Sygn. akt: KIO 1507/22

WYROK

z dnia 24 czerwca 2022 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący: **Ewa Sikorska**

Członkowie: **Justyna Tomkowska**

Agnieszka Trojanowska

Protokolant: **Rafał Komoń**

po rozpoznaniu na rozprawie w dniu 21 czerwca 2022 roku w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 6 czerwca 2022 r. przez wykonawcę **PYSENSE Spółka z ograniczoną odpowiedzialnością we Wrocławiu** w postępowaniu prowadzonym przez zamawiającego – **PGE Dystrybucja Spółka akcyjna Oddział w Lublinie**

przy udziale:

A. wykonawcy **Elmess Metering Spółka z ograniczoną odpowiedzialnością w Zgierzu,** zgłaszającego przystąpienie do postępowania odwoławczego po stronie **odwołującego,**

B. wykonawcy **Esmetric Spółka z ograniczoną odpowiedzialnością Spółka komandytowa w Warszawie,** zgłaszającego przystąpienie do postępowania odwoławczego po stronie **zamawiającego,**

orzeka:

1. umarza odwołanie w zakresie zarzutów naruszenia:
- art. 16 pkt 1 i 3 w zw. z art. 66 Dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z dnia 16 lutego 2014 roku w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca Dyrektywę 2004/17/WE z dnia 26 lutego 2014 roku (Dz. Urz.UE.L Nr 94, str. 243) poprzez wyznaczenie zbyt krótkiego terminu składania ofert, ograniczającego konkurencję i nieodpowiedniego do specyfiki zamówienia oraz niewystarczającego do ich przygotowanie i złożenia, w sytuacji, w której zgodnie z pkt. 5.1.1-5.1.11 specyfikacji warunków zamówienia (s.w.z.) wraz z ofertą wymagane jest złożenie próbek oraz dotyczących ich pozostałych

przedmiotowych środków dowodowych, co prowadzi dodatkowo do naruszenia zasad uczciwej konkurencji i równego traktowania wykonawców oraz zasady proporcjonalności,
- art. 16 pkt 1, 2, 3 w zw. z art. 106 ust. 1-3 oraz w zw. z art. 107 ust. 1 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz. U. z 2021 roku, poz. 1129 ze zm. – ustawa P.z.p.) poprzez wskazane w sposób ogólny i niejednoznaczny wymagań w zakresie żądanych przedmiotowych środków dowodowych, przy jednoczesnym braku przewidzenia możliwości ich uzupełnienia w przypadku, gdy złożone przedmiotowe środki dowodowe niekompletne, co jest nieproporcjonalne i naruszające zasady uczciwej konkurencji i równego traktowania wykonawców w odniesieniu w szczególności do przedmiotowych środków dowodowych wskazanych w pkt. 5.1.5, 5.1.8, 5.1.9, 5.1.10, i 5.1.11 s.w.z.,
- art. 99 ust. 1, 2 i 4 oraz art. 103 ust. 3 w zw. z 16 pkt 1 i 3 ustawy P.z.p. poprzez opisanie przedmiotu zamówienia w sposób niejednoznaczny i niejasny oraz niedostatecznie wyczerpujący i wewnętrznie sprzeczny, a także nieproporcjonalny do przedmiotu zamówienia i naruszający uczciwą konkurencję, w zakresie dotyczącym wymagań bezpieczeństwa dla modemów,
- art. 436 pkt 3 ustawy P.z.p. w zw. z art. 5 oraz art. 487 § 2 ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny (Dz. U. 2020 r., poz. 1740 ze zm. – K.c.) w zw. z art. 8 ust. 1 ustawy P.z.p. poprzez sporządzenie wzoru umowy w sposób niezgodny z przepisami ustawy oraz naruszający zasady współżycia społecznego i równowagę stron umowy oraz nadmiernie obciążający wykonawcę w zakresie, w jakim zamawiający przewidział nadmiernie wysoki limit łącznej maksymalnej wartości kar umownych oraz wyłączył spod niego kary z tytułu odstąpienia od umowy;

2. w pozostałym zakresie odwołanie oddala;

3. kosztami postępowania obciąża wykonawcę **PYSENSE Spółka z ograniczoną odpowiedzialnością we Wrocławiu** i**:**

3.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **15 000 zł 00 gr** (słownie: piętnaście tysięcy złotych zero groszy) uiszczoną przez wykonawcę **PYSENSE Spółka z ograniczoną odpowiedzialnością we Wrocławiu** tytułem wpisu od odwołania,

Stosownie do art. 579 ust. 1 i 580 ust. 1 i 2 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.), na niniejszy wyrok, w terminie 14 dnia od dnia jego doręczenia, przysługuje skarga, za pośrednictwem Prezesa Krajowej Izby Odwoławczej, do Sądu Okręgowego w Warszawie.

……

……

……

Uzasadnienie

Zamawiający – PGE Dystrybucja Spółka akcyjna Oddział w Lublinie – prowadzi postępowanie o udzielenie zamówienia publicznego, którego przedmiotem jest „Dostawa Liczników Zdalnego Odczytu 1 i 3-fazowych dla odbiorców końcowych przyłączonych do sieci niskiego napięcia w podziale na 3 Części".

Postępowanie prowadzone jest na podstawie przepisów ustawy z dnia 11 września 2019 roku (Dz. U. z 2021 roku, poz. 1129 ze zm.), zwanej dalej ustawą P.z.p.

W dniu 6 czerwca 2022 roku wykonawca PYSENSE Spółka z ograniczoną odpowiedzialnością we Wrocławiu (dalej: odwołujący) wniósł odwołanie wobec treści ogłoszenia o zamówieniu i warunków zamówienia ustalonych przez zamawiającego.

Odwołujący zarzucił zamawiającemu naruszenie:

1) art. 16 pkt 1 i 3 w zw. z art. 66 Dyrektywy Parlamentu Europejskiego i Rady 2014/25/UE z dnia 16 lutego 2014 roku w sprawie udzielania zamówień przez podmioty działające w sektorach gospodarki wodnej, energetyki, transportu i usług pocztowych, uchylająca Dyrektywę 2004/17/WE z dnia 26 lutego 2014 roku (Dz. Urz.UE.L Nr 94, str. 243) poprzez wyznaczenie zbyt krótkiego terminu składania ofert, ograniczającego konkurencję i nieodpowiedniego do specyfiki zamówienia oraz niewystarczającego do ich przygotowanie i złożenia, w sytuacji, w której zgodnie z pkt. 5.1.1-5.1.11 specyfikacji warunków zamówienia (s.w.z.) wraz z ofertą wymagane jest złożenie próbek oraz dotyczących ich pozostałych przedmiotowych środków dowodowych, co prowadzi dodatkowo do naruszenia zasad uczciwej konkurencji i równego traktowania wykonawców oraz zasady proporcjonalności,
2) art. 16 pkt 1, 2, 3 w zw. z art. 106 ust. 1-3 oraz w zw. z art. 107 ust. 1 ustawy z dnia 11 września 2019 roku – Prawo zamówień publicznych (Dz. U. z 2021 roku, poz. 1129 ze zm. – ustawa P.z.p.) poprzez wskazane w sposób ogólny i niejednoznaczny wymagań w zakresie żądanych przedmiotowych środków dowodowych, przy jednoczesnym braku przewidzenia możliwości ich uzupełnienia w przypadku, gdy złożone przedmiotowe środki dowodowe niekompletne, co jest nieproporcjonalne i naruszające zasady uczciwej konkurencji i równego traktowania wykonawców w odniesieniu w szczególności do przedmiotowych środków dowodowych wskazanych w pkt. 5.1.5, 5.1.8, 5.1.9, 5.1.10, i 5.1.11 s.w.z.,
3) art. 99 ust. 1, 2 i 4 oraz art. 103 ust. 3 w zw. z 16 pkt 1 i 3 ustawy P.z.p. poprzez opisanie przedmiotu zamówienia w sposób niejednoznaczny i niejasny oraz niedostatecznie wyczerpujący i wewnętrznie sprzeczny, a także nieproporcjonalny do przedmiotu

zamówienia i naruszający uczciwą konkurencję, w zakresie dotyczącym wymagań bezpieczeństwa dla liczników zdalnego odczytu oraz modemów,
4) art. 436 pkt 3 ustawy P.z.p. w zw. z art. 5 oraz art. 487 § 2 ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny (Dz. U. 2020 r., poz. 1740 ze zm. – K.c.) w zw. z art. 8 ust. 1 ustawy P.z.p. poprzez sporządzenie wzoru umowy w sposób niezgodny z przepisami ustawy oraz naruszający zasady współżycia społecznego i równowagę stron umowy oraz nadmiernie obciążający wykonawcę w zakresie, w jakim zamawiający przewidział nadmiernie wysoki limit łącznej maksymalnej wartości kar umownych oraz wyłączył spod niego kary z tytułu odstąpienia od umowy.

Odwołujący wniósł o uwzględnienie odwołania i nakazanie zamawiającemu dokonania zmiany ogłoszenia o zamówieniu oraz postanowień s.w.z. i załączników, w sposób uwzględniający argumentację odwołania zawartą w uzasadnieniu, tj.:
1) zmianę terminu składania ofert i próbek na dzień nie wcześniejszy niż 25.10.2022 r.;
2) zmianę pkt 5.2 s.w.z. poprzez przewidzenie wezwania przez zamawiającego do uzupełnienia przedmiotowych środków dowodowych, o których mowa w pkt 5.1 . 5, 5.1.8, 5.1.9, 5.1 .10 i 5.1.11 s.w.z. w wyznaczonym terminie, w przypadku, gdy nie zostały one złożone lub będą niekompletne;
3) modyfikację załącznika nr 1 do s.w.z. - Opis przedmiotu zamówienia (OPZ) w pkt. 3.F pkt 8 poprzez usunięcie lit. a);
4) modyfikację postanowień OPZ w pkt 3.B ppkt 1 1 i 12 poprzez usunięcie dotychczasowych wymagań i zastąpienie ich wymaganiem stosowania w komunikacji bezpośredniej między licznikiem a systemem pomiarowym OSD oraz oprogramowaniem narzędziowym oraz w komunikacji przez optozłącze oraz na innych interfejsach komunikacyjnych, standardu DLMS Security Suite 1 lub DLMS Security Suite 2.
5) zmianę brzmienia §17 ust. 4 umowy, poprzez obniżenie maksymalnej łącznej wysokości kar umownych do poziomu 20% wartości netto umowy określonej w § 3 ust. 1 pkt 1 umowy;
6) zmianę brzmienia §17 ust. 4 umowy, poprzez usunięcie sformułowania „nie wliczając w to kar z tytułu odstąpienia od umowy”, tj. objęcie limitem łącznej maksymalnej wysokości kar umownych wszystkich kar przewidzianych w umowie.

Odwołujący podniósł, że ma interes we wniesieniu odwołania. W wyniku naruszenia przez zamawiającego ww. przepisów ustawy, interes odwołującego w uzyskaniu zamówienia doznał uszczerbku, gdyż objęta odwołaniem czynność zamawiającego (ukształtowane w postępowaniu warunki zamówienia) uniemożliwia odwołującemu ubieganie się o udzielenie zamówienia i przygotowanie prawidłowej oferty, a tym samym, wybór jego oferty i uzyskanie przedmiotowego zamówienia może okazać się niemożliwe. Wskazał, iż uwzględnienie odwołania doprowadzi do eliminacji dokonanego przez zamawiającego nadmiernie rygorystycznego i nieproporcjonalnego do przedmiotu zamówienia ograniczenia kręgu

potencjalnych wykonawców, w tym odwołującego, którzy będą mogli złożyć ofertę z realną szansą na uzyskanie zamówienia. Wskazał nadto, iż objęta odwołaniem czynność zamawiającego prowadzi do możliwości poniesienia szkody przez odwołującego polegającej na uniemożliwieniu odwołującemu złożenia oferty i ubiegania się o udzielenie zamówienia. Odwołujący stwierdził, że ma interes we wniesieniu odwołania, gdyż sprzeczna z ustawą ww. czynność zamawiającego w sposób negatywny oddziałuje na możliwość uzyskania przed odwołującego przedmiotowego zamówienia.

W odpowiedzi na odwołanie z dnia 20 czerwca 2022 roku zamawiający wniósł o:

1. oddalenie odwołania w zakresie zarzutów nieuwzględnionych przez zamawiającego;
2. zasądzenie kosztów postępowania.

Zamawiający uwzględnił zarzut 1 odwołania i zmienił wyznaczony termin składania ofert na dzień 5 października 2022 r., a więc wydłużył pierwotny termin o 3 miesiące (z 05.07. na 05.10.2022 r.). Zamawiający uwzględnił argumenty odwołującego, z których wynika złożoność zamówienia oraz czas konieczny na przygotowanie oferty, zwłaszcza w sytuacji, gdy wraz z ofertą wykonawca ma obowiązek przedłożyć próbkę oferowanego urządzenia.

W ocenie zamawiającego termin 5 października 2022 r. jest wystarczający i obiektywnie umożliwiający przygotowanie rzetelnej oferty przez wszystkich wykonawców, a więc zasada konkurencji w ogłoszonym postępowaniu nie ucierpi. Odwołujący domagał się wydłużenia terminu składania ofert o 3 miesiące i 20 dni, zamawiający wydłużył o 3 miesiące, a więc zamawiający uwzględnił żądanie odwołującego w ponad 80%.

W świetle powyższego, zamawiający wniósł o oddalenie zarzutu.

Zamawiający uwzględnił zarzut 2 i zgodnie z art. 107 ust. 2 ustawy P.z.p. przewidział czynność wezwania do złożenia lub uzupełnienia w wyznaczonym terminie przedmiotowych środków dowodowych. Zamawiający podtrzymał brak możliwości uzupełnienia próbek urządzeń, zgodnie z punktem 5.3. s.w.z.

Zamawiający wniósł o oddalenie zarzutów 3 i 4.

Do postępowania odwoławczego po stronie odwołującego przystąpił wykonawca Elmess Metering Spółka z ograniczoną odpowiedzialnością w Zgierzu (przystępujący 1). Przystępujący 1 poparł stanowisko odwołującego i wniósł o uwzględnienie odwołania.

Do postępowania odwoławczego po stronie zamawiającego przystąpił wykonawca Esmetric Spółka z ograniczoną odpowiedzialnością Spółka komandytowa w Warszawie (przystępujący 2). Przystępujący 2 oświadczył, że nie wnosi sprzeciwu wobec uwzględnienia przez zamawiającego zarzutów odwołania. W zakresie zarzutów nieuwzględnionych przez zamawiającego, przystępujący 2 poparł stanowisko zamawiającego i wniósł o ich oddalenie.

Na posiedzeniu Krajowej Izby Odwoławczej w dniu 21 czerwca 2022 roku odwołujący oświadczył, że cofa zarzut 1, wnosi o umorzenie zarzutu nr 2, cofa zarzut 4, cofa zarzut 3 w zakresie żądania określonego pkt 3, str. 3 odwołania, tj. modyfikacji załącznika nr 1 do s.w.z. - Opis przedmiotu zamówienia (OPZ) w pkt 3.F pkt 8 poprzez usunięcie lit. a.

Odwołujący oświadczył, że modyfikuje żądanie 4 na str. 3 odwołania poprzez zastąpienie dotychczasowych zapisów wymaganiem stosowania w komunikacji przez optozłącze oraz innych interfejsach komunikacyjnych standardu DLMS Security Suite 0 z możliwością późniejszej zdalnej aktualizacji oprogramowania do standardu DLMS Security Suite 1. Urządzenie/licznik powinno spełniać wymagania pamięciowe i sprzętowe obydwu standardów.

Uzasadniając podtrzymany zarzut odwołujący w treści odwołania podniósł, że w punkcie 3.B ppkt 11 OPZ zamawiający wymaga, aby komunikacja przez optozłącze oraz na innych interfejsach komunikacyjnych miała możliwość szyfrowania algorytmem AES co najmniej 128 bit (HLS) dla protokołu odczytu danych zgodnego z DLMS/COSEM.

Dodatkowo w punkcie 3.B ppkt 12 zamawiający wymaga, aby komunikacja bezpośrednia między licznikiem a systemem pomiarowym OSD oraz oprogramowaniem narzędziowym miała możliwość szyfrowania algorytmem AES co najmniej 128 bit (HLS) dla protokołu odczytu DLMS/COSEM na całej ścieżce komunikacji. Wymagane jest uwierzytelnianie licznika podczas nawiązywania komunikacji z systemem pomiarowym OSD oraz oprogramowaniem narzędziowym.

Odwołujący wskazał, że biorąc pod uwagę to, że liczniki energii elektrycznej, których wymaga zamawiający są wyposażone w układ rozłącznikowy, implikuje to, że trzeba traktować tego typu urządzenia jako infrastrukturę krytyczną, która powinna być zabezpieczona za pomocą najwyższych możliwych standardów bezpieczeństwa w zakresie szyfrowania, autoryzacji oraz wymiany certyfikatów. Należy również zwrócić uwagę na fakt, że zamawiający wymaga w punkcie A. 3 aby „Budowa licznika zapewniała możliwość fizycznego użytkowania zgodnie z jego przeznaczeniem przez okres co najmniej 12 lat.”

Odwołujący podniósł, że zgodnie z obowiązującymi standardami i normami bezpieczeństwa, a także profesjonalną wiedzą odwołującego w tym zakresie (odwołujący

jest aktywnym członkiem DLMS User Association), powyższe wymagania stanowią zagrożenie bezpieczeństwa komunikacji oraz zawierają niedoprecyzowane wymagania w zakresie warstwy security DLMS/COSEM w licznikach energii stanowiących przedmiot dostawy. Treść opisu przedmiotu zamówienia w tym zakresie jest niekompletna i niejednoznaczna, co uniemożliwia złożenie prawidłowych i porównywanych ofert. Przede wszystkim wymaganie pkt 3.B.11 tj. określenie wymagania szyfrowania algorytmem AES co najmniej 128 bit, jest sformułowane w sposób niejednoznaczny i niewyczerpujący: Mechanizm AES musi definiować tryb szyfrowania blokowego. Siła algorytmu szyfrującego bazuje na długości klucza oraz trybie szyfrowania blokowego. Przykładowo, jeśli klucz jest nawet długości 256 bitów w trybie ECB (Electronic Codebook), czyni to algorytm bardzo słabym i podatnym na ataki. Tryb ECB nie powinien być używany. Najlepszym rozwiązaniem jest tryb GCM (Galois Counter Mode). Dodatkowo wymaganie samego algorytmu AES nie chroni przed tzw. atakiem zwrotnym (Reply Attack). Wymaganie nie definiuje w żadnym zakresie autentykacji danych podpisu cyfrowego, MAC, itp. Postawione przez zamawiającego wymagania OPZ nie specyfikują dokładnego poziomu bezpieczeństwa. Standard DLMS, który jest powszechnie implementowany w infrastrukturze pomiarowej, definiuje 3 poziomy bezpieczeństwa DLMS Security Suite 0, 1 oraz 2. DLMS Security Suite 0 oznacza wyłącznie szyfrowanie za pomocą symetrycznych kluczy, a DLMS Security 1 oraz 2 - wykorzystanie szyfrowania asymetrycznego o różnej długości klucza i wykorzystanie infrastruktury klucza publicznego (PKI) do autoryzacji, autentykacji oraz szyfrowania. Aby wdrożyć w pełni bezpieczny system komunikacji z licznikami, które mają być wykorzystywane przez kolejne 12 lat, komunikacja DLMS/COSEM musi implementować infrastrukturę klucza publicznego w ramach minimum DLMS Security Suite 1, a najlepiej DLMS Security Suite 2. W ramach asymetrycznego szyfrowania bazującego na PKI wciąż wykorzystywane są symetryczne klucze AES do szyfrowania danych. Infrastruktura PKI służy do uzgadniania symetrycznych kluczy i podpisu cyfrowego, co nie jest możliwe bez infrastruktury PKI. Przy czym, wykorzystywanie infrastruktury klucza publicznego PKI jest bez wątpienia korzystniejszym dla zamawiającego rozwiązaniem: W sytuacji, gdy do zabezpieczenia liczników nie jest wykorzystywana infrastruktury klucza publicznego PKI: Producent liczników musi preinstalować symetryczne klucze inicjalizacyjne w licznikach podczas produkcji. Przynajmniej KEK (Key for Key Encryption) musi zostać zainstalowany. Używając tych inicjalizacyjnych kluczy OSD jest w stanie zmienić te klucze na swoje własne. Pojawia się problem jak przetransportować w bezpieczny sposób te inicjalizacyjne klucze od producenta liczników do zakładu energetycznego. Klucze inicjalizacyjne są wygenerowane przez producenta liczników, więc zakład energetyczny (OSD) nie ma 100% pewności, że nie nastąpił wyciek kluczy. OSD nie ma kontroli nad tym procesem. Każdy kto posiada te klucze inicjalizacyjne może spersonalizować licznik na nowe klucze. Nie ma żadnej autoryzacji tego

procesu. W sytuacji, gdy do zabezpieczenia liczników jest wykorzystywana infrastruktury klucza publicznego PKI: Producent liczników musi preinstalować tzw. kotwicę zaufania („Trust Anchor”) podczas produkcji liczników. To jest klucz publiczny w certyfikacie CA. Certyfikat pochodzi od zakładu energetycznego (OSD). Zakład energetyczny (OSD) posiada klucz prywatny, który jest powiązany z tym kluczem publicznym. Zakład energetyczny (OSD) nie ujawnia nikomu klucza prywatnego. Nawet producent liczników go nie potrzebuje. Producent liczników nie musi instalować żadnych sekretnych kluczy prywatnych na etapie produkcji. „Trust Anchor” CA jest wystarczający. Certyfikat CA jest publiczną informacją. Nie jest wymagany żaden bezpieczny kanał przesyłania CA od zakładu energetycznego (OSD) do producenta liczników. Inny certyfikat (sygnatura, KA) jest wysyłany do licznika. Jest sprawdzany przez CA. Tylko certyfikat podpisany za pomocą prywatnego klucza przez OSD jest akceptowany. Klucze symetryczne są potwierdzane i uzgadniane przez algorytm DH (Diffie-Hellman) pomiędzy licznikiem a systemem HES. Dzięki wykorzystaniu algorytmu DH nikt inny nie zna tych kluczy. Licznik produkowany jest z kluczem publicznym w postaci kotwicy zaufania (Trust Anchor) zakładu energetycznego (OSD). Tylko zakład energetyczny może spersonalizować licznik z wykorzystaniem swojego prywatnego klucza. Aby zabezpieczyć infrastrukturę licznikową należy skorzystać ze standardu bezpieczeństwa, który jest w tym momencie rekomendowany przez DLMS User Association. Zalecane jest wdrożenie DLMS Security Suite 2 z pełną infrastrukturą PKI oraz dłuższymi kluczami 384-bitowymi - tego typu rozwiązanie jest najbezpieczniejsze i powinno stanowić, jeśli nie wymaganie obligatoryjne, to przynajmniej opcjonalny wymóg, dodatkowo punktowany w ramach pozacenowego kryterium oceny ofert. W podstawowej wersji może zostać wykorzystany DLMS Security Suite 1 z pełną infrastrukturą PKI oraz kluczami 256-bitowymi. DLMS Security Suite 0, czyli tylko szyfrowanie symetryczne kluczami AES jest skompromitowane i nie zapewnia żadnego poziomu bezpieczeństwa i nie może być stosowane dla rozwiązań, które mają działać przez kolejne 12 lat. Na rynku istnieje wiele artykułów naukowych, które opisują problem braku bezpieczeństwa w protokole DLMS/COSEM z wykorzystaniem luk w zabezpieczeniach dla DLMS Security Suite 0 (AES128) oraz metody ataków. Wszystkie organizacje rządowe zajmujące się bezpieczeństwem w Europie oraz USA nakazują stosowanie mechanizmów i algorytmów bazujących na tzw. krzywych eliptycznych oraz infrastrukturze klucza publicznego PKI. Dokładnie te mechanizmy implementuje standard DLMS Security Suite 1 oraz DLMS Security Suite 2.

Przystępujący 1 poparł stanowisko odwołującego.

Zamawiający podtrzymał dotychczasowe stanowisko, wniósł o oddalenie odwołania.

W zakresie podtrzymanego przez odwołującego zarzutu zamawiający podniósł, że opis przedmiotu zamówienia powinien odpowiadać uzasadnionym i rzeczywistym potrzebom zakupowym zamawiającego. Określenie wymagań dotyczących przedmiotu zamówienia należy do zamawiającego, który jest gospodarzem postępowania i nabywcą określonego zamówienia. Zamawiający przywołał wyrok Krajowej Izby Odwoławczej z dnia 17 stycznia 2008 r., sygn. akt KIO/UZP 80/07, w którym Izba stwierdziła, iż zamawiający ma prawo opisać swoje potrzeby w taki sposób, aby przedmiot zamówienia spełniał jego wymagania i zaspokajał potrzeby, pod warunkiem, że dokonany opis nie narusza konkurencji ani równego traktowania wykonawców.

Zamawiający podkreślił, że jego wymagania w zakresie bezpieczeństwa dla liczników są zgodne z zapisami rozporządzenia Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. w sprawie systemu pomiarowego oraz najlepszą wiedzą, doświadczeniem i praktyką zamawiającego. Przedmiotowe wymagania są wymaganiami minimalnymi i nie wykluczają urządzeń, które zapewniają wyższy poziom bezpieczeństwa. Zapisy rozporządzenia, o którym mowa powyżej, były konsultowane przed opublikowaniem w szerokim gronie podmiotów zaangażowanych w polską energetykę, w tym z operatorami systemów dystrybucyjnych oraz producentami liczników energii elektrycznej. Zwiększenie wymagań minimalnych w zakresie bezpieczeństwa określonych w rozporządzeniu Ministra Klimatu i Środowiska z dnia 22 marca 2022 r. w sprawie systemu pomiarowego może prowadzić do ograniczenia rynku dla potencjalnych wykonawców. Jednocześnie zastosowanie wyższego poziomu bezpieczeństwa dla oferowanych urządzeń nie eliminuje żadnego z wykonawców. W związku z powyższym zamawiający podtrzymuje wymagania minimalne dla bezpieczeństwa LZO.

Zamawiający podniósł, że odwołujący stawia konkretne wymagania co do opisu przedmiotu zamówienia, natomiast nie wskazuje, jakie konkretne zasady i przepisy P.z.p. naruszył zamawiający opisując przedmiot zamówienia. Zamawiający wskazał, iż nie ma obowiązku dokonywania opisu przedmiotu zamówienia w sposób najbardziej dogodny dla ewentualnych wykonawców. Dopóki odwołujący nie wykaże, że opis przedmiotu zamówienia narusza normy wynikające z ustawy P.z.p., dopóty tej czynności zamawiającego nie można uznać za niezgodną z ustawą P.z.p., nawet jeśli ukształtowanie tych wymagań dla odwołującego czy też innych potencjalnych wykonawców byłoby korzystniejsze czy też bardziej uzasadnione.

W świetle powyższego, zamawiający wniósł o oddalenie zarzutu.

Przystępujący 2 podtrzymał dotychczasowe stanowisko, wniósł o oddalenie odwołania.

Izba ustaliła, co następuje:

W pkt. 2 OPZ zamawiający wymaga wykonania przedmiotu zamówienia zgodnie z normami, a w szczególności z następującymi normami:

2.8. - DLMS UA 1000-2 ED. 10

2.9. - DLMS UA 1000-1 ED. 14

2.10. lub normami je zastępującymi wydanymi odpowiednio przez Polski Komitet Normalizacyjny albo DLMS User Association

36. Komunikacja z licznikiem przez optozłącze oraz wszystkie dostępne elektryczne interfejsy komunikacyjne musi odbywać się wyłącznie w protokole DLMS w wersji co najmniej 14.

W punkcie 3.B ppkt 11 OPZ zamawiający wymaga, aby komunikacja przez optozłącze oraz na innych interfejsach komunikacyjnych miała możliwość szyfrowania algorytmem AES co najmniej 128 bit (HLS) dla protokołu odczytu danych zgodnego z DLMS/COSEM.

W punkcie 3.B ppkt 12 zamawiający wymaga, aby komunikacja bezpośrednia między licznikiem a systemem pomiarowym OSD oraz oprogramowaniem narzędziowym miała możliwość szyfrowania algorytmem AES co najmniej 128 bit (HLS) dla protokołu odczytu DLMS/COSEM na całej ścieżce komunikacji. Wymagane jest uwierzytelnianie licznika podczas nawiązywania komunikacji z systemem pomiarowym OSD oraz oprogramowaniem narzędziowym.

Stan faktyczny Izba ustaliła na podstawie dokumentacji postępowania, w tym w szczególności Opisu Przedmiotu Zamówienia, stanowiącego załącznik nr 1 do specyfikacji warunków zamówienia.

Izba zważyła, co następuje:

Zarzuty 1, 4 oraz 3 w zakresie żądania określonego pkt 3, str. 3 odwołania podlegają umorzeniu na podstawie art. 568 pkt 1 ustawy P.z.p.

Zarzut 2 odwołania podlega umorzeniu na podstawie art. 522 ust. 4 ustawy P.z.p.

W pozostałym zakresie odwołanie jest bezzasadne i podlega oddaleniu.

W pierwszej kolejności Izba stwierdziła, że odwołujący jest uprawniony do korzystania ze środków ochrony prawnej na podstawie art. 505 ust. 1 ustawy P.z.p. Okoliczność ta nie była pomiędzy stronami sporna.

Odwołujący podniósł zarzut naruszenia art. 99 ust. 1, 2 i 4 oraz art. 103 ust. 3 w zw. z 16 pkt 1 i 3 ustawy P.z.p. poprzez opisanie przedmiotu zamówienia w sposób niejednoznaczny i niejasny oraz niedostatecznie wyczerpujący i wewnętrznie sprzeczny, a także nieproporcjonalny do przedmiotu zamówienia i naruszający uczciwą konkurencję, w zakresie dotyczącym wymagań bezpieczeństwa liczników zdalnego odczytu.

Unormowania zawarte w art. 99 ust. 1 i nast. ustawy P.z.p. regulują zasady sporządzania przez zamawiającego opisu przedmiotu zamówienia. Zgodnie z ust. 1, przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty. W myśl ust. 2, zamawiający określa w opisie przedmiotu zamówienia wymagane cechy dostaw, usług lub robót budowlanych. Cechy te mogą odnosić się w szczególności do określonego procesu, metody produkcji, realizacji wymaganych dostaw, usług lub robót budowlanych, lub do konkretnego procesu innego etapu ich cyklu życia, nawet jeżeli te czynniki nie są ich istotnym elementem, pod warunkiem że są one związane z przedmiotem zamówienia oraz proporcjonalne do jego wartości i celów. Stosownie do ust. 4, przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów.

Wskazane wyżej regulacje zamawiający obowiązany jest stosować opisując przedmiot zamówienia. Naruszenie którejkolwiek z nich naraża zamawiającego na zakwestionowanie opisu przedmiotu zamówienia w drodze wniesionego odwołania. Niemniej jednak, dla skuteczności podnoszonych w tym zakresie zarzutów nie wystarczy stwierdzenie, że sporządzony przez zamawiającego opis przedmiotu zamówienia narusza wskazane wyżej przepisy ustawy P.z.p., ale odwołujący winien wykazać słuszność swego stanowiska poprzez odpowiednią argumentację i przedłożenie stosownych wniosków dowodowych.

Tymczasem, w rozpoznawanym przypadku, odwołujący nie uzasadnił swego stanowiska w sposób skuteczny. Odwołujący podniósł, że wymaganie pkt. 3.B.11, tj. określenie wymagania szyfrowania algorytmem AES co najmniej 128 bit, jest sformułowane w sposób niejednoznaczny i niewyczerpujący, ponieważ mechanizm AES musi definiować

tryb szyfrowania blokowego i wymaganie nie definiuje w żadnym zakresie autentykacji danych. Odwołujący zdaje się pomijać okoliczność, że zamawiający wskazał w OPZ na konieczność wykonania zgodnie z protokołem DLMS. Wydaje się, że w sytuacji, w której uczestnikami postępowania o udzielenie zamówienia są profesjonaliści, winni oni znać wszelkiego rodzaju normy i dokumenty zawierające specyfikę wymagań zawartych w dokumentacji przedmiotowego postępowania.

Izba przeprowadziła dowody ze złożonych przez przystępującego 2 dokumentów: „Audyt bezpieczeństwa implementacji protokołu komunikacyjnego DLMS/COSEM Smart Grid" oraz „Raport techniczny. Architektura i protokoły DLSM/COSEM" o skonstatowała, że zawierają one informacje dotyczące trybu szyfrowania blokowego oraz autentykacji danych:

- „Audyt…" Rozdział 2 „Kontekst i powiązane prace": „DLMS/COSEM obsługuje trzy poziomy mechanizmów uwierzytelniania: (…) najniższy (…), niski (…) i wysoki poziom bezpieczeństwa (HLS). (…) Uwierzytelnianie HLS może wykorzystywać jeden z pięciu dostępnych mechanizmów, przedstawionych w tabeli 2.2."

- „Raport…" pkt 9.2.3.7 „Pakiet zabezpieczeń":

„Pakiety zabezpieczeń DLMS/COSEM (…) są oparte na pakiecie NSA Suite B i zawierają algorytmy kryptograficzne do uwierzytelniania, szyfrowania, uzgadniania kluczy, podpisu cyfrowego i mieszania specyficznych dla:

1. uwierzytelnianie i szyfrowanie: stosuje się Advanced Encryption Standard (AES) zgodnie z FIPS PUB 197, z kluczami o rozmiarach 128 i 256 bitów. AES stosuje się z trybem działania Galois/Counter (GCM) określonym w NIST SP 800-38D:2007".

pkt 9.4.2.2.3 „Nazwa mechanizmu uwierzytelniania COSEM"

Uwierzytelnianie klienta, serwera lub obu jest jednym z aspektów bezpieczeństwa uwzględnionych w specyfikacji DLMS/COSEM. Określono trzy poziomy zabezpieczeń uwierzytelniania:

(…)

3. Uwierzytelnianie wysokiego poziomu zabezpieczeń (HLS)…".

Wskazując na powyższe Izba stwierdziła, że zarzut opisania przedmiotu zamówienia w sposób niejednoznaczny i niewyczerpujący, w zakresie, w jakim nie zawiera niezbędnych danych odnośnie trybu szyfrowania blokowego i autentykacji danych, jest nieuzasadniony.

Odwołujący podniósł, że postawione przez zamawiającego wymagania OPZ nie specyfikują dokładnego poziomu bezpieczeństwa. Wskazał, że standard DLMS, który jest

powszechnie implementowany w infrastrukturze pomiarowej, definiuje 3 poziomy bezpieczeństwa DLMS Security Suite 0, 1 oraz 2. DLMS Security Suite 0 oznacza wyłącznie szyfrowanie za pomocą symetrycznych kluczy, a DLMS Security 1 oraz 2 – wykorzystanie szyfrowania asymetrycznego o różnej długości klucza i wykorzystanie infrastruktury klucza publicznego (PKI) do autoryzacji, autentykacji oraz szyfrowania.

Izba nie podziela stanowiska odwołującego, jakoby zamawiający nie określił poziomu bezpieczeństwa. Izba przeprowadziła dowód z dokumentu „Raport techniczny. Architektura i protokoły DLSM/COSEM" pkt 9.2.3.7 „Pakiet zabezpieczeń" tabela 27 – Pakiety bezpieczeństwa DSLM/COSEM i stwierdziła, że pakiet zabezpieczeń AES-GCM-128 odpowiada w protokole DLSM poziomowi Security Suite 0.

W dalszej kolejności odwołujący podniósł, że – aby wdrożyć w pełni bezpieczny system komunikacji z licznikami, które mają być wykorzystywane przez kolejne 12 lat – komunikacja DLMS/COSEM musi implementować infrastrukturę klucza publicznego w ramach minimum DLMS Security Suite 1, a najlepiej DLMS Security 2. Stwierdził, że wykorzystywanie infrastruktury klucza publicznego PKI jest bez wątpienia korzystniejszym dla zamawiającego rozwiązaniem.

Izba wskazuje, że zamawiający ma prawo opisać przedmiot zamówienia w sposób uwzględniający jego uzasadnione potrzeby. Zamawiający realizuje określone cele statutowe i ma najlepszą wiedzę w zakresie tego, w jaki sposób mogą one zostać osiągnięte. To zamawiający jako gospodarz postępowania określa zakres zarówno przedmiotowy, jak i podmiotowy, charakteryzujący cel, jaki zamierza osiągnąć. Zasada swobody kontraktowania uprawnia wykonawców do składania propozycji co do modyfikacji określonych zapisów dokumentacji postępowania, ale zamawiający, w zależności od własnych interesów i potrzeb, może, lecz nie musi ich uwzględniać.

Odwołujący podniósł, że – aby zabezpieczyć infrastrukturę licznikową – należy skorzystać ze standardu bezpieczeństwa, który jest w tym momencie rekomendowany przez DLMS User Association. Wskazał, że zalecane jest wdrożenie DLMS Security Suite 2 z pełną infrastrukturą PKI oraz dłuższymi kluczami 384-bitowymi. W podstawowej wersji może być wykorzystany DLMS Security Suite 1 z pełną infrastrukturą PKI oraz kluczami 256-biotwymi.

Izba nie podziela stanowiska odwołującego. Odwołujący nie udowodnił, że rekomendowanym standardem bezpieczeństwa jest DLMS Security Suite 2. W szczególności nie wynika to ze złożonych przez odwołującego dowodów. Mimo że w treści odwołania odwołujący podnosi, że istnieje szereg artykułów naukowych, które opisują

problem braku bezpieczeństwa w protokole DLMS/COSEM, żaden taki artykuł nie został przez odwołującego przedłożony.

Izba przeprowadziła dowód z dokumentów przedłożonych przez przystępującego 2:

- BSI – Wytyczne techniczne Federalnego Urzędu ds. Bezpieczeństwa Informacji pt. „Mechanizmy kryptograficzne: Zalecenia i długości kluczy"

- „Bezpieczeństwo w DLMS" White Book DLMS User Association

i ustaliła, że wymagany przez zamawiającego standard bezpieczeństwa odpowiada aktualnym wymogom rekomendowanym w tych dokumentach. W szczególności z dokumentu „Mechanizmy kryptograficzne…" wynika, że „W przypadku nowych aplikacji kryptograficznych należy używać tylko szyfrów blokowych, których rozmiar bloku wynosi co najmniej 128 bitów. Następujące szyfry blokowe są zalecane do stosowania w nowych systemach kryptograficznych: AES-128…" (str. 25). Z kolei dokument „Bezpieczeństwo w DLMS" zawiera informację na temat oferowania przez DLMS trzech zestawów zabezpieczeń (pakiety bezpieczeństwa 0, 1 i 2) i wskazuje, że „Koncepcja pakietów bezpieczeństwa zapewnia, że specyfikacja bezpieczeństwa DLMS jest gotowa na przyszłość: mechanizmy bezpieczeństwa mogą być używane w ten sam sposób z nowymi pakietami bezpieczeństwa, które mogą być dodane w przyszłości, aby dotrzymać kroku najnowszym osiągnięciom kryptografii".

Odwołujący na rozprawie w dniu 21 czerwca 2022 roku złożył jako dowód w sprawie wyciąg z przepisów rozporządzenia Ministra Klimatu i Środowiska z dnia 22 marca 2022 roku w sprawie systemu pomiarowego (Dz. U. poz. 788) m.in. na okoliczność wykazania, że cały system pomiarowy powinien umożliwiać podnoszenie (upgrade) poziomu bezpieczeństwa do wyższych standardów, podczas gdy w wymaganiach OPZ dla liczników nie przewidziano takiej możliwości.

Izba wskazuje, że ten zarzut nie został podniesiony w treści odwołania, zatem Izba – na zasadzie art. 555 ustawy P.z.p. – nie mogła tego zarzutu rozpoznać.

Wskazane wyżej rozporządzenie zostało złożone również na okoliczność wykazania, że należy kierować się odpowiednimi normami technicznymi, co w przypadku wymagania wykorzystywania przez liczniki oferowane w postępowaniu protokołu DLMS/COSEM wskazuje, że powinno się stosować standard opisu warstwy bezpieczeństwa zgodny z tą normą, czyli DLMS Security Suite 0, 1 i 2. Na tę okoliczność odwołujący przedłożył również dowody: wyciąg z dokumentu „Zabezpieczenie i ochrona prywatności systemów informatycznych oraz organizacji", wyciąg z dokumentu „Bezpieczeństwo w DLMS", wyciąg z

dokumentu „Wymagania bezpieczeństwa dla zamawianych liczników energii i koncentratorów danych”

Izba przenalizowała wskazane wyżej dowody i skonstatowała, że okoliczności, na jakie zostały one złożone, nie budzą wątpliwości. Niemniej jednak Izba ponownie podkreśla, że zamawiający w treści OPZ zawarł wymagane w tym zakresie informacje, na co wskazuje treść pkt. 3.B 11 i 12 OPZ.

Odwołujący wskazał również na załącznik nr 1 do rozporządzenia „Minimalne wymagania techniczno-funkcjonalne dla liczników zdalnego odczytu. Bezpieczeństwo – kategoria 1 (kolumna pierwsza), pkt 10.4, 10.5 i 10.12 na okoliczność wykazania, że opisane wymagania w zakresie uwierzytelniania, autoryzacji, certyfikatów oraz zabezpieczenia przed powielaniem i modyfikacją danych, są możliwe tylko w przypadku zastosowania infrastruktury klucza publicznego, opisanego w wymaganiach DLMS Security Suite 1 oraz 2.

Zgodnie z pkt. 10.4 załącznika:

„Dostęp do wszystkich interfejsów komunikacyjnych licznika zdalnego odczytu jest realizowany wyłącznie po uwierzytelnieniu. W przypadku interfejsu komunikacyjnego, o którym mowa w pkt. 7.3.2. jest wymagane szyfrowanie komunikacji”

Zgodnie z pkt. 10.5 załącznika:

„Licznik zdalnego odczytu ma funkcjonalność zdalnej i lokalnej zmiany certyfikatu (klucza) do uwierzytelniania na poszczególnych interfejsach komunikacyjnych.”

Zgodnie z pkt. 10.12 załącznika:

„Każde polecenie przesyłania między systemem zdalnego odczytu a licznikiem zdalnego odczytu ma zabezpieczenie przed powieleniem, repliką oraz modyfikacją”.

Izba przeanalizowała wskazane pozycje i nie stwierdziła, by zawierały one wymóg zastosowania klucza publicznego. Zawierają one wymogi w zakresie uwierzytelniania i szyfrowania komunikacji, jednakże bez wskazania na konieczność wykorzystywania do tego klucza publicznego.

Izba wskazuje natomiast na pozycję 10.11 tegoż załącznika, z którego wynika konieczność zapewnienia „Dwukierunkowej komunikacji między systemem zdalnego odczytu a licznikiem zdalnego odczytu jest uwierzytelniana i szyfrowana algorytmem o długości klucza 128 bitów według specyfikacji AES lub równoważnej zapewniającej ten sam lub wyższy poziom bezpieczeństwa.” Uwarunkowania te zamawiający uwzględnił w pkt. 3.B 11 i 12 OPZ Tym samym zarzut niezgodności zapisów OPZ z przepisami rozporządzenia należy uznać za nieuzasadniony.

Izba odmówiła przeprowadzenia dowodów z dokumentacji z innych postępowań o udzielenie zamówienia publicznego z uwagi na fakt, że nie mają one istotnego znaczenia dla rozstrzygnięcia sprawy (argumentacja *a contrario* z art. 531 ustawy P.z.p.). Izba wskazuje, że przedmiotem rozstrzygnięcia jest ustalenie, czy czynności zamawiającego nie naruszają przepisów ustawy. Wymaga to ustalenia stanu faktycznego i jego skonfrontowania z normami prawnymi. Okoliczność, że w innych postępowaniach zamawiający dokonywali analogicznych lub innych czynności nie ma wpływu na ustalenie, czy w rozpoznawanym przypadku czynności zamawiającego są zgodne z prawem.

Z uwagi na powyższe orzeczono jak na wstępie.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 575 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych, stosownie do wyniku postępowania oraz na podstawie § 8 ust. 2 pkt 1 w zw. z § 9 ust. 3 pkt 2 rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz. U. z 2020 r. poz. 2437).

Przewodniczący: ……

……

……