazane nieprzewidziane znaczniki, e-mail z treścią komunikatu nie zostanie przetworzony.

Temat wiadomości do HP SM jest stały i brzmi: HP Service Manager Email – wiadomości z błędnym tematem lub bez niego nie zostanie przetworzony.

1.1 Treść komunikatów wychodzących z HP Service Manager (ZUS) do serwisu Dostawcy

W poniższych opisach, w celu zwiększenia czytelności ich struktury, komunikaty przedstawiono w postaci wielu linii**, jednak rzeczywisty komunikat XML nie powinien zawierać żadnych znaków końca linii (LF, CR itp.) w tekście, tzn. cały komunikat powinien być wysłany jako jedna linijka tekstu**.

W treści komunikatów nie należy stosować nagłówków XML (z definicją wersji języka i kodowania). Treść ma zawierać tylko sekcję <zs>.

Struktura komunikatów przesyłanych z *HP SM* w ZUS do systemu **Dostawcy** jest następująca:

```
<zs cat="ZUS" id="ZS38899" idSC=" " time="31/10/2012 14:51:30"
type="[O|A|I|R|Z|DN|ZEN|ZNN|ZT|ZTN|ZP]" integrator=" true lub false">
        <usl id="<identyfikator usługi dostawcy>" poziom="<poziom programu np.
        poziom priorytetowy>"    priorytet=" <np. błąd zwykły> " serw="<identyfikator
        programu serwisowego> "/>
        <contact email="Maria.Nowak100@zus.pl" loc="<lokalizacja zgłaszającego np. Rybnik>"
name="NOWAK, MARIA" tel="324390114"/>
<opis>
        <p id="1" war="pierwsza linia opisu"/>
        <p id="2" war="druga linia opisu"/>
        <p id="3" war="kolejna linia opisu"/>
        <p id="4" war="kolejna linia opisu…"/>
</opis>
<parametry>
        <param id="ek" name="Źródłowe EK:" war="bmu#00 (BMC Portal)"/>
        <param id="subcategory" name="Podkategoria:" war="Programy, portale i serwisy
        intranetowe"/>
        <param id="product.type" name="Typ produktu:" war="Narzędzia BMC"/>
        <param id="problem.type" name="Typ problemu:" war="Wniosek Standardowy"/>
</parametry>
</zs>
```

Wymagany zakres przekazywanej informacji:

- ***id*** – identyfikator zgłoszenia serwisowego w *HP SM* w ZUS,
- ***idSC*** – zewnętrzny identyfikator zgłoszenia serwisowego,
- ***integrator*** – nie dotyczy tej Umowy (przyjmuje zawsze wartość false)
- ***type*** – typ komunikatu. Dopuszczalne wartości:
  - **O** – Otwarcie. Rejestracja zgłoszenia serwisowego w systemie Dostawcy, z pustym atrybutem *idSC*.
  - **A** – Aktualizacja. Powtórne wysłanie ZS z *HP SM* w ZUS do serwisu Dostawcy. Wypełnione atrybuty *id* i *idSC*. **Obowiązkowy element <opis>**, możliwy element <parametry>. **Komunikat wznawia czas obsługi zgłoszenia**,
  - **I** – Nieformalna wiadomość. Zwykły komunikat informacyjny z *HP SM* w ZUS do serwisu Dostawcy. Wypełnione atrybuty *id* i *idSC*. Obowiązkowy element <opis>, możliwy element <parametry>. **Komunikat nie będzie związany z przeliczaniem czasu zgłoszenia**
  - **R** – Reklamacja. Wypełnione atrybuty *id* i *idSC*. **Obowiązkowy element <opis>**.
  - **ZEN** – negacja przesłanego przez serwis Dostawcy komunikatu o konieczności eskalacji zgłoszenia. **Wypełnione atrybuty *id*, *idSC* oraz Obowiązkowy element <opis>. Komunikat wznawia bieg czasu obsługi zgłoszenia.**
  - **ZP** – Żądanie zmiany programu serwisowego. **Wypełnione atrybuty *id* i *idSC* oraz element <usl> zawierający proponowany poziom (program serwisowy) w *HP SM* w ZUS**,
  - **ZNN** – negacja przedstawionych przez serwis Dostawcy zaleceń naprawczych. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis>. Komunikat wznawia bieg czasu obsługi zgłoszenia,**
  - **Z** – Zamknięcie. Informacja o zamknięciu zgłoszenia w *SM*. Komunikat ma znaczenie wyłącznie informacyjne i oznacza zakończeni obsługi zgłoszenia w ZUS - **po tym komunikacie zgłoszenie serwisowe nie jest już aktualizowane**,
  - **ZT** – potwierdzenie skuteczności zaproponowanego przez serwis Dostawcy obejścia. **Wypełnione atrybuty *id* i *idSC* oraz opcjonalny element <opis>. Komunikat wstrzymuje czas obsługi zgłoszenia,**
  - **ZTN** - negacja zaproponowanego przez serwis Dostawcy obejścia. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis>, Komunikat wznawia czas obsługi zgłoszenia,**

- ***DN*** **-** *negacja zaproponowanej przez serwis Dostawcy diagnozy.* ***Wypełnione atrybuty id i idSC oraz Obowiązkowy element <opis>, Komunikat wznawia czas obsługi zgłoszenia,***[1]

Komunikat typu *„**O**”* będzie powodował utworzenie zgłoszenia serwisowego.

Poszczególne pola w treści XML zawierają jak opisano:

- ***time*** – data i czas przesłania komunikatu XML,
- ***cat*** – kategoria, wartość stała, zawsze *„ZUS”,*
- ***usl*** – informacje o usłudze:
  - ***id*** – identyfikator usługi Dostawcy, której dotyczy zgłoszenie, zawarty w polu elementu konfiguracji zgłoszenia serwisowego,
  - ***serw*** – identyfikator usługi serwisowej Dostawcy, odpowiadający umowie w rejestrach dla zgłoszeń serwisowych,
  - ***poziom*** – wybrany poziom usługi serwisowej Dostawcy, odpowiadający programowi umowy w rejestrach dla zgłoszeń serwisowych,
  - ***priorytet*** – priorytet dotyczący błędu, tylko dla wybranych usług Dostawcy.
- ***contact*** – dane kontaktowe (imię i nazwisko, e-mail, telefon) zgłaszającego,
- ***opis*** – opis zgłoszenia serwisowego.

Pozostałe wartości (opcjonalnie):

- ***parametry*** – dodatkowe wartości przekazywane w zgłoszeniu. Obecnie są to wartości z incydentu, z którego utworzono ZS:
  - Element Konfiguracji,
  - Podkategoria,
  - Typ produktu,
  - Typ Problemu.

[1] Komunikat planowany na potrzeby umowy utrzymaniowej

Treść komunikatów przychodzących do HP Service Manager (ZUS) z serwisu Dostawcy

Odpowiedź z systemu serwisu Dostawcy do *HP SM* w ZUS ma następującą strukturę:

<zs **id**="ZS00122" **idSC**="XXXXXX" **type**="[**A|O|I|R|P|D|ZE|ZN|ZT|ZP|Z**]">
<usl **id**="<identyfikator usługi dostawcy>" **serw**="<identyfikator programu serwisowego>" **poziom**="<poziom programu np. Incydent krytyczny"/>
<**opis**>
<p **id**="1" **war**="pierwsza linia opisu"/>
<p **id**="2" **war**="kolejna linia opisu"/>
</**opis**>
</zs>

Istotne znaczenie ma atrybut *type*, który w tym przypadku może zawierać następujące wartości:

- **O** – rejestracja w serwisie Dostawcy i nadanie *idSC*. **Nie zawiera elementu opis**. **Komunikat powoduje uruchomienie naliczania czasu obsługi zgłoszenia**.
- **A** - komunikat aktualizacyjny stosowany przez serwis Dostawcy w sytuacji, gdy odpowiedź zostanie pozyskana wcześniej, przed wysyłką komunikatu „A" z ZUS. **Wypełnione atrybuty *id* i *idSC* oraz obowiązkowy element <opis> zawiera treść aktualizacji**. **Komunikat wznawia czas obsługi zgłoszenia,**
- **P** – pytanie do użytkownika. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis> zawiera treść pytania**. **Komunikat wstrzymuje czas obsługi zgłoszenia,**
- **I** – Nieformalna wiadomość. Zwykły komunikat informacyjny z serwisu Dostawcy do ZUS. Wypełnione atrybuty *id* i *idSC*. Obowiązkowy element <opis>, możliwy element <parametry>. **Komunikat nie będzie związany z przeliczaniem czasu zgłoszenia,**
- **D** – Diagnoza zgłoszenia. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis>** z opisem diagnozy **Komunikat wstrzymuje czas obsługi zgłoszenia.**
- **R** – reklamacja usługi i poziomu zgłoszenia. **Wypełnione atrybuty *id* i *idSC* oraz element <opis> oraz <usl /> z sugerowaną inną usługą i poziomem. Komunikat wstrzymuje czas zgłoszenia.** Oczekiwanym komunikatem ze strony ZUS jest **ZP**, który po potwierdzeniu komunikatem z serwisu Dostawcy przelicza czas obsługi zgłoszenia wg reklamowanych parametrów.
- **ZE** – Eskalacja zgłoszenia (zgłoszenie błędnie skierowane do Dostawcy). **Wypełnione atrybuty *id* i *idSC* oraz obowiązkowy element <opis>. Komunikat wstrzymuje naliczanie czasu obsług zgłoszenia**. Spodziewaną odpowiedzią ze strony ZUS jest zamknięcie zgłoszenia serwisowego lub komunikat **ZEN**.

- **ZN** – Zalecenia naprawcze. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis> z zaleceniami naprawczymi. Komunikat wstrzymuje czas obsługi zgłoszenia.** Spodziewaną odpowiedzią ze strony ZUS jest zamknięcie zgłoszenia lub negacja zaleceń naprawczych (rozwiązania) – komunikat typu **ZNN**.
- **ZP** – Potwierdzenie rejestracji żądania programu serwisowego. **Wypełnione atrybuty *id* i *idSC.* Komunikat zmienia czas obsługi przeliczając czas wg parametrów zmienionego programu serwisowego.**
- **ZT** – Zalecenia tymczasowe. **Wypełnione atrybuty *id* i *idSC* oraz Obowiązkowy element <opis> z zalecaniami tymczasowymi (obejściem). Komunikat wstrzymuje czas obsługi zgłoszenia.** Spodziewanym komunikatem ze strony ZUS jest potwierdzenie obejścia komunikat **ZT** lub komunikat **ZTN** (ponownie uruchamiający bieg czasu zgłoszenia),
- **Z** – Prośba o zamknięcie. **Wypełnione atrybuty *id* i *idSC***

UWAGA: Komunikatem potwierdzającym przyjęcie do obsługi zgłoszenia jest komunikat typu „O" wysyłany do HP SM. Dopiero po nim serwis Dostawcy może przekazywać komunikaty pozostałych typów.

Po otrzymaniu z HP SM komunikatu informacyjnego typu „Z" (o zamknięciu zgłoszenia) nie ma już możliwości rejestracji komunikatów dotyczących danego zgłoszenia serwisowego.

Mapowanie pól komunikatu xml na pola w bazie przechowującej dane obsługiwanych zgłoszeń

Dla poprawnego przetwarzania i przechowywania danych związanych z przekazywanymi komunikatami ZS niezbędne jest zachowanie dozwolonych rozmiarów pól komunikatu. Mapowania pól dla komunikatów wychodzących i przychodzących do HP Service Manager zawarte są w poniższych tabelach:

Pole komunikatu XML		Parametry pola w bazie SQL
Element XML	**Atrybut XML**	
zs	**id**	**[varchar](60)**
	idSC	**[varchar](50)**
	type	**stałe = O,A,I,R,ZEN,ZP,ZNN,Z,ZT,ZTN**
	cat	**stały = ZUS**
usl	**id**	**[varchar](300)**
	serw	**[varchar](60)**
	poziom	**[varchar](60)**
	priorytet	**[varchar](60)**
contact	**name**	**[varchar](100)**
	email	**[varchar](140)**
	tel	**[varchar](60)**
	loc	**[varchar](50)**
opis	**p**	**[varchar](1000) – ograniczenie dotyczy każdego wiersza opisu w komunikacie**
parametry	**param**	**[text]**

Tabela 1. Mapowanie pól komunikatu xml w komunikacie do serwisu Dostawcy

Komunikaty do HP Service Manager

Pole komunikatu XML		Parametry pola w bazie SQL
Element XML	**Atrybut XML**	
zs	**id**	**[varchar](60)**
	idSC	**[varchar](50)**
	type	**stałe = A,O,P,D,I,R,ZE,ZN,ZP,ZT, Z**
opis	**p**	**[varchar](1000) – ograniczenie dotyczy każdego wiersza opisu w komunikacie**

Tabela 2. Mapowanie pól komunikatu xml w komunikacie do HP Service Manager

W przypadku gdy znacznik XML powiązany jest z polem typu *text*, jego długość ograniczona jest parametrami pola w tablicy.

Dla komunikatów XML, w których występuje wielokrotność elementów tego samego typu, ich ilość jest nieograniczona. Element *idSC* (Identyfikator zewnętrzny) jest generowany poza *HP SM* w ZUS, w związku z czym jego format musi być znakowy.

Implementacja automatycznej komunikacji w zakresie zgłoszeń serwisowych pomiędzy HP Service Manager (ZUS) a serwisem Dostawcy

Wdrożenie automatycznej komunikacji w zakresie obsługi zgłoszeń serwisowych poprzedzone jest zawsze testami przedprodukcyjnymi w środowisku testowym HP Service Manager i środowisku testowym Dostawcy usług. Dopuszczalne jest odstąpienie od testów dla Dostawcy, który wcześniej takie testy pomyślnie przeszedł, a rozszerzeniu ulega katalog umów świadczonych przez niego. Dla odpowiedniego zamodelowania usług Dostawcy konieczne jest bezpośredni kontakt technologów odpowiedzialnych za wdrożenie po obu stronach i dane dotyczące metryk świadczonych usług:

- nazwa umowy serwisowej,
- nazwy świadczonych usług,
- programy serwisowe dla usług (z określonymi priorytetami),
- powołane usługi wewnętrzne w ZUS wspierające usługi Dostawcy,
- harmonogram testów i wdrożenia.

Po zamodelowaniu środowisk testowych testy przebiegają z udziałem centrum wsparcia informatyki, które docelowo obsługiwać ma zgłoszenia Dostawcy. W czasie testów symulowana jest obsługa wszystkich możliwych komunikatów jakie obsługuje opisana w dokumencie funkcjonalność .

Po zakończeniu pomyślnym testów ustalona zostaje data implementacji rozwiązania w środowisku produkcyjnym.

Należy pamiętać, że jednostronne wprowadzanie nie testowanych zmian w konfiguracji komunikacji i strukturze komunikatów jest niedopuszczalne i może skutkować błędami w przetwarzaniu komunikatów.

Scenariusze testowe

Poniżej zamieszczono przykład standardowego scenariusza testów wymiany komunikatów XML między systemami Dostawcy a Zamawiającego przed integracją na środowisku produkcyjnym.

NR KROKU	OPIS KROKU SCENARIUSZA	OCZEKIWANY WYNIK
1	komunikat typu O do SZ - otwarcie ZS w ZUS	Założony ZS po stronie SZ
2	komunikat typu O do ZUS - potwierdzenie przyjęcia zs do obsługi	Zarejestrowany idSC w ZUS - start czasu obsługi zgłoszenia
3	komunikat typu D - diagnoza	Zarejestrowana Diagnoza w historii ZS
4	komunikat I do SZ - czas obsługi bez zmian	zarejestrowany w SZ komunikat typu I - czas obsługi bez zmian
5	Komunikatu typu ZN do ZUS	Zarejestrowane zalecenia naprawcze w ZUS - wstrzymany czas obsługi ZS
6	komunikatu typu ZNN do SZ - wznowiony czas obsługi ZS w ZUS	zarejestrowany w SZ komunikat typu ZNN
7	komunikatu typu P do ZUS	Zarejestrowane w ZUS pytanie do użytkownika - wstrzymany czas obsługi
8	komunikatu typu A do SZ - wznowiony czas obsługi	zarejestrowana aktualizacja w SZ
9	komunikat typu ZT do ZUS	Zarejestrowane obejście w ZUS - wstrzymany czas obsługi ZS
10	komunikat ZTN do SZ - wznawia czas obsługi ZS	Zarejestrowany ZTN w SZ
11	komunikat ZN do ZUS	Zarejestrowane zalecenia naprawcze w ZUS - wstrzymany czas obsługi ZS
12	komunikat typu Z do SZ - zamknięcie zgłoszenia	Zarejestrowany komunikat typu Z

Prawidłowa sekwencja dla niektórych typów komunikatów:

Komunikaty z HP SM ZUS (czynność/typ komunikatu)	***Oczekiwany komunikat od Dostawcy(czynność/typ komunikatu)***
Otwarcie zgłoszenia/O	Potwierdzenie rejestracji zgłoszenia/O
	Przekazania diagnozy/D
	Przekazanie zaleceń tymczasowych/ZT
	Przekazanie zaleceń naprawczych/ZN
Potwierdzenia lub negacja zaleceń tymczasowych lub naprawczych/DN, ZT, ZTN, ZNN*	
	Prośba o zamknięcie zgłoszenia/Z
Zamknięcie zgłoszenia/Z	

Opcjonalnie w razie potrzeby w obsłudze zgłoszenia serwisowego mogą pojawić się w obiegu następujące kroki:

Komunikaty z HP SM ZUS (czynność/typ komunikatu)	***Oczekiwany komunikat od Dostawcy***
	Eskalacja zgłoszenia/ZE
Negacja eskalacji/ZEN lub zamknięcie zgłoszenia/Z	
	Reklamacja poziomu usługi/R
Żądanie zmiany programu serwisowego/ZP	
	Potwierdzenie zmiany programu serwisowego/ZP
	Pytanie do użytkownika/P
Aktualizacja- przekazanie dodatkowych danych/A	

Zapisy dotyczące Integracji

Moment Integracji systemów Dostawcy oraz Zamawiającego inicjuje Dostawca zgodnie z czasem określonym w Umowie.

Pisemne potwierdzenie integracji zostaje podpisane po pomyślnie przeprowadzonych testach wg scenariuszy testowych.

Załącznik nr 10 do umowy nr ……(TZ/271/79/15)

PROTOKÓŁ POTWIERDZENIA INTEGRACJI
SYSTEMU OBSŁUGI ZGŁOSZEŃ WYKONAWCY Z SYSTEMEM OBSŁUGI ZGŁOSZEŃ ZAMAWIAJĄCEGO

Zgodnie z umową nr …….. z dnia …… nr **.....** Zespół w składzie:

PRZEDSTAWICIELE WYKONAWCY:	PRZEDSTAWICIELE ZAMAWIAJACEGO:
1.....	1.....
2.....	2.....

potwierdził, integrację systemu obsługi zgłoszeń Wykonawcy z systemem obsługi zgłoszeń ZAMAWIAJĄCEGO:

PRZEDSTAWICIELE WYKONAWCY:	PRZEDSTAWICIELE ZAMAWIAJACEGO:
1.....	1.....
2.....	2.....

…….
(miejscowość) (data)

Załącznik nr 11 do umowy nr ……(TZ/271/79/15)

Nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych

……
(miejsce i data nadania upoważnienia)

Nr upoważnienia : …….

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Upoważniam Panią/Pana

1) …….....
2) …….....
3) …….....
itd. …….....
(imię i nazwisko osoby upoważnianej)

wykonujących w Zakładzie Ubezpieczeń Społecznych zadania, w związku z realizacją umowy nr …, zawartej w dniu……, przez strony umowy:..……

do przetwarzania następujących danych osobowych w zakresie:

- danych klientów Zakładu Ubezpieczeń Społecznych oraz pracowników Zakładu, niezbędnych do realizacji przedmiotu umowy,
- operacji na danych, niezbędnym do wykonywania zadań wynikających z ww. umowy, tj……,
- przetwarzania danych osobowych w systemach informatycznych: ……., zgodnie z nadanymi uprawnieniami.

2. Okres trwania upoważnienia:

….....
(okres obowiązywania upoważnienia niezbędny do realizacji umowy)

Wystawił:
….....
(podpis osoby reprezentującej Zakład Ubezpieczeń Społecznych, jako administratora danych)

Osoby upoważnione do przetwarzania danych w zakresie, o którym mowa wyżej, są zobowiązane do zachowania ich w tajemnicy, również po ustaniu umowy oraz zachowania w tajemnicy informacji o ich zabezpieczeniu.
Data i podpisy osób upoważnionych:
1) …….....
2) …….....
3) …….....
itd. …….....

Załącznik nr 12 do Umowy…… (TZ/271/79/15)

PROTOKÓŁ PRZEPROWADZENIA SZKOLENIA

W dniu ..... w ..... na podstawie umowy nr …… (TZ/271/79/15) z dnia ……..... potwierdzamy przeprowadzenie szkolenia w zakresie ..... (nr kursu .....)

Lp	Imię i Nazwisko	Podpis osoby przeszkolonej

Uwagi uczestnika szkolenia:
.....
.....
.....
.....

za WYKONAWCĘ

za ZAMAWIAJĄCEGO

(imię i nazwisko)

(imię i nazwisko)

(pieczątka firmowa)

(pieczątka firmowa)

Załącznik nr 13 do Umowy…… (TZ/271/79/15)

MIESIĘCZNY RAPORT Z WYKONANYCH USŁUG

Raport za miesiąc/rok: _____/_____	**Miesięczny Raport Wykonanych Usług**	Data sporządzenia: _____._____._____
Dotyczy umowy:	**Wykonawca raportu**: Imię i Nazwisko:	

Czynności serwisowe (1)	
Liczba Zgłoszeń Serwisowych:	
Liczba Rozpoczętych Interwencji Serwisowych:	
Liczba Zakończonych Interwencji Serwisowych:	

Uwagi:
(1) Wszystkie wymienione w raporcie czynności mają swoje potwierdzenie w postaci odpowiednich protokołów, których kopie zostaną dołączone jako załączniki do niniejszego raportu.

Podpis osoby sporządzającej raport:	
Uwagi osoby odbierającej raport:	
Data otrzymania raportu:	**Podpis osoby odbierającej raport**:

Załącznik nr 3
do SIWZ TZ/271/79/15

W Z Ó R

.....
miejscowość, data

OŚWIADCZENIE

Niniejszym oświadczam, że .....
N a z w a W y k o n a w c y

spełnia warunki określone w art. 22 ust. 1 pkt 1) – 4) ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164).

.....
podpis osoby upoważnionej do reprezentowania Wykonawcy

W załączeniu dowód, w szczególności pisemne zobowiązanie innych podmiotów (art. 22 ust. 1 pkt 2), 3) i 4) ustawy Prawo zamówień publicznych) do oddania Wykonawcy do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonaniu zamówienia:*

1. ……
2. ……
3. ……

** wypełnia Wykonawca, którego dotyczy określona sytuacja*

Załącznik nr 4
do SIWZ TZ/271/79/15

W Z Ó R

.....
miejscowość, data

OŚWIADCZENIE

Niniejszym oświadczam, że .....
N a z w a W y k o n a w c y

nie podlega wykluczeniu z postępowania o udzielenie zamówienia publicznego na podstawie art. 24 ust. 1 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j. Dz. U. z 2015 r. poz. 2164).

.....
podpis osoby upoważnionej do reprezentowania
Wykonawcy

Załącznik nr 5
do SIWZ TZ/271/79/15

……
miejscowość, data

WYKAZ WYKONANYCH BĄDŹ WYKONYWANYCH DOSTAW

Wykaz co najmniej 2 wykonanych lub wykonywanych dostaw, zrealizowanych w okresie ostatnich 3 lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, odpowiadających przedmiotowi zamówienia, każda o wartości równej lub przekraczającej kwotę 8 000 000,00 zł brutto, w tym co najmniej jedna z nich obejmująca swoim zakresem również wdrożenie, konfigurację dostarczonych urządzeń sieciowych, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane, oraz załączeniem dowodów, czy zostały wykonane lub są wykonywane należycie. Poprzez dostawę odpowiadającą przedmiotowi zamówienia należy rozumieć należycie zrealizowane dostarczenie sprzętu sieciowego, takiego jak: routery, przełączniki sieciowe, zapory sieciowe itp. W przypadku zamówień, które są w trakcie realizacji, wykonana część musi odpowiadać powyższym wymaganiom.

W przypadku Wykonawców składających wspólną ofertę przynajmniej jeden z nich musi wykazać się spełnieniem warunku, o którym mowa powyżej. W przypadku, gdy Wykonawca polega na wiedzy i doświadczeniu innych podmiotów, to co najmniej jeden z nich powinien samodzielnie spełnić powyższy warunek udziału w postępowaniu. W przypadku, gdy Wykonawca wykaże na potwierdzenie spełnienia powyższego warunku udziału w postępowaniu, dostawy, przy realizacji których brał udział, jako członek konsorcjum, z dowodów, czy dostawy zostały wykonane lub są wykonywane należycie, powinien wynikać zakres prac wykonanych przez Wykonawcę, jako członka konsorcjum.

Lp.	Odbiorca dostawy (nazwa i adres)	Przedmiot dostawy	Wartość dostawy (brutto)	Data rozpoczęcia i zakończenia wykonywania dostawy (dzień, miesiąc, rok)/ Data rozpoczęcia (dzień, miesiąc, rok)*

Do oferty załączono dokumenty potwierdzające, że dostawy wskazane w wykazie zostały wykonane lub są wykonywane należycie:

1) …….……
2) ……..

Z treści dokumentów potwierdzających, że dostawy wymienione w wykazie zostały wykonane należycie, musi jednoznacznie wynikać, iż dotyczą dostaw wskazanych w wykazie.

** W przypadku dostaw wykonywanych należy podać datę rozpoczęcia i zaznaczyć, że dostawa jest w trakcie realizacji.*

.....
podpis osoby upoważnionej do reprezentowania Wykonawcy