

Sygn. akt: KIO 78/16

WYROK

z dnia 3 lutego 2016 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: Agnieszka Trojanowska

Protokolant: Agata Dziuban

po rozpoznaniu na rozprawie w Warszawie w dniu 3 lutego 2016 r. odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 22 stycznia 2016r. przez **wykonawcę Asseco Poland Spółka Akcyjna z siedzibą w Rzeszowie, ul. Olchowa 14** w postępowaniu prowadzonym przez zamawiającego **Operatora Gazociągów Przesyłowych Gaz-System Spółka Akcyjna z siedzibą w Warszawie, ul. Mszczonowska 4**

przy udziale **wykonawcy Qumak Spółki Akcyjnej z siedzibą w Warszawie, Al. Jerozolimskie 134** zgłaszającym swoje przystąpienie w sprawie sygn. akt KIO 78/16 po stronie zamawiającego

orzeka:

- 1. uwzględnia odwołanie i nakazuje zamawiającemu unieważnienie czynności oceny ofert, unieważnienie czynności wyboru oferty jako najkorzystniejszej oferty Qumak Spółka Akcyjna z siedzibą w Warszawie, nakazuje powtórzenie oceny ofert, dokonanie zaniechanej czynności odrzucenia oferty Qumak Spółka Akcyjna z siedzibą w Warszawie na podstawie art. 89 ust. 1 pkt 2 ustawy z uwagi na to, że treść oferty tego wykonawcy nie odpowiada treści specyfikacji istotnych warunków zamówienia określonej w załączniku nr 1 a do siwz w pkt. 4.6. tj. zaoferowane rozwiązanie równoważne nie zapewnia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności produktu z funkcjonalnością GET VPN systemu IOS 12.4 advipservicesk9 oraz nakazuje dokonanie wyboru oferty najkorzystniejszej,**
- 2. kosztami postępowania obciąża wykonawcę Qumak Spółki Akcyjnej z siedzibą w Warszawie, Al. Jerozolimskie 134 i:**

2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez **wykonawcę**

Asseco Poland Spółka Akcyjna z siedzibą w Rzeszowie, ul. Olchowa 14 tytułem wpisu od odwołania,

2.2. zasądza od **wykonawcy Qumak Spółki Akcyjnej z siedzibą w Warszawie, Al. Jerozolimskie 134** na rzecz **wykonawcy Asseco Poland Spółka Akcyjna z siedzibą w Rzeszowie, ul. Olchowa 14** kwotę **15 000 zł 00 gr** (słownie : piętnaście tysięcy złotych zero groszy) stanowiącą koszty postępowania odwoławczego poniesione z tytułu wpisu.

Stosownie do art. 198a i 198b ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2015 r., poz. 2164) na niniejszy wyrok - w terminie 7 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w **Warszawie**.

Przewodniczący:

Uzasadnienie

Postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego na zakup i wdrożenie urządzeń sieciowych zostało wszczęte ogłoszeniem o zamówieniu publicznym opublikowanym w Dzienniku Urzędowym Unii Europejskiej z dnia 2 września 2015r.

W dniu 12 stycznia 2016r. zamawiający poinformował wykonawców o wynikach postępowania, w tym o wyborze jako najkorzystniejszej oferty wykonawcy Qumak Spółka Akcyjna z siedzibą w Warszawie.

W dniu 22 stycznia 2016r. odwołanie wniósł wykonawca Asseco Poland Spółka Akcyjna z siedzibą w Rzeszowie. Odwołanie zostało podpisane przez pełnomocnika działającego na podstawie pełnomocnictwa z dnia 2 października 2015r. udzielonego przez dwóch wiceprezesów zarządu ujawnionych w KRS i upoważnionych do łącznej reprezentacji, zgodnie z odpisem z KRS załączonym do odwołania. Kopia odwołania została przekazana zamawiającemu w dniu 22 stycznia 2016r. drogą elektroniczną.

Odwołujący zaskarżył zaniechanie odrzucenia oferty wykonawcy Qumak SA oraz czynność wyboru tej oferty jako najkorzystniejszej.

Odwołujący zarzucił zamawiającemu naruszenie następujących przepisów ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2015 r., poz. 2164 – dalej ustawy): art. 7 ustawy, art. 82 ustawy, art. 89 ust. 1 pkt 2 ustawy

Naruszenia te spowodowały w konsekwencji niemożność oceny ofert, czyli naruszenie art. 91 ust. 1 i 2 ustawy.

Odwołujący wniósł o uwzględnienie odwołania w całości oraz o nakazanie zamawiającemu:

1. unieważnienie czynności oceny ofert;
2. unieważnienia czynności wyboru oferty jako najkorzystniejszej oferty Qumak;
3. dokonanie ponownej oceny ofert,
4. odrzucenie oferty Qumak
5. wybór oferty odwołującego jako najkorzystniejszej,

Odwołujący wskazał, że ma interes we wniesieniu niniejszego odwołania, gdyż ma interes w uzyskaniu zamówienia oraz może ponieść szkodę w wyniku naruszenia przepisów. Odwołujący jest podmiotem, który złożył ofertę w niniejszym postępowaniu. Oferta odwołującego jest, ofertą nie podlegającą odrzuceniu. Oferta odwołującego jest na drugiej pozycji - po skarżonej ofercie Qumak. Zatem, gdyby zamawiający nie naruszył wskazanych w odwołaniu przepisów - oferta odwołującego zostałaby wybrana jako oferta najkorzystniejsza.

W uzasadnieniu odwołujący podniósł, że zamawiający w wyniku rozstrzygnięcia postępowania chce rozbudować (a nie wymienić/zastąpić) funkcjonującą u siebie sieć. Zamawiający, zdaniem odwołującego, zachował konkurencyjność warunków postępowania dopuszczając sprzęt innych producentów niż posiadany przez siebie. Z uwagi jednak na zapewnienie właściwego funkcjonowania całej rozbudowanej sieci - w stosunku do urządzeń oferowanych w postępowaniu sformułowano szczegółowe kryteria równorzędności. Parametry i właściwości oferowanych przez wykonawców urządzeń muszą bowiem gwarantować pełną interoperacyjność.

W siwz - w tym w Załączniku nr 1a „Formularz Specyfikacji Technicznej” zamawiający wskazał, jakie wymagania minimalne muszą zostać spełnione w odniesieniu do oferowanych przez wykonawców urządzeń (w tym urządzeń równoważnych).

We wskazanym dokumencie zamawiający podał, że cyt.:

„Wykonawca zobowiązany jest do wypełnienia formularza oferty technicznej (przedstawionych poniżej tabeli) przez wpisanie nazwy producenta i typu urządzenia, i wypełnienie kolumny „Parametry techniczne oferowanego sprzętu” poprzez wstawienie sformułowania „spełnia” lub „nie spełnia”

W przypadku zaoferowania przez Wykonawcę produktu (rozwiązania) równoważnego, Wykonawca co najmniej musi wskazać nazwę, typ i wersję produktu oraz nazwę producenta produktu i nazwę i adres podmiotu świadczącego serwis autoryzowany przez producenta, a także wykazać, że produkt (rozwiązanie) równoważne spełnia wymagania Zamawiającego.

Jeśli nie zaznaczono inaczej, wszelkie zapisy konfiguracji „Wymagań minimalnych” należy traktować, jako parametry i wymagania minimalne.

Odnośnie routerów Router - RT-TJE wymagania te zawarto w Sekcji 2 Załącznika 1a i są to między innymi:

„4. Funkcjonalność:

(...) 22) Zaawansowane funkcjonalności bezpieczeństwa:

- a) IPSecVPN,
- b) dynamiczne, wielopunktowe tunelowanie VPN
- c) oraz GET VPN lub równoważne** w roli członka grupy (w zakresie GET VPN, wymagana jest kompatybilność z routerami Cisco, które pełnią rolę członków grupy i serwera kluczy)

** Warunki równoważności na rozwiązanie GET VPN:

1. Zamawiający posiada obecnie wdrożony system szyfrowania w sieci WAN w topologii full mesh, oparty o technologię GET VPN, o następujących cechach:

1.1. Oparty jest na licencjach oprogramowania systemowego IOS 15 universalk9: ipbasek9+securityk9 oraz IOS 12.4 advipservicesk9 funkcjonujących na urządzeniach sieciowych firmy CISCO.

- 1.2. Wykupionej usłudze subskrypcji ww oprogramowania.
 - 1.3. System szyfrowania został wdrożony z uwzględnieniem polityki bezpieczeństwa i wdrożonych procedur ochrony informacji funkcjonujących u zamawiającego.
 2. Zakup urządzeń RT-TJE jest przeznaczony do funkcjonowania w środowisku sieci WAN eksploatowanej obecnie u zamawiającego.
 3. Dopuszcza się zaoferowanie produktów równoważnych do produktów określonych w pkt 1.
 4. Równoważność dotyczy licencji oprogramowania systemowego w zakresie funkcjonalności GET VPN i usługi subskrypcji. Równoważność oznacza, że:
 - 4.1. warunki licencji w każdym aspekcie licencjonowania są nie gorsze niż licencja każdego z produktów określonych w pkt 1,
 - 4.2. funkcjonalność rozwiązania równoważnego nie może być gorsza od funkcjonalności GET VPN technologii określonej w pkt 1,
 - 4.3. rozwiązanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u zamawiającego,
 - 4.4. rozwiązanie równoważne nie może zakłócić pracy środowiska systemowo-programowego zamawiającego,
 - 4.5. rozwiązanie równoważne musi w pełni współpracować z systemami już eksploatowanymi u zamawiającego,
 - 4.6. rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienną produktu z funkcjonalnością GET VPN systemu IOS 15 univsaik9: ipbasek9+securityk9 oraz IOS 12.4 advipservicesk9,
 - 4.7. rozwiązanie równoważne musi umożliwiać wymianę routerów w sieci zamawiającego, w sposób, który umożliwi zachowanie ciągłości dla usługi szyfrowania ruchu przesyłanego przez sieć WAN (o topologii full mesh),
 - 4.8. warunki i zakres subskrypcji i konserwacji dla oprogramowania zapewniającego rozwiązanie równoważne muszą być nie gorsze niż usługa subskrypcji określona w pkt 1.
 5. Wykonawca, który zaoferuje rozwiązanie równoważne musi udowodnić spełnienie wszystkich warunków określonych w pkt 4. W tym celu Wykonawca:
 - 5.1. złoży wraz z ofertą nw. oświadczenia i dokumenty:
 - 5.1.1. pełne postanowienia licencji oprogramowania zapewniającego rozwiązanie równoważnego,
 - 5.1.2. wykaz pełnej funkcjonalności rozwiązania równoważnego,
 - 5.1.3. pełne warunki i zasady świadczenia usługi subskrypcji i konserwacji dla oprogramowania zapewniającego rozwiązanie równoważne."
- Odwołujący podniósł, iż routery Huawei zaoferowane przez wykonawcę Qumak, nie są urządzeniami spełniającymi wszystkie wymogi równoważności oraz interoperacyjności

postawionymi przez zamawiającego, a więc nie spełniają one warunków minimalnych co powoduje, iż oferta wykonawcy jest niezgodna z siwz. Wniosek taki, zdaniem odwołującego, potwierdza szczegółowa analiza wyjaśnień złożonych przez Qumak w odpowiedzi na zgłoszone przez samego zamawiającego wątpliwości.

W wyjaśnieniach z dnia 15 grudnia 2015 roku Qumak zapewnia o interoperacyjności routerów Huawei z ruterami Cisco wskazując wyraźnie, iż do zapewnienia prawidłowej współpracy oferowanych routerów Huawei z posiadanymi przez Zamawiającego routerami Cisco wystarczy tylko wspieranie przez urządzenia Huawei standardu draft-weis-gdoi-rekey-ack-01 (GDOI GROUPKEY-PUSH Acknowledgement Message).

Qumak wskazuje, iż twierdzenie to wynika z treści dokumentu firmy Cisco : http://www.cisco.com/c/en/us/td/docs/ios-xmi/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn-15-mt-book.pdf.

Analiza dokumentu firmy Cisco prowadzi odwołującego jednak do odmiennych wniosków. Dokument ten wymienia bowiem jeszcze inne standardy/funkcjonalności, które są wymagane do zapewnienia interoperacyjności.

Oprócz już wcześniej wymienionego standardu są to:

- draft-weis-delay-detection-00 IP Delivery Delay Detection Protocol (strona 248 w/w dokumentu ze strony www.cisco.com)
- funkcjonalność „Activation Time Delay” zdefiniowana w sekcji 4.2.1 dokumentu RFC 6407 (strona 248 w/w dokumentu ze strony www.cisco.com)

Tak więc dla zapewnienia prawidłowej współpracy między urządzeniami wszystkie trzy powyżej wymienione standardy/funkcjonalności powinny być spełnione przez urządzenia firmy Huawei mające pracować jako „Group Member”.

Wymogi te, zdaniem odwołującego, dotyczą każdego routera, który ma współpracować w sieci GET VPN bez względu na pełnioną rolę w tej sieci: GM (Group Member) i KS (Key Server).

Qumak podał w swoim wyjaśnieniu jedynie informację o wspieranie przez urządzenia Huawei standardu draft-weis-gdoi-rekey-ack-01 (GDOI GROUPKEY-PUSH Acknowledgement Message).

Drugą kluczową według odwołującego kwestią jest okoliczność, iż zamawiający posiada obecnie dwa rodzaje routerów Cisco:

- z2wq oprogramowaniem w wersji IDS 15 universalk9: ipbasek9+securityk9
- z oprogramowaniem w wersji 12.4 advipservicesk9

Zamawiający wymagał w siwz by urządzenia dostarczone i wdrożone w wyniku niniejszego postępowania współpracowały z oboma funkcjonującymi typami routerów Cisco.

Zamawiający w Załączniku nr 1a w warunkach równoważności zawarł wymaganie: „4.6. rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie

rzeczywistym i pełną funkcjonalną zamienną produktu z funkcjonalnością GET VPN systemu IOS 15 universal9: ipbase9+security9 oraz IOS 12.4 advipservices9 w szczególności".

Firma Qumak w swoim wyjaśnieniu pominęła fakt, że wsparcie dla wszystkich trzech standardów/funkcjonalności a więc: standard draft-weis-gdoi-rekey-ack-01, standard draft-weis-delay-detection-00, funkcjonalność „Activation Time Delay” zdefiniowana w sekcji 4.2.1 standardu RFC 6407, zostało wprowadzone przez firmę Cisco od wersji 15.5(1)T oprogramowania.

Oferowane przez Qumak rozwiązanie nie jest zgodne z tym wymaganiem, ponieważ nie spełnia wymagania interoperacyjności z wersją 12.4 oprogramowania routerów Cisco. Oferowane przez firmę Qumak rozwiązanie zapewnia wg jego oświadczenia interoperacyjność tylko z oprogramowaniem w wersji 15.

W świetle tych okoliczności odwołujący uważa, że niespełnianie przez oferowane urządzenia wymagań minimalnych zamawiającego powoduje, iż oferta winna zostać odrzucona jako nieodpowiadająca siwz. Bez znaczenia są w takiej sytuacji dodatkowe parametry urządzeń, punkty za spełnianie kryteriów dodatkowych oraz cena oferty.

Skutek w postaci bezwzględnego obowiązku odrzucenia oferty przewidują wprost przywołane przepisy prawa zamówień publicznych.

Jako dowody na wykazanie istnienia podstaw odrzucenia oferty wykonawcy Qumak SA odwołujący powołał załącznik nr 1 a do siwz, ofertę Qumak, wyjaśnienia Qumak z dnia 15 grudnia 2015r.

W dniu 25 stycznia 2016r. zamawiający poinformował wykonawców o wniesieniu odwołania przekazując jego kopię i wezwał do wzięcia udziału w postępowaniu odwoławczym.

W dniu 28 stycznia 2016r. do postępowania odwoławczego po stronie zamawiającego zgłosił swój udział wykonawca Qumak Spółka Akcyjna z siedzibą w Warszawie wskazując, że posiada interes w rozstrzygnięciu na korzyść zamawiającego, gdyż jego oferta została uznana obecnie za najkorzystniejszą, a uwzględnienie odwołania może spowodować odrzucenie oferty Qumak SA i pozbawienie go szansy na uzyskanie zamówienia. Wniósł o oddalenie odwołania jako bezzasadnego. Zgłoszenie zostało podpisane przez pełnomocnika działającego na podstawie pełnomocnictwa z dnia 5 października 2015r. udzielonego przez prezesa zarządu i prokurenta ujawnionych w KRS i upoważnionych do łącznej reprezentacji, zgodnie z odpisem z KRS załączonym do zgłoszenia. Kopia zgłoszenia została przekazana zamawiającemu i odwołującemu drogą elektroniczną w dniu 28 stycznia 2016r.

W dniu 1 lutego 2016r. przystępujący złożył pismo, w którym podtrzymał wniosek o oddalenie odwołania. Wyraził podgląd, że oferta równoważna, to nie oferta tożsama z przedmiotem zamówienia, ale posiadająca pewne istotne dla zamawiającego zbliżone do produktu referencyjnego cechy i parametry. Odwołał się do wyroku KIO z dnia 26 stycznia 2010r. sygn. akt KIO/UZP 1733/09 oraz wyroku KIO z dnia 10 kwietnia 2012r. sygn. akt KIO 573/12. Podkreślił, że wykazał spełnianie wymagań postawionych przez zamawiającego dla rozwiązania równoważnego, a w zakresie budzącym wątpliwości zamawiającego składał wyjaśnienia. Podkreślił, że odwołujący nie sprecyzował treści siwz, z którą byłaby sprzeczna oferta przystępującego oraz nie udowodnił któregoś z postawionych zarzutów.

W dniu 2 lutego 2016r. zamawiający złożył odpowiedź na odwołanie, w której oświadczył, że uwzględni w całości zarzuty odwołania.

Na posiedzeniu z udziałem stron i uczestników postępowania przystępujący zgłosił sprzeciw.

Izba ustaliła następujący stan faktyczny:

Izba dopuściła dowody z dokumentacji postępowania tj. : siwz wraz z załącznikami, wyjaśnień treści siwz z dnia 13 października 2015r., oferty wykonawcy Qumak SA, wezwania zamawiającego do Qumak SA z dnia 17 listopada 2015r., odpowiedzi wykonawcy Qumak z dnia 23 listopada 2015r., wezwania zamawiającego do Qumak SA z dnia 10 grudnia 2015r. oraz odpowiedzi wykonawcy Qumak SA udzielonej w dniu 15 grudnia 2015r.

Na podstawie powyższych dowodów Izba ustaliła, co następuje:

Treść pkt. 2 Router RT- TJE Funkcjonalności nr 4 pkt 22 oraz definicji równoważności dla GET VPN przytoczona w odwołaniu jest zgodna z treścią zawartą w załączniku nr 1a do siwz.

W załączniku nr 2 do siwz Opis przedmiotu zamówienia w rozdziale IV Projekt techniczny, instalacja i konfiguracja środowiska w części zatytułowanej - Lista wymaganych do uruchomienia i skonfigurowania usług sieciowych i bezpieczeństwa na dostarczanych routerach RT-TJE, zamawiający wskazał, że:

Wykonawca powinien zaimplementować funkcje które uruchomione są na wymienianych urządzeniach i skonfigurować je w taki sposób żeby spełniały takie same jak obecnie funkcje. W szczególności:

- przeniesienie obecnej konfiguracji GET VPN lub zastosowanie równoważnej technologii szyfrowania ruchu.
- przeniesienie obecnych list dostępu (ACL),
- przeniesienie obecnej konfiguracji QoS,
- konfiguracja routingu,

- dostęp poprzez SSHv2,
- SNMP.

Wykonawca powinien zaimplementować nowe funkcjonalności wynikające ze zmiany topologii spowodowanej wymianą urządzeń. W szczególności:

- Spięcie z obecną infrastrukturą w sposób wykorzystujący zalety wynikające z obecności redundancji urządzeń – konfiguracja połączeń zdublowanych,
- konfiguracja SNMP zgodnie z dostarczonym przez Zamawiającego szablonem,
- konfiguracja dedykowanego interfejsu do zdalnego zarządzania (do zaadresowania urządzenia),
- konfiguracja SSHv2,
- konfiguracja QoS dla telefonii IP,
- konfiguracja eksportu statystyk za pomocą NetFlow/J-Flow/sFlow (lub odpowiednika),
- TRUNK, Spanning tree,
- włączenie mechanizmów uwierzytelniania, autoryzacji i kontroli dostępu (AAA),
- konfiguracja połączenia z istniejącymi serwerami AAA (TACACS+/ Radius),
- konfiguracja szyfrowanej łączności backupowej z wykorzystaniem modułu 3G/4G LTE jednego z routerów.

Routery mają zapewnić obsługę łączy WAN. Zamawiający wymaga, żeby wymiana routerów odbyła się w sposób który umożliwi zachowanie ciągłości dla usługi szyfrowania ruchu przesyłanego przez sieć WAN. Podstawowa sieć WAN oparta jest na usłudze MPLS VPN operatora telekomunikacyjnego i zapewnia topologię typu full mesh. Szyfrowanie musi obowiązywać dla ruchu przesyłanego pomiędzy wszystkimi lokalizacjami zamawiającego.

Z wyjaśnień treści siwz z dnia 13 października 2015r. wynikają następujące ustalenia:

Na pytanie nr 7 o treści Załącznik nr 1 do SIWZ Formularz Specyfikacji Technicznej, punkt 2 Router RT-TJE, Element konfiguracji Funkcjonalność, podpunkt 22 c). Wymaganie: „oraz GET VPN lub równoważne”* w roli członka grupy w zakresie GET VPN, wymagana jest kompatybilność z routerami Cisco, które pełnią rolę członków grupy i serwera kluczy)”
Pytanie: Prosimy o podanie typu, modelu oraz ilości routerów które w sieci Zamawiającego pełnią rolę Serwerów kluczy (KS GET VPN) oraz Członków Grupy (GM GET VPN), zamawiający odpowiedział, że ze względów bezpieczeństwa nie może ujawniać szczegółowych rozwiązań dotyczących elementów bezpieczeństwa swojej sieci, w szczególności parametrów konfiguracji elementów sieci. Funkcjonalność GET VPN w roli członka grupy, opisana w Załącznik nr 1 do SIWZ Formularz Specyfikacji Technicznej, punkt 2 Router- RT-TJE, Element Konfiguracji: Funkcjonalność, podpunkt 22 c) jest realizowana w

sposób jednakowy przez wszystkie routery posiadające tę funkcjonalność. Funkcjonalność routerów Zamawiającego została określona w Załączniku nr 1 do SIWZ - Formularz Specyfikacji Technicznej, punkty 2 Router- RT-TJE, Warunki równoważności na rozwiązanie GET VPN, pkt 1.1, Zamawiający posiada routery pełniące te funkcje zarówno w TJE, jak i w Oddziałach oraz CPD i ZCPD, Szczegółowe informacje na temat funkcjonowania serwisu GET VPN, w szczególności dopuszczalna liczba serwerów kluczy, dostępne są w materiałach producentów sprzętu sieciowego.

W odpowiedzi na pytanie nr 8 o treści Załącznik nr 1 do SIWZ Formularz Specyfikacji Technicznej, punkt 2 Router - RT-TJE, **Warunki równoważności na rozwiązanie GET VPN, punkt 4.5. Wymaganie „rozwiązanie równoważne musi w pełni współpracować z systemami już eksploatowanymi u Zamawiającego,” Pytanie: Prosimy o podanie nazw oraz producentów eksploatowanych systemów oraz wymagane zakresy współpracy., zamawiający odpowiedział, że ze względów bezpieczeństwa nie może ujawniać szczegółowych rozwiązań dotyczących elementów bezpieczeństwa swojej sieci, w szczególności typów urządzeń, nazw oraz producentów oprogramowania bezpieczeństwa, czy parametrów konfiguracji elementów sieci. W celu umożliwienia Wykonawcom przygotowania oferty Zamawiający wyjaśnia, iż sformułowanie użyte w Załączniku nr 1 do SIWZ -Formularz Specyfikacji Technicznej, punkt 2 Router - RT-TJE, Warunki równoważności na rozwiązanie GET VPN, punkt 4.5. oznacza konieczność współpracy dostarczanych urządzeń z systemami Zamawiającego wymienionymi w pkt 1.1. Warunków równoważności na rozwiązanie GET VPN. Systemy te funkcjonują w obecnej sieci WAN o topologii full mesh. Należy zaznaczyć, iż konieczność bezkonfliktowej współpracy dostarczonych urządzeń odnosi się również do procesu wdrożenia, w którym wymiana poszczególnych urządzeń w TJE nie może spowodować przerwy w funkcjonowaniu sieci Zamawiającego, ani w funkcjonowaniu usługi szyfrowania ruchu przesyłanego przez sieć WAN, co zostało określone w OPZ, w pkt IV.PROJEKT TECHNICZNY, INSTALACJA I KONFIGURACJA ŚRODOWISKA, Lista wymaganych do uruchomienia i skonfigurowania usług sieciowych i bezpieczeństwa na dostarczanych .routerach RT-TJE Załącznika nr 2 do SIWZ - Opis przedmiotu zamówienia.

Na pytanie nr 11 o treści „Załącznik nr 1 do SIWZ Formularz Specyfikacji Technicznej, punkt 2 Router RT-TJE, Element Konfiguracji Funkcjonalność, punkt 22 b). Wymaganie: „dynamiczne, wielopunktowe tunelowe VPN” Pytanie: Czy poprzez wymaganie Zamawiający ma na myśli rozwiązanie w postaci dostarczenia technologii do automatycznego zestawiania tuneli site-to-site w oparciu o otwarte protokoły NHRP oraz mGRE? Jeśli nie to prosimy o wyjaśnienie, zamawiający odpowiedział, że nie określa szczegółowego sposobu

realizacji wymagania określonego w załączniku nr 1 do siwz –Formularz Specyfikacji Technicznej, pkt. 2 Router RT-TJE, Element Konfiguracji: Funkcjonalność pkt. 22b).

W ofercie Qumak na str. 81 w pkt. 2 Router RT-TJE, Elementy Konfiguracji pkt. 4 Funkcjonalność ppkt. 22 Qumak SA czterokrotnie oświadczył, że spełnia wymagania zamawiającego.

W dniu 17 listopada 2015r. zamawiający wezwał wykonawcę Qumak SA w trybie art. 87 ust. 1 ustawy do wyjaśnienia m. in. przez wykazanie (np. za pomocą dokumentów od producenta) czy urządzenie, tj. HUAWEI AR1220E, ma możliwość obsługi GET WPN lub równoważne w roli członka grupy, z wykorzystaniem następującej (standardowej w GET VPN zgodnie z opisem w Załączniku nr 1a do SIWZ, pod tabelą 2. Router-RT-TJE, „Warunki równoważności na rozwiązanie GET VPN”) funkcjonalności:

- a) możliwość pracy routera w roli członka grupy w sieci z minimum czterema serwerami kluczy (redundancja i rozproszenie geograficzne – każdy serwer kluczy w innej lokalizacji/podsieci)
- b) możliwość pracy w sieci nie obsługującej ruchu Multicast (Rekey w trybie Unicast),
- c) możliwość pracy w sieci minimum 250 współpracujących- routerów występujących w roli członka grupy,
- d) sposób wdrożenia nowych routerów tak, aby nie powodować przerw w obecnej szyfrowanej transmisji pomiędzy lokalizacjami Zamawiającego - wymiana/podłączenie nowych routerów powinno odbywać się w sposób powodujący jednoczesną niedostępność tylko jednej lokalizacji w sieci WAN o topologii full mesh. Należy zapewnić pełną współpracę z istniejącymi w sieci Zamawiającego routerami w zakresie szyfrowania przesyłanego ruchu, bez obniżania poziomu zabezpieczeń

Zamawiający wskazał, że w Formularzu Specyfikacji Technicznej, Qumak oświadczył, iż oferowane urządzenie tj. HUAWEI AR1220E posiada funkcjonalność, o której" mowa Tabeli 2 poz. 5 *Funkcjonalność, pkt 22 Zaawansowane funkcjonalności techniczne lit. c) GET VPN lub równoważne w roli członka grupy (w zakresie GET VPN wymagana jest kompatybilność i routerami Cisco, które pełnią rolę członków grupy i serwera kluczy).*

Zamawiający, opierając się na dostępnych mu materiałach, powziął wątpliwości, czy urządzenie spełnia ww, warunek.

W dniu 23 listopada 2015r. Qumak SA wyjaśnił, że urządzenie Huawei AR1220E posiada możliwość obsługi GET VPN lub równoważne w roli członka grupy z wykorzystaniem następującej funkcjonalności:

- a. Możliwość pracy routera w roli członka grupy w sieci z minimum czterema serwerami kluczy (redundancja i rozproszenie geograficzne - każdy serwer kluczy w innej lokalizacji/podsieci),

- b. Możliwość pracy w sieci nie obsługującej ruchu Multicast (Rekey w trybie Unicast, zgodnie z obsługiwany przez routery Cisco draftem IETF draft-weis-gdoi-rekey-ack)
- c. Możliwość pracy w sieci minimum 250 współpracujących routerów występujących w roli członka grupy
- d. Umożliwiają wdrożenie nowych routerów tak, aby nie powodować przerw w obecnie szyfrowanej transmisji pomiędzy lokalizacjami - wymiana/podłączenie nowych routerów może odbywać się w sposób powodujący jednoczesną niedostępność tylko jednej lokalizacji w sieci WAN o topologii full mesh, Ponadto zapewnia możliwość pełnej współpracy z istniejącymi w sieci Zamawiającego routerami w zakresie szyfrowania przesyłanego ruchu bez obniżania poziomu bezpieczeństwa.

Urządzenie Huawei AR1220E spełnia wymagania SIWZ. Na potwierdzenie przedstawił oświadczenie producenta zaoferowanych urządzeń.

Z oświadczenia producenta wynika, że urządzenie Huawei AR1220E ma możliwość obsługi GET VPN lub równoważne w roli członka grupy z wykorzystaniem następującej funkcjonalności:

- a. Możliwość pracy routera w roli członka grupy w sieci z minimum czterema serwerami kluczy (redundancja i rozproszenie geograficzne - każdy serwer kluczy w innej lokalizacji/podsieci),
- b. Możliwość pracy w sieci nie obsługującej ruchu Multicast (Rekey w trybie Unicast), zgodnie z obsługiwany przez routery Cisco draftem IETF draft-weis-gdoi-rekey-ack)
- c. Możliwość pracy w sieci minimum 250 współpracujących routerów występujących w roli członka grupy
- d. Umożliwiają wdrożenie nowych routerów tak, aby nie powodować przerw w obecnie szyfrowanej transmisji pomiędzy lokalizacjami - wymiana/podłączenie nowych routerów może odbywać się w sposób powodujący jednoczesną niedostępność tylko jednej lokalizacji w sieci WAN o topologii full mesh. Ponadto zapewnia możliwość pełnej współpracy z istniejącymi w sieci Zamawiającego routerami w zakresie szyfrowania przesyłanego ruchu bez obniżania poziomu bezpieczeństwa.

W dniu 10 grudnia 2015r. zamawiający ponownie w trybie art. 87 ust. 1 ustawy wezwał Qumak SA do wyjaśnienia treści oferty przez wykazanie (np. za pomocą dokumentów od producenta) czy urządzenie, tj. HUAWEI AR1220E, ma możliwość obsługi GET VPN lub równoważne w roli członka grupy, z wykorzystaniem następującej (standardowej w GET

VPN zgodnie z opisem w Załączniku nr 1a do SIWZ, pod tabela 2. Router-RT-TJE, „** Warunki równoważności na rozwiązanie GET VPN”) funkcjonalności:

b. możliwość pracy w sieci nie obsługującej ruchu Multicast (w której proces odnowienia kluczy (Rekey) odbywa się w trybie Unicast). Zamawiający wskazał, że Qumak odnosi się do dokumentu (draft-weis-gdoi-rekey-ack), który nie jest dokładnie oznaczony (brakuje pełnego adresu sieciowego do dokumentu), ani nie jest aktualny (dokument dostępny na stronach organizacji The Internet Engineering Task Force (IETF <https://datatracker.ietf.org/doc/draft-weis-gdoi-rekey-ack/> jest oznaczony statusem - nieaktualny (expired). Nie jest również jasne, jaką rolę ma pełnić przywołany dokument przy wykazywaniu spełniania wymagania, Dostępna w sieci dokumentacja techniczna oferowanego urządzenia HUAWEI AR1220E potwierdza niespełnianie wymagania o którym mowa.

W dniu 15 grudnia 2015r. Qumak SA odpowiedział, że routery Huawei AR1220E mają możliwość pracy w sieci nie obsługującej Multicast poprzez funkcjonalność Rekey w trybie Unicast zgodnie z draftem IETF draft-weis-gdoi-rekey-ack-01 opublikowanym na stronie <https://tools.ietf.org/html/draft-weis-gdoi-rekey-ack-01>. Qumak wskazał też, że kluczowa w tym rozwiązaniu jest pełna zgodność i równoważność do rozwiązania firmy Cisco - GET VPN, które zapewnia Unicast Rekey zgodnie z tym samym draftem IETF draft-weis-gdoi-rekey-ack-01, co zostało udokumentowane na stronie Cisco: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-mt/sec-get-vpn-15-mt-book.pdf

W szczególności odnoszą się do tego następujące fragmenty powyższego dokumentu:

- strona 12 rozdział zatytułowany „Unicast Rekeying and Sas”,
- strona 248 rozdział zatytułowany „Additional References for GET VPN Interoperability”, tabela druga zatytułowana „Standards and RFCs”,

które Qumak dołączył do wyjaśnień wraz z tłumaczeniem na język polski.

Tym samym Qumak wskazał, iż równoważność i pełna zgodność z tym samym draftem IETF zapewnia jednocześnie interoperacyjność obu rozwiązań, a więc możliwość pracy routerów Cisco i Huawei w jednej sieci GET VPN. Podkreślił, że funkcjonalność Rekeying w GET VPN jest realizowana w routerach Cisco za pomocą dwóch metod: metoda własna Cisco (ang. Cisco proprietary) oraz zgodnie z wspomnianym draftem IETF, Routery Cisco pełniące rolę serwerów kluczy mogą obsługiwać obie te metody równolegle - można więc posiadać w sieci routery Cisco pełniące rolę członków grupy i korzystające z rozwiązania własnego Cisco, jak i jednocześnie routery Huawei lub Cisco korzystające z rozwiązania opartego o draft IETF, Metoda Cisco jest własnym, opatentowanym rozwiązaniem firmy Cisco, z którego nie mogą korzystać inni producenci. Natomiast wspomniany wyżej draft IETF jest otwartym standardem, który może być implementowany przez innych producentów. Zamawiający opisując przedmiot zamówienia dopuścił zastosowanie równoważnego rozwiązania dla wymagania GET VPN. Tym samym musiał mieć świadomość, że wspomniana funkcjonalność innego producenta niż

Cisco musi być realizowana w oparciu o draft IETF. Qumak wskazał ponadto, że ostatnia dostępna w sieci dokumentacja jest datowana na 30 sierpnia 2015 i nie zawiera jeszcze informacji na temat funkcjonalności będącej przedmiotem niniejszego wyjaśnienia.

Z podręcznika konfiguracji sieci szyfrowanych za pomocą technologii GET VPN, Cisco IOS wersja 15M&T wynikają następujące standardy :

- draft – weis-delay-detection-00, draft-weis-gdoi-rekey-ack-01, RFC 5373 Sekcja 5.4. – Polityka powiązanych grup, RFC 6407 – Sekcja 4.2.1. Opóźnienie czasu uruchomienia.

Z pisma Cisco Systems Polska spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie wynika że oprogramowanie IOS 12.4 routerów ISK nie wspiera następujących funkcjonalności - draft – weis-delay-detection-00, draft-weis-gdoi-rekey-ack-01, RFC 6407 – Activation Time Delay. Wsparcie tych funkcjonalności występuje od wersji oprogramowania 15.5 (1) T.

Z oświadczenia Huawei Polska spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie wynika, że producent routerów Huawei potwierdza interoperacyjność routerów Huawei z routerami Cisco zarówno poprzez wspieranie przez urządzenia Huawei standardu - draft-weis-gdoi-rekey-ack-01, jak i poprzez wspieranie standardu - draft – weis-delay-detection-00, i funkcjonalności Activation Time Delay zdefiniowanej w kodzie RFC 6407 . Wsparcie tych standardów i funkcjonalności zapewnia możliwość wymiany starych routerów Cisco zgodnie z intencją zamawiającego i wymaganiami siwz.

Z oświadczenia Huawei Polska spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie wynika, że producent routerów Huawei oświadczył, że oferowane rozwiązanie spełnia również wymagania interoperacyjności z wersją 12.4 oprogramowania routerów Cisco. Funkcjonalność ze standardu draft-weis-gdoi-rekey-ack-01, którą Cisco obsługuje w oprogramowaniu w wersji 15 jest wymagana tylko na serwerach kluczy oraz na nowych routerach dostarczonych w ramach postępowania. Stare routery Cisco, które tymczasowo w trakcie procesu wymiany będą jeszcze działać razem z nowymi routerami w jednej sieci nie muszą tej funkcjonalności posiadać (mogą mieć software 12.4). Serwer kluczy Cisco będzie obsługiwał stare routery Cisco technologią własną, a nowe routery według technologii otwartej. Nowe i stare routery będą mogły się porozumiewać i do tego nie jest wymagana obsługa funkcjonalności ze standardu draft-weis-gdoi-rekey-ack-01 przez stare routery Cisco z oprogramowaniem 12.4. Gdyby potraktować ten zapis inaczej to oznaczałoby to, że nie można zaoferować routerów innych niż Cisco, co ogranicza konkurencję i jest niezgodne z intencją zamawiającego, który dopuścił rozwiązania równoważne, a nie tylko Cisco.

Z odpisu z KRS dla Huawei Polska sp. z o.o. wynika, że osoba składająca omówione wyżej dwa oświadczenia jest prokurentem samoistnym tej firmy.

Z artykułu pt. Huawei zmodernizował część sieci WAN w PKP Polskich Liniach Kolejowych SA” wynika, że routery ASR1000 i ISR firmy Cisco komunikują się z routerami AR2240 firmy Huawei przez połączenie wykorzystywanej w PKP PLK technologii Cisco DMVPN z technologią Huawei DSVPN.

Izba oceniła dowody z certyfikatów firmy Huawei i Cisco wystawione na nazwisko P. G. jako nieistotne dla rozstrzygnięcia, gdyż po pierwsze zostały przedstawione w języku obcym bez wymaganego regulaminem przy rozpoznawaniu odwołań tłumaczenia, a nadto mają potwierdzać kompetencję techniczne pełnomocnika przystępującego, które nie były przez strony kwestionowane, a sam pełnomocnik nie był osobowym źródłem dowodowym.

Izba zważyła co następuje:

Izba stwierdziła, że zgłoszone przystąpienie spełnia wymogi formalne określone w art. 185 ust. 2 ustawy.

Izba nie dopatrzyła się zaistnienia przesłanek określonych w art. 189 ust. 2 ustawy, które skutkowałyby odrzuceniem odwołania.

Izba ustaliła, że odwołujący wykazał interes w uzyskaniu przedmiotowego zamówienia oraz możliwość poniesienia przez niego szkody spełniając przesłanki wynikające z art. 179 ust. 1 ustawy.

Zarzut naruszenia przez zamawiającego art. 7 ustawy, art. 82 ustawy, art. 89 ust. 1 pkt 2 ustawy, a w konsekwencji naruszenie art. 91 ust. 1 i 2 ustawy przez zaniechanie odrzucenia oferty wykonawcy Qumak mimo tego, że wykonawca ten nie wykazał określonych w załączniku nr 1a do siwz w pkt. 2 Routery RT-TJE ppkt. 4 Funkcjonalność ppkt 22 lit. c oraz GET VPN lub równoważne** w roli członka grupy (w zakresie GET VPN, wymagana jest kompatybilność z routerami Cisco, które pełnią rolę członków grupy i serwera kluczy), a w szczególności pkt. 4.6. warunków równoważności: rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamiennność produktu z funkcjonalnością GET VPN systemu IOS 15 universaik9: ipbasek9+securityk9 oraz IOS 12.4 advipservicesk9 tj. nie wykazał, że oferowane routery zapewniają standardy draft-weis-delay-detection-00 i Activation Time Delay- RFC 6407 oraz, że zaoferowane routery zapewniają współpracę ze wszystkimi routerami zamawiającego, w tym opartymi o oprogramowanie IOS 12.4 advipservicesk9.

Zarzut częściowo zasługuje na uwzględnienie. Przepis art. 7 ust. 1 ustawy stanowi, że zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców, zaś z

ust. 3 tegoż przepisu wynika, iż zamówienia udziela się wyłącznie wykonawcy wybranemu zgodnie z przepisami ustawy. W myśl art. 82 ust. 1 ustawy wykonawca może złożyć jedną ofertę, natomiast ust. 3 stanowi, że treść oferty musi odpowiadać treści specyfikacji istotnych warunków zamówienia. Zgodnie z przepisem art. 89 ust. 1 pkt 2 ustawy zamawiający odrzuca ofertę, jeżeli jej treść nie odpowiada treści specyfikacji istotnych warunków zamówienia, z zastrzeżeniem art. 87 ust. 2 pkt 3 ustawy.

Zgodnie z art. 91 ust. 1 ustawy zamawiający wybiera ofertę najkorzystniejszą na podstawie kryteriów oceny ofert określonych w specyfikacji istotnych warunków zamówienia. Kryteriami oceny ofert są według art. 91 ust. 2 ustawy - cena albo cena i inne kryteria odnoszące się do przedmiotu zamówienia, w szczególności jakość, funkcjonalność, parametry techniczne, aspekty środowiskowe, społeczne, innowacyjne, serwis, termin wykonania zamówienia oraz koszty eksploatacji.

Mając powyższe ramy prawne na uwadze Izba stwierdziła, że zarzut dotyczący niewykazania równoważności oferowanych rozwiązań z uwagi na niewykazanie, że urządzenie router Huawei AR1220E wspiera poza standardem draft-weis-gdoi.rekey-ack-01 także standardy draft-weis-delay0detection-00 i Activation Time Delay nie potwierdził się, gdyż w tym zakresie Izba w oparciu o oświadczenie producenta urządzenia z dnia 2 lutego 2016r. ustaliła, że oferowane urządzenie wspiera wszystkie trzy opisane przez odwołującego standardy. Biorąc to pod uwagę Izba oceniła, że w tym zakresie nie można w treści oferty przystępującego dopatrzeć się niezgodności z treścią siwz tj. z wymaganiem określonym w załączniku nr 1a do siwz w pkt. 2 Routery RT-TJE ppkt. 4 Funkcjonalność ppkt 22 lit. c oraz GET VPN lub równoważne** w roli członka grupy (w zakresie GET VPN, wymagana jest kompatybilność z routerami Cisco, które pełnią rolę członków grupy i serwera kluczy).

Natomiast Izba oceniając zgromadzony materiał dowodowy uznała, że druga z podstaw faktycznych zarzutu zasługuje na uwzględnienie. W tym zakresie Izba oparła się na preambule załącznika nr 1 a do siwz oraz literalnym brzmieniu pkt. 4.6. pod tabelą 2. Routery RT-TJE tj. rozwiązanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienną produktu z funkcjonalnością GET VPN systemu IOS 15 universaik9: ipbasek9+securityk9 oraz IOS 12.4 advipservicesk9. Izba podzieliła w tym zakresie stanowisko odwołującego i zamawiającego, że z treści tych postanowień wynika, że zamawiający przez rozwiązanie rozumiał produkt równoważny, a zatem oferowany router. Izba uznała także, że literalna treść postanowienia 4.6. cytowanego powyżej świadczy o tym, że równoległa współpraca w czasie rzeczywistym miała dotyczyć współpracy z funkcjonalnością GET VPN tak dla systemu IOS 15 jak i IOS 12.4. Zamawiający w pkt 1 wymagań równoważności wyraźnie opisał, że posiada obecnie wdrożony system szyfrowania w sieci WAN w topologii full mesh, oparty o z technologię GET VPN, o który oparty jest na licencjach oprogramowania systemowego IOS

15 universalk9: ipbasek9+securityk9 oraz IOS 12.4 advipservicesk9 funkcjonujących na urządzeniach sieciowych firmy CISCO.

Zamawiający nie określał które z oprogramowań systemowych funkcjonuje na routerach typu Key Serwer, a które na routerach typu Group Member. Wymagał nadto w pkt. 4.3., że rozwiązanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem funkcjonującym u zamawiającego, a w pkt 4.4., że rozwiązanie równoważne nie może zakłócić pracy środowiska systemowo-programowego zamawiającego, oraz zgodnie z pkt. 4.5. rozwiązanie równoważne musi w pełni współpracować z systemami już eksploatowanymi u zamawiającego. W świetle tych postanowień siwz w ocenie Izby prawidłową należy przyjąć interpretację postanowień siwz dokonaną przez zamawiającego i odwołującego, że wymogiem treści siwz było, aby router Huawei AR 1220E zapewniał równoległą współpracę w czasie rzeczywistym z routerem Cisco pracującym w systemie IOS 12.4 advipservicesk9. Wobec tak ustalonej treści siwz. Izba oceniła, że z dowodu przedstawionego przez przystępującego tj. oświadczenia producenta urządzenia z dnia 2 lutego 2016r. wynika, że przystępujący nie przewiduje bezpośredniej współpracy tych urządzeń, a komunikację pomiędzy nimi zamierza przeprowadzić za pośrednictwem routerów Cisco wyposażonych w wersję oprogramowania IOS 15. W ocenie Izby, choć być może taki sposób komunikacji, jest logiczny i mógłby technicznie rozwiązywać brak bezpośredniej współpracy urządzeń, to jednak nie został dopuszczony przez zamawiającego jako warunek równoważności. W tym stanie rzeczy należało ocenić, iż treścią oferty jest zaprezentowane w piśmie producenta urządzenia rozwiązanie, a tak ustalona treść nie odpowiada ustalonej treści siwz. Próba doprowadzenia do zgodności tych treści powodowałaby istotną zmianę treści oferty, a zatem nie było możliwe zastosowanie art. 87 ust. 2 pkt 3 ustawy. W konsekwencji Izba oceniła, że zamawiający naruszył przepis art. 89 ust. 1 pkt 2 ustawy przez jego niezastosowanie, a konsekwencji wybrał jak najkorzystniejszą ofertę, która powinna podlegać odrzuceniu, co oznacza, że zamawiający naruszył także art. 7 i 91 ust. 1 ustawy. W świetle powyższego konieczne stało się uwzględnienie odwołania i nakazanie zamawiającemu unieważnienia czynności oceny ofert, unieważnienia czynności wyboru oferty jako najkorzystniejszej oferty Qumak Spółka Akcyjna z siedzibą w Warszawie, nakazanie powtórzenia oceny ofert, dokonania zaniechanej czynności odrzucenia oferty Qumak Spółka Akcyjna z siedzibą w Warszawie na podstawie art. 89 ust. 1 pkt 2 ustawy z uwagi na to, że treść oferty tego wykonawcy nie odpowiada treści specyfikacji istotnych warunków zamówienia określonej w załączniku nr 1 a do siwz w pkt. 4.6. tj. zaoferowane rozwiązanie równoważne nie zapewnia pełnej, równoległej współpracy w czasie rzeczywistym i pełnej funkcjonalnej zamienności produktu z funkcjonalnością GET VPN systemu IOS 12.4 advipservicesk9 oraz nakazanie dokonania wyboru oferty najkorzystniejszej.

Mając na uwadze powyższe orzeczono jak w sentencji na podstawie art. 192 ust.1, 2, 3 ustawy.

O kosztach postępowania orzeczono na podstawie art. 192 ust. 9 i 10 ustawy stosownie do wyniku spraw oraz zgodnie z § 3 pkt. 1 i § 5 ust. 2 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 15 marca 2010 r. w sprawie wysokości i sposobu pobierania wpisu od odwołania oraz rodzajów kosztów w postępowaniu odwoławczym i sposobu ich rozliczania (Dz. U. Nr 41, poz. 238) obciążając przystępującego kosztami postępowania w postaci uiszczonego przez odwołującego wpisu od odwołania oraz nakazując przystępującemu dokonanie zwrotu na rzecz odwołującego kosztów związanych z wniesionym wpisem.

Przewodniczący: